Conceptos básicos

Es un conjunto de protocolos organizados por niveles que trabajan de forma conjunta para la transferencia de datos y ofrecer servicios de forma segura y fiable

La arquitectura de red es el diseño de una red de comunicaciones

Viene definida en tres características

* Topología: establece la configuración básica de interconexión de estaciones
* Método de acceso a red: regular el orden en que transmiten los equipos
* Protocolos de comunicación: reglas y procedimientos utilizados en una red para realizar la comunicación

Como funciona dentro de la maquina

* Cada nivel utiliza los servicios del nivel inferior
* Un servicio se define como un conjunto de operaciones que una capa proporciona a la capa superior o al usuario
  + Servicio web
* En el emisor la información viaja hacia abajo (del usuario al medio) y cada nivel del emisor añade su propia información en forma de cabecera
* En el receptor la información viaja hacia arriba (desde medio hacia el usuario) y cada nivel del receptor extrae la información de cabecera que le corresponde y entrega el resto al nivel superior

Entre maquinas distintas

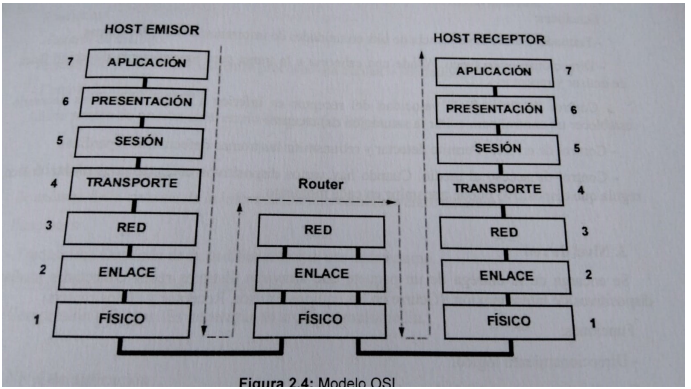
* El nivel n de la maquina A se comunica con el nivel n de la maquina B mediante un protocolo
* Los procesos del mismo nivel que se comunican se llaman procesos pares
  + Servidor web httpd.exe al cliente Chrome.exe
* Protocolo: conjunto de reglas que regulan el formato y significado de los paquetes que intercambian dos procesos pares
  + HTTP

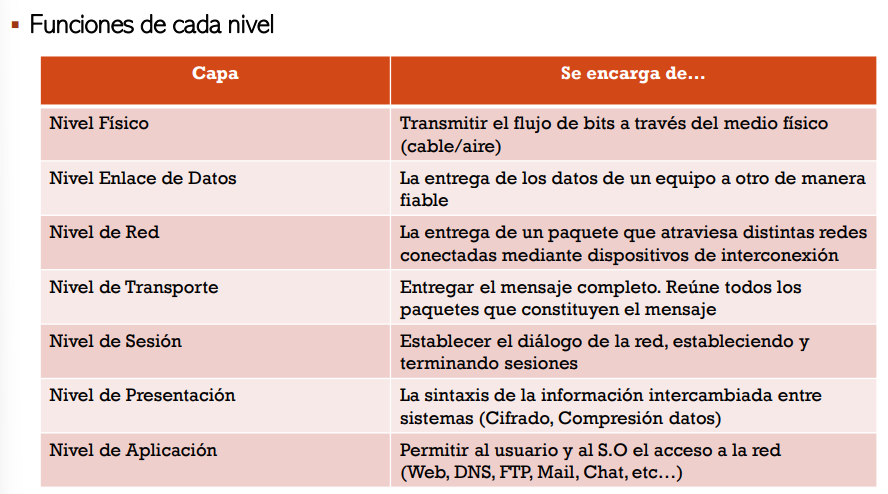
MODELO OSI

Es un estándar desarrollado por la Organización internacional de estandarización en 1983

