Implementaciones y comportamiento de fragmentación de EAP

Contenido

Introducción

Este documento describe cómo entender y resolver problemas de sesiones de protocolo de autenticación extensible (EAP).

Antecedentes

Las secciones de este documento están dedicadas a la cobertura en estas áreas:

- Comportamiento de los servidores de autenticación, autorización y cuentas (AAA) cuando devuelven el certificado de servidor para la sesión EAP-TLS (protocolo de autenticación extensible-seguridad de capa de transporte)
- Comportamiento de los solicitantes cuando devuelven el certificado de cliente para la sesión EAP-TLS
- Interoperabilidad cuando se utilizan tanto el suplicante nativo de Microsoft Windows como el administrador de acceso de red (NAM) de Cisco AnyConnect
- Fragmentación en IP, RADIUS y EAP-TLS y proceso de reensamblado realizado por dispositivos de acceso a la red
- Atributo de unidad de transmisión máxima (MTU) enmarcada de RADIUS
- Comportamiento de los servidores AAA cuando realizan la fragmentación de paquetes EAP-TLS

Prerequisites

Requirements

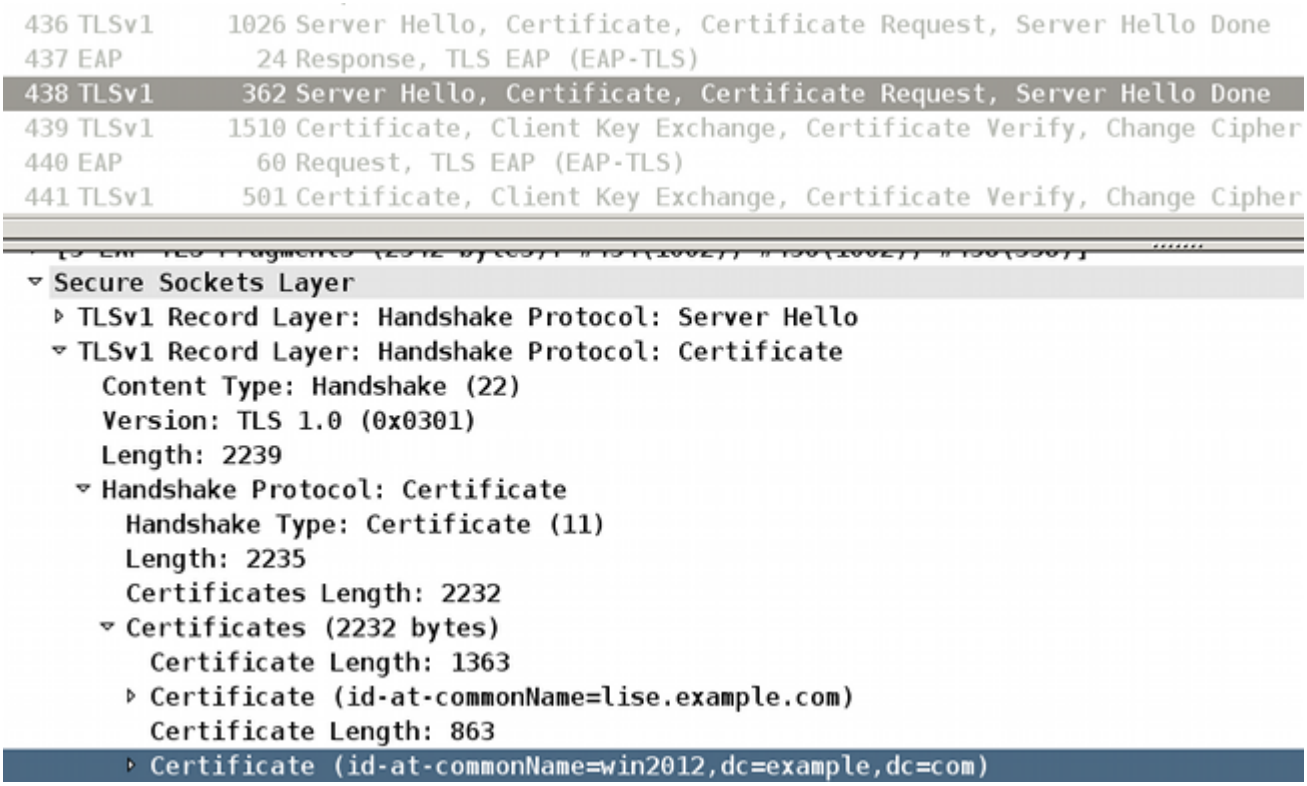
Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolos EAP y EAP-TLS
- Configuración de Cisco Identity Services Engine (ISE)
- Configuración CLI de los switches Cisco Catalyst

Es necesario tener un buen conocimiento de EAP y EAP-TLS para comprender este artículo.

Cadena de certificados devuelta por el servidor

El servidor AAA (Access Control Server (ACS) e ISE) siempre devuelve la cadena completa para el paquete EAP-TLS con el saludo del servidor y el certificado del servidor:



El certificado de identidad de ISE (Common Name (CN)=lise.example.com) se devuelve junto con la autoridad de certificación (CA) que firmó el CN=win2012,dc=example,dc=com. El comportamiento es el mismo para ACS e ISE.

Cadena de certificado devuelta por el solicitante

Suplicante nativo de Microsoft Windows

El suplicante nativo de Microsoft Windows 7 configurado para utilizar EAP-TLS, con o sin la "Selección de certificado simple", no envía la cadena completa del certificado de cliente.

