Implementierung und Verhalten der EAP-Fragmentierung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie EAP-Sitzungen (Extensible Authentication Protocol) verstehen und Fehler bei diesen beheben.

Hintergrundinformationen

Die Abschnitte dieses Dokuments behandeln folgende Bereiche:

- Verhalten von AAA-Servern (Authentication, Authorization und Accounting), wenn diese das Serverzertifikat für die EAP-TLS-Sitzung (Extensible Authentication Protocol-Transport Layer Security) zurückgeben
- Verhalten von Supplicants, die das Client-Zertifikat für die EAP-TLS-Sitzung zurückgeben
- Interoperabilität bei Verwendung von Microsoft Windows Native Supplicant und Cisco AnyConnect Network Access Manager (NAM)
- Fragmentierung von IP-, RADIUS- und EAP-TLS sowie Reassemblierung durch Netzwerkzugriffsgeräte
- Das RADIUS Framed-Maximum Transmission Unit (MTU)-Attribut
- Verhalten der AAA-Server bei der Fragmentierung von EAP-TLS-Paketen

Voraussetzungen

Anforderungen

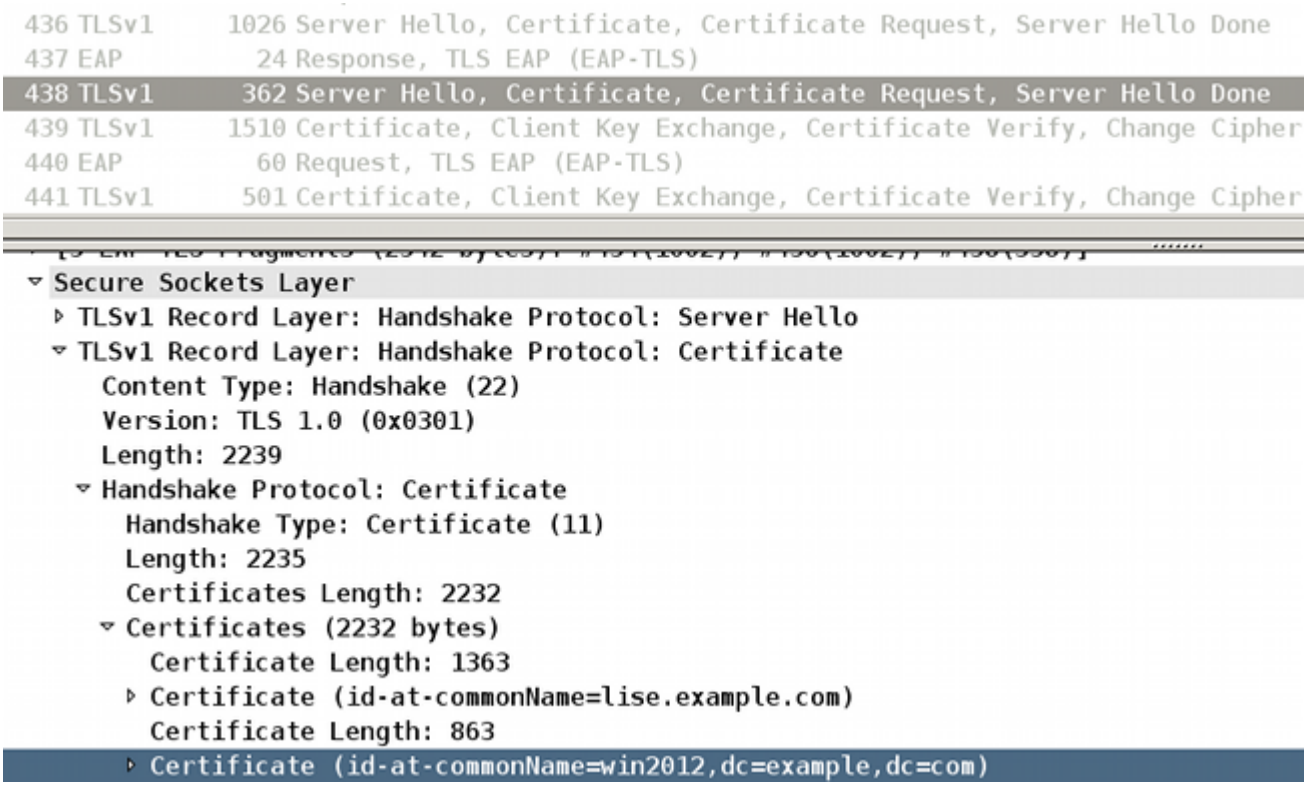
Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- EAP- und EAP-TLS-Protokolle
- Konfiguration der Cisco Identity Services Engine (ISE)
- CLI-Konfiguration von Cisco Catalyst Switches

Um diesen Artikel zu verstehen, ist ein gutes Verständnis von EAP und EAP-TLS erforderlich.

Vom Server zurückgegebene Zertifikatskette

Der AAA-Server (Access Control Server (ACS) und die ISE) geben immer die vollständige Kette für das EAP-TLS-Paket mit dem Server Hello und dem Serverzertifikat zurück:



Das ISE-Identitätszertifikat (Common Name (CN)=lise.example.com) wird zusammen mit der Zertifizierungsstelle zurückgegeben, die CN=win2012,dc=example,dc=com signiert hat. Das Verhalten ist für ACS und ISE identisch.

