TEMA 2:

Redes de ordenadores

Un poco de historia

La primera transmisión de datos entre ordenadores se produjo el 20 de octubre de 1969 entre las universidades de UCLA y Stanford en Estados Unidos y fue la culminación de multitud de trabajos y esfuerzos. La idea de crear una red de ordenadores surge después de la Segunda Guerra Mundial, durante la guerra fría entre EEUU y la URSS, ante un ataque repentino de la URSS, EEUU tendría muchas dificultades para organizarse. Para conseguirlo, se necesitaba un método más efectivo que los existentes en esa época como podía ser el telégrafo.
La primera red de ordenadores estaba compuesta por cuatro nodos situados en universidades americanas y se denominó ARPANET, que posteriormente pasó a llamarse Internet. Esta red se fue ampliando y mejorando la comunicación, creándose en 1970 el protocolo TCP/IP ampliamente utilizado en Internet y desarrollando diferentes servicios para la comunicación, como el chat, navegación a través de hipertexto...

Redes de ordenadores

Una red de ordenadores es un grupo de ordenadores conectados entre sí que pueden comunicarse y pueden compartir información y recursos como impresoras, acceso a Internet...

1. Tipos de redes

Las redes de ordenadores se pueden clasificar según varios criterios, el tipo más extendido es la clasificación dependiendo de la extensión que ocupa, los tipos principales que nos podemos encontrar son:

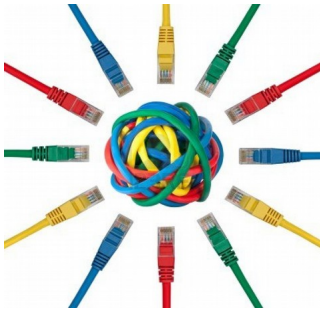
RED DE ÁREA LOCAL (Local Area Network). Esta red conecta equipos en un área geográfica limitada, tal como una oficina o un edificio. Todos los equipos conectados tienen acceso a la información y a los recursos de forma rápida y sencilla.

RED DE ÁREA AMPLIA (Wide Area Network). Estas redes se basan en la conexión de equipos informáticos ubicados en un área geográfica extensa, por ejemplo entre países o distintos continentes. Al comprender una distancia tan grande la transmisión de datos se realiza a una velocidad menor Sin embargo, tienen la ventaja de trasladar una cantidad de información mucho mayor.

2. Dispositivos físicos para redes cableadas

Para que un ordenador pueda conectarse a una red de ordenadores es necesario que disponga de una serie de dispositivos. Algunos de ellos lo tienen instalados internamente y otros son externos a él. Los más frecuentes son los siguientes:

Tarjeta de red: permite conectar el ordenador a la red siempre que tenga los datos de configuración de forma adecuada. Podemos encontrar tarjetas de red cableada o inalámbrica.



Cable de red: Es el medio de comunicación por el que circulan los datos en la red de ordenadores. Podemos encontrarnos:

Par Trenzado: Se utiliza en redes locales y consta de un grupo de cables recubiertos de un material aislante. Se suele emplear par trenzado categoría 6, que permite velocidades de hasta 1000 Mbps.

Fibra óptica: envía pulsos de luz para transmitir los datos y permite velocidades de conexión muy elevadas, así como grandes capacidades de transmisión.

Concentrador o hub: dispositivo que recibe paquetes de información y los reenvía a todos los ordenadores conectados a él excepto el que envía la información mediante loa puertos de conexión que dispone.

Conmutador o switch: Su función es similar a la del concentrador, pero envía la información exclusivamente al ordenador o dispositivo que espera recibir la información.

Router, enrutador o encaminador: Dispositivo que sirve para conectar dos redes de ordenadores, es el dispositivo que se suele entregar cuando contratamos un acceso a Internet. Este acceso a Internet realmente es la comunicación entre una red de ordenadores, Internet, con otra red de ordenadores formada por los ordenadores que tenemos en casa.

3. Redes inalámbricas

Este tipo de redes no utiliza cables para el envío de datos, utilizando ondas electromagnéticas para el envío de datos. Con este tipo de redes se evita tener que instalar los cables de conexión, aunque al enviar la información en forma de ondas se tiene un problema en cuanto a la seguridad de datos. Podemos distinguir dos tipos de redes de este tipo que son ampliamente utilizadas:

- Redes Wi-Fi: Son redes de ordenadores que tienen la misma función que las redes cableadas, teniendo un ancho de banda y alcance mayor que las redes Bluetooth
- Redes Bluetooth: conecta distintos dispositivos de bajo consumo con un alcance pequeño, alrededor de 10 metros y permite la transmisión de voz y datos.