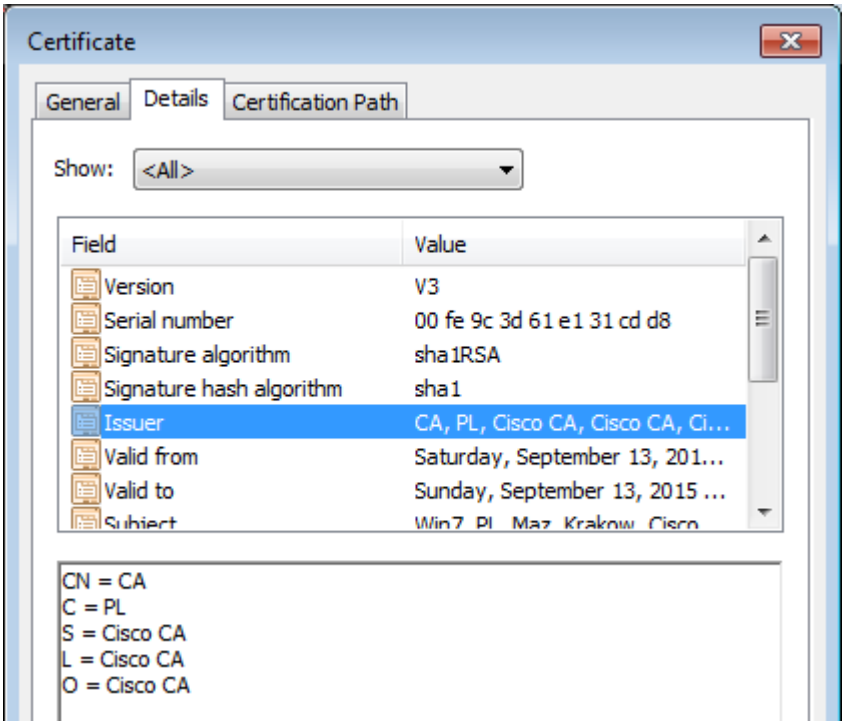
Este comportamiento se produce incluso cuando el certificado de cliente está firmado por una CA (cadena)

distinta del certificado de servidor.

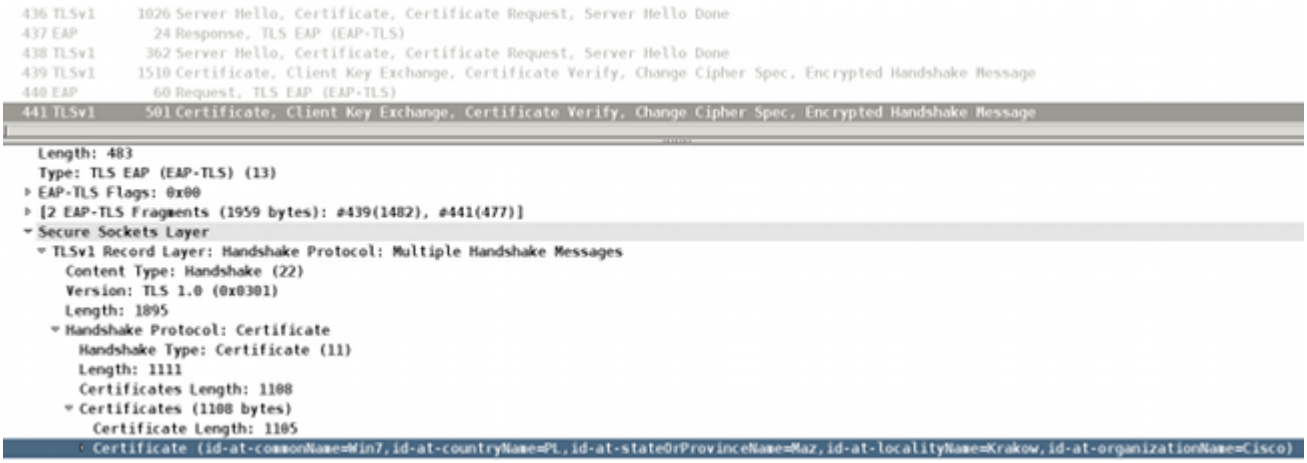
Este ejemplo está relacionado con el Hello y el Certificate del Servidor presentados en la captura de pantalla anterior.

En ese caso, el certificado de ISE lo firma la CA con un nombre de sujeto, CN=win2012,dc=example,dc=com.

Sin embargo, el certificado de usuario instalado en el almacén de Microsoft está firmado por una CA diferente, CN=CA,C=PL,S=Cisco CA,L=Cisco CA, O=Cisco CA.



Como resultado, el solicitante de Microsoft Windows responde sólo con el certificado de cliente. La CA que la firma (CN=CA,S=PL,S=CA de Cisco, L=CA de Cisco, O=CA de Cisco) no está asociada.



Debido a este comportamiento, es posible que los servidores AAA experimenten problemas al validar los certificados de cliente. El ejemplo se refiere a Microsoft Windows 7 SP1 Professional.

Solución

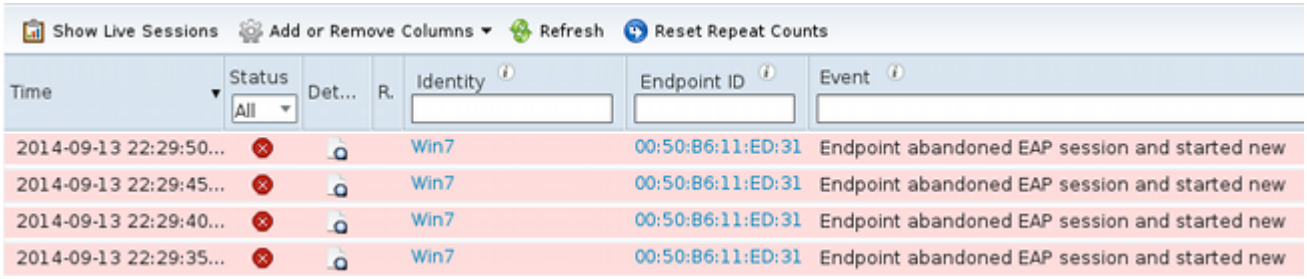
Se debe instalar una cadena de certificados completa en el almacén de certificados de ACS e ISE (todos los

certificados de cliente de firmas de CA y CA secundaria).

