瞭解9800 WLC上的RADIUS MTU和分段

目錄

簡介

本檔案介紹如何設定WLC傳送到RADIUS伺服器的RADIUS封包的MTU。

必要條件

需求

思科建議您對以下主題有基本瞭解：

- 9800無線LAN控制器(WLC)AAA組態
- 驗證、授權及記帳(AAA)RADIUS概念
- 可擴展身份驗證協定EAP
- 最大傳輸單位(MTU)

採用元件

- 思科身分識別服務工程師(ISE)3.2
- Catalyst 9800無線控制器系列(Catalyst 9800-L)
- Cisco IOS® XE 17.15.2
- Windows 11無線客戶端

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景

在本檔案中，使用的遠端驗證撥入使用者服務(RADIUS)伺服器是Cisco ISE。首先，演示了可擴展身份驗證協定(EAP)過程中資料包如何無外部干預地流動。下一步是設定選項，變更WLC傳送到任何RADIUS伺服器的存取要求的大小。此選項是在IOS-XE版本17.11中新增的。

9800 RADIUS MTU

通常RADIUS封包的MTU並不重要，因為它們通常較小，且無論如何不會命中MTU。但是，當一側必須傳送證書（通常為2-5KB）時，裝置需要將該證書分段以使其低於其MTU。

當使用者端必須向RADIUS伺服器傳送憑證時(如EAP傳輸層安全(EAP-TLS))，會向WLC提供這樣一種情況，由於必須隨其傳送的RADIUS資料數量而需要將封包重新分段。直到17.11之前，網路管理員幾乎無法控制此程式，但現在，工程師可以選擇操縱WLC傳送的存取要求的大小。

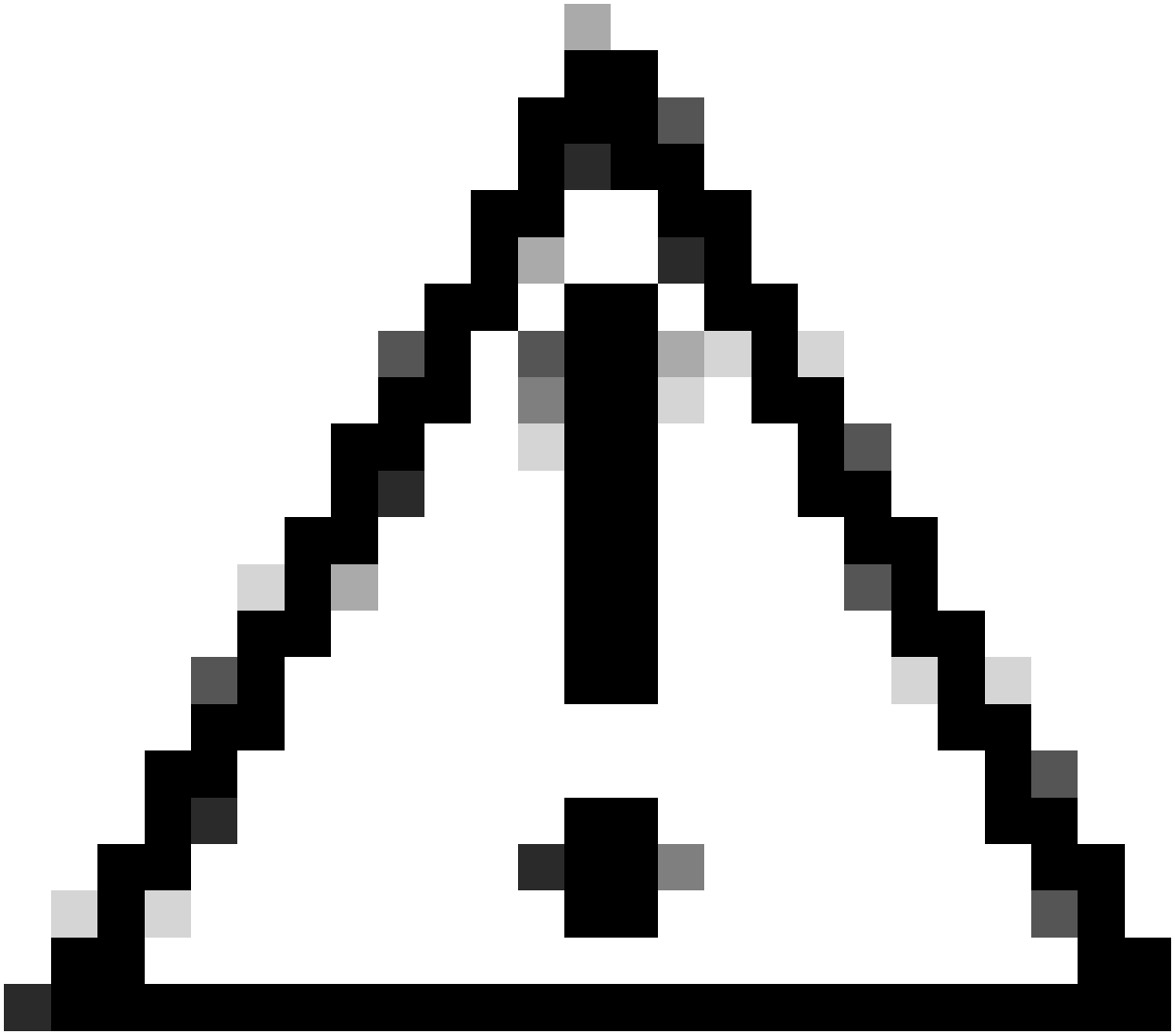
EAP-TLS資料包流

這在一定程度上深入瞭解了資料包的外觀以及無線基礎設施如何處理這些資料包。為了充分理解本文檔中介紹的更改，在使用dot1x和更具體的EAP-TLS時，瞭解無線身份驗證過程中的資料包流非常重要。

如果您已經深入瞭解EAP和RADIUS資料包流在Cisco無線基礎架構中的工作方式，則轉到行為更改部分，該部分將說明17.11中新增的內容，使網路管理員能夠更好地控制RADIUS MTU。首先，請檢視EAP標識(EAP-ID)。

EAP-ID

EAP-ID由身份驗證器（本例中為WLC）啟動。這必須是EAP流程的第一部分。有時，無線客戶端會傳送EAPOL-Start。這通常表示客戶端從未收到EAP-ID請求或想要重新開始。



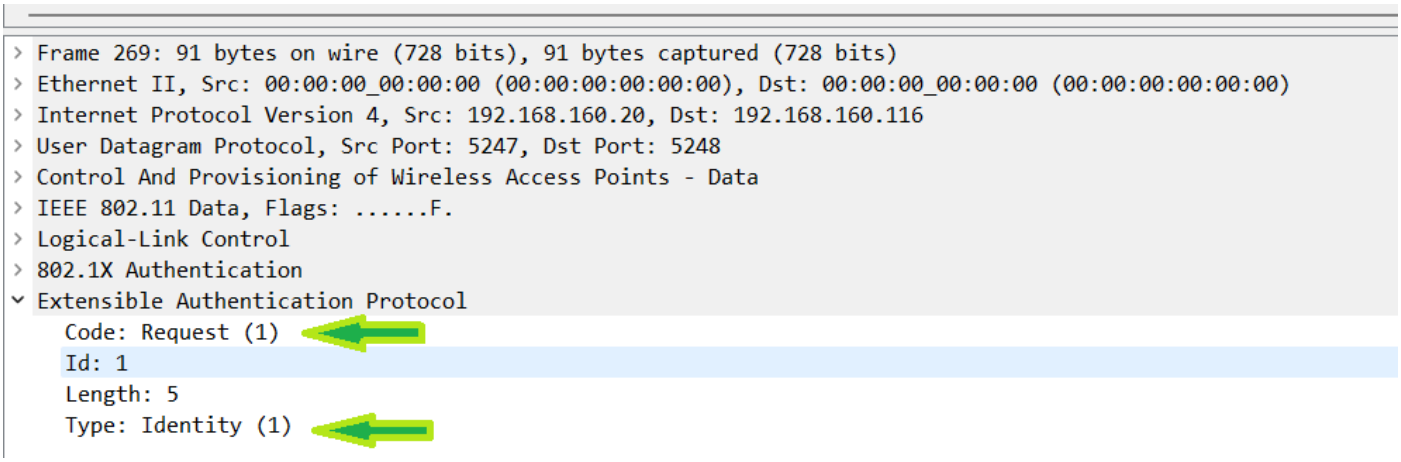
注意：EAP-ID資料包和EAP資料包ID之間存在差異。EAP-ID資料包用於標識請求方，其中EAP資料包ID是一個數字，用於在特定資料包通過網路時對其進行跟蹤。

