Comprensión de RADIUS MTU y fragmentación en 9800 WLC

Contenido

Introducción

Este documento describe cómo configurar la MTU de los paquetes RADIUS que el WLC envía al servidor RADIUS.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre estos temas:

- Configuración AAA del controlador LAN inalámbrico (WLC) 9800
- Conceptos RADIUS de autenticación, autorización y administración de cuentas (AAA)
- EAP de protocolo de autenticación extensible
- Unidad de transmisión máxima (MTU)

Componentes Utilizados

- Cisco Identity Service Engineer (ISE) 3.2
- Controlador inalámbrico Catalyst serie 9800 (Catalyst 9800-L)
- Cisco IOS® XE 17.15.2
- Cliente inalámbrico Windows 11

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

A efectos de este documento, se utiliza el servidor RADIUS (Servicio de autenticación remota telefónica de usuario) de Cisco ISE. En primer lugar, se demuestra cómo fluirían los paquetes sin ninguna intervención externa durante el proceso del protocolo de autenticación extensible (EAP). A continuación se encuentra la opción de configuración para cambiar el tamaño de la solicitud de acceso que el WLC envía a cualquier servidor RADIUS. Esta opción se agregó en la versión 17.11 de IOS-XE.

MTU RADIUS 9800

Por lo general, la MTU de los paquetes RADIUS no importa, ya que son típicamente pequeños y no llegan a la MTU de todos modos. Sin embargo, cuando un lado tiene que enviar un certificado, que generalmente es de 2-5 KB, el dispositivo necesita fragmentar ese certificado para obtenerlo bajo su MTU.

Cuando el cliente tiene que enviar un certificado al servidor RADIUS, como es el caso con EAP Transport Layer Security (EAP-TLS), presenta el WLC con una situación donde el paquete necesita ser fragmentado nuevamente debido a la cantidad de datos RADIUS que se tiene que enviar con él. Hasta la 17.11, el administrador de la red tenía poco control sobre este proceso, pero ahora los ingenieros tienen la opción de manipular el tamaño de la solicitud de acceso enviada por el WLC.

Flujo de paquetes EAP-TLS

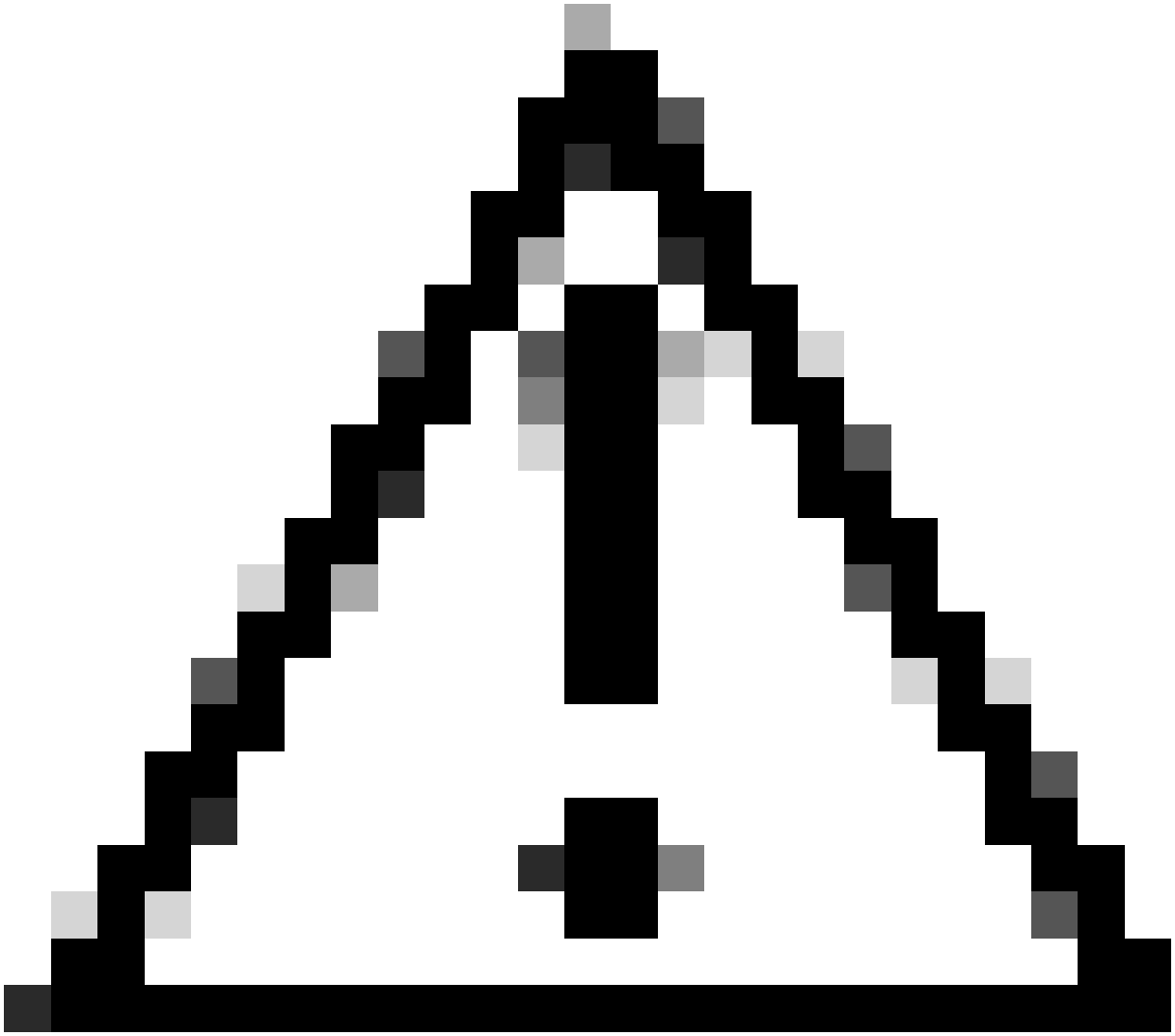
Se trata de una profundización en el aspecto de los paquetes y cómo los trata la infraestructura inalámbrica. Para que se comprendan completamente los cambios introducidos en este

documento, es importante conocer el flujo de paquetes durante el proceso de autenticación inalámbrica cuando se utiliza dot1x y, más específicamente, EAP-TLS.

Si ya tiene un conocimiento profundo de cómo funciona el flujo de paquetes EAP y RADIUS en la infraestructura inalámbrica de Cisco, pase a la sección de cambio de comportamiento que explica lo que se agregó en 17.11, lo que le da a los administradores de red un mayor control sobre la MTU RADIUS. En primer lugar, eche un vistazo a EAP Identification (EAP-ID).

EAP-ID

El autenticador inicia el EAP-ID, en este caso el WLC. Esta debe ser la primera parte del proceso EAP. A veces, el cliente inalámbrico envía un EAPOL-Start. Esto normalmente significa que el cliente nunca recibió la solicitud de EAP-ID o que quiere empezar de nuevo.



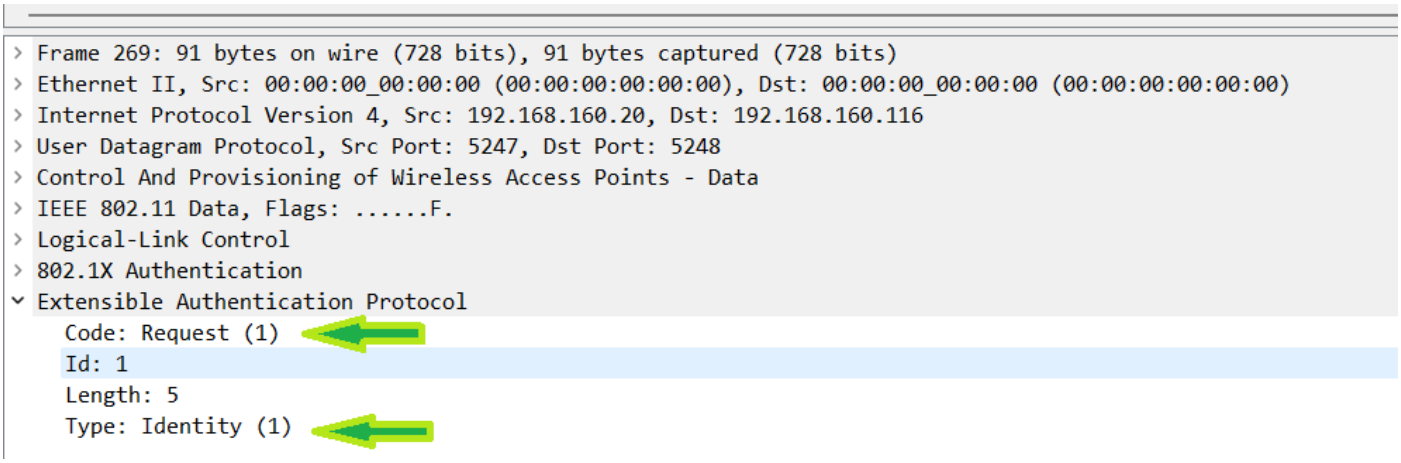
Precaución: Existe una diferencia entre el paquete EAP-ID y el ID de paquete EAP. El paquete EAP-ID se utiliza para identificar al solicitante, donde el ID de paquete EAP es un número utilizado para rastrear el paquete específico a medida que se mueve a través de la red.

Solicitud EAP-ID

En primer lugar, el dispositivo cliente inalámbrico se conecta a la red mediante el proceso de asociación normal. Cuando la red de área local inalámbrica (WLAN) se configura para dot1x, el WLC primero necesita saber quién es el cliente antes de que pueda solicitar el acceso del servidor RADIUS. Para encontrar esta información el WLC envía el cliente y la solicitud de EAP-ID.

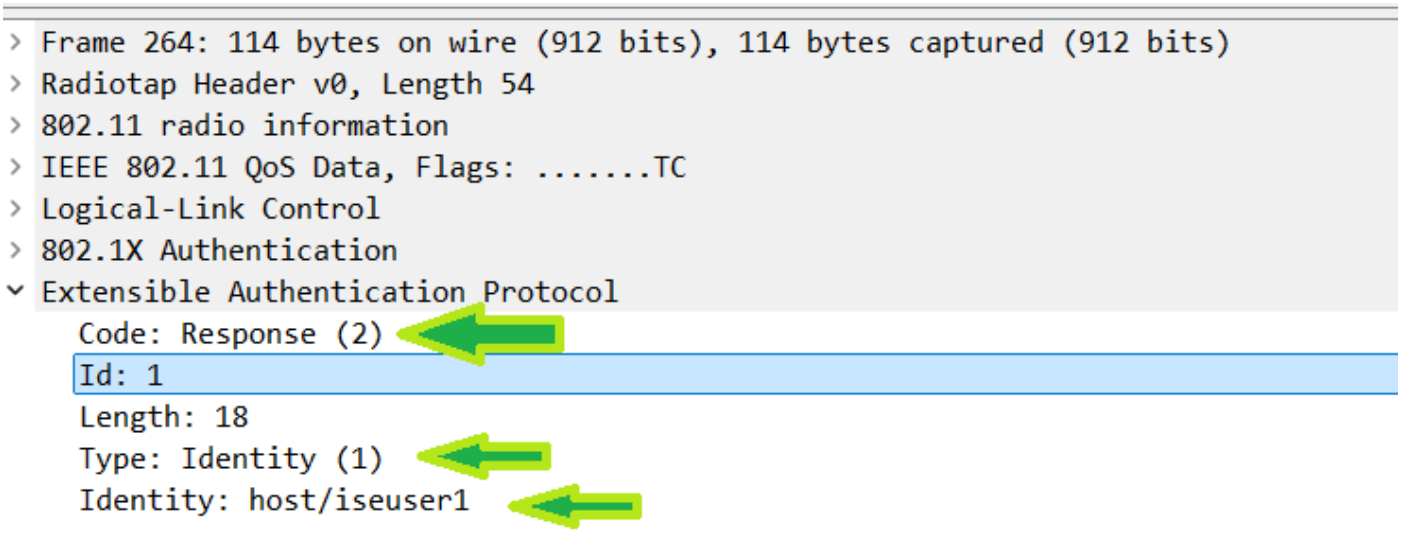
Se espera que el cliente responda con la respuesta EAP-ID. Esto le da al WLC lo que necesita para poder construir la solicitud de acceso y enviarla al ISE. La solicitud EAP-ID es cuando se le solicitaría al cliente que pusiera su nombre de usuario y contraseña en una autenticación PEAP normal.

