Implementazioni e comportamento della frammentazione EAP

Sommario

Introduzione

In questo documento viene descritto come comprendere e risolvere i problemi relativi alle sessioni EAP (Extensible Authentication Protocol).

Premesse

Le sezioni del presente documento si dedicano alla copertura in questi settori:

- Comportamento dei server di autenticazione, autorizzazione e accounting (AAA) quando restituiscono il certificato server per la sessione EAP-TLS (Extensible Authentication Protocol-Transport Layer Security)
- Comportamento dei supplicant quando restituiscono il certificato client per la sessione EAP-TLS
- Interoperabilità quando si usano sia Microsoft Windows Native Supplicant sia Cisco AnyConnect Network Access Manager (NAM)
- Frammentazione in IP, RADIUS ed EAP-TLS e processo di riassemblaggio eseguito da dispositivi di accesso alla rete
- Attributo MTU (Framed-Maximum Transmission Unit) RADIUS
- Comportamento dei server AAA quando eseguono la frammentazione dei pacchetti EAP-TLS

Prerequisiti

Requisiti

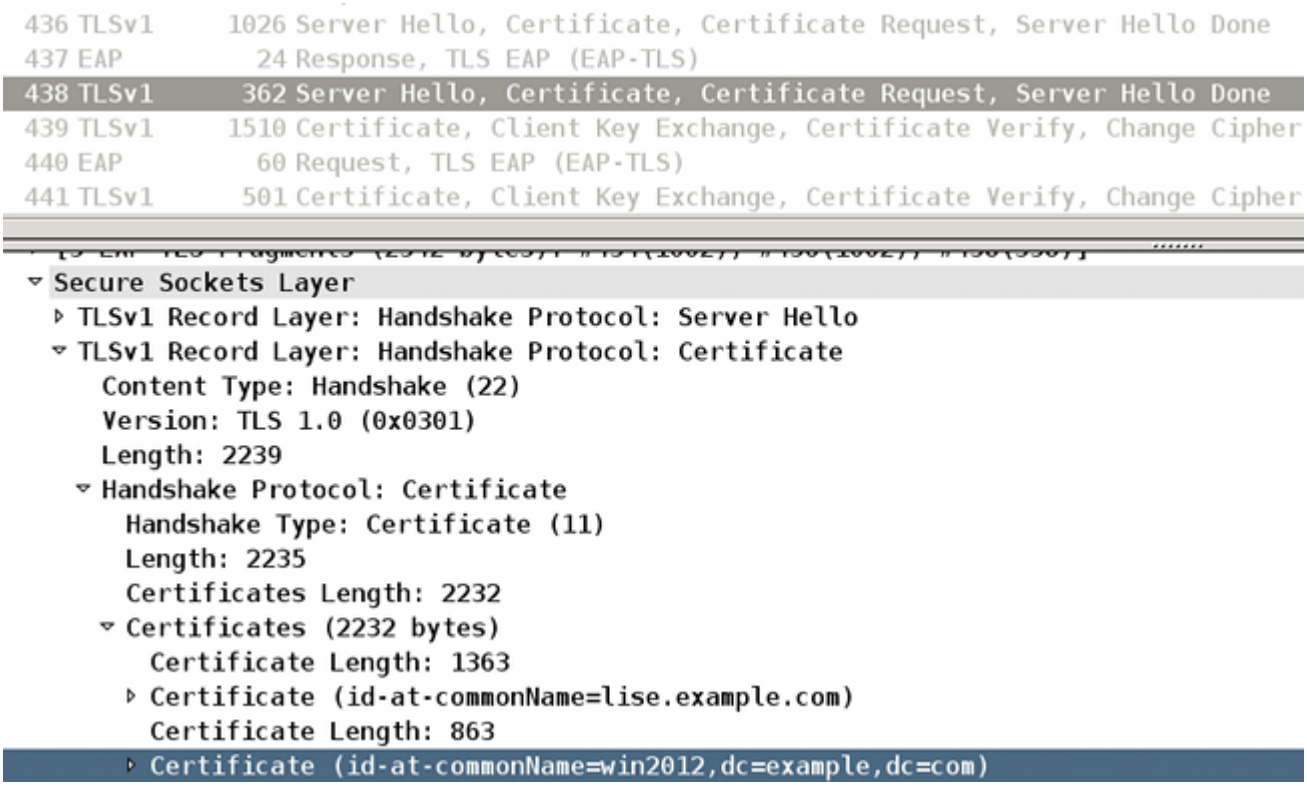
Cisco raccomanda la conoscenza dei seguenti argomenti:

- Protocolli EAP e EAP-TLS
- Configurazione di Cisco Identity Services Engine (ISE)
- Configurazione CLI degli switch Cisco Catalyst

È necessario avere una buona comprensione di EAP e EAP-TLS per poter comprendere questo articolo.

Catena di certificati restituita dal server

Il server AAA (Access Control Server (ACS) e ISE) restituisce sempre l'intera catena per il pacchetto EAP-TLS con Server Hello e il certificato server:



Il certificato di identità ISE (CN=lise.example.com) viene restituito insieme all'autorità di certificazione (CA) che ha firmato CN=win2012,dc=example,dc=com. Il comportamento è lo stesso per ACS e ISE.

