Unidad 1

Caracterización de redes

Planificación y Administración de Redes

Índice

Introducción

A lo largo de la historia la comunicación ha sido uno de los principales campos donde la tecnología más ha intentado avanzar.

Junto con el inicio de los ordenadores, fue surgiendo la necesidad de establecer un modo de comunicación entre los distintos equipos para poder realizar los traspasos de información.

En esta unidad introductoria, iremos viendo de manera progresiva en que se basa la comunicación, para finalmente poder hablar del concepto de red en concreto, y explicar cómo surge y a que se debe que haya cobrado tanta importancia hoy en día.

Se tratará de primera mano con el modelo OSI y sus distintos protocolos, realizando una comparativa entre este y el modelo TCP/IP.

Por último, tendremos en cuenta que hay ciertas aplicaciones de terceros que nos ayudarán a realizar monitorizaciones de la red.

Al finalizar esta unidad

- Conoceremos los principios de la comunicación.
- Sabremos lo que es una red, sus distintas características y las topologías que se aplican a ellas.
- Podremos clasificar las redes dependiendo del área que abarquen.
- Seremos capaces de hacer conversiones entre los principales sistemas de numeración y usarlos correctamente.
- Sabremos los estándares que definen las redes y su composición.
- Podremos definir la arquitectura TCP/IP, los protocolos que se abarcan, y el modelo OSI.
- Seremos capaces de realizar capturas de red con WireShark.

1.1. La comunicación

1.1.1. Conceptos

La función de un ordenador es la de procesar la información que le llega de acuerdo a las instrucciones de un programa. Hay que destacar que no siempre coinciden el lugar donde se procesa al que se ha almacenado. Esto se traduce en que existe la necesidad de transportar dicha información desde donde se encuentra almacenada a donde se ha creado, lo que produce una comunicación.

Cuando hablamos de una comunicación a distancia entre equipos informáticos nos referimos a la telecomunicación, que se produce mediante el envío de señales. Para que esto funcione debemos de tener en cuenta todas las especificaciones lógicas como puede ser la detección y corrección de errores y hay que establecer una conexión física eligiendo el tipo de señal, por ejemplo.

Es importante que no confundamos la comunicación con la transmisión de señal, ya que esta última es la base sobre la que se establece la comunicación, pero no es lo mismo.

Concepto de transmisión

Nos referimos a la transmisión como un proceso en q leu las señales son transportadas de un lugar a otro.

Las señales son entidades diversamente naturales manifestadas como magnitudes físicas, Las magnitudes físicas que más las suelen representar son las electromagnéticas y mecánicas.

Concepto de comunicación

Cuando transportamos la información realizando una transmisión de señales, estamos dando lugar a la comunicación.

Cada vez que hablamos de comunicación existe necesariamente una transmisión de señal, mientras que cuando hablamos de transmisión de señales, esta puede no llegar a dar lugar a la comunicación, porque no se transporta información, como pasa por ejemplo con las señales de radiación a las que estamos expuestos mediante el sol.

Mientras que la transmisión habla del transporte de señales físicas, la comunicación se refiere al transporte de la información en sí misma, de los datos. Esto quiere decir que la información es independiente de las señales que se use, pues es un mensaje que descifrará el receptor (o así al menos debe ser).

1.1.2. Elementos de un sistema de comunicación

En la imagen que más abajo se mostrará veremos que tanto emisor como receptor son los elementos que acotan la comunicación que llegan a través de un canal que contiene la información almacenada en un mensaje codificado mediante algún protocolo en concreto. De estos protocolos hablaremos más adelante.

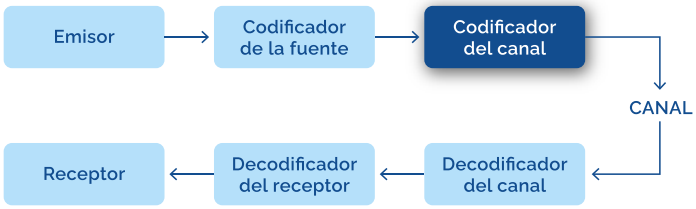

Imagen 1. Sistema de comunicación

El emisor y el receptor

El emisor es el primer elemento que interviene en el proceso de comunicación, pues es el encargado de comenzar el envío de información mientras que el receptor es el último elemento, este recoge la información y la descodifica para su entendimiento. En la gran mayoría de ocasiones, la información obtiene respuesta, lo que hace que ambos elementos terminales se intercambien el papel.

Emisor y receptor van siempre unidos, es decir, si no hay donde recibir información, no tiene sentido que sea enviada; lo mismo ocurre al revés. Es común también que, para un mismo emisor, haya múltiples receptores, como la radio, en la que una emisora de radio emite una información mediante ondas electromagnéticas hasta llegar a las antenas receptoras.

Aunque menos común, también hay veces en las que son múltiples los emisores y múltiples los receptores, y en muy pocos casos, múltiples emisores y un solo receptor.

El canal

La información se transmite a través de una señal, y esta a su vez es transportado en un medio al que definimos como canal.

Debido a que cada señal es de una naturaleza distinta, el canal debe ser óptimo para esta señal, por eso que cada uno es específico. Todo esto viene dado por las características físicas del mismo canal como por ejemplo la velocidad de transmisión, el nivel de ruido que genera, si es necesario una traducción, etc.

En términos de informática las señales más comunes son las electromagnéticas, que se pueden transportar a través del aire, por ejemplo. Un ejemplo de un canal también podría ser un cable de red, que manda la información mediante impulsos eléctricos.

El mensaje

Nos referimos al mensaje como los datos que deseamos intercambiar, a la información en sí, que puede estar formada por números, palabras, o simplemente codificaciones específicas.

El protocolo

Para poder transmitir los datos necesitamos que se establezcan unas ciertas reglas que nos ayudarán a controlar la representación, señalización, autenticación y transmisión de los datos a través de cualquier canal. Este conjunto de reglas es lo que definimos como protocolo.

Los protocolos tienen la función que procurar que, aunque haya un deterioro en el canal, la entrega de la información sea fiable.

Los elementos de un protocolo son:

- **Sintaxis.** Especifica el formato de los datos.
- **Semántica.** Especifica qué significa cada sección de los datos, o bien el significado del comando recibido, incluye información para el control de errores.
- **Temporización.** especifica cuándo pueden enviar los datos y la velocidad de transmisión.

Elementos físicos de una comunicación

A la hora de establecer la comunicación, hay una serie de elementos físicos que pueden intervenir dependiendo del tipo de comunicación, los más importantes son:

- **Equipos terminales.** Son los encargados de enviar y recibir los datos, como, por ejemplo, los teléfonos móviles o los televisores.
- **Transductores.** Un transductor se encarga de transformar señal de modo que sea comprensible tanto para el receptor como para el emisor.
- **Amplificadores.** Las señales analógicas sufren deformaciones al establecerse la comunicación, y el amplificador se encarga de devolverle su amplitud de onda.
- **Repetidores.** Regeneran señales digitales. Lo que hace este elemento no es amplificar la señal, sino que vuelve a construirla de nuevo para lanzarla como una nueva, pero con el mismo contenido.
- **Conmutadores.** Se encargan de que haya un canal de comunicación apropiado para cada situación. Comúnmente llamados Switches cuando hablamos del aparato en sí, hay también grandes conmutadores formados por varios dispositivos, un ejemplo de esto es una central telefónica.
- **Routers.** Su misión es la de darle la dirección correcta a las señales que recibe dependiendo de múltiples factores como distancia, longitud de señale, etc.

1.1.3. Modos de transmisión

Los modos de transmisión hacen referencia a las direcciones que toman los flujos de datos y hay tres tipos de comunicación dependiendo de los modos de transmisión:

- **Comunicación simplex.** En este tipo de comunicación solo tenemos un emisor y u receptor, y la dirección en la que va la información es única uniforme, siempre la misma.

Imagen 2. Modo de transmisión simplex

- **Comunicación semidúplex.** En este tipo de comunicación, ambos dispositivos son capaces de actuar de emisor y receptor alternándose, es decir, la información se puede transmitir en ambas direcciones, pero no de manera simultánea.