Sin embargo, esta conversación gira en torno a EAP-TLS, por lo que la respuesta EAP-ID aquí solo tendría el ID de usuario. En la demostración, el ID de usuario es iseuser1. En este paquete, puede ver la solicitud EAP-ID que el WLC envía al cliente inalámbrico preguntando quiénes son. Dado que este es un cliente inalámbrico, el WLC encapsula la solicitud en CAPWAP y la envía al punto de acceso (AP) para ser enviada por el aire. En los datos EAP, el código 1 indica que se trata de una solicitud y el tipo 1 indica que es para la identidad.



Respuesta EAP-ID

A continuación, se espera que el cliente inalámbrico responda con la respuesta EAP-ID. En los datos EAP, el código ha cambiado a 2, lo que significa que es una respuesta, pero el tipo permanece como 1, mostrando que es para la identidad. Aquí, incluso puede ver el nombre de usuario que el cliente está utilizando. Una cosa más para verificar en estos paquetes es el número de identificación del paquete EAP. Para el intercambio de EAP-ID siempre es 1, pero este número cambia posteriormente a otro cuando ISE se involucra.



Puede ver que ambos paquetes son bastante pequeños, por lo que la MTU no tiene relación aquí ya que está muy por debajo de los 1500 bytes utilizados en la red.

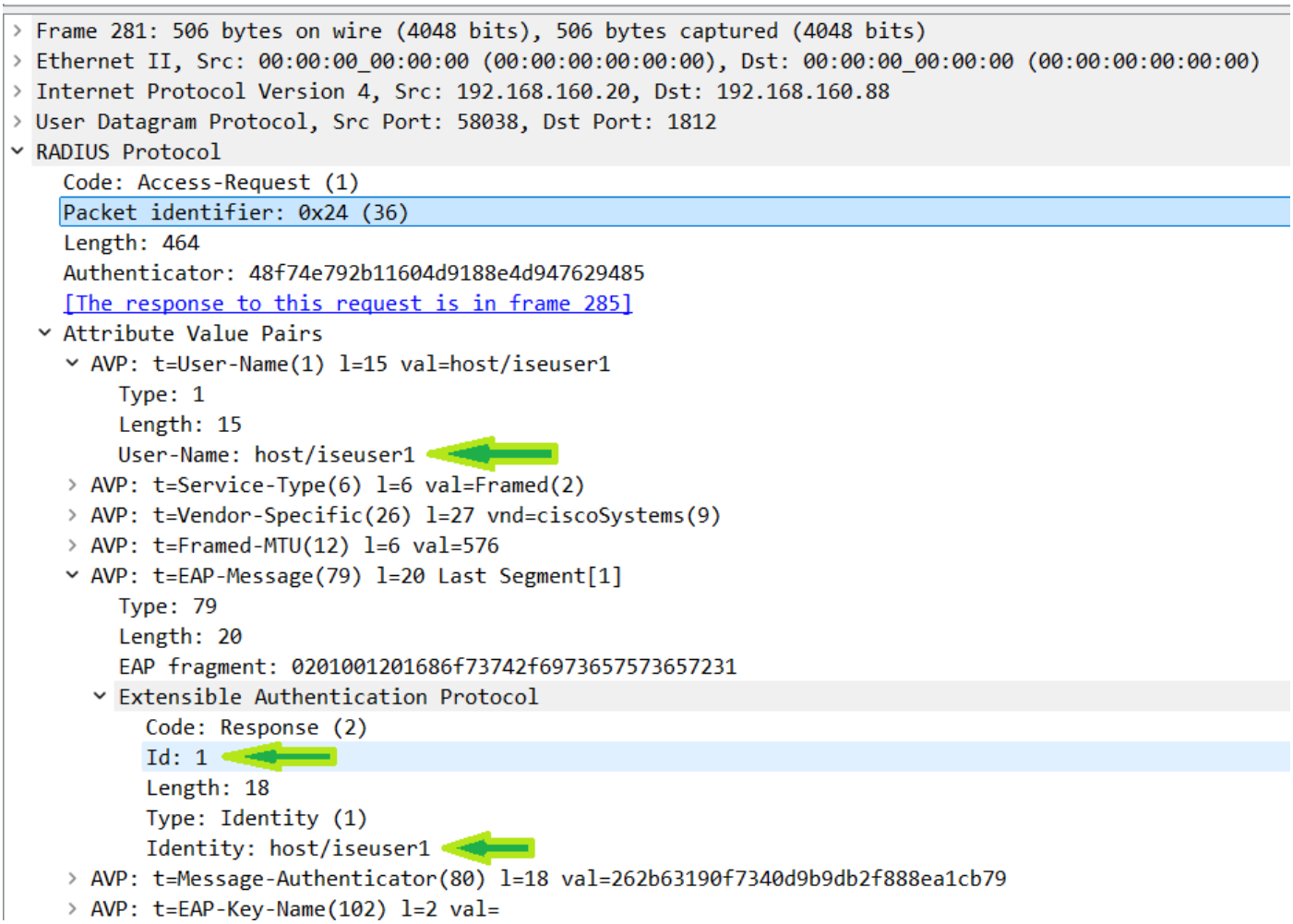
Access-Request y Access-Challenge

La comunicación con el cliente es EAP y la comunicación entre el WLC e ISE es RADIUS. Para la comunicación RADIUS se utilizan los paquetes de solicitud de acceso y desafío de acceso. El WLC recibe el paquete EAP del suplicante y lo reenvía a ISE mediante la solicitud de acceso RADIUS. En una red en funcionamiento, ISE respondería con un desafío de acceso.

Solicitud de acceso

Ahora que el WLC sabe la identidad del cliente, necesita preguntar al servidor RADIUS si ese cliente está permitido en la red. Para hacer eso, el WLC solicita el acceso para ese cliente enviando el paquete access-request. Hay otros pedazos de datos que el WLC va a enviar junto con los datos EAP. Colectivamente éstos se llaman pares del valor del atributo, AVPs, o pares AV dependiendo de quién está hablando.

Este documento no va a llegar lejos en los AVPs ya que eso está fuera del alcance de esta discusión. Aquí solo tiene que ver que el nombre de usuario (datos EAP) se incluye y se envía al servidor RADIUS, que, en este caso, es ISE. Además, puede ver que el número EAP-ID 1 también se envía a ISE. Recuerde que cuando miró el ID de paquete EAP por aire, también estaba 1. Lo último importante a tener en cuenta aquí es que desde que el WLC ha agregado todos estos AVP, el paquete de 114 bytes que el cliente envió ahora se convierte en un paquete de 488 bytes antes de ser enviado a ISE.

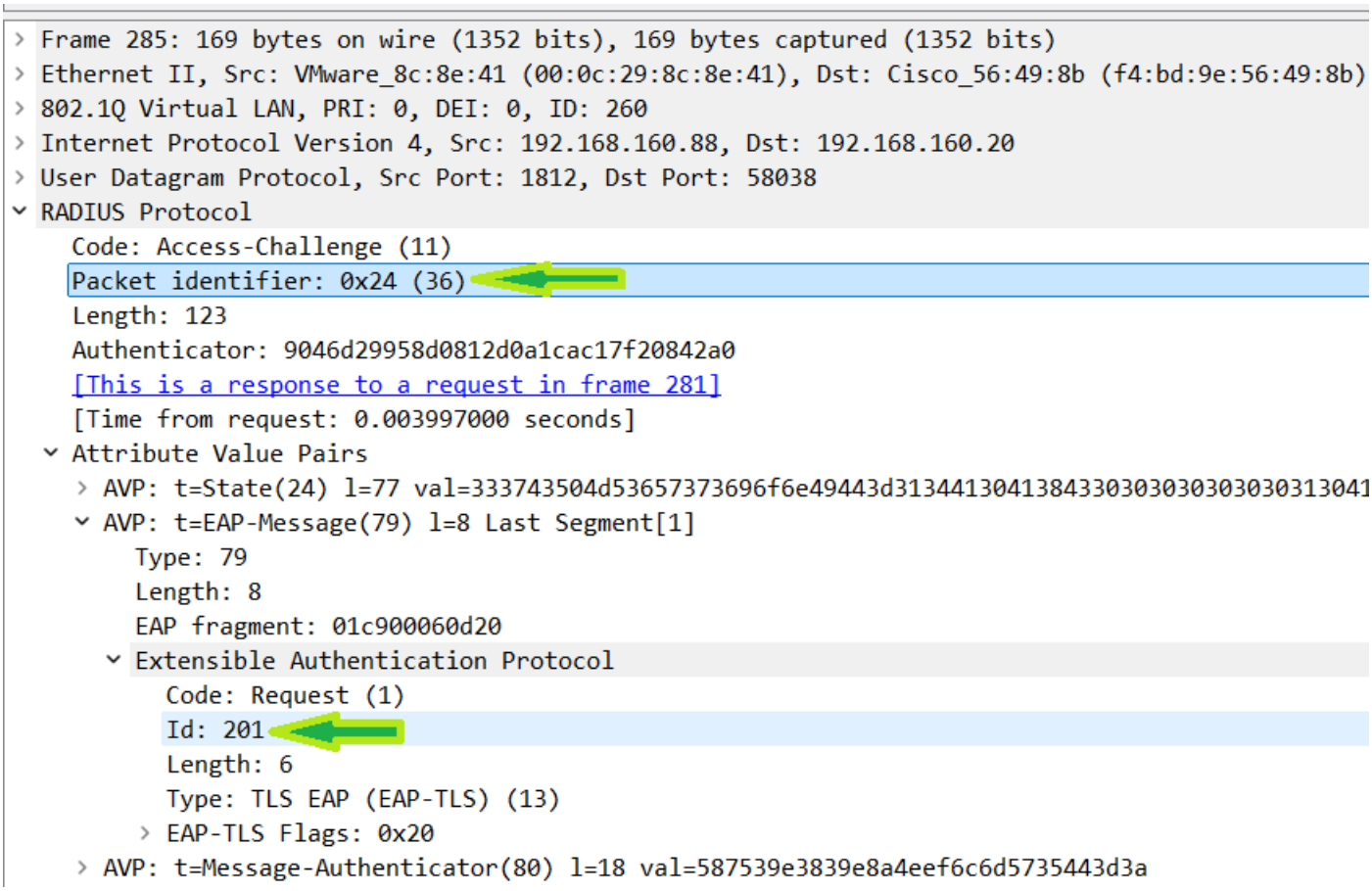


Acceso-Desafío

Suponiendo que ISE reciba la solicitud de acceso y decida responder, se espera que esta respuesta se produzca como un desafío de acceso de ISE. Si observa la solicitud de acceso, verá el ID de paquete RADIUS de 36 antes de que se inicien los AVP.

