

UNIDAD 5: CONEXIÓN DE SISTEMAS EN RED

Módulo Profesional: Sistemas Informáticos

Índice

RESUMEN INTRODUCTORIO	3
INTRODUCCIÓN	3
CASO INTRODUCTORIO.....	4
1. MODELOS DE RED. EL MODELO OSI.....	5
1.1 Definiciones	6
1.2 Las capas del modelo OSI.....	8
1.2.1 La capa física (nivel 1).....	9
1.2.2 La capa de enlace (nivel 2)	9
1.2.3 La capa de red (nivel 3).....	10
1.2.4 La capa de transporte (nivel 4).....	10
1.2.5 La capa de sesión (nivel 5).....	11
1.2.6 La capa de presentación (nivel 6)	11
1.2.7 La capa de aplicación (nivel 7).....	11
2. EL MODELO TCP/IP	13
2.1 Comparativa con el modelo OSI	14
2.2 Principales protocolos del modelo TCP/IP.....	15
2.2.1 Protocolos de la capa de Internet.....	16
2.2.2 Protocolos de la capa de transporte.....	16
2.2.3 Protocolos de la capa de aplicación.....	16
3. CONFIGURACIÓN DEL PROTOCOLO TCP/IP.....	18
3.1 Direcciones IP. IPv4. IPv6	18
3.2 Máscara de subred, puerta de enlace y DNS	20
3.3 DHCP	21
3.4 Configuración de TCP/IP en sistemas Windows	22
3.5. Configuración de TCP/IP en sistemas Linux.....	25
3.6 Ficheros de configuración de red	27
4. GESTIÓN DE PUERTOS	30
5. RESOLUCIÓN DE PROBLEMAS DE CONECTIVIDAD EN S.O. EN RED	32
5.1 Verificación del funcionamiento de una red mediante el uso de comandos.	32
5.2 Herramientas de monitorización de redes	34
RESUMEN FINAL	36

RESUMEN INTRODUCTORIO

A lo largo de esta unidad revisaremos el concepto de modelo de red, y la importancia que tiene a la hora de conseguir que dispositivos conectados a diferentes redes puedan interconectarse entre sí. Describiremos con detalle los dos modelos de red principales, OSI y TCP/IP, y veremos cómo ambos dividen las funcionalidades de una red en una serie de capas o niveles, que también estudiaremos.

Una vez fijado el marco teórico, pasaremos a comprobar cómo se configura y utiliza en la práctica, tanto en sistemas Windows como Linux, el modelo TCP/IP, que es el que más habitualmente encontraremos en nuestros equipos. Se revisarán con detalle conceptos fundamentales, como el de dirección IP, máscara de subred, DNS o DHCP.

También hablaremos de los puertos de comunicaciones, y cómo nos permiten ejecutar de forma simultánea varias aplicaciones de red disponiendo de una sola conexión.

Y finalmente nos centraremos en la resolución de los posibles problemas de conectividad que pudieran surgir en nuestras redes. Para ello se emplearán tanto herramientas propias de los sistemas operativos como externas, que complementan la funcionalidad de las primeras.

INTRODUCCIÓN

En la Unidad 1 ya tuvimos un primer contacto con las redes de ordenadores, describiendo sus principales componentes, los tipos de redes existentes, sus topologías, los mapas físicos y lógicos... Pero fue simplemente una visión genérica, sin entrar en terreno práctico.

Esta Unidad viene a aportar esa componente práctica. En ella se verá cómo se estructura una red siguiendo unos modelos que permitan interconectarla con otras redes diferentes, cómo se configuran dichos modelos en un dispositivo concreto, sea cual sea su sistema operativo, cómo se gestionan las conexiones de red para sacarles el máximo rendimiento, y cómo se pueden detectar y solucionar los posibles problemas de conectividad que pudieran ir surgiendo.

Todos estos conceptos, tanto teóricos como prácticos, deben ser asimilados por cualquier desarrollador, ya que hoy en día prácticamente no se concibe una aplicación que no esté conectada de algún modo: bien en su propia operativa, bien en su instalación, bien en sus actualizaciones.

CASO INTRODUCTORIO

Te contratan para realizar una aplicación de gestión para una pequeña empresa, y al realizar un primer estudio de necesidades detectas que sus ordenadores no están conectados en red, sino que cada uno de ellos trabaja de forma independiente. Lógicamente quieres que tu aplicación esté diseñada para trabajar en red, así que, tras mostrar a la empresa las ventajas de esta opción, le ofreces como servicio complementario la instalación y configuración de una red local que conecte sus equipos.

Al finalizar la unidad conocerás los distintos modelos de red existentes, las características principales de cada uno de ellos, y sus diferencias más significativas, serás capaz de configurar una red utilizando el modelo TCP/IP, podrás gestionar los puertos que necesitan sus aplicaciones, y serás capaz de detectar y solucionar, utilizando las herramientas más adecuadas para ello, los posibles problemas que pueden darse en una red de ordenadores.

1. MODELOS DE RED. EL MODELO OSI

Cuando se diseña una red de datos se desea sacar el máximo rendimiento de sus capacidades. Para conseguir esto, la red debe estar preparada para efectuar conexiones a través de otras redes, sin importar qué características posean.

El objetivo de la interconexión de redes es dar un servicio de comunicación de datos que involucre diversas redes con diferentes tecnologías de forma transparente para el usuario.

Las primeras redes de ordenadores no seguían un modelo común, sino que cada fabricante establecía las especificaciones que le parecían oportunas. Esto hacía que esas redes primitivas fueran muy difíciles de interconectar.

El **CCITT** (Comité Consultivo Internacional para la Telegrafía y Telefonía), se fundó en 1965 para establecer recomendaciones que definiesen estándares abiertos para las comunicaciones de textos y voz entre ordenadores. El trabajo más significativo en el establecimiento de estándares internacionales para la interconexión de sistemas abiertos de ordenadores se debe a la Organización Internacional de Estándares (**ISO**). El primer paso hacia el establecimiento de una arquitectura abierta como alternativa a las arquitecturas comerciales lo dio en 1977 el comité ISO / TC97 / SC16 que desarrolló un modelo de referencia para la interconexión de Sistemas Abiertos (el **modelo OSI**); este modelo es la base para la coordinación y el desarrollo de estándares para las redes de comunicaciones.

OSI es el Open Systems Interconnection Reference Model (modelo de referencia para la interconexión de sistemas abiertos). Es el protocolo o modelo estándar. Tiene **siete niveles**. Los 3 niveles inferiores están orientados a la transmisión de datos digitales a través de una red, el cuarto nivel al transporte extremo-a- extremo de la información, y los 3 superiores a la aplicación. Es necesario señalar que este modelo no es una arquitectura de red en sí mismo, dado que especifica las capas, pero no los protocolos.

Las capas o niveles son:

1. Física
2. Enlace
3. Red
4. Transporte
5. Sesión
6. Presentación
7. Aplicación

1.1 Definiciones

A continuación se desarrollarán algunas definiciones de especial importancia:

- **ENTIDAD:** se llaman entidades a los elementos activos que se encuentran en cada una de las capas. Hay entidades software como un proceso, y entidades hardware como un chip encargado de hacer la entrada y salida de datos. A las entidades de la misma capa, residentes en distintos nodos, se les llama «entidades pares» o «iguales».
- **PROTOCOLO:** los protocolos son reglas y procedimientos para la comunicación. El término “protocolo” se utiliza en distintos contextos. Por ejemplo, los diplomáticos de un país se ajustan a las reglas del protocolo creadas para ayudarles a interactuar de forma correcta con los diplomáticos de otros países. De la misma forma se aplican las reglas del protocolo al entorno informático. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.
- **INTERFAZ:** en informática, las interfaces son las conexiones entre sistemas, dispositivos o programas, que permiten su comunicación. En este caso concreto, la interfaz es la conexión entre cada dos niveles del modelo OSI.

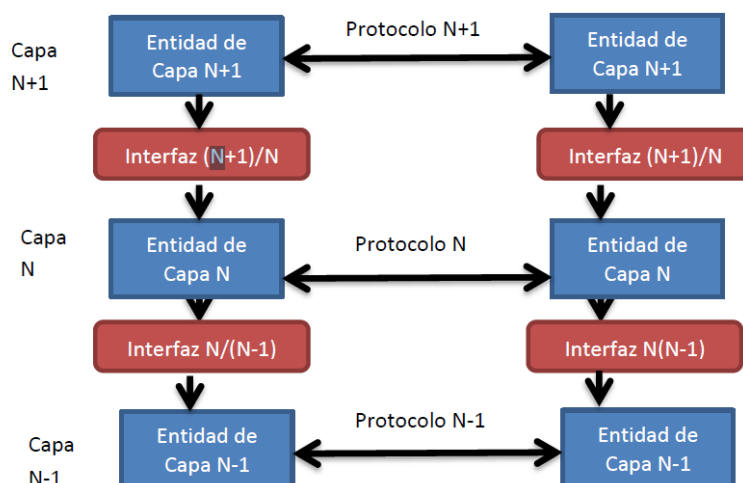


Imagen: Entidades, interfaces y protocolos en el modelo OSI

- **PUNTO DE ACCESO AL SERVICIO (SAP):** los SAP (Service Access Points) son los puntos en donde una capa puede encontrar disponibles los servicios de la capa inmediatamente inferior. Cada SAP tiene una dirección que le identifica y por la que se invoca el servicio. Por ejemplo, en el sistema postal, los SAP serían equivalentes a las direcciones postales de cada uno de los domicilios.

