EAP フラグメンテーションの実装と動作

内容

はじめに

このドキュメントでは、拡張可能認証プロトコル（EAP）セッションを理解してトラブルシュートする方法について説明します。

背景説明

このドキュメントのセクションは、次の領域を力バーしています。

- 認証、許可、およびアカウンティング（AAA）サーバが Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）セッションのサーバ証明書を返す場合の動作
- サプリカントが EAP-TLS セッションのクライアント証明書を返す場合の動作
- Microsoft Windows ネイティブ サプリカントと Cisco AnyConnect Network Access Manager（NAM）の両方を使用した場合の相互運用性
- IP、RADIUS、および EAP-TLS でのフラグメンテーションとネットワーク アクセス デバイ

スで実行される再構成プロセス
- RADIUS のフレーム化された最大伝送ユニット（MTU）属性
- AAA サーバが EAP-TLS パケットのフラグメンテーションを実行する場合の動作

前提条件

要件

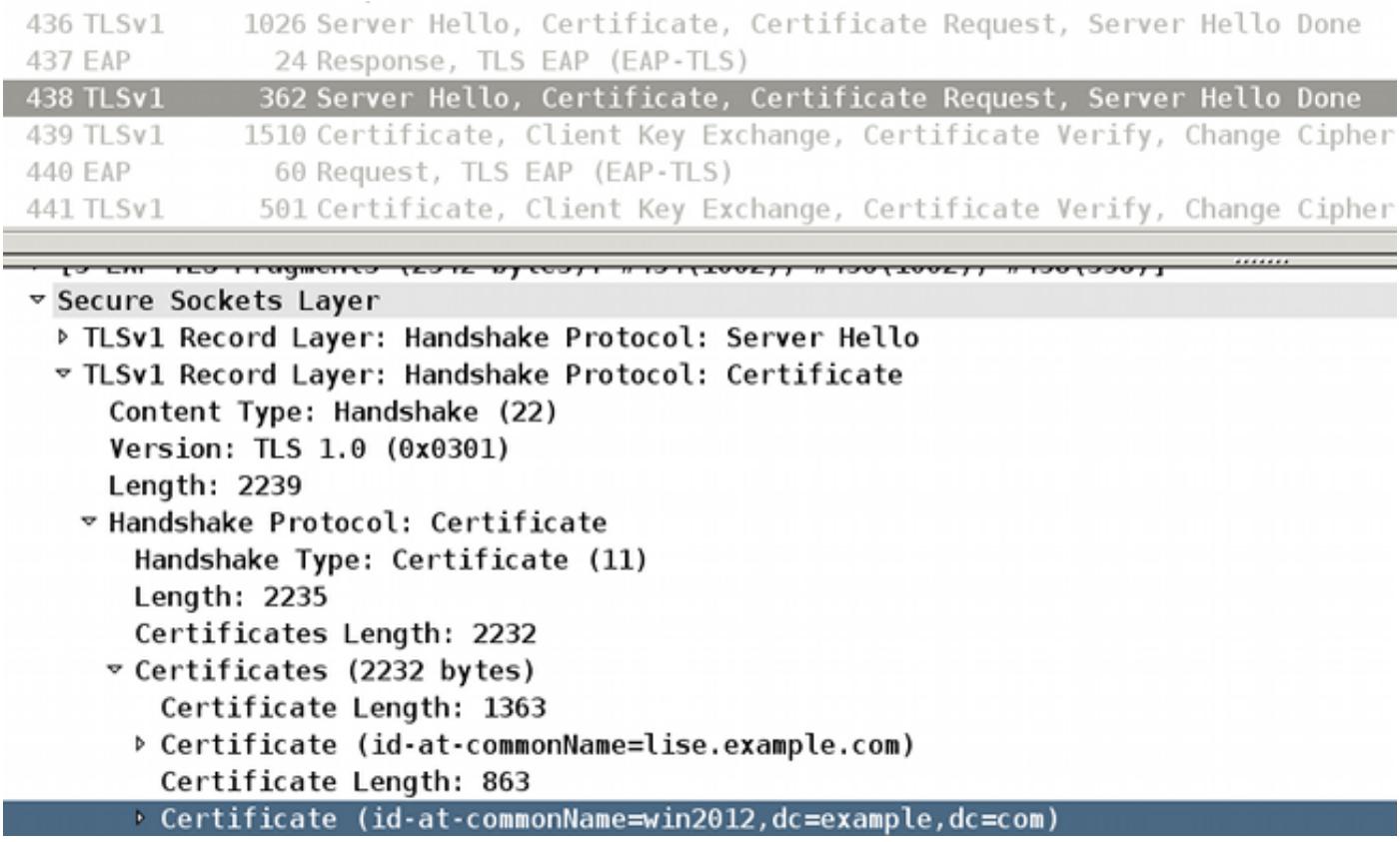
次の項目に関する知識があることが推奨されます。

- EAP プロトコルと EAP-TLS プロトコル
- Cisco Identity Services Engine（ISE）の設定
- Cisco Catalyst スイッチの CLI 設定

この記事を理解するためには、EAP と EAP-TLS に精通している必要があります。

サーバによって返される証明書チェーン

AAA サーバ（Access Control Server（ACS）と ISE）は常に、サーバ Hello とサーバ証明書を含む EAP-TLS パケットのチェーン全体を返します。



CN=win2012,dc=example,dc=com に署名した認証局（CA）と一緒に、ISE アイデンティティ証明書（Common Name（CN）= lise.example.com）が返されます。この動作は ACS と ISE の両方で同じです。

