Comprendere le MTU e la frammentazione RADIUS su 9800 WLC

Sommario

Introduzione

In questo documento viene descritto come configurare l'MTU dei pacchetti RADIUS che il WLC invia al server RADIUS.

Prerequisiti

Requisiti

Cisco raccomanda una conoscenza di base dei seguenti argomenti:

- Configurazione 9800 Wireless LAN Controller (WLC) AAA
- Concetti sul RADIUS AAA (Authentication, Authorization and Accounting)
- Extensible Authentication Protocol EAP
- MTU (Maximum Transmission Unit)

Componenti usati

- Cisco Identity Service Engineer (ISE) 3.2
- Catalyst serie 9800 Wireless Controller (Catalyst 9800-L)
- Cisco IOS® XE 17.15.2
- client wireless Windows 11

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Introduzione

Ai fini di questo documento, il server RADIUS (Remote Authentication Dial-In User Service) utilizzato è Cisco ISE. In primo luogo, viene dimostrato il flusso dei pacchetti senza alcun intervento esterno durante il processo EAP (Extensible Authentication Protocol). Di seguito viene riportata l'opzione di configurazione che consente di modificare le dimensioni della richiesta di accesso inviata dal WLC a qualsiasi server RADIUS. Questa opzione è stata aggiunta in IOS-XE versione 17.11.

9800 RADIUS MTU

In genere, l'MTU dei pacchetti RADIUS non conta, in quanto sono in genere piccoli e non raggiungono comunque l'MTU. Tuttavia, quando un dispositivo deve inviare un certificato, che in genere è di 2-5 KB, deve frammentare il certificato per ottenerlo con la MTU.

Quando il client deve inviare un certificato al server RADIUS, come nel caso di EAP-TLS (Transport Layer Security), il WLC si trova in una situazione in cui il pacchetto deve essere frammentato di nuovo a causa della quantità di dati RADIUS che devono essere inviati con il pacchetto. Fino alle 17.11 l'amministratore di rete aveva poco controllo su questo processo, ma ora ai tecnici è data la possibilità di modificare le dimensioni della richiesta di accesso inviata dal WLC.

Flusso di pacchetti EAP-TLS

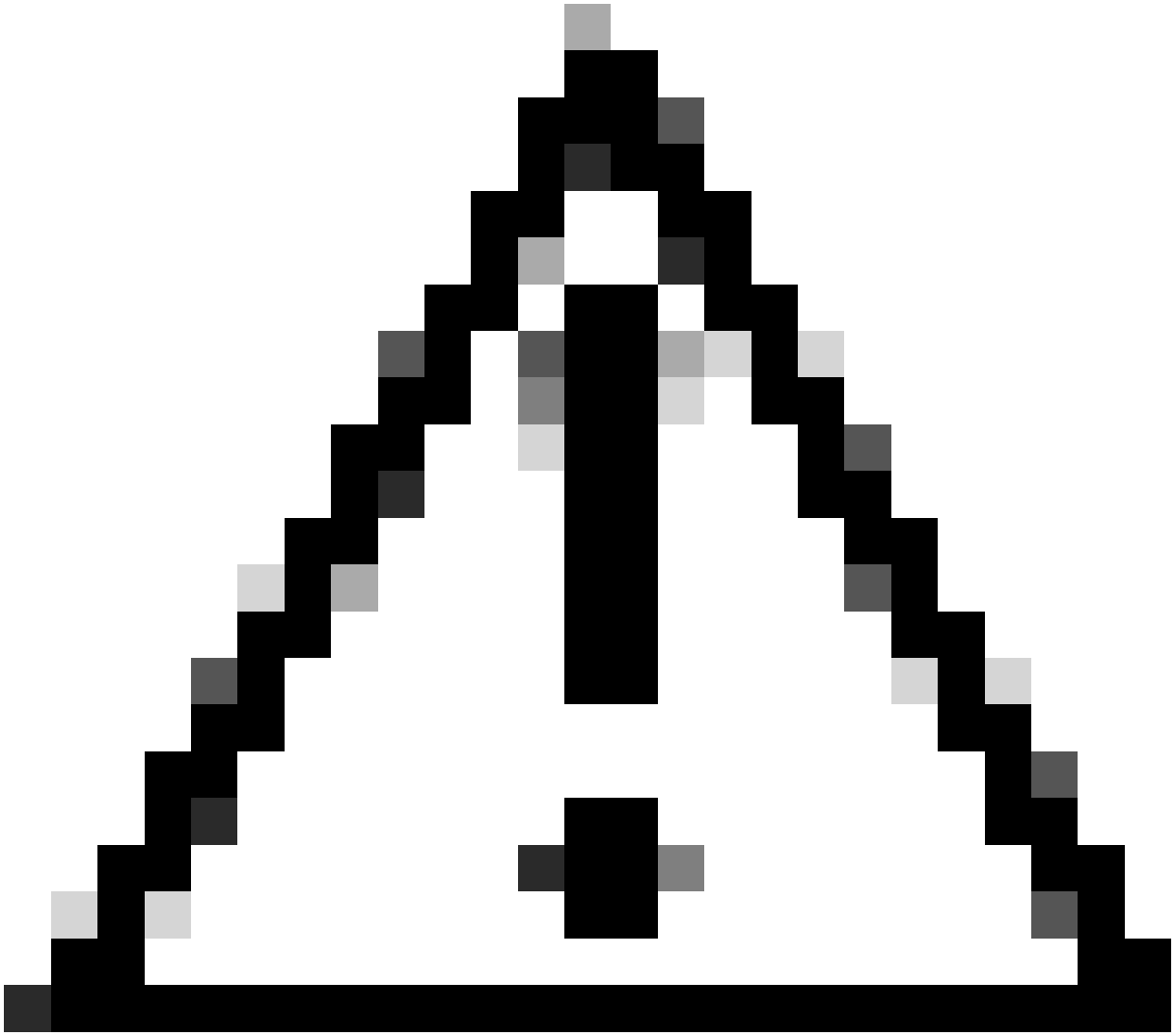
Questa è un'analisi approfondita dell'aspetto dei pacchetti e del modo in cui vengono gestiti dall'infrastruttura wireless. Per comprendere appieno le modifiche introdotte in questo documento, è importante conoscere il flusso dei pacchetti durante il processo di autenticazione wireless

quando si utilizza il dot1x e più specificamente EAP-TLS.

Se si ha già una profonda conoscenza del funzionamento del flusso di pacchetti EAP e RADIUS nell'infrastruttura wireless Cisco, passare alla sezione delle modifiche del comportamento, in cui viene spiegato cosa è stato aggiunto nella versione 17.11, offrendo agli amministratori di rete un maggiore controllo sull'MTU RADIUS. Osservare innanzitutto l'identificazione EAP (EAP-ID).

EAP-ID

L'EAP-ID viene avviato dall'autenticatore, in questo caso il WLC. Questa deve essere la prima parte del processo EAP. A volte il client wireless invia un messaggio di avvio EAPOL. Ciò significa in genere che il client non ha mai ricevuto la richiesta EAP-ID o desidera ricominciare.



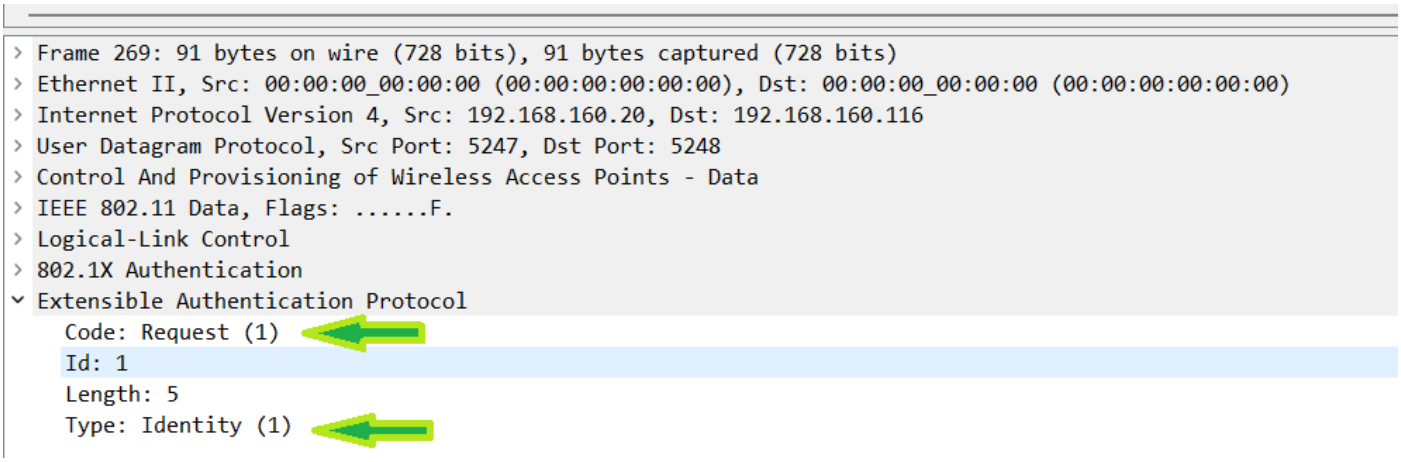
Attenzione: Esiste una differenza tra il pacchetto EAP-ID e l'ID del pacchetto EAP. Il pacchetto EAP-ID viene utilizzato per identificare il richiedente dove l'ID pacchetto EAP è un numero utilizzato per tenere traccia del pacchetto specifico mentre si sposta attraverso la rete.

Richiesta EAP-ID

Innanzitutto, il dispositivo client wireless si connette alla rete utilizzando il normale processo di associazione. Quando la rete WLAN (Wireless Local Area Network) è configurata per il punto1x, il WLC deve prima sapere chi è il client prima di poter richiedere l'accesso dal server RADIUS. Per trovare queste informazioni, il WLC invia il client e la richiesta EAP-ID.

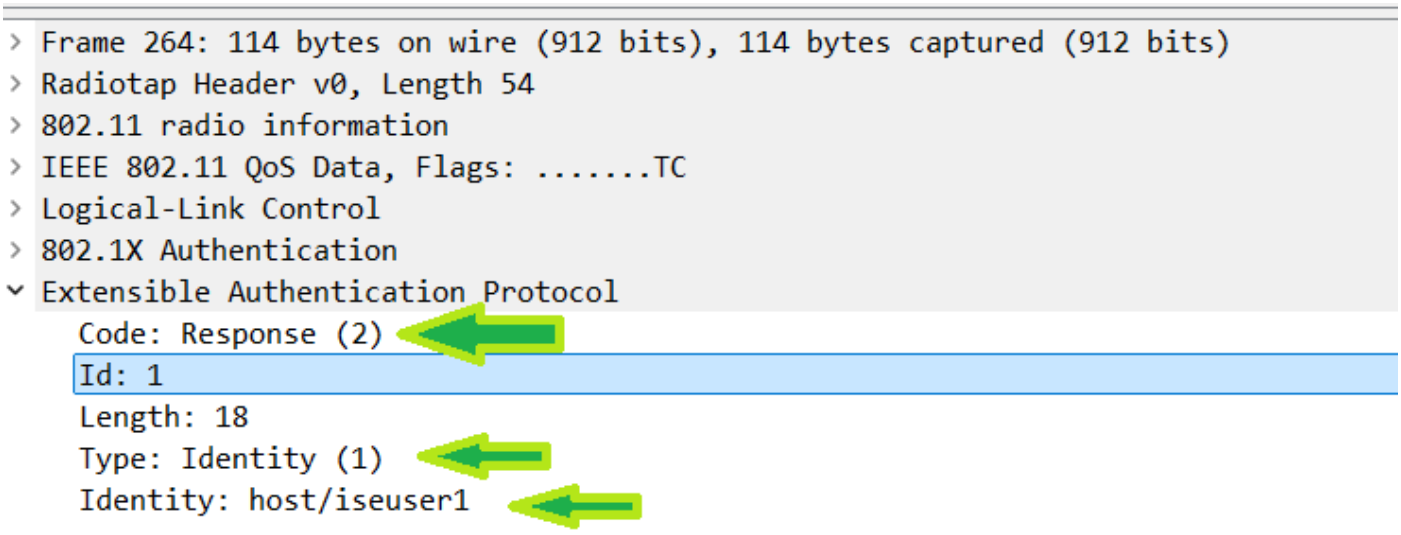
Il client deve rispondere con la risposta EAP-ID. Questo fornisce al WLC ciò di cui ha bisogno per creare la richiesta di accesso e inviarla all'ISE. La richiesta EAP-ID si verifica quando al client viene richiesto di inserire il nome utente e la password in una normale autenticazione PEAP.