EAP-ID請求

首先，無線客戶端裝置使用正常關聯過程連線到網路。當無線區域網路(WLAN)設定為dot1x時，WLC在可以從RADIUS伺服器要求存取之前，首先需要知道使用者端是誰。要查詢此資訊，WLC會傳送客戶端和EAP-ID請求。

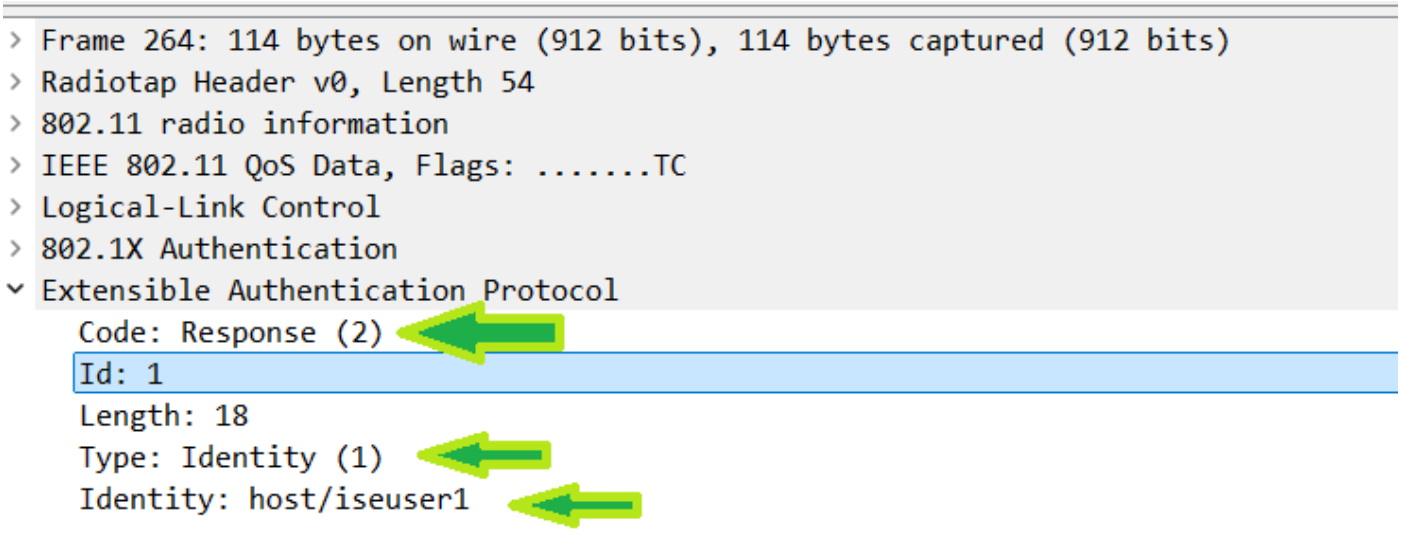
客戶端應使用EAP-ID響應進行響應。這使WLC能夠構建訪問請求並將其傳送到ISE所需的功能。EAP-ID請求是指在正常PEAP身份驗證中要求客戶端輸入其使用者名稱和密碼的時間。

但是，此討論圍繞EAP-TLS，因此，這裡的EAP-ID響應將僅具有使用者ID。在演示中，使用者ID為iseuser1。在此資料包中，您可以看到WLC向無線客戶端傳送的EAP-ID請求，詢問他們是誰。由於這是一個無線使用者端，WLC會將要求封裝在CAPWAP中，並將其傳送到存取點(AP)以透過空中傳送。在EAP資料中，代碼1表示它是請求，型別1表示它是用於身份的。



EAP-ID響應

接下來，將會看到無線客戶端使用EAP-ID響應進行響應。在EAP資料中，代碼已更改為2，表示它是響應，但型別仍為1，仍顯示為身份標識。在這裡，您甚至可以看到客戶端所使用的使用者名稱。還要檢查這些資料包的是EAP資料包的ID號。對於EAP-ID交換，它始終為1，但是在ISE參與後，此號碼會更改為其他值。



您可以看到兩個封包都相當小，因此MTU此處沒有影響，因為它已完全低於網路中使用的1500位元組。

Access-Request和Access-Challenge

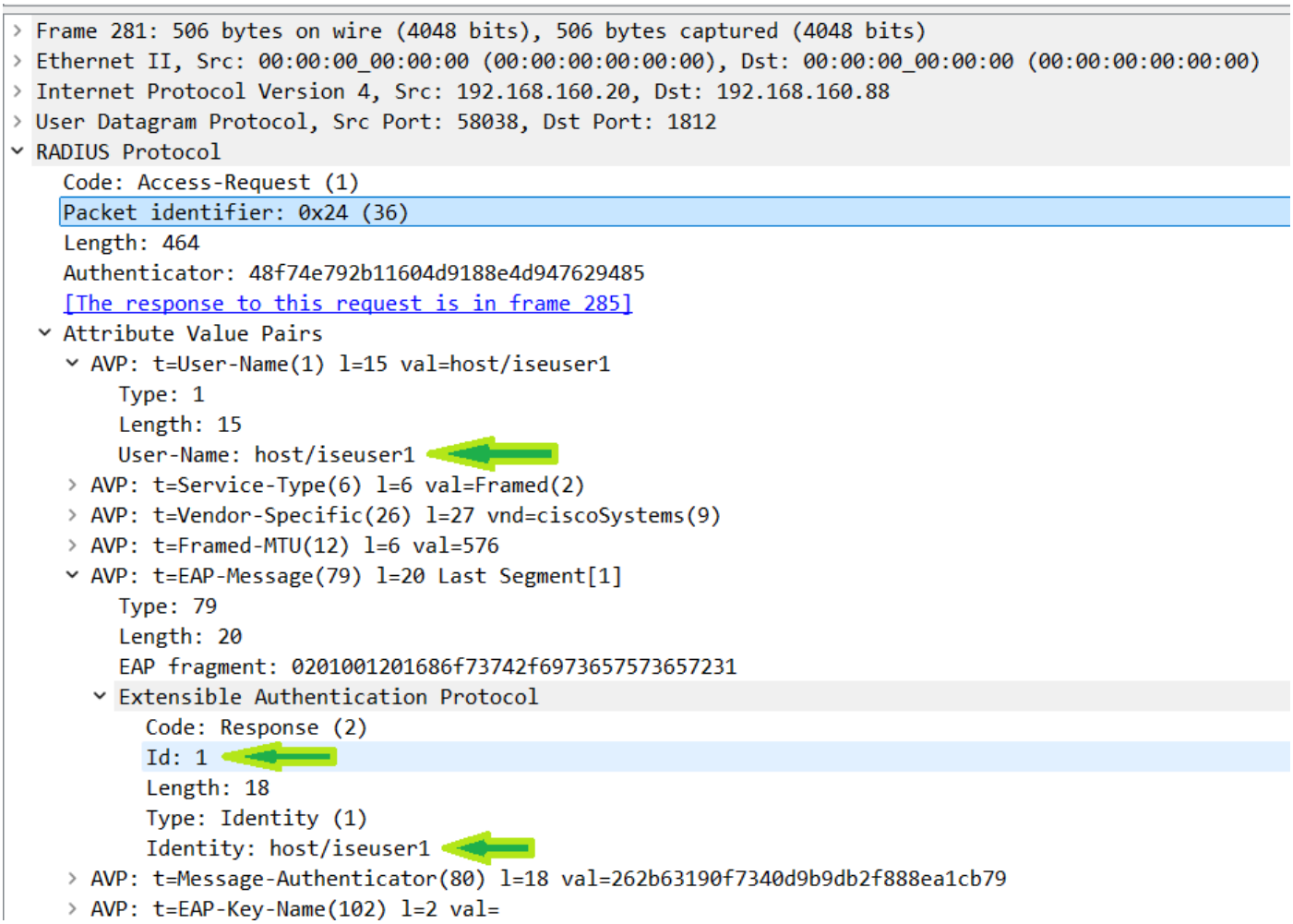
與客戶端的通訊為EAP，WLC和ISE之間的通訊為RADIUS。 對於RADIUS通訊，使用訪問請求和訪問質詢資料包。WLC從請求方接收EAP資料包，並使用RADIUS訪問請求將其轉發到ISE。在工作網路中，ISE會以訪問質詢進行響應。

