Modulo 8: capa de red

8.0 Introducción

Desplázate para empezar

8.0.1 ¿Por qué debería tomar este módulo?

¡Bienvenido a Capa de red!

Por ahora puede haber notado que los módulos en este curso están progresando de abajo hacia arriba a través de las capas del modelo OSI. En la capa de red del modelo OSI, le presentamos protocolos de comunicación y protocolos de enrutamiento. Supongamos que desea enviar un correo electrónico a un amigo que vive en otra ciudad, o incluso en otro país. Esta persona no está en la misma red que usted. Una simple red conmutada no puede recibir su mensaje más allá del final de su propia red. Necesitas ayuda para mantener este mensaje en movimiento a lo largo del camino hacia el dispositivo final de tu amigo. Para enviar un correo electrónico (un video, un archivo, etc.) a cualquier persona que no esté en su red local, debe tener acceso a routers. Para acceder a los routers, debe usar protocolos de capa de red. Para ayudarle a visualizar estos procesos, este módulo contiene dos actividades Wireshark. ¡Disfrute!

8.0.2 ¿Qué aprenderé en este módulo?

Título del módulo: Capa de red

Objetivos del módulo: Explique cómo los routers utilizan los protocolos y los servicios de capa de red para habilitar la conectividad integral.

Título del tema	Objetivo del tema
Características de la capa de red	Explique cómo la capa de red utiliza los protocolos IP para una confiabilidad de comunicaciones.
Paquete IPv4	Explique la función de los principales campos de encabezado en el paquete IPv4.
Paquete IPv6	Explique la función de los principales campos de encabezado en el paquete IPv6.
Cómo arma las rutas un host	Explique cómo los dispositivos de red usan tablas de enrutamiento para dirigir paquetes a un red de destino.
Tablas de enrutamiento de router	Explique la función de los campos en la tabla de enrutamiento de un router.

8.1 Características de la capa de red

Desplázate para empezar

8.1.1 La capa de red

La capa de red, o Capa OSI 3, proporciona servicios para permitir que los dispositivos finales intercambien datos a través de redes. Como se muestra en la figura, IP versión 4 (IPv4) e IP versión 6 (IPv6) son los principales protocolos de comunicación de la capa de red. Otros protocolos de capa de red incluyen protocolos de enrutamiento como Open Shortest Path First (OSPF) y protocolos de mensajería como Internet Control Message Protocol (ICMP).

Protocolos de capa de red

7654321

- Protocolo de Internet versión 4 (IPv4)
- Protocolo de Internet versión 6 (IPv6)

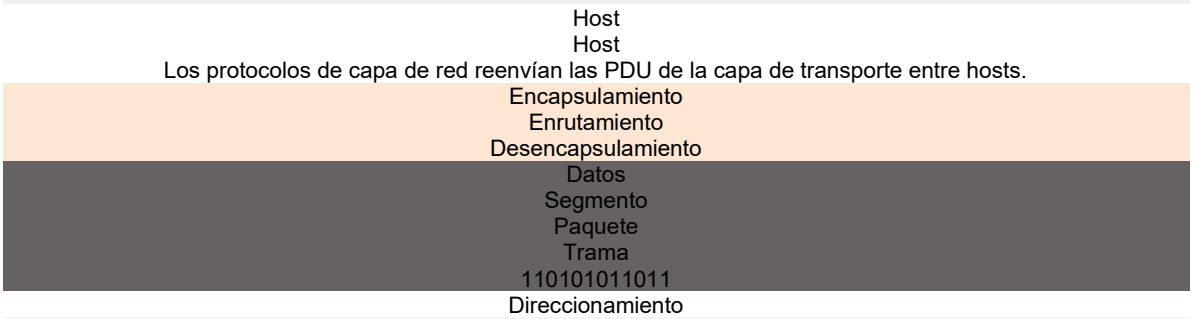
Aplicación
Presentación
Sesión
Transporte
Red
Enlace de datos
Física

Para lograr comunicaciones end-to-end a través de los límites de la red, los protocolos de capa de red realizan cuatro operaciones básicas:

- **Direccionamiento de dispositivos finales :** los dispositivos finales deben configurarse con una dirección IP única para la identificación en la red.
- **Encapsulación:** La capa de red encapsula la unidad de datos de protocolo (PDU) de la capa de transporte en un paquete. El proceso de encapsulamiento agrega información de encabezado IP, como la dirección IP de los hosts de origen (emisores) y de destino (receptores). El proceso de encapsulación lo realiza el origen del paquete IP.
- **Enrutamiento:** La capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para transferir un paquete a otras redes, debe procesarlo un router. La función del router es seleccionar la mejor ruta y dirigir los paquetes al host de destino en un proceso que se denomina "enrutamiento". Un paquete puede cruzar muchos routers antes de llegar al host de destino. Se denomina "salto" a cada router que cruza un paquete antes de alcanzar el host de destino.
- **Desencapsulación:** Cuando el paquete llega a la capa de red del host de destino, el host verifica el encabezado IP del paquete. Si la dirección IP de destino dentro del encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete. Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene se transfiere al servicio apropiado en la capa de transporte. El proceso de desencapsulación lo realiza el host de destino del paquete IP.

A diferencia de la capa de transporte (Capa OSI 4), que gestiona el transporte de datos entre los procesos que se ejecutan en cada host, los protocolos de comunicación de la capa de red (es decir, IPv4 e IPv6) especifican la estructura de paquetes y el procesamiento utilizado para transportar los datos de un host a otro host. La capa de red puede transportar paquetes de varios tipos de comunicación entre varios hosts porque funciona sin tener en cuenta los datos que contiene cada paquete.

Haga clic en Reproducir en la ilustración para ver una animación sobre el intercambio de datos.



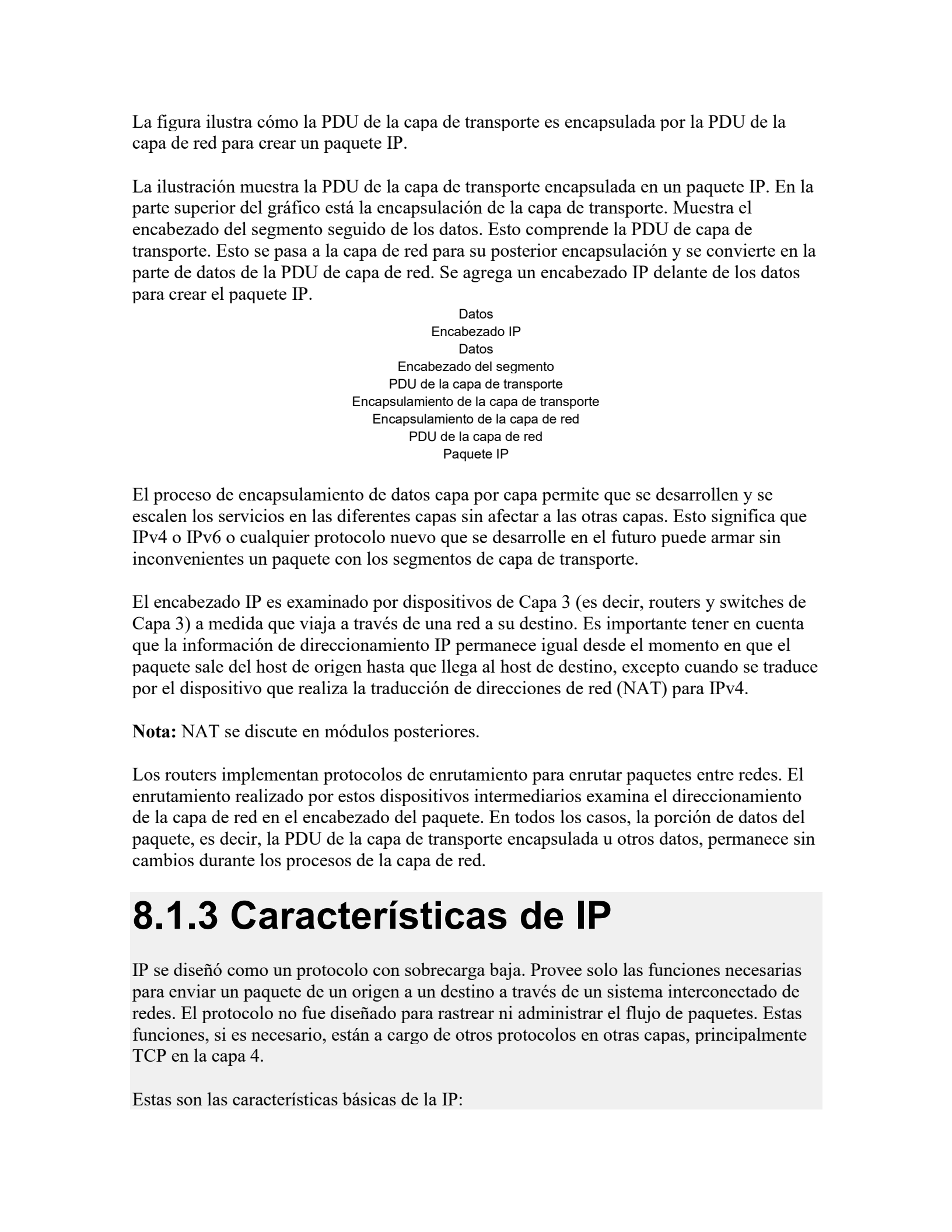
play_circle_filled

8.1.2 Encapsulación IP

IP encapsula el segmento de la capa de transporte (la capa justo por encima de la capa de red) u otros datos agregando un encabezado IP. El encabezado IP se usa para entregar el paquete al host de destino.