Cubre todos los aspectos de las redes de comunicaciones

Este compuesto por 7 niveles





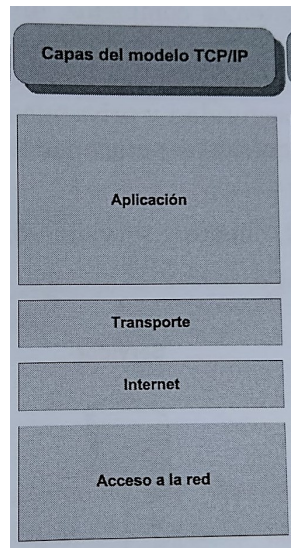
Arquitectura TCP/IP

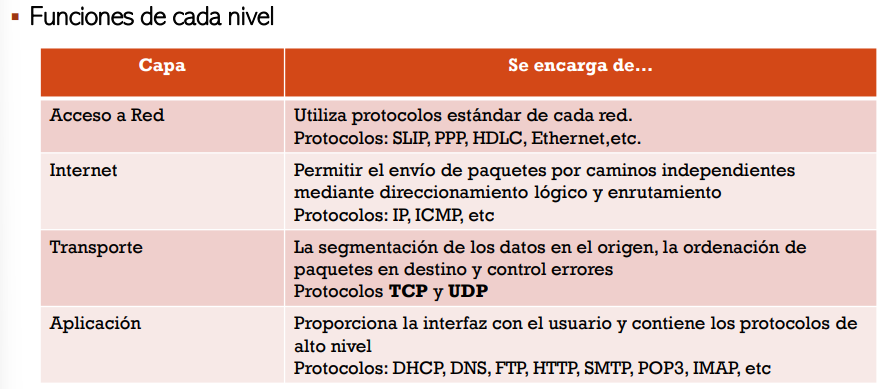
Se desarrollo antes que el modelo OSI

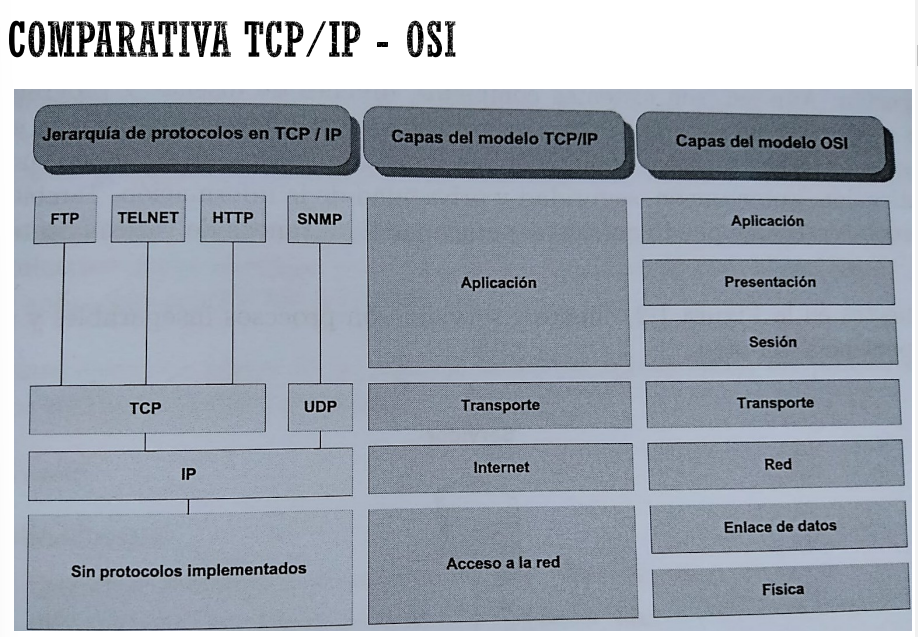
Proporciona una estructura y una serie de normas de funcionamiento para poder interconectar sistemas

TCP/IP es un conjunto de protocolos organizados jerárquicamente con una función determinada y una cierta independencia entre si

Se compone de 4 niveles







Modelo cliente/servidor

Está formado por dos procesos, el proceso cliente y el proceso servidor

El cliente

* Inicia comunicación > papel activo
* Envía la petición a un proceso servidor
* Queda a la espera de la respuesta

El servidor

* Permanece a la espera escuchando > papel pasivo
* Envía una respuesta al cliente
* Complejos: autentificación, autorización, seguridad y privacidad

El servidor se queda en escucha todo el rato, el cliente quiere conseguir el recurso que está en el servidor, por lo que manda una petición para obtener el recurso del servidor, se queda en espera mientras el servidor recibe la petición y la envía al cliente, el servidor cierra la petición

Servicios de red

Función o prestación que ofrecen las aplicaciones y los protocolos a los usuarios o a otras aplicaciones

Las aplicaciones son sistemas de software que se comunican e intercambian información con otras aplicaciones con la ayuda de los protocolos de la arquitectura TCP/IP

OJO: no confundir los protocolos del nivel de aplicación con las aplicaciones que lo utilizan

Definiciones

* Aplicación: Programas de los usuarios o del sistema operativo que se sirve de los protocolos de la arquitectura TCP/IP para comunicarse
  + Thunderbird, apache
* Protocolo: normas concretas que detallan como se produce la comunicación entre los sistemas para ofrecer los servicios de red
  + IMAP,HTTP

Hay protocolos en todas las capas, y los protocolos de una capa, utilizan los protocolos de la capa inferior