サプリカントによって返される証明書チェーン

Microsoft Windows ネイティブ サプリカント

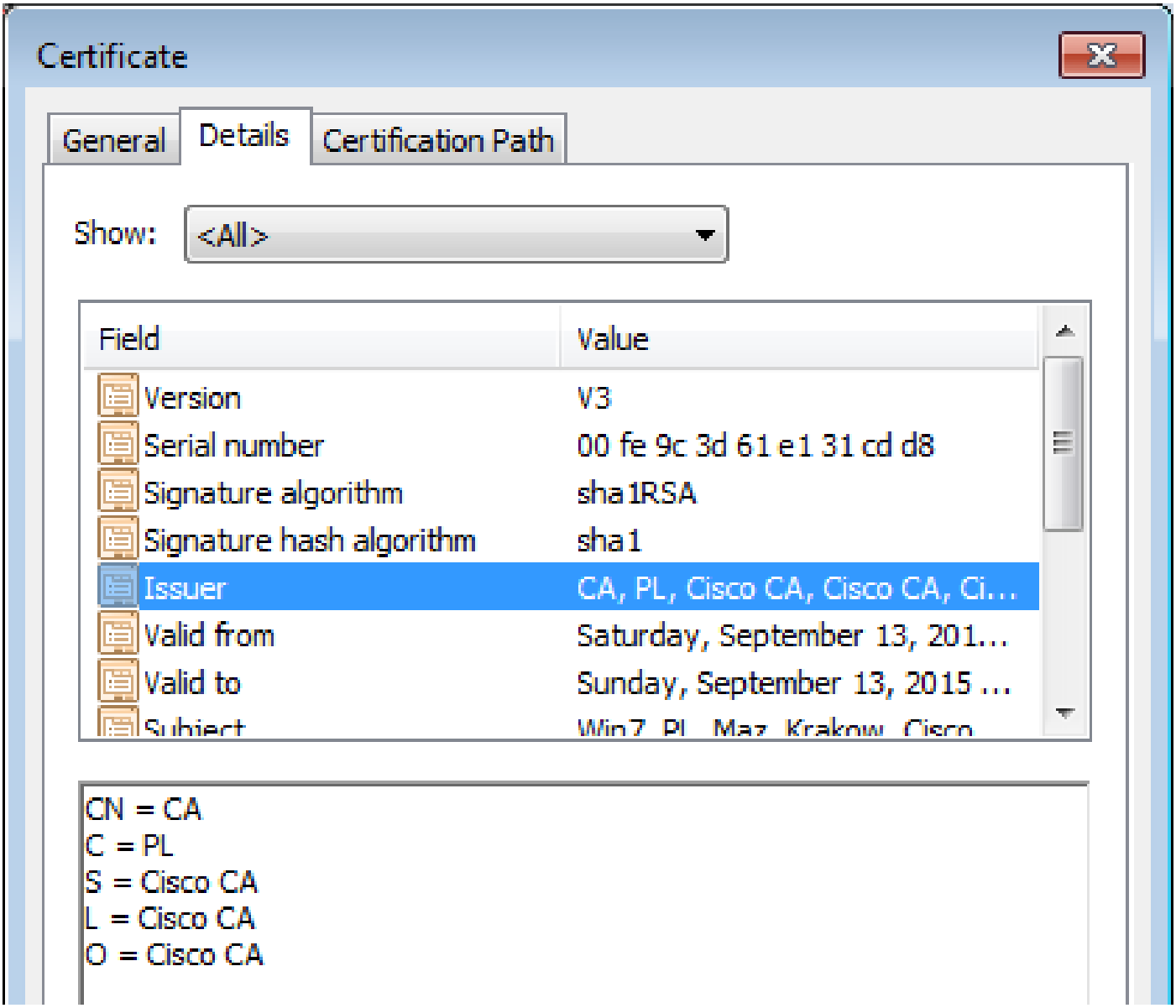
EAP-TLS を使用するように設定された Microsoft Windows 7 ネイティブ サプリカントは、「Simple certificate selection」の有無に関係なく、クライアント証明書のチェーン全体を送信しません。

この動作は、クライアント証明書がサーバ証明書とは異なる CA（別のチェーン）によって署名された場合でも発生します。

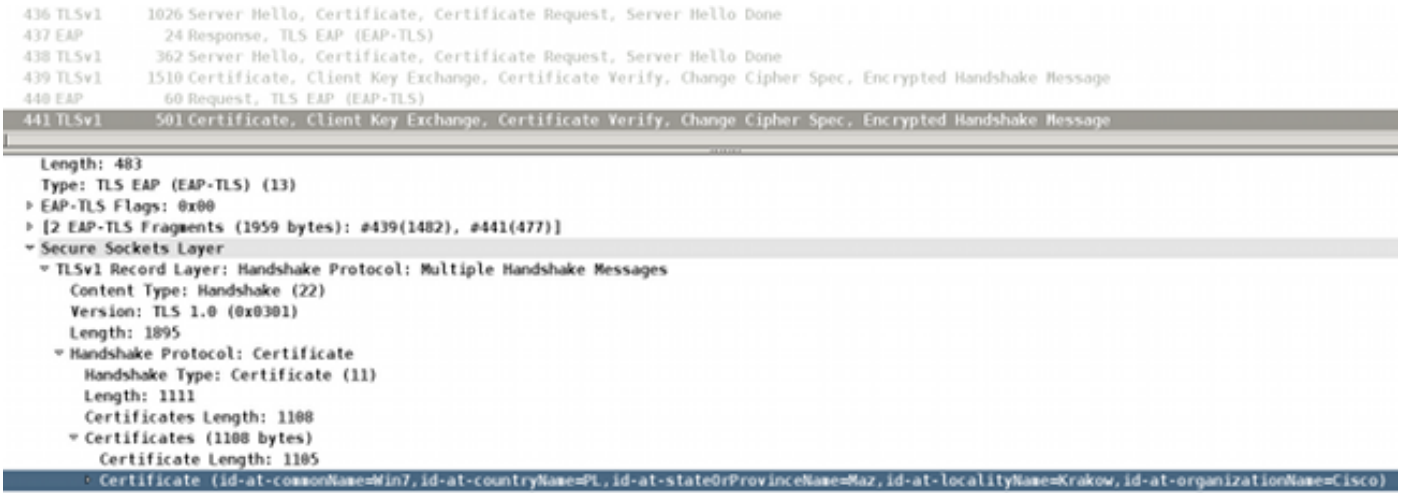
次の例は、前のスクリーンショットで示したサーバ Hello と証明書に関連しています。

