Protocolo IP

Transcribed on July 12, 2025 at 4:11 PM by Minutes AI

Speaker 1 (00:04)

Hola a todos y bienvenidos a esta sesión donde vamos a estar hablando del Protocolo Ip.

En esta clase veremos con más detalle qué es el protocolo ip, cómo es el formato de un datagrama Ip, cómo es el direccionamiento ip dentro de una red y también cómo es el enrutamiento ip en Internet.

Veremos qué son las tablas de enrutamiento y las técnicas de routing que existen.

¿Y qué es el protocolo Ip?

Pues tenemos el RFc 791 que lo que nos dice es que el propósito de este protocolo de Internet ip es mover datagramas a lo largo de un conjunto interconectado de redes.

Por tanto, podemos ver que el protocolo ip lo que nos permite es mover datagramas a lo largo de diferentes redes que están interconectadas entre sí.

Y a diferencia del protocolo Ethernet, en el protocolo Ip no nos centramos únicamente en el segmento de red al que pertenecemos, sino que lo que nos permite es conectar diferentes segmentos de red.

En esta clase nos vamos a centrar principalmente en la versión cuatro de este protocolo, por lo que las direcciones y el enrutamiento que veamos será explícitamente para esta versión.

Algunas características de este protocolo son que no es orientado a conexión y ya no es confiable.

Que no sea orientado a conexión significa que los paquetes se enrutan a su destino como entidades individuales sin un acuerdo previo, es decir, no hay una conexión inicial entre origen y destino.

Y que no sea confiable lo que significa es que ni nos asegura la entrega del paquete ni tampoco nos asegura el orden de llegada.

La red por diseño es insegura, los paquetes se pierden, no llegan a su destino o se quedan dando vueltas por la red.

Para asegurar la confiabilidad de los paquetes veremos como capas superiores, como por ejemplo la capa de transporte con el protocolo TCP, se añade una serie de reglas para garantizar la entrega y el orden de llegada.

Vamos ahora a hablar del formato del datagrama IP.

Como podéis ver por aquí tenemos diferentes campos y comenzamos por el primero que nos imagina la versión del protocolo IP que vamos a utilizar, un cuatro, pues indicamos que vamos a utilizar IPV 1 seis IPV.

Luego tenemos el campo IHL o Internet Header de cuatro bits y que lo que nos indica es la longitud de la cabecera.

Luego tenemos el tipo de servicio o Type of service, que lo que nos permite es priorizar el tráfico ante la congestión o diferencias de servicios.

Se llama también calidad de servicio.

Después, con una longitud de 16 bits tenemos el campo de Total Length que nos indica la longitud Total del paquete incluyendo la cabecera.

El máximo tamaño de un paquete ip es 65536.

Luego tenemos el número de identificación del datagrama, que es que cuando se fragmenta un paquete pues todos los fragmentos del mismo datagrama origen pues tendrán un valor igual en este campo.

Luego tenemos la parte de flags y tenemos dos opciones, el flag df y el flagmf.

El flag df nos dice don'tfragment, es un bit que lo que hace es pedir a los routers que no fragmentan este paquete.

Y luego tenemos el flagmf o more fragments que lo que nos indica es que este fragmento no es el último, si fuese el último el bit estaría a cero, si no es el último el bit está a un.

En el caso de paquetes que no son fragmentables porque no están fragmentados, este bit está siempre a.

Luego tenemos el fragment set que lo que nos indica es la posición del fragmento en el datagrama original, es decir, se ha fragmentado por ejemplo en cuatro, pues aquí tendremos un cuatro.

Si este es el último, deciros que tanto el primer fragmento cuando se rompe y se trocea un datagrama IP como un datagrama que nos ha troceado en este campo va a tener siempre un valor cero.

Luego tenemos el apartado de tiempo de vida o TTL, que es el máximo tiempo porque el paquete puede estar vivo en la red.

