Implémentations et comportement de fragmentation EAP

Table des matières

Introduction

Ce document décrit comment comprendre et dépanner les sessions EAP (Extensible Authentication Protocol).

Informations générales

Les sections de ce document sont consacrées aux domaines suivants :

- Comportement des serveurs AAA (Authentication, Authorization, and Accounting) lorsqu'ils renvoient le certificat de serveur pour la session EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)
- Comportement des demandeurs lorsqu'ils renvoient le certificat client pour la session EAP-

TLS
- Interopérabilité lorsque Microsoft Windows Native Supplicant et Cisco AnyConnect Network Access Manager (NAM) sont utilisés
- Fragmentation dans IP, RADIUS et EAP-TLS et processus de réassemblage effectué par les périphériques d'accès réseau
- Attribut RADIUS Framed-Maximum Transmission Unit (MTU)
- Comportement des serveurs AAA lorsqu'ils effectuent la fragmentation de paquets EAP-TLS

Conditions préalables

Exigences

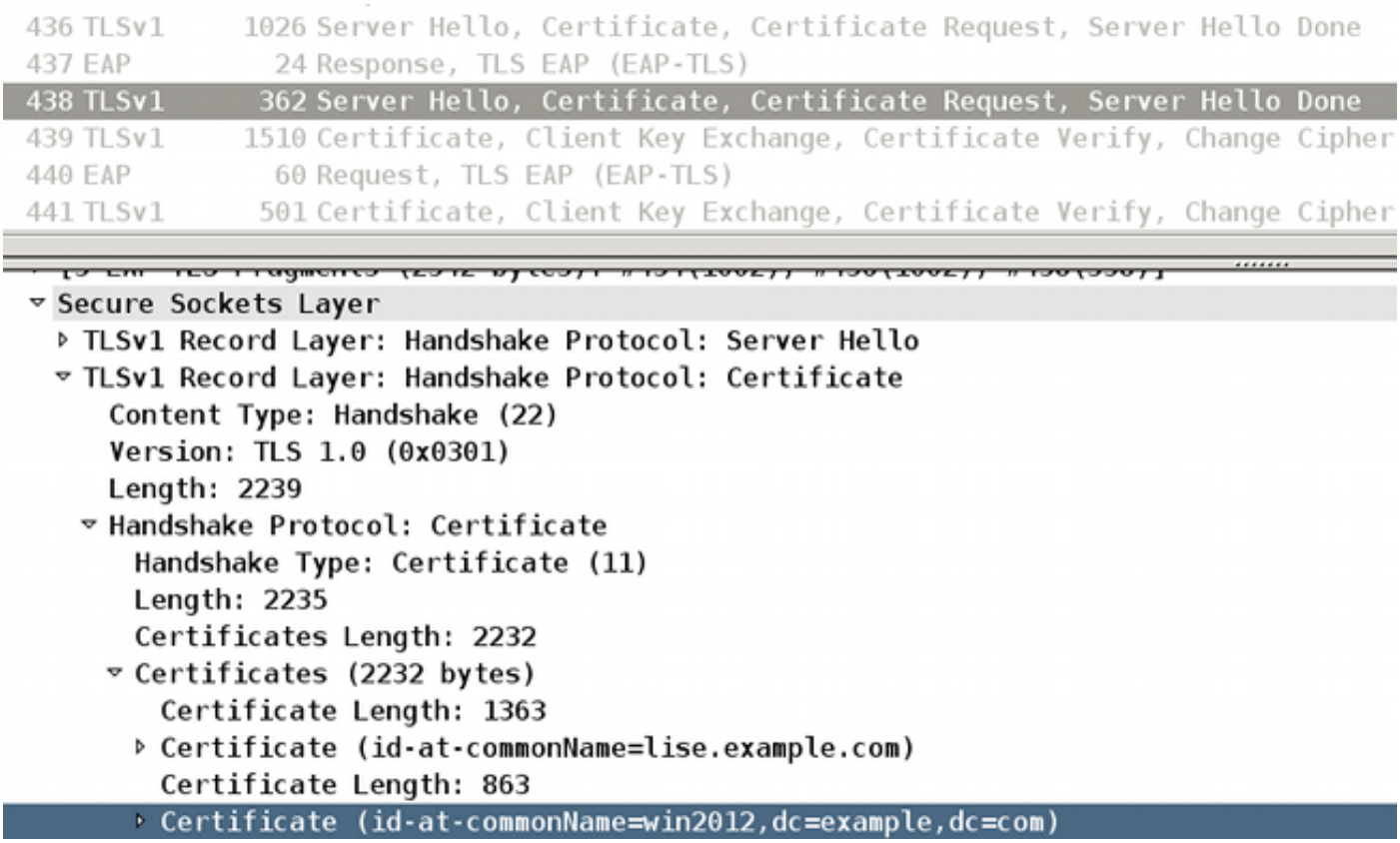
Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Protocoles EAP et EAP-TLS
- Configuration de Cisco Identity Services Engine (ISE)
- Configuration CLI des commutateurs Cisco Catalyst

Il est nécessaire d'avoir une bonne compréhension d'EAP et d'EAP-TLS afin de comprendre cet article.

Chaîne de certificats retournée par le serveur

Le serveur AAA (Access Control Server (ACS) et ISE) renvoie toujours la chaîne complète pour le paquet EAP-TLS avec le paquet Hello du serveur et le certificat du serveur :



Le certificat d'identité ISE (Common Name (CN)=lise.example.com) est renvoyé avec l'autorité de certification (CA) qui a signé le CN=win2012, dc=example, dc=com. Le comportement est le même pour ACS et ISE.