La figura ilustra cómo la PDU de la capa de transporte es encapsulada por la PDU de la capa de red para crear un paquete IP.

La ilustración muestra la PDU de la capa de transporte encapsulada en un paquete IP. En la parte superior del gráfico está la encapsulación de la capa de transporte. Muestra el encabezado del segmento seguido de los datos. Esto comprende la PDU de capa de transporte. Esto se pasa a la capa de red para su posterior encapsulación y se convierte en la parte de datos de la PDU de capa de red. Se agrega un encabezado IP delante de los datos para crear el paquete IP.



El proceso de encapsulamiento de datos capa por capa permite que se desarrollen y se escalen los servicios en las diferentes capas sin afectar a las otras capas. Esto significa que IPv4 o IPv6 o cualquier protocolo nuevo que se desarrolle en el futuro puede armar sin inconvenientes un paquete con los segmentos de capa de transporte.

El encabezado IP es examinado por dispositivos de Capa 3 (es decir, routers y switches de Capa 3) a medida que viaja a través de una red a su destino. Es importante tener en cuenta que la información de direccionamiento IP permanece igual desde el momento en que el paquete sale del host de origen hasta que llega al host de destino, excepto cuando se traduce por el dispositivo que realiza la traducción de direcciones de red (NAT) para IPv4.

Nota: NAT se discute en módulos posteriores.

Los routers implementan protocolos de enrutamiento para enrutar paquetes entre redes. El enrutamiento realizado por estos dispositivos intermediarios examina el direccionamiento de la capa de red en el encabezado del paquete. En todos los casos, la porción de datos del paquete, es decir, la PDU de la capa de transporte encapsulada u otros datos, permanece sin cambios durante los procesos de la capa de red.

8.1.3 Características de IP

IP se diseñó como un protocolo con sobrecarga baja. Provee solo las funciones necesarias para enviar un paquete de un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones, si es necesario, están a cargo de otros protocolos en otras capas, principalmente TCP en la capa 4.

Estas son las características básicas de la IP:

- **Sin conexión:** - no hay conexión con el destino establecido antes de enviar paquetes de datos.
- **Mejor esfuerzo:** - la IP es inherentemente poco confiable porque no se garantiza la entrega de paquetes.
- **Medios independientes:** - Medios independientes: la operación es independiente del medio (es decir, cobre, fibra óptica o inalámbrico) que transporta los datos.

8.1.4 Sin conexión

IP no tiene conexión, lo que significa que IP no crea una conexión de extremo a extremo dedicada antes de enviar los datos. La comunicación sin conexión es conceptualmente similar a enviar una carta a alguien sin notificar al destinatario por adelantado. La figura resume este punto clave.

Sin conexión - Analogía

un paquete, que consiste en un encabezado y un segmento IP, se envía desde una red origen con destino a otra red

Se envía una carta.

Carta
Carta
Buzón de correo

Las comunicaciones de datos sin conexión funcionan con el mismo principio. Como se muestra en la figura, IP no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que se reenvíen los paquetes.

Sin conexión: red

Se envía un paquete.

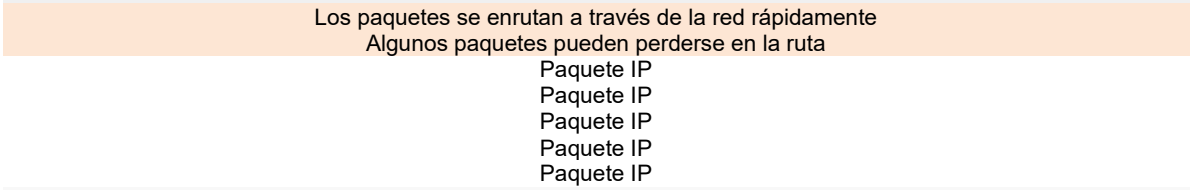
Encabezado IP
segmento
Encabezado IP
segmento

8.1.5 Mejor esfuerzo

La IP tampoco necesita campos adicionales en el encabezado para mantener una conexión establecida. Este proceso reduce en gran medida la sobrecarga del protocolo IP. Sin embargo, sin una conexión completa preestablecida, los remitentes no saben si los dispositivos de destino están presentes y en funcionamiento cuando envían paquetes, ni tampoco si el destinatario recibe el paquete o si puede acceder al paquete y leerlo.

El protocolo IP no garantiza que todos los paquetes que se envían, de hecho, se reciban. En la ilustración, se muestran las características de entrega de mejor esfuerzo o poco confiable del protocolo IP.

El diagrama muestra un origen en una red y un destino en otra red. Entre los dos hosts hay una nube que consta de cuatro routers en una topología de malla. Tres paquetes IP salen del host de origen, pero sólo dos llegan al host de destino. El texto del gráfico dice: Los paquetes se enrutan rápidamente a través de la red; Algunos paquetes pueden perderse en el camino.



Dado que es un protocolo de capa de red no confiable, el protocolo IP no garantiza que se reciban todos los paquetes enviados. Otros protocolos administran el proceso de seguimiento de paquetes y de aseguramiento de entrega.

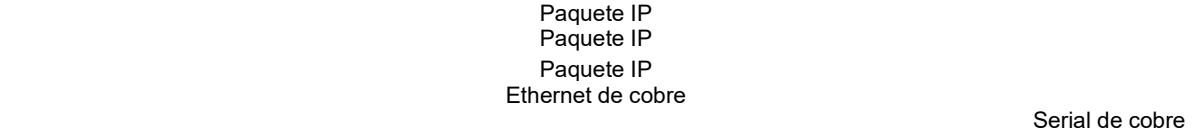
8.1.6 Independiente de los medios

Que sea poco confiable significa que IP no tiene la funcionalidad para administrar o recuperar paquetes no recibidos o dañados. Esto se debe a que, si bien los paquetes IP se envían con información sobre la ubicación de la entrega, no contienen información que pueda procesarse para informar al remitente si la entrega fue exitosa. Es posible que los paquetes lleguen dañados o fuera de secuencia al destino o que no lleguen en absoluto. IP no tiene la funcionalidad de retransmitir paquetes si se producen errores.

Las aplicaciones que utilizan los datos o los servicios de capas superiores deben solucionar problemas como el envío de paquetes fuera de orden o la pérdida de paquetes. Esta característica permite que IP funcione de manera muy eficaz. En el conjunto de protocolos TCP / IP, la confiabilidad es la función del protocolo TCP en la capa de transporte.

IP funciona independientemente de los medios que transportan los datos en las capas más bajas de la pila de protocolos. Como se muestra en la ilustración, los paquetes IP pueden ser señales electrónicas que se transmiten por cables de cobre, señales ópticas que se transmiten por fibra óptica o señales de radio inalámbricas.

El diagrama muestra una topología de red dentro de una nube con un paquete que viaja a través de varios tipos de medios entre dos hosts. Se muestra un paquete IP moviéndose entre un host y un router a través de una conexión Ethernet de cobre. El primer router está conectado al segundo router a través de una conexión en serie de cobre. Se muestra un paquete IP moviéndose entre el segundo router y el tercer router a través de una conexión de fibra óptica. El tercer router está conectado a un cuarto router, que es un router inalámbrico. Se muestra un paquete IP moviéndose entre el cuarto router y un host a través de una conexión inalámbrica.



Fibra óptica
Conexión inalámbrica
Ethernet de cobre

Los paquetes IP pueden trasladarse a través de diferentes medios.

La capa de enlace de datos OSI es responsable de tomar un paquete IP y prepararlo para la transmisión a través del medio de comunicación. Esto significa que la entrega de paquetes IP no se limita a ningún medio en particular.

Sin embargo, la capa de red tiene en cuenta una de las características más importantes del medio, que es el tamaño máximo de PDU que cada medio puede transportar. Esta característica se conoce como "unidad de transmisión máxima" (MTU). Parte del control de la comunicación entre la capa de enlace de datos y la capa de red consiste en establecer el tamaño máximo del paquete. La capa de enlace de datos pasa el valor de MTU a la capa de red. La capa de red luego determina qué tamaño pueden tener los paquetes.

En algunos casos, un dispositivo intermedio, generalmente un router, debe dividir un paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña. Este proceso se denomina “fragmentación de paquetes” o “fragmentación”. La fragmentación provoca latencia. El router no puede fragmentar los paquetes IPv6.

8.2 Paquete IPv4

Desplázate para empezar

8.2.1 Encabezado de paquetes IPv4

IPv4 es uno de los protocolos de comunicación de la capa de red principal. El encabezado del paquete IPv4 se utiliza para garantizar que este paquete se entrega en su siguiente parada en el camino a su dispositivo final de destino.

El encabezado de paquetes IPv4 consta de campos que contienen información importante sobre el paquete. Estos campos tienen números binarios que examinan el proceso de capa 3.

