EAP 프래그먼트화 구현 및 동작

목차

소개

이 문서에서는 EAP(Extensible Authentication Protocol) 세션을 이해하고 문제를 해결하는 방법에 대해 설명합니다.

배경 정보

이 문서의 섹션은 다음 영역의 지원 범위를 대상으로 작성되었습니다.

- EAP-TLS(Extensible Authentication Protocol-Transport Layer Security) 세션에 대한 서버 인증서를 반환할 때 AAA(Authentication, Authorization, and Accounting) 서버의 동작
- EAP-TLS 세션에 대한 클라이언트 인증서를 반환 할 때 서 플리 컨 트의 동작
- Microsoft Windows Native Supplicant와 Cisco AnyConnect NAM(Network Access Manager)을 모두 사용하는 경우의 상호 운용성
- IP, RADIUS, EAP-TLS의 단편화 및 네트워크 액세스 디바이스에 의해 수행되는 리어셈블리

프로세스
- RADIUS Framed-Maximum Transmission Unit (MTU) 특성
- AAA 서버가 EAP-TLS 패킷의 단편화를 수행할 때의 동작

사전 요구 사항

요구 사항

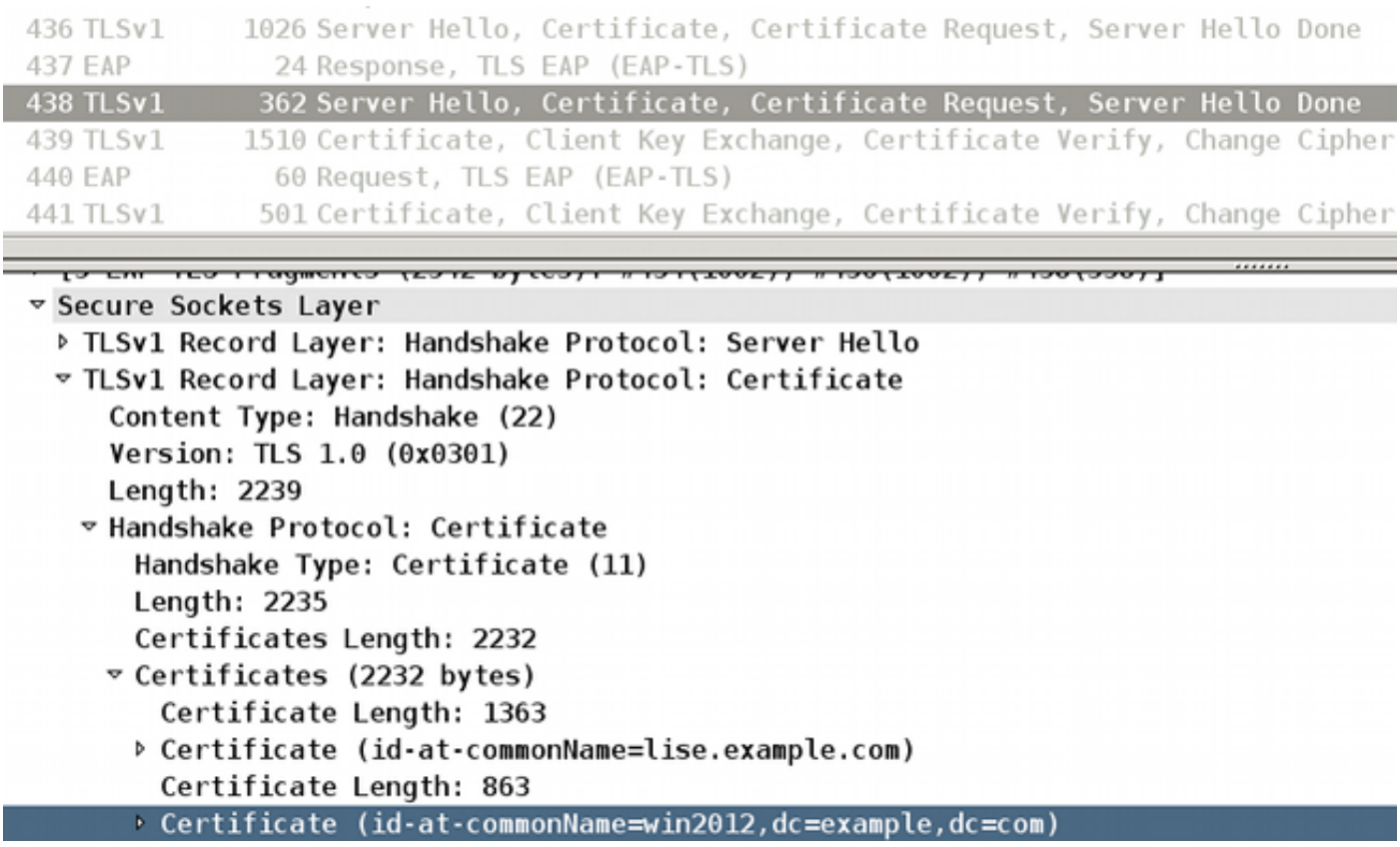
다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- EAP 및 EAP-TLS 프로토콜
- Cisco ISE(Identity Services Engine) 구성
- Cisco Catalyst 스위치의 CLI 컨피그레이션

이 문서를 이해하기 위해서는 EAP 및 EAP-TLS에 대한 이해가 필요합니다.

서버에서 반환한 인증서 체인

AAA 서버(ACS(Access Control Server) 및 ISE)는 항상 서버 Hello 및 서버 인증서가 포함된 EAP-TLS 패킷의 전체 체인을 반환합니다.



ISE ID 인증서(CN(Common Name)=lise.example.com)가 CN=win2012,dc=example,dc=com에 서명한 CA(Certificate Authority)와 함께 반환됩니다. 동작은 ACS와 ISE 모두에서 동일합니다.

