

## Modulo 8 Resumen.

### 8.1 Características de la capa de red

- La capa de red → Capa 3 proporciona servicios para permitir que los dispositivos finales intercambien datos a través de redes. IPv4 y IPv6 son los protocolos principales. OSPF, ICMP, realiza 4 operaciones básicas: **Direccionamiento de dispositivos finales** → Los host deben configurarse con una IP única. **Encapsulación** → Encapsula la unidad de datos de protocolo (PDU) de la capa de transporte en paquete. Agrega información de encabezado IP. **Enrutamiento** → Proporciona servicios para dirigir los paquetes a un host de destino en otra red. La función de un **router** es seleccionar la mejor ruta y dirigir los paquetes al host destino en un proceso de **enrutamiento**. Un paquete puede cruzar muchos routers antes de llegar al destino. Cada **Salto** en cada router cruza un paquete ante's del host destino. **Desencapsulación**: Cuando el paquete llega a la capa red del host destino, el host verifica el encabezado IP. Si la IP es la misma elimina el encabezado IP. La PDU de capa 4 se transfiere al servicio apropiado en la capa de transporte. La capa de red transporta paquetes de varios tipos sin importar el contenido.  
**Datos → Segmento → Paquete → trama** → Proceso de encapsulación.

- Encapsulación IP → IP encapsula el segmento de la capa de transporte agregando un encabezado IP. Este encabezado se usa para entregar el paquete al host destino.  
**Encapsulamiento de transporte (encabezado del segmento, datos) PDU.**

#### **Encapsulamiento de red (encabezado IP, Datos) Paquete IP**

Encapsulamiento de datos capa por capa permite que se desarrollen y escalen los servicios en las capas. El encabezado IP es examinado por dispositivos de capa 3 en cada salto a través de una red a su destino. La información IP es intacta de origen a destino con excepción al traducirse en las direcciones NAT para IPv4. Cada router implementa los protocolos de enrutamiento para enrutar paquetes entre redes.

- Características de IP → Diseñado con sobrecarga baja. Provee funciones necesarias para enviar un paquete de origen a destino con un sistema interconectado de redes. No diseñado para rastrear ni administrar el flujo de paquetes. **Características:**

**Sin conexión** → No hay conexión con el destino establecida antes de enviar paquetes de datos.

**Mejor esfuerzo** → La IP es inherentemente poco confiable porque no garantiza la entrega de paquetes.

**Medios independientes** → La operación es independiente del medio (cable) que transporta los datos.

- Sin conexión → La IP no tiene conexión, lo que significa que IP no crea una conexión de extremo a extremo dedicada antes de enviar los datos. Funcionan con el mismo

Principio. No requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que se reenvíen los paquetes. **Se envía un paquete**

- Mejor esfuerzo → La IP no necesita campos adicionales en el encabezado para mantener una conexión establecida. Reduce la sobrecarga del protocolo IP. Sin embargo, sin la conexión preestablecida, los remitentes no saben si los destinos están presentes. No garantiza que los paquetes enviados se reciban. Algunos paquetes se pierden en la ruta. Es un protocolo de capa de red no confiable. Otros protocolos se encargan del seguimiento y entrega segura.

- Independiente de los medios → IP no administra o recupera paquetes no recibidos o dañados.

Ya que los paquetes IP tienen información de la ubicación de entrega pero no información para procesar si la entrega fue exitosa, tampoco de retransmitir. Las capas superiores deben solucionar problemas como el envío de paquetes fuera de orden o pérdida de paquetes. Permite que IP funcione de manera eficaz. Los paquetes pueden enviarse mediante cobre, fibra óptica, WLAN, etc.

**Los paquetes IP pueden trasladarse en diferentes medios.** Una característica importante del medio que es el tamaño máximo de PDU que cada medio puede transportar. También conocida como "**Unidad de transmisión máxima**" (MTU). La capa de enlace de datos pasa el valor de MTU a la capa de red. Determina qué tamaño pueden tener los paquetes. En IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña. Se llama **fragmentación de paquetes o fragmentación**. El router no puede fragmentar los paquetes IPv6.

