Material de estudio obligatorio Eje Temático N° 1

Sitio: Instituto Superior Politécnico Córdoba
Curso: Programador de Aplicaciones Móviles - TSDWAD - 2022
Libro: Material de estudio obligatorio Eje Temático N° 1

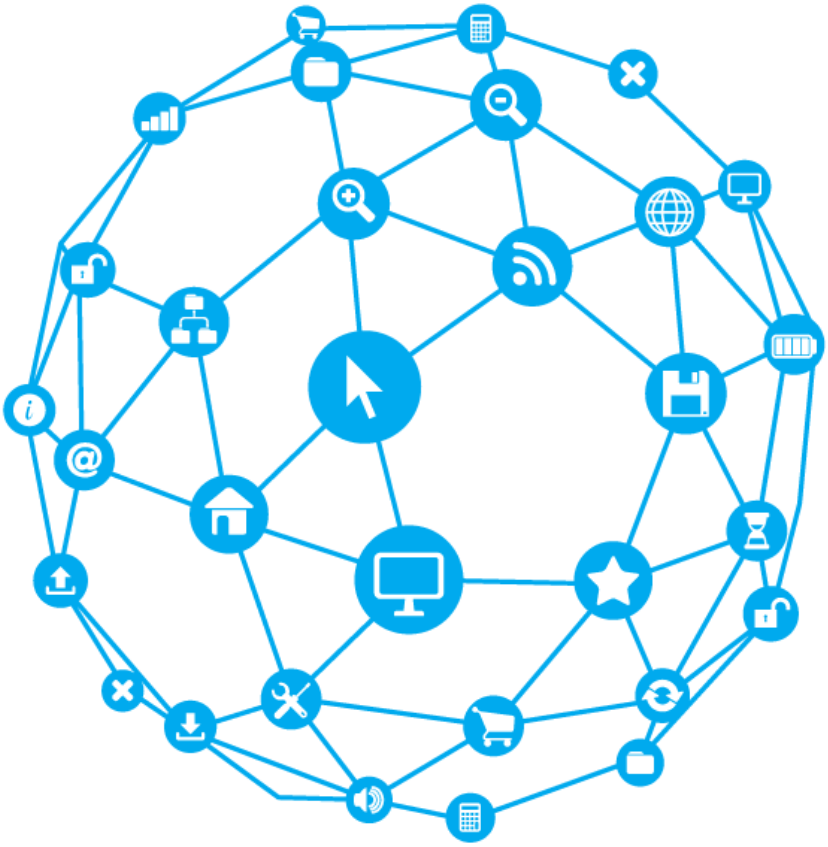
Imprimido por: Ezequiel Maximiliano GIAMPAOLI
Día: martes, 22 agosto 2023, 4:43 PM

Descripción

Redes

Tabla de contenidos

1. capitulo 1: redes



1.1. Topologías de Red

Topología de red

La topología de red define la estructura de una red.

Por una parte de la definición tenemos la **topología física,** que es la disposición real de los cables o medios.

Por parte es la **topología lógica**, que define la forma en que los hosts acceden a los medios para enviar datos.

Topologías Físicas

Las topologías físicas más comúnmente usadas son las siguientes:

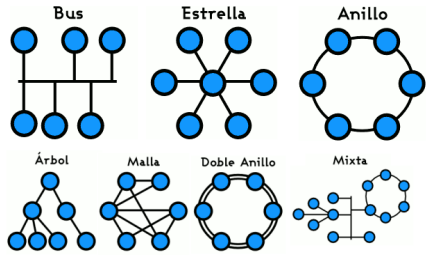


Figura: Topologías Físicas

BUS

• Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.

ANILLO

• La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.

ESTRELLA

• La topología en estrella conecta todos los cables con un punto central de concentración.

ESTRELLA EXTENDIDA

• Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.

JERÁRQUICA

• Una topología jerárquica es similar a una estrella extendida. Conectando de modo jerárquico switches entre sí o switches y routers.

MALLA

La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente.

TOPOLOGIA LÓGICA

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

Broadcast

La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás

hosts del medio de red.

- No existe una orden que las estaciones deban seguir para utilizar la red.
- Es por orden de llegada.
- **Ej:** Ethernet funciona así.

Tokens

La segunda topología lógica es la transmisión de tokens.

La transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial.

- Cuando un host recibe el token, ese host puede enviar datos a través de la red.
- Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir.
- Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos
- distribuida por fibra (FDDI).

1.2. Tipos de Redes, Caracteristicas y Funciones

Tipo de redes, características y funciones

Introducción

Comenzamos con un poco de historia sobre redes luego seguiremos describiendo los dispositivos de red y las disposiciones físicas, lógicas y del cableado de las redes.

Luego comparamos los distintos tipos de redes: Redes de área local (LAN), redes de área

metropolitana (MAN), redes de área amplia (WAN) y redes privadas virtuales (VPN).

Redes de datos

Las redes de datos se desarrollaron como consecuencia del desarrollo de aplicaciones comerciales

diseñadas para las computadoras personales PC y fueron evolucionando con el paso del tiempo:

1-Originalmente los sistemas informáticos estaban constituidos por un MainFrame, que se encargada de realizar el procesamiento de todos los datos, al cual se conectaban terminales bobas.

2- las computadoras no estaban interconectadas entre sí, no había una manera eficaz de compartir datos entre varias computadoras.

3- Para compartir datos entre computadoras y/o usuarios se utilizaban los disquetes (no era eficaz ni económico).

Ej: si se modificaba un archivo era necesario compartirlo con el resto de las personas que lo usaban

Ej: si dos usuarios modificaban un archivo, al compartirse se perdía alguna de las dos modificaciones

Era necesaria una solución que permitiera:

- Compartir archivos
- Compartir periféricos
- Comunicar los ordenadores con eficiencia.

Llegaron las redes y las empresas se dieron cuenta que dicha tecnología les permitiría aumentar la productividad y disminuir los gastos. De este modo las redes se extendieron con gran rapidez.

La situación de los 80’

A mediados de la década de 1980, las tecnologías de red que habían emergido se habían creado con implementaciones de hardware y software propietarios de cada empresa, por lo que utilizaban sus propios estándares corporativos.

Esto ocasionó que las redes y protocolos desplegados por empresas competidoras no fueran compatibles entre si, lo que obligaba a las empresas a desechar las redes actuales para desplegar una nueva red completamente desde cero con otra tecnología de hardware y software cuando se veían en la necesidad de ampliar las redes actuales.