Ejemplos reales

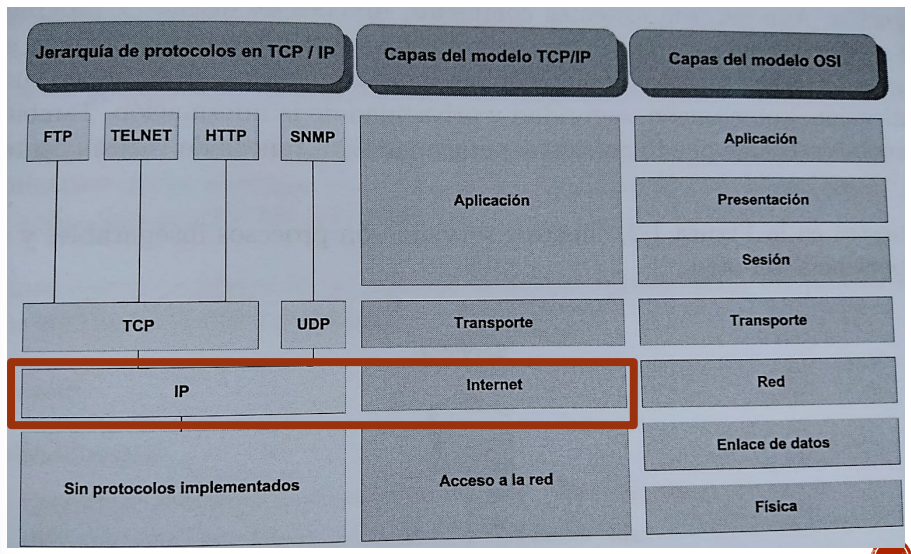
Servicio WEB

* Aplicaciones
  + Servidor IIS,APACHE,ETC
  + Cliente: FIREFOX, CHROME, etc
* Protocolos: HTTP, HTTPS

Servicio de correo electrónico

* Aplicaciones
  + Servidor: Exchange, Sendmail, ETC
  + Cliente: Outlook, thunderbird
* Protocolos: IMAP, POP, SMTP

Para entender el funcionamiento del servicio de red hay que prestar atención a los niveles de red y transporte de la arquitectura TCP/IP



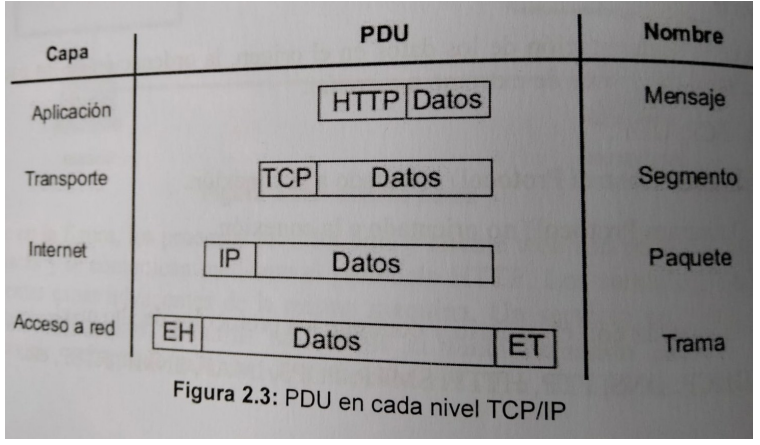
A nivel de red se realiza el direccionamiento de los dispositivos y el encaminamiento de la información a través de la red

La comunicación a nivel IP se hace mediante unidades de datos llamadas datagramas.

Actualmente se emplea IPv4, pero se está implementando la IPv6

El protocolo IP proporciona conectividad extremo a extremo en la comunicación

Cada dispositivo está identificado por una (dirección) IP.



Encaminamiento IP

* Proceso de llevar un datagrama de una maquina origen a la maquina destino
* El responsable es el protocolo IP
* Si las maquinas no están en la misma red se utilizan encaminadores

Encaminador o router

* Dispositivos de nivel 3 (internet o red) que enlazan las diferentes redes
* Conectan al menos 2 redes
* Encaminan todo el tráfico de datagramas que pasa por ellos, mediante tablas de encaminamiento

Encaminamiento

Todos los componentes a nivel de red (host, Routers, …) tiene tablas de encaminamiento o enrutamiento

Cuando un equipo va a enviar un datagrama comprueba la tabla de enrutamiento simplificando:

* Si el destino está en su misma red, hace un envió directo
* Si el destino en una red distinta, lo dirige al encaminador (puerta de enlace)

Cuando un router recibe un datagrama comprueba su tabla de enrutamiento

* Si va a una dirección que pertenece a una red conectada directamente, envió directo
* Si no, lo redirige a otro encaminador, siguiendo su tabla de encaminamiento. Este proceso puede ser recursivo y termina cuando se agota el tiempo de vida (TTL)

Tabla de enrutamiento

Almacena información necesaria para el encaminamiento en datagramas y están implementadas tanto en los Routers como en los hosts

Campos más importantes   
destino (D): dirección IP de una red o host

* Ruta de red: referencia una red
* Ruta de host: referencia un host
* Ruta por defecto: cuando no es ninguna de las anteriores

Mascara de red (MR): Asociada al destino y sirve para conocer todas las direcciones IP que incluye.