Tuttavia, questa discussione si basa su EAP-TLS, quindi la risposta EAP-ID qui avrebbe solo l'ID utente. Nella demo, l'ID utente è iseuser1. In questo pacchetto è possibile vedere la richiesta EAP-ID inviata dal WLC al client wireless per chiedere chi sono. Poiché si tratta di un client wireless, il WLC incapsula la richiesta in CAPWAP e la invia al punto di accesso (AP) per essere inviata via etere. Nei dati EAP, il codice 1 indica che si tratta di una richiesta e il tipo 1 indica che si tratta di una richiesta per l'identità.



Risposta EAP-ID

Successivamente, si prevede che il client wireless risponda con la risposta EAP-ID. Nei dati EAP il codice è stato modificato in 2, a indicare che si tratta di una risposta, ma il tipo rimane 1, a indicare che si tratta dell'identità. Qui è anche possibile visualizzare il nome utente utilizzato dal client. Un'altra cosa da controllare su questi pacchetti è il numero ID del pacchetto EAP. Per lo scambio EAP-ID è sempre 1, ma questo numero cambierà in seguito in qualcos'altro una volta che ISE sarà coinvolto.



Entrambi i pacchetti sono piuttosto piccoli, quindi l'MTU non è rilevante in questo caso in quanto è inferiore ai 1500 byte utilizzati nella rete.

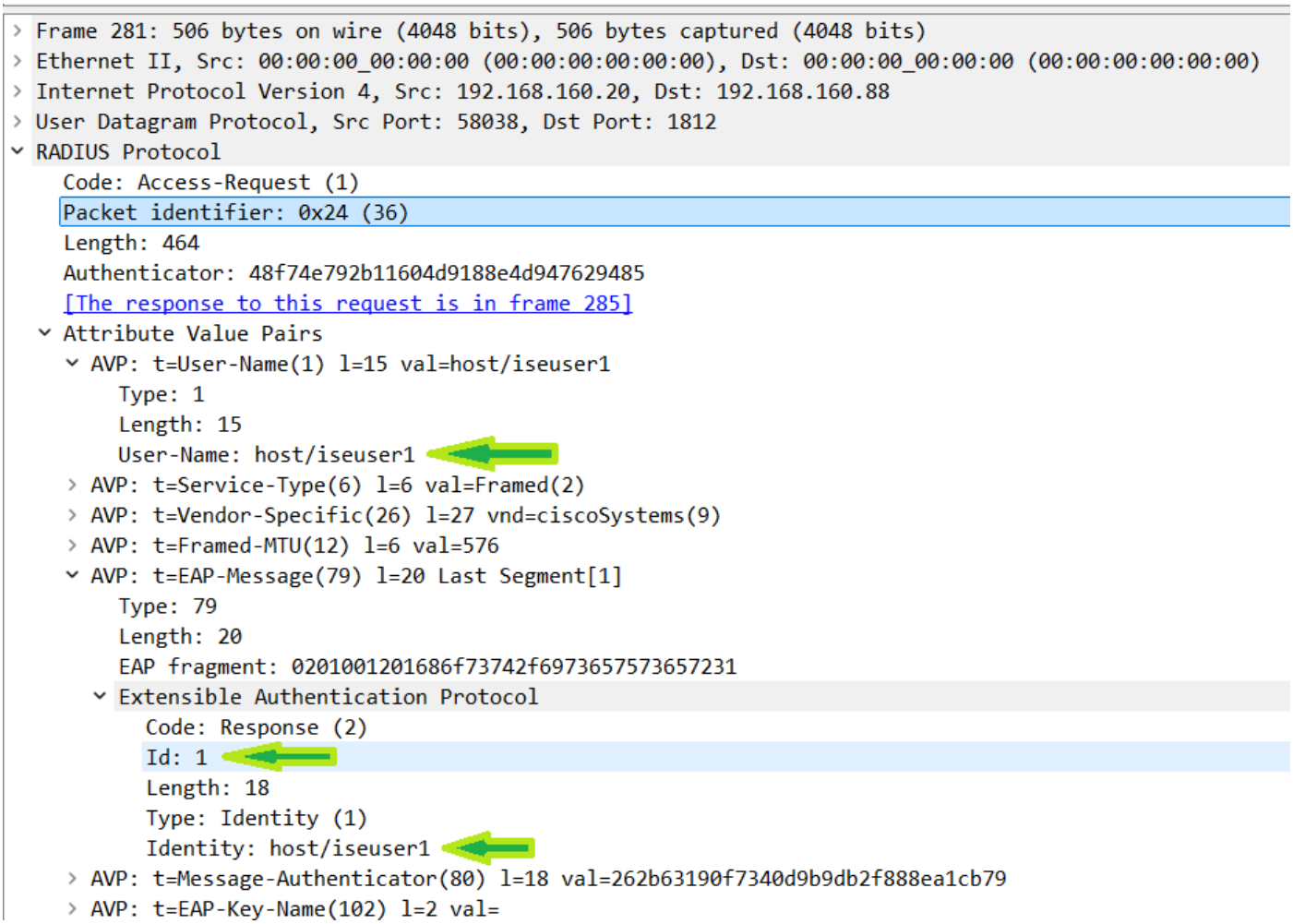
Access-Request e Access-Challenge

La comunicazione con il client è EAP e la comunicazione tra il WLC e ISE è RADIUS. Per la comunicazione RADIUS vengono utilizzati i pacchetti access-request e access-challenge. Il WLC riceve il pacchetto EAP dal supplicant e lo inoltra all'ISE utilizzando la richiesta di accesso RADIUS. In una rete funzionante, ISE risponderebbe con un errore di accesso.

Access-Request

Ora che il WLC conosce l'identità del client, deve chiedere al server RADIUS se il client è autorizzato sulla rete. A tale scopo, il WLC richiede l'accesso per il client inviando il pacchetto di richiesta di accesso. Il WLC invierà altri dati insieme ai dati EAP. Nell'insieme, questi dati vengono definiti coppie di valori attributo, AVP o AV a seconda di chi parla.

Il presente documento non andrà a fondo degli AVP in quanto ciò esula dall'ambito di questa discussione. Qui è sufficiente verificare che il nome utente (dati EAP) sia incluso e inviato al server RADIUS, che in questo caso è ISE. Inoltre, è possibile notare che anche il numero EAP-ID 1 viene inviato ad ISE. Ricordate che quando avete visto l'ID del pacchetto EAP durante la trasmissione, era 1 anche lì. L'ultima cosa importante da notare è che dal momento che il WLC ha aggiunto tutti questi AVP, il pacchetto da 114 byte inviato dal client viene ora trasformato in un pacchetto da 488 byte prima di essere inviato all'ISE.

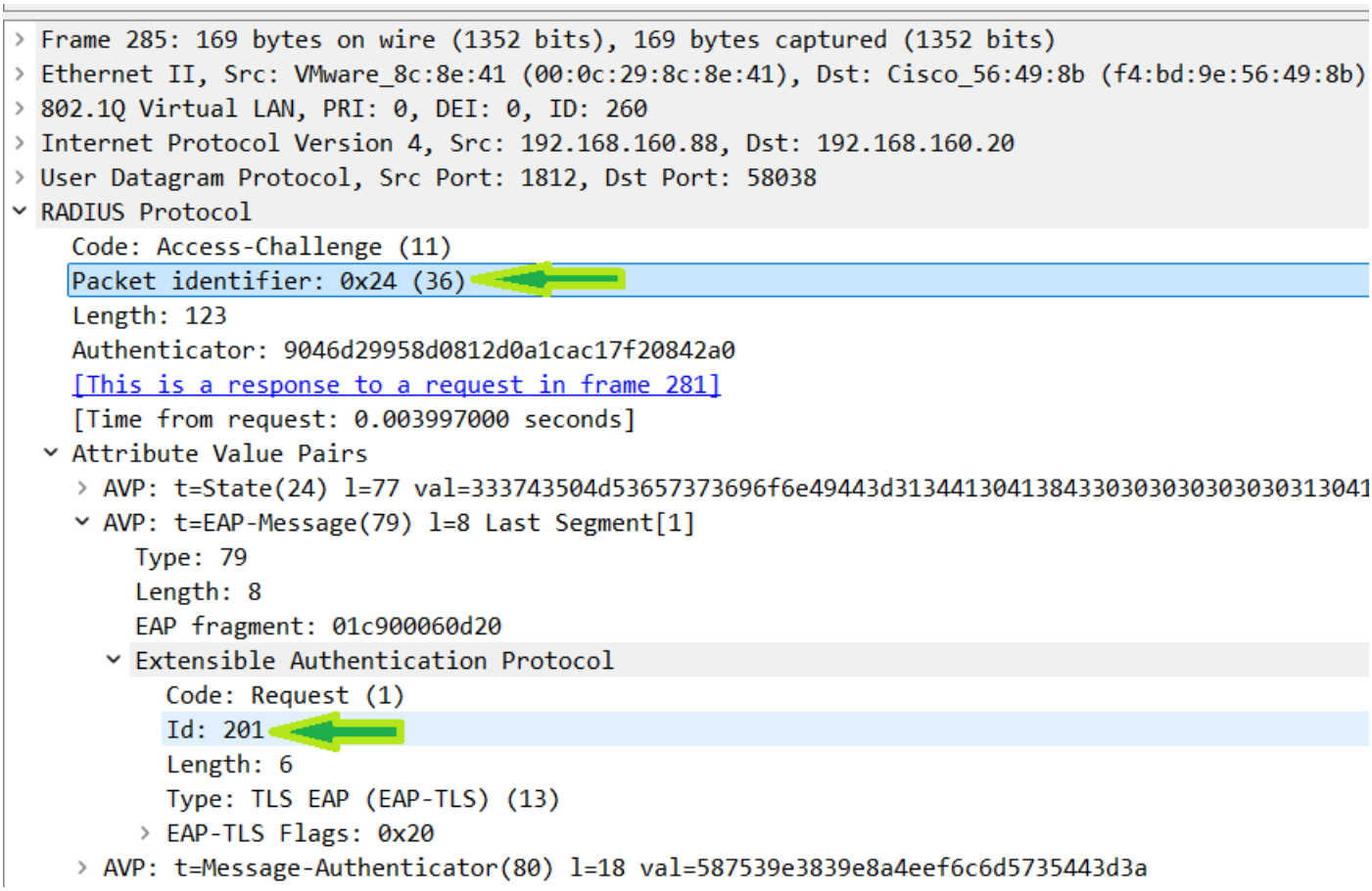


Access-Challenge

Supponendo che ISE riceva la richiesta di accesso e decida di rispondervi, si prevede che la risposta verrà interpretata come una richiesta di accesso da ISE. Guardando indietro alla richiesta di accesso, si vedrebbe l'ID pacchetto RADIUS 36 prima dell'avvio degli AVP.

Quando il WLC riceve la richiesta di accesso, l'ID RADIUS deve corrispondere all'ID pacchetto della richiesta di accesso. L'ID pacchetto RADIUS è destinato alla comunicazione RADIUS tra ISE e WLC. Inoltre, è possibile notare che ISE ha impostato un nuovo ID EAP di 201, che viene utilizzato per seguire la comunicazione tra ISE e il client. A questo punto, il WLC è solo un pass-through per la comunicazione tra ISE e il client.