En cada salto que da este paquete entre un router y otro o entre un host 1 router, lo que pasa es que en cada salto se resta un un a este contador.

Cuando alcanza el valor cero pues el paquete se descarta y no se sigue reenviando.

Luego tenemos un campo para el protocolo que lo que hace es describir la carga útil del paquete.

Por ejemplo en icmp tenemos el código un, en tcp el código seis, en ip el código cuatro y es la llana quien indica estos códigos.

El header testum por su parte lo que hace es calcular los datos de la cabecera para detectar errores y se recalcula por supuesto cada vez que cambia el ttl porque si no cuando fuera a calcularse en destino este campo no coincidiría.

Luego tenemos la ip origen y destino respectivamente, un campo de opciones que no se suele utilizar y es más, algunos routers pueden considerar peligrosos los paquetes que contienen algunas opciones e incluso bloquearlos.

Y por último los datos que nos llegan de la capa anterior o que queremos enviar pues van en este último apartado.

En cuanto al direccionamiento ip, la dirección ip es un número de 32 bits que identifica a un host dentro de una red.

Un host puede tener varias interfaces de red y por tanto varias direcciones, una por cada interfaz.

Al igual que pasaba con la dirección Mac.

La ip se puede dividir en dos netid y hostid.

El netid lo que identifica en la red, en este caso la uno nueve dos cero 168 tres cero 24 y el host id lo que hace es identificar al host dentro de la red.

Tenemos una red 24, que el 24 es la máscara de red y esto nos indica que tenemos desde la uno nueve 2.168 .30 hasta la uno nueve 2.1683.

.255.

Tanto la primera como la última dirección de red no se utilizan, por tanto tenemos 254 posibles host en esta red.

¿Por qué no se utiliza ni la primera dirección ni la última?

La primera dirección es la dirección de la red, significa que nos permite identificar a la red y por tanto no puede identificar ownhost.

Y la última dirección es la dirección broadcast, que si enviamos algo a esta dirección pues enviará a toda la red.

Fijaros que estábamos comentando sobre direcciones de red, direcciones broadcast, pues es justo lo que vamos a hablar en esta diapositiva, direcciones especiales y direcciones o direccionamiento privado.

Fijaros que el lo que nos permite es en este host vamos a escuchar en cualquier interfaz, cuando por ejemplo levantamos un servidor y lo levantamos en esta dirección ip, lo levantamos para que escuche en todas las interfaces de red.

Después si nos queremos dirigir a todos los juegos, vamos a poner la ip 255 millones 255255255.

Luego tenemos direcciones de red como la que comentábamos uno nueve 2.16.

También tenemos todos los hosts de una red.

Si nos queremos dirigir a todos los hosts de una red, por ejemplo a uno nueve 2.198, .30 pues ponemos esa dirección terminada en 255.

Si nos queremos dirigir a un juego específico de esta red, por ejemplo, pues ponemos su dirección ip uno nueve 2.168.

.3.

.7.

Y si lo que queremos es ir a localhost, a nuestra propia máquina, es decir, dirigirnos a nuestra máquina, no tenemos por qué saber qué dirección tenemos en esa red, sino que la 127001 es la dirección lootback, la interfaz virtual interna de la máquina.

Luego tenemos otro caso especial que son las direcciones privadas.

El RFC en 1918 nos marca que algunos bloques están reservados para direccionamiento privado y los paquetes con una dirección de destino privado nunca deben salir de la red hacia Internet.

Las direcciones privadas que marca este RFC son las uno 0.0, .0, .08, las uno siete dos puntos y la uno nueve 2.168.

.0.

.0.

Extensión 16 es el direccionamiento que normalmente encontramos dentro de nuestras casas, dentro de nuestra escuela o dentro de las diferentes organizaciones y empresas.

Pasamos a hablar del enrutamiento IP.

Todos los hosts tienen una tabla de enrutamiento que lo que hace es asociar parejas dirección Ip y masterup con un método de entrega y tenemos dos mé la entrega directa o la entrega indirecta.