Soluciones a este problema

Una de las primeras soluciones a este inconveniente fue la creación de los estándares de Red de área local (**LAN – Red de área local**).

-Estos estándares definieron un conjunto abierto de reglas a seguir para el desarrollo de hardware y software de red, de modo que las redes desplegadas por una empresa, fueran compatibles con cualquier otra asegurando de ese modo la interoperatividad entre equipos de diferentes empresas.

Surgen nuevas necesidades

Las redes de área local LAN crecieron rápidamente y trajeron muchas ventajas al trabajo diario, pero con el rápido crecimiento del intercambio de datos y de la necesidad de compartir recursos, estas redes tampoco fueron suficientes para el avance de la tecnología.

Entonces, surgió la necesidad de intercambiar información entre sucursales geográficamente distantes de la misma empresa, e incluso entre distintas empresas, esto dio lugar al surgimiento re las redes de área metropolitana (**MAN- red de área metropolitana)** y redes de área amplia (**WAN – red de área extensa**).

Las redes WAN permitieron conectar redes de usuarios dentro de áreas geográficas extensas, permitiendo que las empresas se comunicaran entre sí a grandes distancias.

La siguiente tabla muestra las dimensiones de las redes LAN y WAN.

Distancia entre PCs	Ubicación de las PCs	Denominación
10m	Habitación	LAN
100m	Edificio	LAN
1000m	Campus	LAN
100Km	País	WAN
1000Km	Continente	WAN
10000Km	Planeta	WAN

Elementos de red

Los equipos que se conectan a una red se denominan dispositivos o elementos de red.

Estos elementos pueden ser de usuario final o de red.

Elementos de usuario final

Entre los elementos de usuario final nos encontramos con PCs, Tablets, Smartphones, Cámaras IP,

Impresoras, escáneres y todos los dispositivos que interactúan directamente con el usuario final.

-Estos elementos, también llamados Hosts, permiten a los usuarios compartir, crear y obtener

información y están físicamente conectados con los medios de red mediante una tarjeta de interfaz

de red (**NIC**).

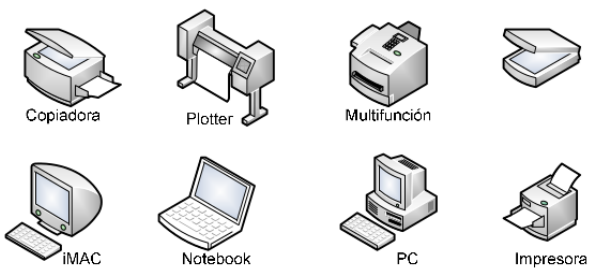


Figura: Elementos de red de usuario final.

NIC

Una tarjeta de red o adaptador de red es una placa de circuito impreso que adaptará la información al medio al cual está conectado el Host, dicho medio puede ser cobre (cable UTP), fibra óptica o el aire para las conexiones inalámbricas utilizadas hoy.

La tarjeta de red puede estar integrada en el Host, como es el caso de las notebooks, netbooks, tables y smartphone, o puede agregarse mediante la conexión a un puerto USB o en una de las ranuras de expansión de las Pcs.

MAC

Cada tarjeta de red, tiene un código único, denominado dirección de control de acceso al medio (MAC), la cual se utiliza para controlar la comunicación entre el Host y la red.

Los dispositivos de red

Los elementos de red, son aquellos que interconectan los distintos elementos de la red, permitiendo el intercambio de información y la comunicación entre elementos de usuario. Estos proporcionan:

- la red de transporte de información, -

- la concentración de conexiones,

- la conversión de los formatos de datos

- la administración de transferencia de datos

Con todo lo anterior se hace posible el buen funcionamiento de las redes y se logra que los Hosts puedan intercambiar información y recursos.

Elementos más Utilizados

Los elementos de red utilizados hoy son:

-puentes

-switches

-puntos de acceso (AP)

- routers inalámbricos y routers.

A continuación se brinda una breve descripción de estos elementos.

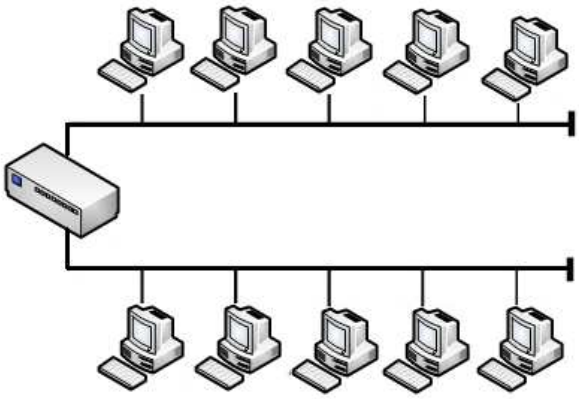
Repetidor

Los repetidores son dispositivos de red que se utilizan para regenerar las señales analógicas o digitales que se distorsionan a causa de pérdidas en la transmisión producidas por la

atenuación.

Un repetidor no toma decisiones inteligentes sobre los paquetes que recibe, consta por

lo general de dos puertos y todo lo que recibe por un puerto se replica por el otro.



Hub:

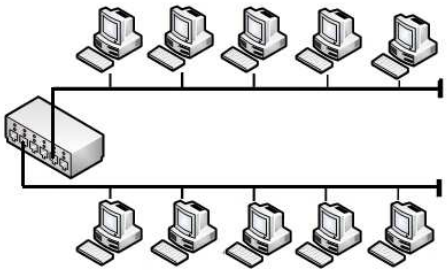
se utilizan para concentrar las conexiones y facilitar de ese modo el cableado de la red. La

aparición de los Hubs permitió utilizar cable UTP en lugar del cable coaxial para interconectar los

dispositivos de la red.

Tipos

Los Hubs pueden ser del tipo pasivo, de modo que no interfieren en la transmisión de datos, ó pueden ser activos que no sólo concentran hosts, sino que además regeneran señales.



Puente o Bridge: permiten la interconexión de distintos tipos de red.

por ejemplo una red Ethernet con una red Token ring ó una red Ethernet con una red WiFi

También se pueden utilizar para dividir una red grande en segmentos mas pequeños.

Función

Su función es adaptar el formato de transmisión de los datos de una red al formato de la otra para que puedan entenderse.

Los puentes realizan la administración básica de la transmisión de datos:

1) Conectan las LAN's

2) Además verifican los datos para determinar si les corresponde o no cruzar el puente.

Esto aumenta la eficiencia de cada parte de la red.

