

Redes Locales

CFGs

Unidad 3 – Introducción a las Redes



Índice

1. Introducción.....	4
2. Conceptos importantes.....	4
2.1. Comunicación, extremo, mensaje.....	4
2.2. Señal.....	4
2.3. Emisor y receptor – Equipo Transistor de Datos (ETD).....	5
2.4. Medio.....	5
2.5. Transmisión.....	5
2.6. Código.....	6
2.7. Comunicación (ampliación).....	6
2.8. Datos e información.....	6
2.9. Línea.....	7
2.10. Ancho de banda, capacidad, bps, Kbps, Mbps, Tbps.....	7
2.11. Nodo.....	7
2.12. Estándar.....	8
2.13. Líneas de comunicación. Circuitos.....	8
2.14. Topología.....	9
2.14.1. Topología en Bus.....	9
2.14.1. Topología en Anillo.....	10
2.14.2. Topología en Estrella.....	11
2.14.3. Otras topologías de red.....	12
2.14.4. Topología de Malla.....	12
2.14.5. Topología en Árbol.....	13
2.14.6. Topología de Interconexión Total.....	13
3. Tipos de transmisión y comunicación.....	14
3.1. Analógica y digital.....	14
3.2. En banda base y Modulada.....	14
3.3. Serie y paralelo.....	15
3.3.1. Paralelo.....	15
3.3.2. Serie.....	15
3.4. Sincronismo.....	16
3.4.1. Transmisión asíncrona.....	16
3.4.2. Transmisión sincrónica.....	16
3.5. Simplex, dúplex, semi-dúplex.....	17
3.5.1. Simplex.....	17
3.5.2. Duplex o Semi-dúplex.....	17
3.5.3. Full Duplex.....	17
3.6. Problemas de transmisiones.....	18
3.6.1. Atenuación.....	18
3.6.2. Ruido.....	18
3.6.3. Identificador del emisor y receptor.....	18
3.6.4. Entramado.....	19
3.6.5. Control de errores.....	19
3.6.6. Colisiones.....	19
3.6.7. Control del medio.....	20

3.6.8. Congestión.....	20
3.7. Tasa de transmisión.....	20
4. Servicios.....	20
4.1. Con y Sin Acuse de recibo.....	21
4.2. Con y Sin Conexión.....	21
4.3. Encaminamiento o rutado.....	22
5. Componentes de una red informática.....	22
5.1. Clasificación de los medios de transmisión.....	23
5.2. Cableado y conectores.....	24
5.2.1. Cableado estructurado.....	25
5.3. Elementos de interconexión.....	26
5.4. Tarjetas de red y direccionamiento MAC.....	27
5.5. Conmutadores (switch).....	28
5.6. Router o enrutador.....	30
5.7. IDS.....	31
6. Redes inalámbricas 802.11.....	32
6.1. Tipos de redes 802.11 - Características.....	33
6.2. El SSID de una red 802.11.....	34
6.3. Seguridad en 802.11.....	35
7. Direccionamiento IP.....	37
7.1. Clases de direcciones IP.....	37
7.2. Tipos de direcciones IP.....	39

1. Introducción

La introducción a los sistemas telemáticos destaca la importancia de comprender ciertos términos clave en redes para facilitar el aprendizaje del curso. Algunas palabras pueden tener significados distintos para los informáticos en comparación con el uso cotidiano.

2. Conceptos importantes

Todas estas palabras tienen significados relacionados con la comunicación, ya sea entre personas o entre máquinas.

2.1. Comunicación, extremo, mensaje

Un **mensaje** es la información que se transmite de un dispositivo a otro dentro de una red. Puede incluir datos, comandos o cualquier otro tipo de contenido digital.

La **comunicación** es el proceso de intercambio de mensajes entre dos o más dispositivos dentro de la red. Está implicada tanto en el envío y como en la recepción de información siguiendo ciertos protocolos.

Los **extremos** son los dispositivos que actúan como punto de origen o destino en una comunicación dentro de la red, como ordenadores, servidores o impresoras conectadas.

2.2. Señal

Una señal es una **magnitud física** que varía en el tiempo y puede medirse, como el voltaje, la corriente o las ondas electromagnéticas. En redes locales, las señales transportan información en forma de ceros y unos (binario). Sin embargo, no todas las señales son útiles para la comunicación, ya que pueden sufrir interferencias o degradación. Para que una señal sea efectiva, debe propagarse adecuadamente a través del medio de transmisión y conservar su integridad hasta llegar al extremo receptor.

2.3. Emisor y receptor – Equipo Transistor de Datos (ETD)

En una **comunicación entre dos dispositivos** dentro de una red, la transmisión de señales tiene un origen y un destino. El dispositivo que genera y envía las señales se denomina emisor, mientras que el dispositivo que recibe estas señales y las interpreta es el receptor. A través de estas señales viaja el mensaje que transporta la información.

En algunos casos, el emisor no conoce de antemano al receptor, o puede enviar la señal a múltiples destinatarios (difusión o multidifusión). Cuando la comunicación es bidireccional, es decir, el receptor también puede enviar respuestas al emisor, ambos dispositivos cumplen ambas funciones y se denominan Equipos Transmisores de Datos (ETD).

2.4. Medio

El **medio** es el soporte físico o material a través del cual viajan las señales que transportan los datos. Este medio puede ser un cable metálico para señales eléctricas, el aire o el espacio para señales inalámbricas, o una fibra óptica para señales luminosas.

2.5. Transmisión

La **transmisión** es el proceso mediante el cual se transportan señales de un lugar a otro. Estas señales son entidades de naturaleza diversa que se manifiestan como magnitudes físicas, principalmente electromagnéticas o mecánicas, como señales luminosas, eléctricas o acústicas.

Los parámetros de cualquier transmisión son siempre magnitudes físicas, tales como tensión, intensidad de corriente, presión, frecuencia y amplitud.

2.6. Código

El código es un conjunto de **normas, símbolos y convenios** que define la forma en que un mensaje debe estructurarse y transmitirse para que el emisor y el receptor logren una comunicación efectiva y un entendimiento mutuo. El código establece limitaciones sobre cómo se debe representar la información durante la transmisión, lo que puede restringir los matices o detalles que se pueden comunicar.

2.7. Comunicación (ampliación)

En todo **proceso de comunicación**, siempre hay transmisión de señales, pero no siempre que exista transmisión de señales se está llevando a cabo una comunicación efectiva.

La comunicación se define como la transmisión de señales mediante un código común entre el emisor y el receptor, con el objetivo de transmitir un mensaje del emisor al receptor. En este contexto, podemos decir que la señal es a la transmisión lo que la información es a la comunicación.

2.8. Datos e información

Datos son hechos individuales o cifras que, por sí solos, no tienen un significado claro o utilidad directa. Estos hechos pueden ser números, observaciones o cualquier otro tipo de representación que, aislada, no aporta contexto ni valor interpretativo.

Información, por otro lado, es el conjunto de datos organizados y relacionados de manera que adquieren un significado o valor. La información proporciona un contexto que permite comprender, interpretar y extraer conclusiones útiles a partir de los datos.

