Implementações e comportamento da fragmentação de EAP

Contents

[Introdução](#)
[Informações de Apoio](#)
[Pré-requisitos](#)
[Requisitos](#)
[Cadeia de Certificados Retornada pelo Servidor](#)
[Cadeia de Certificados Retornada pelo Requerente](#)
[Solicitante Nativo do Microsoft Windows](#)
[Solução](#)
[NAM do AnyConnect](#)
[Solicitante nativo do Microsoft Windows junto com o NAM do AnyConnect](#)
[Fragmentação](#)
[Fragmentação na Camada IP](#)
[Fragmentação em RADIUS](#)
[Fragmentação em EAP-TLS](#)
[Confirmação de fragmento EAP-TLS](#)
[Fragmentos EAP-TLSreagrupados com tamanhos diferentes](#)
[Atributo RADIUS Framed-MTU](#)
[Servidores AAA e comportamento do suplicante ao enviar fragmentos EAP](#)
[ISE](#)
[Servidor de Políticas de Rede (NPS) da Microsoft](#)
[AnyConnect](#)
[Solicitante Nativo do Microsoft Windows](#)
[Informações Relacionadas](#)

Introdução

Este documento descreve como entender e solucionar problemas de sessões do EAP (Extensible Authentication Protocol).

Informações de Apoio

As seções deste documento são dedicadas à cobertura nestas áreas:

- Comportamento dos servidores de Autenticação, Autorização e Tarifação (AAA - Authentication, Authorization, and Accounting) quando eles retornam o Certificado de Servidor para a sessão EAP-TLS (Extensible Authentication Protocol-Transport Layer Security).
- Comportamento dos solicitantes ao retornarem o Certificado de Cliente para a sessão EAP-TLS
- Interoperabilidade quando ambos o Microsoft Windows Native Supplicant e o Cisco AnyConnect Network Access Manager (NAM) são usados
- Fragmentação em IP, RADIUS e EAP-TLS e processo de remontagem executado por dispositivos de acesso à rede
- O atributo MTU (Unidade Máxima de Transmissão) de quadro RADIUS
- O comportamento dos servidores AAA quando executam a fragmentação de pacotes EAP-TLS

Pré-requisitos

Requisitos

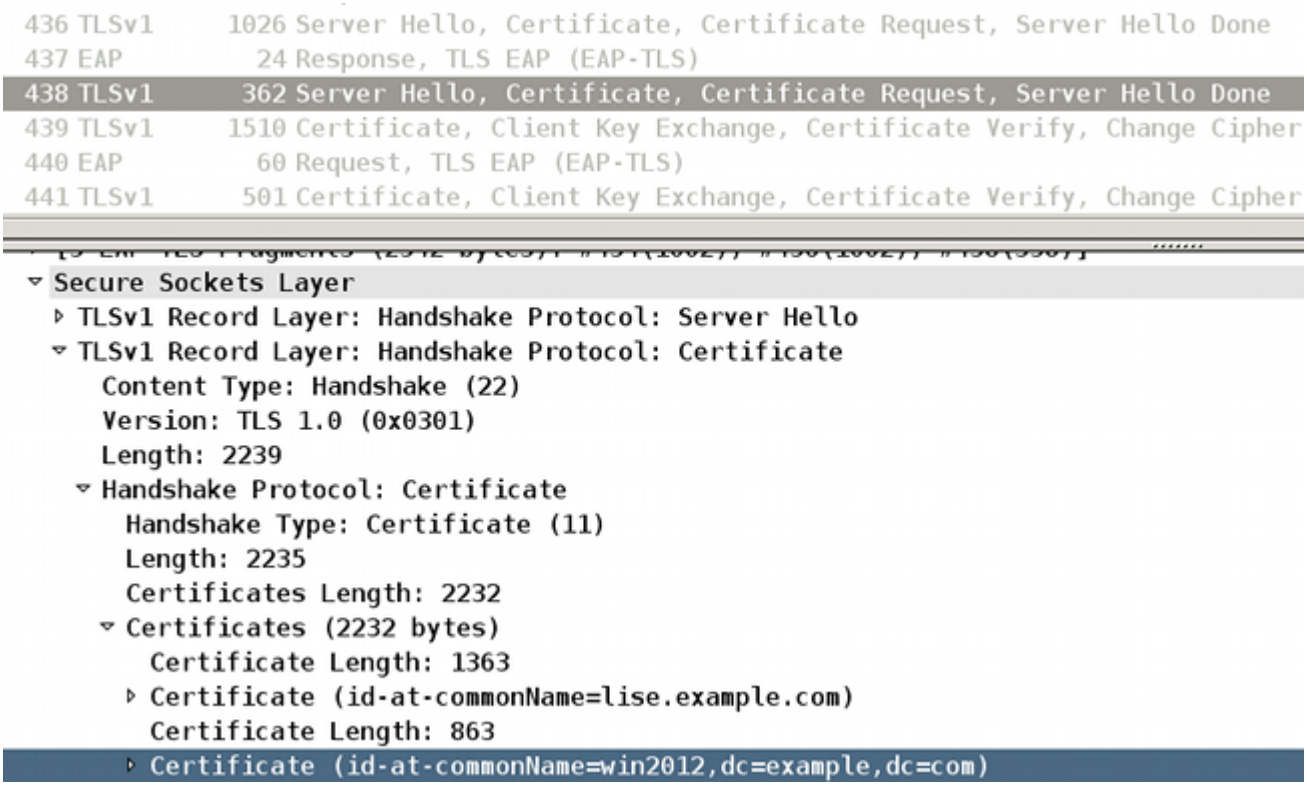
A Cisco recomenda que você tenha conhecimento destes tópicos:

- Protocolos EAP e EAP-TLS
- Configuração do Cisco Identity Services Engine (ISE)
- Configuração CLI dos switches Cisco Catalyst

É necessário ter um bom entendimento de EAP e EAP-TLS para entender este artigo.