Dirección de salto (DS): Dirección IP a la que se enviara el datagrama si su dirección IP de destino coincide con la especificada por destino y mascara de red

Interfaz: dirección IP de encaminador por la que hay que enviar el datagrama a la dirección de salto

Protocolos de encaminamiento

* Encadenamiento estático
  + La configuración de las tablas de rutas es de forma manual
* Encadenamiento dinámico
  + El encaminador actualiza sus tablas de ruta gracias a protocolos específicos
    - Rip
    - Ospf
    - BDG

El protocolo IP permite comunicar dos máquinas, pero si dos o más aplicaciones requieren comunicación entre esas dos máquinas, el protocolo IP no permite diferenciar de que aplicación son los datagramas

El nivel de transporte provee elementos para diferenciar y gestionar múltiples orígenes y destinos en una comunicación, y múltiples comunicaciones en cada equipo de forma simultanea

Puertos de comunicaciones

Los protocolos del nivel de transporte implementan el concepto de puerto de comunicaciones que permite identificar los procesos del nivel de aplicación entre lo que se establece la comunicación

Cada proceso del nivel de aplicación tiene asociado uno o varios puertos a través de los cuales es accesible

Los puertos se identifican con un numero de 16 bits (0-65535)

* Puertos conocidos (0-1023) se conocen como well known ports, que están reservados para aplicaciones y servicios estándar (http, ftp…)
* Puertos registrados (1024-49151): para aplicaciones no estándar instaladas por el usuario que no tienen un puerto well known preasignado. Estos puertos pueden asignarse dinámicamente a clientes, si ningún servicio está haciendo uso de ellos
* Puertos dinámicos (49152-65535): habitualmente se emplean para iniciar conexiones desde el cliente. No suelen emplearse en procesos servidores.

La correspondencia entre procesos y puertos se hace de dos formas distintas

* Asignación estática
  + Los puertos conocidos están reservados para aplicaciones estándar y solo pueden ser empleados por estos procesos. Algunas aplicaciones se configuran para arrancar sobre algún puerto no conocido. Pero si la aplicación esta apagada no hay reserva de puerto
* Asignación dinámica
  + Cuando un proceso necesita un puerto y este no se asigna estáticamente, el sistema operativo le asigna uno que esté disponible

En el nivel de transporte tenemos dos protocolos (TCP y UDP). Ambos manejan sus 64K puertos de forma independiente. Por ejemplo, el puerto 80 de UDP es distinto al puerto 80 de TCP

Protocolo UDP

El protocolo UDP (user Datagram Protocol) proporciona un servicio no orientado a la conexión

* No se establece la conexión previa a la transmisión
* No hay control de flujo: pueden enviarse segmentos duplicados o desordenados

Se emplea en casos donde es más importante la velocidad de la transmisión que la fiabilidad, o bien en aplicaciones sencillas del tipo de petición respuesta como DHCP, DNS, streaming y voz IP.

Protocolo TCP

El protocolo TCP proporciona un servicio orientado a la conexión

* Hay establecimiento previo de la conexión
* Hay control de flujo y de errores
* Es un servicio fiable

Establecimiento de la conexión: una vez que se ha establecido la conexión, cualquiera de los dos extremos puede empezar a transmitir. Cualquiera puede terminar la conexión

Una conexión TCP se define por:

* Dirección IP origen, puerto Origen
* Dirección IP destino, Puerto Destino

No puede haber dos conexiones TCP que tengan en común estos 4 datos

Traducción de direcciones de red: NAT Y PAT

El número de dispositivos conectados a internet crece exponencialmente

El número de direcciones IP tiende a agotarse

Por el agotamiento de direcciones IPv4 se está usando IPv6 y poder aprovechar más eficientemente el espacio de direcciones

* CIDR
* Supernetting
* Traducciones de direcciones de red – NAT

NAT: network address translation

Permite que direcciones IP privadas puedan acceder a internet a través de una dirección IP publica

El router reescribe algunos datos del datagrama que encamina. En función de lo que modifique:

* Nat básico: únicamente se modifica la dirección IP
* NAPT (network address por translación) / PAT (port address translation): Se modifica la IP, y los puertos empleados en la comunicación

Actualmente lo que se usa es NAPT, y lo podemos ver escrito tanto como NAPT como NAT (utilizaremos este término)

NAT: modificación de datagramas

Se modifican las IP y los puertos al pasar el datagrama por el router:

* Se modifican la IP origen y el puerto de origen en el tráfico saliente por los datos del router
* Se modifican la IP de destino y el puerto de destino en el tráfico entrante por los datos de destino

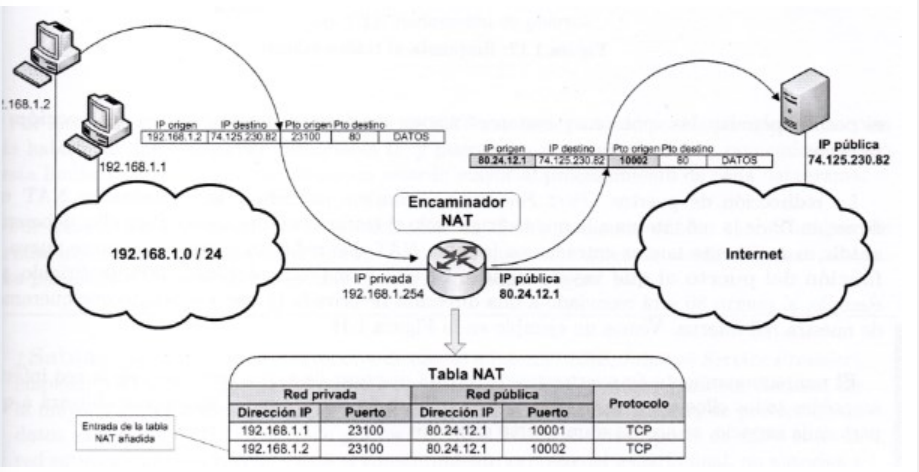
Para ello se mantienen una tabla con la siguiente información:

* Dirección IP interna (privada)
* Puerto interno
* Dirección IP externa (publica)
* Puerto externo
* Protocolo de nivel de transporte (TCP o UDP)

NAT: TRAFICO SALIENTE

Se reemplaza la dirección IP origen y el puerto origen por la dirección IP de salida, y por un puerto disponible en el router

En la tabla NAT se guarda esta equivalencia



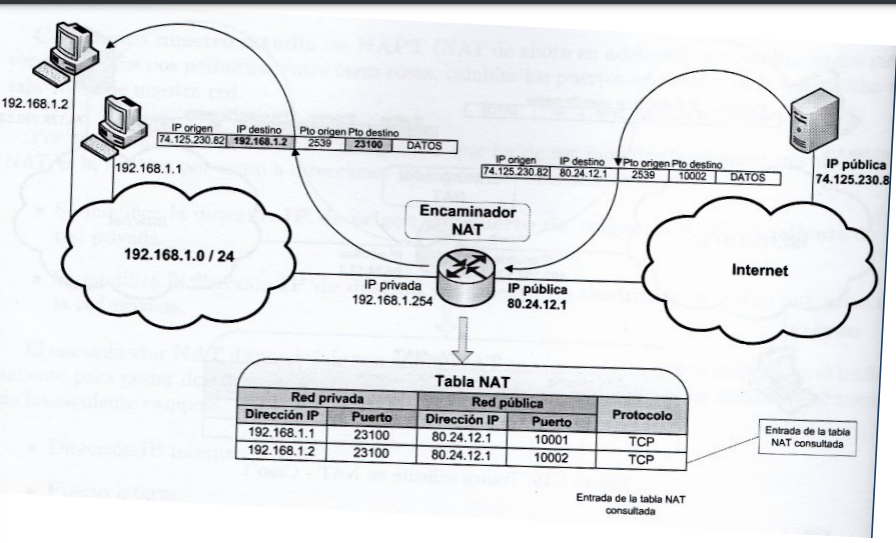
Nat: respuesta al trafico saliente

Cuando el router le llega un datagrama del exterior, comprueba si la dirección IP de destino y el puerto de destino del datagrama entrante coinciden con alguna fila de su tabla NAT en los campos IP externa y Puerto externo

Cuando coinciden, modifica el datagrama, modificando la dirección IP destino y el puerto destino, con los datos de la red interna de esta fila de la tabla NAT

* Redirige el datagrama a esta IP

Si no hay coincidencia, por lo general, descarta el datagrama. Solo si el propio router tiene un servidor escuchando en ese puerto, procesa el datagrama.



NAT: trafico entrante nuevo

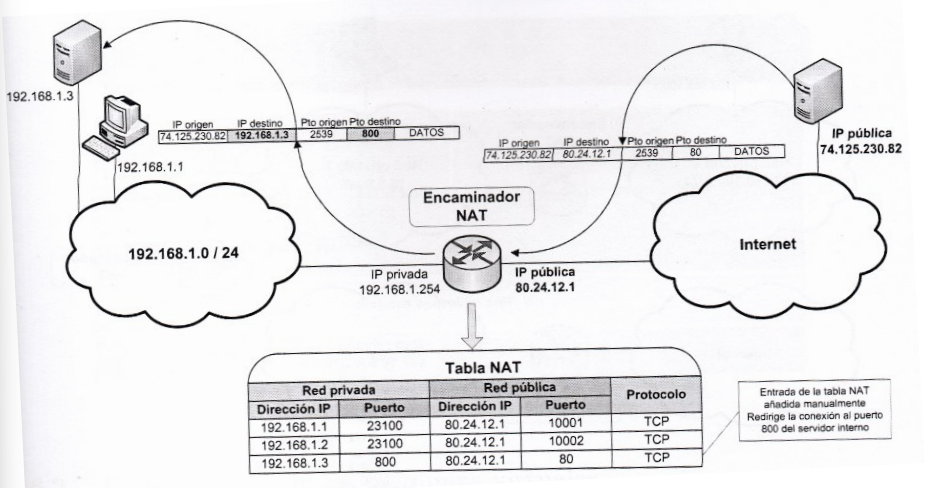
Como los datagramas que no se encuentran equivalencia en la tabla NAT se descartan, en nuestra red interna no podemos tener ningún servidor.