2.9. Línea

Una **línea** es el conjunto de medios de transmisión a través de los cuales viaja una señal desde un punto a otro. No necesariamente va desde el origen al destino final.

2.10. Ancho de banda, capacidad, bps, Kbps, Mbps, Tbps

El ancho de banda y la capacidad se utilizan para medir o categorizar la cantidad de datos que pueden transmitirse a través de un medio de comunicación en una unidad de tiempo. Las **unidades comunes para medir** esto incluyen bps (bits por segundo), Kbps (kilobits por segundo), Mbps (megabits por segundo) y Tbps (terabits por segundo).

A mayor ancho de banda, mayor es la capacidad de transmisión en el medio de comunicación y en los dispositivos que forman la red. Cada equipo y línea de comunicación tiene un flujo máximo de datos que puede soportar. La importancia del ancho de banda depende del tipo de uso de la red.

2.11. Nodo

En una comunicación prolongada, el emisor y el receptor pueden intercambiar sus roles constantemente, actuando ambos de manera similar. En estos casos, los dispositivos involucrados en la comunicación se denominan nodos.

Un **nodo** es cualquier dispositivo dentro de una red que puede emitir, recibir o retransmitir señales e información. Este término se usa para diferenciar estos dispositivos de los medios de transmisión, como los cables, que solo transportan datos sin procesarlos.

Además, en muchas redes existen nodos intermedios que retransmiten la información para asegurar que llegue correctamente de un punto a otro. Estos nodos pueden ser *enrutadores*, *switches* o *repetidores*.

2.12. Estándar

El **proceso de comunicación** requiere que fabricantes, organismos internacionales y Estados acuerden cómo se llevará a cabo la comunicación, tanto a nivel físico como lógico. Para lograrlo, se establecen normas que los fabricantes pueden o deben seguir, definiendo los requisitos que deben cumplir sus equipos para garantizar la interoperabilidad.

En algunos casos, son los propios fabricantes quienes proponen normas para sus equipos, que luego pueden ser adoptadas y estandarizadas por asociaciones especializadas. En otras ocasiones, las asociaciones de estándares son las que desarrollan y establecen estas normativas.

Existen dos tipos de estándares:

- **Estándar de hecho:** aceptado por el mercado por su uso generalizado. (TCP-IP)
- **Estándar de derecho:** propuesto por una asociación de estándares a los fabricantes (OSI).

2.13. Líneas de comunicación. Circuitos

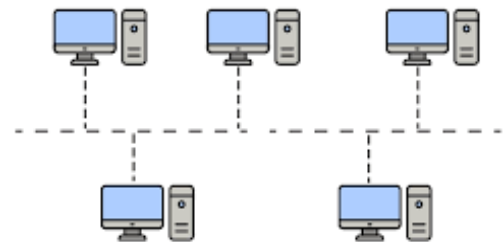
Las líneas de comunicación son los **medios físicos** que transportan o por los que se transmiten las señales que forman una transmisión, cuando se considera una extensión grande. En sistemas más complejos, las líneas de comunicación pueden incluir cables de *fibra óptica*, *cables coaxiales* o *enlaces satelitales*, dependiendo del tipo de transmisión.

2.14. Topología

La **topología de una red** se refiere a la forma en que están organizados e interconectados los nodos y las líneas de comunicación dentro de un sistema. Cuando varios emisores y receptores deben estar conectados, los enlaces entre ellos pueden seguir distintos patrones estructurados y ordenados, lo que define la topología de la red.

2.14.1. Topología en Bus

En la **topología en bus**, todos los nodos comparten un único medio de transmisión (bus) que funciona como un canal de comunicación multipunto. Los dispositivos se conectan al bus y envían mensajes que son recibidos por todos, pero solo el nodo con la dirección correspondiente los procesa.



Sus características principales son las siguientes:

- El bus tiene una estructura lineal.
- Es una topología multipunto donde todos los nodos comparten el mismo canal.
- Los mensajes viajan a través del bus hasta alcanzar el destinatario adecuado.
- Los dispositivos requieren un mínimo nivel de inteligencia para reconocer su propia dirección y procesar los mensajes.

Ventajas de la topología de bus:

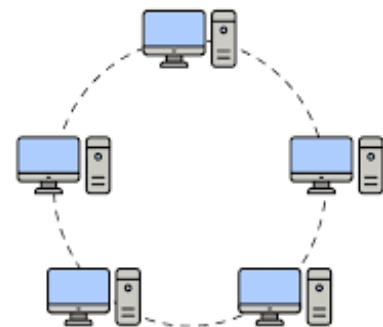
- ✓ Fácil instalación y expansión donde comparten un mismo canal.
- ✓ Eficiencia en redes más pequeñas.
- ✓ Medio de transmisión pasivo, de forma que reduce el consumo energético.

Desventajas de la topología de bus:

- ✗ Cuello de botella, es decir que comparten el mismo canal de transmisión.
- ✗ Tiene alta probabilidad de vulnerabilidad, de forma que el cable principal puede hacer que la red falle.
- ✗ Se limita la longitud del medio de transmisión en distancia máxima que puede cubrir.

2.14.1. Topología en Anillo

La **topología en anillo** se caracteriza porque cada nodo está conectado directamente con dos nodos adyacentes, formando un circuito cerrado. El último nodo está conectado al primero, completando así el anillo.



Ventajas la topología de anillo:

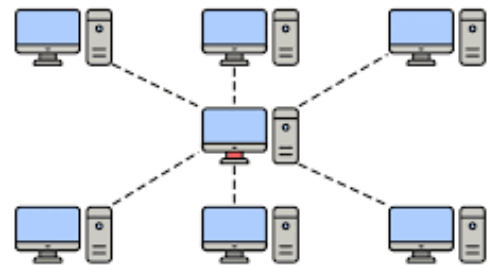
- ✓ Evitan colisiones ya que el medio está controlado en el canal.
- ✓ Tiene buen rendimiento en redes con un tráfico alto sobre le flujo de datos constante.
- ✓ Estructura organizada y facilita la gestión de la red

Desventajas de la topología de anillo:

- ✗ Puede tener fallos en el nodo e interrumpir a toda la red.
- ✗ Dificulta la expansión si se quiere agregar o quitar algún dispositivo.
- ✗ Tiene mayor latencia por lo que los datos deben pasar por todos los nodos antes de llegar al destino.

2.14.2. Topología en Estrella

En la **topología en estrella**, todos los nodos de la red están conectados a un dispositivo central, conocido como concentrador o hub. Este nodo central actúa como intermediario, gestionando la comunicación entre los demás dispositivos.



Ventajas la topología de estrella:

- ✓ Fácil detección y solución de fallos, ya que cada nodo tiene una conexión independiente.
- ✓ Mayor estabilidad, un fallo en un nodo no afecta al resto de la red.
- ✓ Escalabilidad, permite agregar o eliminar nodos sin afectar la red global.

Desventajas de la topología de estrella:

- ✗ Dependencia del nodo central, si el concentrador falla, toda la red deja de funcionar.
- ✗ Mayor consumo de cableado, ya que cada nodo requiere una conexión individual al concentrador.