Access-Request

現在，WLC知道使用者端的身分，因此它需要詢問RADIUS伺服器是否允許該使用者端在網路上。為此，WLC會透過傳送存取要求封包來要求該使用者端存取。WLC將與EAP資料一起傳送其他資料

段。這些資料段統稱為屬性值對、AVP或AV對，具體取決於說話者。

本文檔不會深入到AVP中，因為這超出了本討論的範圍。在這裡，您只需看到使用者名稱（EAP資料）被包含並傳送到RADIUS伺服器（在本例中為ISE）。此外，您還可以看到EAP-ID編號1也被傳送到ISE。請記住，當您檢視EAP資料包ID over air時，該地址也為1。此處要注意的最後一點是，因為WLC已新增所有這些AVP，所以使用者端傳送的114位元組封包現在會轉換為488位元組封包，然後才會傳送到ISE。

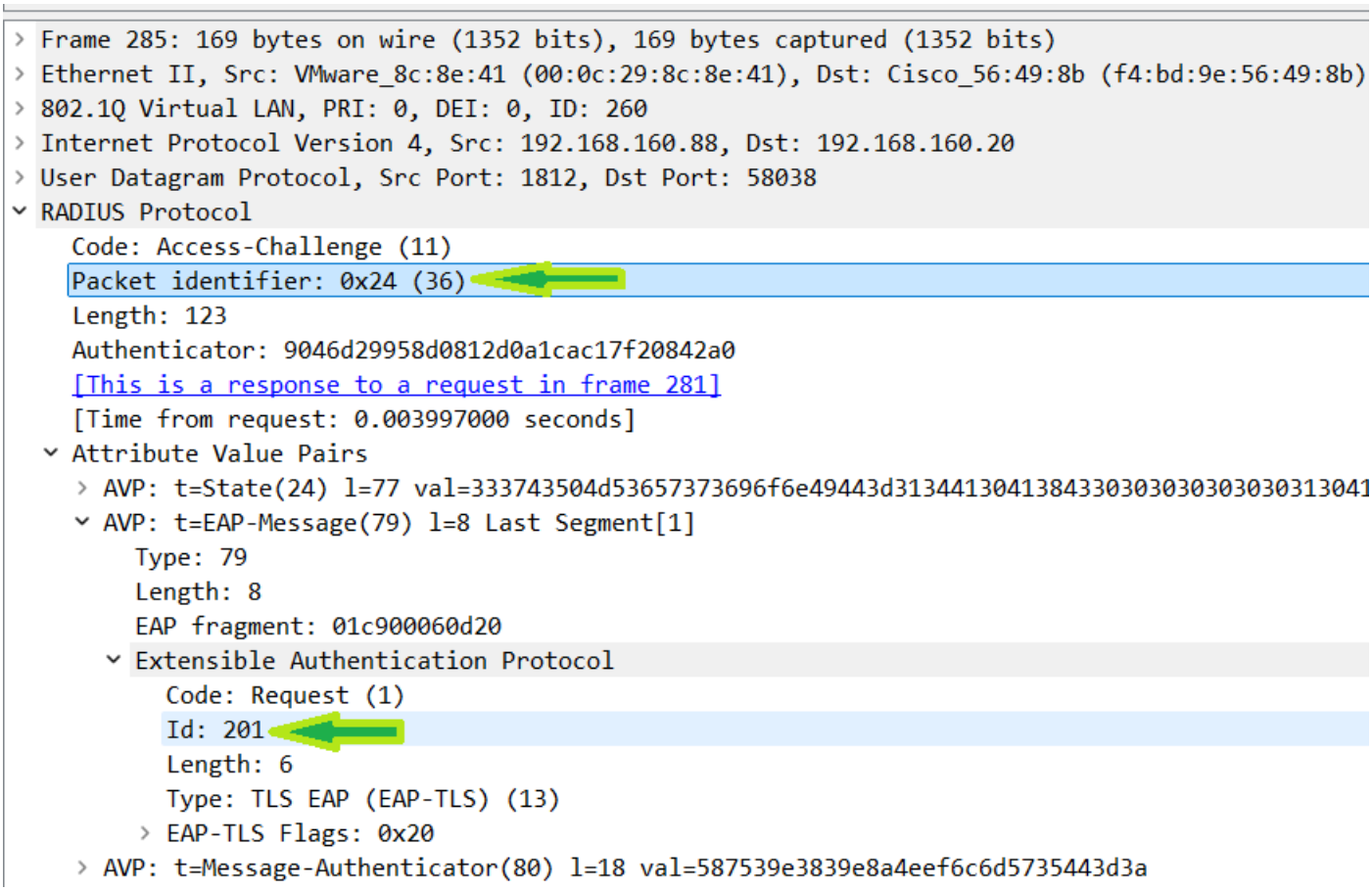


訪問挑戰

假定ISE收到訪問請求並決定響應，則此響應預期會作為ISE的訪問質詢。回首存取要求，您會看到AVP啟動前的RADIUS封包ID為36。

當WLC收到存取要求時，RADIUS ID必須與存取要求的封包ID相符。RADIUS封包ID用於ISE和WLC之間的RADIUS通訊。您還可以在此資料包中看到ISE已設定新的EAP ID 201，用於跟蹤ISE和客戶端之間的通訊。此時，WLC只是ISE和客戶端之間通訊的直通路由器。

請務必在此處記錄所有這些資料包ID，以便您瞭解通訊流以及如何通過網路跟蹤這些資料包。在生產環境中通常同時進行多個身份驗證。使用calling-station-id 命令將資料包與客戶端的MAC地址進行匹配。然後，您可以使用RADIUS資料包ID和EAP資料包ID跟蹤此特定客戶端的資料包流。到目前為止，兩端都沒有傳送任何證書，因此仍然不需要擔心MTU。



EAP請求和EAP響應

提醒一下，使用者端說EAP而不是RADIUS。也就是說，當WLC收到訪問質詢時，它必須刪除RADIUS資料並取出EAP請求，以便將其傳送到客戶端。

EAP請求

這必須與WLC收到存取挑戰時其在內部所做的完全相同。但是，所有RADIUS內容都已被刪除，只有EAP部分被傳送到客戶端。

您仍然可以在此處看到EAP資料包ID 201，就像訪問質詢中一樣，因為它與WLC從ISE接收的資料相同。此處的流程與EAP-ID相同，只是現在它不是來自WLC，而是用於建立EAP方法。此資料包仍然非常小，因為它只是為了建立EAP-TLS會話的開始。

```
> Frame 347: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
> Radiotap Header v0, Length 54
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: ......F.C
> Logical-Link Control
> 802.1X Authentication
v Extensible Authentication Protocol
    Code: Request (1)
    Id: 201
    Length: 6
    Type: TLS EAP (EAP-TLS) (13)
  v EAP-TLS Flags: 0x20
      0... .... = Length Included: False
      .0.. .... = More Fragments: False
      ..1. .... = Start: True
```