Cadeia de Certificados Retornada pelo Servidor

O servidor AAA (Access Control Server (ACS) e ISE) sempre retorna a cadeia completa para o pacote EAP-TLS com o Server Hello e o Server Certificate:



O certificado de identidade do ISE (Nome comum (CN)=lise.example.com) é retornado junto com a Autoridade de certificação (CA) que assinou o CN=win2012,dc=example,dc=com. O comportamento é o mesmo para o ACS e o ISE.

Cadeia de Certificados Retornada pelo Requerente

Solicitante Nativo do Microsoft Windows

O solicitante nativo do Microsoft Windows 7 configurado para usar EAP-TLS, com ou sem a "Seleção de certificado simples", não envia a cadeia completa do certificado do cliente.

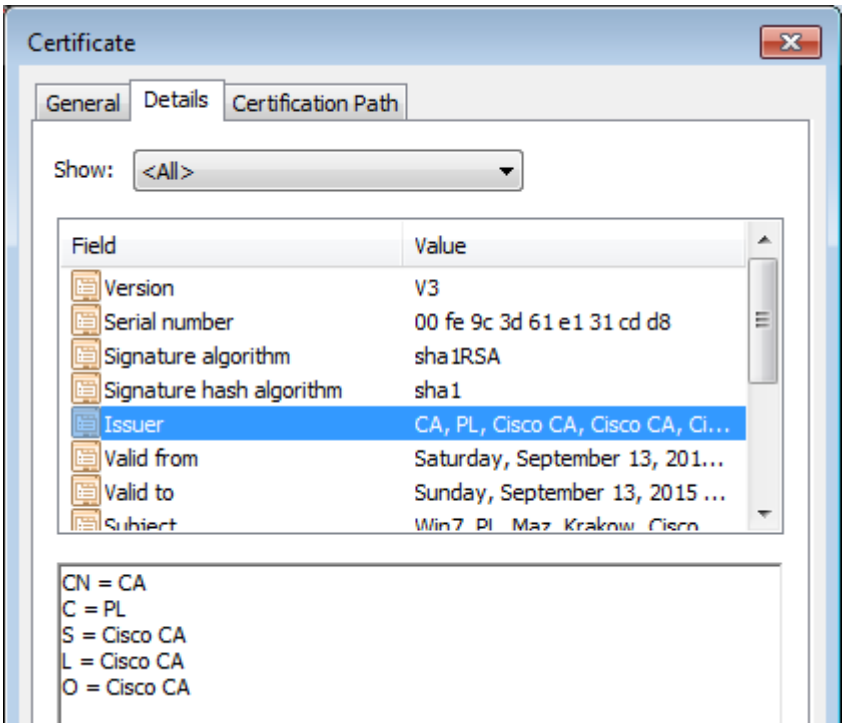
Esse comportamento ocorre mesmo quando o certificado do cliente é assinado por uma CA (cadeia

diferente) diferente do certificado do servidor.

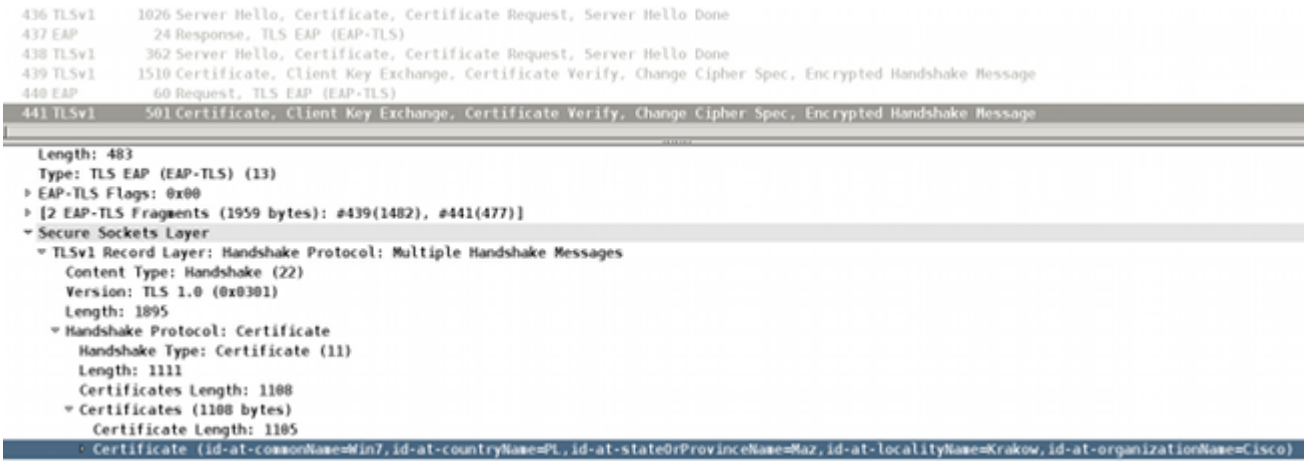
Este exemplo está relacionado ao Servidor Hello e Certificado apresentado na captura de tela anterior.

Para esse cenário, o certificado ISE é assinado pela CA com o uso de um nome de assunto, CN=win2012,dc=example,dc=com.

Mas o certificado de usuário instalado na loja da Microsoft é assinado por uma CA diferente, CN=CA,C=PL,S=Cisco CA,L=Cisco CA, O=Cisco CA.