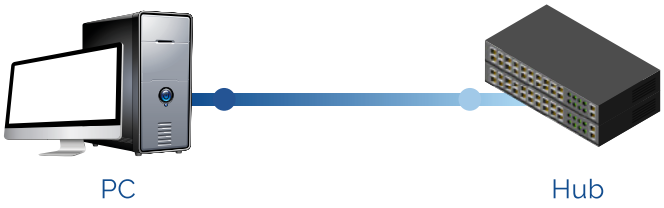

Imagen 3. Modo de transmisión semidúplex

- **Comunicación dúplex.** Es aquí cuando ambos dispositivos funcionan al mismo tiempo como emisor y receptor, y transmiten información en ambas direcciones simultáneamente. Este es realmente el método más usado y el más frecuente en términos de red.

Imagen 4. Modo de transmisión dúplex

1.2. Concepto de red. Ventajas

1.2.1. Concepto de red

Una red se trata de una agrupación de equipos informáticos que se encuentran interconectados entre sí e intercambian información y recursos.

Dependiendo de la necesidad que tengamos y del rango que queramos cubrir, tenemos varios tipos de redes, las cuales pueden estar compuestas desde dos ordenadores conectados por un cable hasta millones de ordenadores interconectados como es el caso de Internet.

Los componentes básicos de una red son:

- El software de red que suele ir implementado en el sistema operativo ya sea cliente o servidor.
- La tarjeta o adaptador de red, inalámbrico o cableado.
- El medio, ya hemos dicho antes que puede ser muy variado.
- Los equipos terminales, es decir, emisor y receptor de comunicación (ordenadores, impresoras, móviles).

Intranet

Una Intranet es un conjunto de equipos informáticos que tienen salida a internet, pero internet no puede acceder a ellos, de modo que sí que se puede ofrecer todo servicio típico de internet entre ellos de manera interna como puede ser un servidor dns o un servidor de correo.

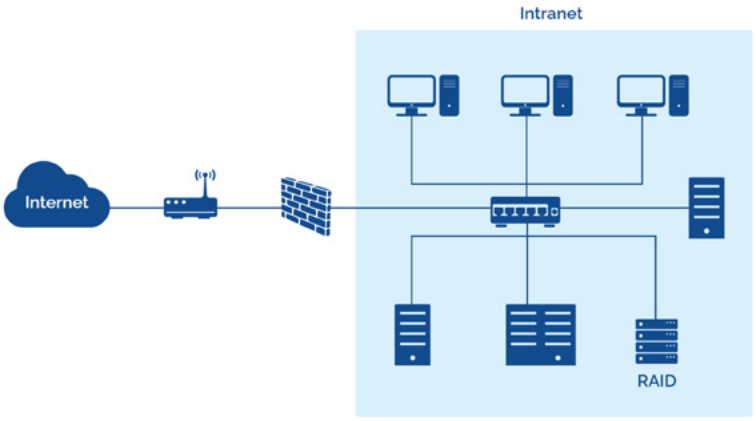

Imagen 5. Intranet

1.2.2. Ventajas de las redes

Compartir archivos y programas

Las redes nos ayudan en multitud de tareas, pero sin duda una de las más grandes e importantes en la capacidad de intercambiar información.

Esta información se puede transmitir de distintos modos, pero es común que haya un servidor central que haga de servidor de ficheros donde se almacenan archivos y recursos establecidos de manera jerárquica de modo que solo puedan acceder ciertos usuarios con unos permisos preestablecidos.

En el caso de los programas, suele haber un servidor central donde se instala el programa principal y en los demás distintos equipos se instala el cliente que va a ayudar a que haya comunicación con el master y los demás equipos de la red.

Compartir los dispositivos

Algunos de los recursos de hardware en una red una red incluye impresoras, scanners, discos duros, puntos de acceso inalámbricos, etc. Cuando se trabaja en red, se hace lógico comprar dispositivos de mejor calidad ya que una gran cantidad de usuarios accederán a ellos y llevará un desgaste mayor.

Gestión centralizada

Antes hemos comentado que hay programas que se instalan en un servidor central que controla los clientes instalados en los equipos, pues bien, esto es debido a que, por lo general, en los sistemas en red se usa una gestión centralizada.

Esta gestión se basa en que todo lo que no depende de manera estricta de cada sistema operativo en particular es controlado por un servidor central. Aquí por ejemplo hablamos de las actualizaciones de los equipos, las copias de seguridad, el antivirus, el mantenimiento regular de equipos a nivel de software, etc.

Seguridad

La seguridad va de la mano de varios puntos anteriormente nombrados ya que nos referimos a la gestión de malware en los equipos, pero también a que haya unas ACL o control de accesos para los archivos y programas compartidos en la red.

Interconexión

Como veremos más adelante, casi todos los sistemas operativos, independientemente de su estructura soportan los distintos protocolos de red establecidos y suelen trabajar con los más famosos. Esto hace posible que pueda haber una comunicación de red entre distintos equipos independientemente de si son Unix/Linux o Windows.

Organización de la empresa

A la hora de trabajar en conjunto por departamentos o secciones no siempre es necesario o posible que se disponga de una misma ubicación física, lo que se traduce en que gracias a distintas organizaciones que se adoptan a la hora de crear a los usuarios estos pueden compartir recursos, acceder a los mismos sitios, etc. Estas medidas son muy útiles a la hora de trabajar en proyectos en común y facilitan muchas labores tediosas.

1.3. Topologías de red

Llamamos topología a la distribución física de una red. Aunque existen multitud de ella, las principales son:

- **En bus:** todos los ordenadores se conectan a un bus o cable central.
- **En estrella:** todos los ordenadores se conectan a un dispositivo central.
- **En anillo:** los ordenadores se conectan unos a otros formando un círculo.
- **En árbol:** no todos los ordenadores están conectados con un cable; en algunas ocasiones habrá que pasar por varios ordenadores para intercambiar información entre otros dos.
- **En malla:** hay multitud de cables. Hay dos tipos de mallas a la hora de la verdad: un primer tipo en el que un equipo se interconecta con todos y en el segundo todos o casi todos los equipos se conectan entre sí mediante cables.

Un protocolo es un conjunto de normas y reglas establecidas de mutuo acuerdo entre los participantes de una comunicación, que deben seguir para poder comunicarse entre sí.

Para que la comunicación entre los equipos se establezca, estos deben de usar el mismo protocolo, es decir, deben de seguir las mismas reglas. Como un protocolo de vestuario en una celebración, en la cual no puedes entrar si no llevas el vestuario solicitado.

1.3.1. Topología en estrella

La estructura de esta topología es la siguiente: contamos con un elemento central que es al que se conectan los distintos elementos de una red.

Este elemento central es denominado centro, conmutador, repetidor o estación concentradora de la estrella. No tiene por qué tratarse de un ordenador, de hecho, no suele serlo, sino un dispositivo especial dedicado especialmente para esta función. (más adelante veremos cuales pueden ser).

Se trata de una estructura más bien débil porque depende de manera total del elemento central. Aunque también cabe destacar que todos los demás elementos podrían fallar de manera individual sin alterar el funcionamiento de la red.

Funcionamiento

Si un elemento de la red quiere enviar información a otro, se envía al dispositivo central y este mismo lo mandará al destinatario sin necesidad de pasar por todos los demás.

Ventajas

- Posee una fuerte seguridad porque el dispositivo central se encarga de filtrar la información, no enviándola en caso de detectar cualquier anomalía.
- Si un elemento que no sea el dispositivo central se estropea o incluso un extremo del cableado, la red no se ve alterada.
- Su instalación y configuración a la hora de añadir nuevos elementos es bastante sencilla.

Inconvenientes

- Disponemos de mucho cableado que conecta al elemento central de la red.
- Si falla este elemento central, se nos caerá la red en su totalidad.
- Es común que surjan cuellos de botella a la hora de acumular la información.
- Los mensajes con información han de pasar de manera obligatoria por el dispositivo central sin excepción alguna.

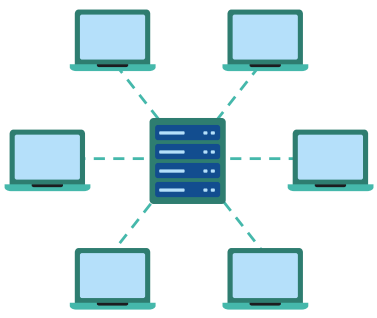

Imagen 6. Topología en estrella

1.3.2. Topología en bus

Esta topología se caracteriza porque tenemos un único canal de comunicaciones que es común para los equipos de la red.