신청자가 반환한 인증서 체인

Microsoft Windows 네이티브 서 플리 컨 트

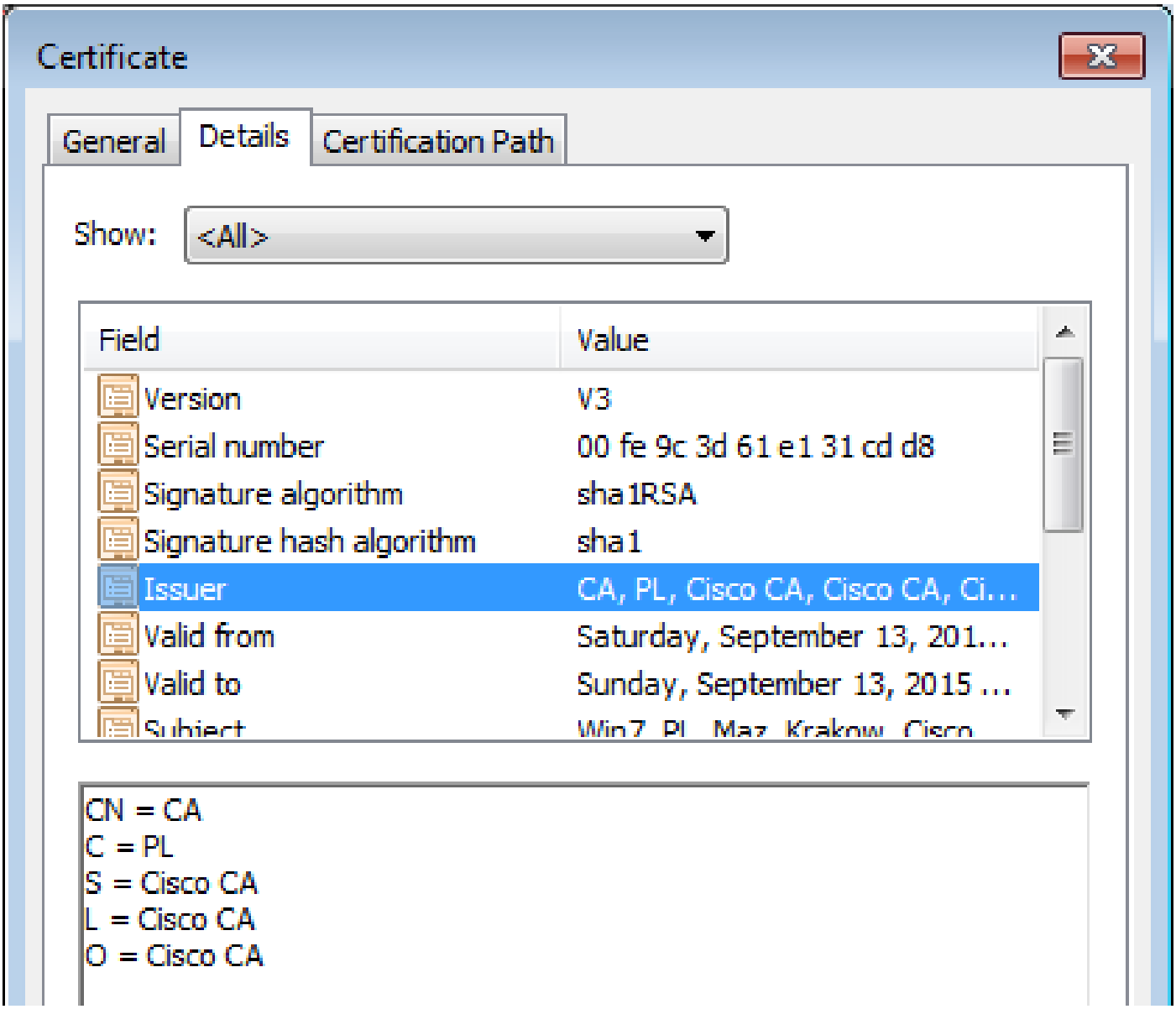
EAP-TLS를 사용하기 위해 구성된 Microsoft Windows 7 기본 신청자는 "단순 인증서 선택"을 사용하거나 사용하지 않고 클라이언트 인증서의 전체 체인을 전송하지 않습니다.

이 동작은 클라이언트 인증서가 서버 인증서와 다른 CA(다른 체인)에 의해 서명된 경우에도 발생합니다.

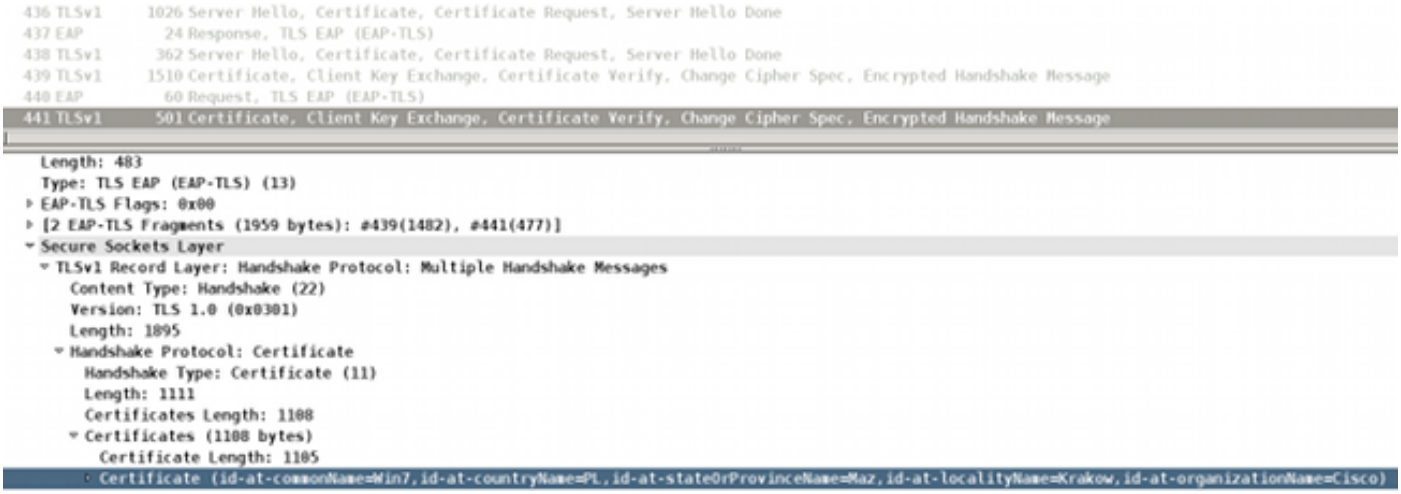
이 예는 이전 스크린샷에 나온 Server Hello 및 Certificate와 관련된 것입니다.

이 시나리오에서 CA는 주체 이름 CN=win2012,dc=example,dc=com을 사용하여 ISE 인증서를 서명합니다.

그러나 Microsoft 저장소에 설치된 사용자 인증서는 다른 CA, CN=CA,C=PL,S=Cisco CA,L=Cisco CA, O=Cisco CA에 의해 서명됩니다.