## 8.2 Paquete IPv4

- Encabezado de paquetes IPv4 → El encabezado del paquete IPv4 se utiliza para garantizar que el paquete se entregue en su siguiente parada en el camino a su dispositivo final destino. consta de campos que contienen información importante del paquete. Tienen números binarios que examinan el proceso de capa 3.

- Campos de encabezado de paquete IPv4 → Los campos binarios identifican diversos parámetros de configuración del paquete IP. Los diagramas de encabezado se leen de Izq a derecha y de arriba-abajo. Campos:

**Versión** → Contiene un valor binario de 4 bits establecido en 0100 que identifica como paquete IPv4

**Servicios diferenciados (Ds)** → Definido como tipo de servicio (TOS), es un campo de 8 bits utilizados para determinar la prioridad de cada paquete. Los 6 bits más significativos son **DSCP y dos últimos (ECN)**.

**Suma de Comprobación de encabezado** → Se utiliza para detectar daños en el encabezado IPv4

**Tiempo de duración (Time to Live, TTL)** → Valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. El dispositivo de origen del IPv4 establece el valor TTL inicial.

Se reduce uno cada vez que el paquete es procesado por un router. Si el campo TTL llega a cero, el router descarta el paquete y envía a la dirección IP de origen un mensaje de tiempo superado del protocolo de mensajes de control de Internet. **ICMP**.

**Protocolo** → Este campo identifica el protocolo del siguiente nivel. Valor binario de 8 bits indica el tipo de carga de datos que lleva el paquete, lo que permite que la capa de red transmita datos al protocolo de capa superior. **ICMP(1), TCP(6), UDP(17)** valores comunes.

**Dirección IPv4 de origen** → Valor binario de 32 bits que representa la IPv4 de origen del paquete. La dirección IPv4 siempre es unicast.

**Dirección IPv4 de destino** → Contiene valor binario de 32 bits que representa la IPv4 de destino. Puede ser unicast, multicast o difusión.

Para identificar y validar el paquete, se usan campos de longitud del encabezado de Internet **IHL**, longitud total y encabezado checksum. Para reordenar un paquete fragmentado, se usan otros campos. **Identificación, señaladores y desplazamiento de fragmentos para llevar un control de los fragmentos**.

### ● Video & ejemplos de encabezados IPv4 en wireshark

Un ejemplo sencillo puede ser mostrado es en wireshark.

Internet Protocol version 4, Src: 192.168.1.109 (192.168.1.109), DST: 192.168.1.1

Version 4, Header length: 20 bytes, Total length: 52, Identification: 0x31fc (12796)

### 8.3 Paquete IPv6

● Limitaciones de IPv4 → IPv4 tiene 3 grandes problemas:

**Agtamiento de la dirección IPv4** → IPv4 tiene un número limitado de direcciones públicas únicas disponibles. Aproximadamente 4,000 millones. Su incremento ha sido importante para el número.

**Falta de conectividad extremo-extremo** → La traducción de direcciones de red (NAT) es una tecnología implementada dentro de IPv4. NAT proporciona una manera de varios dispositivos Compartan una única IPv4 pública. IPv4 oculta un host de la red interna. Problemas en conectividad completa.

**Mayor complejidad de la red** → NAT es un tratado para usar el mecanismo de transición a IPv6. NAT Crea una complejidad adicional en la red, creando latencia.

### ● Información general sobre IPv6 → Mejoras que ofrece IPv6 →

**Manejo de paquetes mejorado** → Las direcciones IPv6 se basa en direccionamiento jerárquico de 128 bits y IPv4 en 32 bits.

**Mejor manejo de paquetes** → El encabezado IPv6 se ha simplificado con menos campos.

**Eliminar la necesidad de NAT** → Con una cantidad grande de IPv6 públicas, no se necesita NAT. Solucionando conectividad extremo-extremo.

El espacio entre las direcciones de IPv4 e IPv6 son enormes. IPv4 de 32 bits ofrece 4.294.967.296 direcciones únicas. IPv6 ofrece 340 undeciliones de direcciones. 1 sextillón aproximadamente a cada grano de arena en la tierra.