Funcionamiento

La estructura principal es un cable largo actuando como una red troncal que hace posible la conexión de todos los equipos de red.

La información de un equipo a otro se producirá de manera directa o indirecta dependiendo de si contamos o no con un controlador que enrute los datos.

Un equipo enviará una serie de información a todos los equipos de la red, y cada tarjeta de red examinará dicha información para saber si es para ese equipo o no.

Ventajas

- Necesita poco cableado
- Es económica.
- Es fácil de instalar.
- Se pueden enviar los mensajes en los dos sentidos.
- Si un ordenador se estropea, la red puede seguir funcionando.
- Es fácil localizar el equipo que se ha estropeado.

Inconvenientes

- Si falla o se estropea el bus, la red no funcionará de ningún modo.
- Tiene muchos problemas de tráfico ya que toda la información pasa por todos los equipos.

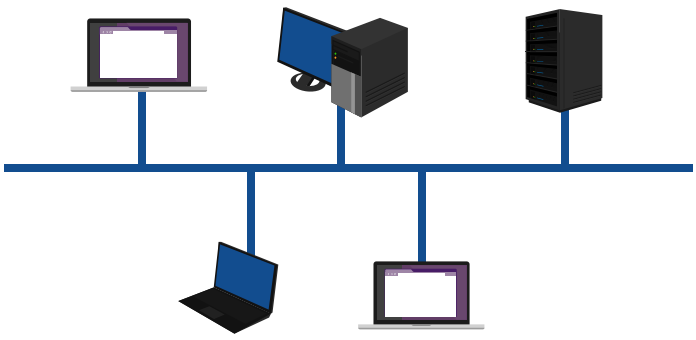

Imagen 7. Topología en bus

1.3.3. Topología en anillo

Dicha topología se caracteriza porque todos los elementos se encuentran unidos a otros dos, lo que hacer que se forme una estructura circular en forma de anillo. La información en este ámbito pasa de un equipo a otro mediante un puerto de entrada pasando a otro de salida hasta llegar al destinatario.

Los mensajes solo se envían en un único sentido, es decir, de manera unidireccional.

Funcionamiento

Un equipo manda la información desde el puerto de salida, y este va pasando por cada uno de los demás equipos hasta llegar a su destino, donde lo recibe el puerto de entrada.

Se pueden producir colisiones entre dos equipos si estos intentan mandar un mensaje al mismo tiempo, para lo que se suele usar un testigo o token que estará siempre circulando en el anillo. Si un equipo quiere enviar un paquete o token, buscará el testigo y si lo encuentra, querrá decir que ningún otro equipo intenta enviar información. Llegado a este punto el equipo recoge el testigo y da salida al mensaje hasta que llegue al destino, es entonces cuando liberará dicho testigo. Este método es conocido como técnica de paso de testigo.

Ventajas

- No hay problemas de congestión de trafico
- Es económica.
- Es fácil de instalar y de reconfigurar, en caso necesario.
- Si se produce un error, es fácil detectarlo.

Inconvenientes

- Si un ordenador o un cable se estropea, toda la red deja de funcionar.
- La información solo va en un sentido, lo que puede hacer que en algunas ocasiones sea un poco lento.
- La información debe pasar por muchos ordenadores.
- Al tener que pasar por muchos ordenadores, la información se puede ir deteriorando.

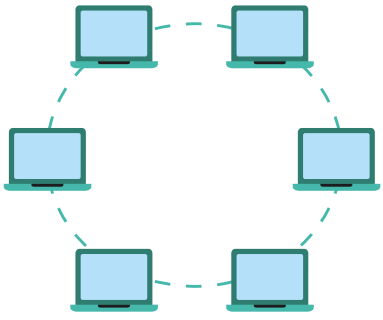

Imagen 8. Topología en anillo

1.3.4. Topología en árbol (estrella jerárquica)

Cuando los equipos informáticos empezaron a utilizarse en las empresas, surgió esta topología en la que los equipos se organizan de manera que su estructura es similar a la que tendrían los departamentos de una empresa.

Funcionamiento

Si un equipo lanza una serie de información, esta recorrerá todo el árbol hasta llegar a su destino.

Ventajas

- Es fácil de instalar y de añadir nuevos ordenadores
- Se pueden aislar las comunicaciones en una rema del árbol, si lo consideremos oportuno.

Inconvenientes

- Es poco utilizada, ya que normalmente es preferible utilizar otro tipo de topología.
- Se pueden generar cuellos de botella.
- Los mensajes tienen que recorrer mucho camino.
- Se necesita mucho cable.

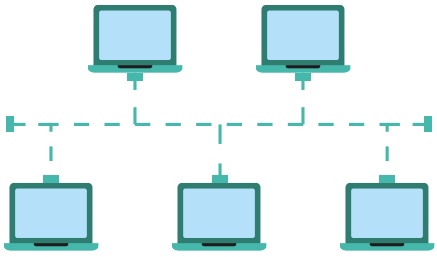

Imagen 9. Topología en árbol

1.3.5. Topología en malla

Todos los equipos se encuentran interconectados entre sí, de modo que, si una ruta falla, siempre habrá un camino distinto.

Funcionamiento

La ruta que llevará la información enviada podrá ser la elegida por el equipo, generalmente la más corta.

Ventajas

- Si en un camino o ruta falla el cableado, podemos enviar el mensaje por otro camino.
- Si un ordenador o un cable falla, la red seguirá funcionando.
- Es la mejor topología a la hora de enviar la información ya que siempre habrá canales disponibles. Además, casi siempre será una conexión directa a no ser que sea justo esa la que esté fallando,

Inconvenientes

- Es cara.
- Necesita de mucho cableado de red.
- Suelen ser unos pocos equipos, porque si no, se necesitaría mucho cableado.

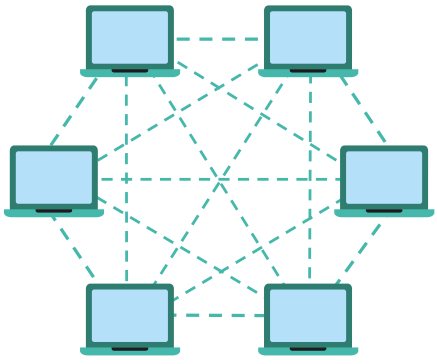

Imagen 10. Topología en malla

1.4. Clasificación general de las redes

Según el espacio que ocupan las clasificamos en:

- **PAN (personal area network = redes de área personal).** Son las redes de tamaño más pequeño. Normalmente se utilizan para conectar el móvil al ordenador y sincronizar datos o la impresora al ordenador, etc.
- **LAN (local area network = redes de área local).** Son redes de tamaño más grande que las anteriores, pero siguen siendo de tamaño reducido. Se utilizan para conectar algunos equipos entre sí y aprovechar todos los recursos que posee la red.
- **MAN (metropolitan area network = redes de área metropolitana).** Se consideran de tamaño mediano. Dan un radio de cobertura muy extenso, por ejemplo, una ciudad. Son las más utilizadas para distribuir el servicio de televisión por cable.
- **WAN (wide area network = redes de área amplia).** Poseen el tamaño más grande que existe. Son capaces de dar cobertura a espacios que engloban países. El ejemplo que más conocemos de red WAN es Internet.

1.4.1. PAN. Personal Area Network

Este tipo de redes son las más pequeñas y por lo general suelen girar en torno a una persona y a un solo equipo informático.

Lo más común es que se encuentren formadas por un ordenador, impresora, cascos, otro dispositivo portátil que se use menos, un teléfono móvil, etc.

Además, cabe destacar que su medio de comunicación suele ser por cables USB o por red inalámbrica bluetooth o Wi-Fi. Estas redes WPAN inalámbricas vienen definidas en el estándar IEE 802.15.