Catena di certificati restituita dal richiedente

Supplicant nativo di Microsoft Windows

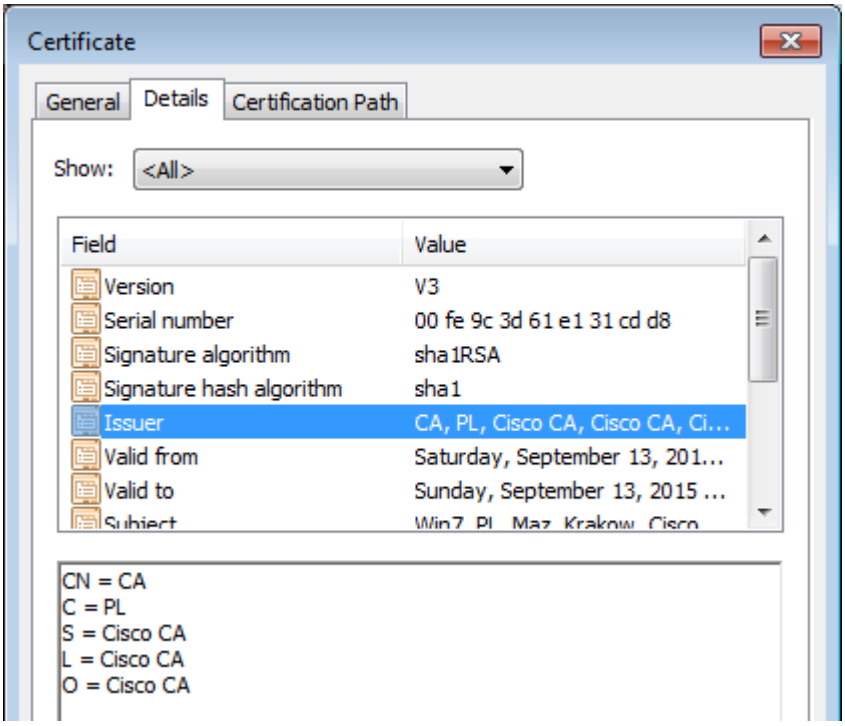
Il supplicant nativo di Microsoft Windows 7 configurato per l'utilizzo di EAP-TLS, con o senza la "selezione semplice del certificato", non invia l'intera catena del certificato client.

Questo comportamento si verifica anche quando il certificato client è firmato da un'autorità di certificazione (catena diversa) diversa da quella del certificato server.

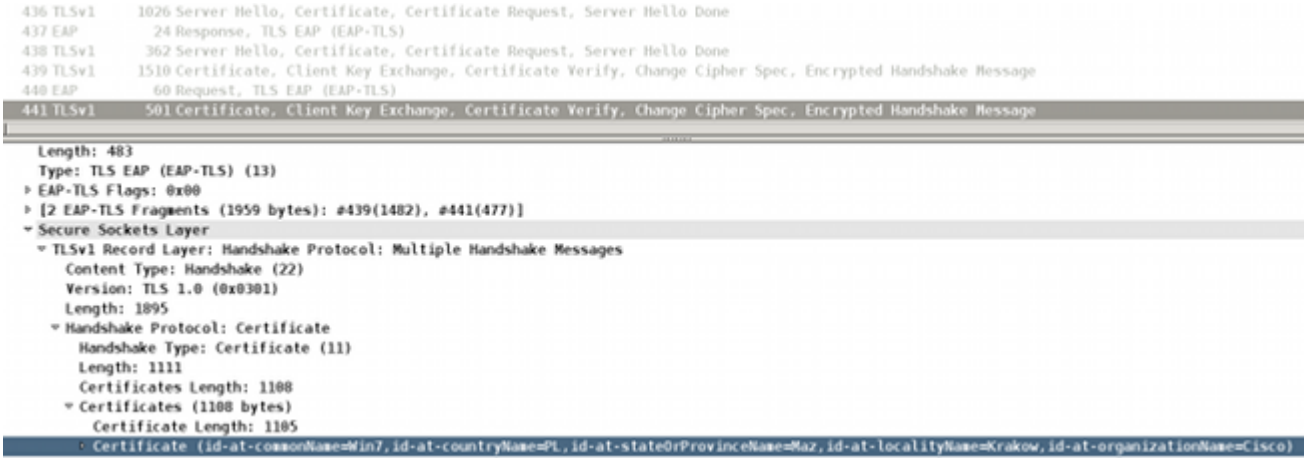
Questo esempio è relativo a Server Hello e Certificate presentati nella schermata precedente.

In questo scenario, il certificato ISE viene firmato dalla CA con l'utilizzo di un nome soggetto, CN=win2012,dc=example,dc=com.

Il certificato utente installato nell'archivio di Microsoft è firmato da un'altra CA, CN=CA,C=PL,S=Cisco CA,L=Cisco CA, O=Cisco CA.



Di conseguenza, il supplicant di Microsoft Windows risponde solo con il certificato client. La CA che la firma (CN=CA,S=PL,S=Cisco CA, L=Cisco CA, O=Cisco CA) non è collegata.



A causa di questo comportamento, i server AAA potrebbero incontrare problemi durante la convalida dei certificati client. L'esempio è relativo a Microsoft Windows 7 SP1 Professional.