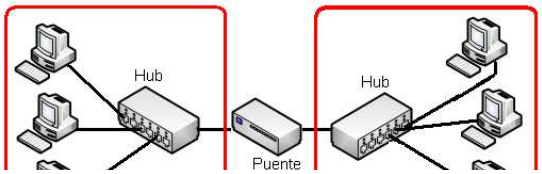


Figura: Puente o Bridge

Switch:

un switch es como un puente, pero en lugar de tener 2 puertos, puede tener múltiples

puertos ya sea para:

-conectar dispositivos finales de usuario,

- o para conectar a otros dispositivos de red.

Importante:

- Agregan inteligencia a la administración de transferencia de datos,

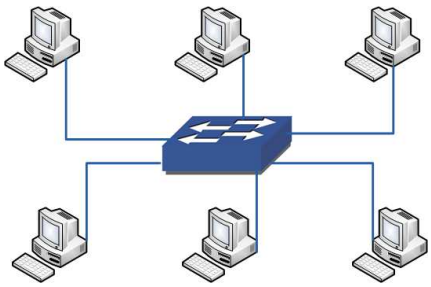
- son capaces de determinar si los datos deben permanecer o no en una LAN

-, y además pueden transferir los datos únicamente a la conexión que necesita esos datos basándose en la dirección de destino del paquete identificada

Ej: por la dirección MAC en las redes Ethernet y redes WiFi.

Diferencia entre Puente y Switch

Una diferencia importante entre un puente y un switch es que un switch no convierte formatos de transmisión de datos, es decir para interconectar una red Ethernet a una red WiFi, necesitamos conectar un puente al Switch para que realice la conversión, pero para el caso de interconectar dos redes Ethernet es suficiente con el Switch.



Routers:

Los routers poseen todas las capacidades indicadas arriba. Además:

- Los routers pueden regenerar señales.

- concentrar múltiples conexiones.

- convertir formatos de transmisión de datos.

- manejar transferencias de datos.

También pueden conectarse a una WAN, lo que les permite conectar LAN que se encuentran separadas por grandes distancias.

Ninguno de los demás dispositivos puede proporcionar este tipo de conexión.

1.3. Clasificación de Redes

Clasificación de Redes

Redes de área local (LAN)

Es un grupo de computadoras y dispositivos periféricos que comparten una línea de comunicaciones común o un enlace inalámbrico a un servidor dentro de un área geográfica específica.

Una red de área local puede servir a tan solo dos o tres usuarios en una oficina en casa o miles de usuarios en la oficina central de una corporación. Los propietarios de viviendas y los administradores de tecnología de la información (TI) configuran una LAN para que los nodos de la red puedan comunicarse y compartir recursos como impresoras o almacenamiento en red.

La red LAN requiere cables Ethernet y conmutadores de Capa 2 junto con dispositivos que se puedan conectar y comunicarse mediante Ethernet.

Las LAN más grandes a menudo incluyen conmutadores o enrutadores de capa 3 para agilizar los flujos de tráfico.

Una LAN permite a los usuarios conectarse a servidores internos, sitios web y otras LAN que pertenecen a la misma red de área amplia (WAN).

Ethernet y Wi-Fi son las dos formas principales de habilitar las conexiones LAN.

Las LAN constan de los siguientes componentes:

Computadores

Tarjetas de interfaz de red

Dispositivos periféricos

Medios de networking

Dispositivos de networking

Las LAN se encuentran diseñadas para:

Permitir el acceso múltiple a los medios.

Proporcionar conectividad continua a los servicios locales.

Controlar la red de forma privada con administración local.

Conectar dispositivos físicamente adyacentes.

Las LAN permiten a las empresas aplicar tecnología informática para compartir localmente

archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas. Un buen

ejemplo de esta tecnología es el correo electrónico.

Utilizan los siguientes dispositivos:

Repetidores

Hubs

Puentes

Switches Ethernet

Routers

Ej: Algunas de las tecnologías comunes de LAN son Ethernet, Token Ring y FDDI.

Redes de área amplia (WAN)

Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares.

Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias.

- Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes.
- Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas.

El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. Networking de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.

Las WAN están diseñadas para:

Operar entre áreas geográficas extensas y distantes	Posibilitar capacidades de comunicación en tiempo real entre usuarios
Brindar recursos remotos de tiempo completo, conectados a los servicios locales	Brindar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico

Las WAN están diseñadas para:

Operar dentro de un área geográfica extensa.	Permitir el acceso a través de interfaces seriales.
Suministrar conectividad parcial y continua.	Conectar dispositivos separados por grandes distancias.

Algunas de las tecnologías comunes de WAN son:

• Red digital de servicios integrados (RDSI)

• Línea de suscripción digital (DSL - Digital Subscriber Line)

• Redes IP/MPLS de proveedores de servicios telefónicos.

• Red óptica síncrona (SONET/SDH)

Redes de área metropolitana (MAN)

La MAN es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana.

Una MAN generalmente consta de una o más LAN dentro de un área geográfica común.

Ej: un banco con varias sucursales puede utilizar una MAN.

Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos.

También se puede crear una MAN usando tecnologías de puente inalámbrico.

Red privada virtual (VPN)

Una VPN es una red privada que se construye dentro de una infraestructura de red pública, como Internet.

Con una VPN, un empleado a distancia puede acceder a la red de la sede de la empresa a través de Internet, formando un túnel seguro entre el PC del empleado y un router VPN en la sede.

La VPN es un servicio que ofrece conectividad segura y confiable en una infraestructura de red pública compartida, como Internet.

Las VPN conservan las mismas políticas de seguridad y administración que una red privada.

Son la forma más económica de establecer una conexión punto-a-punto entre usuarios remotos y la red de un cliente de la empresa.

Tipos de VPN

Existen tres tipos principales tipos de VPN:

VPN de acceso:

Las VPN de acceso brindan acceso remoto a un trabajador móvil y una oficina pequeña/oficina hogareña (SOHO), a la sede de la red interna o externa, mediante una infraestructura compartida. Las VPN de acceso usan tecnologías analógicas, de acceso telefónico, RDSI, línea de suscripción digital (DSL), IP móvil y de cable para brindar conexiones seguras a usuarios móviles, empleados a distancia y sucursales.

Redes internas VPN:

Las redes internas VPN conectan a las oficinas regionales y remotas a la sede de la red interna mediante una infraestructura compartida, utilizando conexiones dedicadas.

Las redes internas VPN difieren de las redes externas VPN, ya que sólo permiten el acceso a empleados de la empresa.

Redes externas VPN:

Las redes externas VPN conectan a socios comerciales a la sede de la red mediante una infraestructura compartida, utilizando conexiones dedicadas.