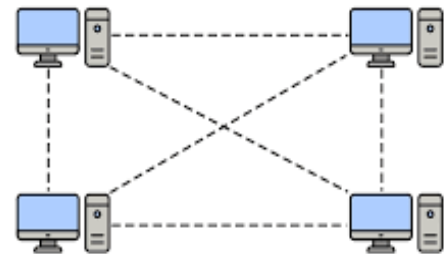
- ✗ Costo más alto, debido a la necesidad de un dispositivo central y más cables.

2.14.3. Otras topologías de red

En ocasiones, y para aplicaciones muy específicas, se utilizan topologías más complejas que permiten conexiones múltiples entre distintos equipos.

2.14.4. Topología de Malla

La **topología de malla** se caracteriza porque todos los nodos están interconectados entre sí, formando una estructura de múltiples caminos para la transmisión de datos.



Ventajas la topología de malla:

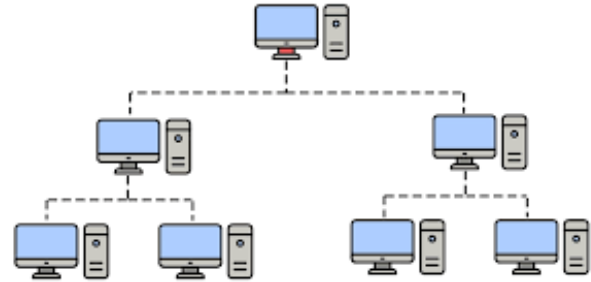
- ✓ Alta redundancia y fiabilidad, ya que existen múltiples caminos alternativos.
- ✓ Evita puntos únicos de fallo, mejorando la estabilidad de la red.
- ✓ Mayor seguridad, porque los datos pueden viajar por rutas alternativas en caso de ataques o fallos.

Desventajas de la topología de malla:

- ✗ Alto costo y complejidad, requiere más cableado y hardware.
- ✗ Configuración y mantenimiento difíciles, debido a la gran cantidad de conexiones.
- ✗ Mayor latencia en redes grandes, porque los datos pueden recorrer múltiples rutas antes de llegar a su destino.

2.14.5. Topología en Árbol

La **topología en árbol** es una extensión de la topología en bus, en la que un bus troncal (línea principal) actúa como el eje central desde donde se ramifican varias subredes o segmentos de red.



Ventajas la topología de árbol:

- ✓ Fácil expansión, permite agregar nuevas subredes sin afectar la estructura general.
- ✓ Organización jerárquica, facilita la gestión y control de la red.
- ✓ Mayor eficiencia en comparación con una red completamente en bus.

Desventajas de la topología de árbol:

- ✗ Dependencia del bus troncal, si falla, toda la red se ve afectada.
- ✗ Mayor uso de cableado en comparación con una topología en bus simple.
- ✗ Mayor complejidad en la instalación y mantenimiento.

2.14.6. Topología de Interconexión Total

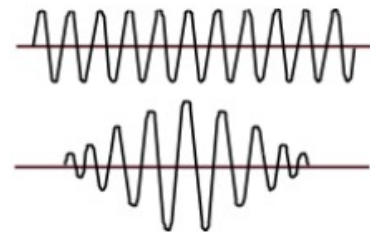
El funcionamiento consiste en conectar todos los ordenadores de una red entre sí a través de líneas punto a punto. Se utiliza una cantidad de recursos necesarios aunque es más segura.

3. Tipos de transmisión y comunicación

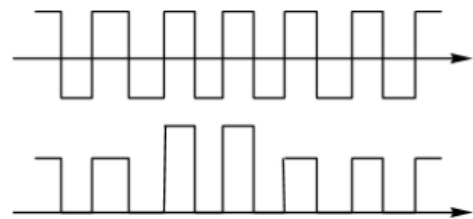
Es una estructura definida para un sistema operativo, además del funcionamiento interno del sistema. El kernel es el núcleo del sistema, se encarga de gestionar los recursos hardware, como la CPU, memoria y los dispositivos de entrada/salida.

3.1. Analógica y digital

- **Transmisión analógica:** La señal es capaz de tomar todos los valores en un rango. Tiene forma de onda.



- **Transmisión digital:** Sólo puede tomar un conjunto finito de valores. Tiene forma de escalones porque sólo se mantiene a unos niveles concretos, y el cambio entre esos niveles es brusco.



3.2. En banda base y Modulada

- **Transmisión en banda base:** se transmite la señal original sin modificaciones ni alteraciones. Es común en redes locales (LAN) donde no es necesario adaptar la señal para su transmisión.
- **Transmisión en banda ancha o modulada:** la señal es sometida a un proceso de modulación, que la combina con otra señal para facilitar su transporte. Durante este proceso, una característica de la señal (amplitud, fase o frecuencia) es alterada de acuerdo con otra señal llamada señal moduladora.

Los tipos de modulación son los siguientes:

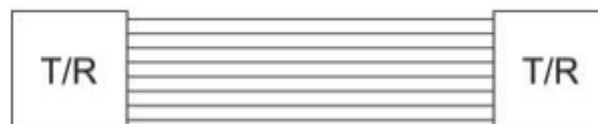
- **Señal moduladora:** Representa lo que se quiere transmitir. No puede viajar por el medio con facilidad. Tiene cambios pertinentes a medida que la señal se va transmitiendo.
- **Señal portadora:** La señal que puede viajar por el medio con facilidad.
- **Señal modulada:** Es la resultante de unir ambas según la modulación elegida, contiene la información de la modulada y la facilidad de transmisión de la portadora.

3.3. Serie y paralelo

La comunicación en los medios informáticos se realiza de dos maneras en cuanto a la transmisión simultánea de bits

3.3.1. Paralelo

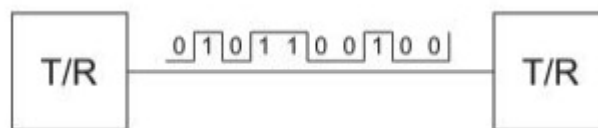
Todos los bits se **transmiten simultáneamente** cada cual por un hilo diferente. Este tipo de transmisión tiene lugar en el interior de una máquina o entre máquinas cuando la distancia es muy corta. La principal ventaja de este modo de transmitir datos es la velocidad de transmisión y la mayor desventaja es el costo del cableado necesario.



3.3.2. Serie

En este caso de que los **números de bits** se compongan de un mensaje se **transmiten uno detrás de otro por la misma línea**.

A la salida de una máquina los datos en paralelo se convierten los datos en serie, los mismos se transmiten y luego en el receptor tiene lugar el proceso inverso, volviéndose a obtener los datos en paralelo. La secuencia de bits transmitidos es por orden de peso creciente y generalmente el último bit es de paridad. Habitualmente se usa la transmisión en serie por ser más económica.



3.4. Sincronismo

El **sincronismo** en la transmisión serie se refiere al proceso mediante el cual el transmisor y el receptor coordinan el momento exacto para leer los bits correctamente. Esto incluye tanto la identificación de los ceros y unos de los bits como el reconocimiento del inicio y final de la transmisión.