Soluzione

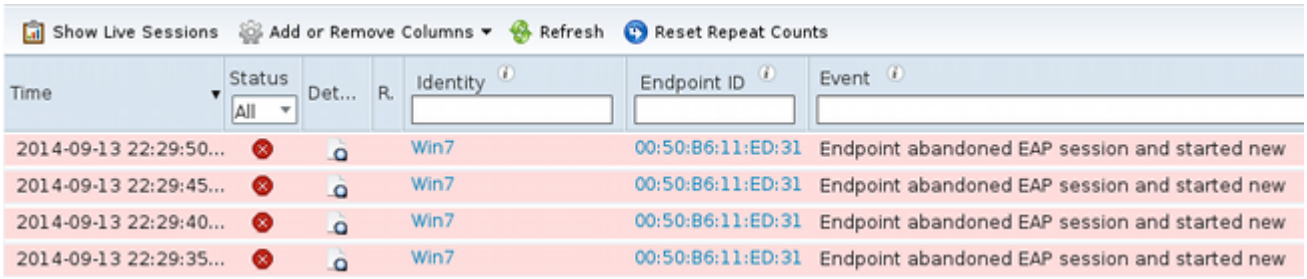
Una catena di certificati completa deve essere installata nell'archivio certificati di ACS e ISE (tutti i certificati client di firma CA e CA secondaria).

Problemi con la convalida del certificato possono essere facilmente rilevati su ACS o ISE. Vengono

presentate le informazioni sui certificati non attendibili e ISE riporta:

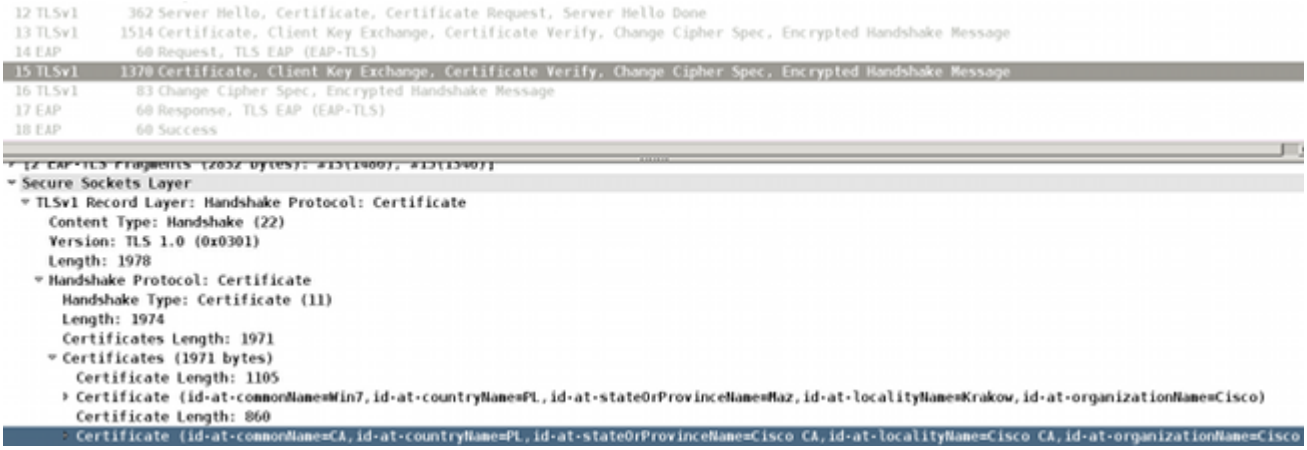
```
12514 EAP-TLS failed SSL/TLS handshake because of an unknown CA in the client
certificates chain
```

I problemi relativi alla convalida dei certificati nel richiedente non sono facilmente rilevabili. Di solito il server AAA risponde che "la sessione EAP dell'endpoint è stata abbandonata":



AnyConnect NAM

AnyConnect NAM non ha questa limitazione. Nello stesso scenario, viene collegata la catena completa del certificato client (viene allegata la CA corretta):



Supplicant nativo di Microsoft Windows con AnyConnect NAM

Quando entrambi i servizi sono attivi, AnyConnect NAM ha la precedenza.

Anche quando il servizio NAM non è in esecuzione, continua a collegarsi all'API di Microsoft Windows e inoltra i pacchetti EAP, causando problemi al supplicant nativo di Microsoft Windows.

Ecco un esempio di tale fallimento.

In Microsoft Windows l'analisi può essere attivata con questo comando:

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

Le tracce (**c:\windows\trace\svchost_RASTLS.LOG**) mostrano:

<#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)

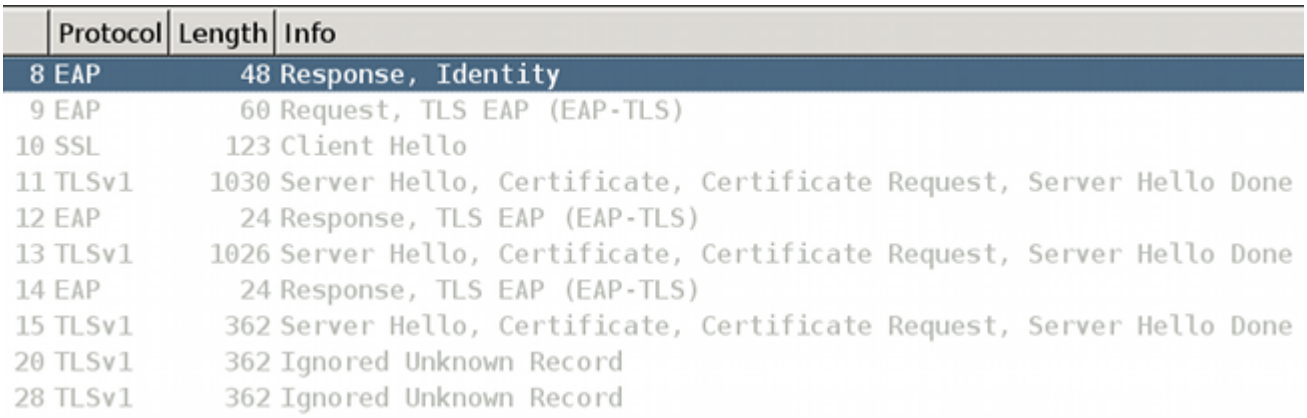
packet: Id: 125, Length:

1492

, Type: 13,

TLS blob length: 1819. Flags: LM

L'ultimo pacchetto è un certificato client (frammento EAP-TLS 1 con dimensione EAP 1492) inviato dal supplicant nativo di Microsoft Windows. Sfortunatamente, Wireshark non mostra quel pacchetto:



	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 quel pacchetto non è realmente inviato; l'ultimo è stato il terzo frammento del certificato del server di trasporto EAP-TLS.