Las redes externas VPN difieren de las redes internas VPN, ya que permiten el acceso a usuarios que no pertenecen a la empresa.

Redes internas y externas

Internas

Una de las configuraciones comunes de una LAN es una red interna, a veces denominada "Intranet".

- Los servidores de Web de red interna son distintos de los servidores de Web públicos,
- ya que es necesario que un usuario público cuente con los correspondientes permisos y contraseñas
- para acceder a la red interna de una organización.
- Las redes internas están diseñadas para permitir el acceso por usuarios con privilegios de acceso a la LAN interna de la organización.
- Dentro de una red interna, los servidores de Web se instalan en la red. La tecnología de navegador se utiliza como interfaz común para acceder a la información, por ejemplo datos financieros o datos basados en texto y gráficos que se guardan en esos servidores.

Externas

Las redes externas hacen referencia a aplicaciones y servicios basados en la red interna, y utilizan un acceso extendido y seguro a usuarios o empresas externas.

Este acceso generalmente se logra mediante contraseñas, identificaciones de usuarios, y seguridad a nivel de las aplicaciones.

Por lo tanto, una red externa es la extensión de dos o más estrategias de red interna, con una interacción segura entre empresas participantes y sus respectivas redes internas.

Unidades Métricas

En los sistemas digitales, la unidad básica del ancho de banda es bits por segundo (bps).

Ancho de Banda:

El ancho de banda es la medición de la cantidad de información, o bits, que puede fluir desde un lugar hacia otro en un período de tiempo determinado, o segundos.

-Aunque el ancho de banda se puede describir en bits por segundo, se suelen usar múltiplos de bits por segundo. En otras palabras, el ancho de banda de una red generalmente se describe en términos de miles de bits por segundo (kbps), millones de bits por segundo (Mbps), miles de millones de bits por segundo (Gbps) y billones de bits por segundo (Tbps).

A pesar de que las expresiones ancho de banda y velocidad a menudo se usan en forma indistinta, no significan exactamente lo mismo.

Se puede decir, por ejemplo, que una conexión T3 a 45Mbps opera a una velocidad mayor que una conexión T1 a 1,544Mbps. No obstante, si sólo se utiliza una cantidad pequeña de su capacidad para transportar datos, cada uno de estos tipos de conexión transportará datos a aproximadamente la misma velocidad.

Por ejemplo, una cantidad pequeña de agua fluirá a la misma velocidad por una tubería pequeña y por una tubería grande. Por lo tanto, suele ser más exacto decir que una conexión T3 posee un mayor ancho de banda que una conexión T1. Esto es así porque la conexión T3 posee la capacidad para transportar más información en el mismo período de tiempo, y no porque tenga mayor velocidad.

Ej: Unidades de transferencia

Unidad de Ancho de	Abreviatura	Banda Equivalencia
Bits por segundo	bps	1 bps = unidad fundamental del ancho de banda
Kilobits por segundo	Kbps	1 Kbps = 1000 bps = 10^3 bps
Megabits por segundo	Mbps	1 Mbps = 1000000 bps = 10^6 bps
Gigabits por segundo	Gbps	1 Gbps = 1000000000 bps = 10^9 bps
Terabits por segundo	Tbps	1 Tbps = 1000000000000 bps = 10^{12} bps

1.4. Redes Ethernet

¿Qué es Ethernet y para qué sirve? Definición, usos y ventajas

Ethernet

Ethernet es un **estándar de redes de área local** creadas por la unión de varios ordenadores a través de cable. Este protocolo nace en 1970 de manos de Norman Abramson, el cual comenzaba a desarrollar su tesis doctoral que no vería la luz hasta el año 1973.

El objetivo era crear una conexión entre varios equipos informáticos que se encontraban en un área local cercana. Ej: hogar, oficina, etc

De manera que se podría compartir información entre ellos sin la necesidad de una conexión externa.

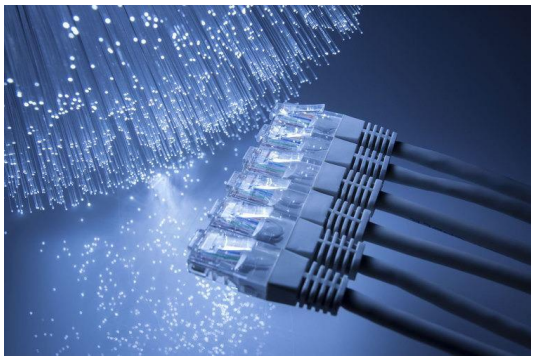
Es decir, por una parte tenemos la conexión de Internet es la que nos permite recibir datos de otros ordenadores externos sobre los que no tenemos control alguno, y por otra parte tenemos la conexión Ethernet que es la que establecíamos dentro de una red de ordenadores propios, pudiendo estar o no conectados a Internet, esto no afectaría en cuanto a la conexión interna.

Esta conexión se establece a través de un LAN donde irán conectados todos los ordenadores, periféricos y módems, de manera que habrá siempre un único cable que partirá desde cualquiera de los equipos o periféricos hacia el Lan, y por supuesto, todos los periféricos y ordenadores que estén conectados a dicho Lan, permanecerán conectados también entre sí.

Cómo funciona Ethernet

Para conseguir enviar los datos, es necesario que se fragmenten en pequeñas fracciones, lo cual es denominado "*Conmutación de paquetes*".

-Gracias a ello se evita que los datos se superpongan, contando cada uno de estos paquetes con una información concreta que será la que permita al propio paquete saber dónde se tiene que dirigir, es decir, a qué ordenadores tienen que acceder.



CSMA/CD

Uno de los principales problemas que tenían lugar antes de la **aparición del CSMA/CD**, era precisamente que en ocasiones varios equipos enviaban paquetes a la vez, lo que **hacía que se produjese una colisión entre los datos que afectaba a la transmisión**.

Sin embargo, gracias a este protocolo, antes de realizar el envío de los paquetes, los dispositivos:

1- contactan con la red para saber si se encuentra libre para realizar la transmisión, de manera que, en caso de ser así, enviar a los datos

2- si no esta disponible, esperará a que se libere para realizar el envío.

Nota:

Gracias a ello los datos llegan en perfecto estado y no se produce ningún tipo de colisión entre ellos en ningún momento, lo cual garantiza un funcionamiento mucho más fluido y sobre todo nos asegura que los datos siempre permanecerán en perfecto estado.

Ethernet - Wi-Fi

En general, una **conexión Ethernet es una conexión de Red mediante cable**, mientras que una **conexión Wi-Fi es una colección de Red de forma inalámbrica**.

