Video: Ejemplos de encabezados IPv4 en Wireshark (6 min)

Veamos cómo la información de la capa de red se puede observar y analizar en una captura de paquetes de Wireshark. Tengo una captura de pantalla de una captura de paquetes de Wireshark. Y pueden observar que el segundo paquete que se captura se ha destacado. y luego en la ventana de detalles del paquete, se ha extendido la información de la capa de red para mostrarnos todas las cosas que ocurren en la capa de red.

Veamos lo que sucede en este paquete determinado que estamos examinando. Podemos ver que, primero que todo, el protocolo de capa de red, o protocolo de capa de Internet, con la que nos enfrentamos era el Protocolo de Internet versión 4, IPv4. También podemos ver que la dirección IP de origen era 192.168.1.109. Podemos ver de forma destacada aquí en el área de ventanas de la lista de paquetes y que la dirección IP de destino era 192.168.1.1. Y también podemos ver eso aquí arriba. Podemos ver que, en la capa superior, este es un paquete de protocolo TCP. Pero si nos limitamos solo a los campos IPv4, o la información IPv4, podemos ver los diferentes tipos de información de control que se incluyen en cada paquete IPV4.

Por ejemplo, el número de versión, que es 4, identificando esto como IPv4, en oposición al paquete IPv6. La longitud del encabezado, o la longitud del encabezado-- esto es el tamaño mínimo de un encabezado de IPv4. El campo de servicios diferenciados, que se utiliza para la prioridad de paquetes y es útil para aplicaciones como voz sobre IP. La longitud total del paquete, el número de identificación, que se utiliza para realizar la fragmentación. Los indicadores, puede ver que el bit DF se ha configurado. qué significa "don't fragment." Este paquete no es lo suficientemente grande o no es identificado para fragmentación. Un desplazamiento de fragmentos, TTL, o tiempo de duración que se establece en 128. Cada vez que un paquete se enruta desde un salto al siguiente, se reduce la cantidad de TTL. Cuando el número de TTL llega a 0, el paquete se descarta. y garantiza que los paquetes no circulen en Internet para siempre en un bucle infinito. El valor TTL también es compatible con las rutas de rastreo de ICMP y pings. El campo de protocolo nos permite conocer el tipo de información para esperar en la porción de datos del paquete. un 6 identifica la porción de datos de este paquete como un paquete TCP. El campo de checksum del encabezado, que le permite a los routers revisar para ver si existe algún error o falta de uniformidad en el encabezado IP. Si existiera, el paquete se descartará.

Y luego, por último, las direcciones IP de origen y de destino, que son la parte más importante de paquete IPV4. Veamos dos capturas de pantalla más de captura de paquetes de Wireshark, y veremos algunas similitudes y diferencias. La próxima captura de pantalla nos muestra que ahora miramos el octavo paquete que se capturó. La dirección IP de origen del paquete también es 192.188.1.109, y la dirección IP de destino es 192.168.1.1 excepto este paquete es una solicitud HTTP GET. Así que esta es una solicitud a un servidor Web ubicada en 192.168.1.1. Pueden ver que la capa de red, o información de la capa de Internet, se ha expandido, que también es el protocolo de IP versión 4, y que tenemos información similar en los campos diferentes.

Noten bajo el campo de longitud total que este paquete es de 411 bytes, en comparación con el paquete anterior, que solo era de 52 bytes. Podemos decir que este paquete tiene mucho más información, o es un paquete mucho más grande, que el anterior. Si examinamos a continuación la información de Protocolo de Internet versión 4, podemos ver la información de TCP y luego debajo hay un protocolo de transporte de hipertexto, o protocolo HTTP, información de este paquete también. Me trasladaré hacia el próximo paquete, y podrá ver que este paquete es el 16to paquete capturado aquí. También es de host 192.168.1.109 al host 192.168.1.1, excepto esto es el protocolo ICMP. Puede ver la información en la ventana de la lista de paquetes que esto en una solicitud de eco, o ping. Si vemos la información de Protocolo de Internet versión 4 en el área de detalles, podemos ver algunas diferencias menores. La versión todavía es la 4. La longitud del encabezado sigue siendo 20 bytes. Pero podemos observar que los indicadores son levemente diferentes y que el campo de protocolo ahora está establecido en 1, que indica que la porción de datos de este paquete es un mensaje del protocolo ICMP. Observe que en la ventana de detalles en la parte inferior hay un área extendida para ver la información del encabezado específico del ICMP.