È stato usato dal modulo AnyConnect NAM che si collega all'API di Microsoft Windows.

Per questo motivo, non si consiglia di utilizzare AnyConnect con il supplicant nativo di Microsoft Windows.

Quando si usano i servizi AnyConnect, si consiglia di usare anche NAM (quando sono necessari i servizi 802.1x), non Microsoft Windows Native Supplicant.

Frammentazione

È possibile che la frammentazione si verifichi su più livelli:

- IP
- Coppie di valori di attributo RADIUS (AVP)
- EAP-TLS

Gli switch Cisco IOS® sono molto intelligenti. Sono in grado di comprendere i formati EAP e EAP-TLS.

Sebbene lo switch non sia in grado di decrittografare il tunnel TLS, è responsabile della frammentazione, nonché dell'assemblaggio e del riassemblaggio dei pacchetti EAP quando incapsulato in EAPoL (Extensible Authentication Protocol over LAN) o RADIUS.

Il protocollo EAP non supporta la frammentazione. Di seguito è riportato un estratto della RFC 3748 (EAP):

"La frammentazione non è supportata all'interno del protocollo EAP stesso, ma è possibile che sia supportata dai singoli metodi EAP."

EAP-TLS è un esempio di questo tipo. Di seguito è riportato un estratto della RFC 5216 (EAP-TLS), sezione 2.1.5 (frammentazione):

"Quando un peer EAP-TLS riceve un pacchetto EAP-Request con bit M impostato, DEVE rispondere con una risposta EAP-Type=EAP-TLS e senza dati.

Questa funzione viene utilizzata come ACK di frammenti. **Il server EAP DEVE attendere di ricevere la risposta EAP prima di inviare un altro frammento**."

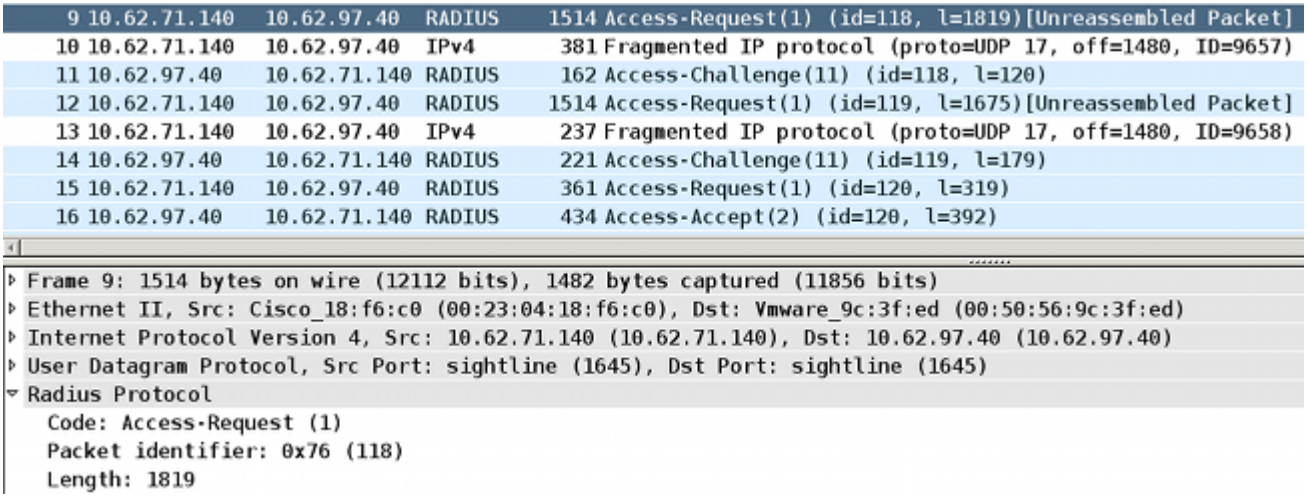
L'ultima frase descrive una caratteristica molto importante dei server AAA. Prima di inviare un altro frammento EAP, devono attendere l'ACK. Una regola simile viene utilizzata per il supplicant:

"Il peer EAP DEVE attendere di ricevere la richiesta EAP prima di inviare un altro frammento."

Frammentazione nel layer IP

La frammentazione può avvenire solo tra il dispositivo di accesso alla rete (NAD) e il server AAA (IP/UDP/RADIUS usato come trasporto).