Chaîne de certificats retournée par le demandeur

Supplicant natif Microsoft Windows

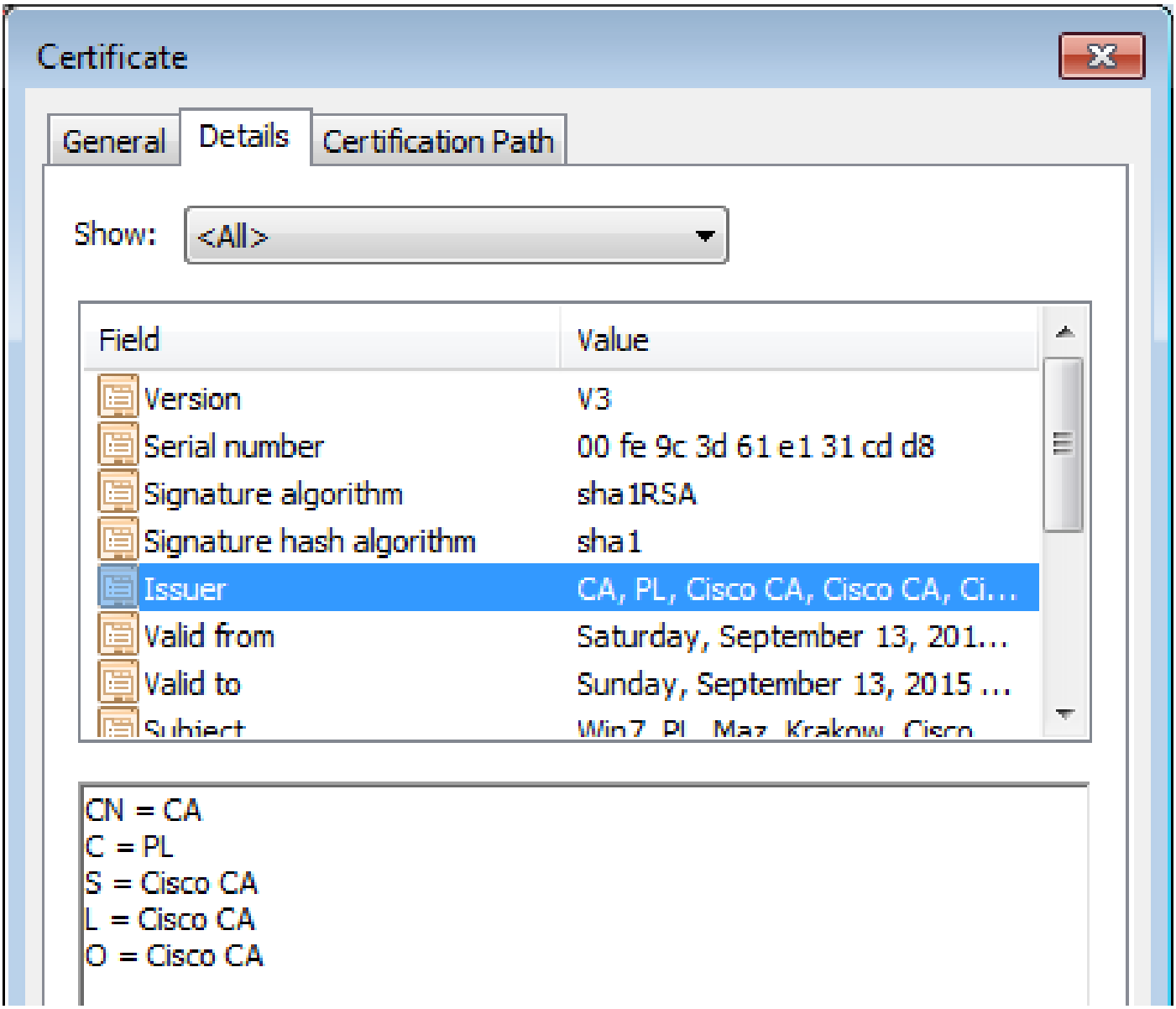
Microsoft Windows 7 Native supplicant configuré afin d'utiliser EAP-TLS, avec ou sans la « Sélection de certificat simple », n'envoie pas la chaîne complète du certificat client.

Ce comportement se produit même lorsque le certificat client est signé par une autre autorité de certification (chaîne différente) que le certificat serveur.

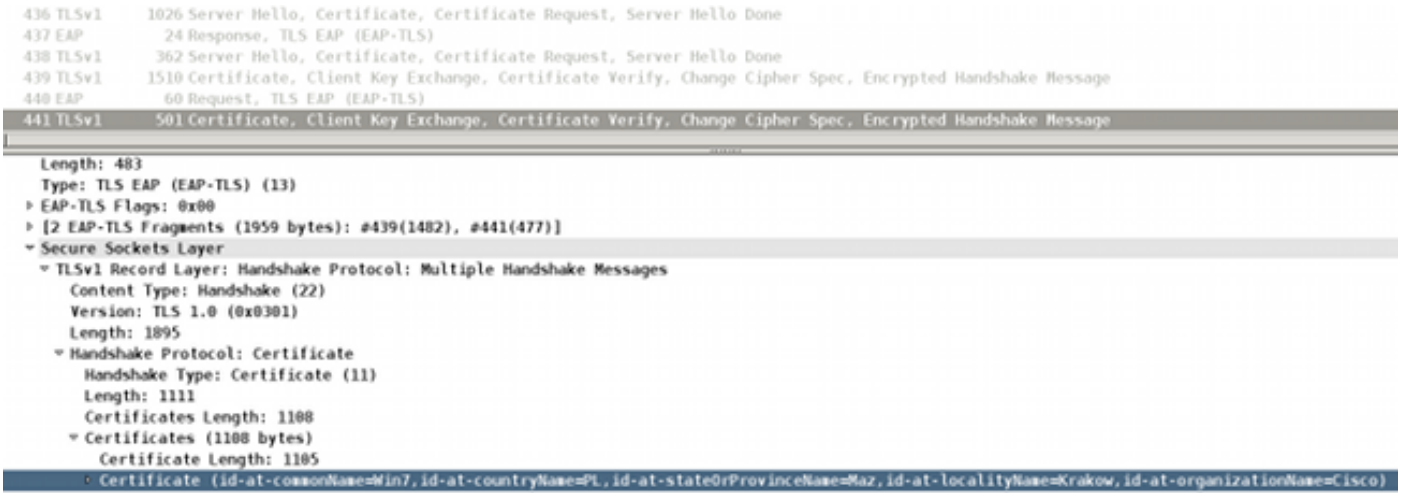
Cet exemple est lié au Hello et au certificat du serveur présentés dans la capture d'écran précédente.

Pour ce scénario, le certificat ISE est signé par l'autorité de certification avec l'utilisation d'un nom de sujet, CN=win2012, dc=example, dc=com.

Mais le certificat utilisateur installé dans le magasin Microsoft est signé par une autre autorité de certification, CN=CA, C=PL, S=Cisco CA, L=Cisco CA, O=Cisco CA.



Par conséquent, le demandeur Microsoft Windows répond uniquement avec le certificat client. L'autorité de certification qui la signe (CN=CA, S=PL, S=Cisco CA, L=Cisco CA, O=Cisco CA) n'est pas jointe.