Los problemas con la validación de certificados se pueden detectar fácilmente en ACS o ISE. Se presenta la información acerca del certificado no confiable e ISE informa:

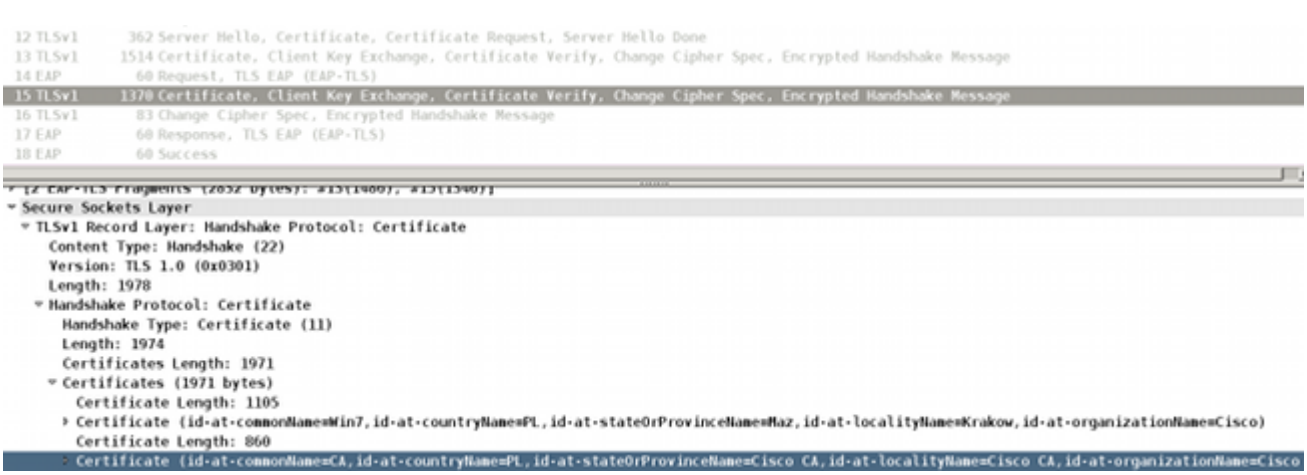
```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

Los problemas con la validación de certificados en el solicitante no son fácilmente detectables. Por lo general, el servidor AAA responde que "la sesión EAP abonada del terminal":



NAM de AnyConnect

El NAM de AnyConnect no tiene esta limitación. En el mismo escenario, adjunta la cadena completa del certificado de cliente (se adjunta la CA correcta):



Suplicante nativo de Microsoft Windows junto con AnyConnect NAM

Cuando ambos servicios están activos, AnyConnect NAM tiene prioridad.

Incluso cuando el servicio NAM no se ejecuta, sigue enlazado a la API de Microsoft Windows y reenvía los paquetes EAP, lo que puede causar problemas al suplicante nativo de Microsoft Windows.

He aquí un ejemplo de tal fracaso.

El seguimiento se habilita en Microsoft Windows con este comando:

```
C:\netsh ras set tracing * enable
```

Los seguimientos (**c:\windows\trace\svchost_RASTLS.LOG**) muestran:

<#root>

```
[2916] 09-14 21:29:11:254: >> Received Request (Code: 1) packet: Id: 55, Length:
6, Type: 13, TLS blob length: 0. Flags: S
[2916] 09-14 21:29:11:254: << Sending Response (Code: 2) packet: Id: 55, Length:
105, Type: 13, TLS blob length: 95. Flags: L
[1804] 09-14 21:29:11:301: >> Received Request (Code: 1) packet: Id: 56, Length:
1012, Type: 13, TLS blob length: 2342. Flags: LM
[1804] 09-14 21:29:11:301: << Sending Response (Code: 2) packet: Id: 56, Length:
6, Type: 13, TLS blob length: 0. Flags:
[1804] 09-14 21:29:11:348: >> Received Request (Code: 1) packet: Id: 57, Length:
1008, Type: 13, TLS blob length: 0. Flags: M
[1804] 09-14 21:29:11:348: << Sending Response (Code: 2) packet: Id: 57, Length:
6, Type: 13, TLS blob length: 0. Flags:
[1804] 09-14 21:29:11:363: >> Received Request (Code: 1) packet: Id: 58, Length:
344, Type: 13, TLS blob length: 0. Flags:
[1804] 09-14 21:29:11:363: << Sending Response (Code: 2) packet: Id: 58, Length:
1492, Type: 13, TLS blob length: 1819. Flags: LM
[3084] 09-14 21:31:11:203: >> Received Request (Code: 1) packet: Id: 122, Length:
6, Type: 13, TLS blob length: 0. Flags: S
[3084] 09-14 21:31:11:218: << Sending Response (Code: 2) packet: Id: 122, Length:
105, Type: 13, TLS blob length: 95. Flags: L
[3420] 09-14 21:31:11:249: >> Received Request (Code: 1) packet: Id: 123, Length:
1012, Type: 13, TLS blob length: 2342. Flags: LM
[3420] 09-14 21:31:11:249: << Sending Response (Code: 2) packet: Id: 123, Length:
6, Type: 13, TLS blob length: 0. Flags:
[3420] 09-14 21:31:11:281: >> Received Request (Code: 1) packet: Id: 124, Length:
1008, Type: 13, TLS blob length: 0. Flags: M
[3420] 09-14 21:31:11:281: << Sending Response (Code: 2) packet: Id: 124, Length:
6, Type: 13, TLS blob length: 0. Flags:
[3420] 09-14 21:31:11:281: >> Received Request (Code: 1) packet: Id: 125, Length:
344, Type: 13, TLS blob length: 0. Flags:
[3420] 09-14 21:31:11:296: <<
```

Sending Response (Code: 2)

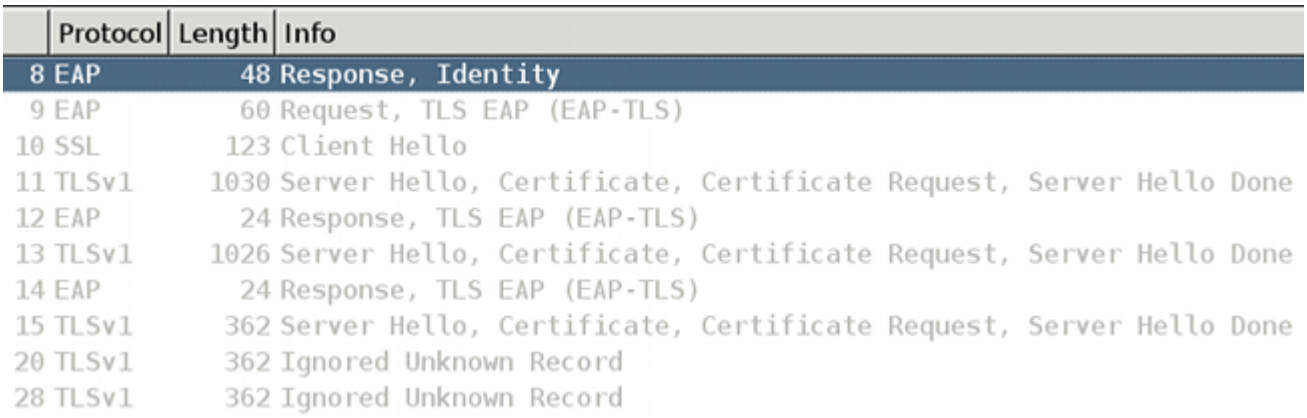
```
 packet: Id: 125, Length:
```

1492