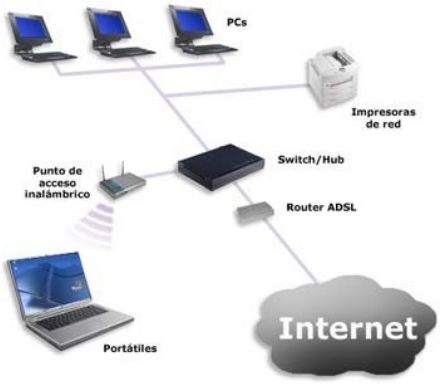
Para montar una red inalámbrica debemos de tener una serie de dispositivos similares a las redes cableadas, así se deben instalar:

- Tarjeta de red inalámbrica
- Router inalámbrico
- Punto de acceso: tienen la función similar a los concentradores o conmutadores o incluso la de un router.

La comunicación Wi-Fi corresponde con el estándar 802.11, que define las características de una red de área local inalámbrica. Este estándar tiene una serie de variantes que han ido mejorando el estándar original en velocidad de transmisión y en seguridad, entre ellos podemos nombrar:

- 802.11b: establece el método de acceso a la red y velocidades de transmisión de 11Mbps.
- 802.11g: Es la evolución del estándar anterior. Establece velocidades de transmisión máximas de 54Mbps.
- 802.11n: Establece velocidades de transmisión máximas de 300Mbps, aunque se consiguen realmente de 80 a 100 Mbps.

4. Configuración de red



Una vez que disponemos de los ordenadores y el resto de componentes necesarios para montar una red de ordenadores tenemos que realizar el segundo paso: configurar cada uno de los dispositivos para que los ordenadores se puedan conformar una red.

Una red de ordenadores puede estar conectada a Internet o puede ser una red aislada sin acceso a Internet, depende de los dispositivos que disponga.

Para configurar una red de ordenadores es necesario configurar los siguientes parámetros asociados a cada ordenador:

- **Nombre de equipo:** es un nombre único que lo identifica en la red. Por ejemplo PC18.
- **Grupo de trabajo:** es un conjunto de ordenadores que van a trabajar en común. Es necesario que aquellos ordenadores que quieran trabajar en común tengan el mismo grupo de trabajo. Por ejemplo ADMINISTRACION.
- **Dirección IP (versión 4):** utiliza direcciones numéricas compuestas por cuatro números enteros entre 0 y 255, y escritos en el formato xxx.xxx.xxx.xxx. Por ejemplo 192.168.0.126.
- **Máscara de subred:** es un código numérico que complementa a la dirección IP que sirve para detectar los ordenadores que forman parte de la red y pueden trabajar conjuntamente y, los que estando en la misma red, no pueden trabajar en común. Este código numérico es útil para hacer subredes.
- **Puerta de Enlace:** Indica la dirección del dispositivo que da acceso a otra red, normalmente Internet. Es decir, enlaza dos redes.
- **Servidor DNS:** Este parámetro especifica la dirección IP que tiene un ordenador en Internet que utiliza el ordenador cada vez que desea navegar por Internet. Cuando queremos navegar por Internet ponemos una dirección del tipo www.wikipedia.org. Este dato no es comprensible por la red, ya que él sabe utilizar direcciones IP. El servidor DNS convierte el nombre de dominio (www.wikipedia.org) en la dirección IP que corresponde con esa página Web. Por ejemplo, la dirección IP 173.194.78.94 corresponde al dominio www.google.es.

En la siguiente tabla se va a configurar una red para tres ordenadores:

	Nombre	G. T.	IP	Máscara de subred	Puerta de enlace	DNS 1ª	DNS 2ª
Ordenador 1	PC1	AULA3	192.168.0.12	255.255.255.0	192.168.0.1	62.42.230.24	62.42.63.52
Ordenador 2	PC2	AULA3	192.168.0.6	255.255.255.0	192.168.0.1	62.42.230.24	62.42.63.52
Ordenador 3	PC3	AULA3	192.168.0.231	255.255.255.0	192.168.0.1	62.42.230.24	62.42.63.52

5. Seguridad informática

La seguridad informática se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (personas que se conectan a Internet e ingresan a distintos sistemas).

5.1 Seguridad activa y pasiva

Seguridad activa: Tiene como objetivo proteger y evitar posibles daños en los sistemas informáticos. Podemos encontrar diferentes recursos para evitarlos como:

- utilización adecuada de contraseñas
- utilización de software de seguridad informática, como un antivirus y un firewall actualizado
- encriptación de los datos

Seguridad pasiva: Su fin es minimizar los efectos causados por un accidente, un usuario o un malware. Las practicas de seguridad pasiva más frecuentes y mas utilizadas hoy en día son:

- utilización de hardware adecuado contra accidentes y averías.
- utilización de copias de seguridad de datos y del sistema operativo.