このシナリオでは、ISE 証明書がサブジェクト名 CN=win2012,dc=example,dc=com を使用して CA によって署名されます。

ただし、Microsoft ストアにインストールされたユーザ証明書は、別の CA（CN=CA,C=PL,S=Cisco CA,L=Cisco CA,O=Cisco CA）によって署名されます。



そのため、Microsoft Windows サプリカントはクライアント証明書だけで応答します。それに署名した CA（CN=CA,S=PL,S=Cisco CA, L=Cisco CA, O=Cisco CA）は添付されません。



この動作のため、AAAサーバがクライアント証明書を検証するときに問題が発生する可能性があります。この例は、Microsoft Windows 7 SP1 Professional に関連しています。

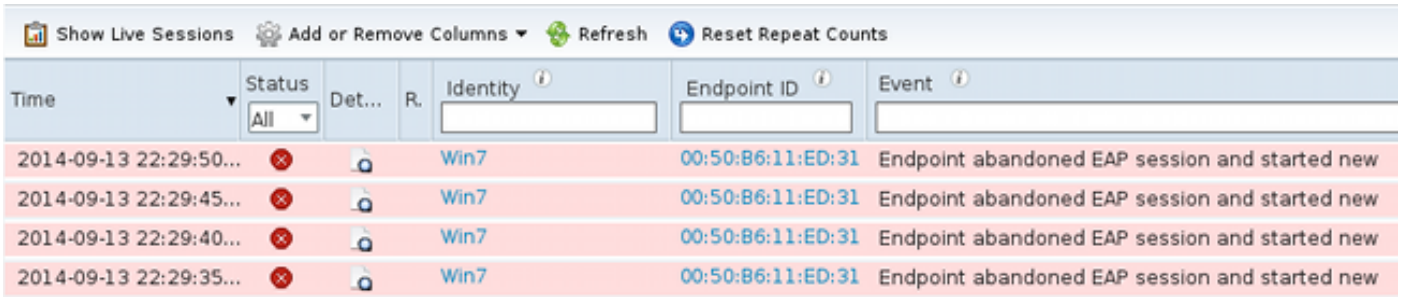
解決方法

完全な証明書チェーンがACSおよびISEの証明書ストア（すべてのCAおよびサブCA署名クライアント証明書）にインストールされます。

証明書検証に伴う問題は、ACS または ISE で簡単に検出できます。信頼できない証明書に関する情報が提示され、ISE から次のように報告されます。

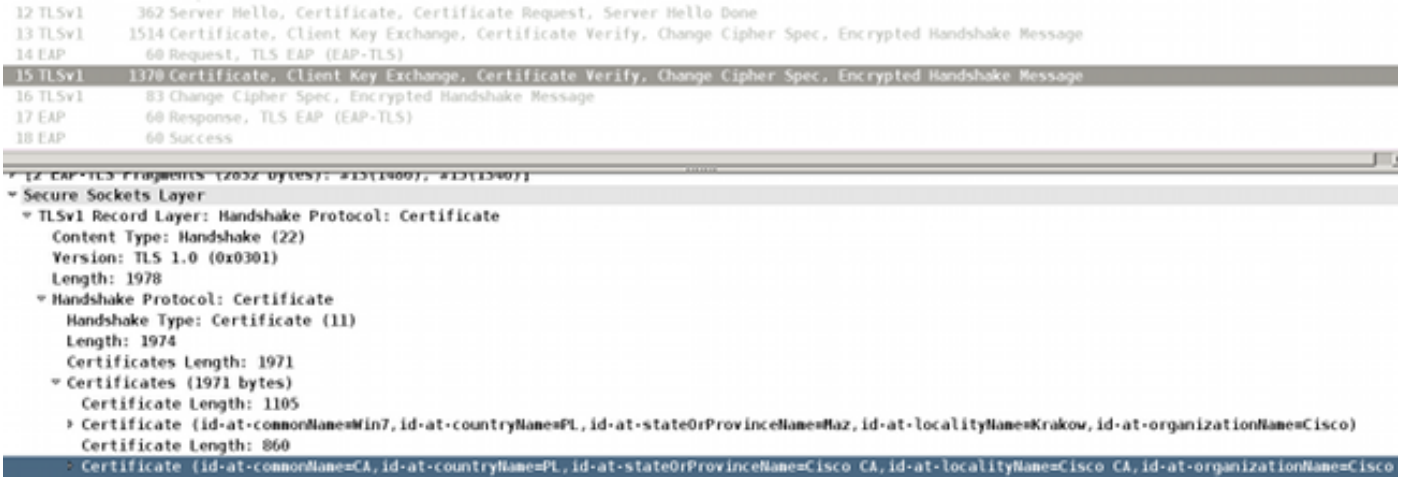
```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

サプリカントでの証明書検証に伴う問題は簡単には検出できません。通常は、AAA サーバが「Endpoint abondoned EAP session」で次のように応答します。



AnyConnect NAM

AnyConnect NAM にはこの制限がありません。同じシナリオで、クライアント証明書のチェーン全体が添付されます（正しい CA が添付されます）。



Microsoft Windows ネイティブ サプリカントと AnyConnect NAM

両方のサービスが稼働している場合は、AnyConnect NAM が優先されます。

NAM サービスを実行していない場合でも、Microsoft Windows API を呼び出して EAP パケットを転送するため、Microsoft Windows ネイティブ サプリカントの問題が発生する可能性があります。

このような障害の例を次に示します。

次のコマンドを使用して、Microsoft Windows 上のトレースを有効にします。

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

トレース（c:\windows\trace\svchost_RASTLS.LOG）には次のように表示されます。

<#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