- **UNIDAD DE DATOS DEL INTERFAZ (IDU, INTERFACE DATA UNIT):** es el bloque informativo que la entidad de la capa N pasa a la entidad correspondiente de la capa N-1 a través del interfaz N/(N-1).
- **UNIDAD DE DATOS DEL SERVICIO (SDU, SERVICE DATA UNIT):** cada IDU está compuesto de un campo con información para el control del interface (campo ICI, Interface Control Interface) y de un segundo campo llamado «SDU» que es la información que se pasa a través de la red, a la entidad par, es decir, a su equivalente en el host destinatario.

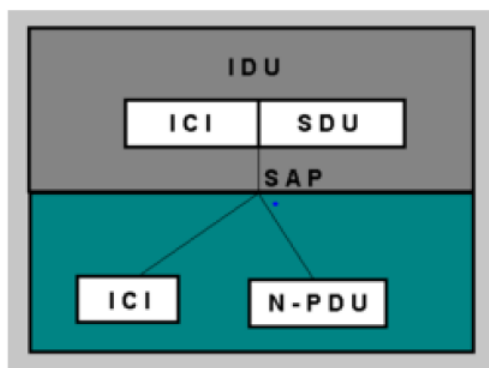


Imagen: Intercambio de información entre dos capas OSI

- **UNIDAD DE DATOS DEL PROTOCOLO (PDU, PROTOCOL DATA UNIT):** la información del SDU no siempre se puede transmitir en directo. A veces, hay que fraccionarla porque su tamaño no es adecuado para la transmisión directa, y además siempre habrá que ponerle alguna cabecera con información de control.

Al campo SDU más la cabecera de control es a lo que se le llama PDU. Si estamos operando en la capa N, el PDU recibe el nombre de N-PDU, aunque en algunas capas de OSI se utilizan sinónimos mnemotécnicos, algunos de los cuales irán apareciendo más adelante. Los N-PDU son las unidades de intercambio entre las entidades pares de capa N de dos nodos, utilizando su protocolo de capa N.

Las cabeceras que cada capa añade a los datos que le llegan de su capa inmediatamente superior llevan la información de control necesaria para el interface y para la propia capa. Por ejemplo, si deseamos enviar un mensaje en papel y es necesario segmentarlo en diversas porciones, cada trozo deberá ir acompañado de una etiqueta identificativa con el fin de poder reconstruir en el destino el mensaje original. La información de numeración de estas etiquetas podría ser la cabecera de cada porción.

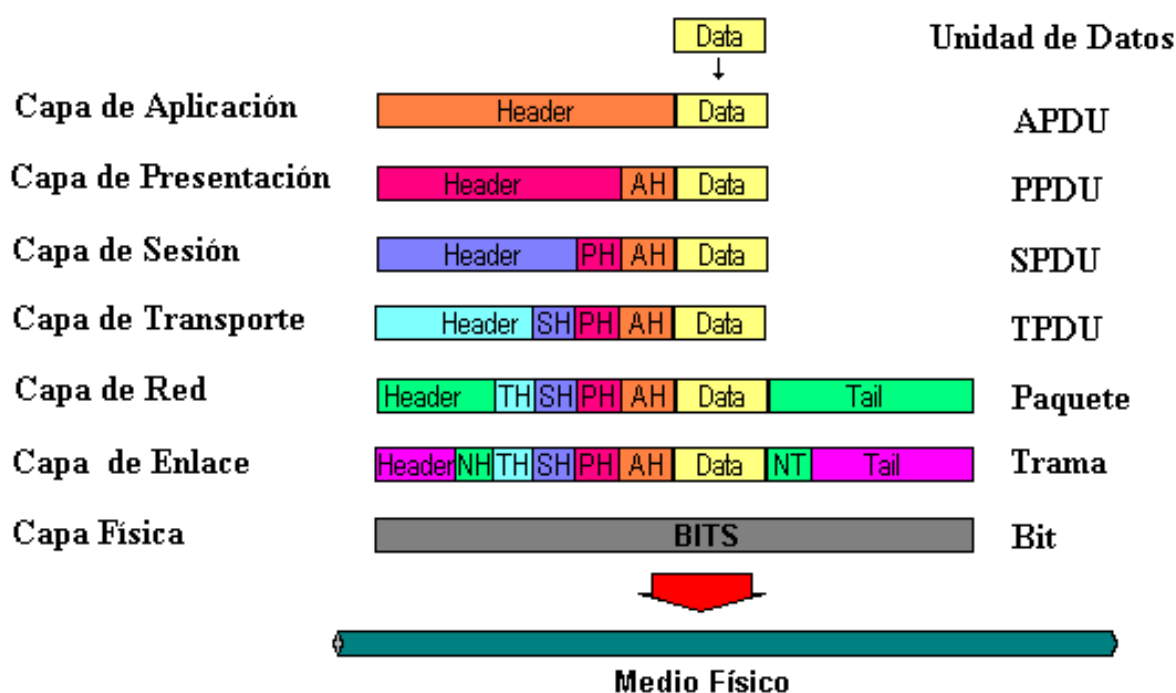


Imagen: PDUs de las diferentes capas

1.2 Las capas del modelo OSI

A continuación se desarrollarán las siete capas o niveles del modelo OSI:



1.2.1 La capa física (nivel 1)

Es la capa de más bajo nivel, por lo tanto es la que se ocupa de la transmisión real de los bits de que se compone la información que se intercambia. Esta capa es la que se encarga de definir las características físicas (eléctricas, mecánicas, funcionales, de procedimiento, etc.) para que se produzca una conexión entre dos equipos de la red, o para que se dé un enlace de datos.

- **Características eléctricas:** Se definen las características eléctricas para intentar tener la mayor inmunidad frente a las posibles interferencias (velocidad máxima de la transmisión, longitud, voltajes, etc.).
- **Características funcionales:** Se debe definir qué circuitos son necesarios para establecer la transmisión. Es aquí donde examina la compatibilidad de los conectores, cuantos pines tienen cada equipo conectado, y la función de cada pin, número de polos en un enchufe, etc.
- **Características de procedimiento:** Se define la secuencia de datos que se deben intercambiar entre la estación emisora y receptora y cómo tendrán lugar estas (el orden en el que se hacen las negociaciones de envío y recepción).

En esta capa se encuentran dispositivos como los cables, tarjetas, repetidores (**hubs**), etc.

1.2.2 La capa de enlace (nivel 2)

Principalmente controla el flujo de datos, la sincronización y los errores que pueden darse, proporcionando un intercambio de datos fiable a través de un enlace físico. Tiene como misión:

- La sincronización de las estructuras de la información que se envía y recibe.
- El control de errores.
- El control de los estados de la comunicación (a la escucha, mandando, espera, etc).
- El control del medio de comunicación.

En definitiva esta capa se encarga de garantizar la integridad de la comunicación. En esta capa se encuentran dispositivos como los puentes (**bridges**).

1.2.3 La capa de red (nivel 3)

Encamina los datos a su destino (enrutamiento), eligiendo el camino o ruta más efectiva. Esta capa tiene unas funciones que no solo afectan a los extremos de los terminales comunicados, sino a toda la red. Su principal función es la de proporcionar los mecanismos necesarios para intercambiar información entre equipos que pueden estar ubicados en redes geográficamente distintas.

Esta capa controla los nodos de una red, y debe definir por tanto las normas de conexión entre los diferentes nodos. El nivel de red permite conexiones entre terminales remotas. Según sea esta comunicación podemos hablar de:

- **Circuitos virtuales:** se debe establecer una conexión entre los equipos que quieran comunicarse.
- **Datagramas:** No se realiza ninguna conexión con el otro extremo sino que se envían paquetes a la red, y esta los distribuye automáticamente. El nivel de red debe controlar el flujo de la información, el encaminamiento, y el control de gestión. De ello se encarga el dispositivo denominado **router**. El nivel de red debe disponer de mecanismos suficientes para solventar atascos, evitar que los emisores saturen a los receptores y buscar vías de transmisiones rápidas y económicas. Esta capa se encarga de realizar el encaminamiento de red que seguirían los mensajes y controlar la congestión de la red.

1.2.4 La capa de transporte (nivel 4)

Esta es una capa intermedia entre las capas orientadas a la red y las capas orientadas a las aplicaciones.

Principalmente se encarga de transportar la información de una manera fiable para que llegue a su destino, intentando proporcionar un servicio que aísle a las capas de nivel superior de los detalles físicos de dicho transporte. Esta capa garantiza la integridad de los mensajes entre el origen y el destino, encargándose de que se mantenga su secuencia de temporalidad o almacenándolos si el sistema no puede dar respuesta con suficiente velocidad. No depende ni del software (capas superiores) ni del hardware (capas inferiores).

En esta capa aparece la pasarela (**gateway**) como elemento de interconexión entre redes (normalmente diferentes entre sí).

1.2.5 La capa de sesión (nivel 5)

Se encarga de ciertos aspectos de la comunicación, como el control de los tiempos. Permite el diálogo entre emisor y receptor estableciendo una sesión. A través de dicha sesión se puede llevar a cabo el transporte de información.

