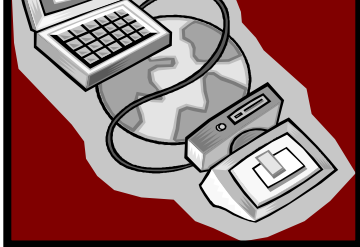


Página principal

El objetivo del curso de Red es aprender como funcionan las redes, de forma simple y didáctica y está dirigido a todas aquellas personas interesadas en conocer cómo es posible la comunicación entre diferentes máquinas en red.

Los participantes trabajan con casos prácticos reales, plenos de las exigencias de clientes reales de alto desempeño Empresarial, que han exigido el desarrollo de sistemas de alta capacidad de organización y procesamiento de información y data, aunada a un alto nivel de interactividad y amigabilidad con el usuario.

- **Página principal**
- **Fundamentos**
- **Tipos de redes**
- **Topologías**
- **Dispositivos**
- **Protocolos de comunicación**
- **Medios de Trasmisión**
- **Modelo OSI y TCP/IP**
- **Cableado RJ45 y práctica**



Una Red es un conjunto de equipos por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat, juegos), etc.

Las primeras redes de datos estaban limitadas a intercambiar información basada en caracteres entre sistemas informáticos conectados. Las redes actuales evolucionaron para agregarle voz, flujos de video, texto y gráficos, a los diferentes tipos de dispositivos.

Internet básicamente es la red de redes y nos proporciona:

Cursos enviados utilizando recursos de Internet o de red generalmente se denominan experiencias de aprendizaje en línea (e-learning).

Las empresas utilizaban redes de datos para registrar, administrar información, sistemas de nómina, pero, ahora permiten diferentes tipos de servicios de información, como e-mail, video, mensajería y telefonía.

Las intranets, redes privadas utilizadas sólo por una empresa, les permiten comunicarse y realizar transacciones entre empleados y sucursales globales.

Escuchamos artistas grabados, vemos o disfrutamos de avances de películas, leemos libros completos y descargamos material.

Los mercados y los sitios de subasta en línea brindan la oportunidad de comprar, vender y comercializar todo tipo de Mercancía.

Elementos de una Red:

Reglas, medios, mensajes y **dispositivos**.

Los protocolos son las **reglas** que utilizan los dispositivos de red para comunicarse entre sí (http, smtp, pop, sip, TCP, IP).

Los medios de cobre incluyen cables, como el par trenzado del cable de teléfono, el cable coaxial o generalmente conocido como cable de par trenzado no blindado (UTP) de Categoría 5. Las fibras ópticas, hebras finas de vidrio o plástico que transmiten señales de luz, son otra forma de medios de networking. Los medios inalámbricos incluyen conexiones inalámbricas domésticas entre un router inalámbrico y una computadora con una tarjeta de red inalámbrica, conexión inalámbrica terrestre entre dos estaciones de tierra o comunicación entre dispositivos en tierra y satélites.

Redes Convergentes: consolidar redes dispersas con diferentes servicio(computadoras personales, teléfonos, televisores, asistentes personales y registradoras de puntos de venta minoristas Telefonía IP) en una única plataforma.

Características :

Seguridad: La privacidad de los datos se logra permitiendo que lean los datos solamente los receptores autorizados y designados. Encriptamiento de datos.

Tolerancia a fallas: que la red no deje de funcionar por complete si algún dispositivo falla.

Escalabilidad: que pueda crecer sin que implique una reestructuración.

QoS: Calidad de servicio, imprescindible para comunicaciones VoIP, video, música.

Dirección IP y Dirección MAC:

Dirección IP: Serie de números asociadas a un dispositivo (generalmente una computadora), con la cual es posible identificarlo dentro de una red configurada específicamente para utilizar este tipo de direcciones.

Dirección MAC: Media Access Control o *control de acceso al medio* es un identificador que corresponde de forma única a una de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE y el fabricante.