Como resultado, o solicitante do Microsoft Windows responde apenas com o certificado do cliente. A CA que a assina (CN=CA,S=PL,S=Cisco CA, L=Cisco CA, O=Cisco CA) não está anexada.



Devido a esse comportamento, os servidores AAA possivelmente encontram problemas ao validar certificados de cliente. O exemplo se refere ao Microsoft Windows 7 SP1 Professional.

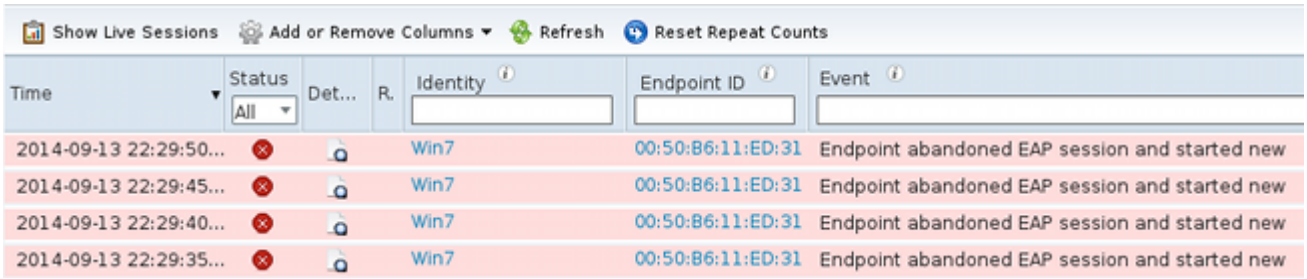
Solução

Uma cadeia de certificados completa deve ser instalada no armazenamento de certificados do ACS e do ISE (todos os certificados de cliente de assinatura CA e sub CA).

Problemas com validação de certificado podem ser facilmente detectados no ACS ou no ISE. As informações sobre certificados não confiáveis são apresentadas e o ISE relata:

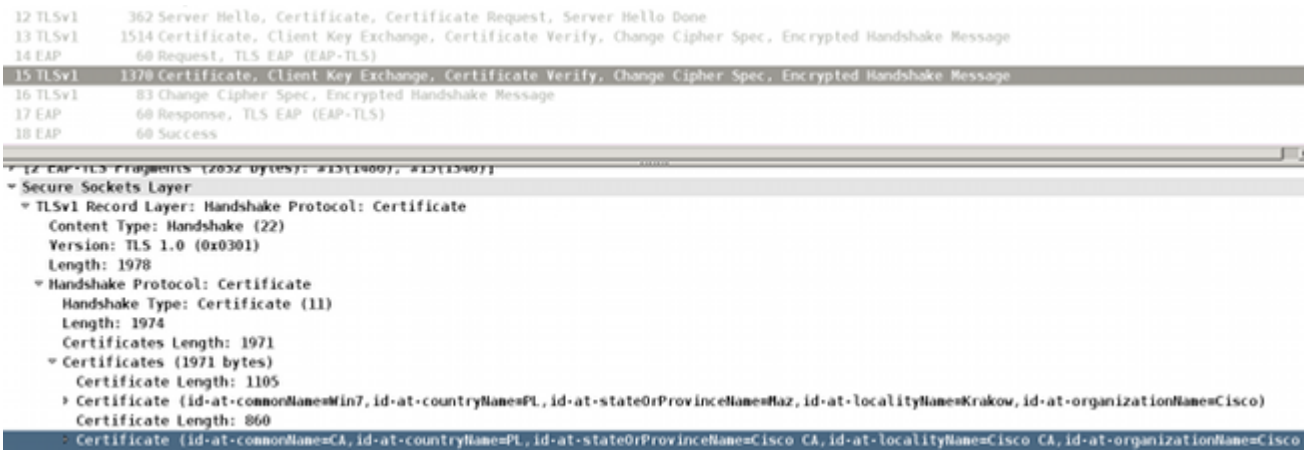
```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

Os problemas com a validação do certificado no requerente não são facilmente detectáveis. Geralmente, o servidor AAA responde que "Endpoint abondoned EAP session":



NAM do AnyConnect

O NAM do AnyConnect não tem essa limitação. No mesmo cenário, ele anexa a cadeia completa do certificado do cliente (a CA correta é anexada):



Solicitante nativo do Microsoft Windows junto com o NAM do AnyConnect

Quando ambos os serviços estão ativos, o AnyConnect NAM tem precedência.

Mesmo quando o serviço NAM não é executado, ele ainda se conecta à API do Microsoft Windows e encaminha os pacotes EAP, o que pode causar problemas para o solicitante nativo do Microsoft Windows.

Aqui está um exemplo de tal fracasso.

Você habilita o rastreamento no Microsoft Windows com este comando:

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

Os rastreamentos (**c:\windows\trace\svchost_RASTLS.LOG**) mostram:

<#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)

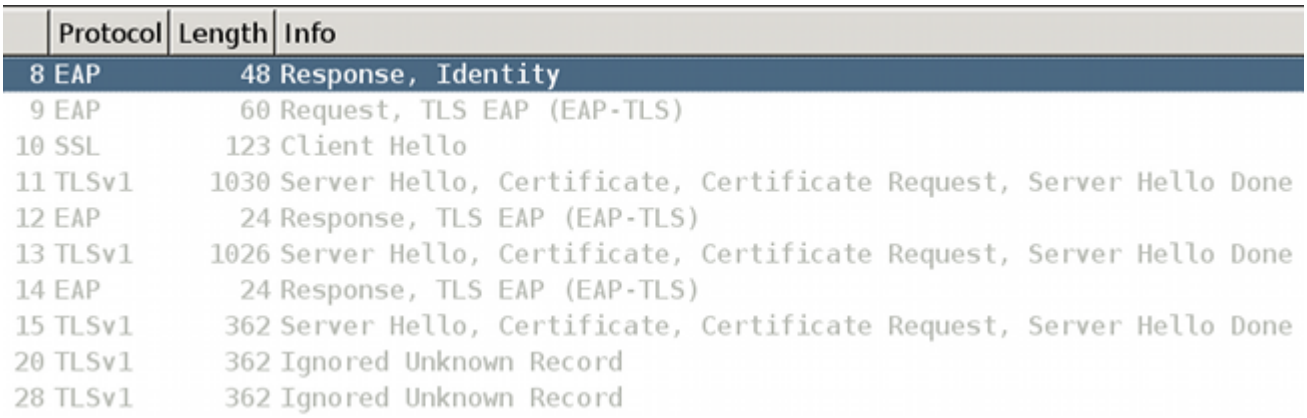
packet: Id: 125, Length:

1492

, Type: 13,

TLS blob length: 1819. Flags: LM

O último pacote é um certificado de cliente (fragmento 1 EAP-TLS com tamanho 1492 EAP) enviado pelo solicitante nativo do Microsoft Windows. Infelizmente, o Wireshark não mostra esse pacote:



	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

E esse pacote não é realmente enviado; o último era o terceiro fragmento do EAP-TLS que transportava o certificado do servidor.

Ele foi consumido pelo módulo NAM do AnyConnect que se conecta à API do Microsoft Windows.

É por isso que não é aconselhável usar o AnyConnect junto com o solicitante nativo do Microsoft Windows.

Quando você usa qualquer serviço do AnyConnect, é aconselhável usar o NAM também (quando serviços 802.1x são necessários), não o Microsoft Windows Native Supplicant.

Fragmentação

A fragmentação possivelmente ocorre em várias camadas:

- IP
- Pares de Valores de Atributos RADIUS (AVP)
- EAP-TLS

Os switches Cisco IOS® são muito inteligentes. Eles podem entender os formatos EAP e EAP-TLS.

Embora o switch não seja capaz de descriptografar o túnel TLS, ele é responsável pela fragmentação, montagem e remontagem dos pacotes EAP durante o encapsulamento no EAPoL (Extensible Authentication Protocol over LAN) ou no RADIUS.