最後のパケットは、Microsoft Windows ネイティブ サプリカントから送信されたクライアント証明書（EAP サイズが 1492 の EAP-TLS フラグメント 1）です。残念ながら、Wireshark にはこのパケットが表示されません。

	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

そして、そのパケットは実際には送信されません。最後のパケットは、EAP-TLSを伝送するサーバ証明書の3番目のフラグメントです。

これは、Microsoft Windows API を呼び出す AnyConnect NAM モジュールによってすでに消費されています。

このため、AnyConnect を Microsoft Windows ネイティブ サプリカントと一緒に使用することはお勧めできません。

AnyConnect サービスを使用する場合は、Microsoft Windows ネイティブ サプリカントではなく、NAM（802.1x サービスが必要な場合）を一緒に使用することをお勧めします。

フラグメンテーション

フラグメンテーションは複数のレイヤで発生する可能性があります。

- IP
- RADIUS 属性値ペア（AVP）
- EAP-TLS

Cisco IOS® スイッチは高い処理能力を備えています。EAP 形式と EAP-TLS 形式を解釈できます。

このスイッチは TLS トンネルを復号化することはできませんが、Extensible Authentication Protocol over LAN（EAPoL）または RADIUS でのカプセル化時の EAP パケットの構成と再構成およびフラグメンテーションを扱います。

EAP プロトコルはフラグメンテーションをサポートしません。RFC 3748（EAP）の抜粋を次に示します。

「フラグメンテーションはEAP自体ではサポートされませんが、個々のEAP方式ではサポートされる場合があります。」

EAP-TLS がそのような例です。RFC 5216（EAP-TLS）第 2.1.5 項（fragmentation）の抜粋を次に示します。

"When an EAP-TLS peer receives an EAP-Request packet with the M bit set, it MUST respond with an EAP-Response with EAP-Type=EAP-TLS and no data.

This serves as a fragment ACK.The EAP server MUST wait until it receives the EAP-Response before sending another fragment."

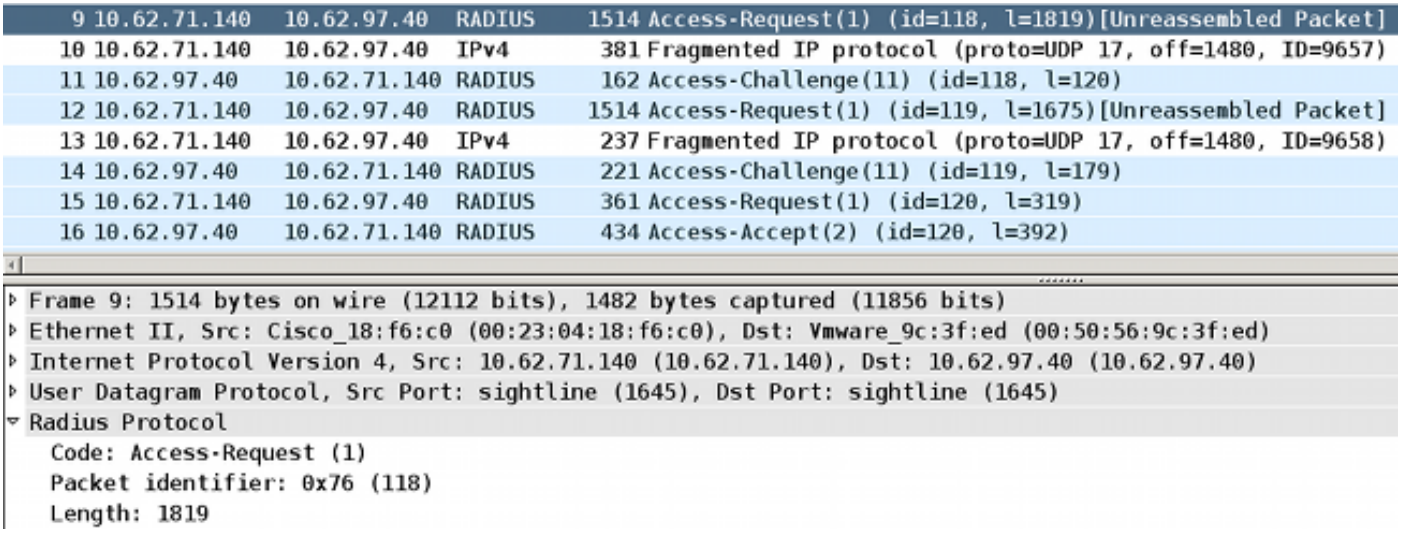
最後の文は AAA サーバの非常に重要な機能に関する説明です。別の EAP フラグメントを送信するためには、その前に ACK を待つ必要があります。同様のルールがサプリカントに使用されます。