- Podemos establecer conexiones Wi-Fi entre nuestros equipos, habitualmente a través de un router.
- La diferencia principal es que utilizamos Ethernet con la idea de conectar varios equipos dentro de una Red privada o interna de la propia empresa o vivienda, mientras que el Wi-Fi y generalmente se utiliza para la conexión a Internet.

Es decir, podemos utilizar ambos tipos de conexión en cualquier caso, pero siendo cada una de ellas para un tipo de conexión diferente.

La diferencia principal entre Wi-Fi y Ethernet es por un lado la velocidad de la conexión y por otro la fiabilidad:

El sistema inalámbrico puede resultar muy cómodo ya que evita la utilización de cables. Pero es mas lento que una conexión Ethernet.

Es decir, con Ethernet vamos a compartir información más rápidamente y con mayor fiabilidad que con Wi-Fi, mientras que con Wi-Fi tendremos más comodidad para establecer la conexión, evitando la utilización de cables entre los equipos.

Importante:

Es importante tener en cuenta la categoría del cable, en función de la velocidad a la que queramos transmitir los datos: en la actualidad, las categorías más habituales son la Cat. 5, Cat. 5e, Cat 6 y Cat 6a, permitiendo conexiones máximas de 100, 1000, 1000 y 10000 Mb/s respectivamente, logrando una mayor efectividad de la conexión conforme aumentamos la categoría y en relación con la distancia de la conexión.

1.5. Direccionamiento

direcciones de red- tipos-subneteo

1.6. Modelo OSI

Modelo de Referencia OSI

¿Qué es el modelo OSI?

El modelo de interconexión de sistemas abiertos (OSI, por sus siglas en inglés) es un modelo conceptual, creado por la Organización Internacional de Normalización (ISO), que permite que diversos sistemas de comunicación se comuniquen usando protocolos estándar.

En resumidas cuentas, el modelo OSI proporciona un estándar para comunicar sistemas entre sí.

El modelo OSI se puede entender como un lenguaje universal de comunicación entre sistemas de redes informáticas que consiste en dividir un sistema de comunicación en siete capas abstractas, apiladas en vertical.

Ej. de seguridad----Cada capa del modelo OSI tiene una función específica y se comunica con las capas superiores e inferiores. Los ataques Ddos se dirigen a capas específicas de una conexión de red, los ataques a la capa de aplicación se dirigen a la capa 7, mientras que los ataques a la capa de protocolo se dirigen a las capas 3 y 4.

¿Por qué es importante el modelo OSI?

Aunque la red moderna de Internet no se adhiere estrictamente al modelo OSI (más bien al conjunto de protocolos de Internet más sencillo), este continúa siendo muy útil de cara a la resolución de diversos problemas de red. Tanto si se trata de una persona que no puede acceder a Internet utilizando su portátil o la interrupción de una página web que impide el acceso a miles de usuarios, el modelo OSI puede ayudar a reducir el problema y aislar la fuente del mismo. Si el problema se puede reducir a una capa específica del modelo, se puede evitar mucho trabajo innecesario.

¿En que consiste?

El modelo OSI consiste en siete capas una que fueron diseñadas a partir de los siguientes principios:

• Una capa se debe crear donde se necesite una abstracción diferente.

• Cada capa debe realizar una función bien definida.

• La función de cada capa se debe elegir con la intención de definir protocolos estandarizados internacionalmente.

• Los límites de las capas se deben elegir a fin de minimizar el flujo de información a través de las interfaces.

• La cantidad de capas debe ser suficientemente grande para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

¿Cuales son las capas?

Capas

Se analizará cada capa del modelo, comenzando con la capa inferior y llegando a la superior en última instancia.

Importante:

El modelo OSI en sí mismo no puede ser considerado una arquitectura de red, ya que no especifica los servicios y protocolos exactos que se utilizarán en cada capa, solo indica lo que debe hacer cada capa.

Una división macro puede establecerse de la siguiente manera:

• **Capas altas:** Tratamiento de la información.

• **Capas bajas:** Encaminamiento de la información entre sistemas (PC, equipos) distantes.

Grupo	#	Nombre	Tecnología y protocolos	Componentes comunes
Capas superiores	7	Aplicación	DNS – DHCP – SNMP – FTP – POP3 – HTTP – TELNET	Aplicaciones compatibles con la red, correo electrónico, navegadores, servidores WEB
	6	Presentación	SSL – Shells – MIME	
	5	Sesión	NetBIOS Llamadas de procedimiento remoto	
Capas inferiores	4	Transporte	TCP & UDP	VoIP & Video – Firewall
	3	Red	IPv4 – IPv6 IPNAT – ARP RARP - ICMP	Direccionamiento IP – Ruteo
	2	Enlace de datos	Frame Ethernet – WLAN - ATM	Interfaces de red y controladores – WAN
	1	Física	Señales electricas – Ondas luminosas – Radio	Medios físicos, hubs y repetidores

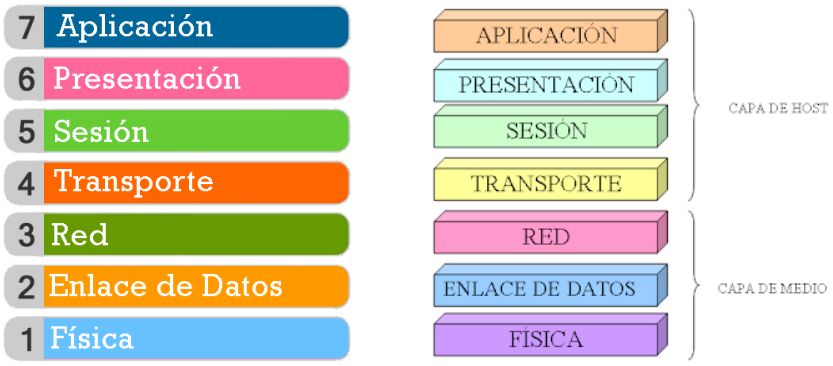


Figura 1.7: Modelo de referencia OSI

La Capa Física

En esta capa se lleva a cabo la transmisión de bits puros a través de un canal de comunicación.

Es la que se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere a:

• El medio físico:

- medios guiados: par trenzado, cable coaxial, fibra óptica, etc.

- medios no guiados: radio, infrarrojos, microondas, redes inalámbricas, etc.

• Características del medio: tipo y calidad del cable, tipo de conectores normalizados, etc.