5.2 Amenazas silenciosas

Las amenazas silenciosas son programas que se instalan en el ordenador normalmente sin nuestro conocimiento y que suponen una amenaza para el sistema informático, ya que el sistema realizará tareas adicionales a las que normalmente realiza y supondrá una ralentización del equipo informático, así como la realización de tareas sin nuestra autorización que pueden dañar el sistema incluyendo la pérdida de datos. Este tipo de programas son denominados malware o programa malicioso. Las amenazas más importantes que nos podemos encontrar son las siguientes:

- **Virus informático:** programa malicioso que infectan a otros archivos del sistema con la intención de modificarlo o dañarlo. Dicha infección consiste en incrustar su código malicioso en el interior del archivo "víctima" (normalmente un ejecutable) de forma que a partir de ese momento dicho ejecutable pasa a ser portador del virus y por tanto, una nueva fuente de infección.

- **Gusano informático:** programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador". El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos.
- **Troyano:**programa que puede considerarse malicioso, en función de su uso, el cual se instala en una computadora, para así permitirle al usuario el control remoto del equipo. Es en este punto donde entra lo negativo de lo que es un troyano informático.

- **Spyware:** A pesar de su nombre, el término "spyware" no se refiere a algo usado por espías, sino algo usado por la industria de la publicidad. De hecho, el spyware también se conoce como "adware" (software de anuncios) Se refiere a una categoría de software que, cuando está instalada en su computadora, puede enviarle ads, pop-up's o anuncios para re-dirigir su Navegador a cierto Web Site, o monitorea los Web sites que usted visita. Algunas versiones extremas, invasoras del spyware pueden registrar exactamente qué teclas mecanografía.
- **Phishing y Pharming:** Viene a significar "pescar, pescando incautos". Es una técnica que se basa en intentar engañar al usuario (ingeniería social), normalmente mediante un correo electrónico, diciéndole que pulse en un determinado enlace, para validar sus claves por tal motivo o tal otro. El pharming es más peligroso que el phishing, ya que es más difícil de descubrir. Se basa en redirigirnos a la página falsa del banco diseñada por lo ladrones de forma automática, es decir, sin que nosotros necesitemos pulsar ningún enlace. A continuación veremos como lo consiguen, para ello debemos estudiar primero lo que es una dirección IP, un dominio y un servidor DNS.
- **Keylogger:** (Registro de teclas) su función consiste en registrar todas las pulsaciones que el usuario realiza en su teclado, para posteriormente almacenarlas en un archivo y enviarlo por Internet al creador del keylogger.
- **Rogue software:** O falso programa de seguridad. Se trata de falsos programas antivirus o antiespías que hacen creer al usuario que su sistema se encuentra infectado. Para hacerle comprar un programa que elimine esta falsa infección.
- **Hoaxes:** Esta clase de alarmas, suelen ser falsas o basadas en hechos erróneos, pero lo que es peor activan un tipo de "contaminación" muy diferente, propagar cientos y hasta miles de mensajes de advertencia sobre los mismos. Y aún en el caso de denuncias basadas en hecho reales, esta forma de hacerlo desvirtúa totalmente su verdadero objetivo.

6. Programas de seguridad informática

Para protegernos de las distintas amenazas que pesan sobre el sistema informático, es necesario instalar programas que nos ayuden a esa labor. Entre ellos podemos destacar:

- **Antivirus:** Es un programa cuya finalidad es detectar, impedir la ejecución y eliminar software malicioso como virus informáticos, gusanos, espías y troyanos. Ejemplos: Kaspersky Antivirus (de pago) y Avast Antivirus (gratuito).
- **Cortafuegos:** Es un mecanismo de seguridad contra ataques de Internet. Filtra y controla todas las comunicaciones que pasan de una red a otra evitando el ingreso y salida de ciertos procesos o aplicaciones no seguras, de este modo un firewall puede permitir o denegar desde una red local hacia Internet servicios de Web, correo, ftp, IRC, etc. Ejemplos: eBox Platform (de pago) y Zone Alarm Free Firewall (gratuito).

- **Software antiespía:** Impide que un programa espía se instale en el ordenador, limpiando el ordenador de estos programas y sus cookies e impidiendo su instalación automática. También busca y elimina troyanos, gusanos y otro tipos de programas maliciosos. Hay gran cantidad de programas gratuitos que se encargan de realizar esta labor, como SpyBot Search & Destroy y Malwarebytes Anti-Malware.