# Encapsulación TCP/IP

Transcribed on July 12, 2025 at 9:27 AM by Minutes AI

Speaker 1 (00:19)

Bienvenidos a esta nueva sesión donde vamos a tratar el concepto de encapsulación.

En esta sesión, aparte de saber qué es la Encapsulación del Tráfico de red, vamos a hablar de las capas Tcpip en función de lo que ya hemos visto en otras sesiones y vamos a analizar ese encapsulamiento desde ese tipo de arquitectura.

Es importante para la parte de ciberseguridad conocer bien la arquitectura Tcpip porque ya veréis como más adelante la parte de escaneos de red, la parte de numeración, hace mucho uso de los diferentes protocolos de red, las diferentes capas.

Cada uno de estos protocolos de red y cada una de estas capas de la arquitectura tcpp nos puede dar mucha información sobre puertos abiertos, sobre servicios que podemos identificar, sobre versiones de aplicaciones que se ejecutan detrás de un puerto, saber qué máquinas existen en la red, sobre versiones de aplicaciones que se ejecutan detrás de un puerto, saber qué máquinas existen en la red, qué máquinas están despiertas o están vivas.

Entonces toda esta información es importante y se va conociendo a través de los diferentes protocolos que forman una arquitectura de red, como en este caso es la que estamos trabajando, que es TCP IP.

También veremos un ejemplo de encapsulación dentro del Modelo, dentro de la arquitectura TCPip, el cual nos va a ayudar a entender bien el concepto de encapsulación y la importancia que tiene que tiene este concepto.

Además vamos a fortificar también el conocimiento.

Tenemos unas capas dentro, unos niveles dentro de una arquitectura de red y esos niveles tienen unas funciones muy concretas que ya hemos estado viendo.

Estos niveles nos aportan unas funciones.

Vamos a ver con el encapsulamiento cómo cada uno se encarga de hacer sus funciones y va delegando luego ciertos datos al nivel inferior o vamos obteniendo los datos hacia el nivel superior.

Iremos viendo después en el ejemplo para entender esto bien.

¿Qué es la encapsulación?

Bueno, pues al final la encapsulación es el proceso en el cual los datos se van embebiendo en capas inferiores dentro de una arquitectura de red con el objetivo de que se conforme una trama de red que al final estará compuesto por todos los niveles de la arquitectura tcbp y los datos saldrán de nuestro equipo en busca de la máquina de destino para que puedan ser interpretados cuando lleguen allí.

Para entenderlo bien podemos decir que para poner un ejemplo, decimos que queremos enviar datos desde una aplicación, desde una máquina a hacia una aplicación que se encuentra en la máquina B.

Fijaos que hablamos de aplicaciones, podría ser un ejemplo real, podría ser una aplicación que se encuentra en la máquina A, podría ser el navegador 1 aplicación que se encuentra en la máquina B, podría ser perfectamente un servidor web, que tiene aplicaciones web.

Si os fijáis, cada uno de esos extremos trabajaría en el nivel de aplicación.

Dentro de la arquitectura de CP eso es importante porque al final se trabaja entre pares.

Los datos se van encapsulando en niveles inferiores, es decir, de los datos que queremos hacer la petición desde el navegador hasta la máquina b, tenemos que nuestro proceso va a coger esos datos, utiliza un protocolo de aplicación, ese protocolo de aplicación se va a encapsular en el nivel inferior que sería capa de transporte, tcp o protocolo que sea, pero lo encapsula, es decir, cuando el usuario de la aplicación de la máquina le da a enviar un mensaje o le hace la petición al servidor web o a la aplicación que sea, estos datos se encapsularán en el nivel superior, se ponen las cabeceras y se pasa al nivel inferior que será el protocolo de transporte.

Cuando el usuario de la aplicación de la máquina le da a enviar un mensaje, esos datos se encapsulan como hemos dicho.

¿Qué ocurre después?

La capa de transporte recoge esa información, hemos dicho, y luego cuando la capa de transporte datos llegan a nivel transporte, la capa de transporte meterá sus cabeceras, encapsularán en el siguiente nivel que es el nivel de red.

