Internet Protocol

Cabecera IP

TCP/IP usa la ordenación de bytes "big endian" (de izquierda a derecha) Si un equipo usa el formato "little endian" debe hacerse la conversión al transmitir y al recibir. **Versión** Versión actual de IP **Longitud de cabecera**: número de palabras de 32 bits de la cabecera, incluidas las opciones si las hubiera <= 60 bytes. **Tipo de servicio**: diseñado para Quality of Service, QoS, aunque nunca fue ampliamente usado. **Servicios diferenciados** (DS): campo de 6 bits utilizado para dar soporte a QoS mediante la técnica de DS. **Explicit Congestion Notification**, ECN: indicador de congestión o futura congestión en un router (2 bits). **Longitud total**: longitud total de datagrama IP en bytes. Longitud total - cabecera = tamaño datos. Campo de 16 bits: máximo tamaño de 65535 bytes. Se precisa este campo porque algunos protocolos del nivel inferior pueden no conocer de manera precisa el tamaño del datagrama encapsulado. **Identificación**: identifica unívocamente el datagrama IP enviado por una máquina. Normalmente se incrementa en una unidad cada vez que se envía un datagrama. **Flags y offset de fragmentación**: campos para fragmentación. **Time To Live, TTL**: establece un tiempo máximo de vida para el datagrama. Previene bucles indefinidos por problemas de enrutamiento. Establece un límite en el número de routers por los que puede pasar un datagrama. Cada vez que el datagrama pasa por un router, se decrementa en una unidad el valor de este campo. Cuando vale 0 se descarta el datagrama y se notifica al remitente con un mensaje ICMP. **Protocolo**: usado por IP para demultiplexar. Permite identificar de qué protocolo de la capa de transporte son los datos enviados. **Checksum de cabecera**: sólo para la cabecera. **Dirección IP de origen y destino**: 32 bits cada una. **Opciones**: información opcional de longitud variable. Algunas opciones son: Registro de enrutamiento, cada router marca su hora y dirección IP, máximo de 9 routers. Timestamp, se registra la ruta y además pone una marca de tiempo en cada salto, máximo de 4 routers. Lista estricta de enrutamientos: la cabecera contiene la ruta paso a paso que debe seguir el datagrama, máximo 9 routers. Lista difusa de enrutamientos: la cabecera lleva una lista de routers por los que debe pasar el datagrama, pero puede pasar además por otros (máximo 9). NoOp: la longitud ha de ser múltiplo de 32 bits. Esta opción permite añadir bytes de relleno para cumplir esta condición.

Subredes

Una subred consiste en dividir una red en partes más pequeñas.

- Nivel jerárquico intermedio entre red y host.
- Utiliza unos bits de la parte del identificador de host para la subred.
- Organización jerárquica de la red, visión externa como una sola red, aunque internamente esté dividida en subredes.

Máscara de subred

Indica cuantos bits forman parte del identificador de red y subred, y cuantos forman el identificador host. Se ponen a 1 todos los bits correspondientes al identificador de red o subred. Se ponen a 0 todos los bits correspondientes al identificador de host. Cada máquina almacena su dirección IP y su máscara de subred.

Direcciones de subred

En cada subred hay dos **direcciones reservadas**, la dirección de subred y la de broadcast en la subred. **Dirección de subred**: identifica la subred, se calcula para cada subred poniendo a 0 el identificador de host; coincide con la primera IP del rando; es quivalente a realizar una operación AND entre la dirección IP y la máscara de subred. **Dirección de broadcast en la subred**: Se calcula poniendo todo a 1 el identificador de host. Coincide con la última IP del rango. Representa a todas las máquinas de la subred.

Máscaras de subred de tamaño variable

Fixed Lenght Subnet Masks (FLSM): todas las subredes usan la misma máscara, lo cual desprecia direcciones IP. Variable Lenght Subnet Masks (VLSM): cada subred usa la máscara óptima para su número de hosts.