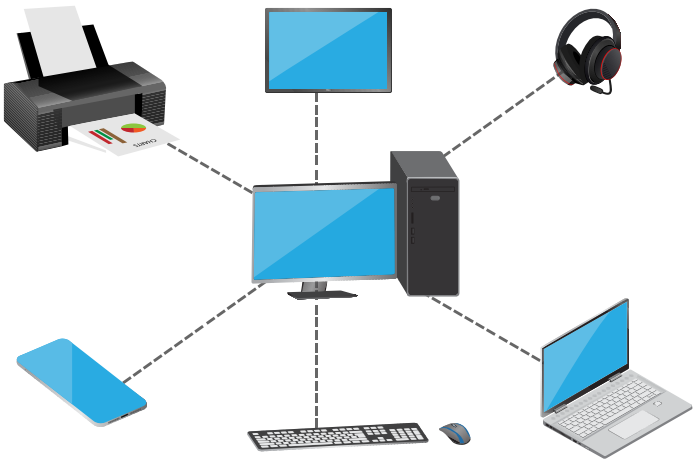

Imagen 11. PAN

1.4.2. LAN. Local Area Network

Las LAN o redes de área local son las que se establecen de manera privada y que por lo general se compenetra con la intranet. Estas suelen ser de poco tamaño, como una sede u organización hasta unos pocos kilómetros (muy pocos).

Como hemos dicho, normalmente se usan en empresas para interconectar los equipos de red con la intención de compartir recursos e información. Generalmente tienen una topología en bus, anillo o estrella.

Por último, hay que destacar que, aunque son para unos pocos kilómetros, desde hace años se han empezado a establecer Macro LANS que hacen posible que actúe como una LAN desde varios puntos del mundo ya que pertenecen a la misma organización.

Imagen 12. LAN

1.4.3. MAN. Metropolitan Area Network

Hablamos de una MAN como una red con una extensión superior a la de una ALN que, de manera general ocupa un área geográfica similar a una ciudad (de4 ahí su nombre), con alta tasa de transferencia y que integra varios servicios para toda el área como pueden ser datos, voz, video sobre fibra óptica, etc.

Casi siempre hoy en día estas redes se instauran por las compañías telefónicas y de internet, lo que hace que su estructura se base en fibra óptica multimodo.

Las distintas ventajas de las MAN son:

- Un muy buen ancho de banda ya que es necesario debido a la cantidad de recursos multimedia necesitados.
- Pueden tener hasta más de 500 nodos de acceso a la red distintos.
- Su extensión puede llegar hasta más o menos los 50Km, siempre lógicamente dependiendo de condiciones como la tecnología usada.
- Al ser redes tan "complejas", dispone de multitud de mecanismos que ayudan en la detección y corrección de errores, haciendo posible una alta disponibilidad.
- Como por lo general se usa fibra óptica y esta tiene una resistencia óptima a interferencias y ruidos, tiene una fiabilidad bastante alta frente a errores de transmisión.
- Por último, la fibra óptica como medio también hace posible que se traten de redes más seguras ya que solo se pueden interceptar si se intercepta el medio físico.

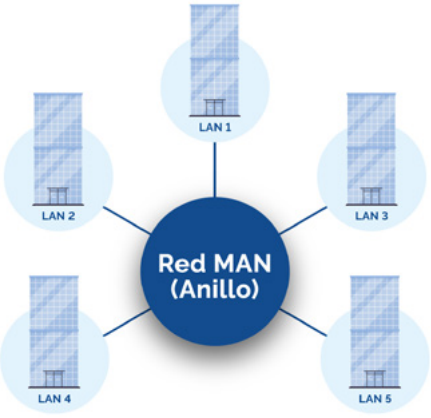

Imagen 13. MAN

1.4.4. WAN. Wide Area Network

Las redes o WAN o redes de área extensa ocupan un gran espacio geográfico llegando a ser del tamaño de un país o un continente y se usan para transmitir una información muy similar a la de las MAN.

Las tecnologías que más se usan a la hora de construir redes WAN son xDSL, ATM, Fream Relay y UTMs para teléfonos móviles.

Las WAN suelen utilizar enlaces punto a punto con paquete conmutado.

Durante mucho tiempo se han usado estos medios para para poder trabajar con redes en distintos países, pero desde hace unos años se ha empezado a usar de manera mucho más general las redes VPN.

Estas VPN (redes privadas virtuales) se componen de un sistema cifrado de información que hace el efecto de túnel de cara a que estemos conectados en la red interna de la empresa.

Unos de los ejemplos de redes WAN son por ejemplo la red telefónica conmutada de telefónica.

Imagen 14. WAN

1.5. Evolución del trabajo en red (networking)

La gran mayoría de quehaceres de una empresa de hoy en día necesitan de conexión a red, pero no siempre ha sido así, por eso vamos a introducir como ha ido evolucionando el trabajar con las redes.

Networking: Fase 1

Aunque al principio fue más bien lento, hubo un incremento exponencial en el uso de los equipos personales por parte de las empresas. Este impulso vino acontecido por algunos programas de gestión como puede ser Lotus (19839 u otros que se crearon de uso específico para empresas.

Networking: Fase 2

En esta segunda fase, con los equipos ya montados, a veces se necesitaba imprimir ciertos documentos y para solucionar esto se instalaban impresoras locales a esos ordenadores, pero no había para todos.

Cuando un empleado cuyo ordenador no tenía impresora necesitaba imprimir cualquier cosa, debía grabarla en un disquete y volcar esta información en un equipo con impresora conectada para posteriormente imprimirlo. Esto es conocido como "red a pie".

Networking: Fase 3

Conforme las empresas iban creciendo se empezaban a notar los numerosos inconvenientes derivados del uso de las "redes a pie". A raíz de esto las grandes organizaciones empezaron a invertir en redes LAN o de área local ya que esto facilitaba la transferencia de información a través de la red, no siendo necesario que se tenga que ir con el disquete de un equipo a otro. Además, con el nacimiento de las LAN también surgieron las primeras impresoras de red para todo el departamento o área en el que se trabaja.

No obstante, no se podía compartir la impresora de manera interdepartamental, lo que hacía que el problema no estuviera solucionado del todo aún.

Networking: Fase 4

En esta cuarta fase es cuando las empresas empiezan a tener una mayor extensión física divida en departamentos, ciudades, e incluso distintos continentes.

Esto resulta en que las LAN se distribuyeran por sedes, adaptando el hardware y el software específico para cada una de las sedes.

En este caso, cada uno de los departamentos, aunque aislado de los distintos departamentos, funcionaba de manera eficiente.

Para terminar, la pega fue que debido a esta no compenetración total entre departamentos había operaciones ineficientes que necesitaban ocupar a toda la empresa al igual que ciertos tiempos de espera amplios en lo referente al traspaso de información.

1.6. Sistemas de numeración

El equipo solo conoce dos estados, cero y uno, entonces, toda la información transmitida debe ser una sucesión de ambos dos; este es el llamado sistema binario {0,1}. Para que sea más cercano al usuario final también se han creado otros sistemas de numeración:

- **Octal:** utiliza ocho símbolos {0,1,2,3,4,5,6,7}.
- **Decimal** (el usado comúnmente para la representación numérica): utiliza diez símbolos {0,1,2,3,4,5,6,7,8,9}.
- **Hexadecimal:** utiliza dieciséis símbolos {0,1,2,3,4,5,6,7,8,9}.

Equivalencia entre sistemas de numeración			
Decimal	Binario	Octal	Hexadecimal
0	00000	0	0
1	00001	1	1
2	00010	2	2
3	00011	3	3
4	00100	4	4
5	00101	5	5
6	00110	6	6
7	00111	7	7
8	01000	10	8
9	01001	11	9
10	01010	12	A
11	01011	13	B
12	01100	14	C
13	01101	15	D
14	01110	16	E
15	01111	17	F
16	10000	20	10

1.6.1. Sistema de numeración decimal

Desde principios de los tiempos se ha usado por el ser humano el sistema decimal como numeración adaptado por el uso de los 10 dedos de las manos.

El sistema de numeración decimal es un sistema posicional, en el que dependiendo del lugar en el que se posicione cada uno de los distintos símbolos que engloba el significado será uno u otro, Por ejemplo, no es lo mismo 23 que 32.

El sistema decimal también se puede llamar sistema en base 10 porque engloba un grupo de 10 símbolos, los números del 0 al 9: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}.

Un ejemplo es $87456784_{(10)}$.

1.6.2. Sistema de numeración binario

El sistema de numeración binario o en base 2 es al igual que el anterior un sistema posicional que usa simplemente el 0 y el 1 como símbolos.

Un ejemplo es $010001_{(2)}$.