EAP響應

當客戶端收到EAP-Request時，它必須使用EAP-Response進行響應。 在EAP-Response中，客戶端開始建立TLS會話。這看起來與任何其它使用TLS的情況相同。它以「客戶端hello」消息開頭。本文檔不會深入研究客戶端Hello中的內容，因為它與此主題無關。您在這裡需要注意的是TLS會話正在設定。

您可以在此處檢視資料包中的資料，就像檢視其他任何TLS設定時一樣。與EAP-ID響應一樣，此封包會命中WLC並轉換為存取請求。ISE以封裝在訪問質詢中的EAP請求進行響應。從現在開始，這仍舊是流動的。

```
> Frame 349: 300 bytes on wire (2400 bits), 300 bytes captured (2400 bits)
> Radiotap Header v0, Length 54
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
> 802.1X Authentication
v Extensible Authentication Protocol
    Code: Response (2)
    Id: 201
    Length: 204
    Type: TLS EAP (EAP-TLS) (13)
  v EAP-TLS Flags: 0x80
      1... .... = Length Included: True
      .0.. .... = More Fragments: False
      ..0. .... = Start: False
    EAP-TLS Length: 194
  v Transport Layer Security
    v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 189
      > Handshake Protocol: Client Hello
```

TLS證書

此處是您將看到資料包大小增加的點。取決於是否存在一個或多個中間憑證授權單位(CA)，憑證可能相當大。 如果是自簽名的證書，其大小顯然比裝置證書連結到2個中間CA和1個根CA的證書小。無論哪種方式，您通常看到憑證的所有者開始在此處對其自己的封包進行分段。

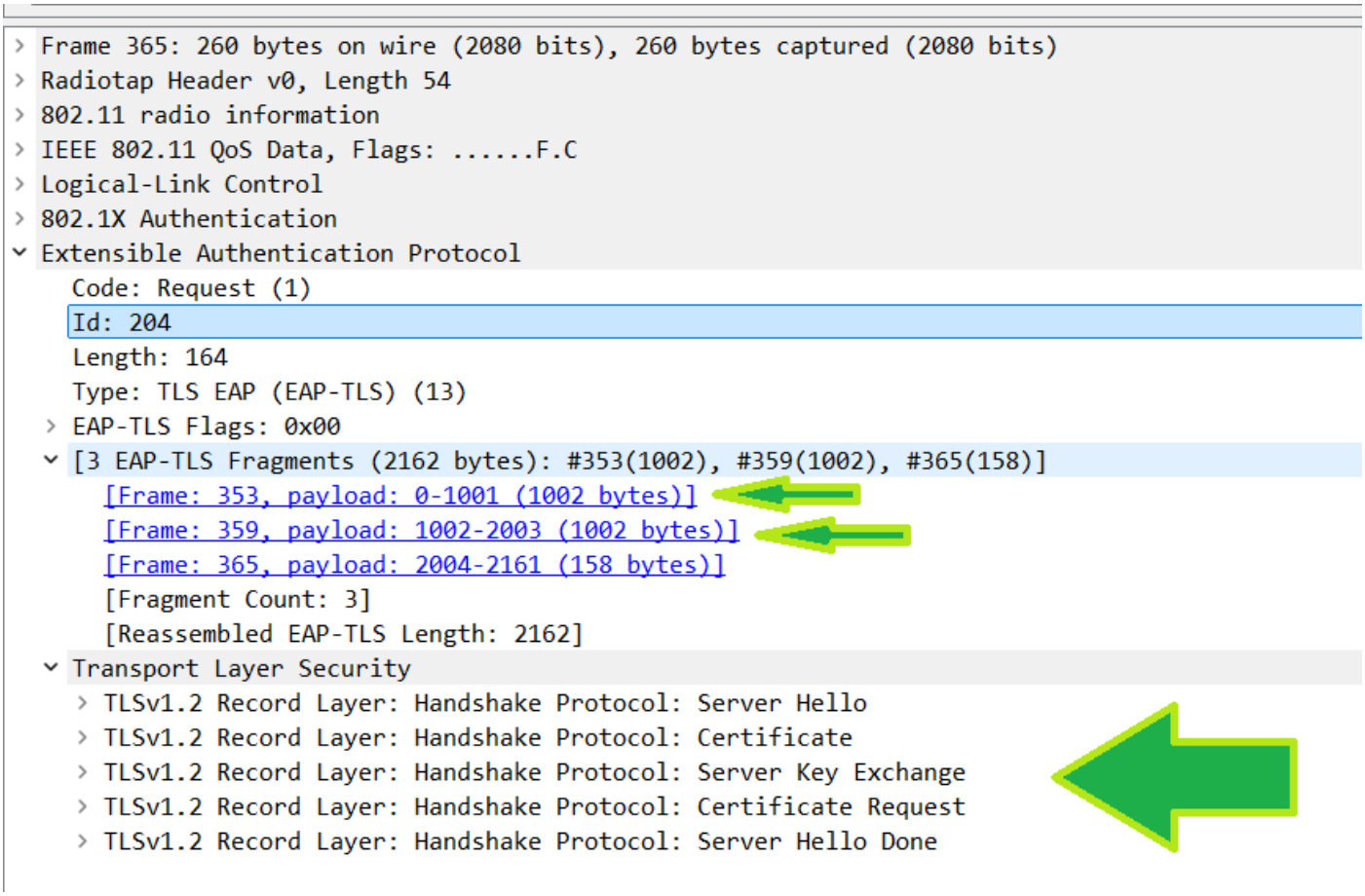
ISE證書

現在ISE已收到TLS客戶端hello，它將以另一個EAP請求進行響應。在此新的EAP請求中，ISE會同時傳送「伺服器問候」消息、其證書、「伺服器金鑰交換」、「證書請求」和「伺服器問候完成」消息。如果在一個封包中傳送所有這些，則封包會大於網路的MTU。因此，ISE將封包本身分段，使其低於MTU。使用ISE時，它會分段資料包的資料部分，使其不大於1002位元組，希望避免雙重分段。

雙重分段是什麼意思？由於ISE想要傳送的資料太大，無法容納網路的MTU，因此在ISE上進行了第一次分段。此外，網路中可能還有其他地方，雖然網路的MTU相同，但由於網路的設定方式，裝置可能需要將封包分段，以便新增標頭並停留在MTU之下。即使選中了do not fragment 位，也可能出現這種情況。

VPN隧道或任何隧道就是很好的例子。要將資料放入VPN隧道，VPN路由器必須將其報頭新增到流量中。如果此RADIUS流量在MTU或接近MTU處進行分段，當涉及此VPN時，無法將資料保持在MTU下並新增額外標頭。對於CAPWAP隧道，情況也是如此，稍後您可以看到。

因此，為避免這些資料包進入其他裝置可以再次對其進行分段的情況，ISE會在大多數網路中可以避免這一情況的地點對資料包進行分段。這意味著ISE在每次等待空的EAP響應的多個EAP請求中傳送此資料。EAP ID隨每個片段的傳送而增加。從WLC的角度來看，這是對每個片段的存取詢問和存取要求交換，RADIUS封包ID會隨著每個片段的傳送而增加。



客戶端證書

一旦ISE傳送所有片段並由客戶端重組這些片段，資料包流將轉移到客戶端以傳送某些內容。在TLS中，客戶端此時會傳送自己的證書以完成身份驗證。事情就是在這裡變得更加複雜的。與ISE一樣，客戶端將同時傳送多個TLS部分，其中一個是其證書。