En raison de ce comportement, les serveurs AAA peuvent rencontrer des problèmes lors de la

validation des certificats clients. L'exemple concerne Microsoft Windows 7 SP1 Professionnel.

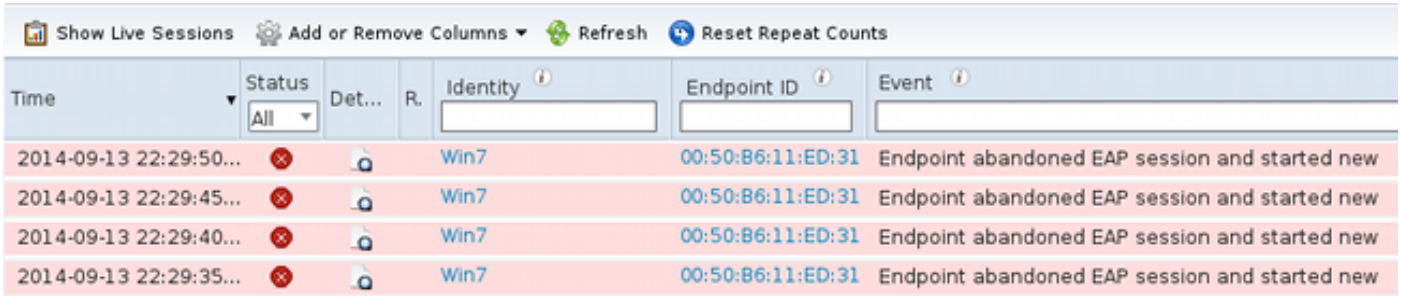
Solution

Une chaîne de certificats complète doit être installée sur le magasin de certificats d'ACS et d'ISE (tous les certificats clients de signature de CA et de sous-CA).

Les problèmes de validation de certificat peuvent être facilement détectés sur ACS ou ISE. Les informations relatives aux certificats non approuvés sont présentées et ISE signale :

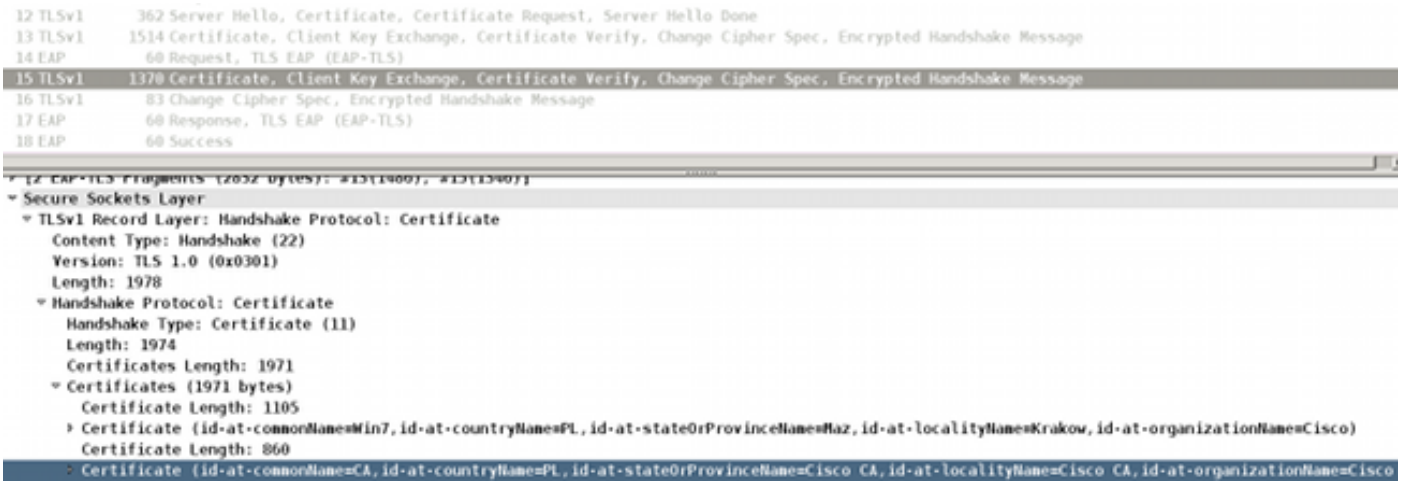
```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

Les problèmes de validation de certificat sur le demandeur ne sont pas facilement détectables. Généralement, le serveur AAA répond que « Endpoint a abandonné la session EAP » :



AnyConnect NAM

Le module NAM AnyConnect ne présente pas cette limitation. Dans le même scénario, il joint la chaîne complète du certificat client (l'autorité de certification appropriée est jointe) :



Supplicant natif Microsoft Windows avec AnyConnect NAM

Lorsque les deux services sont activés, AnyConnect NAM est prioritaire.

Même lorsque le service NAM ne s'exécute pas, il s'accroche toujours à l'API Microsoft Windows et transfère les paquets EAP, ce qui peut entraîner des problèmes pour le demandeur natif Microsoft Windows.

Voici un exemple d'un tel échec.

Vous activez le suivi sur Microsoft Windows avec cette commande :

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

Les traces (c:\windows\trace\svchost_RASTLS.LOG) montrent :

<#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)

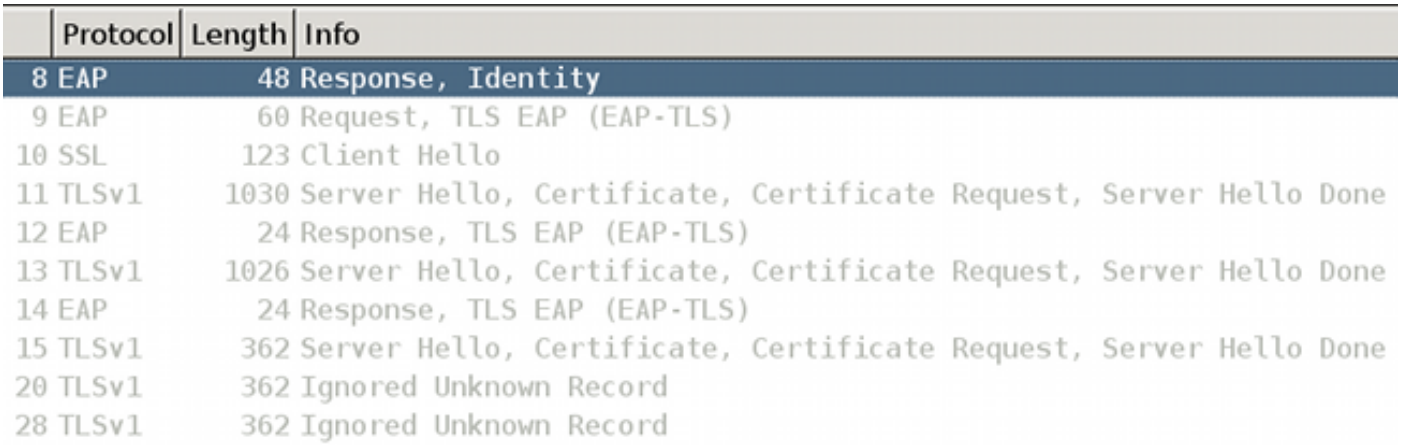
```
 packet: Id: 125, Length:
```

1492