Para solucionar este problema, se permite la redirección de puertos (port forwarding)

Port forwarding: consiste en indicar el router NAT una dirección interna a la que redirigir todo el trafico entrante nuevo. También se puede hacer para solo un puerto concreto

Para ello, hay que añadir manualmente una entrada en la tabla NAT

Esto permite tener varios servidores en la misma IP publica, pero cada uno con un puerto distinto



Nat: limitaciones

Hay protocolos del nivel de aplicación que incluyen las direcciones IP

El encaminador NAT solo actúa sobre las cabeceras IP, por lo que no modifica la parte de datos del datagrama, y, por tanto, no habrá correspondencia entre estas aplicaciones y las direcciones IP que aparecen en las aplicaciones

Las ultimas implementaciones de NAT incorporan conocimiento de los protocolos más habituales de encapsulamiento de direcciones, y modifican también los datos.

DHCP (Dinamic Host Configuration Protocol – protocolo de configuración dinámica de host) es un protocolo de capa de aplicación diseñado para implementar un servicio de configuración automática de red en redes TCP/IP.

La función principal de DHCP es permitir a los equipos de una red obtener sus parámetros de configuración automáticamente, evitando tener que configurar manualmente los parámetros TCP/IP en cada equipo

1985 BOOTP >> 1993 DHCP >> 2006 DHCPv6

Componentes DHCP

DHCP esta basado en el modelo cliente/servidor, y esta formado por los siguientes componentes:

* Servidor DHCP: Dispositivo de red que se encarga de hacer la gestión, entrega y supervisión de las direcciones IP de la red.
* Cliente DHCP: dispositivos de red que se realizan peticiones al servidor DHCP y configuran los parámetros TCP/IP con las opciones que recibe del servidor DHCP
* Protocolo DHCP: conjunto de normas y reglas en base a las cuales “dialogan” los clientes y los servidores DHCP. Dentro del protocolo se establecen
  + Ámbitos de comunicación
  + Opciones
* Agentes de retransmisión DHCP (DHCP relay): Escuchan peticiones de clientes DHCP y las retransmiten a servidores DHCP ubicados en otras redes. Se utilizan para centralizar la configuración del servicio DHCP en múltiples redes

Los servidores DHCP permiten asignar la configuración de red al resto de máquinas presentes en la red cuando estos arrancan o inician sus interfaces de red. Para ello, escuchan las peticiones a través del puerto 67/UDP.

Permiten configurar de forma automática parámetros como:

* Dirección IP
* Mascara de subred
* Puerta de enlace
* Servidores DNS
* Nombre DNS

Los parámetros se pueden configurar a nivel de servidor DHCP, a nivel de ámbito o a nivel de una reserva

Clientes DHCP

Realizan peticiones al servidor DHCP y configuran sus parametros TCP/IP con las opciones que recibe del servidor DHCP

Utilizan el puerto 68/UDP

Estos clientes están integrados en los sistemas operativos

Protocolo DHCP

Determina el conjunto de normas y reglas en base a las cuales dialogan los clientes y servidores DHCP

Proviene del protocolo BOOTP, y por tanto, su mensaje, también proviene del mensaje BOOTP

El formato de mensaje DHCP tiene una parte fija que parece en todos los mensajes aunque se utilicen los campos, y una parte variable (options), donde van las opciones específicas de DHCP

Comunicación por UDP (user Datagram protocol) en los puertos 67 y 68 a toda la red (broadcasting)

Cuando un servidor DHCP lo recibe se establece una comunicación DORA

* Discovery (Descubrimiento)
* Offer (Oferta)
* Request (petición)
* Acknowledge (Aceptación)

FUNCIONAMIENTO DHCP

1. Cuando un cliente DHCP se conecta a la red envía una solicitud en forma de broadcast a través de la red. (OJO ESTO SOLO LO PUEDE HACER A SU RED, NO PODRIA HACERLO A OTRA SUBRED)
2. Todos los servidores alcanzados por la solicitud responden al cliente con sus respectivas propuestas
3. El cliente acepta una de ellas haciéndolo saber al equipo elegido
4. El servidor le otorga la información requerida. En este mensaje le otorga un plazo de concesión
5. Esta informacion se mantiene asociada al cliente mientras este no desactive su interfaz de red o no expire el plazo del contrato o concesión
6. Renovaciones
   1. Cada vez que el cliente arranca, cada cierto tiempo o cuando se alcanza el limite de la concesión, el cliente tiene que solicitar su renovación
   2. Una vez vencido el plazo del contrato, el servidor puede renovar la información del cliente (ampliar el plazo) o asignarle una nueva

Funcionamiento

El cliente manda un mensaje DHCPdiscover a la red, los servidores están escuchando y mandan un mensaje DHCPOFFER, el cliente acepta el primer mensaje que recibe y manda con un DHCPREQUEST al servidor que ha elegido esa IP, luego el server envia el resto de mensajes como la configuración de red y el tiempo de reserva con un mensaje DHCPPACK

Si el server escucha un mensaje DHCPREQUEST con otra dirección, considera que su oferta ha sido rechazada

Si la dirección IP aun esta disponible se mandara un DHCPPACK

Si no esta disponible mandara un DHCPNAK

Si el cliente recibe un DHCPPACK puede usar la dirección, verifica primero que la dirección ip es valida y no esta duplicada

Si no esta duplicada el cliente inicializa con los datos suministrados, y si encuentra un problema envia un DHCPDECLINE al server