• Campos de encabezado de paquete IPv4 en el encabezado de paquete IPv6 → En IPv6 algunos campos se han mantenido igual que IPv4 y otros han cambiado de nombre, posición. Campos guardados en IPv4 - IPv6 → Versión, dirección origen, dirección destino.

Cambio de nombre y posición en IPv6 → Tipo de servicio, longitud total, Protocolo, tiempo de duración.

Nuevo campo en IPv6 → IHL, Identificación, señaladores, desplazamiento de fragmentos, suma de comprobaciones del encabezado, opciones, relleno.

El encabezado IPv6 simplificado consiste en un encabezado con longitud fija de 40 octetos.

• Encabezado de paquetes → Version → Contiene un valor binario de 4 bits establecido en 0110 que identifica un paquete IPv6. Clase de tráfico → Campo de 8 bits es equivalente al campo de servicios diferenciados (DS) IPv4. Etiqueta de flujo → Campo de 20 bits sugiere que todos los paquetes con la misma etiqueta de flujo reciben el mismo tipo de manejo por routers. Longitud de carga útil → Campo de 16 bits indica la longitud de porción de datos o carga útil del paquete IPv6. No incluye la longitud del encabezado. Encabezado siguiente → Campo de 8 bits equivalente a Protocolo IPv4. Valor que indica el tipo de contenido de datos que lleva el paquete.

Límite de salto → Campo de 8 bits reemplaza al campo TTL de IPv4. Cada router que reenvía el paquete reduce este valor en 1. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje ICMPv6, indicando que el paquete no llegó a su destino porque se excedió el límite de saltos. Dirección IPv6 de origen → Campo de 128 bits que identifica la dirección IPv6 del host emisor. Dirección IPv6 destino → Campo de 128 bits que identifica la dirección IPv6 del host receptor.

También puede contener EH, encabezados de extensión que proveen información optativa de red. Se usan para fragmentar, dar seguridad, admitir movilidad y otras acciones.

• Ejemplos de encabezados IPv6 en Wireshark

## 8.4 Cómo arma las rutas el host?

- La decisión de reenvío de host → Con IPv4 e IPv6 los paquetes se crean en el host origen. Dirige el paquete al host destino. Los dispositivos finales crean su tabla de enrutamiento. Un host puede enviar un paquete a lo siguiente: **Itself** → IPv4 → 127.0.0.1 or IPv6 ::1, Se conoce como **interfaz de bucle invertido**. Pone a prueba la pila del protocolo TCP/IP en el host.

**Local Host** → Host destino que se encuentra en la misma red local que el host remitidor. Comparten la misma dirección de red. **Host remoto** → Host destino en una red remota. No comparten la misma dirección de red.

El host de origen determina si el paquete es para un host local o remoto. La versión **IPv4** utiliza su propia máscara de subred con su IPv4 y la IPv4 de destino para determinarlo y **IPv6** utiliza el router local anunciando la dirección de red local a todos los dispositivos red. Si un host está enviando un paquete a un dispositivo configurado en la misma red IP el paquete se envía desde la interfaz del host. Utiliza un dispositivo intermedio. Los dispositivos fuera del segmento de red local se denominan "**módulo remoto de E/S**".

- **Puerta de enlace predeterminada (Gateway)** → Es el dispositivo de red (router o switch de capa 3) que puede enrutar el tráfico a otras redes. Puede ser un router con una dirección IP local en el mismo rango de direcciones que otros host en la LAN. Puede aceptar datos en la red local y reenviar datos fuera de la red local. Enruta el tráfico a otras redes.

Se requiere una puerta de enlace predeterminada para enviar tráfico fuera de la red local.

- Un host enruta a la puerta de enlace predeterminada → La tabla de enrutamiento incluye el gateway. En IPv4, el host recibe la dirección IPv4 del gateway, ya sea dinámica con DHCP o manual. En IPv6, el router anuncia la dirección del gateway predeterminado o el host la configura. La configuración de un gateway predeterminado genera una ruta predeterminada en la tabla de enrutamiento de la PC. Una **ruta predeterminada** es la ruta o camino de la PC para conectarse a la red remota.