```
, Type: 13,
```

TLS blob length: 1819. Flags: LM

Le dernier paquet est un certificat client (EAP-TLS fragment 1 avec EAP taille 1492) envoyé par le demandeur natif Microsoft Windows. Malheureusement, Wireshark n’affiche pas ce paquet :



	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

Et ce paquet n'est pas réellement envoyé ; le dernier était le troisième fragment du certificat de serveur porteur EAP-TLS.

Il a été utilisé par le module NAM AnyConnect qui s'accroche à l'API Microsoft Windows.

C'est pourquoi il est déconseillé d'utiliser AnyConnect avec le demandeur natif Microsoft Windows.

Lorsque vous utilisez des services AnyConnect, il est conseillé d'utiliser également NAM (lorsque des services 802.1x sont nécessaires), et non le demandeur natif Microsoft Windows.

Fragmentation

La fragmentation peut se produire sur plusieurs couches :

- IP
- Paires de valeurs d'attribut RADIUS (AVP)
- EAP-TLS

Les commutateurs Cisco IOS® sont très intelligents. Ils peuvent comprendre les formats EAP et EAP-TLS.

Bien que le commutateur ne puisse pas décrypter le tunnel TLS, il est responsable de la fragmentation, de l'assemblage et du réassemblage des paquets EAP lors de l'encapsulation dans le protocole EAPoL (Extensible Authentication Protocol over LAN) ou RADIUS.

Le protocole EAP ne gère pas la fragmentation. Voici un extrait de RFC 3748 (EAP) :

"La fragmentation n'est pas prise en charge dans EAP lui-même ; cependant, des méthodes EAP individuelles peuvent prendre en charge cela."

EAP-TLS en est un exemple. Voici un extrait de RFC 5216 (EAP-TLS), section 2.1.5 (fragmentation) :

"Lorsqu'un homologue EAP-TLS reçoit un paquet de requête EAP avec le bit M défini, il DOIT répondre avec une réponse EAP avec EAP-Type=EAP-TLS et aucune donnée.

Il s'agit d'un fragment ACK. Le serveur EAP DOIT attendre de recevoir la réponse EAP avant d'envoyer un autre fragment."

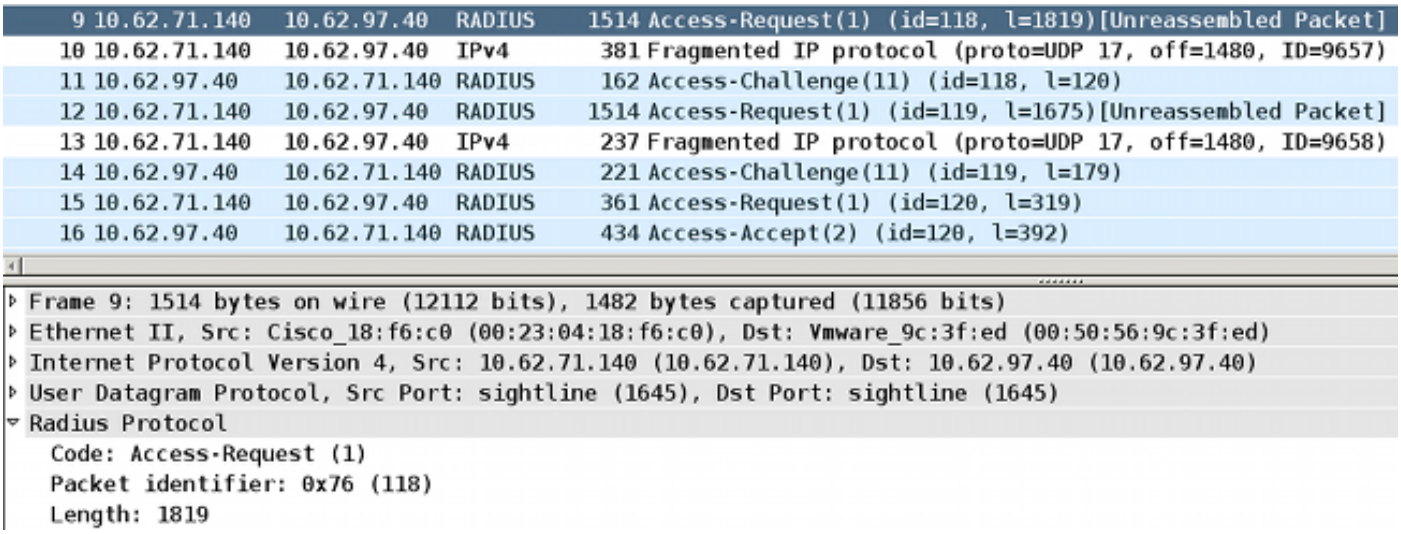
La dernière phrase décrit une fonctionnalité très importante des serveurs AAA. Ils doivent attendre l'accusé de réception avant de pouvoir envoyer un autre fragment EAP. Une règle similaire est utilisée pour le demandeur :

"L'homologue EAP DOIT attendre de recevoir la requête EAP avant d'envoyer un autre fragment."

