Conexión de sistemas en red (Sistemas informáticos)

Configuración del protocolo TCP/IP en un cliente de red. Direcciones IP. Máscaras de subred. IPv4. IPv6. Configuración estática. Configuración dinámica automática

Los sistemas operativos se pueden conectar a la red de diversas formas, lo primero que hay que tener en cuenta es el dispositivo que permite la conexión a la red y lo segundo cómo se configura dicho dispositivo.

Se pueden utilizar varios dispositivos para realizar una conexión, por ejemplo un modem (puede ser USB o no) con un cable RJ-11, una tarjeta de red con un cable RJ-45, una tarjeta inalámbrica, etc.

Los parámetros de configuración básicos para una red son la dirección IP, la máscara de red, la puerta de enlace (Gateway) y los DNS. Veamos brevemente que es cada parámetro:

- La dirección IP (Internet Protocol, Protocolo de Internet) es un código que identifica a un interfaz como único, el interfaz es un dispositivo como una tarjeta de red, un punto de acceso, etc. Hay distintas versiones de direcciones IP:
    - La IPv4 está formada por un número binario de 32 bits, que normalmente se representa como 4 números en base decimal del 0 al 255, separados por puntos. Ejemplo: Dirección localhost en IPv4: 127.0.0.1

        - La otra versión es la IPv6 que son un número de 128 bits, representado en hexadecimal con 32 dígitos, separados por dos puntos en grupos de 4 dígitos. Ejemplo: Direccion localhost en IPv6: 0:0:0:0:0:0:0:1
    - La máscara sirve para saber si se deben enviar los datos dentro o fuera de las redes. Por ejemplo, si el sistema operativo tiene la IP 192.168.1.1 y máscara de red 255.255.255.0, entiende que todo lo que se envía a una IP que empiece por 192.168.1 va para la red local y todo lo que va a otras ips, para fuera (internet, otra red local mayor…).
    - Un Gateway (puerta de enlace) es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. El valor de la puerta de enlace es otro de los valores que se deben indicar a la hora de configurar la conexión de red.
    - Los DNS son dirección IP que sirven para resolver los nombres de dominio FQDN (Fully Qualified Domain Names) y traducirlos a direcciones IPv4.

Los parámetros que acabamos de ver se pueden asignar de las siguientes formas:

- Manual: La dirección IP se introduce mediante el teclado o cualquier otro dispositivo que lo permita.
- Automáticamente: El servidor DHCP (Dynamic Host Configuration Protocol), asigna siempre la misma IP a un dispositivo.
- Dinámicamente: El servidor DHCP asigna una IP del rango de direcciones que tiene disponible, la dirección IP puede coincidir.

Ficheros de configuración de red

Dependiendo del sistema operativo encontramos unos u otros ficheros relacionados con la configuración de la red.

Gestión de puertos

Los puertos son asignados por el sistema operativo de tu dispositivo cada vez que un proceso va a hacer una conexión de red. Por ejemplo, cuando abres una página web, tu navegador le pide al sistema operativo un puerto para poder recibir la respuesta del pedido que va a enviar.

Resolución de problemas de conectividad en sistemas operativos en red

Existen herramientas para resolver problemas de conectividad tanto en Windows como en Linux.