3.4.1. Transmisión asíncrona

En la transmisión **asíncrona**, la señal no está sincronizada con un reloj fijo y se transmite de forma desencadenada o sin un ritmo constante. En este tipo de transmisión, cada carácter o bloque de datos se envía de manera independiente, sin necesidad de que el transmisor y receptor estén sincronizados continuamente.

3.4.2. Transmisión sincrónica

La transmisión **sincrónica** es un tipo de comunicación en la que tanto el **transmisor** como el **receptor** deben estar sincronizados, utilizando la **misma frecuencia de reloj**.

En este caso, la información se transmite en **bloques**, y para indicar el **inicio** y el **fin** de cada bloque, se utilizan **delimitadores** específicos.

3.5. Simplex, dúplex, semi-dúplex

Existen canales de comunicación por los que viajan los datos.

3.5.1. Simplex

La comunicación **simplex** es unidireccional, lo que significa que solo hay un transmisor y un receptor claramente definidos. En este tipo de comunicación, la información fluye en una única dirección. Un ejemplo común de comunicación simplex son las redes de radiodifusión, como la radio, donde los oyentes solo reciben información del periodista sin poder enviar ningún dato de vuelta al transmisor.

3.5.2. Duplex o Semi-dúplex

En la comunicación **duplex o semi-dúplex**, ambos extremos (transmisor y receptor) pueden alternarse entre transmitir y recibir datos, pero no simultáneamente. Es decir, ambos pueden comunicarse en ambas direcciones, pero uno debe esperar a que el otro termine de transmitir antes de poder responder. Este tipo de comunicación es común en la interacción entre terminales y computadoras centrales.

3.5.3. Full Duplex

La comunicación **full duplex** permite que los datos se transmitan en ambos sentidos de forma simultánea. Para que esto suceda, ambos dispositivos deben tener medios separados

para la transmisión (por ejemplo, frecuencias diferentes o dos caminos de comunicación distintos). Este tipo de comunicación es más eficiente que el semi-duplex, ya que permite una transmisión continua en ambas direcciones al mismo tiempo.

3.6. Problemas de transmisiones

Hay problemas en la comunicación entre las redes de ordenadores y esos problemas pueden ser resueltos. (distorsión no).

3.6.1. Atenuación

La **atenuación** es la disminución de la intensidad de una señal a medida que viaja a través de un medio de transmisión. Cuanto mayor sea la distancia que recorre la señal, mayor será la atenuación. Además limita las distancias a las que puede realizarse una transmisión eficiente, lo que obliga a elegir medios y materiales con baja atenuación o a instalar equipos adicionales, como repetidores, para amplificar la señal.

3.6.2. Ruido

El **ruido** es una señal no deseada que se mezcla con la señal transmitida y viaja a la par con ella. Tanto la señal deseada como el ruido son captados por el receptor, lo que puede causar errores al intentar interpretar la señal y convertirla en datos.

3.6.3. Identificador del emisor y receptor

Cada vez que se **realiza una comunicación**, el emisor debe incluir un dato adicional junto con el mensaje para identificarse. Esto permite que el receptor sepa quién es el

origen del mensaje. Además, el mensaje debe especificar para qué equipo o receptor está destinado.

3.6.4. Entramado

El **entramado** se refiere a la dificultad que puede tener el receptor para saber cuándo comienza y termina una transmisión. Esto sucede cuando no hay una señal clara que indique el inicio y el fin del mensaje. Se puede confundir con el sincronismo, que tiene que ver con la diferenciación precisa de un bit del siguiente. En algunos casos, las técnicas usadas para lograr el sincronismo también pueden solucionar el problema del entramado.

3.6.5. Control de errores

El **control de errores** es un conjunto de técnicas empleadas para detectar y corregir cualquier error que pueda surgir durante la transmisión de la señal, alterando el mensaje original. Se tiene un control sobre los errores de manera que permita corregir, verificar los errores durante la transmisión de los mensajes.

3.6.6. Colisiones

Una **colisión** ocurre cuando dos o más dispositivos intentan transmitir simultáneamente en el mismo canal de comunicación, causando interferencias que impiden la correcta transmisión de las señales. Las colisiones son frecuentes en sistemas donde varios dispositivos comparten el mismo medio de transmisión, como en las redes Ethernet tradicionales.

3.6.7. Control del medio

El **control del medio** es un conjunto de técnicas que gestionan la transmisión de datos entre diferentes emisores que comparten el mismo medio de comunicación. Este control asegura que las transmisiones no se solapen en el tiempo, evitando colisiones.

3.6.8. Congestión

La **congestión** ocurre cuando los nodos intermedios de una red reciben más mensajes de los que pueden procesar y reenviar. Estos nodos intermedios actúan como retransmisores que gestionan el flujo de información entre diferentes puntos de la red. Si la carga de trabajo es excesiva, los nodos pueden comenzar a retener paquetes en memoria hasta que puedan ser procesados y reenviados. Sin embargo, la memoria de estos nodos es limitada, por lo que si se sobrecarga, algunos paquetes podrían perderse.

3.7. Tasa de transmisión

Se suele medir en (Kilo/Mega/Giga/Tera)BitsPorSegundo (bps) **indicando el número de bits** que puedan atravesar una parte del medio durante el segundo. Esos bits no solo son datos por los que se transmiten a través de los ordenadores, sino metadatos y la sincronización, el control de errores,... de manera que produzcan un rendimiento en la comunicación.

4. Servicios

Es una estructura definida para un sistema operativo, además del funcionamiento interno del existe

4.1. Con y Sin Acuse de recibo

Cuando se comunican dos ordenadores pueden hacerlo de dos formas distintas:

- **Estableciendo una conexión estable y acordada** que se mantiene durante un tiempo. La comunicación es bidireccional (para que los datos puedan transmitirse según haya iniciado la conexión a otro que lo ha recibido). Durante ese tiempo que mantiene la conexión, los ordenadores están listos para enviar o recibir cuando haga falta.
- **Enviando un mensaje sin establecer una conexión** previa. El mensaje cuando es enviado y no hay un proceso previo para establecer ninguna conexión. Se emite un mensaje de aviso de forma que emita la respuesta.

4.2. Con y Sin Conexión

- **Con conexión**, se establece un canal de comunicación entre los dispositivos antes de que se transmitan los datos. Este tipo de comunicación se asegura de que ambos dispositivos estén listos para la transmisión y recepción de datos. La conexión se mantiene durante el proceso de transmisión, y se pueden gestionar aspectos como el control de errores y la sincronización. Un ejemplo de comunicación con conexión es la telefonía móvil o TCP (Transmission Control Protocol), que asegura que los datos lleguen en el orden correcto y sin errores.
- **Sin conexión**, en este tipo de comunicación, no se establece un canal previo. Los datos se envían en forma de paquetes, sin establecer una conexión persistente entre los dispositivos. Un ejemplo de comunicación sin conexión es el UDP (User Datagram Protocol), que permite enviar datos sin garantizar que el receptor esté listo o que los datos lleguen correctamente.

4.3. Encaminamiento o rutado

El **encaminamiento** o **rutado** es el proceso por el cual los paquetes de datos viajan desde el origen hasta el destino a través de una red. Implica la toma de decisiones sobre qué ruta seguir en función de la red, el tráfico, la disponibilidad de nodos intermedios y otros factores.