Vom Supplicant zurückgegebene Zertifikatskette

Microsoft Windows Native Supplicant

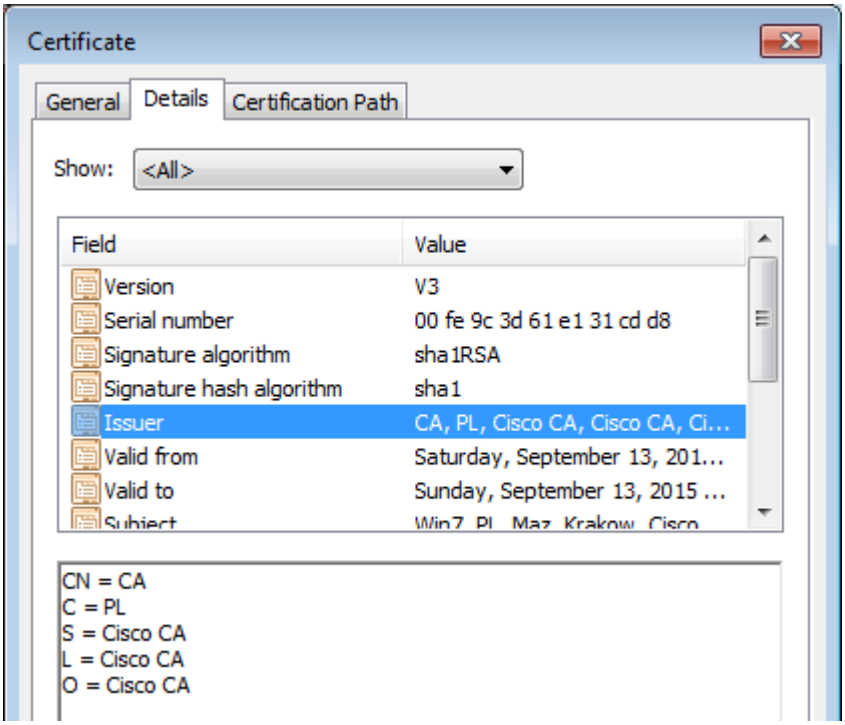
Die systemeigene Komponente von Microsoft Windows 7, die für die Verwendung von EAP-TLS konfiguriert wurde, sendet mit oder ohne "Einfache Zertifikatauswahl" nicht die gesamte Kette des Clientzertifikats.

Dieses Verhalten tritt auch dann auf, wenn das Clientzertifikat von einer anderen Zertifizierungsstelle (einer anderen Kette) signiert wird als das Serverzertifikat.

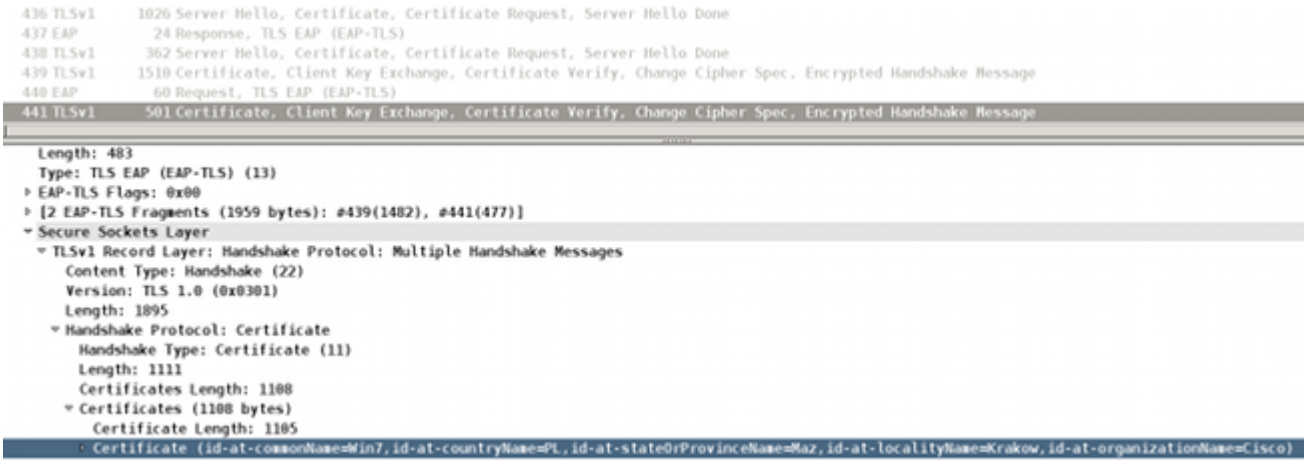
Dieses Beispiel bezieht sich auf den Server Hello und das Zertifikat im vorherigen Screenshot.

In diesem Szenario wird das ISE-Zertifikat von der Zertifizierungsstelle signiert, wobei der Antragstellername CN=win2012,dc=example,dc=com verwendet wird.

Das im Microsoft Store installierte Benutzerzertifikat wird jedoch von einer anderen Zertifizierungsstelle signiert: CN=CA,C=PL,S=Cisco CA,L=Cisco CA, O=Cisco CA.



Daher antwortet die Microsoft Windows-Komponente nur mit dem Clientzertifikat. Die Zertifizierungsstelle, die sie signiert (CN=CA,S=PL,S=Cisco CA, L=Cisco CA, O=Cisco CA), ist nicht angeschlossen.



Aufgrund dieses Verhaltens kann es bei den AAA-Servern zu Problemen kommen, wenn sie Client-Zertifikate validieren. Das Beispiel bezieht sich auf Microsoft Windows 7 SP1 Professional.