Fragmentation dans la couche IP

La fragmentation ne peut se produire qu'entre le périphérique d'accès réseau (NAD) et le serveur AAA (IP/UDP/RADIUS utilisé comme transport).

Cette situation se produit lorsque NAD (commutateur Cisco IOS) tente d'envoyer la requête RADIUS qui contient la charge utile EAP, qui est plus grande que la MTU de l'interface :

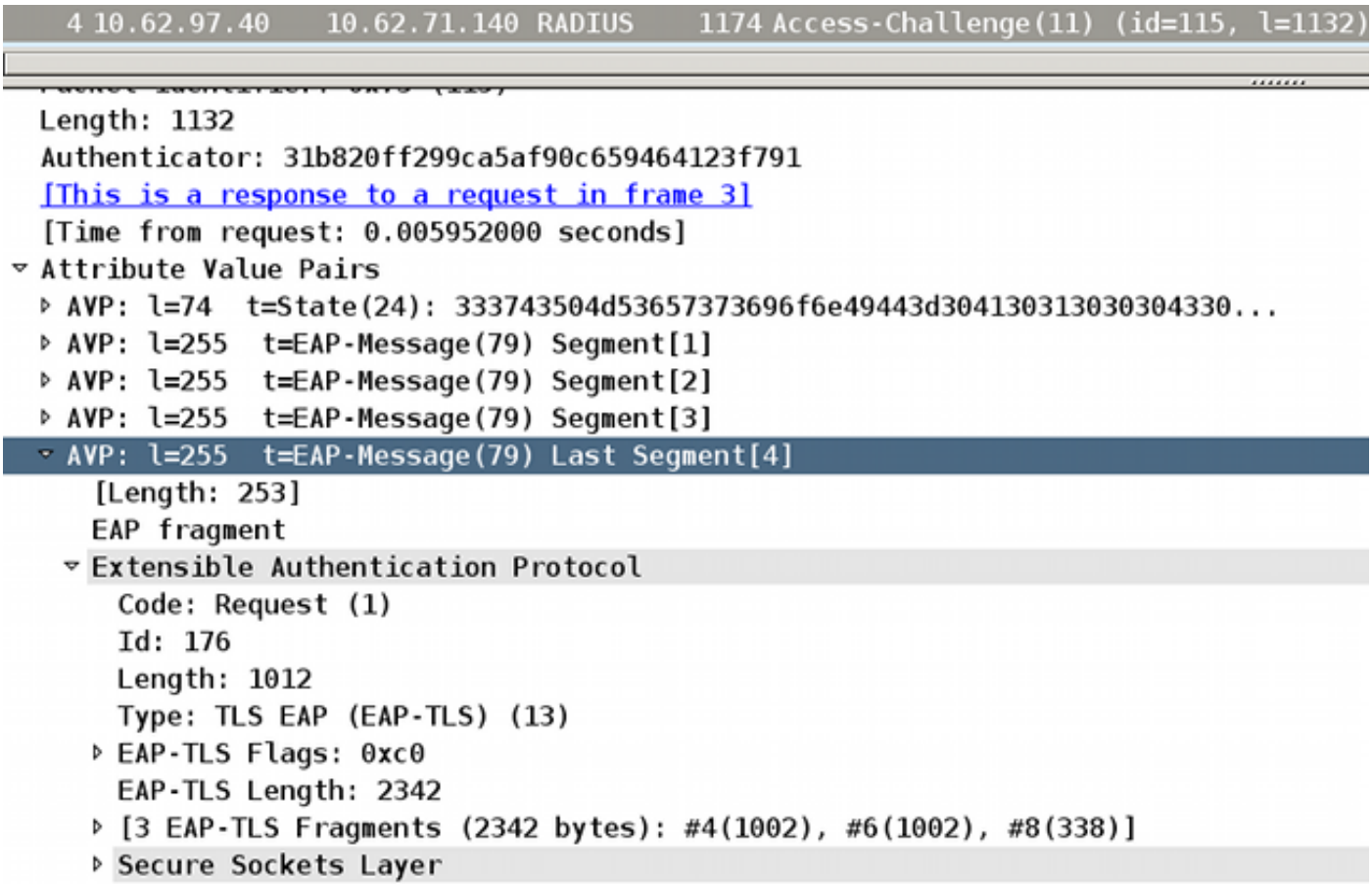


La plupart des versions de Cisco IOS ne sont pas assez intelligentes et n'essaient pas d'assembler les paquets EAP reçus via EAPoL et de les combiner dans un paquet RADIUS qui peut tenir dans le MTU de l'interface physique vers le serveur AAA.

Les serveurs AAA sont plus intelligents (comme présenté dans les sections suivantes).

Fragmentation dans RADIUS

Il ne s'agit pas vraiment d'une fragmentation. Conformément à la RFC 2865, un seul attribut RADIUS peut avoir jusqu'à 253 octets de données.De ce fait, la charge utile EAP est toujours transmise dans plusieurs attributs RADIUS EAP-Message :



Ces attributs EAP-Message sont réassemblés et interprétés par Wireshark (l'attribut « Last Segment » révèle la charge utile de l'ensemble du paquet EAP).

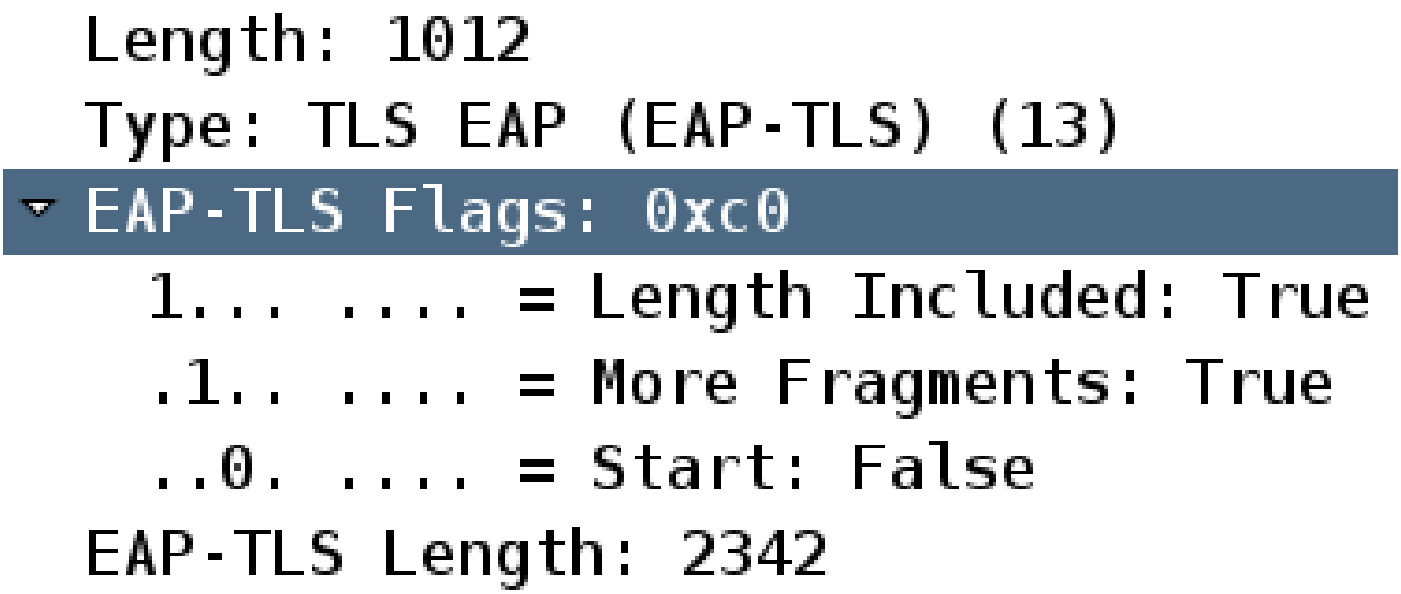
L'en-tête de longueur du paquet EAP est égal à 1 012, et quatre AVP RADIUS sont nécessaires pour le transporter.

Fragmentation dans EAP-TLS

Dans la même capture d'écran, vous pouvez voir que :

- La longueur du paquet EAP est de 1 012
- La longueur EAP-TLS est de 2 342

Cela suggère qu'il s'agit du premier fragment EAP-TLS et que le demandeur en attend plus, ce qui peut être confirmé si vous examinez les indicateurs EAP-TLS :



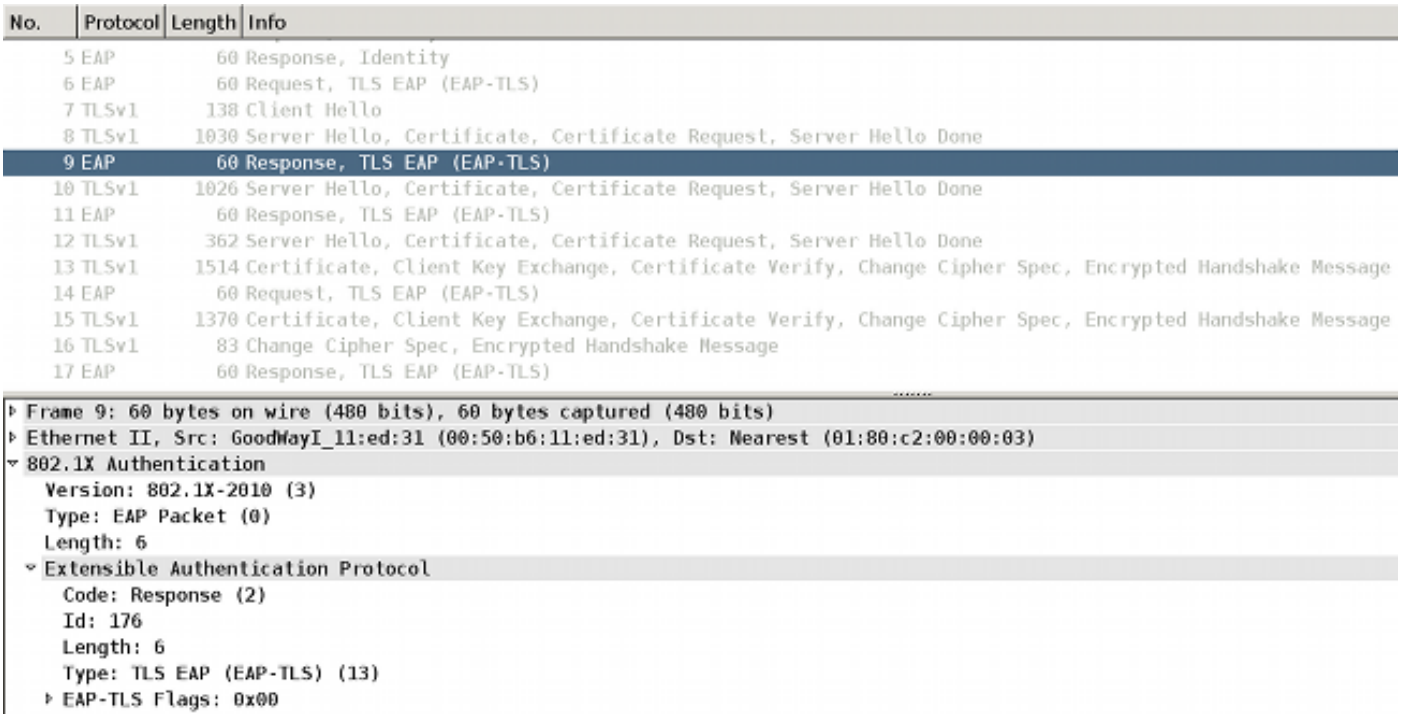
Ce type de fragmentation se produit le plus souvent dans :

- Le défi d'accès RADIUS envoyé par le serveur AAA, qui transporte la requête EAP avec le certificat de serveur SSL (Secure Sockets Layer) avec toute la chaîne.
- Demande d'accès RADIUS envoyée par NAD, qui transporte la réponse EAP avec le certificat client SSL avec toute la chaîne.

Confirmation de fragment EAP-TLS

Comme expliqué précédemment, chaque fragment EAP-TLS doit faire l'objet d'un accusé de réception avant que les fragments suivants ne soient envoyés.