與ISE所見不同，大多數客戶端傳送其EAP資料僅略低於MTU。在本演示中，802.1x資料為1492。問題在於AP需要新增CAPWAP標頭才能將其傳送到WLC。

怎麼辦呢？AP必須將封包分段，以便新增標頭並將其傳送到WLC。 AP無法在不將封包分段的情況下將其獲取到WLC。也就是說，此處資料包是雙重分段的，首先從客戶端，然後再次從AP。但是，此分段通常不會像預期的CAPWAP那樣成為問題。

空中傳送的封包：

```
> Frame 367: 1588 bytes (12704 bits), 1588 bytes captured (12704 bits)
> Radiotap Header v0, Length 54
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: .......TC
> Logical-Link Control
> 802.1X Authentication
v Extensible Authentication Protocol
    Code: Response (2)
    Id: 204
    Length: 1492
    Type: TLS EAP (EAP-TLS) (13)
  v EAP-TLS Flags: 0xc0
      1... .... = Length Included: True
      .1.. .... = More Fragments: True
      ..0. .... = Start: False
    EAP-TLS Length: 4692
```

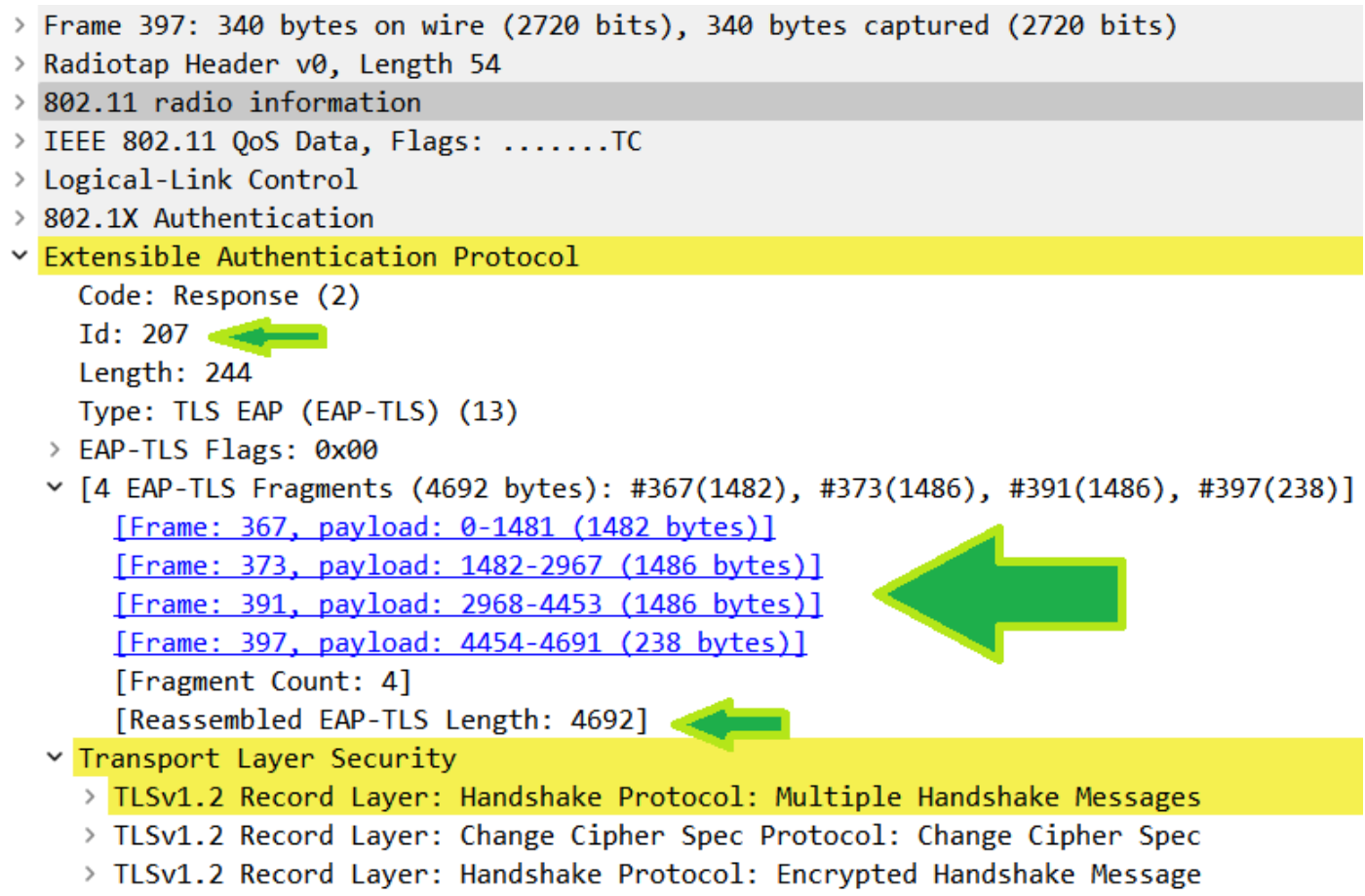
線路上的封包片段：

```
> Frame 56: 1482 bytes (11856 bits), 1482 bytes captured (11856 bits) on interface /tmp
> Ethernet II, Src: Cisco_b5:e6:00 (0c:75:bd:b5:e6:00), Dst: Cisco_56:49:8b (f4:bd:9e:56:49:8b)
> Internet Protocol Version 4, Src: 192.168.160.116, Dst: 192.168.160.20
> User Datagram Protocol, Src Port: 5248, Dst Port: 5247
> Control And Provisioning of Wireless Access Points - Data
  [Reassembled in: 57]
v Data (1424 bytes)
    Data: 018800000c75bdb3022038689362ec7e0c75bdb3022f00010000aaaa03000000888e0100…
    [Length: 1424]
```

封包已線上路上重組：

```
Wireshark · Packet 57 · FromTheWire2.pcap
> Frame 57: 156 bytes (1248 bits), 156 bytes captured (1248 bits) on interface /tmp/epc_ws/wif_to_ts_pipe, id 0
> Ethernet II, Src: Cisco_b5:e6:00 (0c:75:bd:b5:e6:00), Dst: Cisco_56:49:8b (f4:bd:9e:56:49:8b)
> Internet Protocol Version 4, Src: 192.168.160.116, Dst: 192.168.160.20
> User Datagram Protocol, Src Port: 5248, Dst Port: 5247
> Control And Provisioning of Wireless Access Points - Data
> [2 Message fragments (1530 bytes): #56(1424), #57(106)]
> IEEE 802.11 QoS Data, Flags: .......T
> Logical-Link Control
> 802.1X Authentication
v Extensible Authentication Protocol
    Code: Response (2)
    Id: 204
    Length: 1492
    Type: TLS EAP (EAP-TLS) (13)
  > EAP-TLS Flags: 0xc0
    EAP-TLS Length: 4692
```