- Ordenar las subredes de mayor a menor nº de hosts.
- Calcular la máscara para cada subred usando FLSM

DHCP

Dynamic Host Configuration Protocol: permite asignar direcciones IP dinámicas automáticamente a los hosts (**plug-and-play**):

- Las direcciones IP se asginan durante un tiempo limitado, después es necesario renovarlas.
- También incluye otros parámetros como máscaras de subred , router por defecto y servidores DNS. Se basa en el modelo cliente-servidor.
- Cliente DHCP: cualquier máquina "nueva" en la red que se esté iniciando y necesite una configuración de red.
- Servidor DHCP: granatiza que todas las direcciones IP son únicas durante su tiempo de vida. Métodos de asignación de direcciones
- **Estática** o **manual**: se asigna una dirección IP a una máquina concreta, en base a su dirección MAC. Evita que se conectien clientes no identificados.
- **Dinámica**: se utiliza un rango de direcciones IP y cada ordenador de la red está configurado para solicitar su dirección IP al iniciarse la interfaz. Permite la reutilización de las direcciones IP y facilita la instalación de nuevas máquinas en la red.
- **Automática**: similar al modo dinámico, pero un equipo siempre obtiene la misma IP.

DHCP: Funcionamiento

Modelo cliente-servidor basado en UDP: puerto 67 para el servidor y 68 para el cliente. Mensajes DHCP: el cliente incluye un identifcador de transacción en el mensaje de descubrimiento, que deberá ser repetido en los siguientes.

- **Discovery**: mensaje difundido en la red por el cliente para descubrir el/los servidores DHCP.
- **Offer**: mensaje que contiene la dirección IO que el servidor ofrece al cliente DHCP. Incluye la dirección MAC del cliente, la IP ofertada, la máscara, el tiempo de validez y la dirección IP que el servidor ofrece al cliente DHCP.
- **Request**: el cliente seleccionará una dirección de las ofertadas. En caso de existir varios servidores, se indica el servidor del que se acepta la oferta.
- **Acknowledgement**: el servidor confirma la solicitud del cliente y le indica cualquier otra información solicitada por el cliente. El cliente no tiene dirección IP y no conoce al servidor DHCP. Los mensajes DHCP tienen como destino la dirección de **broadcast** 255.255.255.255.

NAT: Direcciones privadas

Cuando contratamos una banda ancha, mi ISP me proporciona **una dirección IP**, pero ¿y si quiero conectar más de un dispositivo a internet? Direcciones IP públicas: identifican un dispositivo en Internet. **Direcciones IP privadas**: exclusivamente para uso interno.

- Los dispositivos de la red privada se pueden comunicar entre si con esas direcciones.
- Pero no se pueden comunicar con el exterior, Internet. Solución: NAT. Rangos de direcciones IP privadas:
- Clase A: 10.0.0.0 (1 red)
- Clase B: 172.16.0.0 a 172.31.0.0 (16 redes)
- Clase C: 192.168.0.0 - 192.168.255.0 (256 redes)

NAT

Network Address Translation: consiste en modificar la dirección IP origen y/o destino de un datagrama IP al pasar a través de un router o firewall. Permite a múltiples máquinas en una red privada acceder a Internet usando una única dirección IP pública. Surge debido a dos problemas: escasez de direcciones IP y escalabilidad del enrutamiento. También ofrece seguridad, no se admiten conexiones desde fuera. Tipos de NAT:

- **Port Addresss Translation, PAT**, o **Network Address Port Translation, NAPT**, múltiples máquinas comparten una única dirección IP pública, la traducción se realiza mapeando números de puerto.
- **Basic NAT**: solo se realiza el mapeo de direcciones IP. Cada dirección IP privada tiene asignada una dirección IP pública.
- **Carrier-grada NAT, CGNAT**: uso de redes privadas a nivel ISP para compartir un pool de IPs públicas por múltiples clientes.

Ventajas

Seguridad: no se permiten conexiones bidireccionales. Una máquina interna debe iniciar la conexión con una máquina de Internet, evita conexiones maliciosas desde el exterior. Solución para la escasez de direcciones IPv4:

- Utilizar direcciones IP públicas sólo para máquinas que requieran conexión bidireccional a Internet.
- Direcciones privadas para las máquinas que sólo se conectan a Internet.

Inconvenientes

No existe una conectividad extremo a extremo real.

- Se usan los números de puerto para direccionar hosts, no procesos.
- Los routers sólo deberían implementar hasta el nivel de red. Es un parche para la escasez de direcciones, cuando IPv6 soluciona el problema de raíz. Plantea problemas en las aplicaciones que requieren que se inicien conexiones desde el exterior. Problema de **NAT traversal**.