Esta capa indica la cantidad y la velocidad a lo que se pueden mandar los datos y establece puntos de sincronización, pudiendo así recuperar transmisiones en ciertas partes sin tener que volver a retransmitirlo todo en caso de error.

En el establecimiento de una sesión se pueden diferenciar dos etapas:

- El establecimiento de la sesión y la creación de un buzón donde se reciban los mensajes, procedentes de las capas inferiores.
- El intercambio de datos entre los buzones del emisor y del receptor siguiendo unas reglas para dialogar.

1.2.6 La capa de presentación (nivel 6)

Esta capa se ocupa de la sintaxis y de la semántica de la información que se pretende transmitir, definiendo estructuras de representación abstractas para hacer posible la comunicación entre ordenadores que utilizan representaciones internas diferentes.

Indica el orden en que hay que mandar los datos y gestiona las terminales virtuales. También traduce distintos alfabetos usados por los ordenadores, logrando una comunicación compatible entre todos.

Esta capa está íntimamente relacionada con la capa de nivel 7. Se dedica a interpretar o convertir los datos que usará la capa 7. También se encarga de la encriptación, compresión, etc.

1.2.7 La capa de aplicación (nivel 7)

Es la capa que está en contacto directo con el usuario. Es diferente al resto de capas del modelo OSI en el sentido de que no proporciona servicios a otras capas, sino únicamente a las aplicaciones que el usuario desea ejecutar (que se encuentran fuera del modelo).

Dichas aplicaciones proporcionan los servicios requeridos por el usuario: comandos, órdenes, etc. Servicios gestionados por programas o aplicaciones del tipo: navegador web, cliente ftp, telnet...

Por tanto, la función principal de la capa de aplicación es proporcionar los procedimientos precisos que permitan al usuario ejecutar los comandos relativos a sus propias aplicaciones (transferencia de ficheros o correo electrónico, por ejemplo).

2. EL MODELO TCP/IP

A diferencia del modelo OSI, que es simplemente un marco teórico para la definición de una red de ordenadores, el modelo TCP/IP sí tiene una **implementación real**, utilizada en buena parte de las redes de ordenadores actuales. Comenzando por la red de redes, Internet.

Constituye una familia de protocolos de comunicación diseñados con una motivación fundamental: lograr la interoperabilidad entre los diferentes sistemas de comunicación de una red heterogénea/multivendedor en forma transparente para el usuario final. Tal heterogeneidad se manifiesta a diferentes niveles de interconexión los cuales van desde los protocolos de la capa física hasta las aplicaciones.

Se utiliza para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, Mac, mini computadoras y servidores de redes de área local y área extensa. TCP/IP no depende del sistema operativo ni del computador, sino que cualquiera puede desarrollar productos que se ajusten a sus especificaciones.

Para poder aplicar el modelo TCP/IP en cualquier equipo, independientemente del sistema operativo, el sistema de protocolos TCP/IP se ha dividido en diversos módulos. Cada uno de ellos realiza una tarea específica. Además, estos módulos realizan sus tareas uno después del otro en un orden específico. Ésta es la razón por la cual se habla, como en el caso de OSI, de un modelo de capas.

Este modelo fue desarrollado por el Departamento de Defensa de los Estados Unidos, ejecutándolo por primera vez en 1972 en ARPANET, una red de área extensa del citado departamento. Actualmente es mantenido por la IETF (Internet Engineering Task Force).

TCP/IP es, como decíamos, un conjunto de más de 100 protocolos. Las siglas TCP/IP, que significan "Protocolo de control de transmisión/Protocolo de Internet", y provienen de los nombres de los dos protocolos más importantes del conjunto: TCP, que se encarga de garantizar que los datos enviados se reciben en el mismo orden en que se mandaron y libres de errores; mientras que IP se encarga del direccionamiento de los datos y la búsqueda de la mejor ruta posible para ellos.

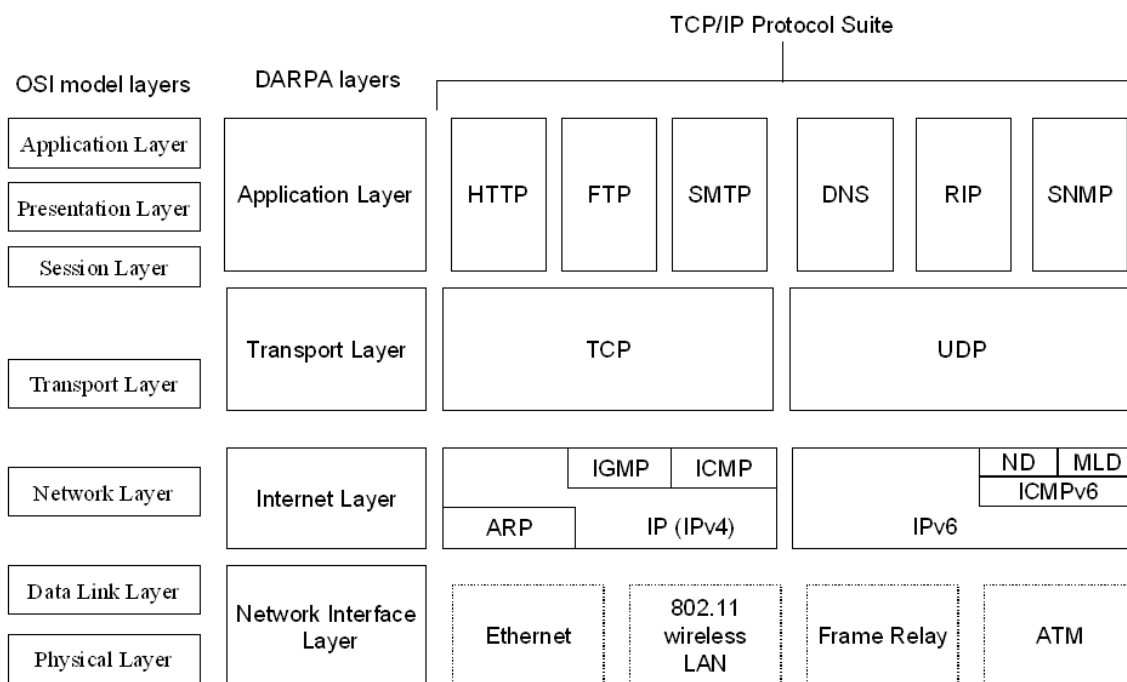


Imagen: Principales protocolos del modelo TCP/IP.

Fuente: <http://technet.microsoft.com>



ENLACE DE INTERÉS

En el siguiente enlace podrás encontrar más información sobre el protocolo TCP/IP:

<http://docs.oracle.com/cd/E19957-01/820-2981/ipov-10/index.html>

2.1 Comparativa con el modelo OSI

A diferencia de OSI, el modelo TCP/IP sólo contempla 4 niveles o capas:

- **Capa 1 o capa de acceso a la red:** se encarga de la transmisión física de los datos, y se asimila a las capas 1 (física) y 2 (de enlace de datos) del modelo OSI.
- **Capa 2 o capa de Internet:** es la equivalente a la capa 3 (de red) de OSI. Prepara los paquetes de datos (datagramas) para su transmisión.
- **Capa 3 o capa de transporte:** se asimila a la capa 4 (igualmente llamada de transporte) del modelo OSI, y se encarga del enrutamiento de datos.

- **Capa 4 o de aplicación:** engloba las funcionalidades de las capas 5 (sesión), 6 (presentación) y 7 (aplicación) de OSI. Da soporte a las aplicaciones de red de los usuarios.

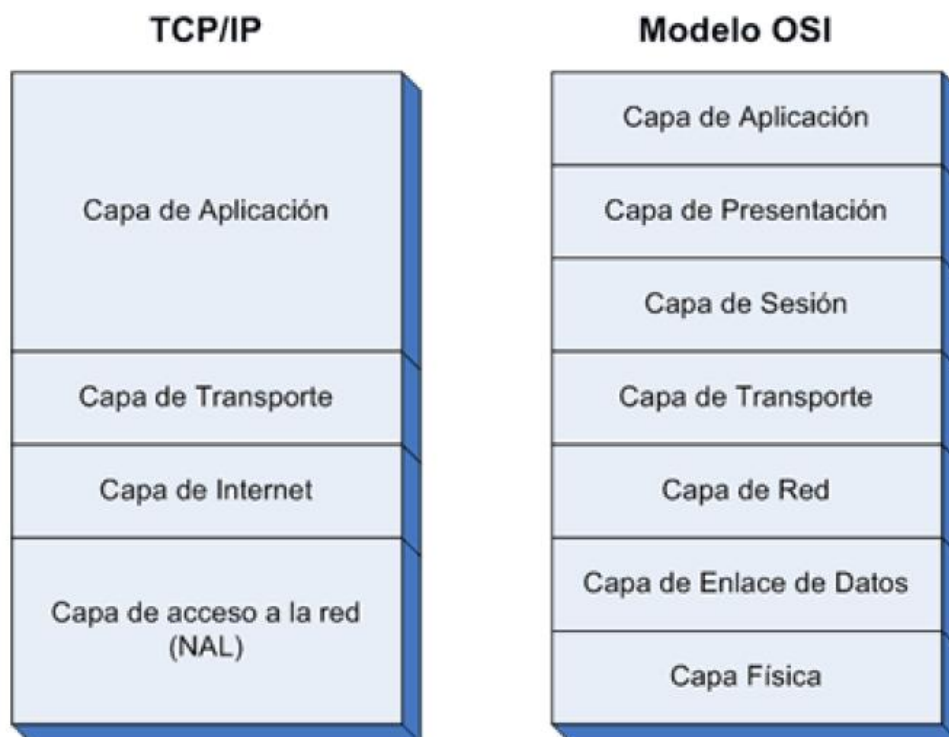


Imagen: Comparativa de los modelos OSI y TCP/IP.