Cuando el WLC recibe el desafío de acceso, el ID de RADIUS debe coincidir con ese ID de paquete de la solicitud de acceso. El ID de paquete RADIUS es para la comunicación RADIUS entre ISE y el WLC. También puede ver en este paquete que ISE ha establecido un nuevo ID de EAP de 2010 que se utiliza para realizar un seguimiento de la comunicación entre ISE y el cliente. En este punto, el WLC es solo un paso a través para la comunicación entre ISE y el cliente.

Es importante tener en cuenta todos estos ID de paquete aquí para que pueda comprender el flujo de comunicación y cómo realizar un seguimiento de estos paquetes a través de la red. En un entorno de producción, normalmente se producen varias autenticaciones al mismo tiempo. Utilice el comando calling-station-id para hacer coincidir el paquete con la dirección MAC del cliente. A continuación, puede utilizar el ID de paquete RADIUS y el ID de paquete EAP para realizar un seguimiento del flujo de paquetes para este cliente específico. Hasta este momento, ninguna de las partes ha enviado ningún certificado, por lo que todavía no ha sido necesario preocuparse por la MTU.



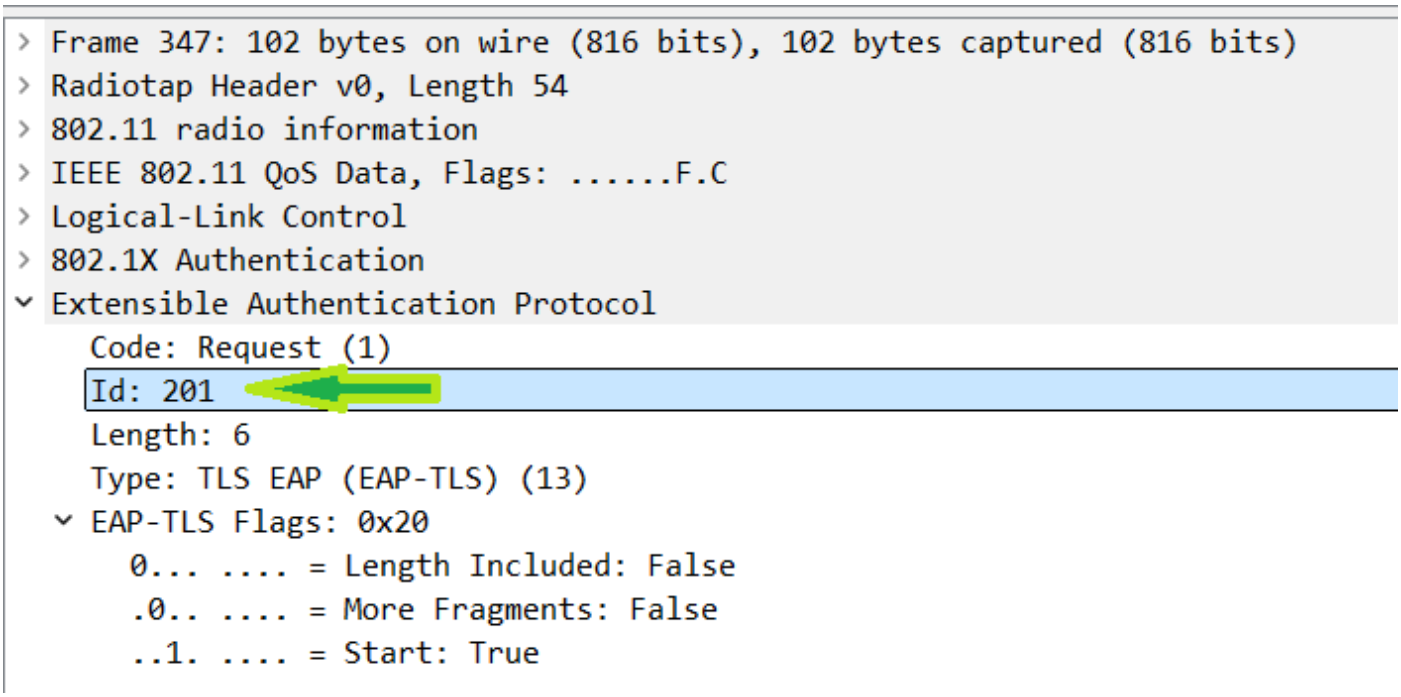
Solicitud EAP y respuesta EAP

Solo un recordatorio, el cliente habla EAP no RADIUS. Dicho esto, cuando el WLC recibe el desafío de acceso tiene que quitar los datos RADIUS y sacar la solicitud EAP para que pueda ser enviada al cliente.

Solicitud EAP

Esto debe verse exactamente como lo hizo dentro del desafío de acceso cuando el WLC lo recibió. Sin embargo, todo el material RADIUS se ha eliminado y sólo la parte EAP se envía al cliente.

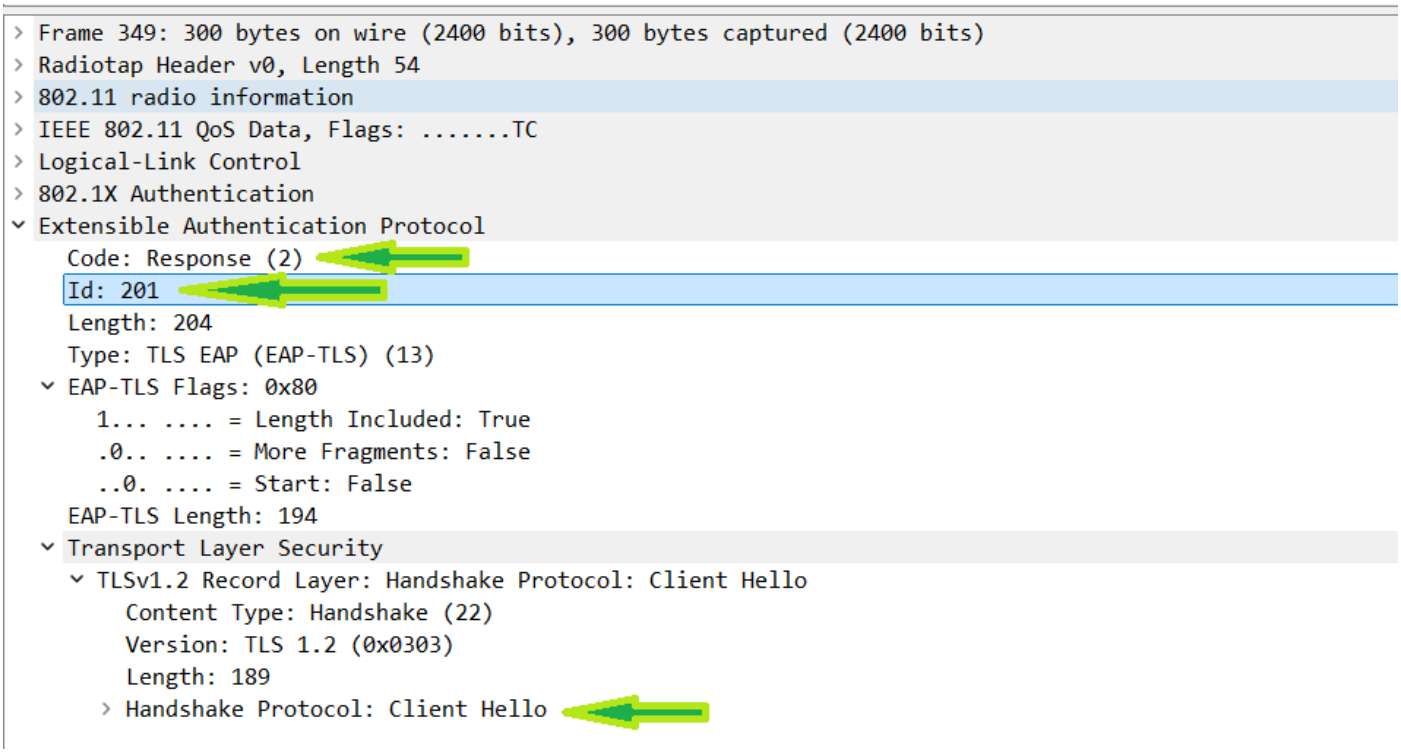
Todavía puede ver el ID de paquete EAP de 201 aquí tal como estaba en el desafío de acceso porque son los mismos datos que el WLC recibió de ISE. El flujo aquí es el mismo que con el EAP-ID, solo que ahora no viene del WLC y se utiliza para establecer el método EAP. Este paquete sigue siendo bastante pequeño porque es solo para establecer el inicio de una sesión EAP-TLS.



Respuesta EAP

Cuando el cliente recibe la solicitud EAP, debe responder con una respuesta EAP. En EAP-Response, el cliente comienza a establecer la sesión TLS. Esto se ve igual que en cualquier otra situación en la que se utilice TLS. Comienza con el mensaje de "saludo al cliente". Este documento no va a profundizar en lo que entra en el saludo del cliente, ya que es irrelevante para este tema. Lo que debe observar aquí es que se está configurando una sesión TLS.

Aquí puede ver los datos en los paquetes como lo haría con cualquier otra configuración de TLS. Al igual que con la respuesta EAP-ID, este paquete llega al WLC y se convierte en una solicitud de acceso. ISE responde con una solicitud de EAP empaquetada en un desafío de acceso. Este sigue siendo el flujo de ahora en adelante.



Certificados TLS

Este es el punto en el que observará un aumento en el tamaño de los paquetes. Los certificados pueden ser bastante grandes en función de la presencia de una o varias entidades emisoras de certificados intermedias (CA). Si se trata de un certificado autofirmado, obviamente sería más pequeño que un certificado con un certificado de dispositivo encadenado a 2 CA intermedias y una CA raíz. De cualquier manera, normalmente verá que el propietario del certificado comienza a fragmentar sus propios paquetes aquí.