1.6.3. Sistema de numeración octal

El sistema de numeración en base 8 u octal vuelve a ser un sistema posicional caracterizado por usar los números del 0 al 7, es decir, un grupo de 8.

Además, si nos damos cuenta, $2^3 = 8$, por lo que los números en octal son una reducción directa de los números en binario.

Un ejemplo es $456_{(8)}$.

1.6.4. Sistema de numeración hexadecimal

Volvemos a hablar por última de un sistema de numeración posicional al referirnos al sistema de numeración hexadecimal o en base 16 que usa un grupo de 16 símbolos para identificarse, los cuales son: {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}.

Al igual que pasaba con el sistema octal, como $24 = 16$, los números hexadecimales son una reducción de los números binarios (cada cuatro números binarios, hay uno hexadecimal).

Un ejemplo es $A2F_{(16)}$.

Este sistema es el más usado en programación y cabe destacar que suele ponerse como sufijo 0x para identificar que hablamos de un número en base 16.

1.6.5. Conversión de un sistema cualquiera al sistema decimal

Se expresa 'X' como la suma de potencias de 'X' y se realizan los cálculos oportunos.

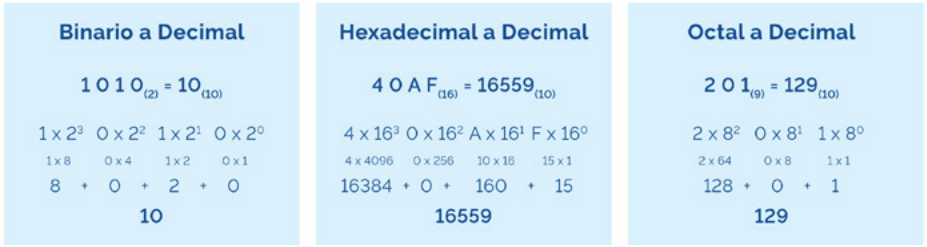

Imagen 15. Conversión de los demás sistemas a decimal

1.6.6. Conversión del sistema decimal a cualquiera

Se debe dividir la parte entera de un número y sus sucesivos cocientes entre 'X'. Los restos de estas divisiones y el ultimo cociente determinan el resultado de la conversión. La parte decimal del número se multiplica sucesivamente por la base 'X' hasta llegar a cero o un numero periódico. Es un método denominado divisiones sucesivas.

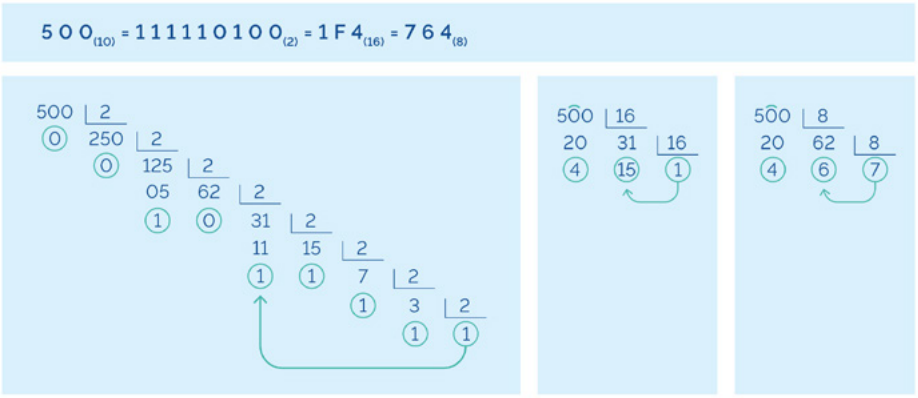

Imagen 16. Conversión de decimal a los demás sistemas de numeración

1.6.7. Conversión entre binario, octal y hexadecimal

Cuando lo que queremos es pasar un número de binario a octal, tendremos que hacer lo siguiente que mostraremos con un ejemplo:

- El número $01110_{(2)}$ lo queremos pasar a octal.
- Dividimos el número en grupos de 3 empezando por la derecha:

  [01] [110]

- Ponemos un 0 al tercer grupo que ha salido para tener los 3 dígitos:

  [001] [110]

- Y ahora o pasamos a decimal y después a octal, o directamente se usa la tabla que más arriba se ha visto y se pasa el número directamente, el nuestro quedaría así:

  $16_{(8)}$

Si lo que queremos es pasar un número de octal a binario, el resultado se obtendría al revés, separando cada digito octal y convirtiéndolo en un grupo de tres dígitos binarios.

El proceso para pasar de hexadecimal a binario es el mismo que el anterior, pero usando grupos de 4 en vez de grupos de 3. Lógicamente lo mismo al revés.

Por último, para pasar entre octal y hexadecimal, en ambas direcciones, lo correcto es pasar el número a binario y después a la base deseada.

1.7. Organizaciones de estándares

Para que los fabricantes de los medios de transmisión de redes puedan crear elementos compatibles deben seguir una serie de normas o estándares.

Un estándar es un conjunto de normas o reglas que deben de cumplir los distintos fabricantes y que se pueden crear porque se han ido aceptando por los usuarios de manera general de hecho, o porque se ha impuesto por las organizaciones de estándares, por derecho.

Una organización de estándar puede ser desde una empresa privada hasta un organismo gubernamental.

Las principales organizaciones de estándares son: IEE, ITU, ANSI, ISO, ISOC y W3C.

1.8. Arquitectura de red

Todos y cada uno de los elementos hardware y software que componen una red como pueden ser ordenadores, cableado, routers, protocolos, etc. se engloban en el término arquitectura de red.

1.8.1. Características

Actualmente la arquitectura de red cumple principalmente con cuatro características básicas:

Tolerancia a fallos

En todas y cada una de las redes hay probabilidad de sufrir un fallo, pero esta tolerancia habla de que se minimice al máximo el impacto que conlleve el fallo e intentar recuperarse lo más rápido posible. Un ejemplo es si se rompe un cable de red, por ejemplo, que haya una red wifi a la que conectarse nos solucionaría el problema. Por lo general, la mayoría de las veces esta tolerancia se consigue mediante la redundancia, es decir, que haya varias maneras de llegar a los nodos de red.

Escalabilidad

La técnica de la escalabilidad trata de poder hacer que la red crezca de manera que su funcionamiento no se vea afectado,

Calidad del servicio (QoS)

Esta calidad se refiere en términos de tiempo y no de errores y viene asociada a las nuevas tecnologías que se están usando hoy en día como por ejemplo el aumento de juego online. Esto se traduce en que se necesitan unas nuevas tecnologías que no son las tradicionales.

Seguridad

La característica que posiblemente más se trabaje hoy en día, y una de las más importantes, porque con todos los avances tecnológicos de hoy en día como puede ser el comercio online o la banca electrónica. Estos usos de las redes conllevan un tráfico de datos personales y muy delicados a gran escala, lo que requiere que haya un mayor riesgo y que se le dé más importancia a la seguridad. Algunos de los métodos usados son la encriptación de datos, los antivirus, firewalls, etc.

1.8.2. Diseño

La arquitectura de la red se organiza en capas o niveles reduciendo la complejidad de su diseño. Dividir un sistema complejo en sistemas más pequeños es un principio clásico de programación modular y ofrece ventajas. Por ejemplo, facilita la comprensión del problema, separa funciones de cada módulo, facilita la construcción de cada uno y su mantenimiento, un módulo puede utilizar los servicios de otro módulo, etc.

La arquitectura de red se encuentra formada por varias capas superpuestas, es decir, es una arquitectura vertical y estratificada, Cada una de las capas debe de proporcionar los servicios necesarios a su capa superior al ejecutar ciertas acciones internas que usan protocolos de redes y as u vez se usan los servicios que nos ofrece la capa inferior.

Si queremos podemos diseñar una arquitectura general, para cualquier red, debemos tener en cuenta las siguientes cuestiones:

Acceso al medio

Cuando tenemos varios equipos en una red que use el mismo medio, tenemos que regular en que orden se va a transmitir la información de manera que la envíen todas a la vez.

Si se envían todos a la vez podría provocar una colisión que acabe con la información al completo.

Saturación del receptor

Si el emisor lanza muchos mensajes muy rápidos y el receptor no es capaz de asimilarlos porque su procesamiento es más lento, se perderá información que no pueda ser procesada.

Para esto el receptor debe de enviar una respuesta al emisor de que ya está listo para más información.