Fuente: <http://www.textoscientificos.com>

2.2 Principales protocolos del modelo TCP/IP

Los principales protocolos del modelo TCP/IP, que se estudiarán a continuación son:

- **Protocolos de la capa de Internet:** IP (Internet Protocol) y ICMP (Internet Control Message Protocol)
- **Protocolos de la capa de transporte:** TCP (Transmission Control Protocol) y UDP (User Datagram Protocol)
- **Protocolos de la capa de aplicación:** HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol) y SMTP (Simple Mail Transfer Protocol).

2.2.1 Protocolos de la capa de Internet

Existen dos protocolos de la capa de Internet:

- **IP (Internet Protocol):** Es uno de los protocolos más importantes del modelo, y se encarga de la preparación de los paquetes de datos (datagramas IP) para su envío. Para ello se añaden a dichos paquetes tanto la dirección IP del emisor como la del destinatario, de modo que se pueda saber exactamente a qué equipo debe entregarse la información.
- **ICMP (Internet Control Message Protocol):** Es un protocolo de control y notificación de errores. Se emplea, por ejemplo, cuando ejecutamos el comando ping.

2.2.2 Protocolos de la capa de transporte

Existen dos protocolos de la capa de transporte:

- **TCP (Transmission Control Protocol):** Es, junto a IP, el protocolo que da nombre al modelo. A diferencia de IP, es un protocolo orientado a conexión. Es decir, que se encarga de que se establezca una conexión entre la máquina emisora y la receptora de los datos enviados, pudiendo así comprobar que dichos datos se han entregado de forma correcta. Para ello añade una serie de información de control a los datagramas IP, generando un nuevo bloque de datos que se denomina segmento TCP.
- **UDP (User Datagram Protocol):** A diferencia del anterior, es un protocolo no orientado a conexión, que no proporciona detección de errores. Es por ello más rápido, y suele emplearse en comunicaciones de voz y vídeo, en las que pueden admitirse algunos errores en la transmisión.

2.2.3 Protocolos de la capa de aplicación


Existen tres protocolos de la capa de aplicación:

- **HTTP (HyperText Transfer Protocol):** Es la base de la transmisión de datos en la web (WWW). Cuando, a través de un navegador, se solicita un recurso (como una página web) este protocolo realiza una petición al servidor que lo contiene, estableciéndose un intercambio de peticiones y respuestas que nos permitirán acceder a dicho recurso.

- **FTP (File Transfer Protocol):** Es el protocolo que se utiliza para transferir ficheros entre un equipo cliente y otro servidor. Se emplea, por ejemplo, para alojar un sitio web dentro del servidor correspondiente.
- **SMTP (Simple Mail Transfer Protocol):** Junto a POP e IMAP, es el protocolo encargado de gestionar el servicio de correo electrónico (e-mail).

3. CONFIGURACIÓN DEL PROTOCOLO TCP/IP

Para que un equipo, sea cual sea su fabricante y su sistema operativo, pueda acceder a una red TCP/IP debe, en primer lugar, disponer de una **dirección IP**, que le permita identificarse dentro de dicha red. Además de ella, también se necesita una máscara de subred. Y si también queremos que disponga de conexión a Internet, será necesario configurar la dirección IP de la puerta de enlace y la dirección IP de dos servidores DNS.



Ejemplo configuración TCP/IP	
Dirección IP	192.168.0.15
Máscara de subred	255.255.255.0
Puerta de enlace	192.168.0.254
DNS preferido	80.58.0.33
DNS alternativo	80.58.32.97

Imagen: Datos necesarios para configurar TCP/IP en un equipo

3.1 Direcciones IP. IPv4. IPv6

Una **dirección IP** es un número que identifica a un dispositivo (normalmente un ordenador, pero también un teléfono, una tableta, una impresora...) dentro de una red TCP/IP. Dicho número no debe confundirse con la dirección MAC, que es un número hexadecimal fijo asignado al dispositivo de red por el fabricante.

Una dirección IP clásica (**IPv4**) tiene una longitud de 32 bits y consta de dos campos:

- Un campo identificador de red (netid), que identifica la red a la que está conectado el host.
- Un campo identificador de host (hostid), que asigna un identificador único a cada host de una red específica.

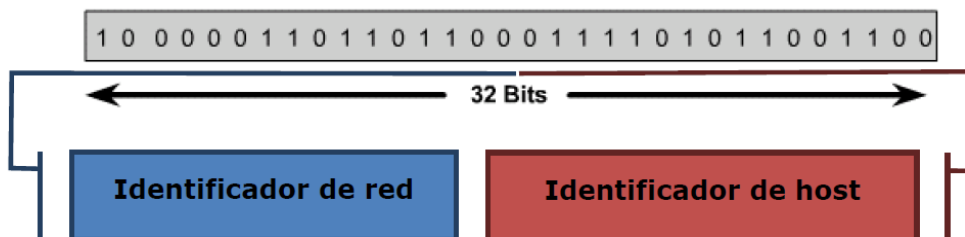


Imagen: Dirección IPv4.

Para simplificar su representación, estos 32 bits se dividen en cuatro octetos, que se expresan en sistema decimal separados por puntos. Esta forma de escribir una dirección se conoce como formato decimal con puntos o punteado. El valor decimal de cada octeto puede ir desde 0 a 255.

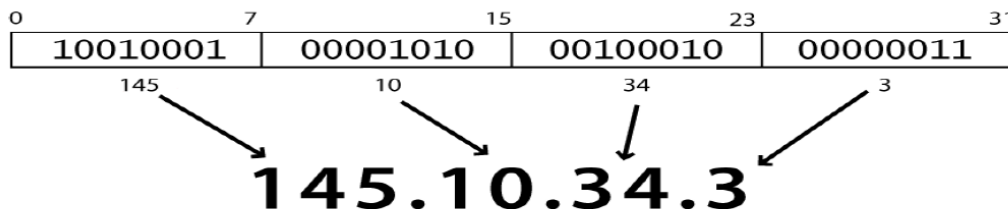


Imagen: Dirección IPv4 en formato punteado

IPv4 se ha venido utilizando con éxito desde los inicios de Internet. Pero en los últimos años ha planteado un grave problema: su **capacidad de direccionamiento** no puede soportar el ritmo de crecimiento de la Red. Hay que tener en cuenta que con 32 bits (dejando aparte el hecho de que no todas las posibles direcciones obtenibles se pueden utilizar, ya que algunas de ellas están reservadas), apenas se pueden direccionar 4000 millones de dispositivos (2^{32}). Se emplean técnicas que permiten ampliar esta capacidad, pero aun así el problema del direccionamiento con IPv4 no se soluciona.

Es por eso que IPv4 se está sustituyendo progresivamente por la nueva versión del protocolo, **IPv6**, que proporciona direcciones de 128 bits. Esto supone una capacidad de direccionamiento de 2^{128} dispositivos, lo que debería resolver el problema por bastantes años.

Las direcciones IPv6 también tienen un formato abreviado, aunque en este caso no se emplean números decimales, sino hexadecimales. Así una dirección IPv6 consta de 8 grupos de 4 dígitos hexadecimales, separados por el signo ":". Cada grupo puede tomar valores entre 0 y FFFF. Los grupos formados únicamente por ceros se pueden omitir, indicándolo con "::".

Una dirección IPv6 (en hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000

↓ ↓ ↓ ↓ |
2001:0DB8:AC10:FE01:: Se pueden omitir los ceros

1000000000000001:0000110110111000:1010110000010000:1111111000000001:
 0000000000000000:0000000000000000:0000000000000000:0000000000000000

Imagen: Ejemplo de dirección IPv6. Fuente: Wikipedia



ENLACE DE INTERÉS

En el siguiente enlace descubrirás por qué surgió el estándar IPv6:

http://es.wikipedia.org/wiki/Agotamiento_de_las_direcciones_IPv4

3.2 Máscara de subred, puerta de enlace y DNS

Definimos estos tres conceptos:

- La **máscara de subred** nos indica qué parte de la dirección IP pertenece a la red, y cuál al equipo. Es por ello que determina el número máximo de equipos de la red. En sistemas de tamaño pequeño se suele utilizar la máscara 255.255.255.0 que corresponde a un rango de 256 direcciones IP (suficientes para cualquier pequeña empresa), en los que todos los dispositivos tienen los tres primeros números de la IP iguales (sería la parte de la red) y solo cambia el último. Lo normal es que todos los equipos de nuestra red tengan configurada la misma máscara de subred.
- La **puerta de enlace** es un dispositivo que sirve de enlace entre dos redes. En nuestro caso, entre la red local e Internet. Cuando un dispositivo de una red local quiere acceder a Internet, habrá que indicarle la dirección de la puerta de enlace, que deberá ser una IP del rango ya que, de lo contrario, nuestro PC no será capaz de comunicarse con ella. Lo normal es que todos los PCs de nuestra red tengan configurada la misma puerta de enlace. Si no sabemos la IP de nuestra puerta de enlace, podemos verla en otro PC en el que funcione correctamente la conexión de Internet.
- El **DNS (servidor de nombres de dominio)** es un equipo que se encarga de convertir las direcciones que escribimos cuando queremos acceder a un recurso, por ejemplo, en un navegador web, en las correspondientes direcciones IP de los servidores que contienen dicho recurso. Los **DNS preferido y alternativo** nos los debe proporcionar la compañía que presta el servicio de Internet. Telefónica, por ejemplo, usa el 80.58.0.33 y el 80.58.32.97. Lo normal es que todos los PCs de nuestra red tengan configurados los mismos DNS así que, como en el caso anterior, si no sabemos la IP de los DNS podemos consultarla en otro PC en que funcione correctamente la conexión de Internet.