따라서 Microsoft Windows 신청자는 클라이언트 인증서로만 응답합니다. 서명하는 CA(CN=CA,S=PL,S=Cisco CA, L=Cisco CA, O=Cisco CA)는 연결되어 있지 않습니다.



이러한 동작으로 인해 AAA 서버가 클라이언트 인증서를 검증할 때 문제가 발생할 수 있습니다. 이 예는 Microsoft Windows 7 SP1 Professional과 관련이 있습니다.

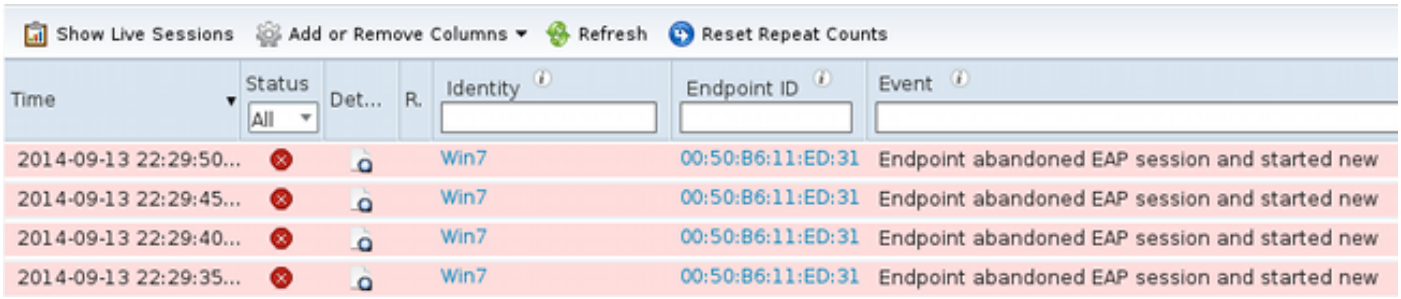
솔루션

전체 인증서 체인은 ACS 및 ISE의 인증서 저장소에 설치됩니다(모든 CA 및 하위 CA 서명 클라이언트 인증서).

인증서 유효성 검사 문제는 ACS 또는 ISE에서 쉽게 탐지할 수 있습니다. 신뢰할 수 없는 인증서에 대한 정보가 표시되고 ISE가 다음을 보고합니다.