• Forma en la que se transmite la información: codificación de la señal, niveles de tensión/intensidad de corriente eléctrica, modulación, tasa binaria, etc.

Funciones

Sus principales funciones se pueden resumir como:

• **Definir el medio o medios físicos** por los que va a viajar la comunicación:

- cable de pares trenzados (o no, como en RS232/EIA232),

- coaxial,

- guías de onda,

-aire,

- fibra óptica.

• **Definir las características materiales** (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos.

• **Definir las características funcionales de la interfaz** (establecimiento, mantenimiento y liberación del enlace físico).

• **Transmitir el flujo de bits a través del medio.**

• **Manejar las señales eléctricas/electromagnéticas**

• **Especificar cables, conectores y componentes** de interfaz con el medio de transmisión, polos en un enchufe, etc.

• **Garantizar la conexión** (aunque no la fiabilidad de ésta).

Importante:

Indirectamente el tipo de conexión que se haga en la capa física puede influir en el diseño de la capa de Enlace.

Atendiendo al número de equipos que comparten un medio hay dos posibilidades:

- **Conexiones punto a punto:** que se establecen entre dos equipos y que no admiten ser compartidas por terceros
- **Conexiones multipunto:** en las que dos o más equipos pueden usar el medio.

Consideraciones:

1-Así por ejemplo la fibra óptica no permite fácilmente conexiones multipunto y por el contrario las conexiones inalámbricas son inherentemente multipunto.

2-Hay topologías como el anillo, que permiten conectar muchas máquinas a partir de una serie de conexiones punto a punto.

3- A la hora de diseñar una red hay equipos adicionales que pueden funcionar a nivel físico, se trata de los repetidores (Hubs). En esencia se trata de equipos que amplifican la señal, pudiendo también regenerarla. Pregunta parcial

Y que actúan exclusivamente a nivel físico, a diferencia de los conmutadores Switches que actúan a nivel de enlace.

Capa de enlace de datos

Transmite datos

-sin error,

- sin duplicación,

-sin pérdida

entre sistemas adyacentes.

a)Enmascara a las capas superiores de las imperfecciones de los medios de transmisión utilizados.

b) Toma un medio de transmisión en bruto y lo transforma en una línea que parezca libre de errores de transmisión no detectados en la capa de red.

Procedimiento:

1- Esto lo lleva a cabo haciendo que el emisor divida los datos de entrada en marcos (tramas) de datos, que se transmitan en forma secuencial y se procesen los acuses de recibo que devuelve el receptor.

2- La capa enlace de datos se ocupa de crear y de reconocer los límites de los marcos, lo cual se

logra colocando patrones especiales de bits al principio y al final del marco.

3- Se ocupa de la retransmisión del marco, en caso de que una ráfaga de ruido lo haya destruido, pero las retransmisiones introducen la posibilidad de duplicarlos.

Debe resolver los problemas de marcos dañados, perdidos y duplicados.

• Proporciona la transmisión en bloques de bits.

• Proporciona detección de errores para ofrecerle al nivel superior una transmisión libre de errores.

• Establece el método de acceso al medio.

Capa de red

Dos sistemas comunicándose, pueden no ser adyacentes; es por ello que existen otros sistemas intermedios que sirven de relevo (nodos de redes).

La capa de red brinda los medios de comunicación de un sistema **extremo hacia otro**, asegurando el encaminamiento de la información.

Entonces:

1-Las rutas que seguirá la información se pueden basar en tablas estáticas, se pueden establecer al inicio de cada conversación o pueden ser altamente dinámicas.

2- Controla que en la red no se encuentren presentes demasiados paquetes a la vez, formando los cuellos de botella.

Problemas

La capa de red debe solucionar los siguientes problemas:

1- cuando un paquete debe pasar por varias redes hasta alcanzar su destino, puede que la dirección de las redes sea diferente de la enviada por la anterior o que una red no acepte el paquete por ser demasiado grande.

2- La capa de red debe lograr la comunicación entre redes heterogéneas.

3- En las redes de difusión, el encaminamiento es simple y esta capa con frecuencia es delgada o incluso inexistente.

• Define el encaminamiento y el envío de paquetes entre anfitriones.

• Responsable de conmutar y encaminar la información en la red.

• Debe conocer la topología para optar por la ruta mas corta.

Capa de Transporte

Se ubica en la frontera de las capas orientadas a transmisión y a tratamiento.

Funcion

Su función es ofrecer un servicio constante para las entidades de sesión, independientemente de la QoS de la red, **asegurando un servicio punto a punto.**

Entonces:

1- Acepta datos de la capa sesión, los divide en unidades más pequeñas si es necesario, los pasa a la capa de red y asegura que todos los pedazos lleguen correctamente al otro extremo.

2- Esta capa debe ser lo suficientemente versátil, como para aislar a las capas superiores de los cambios tecnológicos.

3- La capa transporte crea una conexión de red distinta para cada conexión de transporte que requiera la capa sesión.

-Si el volumen de transmisión es alto, esta capa puede crear múltiples conexiones de red, d ividiendo los datos entre las conexiones o puede multiplexar varias conexiones de transporte en la misma conexión de red para reducir el costo.

4- La multiplexación debe ser transparente a la capa sesión.

5- El tipo de servicio se determina al iniciar la sesión.

Nota:

-El tipo de conexión más común es un canal punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron.

-Otro tipo de conexión es el transporte de mensajes aislados sin garantía respecto al orden de entrega y la difusión de mensajes a múltiples destinos.

Importante!

La capa transporte es una verdadera capa de **extremo a extremo**, es decir un programa de la máquina fuente sostiene una conversación con un programa similar en la máquina destino. En las capas bajas, los protocolos se usan entre cada máquina y sus vecinas inmediatas (routers), y no entre las máquinas de origen y destino que pueden estar separadas por muchos enrutadores.

Nota:

Las capas 1, 2 y 3 están encadenadas (link to link), mientras que las capas 4, 5, 6 y 7 son extremo a extremo (end to end).

Mensajes:

El encabezado de cada mensaje sirve para saber a cuál conexión pertenece éste al pasar por un nodo de enrutamiento.

-La capa de transporte debe establecer y liberar conexiones, para ello debe poseer algún mecanismo de asignación de nombres, para que un proceso en una máquina pueda describir con quién quiere conversar.

-Proporciona un mecanismo denominado control de flujo para regular el flujo de información, a fin de que un nodo rápido no sature a uno lento.

Entonces:

- Garantiza una entrega confiable de la información.
- Permite soportar múltiples conexiones en un mismo anfitrión.
- Realiza control de flujo.
- Realiza control extremo a extremo para asegurarse que los datos lleguen correctamente.