3.3 DHCP

Para que los equipos de una red puedan comunicarse es necesario configurar en cada uno de ellos la dirección IP, la máscara de subred, la puerta de enlace, el DNS preferido y el DNS alternativo. Pero si el número de dispositivos de nuestra red es elevado, existe la posibilidad de configurar las direcciones IP de forma automática.

Para que el equipo pueda obtener una dirección IP automáticamente, es necesario que alguien se la proporcione. Ese alguien es un **servidor DHCP**. La mayoría de los routers ADSL actuales disponen de servidor DHCP. Si activamos dicha función, podríamos configurar las IPs de nuestra red de forma automática:

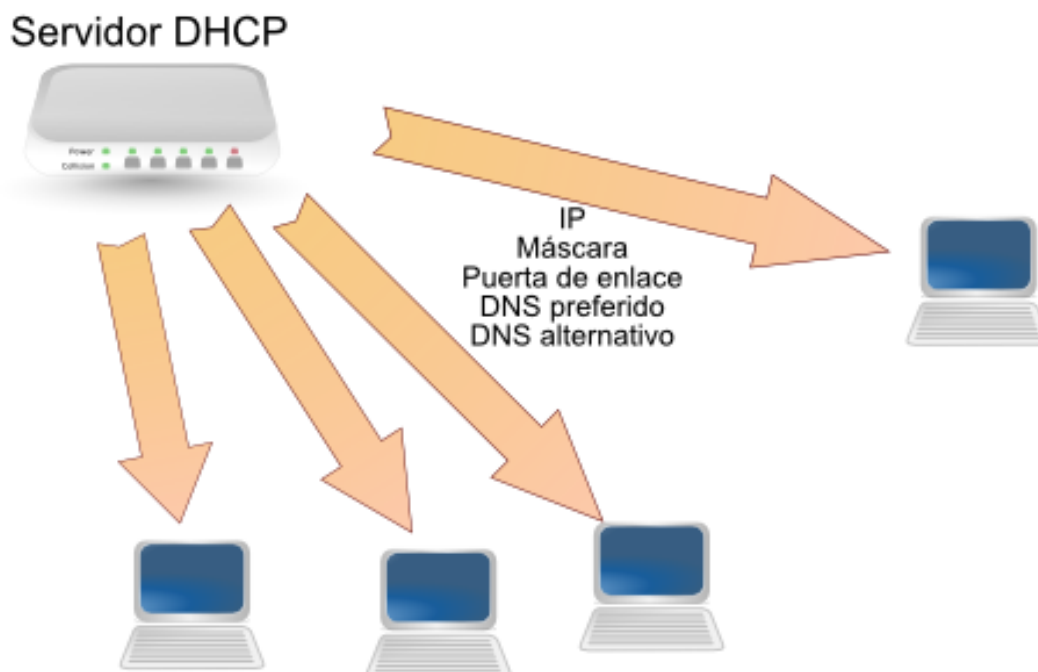


Imagen: Funcionamiento de un servidor DHCP



ENLACE DE INTERÉS

Información adicional sobre DHCP:

<http://technet.microsoft.com/es-es/library/dd145320%28v=ws.10%29.aspx>

3.4 Configuración de TCP/IP en sistemas Windows

Para establecer los parámetros de TCP/IP anteriormente comentados en un sistema Windows, se deben seguir estos pasos:

1. Desde el Panel de control, en la sección Redes e Internet, se accede al **Centro de redes y recursos compartidos**.

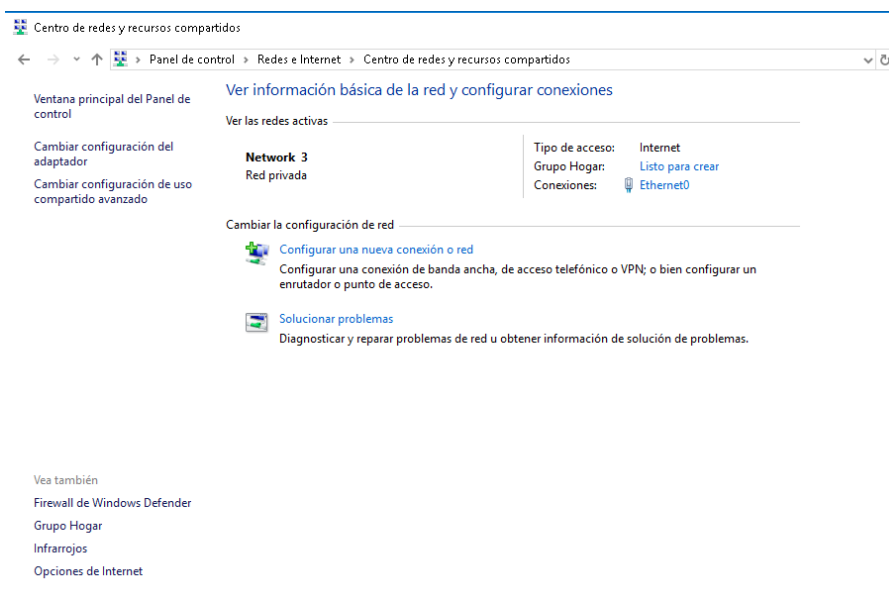


Imagen: Centro de redes y recursos compartidos en Windows 10

2. Se elige la opción **"Cambiar configuración del adaptador"** para acceder a las Conexiones de red de nuestro equipo.

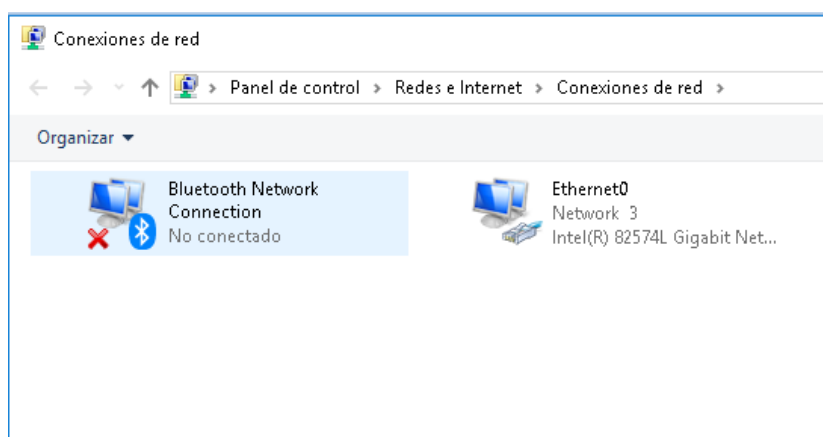


Imagen: Conexiones de red

3. Se pulsa con el botón derecho sobre la conexión que se desea cambiar y, a continuación, se elige la opción **Propiedades**. Si se solicita una contraseña de administrador o una confirmación, se escribe la contraseña o se proporciona la confirmación.

4. En la ventana que se muestra se ofrece toda la información acerca de la conexión elegida. Para la configuración que deseamos realizar se utilizan los elementos **Protocolo de Internet versión 4 (TCP/IPv4)** o **Protocolo de Internet versión 6 (TCP/IPv6)**, en función de la versión del protocolo con la que se desee trabajar. Seleccionada dicha versión, se pulsa el botón **Propiedades**.

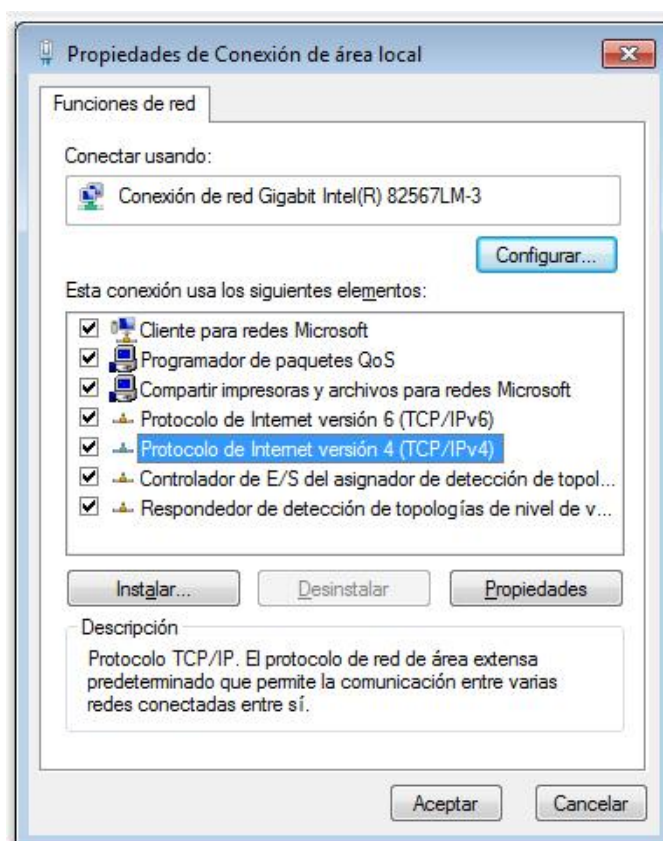


Imagen: Propiedades de la conexión de red

5. Para especificar la configuración de una dirección IPv4 (el proceso con IPv6 sería muy similar), tenemos dos opciones:
- Para obtener la configuración de TCP/IP de forma automática, utilizando DHCP, se marca la opción **Obtener una dirección IP automáticamente**.
 - Para especificar una dirección IP de forma manual, se elige la opción **Utilizar la siguiente dirección IP** y se rellenan los campos **Dirección IP**, **Máscara de subred** y **Puerta de enlace predeterminada**, atendiendo a las indicaciones facilitadas en apartados anteriores.