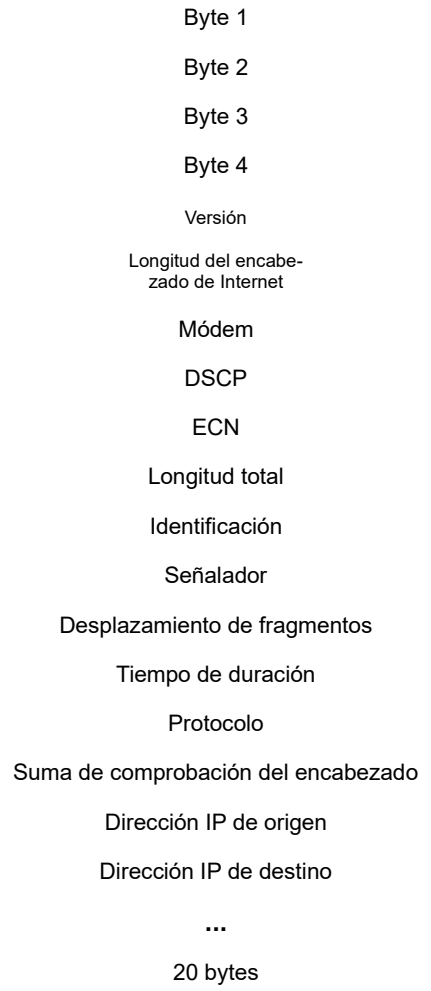
8.2.2 Campos de encabezado de paquete IPv4

Los valores binarios de cada campo identifican diversos parámetros de configuración del paquete IP. Los diagramas de encabezado del protocolo, que se leen de izquierda a derecha y de arriba hacia abajo, proporcionan una representación visual de consulta al analizar los

campos de protocolo. El diagrama de encabezado del protocolo IP en la ilustración identifica los campos de un paquete IPv4.

Campos del encabezado de paquetes IPv4

nombres y longitud de bits de los campos en un encabezado de paquete IPv4



Los campos significativos en el encabezado IPv4 incluyen lo siguiente:

- *Versión - Contiene un valor binario de 4 bits establecido en 0100 que identifica esto como un paquete IPv4.*
- *Servicios diferenciados o DiffServ (DS) - Este campo, formalmente conocido como Tipo de servicio (ToS), es un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete. Los seis bits más significativos del campo DiffServ son los bits de punto de código de servicios diferenciados (DSCP) y los dos últimos bits son los bits de notificación de congestión explícita (ECN).*
- *Suma de comprobación de encabezado - Se utiliza para detectar daños en el encabezado IPv4.*

- *Tiempo de duración (Time to Live,TTL) - TTL contiene un valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. El dispositivo de origen del paquete IPv4 establece el valor TTL inicial. Se reduce en 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). Debido a que el router disminuye el TTL de cada paquete, el router también debe volver a calcular la suma de comprobación del encabezado.*
- *Protocolo - Este campo se utiliza para identificar el protocolo del siguiente nivel. Este 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 los datos al protocolo de la capa superior apropiado. ICMP (1), TCP (6) y UDP (17) son algunos valores comunes.*
- *Dirección IPv4 de origen - Contiene un valor binario de 32 bits que representa la dirección IPv4 de origen del paquete. La dirección IPv4 de origen es siempre una dirección unicast.*
- *Dirección IPv4 de destino - Contiene un valor binario de 32 bits que representa la dirección IPv4 de destino del paquete. La dirección IPv4 de destino es una dirección unicast, multicast o de difusión.*

Los dos campos a los que se hace más referencia son los de dirección IP de origen y de destino En estos campos, se identifica de dónde viene el paquete y a dónde va. Por lo general, estas direcciones no cambian mientras se viaja desde el origen hasta el destino.

Para identificar y validar el paquete, se usan los campos de longitud del encabezado de Internet (IHL), longitud total y el encabezado checksum.

Para reordenar un paquete fragmentado, se usan otros campos. Específicamente, el paquete IPv4 utiliza los campos de identificación, señaladores y desplazamiento de fragmentos para llevar un control de los fragmentos. Un router puede tener que fragmentar un paquete IPv4 cuando lo reenvía de un medio a otro con una MTU más pequeña.

Los campos Opciones y Relleno rara vez se usan y están fuera del alcance de este módulo.

8.2.3 Video - Ejemplos de encabezados IPv4 en Wireshark

Haga clic en Reproducir en la figura para ver una demostración de una revisión de encabezados IPv4 en una captura de Wireshark.

Transcripción:

- 00:03- [Instructor] tengo una captura de pantalla de mi Wireshark
- 00:05captura de paquetes y se puede ver que el segundo paquete
- 00:08que se capturó se resaltó,

- 00:11y luego, en la ventana de detalles del paquete,
- 00:14la información de la capa de red se expandió
- 00:17para mostrarnos todas las cosa que ocurren en la capa de red.
- 00:21Así que vamos a ver lo que sucede
- 00:23en este paquete en particular que estamos analizando.
- 00:25Podemos ver que, en primer lugar,
- 00:28el protocolo de capa de red, o protocolo de capa de Internet
- 00:31que estamos tratando era la versión de protocolo de Internet 4.
- 00:35IPV 4.
- 00:36También podemos ver que la dirección IP de origen
- 00:39era 192.168.1.109.
- 00:42Podemos verlo también de forma destacada, aquí,
- 00:44en el área de ventanas de la lista de paquetes.
- 00:47Y que la dirección IP de destino era 192.168.1.1,
- 00:52Y también podemos ver eso aquí arriba.
- 00:54Podemos ver que, en la capa superior,
- 00:56este es un paquete de protocolo TCP,
- 01:00pero si nos limitamos solo a los campos IPv4,
- 01:04o la información IPv4,
- 01:06podemos ver los diferentes tipos de información de control
- 01:08que se incluyen en cada paquete IPV4.
- 01:11Por ejemplo, el número versión, que es cuatro,
- 01:14lo identifica como un IPv4, en lugar de un paquete IPv6.
- 01:18La longitud del encabezado, o el largo del encabezado,
- 01:21este es el tamaño mínimo de un encabezado de IPv4.
- 01:24El campo de servicios diferenciados,
- 01:27que se utiliza para la prioridad de paquetes
- 01:30y es útil para aplicaciones, como voz por Internet.
- 01:34La longitud total del paquete,
- 01:36El número de identificación, que se utiliza para la fragmentación.
- 01:41En los indicadores pueden ver que se estableció el bit DF,
- 01:45qué significa “don't fragment” (no fragmentar).
- 01:47Este paquete no es lo suficientemente grande,
- 01:49o no se identifica para fragmentación.
- 01:52Desplazamiento de fragmentos
- 01:54El TTL o tiempo de vida que se define en 128.
- 01:58Cada vez que un paquete se enruta desde un salto al siguiente,
- 02:03se reduce la cantidad de TTL.
- 02:06Cuando la cantidad de TTL llega a cero, el paquete se descarta
- 02:09y garantiza que los paquetes no circulen
- 02:11en internet para siempre en un bucle infinito.
- 02:14El valor TTL también se utiliza con rutas de rastreo de ICMP y pings.
- 02:19El campo de protocolo nos permite conocer el tipo de información
- 02:23para esperar en la porción de datos del paquete.
- 02:25Un seis identifica la porción de datos

- 02:28de este paquete como un paquete TCP.
- 02:32El campo de checksum del encabezado,
- 02:33que permite al router comprobar para ver
- 02:35si hay errores o inconsistencias en el encabezado
- 02:39Si los hay, el paquete será descartado.
- 02:42Y luego, por último, las direcciones IP de origen y de destino,
- 02:46que son la parte más importante del paquete IPV4.
- 02:50Veamos dos capturas de pantalla más
- 02:53de las capturas de paquetes de Wireshark,
- 02:54y veremos algunas similitudes y diferencias.
- 02:58La siguiente captura de pantalla nos muestra que ahora estamos viendo
- 03:01el octavo paquete capturado.
- 03:04La dirección IP de origen del paquete también es 192.168.1.109,
- 03:09y la dirección IP de destino es 192.168.1.1,
- 03:14excepto este paquete es una solicitud HTTP GET.
- 03:19Así que esta es una solicitud a un servidor Web
- 03:23ubicado en 192.168.1.1.
- 03:27Pueden ver que la capa de red,
- 03:29o la información de la capa de red se expandió,
- 03:32que también es el protocolo de IP versión 4,
- 03:36y que tenemos información similar
- 03:39en los diferentes campos.
- 03:40Observe debajo del campo de longitud totall que este paquete
- 03:44es de 411 bytes, en comparación con el paquete anterior,
- 03:48que solo era de 52 bytes.
- 03:50Podemos decir que este paquete htiene mucha más información,
- 03:53o que es un paquete mucho más grande que el anterior.
- 03:57si miramos a continuación la información de la versión 4 del protocolo de internet
- 04:02podemos ver la información TCP y luego debajo de eso
- 04:05que hay un protocolo de transferencia de hipertexto
- 04:08o información de protocolo HTTP en este paquete también.
- 04:13Voy a avanzar al próximo paquete,
- 04:15y pueden ver que este paquete
- 04:17es el decimosexto paquete capturado aquí.
- 04:20También es de host 192.168.1.109
- 04:25al host 192.168.1.1,
- 04:29excepto esto es el protocolo ICMP.
- 04:32Pueden ver la información en la ventana de la lista de paquetes,
- 04:36que esta es una solicitud de eco, o ping.
- 04:40Si vemos la información de la versión 4 de protocolo de Internet,
- 04:44en el área de detalles podemos ver algunas diferencias de menor importancia.
- 04:48La versión sigue siendo cuatro.