È importante annotare tutti questi ID di pacchetto qui in modo da comprendere il flusso di comunicazione e come tracciare questi pacchetti attraverso la rete. In un ambiente di produzione in genere vengono eseguite più autenticazioni contemporaneamente. Usare il comando calling-station-id per far corrispondere il pacchetto all'indirizzo MAC del client. È quindi possibile utilizzare l'ID pacchetto RADIUS e l'ID pacchetto EAP per tenere traccia del flusso di pacchetto per il client specifico. Fino a questo momento, nessuna delle due parti ha inviato alcun certificato, quindi non c'è stato bisogno di preoccuparsi per l'MTU.



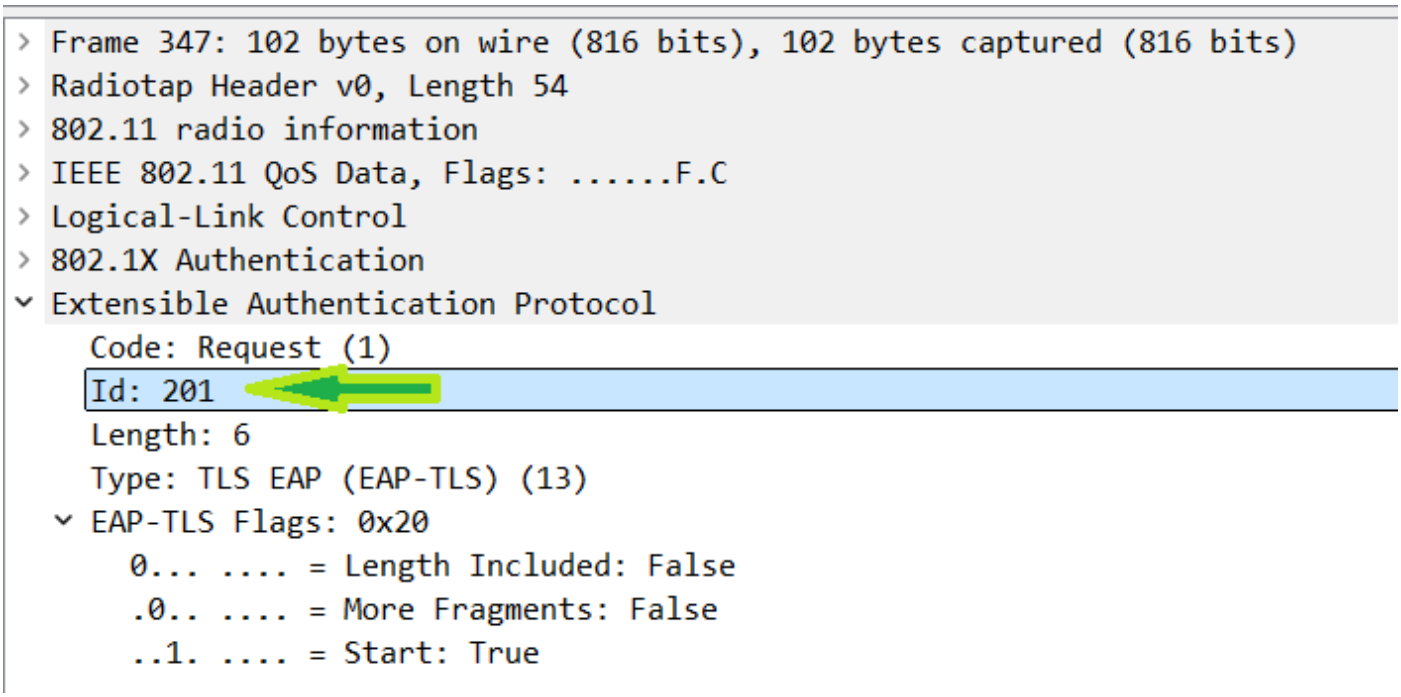
Richiesta EAP e risposta EAP

Solo un promemoria: il client parla EAP e non RADIUS. Ciò detto, quando il WLC riceve la richiesta di accesso, deve rimuovere i dati RADIUS ed estrarre la richiesta EAP in modo che possa essere inviata al client.

Richiesta EAP

Questa operazione deve essere esattamente come è stata eseguita all'interno della richiesta di accesso quando il WLC l'ha ricevuta. Tuttavia, tutto il materiale RADIUS è stato rimosso e solo la parte EAP viene inviata al client.

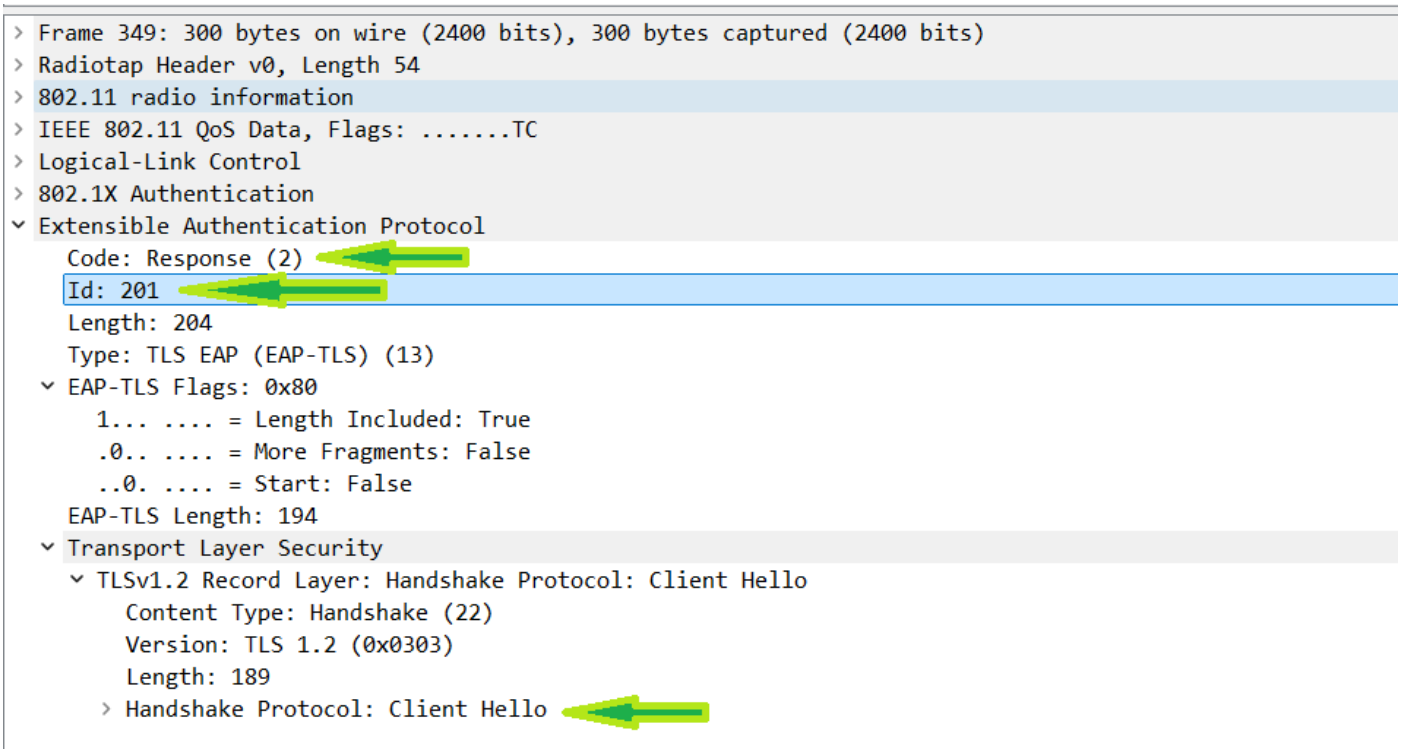
Potete ancora vedere qui l'ID pacchetto EAP del 201 così come era nella richiesta di accesso perché sono gli stessi dati che il WLC ha ricevuto da ISE. Il flusso è lo stesso dell'EAP-ID, ma ora non proviene dal WLC ed è utilizzato per stabilire il metodo EAP. Questo pacchetto è ancora piuttosto piccolo perché serve solo per stabilire l'inizio di una sessione EAP-TLS.



Risposta EAP

Quando il client riceve la richiesta EAP, deve rispondere con una risposta EAP. Nel modulo EAP-Response il client inizia a stabilire la sessione TLS. Il risultato è simile a quello ottenuto in qualsiasi altra situazione in cui viene utilizzato TLS. Comincia con il messaggio di "saluto del cliente". Questo documento non approfondirà ciò che entra nell'hello del cliente, in quanto è irrilevante per questo argomento. È sufficiente notare che è in corso la configurazione di una sessione TLS.

Qui potete vedere i dati nei pacchetti come fareste con qualsiasi altra configurazione TLS. Come per la risposta EAP-ID, questo pacchetto colpisce il WLC e viene convertito in una richiesta di accesso. ISE risponde con una richiesta EAP inserita in un pacchetto di richiesta di accesso. Questo continua ad essere il flusso d'ora in avanti.



Certificati TLS

Qui è il punto in cui si sta per vedere l'aumento delle dimensioni del pacchetto. Le dimensioni dei certificati dipendono dalla presenza di una o più Autorità di certificazione (CA) intermedie. Se si tratta di un certificato autofirmato, sarà ovviamente più piccolo di un certificato con un certificato di dispositivo concatenato a due CA intermedie e una CA radice. In entrambi i casi, in genere il proprietario del certificato inizia a frammentare i propri pacchetti qui.

