**Componentes de la comunicación en la capa de red**

En la lectura sobre el [modelo OSI](https://www.coursera.org/learn/conexion-y-proteccion-redes-y-seguridad-de-redes/supplement/YbKL0/el-modelo-osi), viste las siete capas del modelo OSI que se utilizan para conceptualizar cómo se transmiten los datos a través de Internet. Ahora, aprenderás más sobre qué operaciones se desarrollan en la capa 3: la capa de red.

**Operaciones en la capa de red**

Las funciones en la capa de red organizan la dirección y la entrega de paquetes de datos a través de la red e Internet desde el dispositivo host hasta el de destino. Esto incluye dirigir los paquetes de un enrutador a otro a través de Internet, basándose en la dirección del protocolo de Internet (IP) de la red de destino. La dirección IP de destino se encuentra dentro del encabezado de cada paquete de datos. Esta dirección se almacenará en tablas de enrutamiento a lo largo del camino del paquete hacia su destino, para futuros propósitos de enrutamiento.

Todos los paquetes de datos incluyen una dirección IP; esto se denomina paquete IP o datagrama. Un router utiliza la dirección IP para enrutar paquetes de una red a otra, basándose en la información contenida en el encabezado IP de un paquete de datos. La información del encabezado no comunica solo la dirección del destino. También incluye información, como la dirección IP de origen, el tamaño del paquete y qué protocolo se utilizará para el área de datos del paquete.

**Formato de un paquete IPv4**

A continuación, puedes ver el formato de un paquete IP versión 4 (IPv4) y un gráfico que detalla el encabezado del paquete. Un paquete IPv4 se compone de dos secciones, el encabezado y los datos:

* El tamaño del encabezado IP oscila entre 20 y 60 bytes. Incluye la información de enrutamiento IP que los dispositivos utilizan para dirigir el paquete. El formato de un encabezado de paquete IP está determinado por el protocolo IPv4.
* La longitud de la sección de datos de un paquete IPv4 puede variar mucho, pero el tamaño máximo posible de un paquete IP es 65.536 bytes. Contiene el mensaje que se transfiere a la transmisión, como la información del sitio web o el texto del correo electrónico.

Hay 13 campos dentro del encabezado de un paquete IPv4:

* **Versión:** el primer encabezado de 4 bits indica a los dispositivos receptores qué protocolo está utilizando el paquete. El paquete utilizado en la ilustración anterior es un paquete IPv4.
* **Longitud del encabezado IP (HLEN):** HLEN es la longitud del encabezado del paquete. Este valor indica dónde termina el encabezado del paquete y comienza el segmento de datos.
* **Tipo de servicio (ToS):** los routers priorizan los paquetes a entregar con el fin de mantener la calidad del servicio en la red. El campo ToS proporciona esta información al router.
* **Longitud total:** este campo comunica la longitud total de todo el paquete IP, incluidos el encabezado y los datos. El tamaño máximo de un paquete IPv4 es de 65.535 bytes.
* **Identificación:** si el paquete IPv4 es superior a 65 535 bytes, se divide o fragmenta en paquetes IP más pequeños. El campo de identificación proporciona un identificador único para todos los fragmentos del paquete IP original para que puedan volver a ensamblarse cuando lleguen a su destino.
* **Indicadores:** este campo proporciona al dispositivo de enrutamiento más información sobre si el paquete original se fragmentó y si hay más fragmentos en tránsito.
* **Desplazamiento de fragmentación:** el campo de desplazamiento de fragmento indica a los dispositivos de enrutamiento a qué parte del paquete original pertenece el fragmento.
* **Período de vida (TTL):** evita que los routers reenvíen los paquetes de datos de manera indefinida. Contiene un contador que determina la fuente. El contador disminuye de a uno, a medida que pasa por cada router. Cuando el contador TTL llega a cero, el router descartará el paquete y enviará al emisor un mensaje de tiempo superado ICMP.
* **Protocolo:** este campo indica al dispositivo receptor qué protocolo se utilizará para el área de datos del paquete.
* **Suma de comprobación del encabezado:** este campo contiene una suma de comprobación que se puede usar para detectar si la cabecera IP en tránsito está dañada. Los paquetes dañados se descartan.
* **Dirección IP de origen:** es la dirección IPv4 del dispositivo emisor.
* **Dirección IP de destino:** es la dirección IPv4 del dispositivo receptor.
* **Opciones:** este campo permite aplicar opciones de seguridad al paquete si el valor HLEN es mayor que cinco. Además, comunica estas alternativas a los dispositivos de enrutamiento.

**Diferencia entre IPv4 e IPv6**

En una parte anterior de este curso, aprendiste sobre la historia de las direcciones IP. Con el crecimiento de Internet, se hizo evidente que todas las direcciones IPv4 se consumirían en algún momento, lo que se conoce como el agotamiento de direcciones IPv4. En ese momento, nadie había anticipado la cantidad de dispositivos informáticos que necesitarían una dirección IP en el futuro. En respuesta a esta problemática, se desarrolló IPv6, con el fin de mitigar el agotamiento de direcciones IPv4 y abordar otras preocupaciones relacionadas con esto.

Una de las principales diferencias entre IPv4 e IPv6 es la longitud de las direcciones. Las direcciones IPv4 son numéricas, están compuestas por 4 bytes y admiten hasta 4300 millones de direcciones posibles. Un ejemplo sería: 198.51.100.0. En cambio, las direcciones IPv6 son hexadecimales, están compuestas por 16 bytes y permiten hasta 340 undecillones de direcciones (la cifra 340 seguida de 36 ceros). Un ejemplo de una dirección IPv6 sería: 2002:0db8:0000:0000:0000:ff21:0023:1234.

También hay algunas diferencias en el diseño del encabezado de un paquete IPv6. El formato del IPv6 es mucho más simple que el del IPv4. Por ejemplo, el encabezado de IPv4 incluye los campos HLEN, identificación e indicadores, mientras que el IPv6 no lo hace. El encabezado de IPv6 tiene otros campos que no están incluidos en IPv4, como etiqueta de flujo y clase de tráfico.

Hay algunas diferencias de seguridad importantes entre IPv4 e IPv6. IPv6 ofrece un enrutamiento más eficiente y elimina las colisiones de direcciones privadas que pueden ocurrir en IPv4 cuando dos dispositivos de la misma red intentan usar la misma dirección.

**Conclusiones clave**

Las/los analistas de seguridad pueden utilizar herramientas de captura de paquetes, o PCAP, para inspeccionarlos mientras están en tránsito. Analizar los diferentes campos en un paquete de dirección IP puede servir para descubrir información importante relacionada con la seguridad  del paquete. Algunos ejemplos de información relacionada con la seguridad que se encuentran en los paquetes de direcciones IP son: desde dónde proviene el paquete, hacia dónde se dirige y qué protocolo está utilizando. Comprender los datos en un paquete de datos IPv4 te permitirá tomar decisiones críticas respecto a las implicaciones de seguridad de los paquetes que inspecciones.