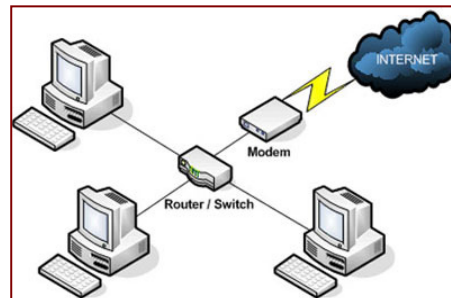
TIPOS DE REDES

Las infraestructuras de red pueden variar en gran medida en términos de: el tamaño del área cubierta, la cantidad de usuarios conectados, y la cantidad y tipos de servicios disponibles.

LAN:

Una red individual generalmente cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región.

Una Red de área local generalmente utiliza una tecnología de ancho de banda alto que es capaz de sostener gran cantidad de hosts.

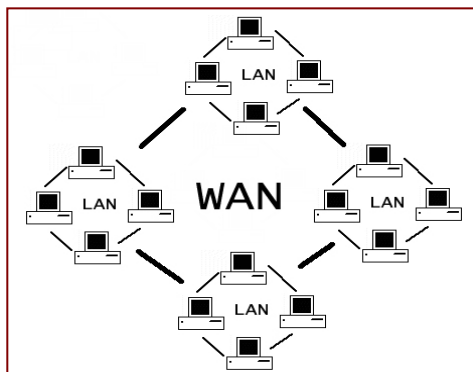


WAN:

Son todas aquellas que cubren una extensa área geográfica. Son generalmente una serie de dispositivos de conmutación interconectados. Se desarrollan o bien utilizando tecnología de conmutación de circuitos o conmutación de paquetes.

Estas redes que conectan las LAN en ubicaciones separadas geográficamente. Una conexión de dos o más redes de datos forma una internetwork.

El costo de los enlaces físicos de larga distancia y la tecnología utilizada para transportar las señales a través de esas distancias, generalmente, ocasiona una menor capacidad de ancho de banda.



REDES: Nivel 1

Ing. Vaneska Hernandez

Topologías

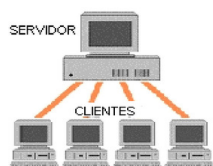
La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Las topologías de red pueden verse en el nivel físico y el nivel lógico.

La topología física es una configuración de nodos y las conexiones físicas entre ellos. La representación de cómo se usan los medios para interconectar los dispositivos es la topología física.

Una topología lógica es la forma en que una red transfiere tramas de un nodo al siguiente. Esta configuración consiste en conexiones virtuales entre los nodos de una red independiente de su distribución física.

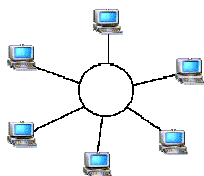
Las topologías lógica y física generalmente utilizadas en redes son: Punto a Punto, Multi-Acceso, Anillo.

PUNTO a PUNTO



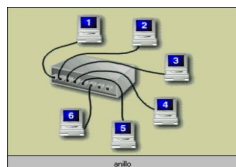
Conecta dos nodos directamente entre sí. En redes punto a punto, si los datos sólo pueden fluir en una dirección a la vez, está operando como un enlace half-duplex. Si los datos pueden fluir con éxito a través del enlace desde cada nodo simultáneamente, es un enlace duplex. La conexión lógica entre nodos forma lo que se llama circuito virtual. Un circuito virtual es una conexión lógica creada dentro de una red entre dos dispositivos de red.

MULTI-ACCESO



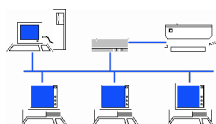
Una topología lógica multi-acceso permite a una cantidad de nodos comunicarse utilizando los mismos medios compartidos.