6. Para especificar la configuración de los servidores DNS, igualmente tenemos dos opciones:

- Para obtener la dirección de servidor DNS automáticamente, se marca la opción **Obtener la dirección del servidor DNS automáticamente**.
- Para especificar manualmente una dirección de servidor DNS (o dos, si también proporcionamos el servidor alternativo), se selecciona **Usar las siguientes direcciones de servidor DNS** y, en **Servidor DNS preferido** y **Servidor DNS alternativo**, se escriben las direcciones de los servidores DNS principal y secundario, respectivamente.

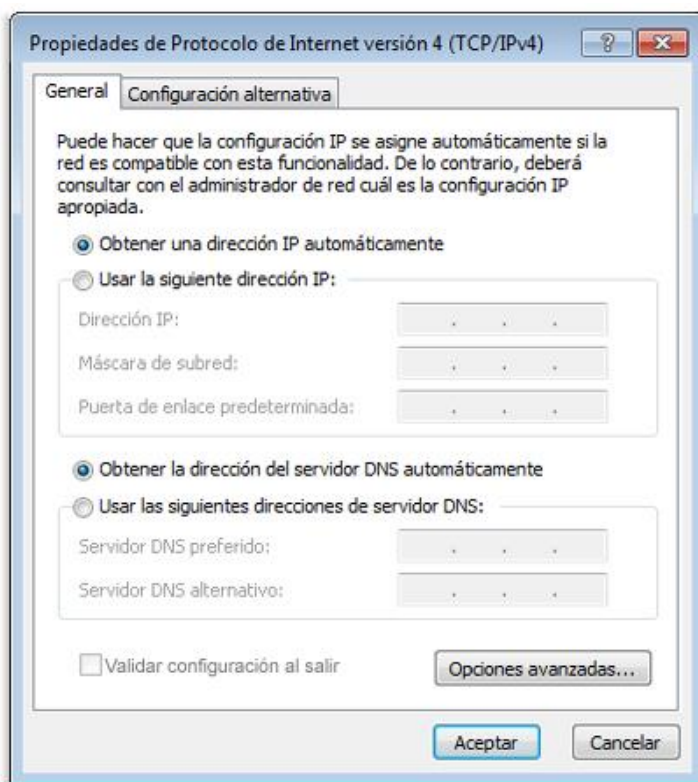


Imagen: Configuración del Protocolo de Internet versión 4 (IPv4)

En el caso de **redes inalámbricas**, el procedimiento de configuración es muy similar. Simplemente tendremos que seleccionar en el paso 3 nuestro dispositivo inalámbrico, y a partir de aquí la operativa es la misma.

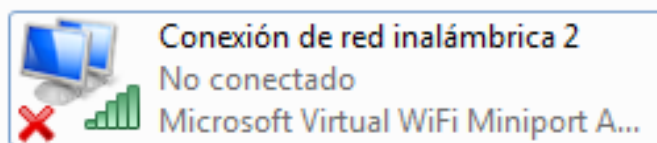


Imagen: Configuración de dispositivo inalámbrico



ENLACE DE INTERÉS

Para ver un tutorial detallado de la configuración de una red inalámbrica en un sistema Windows, revisad el siguiente enlace:

<https://support.hp.com/es-es/document/c03531390>

3.5. Configuración de TCP/IP en sistemas Linux

En sistemas Linux, la configuración del protocolo TCP/IP se hace de forma muy similar a la descrita anteriormente para los sistemas Windows.

1. En este caso se hace uso de las **Conexiones de red**, herramienta a la que podemos acceder desde el buscador de Unity.

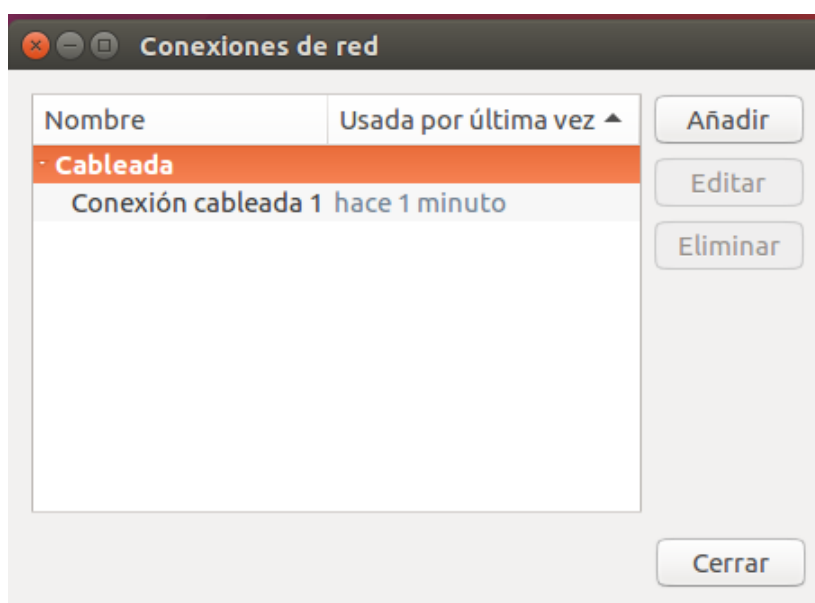


Imagen: Conexiones de red en Ubuntu

2. Se selecciona la conexión que se desea configurar, y se pulsa el botón **Editar**.

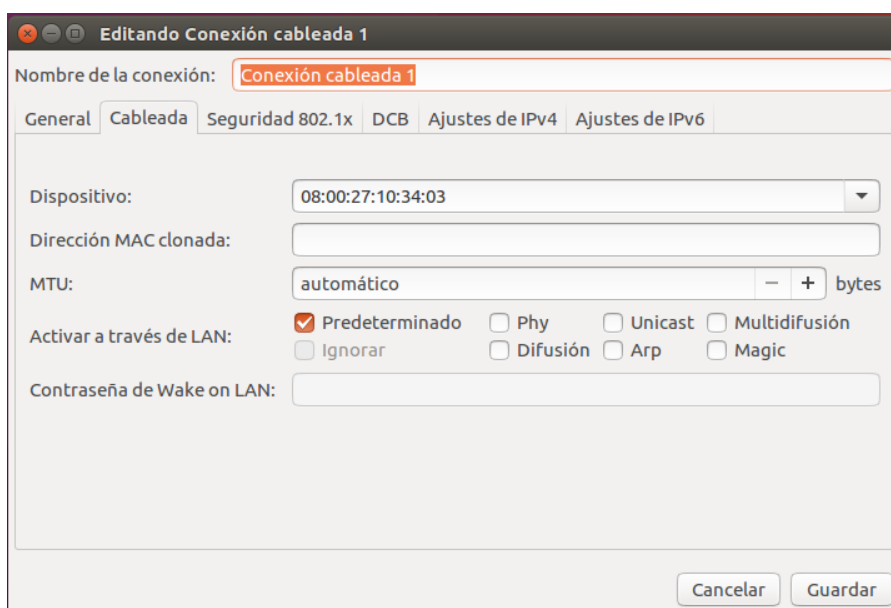


Imagen: Configuración de la conexión seleccionada

3. Como puede apreciarse en la imagen anterior, se dispone de pestañas para configurar tanto IPv4 como IPv6. Si se elige la primera de ellas, por ejemplo, se ve como la opción por defecto es aplicar una configuración automática, mediante DHCP.