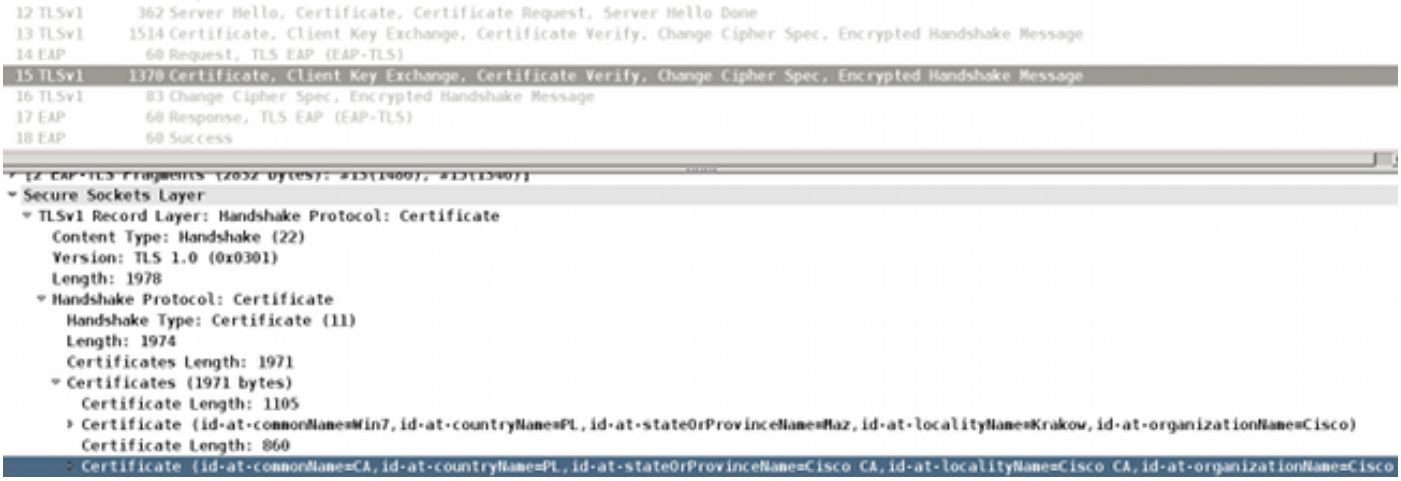
```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

신청자에 대한 인증서 유효성 검사 문제는 쉽게 감지되지 않습니다. 일반적으로 AAA 서버는 "엔드포인트가 EAP 세션을 중단함"에 응답합니다.



AnyConnect 이름

AnyConnect NAM에는 이 제한이 없습니다. 동일한 시나리오에서 클라이언트 인증서의 전체 체인을 연결합니다(올바른 CA가 연결됨).



Microsoft Windows 기본 신청자와 AnyConnect NAM

두 서비스가 모두 작동하면 AnyConnect NAM이 우선적으로 적용됩니다.

NAM 서비스가 실행되지 않는 경우에도 Microsoft Windows API에서 후크하고 EAP 패킷을 전달하므로 Microsoft Windows 네이티브 서 플리 컨 트에 문제가 발생할 수 있습니다.

다음은 그러한 실패의 예입니다.

다음 명령을 사용하여 Microsoft Windows에서 추적을 활성화합니다.

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

추적(c:\windows\trace\svchost_RASTLS.LOG)에는 다음이 표시됩니다.

<#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

마지막 패킷은 Microsoft Windows 네이티브 서 플리 컨 트가 전송 된 클라이언트 인증서 (EAP 크기 1492 EAP-TLS 조각 1) 입니다. 안타깝게도 Wireshark는 해당 패킷을 표시하지 않습니다.

	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

그리고 이 패킷은 실제로 전송되지 않습니다. 마지막 패킷은 EAP-TLS 전달 서버 인증서의 세 번째 프래그먼트입니다.

Microsoft Windows API를 후크하는 AnyConnect NAM 모듈에서 사용되었습니다.

따라서 Microsoft Windows 네이티브 서 플리 컨 트와 함께 AnyConnect를 사용 하는 것이 좋습니다.

AnyConnect 서비스를 사용할 때는 Microsoft Windows 기본 신청자가 아니라 NAM(802.1x 서비스가 필요한 경우)도 사용하는 것이 좋습니다.

단편화

조각화는 여러 레이어에서 발생할 수 있습니다.

- IP
- RADIUS AVP(Attribute Value Pairs)

- EAP-TLS

Cisco IOS® 스위치는 매우 지능적입니다. EAP 및 EAP-TLS 형식을 이해할 수 있습니다.

스위치는 TLS 터널을 해독할 수 없지만 EAPoL(Extensible Authentication Protocol over LAN) 또는 RADIUS에서 캡슐화할 때 EAP 패킷의 단편화, 조립 및 재결합을 담당합니다.