- **Tablas de enrutamiento de host** → El comando **route print** o **netstat -r** se usa para mostrar la tabla de enrutamiento del host. Muestra 3 secciones con relaciones TCP/IP:

**Lista de interfaces** → Enumera la dirección de control de acceso a medios (MAC) y el número de interfaz asignado de cada interfaz con capacidad de red en el host.

**Tabla de rutas IPv4** → Enumera todas las rutas IPv4 conocidas, conexiones direcadas, LAN y locales pred.

**Tabla de rutas IPv6** → Enumera todas las rutas IPv6 conocidas.

## 8.5 Introducción al enrutamiento

● Descripción de envío de paquetes del router → Cuando un host envía un paquete a otro host, consulta su tabla de enrutamiento para determinar dónde enviar el paquete. Si el host **está en una red remota**, el paquete se envía al gateway. Cuando llega al router, el router examina la IP de destino del paquete y busca en su tabla de enrutamiento para reenviar el paquete. Esta tabla contiene una lista de todas las direcciones de red conocidas (**prefixos**).

El paquete llega a la interfaz g0/0/0, desencapsula el encabezado Ethernet y el remolque. El router examina la IP y destino y busca la mejor coincidencia en su tabla de enrutamiento. Encapsula en encabezado Ethernet y lo reenvía.

● Tabla de enrutamiento IP del router → Contiene entradas de ruta de red que enumeran todos los posibles destinos de red conocidos. Almacena 3 tipos de entrada de rutas:

**Redes conectadas directamente** → Entradas de ruta de red son interfaces de router activas.

Los routers agregan una ruta conectada directamente cuando una interfaz se configura con una IP y se activa. Cada interfaz de router está conectada a un segmento de red diferentes.

**Redes remotas** → Conectadas a otros routers. Los router aprenden de redes remotas y ~~ya sea~~ con configuración explícita o intercambio de ruta mediante enrutamiento dinámico.

**Ruta predeterminada** → Incluyen gateway predeterminado. La ruta predeterminada se utilizan cuando no hay una mejor coincidencia en la tabla de enrutamiento IP.

Un router descubre redes remotas de dos maneras: **Manualmente** → las redes remotas se ingresan manualmente en la tabla de rutas mediante rutas estáticas. **Dinámicamente** → se aprenden por enrutamiento dinámico.

● Enrutamiento estático → Entradas de ruta que se configuran manualmente. Incluye **dirección de red remota y la IP del router de salto siguiente**. El administrador necesita volver a configurar una ruta estática si hay un cambio en la topología y la ruta no es viable. Una ruta estática es apropiada para redes pequeñas, se usa con un protocolo de enrutamiento dinámico para configurar una ruta predeterminada.

● Enrutamiento dinámico → Permite a los routers aprender automáticamente sobre redes remotas, incluidas las predeterminadas. Comparten automáticamente la información de enrutamiento con otros routers y compensan cualquier cambio a la topología. Los protocolos incluyen **OSPF**, **EIGRP**. La configuración básica solo requiere el administrador habilite las redes conectadas directamente dentro del protocolo de enrutamiento dinámico. Detecta redes remotas, mantiene la información actualizada, elige el mejor camino, intenta encontrar una nueva mejor ruta si la actual no está disponible.

## 1 Introducción a una tabla de enrutamiento IPv4 → El comando show ip route

Se usa para ver la tabla de enrutamiento IPv4. Al principio de cada tabla hay un código que se utiliza para identificar el tipo de ruta o como se aprendió. Fuentes comunes: **L** → Dirección IP de link local conectada directamente. **C** → Red conectada directamente. **S** → Ruta estática. **O** → OSPF. **D** → EIGRP.

Una ruta predeterminada tiene una dirección de red de todos los ceros. Una entrada de ruta estática en la tabla de enrutamiento comienza con un código **S\***.