5. Componentes de una red informática

Todas estas palabras tienen significados relacionados con la comunicación, ya sea entre personas o entre máquinas.

Algunos componentes son:

- ✓ **Cableado de red y conectores** son los que permiten la transmisión de las señales.
- ✓ **Rack o armario** de conexiones son ellos que están puestos para organizar las distintas conexiones que hay en la red. De forma que transmiten las conexiones por la red.
- ✓ **Patch panel** son paneles de conexión del ordenador de distintos ordenadores.
- ✓ **Tarjetas de red** se encargan de permitir la conexión del ordenador, o bien por cable o de manera inalámbrica.
- ✓ **Conmutadores o switch** permiten que la conexión pueda estar en diferentes ordenadores entre sí.
- ✓ **Enrutadores o router** son los que permiten conectar redes diferentes a través de ellos.
- ✓ **Puntos de acceso** permiten la interconexión de los dispositivos cableados o la conexión de dispositivos inalámbricos.

- ✓ **Cortafuegos** pueden ser dispositivos de hardware con un software específico para bloquear el acceso a los no autorizados en la red o software específico de los accesos que no son autorizados.
- ✓ **Servidores** son superordenadores que tienen un sistema operativo específico.

Además de estos componentes, también se consideran parte de la red los ordenadores que trabajan en ella, conocidos como estaciones de trabajo. Cualquier otro dispositivo que se conecte a la red y brinde algún servicio, como impresoras o discos duros de red, también es considerado un componente de la red. Este dispositivo que proporciona servicio y se conecta a un ordenador de la red es llamado nodo de red.

5.1. Clasificación de los medios de transmisión

El medio de transmisión es el canal que permite la comunicación de información entre dos **terminales en un sistema de transmisión**. En redes de ordenadores, estos medios transmiten la información entre nodos como ordenadores, servidores, etc. Las transmisiones suelen realizarse mediante ondas electromagnéticas que se propagan a través de estos canales.

Dependiendo de cómo se transmiten las ondas, los medios de transmisión se dividen en:

- ✓ **Medios guiados:** son los que conducen las ondas electromagnéticas a través de un camino físico, como cables. Los tipos más comunes de cables guiados como el par trenzado, coaxial, fibra óptica,...
- ✓ **Medios no guiados:** son los que no dirigen las ondas electromagnéticas, sino que permiten que se propaguen a través del aire o el vacío. Esto habilita la transmisión inalámbrica, como las redes Wi-Fi, telefonía móvil o la conexión a Internet móvil.

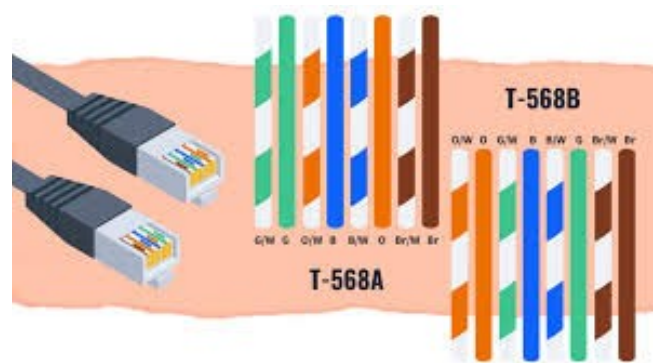
5.2. Cableado y conectores

El cableado y los conectores son **componentes esenciales en las redes de comunicación**, ya que permiten la transmisión de datos entre dispositivos. Existen diferentes tipos de cables, como el par trenzado, el cable coaxial y la fibra óptica, cada uno con características específicas que se adaptan a distintas necesidades de velocidad, distancia y resistencia a interferencias.

PAR TRENZADO

Es el cable más común para conectar los distintos dispositivos para obtener internet.

El estándar que se utiliza es 802.3 (Ethernet). Se utiliza el cableado de RJ-45, conectores tanto macho como hembra. Está formado por pares de cables de cobre trenzados, lo que reduce la interferencia externa y mejora la calidad de la señal.



CABLE COAXIAL

Es un cable que está compuesto de un hilo conductor central, llamado núcleo y una estructura formada por alambres de acero, separados por un aislante, seguido por una malla de alambres de acero que actúan como blindaje para proteger la señal de interferencias externas. Este tipo de cable es comúnmente utilizado en conexiones de televisión por cable y algunas redes de datos.



FIBRA ÓPTICA

Es un medio de transmisión avanzado que utiliza hilos de vidrio o plástico para transmitir datos a través de pulsos de luz. Su principal ventaja es la alta velocidad de transmisión y la capacidad de enviar datos a largas distancias sin pérdida significativa de señal, siendo muy utilizada en redes de alta velocidad y telecomunicaciones.



5.2.1. Cableado estructurado

Es la **infraestructura de telecomunicaciones** que conecta un edificio o conjunto de edificios. Incluye cables, conducciones, armarios, regletas y otros dispositivos esenciales. Este sistema se organiza en varios subsistemas para facilitar la instalación y gestión del cableado.

Algunos de los subsistemas clave son:

- **Cableado de campus:** Interconexión entre edificios.
- **Entrada de edificio:** Punto de conexión entre cables exteriores e interiores.
- **Sala de equipamiento:** Espacio donde se distribuyen las conexiones.
- **Cableado troncal:** Distribución vertical entre plantas.
- **Armarios de distribución:** Donde se montan equipos de interconexión y paneles de parcheo.
- **Cableado horizontal:** Distribución de cableado dentro de la planta.

- **Área de trabajo:** Zona donde se conectan los dispositivos.

En las conexiones de red, se utilizan dos tipos de cables: directos y cruzados.

- **Cables directos:** Ambos extremos siguen la misma norma de cableado, generalmente 568B. Este tipo de cable se usa para conectar dispositivos diferentes, como un ordenador a un switch o un router a un modem.
- **Cables cruzados:** Se utilizan para conectar dos equipos del mismo tipo, como ordenador a ordenador o switch a switch. En un extremo se sigue la norma 568A y en el otro la 568B. Esto permite que las señales se transmitan correctamente entre dispositivos similares.

5.3. Elementos de interconexión

Los **elementos de interconexión** son dispositivos que permiten la conexión de equipos en una red, facilitando la comunicación entre ellos. En redes de área local (LAN), estos elementos son fundamentales para establecer la conectividad y el intercambio de datos. Para clasificarlos, podemos tomar como referencia el modelo OSI (Open Systems Interconnection), que divide las funciones de una red en diferentes capas.

✓ Nivel físico:

- ➔ Tarjetas de red: pueden ser cableadas o inalámbricas. Además se pueden conectar a los equipos de red.
- ➔ Concentradores o hubs (conocidos como historia)
- ➔ Repetidores: pueden ser locales o remotos, y su funcionalidad es repetir la señal para regenerarla o amplificarla.