已在空中重組所有客戶端片段：



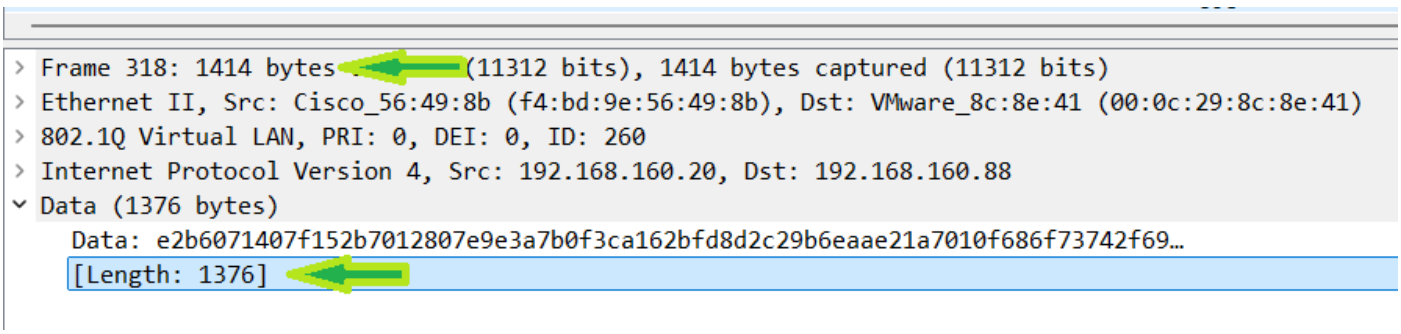
WLC上的使用者端憑證

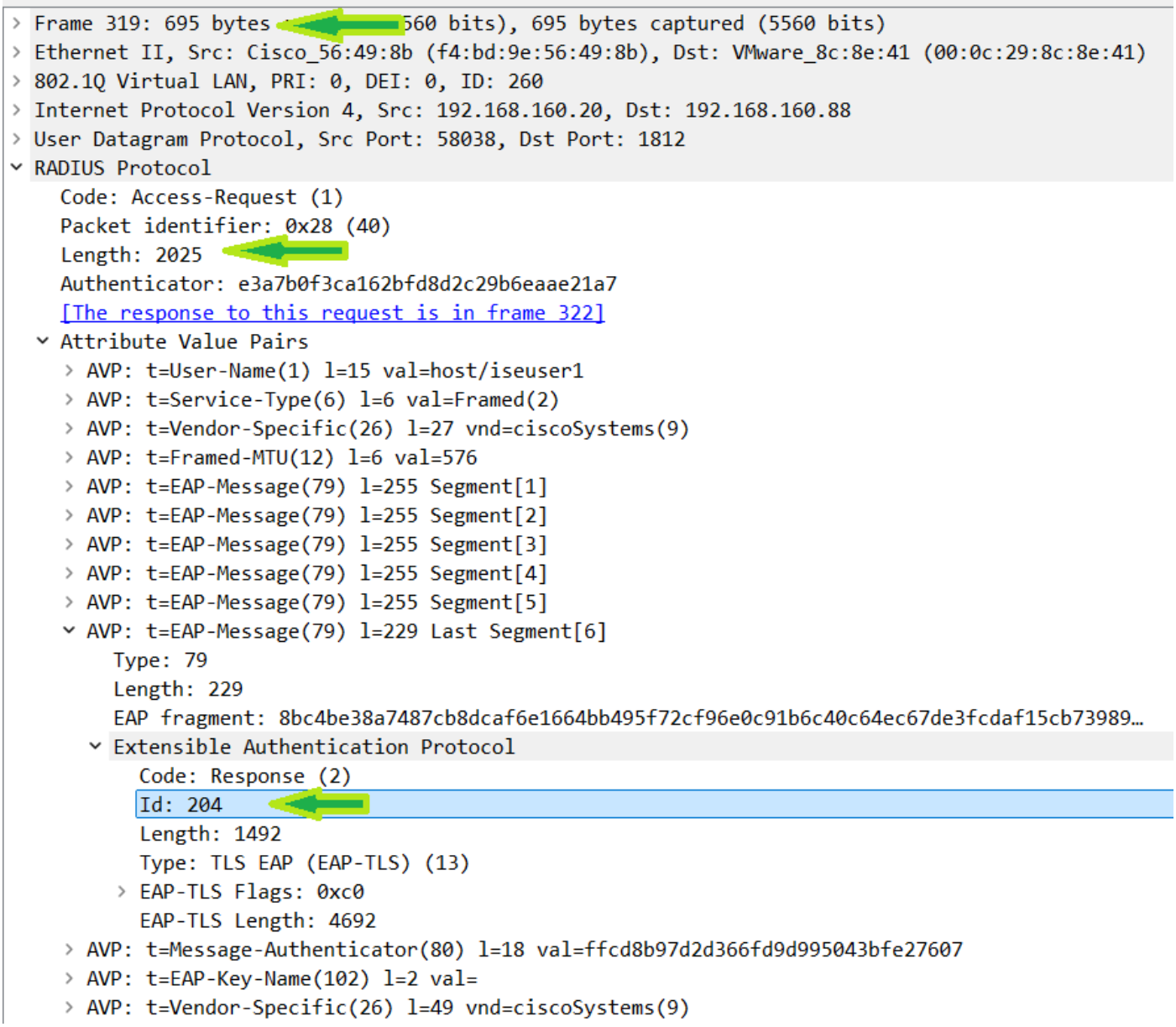
WLC收到兩個CAPWAP片段，並重組它們以從使用者端獲得完整的1492位元組封包，從而還原封包 — 但不久還原。此還原存在時間很短，因為如果您回顧WLC傳送存取要求的方式，您必須記得，它必須將價值約400位元組的RADIUS AVP新增到封包，才能將資料傳送到ISE。

為了簡單計算，假設WLC增加408位元組，使封包總大小達到1900。此數量遠遠超過1500 MTU，因此WLC會怎麼做？再次分段資料包。

這時，WLC預設將封包分段為1396。這裡的想法與ISE相同。我們希望使封包夠小，因此如果必須經過另一個通道，就無需再次分段即可新增標頭。但是，WLC並不像ISE那樣謹慎，因此1396在這裡足夠好。