Capa de Sesión

Permite establecer una relación entre dos aplicaciones:

-, organizar y sincronizar el diálogo,

permitiendo un intercambio

*full duplex, semiduplex o simplex.

Si el tráfico es en un solo sentido a la vez, esta capa puede ayudar a llevar el control de los turnos. Un servicio relacionado es el manejo de fichas, ya que para algunos protocolos es esencial que dos máquinas no intenten la misma operación al mismo tiempo, para ello la capa sesión otorga fichas que se pueden intercambiar.

Sólo el lado que posea la ficha podrá efectuar la operación.

-Gestiona las modalidades de recuperación en caso de incidente.

Para la sincronización de la transferencia de archivos, la capa sesión inserta puntos de verificación en la corriente de datos, de modo que después de cada interrupción sólo se deban repetir los datos que se transfirieron después del último punto de verificación.

Se podría usar una sesión para que un usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas.

Entonces:

- Establece el inicio y final de la sesión.
- Organiza y sincroniza el diálogo entre usuarios.
- Referencia a los dispositivos por nombre y no por dirección
- Recupera la sesión

Capa de Presentación

Se hace cargo, facilitando el trabajo de las entidades de la capa aplicación, de las diferentes sintaxis abstractas o de transferencia, así también como de la semántica de los datos intercambiados.

Sus servicios incluyen:

• Conversiones de código y de formatos de datos.

• La compresión y la encriptación de los datos.

• Un ejemplo, es la codificación de datos en una forma estándar acordada.

La información en una computadora se representa como cadena de caracteres, enteros, cantidades de punto flotante; estos códigos se representan con cadenas de caracteres como (ACSII, Unicode) y enteros (Complemento a uno o a dos).

Con el fin de comunicar computadores con representaciones diferentes, la información a intercambiar se puede definir en forma abstracta, junto con un código estándar que se use en el cable.

De esta manera, la capa presentación adapta la representación que se usa dentro de cada computadora, a la representación estándar de la red y viceversa.

Capa de Aplicación

Brinda los servicios de comunicación a los usuarios. Es una caja de herramientas normalizadas.

Los protocolos pueden ser:

• Relativos a la gestión de las aplicaciones o del sistema, por ejemplo:

explorador de windows, programa para monitorear las redes IP.

• Específicos de la aplicación, por ejemplo: servidores DHCP, DNS,

Proxy, NAT, FTP, e-mail, Web, etc.

Esta capa debe poseer protocolos que sean capaces de crear un Terminal virtual de red abstracta, la cual debe realizar la adaptación de los diferentes programas de aplicaciones que poseen las máquinas de una red, con el fin de lograr la compatibilidad de las mismas.

Se debe crear un programa para lograr la correspondencia entre la terminal virtual y la terminal real.

Se utiliza para la transferencia de archivos, ya que soluciona las incompatibilidades que puede haber en el tratamiento de archivos entre sistemas diferentes. También se emplea para el correo electrónico, la carga remota de trabajos, la búsqueda en directorios y otros recursos de uso general.

1.7. Protocolos TCP/IP

TCP/IP

Modelo de Referencia TCP/IP

Las siglas TCP significan Transmition Control Protocol (**Protocolo de Control de Transmisión)** y las siglas IP significan Internet Protocol **(Protocolo de Internet)**.

- TCP/IP propone un método de interconexión lógico de las redes físicas y define un conjunto de convenciones para el intercambio de datos.

Fue desarrollado por el DARPA (Defence Advanced Research Projects Agancy), y es operacional actualmente sobre la red Internet.

TCP/IP especifica:

• Programas de aplicaciones

• Protocolos asegurando un transporte de principio a fin

• Protocolos encaminando los datos dentro de la red

Analogía con el modelo OSI

• Capas 5-7: FTP, TELNET, SNMP, SMTP, DHCP, DNS, NAT,

Firewalls.

• Capa 4: TCP, UDP.

• Capa 3: IP, ICMP, ARP, RARP

• Capas 1-2: Cualquier Red Física (Ethernet, Token Ring, FDDI)

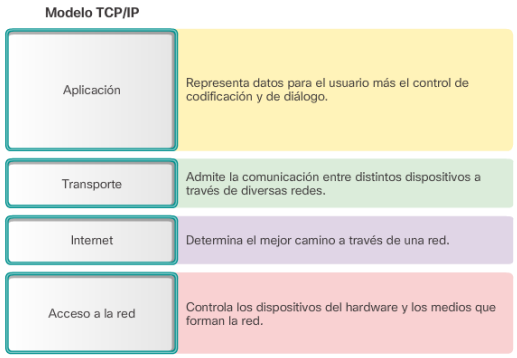


Figura 1.9: Modelo TCP/IP

Las capas que componen el modelo TCP/IP

Las funciones de las cuatro capas del modelo TCP/IP son similares a las capas del modelo OSI. A continuación se explicara brevemente los encabezados agregados por cada capa en el modelo de referencia TCP/IP.

Capa de Interfaz de Red

Esta capa encapsula el datagrama que proviene de la capa de red en un paquete denominado “trama”. Esta capa permite que el medio de transmisión físico sea confiable ya que agrega control y detección de errores.

En esta capa operan los Bridges y Switches de capa 2, ya que los mismos utilizan dos campos del encabezado de la trama para conmutar información desde una computadora origen hacia una de destino.

Los campos de la trama que utilizan los Bridges y Switches son la dirección “MAC de Origen” y la dirección “MAC de Destino”.

También, este nivel está en contacto con el material, es decir circuitos, cables, patch panells, etc...

Capa de Interred

El nivel IP encapsula los paquetes recibidos del nivel transporte en unidades llamadas “datagramas IP”. Los niveles IP cooperan al encaminamiento de los datagramas según un modo no conectado (gracias a unos algoritmos de encaminamiento). A los segmentos que envía la capa aplicación, la capa IP le agrega un encabezado para permitir que los datagramas puedan ser encaminados al pasar por varios enrutadores antes de llegar su destino final. Los campos con los cuales más vamos a trabajar son:

“IP de Origen” e “IP de Destino” y son los campos que utilizan los enrutadores para encaminar los datagramas.

Capa de Transporte

El nivel transporte brinda una comunicación de principio a fin entre dos programas de aplicación. Aquí se han definido dos protocolos de transporte de extremo a extremo.