```
, Type: 13,
```

TLS blob length: 1819. Flags: LM

El último paquete es un certificado de cliente (EAP-TLS fragmento 1 con tamaño EAP 1492) enviado por el suplicante nativo de Microsoft Windows. Desafortunadamente, Wireshark no muestra ese paquete:



	Protocol	Length	Info
8	EAP	48	Response, Identity
9	EAP	60	Request, TLS EAP (EAP-TLS)
10	SSL	123	Client Hello
11	TLSv1	1030	Server Hello, Certificate, Certificate Request, Server Hello Done
12	EAP	24	Response, TLS EAP (EAP-TLS)
13	TLSv1	1026	Server Hello, Certificate, Certificate Request, Server Hello Done
14	EAP	24	Response, TLS EAP (EAP-TLS)
15	TLSv1	362	Server Hello, Certificate, Certificate Request, Server Hello Done
20	TLSv1	362	Ignored Unknown Record
28	TLSv1	362	Ignored Unknown Record

Y ese paquete no se envía realmente; el último fue el tercer fragmento del certificado de servidor portador de EAP-TLS.

Lo ha consumido el módulo NAM de AnyConnect que engancha en la API de Microsoft Windows.

Por este motivo, no se recomienda utilizar AnyConnect junto con el suplicante nativo de Microsoft Windows.

Cuando utiliza cualquier servicio de AnyConnect, se recomienda utilizar NAM también (cuando se necesitan servicios 802.1x), no el Suplicante nativo de Microsoft Windows.

Fragmentación

La fragmentación puede ocurrir en varias capas:

- IP
- Pares de valores de atributos RADIUS (AVP)
- EAP-TLS

Los switches Cisco IOS® son muy inteligentes. Pueden comprender los formatos EAP y EAP-TLS.

Aunque el switch no puede descifrar el túnel TLS, es responsable de la fragmentación, el ensamblado y el reensamblado de los paquetes EAP cuando se encapsula en el protocolo de autenticación extensible sobre LAN (EAPoL) o RADIUS.

El protocolo EAP no admite la fragmentación. Este es un extracto de RFC 3748 (EAP):

"La fragmentación no se admite dentro del propio EAP; sin embargo, los métodos EAP individuales pueden admitirlo."

EAP-TLS es un ejemplo. Este es un extracto de RFC 5216 (EAP-TLS), sección 2.1.5 (fragmentación):

"Cuando un par EAP-TLS recibe un paquete de solicitud EAP con el bit M configurado, DEBE responder con una respuesta EAP-Response con EAP-Type=EAP-TLS y sin datos.

Esto sirve como un fragmento ACK. **El servidor EAP DEBE esperar hasta que reciba la respuesta EAP antes de enviar otro fragmento**."