Certificato ISE

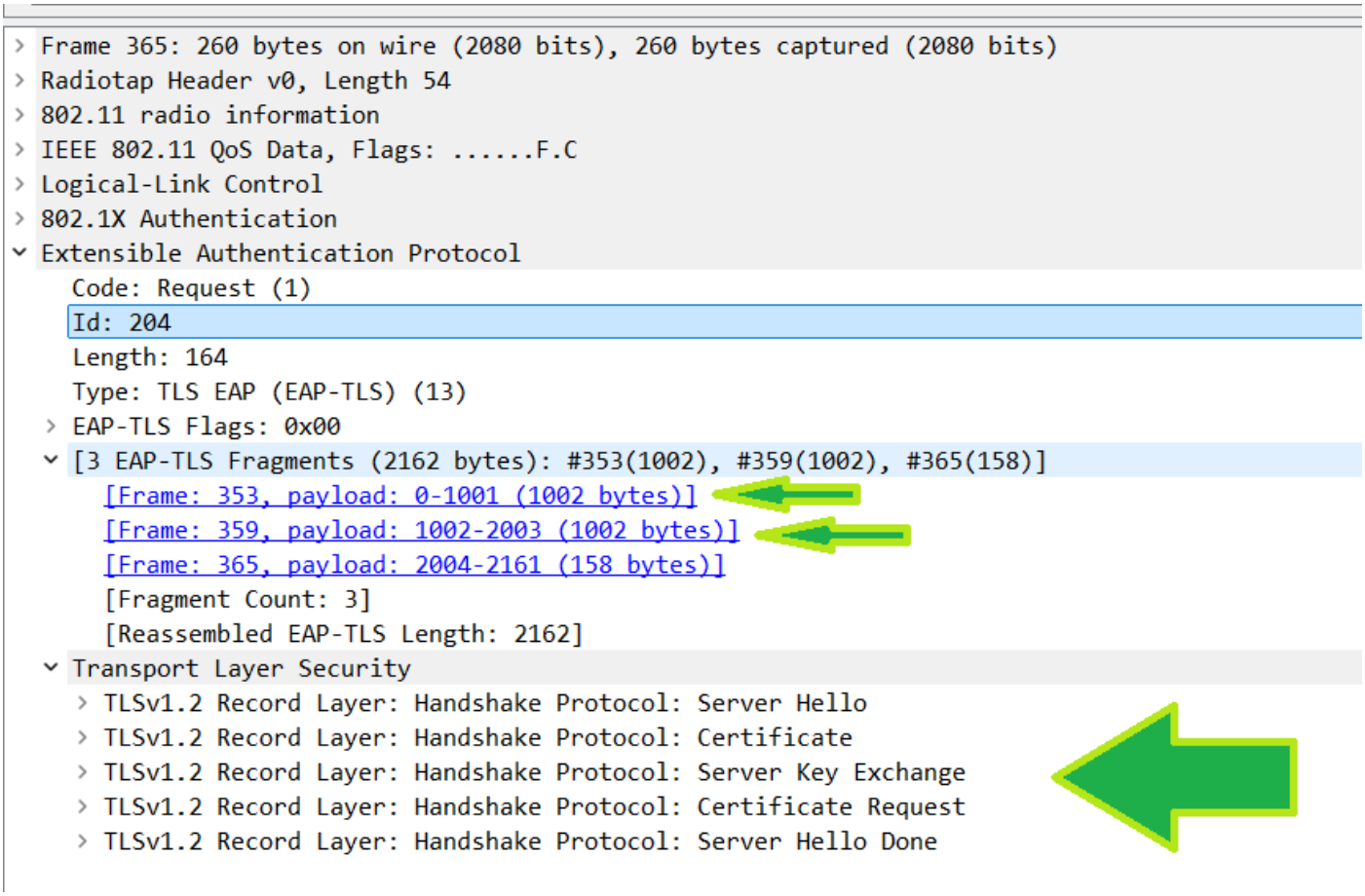
Ora che ISE ha ricevuto il saluto del client TLS, risponde con un'altra richiesta EAP. In questa nuova richiesta EAP, ISE invia contemporaneamente il messaggio di saluto del server, il relativo certificato, lo "scambio di chiavi server", la "richiesta di certificato" e i messaggi di saluto del server. Se inviasse tutto questo in un pacchetto, il pacchetto supererebbe l'MTU della rete. L'ISE frammenta il pacchetto stesso per farlo scendere sotto l'MTU. Con ISE, frammenta la parte dati del pacchetto in modo che non sia più grande di 1002 byte, nella speranza di evitare la doppia frammentazione.

Cosa si intende per doppia frammentazione? La prima frammentazione si sta verificando ad ISE perché i dati che si desidera inviare sono troppo grandi per essere contenuti nella MTU della rete. Tuttavia, ci possono essere altri luoghi nella rete in cui, anche se l'MTU è la stessa, a causa di come la rete è configurata, un dispositivo potrebbe avere bisogno di frammentare il pacchetto per aggiungere le proprie intestazioni e rimanere sotto l'MTU. Ciò può essere vero anche se il bit non frammentare è controllato.

Un buon esempio a riguardo è con un tunnel VPN, o un tunnel qualsiasi. Per inserire i dati in un tunnel VPN, i router VPN devono aggiungere le proprie intestazioni al traffico. Se il traffico RADIUS fosse frammentato all'MTU o in prossimità della MTU, quando si tratta di questa VPN non

sarebbe possibile mantenere i dati all'interno dell'MTU e aggiungere altre intestazioni. Ciò è vero anche per i tunnel CAPWAP che potete vedere un po' più tardi.

Per evitare che questi pacchetti vengano frammentati da un altro dispositivo, ISE frammenta il pacchetto in un punto in cui può essere evitato nella maggior parte delle reti. Ciò significa che ISE invia questi dati in più richieste EAP in attesa ogni volta di una risposta EAP vuota. L'ID EAP aumenta a ogni frammento inviato. Dal punto di vista del WLC, questo implicherebbe una richiesta di accesso e uno scambio di richieste di accesso per ciascun frammento, e l'ID del pacchetto RADIUS aumenterebbe con ciascun frammento inviato.



Certificato client

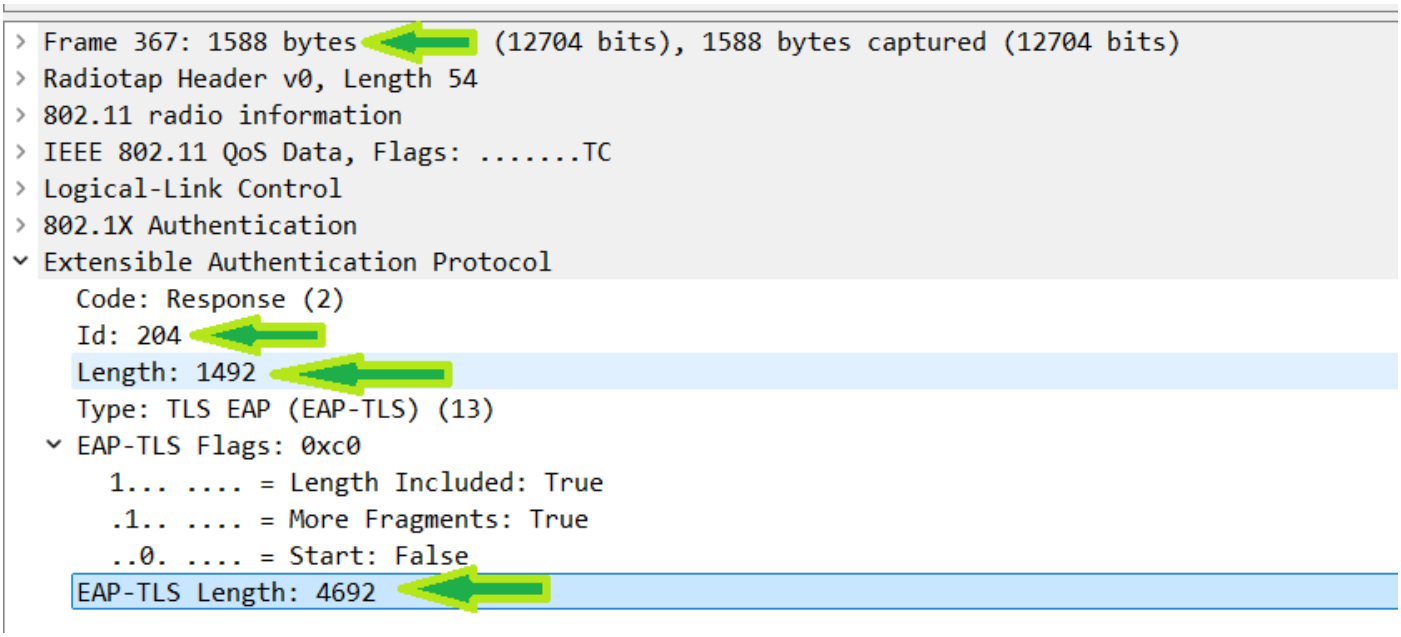
Una volta che ISE ha inviato tutti i frammenti e questi sono ricomposti dal client, il flusso del pacchetto si sposta verso il client per inviare qualcosa. In TLS è previsto che il client invii il proprio certificato a questo punto per completare l'autenticazione. È qui che le cose diventano più complesse. Come ISE, il client invierà più parti TLS contemporaneamente, di cui una è il certificato.

A differenza di quanto visto con ISE, la maggior parte dei client invia i dati EAP appena al di sotto dell'MTU. In questa demo, i dati 802.1x sono 1492. Il problema è che l'access point deve aggiungere le intestazioni CAPWAP in modo da poter essere inviato al WLC.

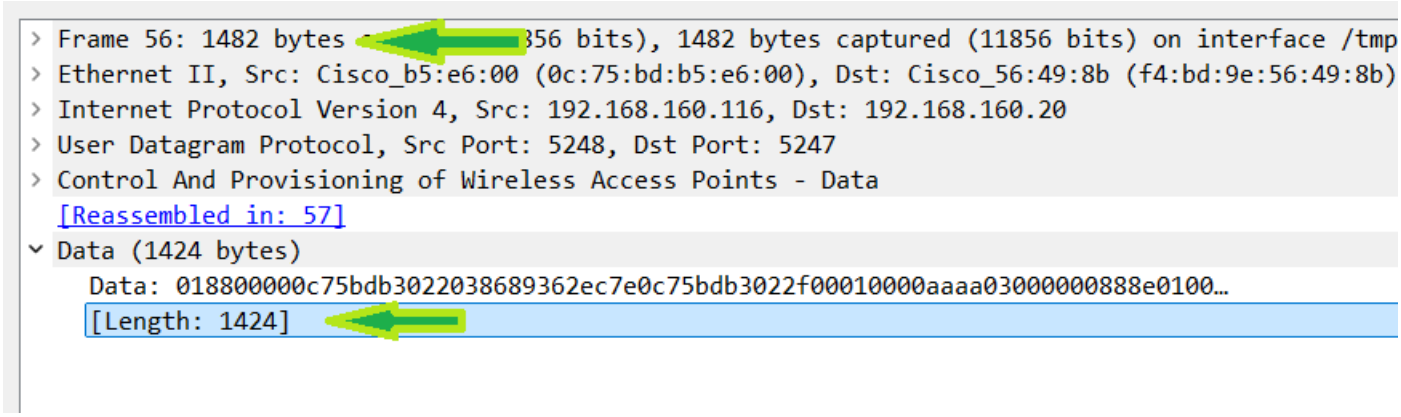
Come si può fare? L'access point dovrà frammentare il pacchetto in modo da poter aggiungere le intestazioni e inviarlo al WLC. L'access point non può ottenere il pacchetto al WLC senza

frammentarlo. Detto questo, il pacchetto viene frammentato due volte, prima dal client, poi di nuovo dall'access point. Tuttavia, questa frammentazione non è in genere un problema, come è previsto con CAPWAP.

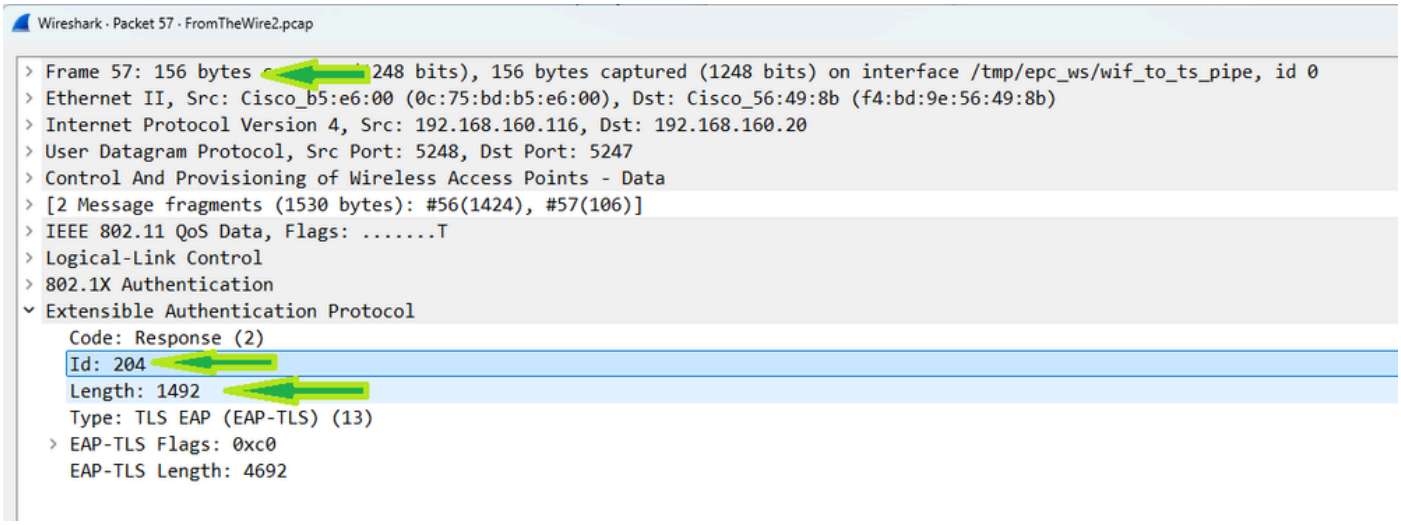
Il pacchetto via etere:



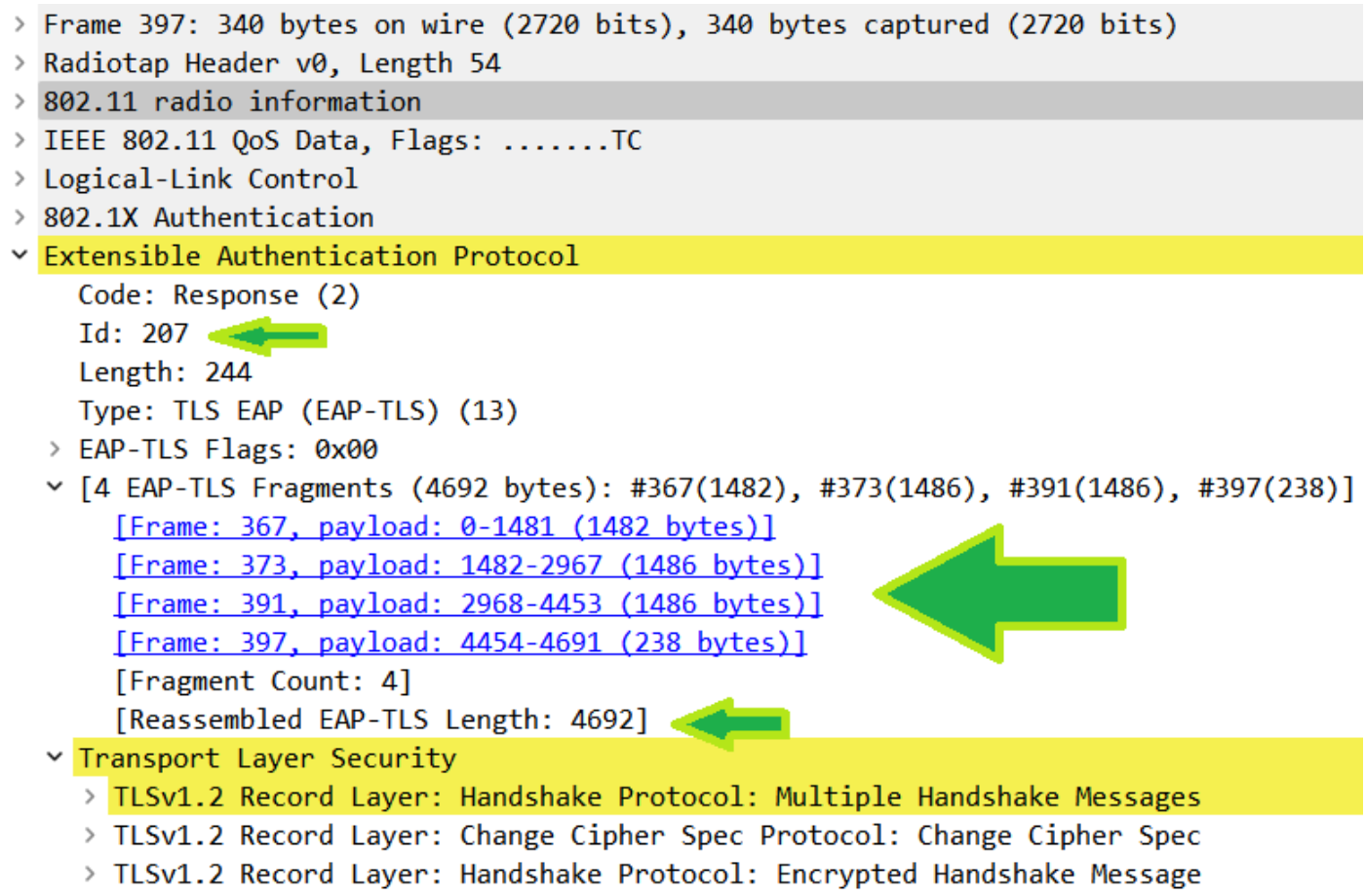
Il frammento di pacchetto sul cavo:



Il pacchetto è stato ricomposto sul cavo:



Tutti i frammenti dei client sono stati ricomposti via etere:



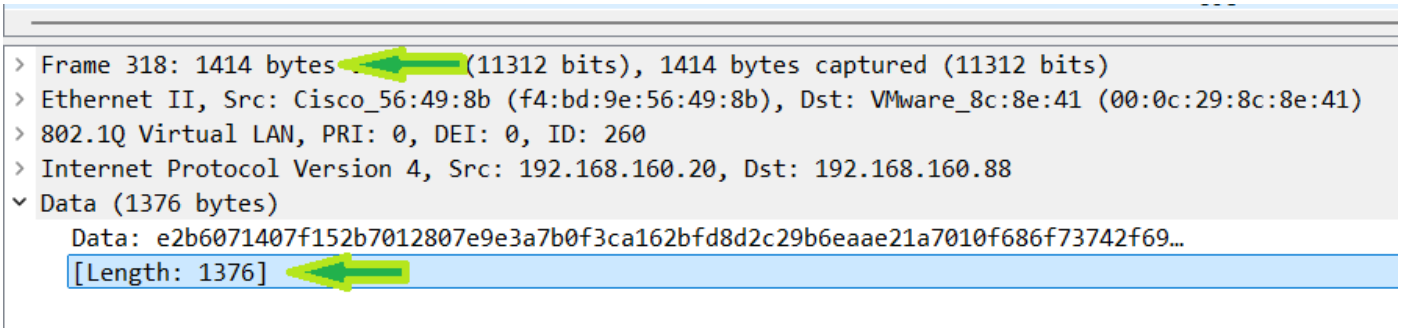
Certificato client sul WLC

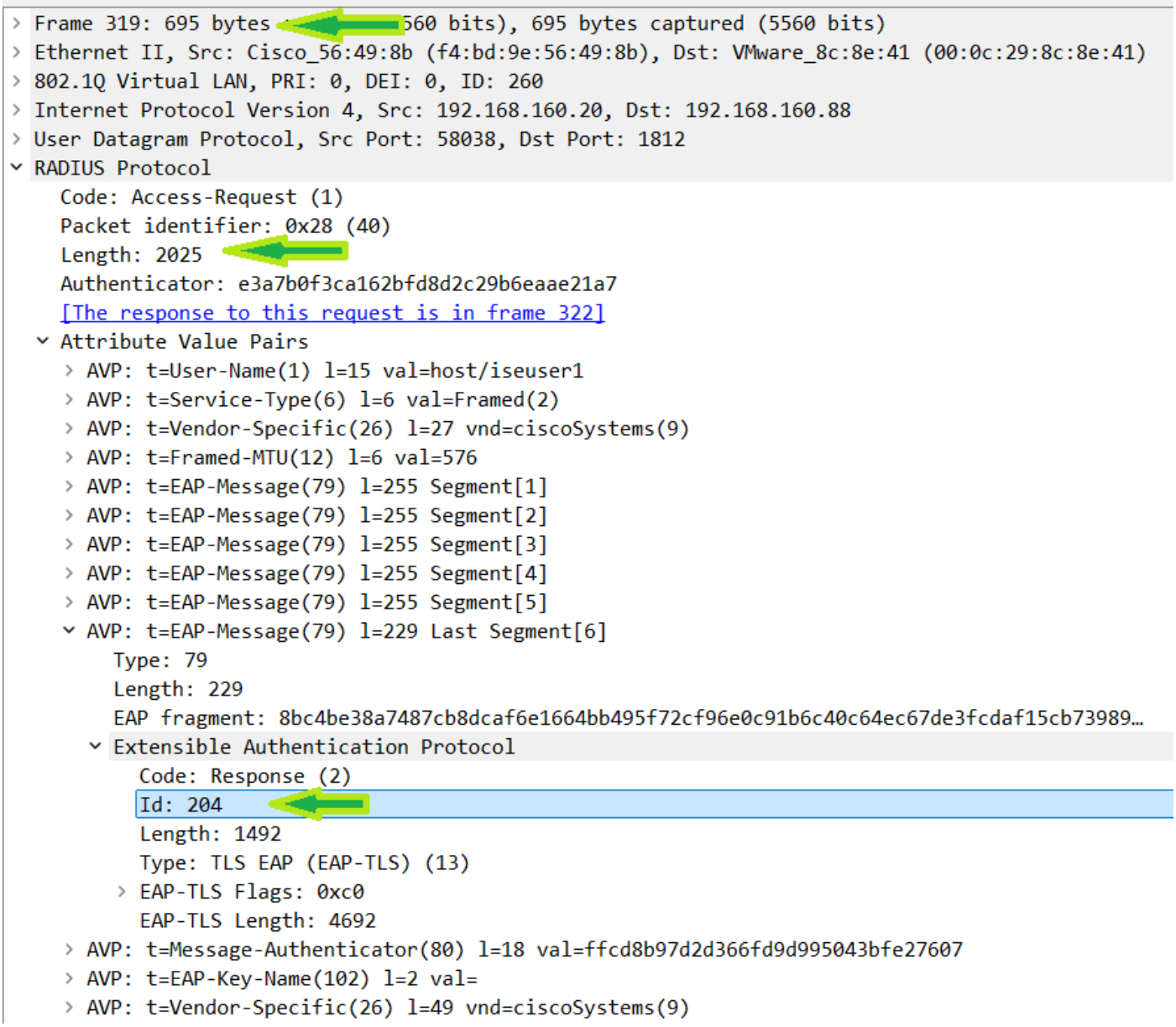
Il WLC riceve i due frammenti CAPWAP e li ricompone in modo che abbiano l'intero pacchetto da 1492 byte dal client, ripristinando il pacchetto, ma non per un periodo di tempo prolungato. Questo ripristino ha vita breve perché, se si guarda indietro al modo in cui il WLC invia la richiesta di accesso, è necessario ricordare che deve aggiungere circa 400 byte di AVP RADIUS al pacchetto prima di poter inviare i dati ad ISE.

Per una semplice analisi matematica, si supponga che il WLC aggiunga 408 byte portando le dimensioni totali del pacchetto a 1900. Questa MTU supera di gran lunga i 1500 MTU, quindi cosa farà il WLC? Frammentare di nuovo il pacchetto.

A questo punto, il WLC frammenterà il pacchetto a 1396 per impostazione predefinita. In questo caso, l'opinione prevalente è la stessa di ISE. La speranza è di rendere il pacchetto sufficientemente piccolo in modo che, se deve passare attraverso un altro tunnel, non debba essere frammentato di nuovo per aggiungere le intestazioni. Tuttavia, il WLC non è così cauto come ISE, quindi 1396 è abbastanza buono qui.