O protocolo EAP não suporta fragmentação. Aqui está um trecho do RFC 3748 (EAP):

"A fragmentação não é suportada no próprio EAP; no entanto, métodos EAP individuais podem suportar isso."

O EAP-TLS é um exemplo. Aqui está um trecho do RFC 5216 (EAP-TLS), seção 2.1.5 (fragmentação):

"Quando um peer EAP-TLS recebe um pacote EAP-Request com o bit M definido, ELE DEVE responder com uma EAP-Response com EAP-Type=EAP-TLS e sem dados.

Isso serve como um ACK de fragmento. **O servidor EAP DEVE aguardar até receber a Resposta EAP antes de enviar outro fragmento**."

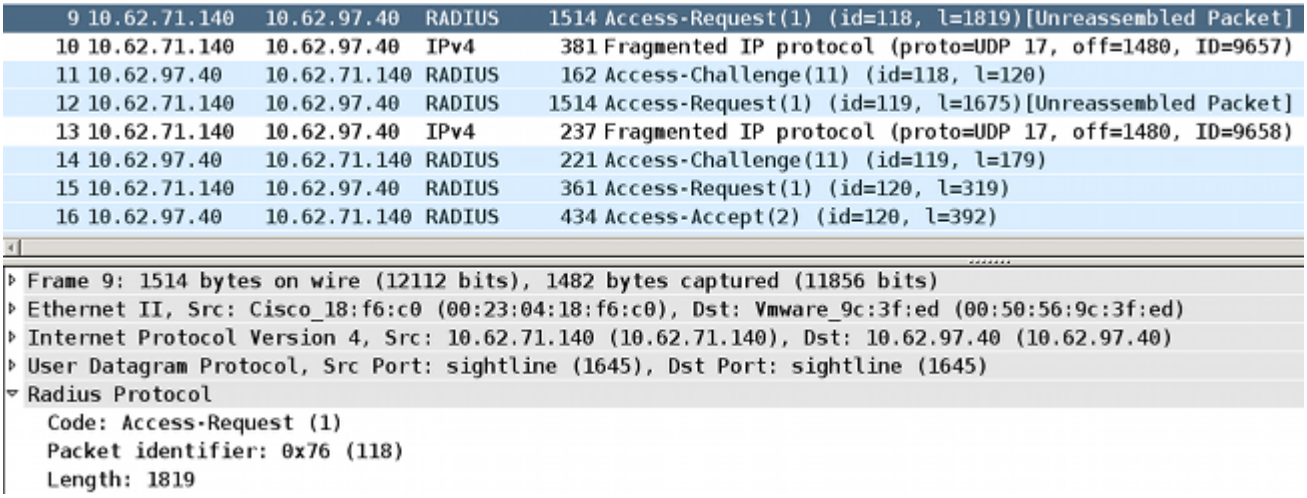
A última frase descreve um recurso muito importante dos servidores AAA. Eles devem aguardar o ACK antes de enviar outro fragmento EAP. Uma regra semelhante é usada para o requerente:

"O peer EAP DEVE aguardar até receber a EAP-Request antes de enviar outro fragmento."

Fragmentação na Camada IP

A fragmentação só pode ocorrer entre o Network Access Device (NAD) e o servidor AAA (IP/UDP/RADIUS usado como transporte).

Essa situação ocorre quando o NAD (switch Cisco IOS) tenta enviar a solicitação RADIUS que contém o payload EAP, que é maior que o MTU da interface:

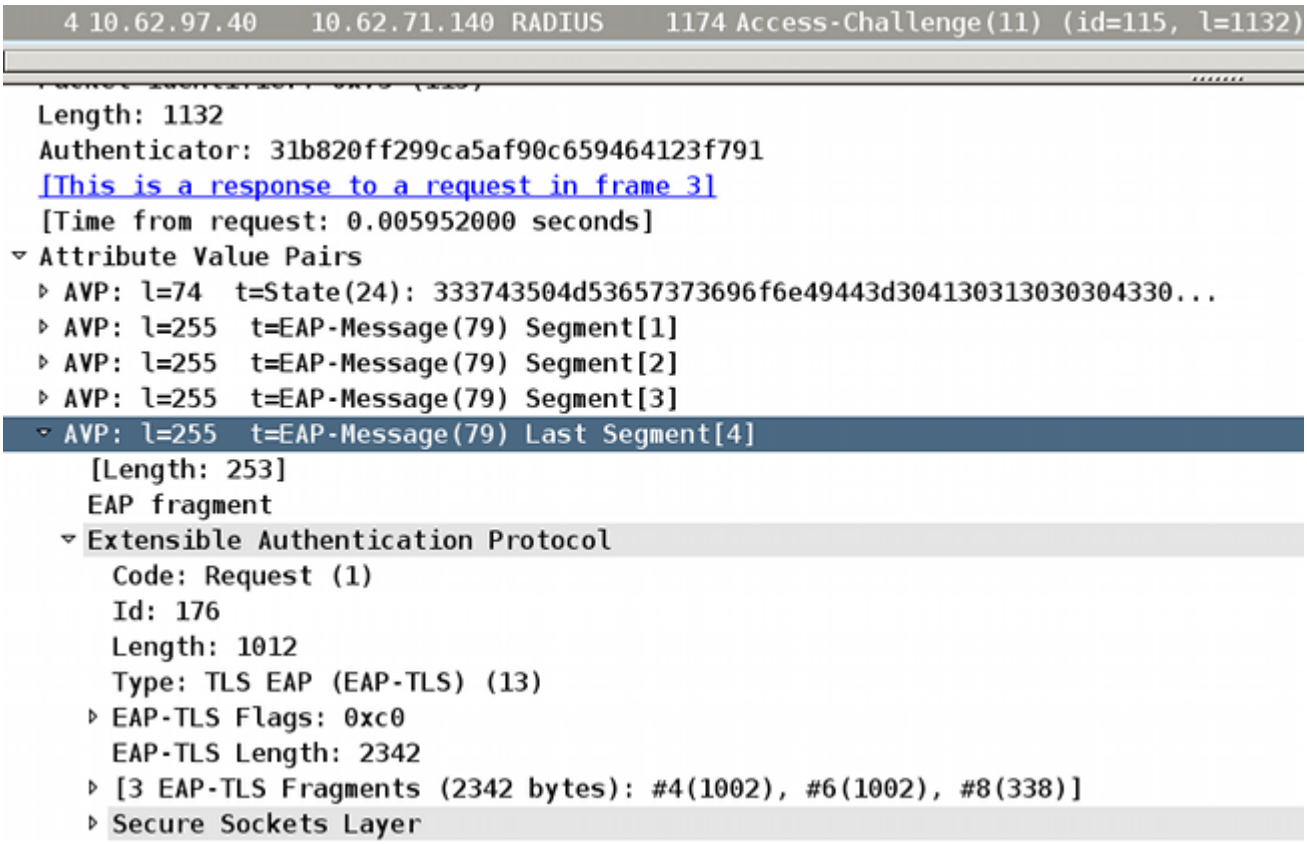


A maioria das versões do Cisco IOS não é inteligente o suficiente e não tenta montar pacotes EAP recebidos via EAPoL e combiná-los em um pacote RADIUS que possa caber na MTU da interface física em direção ao servidor AAA.

Os servidores AAA são mais inteligentes (conforme apresentado nas próximas seções).

Fragmentação em RADIUS

Na verdade, não se trata de qualquer tipo de fragmentação. De acordo com o RFC 2865, um único atributo RADIUS pode ter até 253 bytes de dados.Por isso, o payload EAP é sempre transmitido em vários atributos RADIUS de mensagem EAP:



Esses atributos de mensagem EAP são reagrupados e interpretados pelo Wireshark (o atributo "Último segmento" revela o payload de todo o pacote EAP).

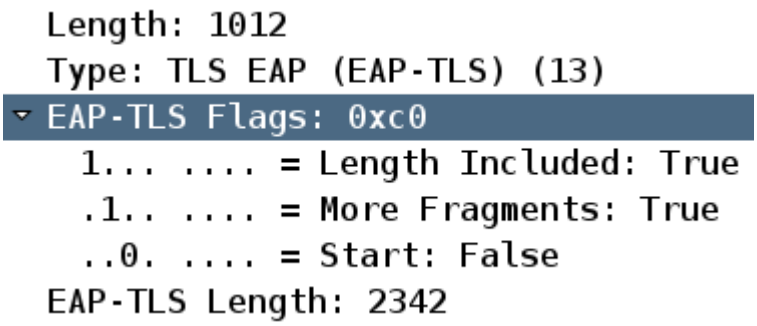
O cabeçalho Length no pacote EAP é igual a 1.012, e quatro AVPs RADIUS são necessários para transportá-lo.

Fragmentação em EAP-TLS

Na mesma captura de tela, você pode ver que:

- O comprimento do pacote EAP é 1.012
- O comprimento de EAP-TLS é 2.342

Isso sugere que é o primeiro fragmento EAP-TLS e o requerente espera mais, o que pode ser confirmado se você examinar as flags EAP-TLS:



Este tipo de fragmentação ocorre mais frequentemente em:

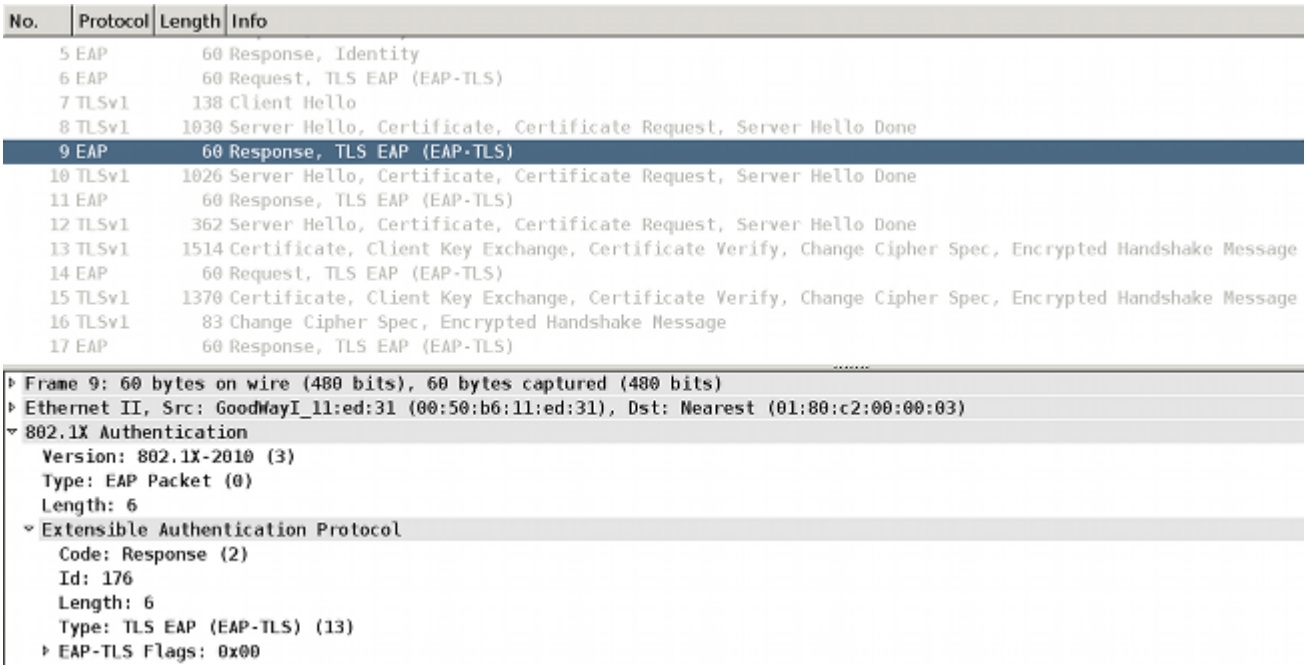
- RADIUS Access-Challenge enviado pelo servidor AAA, que transporta a EAP-Request com o Certificado de Servidor Secure Sockets Layer (SSL) com toda a cadeia.

- Solicitação de Acesso RADIUS enviada pelo NAD, que transporta a Resposta EAP com o Certificado de Cliente SSL com toda a cadeia.

Confirmação de fragmento EAP-TLS

Como explicado anteriormente, cada fragmento EAP-TLS deve ser confirmado antes que os fragmentos subsequentes sejam enviados.

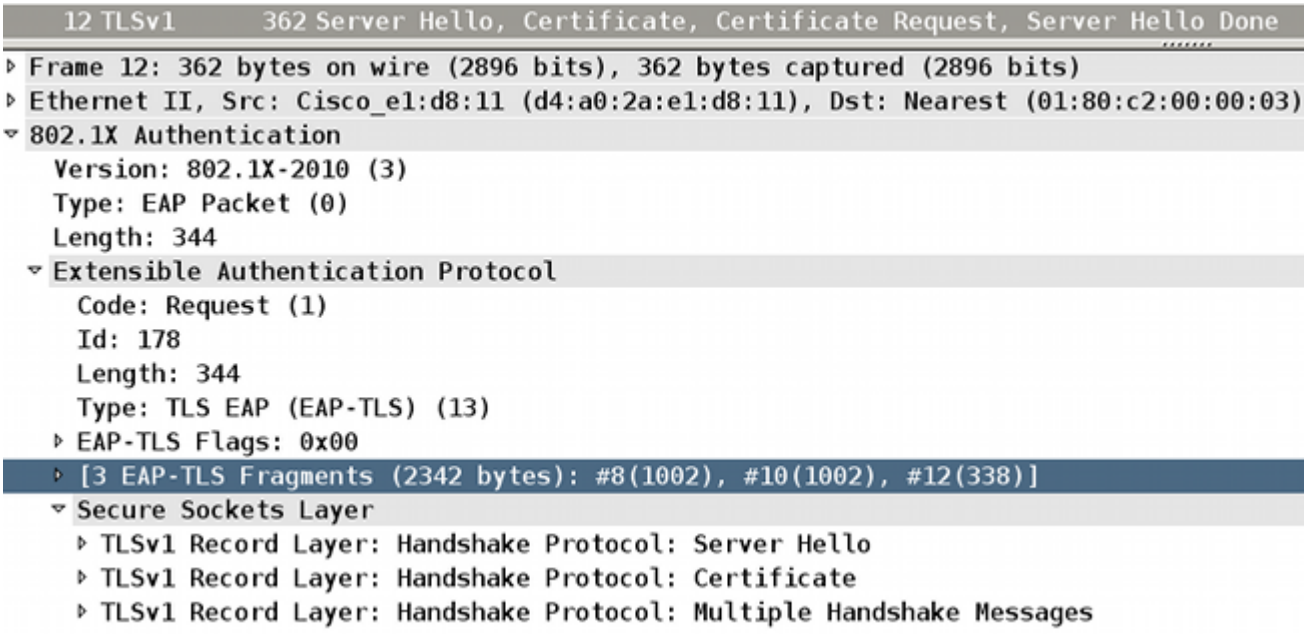
Aqui está um exemplo (capturas de pacotes para EAPoL entre o solicitante e o NAD):



Os quadros EAPoL e o servidor AAA retornam o certificado do servidor:

- Esse certificado é enviado em um fragmento EAP-TLS (pacote 8).
- O requerente reconhece esse fragmento (pacote 9).
- O segundo fragmento EAP-TLS é encaminhado pelo NAD (pacote 10).
- O requerente reconhece esse fragmento (pacote 11).
- O terceiro fragmento EAP-TLS é encaminhado pelo NAD (pacote 12).
- O suplicante não precisa confirmar isso; em vez disso, prossegue com o certificado do cliente que começa no pacote 13.

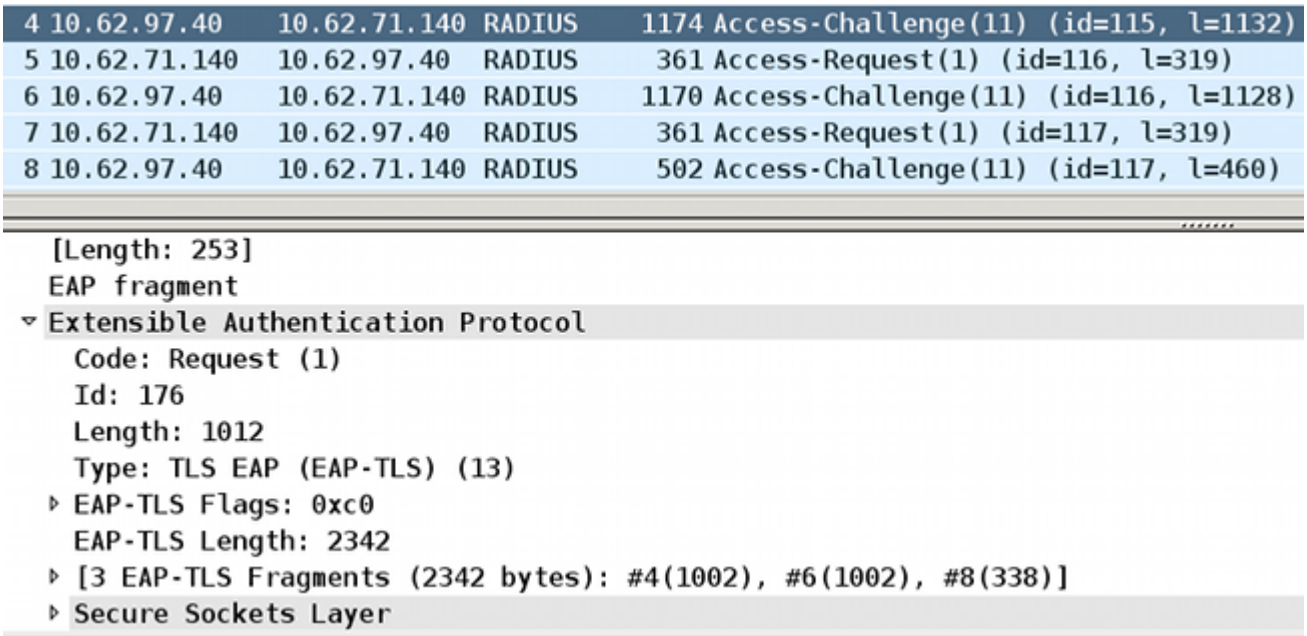
Aqui estão os detalhes do pacote 12:



Você pode ver que o Wireshark remontou os pacotes 8, 10 e 12.

O tamanho dos fragmentos EAP é 1.002, 1.002 e 338, o que eleva o tamanho total da mensagem EAP-TLS para 2342;

O comprimento total da mensagem EAP-TLS é anunciado em cada fragmento. Isso pode ser confirmado se você examinar pacotes RADIUS (entre o NAD e o servidor AAA):



Os pacotes RADIUS 4, 6 e 8 transportam esses três fragmentos EAP-TLS. Os dois primeiros fragmentos são reconhecidos.

O Wireshark é capaz de apresentar as informações sobre os fragmentos EAP-TLS (tamanho: 1.002 + 1.002 + 338 = 2.342).

Esse cenário e esse exemplo foram fáceis. O switch Cisco IOS não precisou alterar o tamanho do fragmento EAP-TLS.

Fragmentos EAP-TLS reagrupados com tamanhos diferentes

Considere o que acontece quando o NAD MTU em direção ao servidor AAA é 9.000 bytes (quadro jumbo) e o servidor AAA também está conectado com o uso da interface que suporta quadros jumbo.

A maioria dos suplicantes típicos estão conectados com o uso de um link de 1 Gbit com um MTU de 1.500.

Nesse cenário, o switch Cisco IOS executa a montagem e a remontagem "assimétrica" EAP-TLS e altera o tamanho dos fragmentos EAP-TLS.