Questa situazione si verifica quando NAD (switch Cisco IOS) tenta di inviare la richiesta RADIUS contenente il payload EAP, che è più grande della MTU dell'interfaccia:

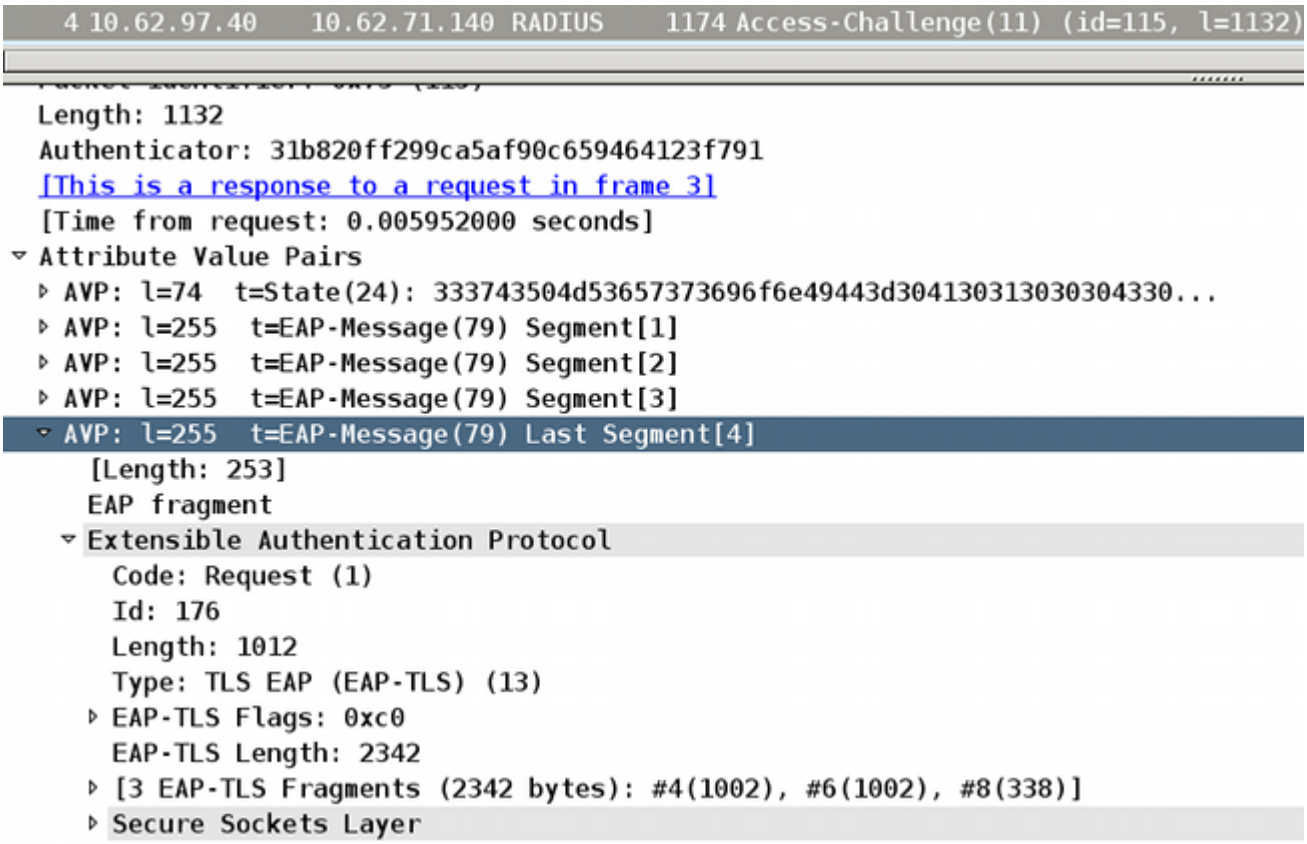


La maggior parte delle versioni di Cisco IOS non è sufficientemente intelligente e non cerca di assemblare i pacchetti EAP ricevuti tramite EAPoL e di combinarli in un pacchetto RADIUS che può essere contenuto nella MTU dell'interfaccia fisica verso il server AAA.

I server AAA sono più intelligenti (come illustrato nelle sezioni seguenti).

Frammentazione in RADIUS

Non si tratta in realtà di una frammentazione. In base alla RFC 2865, un singolo attributo RADIUS può avere fino a 253 byte di dati. Per questo motivo, il payload EAP viene sempre trasmesso in più attributi RADIUS EAP-Message:



Questi attributi EAP-Message sono riassemblati e interpretati da Wireshark (l'attributo "Last Segment" (Ultimo segmento) rivela il payload dell'intero pacchetto EAP).

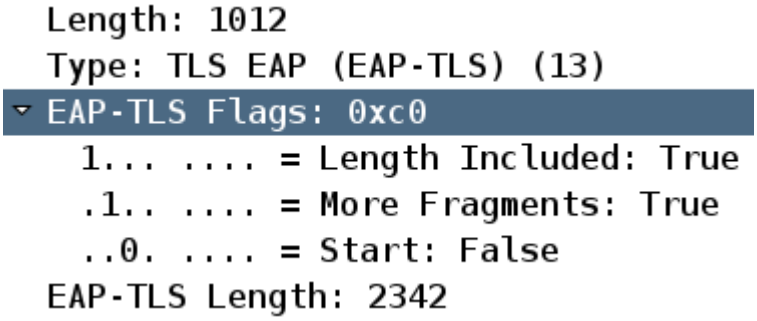
L'intestazione Length nel pacchetto EAP è uguale a 1.012 e per trasportarlo sono necessari quattro AVP RADIUS.