Si os fijáis estamos preparando todo, al final la capa de transporte, si recordáis, lo que hace es cuando reciba las respuestas, tienen que dirigirse a ese puerto para que yo sepa qué proceso es al que le debemos enviar esta información, se añaden cabeceras al nivel de transporte y se pasa al nivel inferior, es decir, a nivel de red.

El nivel de red también hará lo mismo.

Yo de que me encargo de hacer direccionamiento lógico, acordaros de enviar los paquetes a las direcciones IP que deben ser.

Bueno, pues el nivel de red lo que va a hacer es añadir sus cabeceras también con sus ip origen, ip destino, sus campos del protocolo ip y pasará ese datagrama, lo pasará al nivel inferior que es el nivel de enlace.

Y bueno, el enlace lo que va a hacer es enviar, añadir sus caracteres también y enviarlo, pero en el enlace acordaros que trabaja solamente en red local, con lo cual enviará como mucho al router y el router ya luego se encargará de hacer ese reenvío.

Cuando los datos llegan por Internet, llegan al destino, llegan a la máquina b, esta máquina lo va a recibir a través de su email de enlace con su router que sea, han ido pasando entre routers por Internet y ha llegado al destino.

El nivel de enlace de la máquina b va a desencapsular, va a hacer el proceso contrario, es decir, me llega a una trama ethernet miro el campo datos, cojo el campo datos y se lo paso al nivel superior, es decir, estoy quitando las cabeceras, el nivel superior, que es el nivel de red, recoge esos datos y vale, estos datos son mi datagrama y empiezo a analizar las cabeceras y se lo paso a nivel superior que será el nivel de transporte.

En el nivel de transporte dice vale, estas son mis cabeceras, tengo un campo de datos que lo que han encapsulado dentro de ese campo de datos de TCP es el protocolo de aplicación, por lo cual lo desencapsulo y se lo paso hacia arriba y acaba llegando al proceso del servidor web.

De esto vamos a ver un ejemplo, después cuento, aquí tenéis todo resumido en la slide, en la transparencia, pero vamos a hacer un ejemplo después.

Pero antes de hacer el ejemplo tenemos que recordar un poco los diferentes niveles.

Entonces fijaros, al final la encapsulación es el proceso en el cual desde el nivel de aplicación se va encapsulando los datos a niveles inferiores.

La capa de transporte será más grande que la capa de aplicación, la capa de red será más bytes que la capa de transporte porque están capturando en el campo de datos de la capa de red transporte y el enlace será la trama de enlace, la trama de ethernet es la que más ocupa porque tiene encapsulado todos los protocolos por arriba y el desencapsamiento es el proceso contrario, es decir, una vez que llega al destino tenemos que ir quitando capas hasta tener los datos que estamos enviando en el nivel de aplicación y se le llega, se le envía ya al proceso que tiene que procesar la información.

Vamos a ver un ejemplo de esto que es bastante interesante.

Una vez que lo hemos explicado de forma teórica para entenderlo bien, vamos a ver un pequeño ejemplo donde vamos a trabajar con estos conceptos.

Tenemos los datos, nosotros hacemos nuestra petición desde el navegador, por ejemplo, eso genera una petición get HTTP para visualizar un recurso en un servidor web, donde sea eso generamos datos y tenemos nuestro proceso utiliza un protocolo que al final puede ser HTTP, tenemos unas cabeceras, tenemos los datos que queremos enviar.

Lo que va a hacer el sistema operativo es esto, se va a encapsular dentro de la capa de transporte.

¿Qué capa de transporte va a utilizar el protocolo HTTP?

En este caso pues tcp, pero habrá otros protocolos de aplicación que utilizarán otra capa de transporte que puede ser UDP.

Bien, tenemos la capa de transporte, tenemos los datos, si os fijáis la parte de datos engloba la parte cabeceras y datos del protocolo superior, la capa superior, la capa de transporte, lo que es añadir cabeceras, en esas cabeceras recordad puerto origen, puerto destino, los flags de tcp en el caso de que sea tcp son cabeceras tcp, luego se encapsularía en la capa de red que es la que se encarga del direccionamiento, de conseguir crear, conseguir enviar ese paquete fuera de nuestra red, la que se encarga de direccionamiento lógico.