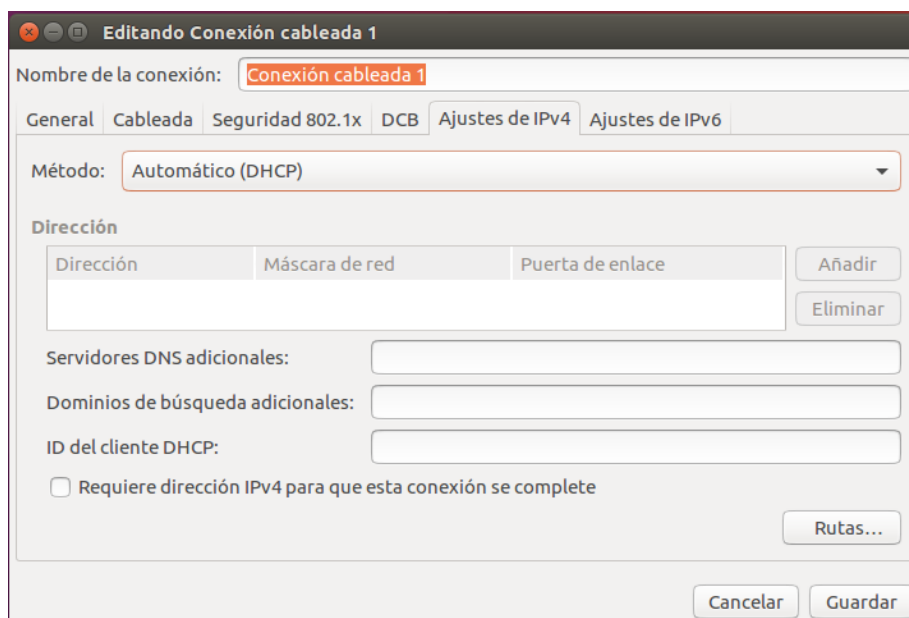


Imagen: Configuración automática de IPv4

4. Se puede cambiar el Método a **Manual**, y de ese modo introducir a mano los valores deseados para la dirección IP, máscara de subred...

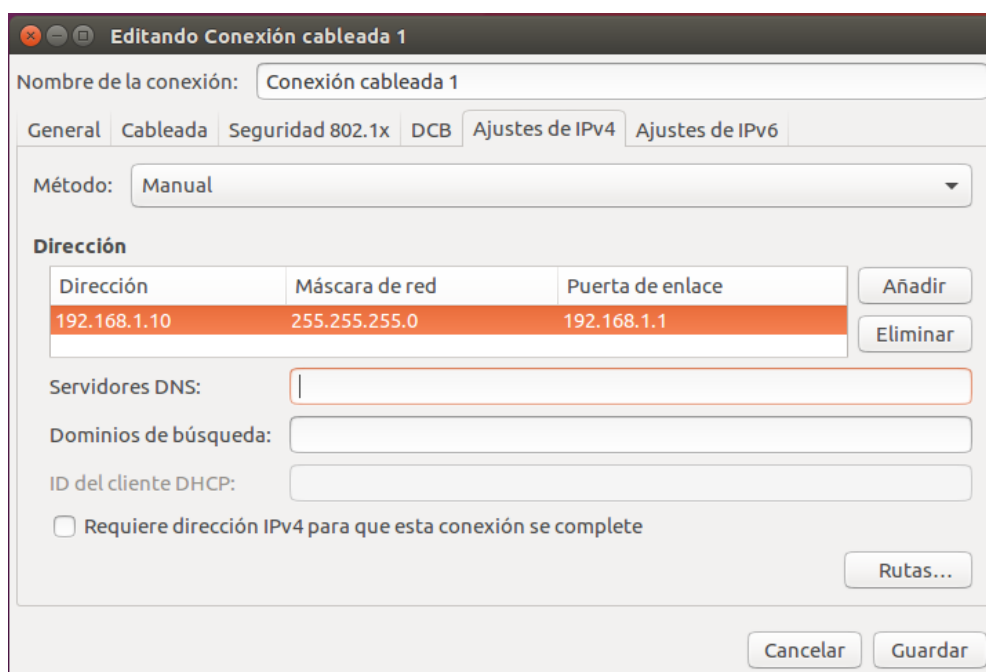


Imagen: Configuración manual de IPv4

3.6 Ficheros de configuración de red

Aunque lo habitual es realizar todos los procesos de configuración de una red mediante entorno gráfico, tal como se ha descrito en el apartado anterior, los sistemas operativos disponen de una serie de ficheros en los que se almacena la información de dicha configuración. Conocer estos ficheros resulta muy útil, bien para consultar los datos de nuestras redes, bien para modificarlos de forma manual si queremos agilizar el proceso.

A continuación se describen los principales archivos de configuración para sistemas Linux.

- **ARCHIVO /etc/network/interfaces:** Contiene la información necesaria para configurar las interfaces de red del host al arrancar el sistema. También permite establecer las rutas estáticas hacia otras redes.

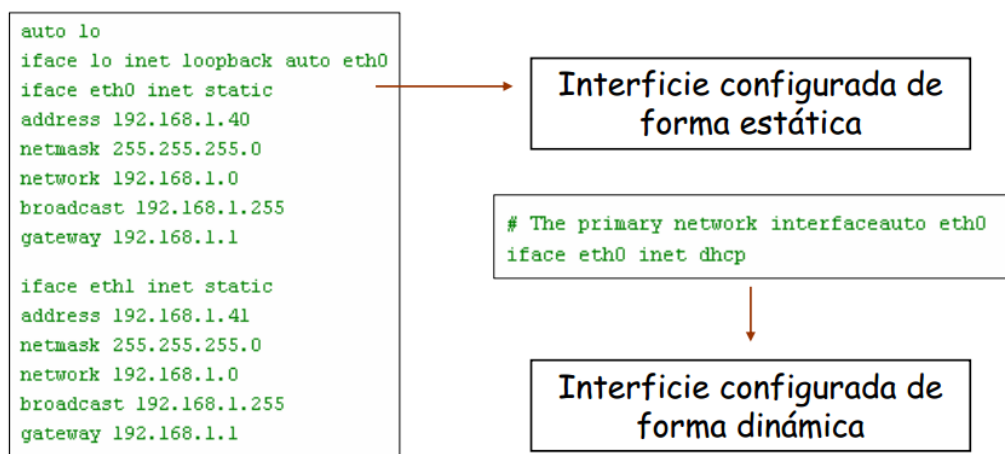


Imagen: Contenido del archivo interfaces

- **ARCHIVO /ETC/HOSTNAME** contiene el nombre del equipo que adopta el S.O. al iniciar el equipo
- **FICHERO /ETC/HOST.CONF** indica al sistema de resolución qué servicios debe usar y en qué orden. El fichero host.conf indica el orden de las fuentes que utilizará el resolver del S.O. para obtener las resoluciones DNS que necesiten las aplicaciones del equipo. Tiene dos opciones:
 - Buscarlas dentro: fichero /etc/hosts.
 - Buscarlas fuera: fichero /etc/resolv.conf

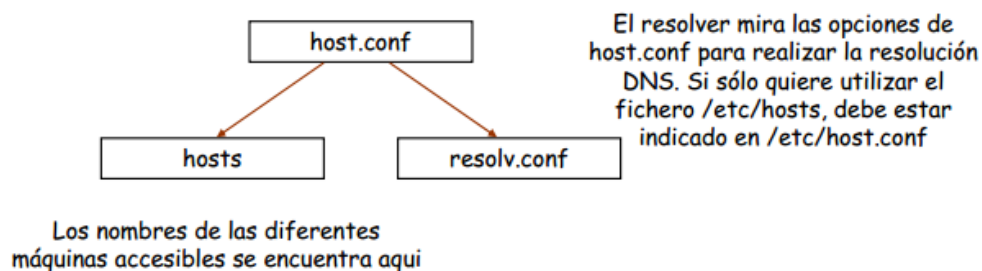


Imagen: Resolución de servidores

- **FICHERO /ETC/HOSTS** representa un mecanismo simple de resolución de nombres. Contiene un registro por línea, consistente en una dirección IP, un nombre de máquina y de forma opcional, una lista de alias para esa máquina. Los campos se separan por tabuladores o espacios y el campo con la @ IP debe empezar en la primera columna.

```
# archivo /etc/hosts
#
# IP            FQDN            aliases
#
# definición del bucle local.
127.0.0.1      localhost
#
172.16.1.1     web.dominio.local    web
172.16.1.2     gate.dominio.local   gate
#
172.16.2.1     mail.dominio.local    mail
172.16.2.2     host.dominio.local   host
```

Tanto el nombre con cualificación completa (oficial) como el nombre local se deben registrar en el fichero `/etc/hosts`, para ser referidos al resolver su dirección IP.

Imagen: Contenido del archivo hosts

- **FICHERO /ETC/RESOLV.CONF** contiene las direcciones IP de las máquinas que pueden ofrecer servicios DNS a nuestro host. La instrucción `nameserver` apunta a servidores DNS que puede utilizar el host para realizar sus resoluciones. El fichero `/etc/hosts` tiene un compañero llamado `/etc/networks`, que asocia nombres de red con los números correspondientes y viceversa.

4. GESTIÓN DE PUERTOS

Como hemos visto en el apartado anterior, cada dispositivo conectado a una red TCP/IP debe tener una dirección IP que lo identifique. Pero dado que el ancho de banda de las conexiones actuales es cada vez mayor, se puede obtener un mejor rendimiento permitiendo que ese dispositivo pueda ejecutar simultáneamente varias aplicaciones mediante una misma conexión.

Por ejemplo, pueden abrirse diferentes navegadores de manera simultánea o navegar por páginas HTML mientras se descarga un archivo de un servidor FTP. Para conseguirlo, a cada una de esas aplicaciones se le asigna una dirección única que se denomina **puerto**.

Los puertos se codifican con 16 bits, por lo que existen 65536 posibilidades distintas. Es por ello que la **IANA** (*Internet Assigned Numbers Authority*) estableció una codificación estándar para ellos.