EAP 프로토콜은 프래그먼트화를 지원하지 않습니다. 다음은 RFC 3748(EAP)의 일부입니다.

"프래그먼트화는 EAP 자체 내에서 지원되지 않습니다. 그러나 개별 EAP 방법은 이를 지원할 수 있습니다."

EAP-TLS가 그러한 예입니다. 다음은 RFC 5216(EAP-TLS), 섹션 2.1.5(프래그먼트화)의 일부입니다.

"EAP-TLS 피어가 M 비트 세트와 함께 EAP-Request 패킷을 수신하면 EAP-Type=EAP-TLS이고 데이터가 없는 EAP-Response로 응답해야 합니다.

이는 프래그먼트 ACK의 역할을 합니다. EAP 서버는 다른 프래그먼트를 전송하기 전에 EAP 응답을 수신할 때까지 기다려야 합니다."

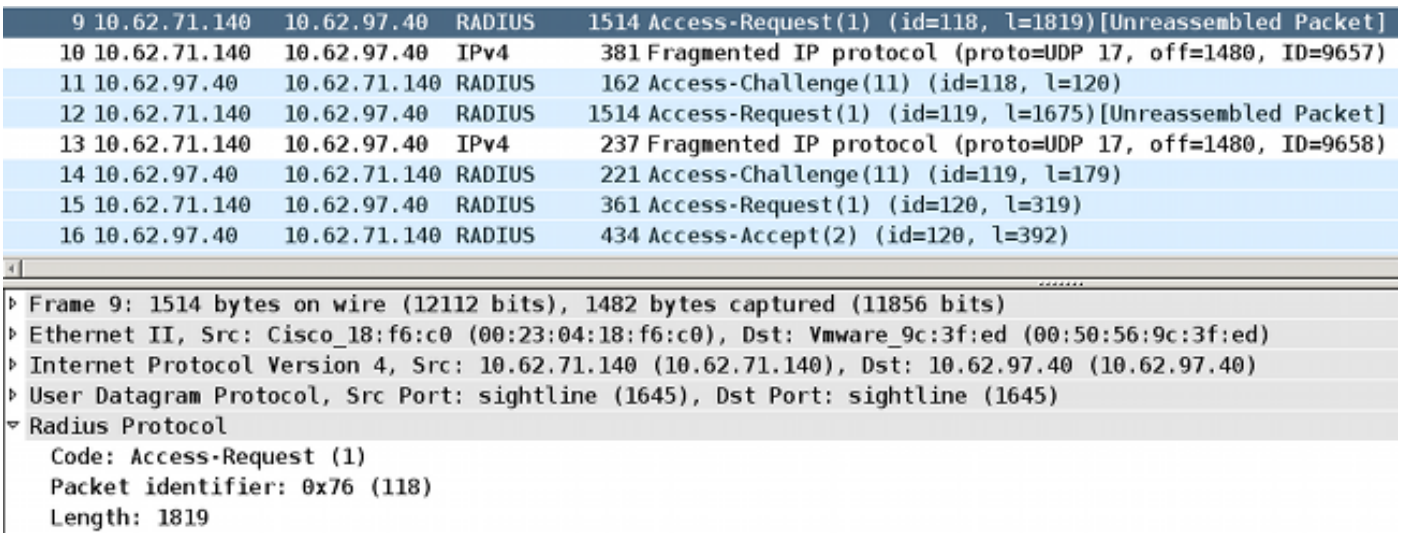
마지막 문장은 AAA 서버의 매우 중요한 특징을 기술한다. 다른 EAP 프래그먼트를 전송하려면 먼저 ACK를 기다려야 합니다. 유사한 규칙이 서 플리 컨 트에 사용 됩니다.

"EAP 피어는 다른 프래그먼트를 전송하기 전에 EAP 요청을 수신할 때까지 기다려야 합니다."

IP 레이어의 프래그먼트화

프래그먼트화는 NAD(Network Access Device)와 AAA 서버(전송으로 사용되는 IP/UDP/RADIUS) 간에만 발생할 수 있습니다.

이 상황은 NAD(Cisco IOS Switch)가 인터페이스의 MTU보다 큰 EAP 페이로드를 포함하는 RADIUS 요청을 전송하려고 할 때 발생합니다.



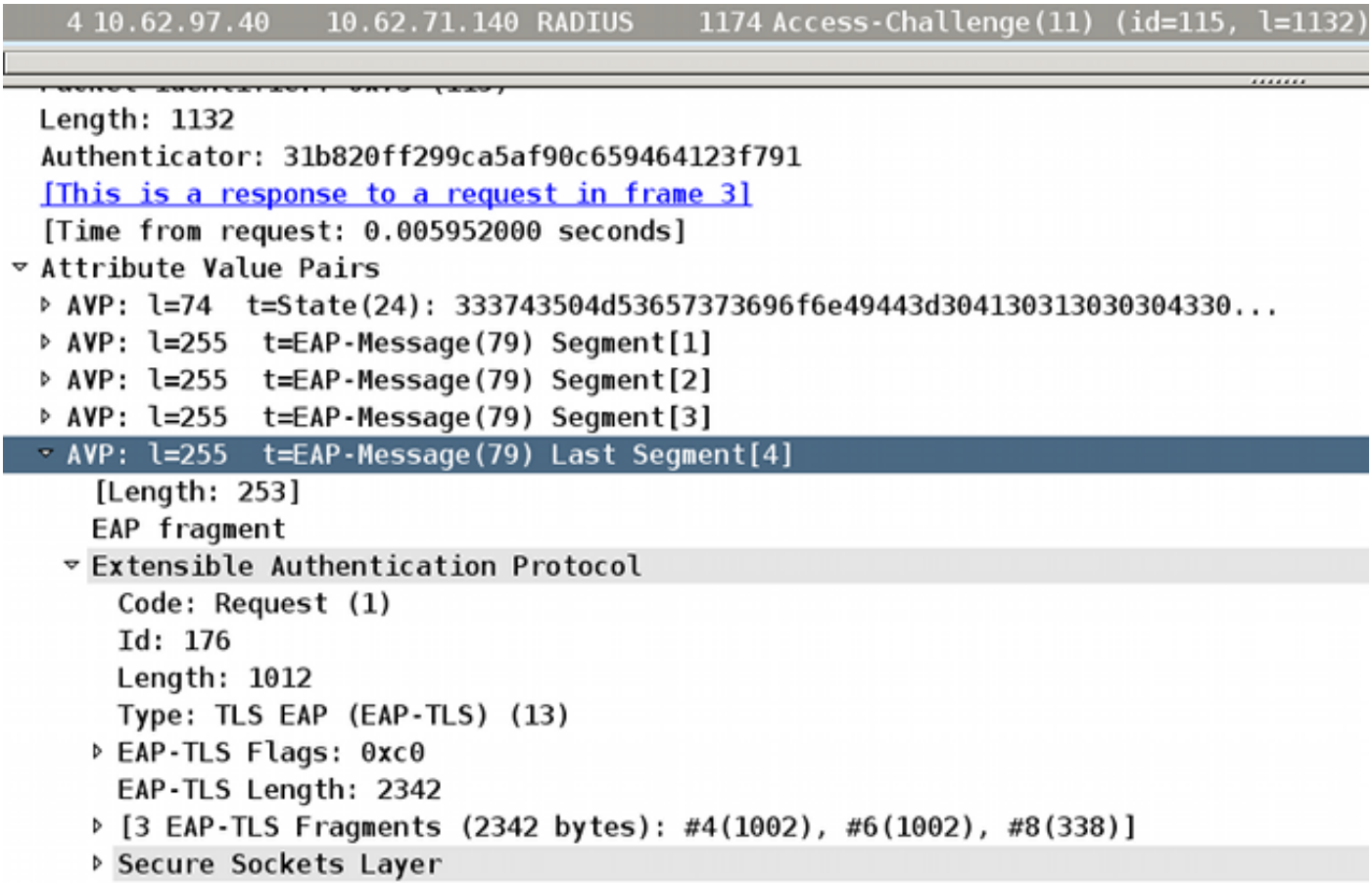
대부분의 Cisco IOS 버전은 충분히 지능적이지 않으며 EAPoL을 통해 수신된 EAP 패킷을 어셈블하고 AAA 서버를 향하는 물리적 인터페이스의 MTU에 적합할 수 있는 RADIUS 패킷에서 결합하려

고 시도하지 않습니다.

AAA 서버가 더 지능적입니다(다음 섹션에 제시된 것처럼).

RADIUS의 단편화

이것은 실제로 어떤 종류의 단편화도 아닙니다. RFC 2865에 따르면 단일 RADIUS 특성은 최대 253바이트의 데이터를 가질 수 있습니다.따라서 EAP 페이로드는 항상 여러 EAP-Message RADIUS 특성으로 전송됩니다.



이러한 EAP-Message 특성은 다시 조합되고 Wireshark에 의해 해석됩니다("Last Segment" 특성은 전체 EAP 패킷의 페이로드를 나타냄).

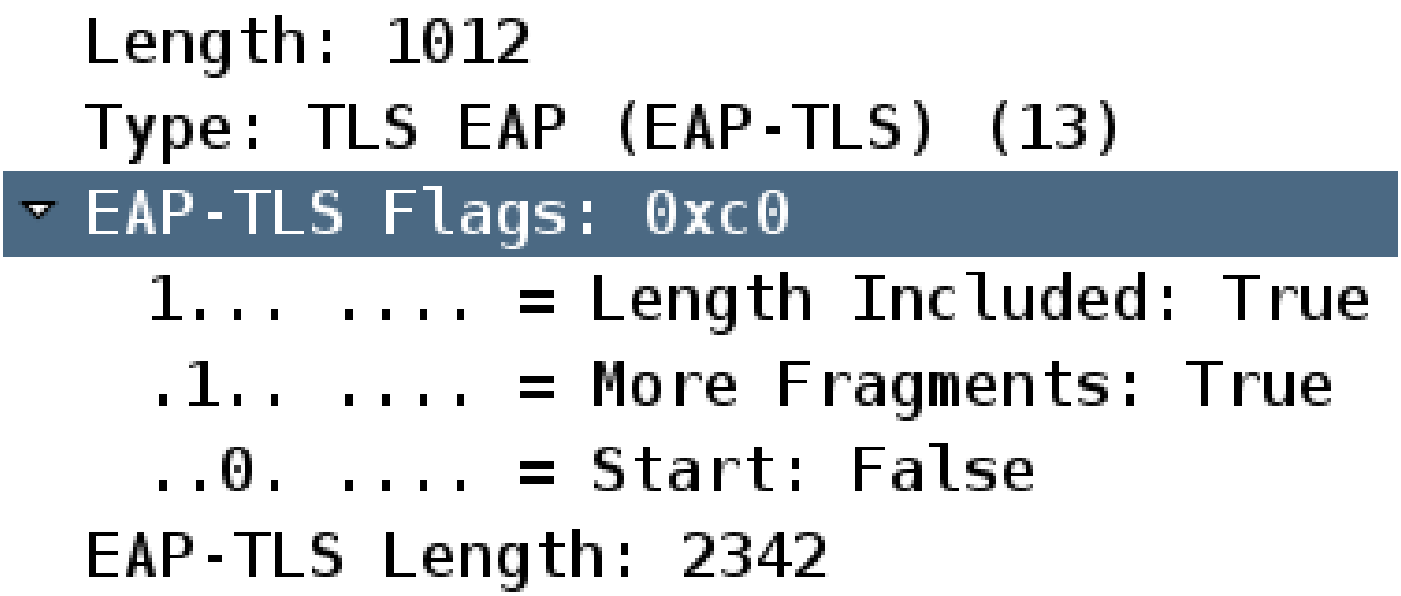
EAP 패킷의 Length 헤더는 1,012이며, 이를 전송하려면 4개의 RADIUS AVP가 필요합니다.

EAP-TLS의 단편화

동일한 스크린샷에서 다음을 확인할 수 있습니다.

- EAP 패킷 길이는 1,012입니다
- EAP-TLS 길이는 2,342입니다.