Direccionamiento

Hay que dejar bien claro que proceso de todos los equipos es el que lleva la información y cuál es el destinatario correcto.

Encaminamiento

Al igual que hay que definir el proceso que se encarga del envío de información y el emisor, hay que indicarle al mensaje el recorrido que debe seguir y si en él se encuentran impedimentos a la hora de la comunicación. Un router por ejemplo se encarga de esta tarea al indicar a cada mensaje que camino debe tomar.

Fragmentación

Al enviar los mensajes con la información pertinente, estos se dividen en distintos fragmentos y en la mayoría de los casos estos fragmentos no llegan de manera ordenada. Es tarea del protocolo que se encargue del transporte el que estos fragmentos se reordenen correctamente y poder dar cohesión al mensaje en cuestión.

Control de errores

Como ya se habló anteriormente, las redes no están exentas de problemas o errores que pueden venir derivados desde una interferencia sónica hasta una malformación física en la estructura. Es por eso por lo que en la red debe de haber mecanismos que nos ayuden a arreglar estos errores buscando siempre la no intervención del usuario.

Multiplexación

Cuando tengamos redes que abarquen grandes distancias, el medio debe ser un elemento capaz de compartir múltiples comunicaciones sin que estas tengan relación entre sí.

1.8.3. Funcionamiento

Dentro de una máquina, el funcionamiento de la arquitectura de red es el siguiente:

- Cada uno de los niveles se servirá de los servicios del nivel anterior.
- Hablamos de servicio como el conjunto de tosas las operaciones que una capa va a proporcionar a su capa superior o en algunos casos al usuario final.
- Cuando se trata del emisor, la información baja hacía abajo, es decir, pasa del usuario al medio, y cada uno de los niveles del emisor se añaden como información en forma de cabecera.
- En el caso del receptor es, al contrario, la información viaja en dirección ascendente, del medio hacia el usuario y en este caso los niveles del receptor se encargan de extraer la información contenida en las cabeceras para entregarlas en los niveles superiores.

Cuando la comunicación se da entre dos máquinas, el funcionamiento es el siguiente:

- El nivel en el que se esté de la máquina se comunicará con su semejante en la otra máquina usándose de un protocolo.
- Los procesos que se están llevando a cabo en los mismos niveles de las dos máquinas a la hora de la comunicación son los procesos pares.
- Cuando hablamos de protocolo nos referimos al conjunto de las reglas que nos indica como tienen que estructurarse los paquetes intercambiados en los procesos pares. Los protocolos son implementados en los programas de comunicación.

1.9. Arquitectura TCP/IP

El origen de Internet surge en los años 60 cuando se crea la red ARPANET pero esta era lenta y con muchos errores, por lo que tras muchas investigaciones se desarrolló en la década de los 70 el protocolo TCP/IP.

El protocolo TCP/IP es a su vez un conjunto de protocolos que se organizan de manera jerárquica y donde cada uno es independiente de otro con una función muy clara. Esta arquitectura es al fin y al cabo una descripción de los protocolos englobados, por lo que no se admiten ningún otro que no sean los que ya están fijados. También hay que recalcar que esto es posible ya que los protocolos que alberga son bastante rápidos y fiables. Esto es lo que ha propiciado que hoy en día sea la base de la comunicación a Internet.

Sus características son las siguientes:

- Las aplicaciones son independientes de los dispositivos y medios de transmisión.
- Se pueden conectar diferentes redes.
- La comunicación es no orientada la conexión, esto se traduce en que los paquetes pueden viajar por distintos caminos con la intención de soportar la perdida de nodos o un exceso de saturación.
- La comunicación no depende de la topología de red que se use.

1.9.1. Los niveles y sus protocolos

Cuando dos máquinas quieren comunicarse necesitan de un protocolo, que funcionará como un idioma entre las mismas. Es por esto por lo que, aunque una máquina tenga varios protocolos no los usará todos, sino el que necesite con la comunicación con la máquina de destino.

Por ejemplo, hoy en día Microsoft incorpora de serie en todos sus equipos el protocolo TPC/IP.

Principales protocolos por niveles del modelo OSI	
Nivel físico	DSL, ISDN
Nivel enlace de datos	PPP. Ethernet
Nivel de red	IP, ICMP, X.25, RIP, OSPF
Nivel de transporte	TCP, UDP
Nivel de sesión	SMTP, FTP
Nivel de presentación	NFS, AFP
Nivel de aplicación	SMTP, DNS, SSH

Los protocolos se pueden clasificar en dos tipos:

- **Protocolos abiertos:** Son los protocolos diseñados según los estándares internacionales. Son los protocolos más utilizados.
- **Protocolos cerrados o propietarios:** Son protocolos diseñados por una empresa privada. Si un fabricante quiere utilizar el protocolo, debe pagar una licencia de uso a la empresa que lo ha diseñado.

También existe otro tipo de clasificación que veremos a continuación:

Protocolos orientados a la conexión

Estos protocolos necesitan que antes de que la comunicación llegue a producirse, se establezca un medio de comunicación entre emisor y receptor.

En este momento es cuando especificamos los detalles de dicha transmisión, lo que hace que la comunicación sea más segura, pero más lenta, porque se realizan los envíos de solicitud, respuesta a la solicitud y confirmación o negación de que la información ha sido recibida con éxito.

Los principales protocolos orientados a la conexión son TPC, Frame Relay y ATM.

Protocolos no orientados a la conexión

Estos protocolos se caracterizan por la no necesidad de un canal para establecer la comunicación. Debido a esto, se usan cuando se requiere menos seguridad, pero más velocidad de transmisión.

Algunos de los protocolos de este tipo son UDP, IP, ICMP e IPX.

Un ejemplo para comprender mejor estos protocolos vamos a ver el caso del correo electrónico: enviamos un correo electrónico a un amigo, pero para eso no necesitamos que él esté delante del ordenador porque cuando llegue y abra su gesto de correo lo verá. Esto es un uso no orientado a conexión.

1.9.2. Encapsulamiento en TCP/IP

Como hemos dicho antes, cuando hablamos de comunicación por parte del emisor la información se envía de manera descendente, es decir, de arriba hacia abajo. Esta información siempre empieza en el nivel de aplicación del emisor y es aquí donde se añade una primera cabecera a los datos para darle forma al mensaje antes de ser enviado. Conforme se van añadiendo cabeceras, el tamaño crece porque incluso la capa de enlace añade una cola al final de los datos. Todo este proceso que se encarga de empaquetar en cada nivel los datos con las cabeceras y enviarlas hacia abajo se llama encapsulamiento.

Lógicamente, en la parte del receptor ocurre todo lo contrario, se desencapsulan poco a poco los datos leyendo las cabeceras en cada vez un nivel superior.

Los paquetes de información con la cabecera se llaman PDU y difiere en cada nivel porque se van añadiendo o quitando las cabeceras.

La terminología usada para la PDU en el protocolo TCP/IP es la siguiente:

Capa	PDU	Nombre
Aplicación	HTTP | Datos	Mensaje
Transporte	TCP | Datos	Segmento
Internet	IP | Datos	Paquete
Acceso a red	EH | Datos | ET	Trama

1.10. Modelo de referencia OSI

El modelo OSI no tiene una forma física, no es tangible. Este es un modelo que se propuso para que fabricantes y usuarios que quieran establecer una red tengan las indicaciones de cómo hacerlo. Sería correcto decir que el modelo OSI se trata de un modelo de referencia y es utilizado en sistemas abiertos.

La ISO define un sistema abierto como un sistema que se compone por uno o más equipos, software asociado, periféricos, procesos físicos, medios de transmisión para la información, etc. Todos estos constituyen un conjunto que por sí solo es capaz de tratar de manera correcta la información.

Dentro del modelo OSI, la ISO ha definido un conjunto de capas en la que cada uno se encuentran unos ciertos servicios. Esto se realizó para que todas las funciones estén organizadas por similitud.

Hay definidas siete capas o niveles para el modelo OSI. Cuanto más baja sea una capa, más cerca de los elementos físicos nos encontramos, mientras que cuanto más alta, estamos más cerca del proceso realizado por el usuario final.