- Los puertos del 0 al 1023 son los "**puertos bien conocidos**" o reservados. En términos generales, están reservados para procesos del sistema o programas que emplean protocolos bien conocidos, como HTTP (puerto 80) o FTP (puerto 21).
- Los puertos del 1024 al 49151 son los "**puertos registrados**". Pueden ser usados por cualquier aplicación.
- Los puertos del 49152 al 65535 son los "**puertos dinámicos o privados**". Suelen utilizarse por aplicaciones P2P (peer to peer).

Como se ha dicho, la dirección IP sirve para identificar de manera única un equipo en la red mientras que el número de puerto especifica la aplicación a la que se dirigen los datos. Así, cuando el equipo recibe información que va dirigida a un puerto, los datos se envían a la aplicación relacionada. Si se trata de una solicitud enviada a la aplicación, la aplicación se denomina aplicación **servidor**. Si se trata de una respuesta, entonces hablamos de una aplicación **cliente**.



PARA SABER MÁS

En un dispositivo determinado, la combinación de *dirección IP* + *puerto* es una dirección única en el mundo denominada socket.



ENLACE DE INTERÉS

En el siguiente enlace se puede consultar una lista de los números de puerto más conocidos y utilizados:

https://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros_de_puertos_de_red

5. RESOLUCIÓN DE PROBLEMAS DE CONECTIVIDAD EN SISTEMAS OPERATIVOS EN RED

En muchas ocasiones, pese a aplicar las técnicas descritas en apartados anteriores, se producen problemas de conectividad que impiden que los dispositivos puedan acceder de forma correcta a las redes.

Los sistemas operativos en red proporcionan una serie de herramientas que nos ayudan con la gestión y mantenimiento de redes. Herramientas a las que hay que sumar un buen número de utilidades adicionales, tanto gratuitas como de pago.

5.1 Verificación del funcionamiento de una red mediante el uso de comandos.

A continuación se describen algunos de los comandos más utilizados para la verificación de una red en entornos Linux. La mayor parte de ellos tienen sus equivalentes en los sistemas Windows (algunos incluso funcionan en ambos sistemas).

- **hostname**

Sintaxis: `hostname [hostname]`

Si no se especifica ningún nombre de equipo la orden proporciona el nombre del equipo. Si se especifica el nombre del equipo en `hostname` la orden cambia el nombre local de la máquina.

- **host**

Sintaxis: `host hostname | IP_address`

Interroga al sistema para obtener la dirección IP del equipo especificado en `hostname` o el nombre del equipo que tiene una IP especificada en `IP_address`

- **dig**

Sintaxis: `dig hostname`

La orden `dig` proporciona información de los servidores DNS que gestionan el nombre de dominio especificado en `hostname`.

- **ifconfig**

Sintaxis: ifconfig interface parameters

La orden ifconfig permite crear y configurar las interfaces de red. Si no se indican parámetros la orden muestra la configuración de la interface especificada. Si tampoco se indica la interface la orden muestra la configuración de todas las interfaces de red del sistema.

Parámetros:

- Dirección: Configura la dirección IP de la interface de red especificada.
- netmask mascara: Configura la máscara de red de la interface de red especificada.
- broadcast dirección: Configura la dirección IP de broadcast.
- up/down Activa/desactiva la interface de red especificada.

- **route**

Sintaxis: route options

route [add|del] [-net|-host] destino

Permite mostrar la tabla de encaminamiento IP del sistema. También permite añadir o eliminar una entrada en la tabla de encaminamiento. Target puede ser una dirección IP numérica o un nombre de equipo o el nombre default. La orden route permite establecer las rutas de encaminamiento estáticas de la red.

Opciones y Parámetros:

- -net Especifica que el target especificado es una red.
- -host Especifica que el target especificado es un equipo.

- **netstat**

Sintaxis: netstat options

En función de la opción la orden netstat muestra las interfaces de red, los PID asociados a cada interface,...

Opciones:

- -c Operación continua. Renueva la información cada segundo hasta que se cancela la orden mediante ctrl-c.
- -i Muestra una lista con todos los interfaces de red.
- -p Muestra una lista de los PID.
- -r Muestra la información de la tabla de encaminamiento.
- -t Muestra las conexiones activas a puertos TCP.
- -u Muestra las conexiones activas a puertos UDP. Si se incluye "a" se mostrarán también los puertos que estén esperando una conexión (que estén escuchando).

- **Ping**

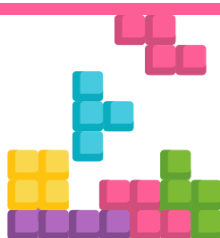
Sintaxis: ping hostname

La orden ping envía una petición de eco del protocolo ICMP al equipo especificado en hostname y muestra el tiempo transcurrido hasta recibir la confirmación del eco. En Windows la opción por defecto envía 4 mensajes. Con el modificar "-t" envía mensajes indefinidamente hasta que se cancela la orden mediante ctrl-c. En Linux por defecto envía mensajes de forma indefinida hasta que se cancele.

- **tracert**

Sintaxis: tracert hostname

Muestra la ruta que los paquetes siguen hasta alcanzar la destinación, mostrando todos las gateways y routes del camino.



EJEMPLO PRÁCTICO

Un equipo de nuestra empresa tiene problemas con la conexión a Internet. Como primera medida queremos comprobar que tiene acceso a la puerta de enlace de nuestra red.

SOLUCIÓN

Se ejecuta el comando PING con la dirección IP de la puerta de enlace:
PING 192.168.1.1

```
cesur@cesur-VirtualBox: ~  
cesur@cesur-VirtualBox:~$ ping 192.168.1.1 -c 4  
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.  
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=2.10 ms  
64 bytes from 192.168.1.1: icmp_seq=2 ttl=63 time=2.97 ms  
64 bytes from 192.168.1.1: icmp_seq=3 ttl=63 time=2.51 ms  
64 bytes from 192.168.1.1: icmp_seq=4 ttl=63 time=6.03 ms  
  
--- 192.168.1.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3006ms  
rtt min/avg/max/mdev = 2.100/3.404/6.032/1.549 ms  
cesur@cesur-VirtualBox:~$
```

5.2 Herramientas de monitorización de redes

El administrador de un sistema informático suele utilizar, además de los comandos citados en el apartado anterior, software especializado en monitorización de redes, que le permite detectar posibles problemas y le ayuda a solucionarlos. Algunas de las herramientas más conocidas en este campo son:

- **Nagios.** Está considerado uno de los más populares, si no el más popular, sistemas de monitorización de red. Fue diseñado originalmente para ejecutarse en Linux, pero actualmente también dispone de versiones para Windows. Nagios proporciona supervisión de los servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH) y recursos de host (carga del procesador, uso de disco, los registros del sistema), entre otros.

Nagios tiene un diseño simple que ofrece a los usuarios la libertad para desarrollar sus chequeos de servicio sin esfuerzo propio basado en las necesidades y mediante el uso de cualquiera de las herramientas de apoyo que guste. Cuando los servicios o los problemas de acogida se plantean, la notificación será enviada a la persona que está a cargo de la red a través del correo electrónico, SMS, etc.

- **Zabbix.** De configuración sencilla, cuenta con una interfaz gráfica bastante intuitiva. Permite monitorizar un elevado número de nodos sin que su rendimiento se vea afectado.

Para almacenar los datos de seguimiento, puede utilizar MySQL, PostgreSQL, Oracle o SQLite como base de datos. Sin necesidad de instalar ningún software en el host de seguimiento, Zabbix permite a los usuarios comprobar la disponibilidad y capacidad de respuesta de los servicios estándar, como SMTP o HTTP. Para supervisar las estadísticas, tales como carga de la CPU, utilización de la red y espacio en disco, un agente de Zabbix debe estar instalado en la máquina host. Zabbix incluye soporte para la monitorización a través de SNMP, TCP y controles ICMP, IPMI y parámetros personalizados como una opción para instalar un agente en los hosts.

- **Pandora FMS.** Se puede considerar una suite de monitorización, ya que además de revisar redes, también permite monitorizar servidores y aplicaciones. Incluso dispositivos móviles, ya que incorpora un avanzado sistema de geolocalización. Dispone de una versión Community, de código abierto, disponible para pequeñas empresas y usuarios particulares.



ENLACE DE INTERÉS

Para ampliar información y descargar estos software se recomienda su web oficial:

<https://www.nagios.com/>

<https://www.zabbix.com/>

<https://pandorafms.com/es/>

RESUMEN FINAL

En esta unidad se ha comenzado por revisar el concepto de modelo de red, y estudiar los dos principales modelos existentes, OSI y TCP/IP. Se han descrito las capas de cada uno de los modelos y se ha establecido una comparativa entre ambos para ver sus similitudes y diferencias.

Se ha visto con detalle, tanto para sistemas operativos libres como propietarios, el proceso de configuración de un dispositivo que se desee conectar a una red TCP/IP, presentando conceptos fundamentales como dirección IP, máscara de subred, puerta de enlace, DNS o DHCP.

Seguidamente se ha visto cómo los puertos pueden ayudarnos a obtener un mayor rendimiento de una conexión a una red.

Y finalmente se han revisado una serie de herramientas, bien propias del sistema (comandos de Linux concretamente), bien externas, diseñadas para verificar y solucionar los problemas habituales que se pueden presentar en un dispositivo conectado en red.