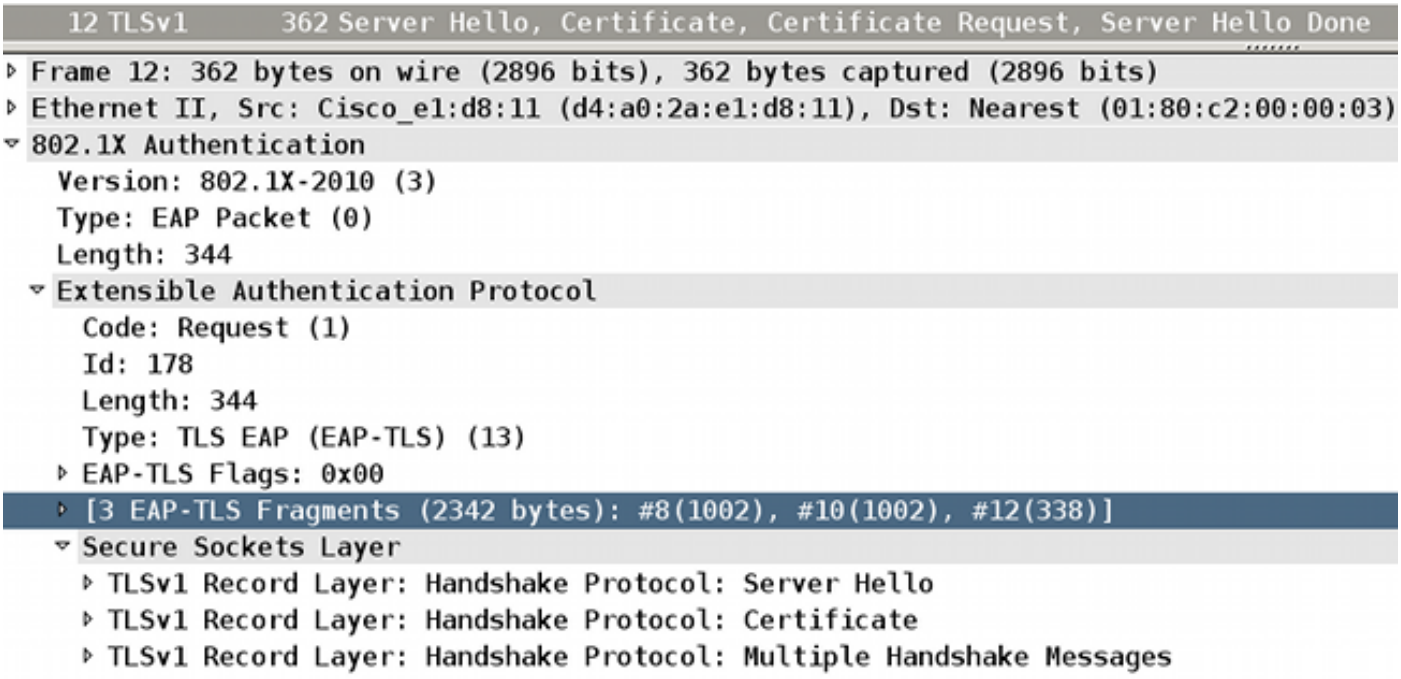
Voici un exemple (captures de paquets pour EAPoL entre le demandeur et le NAD) :



Les trames EAPoL et le serveur AAA renvoient le certificat du serveur :

- Ce certificat est envoyé dans un fragment EAP-TLS (paquet 8).
- Le demandeur accuse réception de ce fragment (paquet 9).
- Le deuxième fragment EAP-TLS est transmis par NAD (paquet 10).
- Le demandeur reconnaît ce fragment (paquet 11).
- Le troisième fragment EAP-TLS est transmis par NAD (paquet 12).
- Le demandeur n'a pas besoin d'accuser réception de cette demande ; il poursuit plutôt avec le certificat client qui commence au paquet 13.

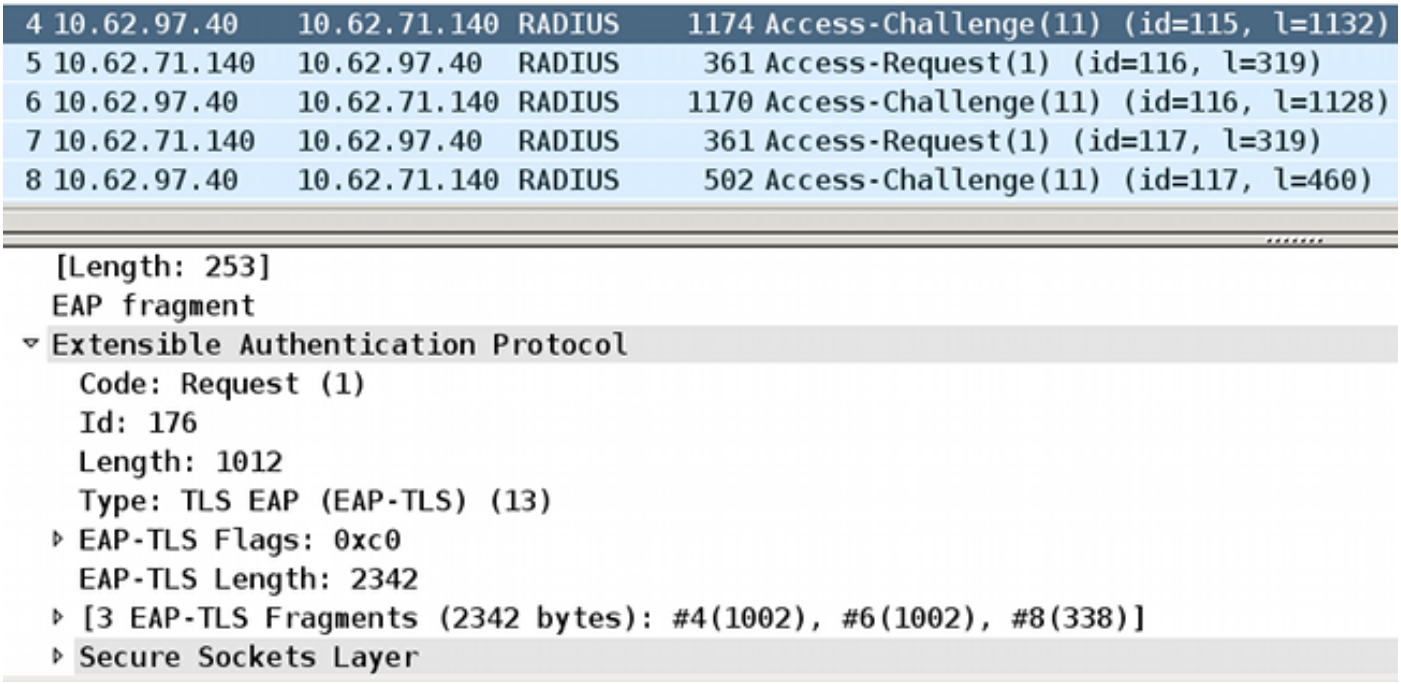
Voici les détails du paquet 12 :



Vous pouvez voir que Wireshark a réassemblé les paquets 8, 10 et 12.

La taille des fragments EAP est de 1 002, 1 002 et 338, ce qui porte la taille totale du message EAP-TLS à 2 342 ;

La longueur totale du message EAP-TLS est annoncée dans chaque fragment. Ceci peut être confirmé si vous examinez les paquets RADIUS (entre NAD et le serveur AAA) :



Les paquets RADIUS 4, 6 et 8 transportent ces trois fragments EAP-TLS. Les deux premiers fragments sont reconnus.

Wireshark peut présenter les informations relatives aux fragments EAP-TLS (taille : 1 002 + 1 002 + 338 = 2 342).

Ce scénario et cet exemple étaient faciles. Le commutateur Cisco IOS n'a pas besoin de modifier la taille du fragment EAP-TLS.

Fragments EAP-TLS réassemblés avec une taille différente

Imaginez ce qui se passe lorsque la MTU NAD vers le serveur AAA est de 9 000 octets (trame jumbo) et que le serveur AAA est également connecté à l'aide de l'interface qui prend en charge les trames jumbo.

La plupart des demandeurs typiques sont connectés à l'aide d'une liaison de 1 Gbit avec une MTU de 1 500.

Dans un tel scénario, le commutateur Cisco IOS effectue un assemblage et un réassemblage « asymétrique » EAP-TLS et modifie la taille des fragments EAP-TLS.

Voici un exemple de message EAP volumineux envoyé par le serveur AAA (SSL Server Certificate) :

1. Le serveur AAA doit envoyer un message EAP-TLS avec un certificat de serveur SSL. La taille totale de ce paquet EAP est de 3 000. Une fois encapsulé dans RADIUS Access-Challenge/UDP/IP, il est toujours inférieur à la MTU de l'interface du serveur AAA. Un seul paquet IP est envoyé avec 12 attributs RADIUS EAP-Message. Il n'y a pas de fragmentation IP ou EAP-TLS.