Frammentazione in EAP-TLS

Dalla stessa schermata, potete vedere che:

- La lunghezza del pacchetto EAP è 1.012
- EAP-TLS è lungo 2.342

Ciò suggerisce che si tratta del primo frammento EAP-TLS e il supplicant si aspetta di più, cosa che può essere confermata se si esaminano i flag EAP-TLS:



Questo tipo di frammentazione si verifica più frequentemente in:

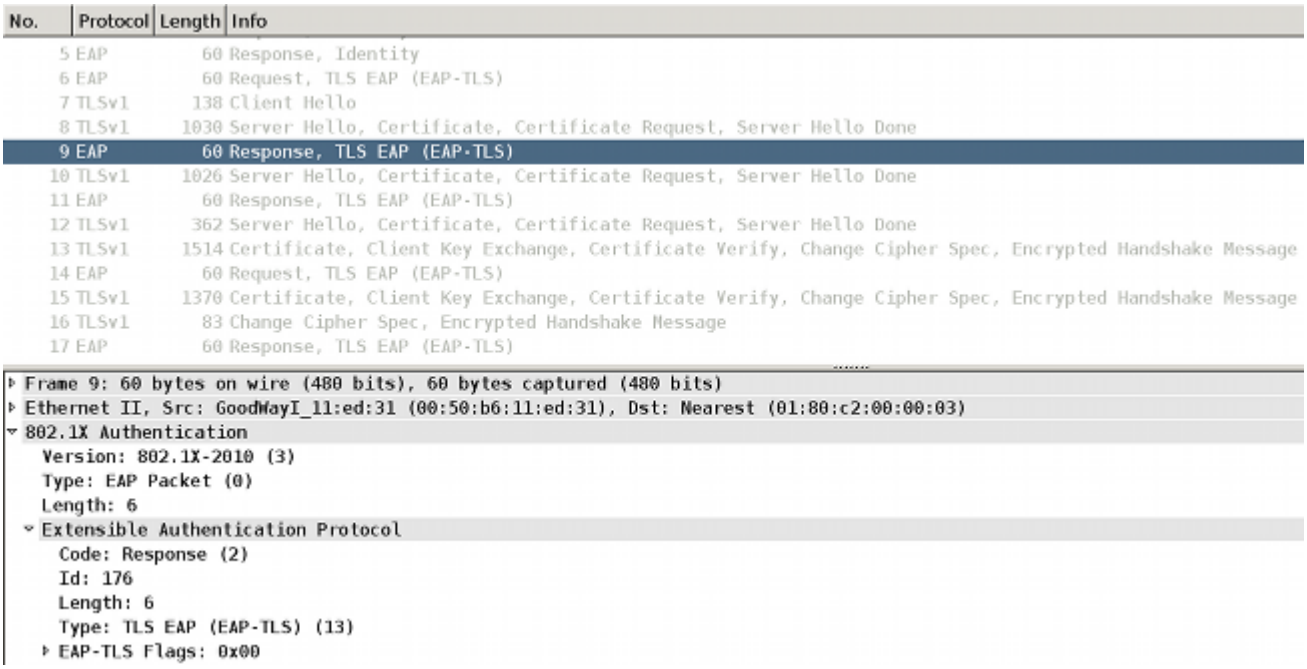
- Richiesta di verifica di accesso RADIUS inviata dal server AAA, che trasmette la richiesta EAP con il certificato server SSL (Secure Sockets Layer) con l'intera catena.

- Richiesta di accesso RADIUS inviata da NAD, che trasporta la risposta EAP con il certificato client SSL con l'intera catena.

Conferma frammentazione EAP-TLS

Come spiegato in precedenza, ogni frammento EAP-TLS deve essere riconosciuto prima dell'invio dei frammenti successivi.

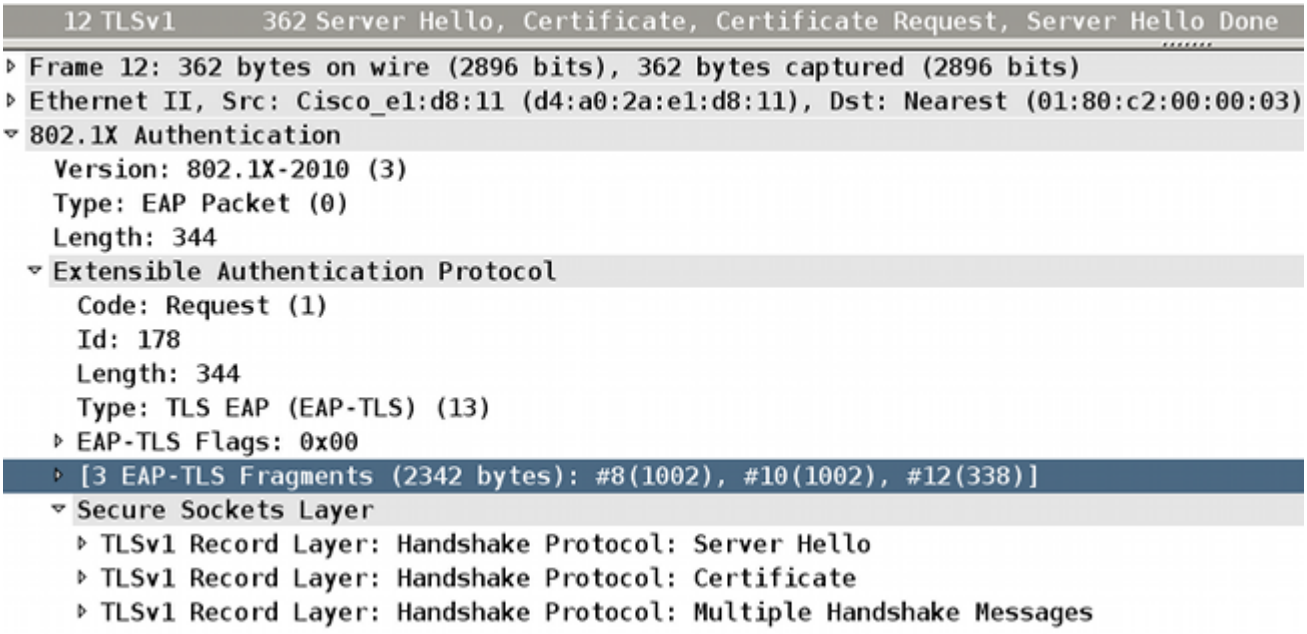
Di seguito è riportato un esempio (il pacchetto viene acquisito per EAPoL tra il supplicant e il NAD):