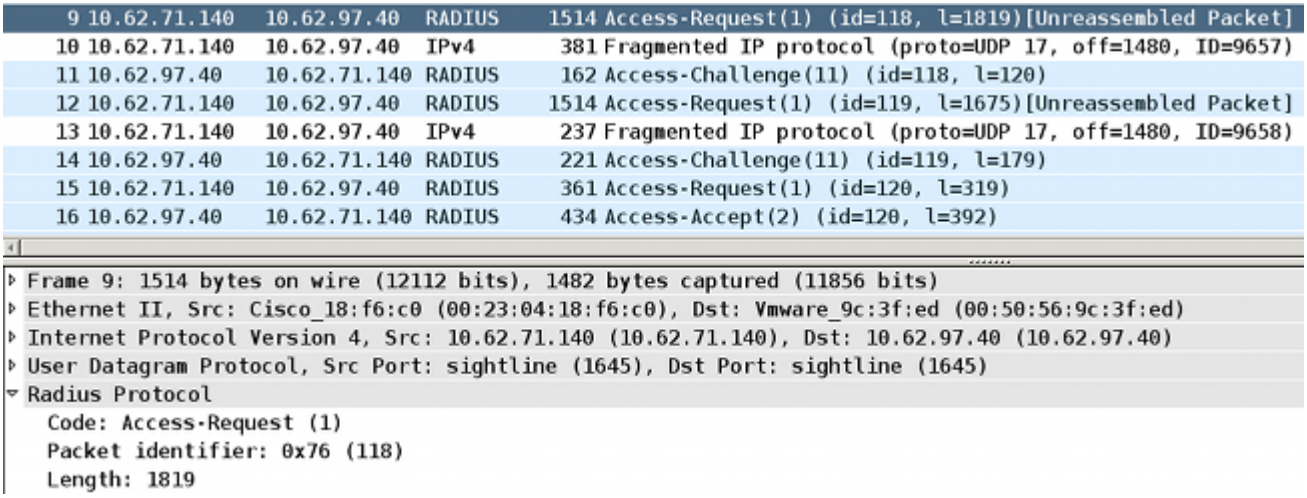
La última frase describe una función muy importante de los servidores AAA. Deben esperar el ACK antes de poder enviar otro fragmento EAP. Se utiliza una regla similar para el solicitante:

"El peer EAP DEBE esperar hasta que reciba la solicitud EAP antes de enviar otro fragmento."

Fragmentación en la capa IP

La fragmentación sólo puede producirse entre el dispositivo de acceso a la red (NAD) y el servidor AAA (IP/UDP/RADIUS utilizado como transporte).

Esta situación ocurre cuando NAD (switch de Cisco IOS) intenta enviar la solicitud RADIUS que contiene la carga útil EAP, que es mayor que la MTU de la interfaz:

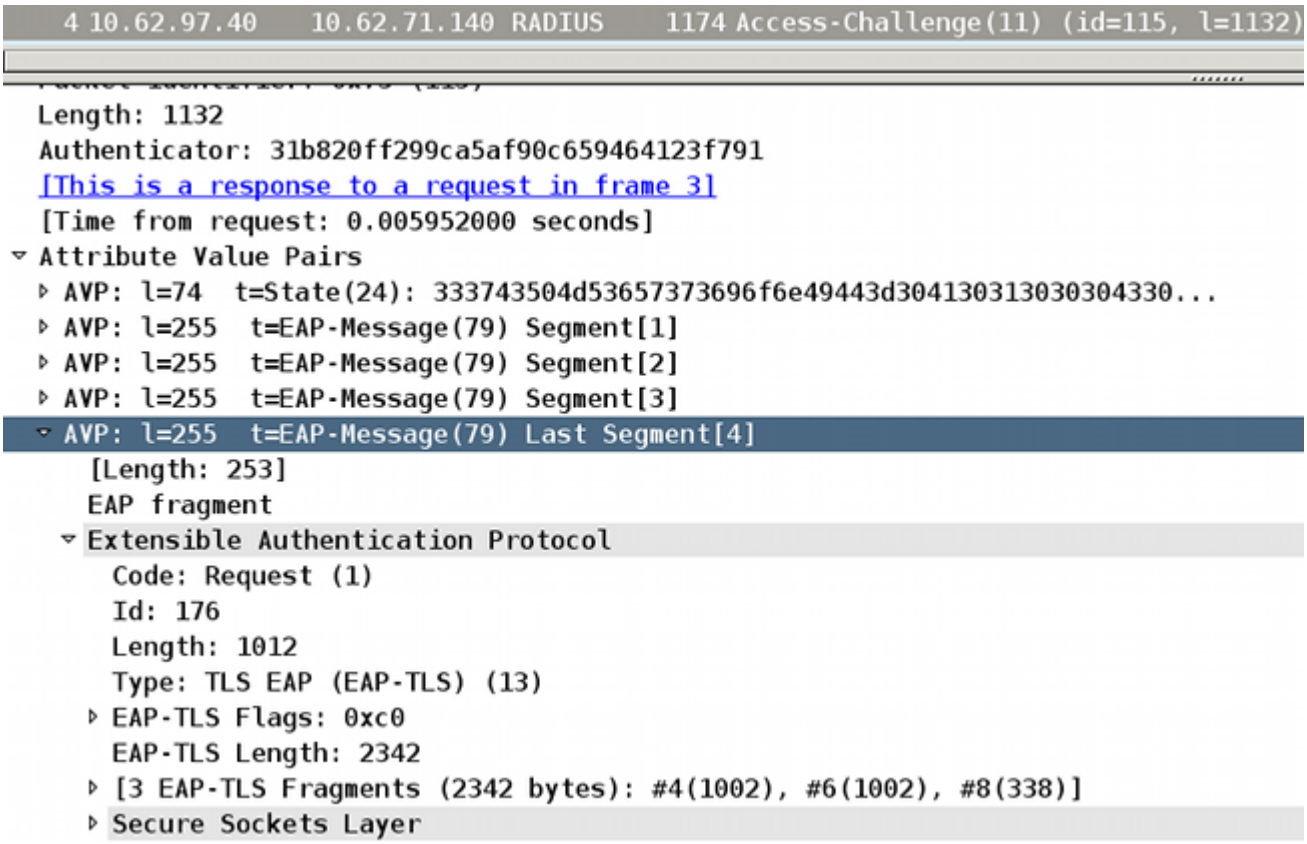


La mayoría de las versiones de Cisco IOS no son lo suficientemente inteligentes y no intentan ensamblar los paquetes EAP recibidos a través de EAPoL y combinarlos en un paquete RADIUS que pueda caber en la MTU de la interfaz física hacia el servidor AAA.

Los servidores AAA son más inteligentes (como se muestra en las siguientes secciones).

Fragmentación en RADIUS

Esto no es realmente ningún tipo de fragmentación. Según RFC 2865, un solo atributo RADIUS puede tener hasta 253 bytes de datos.Debido a eso, la carga útil EAP siempre se transmite en múltiples atributos EAP-Message RADIUS:



Wireshark reensambla e interpreta esos atributos de mensaje EAP (el atributo "Last Segment" revela la carga útil de todo el paquete EAP).

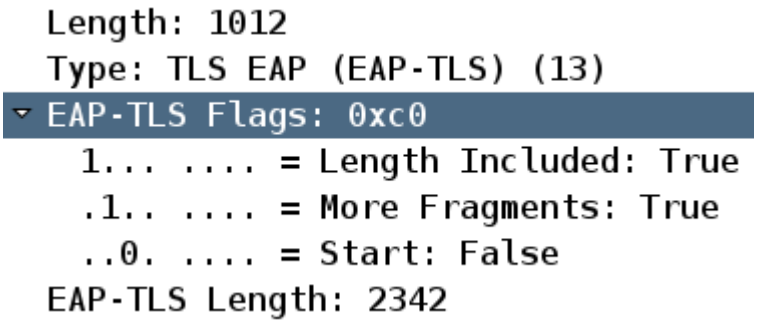
El encabezado Length en el paquete EAP es igual a 1.012 y se necesitan cuatro AVP RADIUS para transportarlo.

Fragmentación en EAP-TLS

En la misma captura de pantalla, puede ver que:

- La longitud del paquete EAP es de 1012
- La longitud de EAP-TLS es de 2342

Esto sugiere que es el primer fragmento de EAP-TLS y que el solicitante espera más, lo que se puede confirmar si examina los indicadores de EAP-TLS:



Este tipo de fragmentación se produce con mayor frecuencia en:

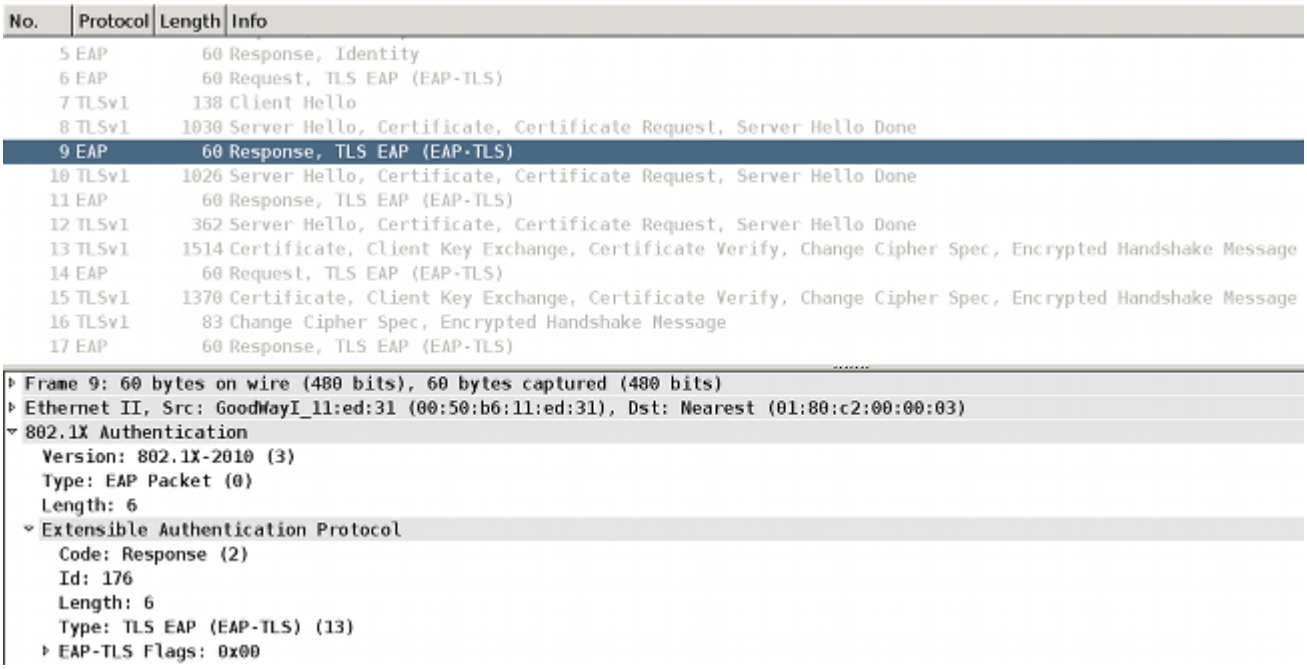
- RADIUS Access-Challenge enviado por el servidor AAA, que transporta la solicitud EAP con el certificado de servidor de capa de sockets seguros (SSL) con toda la cadena.

- RADIUS Access-Request send by NAD, que transporta la respuesta EAP con el certificado de cliente SSL con toda la cadena.