ANILLO



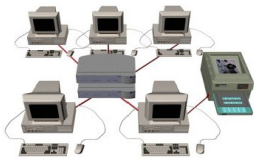
En una topología lógica de anillo, cada nodo recibe una trama por turno. Si la trama no está direccionada al nodo, el nodo pasa la trama al nodo siguiente.

BUS



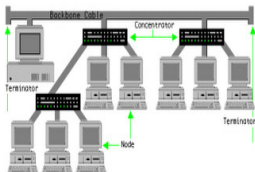
Se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.

ESTRELLA



Red en la cual las estaciones están conectadas directamente al servidor u ordenador y todas las comunicaciones se han de hacer necesariamente a través de él. Esta red crea una mayor facilidad de supervisión y control de información ya que para pasar los mensajes deben pasar por el hub o concentrador, el cual gestiona la redistribución de la información a los demás nodos

ARBOL



Esta estructura se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

REDES: Nivel 1

UNEWB

Dispositivos

Los siguientes son ejemplos de dispositivos de red intermediarios:

- Dispositivos de acceso a la red (hubs, switches y puntos de acceso inalámbricos),
 - Dispositivos de internetworking (routers),
 - Servidores de comunicación y módems, y
 - Dispositivos de seguridad (firewalls).
-

HUB (concentrador)



Permite conectar entre sí otros equipos y retransmite los paquetes que recibe desde cualquiera de ellos a todos los demás. Los hubs han dejado de ser utilizados, debido al gran nivel de colisiones y tráfico de red que propician. Funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos.

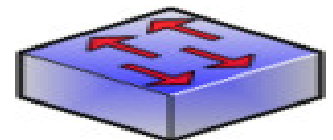
PUENTE

Un *bridge* conecta dos segmentos de red como una sola red usando el mismo protocolo de establecimiento de red. Para hacer el *bridging* o interconexión de más de 2 redes, se utilizan los *switch*. Funciona a través de una tabla de direcciones MAC detectadas en cada segmento a que está conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir datos a un nodo del otro, el bridge copia la trama para la otra subred. Por utilizar este mecanismo de aprendizaje automático, los bridges no necesitan configuración manual.

SWITCH:

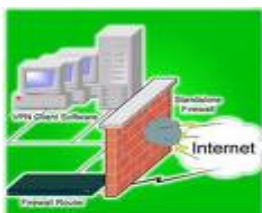
Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un *filtro* en la red.



FIREWALL

Un **cortafuegos** (o *firewall* en inglés) es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo autorizado de comunicaciones. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.



ROUTER

Ayuda a direccionar mensajes mientras viajan a través de una red. Un router es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos. Cada puerto de un router se conecta a una red diferente y realiza el enrutamiento de los paquetes entre las redes. También pueden utilizarse para interconectar redes que utilizan diferentes tecnologías.



Router inalámbrico: un tipo específico de router que generalmente se encuentra en redes domésticas.

REDES: Nivel 1

Ing. Vaneska Hernandez

PROTOSCOLOS

Los protocolos son las reglas que utilizan los dispositivos de red para comunicarse entre sí. Actualmente el estándar de la industria en redes es un conjunto de protocolos denominado TCP/IP (Protocolo de control de transmisión/Protocolo de Internet). TCP/IP se utiliza en redes comerciales y domésticas, siendo también el protocolo primario de Internet. Son los protocolos TCP/IP los que especifican los mecanismos de formateo, de direccionamiento y de enrutamiento que garantizan que nuestros mensajes sean entregados a los destinatarios correctos.

Los protocolos definen:

El formato del mensaje, ¿cómo y cuándo se pasan los mensajes de entre dispositivos?, el método por el cual los dispositivos de red comparte información sobre rutas con otras , ¿Cuándo inician y terminan las sesiones de transferencia?.

Protocolo de aplicación: Un Protocolo de Aplicación define cómo interactúan un cliente y un servidor.

HTTP: es el Protocolo de Transferencia de Hipertexto (en inglés yperText Transfer Protocol).