"The EAP peer MUST wait until it receives the EAP-Request before sending another fragment."

IP 層でのフラグメンテーション

フラグメンテーションは、ネットワーク アクセス デバイス（NAD）と AAA サーバ（トランスポートとして使用される IP/UDP/RADIUS）の間でのみ発生する可能性があります。

この状況は、NAD（Cisco IOS スイッチ）が、インターフェイスの MTU より長い EAP ペイロードを含む RADIUS 要求を送信しようとしたときに起こります。

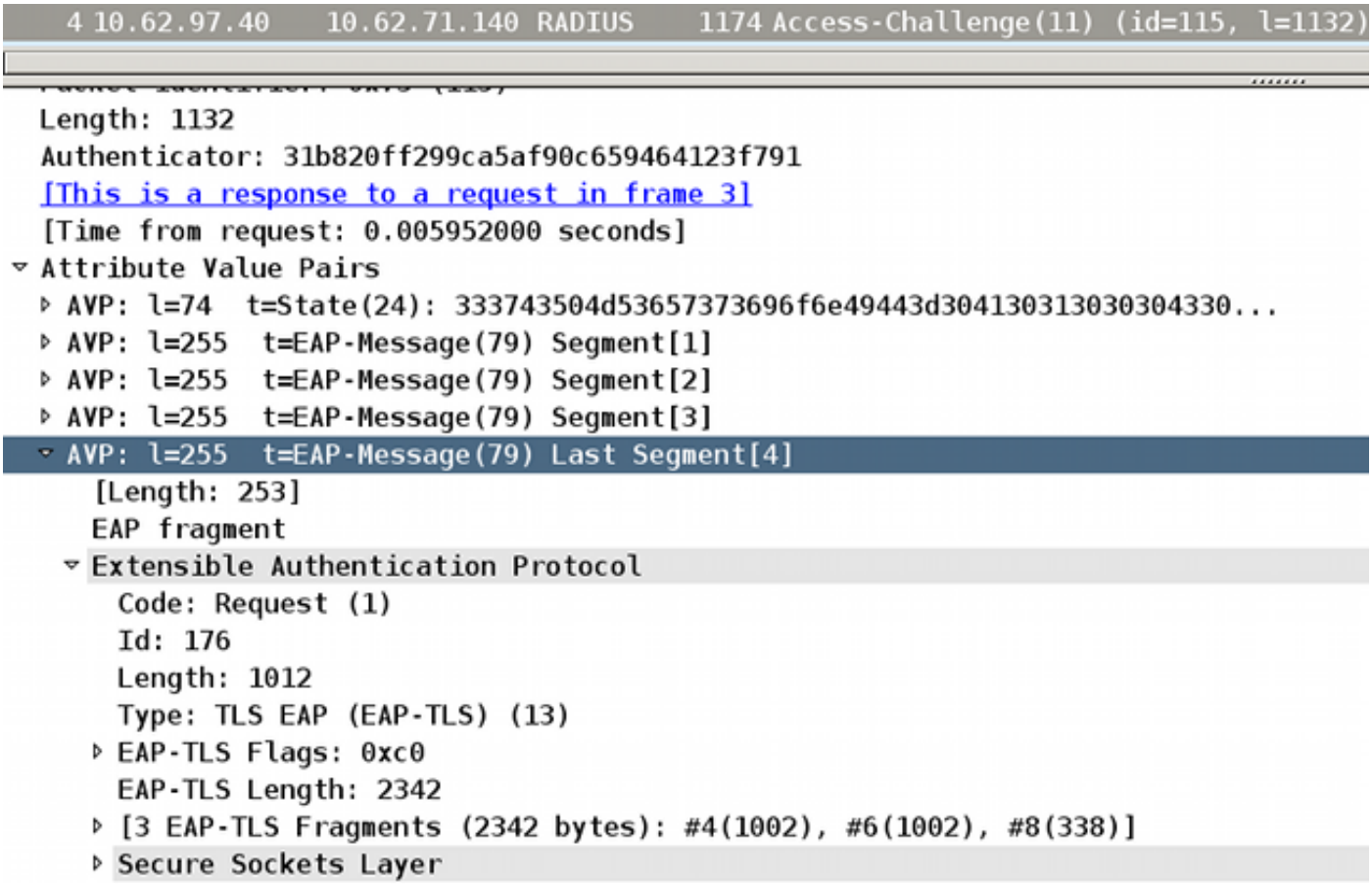


ほとんどの Cisco IOS バージョンが十分な処理能力を備えていないため、EAPoL 経由で受信される EAP パケットを構成して、AAA サーバ宛ての物理インターフェイスの MTU に収まる RADIUS パケットにまとめようとはしません。

AAA サーバはより高い処理能力を備えています（次のセクションを参照）。

RADIUS でのフラグメンテーション

これは実際にはフラグメンテーションではありません。RFC 2865によれば、1つのRADIUS属性に最大253バイトのデータを格納できます。そのため、EAPペイロードは常に複数のEAP-Message RADIUS属性で送信されます。



このような EAP-Message 属性は、Wireshark によって再構成され、解釈されます（「最後のセグメント」属性は EAP パケット全体のペイロードを公開します）。

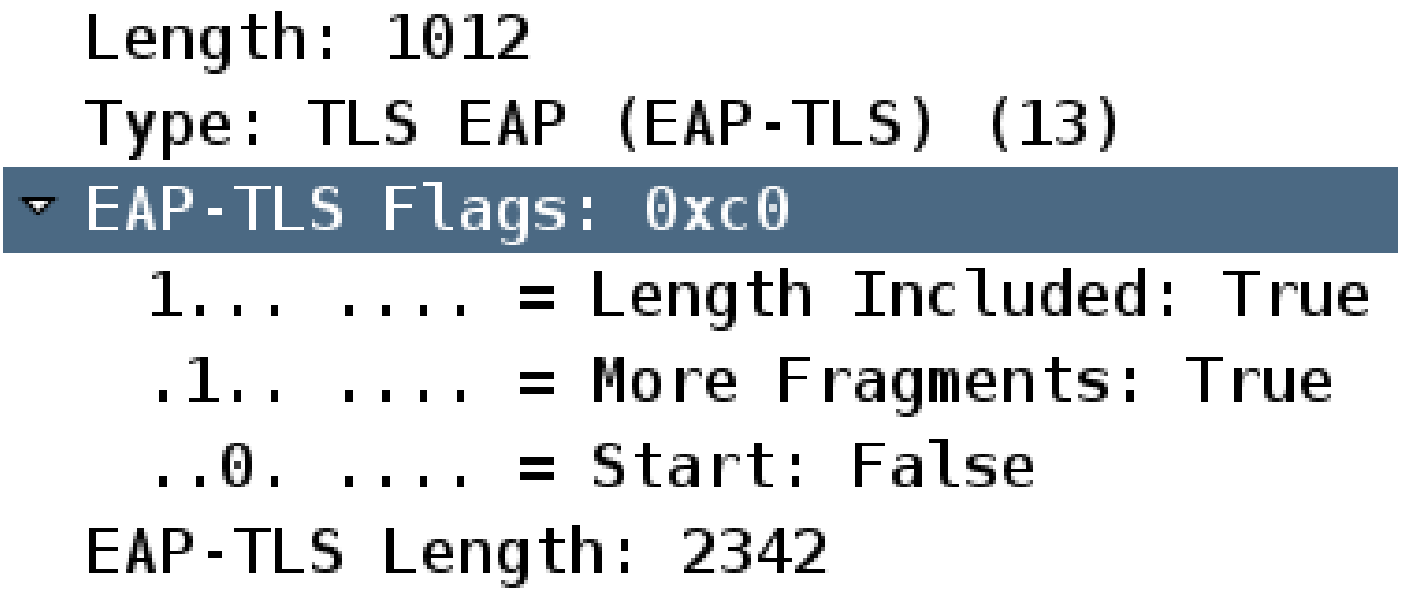
EAP パケット内の Length ヘッダーは 1,012 に等しく、これを伝送するために 4 つの RADIUS AVP が必要です。

EAP-TLS でのフラグメンテーション

同じスクリーンショットから、次のことがわかります。

- EAP パケット長は 1,012 です。
- EAP-TLS 長は 2,342 です。

これは、これが最初のEAP-TLSフラグメントであり、サプリカントが追加を期待していることを示唆します。これは、EAP-TLSフラグを調べると確認できます。



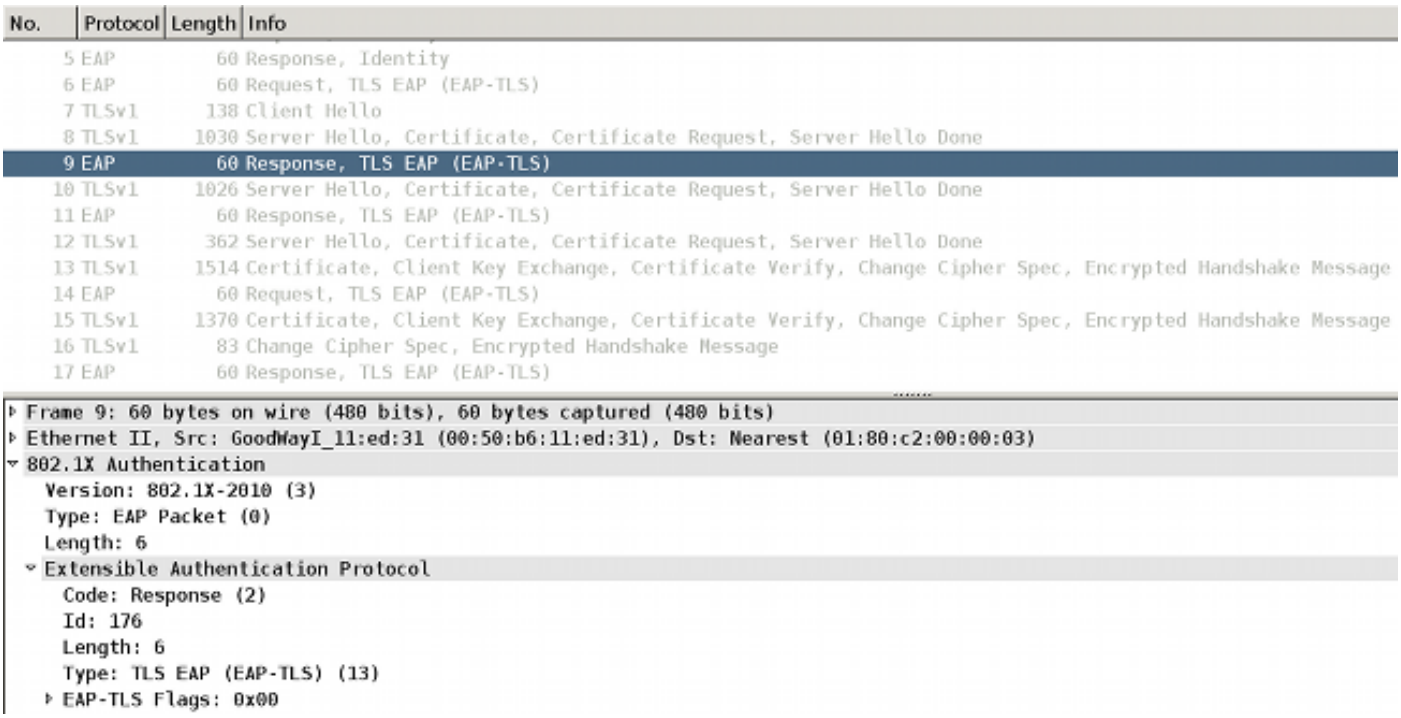
この種のフラグメンテーションは次のような場合に最も頻繁に発生します。

- AAA サーバから、セキュア ソケット レイヤ（SSL）サーバ証明書とチェーン全体を含む EAP-Request を伝送する RADIUS Access-Challenge が送信された場合。
- NAD から、SSL クライアント証明書とチェーン全体を含む EAP-Response を伝送する RADIUS Access-Request が送信された場合。

EAP-TLS フラグメントの確認

前述したように、各 EAP-TLS フラグメントは、後続のフラグメントが送信される前に確認される必要があります。