Certificado ISE

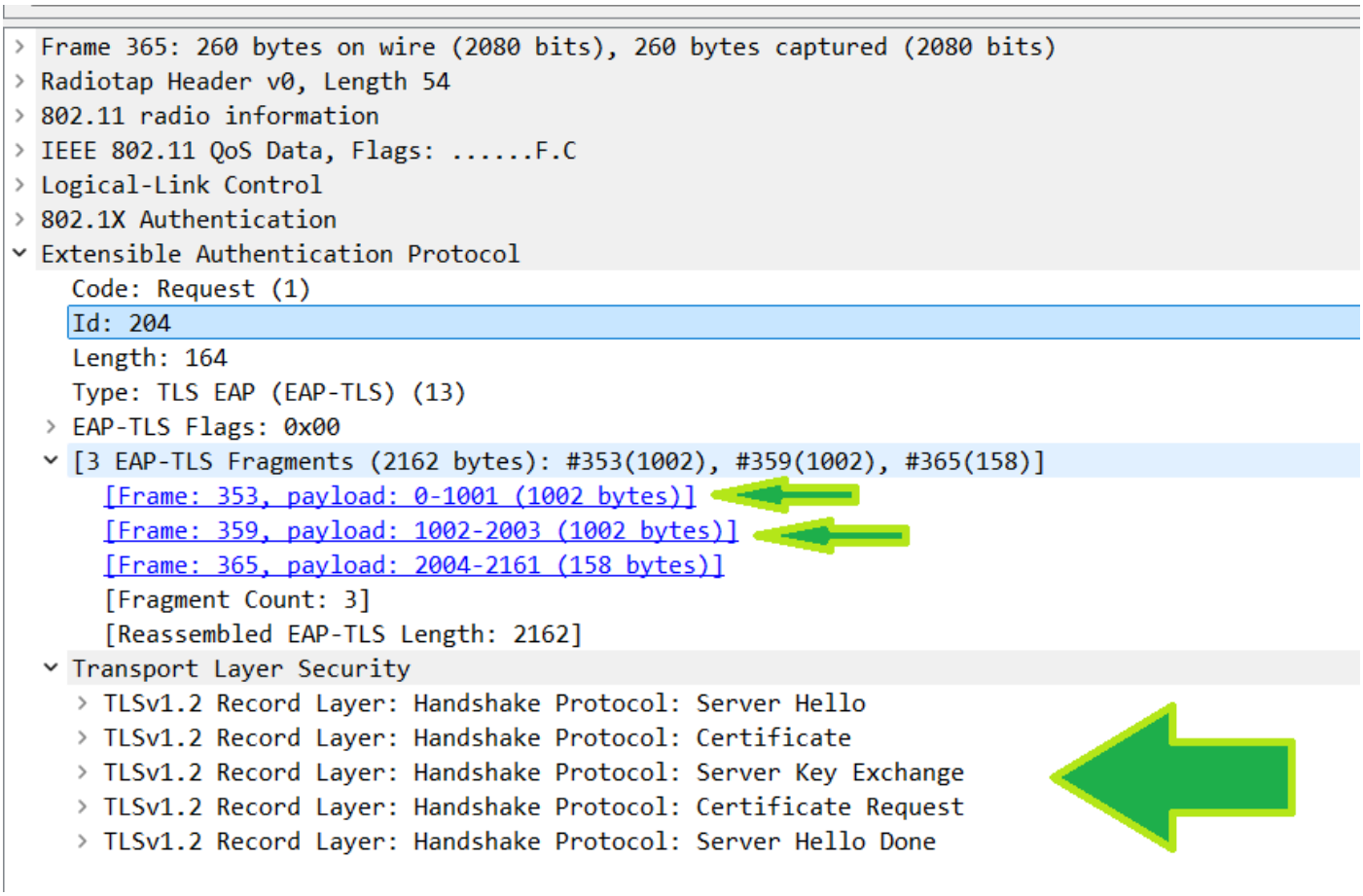
Ahora que ISE ha recibido el saludo del cliente TLS, responde con otra solicitud EAP. En esta nueva solicitud EAP, ISE envía el mensaje de "saludo al servidor", su certificado, los mensajes de "intercambio de claves del servidor", "solicitud de certificado" y "saludo del servidor finalizado" todos a la vez. Si enviara todo esto en un paquete, el paquete estaría sobre la MTU para la red. Por lo tanto, ISE fragmenta el paquete en sí mismo para colocarlo bajo la MTU. Con ISE, fragmenta la porción de datos del paquete para que no supere los 1002 bytes con la esperanza de evitar la doble fragmentación.

¿Qué se entiende por doble fragmentación? La primera fragmentación se produce en ISE, ya que los datos que desea enviar son demasiado grandes para caber en la MTU de la red. Sin embargo, puede haber otros lugares en la red donde, aunque la MTU sea la misma, debido a la configuración de la red, un dispositivo posiblemente necesite fragmentar el paquete para poder agregar sus encabezados y permanecer bajo la MTU. Esto puede ser verdadero incluso si se verifica el bit do not fragment.

Un buen ejemplo de esto es con un túnel VPN, o cualquier túnel para el caso. Para colocar datos en un túnel VPN, los routers VPN deben agregar sus encabezados al tráfico. Si este tráfico

RADIUS se fragmentara en o cerca de la MTU, cuando se trata de esta VPN no habría manera de mantener los datos bajo la MTU y agregar encabezados adicionales. Esto también se aplica a los túneles CAPWAP, que se pueden ver un poco más adelante.

Por lo tanto, para evitar que estos paquetes se encuentren en una situación en la que otro dispositivo pueda volver a fragmentarlos, ISE fragmenta el paquete en un lugar en el que esto se pueda evitar en la mayoría de las redes. Esto significa que ISE envía estos datos en varias solicitudes EAP en espera de una respuesta EAP vacía cada vez. El ID de EAP aumenta con cada fragmento enviado. Desde el punto de vista del WLC, esto sería un desafío de acceso e intercambio de solicitud de acceso para cada fragmento y el ID de paquete RADIUS aumentaría con cada fragmento enviado.



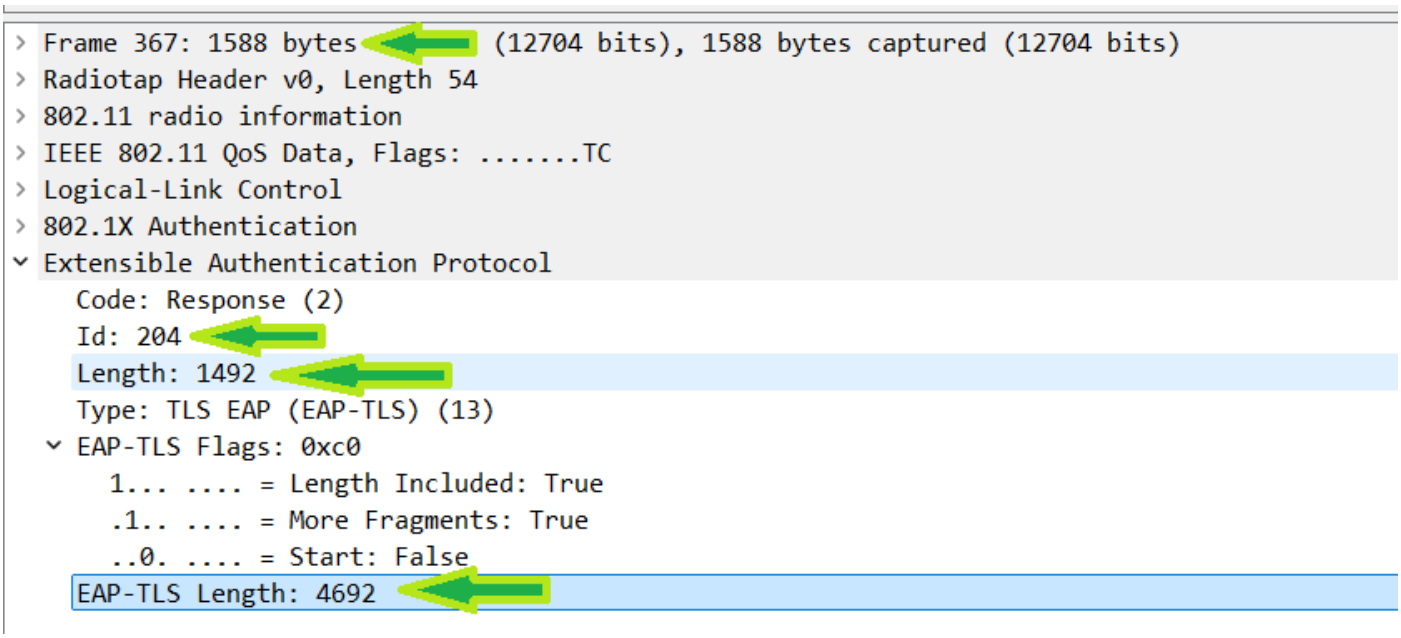
Certificado de cliente

Una vez que ISE envía todos los fragmentos y el cliente los reensambla, el flujo de paquetes pasa al cliente para enviar algo. En TLS se espera que el cliente envíe su propio certificado en este punto para completar la autenticación. Aquí es donde las cosas se vuelven más complejas. Al igual que ISE, el cliente va a enviar varias partes de TLS a la vez, una de las cuales es su certificado.

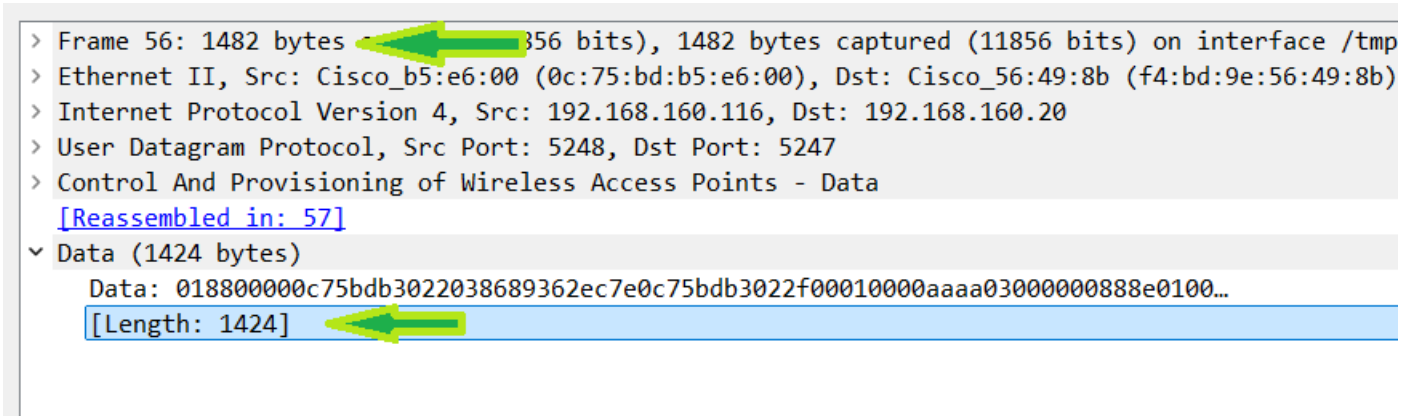
A diferencia de lo que se observó con ISE, la mayoría de los clientes envían sus datos EAP justo por debajo de la MTU. En esta demostración, los datos de 802.1x son 1492. El problema con eso es que el AP necesita agregar los encabezados CAPWAP para que se pueda enviar al WLC.

¿Cómo se puede hacer eso? El AP tendrá que fragmentar el paquete para que pueda agregar los encabezados y enviarlo al WLC. No hay manera para que el AP obtenga el paquete al WLC sin fragmentarlo. Dicho esto, aquí el paquete está fragmentado por partida doble, primero desde el cliente y luego nuevamente desde el AP. Sin embargo, esta fragmentación no suele ser un problema, ya que se espera que ocurra con CAPWAP.