- 04:50La longitud del encabezado sigue siendo 20 bytes.
- 04:53pero podemos observar que los indicadores son levemente diferentes
- 04:58y que el campo de protocolo ahora se estableció en 1,
- 05:01lo que indica que la porción de datos de este paquete
- 05:04es un mensaje del protocolo ICMP.
- 05:07Observe que en la ventana de detalles en la parte inferior,
- 05:11es un área expandida para mirar
- 05:13en la información de encabezado específica de ICMP.

8.3 Paquete IPv6

Desplázate para empezar

8.3.1 Limitaciones de IPv4

IPv4 todavía está en uso hoy en día. Este tema trata sobre IPv6, que eventualmente reemplazará a IPv4. Para comprender mejor por qué necesita conocer el protocolo IPv6, ayuda a conocer las limitaciones de IPv4 y las ventajas de IPv6.

A lo largo de los años, se han elaborado protocolos y procesos adicionales para hacer frente a los nuevos desafíos. Sin embargo, incluso con los cambios, IPv4 aún tiene tres grandes problemas:

- **Agotamiento de la dirección IPv4:** IPv4 tiene un número limitado de direcciones públicas únicas disponibles. Si bien hay aproximadamente 4000 millones de direcciones IPv4, el incremento en la cantidad de dispositivos nuevos con IP habilitado, las conexiones constantes y el crecimiento potencial de regiones menos desarrolladas aumentaron la necesidad de direcciones.
- **Falta de conectividad de extremo a extremo:** La traducción de direcciones de red (NAT) es una tecnología comúnmente implementada dentro de las redes IPv4. NAT proporciona una manera para que varios dispositivos compartan una única dirección IPv4 pública. Sin embargo, dado que la dirección IPv4 pública se comparte, se oculta la dirección IPv4 de un host de la red interna. Esto puede ser un problema para las tecnologías que necesitan conectividad completa.
- **Mayor complejidad de la red** : mientras que NAT ha ampliado la vida útil de IPv4, solo se trataba de un mecanismo de transición a IPv6. NAT en sus diversas implementaciones crea una complejidad adicional en la red, creando latencia y haciendo más difícil la solución de problemas.

8.3.2 Información general sobre IPv6

A principios de la década de 1990, los problemas con IPv4 preocuparon al Grupo de trabajo de ingeniería de Internet (IETF) que, en consecuencia, comenzó a buscar un reemplazo.

Esto tuvo como resultado el desarrollo de IP versión 6 (IPv6). IPv6 supera las limitaciones de IPv4 y representa una mejora importante con características que se adaptan mejor a las demandas de red actuales y previsibles.

Las mejoras que ofrece IPv6 incluyen las siguientes:

- **Manejo de paquetes mejorado:** - las direcciones IPv6 se basan en el direccionamiento jerárquico de 128 bits en lugar de IPv4 con 32 bits.
- **Mejor manejo de paquetes** - Manejo de paquetes mejorado: el encabezado IPv6 se ha simplificado con menos campos.
- **Elimina la necesidad de NAT:** - Elimina la necesidad de NAT: con una cantidad tan grande de direcciones IPv6 públicas, no se necesita NAT entre una dirección IPv4 privada y una IPv4 pública. Esto evita algunos de los problemas inducidos por NAT que experimentan las aplicaciones que requieren conectividad de extremo a extremo.

El espacio de las direcciones IPv4 de 32 bits ofrece aproximadamente 4.294.967.296 direcciones únicas. El espacio de direcciones IPv6 proporciona 340,282,366,920,938,463,463,374,607,431,768,211,456, o 340 undecillones de direcciones. Esto es aproximadamente equivalente a cada grano de arena en la Tierra.

En la ilustración, se puede ver una comparación entre el espacio de direcciones IPv4 e IPv6.

Comparación del espacio de direcciones IPv4 e IPv6

comparación del espacio de direcciones IPv4 e IPv6

Leyenda

Hay 4000 millones de direcciones IPv4.

Hay 340 sextillones de direcciones IPv6.

8.3.3 Campos de encabezado de paquete IPv4 en el encabezado de paquete IPv6

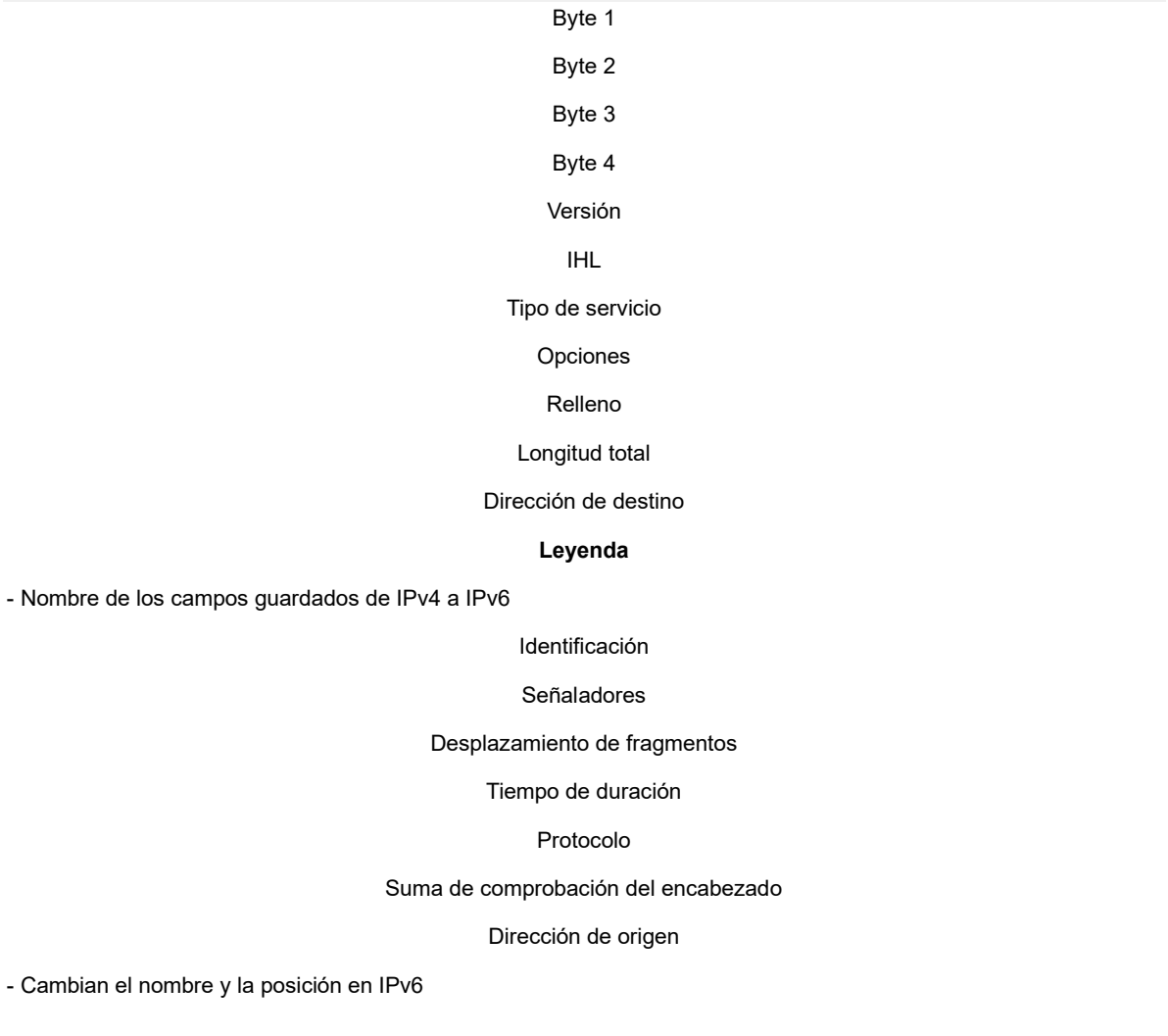
Uno de las mejoras de diseño más importantes de IPv6 con respecto a IPv4 es el encabezado simplificado de IPv6.

Por ejemplo, el encabezado IPv4 consiste en un encabezado de longitud variable de 20 octetos (hasta 60 bytes si se usa el campo Opciones) y 12 campos de encabezado básicos, sin incluir el campo Opciones y el campo Relleno.

Para IPv6, algunos campos se han mantenido igual, algunos campos han cambiado de nombre y posición, y algunos campos de IPv4 ya no son necesarios, como se destaca en la figura.

Encabezado de paquetes IPv4

El diagrama muestra un encabezado de paquete IPv4 e indica qué campos mantenían el mismo nombre, qué campos cambiaron nombres y posición y qué campos no se mantuvieron en IPv6. Los campos que mantienen el mismo nombre son: versión, dirección de origen y dirección de destino. Los campos que cambiaron los nombres y la posición son: tipo de servicio, duración total, tiempo de vida y protocolo. Los campos que no se mantuvieron en IPv6 son: IHL, identificación, indicadores, desplazamiento de fragmentos, suma de comprobación de encabezado, opciones y relleno.



- Nuevo campo en IPv6

20 bytes

La figura muestra los campos de encabezado de paquete IPv4 que se mantuvieron, movieron, cambiaron, así como aquellos que no se mantuvieron en el encabezado de paquete IPv6.

En contraste, el encabezado IPv6 simplificado que se muestra en la siguiente figura consiste en un encabezado de longitud fija de 40 octetos (en gran parte debido a la longitud de las direcciones IPv6 de origen y destino).

El encabezado simplificado IPv6 permite un procesamiento más eficiente de encabezados IPv6.