FTP: es el Protocolo de Transferencia de Archivos(en inglés File Transfer Protocol).

SMTP: es el Protocolo de Transferencia de Correo(en inglés Simple Mail Transfer Protocol).

NNTP: es el Protocolo de Transferencia de Red de Noticias(en inglés Network News Transfer Protocol).

IRC: es el Chat Basado en Internet(en inglés Internet Relay Chat).

Telnet: (TELEcommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla remotamente como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

Protocolo de Transporte:

uno orientado a la conexión y otro no orientado a la conexión. El PROTOCOLO NO ORIENTADO A LA CONEXIÓN ES EL UDP Y EL ORIENTADO ES EL TCP.

UDP: EL CONJUNTO DE PROTOCOLOS DE INTERNET SOPORTA UN PROTOCOLO DE TRANSPORTE NO ORIENTADO A LA CONEXIÓN UDP (PROTOCOLO DE DATAGRAMAS DE USUARIO). ESTE PROTOCOLO PROPORCIONA UNA FORMA PARA QUE LAS APLICACIONES ENVÍEN DATAGRAMAS IP ENCAPSULADOS SIN TENER UNA CONEXIÓN.

TCP: (protocolo de control de transmisión) se diseñó específicamente para proporcionar un flujo de bytes confiable de extremo a extremo a través de una interred no confiable. Una interred difiere de una sola red debido a que diversas partes podrían tener diferentes topologías, anchos de banda, retardos, tamaños de paquete... TCP tiene un diseño que se adapta de manera dinámica a las propiedades de la interred y que se sobrepone a muchos tipos de situaciones.

Protocolo de Internetwork:

El protocolo internetwork más común es el Protocolo de Internet (IP). IP es responsable de tomar los segmentos formateados del TCP, encapsularlos en paquetes, asignarles las direcciones correctas y seleccionar la mejor ruta hacia el host de destino.

Telnet: (TELEcommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla remotamente como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

IPX/SPX: IPX (*Internetwork Packet Exchange*) es un protocolo de Novell que interconecta redes que usan clientes y servidores Novell Netware. Es un protocolo orientado a paquetes y no orientado a conexión (esto es, no requiere que se establezca una conexión antes de que los paquetes se envíen a su destino). Otro protocolo, el SPX (*Sequenced Packet eXchange*), actúa sobre IPX para asegurar la entrega de los paquetes.

NetBIOS: NetBIOS (*Network Basic Input/Output System*) es un programa que permite que se comuniquen aplicaciones en diferentes ordenadores dentro de una LAN. Desarrollado originalmente para las redes de ordenadores personales IBM, fué adoptado posteriormente por Microsoft. NetBIOS se usa en redes con topologías Ethernet y token ring. No permite por sí mismo un mecanismo de enrutamiento por lo que no es adecuado para redes de área extensa (MAN).

NetBEUI: NetBIOS Extended User Interface o Interfaz de Usuario para NetBIOS es una versión mejorada de NetBIOS que sí permite el formato o arreglo de la información en una t r a n s m i s i ó n d e d a t o s . Aunque NetBEUI es la mejor elección como protocolo para la comunicación dentro de una LAN, el problema es que no soporta el enrutamiento de mensajes hacia otras redes, que deberá hacerse a través de otros protocolos (por ejemplo, IPX o TCP/IP).

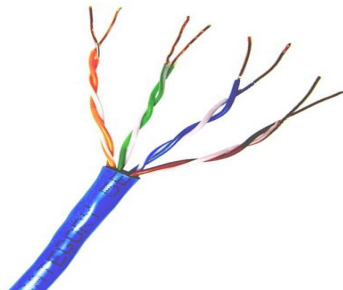
AppleTalk: Es el protocolo de comunicación para ordenadores Apple Macintosh y viene incluido en su sistema operativo, de tal forma que el usuario no necesita configurarlo.