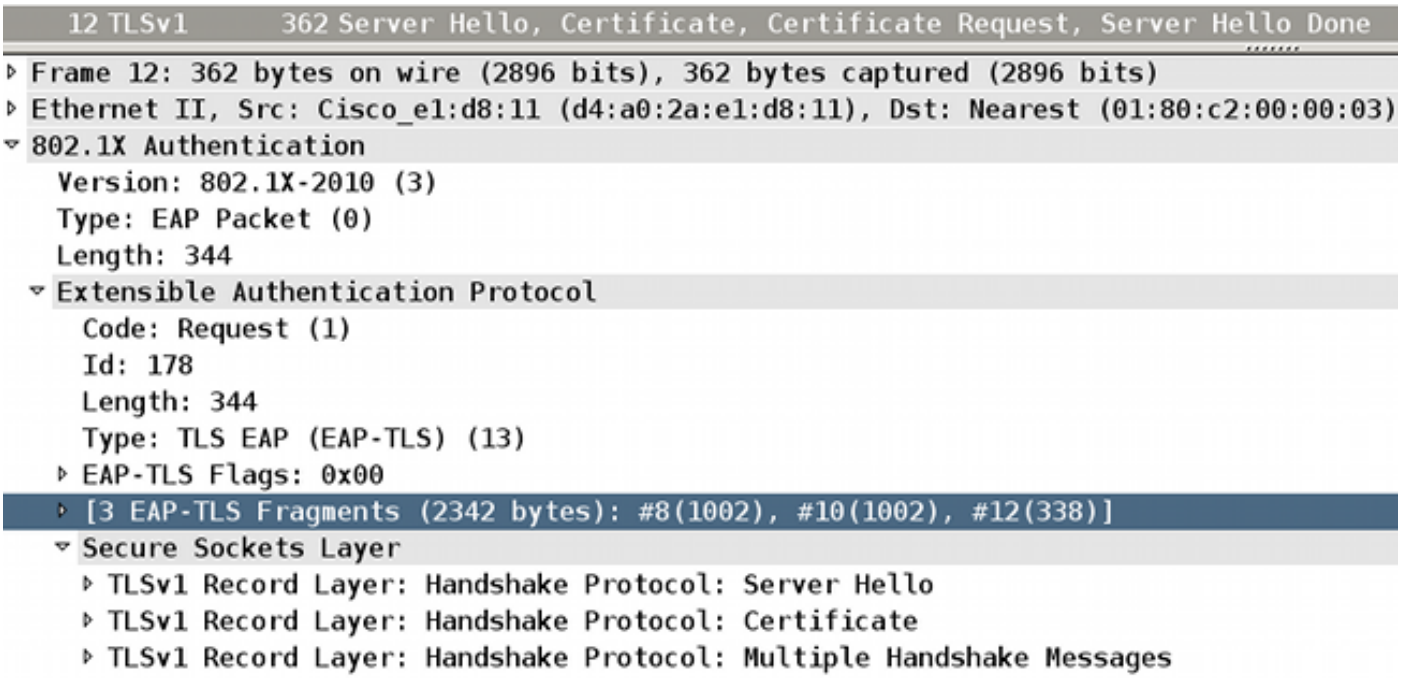
次に例を示します（サプリカントと NAD 間の EAPoL 用のパケット キャプチャ）。



EAPoL フレームと AAA サーバがサーバ証明書を返します。

- この証明書は EAP-TLS フラグメントで送信されます (パケット 8) 。
- サプリカントがそのフラグメントを確認応答します (パケット 9) 。
- 2 番目の EAP-TLS フラグメントが NAD によって転送されます (パケット 10) 。
- サプリカントがそのフラグメントを確認応答します (パケット 11) 。
- 3 番目の EAP-TLS フラグメントが NAD によって転送されます (パケット 12) 。
- サプリカントはこれを確認する必要はなく、パケット13から始まるクライアント証明書に進みます。

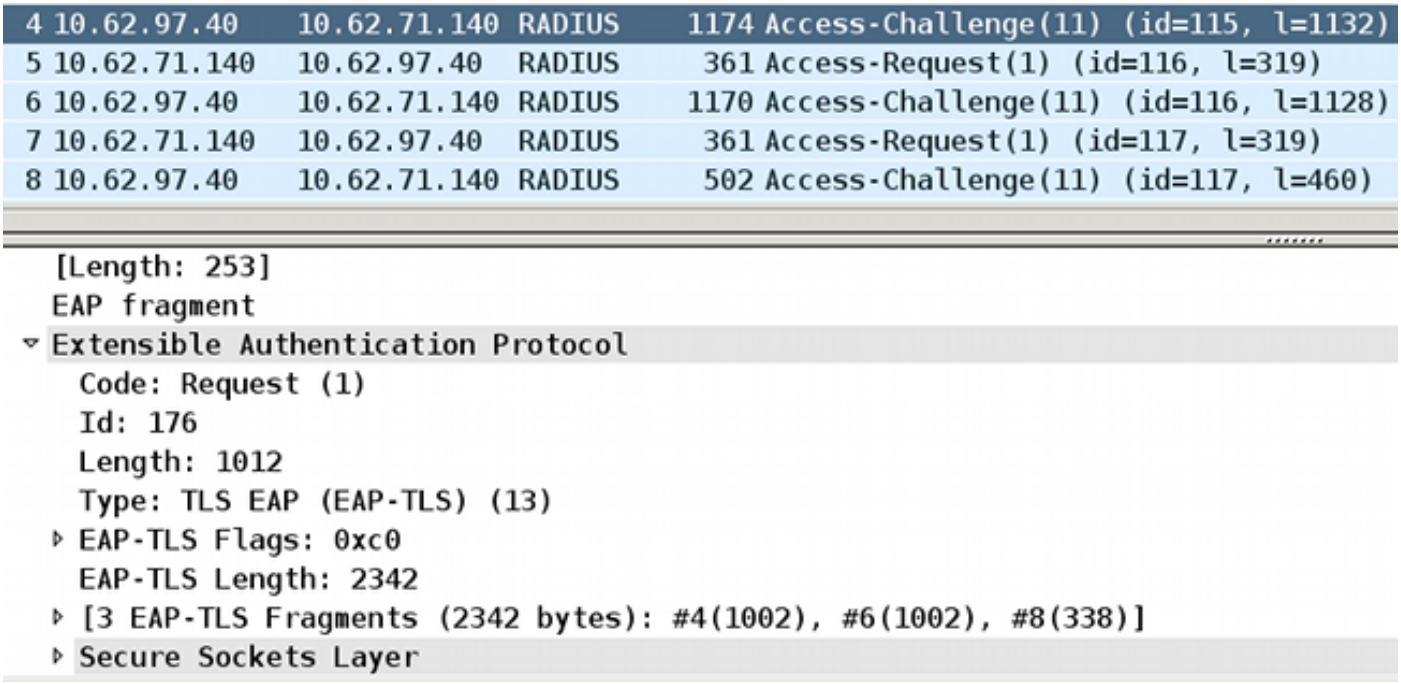
次に、パケット 12 の詳細を示します。



Wireshark がパケット 8、10、および 12 を再構成したことが示されています。

EAPフラグメントのサイズは1,002、1,002、および338で、EAP-TLSメッセージの合計サイズは2342になります。

EAP-TLSメッセージの長さの合計が、すべてのフラグメントでアナウンスされます。これは、（NAD と AAA サーバの間の）RADIUS パケットを検査すると確認できます。



RADIUS パケット 4、6、および 8 でこの 3 つの EAP-TLS フラグメントが伝送されます。最初の 2 つのフラグメントが確認応答されます。

Wiresharkは、EAP-TLSフラグメントに関する情報を表示できます（サイズ：1,002 + 1,002 + 338 = 2,342）。

このシナリオと例は単純でした。Cisco IOS スイッチは、EAP-TLS フラグメント サイズを変更する必要がありませんでした。

別のサイズで再構成された EAP-TLS フラグメント

AAA サーバ宛ての NAD MTU が 9,000 バイト（ジャンボ フレーム）で、AAA サーバがジャンボ フレームをサポートするインターフェイスを使用して接続されている場合の動作を考えます。

一般的なサプリカントのほとんどが 1,500 の MTU を含む 1 Gbit リンクを使用して接続されます。

このようなシナリオでは、Cisco IOS スイッチが EAP-TLS の「非対称」構成と再構成を実行し、EAP-TLS フラグメント サイズを変更します。

次に、AAA サーバから送信された長い EAP メッセージ（SSL サーバ証明書）の例を示します。

1. AAA サーバは、SSL サーバ証明書を含む EAP-TLS メッセージを送信する必要があります。EAP パケットの合計サイズは 3,000 です。RADIUS Access-Challenge/UDP/IP でカプセ