1.10.1. Funciones de los niveles

Nivel físico

El nivel encargado de transmitir los datos a través del medio físico que se esté usando. Sus funciones son:

- Ha de especificar que compone las interfaces y el medio.
- Codificar las secuencias de bits antes de enviarlas.
- Tara los bits.
- Sincronizar los bits enviados.
- Esclarecer el tipo de conexión.
- Concretar la topología física usada.
- Definir de qué modo se va a explotar el 100% de la red.

Nivel de Enlace de datos

Es el nivel encargado de que la entrega de datos se produzca de una manera fiable, su ubicación se encuentra en la tarje de red.

Sus funciones son:

- **Tramado.** Se trata de la división de la secuencia de bits en pequeñas unidades de información que reciben el nombre de tramas.
- **Direccionamiento físico.** Se añade una cabecera a la trama para que se sepa cuál es la dirección física tanto de emisor como de receptor.
- **Control de flujo.** Como se ha dicho antes, puede que la velocidad del receptor sea menor que la del emisor y es por esto por lo que se debe de establecer un control que compruebe que el receptor no se satura y no se pierde información.
- **Control de errores.** Comprueba que las tramas no tengan error y en caso de que o tenga transmite dicho error.
- **Control de acceso al medio.** Regula el orden en el que los distintos dispositivos de red envían información al medio con el fin de evitar la colisión anteriormente nombrada,

Nivel de red

Su función es la de entregar los paquetes que atraviesan distintas redes interconectadas.

Sus principales funciones son:

- **Direccionamiento.** Indicar al paquete cuál es su destino y de donde ha venido.
- **Encaminamiento.** Obtener cual es la ruta idónea para que el paquete llegue al destino e indicarle dicho camino.

1.10.2. Nivel de transporte

Debe de entregar el mensaje completo, es decir, juntar todos y cada uno de los paquetes que constituyen el mensaje, ordenarlos y que cuando el nivel de red los entregue, estén correctos.

Funciones del nivel de transporte:

- **Direccionamiento en punto de servicio:** la entrega de estos paquetes se realiza dese el proceso que se origina en el emisor, pero se termina en el receptor mediante s recepción en los distintos puertos, lo que nos permite varias conexiones a la vez en el mismo equipo, por ejemplo.
- **Segmentación y ensamblado de paquetes.**
- **Control de conexión:** cuando los servicios se encuentran orientados a conexión, los establece y los finaliza.
- **Control de flujo:** igual que en nivel de enlace, pero en este caso de extremo a extremo.
- **Control de errores:** como todas las veces anteriores que se ha nombrado.

Nivel de sesión

Es el encargado de controlar la comunicación como tal, es decir, cuando termina una sesión y empieza otra.

Sus funciones son:

- **Control de diálogo:** lo que nos permite que la comunicación de dos procesos pares sea dúplex o semidúplex.
- **Control de sincronización:** se añaden algunos puntos de envíos de mensajes largos.

Nivel de presentación

Este nivel comprueba que la sintaxis de la información que se ha intercambiado sea correcta.

Funciones:

- **Traducción.** Traduce la información codificada.
- **Cifrado.** Vuelve a cifrar la información una vez comprobada para que no se pierda la privacidad.
- **Comprensión de datos.** Se usa cuando la información está almacenada en archivos multimedia.

Nivel de aplicación

Es el encargado de que el usuario y el sistema operativo tengan acceso a red.

Este nivel es el que proporciona todo lo necesario al usuario para la comunicación con la red: un servidor web, un DHCP, un DNS, etc…

1.10.2. Encapsulación en el modelo OSI

A la hora de comunicarse un equipo con otro distinto, se envía un paquete de datos con la información deseada, el cual debe pasar por todas las capas en el emisor y cuando termina su recorrido, por todas las del receptor.

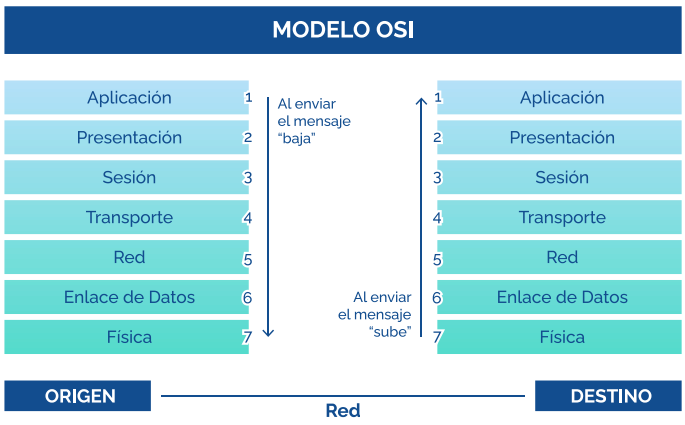

Imagen 18. Esquema de envío y recepción de un mensaje siguiendo el modelo OSI

Cuando se envía un paquete, va a recorrer todas las capas del modelo OSI tanto en receptor como en destinatario, además de los correspondientes sistemas. Cualquier dispositivo físico por el que pase el paquete se encontrará en alguna de las tres primeras capas por lo que no tendrá en cuenta las otras.

Vamos a poner el ejemplo de enviar un correo electrónico, se realizará lo siguiente:

- El correo llega al router y este desencapsula la información y procedemos a recorrer las capas del modelo OSI en sentido inverso:
  1. Se descodifican las señales de la capa 1.
  2. Se leen las direcciones MAC de la capa 2
  3. Se leen las direcciones IP.
- Una vez que el router ha leído la información ya sabe dónde debe enviarla.
- Ahora repetiría el primer proceso nombrado hasta llegar al servidor de correo electrónico, donde ya pasaría la información las 7 capas del modelo OSI.

En el siguiente cuadro detallamos los nombres de los paquetes de datos según la capa en la que se encuentran:

Paquetes de datos en el modelo OSI		
Nivel	**Nombre del paquete**	**Cabecera**
Aplicación	APDU	AH
Presentación	PPDU	PH
Sesión	SPDU	SH
Transporte	TPDU	TH
Red	Paquete	NH
Enlace	Trama	DH Y DT
Físico	Bits	No hay

La parte más pequeña que se usa en los protocolos es la llamada PDU (unidad de datos de protocolo) que en los primeros niveles OSI tienen nombres propios, bits, trama y paquete respectivamente. En los demás niveles el nombre se forma de la siguiente manera:

Primera letra del nombre del nivel + PDU

Esto se puede comprobar en el Cuadro 4 con las capas restantes.

El mismo procedimiento se sigue con las cabeceras de los paquetes, pero sustituyendo PDU por H, que hace referencia a head (cabeza).

La única diferencia en las cabeceras es que el nivel 3 sí que sigue la nomenclatura, en el 2, también se puede nombrar con T en referencia a tail, y en el nivel físico no hay cabeceras.

Para terminar, hemos de decir que las capas se comunican entre sí mediante una interfaz a la que definimos como el conjunto de normas que siguen dichas capas para su correcta comunicación.

1.11. Comparativa del modelo OSI con TCP/IP

Como los protocolos referentes a TCP/IP fueron previos al modelo OSI, los niveles no coinciden de manera exacta.

OSI vs TCP			
Nivel	**OSI**	**TCP/IP**	**Protocolos**
7	Aplicación	Aplicación	TELNET, FTP, TFTP, HTTP, RPC, SMTP
6	Presentación		
5	Sesión		
4	Transporte	Transporte	TCP, UDP
3	Red	Internet	IP, ARP, ICMP
2	Enlace	Acceso a Red	SLIP, PPP; HDLC, ETHERNET, X.25
1	Físico		

Como podemos ver en el cuadro anterior, la capa de Aplicación de TCP/IP equivale a los tres niveles superiores del modelo OSI.

La capa de transporte y red coinciden, solo que en el modelo OSI se llama Red y en TCP/IP se llama Internet.

Por último, los niveles de enlace y físico del modelo OSI coinciden con la capa de Acceso a Red presente en los protocolos TCP/IP.

Inconvenientes de TCP/IP

La arquitectura TCP/IP nació con el propósito de mejorar la comunicación entre equipos conectados por red, no como una base para distintos diseños posteriores de redes y es en parte por esto que no distingue entre servicio y protocolo y que no os sirve para explicar otros conjuntos de protocolos.