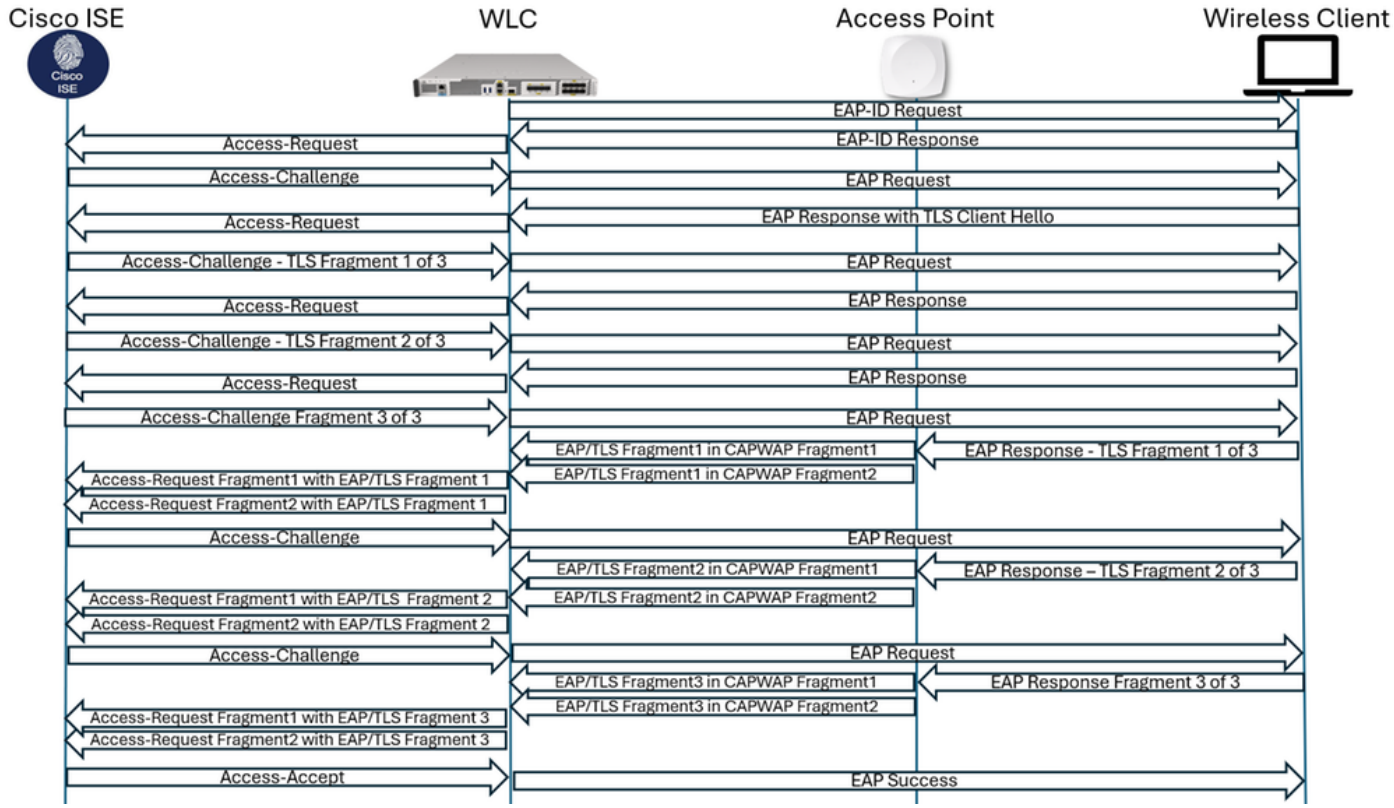
Il pacchetto frammentato in uscita dal WLC:





Packet Flow TL;DR

Quando ISE invia il proprio certificato, frammenta i pacchetti TLS a 1002 byte. Nessun problema. Quando i client inviano il proprio certificato, in genere si frammentano vicino all'MTU. Poiché l'access point deve aggiungere le intestazioni CAPWAP al pacchetto, deve frammentare anche questo pacchetto. Dopo aver ricevuto i frammenti, il WLC deve ricomporre il pacchetto e aggiungere gli AVP RADIUS in modo che il pacchetto venga frammentato di nuovo. Il flusso del pacchetto ha un aspetto simile al seguente:



Modifica comportamento MTU RADIUS

Se si controlla il flusso di pacchetti per qualsiasi traffico di dati client wireless, si osserverà che l'infrastruttura wireless ha influenza su di esso solo in alcuni punti. Il primo luogo si ha quando il traffico lascia il punto di accesso e il secondo quando il traffico lascia il WLC. L'eccezione si verifica con il traffico TCP, dove l'infrastruttura wireless può regolare il valore MSS del client. Tuttavia, EAP non rientra nel protocollo TCP, in realtà è il proprio protocollo.

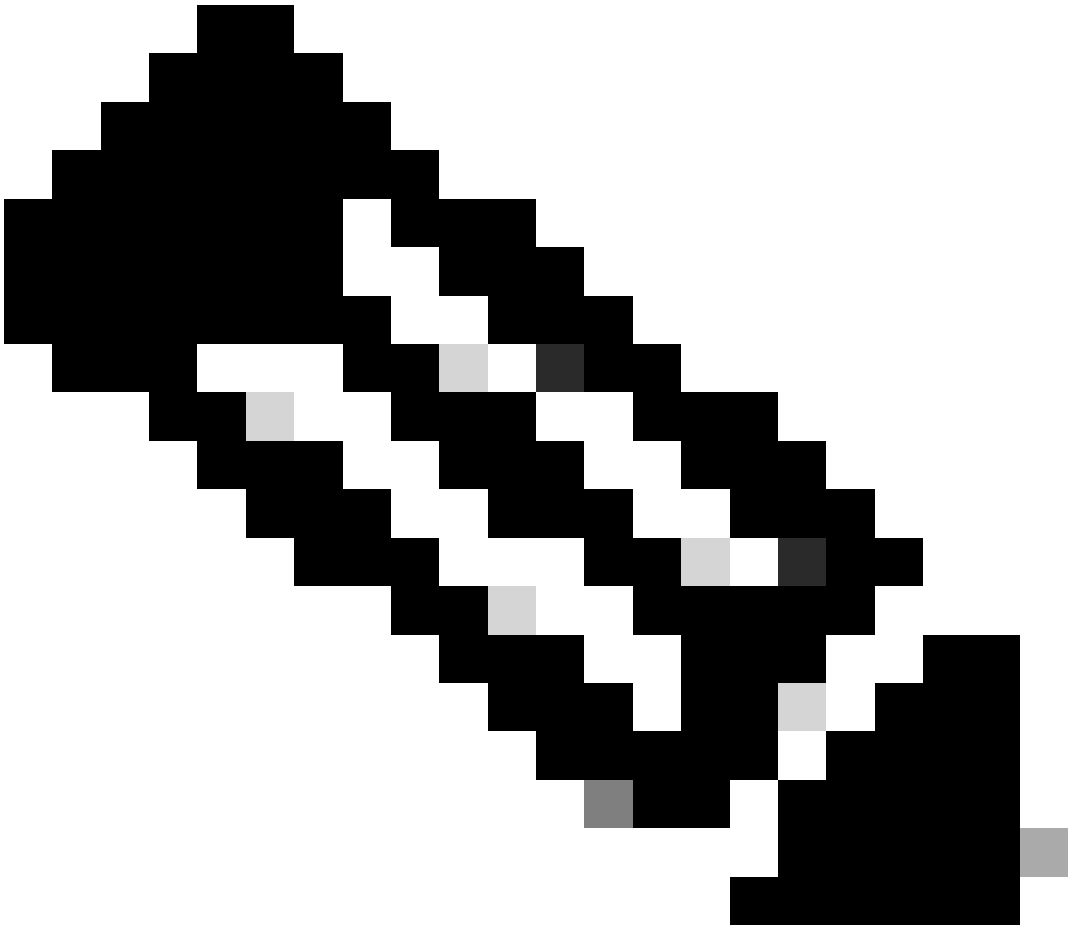
Se si esaminano i flussi di traffico EAP e RADIUS, si osserverà anche che la rete in realtà influenza le dimensioni del traffico sia sul punto di accesso che sul WLC, quando le dimensioni del pacchetto originale si avvicinano troppo all'MTU. Comprendendo correttamente il ruolo del WLC in questo scambio, potete notare che in realtà esiste un solo punto in cui il WLC ha influenza sulle dimensioni del pacchetto RADIUS. Ciò si verifica quando viene ricevuta una risposta EAP e la si modifica in una richiesta di accesso RADIUS.

Elementi modificati

Se la risposta EAP è superiore all'MTU, dopo aver aggiunto gli AVP RADIUS è necessario frammentarla. Poiché è già necessario frammentare il pacchetto in qualsiasi momento, è possibile decidere almeno a quale dimensione frammentarlo. È qui che si inseriscono le modifiche introdotte nella versione 17.11.

Nella richiesta di funzionalità rilevata nell'ID bug Cisco CSCwc81849, si desidera aggiungere il supporto per i pacchetti Jumbo RADIUS. A questo punto, il pacchetto RADIUS non è più frammentato automaticamente a 1396. A questo punto, se si aggiunge il comando ip radius source-interface <interfaccia X>, la richiesta di accesso RADIUS viene inviata all'MTU

dell'interfaccia.



> Nota: Se si utilizza Cisco Catalyst Center, quando si esegue il provisioning delle configurazioni AAA, l'interfaccia di origine viene aggiunta automaticamente al gruppo di server. In questo modo, il comportamento predefinito viene modificato in frammentazione alla dimensione MTU dell'interfaccia usata nel comando.

Come Si Può Utilizzare Questa Modifica?

Poiché l'MTU predefinita di tutte le interfacce è 1500, questa sarebbe la nuova MTU in cui frammentare. L'interfaccia predefinita utilizzata per tutto il traffico RADIUS è WMI (Wireless Management Interface). Quando si controlla la configurazione del gruppo di server, se non è specificata un'interfaccia di origine, il WLC invia il traffico RADIUS a 1396 utilizzando WMI. Tuttavia, se si accede alla configurazione del gruppo di server e si specifica che l'interfaccia di origine è WMI, il WLC invia il traffico RADIUS a 1500, utilizzando ancora WMI.

Ora, supponga che ci sia un dispositivo nella rete come la VPN di cui si è parlato prima. Si

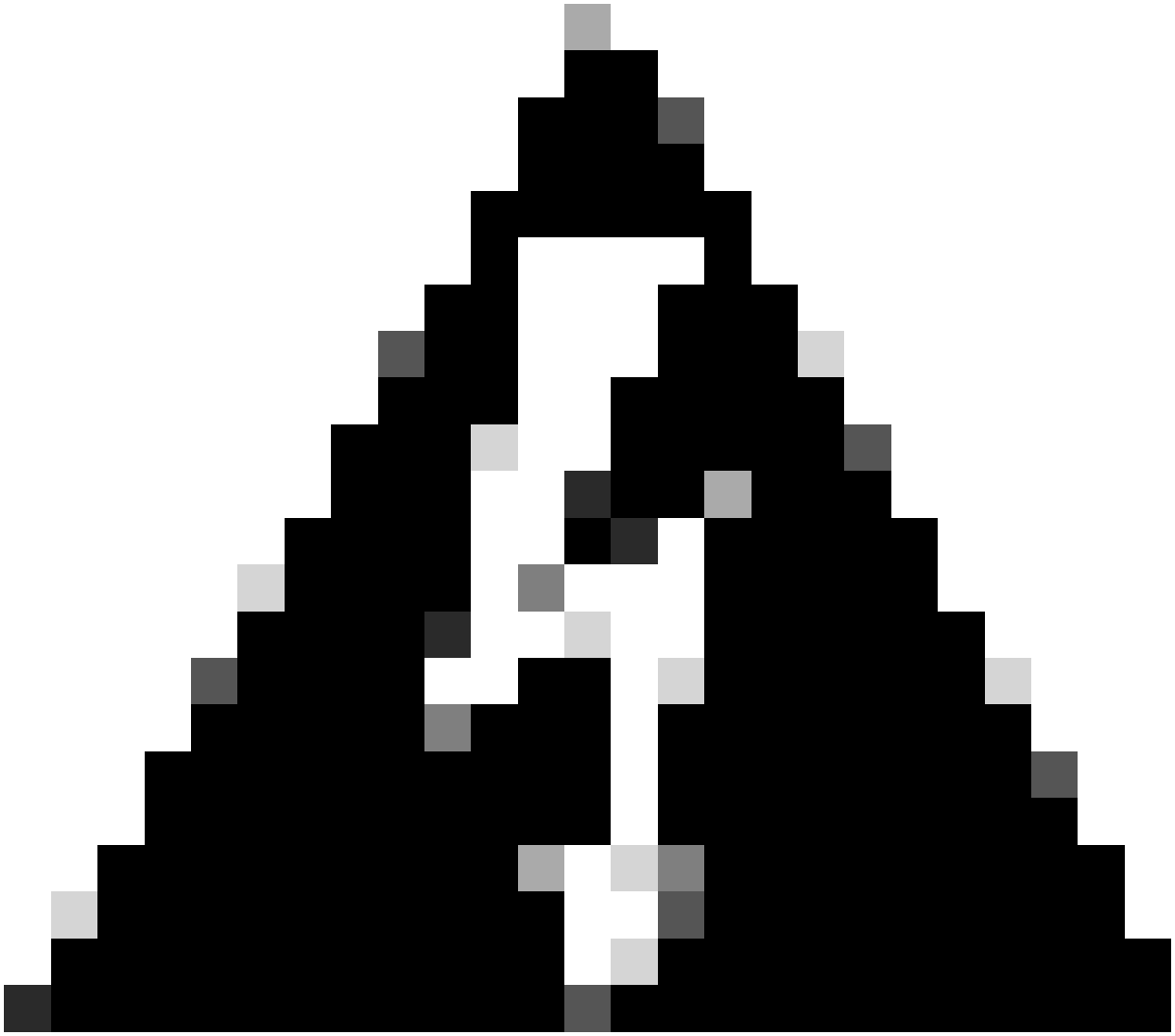
desidera evitare la doppia frammentazione del traffico in modo da poter modificare l'MTU dell'interfaccia in modo da frammentare i pacchetti in un'altra posizione. È possibile modificare l'MTU a qualcosa come 1200 in modo che i pacchetti vengano frammentati sul byte 1200 invece che su 1500.