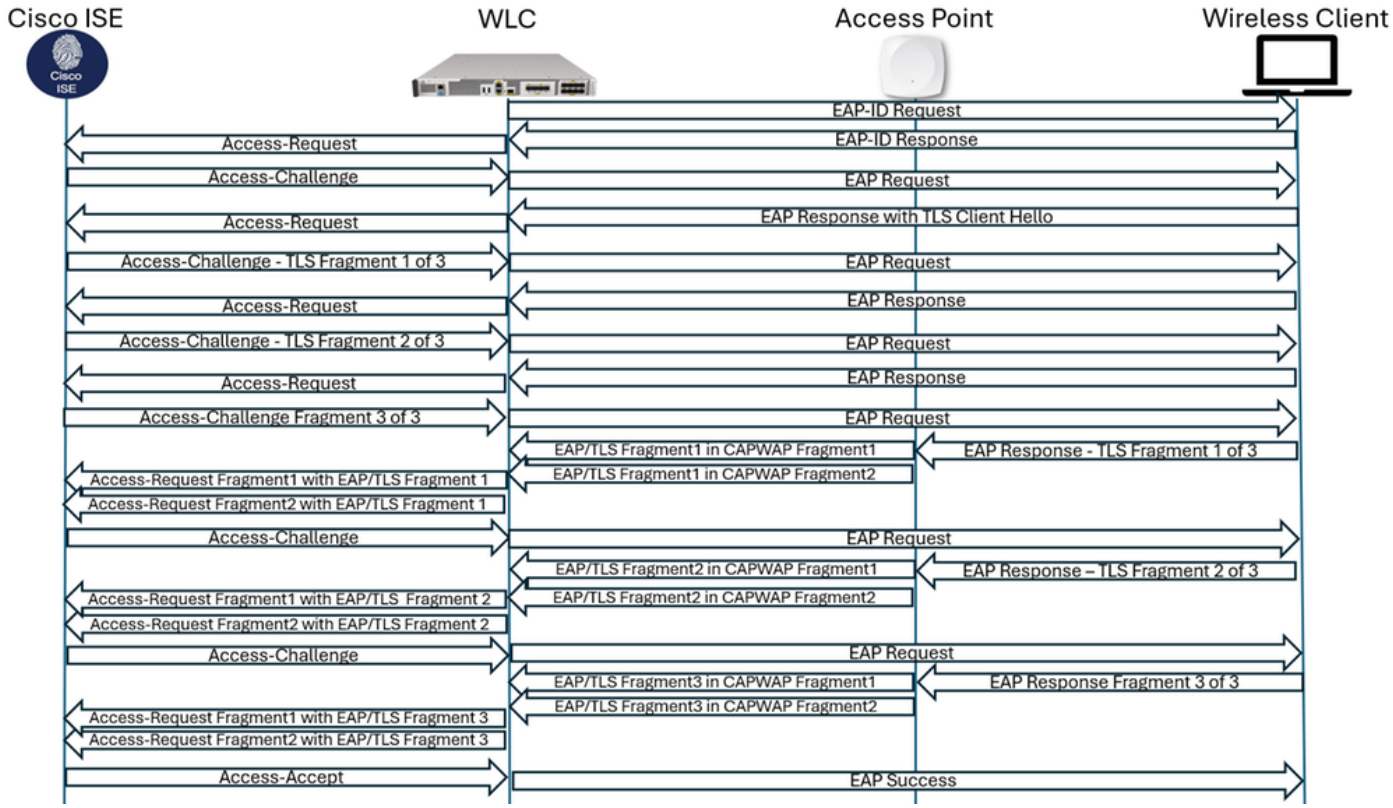
離開WLC的零碎封包：





資料包流TL;DR

當ISE傳送其證書時，它會以1002位元組的速度將TLS資料包分段。那裡沒有問題。當使用者端傳送其憑證時，它們通常會分段到接近MTU的位置。由於AP必須將CAPWAP報頭新增到資料包，因此也必須對此資料包進行分段。WLc收到片段後，必須重組封包，但之後必須新增RADIUS AVP，才能再次將封包分段。 封包流看起來是這樣的：



RADIUS MTU行為變更

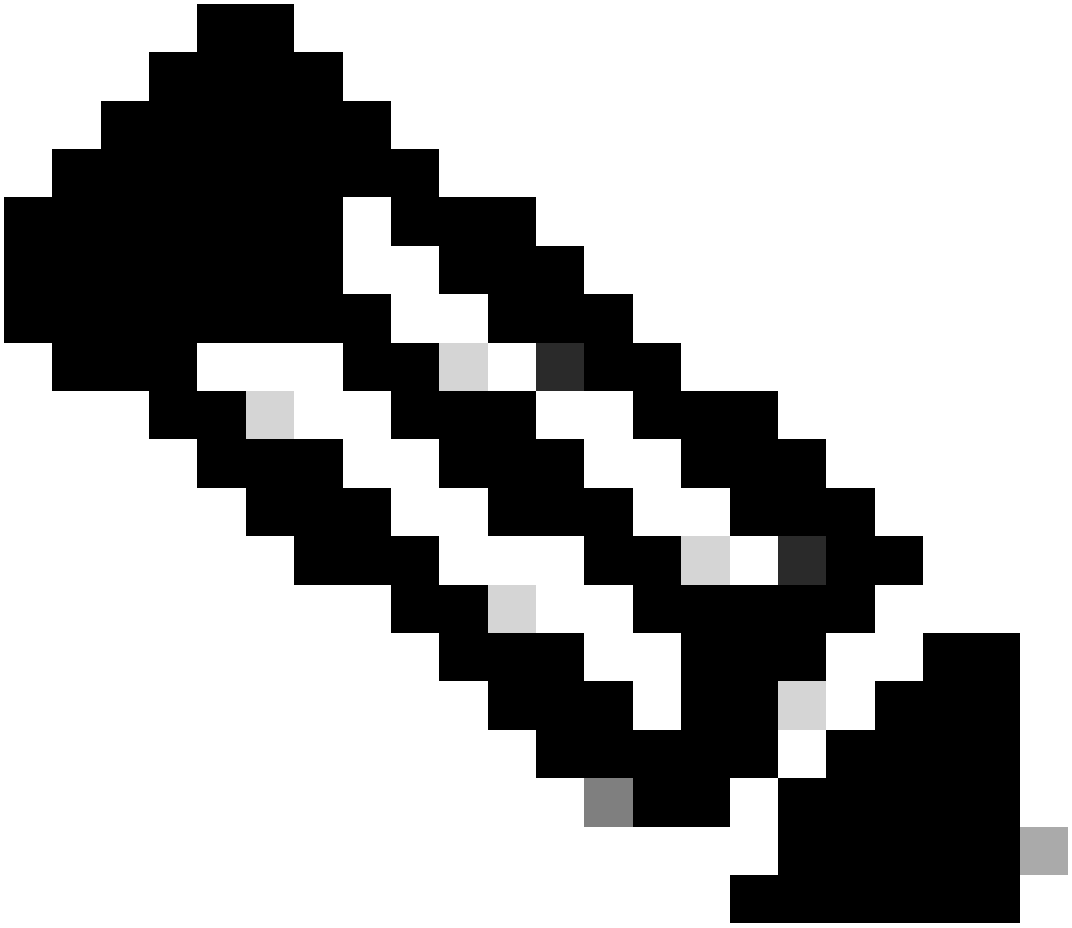
當您檢視任何無線客戶端資料流量的資料包流時，可以看到無線基礎設施只在少數地方對其有影響。第一個位置是流量離開AP時，第二個位置是流量離開WLC時。例外情況是TCP流量，其中無線基礎架構可以調整使用者端MSS。但是，EAP並不屬於TCP協定，實際上，它是它自己的協定。

當您檢視EAP和RADIUS流量時，還可以看到當原始資料包大小太接近MTU時，網路實際上影響AP和WLC的流量大小。透過適當瞭解WLC在此交換中的角色，您可以看到實際上只有一個位置影響RADIUS封包大小。這是當EAP響應傳入並將其更改為RADIUS訪問請求時。

更改內容

如果EAP響應是通過MTU，則一旦新增了RADIUS AVP，您必須將其分段。由於不管資料包大小如何，您都必須將其分段，因此您至少可以決定將其分段的大小。這就是17.11中引入的行為更改的來源。

在Cisco錯誤id CSCwc81849中追蹤的功能要求中，您想要新增對於RADIUS巨量封包的支援。完成此作業的方式是RADIUS封包不再在1396自動分段。現在，如果新增ip radius source-interface <interface X>指令，則會在該介面的MTU傳送RADIUS access-request。