✓ Nivel de enlace de datos:

- ➔ Conmutadores o switch: son encargados de conectar con otros segmentos de red, y de ordenadores entre sí. Esto hace que envíe la información al ordenador que la necesita.
- ➔ Puentes o bridges: se conectan a las subredes de forma que transmite de una a otra el tráfico de la red. Conectando múltiples dispositivos y mejorando el rendimiento.
- ➔ Puntos de acceso: conectan dispositivos inalámbricos a la red cableada y pueden recibir alimentación PoE (Power over Ethernet).

✓ Nivel de red:

- ➔ Router o encaminador: encargado de conectar redes diferentes. Su uso principal en la conexión a Internet ya que permite que redes de área local puedan conectarse a Internet. Se basa en el uso del protocolo IP, y necesita tener al menos dos direcciones, una Intranet y otra red local.
- ➔ Además de manejar protocolos de enrutamiento y control de red. Puede dar servicio inalámbrico y por ese motivo también permite dar servicio de punto de acceso.

✓ Niveles superiores:

- ➔ Pasarelas (Gateways): son equipos de interconexión que trabajan en los niveles superiores del modelo OSI. Existen distintos tipos son encargados de conectar con redes diferentes, además de facilitar el control de acceso a una red, controlar los accesos no autorizados. Según la funcionalidad que realice pueden ser servidores, cortafuegos,...

5.4. Tarjetas de red y direccionamiento MAC

Una **tarjeta de red o adaptador de red** es el que permite la comunicación de los diferentes dispositivos conectados entre sí. Además permite compartir los recursos entre dos o más ordenadores. A las tarjetas de red también se le llama NIC (Network Interface Card - Tarjeta de Interfaz de Red).

Su funcionalidad es permitir que puedan conectarse mediante buses internos (PCI), USB, o venir integradas en la placa base. Su función incluye determinar la velocidad de transmisión, protocolos, y parámetros físicos.

Además, convierten la información en señales eléctricas adecuadas para el medio de transmisión. Las tarjetas aceptan el encendido mediante una señal de la red, son llamadas Wake on LAN.

Las tarjetas de red suelen tener los siguiente componentes:

- **Procesador principal:** es el responsable de la gestión de la transmisión y recepción de datos.
- **Transceptor:** un dispositivo encargado de acceder al medio de transmisión (ya sea cableado o inalámbrico).
- **Conector Wake on LAN:** es el que permite el encendido del ordenador desde otro equipo a través de la red.
- **Indicadores de estado:** de las luces que indican si la tarjeta está conectada y si está enviando o recibiendo datos.
- **Conexión física:** en redes cableadas, se utiliza un conector RJ-45 hembra, mientras que en redes inalámbricas se emplea una antena (interna o externa).

La dirección IP y la dirección MAC (también conocida como dirección física) juegan un papel fundamental en la identificación de un ordenador dentro de una red. La dirección MAC es utilizada para asegurar la entrega correcta de los paquetes dentro de la red local, mientras que la dirección IP permite que los dispositivos se comuniquen entre redes o en internet.

5.5. Conmutadores (switch)

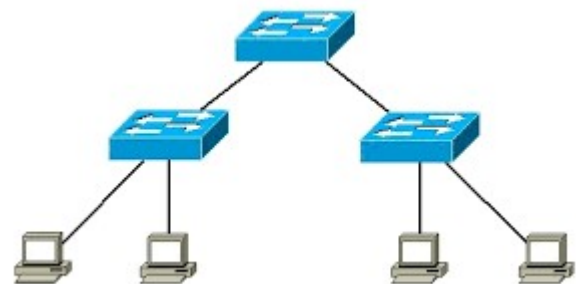
El conmutador es un dispositivo esencial en las redes de área local (LAN), especialmente en aquellas con topología en estrella. **Funciona a nivel de enlace de datos** (capa 2 del modelo OSI), lo que le permite gestionar las direcciones MAC de los dispositivos conectados y averiguar las IP a través del protocolo ARP.

Un conmutador tiene diferentes características que son las siguientes:

- **Conexión eficiente:** El conmutador conecta diferentes dispositivos (como ordenadores) y transmite los datos solo al dispositivo que corresponde, gracias al almacenamiento de las direcciones MAC. Esto reduce el tráfico innecesario, a diferencia de un hub que envía los datos a todos los dispositivos de la red.
- **Velocidad y simultaneidad:** permite altas velocidades de transmisión y facilita que varios dispositivos se comuniquen de manera simultánea, lo que mejora la eficiencia de la red.
- **Operación a nivel de puertos:** el conmutador realiza la conmutación de datos a través de sus puertos, controlando el flujo de información entre los dispositivos conectados a cada uno de esos puertos.
- **Dispositivos avanzados:** los dispositivos de red, como los conmutadores, cada vez ofrecen más características avanzadas, trabajando a niveles superiores y ofreciendo interfaces adicionales para un mejor control y administración de la red.

Los dispositivos de red cada vez ofrecen mayores características, es decir que están a un nivel superior que la tecnología que se necesita. Algunos de ellos ofrecen un interfaz.

VLAN (Redes de Área Local Virtuales) son redes independientes en las que no comparten la misma información a pesar de que estén en la misma red. Pueden elegir la mejor ruta entre esos dispositivos en cuanto a la velocidad y la información de los dispositivos.



5.6. Router o enrutador

El **router o enrutadores** es el equipo de interconexión de redes que se encarga de conectar redes diferentes, gestionando el tráfico de datos entre ellas. Los enrutadores son fundamentales para determinar el camino más eficiente para que los paquetes de datos lleguen a su destino. Para ello, utilizan las direcciones IP de origen y destino, y emplean la tabla de enrutamiento, que almacena la información sobre cómo llegar de una red a otra.

Las características principales de los routers o enrutadores son:

- **Conexión entre redes:** Cada interfaz o puerto del enrutador conecta una red distinta, por lo que cada uno debe tener al menos dos direcciones IP para poder operar correctamente.
- **Función de enrutamiento:** El enrutador decide cómo deben enviarse los paquetes a través de las redes, utilizando rutas estáticas (fijas) o rutas dinámicas (flexibles). Las rutas estáticas se configuran manualmente y son útiles cuando no hay alternativas en el camino, mientras que las rutas dinámicas permiten que el enrutador recabe información y elija automáticamente el mejor camino según las condiciones de la red.
- **Filtrado y seguridad:** Los enrutadores no solo conectan redes, sino que también pueden filtrar paquetes, realizar traducción de direcciones (NAT) y enlaces entre redes. El NAT permite que los dispositivos dentro de una red local puedan acceder a redes externas (como Internet) usando una única dirección IP pública.
- **Configuración:** Para que el enrutador funcione correctamente, debe configurarse adecuadamente. Esto incluye:
 - Asignar direcciones IP a cada interfaz.
 - Configurar máscaras de subred, puertas de enlace, y servidores DNS.
 - Definir configuraciones de DHCP, es un servidor que asigna direcciones IP automáticamente.
 - Configurar puertos abiertos o las redes inalámbricas en routers inalámbricos.

- **Tipos de enrutadores:**
 - **Router ADSL o router de cable:** Usados generalmente para la conexión a Internet. Estos enrutadores suelen venir preconfigurados por los proveedores de servicios de Internet.
 - **Router neutro:** Conecta dos redes locales, pero no está diseñado para proporcionar acceso a Internet.