Confirmación de fragmento de EAP-TLS

Como se explicó anteriormente, cada fragmento EAP-TLS debe ser reconocido antes de enviar los fragmentos subsiguientes.

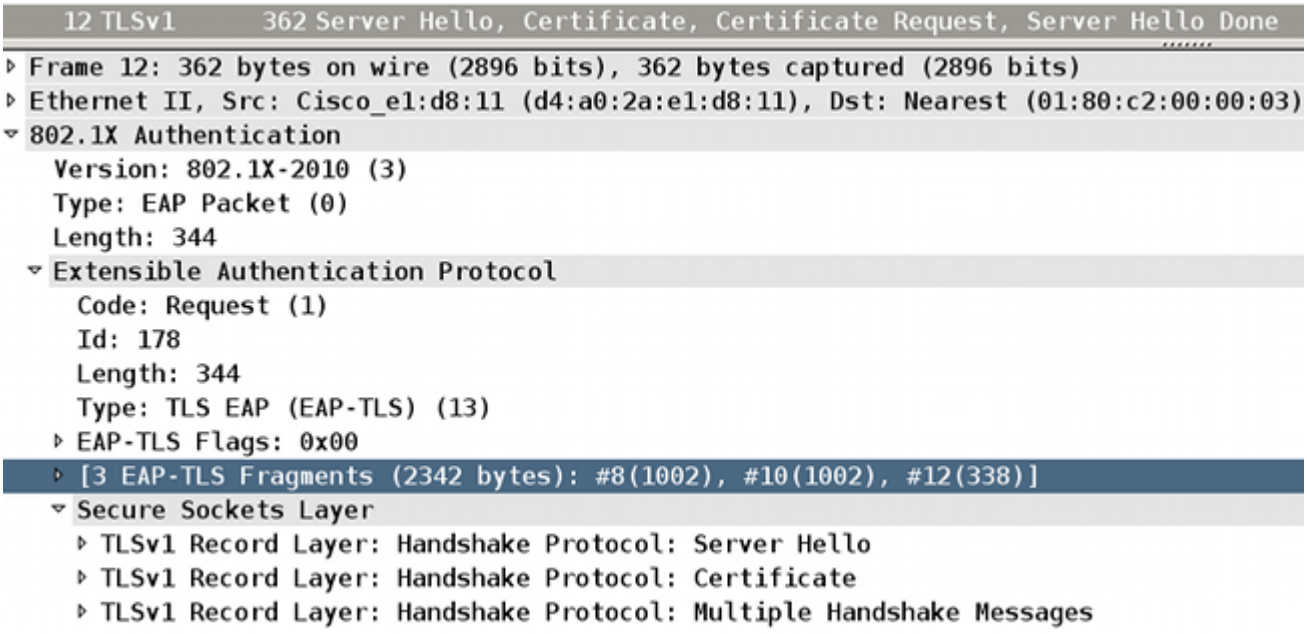
A continuación se muestra un ejemplo (capturas de paquetes para EAPoL entre el solicitante y el NAD):



Las tramas EAPoL y el servidor AAA devuelven el certificado del servidor:

- Ese certificado se envía en un fragmento EAP-TLS (paquete 8).
- El solicitante reconoce ese fragmento (paquete 9).
- El segundo fragmento EAP-TLS es reenviado por NAD (paquete 10).
- El solicitante reconoce ese fragmento (paquete 11).
- El tercer fragmento EAP-TLS es reenviado por NAD (paquete 12).
- El solicitante no necesita reconocer esto; más bien, procede con el certificado de cliente que comienza en el paquete 13.

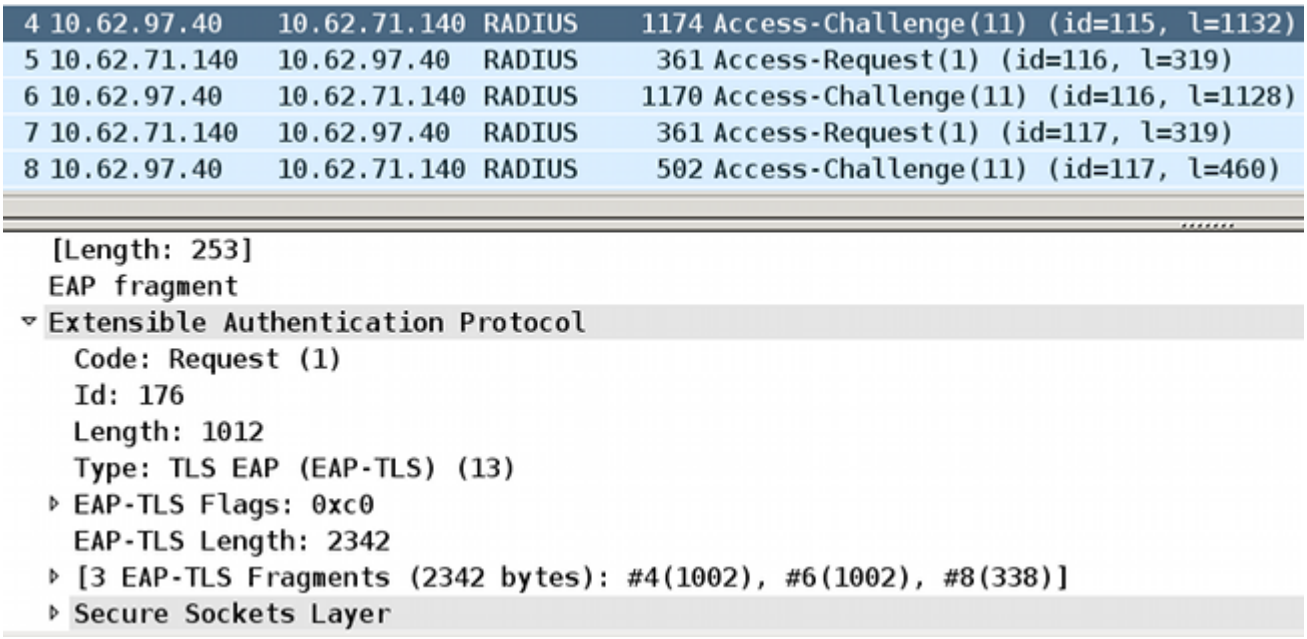
Estos son los detalles del paquete 12:



Puede ver que Wireshark volvió a ensamblar los paquetes 8, 10 y 12.

El tamaño de los fragmentos EAP es 1.002, 1.002 y 338, lo que eleva el tamaño total del mensaje EAP-TLS a 2.342;

La longitud total del mensaje EAP-TLS se anuncia en cada fragmento. Esto se puede confirmar si examina los paquetes RADIUS (entre el servidor NAD y AAA):



Los paquetes RADIUS 4, 6 y 8 transportan esos tres fragmentos EAP-TLS. Se reconocen los dos primeros fragmentos.

Wireshark puede presentar la información sobre los fragmentos EAP-TLS (tamaño: 1.002 + 1.002 + 338 = 2.342).

Este escenario y ejemplo fue fácil. El switch Cisco IOS no necesitaba cambiar el tamaño del fragmento EAP-TLS.

Fragmentos de EAP-TLS reensamblados con tamaños diferentes

Piense en lo que ocurre cuando la MTU de NAD hacia el servidor AAA es de 9000 bytes (trama jumbo) y el servidor AAA también está conectado con el uso de la interfaz que admite tramas jumbo.

La mayoría de los suplicantes típicos están conectados con el uso de un link de 1 Gbit con una MTU de 1,500.

En tal escenario, el switch del IOS de Cisco realiza el ensamblado y el reensamblado "asimétricos" de EAP-TLS y cambia los tamaños de los fragmentos de EAP-TLS.

Este es un ejemplo de un mensaje EAP grande enviado por el servidor AAA (Certificado de servidor SSL):