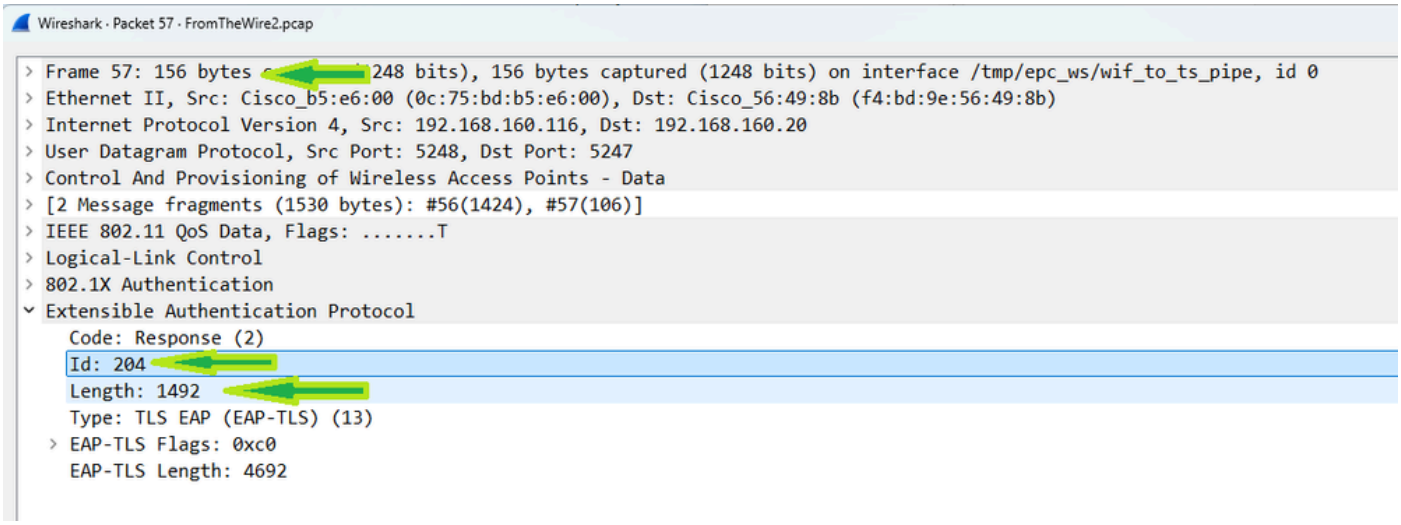
El paquete en el aire:



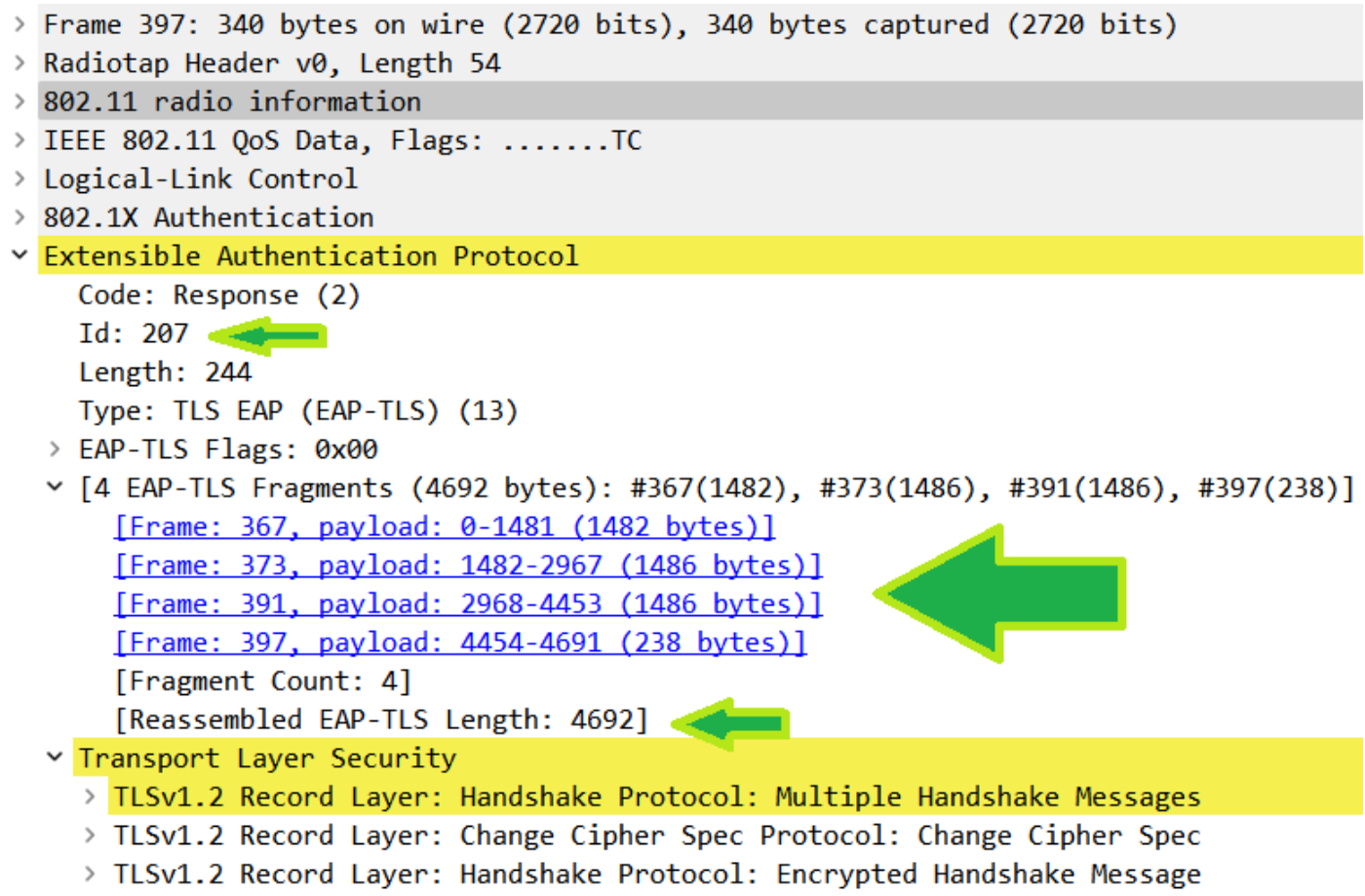
El fragmento de paquete en el cable:



El paquete reensamblado en el cable:



Todos los fragmentos de cliente reensamblados en el aire:



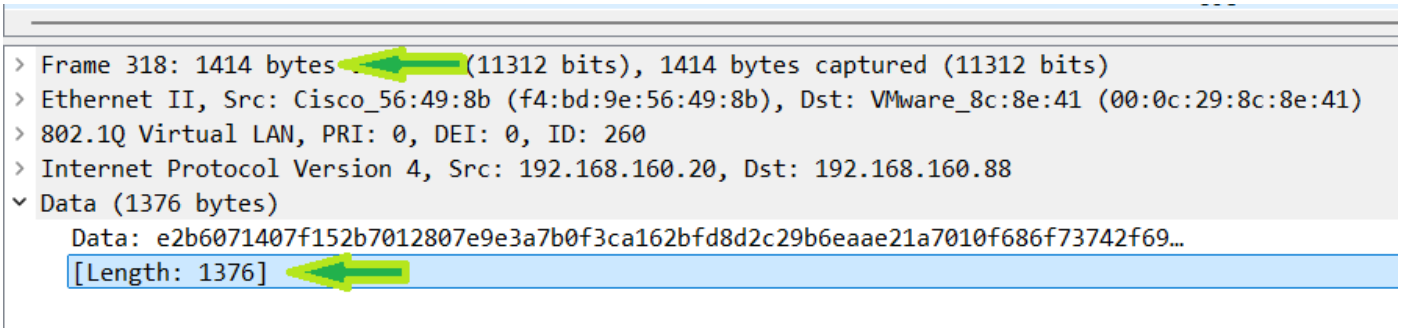
Certificado de cliente en el WLC

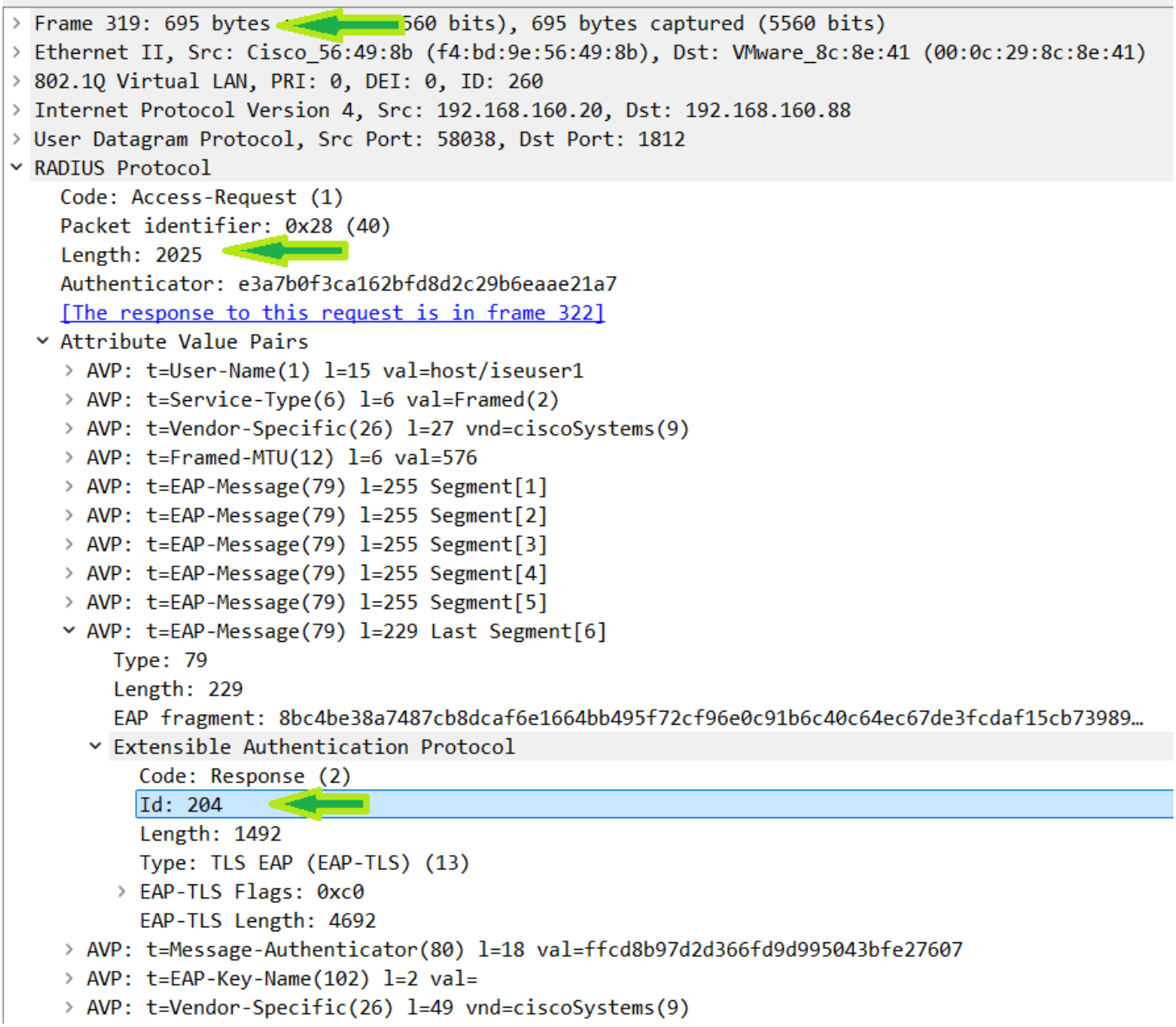
El WLC recibe los dos fragmentos CAPWAP y los reensambla para tener el paquete entero de 1492 bytes del cliente, restaurando el paquete - pero no por mucho tiempo. Esta restauración es de corta duración porque, si mira hacia atrás a cómo el WLC envía la solicitud de acceso, debe recordar que tiene que agregar alrededor de 400 bytes de AVP RADIUS al paquete antes de que pueda enviar los datos a ISE.

Para una matemática simple, suponga que el WLC agrega 408 bytes, llevando el tamaño total del paquete a 1900. Esto está muy por encima de la MTU 1500, así que ¿qué va a hacer el WLC? Fragmente el paquete de nuevo.

En este punto, el WLC va a fragmentar el paquete en 1396 de forma predeterminada. La idea aquí es la misma que con ISE. La esperanza es hacer que el paquete sea lo suficientemente pequeño para que si tiene que pasar por otro túnel, no tenga que ser fragmentado nuevamente para agregar los encabezados. Sin embargo, el WLC no es tan cauteloso como ISE así que 1396 es bastante bueno aquí.