Avviso: La modifica dell'MTU di WMI influisce su tutto il traffico in entrata e in uscita dall'indirizzo IP di gestione WLC.

Anche se non si desidera modificare la MTU di WMI, lo scopo di specificare un'interfaccia di origine è modificarla passando da WMI a un'altra interfaccia e utilizzarla per il traffico RADIUS, nonché modificare la MTU di tale interfaccia. Poiché questa configurazione viene eseguita a livello di gruppo di server, è possibile specificare il traffico RADIUS su cui si desidera che la modifica venga influenzata.

Questa configurazione non è legata a un server AAA o a una WLAN. È possibile disporre di più gruppi di server con gli stessi server e specificare l'interfaccia di origine solo su uno di essi, se lo si desidera. Questo gruppo di server viene aggiunto a un elenco di metodi e quindi a una WLAN. Ad

esempio, se si desidera apportare la modifica a una sola WLAN, anche se si dispone di un solo server AAA, è possibile creare un nuovo gruppo di server, usare il comando ip radius source-interface che punta all'interfaccia con l'MTU che si desidera usare, aggiungere il server AAA al nuovo gruppo, creare un nuovo elenco di metodi con il nuovo gruppo e quindi aggiungere tale elenco alla WLAN specifica su cui si desidera apportare la modifica.



Avviso: Si consiglia sempre di eseguire questa operazione durante un intervento di manutenzione quando si apportano modifiche a una rete attiva.

La prova è nell'acquisizione del pacchetto

È comunemente notoIn questo modo, se non lo avete acquisito, non potete provarlo. Di seguito sono riportati un paio di esempi di configurazione con queste modifiche per mostrarvi come funziona.

Ecco una configurazione WLAN. Durante il test, viene modificato solo il gruppo di server utilizzato nell'elenco dei metodi.

```
9800#show run wlan
wlan TLS-Test 2 TLS-Test
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 security dot1x authentication-list TLS-AuthC
 no shutdown
!
```

Aggiunta Del Comando Source-Interface Con L'MTU Predefinita

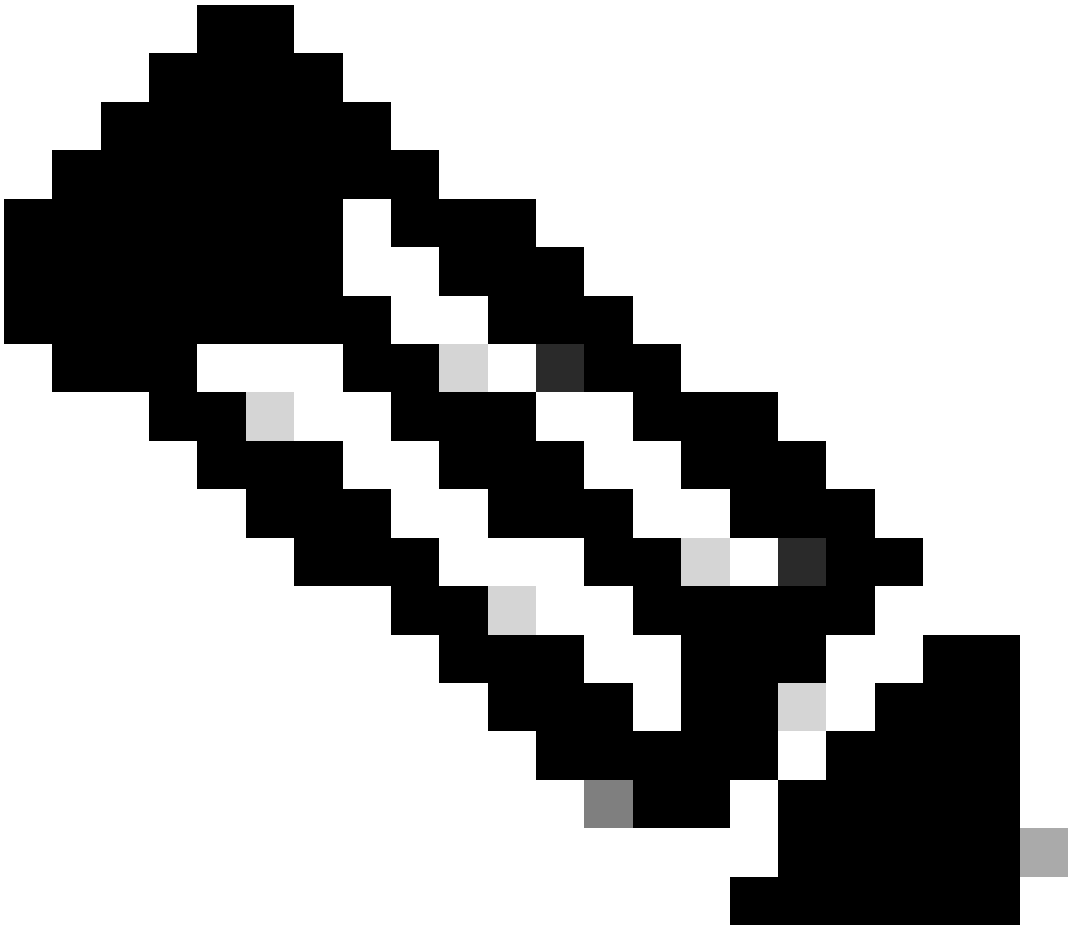
In questo caso, si tratta di un normale gruppo di server che punta al server ISE. Il comando dell'interfaccia di origine è stato aggiunto puntando a WMI senza MTU impostata. Ecco l'aspetto della configurazione.

```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group NoMTU
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObF[^bPBVNaYibbBMhNMFAbKUAAB
!
aaa group server radius NoMTU
 server name ISE
 ip radius source-interface Vlan260
 deadtime 5
!
9800#show run inter vlan 260
!
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
 no ip proxy-arp
end
```

Come si può vedere, il gruppo di server NoMTU è stato aggiunto all'elenco dei metodi di autenticazione associato alla WLAN. il comando ip radius source-interface VLAN260 viene usato per questo gruppo di server e la VLAN 260 non specifica un MTU che possa usare la MTU di 1500. Per confermare, l'MTU di 1500 può essere usata con il comando show run all e cercare l'interfaccia nell'output.

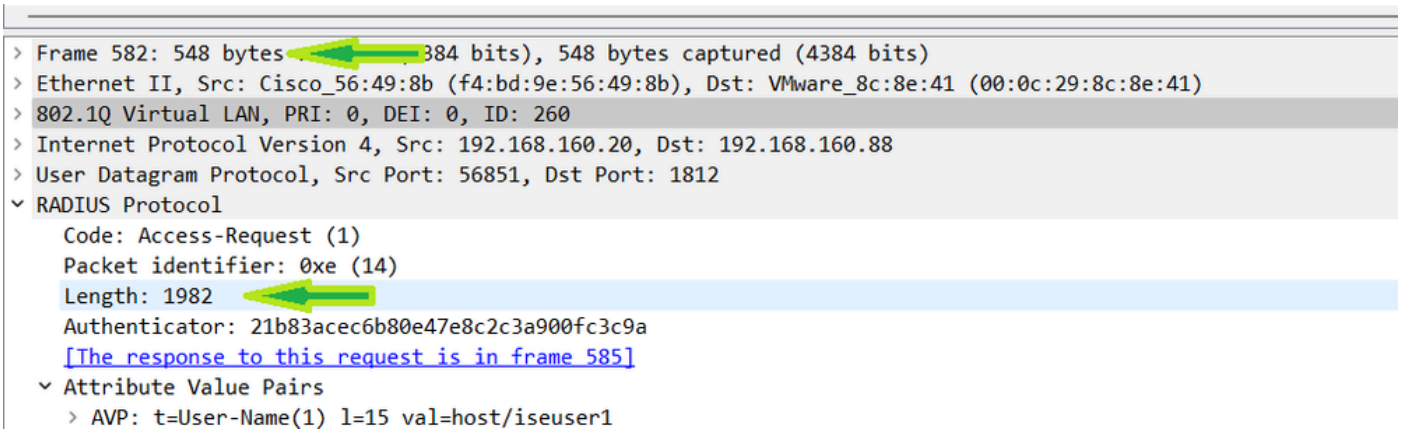
```
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
 no ip clear-dont-fragment
 ip redirects
 ip unreachables
 no ip proxy-arp
 ip mtu 1500
```

Osservare ora il pacchetto in cui il certificato client deve essere inviato all'ISE, quando il WLC aggiunge i dati RADIUS:



Nota: Qui, i byte sulla linea sono 1518. incluse le intestazioni esterne al payload Ethernet, come l'intestazione VLAN e l'intestazione layer 2. Queste non vengono conteggiate ai fini dell'MTU.

```
> Frame 581: 1518 bytes (12144 bits), 1518 bytes captured (12144 bits)
> Ethernet II, Src: Cisco_56:49:8b (f4:bd:9e:56:49:8b), Dst: VMware_8c:8e:41 (00:0c:29:8c:8e:41)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 260
> Internet Protocol Version 4, Src: 192.168.160.20, Dst: 192.168.160.88
v Data (1480 bytes)
    Data: de13071407c63226010e07be21b83acec6b80e47e8c2c3a900fc3c9a010f686f73742f69…
    [Length: 1480]
```