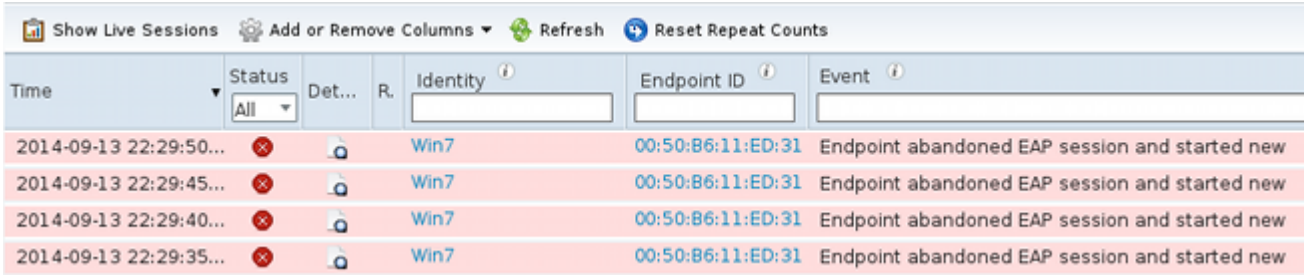
Lösung

Im Zertifikatspeicher von ACS und ISE ist eine vollständige Zertifikatskette zu installieren (alle CA- und Sub-CA-Signaturclientzertifikate).

Probleme mit der Zertifikatsvalidierung können auf ACS oder ISE leicht erkannt werden. Informationen über nicht vertrauenswürdiges Zertifikat werden angezeigt, und die ISE meldet:

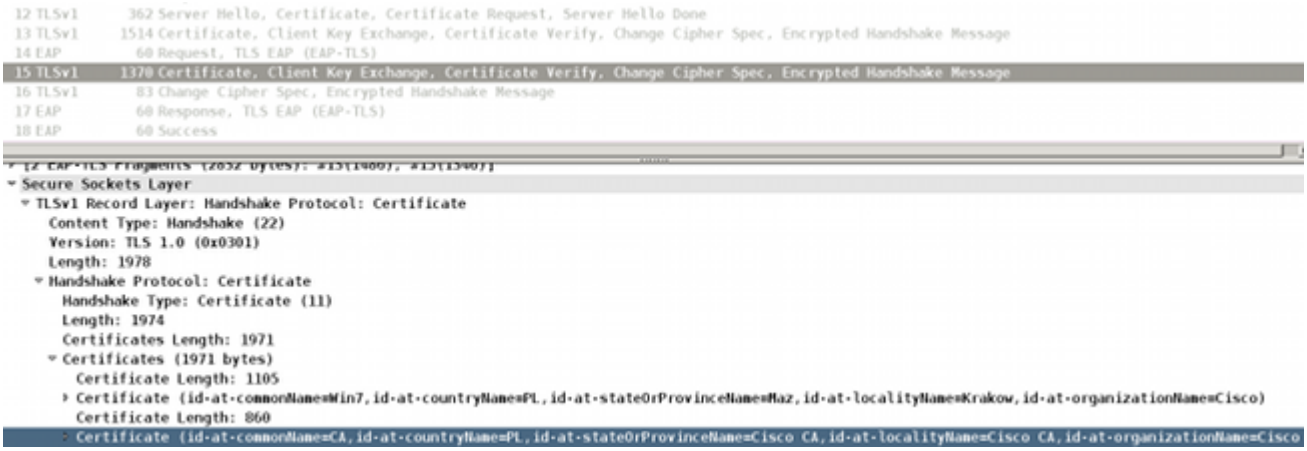
```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

Probleme mit der Zertifikatsvalidierung auf dem Supplicant sind nicht leicht erkennbar. Normalerweise antwortet der AAA-Server, dass die EAP-Sitzung vom Endpunkt abgebrochen wurde:



AnyConnect NAM

Das AnyConnect NAM unterliegt dieser Einschränkung nicht. Im gleichen Szenario wird die gesamte Kette des Client-Zertifikats angefügt (die richtige Zertifizierungsstelle ist angefügt):



Microsoft Windows Native Supplicant und AnyConnect NAM

Wenn beide Dienste aktiv sind, hat AnyConnect NAM Vorrang.

Auch wenn der NAM-Dienst nicht ausgeführt wird, greift er auf die Microsoft Windows-API zu und leitet die EAP-Pakete weiter, was zu Problemen mit der Microsoft Windows Native-Komponente führen kann.

Hier ist ein Beispiel für einen solchen Misserfolg.

Mit dem folgenden Befehl aktivieren Sie die Ablaufverfolgung unter Microsoft Windows:

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

Die Traces (**c:\windows\trace\svchost_RASTLS.LOG**) zeigen:

<#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)

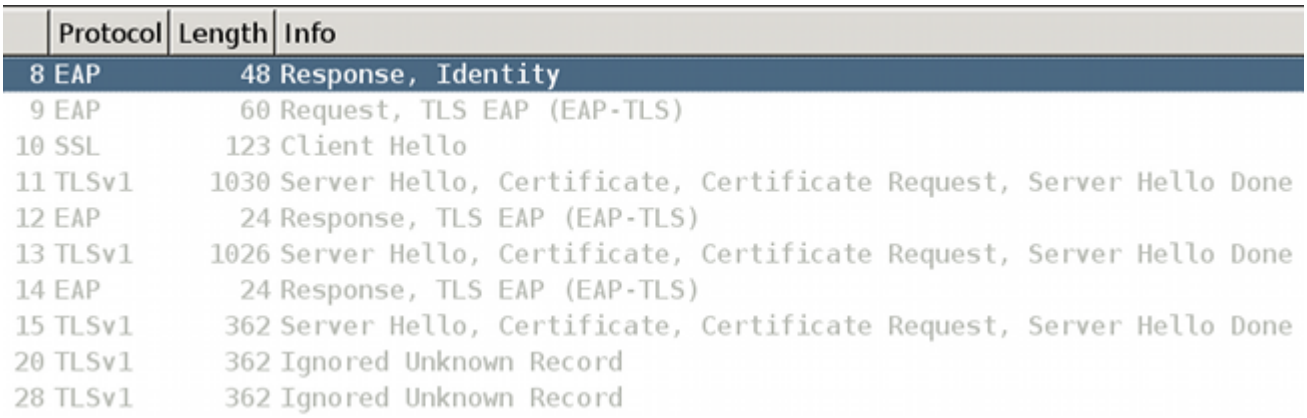
```
 packet: Id: 125, Length:
```

1492