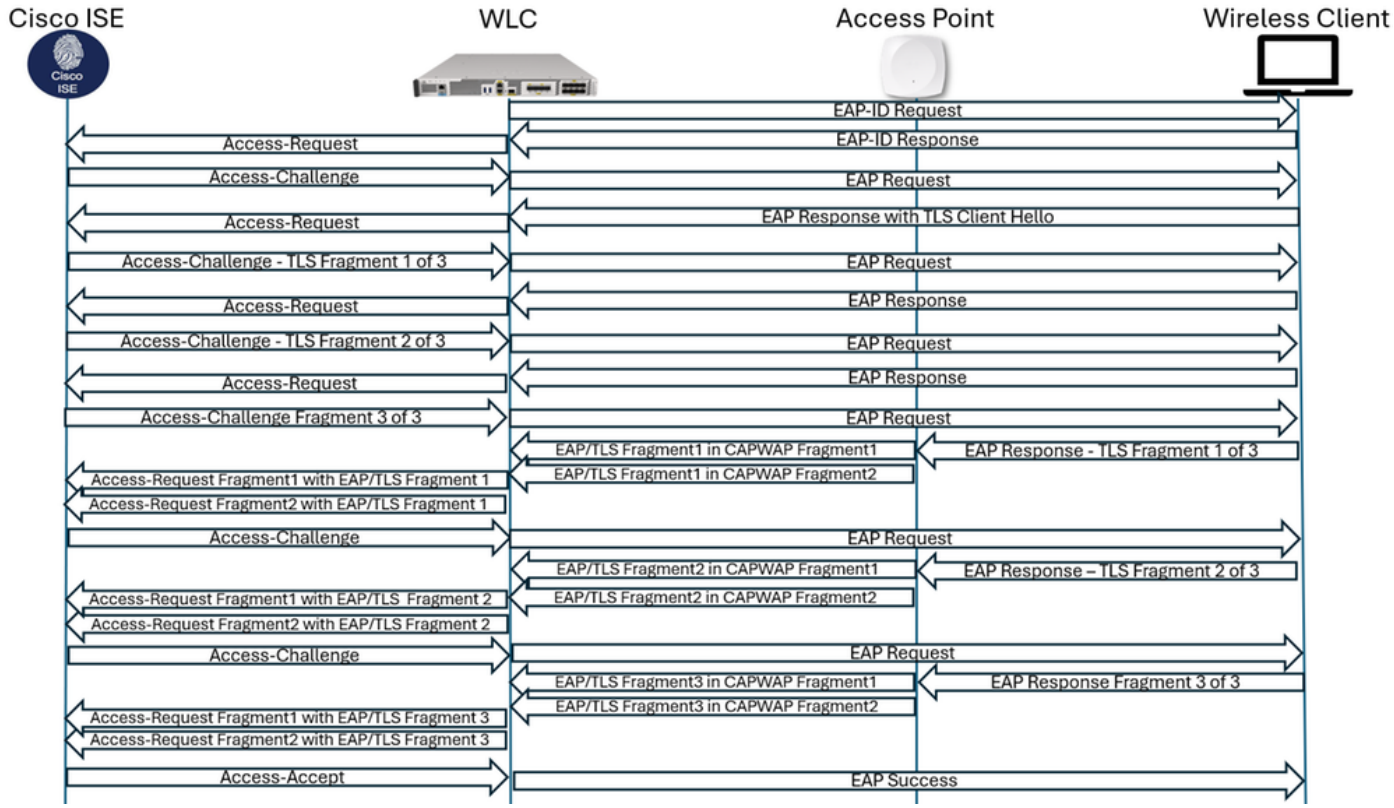
El paquete fragmentado que sale del WLC:





Flujo de paquetes TL;DR

Cuando ISE envía su certificado, fragmenta los paquetes TLS a 1002 bytes. No hay problemas allí. Cuando los clientes envían su certificado, normalmente se fragmentan cerca de la MTU. Dado que el AP tiene que agregar los encabezados CAPWAP al paquete, también tiene que fragmentar este paquete. Una vez que el WLc recibe los fragmentos, tiene que reensamblar el paquete pero luego tiene que agregar los AVP RADIUS para que el paquete se fragmente nuevamente. El flujo de paquetes es similar a lo siguiente:



Cambio de comportamiento de RADIUS MTU

Cuando observa el flujo de paquetes para cualquier tráfico de datos de clientes inalámbricos, puede ver que la infraestructura inalámbrica sólo tiene influencia sobre ella en unos pocos lugares. El primer lugar es cuando el tráfico deja el AP y el segundo lugar es cuando el tráfico deja el WLC. La excepción es con el tráfico TCP donde la infraestructura inalámbrica puede ajustar el MSS del cliente. Sin embargo, EAP no entra dentro de TCP, de hecho, es su propio protocolo.

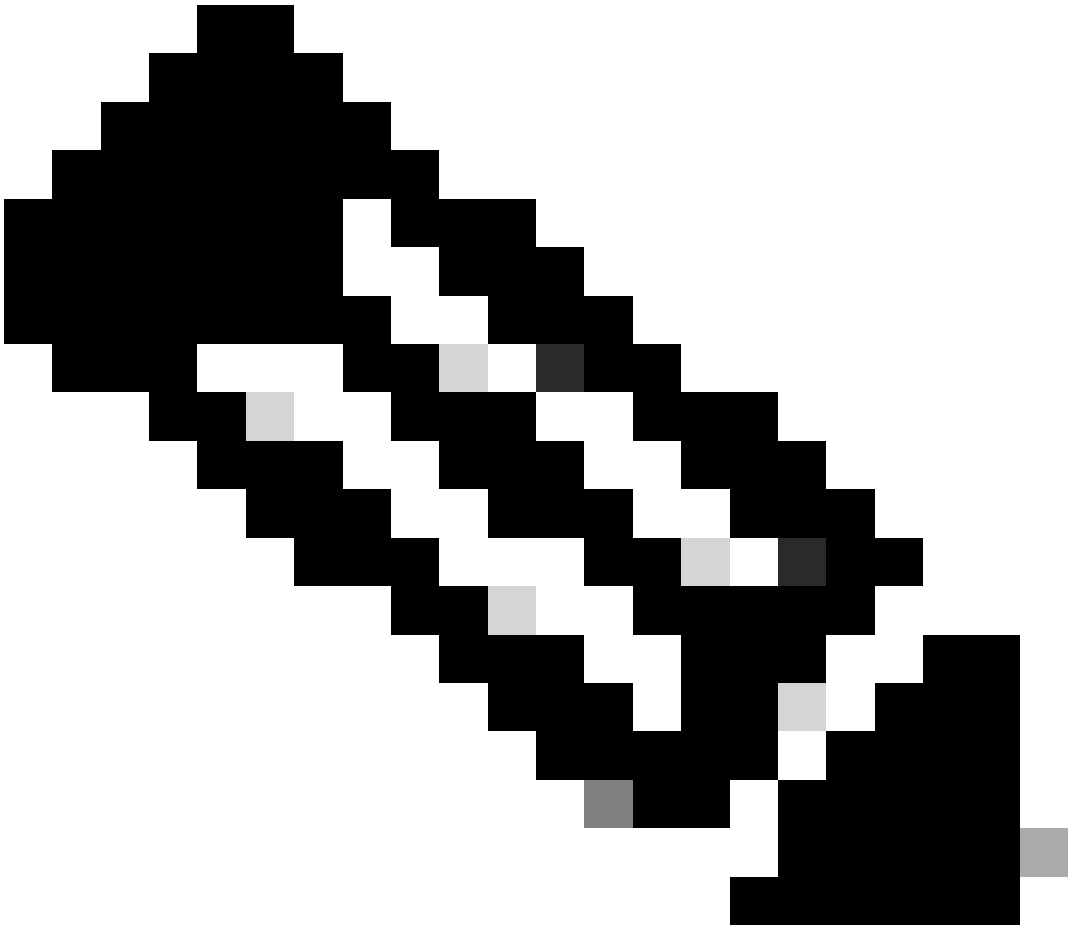
Cuando observa los flujos de tráfico EAP y RADIUS, también puede ver que la red realmente influye en el tamaño del tráfico tanto en el AP como en el WLC cuando el tamaño del paquete original se acerca demasiado a la MTU. Con una comprensión adecuada del papel del WLC en este intercambio, puede ver que hay realmente solo un lugar donde tiene influencia del tamaño del paquete RADIUS. Esto sería cuando llega una respuesta EAP y la cambia a una solicitud de acceso RADIUS.

Qué ha cambiado

Si la respuesta EAP se encuentra sobre la MTU, una vez que agregue los AVP RADIUS debe fragmentarlos. Dado que ya tiene que fragmentar este paquete sin importar qué, al menos puede decidir en qué tamaño desea fragmentarlo. Ahí es donde entra en juego el cambio de comportamiento introducido en 17.11.

En la solicitud de función rastreada en el Id. de bug Cisco CSCwc81849, desea agregar soporte para los paquetes RADIUS Jumbo. La manera en que esto se hizo es que el paquete RADIUS ya no se fragmentó automáticamente en 1396. Ahora, si agrega el comando ip radius source-

interface <interface X>, la solicitud de acceso RADIUS se envía en la MTU de esa interfaz.



Nota: Si utiliza Cisco Catalyst Center, al aprovisionar configuraciones AAA, se agrega automáticamente la interfaz de origen al grupo de servidores. Esto cambia el comportamiento predeterminado para fragmentar en el tamaño de MTU de la interfaz utilizada en ese comando.

¿Cómo Se Puede Utilizar Este Cambio?

Dado que la MTU predeterminada de todas sus interfaces sería 1500, esa sería la nueva MTU a fragmentar. La interfaz predeterminada que se utiliza para todo el tráfico RADIUS es la interfaz de administración inalámbrica (WMI). Cuando observa la configuración de su grupo de servidores, si no hay una interfaz de origen especificada, el WLC envía el tráfico RADIUS en 1396 mediante WMI. Sin embargo, si entra en la configuración del grupo de servidores y le dice que la interfaz de origen es el WMI, el WLC ahora envía el tráfico RADIUS en 1500 que aún utiliza el WMI.

Ahora, supongamos que hay un dispositivo en la red como la VPN mencionada anteriormente. No