Medios de Transmisión

Medios de transmisión guiados

En medios guiados , el ancho de banda o velocidad de transmisión dependen de la distancia y de si el enlace es punto a punto o multipunto .

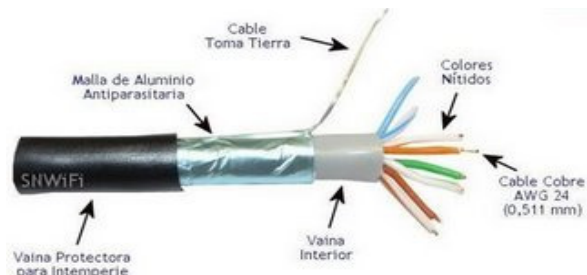
UTP Par Trenzado



Es el medio guiado más barato y más usado . Consiste en un par de cables , embutidos para su aislamiento , para cada enlace de

Comunicación. La utilización del trenzado tiende a disminuir la interferencia electromagnética . Este tipo de medio es posee un inconveniente principal y es su poca velocidad de transmisión y su corta distancia de alcance . Es un medio muy susceptible a ruido y a interferencias . Para evitar estos problemas se suele trenzar el cable con distintos pasos de torsión y se suele recubrir con una malla externa para evitar las interferencias externas .

Pares trenzados apantallados y sin apantallar



Los pares sin apantallar son los más baratos aunque los menos resistentes a interferencias (aunque se usan con éxito en telefonía y en redes de área local) . A velocidades de transmisión bajas , los pares apantallados son menos susceptibles a interferencias , aunque son más caros y más difíciles de instalar.

Cable coaxial



cable coaxial

Consiste en un cable conductor interno (cilíndrico) separado de otro cable conductor externo por anillos aislantes o por un aislante macizo . Todo esto se recubre por otra capa aislante que es la funda del cable . Este cable , aunque es más caro que el par trenzado , se puede utilizar a más larga distancia , con velocidades de transmisión superiores , menos interferencias y permite conectar más estaciones . Se suele utilizar para televisión , telefonía a larga distancia , redes de área local , conexión de periféricos a corta distancia , etc.

Se utiliza para transmitir señales analógicas o digitales . Sus inconvenientes principales son : atenuación , ruido térmico , ruido de intermodulación . Para señales analógicas , se necesita un amplificador cada pocos kilómetros y para señales digitales un repetidor cada kilómetro .

Fibra Óptica



Se trata de un medio muy flexible y muy fino que conduce energía de naturaleza óptica . Su forma es cilíndrica con tres secciones radiales : núcleo , revestimiento y cubierta . El núcleo está formado por una o varias fibras muy finas de cristal o plástico . Cada fibra está rodeada por su propio revestimiento que es un cristal o plástico con diferentes propiedades ópticas distintas a las del núcleo . Alrededor de este conglomerado está la cubierta (constituida de material plástico o similar) que se encarga de aislar el contenido de aplastamientos , abrasiones , humedad , etc.

Es un medio muy apropiado para largas distancias e incluso últimamente para LAN's .

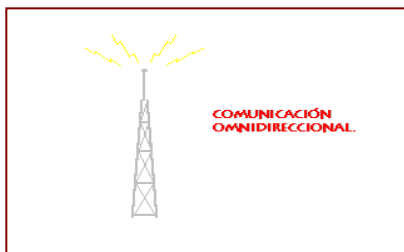
Sus beneficios frente a cables coaxiales y pares trenzados son :

- * Permite mayor ancho de banda .
- * Menor tamaño y peso .
- * Menor atenuación .
- * Aislamiento electromagnético .
- * Mayor separación entre repetidores .