Encabezado de paquetes IPv6

El diagrama muestra un encabezado de paquete IPv6 e indica qué campos mantenían el mismo nombre de IPv4 a IPv6, qué campos cambiaron nombres y posición en IPv6, qué campos no se guardaban en IPv6 y nuevos campos en IPv6. Los nombres de campo que se mantuvieron iguales son: versión, dirección IP de origen y dirección IP de destino. Los campos que cambiaron los nombres y la posición en IPv6 son: clase de tráfico, longitud de carga útil, encabezado siguiente y límite de salto. El campo que es NUEVO para IPv6 es la etiqueta de flujo.

Byte 1

Byte 2

Byte 3

Byte 4

Versión

Clase de tráfico

Etiqueta de flujo

Siguiente encabezado

Longitud de carga útil

Límite de saltos

Dirección IP de destino

Dirección IP de origen

- Nombre de los campos guardados de IPv4 a IPv6

- Cambian el nombre y la posición en IPv6

- Nuevo campo en IPv6

Leyenda

40 bytes

La figura muestra los campos de encabezado de paquetes IPv4 que se mantuvieron o movieron junto con los nuevos campos de encabezado de paquetes IPv6.

8.3.4 Encabezado de paquetes IPv6

El diagrama de encabezado del protocolo IP en la ilustración identifica los campos de un paquete IPv6.

Campos del encabezado de paquetes IPv6

nombres y longitud de bits de los campos en un encabezado IPv6

Byte 1

Byte 2

Byte 3

Byte 4

Versión

Clase de tráfico

Etiqueta de flujo

Siguiente encabezado

Longitud de carga útil

Límite de saltos

Dirección IP de destino

Dirección IP de origen

40 bytes

Los campos en el encabezado del paquete IPv6 incluyen lo siguiente:

- ***Versión*** *- Este campo contiene un valor binario de 4 bits establecido en 0110 que identifica esto como un paquete IP versión 6.*
- ***Clase de tráfico*** *- Este campo de 8 bits es equivalente al campo de Servicios diferenciados (DS) IPv4.*
- ***Etiqueta de flujo*** *- Este 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*** *- Este campo de 16 bits indica la longitud de la porción de datos o carga útil del paquete IPv6. Esto no incluye la longitud del encabezado IPv6, que es un encabezado fijo de 40 bytes.*
- ***Encabezado siguiente*** *- Este campo de 8 bits es equivalente al campo de Protocolo IPv4. Es un valor que indica el tipo de contenido de datos que lleva el paquete, lo que permite que la capa de red transmita la información al protocolo de capa superior apropiado.*

- ***Límite de salto*** *- este 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 Tiempo excedido al host emisor. Esto indica que el paquete no llegó a su destino porque se excedió el límite de saltos. A diferencia de IPv4, IPv6 no incluye una suma de comprobación de encabezado IPv6, ya que esta función se realiza tanto en las capas inferior como superior. Esto significa que la suma de comprobación no necesita ser recalculada por cada router cuando disminuye el campo Límite de saltos, lo que también mejora el rendimiento de la red.*
- ***Dirección IPv6 de origen*** *- Este campo de 128 bits identifica la dirección IPv6 del host emisor.*
- ***Dirección IPv6 de destino*** *- Este campo de 128 bits identifica la dirección IPv6 del host receptor.*

Un paquete IPv6 también puede contener encabezados de extensión (EH), que proveen información optativa de la capa de red. Los encabezados de extensión son opcionales y están ubicados entre el encabezado de IPv6 y el contenido. Los EH se usan para fragmentar, dar seguridad, admitir la movilidad y otras acciones.

A diferencia de IPv4, los routers no fragmentan de los paquetes IPv6 enrutados.

8.3.5 Video - Ejemplos de encabezados IPv6 en Wireshark

Haga clic en Reproducir en la figura para ver una demostración de una revisión de encabezados IPv6 en una captura de Wireshark.

- 00:00- [Instructor] Esta captura de pantalla muestra
- 00:02una Captura de paquetes usando Wireshark
- 00:04y la información de la capa de red de una conversación IPv6.
- 00:08Veamos.
- 00:10En esta captura de pantalla, podemos ver que el paquete destacado
- 00:13es el paquete número 46
- 00:16y que la dirección de origen aquí
- 00:18en la ventana de la lista de paquetes se muestra
- 00:20que es una dirección IPv6 de unidifusión global.
- 00:24Puede ver esto comenzando con el 2001:6 f8.
- 00:30La dirección de destino es también un
- 00:32dirección global de unidifusión 2001:6 f 8:900 y así sucesivamente.
- 00:39Y si miramos en el campo de protocolo, vemos
- 00:42que en las capas superiores este es un paquete TCP
- 00:45y que es un intento de establecer
- 00:47una comunicación inicial con un servidor web HTTP.
- 00:51Si observamos en el área de información de la capa de red,

- 00:54puede ver que la información IPv6 se ha expandido.
- 01:00veamos algo de información de campo de protocolo
- 01:03para Protocolo de Internet versión 6.
- 01:06En primer lugar, se puede ver que la cantidad de información
- 01:10en el encabezado IPv6 es mucho menor que en el encabezado IPv4.
- 01:15Ahora, hay algunas características interesantes.
- 01:17En primer lugar, pueden ver que el campo de versión es el mismo.
- 01:21En este caso dice seis,
- 01:23identificando este paquete como IPv6.
- 01:26También podemos ver los seis binarios aquí.
- 01:29El siguiente campo es el campo de clase de tráfico.
- 01:32El campo de clase de tráfico cumple la misma función
- 01:35que los campo de servicios diferenciados en un paquete IPv4.
- 01:38Administra la priorización del tráfico y congestión.
- 01:43La siguiente sección, puede ver, es el Flowlabel.
- 01:46El campo etiqueta de flujo es un nuevo campo para el protocolo IPv6.
- 01:50su objetivo es mantener los mismos flujos de paquetes
- 01:54a través de routers y switches,
- 01:56para así ayudar a las aplicaciones en tiempo real
- 01:58que necesitan que los paquetes lleguen en el mismo orden.
- 02:01Pueden ver que el siguiente campo es el campo de la longitud de carga.
- 02:05Esto es lo mismo que el campo de la longitud total
- 02:07en el encabezado IPv4.
- 02:09Este campo nos dice el tamaño total del paquete,
- 02:14en este caso, 40 bytes.
- 02:16El siguiente campo de encabezado cumple El siguiente campo de encabezado cumple que el
- 02:20campo de protocolo para IPv4.
- 02:22verán que ha identificado
- 02:24que la porción de datos de la capa superior de este paquete
- 02:28es un seis o TCP.
- 02:31El límite de salto cumple la misma función
- 02:34que el campo TTL en un paquete IPv4.
- 02:37Puede ver que el límite de salto se establece actualmente a 64 saltos.
- 02:41Una vez que esto disminuya a cero, el paquete será eliminado.
- 02:44A continuación tenemos la dirección IPv6 de origen,
- 02:47la dirección IPv6 de destino,
- 02:49y luego, en la capa superior,
- 02:51podemos ver que se trata de un paquete TCP
- 02:53con la información de encabezado TCP.
- 02:56Veamos la próxima captura de pantalla.
- 03:00En la próxima pantalla, se puede ver que
- 03:01ahora hemos destacado el paquete número 49.
- 03:04Y ahora tenemos una conexión con este servidor Web.

- 03:07Este paquete ahora es una solicitud GET al servidor web.
- 03:12Si miramos hacia abajo en el expandido
- 03:14Protocolo de Internet versión 6 ventana de detalles del paquete
- 03:17podemos ver que la longitud de carga es mucho más grande.
- 03:21Podemos ver a continuación la información de IPv6,
- 03:25la información TCP, y que ahora hay
- 03:28Información del protocolo HTTP también dentro de nuestra solicitud GET.
- 03:34Esta es nuestra solicitud GEB para obtener una página web.
- 03:37Si voy a la próxima captura de pantalla,
- 03:39La ultima captura de pantalla muestra
- 03:41un mensaje de solicitud de vecinos de ICMP versión 6.
- 03:46Si observamos la ventana en el paquete aquí destacado
- 03:48en el paquete número 1, veremos que la dirección de origen
- 03:52esta vez no es una dirección IPv6 unidifusión global,
- 03:56si no que es una dirección link-local.
- 03:57Podemos decir eso del fe80 aquí.
- 04:00También podemos ver que esta dirección local de enlace utilizada
- 04:04EUI-64 para resolver la porción de identificación de interfaz
- 04:08de la dirección.
- 04:09Podemos decir eso por el ff:fe dentro de las direcciones.
- 04:14La dirección de destino es una dirección IPv6 ff02,
- 04:19lo que indica que se trata de un paquete de multidifusión.
- 04:22Si observamos el protocolo,
- 04:23vemos que es la versión 6 de ICMP,
- 04:26y luego la información sobre el paquete nos dice
- 04:29que esto es un mensaje de solicitud de vecino
- 04:32para el mismo dispositivo que estábamos contactando
- 04:35en las capturas de pantalla anteriores.
- 04:37La función de este paquete esencialmente, es similar
- 04:41a una solicitud ARP en IPv4.
- 04:43Necesitamos descubrir la dirección link-local de este dispositivo,
- 04:48por lo que enviamos una versión ICMP 6
- 04:51Mensaje de solicitud de vecinos
- 04:53multidifusión que, y esperamos
- 04:55para recuperar una dirección local de enlace de este vecino.
- 04:59Si miramos hacia abajo en la ventana de detalles ampliada,
- 05:03podemos ver que es la versión 6,
- 05:05clase de tráfico, flowlabel,
- 05:07longitud de la carga útil, que es la longitud total del paquete.
- 05:11El siguiente campo de encabezado, que es como el campo de protocolo
- 05:13en IPv4, indicando en 58 que esto es
- 05:16un mensaje ICMP versión 6 en la parte de datos del paquete.
- 05:21el límite de salto-- 255 saltos.