I frame EAPoL e il server AAA restituiscono il certificato del server:

- Il certificato viene inviato in un frammento EAP-TLS (pacchetto 8).
- Il richiedente riconosce tale frammento (pacchetto 9).
- Il secondo frammento EAP-TLS viene inoltrato da NAD (pacchetto 10).
- Il richiedente riconosce quel frammento (pacchetto 11).
- Il terzo frammento EAP-TLS viene inoltrato da NAD (pacchetto 12).
- Il supplicant non ha bisogno di riconoscere questo; piuttosto, procede con il certificato client che inizia con il pacchetto 13.

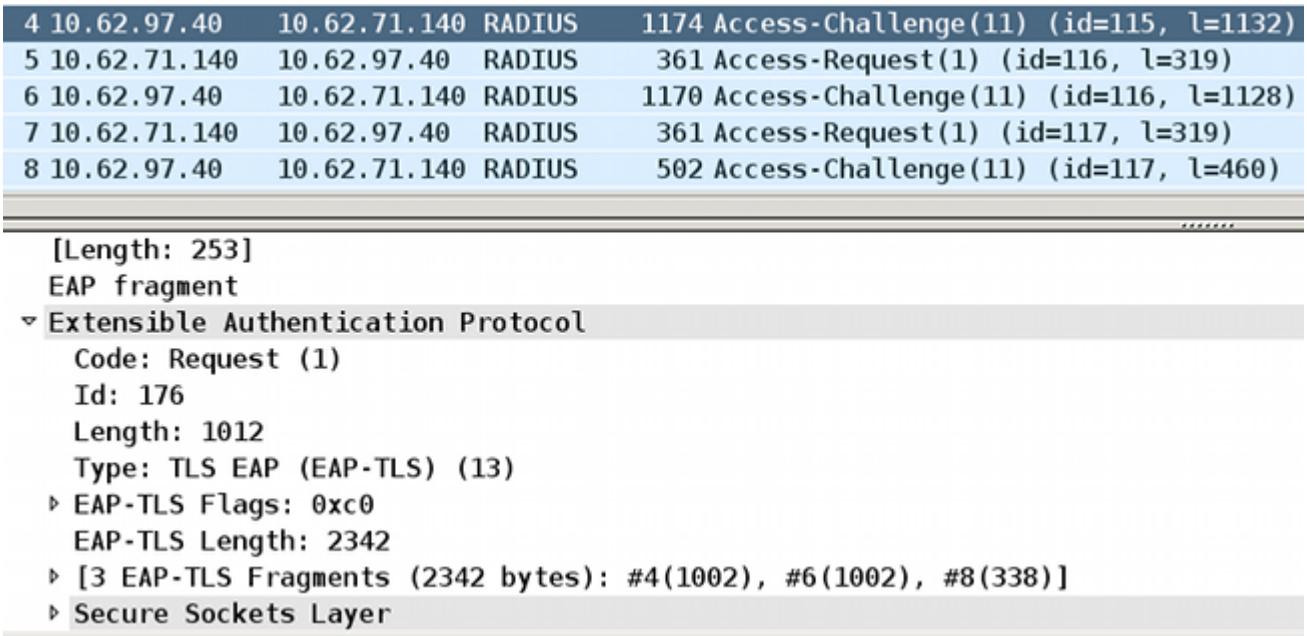
Ecco i dettagli del pacchetto 12:



Potete vedere che Wireshark ha ricomposto i pacchetti 8, 10 e 12.

Le dimensioni dei frammenti EAP sono 1,002, 1,002 e 338, il che porta le dimensioni totali del messaggio EAP-TLS a 2342;

La lunghezza totale del messaggio EAP-TLS viene annunciata in ogni frammento. È possibile verificare questa condizione se si esaminano i pacchetti RADIUS (tra server NAD e AAA):



I pacchetti RADIUS 4, 6 e 8 trasportano questi tre frammenti EAP-TLS. Riconoscimento dei primi due frammenti.

Wireshark è in grado di presentare le informazioni sui frammenti EAP-TLS (dimensioni: 1.002 + 1.002 + 338 = 2.342).

Questo scenario e l'esempio sono stati semplici. Sullo switch Cisco IOS non è stato necessario modificare le dimensioni del frammento EAP-TLS.

Frammenti EAP-TLS riassemblati con dimensioni diverse

Considerare cosa succede quando l'MTU NAD verso il server AAA è di 9.000 byte (frame jumbo) e il server AAA è anche connesso all'uso dell'interfaccia che supporta i frame jumbo.

La maggior parte dei supplicant tipici sono connessi con l'uso di un collegamento da 1 Gbit con una MTU di 1.500.

In uno scenario di questo tipo, lo switch Cisco IOS esegue l'assemblaggio e il riassemblaggio "asimmetrico" EAP-TLS e modifica le dimensioni dei frammenti EAP-TLS.