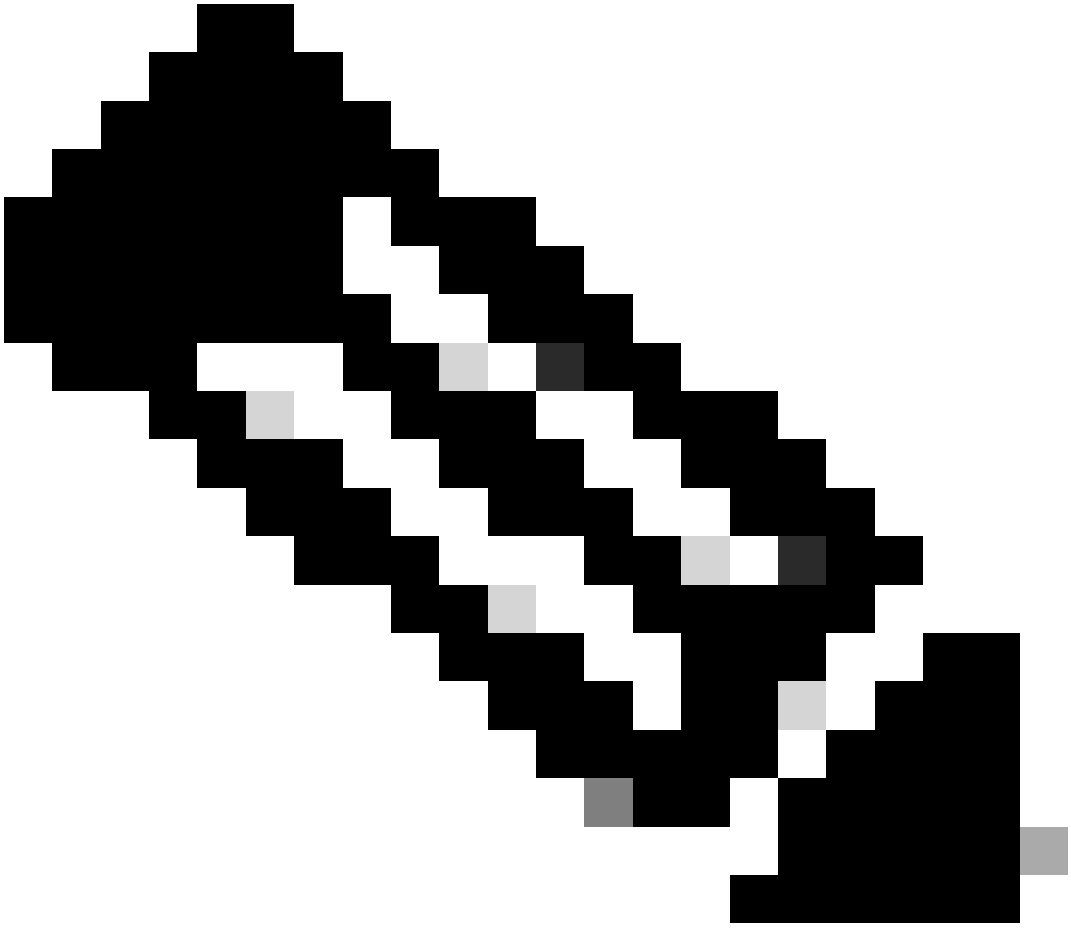
Qui potete vedere che la parte dei dati è frammentata al 1480. Su WMI, è possibile ottenere tale frammento con MTU inferiore a 1500. Il pacchetto successivo è inferiore a 550 byte, ma si può notare che le dimensioni totali dei dati RADIUS sono pari a 1982. Ciò detto, la frammentazione con la nuova MTU ora funziona.

Uso Di Un'Interfaccia Non WMI Con MTU Di 1200

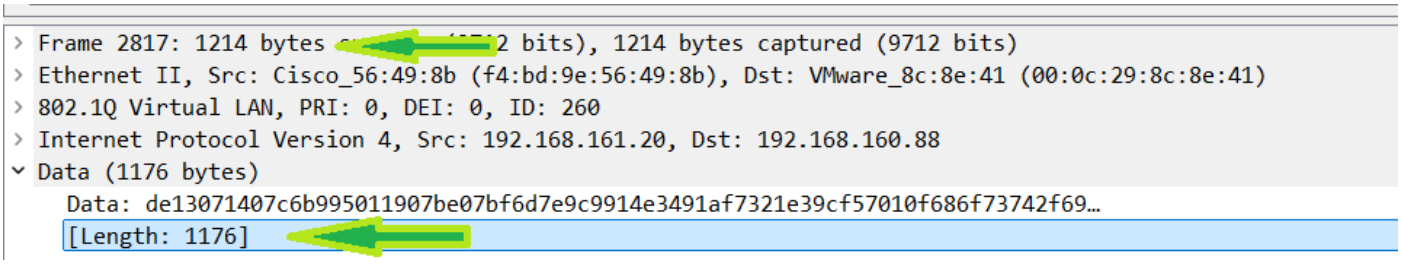
Ora, si supponga di voler frammentare il pacchetto a una MTU più piccola, ma di non voler modificare questa impostazione in modo da influenzare nessun altro tipo di traffico. Nessun problema in questo caso, la configurazione rimane la stessa solo se la configurazione dell'interfaccia di origine punta a una SVI creata appositamente. Modificare l'elenco dei metodi in modo che faccia riferimento a questo nuovo gruppo di server, che utilizza un'interfaccia di origine diversa da WMI e la cui MTU è impostata su 1200. Di seguito è riportato l'aspetto della configurazione:

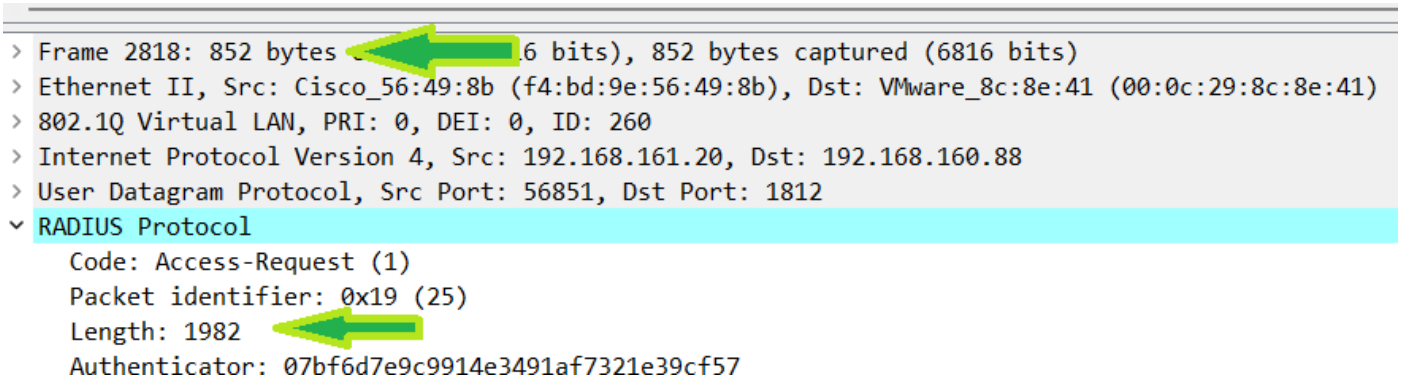
```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group MTU1200
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObFibbBMhNMFAbKUAAB
!
aaa group server radius MTU1200
 server name ISE
 ip radius source-interface Vlan261
 deadtime 5
!
9800#show run inter vlan 261
!
interface Vlan261
 ip address 192.168.161.20 255.255.255.0
 no ip proxy-arp
 ip mtu 1200
end
```

Successivamente, verificare l'aspetto dei pacchetti con questa MTU inferiore.



Nota: La riduzione dell'MTU e la modifica del punto di frammentazione non fanno parte del nuovo comportamento. Questo è sempre stato vero. se il comportamento predefinito della frammentazione a 1396 non rientra nell'MTU, la frammentazione viene effettuata sempre in un punto diverso. Questa sezione contiene informazioni utili per illustrare le opzioni disponibili.





In questo caso, i dati RADIUS sono ancora pari a 1982 byte, ma questa volta i dati sono stati frammentati a 1176 byte invece dei 1376 predefiniti in cui sarebbero stati frammentati se non fosse stata utilizzata l'interfaccia di origine. Tenere presente che quando si imposta l'MTU a 1500 e si usa il comando source-interface, il frammento viene frammentato su 1480. Utilizzando la configurazione qui, è possibile modificare il traffico verso una MTU inferiore senza interferire con il traffico di altro tipo sul WLC.

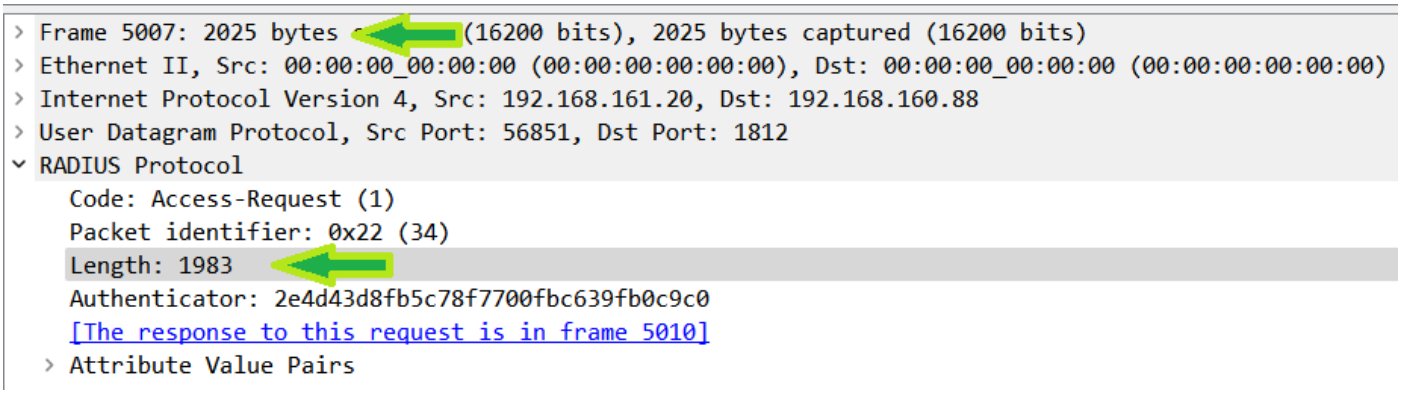
Uso di una MTU di 9000 per frame jumbo

Poiché per l'opzione di invio dei jumbo frame è stata specificata questa funzionalità, sarebbe un peccato non verificarla comunque usando l'interfaccia non WMI della VLAN 261. Tuttavia, ora l'MTU IP è impostata su 9000. Per poter impostare l'MTU IP sulla SVI, è necessario impostare l'MTU su un valore superiore all'MTU IP. Nella configurazione è possibile verificare quanto segue:

```
9800(config-if)#do sho run inter vl 261
!
interface Vlan261
 mtu 9100
 ip address 192.168.161.20 255.255.255.0
 no ip proxy-arp
 ip mtu 9000
end
```

Qui, osservando la cattura, si può notare che il pacchetto non è mai stato frammentato. È stato inviato come un pacchetto completo con le dimensioni dei dati RADIUS nel 1983. A questo scopo, è necessario configurare il resto della rete in modo da consentire il passaggio di un pacchetto di queste dimensioni.

Un'altra cosa da notare è che l'MTU del client non è cambiata, quindi il client sta ancora frammentando il pacchetto EAP a 1492. La differenza è che il WLC può aggiungere tutti i dati RADIUS necessari per inviare il pacchetto all'ISE senza frammentare i dati del client.



Conclusioni

Quando si utilizza EAP-TLS, il client deve inviare il proprio certificato al server AAA. Questi certificati sono in genere più grandi dell'MTU e il client deve frammentarli. Il punto in cui il client frammenta i dati è molto vicino all'MTU. Poiché l'access point deve aggiungere l'intestazione CAPWAP, il contenuto inviato dal client deve essere frammentato. Il WLC riceve questi due pacchetti, li riunisce ma deve frammentarli di nuovo per aggiungere i dati RADIUS. A questo punto, l'amministratore di rete può controllare il modo in cui il WLC frammenta il pacchetto EAP inviato dal client.

Se si aggiunge il comando ip radius source-interface <interfaccia che si desidera utilizzare> al gruppo di server AAA, il WLC utilizza l'interfaccia specificata al posto di (o inclusa) il comando WMI. L'uso di questo comando indica anche al WLC di frammentare l'MTU dell'interfaccia in base al valore predefinito 1396. In questo modo, si ha un maggiore controllo su come i pacchetti si spostano attraverso la rete.

Quando si utilizza Cisco Catalyst Center, il comando di interfaccia di origine viene aggiunto al gruppo di server, modificando il comportamento predefinito.

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).