- 05:24Esto es similar al campo TTL.
- 05:27Y luego la dirección link-local de origen
- 05:29y la dirección de multidifusión de destino IPv6.
- 05:34En la parte inferior, debajo de la información de IPv6,
- 05:38podemos ver que hay un un área expansible
- 05:42al protocolo de mensajes de control de internet versión 6.

8.4 ¿Cómo arma las rutas el host?

Desplázate para empezar

8.4.1 La decisión de reenvío de host

Con IPv4 e IPv6, los paquetes siempre se crean en el host de origen. El host de origen debe poder dirigir el paquete al host de destino. Para ello, los dispositivos finales de host crean su propia tabla de enrutamiento. En este tema se explica cómo los dispositivos finales utilizan las tablas de enrutamiento.

Otra función de la capa de red es dirigir los paquetes entre hosts. Un host puede enviar un paquete a lo siguiente:

- **Itself** - un host puede hacer ping a sí mismo enviando un paquete a una dirección IPv4 especial de 127.0.0.1 o una dirección IPv6 ::1, que se conoce como la interfaz de bucle invertido. El hacer ping a la interfaz de bucle invertido, pone a prueba la pila del protocolo TCP/IP en el host.
- **Host local** - este es un host de destino que se encuentra en la misma red local que el host emisor. Los hosts de origen y destino comparten la misma dirección de red.
- **Host remoto** - este es un host de destino en una red remota. Los hosts de origen y destino no comparten la misma dirección de red.

La figura ilustra la conexión de PC1 a un host local en la misma red y a un host remoto ubicado en otra red.

El diagrama muestra un host, PC1, que se conecta a un host local, PC2, en la misma red y a un host remoto, un servidor, en otra red. PC1 y PC2 están conectados a un switch en la red 192.168.10.0/24. PC1 tiene una dirección de.10 y PC2 tiene una dirección de.15. El switch está conectado a un router, R1, en la dirección .1. En el otro lado de R1 hay una conexión a la nube donde reside el host remoto.

PC1R1.10.1PC2.15

Host
local

Host
remoto

192.168.10.0/24

El dispositivo final de origen determina si un paquete está destinado a un host local o a un host remoto. El dispositivo final de origen determina si la dirección IP de destino está en la misma red en la que está el propio dispositivo de origen. El método de determinación varía según la versión IP:

- **En IPv4** : el dispositivo de origen utiliza su propia máscara de subred junto con su propia dirección IPv4 y la dirección IPv4 de destino para realizar esta determinación.
- **En IPv6** : el router local anuncia la dirección de red local (prefijo) a todos los dispositivos de la red.

En una red doméstica o comercial, puede tener varios dispositivos cableados e inalámbricos interconectados mediante un dispositivo intermediario, como un switch LAN o un punto de acceso inalámbrico (WAP). Este dispositivo intermediario proporciona interconexiones entre hosts locales en la red local. Los hosts locales pueden conectarse y compartir información sin la necesidad de dispositivos adicionales. Si un host está enviando un paquete a un dispositivo que está configurado con la misma red IP que el dispositivo host, el paquete simplemente se reenvía desde la interfaz del host, a través del dispositivo intermediario, y directamente al dispositivo de destino.

Por supuesto, en la mayoría de las situaciones queremos que nuestros dispositivos puedan conectarse más allá del segmento de red local, como a otros hogares, negocios e Internet. Los dispositivos que no están en el segmento de red local se denominan "módulo remoto de E/S". Cuando un dispositivo de origen envía un paquete a un dispositivo de destino remoto, se necesita la ayuda de los routers y del enrutamiento. El enrutamiento es el proceso de identificación de la mejor ruta para llegar a un destino. El router conectado al segmento de red local se denomina gateway predeterminado.

8.4.2 Puerta de Enlace Predeterminada (Gateway)

La puerta de enlace predeterminada es el dispositivo de red (es decir, el router o el switch de capa 3) que puede enrutar el tráfico a otras redes. Si se piensa en una red como si fuera una habitación, el gateway predeterminado es como la puerta. Si desea ingresar a otra habitación o red, debe encontrar la puerta.

En una red, una puerta de enlace predeterminada suele ser un router con estas características:

- Tiene una dirección IP local en el mismo rango de direcciones que otros hosts en la red local.
- 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. El tráfico no se puede reenviar fuera de la red local si no hay una puerta de enlace predeterminada, la dirección de la puerta de enlace predeterminada no está configurada o la puerta de enlace predeterminada está desactivada.

8.4.3 Un host enruta a la puerta de enlace predeterminada

Una tabla de enrutamiento de host generalmente incluirá una puerta de enlace predeterminada. En IPv4, el host recibe la dirección IPv4 de la puerta de enlace predeterminada, ya sea dinámicamente desde el Protocolo de configuración dinámica de host (DHCP) o configurado manualmente. En IPv6, el router anuncia la dirección de la puerta de enlace predeterminada o el host se puede configurar manualmente.

En la figura, PC1 y PC2 están configuradas con la dirección IPv4 de 192.168.10.1 como la puerta de enlace predeterminada.

El diagrama muestra dos hosts, PC1 y PC2, conectados a un switch en la red 192.168.10.0/24, la ruta de red local. El switch está conectado a un router, R1, que luego se conecta a la nube que representa redes remotas. PC1 tiene una dirección de.10, PC2 tiene una dirección de.15 y la interfaz del router a la que está conectado el switch tiene una dirección de .1. Las PC, el switch y la interfaz del router tienen una conexión directa.

.10.1192.168.10.0/24.15PC1R1PC2

Ruta de red local

Redes remotas

Conexión directa

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 que la PC utiliza cuando intenta conectarse a la red remota.

Tanto la PC1 como la PC2 tendrán una ruta predeterminada para enviar todo el tráfico destinado a las redes remotas al R1.

8.4.4 Tablas de enrutamiento de host

En un host de Windows, el comando **route print** o **netstat -r** se puede usar para mostrar la tabla de enrutamiento del host. Los dos comandos generan el mismo resultado. Al principio, los resultados pueden parecer abrumadores, pero son bastante fáciles de entender.

La figura muestra una topología de ejemplo y la salida generada por el **netstat -r** comando.

Tabla de enrutamiento IPv4 para la PC1

```
C:\Users\PC1> netstat -r
(output omitted)
IPv4 Route Table
===========================================================================
==============
Active Routes:
Network
Destination         Netmask       Gateway       Interface
Metric
          0.0.0.0           0.0.0.0   192.168.10.1   192.168.
10.10       25
        127.0.0.0         255.0.0.0        On-
link         127.0.0.1      306
        127.0.0.1   255.255.255.255        On-
link         127.0.0.1      306
  127.255.255.255   255.255.255.255        On-
link         127.0.0.1      306
     192.168.10.0     255.255.255.0        On-
link    192.168.10.10      281
    192.168.10.10   255.255.255.255        On-
link    192.168.10.10      281
   192.168.10.255   255.255.255.255        On-
link    192.168.10.10      281
        224.0.0.0         240.0.0.0        On-
link         127.0.0.1      306
        224.0.0.0         240.0.0.0        On-
link    192.168.10.10      281
  255.255.255.255   255.255.255.255        On-
link         127.0.0.1      306
  255.255.255.255   255.255.255.255        On-
link    192.168.10.10      281
(output omitted)
```

Nota: La salida sólo muestra la tabla de rutas IPv4.

Al ingresar el **netstat -r**comando o el comando equivalente, **route print**se muestran tres secciones relacionadas con las conexiones de red TCP / IP actuales:

- **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, incluidos los adaptadores Ethernet, Wi-Fi y Bluetooth.
- **Tabla de rutas IPv4:** - enumera todas las rutas IPv4 conocidas, incluidas las conexiones directas, la red local y las rutas locales predeterminadas.

- **Tabla de rutas IPv6:** - Tabla de rutas IPv6: enumera todas las rutas IPv6 conocidas, incluidas las conexiones directas, la red local y las rutas locales predeterminadas.

8.5 Introducción al enrutamiento

Desplázate para empezar

8.5.1 Decisión de envío de paquetes del router

En el tema anterior se discutieron las tablas de enrutamiento de host. La mayoría de las redes también contienen routers, que son dispositivos intermediarios. Los routers también contienen tablas de enrutamiento. En este tema se tratan las operaciones del router en la capa de red. Cuando un host envía un paquete a otro host, consulta su tabla de enrutamiento para determinar dónde enviar el paquete. Si el host de destino está en una red remota, el paquete se reenvía a la puerta de enlace predeterminada, que generalmente es el router local.

¿Qué sucede cuando llega un paquete a la interfaz de un router?

El router examina la dirección IP de destino del paquete y busca en su tabla de enrutamiento para determinar dónde reenviar el paquete. La tabla de enrutamiento contiene una lista de todas las direcciones de red conocidas (prefijos) y a dónde reenviar el paquete. Estas entradas se conocen como entradas de ruta o rutas. El router reenviará el paquete utilizando la mejor entrada de ruta que coincida (más larga).