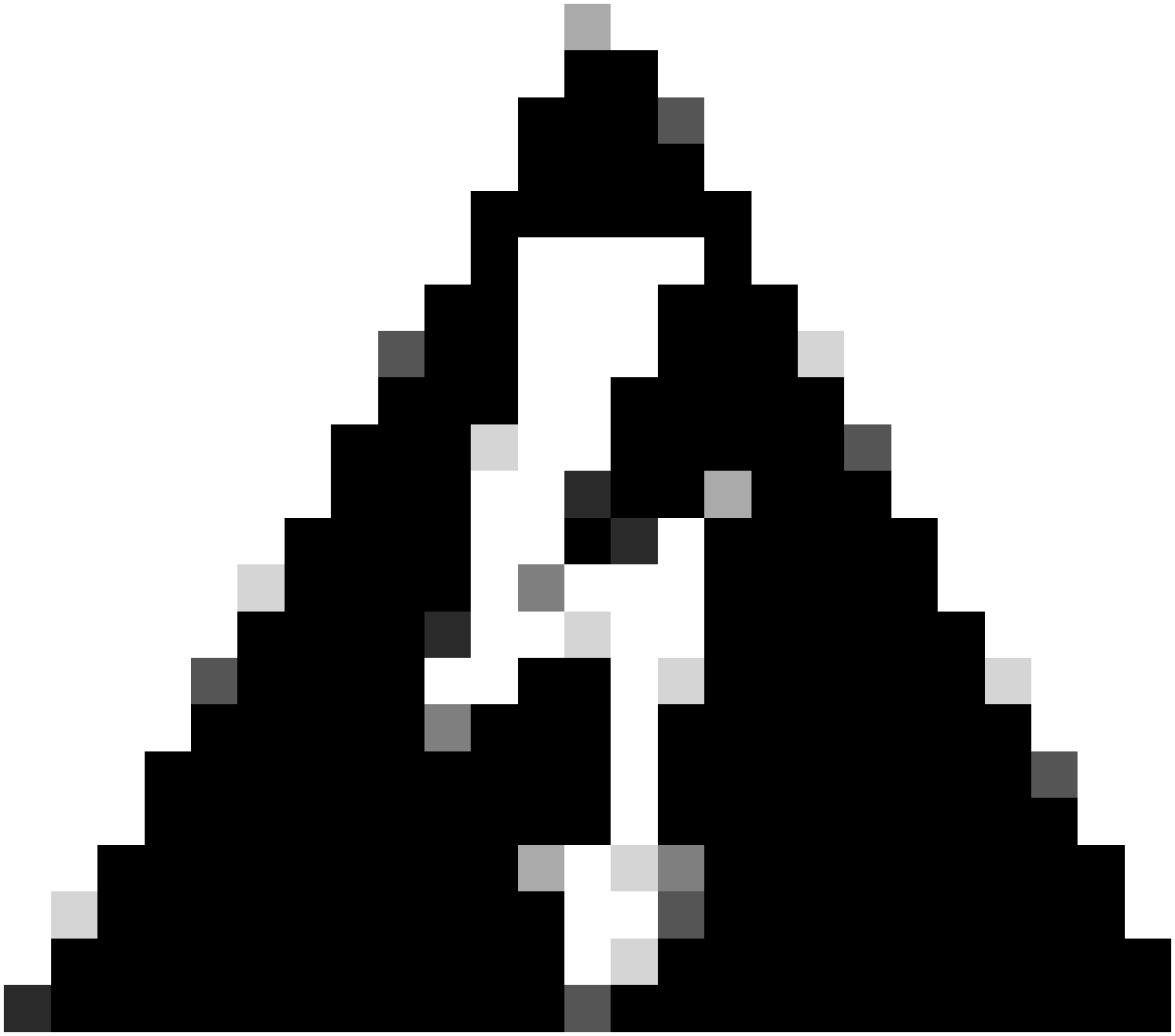
desea que el tráfico se fragmente por partida doble para poder cambiar la MTU de la interfaz a algo más pequeño con el fin de fragmentar los paquetes en un lugar diferente. Puede cambiar la MTU a algo así como 1200 para que los paquetes se fragmenten en la marca de 1200 bytes en lugar de 1500.

Advertencia: El cambio de la MTU del WMI afecta todo el tráfico que va hacia y desde la dirección IP de administración del WLC.

Aunque no desee cambiar la MTU de WMI, el punto de especificar una interfaz de origen es cambiarla de WMI a otra interfaz y utilizar esa interfaz para el tráfico RADIUS, así como cambiar la MTU en esa interfaz. Dado que esta configuración se realiza en el nivel de grupo de servidores, puede ser muy específico sobre qué tráfico RADIUS desea que afecte este cambio.

Esta configuración no está vinculada a un servidor AAA o WLAN. Es posible tener varios grupos de servidores con los mismos servidores en ellos y sólo especificar la interfaz de origen en uno de ellos si así lo desea. Este grupo de servidores se agrega a una lista de métodos y, a continuación, a una WLAN. Así, por ejemplo, si sólo hay una WLAN donde desea que se realice este cambio,

incluso si sólo tiene un servidor AAA, puede crear un nuevo grupo de servidores, utilizar el comando ip radius source-interface que apunta a la interfaz con la MTU que desea utilizar, agregar el servidor AAA a este nuevo grupo, crear una nueva lista de métodos usando este nuevo grupo y luego agregar esa lista de métodos a la WLAN específica donde desea que se realice este cambio.



Advertencia: Siempre se sugiere, cuando se hace CUALQUIER cambio a una red activa, se hace durante una ventana de mantenimiento.

La prueba está en la captura de paquetes

Se conoce comúnmenteEn eso, en la red, si no lo capturaste, no puedes demostrarlo. Aquí hay un par de ejemplos de configuración con estos cambios en su lugar para mostrarle cómo funciona.

Esta es una configuración de WLAN. Durante la prueba, sólo se cambia el grupo de servidores que se utiliza en la lista de métodos.

```
9800#show run wlan
wlan TLS-Test 2 TLS-Test
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 security dot1x authentication-list TLS-AuthC
 no shutdown
!
```

Agregar el comando Source-Interface con la MTU predeterminada

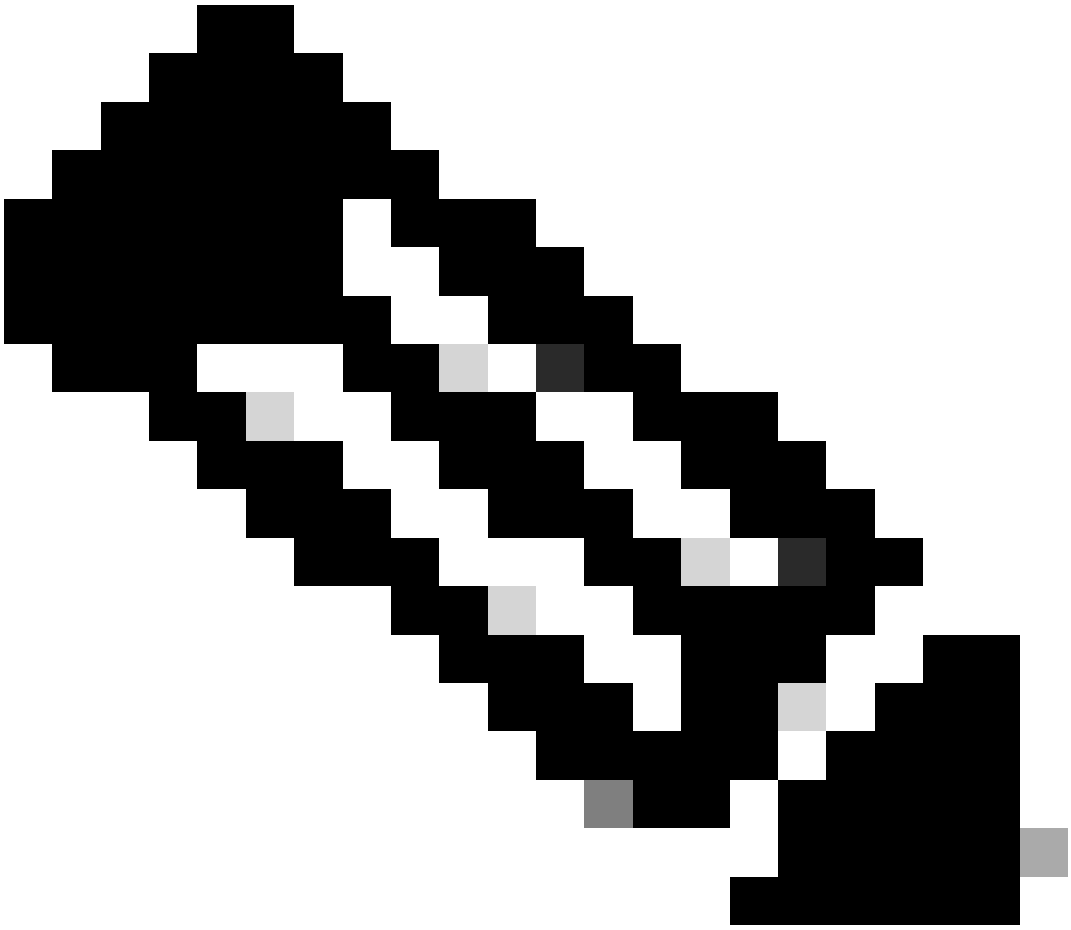
En este caso, se trata de un grupo de servidores normal que apunta al servidor ISE. El comando de la interfaz de origen se agregó apuntando a mi WMI que no tiene establecido MTU. Este es el aspecto de la configuración.

```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group NoMTU
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObF[^bPBVNaYibbBMhNMFAbKUAAB
!
aaa group server radius NoMTU
 server name ISE
 ip radius source-interface Vlan260
 deadtime 5
!
9800#show run inter vlan 260
!
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
 no ip proxy-arp
end
```

Como puede ver, el grupo de servidores NoMTU se ha agregado a la lista de métodos de autenticación que está vinculada a la WLAN. El comando ip radius source-interface VLAN260 se utiliza para este grupo de servidores y la VLAN 260 no especifica una MTU, lo que significa que está utilizando la MTU de 1500. Para confirmar, la MTU de 1500 puede utilizar el comando show run all y buscar la interfaz en el resultado.

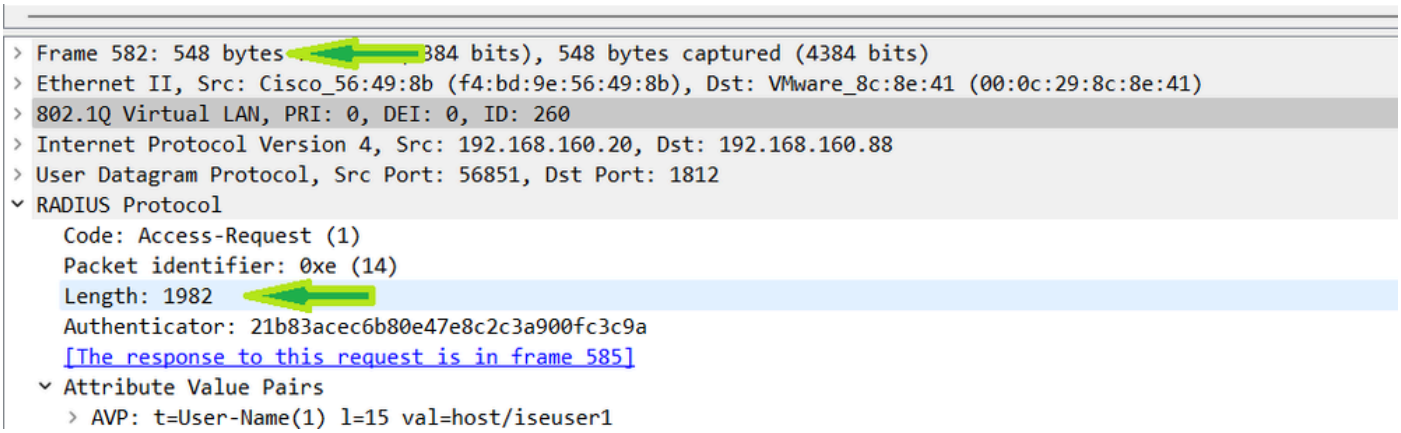
```
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
 no ip clear-dont-fragment
 ip redirects
 ip unreachables
 no ip proxy-arp
 ip mtu 1500
```

Ahora observe el paquete donde el certificado del cliente tiene que ser enviado a ISE una vez que el WLC agrega los datos RADIUS:



Nota: Aquí, los bytes de la línea son 1518. Esto incluye encabezados fuera de la carga útil Ethernet como el encabezado VLAN y el encabezado de capa 2. Estos no se cuentan para la MTU.

```
> Frame 581: 1518 bytes (12144 bits), 1518 bytes captured (12144 bits)
> Ethernet II, Src: Cisco_56:49:8b (f4:bd:9e:56:49:8b), Dst: VMware_8c:8e:41 (00:0c:29:8c:8e:41)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 260
> Internet Protocol Version 4, Src: 192.168.160.20, Dst: 192.168.160.88
v Data (1480 bytes)
    Data: de13071407c63226010e07be21b83acec6b80e47e8c2c3a900fc3c9a010f686f73742f69…
    [Length: 1480]
```