1. El servidor AAA debe enviar un mensaje EAP-TLS con un certificado de servidor SSL. El tamaño total de ese paquete EAP es de 3000. Después de encapsularse en RADIUS Access-Challenge/UDP/IP, sigue siendo menor que la MTU de la interfaz del servidor AAA. Se envía un único paquete IP con 12 atributos de mensaje EAP RADIUS. No hay fragmentación IP ni EAP-TLS.

2. El switch del IOS de Cisco recibe dicho paquete, lo desencapsula y decide que EAP debe enviarse a través de EAPoL al solicitante. Debido a que EAPoL no admite la fragmentación, el switch debe realizar la fragmentación EAP-TLS.

3. El switch Cisco IOS prepara el primer fragmento EAP-TLS que puede caber en la MTU de la interfaz hacia el solicitante (1500).

4. Este fragmento es confirmado por el solicitante.

5. Se envía otro fragmento EAP-TLS después de recibir la confirmación.

6. Este fragmento es confirmado por el solicitante.

7. El switch envía el último fragmento EAP-TLS.

Este escenario revela que:

- En algunas circunstancias, el NAD debe crear fragmentos EAP-TLS.
- El NAD es responsable de enviar/reconocer esos fragmentos.

La misma situación puede ocurrir para un suplicante conectado a través de un link que soporta tramas jumbo mientras que el servidor AAA tiene una MTU más pequeña (entonces el switch Cisco IOS crea fragmentos EAP-TLS cuando envía el paquete EAP hacia el servidor AAA).

MTU entramada de atributo RADIUS

Para RADIUS, hay un atributo Framed-MTU definido en RFC 2865:

"Este atributo indica la unidad de transmisión máxima que se configurará para el usuario cuando no se negocie por otros medios (como PPP). SE PUEDE utilizar en paquetes de aceptación de acceso.

Puede ser utilizado en un paquete Access-Request como una indicación por parte del NAS al servidor de que preferiría ese valor, pero el servidor no está obligado a aceptar la sugerencia."

ISE no respeta la pista. El valor de la MTU con trama enviada por NAD en la solicitud de acceso no tiene ningún impacto en la fragmentación realizada por ISE.

Varios switches Cisco IOS modernos no permiten cambios en la MTU de la interfaz Ethernet excepto para la configuración de tramas jumbo habilitada globalmente en el switch. La configuración de tramas jumbo afecta el valor del atributo Framed-MTU enviado en la solicitud de acceso RADIUS. Por ejemplo, puede establecer:

```
<#root>

Switch(config)#

system mtu jumbo 9000
```

Esto obliga al switch a enviar MTU entramada = 9000 en todas las solicitudes de acceso RADIUS. Lo mismo para la MTU del sistema sin tramas jumbo:

```
<#root>

Switch(config)#

system mtu 1600
```

Esto obliga al switch a enviar MTU entramada = 1600 en todas las solicitudes de acceso RADIUS.

Observe que los switches Cisco IOS modernos no le permiten disminuir el valor de MTU del sistema por debajo de 1,500.

Servidores AAA y comportamiento suplicante al enviar fragmentos EAP

ISE

ISE siempre intenta enviar fragmentos EAP-TLS (normalmente, saludo del servidor con certificado) que tienen una longitud de 1002 bytes (aunque el último fragmento suele ser más pequeño).

No honra la MTU entramada RADIUS. No es posible volver a configurarlo para enviar fragmentos EAP-TLS más grandes.

Microsoft Network Policy Server (NPS)

Es posible configurar el tamaño de los fragmentos EAP-TLS si configura el atributo Framed-MTU localmente en NPS.

A pesar de que el artículo Configure the EAP Payload Size on Microsoft NPS menciona que el valor predeterminado de una MTU con trama para el servidor RADIUS NPS es 1500, el laboratorio del Cisco Technical Assistance Center (TAC) ha demostrado que envía 2000 con la configuración predeterminada (confirmada en un Microsoft Windows 2012 Datacenter).

Se prueba que NPS respeta la configuración **Framed-MTU localmente** según la guía mencionada anteriormente, y fragmenta los mensajes EAP en fragmentos de un tamaño establecido en Framed-MTU. Pero el atributo Framed-MTU recibido en Access-Request no se utiliza (igual que en ISE/ACS).

La configuración de este valor es una solución alternativa válida para corregir problemas en la topología

como este:

Suplicante [MTU 1500] ---- ---- [MTU 9000]Switch[MTU 9000] ----- ----- [MTU 9000]NPS

Actualmente, los switches no le permiten establecer la MTU por puerto; para los switches 6880, esta función se agrega con el ID de bug Cisco CSCuo26327 - 802.1x EAP-TLS no funciona en los puertos de host FEX.

AnyConnect

AnyConnect envía fragmentos EAP-TLS (normalmente certificado de cliente) que tienen 1486 bytes de longitud. Para este tamaño de valor, la trama Ethernet es de 1500 bytes. El último fragmento suele ser más pequeño.

Suplicante nativo de Microsoft Windows

Microsoft Windows envía fragmentos EAP-TLS (normalmente certificado de cliente) que tienen una longitud de 1.486 o 1.482 bytes. Para este tamaño de valor, la trama Ethernet es de 1500 bytes. El último fragmento suele ser más pequeño.

Información Relacionada

- **Configuración de la Autenticación Basada en Puerto IEEE 802.1x**
- **Soporte Técnico y Documentación - Cisco Systems**

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).