Bien, pues si os fijáis el campo de datos del datagrama IP en este caso coincide con las cabeceras y el parte de datos de la capa de transporte se encapsula ahí y en el nivel de red le metemos en cabeceras de origen y de destino, como comentaba antes y se encapsula en la parte datos de la trama ethernet del nivel del Nassim.

Tenemos cabeceras dirección Mac o dirección física origen, dirección Mac destino, que será una máquina de la red o el propio router que está en una red.

Si queremos enviar el paquete, la trama de red fuera de nuestra red, se lo enviamos al router de nuestra red y el router ya se encargará de ir enrutandolo por los diferentes routers de Internet hasta que llegue al destino.

¿Qué ocurre?

Esto al final, esto es lo que enviamos a nuestro router y esto el router se encargará de hacer el enrutamiento hacia el destino.

Bien, el router fijaros que coge las cabeceras de la trama del nivel de enlace, analiza, eso es para mí, cojo la parte de datos y fijaros que la descompone porque el router trabaja a nivel de red, necesita ver cuál es la ip destino de este paquete para poder enrutarlo.

Ese momento pues ya lo puede enrutar, lee esa información, no desencapsula nunca más allá de la capa de red, el router trabaja a nivel de red, no desencapsula por encima y ese paquete lo acaba enviando.

Bien, vamos a pasar ahora a lo que ocurre.

El router, hemos dicho que esto lo enruta y vamos a ver qué ocurre.

Tenemos el paquete de red, lo vamos a trabajar encapsular dentro de un paquete de enlace, el router lo mandará, ha llegado a este router, lo mandará dentro de su red al destino y entonces empezamos a desencapsar ese proceso contrario al encapsulamiento, cogemos el nivel de enlace, quitamos las cabeceras y le pasamos el campo datos al nivel superior, nivel de red.

Lo mismo hace el nivel de red con el nivel de transporte, fijaos, y el nivel de transporte lo mismo con el nivel de aplicación y al final los datos acaban llegando al proceso a quien estamos haciendo la solicitud.

En este caso, por ejemplo, un servidor web, como hemos puesto como ejemplo web, le da esto, me hacen un get a un recurso, bien, responderé y ocurre de nuevo, encapsulo tal, lo envío por red, llega al destino, se capsula y así.

Esta es la fuerza de una arquitectura de red.

Tenemos segmentadas las capas de forma que es muy sencillo saber de qué se encarga cada capa y estamos haciendo que el proceso sea más sencillo, sea más liviano y cada caspa sepa muy bien lo que tiene que hacer y eso simplifica la complejidad que pueda tener este proceso.

Bien, como conclusiones de esta sesión, hemos visto el concepto de encapsulación, es un concepto bastante importante dentro de arquitectura de red, dentro de la arquitectura TCPP, dentro de las arquitecturas por capas, es muy importante entenderlo, cómo funciona el encapsulamiento hacia el envío de paquetes y la recepción de paquetes, cómo procesamos un desencapsamiento para un proceso contrario, para poder analizar la información y este es el juego.

Y luego en los routers al final solamente desencapsulan o encapsulan desde el nivel de red o hasta el nivel de red o desde el nivel de red en el caso.

Hemos visto también un poco el resumen otra vez de la arquitectura tcp ip y cómo el proceso de encapsulamiento aplica sobre esta arquitectura y hemos visto un ejemplo full duplex, es decir, hemos visto cómo se hace el encasulamiento desde que no nosotros, un proceso de nuestra máquina quiere enviar algo por red hasta que llegas al destino.

Cuando llega al destino se hace el desencadenamiento y cómo va funcionando las capas.

Esto con herramientas como Wireshark se puede ver muy bien cuando enviamos o cuando llegan paquetes a nuestra máquina o enviamos paquetes desde nuestra máquina, se puede ver muy bien las capas que existen en los paquetes de red, los diferentes protocolos, los diferentes niveles.

Entonces es algo que tenemos que asentar, tenemos que conocer bien la parte de arquitectura de red, tenemos que conocer bien los protocolos, porque como digo, cuando empecemos a trabajar con escaneos de red, con ciertas vulnerabilidades, va a ser importante ciertos ataques de red, va a ser importante todo el conocimiento dentro de la parte de protocolos de funcionamiento de la arquitectura.

Bien, pues con esto llegamos al final de la sesión.

Nos vemos en la siguiente sesión.