Si recibe un HCPNAK libera la dirección

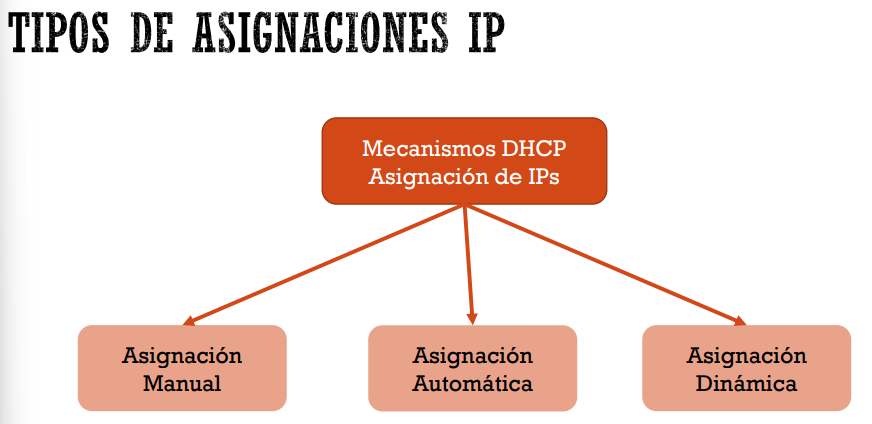
Los clientes al iniciar se aseguran de que pueden usar la dirección IP que tenían anteriormente y si no es así solicita otra

Para renovar la concesión el cliente difunde un DHCPREQUEST con la opción Requested IP address, y la dirección previamente asignada

El servidor devuelve un DHCPPACK o DPCHPNAK

Para liberar una concesión el cliente puede devolver la dirección ip al servidor DHCP que se la concedió antes de que finalice el plazo de concesión, mediante DHCPRELEASE

El cliente manda su dirección IP en el mensaje DHCPRELEASE y no espera respuesta para dejar de utilizar su IP



Asignación estática o manual (reservas): asignar direcciones IP concretas a maquinas concretas a cada dirección física (MAC) le corresponde una dirección IP preasignada “manualmente” por el administrador

Asignación dinámica: el servidor DHCP elige una dirección de un grupo de direcciones disponibles definidas por el administrador (rango/ámbito). Se realiza una concesión de la dirección IP al cliente durante un plazo limitado (lease time)

Asignación automática: asigna direcciones IP de forma permanente a maquinas clientes la primera vez que hacen la solicitud al servidor DHCP y hasta que el cliente las libera. La diferencia con la asignación dinámica radica en que en la asignación automática el plazo de concesión es ilimitado. Hay que usar este tipo con precaución, por que, si un equipo con una asignación sin caducidad es eliminado y no se notifica al servidor DHCP, su dirección IP no se puede reutilizar

Por norma general se utiliza asignación estática para unos pocos equipos conocidos, y dinámica para los demás. Recordad que DHCP no tiene ningún mecanismo de seguridad y asigna IP a todo equipo conectado a la red

Ámbito:

Agrupamiento administrativo de equipos o clientes de una red que utilizan el servicio DHCP. Dentro del ámbito se reserva un rango de direcciones IP para otorgar a los clientes de dicho ámbito

Habitualmente el administrador de red creara un ámbito para cada subred, y definirá un rango de direcciones IP para otorgar

Rango:

Intervalo consecutivo de direcciones IP validas y disponibles para ser concedidas o asignadas a equipos clientes DHCP de una red determinada.

Un servidor DHCP puede configurar tantos ámbitos/rangos como sea necesario para el entorno de red.

Exclusiones:

Un conjunto de direcciones pueden ser excluidas de un rango para no asignarlas a clientes DHCP.

Normalmente se excluyen del rango las direcciones IP que corresponden a equipos que necesitan una dirección IP fija, como servidores, routers o firewalls, y que se configuran manualmente

Reservas:

Asignación de una dirección IP fija a un equipo. Se utiliza para asignar a los servidores y a ciertos equipos la misma dirección siempre. Es algo similar a configurar manualmente una dirección IP estática, pero de forma automática desde el servidor DHCP. Se suelen utilizar ambas cosas (ip fija y reserva) de forma simultanea

Tiempo de concesión

El plazo de contrato o concesión es el tiempo en que un cliente DHCP mantiene como propios los datos de configuración que le otorgo

Cada vez que el cliente arranca , cada cierto tiempo o cuando alcanza el límite de la conexión el cliente solicita una renovación

Una vez vencido el plazo del contrato, el servidor pude asignarle otra nueva concesión o extender el plazo manteniendo la misma información

Esta característica facilita la reestructuración de una red de forma transparente al usuario

Si en una red tenemos un gran numero de direcciones IP y pocos equipos el tiempo de concesion es alto para reducir el trafico de red, pero si hay pocas IP y muchos equipos que cambian de red frecuentemente el tiempo de concesión es bajo

DHCP RELAY

Los clientes DHCP utilizan broadcast para obtener la concesión de una IP en un servidor DHCP

Los routers normalmente no pasan broadcast excepto que estén configurados específicamente para dejarlos pasar