El diagrama es una topología de red que muestra lo que sucede con un paquete IPv4 a medida que se enruta entre redes. El host PC1, con una dirección de.10, está conectado a un switch en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del router R1 con una dirección de .1. La red 209.165.200.224/30 conecta la interfaz G0/0/1 en R1, dirección .225, a otro router, R2 en la dirección .226. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección .10. R2 tambien tiene una conexión a la nube de Internet. Se envía un paquete con la dirección IPv4 de destino 10.1.1.10 desde PC1 a R1. R1 envía el paquete con la dirección IPv4 de destino 10.1.1.10 a R2.

132PC2R2.10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24R1.225G0/0/0PC1

Internet

Dirección IPv4 de destino:
10.1.1.10

Dirección IPv4 de destino:
10.1.1.10

1. *El paquete llega a la interfaz Gigabit Ethernet 0/0/0 del router R1. R1 desencapsula el encabezado Ethernet de Capa 2 y el remolque.*
2. *El router R1 examina la dirección IPv4 de destino del paquete y busca la mejor coincidencia en su tabla de enrutamiento IPv4. La entrada de ruta indica que este paquete se reenviará al router R2.*
3. *El router R1 encapsula el paquete en un nuevo encabezado Ethernet y remolque, y reenvía el paquete al siguiente router de salto R2.*

La siguiente tabla muestra la información pertinente de la tabla de ruteo R1.

R1 Routing Table

8.5.2 Tabla de enrutamiento IP del router

La tabla de enrutamiento del router contiene entradas de ruta de red que enumeran todos los posibles destinos de red conocidos.

La tabla de enrutamiento almacena tres tipos de entradas de ruta:

- **Redes conectadas directamente** - estas entradas de ruta de red son interfaces de router activas. Los routers agregan una ruta conectada directamente cuando una interfaz se configura con una dirección IP y se activa. Cada interfaz de router está conectada a un segmento de red diferente. En la figura, las redes conectadas directamente en la tabla de enrutamiento IPv4 R1 serían 192.168.10.0/24 y 209.165.200.224/30.
- **Redes remotas** - estas entradas de ruta de red están conectadas a otros routers. Los routers aprenden acerca de las redes remotas ya sea mediante la configuración explícita de un administrador o mediante el intercambio de información de ruta mediante un protocolo de enrutamiento dinámico. En la figura, la red remota en la tabla de enrutamiento IPv4 R1 sería 10.1.1.0/24.
- **Ruta predeterminada** - al igual que un host, la mayoría de los routers también incluyen una entrada de ruta predeterminada, una puerta de enlace de último recurso. La ruta predeterminada se utiliza cuando no hay una mejor coincidencia (más larga) en la tabla de enrutamiento IP. En la figura, la tabla de enrutamiento IPv4 R1 probablemente incluiría una ruta predeterminada para reenviar todos los paquetes al router R2.

La figura identifica las redes directamente conectadas y remotas del router R1.

El diagrama es una topología de red que identifica las redes conectadas directamente y las redes remotas de un router. El host PC1, con una dirección de.10, está conectado a un

conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. La red 209.165.200.224/30 conecta la interfaz G0/0/1 en R1, dirección .225, a otro router, R2 en la dirección .226 en G0/0/1. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección .10. R2 tambien tiene una conexión a la nube de Internet. Las redes 192.168.10.0/24 y 209.165.200.224/30 se muestran como redes conectadas directamente a R1 y a la red 10.1.2.0/24 (¿debería ser 10.1.1.0/24?) se muestra como una red remota a R2.

.10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24.225G0/0/0G0/0/0G0/0/1PC2R2R1PC1

Internet

Red conectada directamente

Red conectada directamente

Red remota

R1 tiene dos redes de conexión directa:

- *192.168.10.0/24*
- *209.165.200.224/30*

R1 también tiene redes remotas (es decir, 10.1.1.0/24 e Internet) sobre las que puede aprender.

Un router puede descubrir redes remotas de dos maneras:

- **Manualmente** - las redes remotas se ingresan manualmente en la tabla de rutas mediante rutas estáticas.
- **Dinámicamente** - las rutas remotas se aprenden automáticamente mediante un protocolo de enrutamiento dinámico.

8.5.3 Enrutamiento estático

Las rutas estáticas son entradas de ruta que se configuran manualmente. La figura muestra un ejemplo de una ruta estática que se configuró manualmente en el router R1. La ruta estática incluye la dirección de red remota y la dirección IP del router de salto siguiente.

El diagrama es una topología de red que muestra una configuración de ruta estática para llegar a una red remota. El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. La red 209.165.200.224/30 conecta la interfaz G0/0/1 en R1, dirección .225, a otro enrutador, R2 en la dirección .226. R2 tiene una interfaz con la dirección .1 conectada a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, la dirección .10. R2 tambien tiene una conexión a la nube de Internet. Una configuración de ruta estática en R1 a la red 10.1.1.0/24 dice: R1(config)#IP route 10.1.1.0 255.255.255.0 209.165.200.226.

En la configuración, 10.1.1.0 255.255.0 está etiquetado como red remota y 209.165.200.226 como dirección IP del router de salto siguiente.

R1(config)# ip route 10.1.1.0 255.255.255.0 209.165.200.226
.10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24.225G0/0/0PC2R2R1PC1

Internet

Dirección de red remota

Dirección IP del router del próximo salto

R1 se configura manualmente con una ruta estática para llegar a la red 10.1.1.0/24. Si esta ruta cambia, R1 requerirá una nueva ruta estática.

Si hay un cambio en la topología de la red, la ruta estática no se actualiza automáticamente y debe reconfigurarse manualmente. Por ejemplo, en la figura R1 tiene una ruta estática para llegar a la red 10.1.1.0/24 a través de R2. Si esa ruta ya no está disponible, R1 tendría que reconfigurarse con una nueva ruta estática a la red 10.1.1.0/24 a través de R3. Por lo tanto, el router R3 necesitaría tener una entrada de ruta en su tabla de enrutamiento para enviar paquetes destinados a 10.1.1.0/24 a R2.

El diagrama es una topología de red que muestra un vínculo fallido en una ruta estática. El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. R1 está conectado al router R2 y al router R3 que también se dirigen conectados. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección .10. Se ha configurado una ruta estática en R1 que apunta a R2 como el salto siguiente. Una X roja indica que este enlace ha fallado.

.10.1192.168.10.0/24G0/0/0PC2R2R1PC1R310.1.1.0/24.10

Ruta estática

Si la ruta desde R1 a R2 ya no está disponible, debería configurarse una nueva ruta estática a través de R3. Una ruta estática no se ajusta automáticamente para los cambios de topología.

El enrutamiento estático tiene las siguientes características:

- Una ruta estática debe configurarse manualmente.
- El administrador necesita volver a configurar una ruta estática si hay un cambio en la topología y la ruta estática ya no es viable.
- Una ruta estática es apropiada para una red pequeña y cuando hay pocos o ninguno de los enlaces redundantes.
- Una ruta estática se usa comúnmente con un protocolo de enrutamiento dinámico para configurar una ruta predeterminada.

8.5.4 Enrutamiento dinámico

Un protocolo de enrutamiento dinámico permite a los routers aprender automáticamente sobre redes remotas, incluida una ruta predeterminada, de otros routers. Los routers que usan protocolos de enrutamiento dinámico comparten automáticamente la información de enrutamiento con otros routers y compensan cualquier cambio de topología sin que sea necesaria la participación del administrador de la red. Si se produce un cambio en la topología de red, los routers comparten esta información mediante el protocolo de enrutamiento dinámico y actualizan automáticamente sus tablas de enrutamiento.

Los protocolos de enrutamiento dinámico incluyen OSPF y Enhanced Interior Gateway Routing Protocol (EIGRP). La figura muestra un ejemplo de routers R1 y R2 que comparten automáticamente información de red mediante el protocolo de enrutamiento OSPF.

- R1 está utilizando el protocolo de enrutamiento OSPF para que R2 sepa acerca de la red 192.168.10.0/24.
- R2 está utilizando el protocolo de enrutamiento OSPF para que R1 sepa acerca de la red 10.1.1.0/24.

La configuración básica sólo requiere que el administrador de red habilite las redes conectadas directamente dentro del protocolo de enrutamiento dinámico. El protocolo de enrutamiento dinámico hará automáticamente lo siguiente:

- Detectar redes remotas.
- Mantener información de enrutamiento actualizada.
- Elija el mejor camino hacia las redes de destino
- Intente encontrar una nueva mejor ruta si la ruta actual ya no está disponible

Cuando un router se configura manualmente con una ruta estática o aprende acerca de una red remota dinámicamente mediante un protocolo de enrutamiento dinámico, la dirección de red remota y la dirección de salto siguiente se introducen en la tabla de enrutamiento IP. Como se muestra en la figura, si hay un cambio en la topología de red, los routers se ajustarán automáticamente e intentarán encontrar una nueva mejor ruta.

El diagrama muestra una topología de red en la que los routers que utilizan protocolos de enrutamiento dinámico están ajustando las mejores rutas después de un cambio de topología. El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. R1 está conectado al router R2 y al router R3 que también se dirigen conectados. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección

.10. Una X roja indica que el enlace entre R1 y R2, etiquetado como la mejor ruta anterior, ha fallado. Se muestra un nuevo mejor camino que va de R1 a R3 a R2.