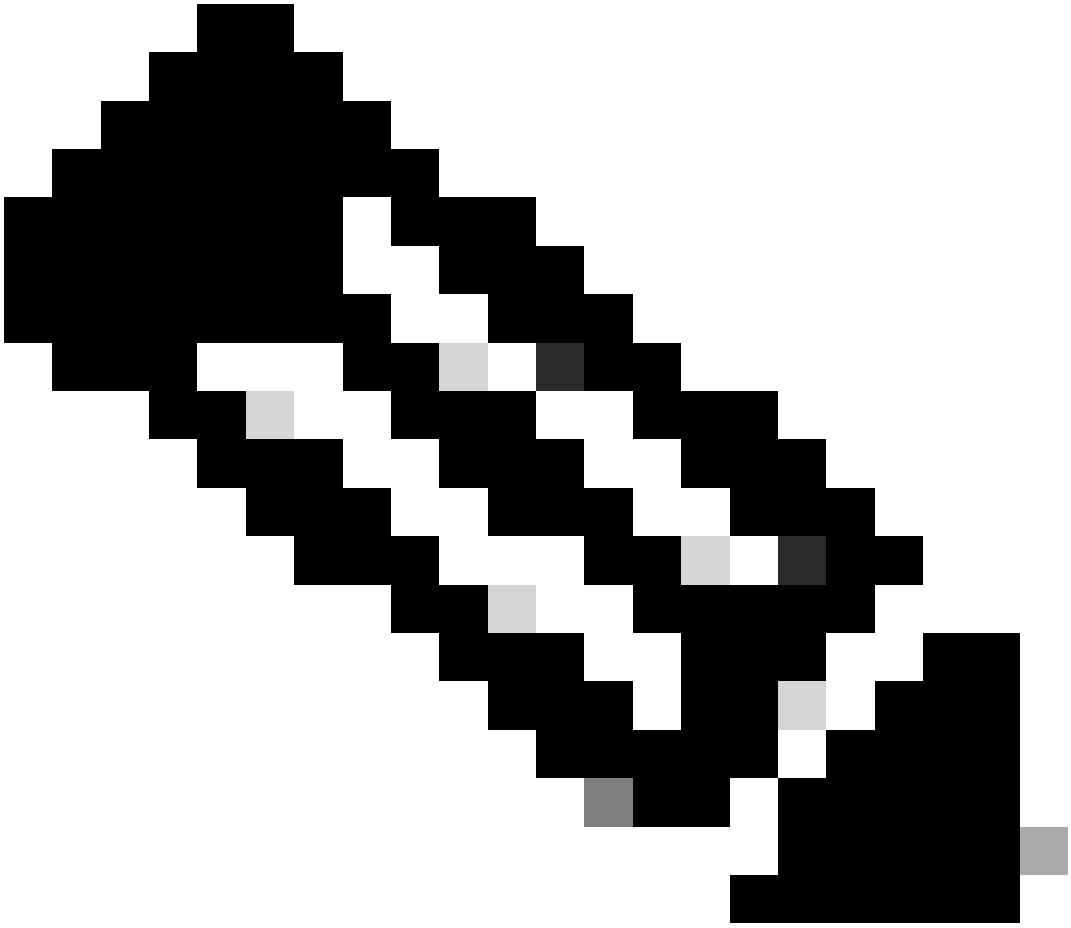
Aquí puede ver que la porción de datos está fragmentada en 1480. Puede obtener ese fragmento bajo la MTU 1500 en WMI. El siguiente paquete tiene menos de 550 bytes, pero puede ver que el tamaño total de los datos RADIUS es 1982. Dicho esto, la fragmentación con la nueva MTU ahora funciona.

Uso de una interfaz no WMI con una MTU de 1200

Ahora, suponga que desea fragmentar en una MTU más pequeña pero no desea que este cambio afecte a ningún otro tráfico. No hay problema aquí, la configuración permanece igual solo la configuración de la interfaz de origen va a apuntar a una SVI que se creó solo para este propósito. Cambie la lista de métodos para que señale a este nuevo grupo de servidores y este grupo de servidores utilice una interfaz de origen que no sea mi WMI y que tenga la MTU establecida en 1200. Este es el aspecto de la configuración:

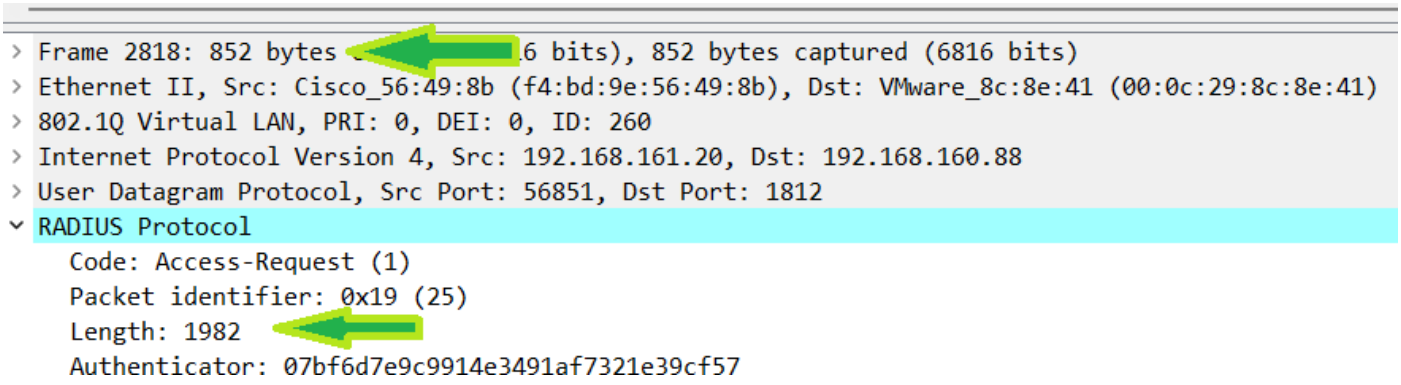
```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group MTU1200
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObFibbBMhNMFAbKUAAB
!
aaa group server radius MTU1200
 server name ISE
 ip radius source-interface Vlan261
 deadtime 5
!
9800#show run inter vlan 261
!
interface Vlan261
 ip address 192.168.161.20 255.255.255.0
 no ip proxy-arp
 ip mtu 1200
end
```

A continuación, vea cómo se ven los paquetes con esta MTU más baja.



Nota: Reducir la MTU y cambiar el punto de fragmentación no es parte del nuevo comportamiento. Esto siempre ha sido cierto. Si el comportamiento predeterminado de fragmentación en 1396 no cabe en la MTU, siempre se fragmentará en un punto diferente. Es parte de esta sección solo para ayudar a explicar las opciones disponibles.

```
> Frame 2817: 1214 bytes [illegible] bits), 1214 bytes captured (9712 bits)
> Ethernet II, Src: Cisco_56:49:8b (f4:bd:9e:56:49:8b), Dst: VMware_8c:8e:41 (00:0c:29:8c:8e:41)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 260
> Internet Protocol Version 4, Src: 192.168.161.20, Dst: 192.168.160.88
v Data (1176 bytes)
    Data: de13071407c6b995011907be07bf6d7e9c9914e3491af7321e39cf57010f686f73742f69…
    [Length: 1176]
```



Aquí, los datos RADIUS siguen siendo 1982 bytes, pero esta vez los datos se fragmentaron en 1176 en lugar de los 1376 predeterminados en los que se fragmentarían si no se hubiera utilizado la interfaz de origen. Recuerde que cuando configura la MTU en 1500 y utiliza el comando source-interface, fragmenta en 1480. El uso de la configuración aquí le permite manipular el tráfico a una MTU más baja sin interferir con otro tráfico en el WLC.

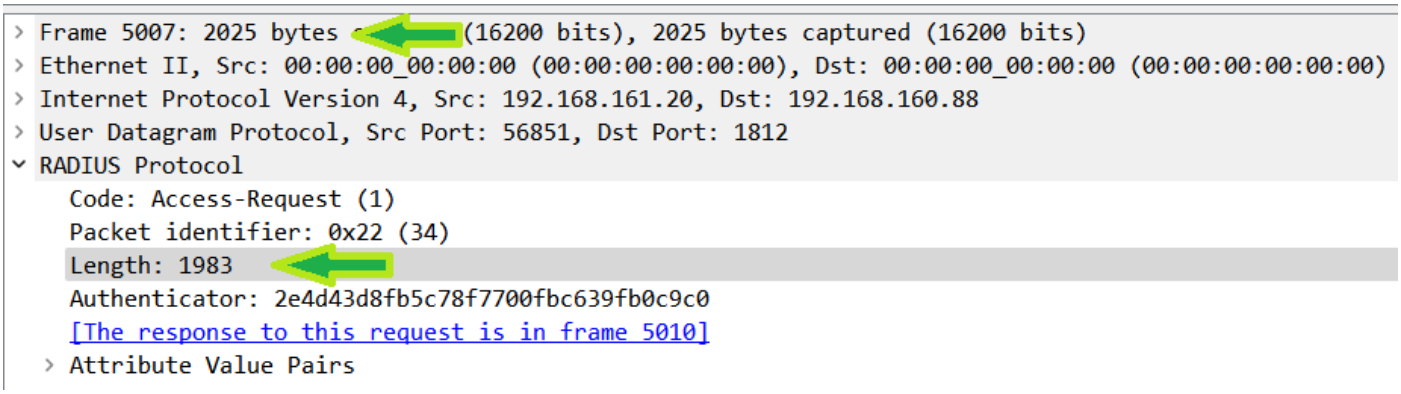
Uso de una MTU de 9000 para tramas Jumbo

Dado que la función se creó para la opción de enviar tramas jumbo, sería una lástima no probar eso también utilizando la interfaz no WMI de VLAN 261. Sin embargo, ahora la MTU IP está configurada en 9000. Una nota rápida, para poder establecer la MTU IP en la SVI, debe establecer la MTU en algo más alto que la MTU IP. Puede ver esto en esta configuración:

```
9800(config-if)#do sho run inter vl 261
!
interface Vlan261
 mtu 9100
 ip address 192.168.161.20 255.255.255.0
 no ip proxy-arp
 ip mtu 9000
end
```

Aquí, al observar la captura, se puede ver que el paquete nunca se fragmentó. Se envió como un paquete completo con el tamaño de datos RADIUS en 1983. Tenga en cuenta que para que esto funcione, el resto de la red debe configurarse para permitir el paso de un paquete de este tamaño.

Otra cosa que debe notarse aquí es que la MTU del cliente no ha cambiado, por lo que el cliente sigue fragmentando el paquete EAP en 1492. La diferencia es que el WLC puede agregar todos los datos RADIUS necesarios para enviar el paquete a ISE sin tener que fragmentar los datos del cliente.



Conclusión

Cuando utiliza EAP-TLS, se espera que el cliente envíe su certificado al servidor AAA. Estos certificados suelen ser más grandes que la MTU, por lo que el cliente tiene que fragmentarla. El punto en el que el cliente fragmenta los datos está bastante cerca de la MTU. Dado que el AP tiene que agregar el encabezado CAPWAP, lo que el cliente está enviando tiene que fragmentarse. El WLC recibe estos dos paquetes, los pone juntos de nuevo pero después tiene que fragmentarlo otra vez para agregar los datos RADIUS. En este punto, el administrador de red recibe cierto control sobre cómo el WLC fragmenta el paquete EAP que el cliente ha enviado.

Si agrega el comando ip radius source-interface <interface que desea utilizar> al grupo de servidores AAA, el WLC utiliza cualquier interfaz que coloque allí en lugar de (o incluyendo) el WMI. El uso de este comando también le indica al WLC que fragmente en cualquier MTU de esa interfaz en lugar del 1396 predeterminado. De esta manera, tendrá más control sobre cómo se mueven los paquetes por la red.

Al utilizar Cisco Catalyst Center, el comando de interfaz de origen se agrega al grupo de servidores, cambiando así el comportamiento predeterminado.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).