2. Le commutateur Cisco IOS reçoit un tel paquet, le décapsule et décide qu’EAP doit être

envoyé via EAPoL au demandeur. EAPoL ne prenant pas en charge la fragmentation, le commutateur doit effectuer la fragmentation EAP-TLS.

3. Le commutateur Cisco IOS prépare le premier fragment EAP-TLS qui peut s'insérer dans le MTU de l'interface vers le demandeur (1 500).

4. Ce fragment est confirmé par le demandeur.

5. Un autre fragment EAP-TLS est envoyé après réception de l'accusé de réception.

6. Ce fragment est confirmé par le demandeur.

7. Le commutateur envoie le dernier fragment EAP-TLS.

Ce scénario révèle que :

- Dans certaines circonstances, le NAD doit créer des fragments EAP-TLS.
- Le NAD est responsable de l'envoi/de la reconnaissance de ces fragments.

La même situation peut se produire pour un demandeur connecté via une liaison qui prend en charge les trames jumbo alors que le serveur AAA a une MTU plus petite (alors le commutateur Cisco IOS crée des fragments EAP-TLS quand il envoie le paquet EAP vers le serveur AAA).

Attribut RADIUS Framed-MTU

Pour RADIUS, il existe un attribut Framed-MTU défini dans RFC 2865 :

Cet attribut indique l'unité de transmission maximale à configurer pour l'utilisateur, lorsqu'elle n'est pas négociée par un autre moyen (tel que PPP). Il PEUT être utilisé dans les paquets d'acceptation d'accès.

Il PEUT être utilisé dans un paquet de requête d'accès comme indication par le NAS au serveur qu'il préférerait cette valeur, mais le serveur n'est pas tenu d'honorer l'indication."

ISE ne tient pas compte de cet indice. La valeur de Framed-MTU envoyée par NAD dans la requête d'accès n'a aucun impact sur la fragmentation effectuée par ISE.

Plusieurs commutateurs Cisco IOS modernes ne permettent pas de modifier la MTU de l'interface Ethernet, à l'exception des paramètres de trames jumbo activés globalement sur le commutateur. La configuration des trames jumbo a un impact sur la valeur de l'attribut Framed-MTU envoyé dans la requête d'accès RADIUS. Par exemple, vous définissez :

<#root>