Este é um exemplo de uma mensagem EAP grande enviada pelo servidor AAA (Certificado de servidor SSL):

1. O servidor AAA deve enviar uma mensagem EAP-TLS com um certificado de servidor SSL. O tamanho total desse pacote EAP é 3.000. Após ser encapsulado no RADIUS Access-Challenge/UDP/IP, ainda é menor que o MTU da interface do servidor AAA. Um único pacote IP é enviado com 12 atributos RADIUS EAP-Message. Não há fragmentação de IP nem EAP-TLS.

2. O switch Cisco IOS recebe esse pacote, desencapsula-o e decide que o EAP precisa ser enviado via EAPoL ao solicitante. Como o EAPoL não oferece suporte à fragmentação, o switch deve executar a fragmentação EAP-TLS.

3. O switch Cisco IOS prepara o primeiro fragmento EAP-TLS que pode caber no MTU da interface em direção ao solicitante (1.500).

4. Este fragmento é confirmado pelo requerente.

5. Outro fragmento EAP-TLS é enviado após o recebimento da confirmação.

6. Este fragmento é confirmado pelo requerente.

7. O último fragmento EAP-TLS é enviado pelo switch.

Este cenário revela que:

- Em algumas circunstâncias, o NAD deve criar fragmentos EAP-TLS.
- O NAD é responsável por enviar/confirmar esses fragmentos.

A mesma situação pode ocorrer para um suplicante conectado através de um link que suporta quadros jumbo enquanto o servidor AAA tem um MTU menor (em seguida, o switch Cisco IOS cria fragmentos EAP-TLS quando envia o pacote EAP para o servidor AAA).

Atributo RADIUS Framed-MTU

Para o RADIUS, há um atributo Framed-MTU definido no RFC 2865:

"Este atributo indica a unidade máxima de transmissão a ser configurada para o usuário quando não é negociada por outros meios (como o PPP). ELE PODE ser usado em pacotes Access-Accept.

ELE PODE ser usado em um pacote de solicitação de acesso como uma dica do NAS para o servidor de que preferiria esse valor, mas o servidor não precisa honrar a dica."

O ISE não honra a dica. O valor de Framed-MTU enviado pelo NAD na Solicitação de Acesso não tem nenhum impacto na fragmentação realizada pelo ISE.

Vários switches Cisco IOS modernos não permitem alterações no MTU da interface Ethernet, exceto para configurações de quadros jumbo ativadas globalmente no switch. A configuração de quadros jumbo impacta o valor do atributo Framed-MTU enviado na solicitação de acesso RADIUS. Por exemplo, você define:

<#root>