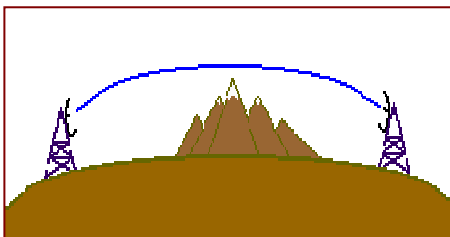
El método de transmisión es : los rayos de luz inciden con una gama de ángulos diferentes posibles en el núcleo del cable , entonces sólo una gama de ángulos conseguirán reflejarse en la capa que recubre el núcleo . Son precisamente esos rayos que inciden en un cierto rango de ángulos los que irán rebotando a lo largo del cable hasta llegar a su destino . A este tipo de propagación se le *multimodal* . Si se reduce el radio del núcleo , el rango de ángulos disminuye hasta que sólo sea posible la transmisión de un rayo , el rayo axial , y a este método de transmisión se le llama *monomodal* .

Transmisión Inalámbrica

SE utilizan medios no guiados , principalmente el aire . Se radia energía electromagnética por medio de una antena y luego se recibe esta energía con otra antena . Hay dos configuraciones para la emisión y recepción de esta energía : direccional y omnidireccional .



Microondas terrestres

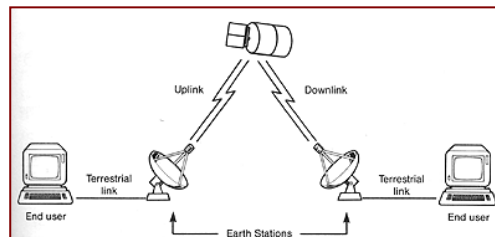


Suelen utilizarse antenas parabólicas . Para conexiones a larga distancia , se utilizan conexiones intermedias punto a punto entre antenas parabólicas .

Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores , Se usan para transmisión de televisión y voz.

La principal causa de pérdidas es la atenuación debido a que las pérdidas aumentan con el cuadrado de la distancia .

Microondas por satélite



El satélite recibe las señales y las amplifica o retransmite en la dirección adecuada . Para mantener la alineación del satélite con los receptores y emisores de la tierra , el satélite debe ser geoestacionario. Se suele utilizar este sistema para :

- Difusión de televisión .
- Transmisión telefónica a larga distancia .
- Redes privadas .

Debido a que la señal tarda un pequeño intervalo de tiempo desde que sale del emisor en la Tierra hasta que es devuelta al receptor o receptores , ha de tenerse cuidado con el control de errores y de flujo de la señal .

Las diferencias entre las ondas de radio y las microondas son :

- Las microondas son unidireccionales y las ondas de radio omnidireccionales .
- Las microondas son más sensibles a la atenuación producida por la lluvia .
- En las ondas de radio , al poder reflejarse estas ondas en el mar u otros objetos ,
- pueden aparecer múltiples señales "hermanas" .

Modelo OSI Vs TCP/IP



Aplicación: proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red subyacente en la cual se transmiten los mensajes.

Presentación: Codificación y conversión de datos para garantizar que los datos del dispositivo de origen puedan ser interpretados por la aplicación, compresión de los datos de forma que puedan ser descomprimidos por el dispositivo de destino. Encriptación de los datos para transmisión y descifre de los datos cuando se reciben en el destino.

Sesión: las funciones en esta capa crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos, y para reiniciar sesiones que se interrumpieron o desactivaron durante un periodo de tiempo

Transporte: seguimiento de la comunicación individual entre aplicaciones en los hosts origen y destino, segmentación de datos y gestión de cada porción, reensamble de segmentos en flujos de datos de aplicación, e identificación de las diferentes aplicaciones.

Red: direcciona, encapsula, enruta, y desencapsula.

Enlace : tomar un paquete IP y prepararlo para transmitirlo por el medio de comunicación. El principal servicio proporcionado por la capa de enlace de datos a las superiores es el de detección de errores y control.

Física: codificar en señales los dígitos binarios que representan las tramas de la capa superior, además de transmitir y recibir estas señales a través de los medios físicos.

Aplicación: Define los protocolos de aplicación TCP/IP y cómo se conectan los programas de host a los servicios del nivel de transporte para utilizar la red.