이는 첫 번째 EAP-TLS 프래그먼트이며 신청자는 더 많은 것을 기대함을 나타냅니다. 이는 EAP-TLS 플래그를 검사할 경우 확인될 수 있습니다.



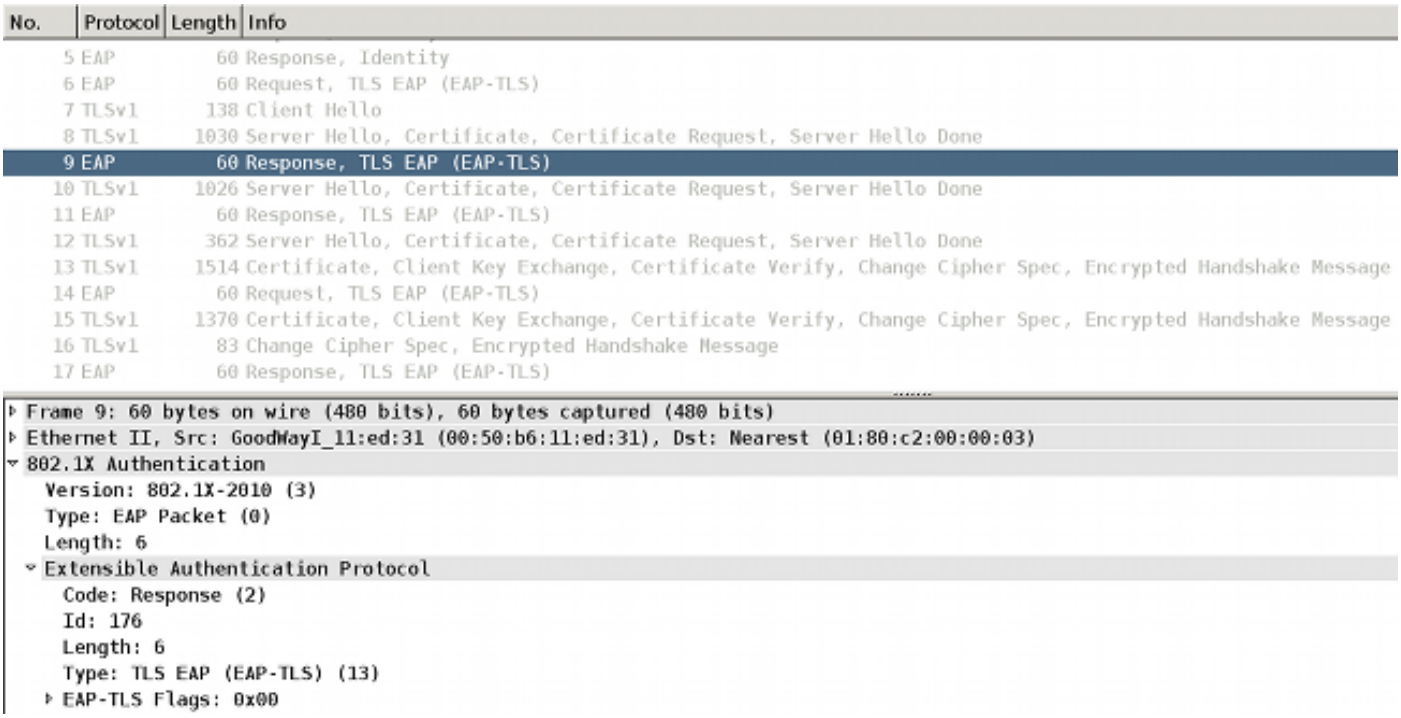
이러한 종류의 단편화는 다음에서 가장 자주 발생합니다.

- AAA 서버가 보낸 RADIUS 액세스 챌린지. 이 서버는 전체 체인의 SSL(Secure Sockets Layer) 서버 인증서와 함께 EAP 요청을 전달합니다.
- RADIUS 액세스 요청 NAD에 의해 전송, 전체 체인의 SSL 클라이언트 인증서와 함께 EAP 응답을 전달 합니다.

EAP-TLS 프래그먼트 확인

앞서 설명한 대로 모든 EAP-TLS 프래그먼트는 다음 프래그먼트가 전송되기 전에 승인되어야 합니다.

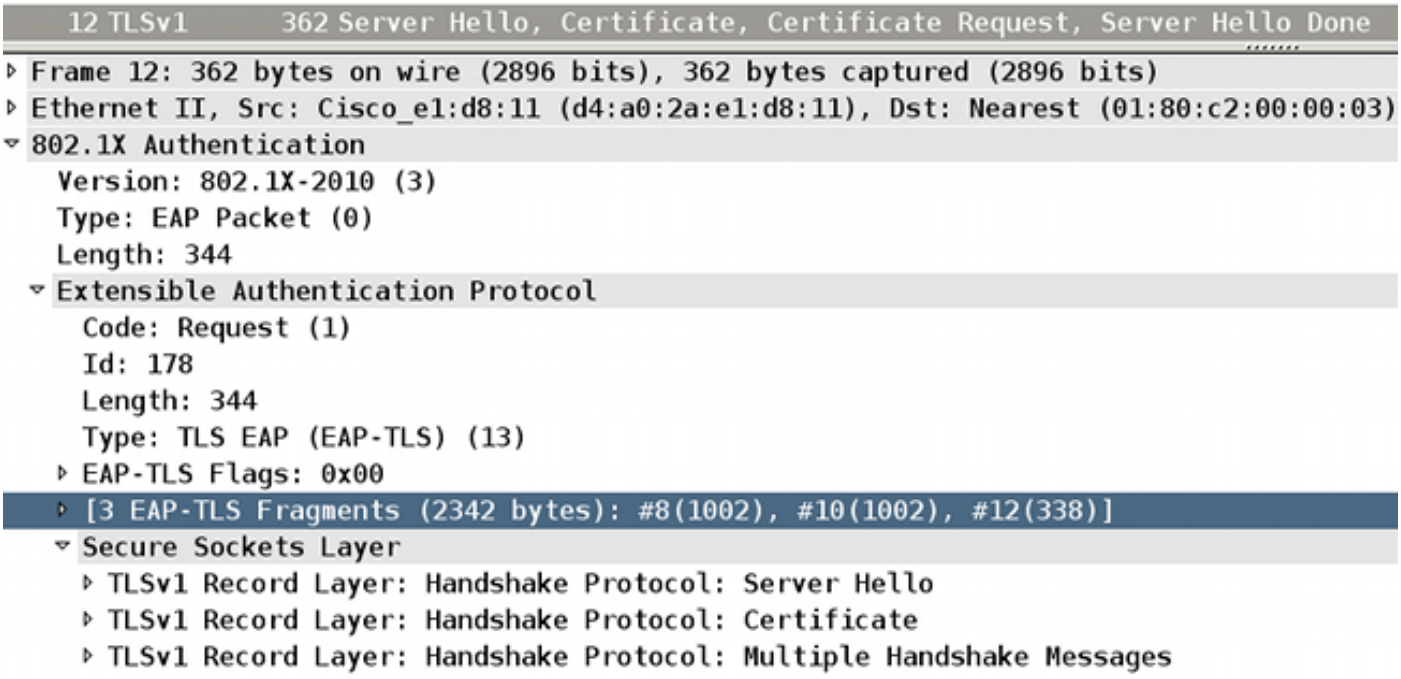
예(신청자와 NAD 간의 EAPoL에 대한 패킷 캡처):



EAPoL 프레임 및 AAA 서버는 서버 인증서를 반환합니다.

- 해당 인증서는 EAP-TLS 프래그먼트(패킷 8)로 전송됩니다.
- 신청자는 해당 프래그먼트(패킷 9)를 승인합니다.
- 두 번째 EAP-TLS 프래그먼트는 NAD(패킷 10)에 의해 전달됩니다.
- 신청자는 해당 프래그먼트(패킷 11)를 승인합니다.
- 세 번째 EAP-TLS 프래그먼트는 NAD(패킷 12)에 의해 전달됩니다.
- 신청자는 이를 승인할 필요가 없으며, 대신 패킷 13에서 시작되는 클라이언트 인증서를 계속 진행합니다.

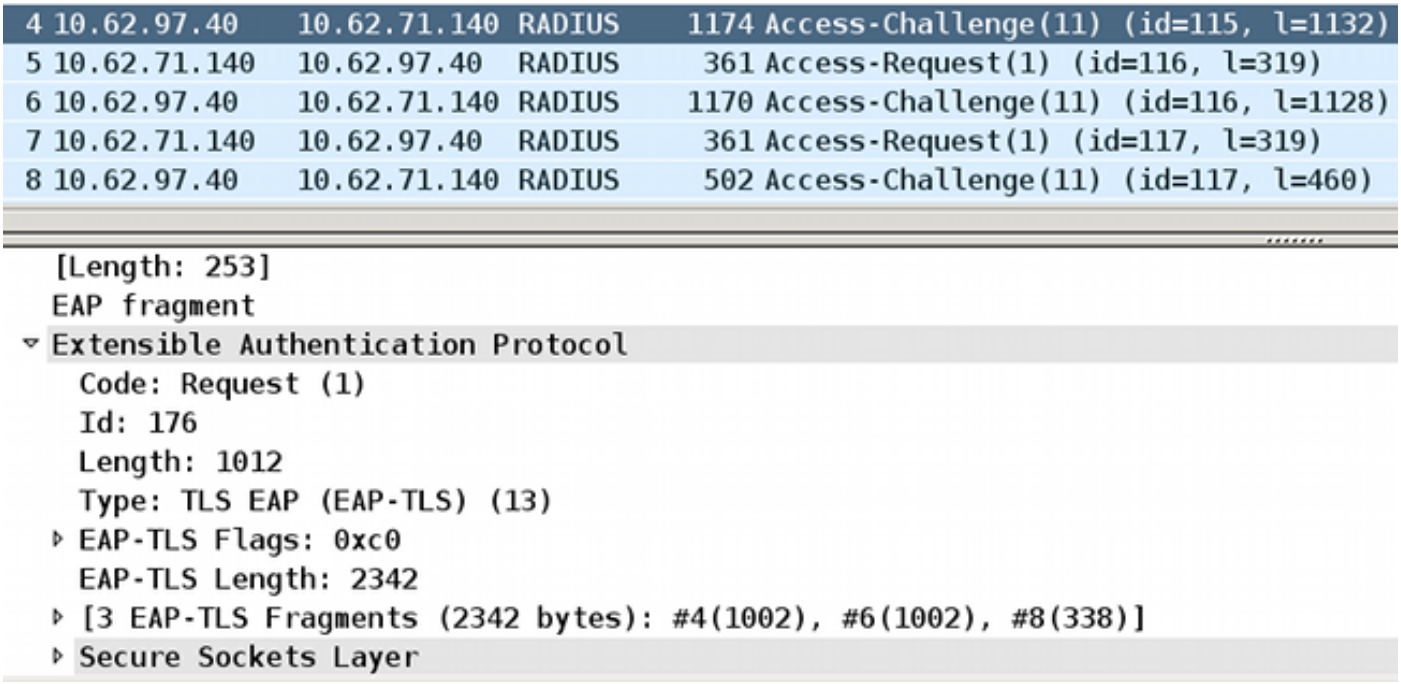
패킷 12에 대한 자세한 내용은 다음과 같습니다.



Wireshark에서 패킷 8, 10, 12를 리어셈블한 것을 확인할 수 있습니다.

EAP 프래그먼트의 크기는 1,002, 1,002 및 338이며, 이는 EAP-TLS 메시지의 총 크기를 2342로 가져옵니다.

모든 프래그먼트에서 총 EAP-TLS 메시지 길이가 공지됩니다. RADIUS 패킷(NAD와 AAA 서버 간)을 검토하는 경우 이를 확인할 수 있습니다.



RADIUS 패킷 4, 6, 8은 이러한 3개의 EAP-TLS 프래그먼트를 전달합니다. 처음 두 조각은 인정됩니다.

Wireshark는 EAP-TLS 프래그먼트에 대한 정보를 제공할 수 있습니다(크기: 1,002 + 1,002 + 338 = 2,342).

이 시나리오와 예시는 쉬웠습니다. Cisco IOS 스위치는 EAP-TLS 프래그먼트 크기를 변경할 필요가 없습니다.

다른 크기로 다시 어셈블된 EAP-TLS 프래그먼트

AAA 서버에 대한 NAD MTU가 9,000바이트(점보 프레임)이고 AAA 서버가 점보 프레임을 지원하는 인터페이스를 사용하여 연결된 경우에도 어떻게 되는지 생각해 보십시오.

대부분의 일반 신청자는 MTU가 1,500인 1Gbit 링크를 사용하여 연결됩니다.