El primero TCP (Protocolo de Control de Transmisión), es un protocolo confiable, orientado a la conexión, que permite que un flujo de bytes que se origina en una máquina se entregue sin errores en cualquier otra máquina en la interred. Divide el flujo de bytes entrantes en mensajes discretos y pasa cada uno de ellos a la capa de interred. En el destino el proceso TCP receptor reensambla e el flujo de salida los mensajes recibidos.

TCP también maneja el control de flujo para asegurarse de que un emisor rápido no sature a un receptor lento con mas mensajes de los que puede manejar.

El segundo, UDP (Protocolo de Datagrama de ususario), es un protocolo no confiable y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control de flujo de TCP y que desean proporcionar el suyo. También tiene un amplio uso en consultas únicas de solicitud-respuesta de tipo cliente-servidor en un solo envío, así como aplicaciones en las que la entrega puntual es mas importante que la precisa, como la transmisión de voz y video.

Capa de Aplicación

Las aplicaciones interactúan con protocolos del nivel transporte para

recibir o emitir informaciones. Cada programa de aplicación elige el tipo de servicio de transporte deseado y transmite sus datos al nivel transporte para encaminarlos.

La capa aplicación genera un mensaje que es pasado hacia la capa de transporte, después de que la aplicación ha elegido cual es el protocolo de transporte utilizado.

Esta capa contiene todos los protocolos de nivel mas alto. Los primeros incluyeron una Terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP).

Con el tiempo se han agregado muchos otros protocolos: DNS (Sistema de nombres de Dominio) para la resolución de nombres de host en sus direcciones de red; NNTP, para transportar artículos de noticias de USENET; http, para las páginas de World Wide Web y muchos otros.

Comparación: Modelos OSI y TCP/IP

Comparando el modelo OSI con los modelos TCP/IP, surgen algunas similitudes y diferencias.

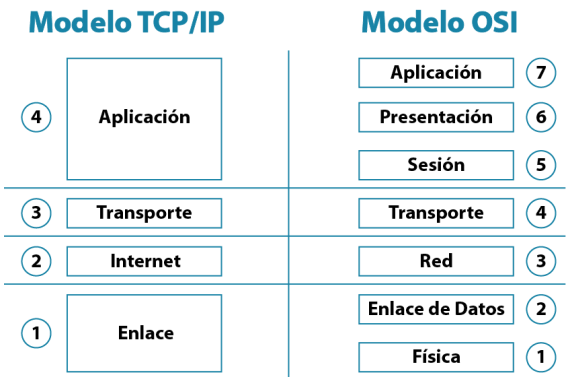


Figura: Comparación de Modelos

Las similitudes incluyen:

• Ambos se dividen en capas.

• Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.

• Ambos tienen capas de transporte y de red similares.

• Ambos modelos deben ser conocidos por los profesionales de networking.

• Ambos suponen que se conmutan paquetes. Esto significa que los paquetes individuales pueden usar rutas diferentes para llegar almismo destino. Esto se contrasta con las redes conmutadas por circuito, en las que todos los paquetes toman la misma ruta.

Las diferencias incluyen:

• TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.

• TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.

• TCP/IP parece ser más simple porque tiene menos capas.

• Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos.

En comparación, por lo general las redes no se desarrollan a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

Aunque los protocolos TCP/IP representan los estándares en base a los cuales se ha desarrollado la Internet, este currículum utiliza el modelo OSI por los siguientes motivos:

• Es un estándar genérico, independiente de los protocolos.

• Es más detallado, lo que hace que sea más útil para la enseñanza y el aprendizaje.

• Al ser más detallado, resulta de mayor utilidad para el diagnóstico de fallas.

1.8. Dominios de colisión y Dominios de Broadcast.

Dominios de colisión y dominios de broadcast.

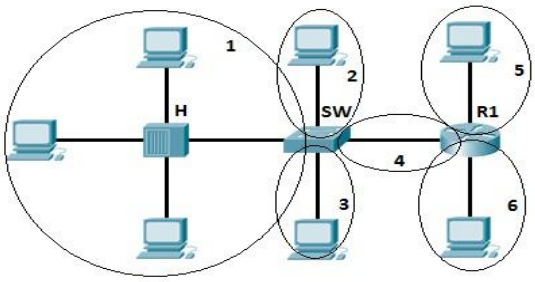
Dominio de colisión

Los dominios de colisión son los puntos de la red en que los mensajes pueden «chocar», este chocar debe entenderse como el momento en que dos o más mensajes son enviados compartiendo el mismo medio físico a la vez.

Cuando esto pasa, el mensaje *a priori* habrá sido alterado o no se puede asegurar que el receptor lo haya recibido correctamente, es por esto que Ethernet implementa **CSMA/CD** (*Carrier sense multiple access with collision detection*) para detectar las colisiones, descartar los tramas (*frames*)

y proceder con la secuencia de reenvío retrasada un tiempo aleatorio.

Importante: las colisiones están asociadas a la capa 2 del modelo OSI—



Ej: áreas que comparten el mismo dominio de colisión.

Consideraciones:

1- los hubs no dividen el dominio de colisión, más bien lo amplian.

2- los Switches y los Routers si separan los dominios de colisión.

Nota:

Cuando nos referimos a dominio de colisión y su medio de transmisión, estamos hablando de cualquier medio físico, no sólo a los cables UTP/STP o coaxiales, estas colisiones también se pueden producir en las transmisiones radio como WiFi que emplea CSMA/CA (*Carrier sense multiple access with collision avoidance*) para atajar este problema.

Dominio de *broadcast*

Un dominio de *broadcast (o do*minio de difusión) es una separación lógica dentro de la red de ordenadores en la que los mensajes, normalmente paquetes de capa 3 en el modelo OSI, pueden ser difundidos para que todos los equipos dentro de ese espacio, definido lógicamente, los puedan recibir.

Los Hub, switches y bridges no limitan el dominio de broadcast.

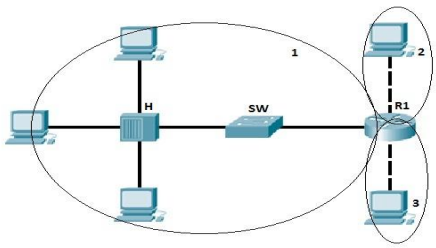


Figura: dominios de broadcast

- los equipos que limitan los dominios de *broadcast* por antonomasia son los *router*

- *los* switches pueden limitar esta difusión creando VLANs

En gral son los puertos del *router* los que marcan la división de los dominios de broadcast.

1.9. DMZ-Anexo

Se anexa un pequeño resumen con los puntos mas importantes de una configuración de seguridad de red DMZ

Link al resumen...