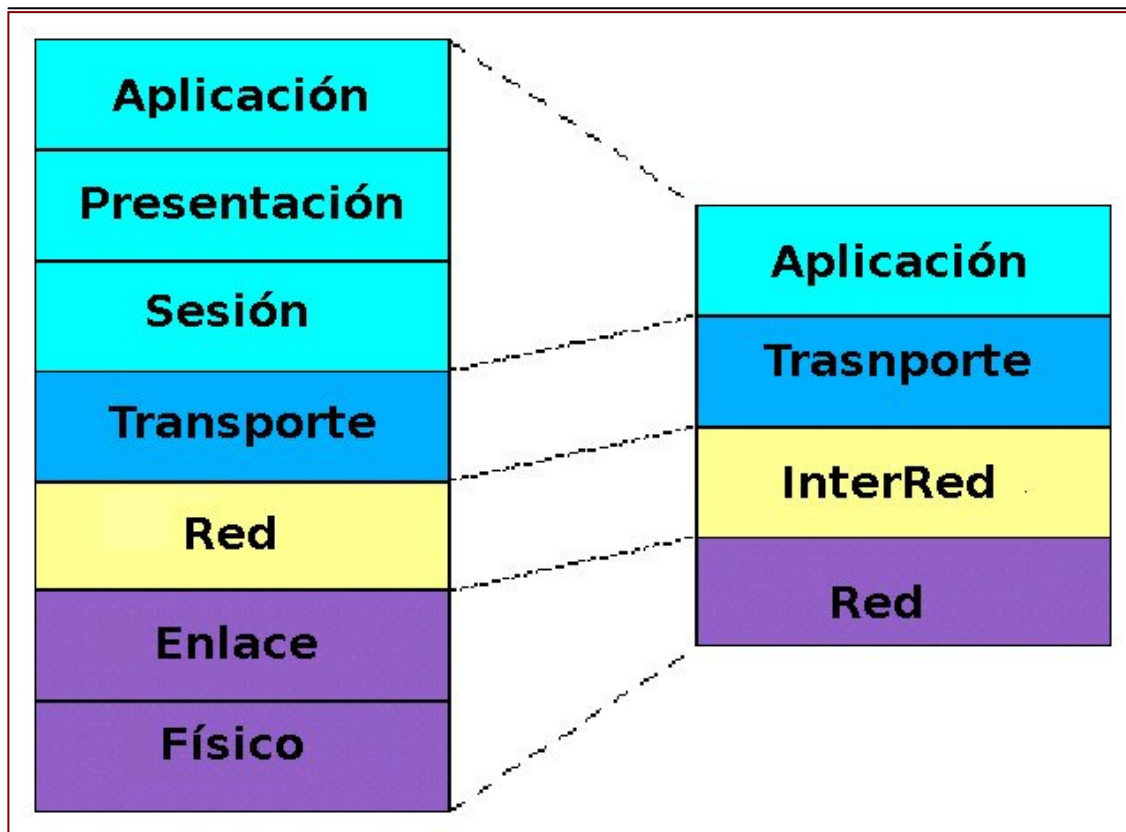
Transporte: Permite administrar las sesiones de comunicación entre equipos host. Define el nivel de servicio y el estado de la conexión utilizada al transportar datos.

Internet: Empaqueta los datos en datagramas IP, que contienen información de las direcciones de origen y destino utilizada para reenviar los datagramas entre hosts y a través de redes. Realiza el enrutamiento de los datagramas IP.

Acceso a Red: Especifica información detallada de cómo se envían físicamente los datos a través de la red, que incluye cómo se realiza la señalización eléctrica de los bits mediante los dispositivos de hardware que conectan directamente con un medio de red, como un cable coaxial, un cable de fibra óptica o un cable de cobre de par trenzado.