이러한 시나리오에서 Cisco IOS 스위치는 EAP-TLS "비대칭" 어셈블리 및 리어셈블리를 수행하고 EAP-TLS 프래그먼트 크기를 변경합니다.

다음은 AAA 서버(SSL 서버 인증서)에서 보낸 대규모 EAP 메시지의 예입니다.

1. AAA 서버는 SSL 서버 인증서와 함께 EAP-TLS 메시지를 보내야 합니다. 해당 EAP 패킷의 총 크기는 3,000입니다. RADIUS Access-Challenge/UDP/IP에서 캡슐화된 후에도 여전히 AAA 서버 인터페이스 MTU보다 작습니다. 단일 IP 패킷은 12 RADIUS EAP-Message 특성과 함께 전송됩니다. IP 또는 EAP-TLS 프래그먼트화가 없습니다.

2. Cisco IOS 스위치는 이러한 패킷을 수신하고 역캡슐화하고 EAPoL을 통해 신청자에게 EAP를 보내야 한다고 결정합니다. EAPoL은 프래그먼트화를 지원하지 않으므로, 스위치는 EAP-TLS 프래그먼트화를 수행해야 합니다.

3. Cisco IOS 스위치는 신청자(1,500)를 향하는 인터페이스의 MTU에 맞출 수 있는 첫 번째

EAP-TLS 프래그먼트를 준비합니다.

4. 이 프래그먼트는 신청자에 의해 확인됩니다.

5. 또 다른 EAP-TLS 프래그먼트는 확인 응답을 받은 후 전송됩니다.

6. 이 프래그먼트는 신청자에 의해 확인됩니다.

7. 마지막 EAP-TLS 프래그먼트는 스위치에 의해 전송됩니다.

이 시나리오에서는 다음을 보여줍니다.

- 어떤 상황에서는 NAD가 EAP-TLS 프래그먼트를 생성해야 합니다.
- NAD는 이러한 프래그먼트를 전송/승인할 책임이 있습니다.

AAA 서버의 MTU가 더 작은 반면 점보 프레임을 지원하는 링크를 통해 연결된 신청자에 대해서도 동일한 상황이 발생할 수 있습니다(그런 다음 Cisco IOS 스위치는 EAP 패킷을 AAA 서버로 전송할 때 EAP-TLS 프래그먼트를 생성합니다).

RADIUS 특성 Framed-MTU

RADIUS의 경우 RFC 2865에 정의된 Framed-MTU 특성이 있습니다.

"이 특성은 PPP와 같은 다른 방법으로 협상되지 않은 경우 사용자에 대해 구성할 최대 전송 단위를 나타냅니다. Access-Accept 패킷에서 사용될 수 있습니다.

NAS에서 서버에 해당 값을 선호한다는 힌트로 Access-Request 패킷에 사용할 수 있지만, 서버가 힌트를 준수하는 데 필요하지 않습니다."

ISE는 힌트를 따르지 않습니다. Access-Request에서 NAD가 전송하는 Framed-MTU의 값은 ISE가 수행하는 단편화에 영향을 미치지 않습니다.

최신 Cisco IOS 스위치를 여러 개 사용하면 스위치에서 전역으로 활성화된 점보 프레임 설정을 제외하고 이더넷 인터페이스의 MTU를 변경할 수 없습니다. 점보 프레임의 컨피그레이션은 RADIUS Access-Request에서 전송되는 Framed-MTU 특성의 값에 영향을 줍니다. 예를 들어 다음을 설정할 수 있습니다.