En la mayoría de los hogares y oficinas, el enrutador permite la conexión a Internet, y su dirección IP es la puerta de enlace que los dispositivos de la red utilizarán para comunicarse con redes externas.

Para ello, el mecanismo NAT traduce las direcciones internas privadas de los dispositivos de la red local a una única dirección pública de la red externa (como Internet).

El enrutador es crucial no solo para la interconexión de redes, sino también para gestionar de manera eficiente el tráfico, aumentar la seguridad y optimizar el acceso a Internet.

5.7. IDS

Un SSID (identificador de red SSID) es el nombre público de una **red de área local inalámbrica** (WLAN) que sirve para diferenciarla de otras redes inalámbricas en la zona.

En la mayor parte de los equipos implementan **medidas de seguridad más o menos complejas**, pero existe la posibilidad de implementar un sistema de detención de intrusos. Suelen existir dos tipos de IDS:

- ✓ **N-IDS** son los encargados de detectar accesos no autorizados en la red.
- ✓ **H-IDS** son los encargados de detectar accesos no autorizados del ordenador o host.

Los N-IDS necesitan un hardware exclusivo porque necesitan analizar todo el tráfico de red. Una de las soluciones es integrar el N-IDS en el cortafuegos de forma que el IDS se encarga de detectar los posibles accesos no autorizados y el cortafuegos de impedir su acceso.

Los H-IDS están integrados en el propio sistema del ordenador y también pueden combinarse con los cortafuegos instalados en cada ordenador.

6. Redes inalámbricas 802.11

Cuando hablamos de redes inalámbricas nos referimos a que los nodos se conectan sin necesidad de una conexión física entre ellos.

Las redes de área local inalámbricas (WLAN) están basadas en su funcionamiento estándar IEEE 802.11 conocidas como redes Wi-Fi. El funcionamiento es el de una red local cableada ya que el estándar se define como trama, ya que es diferente el uso de la MAC, la forma de acceder al medio, las frecuencias de uso,...

Los ordenadores hacen que se comuniquen entre sí formando una trama en una red de tipo ad-hoc lo que permite es conectarse entre sí a unas velocidades bajas pero con una seguridad mínima.

El modo de conexión que tiene la infraestructura, consiste en utilizar un punto de acceso que actúe como todas las conexiones dentro de la infraestructura de la red Wi-Fi.

✓ Algunas ventajas de las redes Wi-Fi:

- ➔ Movilidad: se pueden conectar dispositivos estáticos y móviles.
- ➔ Escalabilidad: son relativamente fáciles de ampliar, tanto en usuarios como en cobertura.
- ➔ Flexibilidad: se puede conseguir un alto grado de conectividad.
- ➔ Menor tiempo de instalación: instalando un punto de acceso se puede conseguir rápidamente conectividad.

✗ Las mayores desventajas:

- ➔ La seguridad: es difícil conseguir un alto grado de seguridad.
- ➔ Interferencias: al trabajar en rangos de frecuencias compartidos por otros dispositivos se pueden tener muchas interferencias.

6.1. Tipos de redes 802.11 - Características

Las redes **802.11** (Wi-Fi) tienen varios componentes clave. Las **estaciones** incluyen ordenadores y dispositivos de interconexión, mientras que el **medio** de transmisión suele ser radiofrecuencia en las bandas de **2,4 GHz y 5 GHz**. Para conectar dispositivos, se usa un **punto de acceso**, que distribuye la señal y permite la comunicación entre estaciones.

- ✓ **Estación:** Ordenadores y elementos de interconexión.
- ✓ **Medio:** Usualmente radiofrecuencia. Las redes Wi-Fi trabajan en las bandas de 2,4 GHz y 5 GHz, estos rangos están en el rango de las microondas.
- ✓ **Punto de acceso**
- ✓ **Sistema de distribución**
- ✓ **Conjunto de servicio básico:** también llamado ad-hoc e infraestructura.
- ✓ **Conjunto de servicio extendido:** la unión de varios modos de conexión o de varias infraestructuras.
- ✓ **Área de servicio básico:** la zona donde se comunican las estaciones.
- ✓ **Movilidad**
- ✓ **Cobertura**

Además del estándar con las diferentes versiones:

- ✓ **IEEE 802.11a:** opera en la banda de 5 Ghz tiene una velocidad máxima de 54 Mbps, con velocidades reales de aproximadamente 20 Mbps, tiene 12 canales sin solapamiento, 8 para redes inalámbricas y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b.
- ✓ **IEEE 802.11b:** opera en la banda de 2,4 Ghz tiene una velocidad máxima de 11 Mbps, con velocidades reales de entre 2 y 4 Mbps, tiene 14 canales, y pueden usarse 3 sin solapamiento en redes inalámbricas. Esta versión tiene una ventaja con respecto a la anterior y es el alcance, puede llegar a dar cobertura a 120 metros en exterior y 60 metros en interior con velocidades adecuadas.

- ✓ **IEEE 802.11g:** opera en la banda de 2,4 Ghz por lo que es compatible con la versión b, pero ofrece las mismas tasas de transferencia que la versión a, por tanto puede alcanzar una velocidad máxima de 54 Mbps con medias de 20 Mbps, tiene 14 canales pudiendo usarse hasta 11, teniendo en cuenta que deben ir de 3 en 3 para impedir el solapamiento, para esto hay que cuidar el diseño de la red. En cuanto a coberturas el estándar nos dice que puede alcanzar hasta 75 metros en exterior y 20 metros en interior, pero algunos fabricantes ofrecen dispositivos con mayores coberturas. Hay que resaltar que aunque la versión b y la g son compatibles se recomienda usar versión g, ya que si un dispositivo versión b se conecta a punto de acceso g, baja la velocidad de toda el área de cobertura, perjudicando a los otros dispositivos.
- ✓ **IEEE 802.11n:** puede operar simultáneamente en las bandas de 5 Ghz y en la de 2,4 Ghz, gracias a esto la versión n es compatible con las otras versiones. Además es útil que trabaje en la banda de 5 Ghz ya que está menos congestionada y sufre menos interferencias de otros dispositivos. Tiene una velocidad máxima de 600 Mbps con velocidades medias de operación de entre 100 y 200 Mbps. En cuanto a cobertura varía respecto al tipo de dispositivo, antena que utiliza,... pero podemos trabajar con coberturas de 250 metros en exterior y unos 80 metros en interior. Al igual que la versión g si los dispositivos que se conectan son de versiones anteriores, las velocidades y coberturas bajan. Esta versión utiliza tecnología MIMO, que significa múltiples entradas y múltiples salidas, esto permite usar múltiples antenas transmisoras y receptoras para mejorar la eficiencia del sistema, permitiendo manejar más información que si utilizáramos una sola antena.

6.2. El SSID de una red 802.11

El SSID (Identificador de Conjunto de Servicio) es el nombre de la red inalámbrica que permite a los dispositivos conectarse a ella. Sirve para identificar a qué red pertenece un dispositivo y con cuáles pueden comunicarse.