Comparación entre ambos modelos



REDES: Nivel 1

UNEWEB

Cableado RJ45

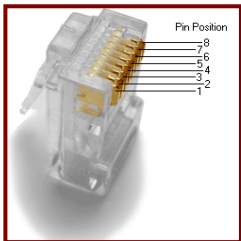
La **RJ-45** es una interfaz física comúnmente usada para conectar redes. de cableado estructurado, (categorías 4, 5, 5e y 6).













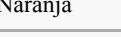

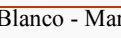
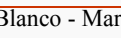
CABLE DIRECTO

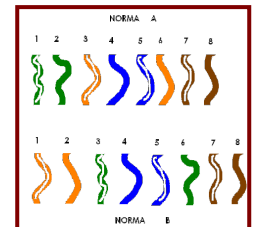
El cable directo de red sirve para conectar dispositivos desiguales, como un computador con un hub o switch. En este caso ambos extremos del cable deben de tener la misma distribución. No existe diferencia alguna en la conectividad entre la distribución 568B y la distribución 568A siempre y cuando en ambos extremos se use la misma, en caso contrario hablamos de un cable cruzado.

CABLE CRUZADO

Un cable cruzado es un cable que interconecta todas las señales de salida en un conector con las señales de entrada en el otro conector, y viceversa; permitiendo a dos dispositivos electrónicos conectarse entre sí con una comunicación full duplex. El cable cruzado sirve para conectar dos dispositivos igualitarios, como 2 computadoras entre sí, para lo que se ordenan los colores de tal manera que no sea necesaria la presencia de un hub. Actualmente la mayoría de hubs o switches soportan cables cruzados para conectar entre sí. A algunas tarjetas de red les es indiferente que se les conecte un cable cruzado o normal, ellas mismas se configuran para poder utilizarlo PC-PC o PC-Hub/switch.



Pin	Función	568A	568B
1	TX+ Transceive data +	 Blanco - Verde	 Blanco - Naranja
2	TX- Transceive data -	 Verde	 Naranja
3	RX+ Receive data +	 Blanco - Naranja	 Blanco - Verde
4	BDD+ Bi-directional data +	 Azul	 Azul
5	BDD- Bi-directional data -	 Blanco - Azul	 Blanco - Azul
6	RX- Receive data -	 Naranja	 Verde
7	BDD+ Bi-directional data +	 Blanco - Marrón	 Blanco - Marrón
8	BDD- Bi-directional data -	 Marrón	 Marrón



REDES: Nivel 1

UNEWB

SEGURIDAD

VARIOS TIPOS DE TÉCNICAS DE SEGURIDAD

Filtro de Paquetes: Se ve en cada paquete que entre o salga de la red y acepta o rechaza basándose en reglas definidas por el usuario. El filtrado de paquetes es bastante eficaz y transparente a los usuarios, pero es difícil de configurar.

Aplicación de Pasarela: Aplica mecanismos de seguridad para aplicaciones específicas, tales como servidores FTP y Telnet. Esto es muy eficaz, pero puede imponer una degradación del rendimiento.

Circuito a nivel de pasarela: Aplica mecanismos de seguridad cuando una conexión TCP o UDP es establecida. Una vez que la conexión se ha hecho, los paquetes pueden fluir entre los anfitriones sin más control.

Servidor proxy: Intercepta todos los mensajes que entran y salen de la red. El servidor proxy oculta de manera eficaz las verdaderas direcciones de red.

Cifrado de la información:

WEP (Privacidad equivalente al cableado): Fácil de romper. Aproximadamente 5 horas sin inyectar tráfico. Media hora con ataque basado en inyección de tráfico. Depende de la suerte.

TKIP (Temporal Key Integrity Protocol): Corrige los fallos del WEP. Internamente cambia la clave periódicamente. No deja inyectar tráfico porque enumera los paquetes. Muy difícil pero teóricamente posible.

CCMP (Counter Mode with CBC-MAC Protocol): Utiliza AES (Rijndael), el cifrado más fuerte actualmente. Necesita hardware especial.