ル化された後でも、AAA サーバ インターフェイスの MTU を下回ります。単一の IP パケットが 12 個の RADIUS EAP-Message 属性と一緒に送信されます。IP フラグメンテーションも EAP-TLS フラグメンテーションもありません。

2. Cisco IOS スイッチはこのようなパケットを受信し、それをカプセル化解除して、EAP を EAPoL 経由でサプリカントに送る必要があると判断します。EAPoL はフラグメンテーションをサポートしないため、スイッチが EAP-TLS フラグメンテーションを実行する必要があります。

3. Cisco IOS スイッチが、サプリカント宛てのインターフェイスの MTU (1,500) に収まる最初の EAP-TLS フラグメントを準備します。

4. このフラグメントがサプリカントによって確認されます。

5. 確認応答の受信後に、別の EAP-TLS フラグメントが送信されます。

6. このフラグメントがサプリカントによって確認されます。

7. 最後の EAP-TLS フラグメントがスイッチによって送信されます。

このシナリオでは、次のことが明らかになります。

- 環境によっては、NAD が EAP-TLS フラグメントを作成する必要があります。
- NAD は、これらのフラグメントの送信/確認応答を扱う必要があります。

ジャンボ フレームをサポートするリンク経由で接続されたサプリカントでも同じ状況が起きる可能性がありますが、AAA サーバではより小さい MTU が使用されます (その後、Cisco IOS スイッチが AAA サーバ宛てに EAP パケットを送信するときに EAP-TLS フラグメントを作成します)。

RADIUS 属性の Framed-MTU

RADIUS の場合は、次のように、RFC 2865 で Framed-MTU 属性が定義されています。

"This Attribute indicates the Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (such as PPP).It MAY be used in Access-Accept packets.

It MAY be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that value, but the server is not required to honor the hint."

ISE はヒントを受け入れません。Access-Request で NAD から送信される Framed-MTU の値は、ISE によって実行されるフラグメンテーションに影響を与えません。

最新のいくつかの Cisco IOS スイッチでは、グローバルに有効にされるジャンボ フレーム設定を除いて、イーサネット インターフェイスの MTU の変更が許可されません。ジャンボ フレームの設定は、RADIUS Access-Request で送信される Framed-MTU 属性の値に影響します。たとえば、次のように設定したとします。