```
Switch(config)#
system mtu jumbo 9000
```

Ceci force le commutateur à envoyer Framed-MTU = 9000 dans toutes les demandes d'accès RADIUS. Idem pour le MTU système sans trames jumbo :

<#root>

```
Switch(config)#
```

```
system mtu 1600
```

Ceci force le commutateur à envoyer Framed-MTU = 1600 dans toutes les demandes d'accès RADIUS.

Notez que les commutateurs Cisco IOS modernes ne vous permettent pas de diminuer la valeur MTU du système en dessous de 1 500.

Serveurs AAA et comportement du demandeur lorsque vous envoyez des fragments EAP

ISE

ISE essaie toujours d'envoyer des fragments EAP-TLS (généralement Server Hello avec certificat) de 1 002 octets (bien que le dernier fragment soit généralement plus petit).

Il n'honore pas le MTU tramé RADIUS. Il n'est pas possible de le reconfigurer pour envoyer de plus gros fragments EAP-TLS.

Serveur NPS (Network Policy Server) Microsoft

Il est possible de configurer la taille des fragments EAP-TLS si vous configurez l'attribut Framed-MTU localement sur NPS.

Même si l'article Configure the EAP Payload Size on Microsoft NPS mentionne que la valeur par défaut d'un MTU tramé pour le serveur NPS RADIUS est 1 500, les travaux pratiques du Centre d'assistance technique Cisco (TAC) ont montré qu'il envoie 2 000 avec les paramètres par défaut (confirmés dans un data center Microsoft Windows 2012).

Il est testé que la configuration Framed-MTU localement selon le guide mentionné précédemment est respectée par NPS, et il fragmente les messages EAP en fragments d'une taille définie dans Framed-MTU. Mais l'attribut Framed-MTU reçu dans la requête d'accès n'est pas utilisé (identique à celui sur ISE/ACS).

Définir cette valeur est une solution de contournement valide afin de résoudre les problèmes dans la topologie comme ceci :

Demandeur [MTU 1500] ---- ---- [MTU 9000]Commutateur[MTU 9000] ----- ----- [MTU 9000]NPS

Actuellement, les commutateurs ne vous permettent pas de définir la MTU par port ; pour les

commutateurs 6880, cette fonctionnalité est ajoutée avec l'ID de bogue Cisco CSCuo26327 - 802.1x EAP-TLS ne fonctionne pas sur les ports hôtes FEX.

AnyConnect

AnyConnect envoie des fragments EAP-TLS (généralement un certificat client) de 1 486 octets. Pour cette valeur, la trame Ethernet est de 1 500 octets. Le dernier fragment est généralement plus petit.

Supplicant natif Microsoft Windows

Microsoft Windows envoie des fragments EAP-TLS (généralement un certificat client) de 1 486 ou 1 482 octets. Pour cette valeur, la trame Ethernet est de 1 500 octets. Le dernier fragment est généralement plus petit.

Informations connexes

- Configuration de l'authentification basée sur les ports IEEE 802.1x
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.