En redes ad-hoc, se usa el BSSID, mientras que en redes con infraestructura y punto de acceso, se emplea el ESSID (Extended Service Set Identifier).

El área que cubre una red inalámbrica se llama IBSS en redes independientes y BSS en redes con punto de acceso, también conocido como celda o área de cobertura. En una red con infraestructura, el BSS define el alcance del punto de acceso, permitiendo que los dispositivos dentro de esa zona se conecten a la red.

Si se necesita ampliar la cobertura, se pueden conectar varios BSS entre sí formando un ESS (Extended Service Set). En este caso, cada punto de acceso usa un canal diferente, pero todos comparten el mismo SSID, asegurando una conexión continua dentro de la red.

6.3. Seguridad en 802.11

Hay que tener en cuenta que las redes Wi-Fi son muy vulnerables a la interceptación de paquetes, a los ataques o simplemente a que usuarios no autorizados se aprovechen de la conexión. Por ello es conveniente implementar medidas de seguridad que prevengan un uso indebido de la red. Desde los puntos de acceso se difunde el SSID para que los ordenadores que estén en cobertura puedan conectarse mediante broadcast o emisión del SSID. Si la función se desactiva deben configurar manualmente el SSID por ello pueden no detectar la red. Existen herramientas fáciles que detectan el SSID oculto, pero es un primer paso.

Existen varios métodos con una distribución considerable que consisten en encriptar o codificar la información de la red. Para ello pueden usarse diferentes tipos:

- ✓ **WEP** (obsoleto) encargado de encriptar la información utilizando claves preconfiguradas para cifrar y descifrar los datos. Es débil ya que es fácil descifrarlo.
- ✓ **WPA** (todavía en uso y más difícil de descifrar), **WPA2** (obsoleto) acceso.

Es conveniente que descartemos los anteriores tipos de encriptación:

- ✓ **WPA-PSK** utiliza un algoritmo de encriptación utilizando el protocolo TKIP que cambia dinámicamente. WPA-PSK es vulnerable en la primera conexión al punto de acceso que es donde se preestablece las claves dinámicamente.
- ✓ **Radius** utilizan servidores de incryptación. Utilizan protocolos de autenticación y autorización de esta manera que se encarga de distribuir claves diferentes entre los usuarios. Este método es el más seguro, pero también el de mayor coste.

Para mayor seguridad, se recomienda usar WPA-PSK, que cambia dinámicamente las claves, aunque es vulnerable en la primera conexión, o Radius, que utiliza servidores de autenticación y autorización para generar claves únicas para cada usuario. Además, el filtrado de direcciones MAC permite restringir el acceso solo a dispositivos autorizados.

La seguridad en redes inalámbrica tiene establecido el estándar IEE 802.1X que originalmente se modificó para ser utilizados en las redes inalámbricas. Consiste en el control de los puertos de acceso a la red, de forma que sólo se abrirá el puerto y la conexión si el usuario está autenticado y autorizado en base a la información guardada en una base de datos alojada en un servidor.

Las redes inalámbricas el estándar tiene tres componentes principales:

- ✓ **Autenticador** será el punto de acceso que recibirá la información del cliente y la translada al servidor Radius.
- ✓ **Solicitante** será el software del cliente que da información de las claves y permisos para mandarla al autenticador.
- ✓ **Servidor de autenticación** será el servidor Radius que debe comprobar los permisos y claves de los usuarios.

En conclusión, debe mantener la seguridad completa en una red inalámbrica, es difícil y de mucho costo, pero combinando las técnicas. Es posible tener un grado de seguridad sin necesidad de un gasto excesivo.

7. Direccionamiento IP

Todos los dispositivos deben tener una única dirección IP. Las IP contienen dos partes: una identifican a la red (ID Network) y el identificador el dispositivo host (dispositivo que está conectado a la red que tiene asignado una IP).

El sistema de direccionamiento IP tiene 32 bits de números binarios. Estos números binarios están separados en 4 partes (bytes) y se pueden representar también en decimal, separados por puntos por cada byte.

7.1. Clases de direcciones IP

Según la dirección IP que represente en la red y el host, eso es conocido como arquitectura de clases. Hay 3 clases de direcciones IP que una organización pueda recibir de parte de Internet Corporation for Assigned Names and Numbers (ICANN):

- ✓ Clase A: el primer octeto se utiliza para identificar la red y el resto para identificar el host (gobiernos y corporaciones internacionales). Está limitada a solo 127 redes de esta clase.
 - La red 0.0.0.0 es utilizada por las máquinas cuando están arrancando o no se les ha asignado dirección.
 - La red 127.0.0.0 se reserva para pruebas de “lookback” (retroalimentación). Los host la utilizan para enviar paquetes hacia ellos mismos.

Network	Host	Host	Host
1er. Octeto	2do. Octeto	3er. Octeto	4to. Octeto

- ✓ Clase B: utiliza los dos primeros octetos para identificar la red dejando 16 bits restantes para el host (grandes compañías, universidades,...).

Network	Network	Host	Host
1er. Octeto	2do. Octeto	3er. Octeto	4to. Octeto

- ✓ Clase C: utiliza los tres primeros octetos para identificar la red dejando 8 bits restantes para el host (redes pequeñas).

Network	Network	Network	Host
1er. Octeto	2do. Octeto	3er. Octeto	4to. Octeto

- ✓ Clase D: usada para multicast de grupos de datos de una determinada aplicación o servicio de un servidor. Una dirección multicast es una dirección exclusiva que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP, por lo tanto, una sola estación puede transmitir de forma simultánea datos a múltiples receptores. Su Rango es 224.0.0.0 a 239.255.255.255.
- ✓ Clase E: está reservada para los usos experimentales. Su rango es 240.0.0.0 a 255.255.255.255.

0	CLASE A
10	CLASE B
110	CLASE C
1110	CLASE D
Nota: un bit siempre está reservado en la clase	

Hay 2 direcciones de subred que están reservados (de host 0 y para definir la red en la que se ubica) y la restante para la dirección de broadcast que tiene una parte de host a 1 y se debe de comunicar con el resto de la red. La primera será para la dirección IP para la subred y la última dirección IP para broadcast.

Tabla 1. Clases de direcciones IP				
Clases	Rango del 1er octeto	Número de redes	Número de hosts	Ejemplo
A	1-126	127	16,777,214	10.15.121.5
B	128-191	16,384	65,534	130.13.44.52
C	192-223	2,097,152	254	200.15.23.8

7.2. Tipos de direcciones IP

- **IP pública** son los que se identifican cuando conectamos a otras redes (Internet) que son asignadas por un proveedor ISP. Pueden ser de dos tipos:
 - **IP estática:** cuando tenemos una dirección IP asignada. Normalmente suelen utilizarse en el ámbito doméstico y son asignadas por los proveedores.
 - **IP dinámica:** es la más utilizada habitualmente nos la asignan cuando nos conectamos a la red (Internet) una dirección que tenga disponible en ese momento (cambia continuamente cada vez que nos conectamos y nos desconectamos).
- **IP privada** es la dirección IP de cada dispositivo conectado a través del protocolo TCP/IP de una red. En la IP privada si que podemos asignarla de forma automática, mediante DHCP.