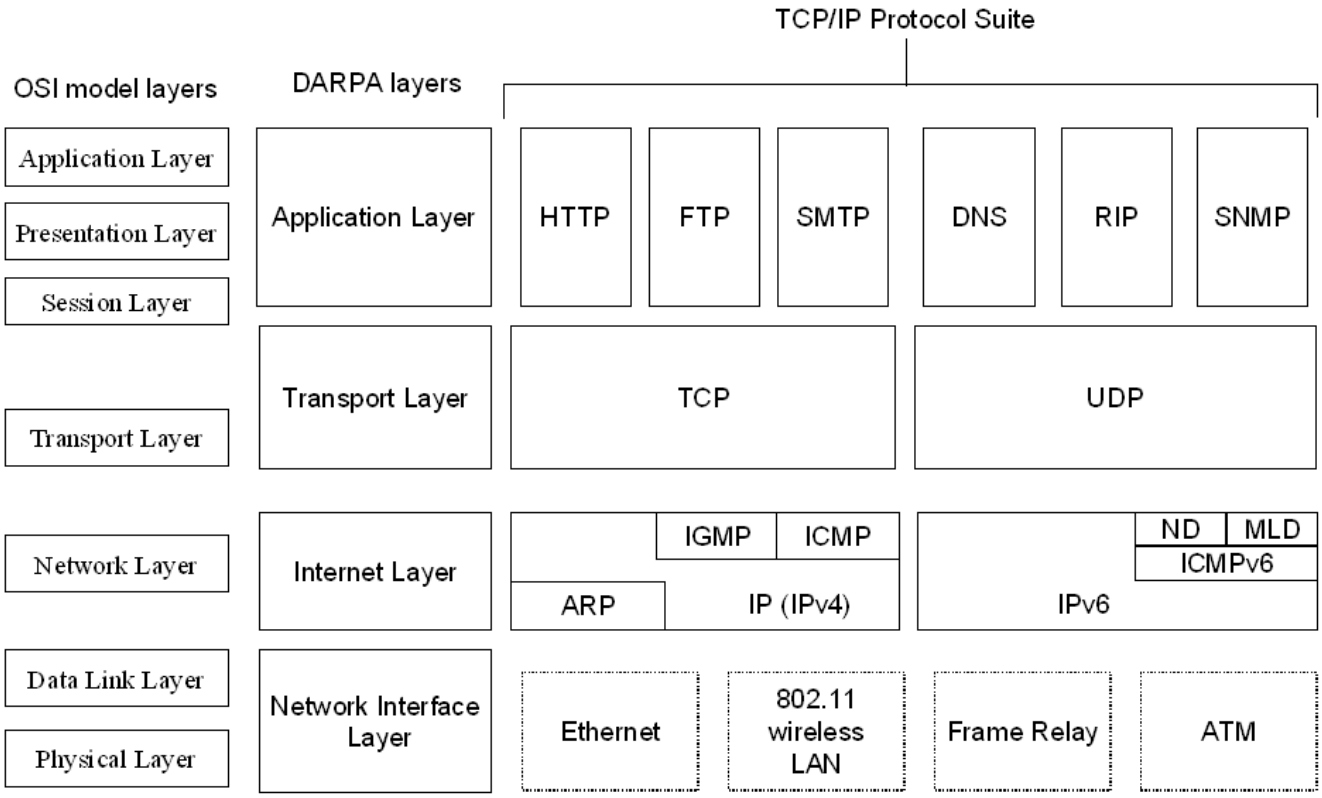
Comandos utilizados en sistemas operativos libres y propietarios

	Modo texto: Símbolo de sistema	**Modo texto: PowerShell**	**Modo texto: Bash**	**Modo gráfico Windows**	**Modo gráfico Ubuntu**
Gestión de red	ipconfig /all netsh	–	iface ifconfig route	Cambiar configuración del adaptador	Conexiones de red – Cableada (pestaña)

Monitorización de redes

La monitorización de las redes se realiza mediante herramientas o comandos.

Protocolos TCP/IP



Relación de las capas del modelo TCP/IP:

Capa física

La capa de red física especifica las características del hardware que se utilizará para la red. Por ejemplo, la capa de red física especifica las características físicas del medio de comunicaciones. La capa física de TCP/IP describe por ejemplo los estándares de hardware como IEEE 802.3 y la especificación del medio de red Ethernet.

Capa de Internet

La capa de Internet, también conocida como capa de red o capa

IP, acepta y transfiere paquetes para la red. Esta capa incluye el potente Protocolo de Internet (IP), el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP).

Capa de transporte

La capa de transporte TCP/IP garantiza que los paquetes lleguen en secuencia y sin errores, al intercambiar la confirmación de la recepción de los datos y retransmitir los paquetes perdidos. Los protocolos de capa de transporte de este nivel son el Protocolo de control de transmisión (TCP) y el Protocolo de datagramas de usuario (UDP). El protocolo TCP proporciona un servicio completo y fiable. UDP proporciona un servicio de datagrama poco fiable.

Capa de aplicación

La capa de aplicación define las aplicaciones de red y los servicios de Internet estándar que puede utilizar un usuario. Estos servicios utilizan la capa de transporte para enviar y recibir datos.

Existen varios protocolos de capa de aplicación. En la lista siguiente se incluyen ejemplos de protocolos de capa de aplicación, algunos ejemplos son:

- Servicios TCP/IP estándar como los comandos ftp, tftp y telnet.
- Servicios de nombres, como NIS o el sistema de nombre de dominio (DNS).
- Servicios de directorio (LDAP).

Configuración de los adaptadores de red en sistemas operativos libres y

propietarios

Los sistemas operativos se pueden conectar a la red de diversas formas, lo primero que hay que tener en cuenta es el dispositivo que permite la conexión a la red y lo segundo cómo se configura dicho dispositivo.