```
<#root>

Switch(config)#

system mtu jumbo 9000
```

그러면 스위치가 모든 RADIUS 액세스 요청에서 Framed-MTU = 9000을 보냅니다. 점보 프레임 없이 시스템 MTU에 대해서도 동일합니다.

```
<#root>
```

```
Switch(config)#
system mtu 1600
```

그러면 스위치가 모든 RADIUS 액세스 요청에서 Framed-MTU = 1600을 보냅니다.

최신 Cisco IOS 스위치에서는 시스템 MTU 값을 1,500 이하로 낮출 수 없습니다.

EAP 프래그먼트를 전송할 때의 AAA 서버 및 신청자 동작

ISE

ISE는 항상 1,002바이트 길이의 EAP-TLS 프래그먼트(일반적으로 Server Hello with Certificate)를 보내려고 시도합니다(마지막 프래그먼트는 대개 더 작지만).

RADIUS Framed-MTU를 준수하지 않습니다. 더 큰 EAP-TLS 프래그먼트를 전송하도록 재구성할 수는 없습니다.

Microsoft NPS(네트워크 정책 서버)

NPS에서 로컬로 Framed-MTU 특성을 구성하는 경우 EAP-TLS 프래그먼트의 크기를 구성할 수 있습니다.

Configure the EAP Payload Size on Microsoft NPS 문서에서 NPS RADIUS 서버에 대한 프레임 MTU의 기본값이 1,500이라고 언급했지만 Cisco TAC(Technical Assistance Center) 랩에서는 기본 설정(Microsoft Windows 2012 Datacenter에서 확인)으로 2,000을 전송하는 것으로 나타났습니다.

앞서 언급한 가이드에 따라 Framed-MTU를 로컬로 설정하는 것은 NPS에서 허용하며, EAP 메시지를 Framed-MTU에 설정된 크기의 조각으로 조각화하는 것이 테스트되었습니다. 그러나 Access-Request에서 받은 Framed-MTU 특성은 사용되지 않습니다(ISE/ACS에서와 동일).

이 값을 설정하면 다음과 같은 토폴로지의 문제를 해결할 수 있습니다.

신청자 [MTU 1500] ---- ---- [MTU 9000]스위치[MTU 9000] ----- ----- [MTU 9000]NPS

현재 스위치에서는 포트당 MTU를 설정할 수 없습니다. 6880 스위치의 경우 이 기능이 Cisco 버그 ID CSCuo26327 - 802.1x EAP-TLS가 FEX 호스트 포트에서 작동하지 않을 때 추가됩니다.

AnyConnect

AnyConnect는 길이가 1,486바이트인 EAP-TLS 프래그먼트(일반적으로 클라이언트 인증서)를 전송합니다. 이 값의 경우 이더넷 프레임은 1,500바이트입니다. 마지막 조각은 대개 더 작습니다.

Microsoft Windows 네이티브 서 플리 컨 트

Microsoft Windows는 길이가 1,486바이트 또는 1,482바이트인 EAP-TLS 프래그먼트(일반적으로

클라이언트 인증서)를 전송합니다. 이 값의 경우 이더넷 프레임은 1,500바이트입니다. 마지막 조각은 대개 더 작습니다.

관련 정보

- IEEE 802.1x 포트 기반 인증 구성
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.