```
Switch(config)#
```

system mtu jumbo 9000

Isso força o switch a enviar Framed-MTU = 9000 em todas as Solicitações de Acesso RADIUS. O mesmo para a MTU do sistema sem quadros jumbo:

<#root>

```
Switch(config)#
```

system mtu 1600

Isso força o switch a enviar Framed-MTU = 1600 em todas as Solicitações de Acesso RADIUS.

Observe que os switches Cisco IOS modernos não permitem que você diminua o valor de MTU do sistema para menos de 1.500.

Servidores AAA e comportamento do suplicante ao enviar fragmentos EAP

ISE

O ISE sempre tenta enviar fragmentos EAP-TLS (geralmente um Hello de servidor com certificado) com 1.002 bytes de comprimento (embora o último fragmento geralmente seja menor).

Ele não honra o RADIUS Framed-MTU. Não é possível reconfigurá-lo para enviar fragmentos EAP-TLS maiores.

Servidor de Políticas de Rede (NPS) da Microsoft

É possível configurar o tamanho dos fragmentos EAP-TLS se você configurar o atributo Framed-MTU localmente no NPS.

Embora o artigo Configure the EAP Payload Size on Microsoft NPS mencione que o valor padrão de uma MTU enquadrada para o servidor RADIUS NPS é 1.500, o laboratório do Cisco Technical Assistance Center (TAC) mostrou que envia 2.000 com as configurações padrão (confirmadas em um Microsoft Windows 2012 Datacenter).

É testado que a configuração **Framed-MTU localmente** de acordo com o guia mencionado anteriormente é respeitada pelo NPS e fragmenta as mensagens EAP em fragmentos de um tamanho definido no Framed-MTU. Mas o atributo Framed-MTU recebido na solicitação de acesso não é usado (o mesmo que no ISE/ACS).

A definição deste valor é uma solução válida para corrigir problemas na topologia como este:

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

Atualmente, os switches não permitem que você defina o MTU por porta; para switches 6880, esse recurso é adicionado com o bug da Cisco ID CSCuo26327 - 802.1x EAP-TLS não funcionando em portas de host FEX.

AnyConnect

O AnyConnect envia fragmentos EAP-TLS (geralmente o certificado do cliente) com 1.486 bytes de comprimento. Para esse tamanho de valor, o quadro Ethernet é de 1.500 bytes. O último fragmento é geralmente menor.

Solicitante Nativo do Microsoft Windows

O Microsoft Windows envia fragmentos EAP-TLS (geralmente o certificado do cliente) que têm 1.486 ou 1.482 bytes de comprimento. Para esse tamanho de valor, o quadro Ethernet é de 1.500 bytes. O último fragmento é geralmente menor.

Informações Relacionadas

- **Configurando a autenticação baseada em porta IEEE 802.1x**
- **Suporte Técnico e Documentação - Cisco Systems**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.