Por lo tanto sin configuración adicional, los servidores DHCP solo proveen direcciones IP a clientes en su red local

Para que podamos asignar direcciones a clientes en otros segmentos, debemos configurar la red para que los DHCP broadcast puedan llegar desde el cliente al servidor DHCP

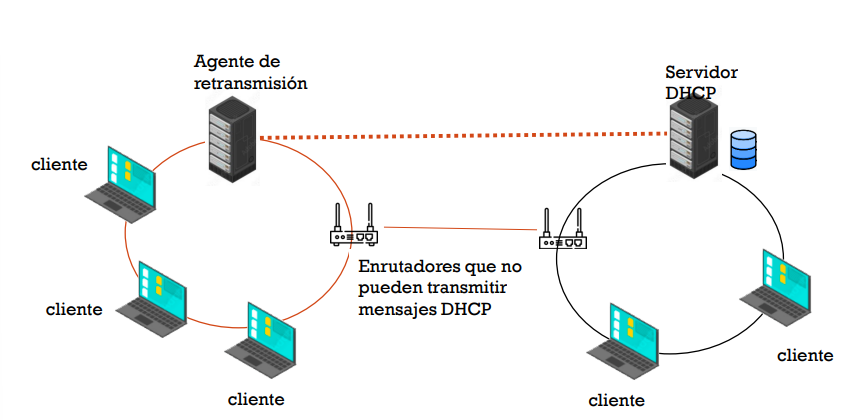
En entornos mas complejos. Por ejemplo, una red de una empresa en 15 oficinas en distintas ciudades

Deberíamos tener en cada red un servidor DHCP, lo cual trae mucho trabajo de administración. Solución: DHCP Relay

DHCP Relay permite la unificación del servicio DHCP para múltiples redes



Un agente de retransmisión DHCP (DHCP Relay) es un servidor o router configurado para escuchar difusiones DHCP procedentes de clientes DHCP y, a continuación, retransmitir dichos mensajes a servidores DHCP ubicados en distintas redes.



Funcionamiento

El cliente envia un paquete broadcast DHCPDISCOVER (como anteriormente para localizar un server DHCP en el segmento de red)

El agente de retransmisión toma la petición y reenvía esta petición al server DHCP

El servidor envia el DHCPOFFER al agente de retransmisión DHCP

El agente envia el broadcast DHCPOFFER

El cliente 1 envía el broadcast DHCPREQUEST (al ver que existe un dhcp pide una dirección)

El agente reenvía esta petición al servidor DHCP

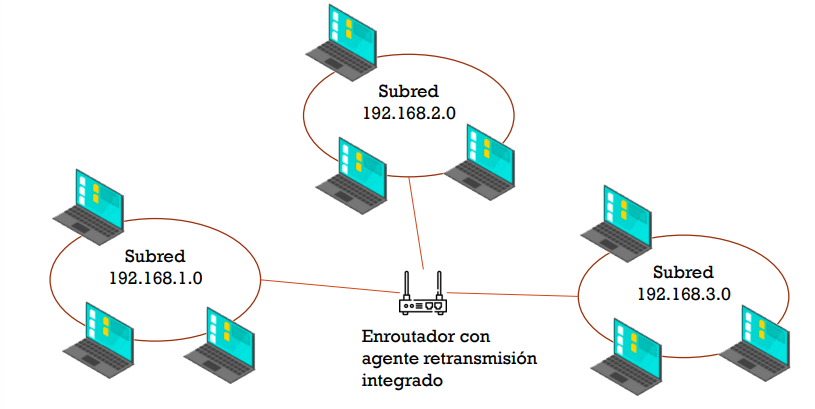
El servidor envía DHCPPACK al agente (que son las siglas de DHCP + ACK estas ultimas de aceptación)

El agente envía el broadcast DHCPPACK

* cada subred a la que sea necesario dar servicio DHCP necesitará un servidor que funcione como agente de retransmisión

otra opción es utilizar routers que tengan integrado un agente de retransmisión DHCP

estos routers tendrán que ser adecuadamente configurados para que retransmitan los paquetes DHCP entre el cliente y el servidor



Cuando dos servidores DHCP trabajan en la misma red, ambos mantienen una base de datos con sus concesiones y el estado de las mismas para evitar que una dirección IP sea asignada por varios servidores, o bien cada una maneja un subconjunto de direcciones, o bien deben sincronizar sus bases de datos de concesiones

El protocolo DHCP failover protocol permite la comunicación entre servidores DHCP

Utilizar múltiples servidores DHCP aumenta la tolerancia a fallos y mejora la disponibilidad

Este protocolo también se puede utilizar para un balanceo de carga

Cuando un equipo solicita su configuración IP, por defecto, el servicio primario le responderá

Solo en el caso de que el servidor primario falle será cuando el servidor secundario proporcione la configuración del cliente

En esta configuración, el servidor secundario no otorga concesiones y solo recibe actualizaciones del servidor primario

En el momento que detecta que no puede comunicarse con el servidor primario será cuando se active como servidor DHCP