```
<#root>

Switch(config)#

system mtu jumbo 9000
```

これによって、スイッチがすべての RADIUS Access-Request で強制的に Framed-MTU = 9000 を送信するようになります。ジャンボ フレームを含まないシステム MTU の場合も同じです。

```
<#root>

Switch(config)#

system mtu 1600
```

これによって、スイッチがすべての RADIUS Access-Request で強制的に Framed-MTU = 1600 を送信するようになります。

最新の Cisco IOS スイッチではシステム MTU 値を 1,500 未満に減らすことができないことに注意してください。

EAP フラグメントを送信したときの AAA サーバとサプリカントの動作

ISE

ISE は、常に 1,002 バイト長の EAP-TLS フラグメント（通常はサーバ Hello と証明書）を送信しようとします（ただし、通常は最後のフラグメントが小さくなります）。

また、ISE は RADIUS Framed-MTU を受け入れません。より大きい EAP-TLS フラグメントを送信するように再設定することはできません。

Microsoft ネットワーク ポリシー サーバ（NPS）

NPS 上で Framed-MTU 属性をローカルに設定した場合は、EAP-TLS フラグメントのサイズを設定することができます。

「Configure the EAP Payload Size on Microsoft NPS」の記事には、NPS RADIUS サーバのフレーム化された MTU のデフォルト値が 1,500 だと記載されていますが、Cisco Technical Assistance Center（TAC）ラボでは、デフォルト設定で 2,000 が送信されることが判明しています（Microsoft Windows 2012 データセンターで確認済み）。

前述のガイドに従った Framed-MTU locally の設定が NPS で尊重され、Framed-MTU で設定されたフラグメント サイズに EAP メッセージが分割されることがテストされています。ただし、Access-Request で受信された Framed-MTU 属性は使用されません（ISE/ACS 上と同様）。

この値の設定は、次のようなトポロジの問題を解決するための有効な回避策になります。

サプリカント[MTU 1500] ---- ---- [MTU 9000]Switch[MTU 9000] ----- ----- [MTU 9000]NPS

現在、スイッチではポートごとにMTUを設定できません。6880スイッチでは、この機能はCisco Bug ID CSCuo26327 - 802.1x EAP-TLSがFEXホストポートで機能しない、で追加されています。

AnyConnect

AnyConnect は 1,486 バイト長の EAP-TLS フラグメント（通常はクライアント証明書）を送信します。この値のサイズとして、イーサネット フレームは 1,500 バイトです。通常、最後のフラグメントはこれより小さくなります。

Microsoft Windows ネイティブ サプリカント

Microsoft Windows は、1,486 または 1,482 バイト長の EAP-TLS フラグメント（通常はクライアント証明書）を送信します。この値のサイズとして、イーサネット フレームは 1,500 バイトです。通常、最後のフラグメントはこれより小さくなります。

関連情報

- IEEE 802.1x ポートベース認証の設定
- テクニカル サポートとドキュメント - Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。