```
, Type: 13,
```

TLS blob length: 1819. Flags: LM

Das letzte Paket ist ein Client-Zertifikat (EAP-TLS-Fragment 1 mit EAP-Größe 1492), das von der Microsoft Windows Native-Komponente gesendet wird. Leider zeigt Wireshark dieses Paket nicht an:



	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

Und dieses Paket wird nicht wirklich versendet; das letzte war das dritte Fragment des EAP-TLS tragenden Serverzertifikats.

Es wurde vom AnyConnect NAM-Modul verwendet, das an die Microsoft Windows-API angeschlossen ist.

Daher wird nicht empfohlen, AnyConnect zusammen mit der Microsoft Windows Native-Komponente zu verwenden.

Wenn Sie AnyConnect-Dienste verwenden, wird empfohlen, auch NAM (wenn 802.1x-Dienste erforderlich sind) und nicht die native Microsoft Windows-Komponente zu verwenden.

Fragmentierung

Die Fragmentierung kann auf mehreren Ebenen auftreten:

- IP
- RADIUS-Attributwertpaare (AVP)
- EAP-TLS

Cisco IOS® Switches sind sehr intelligent. Sie können die Formate EAP und EAP-TLS verstehen.

Obwohl der Switch den TLS-Tunnel nicht entschlüsseln kann, ist er für die Fragmentierung sowie die Zusammenstellung und Reassemblierung der EAP-Pakete bei der Kapselung in Extensible Authentication Protocol over LAN (EAPoL) oder RADIUS verantwortlich.

Das EAP-Protokoll unterstützt keine Fragmentierung. Hier ein Auszug aus RFC 3748 (EAP):

"Fragmentierung wird innerhalb des EAP selbst nicht unterstützt. Einzelne EAP-Methoden können dies jedoch unterstützen."

EAP-TLS ist ein solches Beispiel. Hier ein Auszug aus RFC 5216 (EAP-TLS), Abschnitt 2.1.5 (Fragmentierung):

"Wenn ein EAP-TLS-Peer ein EAP-Request-Paket mit dem gesetzten M-Bit empfängt, MUSS er mit einer EAP-Response mit EAP-Type=EAP-TLS und ohne Daten antworten.

Dies dient als Fragment ACK. **Der EAP-Server MUSS warten, bis er die EAP-Response erhält, bevor er ein weiteres Fragment sendet**."

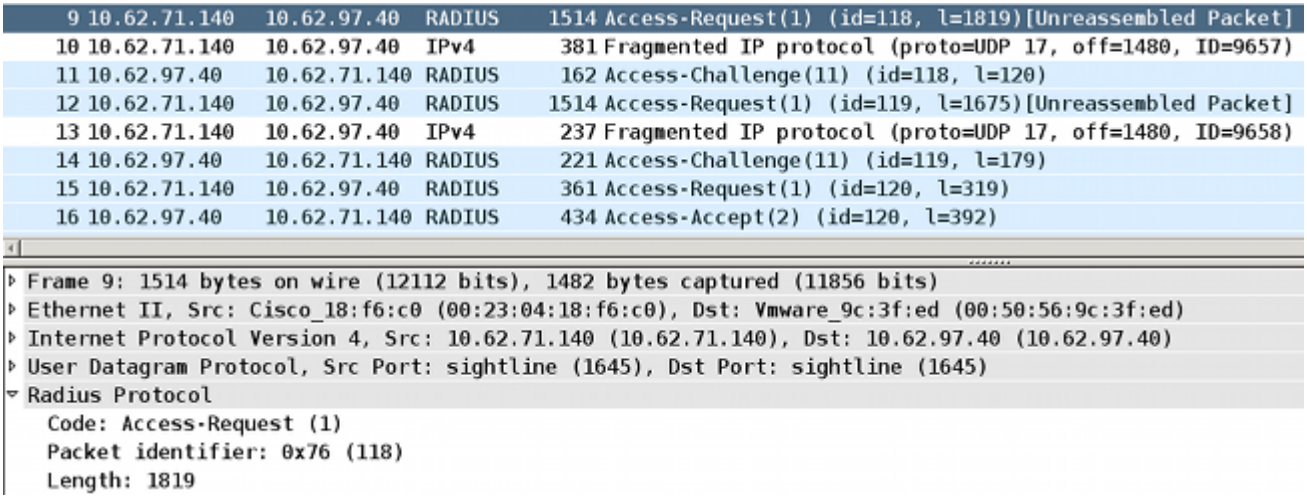
Der letzte Satz beschreibt eine sehr wichtige Funktion von AAA-Servern. Sie müssen auf die Bestätigung warten, bevor sie ein weiteres EAP-Fragment senden können. Eine ähnliche Regel wird für den Supplicant verwendet:

"Der EAP-Peer MUSS warten, bis er die EAP-Anforderung empfängt, bevor er ein weiteres Fragment sendet."

Fragmentierung in der IP-Schicht

Eine Fragmentierung ist nur zwischen dem Netzwerkzugriffsgerät (NAD) und dem AAA-Server (IP/UDP/RADIUS als Transportmedium) möglich.