.10.1192.168.10.0/24G0/0/0PC2R2R1PC1R310.1.1.0/24.10

Mejor ruta anterior

Nuevo mejor camino

R1, R2 y R3 están utilizando el protocolo de enrutamiento dinámico OSPF. Si hay un cambio de topología de red, se pueden ajustar automáticamente para buscar una nueva mejor ruta.

Nota: Es común que algunos routers usen una combinación de rutas estáticas y un protocolo de enrutamiento dinámico.

8.5.5 Video- Tablas de enrutamiento de router IPv4

A diferencia de una tabla de enrutamiento de la computadora host, no hay encabezados de columna que identifiquen la información contenida en la tabla de enrutamiento de un router. Es importante aprender el significado de los diferentes elementos presentes en cada tabla de enrutamiento.

Haga clic en Reproducir en la ilustración para ver una introducción a la tabla de enrutamiento IPv4.

8.5.6 Introducción a una tabla de enrutamiento IPv4

Observe en la figura que R2 está conectado a Internet. Por lo tanto, el administrador configuró R1 con una ruta estática predeterminada que envía paquetes a R2 cuando no hay ninguna entrada específica en la tabla de enrutamiento que coincida con la dirección IP de destino. R1 y R2 también están utilizando el enrutamiento OSPF para anunciar redes conectadas directamente.

El host PC1, con una dirección de.10, está conectado a un conmutador en la red 192.168.10.0/24 que está conectado a la interfaz G0/0/0 del enrutador R1 con una dirección de .1. La red 209.165.200.224/30 conecta la interfaz G0/0/1 en R1, dirección .225, a otro enrutador, R2 en la dirección .226. R2 está conectado a un switch en la red 10.1.1.0/24 al que está conectado el PC2 host, dirección .10. R2 tambien tiene una conexión a la nube de Internet.

.10.1.1G0/0/1.226.10209.165.200.224/30192.168.10.0/2410.1.1.0/24.225G0/0/0PC2R2R1PC1

Internet

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M -
mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF
inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA
external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2
- IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-
user static route
       o - ODR, P - periodic downloaded static route, H -
NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p -
overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226,
GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45,
GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2
masks
C        192.168.10.0/24 is directly connected,
GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected,
GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2
masks
C        209.165.200.224/30 is directly connected,
GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected,
GigabitEthernet0/0/1
R1#
```

El comando **show ip route** de EXEC mode privilegiado se utiliza para ver la tabla de enrutamiento IPv4 en un router Cisco IOS. El ejemplo muestra la tabla de enrutamiento IPv4 del router R1. Al principio de cada entrada de tabla de enrutamiento hay un código que se utiliza para identificar el tipo de ruta o cómo se aprendió la ruta. Entre las fuentes de ruta comunes (códigos) se incluyen las siguientes:

- **L** - Dirección IP de interfaz local conectada directamente
- **C** - Red conectada directamente
- **S** — La ruta estática fue configurada manualmente por un administrador
- **O** - OSPF
- **D** - EIGRP

La tabla de enrutamiento muestra todas las rutas de destino IPv4 conocidas para R1.

Una ruta conectada directamente se crea automáticamente cuando se configura una interfaz de router con información de dirección IP y se activa. El router añade dos entradas de ruta con los códigos C (es decir, la red conectada) y L (es decir, la dirección IP de la interfaz local de la red conectada). Las entradas de ruta también identifican la interfaz de salida que se utilizará para llegar a la red. Las dos redes conectadas directamente en este ejemplo son 192.168.10.0/24 y 209.165.200.224/30.

Los routers R1 y R2 también están utilizando el protocolo de enrutamiento dinámico OSPF para intercambiar información de router. En la tabla de enrutamiento de ejemplo, R1 tiene una entrada de ruta para la red 10.1.1.0/24 que aprendió dinámicamente del router R2 a través del protocolo de enrutamiento OSPF.

Una ruta predeterminada tiene una dirección de red de todos los ceros. Por ejemplo, la dirección de red IPv4 es 0.0.0.0. Una entrada de ruta estática en la tabla de enrutamiento comienza con un código de S *, como se resalta en el ejemplo.

8.6 Práctica del Módulo y Cuestionario

Desplázate para empezar

8.6.1 ¿Qué aprenderé en este módulo?

Características de la capa de red

La capa de red (Capa OSI 3) proporciona servicios para permitir que los dispositivos finales intercambien datos a través de las redes. IPv4 e IPv6 son los principales protocolos de comunicación de la capa de red. La capa de red también incluye el protocolo de enrutamiento OSPF y protocolos de mensajería como ICMP. Los protocolos de capa de red realizan cuatro operaciones básicas: direccionamiento de dispositivos finales, encapsulación, enrutamiento y desencapsulación. IPv4 e IPv6 especifican la estructura de paquetes y el procesamiento utilizado para transportar los datos de un host a otro. IP encapsula el segmento de la capa de transporte agregando un encabezado IP, que se utiliza para entregar el paquete al host de destino. El encabezado IP es examinado por los dispositivos de Capa 3 (es decir, routers) a medida que viaja a través de una red a su

destino. Las características de la IP son que es sin conexión, el mejor esfuerzo e independiente de los medios de comunicación. IP no tiene conexión, lo que significa que IP no crea una conexión de extremo a extremo dedicada antes de enviar los datos. El protocolo IP no garantiza que todos los paquetes que se envían, de hecho, se reciban. Esta es la definición de la característica poco confiable, o mejor esfuerzo. IP funciona independientemente de los medios que transportan los datos en las capas más bajas de la pila de protocolos.

Paquete IPv4

Un encabezado de paquete IPv4 consta de campos que contienen información sobre el paquete. Estos campos tienen números binarios que examinan el proceso de capa 3. Los valores binarios de cada campo identifican diversos parámetros de configuración del paquete IP. Los campos significativos del encabezado IPv6 incluyen: versión, DS, suma de comprobación de encabezado, TTL, protocolo y direcciones IPv4 de origen y destino.

Paquete IPv6

IPv6 está diseñado para superar las limitaciones de IPv4, entre ellas: agotamiento de direcciones IPv4, falta de conectividad de extremo a extremo y mayor complejidad de la red. IPv6 aumenta el espacio de direcciones disponible, mejora el manejo de paquetes y elimina la necesidad de NAT. Los campos en el encabezado del paquete IPv6 incluyen: versión, clase de tráfico, etiqueta de flujo, longitud de la carga útil, siguiente encabezado, límite de salto y las direcciones IPv6 de origen y destino.

Cómo arma las rutas un host

Un host puede enviar un paquete a sí mismo, a otro host local y a un host remoto. En IPv4, el dispositivo de origen utiliza su propia máscara de subred junto con su propia dirección IPv4 y la dirección IPv4 de destino para determinar si el host de destino está en la misma red. En IPv6, el router local anuncia la dirección de red local (prefijo) a todos los dispositivos de la red, para realizar esta determinación. La puerta de enlace predeterminada es el dispositivo de red (es decir, el router) que puede enrutar el tráfico a otras redes. En una red, una puerta de enlace predeterminada suele ser un router que tiene una dirección IP local en el mismo rango de direcciones que otros hosts de la red local, puede aceptar datos en la red local y reenviar datos fuera de la red local, y enrutar el tráfico a otras redes. Una tabla de enrutamiento de host generalmente incluirá una puerta de enlace predeterminada. En IPv4, el host recibe la dirección IPv4 de la puerta de enlace predeterminada de forma dinámica a través de DHCP o se configura manualmente. En IPv6, el router anuncia la dirección de la puerta de enlace predeterminada o el host se puede configurar manualmente. En un host de Windows, el comando **route print** o **netstat -r** se puede usar para mostrar la tabla de enrutamiento del host.

Introducción al enrutamiento

Cuando un host envía un paquete a otro host, consulta su tabla de enrutamiento para determinar dónde enviar el paquete. Si el host de destino está en una red remota, el paquete

se reenvía a la puerta de enlace predeterminada, que generalmente es el router local. ¿Qué sucede cuando llega un paquete a la interfaz de un enrutador? El router examina la dirección IP de destino del paquete y busca en su tabla de enrutamiento para determinar dónde reenviar el paquete. La tabla de enrutamiento contiene una lista de todas las direcciones de red conocidas (prefijos) y a dónde reenviar el paquete. Estas entradas se conocen como entradas de ruta o rutas. El router reenviará el paquete utilizando la mejor entrada de ruta que coincida (más larga). La tabla de enrutamiento de un router almacena tres tipos de entradas de ruta: redes conectadas directamente, redes remotas y una ruta predeterminada. Los routers aprenden sobre redes remotas de forma manual o dinámica utilizando un protocolo de enrutamiento dinámico. Las rutas estáticas son entradas de ruta que se configuran manualmente. Las rutas estáticas incluyen la dirección de red remota y la dirección IP del router de salto siguiente. OSPF y EIGRP son dos protocolos de enrutamiento dinámico. El comando EXEC mode **show ip route** privilegiado se utiliza para ver la tabla de enrutamiento IPv4 en un router Cisco IOS. Al principio de una tabla de enrutamiento IPv4 hay un código que se utiliza para identificar el tipo de ruta o cómo se aprendió la ruta. Las fuentes de ruta comunes (códigos) incluyen:

L - Dirección IP de interfaz local conectada directamente

C - Red conectada directamente

S - La ruta estática fue configurada manualmente por un administrador

O - Open Shortest Path First (OSPF)

D - Enhanced Interior Gateway Routing Protocol (EIGRP)