El modelo OSI distingue muy bien la capa física de la capa de enlace porque no se trata de lo mismo, la primera comprueba que las señales se transmitan mientras que la segunda nos indica la extensión de cada trama y que si están en buen estado. Es por esto anterior que un error de TCP/IP es agruparlas en la capa de acceso a red.

Por eso, cuando hablamos de capas, la referencia se hace al modelo OSI y no al TCP/IP.

Por último, hay que tener en cuenta que, como los niveles de sesión, 5, y de Presentación, 6, son algo inútiles en la práctica, se suele usar un modelo de 5 niveles sin estos dos últimos.

1.12. Captura de tráfico http con WireShark

1. Descarga la última versión estable de la página http://www.wireshark.org/download.html.
2. Hay que incluir la librería Wincap a la hora de instalar la aplicación.
3. Abrimos la aplicación y seleccionamos sobre que tarjeta de red se va a ejecutar la captura. En la lista de interfaces aparecen todas, tanto las virtuales como las reales.

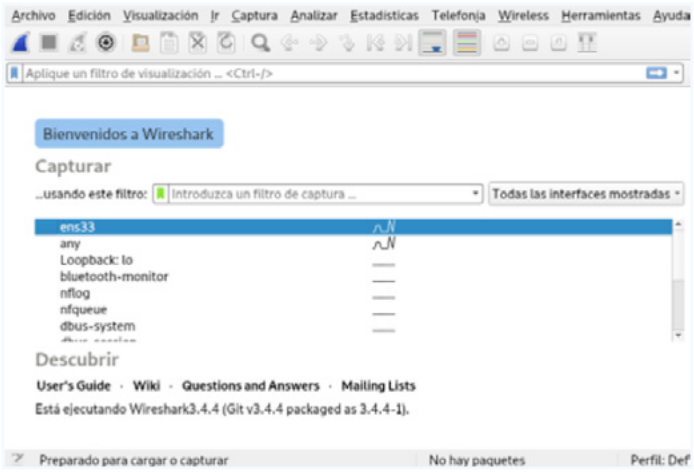

Imagen 19. Selección de la tarjeta de red

4. Abre el navegador.
5. Inicia la captura de tráfico pulsando Capture, Start o bien el botón aleta de tiburón.
6. Escribe en la barra de direcciones cualquier dirección.
7. Vuelve a Wireshark y para la captura con la opción Stop del menú Capture, o bien con el botón Stop de la barra de herramientas.

Imagen 20. Barra de herramientas

8. Observamos gran cantidad de tramas capturadas por las resoluciones DNS previas al tráfico http, y puede, que tráfico de otro tipo.

No.	Time	Source	Destination	Protocol	Length	Info
528	34.499891972	142.250.201.68	192.168.115.128	TCP	60	443 →
529	35.177621858	192.168.115.128	91.198.174.192	TLSv1.2	93	Applic
530	35.177924300	91.198.174.192	192.168.115.128	TCP	60	443 →
531	35.242197370	91.198.174.192	192.168.115.128	TLSv1.2	93	Applic
532	35.242224362	192.168.115.128	91.198.174.192	TCP	54	59410

Imagen 21. Tramas capturadas

9. Hacemos un filtrado de tramas para ver solamente las que contienen el protocolo HTTP. Para lo cual escribimos 'http' en la barra para filtrar.

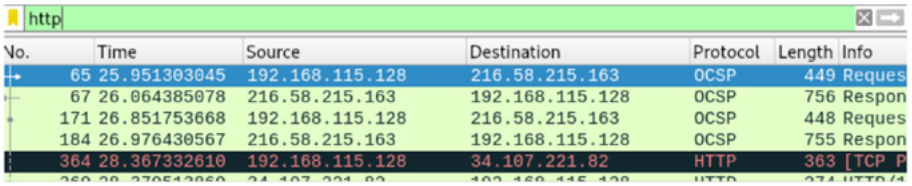

Imagen 22. Filtro http

10. La primera trama que nos aparece es una petición que hace http por GET y nos aparece en la columna de info. Si hacemos doble clic comprobamos que aparece una ventana con el contenido.

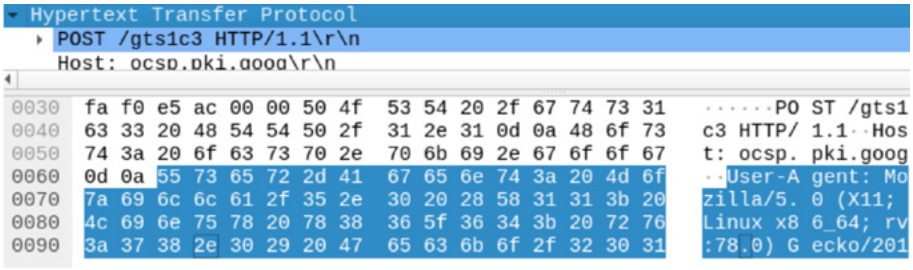

Imagen 23. Contenido de la trama

Podemos observar que aquí hay 5 grupos distintos, Frame, Ethernet II, IPv4, TCP y HTTP.

El Frame nos indica todos los bits que se encuentran sin agrupar.

Ethernet II hace referencia a la cabecera del enlace, IPv4 es la cabecera de red, TCP es la cabecera correspondiente al transporte y por último, HTTP nos indica la petición HTTP que se ha realizado.

11. Si desplegamos el apartado correspondiente al Frame podemos ver en la imagen de más abajo que se distingue:

   - Los protocolos presentes en la trama: Ethernet, IP, TCP y HTTP.

Imagen 24. Apartado frame

12. Si desplegamos la cabecera Ethernet II vamos a poder observar el destino de la trama, en nuestro caso VMware…, debido a que es una máquina virtual; el origen de la trama, VMware…. de nuevo por la razón anterior y por último el protocolo de encapsulación que es IPv4.

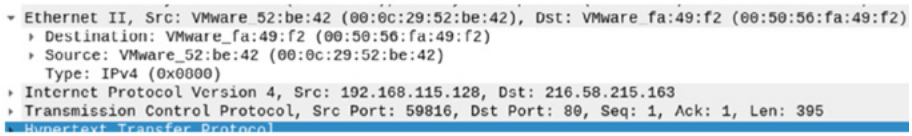

Imagen 25. Cabecera Ethernet II

13. Si ahora nos fijamos en la cabecera IPV4 se puede ver la dirección de origen, 192.168.115.128 y la de destino, 216.58.215.163 de los datos enviados. Además, se ve la versión del protocolo IP (IPv4), la longitud de la cabecera (20 bytes), la longitud total del paquete (435), etc.

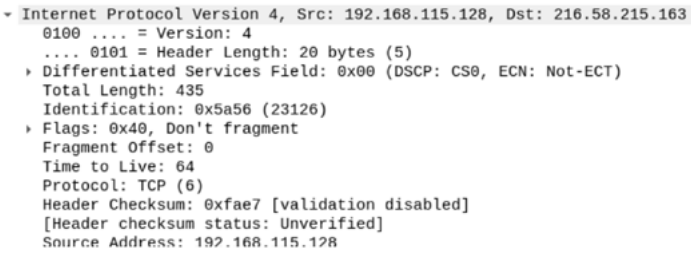

Imagen 26. Cabecera IP

14. Nos toca fijarnos en el apartado de TCP, donde se observa que el puerto de origen es el 59816 y el de destino el 80 así como los que hemos descrito antes con respecto a IP, son muy parecidos como se puede observar.

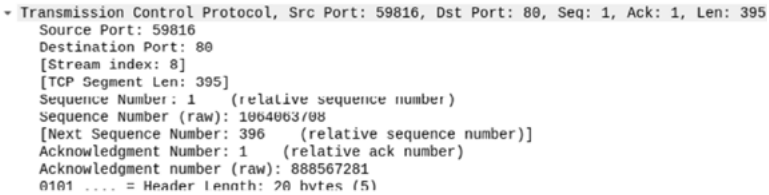

Imagen 27. Cabecera TCP

15. Si se despliega por último la cabecera de HTTP o Hypertext Transfer Protocol se puede ver la cabecera http, el nombre del recurso solicitado, el host de destino, el agente de usuario o navegador usado y el tipo de contenido que ha sido aceptado en general.

16. Si queremos conservar las tramas que hemos capturado, es decir, una imagen de la captura en otro medio externo de almacenamiento, WireSahrk nos la guarda en un archivo de extensión pcapng.

www.universae.com