Diese Situation tritt auf, wenn NAD (Cisco IOS-Switch) versucht, die RADIUS-Anforderung zu senden, die die EAP-Nutzlast enthält, die größer als die MTU der Schnittstelle ist:

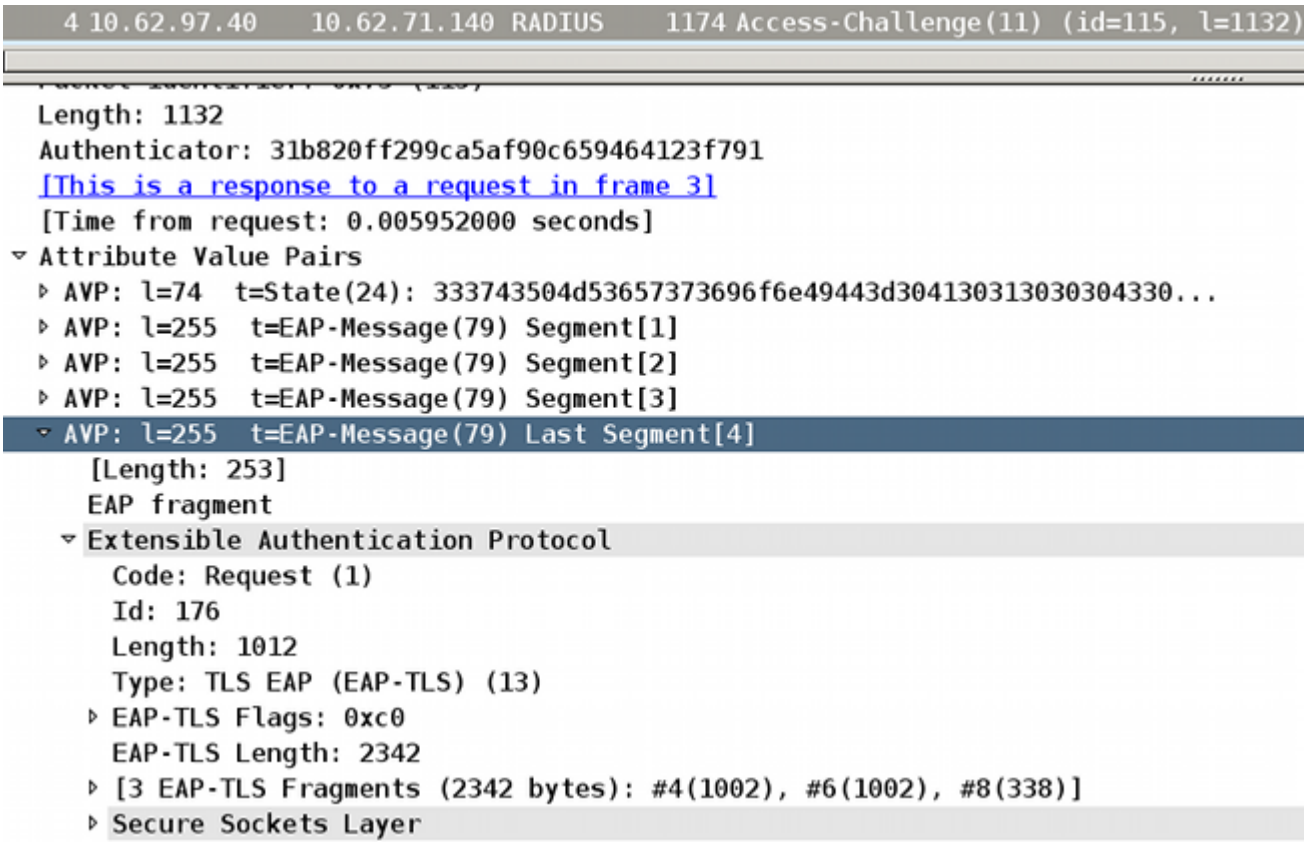


Die meisten Cisco IOS-Versionen sind nicht intelligent genug und versuchen nicht, über EAPoL empfangene EAP-Pakete in einem RADIUS-Paket zusammenzufassen, das in die MTU der physischen Schnittstelle zum AAA-Server passt.

AAA-Server sind intelligenter (wie in den nächsten Abschnitten beschrieben).

Fragmentierung im RADIUS

Das ist keine wirkliche Fragmentierung. Gemäß RFC 2865 kann ein einzelnes RADIUS-Attribut bis zu 253 Byte an Daten enthalten.Aus diesem Grund wird die EAP-Nutzlast immer in mehreren EAP-Message-RADIUS-Attributen übertragen:



Diese EAP-Message-Attribute werden von Wireshark neu zusammengesetzt und interpretiert (das Attribut "Letztes Segment" gibt die Nutzlast des gesamten EAP-Pakets wieder).

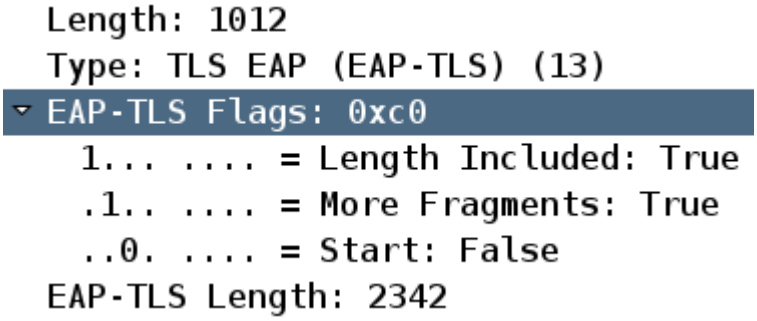
Der Length-Header im EAP-Paket ist gleich 1.012, und für den Transport sind vier RADIUS AVPs erforderlich.

Fragmentierung in EAP-TLS

Im gleichen Screenshot können Sie Folgendes sehen:

- Die EAP-Paketlänge beträgt 1.012.
- EAP-TLS-Länge 2.342

Dies deutet darauf hin, dass es sich um das erste EAP-TLS-Fragment handelt und der Supplicant mehr erwartet, was bestätigt werden kann, wenn Sie die EAP-TLS-Flags untersuchen:



Diese Art der Fragmentierung tritt am häufigsten auf in:

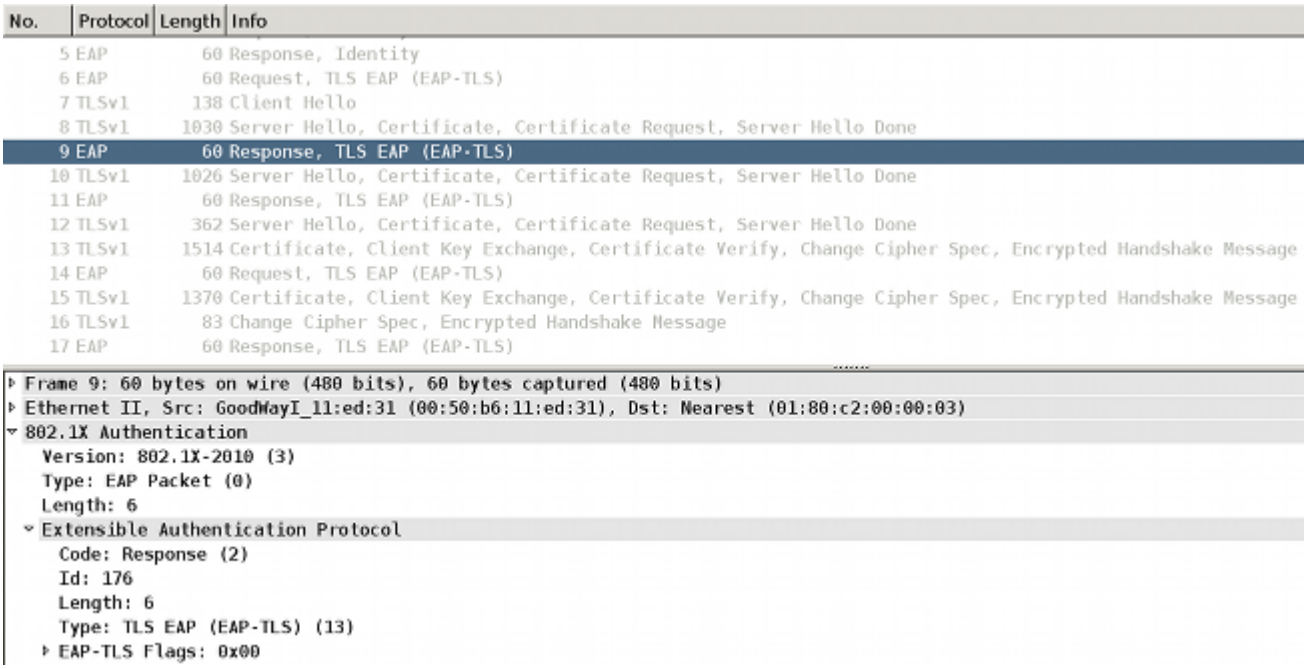
- RADIUS Access-Challenge, gesendet vom AAA-Server, der die EAP-Anforderung mit dem SSL-Serverzertifikat (Secure Sockets Layer) mit der gesamten Kette überträgt.

- RADIUS Access-Request wird von NAD gesendet, das die EAP-Response mit dem SSL Client Certificate mit der gesamten Kette überträgt.

EAP-TLS-Fragmentbestätigung

Wie bereits erläutert, muss jedes EAP-TLS-Fragment bestätigt werden, bevor nachfolgende Fragmente gesendet werden.

Hier ein Beispiel (Paketerfassung für EAPoL zwischen Supplicant und NAD):



EAPoL-Frames und der AAA-Server geben das Serverzertifikat zurück:

- Dieses Zertifikat wird in einem EAP-TLS-Fragment (Paket 8) gesendet.
- Der Supplicant bestätigt dieses Fragment (Paket 9).
- Das zweite EAP-TLS-Fragment wird durch NAD (Paket 10) weitergeleitet.
- Der Supplicant bestätigt dieses Fragment (Paket 11).
- Das dritte EAP-TLS-Fragment wird durch NAD weitergeleitet (Paket 12).
- Der Supplicant muss dies nicht bestätigen, sondern fährt mit dem Client-Zertifikat fort, das bei Paket 13 beginnt.

Hier sind die Details zu Paket 12:

```
   12 TLSv1      362 Server Hello, Certificate, Certificate Request, Server Hello Done
▸ Frame 12: 362 bytes on wire (2896 bits), 362 bytes captured (2896 bits)
▸ Ethernet II, Src: Cisco_e1:d8:11 (d4:a0:2a:e1:d8:11), Dst: Nearest (01:80:c2:00:00:03)
▾ 802.1X Authentication
    Version: 802.1X-2010 (3)
    Type: EAP Packet (0)
    Length: 344
  ▾ Extensible Authentication Protocol
      Code: Request (1)
      Id: 178
      Length: 344
      Type: TLS EAP (EAP-TLS) (13)
    ▸ EAP-TLS Flags: 0x00
    ▸ [3 EAP-TLS Fragments (2342 bytes): #8(1002), #10(1002), #12(338)]
    ▾ Secure Sockets Layer
      ▸ TLSv1 Record Layer: Handshake Protocol: Server Hello
      ▸ TLSv1 Record Layer: Handshake Protocol: Certificate
      ▸ TLSv1 Record Layer: Handshake Protocol: Multiple Handshake Messages
```

Wie Sie sehen, hat Wireshark die Pakete 8, 10 und 12 wieder zusammengesetzt.

Die Größe der EAP-Fragmente beträgt 1.002, 1.002 und 338, wodurch sich die Gesamtgröße der EAP-TLS-Nachricht auf 2.342 erhöht.

Die Gesamtlänge der EAP-TLS-Nachrichten wird in jedem Fragment angegeben. Dies kann bestätigt werden, wenn Sie RADIUS-Pakete (zwischen NAD- und AAA-Server) untersuchen:

```
4 10.62.97.40    10.62.71.140 RADIUS    1174 Access-Challenge(11) (id=115, l=1132)
5 10.62.71.140   10.62.97.40  RADIUS     361 Access-Request(1) (id=116, l=319)
6 10.62.97.40    10.62.71.140 RADIUS    1170 Access-Challenge(11) (id=116, l=1128)
7 10.62.71.140   10.62.97.40  RADIUS     361 Access-Request(1) (id=117, l=319)
8 10.62.97.40    10.62.71.140 RADIUS     502 Access-Challenge(11) (id=117, l=460)
```

```
    [Length: 253]
    EAP fragment
  ▾ Extensible Authentication Protocol
      Code: Request (1)
      Id: 176
      Length: 1012
      Type: TLS EAP (EAP-TLS) (13)
    ▸ EAP-TLS Flags: 0xc0
      EAP-TLS Length: 2342
    ▸ [3 EAP-TLS Fragments (2342 bytes): #4(1002), #6(1002), #8(338)]
    ▸ Secure Sockets Layer
```

Die RADIUS-Pakete 4, 6 und 8 enthalten diese drei EAP-TLS-Fragmente. Die ersten beiden Fragmente werden bestätigt.

Wireshark kann die Informationen über die EAP-TLS-Fragmente (Größe: 1.002 + 1.002 + 338 = 2.342) darstellen.

Dieses Szenario und dieses Beispiel waren einfach. Der Cisco IOS-Switch musste die EAP-TLS-Fragmentgröße nicht ändern.

EAP-TLS-Fragmente mit unterschiedlicher Größe wieder zusammengesetzt

Man bedenke, was passiert, wenn die NAD-MTU zum AAA-Server 9.000 Byte beträgt (Jumbo-Frame) und der AAA-Server auch über die Schnittstelle verbunden ist, die Jumbo-Frames unterstützt.

Die meisten der typischen Supplicants sind über eine 1-Gbit-Verbindung mit einer MTU von 1.500 verbunden.

In einem solchen Szenario führt der Cisco IOS-Switch eine "asymmetrische" EAP-TLS-Zusammenstellung und -Reassemblierung durch und ändert die Größe der EAP-TLS-Fragmente.

Hier ein Beispiel für eine große EAP-Nachricht, die vom AAA-Server (SSL-Serverzertifikat) gesendet wurde:

1. Der AAA-Server muss eine EAP-TLS-Nachricht mit einem SSL-Serverzertifikat senden. Die Gesamtgröße dieses EAP-Pakets beträgt 3.000. Nach der Kapselung in RADIUS Access-Challenge/UDP/IP ist sie immer noch kleiner als die MTU der AAA-Serverschnittstelle. Ein einzelnes IP-Paket wird mit 12 RADIUS EAP-Message-Attributen gesendet. Es gibt keine IP- oder EAP-TLS-Fragmentierung.

2. Der Cisco IOS-Switch empfängt ein solches Paket, entkapselt es und beschließt, dass EAP über EAPoL an den Supplicant gesendet werden muss. Da EAPoL keine Fragmentierung unterstützt, muss der Switch eine EAP-TLS-Fragmentierung durchführen.

3. Der Cisco IOS-Switch bereitet das erste EAP-TLS-Fragment vor, das in die MTU der Schnittstelle zur Komponente (1.500) passen kann.

4. Dieses Fragment wird vom Bittsteller bestätigt.

5. Ein weiteres EAP-TLS-Fragment wird nach Erhalt der Bestätigung gesendet.

6. Dieses Fragment wird vom Bittsteller bestätigt.

7. Das letzte EAP-TLS-Fragment wird vom Switch gesendet.

Dieses Szenario zeigt Folgendes:

- Unter bestimmten Umständen muss der NAD EAP-TLS-Fragmente erstellen.
- Die NAD ist für das Senden/Bestätigen dieser Fragmente verantwortlich.

Dasselbe kann bei einem Supplicant passieren, der über eine Verbindung verbunden ist, die Jumbo Frames unterstützt, während der AAA-Server eine kleinere MTU hat (dann erstellt der Cisco IOS-Switch EAP-TLS-Fragmente, wenn er das EAP-Paket an den AAA-Server sendet).

RADIUS-Attribut Framed-MTU

Für RADIUS ist in RFC 2865 ein Framed-MTU-Attribut definiert:

"Dieses Attribut gibt die maximale Übertragungseinheit an, die für den Benutzer konfiguriert werden muss, wenn sie nicht auf andere Weise (z. B. PPP) ausgehandelt wird. Es kann in Access-Accept-Paketen verwendet werden.

Es kann in einem Access-Request-Paket als Hinweis des NAS an den Server verwendet werden, dass er diesen Wert bevorzugt, aber der Server muss diesen Hinweis nicht berücksichtigen."

Die ISE hält diesen Hinweis nicht ein. Der von NAD in der Access-Request gesendete Wert der Framed-MTU hat keinen Einfluss auf die von der ISE durchgeführte Fragmentierung.

Mehrere moderne Cisco IOS-Switches lassen keine Änderungen an der MTU der Ethernet-Schnittstelle zu. Ausgenommen hiervon sind die global auf dem Switch aktivierten Jumbo Frames-Einstellungen. Die Konfiguration von Jumbo Frames wirkt sich auf den Wert des Framed-MTU-Attributs aus, das in der RADIUS-Zugriffsanforderung gesendet wird. Sie legen beispielsweise Folgendes fest:

```
<#root>

Switch(config)#

system mtu jumbo 9000
```

Dadurch wird der Switch gezwungen, in allen RADIUS-Zugriffsanforderungen Framed-MTU = 9000 zu senden. Dasselbe gilt für die System-MTU ohne Jumbo-Frames:

```
<#root>

Switch(config)#

system mtu 1600
```

Dadurch wird der Switch gezwungen, in allen RADIUS-Zugriffsanforderungen Framed-MTU = 1600 zu senden.

Beachten Sie, dass Sie mit modernen Cisco IOS Switches den System-MTU-Wert nicht unter 1.500 senken können.

AAA-Server und zugehöriges Verhalten beim Senden von EAP-Fragmenten

ISE

Die ISE versucht immer, EAP-TLS-Fragmente (normalerweise Server Hello mit Zertifikat) zu senden, die 1.002 Byte lang sind (obwohl das letzte Fragment normalerweise kleiner ist).

RADIUS Framed-MTU wird nicht berücksichtigt. Eine Neukonfiguration zum Senden größerer EAP-TLS-Fragmente ist nicht möglich.

Microsoft Network Policy Server (NPS)

Die Größe der EAP-TLS-Fragmente kann konfiguriert werden, wenn das Framed-MTU-Attribut lokal auf dem NPS konfiguriert wird.

Obwohl im Artikel Configure the EAP Payload Size on Microsoft NPS (EAP-Payload-Größe konfigurieren) erwähnt wird, dass der Standardwert einer gerahmten MTU für den NPS RADIUS-Server 1.500 beträgt, hat das Cisco Technical Assistance Center (TAC)-Lab gezeigt, dass es 2.000 mit den Standardeinstellungen sendet (bestätigt in einem Microsoft Windows 2012 Datacenter).

Es wird getestet, dass die **lokale** Einstellung von **Framed-MTU** gemäß dem zuvor erwähnten Leitfaden vom NPS eingehalten wird und die EAP-Nachrichten in Fragmente einer in Framed-MTU festgelegten

Größe fragmentiert werden. Das in der Access-Anforderung empfangene Framed-MTU-Attribut wird jedoch nicht verwendet (wie bei ISE/ACS).

Das Festlegen dieses Werts ist eine gültige Problemumgehung, um Probleme in der Topologie wie diese zu beheben:

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

Derzeit können Sie für Switches keine MTU pro Port festlegen. Bei 6880 Switches wurde diese Funktion mit der Cisco Bug-ID CSCuo26327 - 802.1x EAP-TLS hinzugefügt, die an FEX-Host-Ports nicht funktioniert.

AnyConnect

AnyConnect sendet EAP-TLS-Fragmente (in der Regel Client-Zertifikate) mit einer Länge von 1.486 Byte. Für diese Wertgröße beträgt der Ethernet-Frame 1.500 Byte. Das letzte Fragment ist normalerweise kleiner.

Microsoft Windows Native Supplicant

Microsoft Windows sendet EAP-TLS-Fragmente (in der Regel Client-Zertifikate) mit einer Länge von 1.486 oder 1.482 Byte. Für diese Wertgröße beträgt der Ethernet-Frame 1.500 Byte. Das letzte Fragment ist normalerweise kleiner.

Zugehörige Informationen

- **Konfigurieren der portbasierten IEEE 802.1x-Authentifizierung**
- **Technischer Support und Dokumentation für Cisco Systeme**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.