En la entrega directa el destino es un host vecino y ocurre cuando en la misma red se quieren comunicar dos ordenadores, dos host o cuando es el salto del último router a destino, como podéis ver en la imagen de la derecha.

En el caso de la entrega indirecta, en la tabla de enrutamiento lo que tenemos es la dirección del próximo salto, por ejemplo, si queremos ir hacia Internet, es decir, hacia Google por ejemplo, pues en nuestra tabla de rutas lo que tendremos es que esa dirección ip tenemos que ir a la puerta de enlace del router, es decir, el router ya se encargará de volver a enviarlo a otro router y otro router y otro router hasta llegar al servidor de Google.

Un host sabe si la entrega que va a realizar es directa o indirecta haciendo las siguientes comprobaciones.

¿De qué manera?

Pues lo primero que hace es calcular la dirección de red del destino mediante el uso de la máscara y de la dirección IP del destino que tiene en el paquete.

Después comprueba si es su propia dirección de red, en caso afirmativo la entrega es directa ya que el emisor está en dicha red.

En cualquier otro caso la entrega se trata de una entrega indirecta.

Si la entrega es indirecta lo que tenemos que hacer es un reenvío que consiste en colocar el paquete en camino hacia su destino.

Para ello necesitaremos la tabla de enrutado que hablábamos y con esta tabla encontramos el destino o el camino para el destino final.

En Powershell si ejecutamos root print podemos ver algo como lo siguiente, donde vemos que la primera columna es la dirección de destino, ya sea una red o un host específico y la interfaz por donde tiene que salir.

Fijaros que en la primera fila nos dice que para cualquier dirección IP, la puerta de enlace o el siguiente salto es el router en la uno nueve 2.168.

.3.

.1.

Fijaros también en la última columna que tenemos la métrica.

Esto lo que nos dice es el coste asociado a esa ruta.

Cuanto menor sea el valor de la métrica más preferida será la ruta.

Y para calcular esta métrica Windows lo que utiliza es medir la velocidad de conexión, la distancia, fiabilidad y otras características de la red.

Para terminar comentaros que tenemos dos tipos de el estático y el dinámico.

En el estático tenemos unos administradores de red que lo que hacen es configurar manualmente las rutas en los routers y en los host.

Esto significa que cada vez que haya un cambio en la red afecta a la ruta de los datos, el administrador debe actualizar manualmente esa configuración de enrutamiento en los dispositivos.

Esta acción tiene algunas ventajas pero también muchas desventajas.

La primera ventaja es que es simple de configurar y de entender, pero la desventaja es que en caso de cualquier cambio pues hay que actualizar las tablas y las rutas manualmente.

Por otro lado tenemos el enrutamiento dinámico.

Aquí los routers utilizan ciertos protocolos de enrutamiento para intercambiar información sobre las redes disponibles y seleccionar de esa forma las mejores rutas para enviar los datos.

Existen diferentes técnicas y algoritmos como por ejemplo el OSPF Open Shortage Path First, el EIGRP o Enhance Interior Gateway Routing Protocol y el RIP.

La ventaja del enrutamiento dinámico está automáticamente estas rutas se adaptan a los cambios en la topología de red y lo que hace es reducir la carga administrativa.

Por contra puede generar un mayor tráfico en la red y que requiera de una configuración más compleja.

Debido a esta configuración automática que se hace pues a lo mejor tampoco es la más eficiente.

Y con esto llegamos al final de esta clase donde hemos visto que es el protocolo ip, cómo es el formato de las carteras de los datagrama ip, también hemos visto cómo es el direccionamiento ip y por último hemos visto las tablas de enrutamiento y las diferentes técnicas de enrutamiento que siguen los host y routers para enviar un datagrama ip desde un origen a un destino en otra red.

Sin más me despido y nos vemos en la próxima clase donde hablaremos del.