Di seguito è riportato un esempio di messaggio EAP di grandi dimensioni inviato dal server AAA (certificato server SSL):

1. Il server AAA deve inviare un messaggio EAP-TLS con un certificato server SSL. Le dimensioni totali del pacchetto EAP sono 3.000. Dopo essere stata incapsulata in RADIUS Access-Challenge/UDP/IP, è ancora inferiore all'MTU dell'interfaccia del server AAA. Viene inviato un singolo pacchetto IP con 12 attributi RADIUS EAP-Message. Non vi è frammentazione IP o EAP-TLS.

2. Lo switch Cisco IOS riceve un pacchetto di questo tipo, lo decapsula e decide che l'EAP deve essere inviato al richiedente tramite EAPoL. Poiché EAPoL non supporta la frammentazione, lo switch deve eseguire la frammentazione EAP-TLS.

3. Lo switch Cisco IOS prepara il primo frammento EAP-TLS che può essere inserito nella MTU dell'interfaccia verso il richiedente (1.500).

4. Questo frammento è confermato dal richiedente.

5. Dopo la ricezione dell'avviso, viene inviato un altro frammento EAP-TLS.

6. Questo frammento è confermato dal richiedente.

7. L'ultimo frammento EAP-TLS viene inviato dallo switch.

Questo scenario rivela che:

- In alcune circostanze, il server AND deve creare frammenti EAP-TLS.
- Il NAD è responsabile dell'invio/riconoscimento di questi frammenti.

La stessa situazione può verificarsi per un supplicant connesso tramite un collegamento che supporta i frame jumbo mentre il server AAA ha una MTU inferiore (quindi lo switch Cisco IOS crea frammenti EAP-TLS quando invia il pacchetto EAP al server AAA).

Attributo RADIUS Framed-MTU

Per RADIUS, è presente un attributo Framed-MTU definito nella RFC 2865:

"Questo attributo indica l'unità massima di trasmissione da configurare per l'utente quando non viene negoziata in altro modo (ad esempio PPP). PUÒ essere utilizzato in pacchetti Access-Accept.

PUÒ essere utilizzato in un pacchetto di richiesta di accesso come suggerimento da parte del NAS al server che preferirebbe quel valore, ma il server non è tenuto a rispettare il suggerimento."

ISE non rispetta il suggerimento. Il valore della MTU del frame inviato da NAD nella richiesta di accesso non ha alcun impatto sulla frammentazione eseguita da ISE.

Più switch Cisco IOS moderni non consentono modifiche all'MTU dell'interfaccia Ethernet, a eccezione delle impostazioni dei frame jumbo abilitate a livello globale sullo switch. La configurazione dei frame jumbo influisce sul valore dell'attributo Framed-MTU inviato nella richiesta di accesso RADIUS. Ad esempio, è possibile impostare:

```
<#root>

Switch(config)#

system mtu jumbo 9000
```

In questo modo, lo switch invia Framed-MTU = 9000 in tutte le richieste di accesso RADIUS. Lo stesso vale per l'MTU del sistema senza frame jumbo:

```
<#root>

Switch(config)#

system mtu 1600
```

In questo modo, lo switch invia Framed-MTU = 1600 in tutte le richieste di accesso RADIUS.

I moderni switch Cisco IOS non consentono di ridurre il valore MTU del sistema a meno di 1.500.

Server AAA e comportamento del supplicant quando si inviano frammenti EAP

ISE

ISE cerca sempre di inviare frammenti EAP-TLS (generalmente Server Hello con certificato) lunghi 1.002 byte (anche se l'ultimo frammento è in genere più piccolo).

Non rispetta la MTU Framed-MTU RADIUS. Non è possibile riconfigurarlo per inviare frammenti EAP-TLS più grandi.

Server dei criteri di rete Microsoft

È possibile configurare le dimensioni dei frammenti EAP-TLS se si configura l'attributo Framed-MTU localmente sul Server dei criteri di rete.

Evento sebbene nell'articolo Configurazione delle dimensioni del payload EAP su Server dei criteri di rete Microsoft venga indicato che il valore predefinito di una MTU con frame per il server RADIUS Server dei criteri di rete è 1.500, l'esercitazione di Cisco Technical Assistance Center (TAC) ha mostrato di inviare 2.000 con le impostazioni predefinite (confermate in un centro dati di Microsoft Windows 2012).

Il Server dei criteri di rete rispetta l'impostazione **locale di Framed-MTU** come indicato nella guida precedente e frammenta i messaggi EAP in frammenti di dimensioni impostate in Framed-MTU. Tuttavia, l'attributo Framed-MTU ricevuto nella richiesta di accesso non viene utilizzato (come su ISE/ACS).

L'impostazione di questo valore rappresenta una soluzione valida per risolvere problemi di topologia come i seguenti:

Richiedente [MTU 1500] â€” â€” [MTU 9000]Switch[MTU 9000] â€” [MTU 9000]NPS

Al momento gli switch non consentono di impostare l'MTU per porta; per gli switch 6880, questa funzione è stata aggiunta con l'ID bug Cisco CSCuo26327 - 802.1x EAP-TLS che non funziona sulle porte host FEX.

AnyConnect

AnyConnect invia frammenti EAP-TLS (in genere un certificato client) lunghi 1.486 byte. Per questo valore, il frame Ethernet è di 1.500 byte. L'ultimo frammento è in genere più piccolo.

Supplicant nativo di Microsoft Windows

Microsoft Windows invia frammenti EAP-TLS (in genere certificati client) lunghi 1.486 o 1.482 byte. Per questo valore, il frame Ethernet è di 1.500 byte. L'ultimo frammento è in genere più piccolo.

Informazioni correlate

- **Configurazione dell'autenticazione basata sulla porta IEEE 802.1x**
- **Documentazione e supporto tecnico â€“ Cisco Systems**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).