Interconexión de redes: adaptadores de red y dispositivos de interconexión

Se pueden utilizar varios dispositivos para realizar una conexión, por ejemplo un modem (puede ser USB o no) con un cable RJ-11, una tarjeta de red con un cable RJ-45, una tarjeta inalámbrica, etc. Existen más tipos de sistemas para realizar conexiones de red.

Redes cableadas. Tipos y características. Adaptadores de red. Conmutadores, enrutadores, entre otros

Un enrutador (del inglés router) o encaminador, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red. Su función: se encarga de establecer la ruta que destinará a cada paquete de datos dentro de una red informática.

Redes inalámbricas. Tipos y características.

Adaptadores.Dispositivos de interconexión

Las redes inalámbricas (wireless network, wireless) son redes sin cable. Normalmente son las redes que se comunican por medios no guiados y lo hacen por ondas electromagnéticas. La transmisión y la recepción se efectúan a través de antenas.

El Punto de Acceso (Access Point, AP o Wireles Access Point, WAP) es el intermediario de la comunicación en una red inalámbrica con topología en modo infraestructura, comunicándose por ondas de radio, o sea que actúa de puente o bridge.

La diferencia básica de un router inalámbrico, con uno tradicional es que permite la conexión de dispositivos inalámbricos a las redes a las que el router está conectado mediante conexiones por cable.

Seguridad básica en redes cableadas e inalámbricas

Entre los enrutadores inalámbricos, las diferencias que nos pueden hacer elegir un modelo a otro vienen reflejadas en los estándares que soportan.

El problema de las redes WiFi es la seguridad. Existen varias alternativas para garantizar la seguridad de las redes que usan estos estándares.

Consejos que fortalecen la seguridad de las redes inalámbricas:

- Evitar conexiones abiertas.
- Cambiar las contraseñas de acceso.
- Evitar que se pueda tener acceso a través de Internet al router.

- Filtrado de direcciones MAC y direcciones IP.
- Revisar los logs.

Seguridad de comunicaciones

Los datos que circulan a través de la red entre aplicaciones son accesibles por terceras personas ajenas a la comunicación, es necesario evitarlo a toda costa mediante el uso de protocolos seguros.

También si importante asegurarse de que los datos no se modifiquen durante el transporte. Los protocolos que aseguran la información a nivel de capa de transporte son SSL y TLS.

El protocolo SSL

Originalmente diseñado por Netscape para establecer comunicaciones seguras con protocolos como HTTP o FTP. Permite negociar qué algoritmos se van a emplear, intercambiar las claves de encriptación y la autentificación de clientes y servidores.

Existen tres versiones del protocolo, la cuarta es una mejora del SSLv3 y se conoce con el nombre de TLS.

El protocolo TLS (Transport Layer Security)

Es una evolución del protocolo SSL (Secure Sockets Layer). La última propuesta de estándar está documentada en la referencia [RFC_2246].

Los objetivos del protocolo son varios:

- Seguridad criptográfica. El protocolo se debe emplear para establecer una conexión segura entre dos partes.
- Interoperabilidad. Aplicaciones distintas deben poder intercambiar parámetros criptográficos sin necesidad de que ninguna de las dos conozca el código de la otra.
- Extensibilidad. El protocolo permite la incorporación de

nuevos algoritmos criptográficos.

- Eficiencia. Los algoritmos criptográficos son costosos computacionalmente, por lo que el protocolo incluye un esquema de caché de sesiones para reducir el número de sesiones que deben inicializarse desde cero (usando criptografía de clave pública).

El protocolo SSL/TLS tiene multitud de aplicaciones en uso actualmente. La mayoría de ellas son versiones seguras de programas que emplean protocolos que no lo son. Hay versiones seguras de servidores y clientes de protocolos como el http, nntp, ldap, imap, pop3, etc.

Existen multitud de implementaciones del protocolo, tanto comerciales como de libre distribución. Una de las más populares es la biblioteca openssl, escrita en C y disponible bajo licencia GNU. Incluye todas las versiones del SSL y el TLS y un gran número de algoritmos criptográficos, algunos de los cuales ni tan sólo son empleados en el estándar TLS. La biblioteca está disponible en el URL http://www.openssl.org. En esa misma dirección se puede encontrar una lista de referencias a otras implementaciones gratuitas y comerciales de los protocolos SSL y TLS y aplicaciones que los emplean.