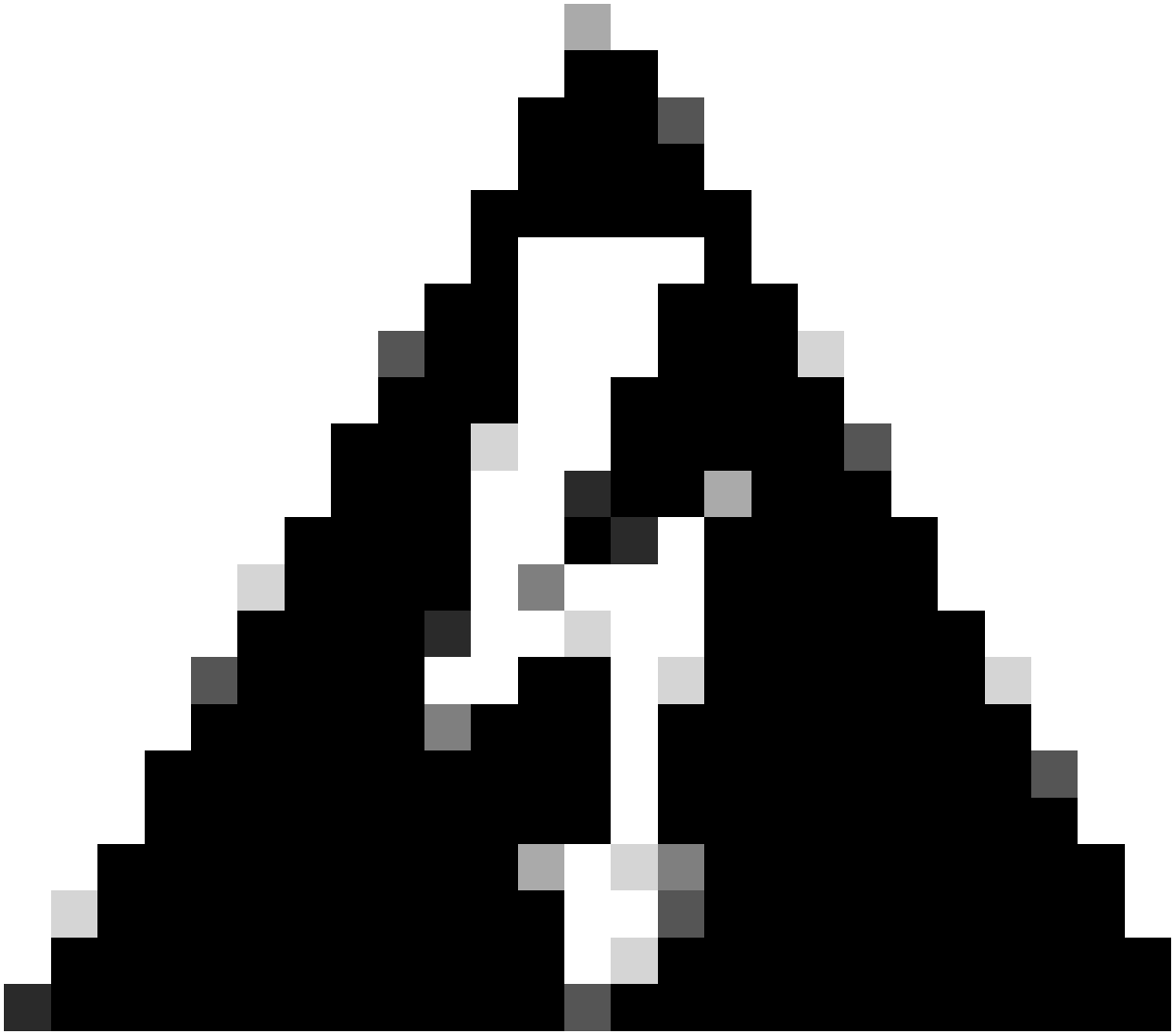


附註：如果您使用的是Cisco Catalyst Center，則在調配AAA配置時，它會自動將源介面新增到伺服器組。這會將預設行為變更為該命令中使用的介面的MTU大小。

如何使用此更改

由於所有介面的預設MTU都將是1500，因此這將是進行分段的新的MTU。用於所有RADIUS流量的預設介面是無線管理介面(WMI)。 當您檢視伺服器組的配置時，如果沒有指定源介面，WLC會使用WMI在1396傳送RADIUS流量。但是，如果您進入伺服器組配置，並告知其源介面是WMI，WLC現在會傳送仍然使用WMI的1500處的RADIUS流量。

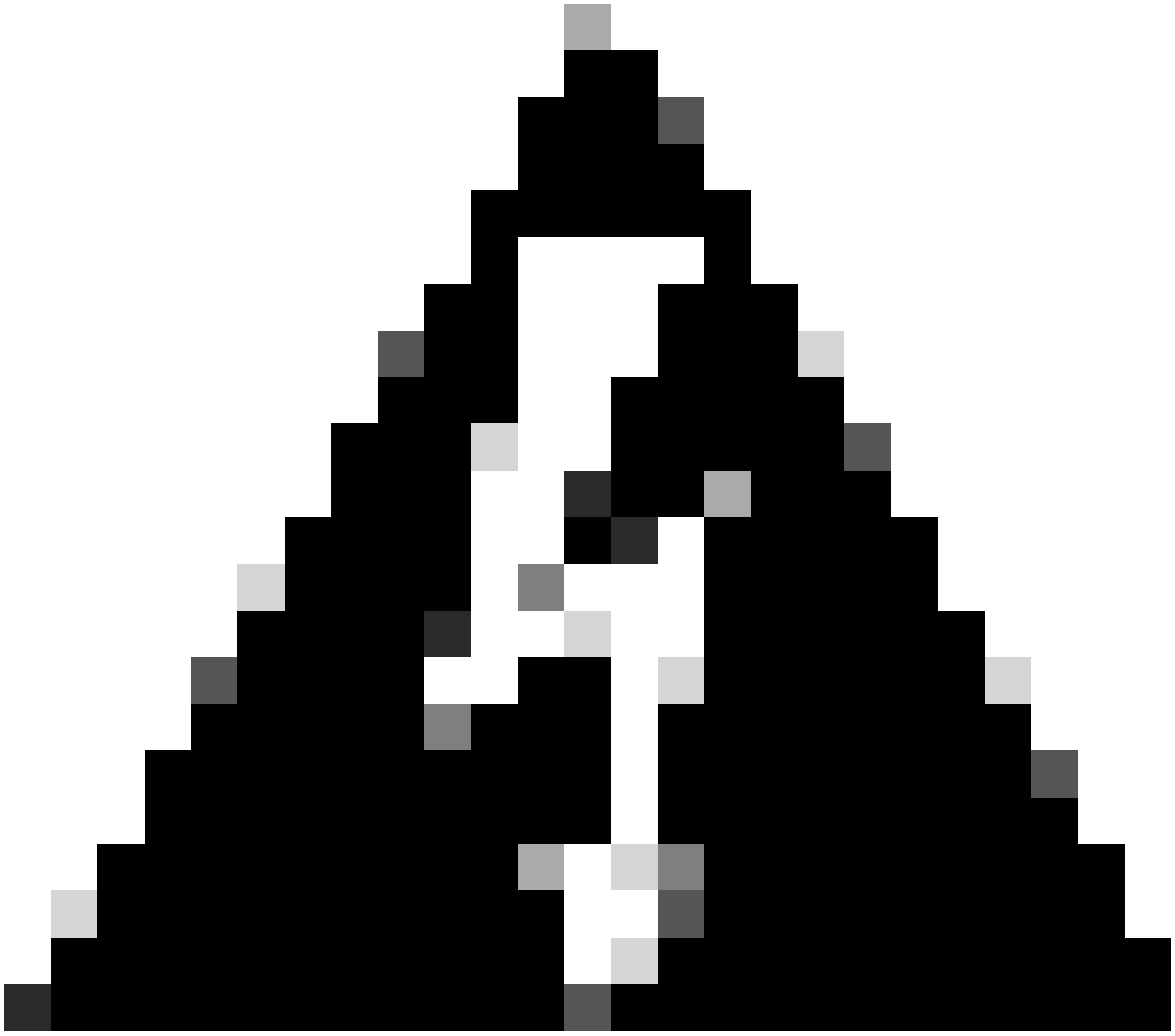
現在，假設網路中有類似於前面討論的VPN的裝置。您不希望流量被雙重分段，因此可以將介面的MTU更改為較小的值，以便將封包分段在不同的位置。您可以將MTU變更為1200等值，以便封包以1200位元組標籤（而不是1500）進行分段。



警告：更改WMI的MTU將影響所有進出該WLC管理IP地址的流量。

即使您不想更改WMI的MTU，指定源介面的要點是將其從WMI更改為另一個介面，並將該介面用於RADIUS流量，以及更改該介面上的MTU。由於此配置是在伺服器組級別完成的，您可以非常具體地確定您希望此更改受到哪些RADIUS通訊量的影響。

此配置不與AAA伺服器或WLAN關聯。可以有多個伺服器組，其中含有相同的伺服器，並且您只需在其中一台伺服器上指定源介面即可。此伺服器組將新增到方法清單，然後新增到WLAN。例如，如果只有一個您要進行此更改的WLAN，即使只有一個AAA伺服器，也可以建立一個新的伺服器組，使用指向要使用的MTU的介面的ip radius source-interface命令，將AAA伺服器新增到此新組，使用此新組建立一個新方法清單，然後將該方法清單新增到要進行此更改的特定WLAN。



警告：建議在對實際網路進行ANY更改時，在維護時段內完成。

證據在資料包捕獲中

一般認為在網路中，如果您未捕獲到它，則無法證明它。以下是幾個設定範例，其中含有這些變更以向您說明此運作方式。

以下是WLAN配置。在測試期間，僅更改方法清單中使用的伺服器組。

```
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
!
```

使用預設MTU新增Source-Interface命令

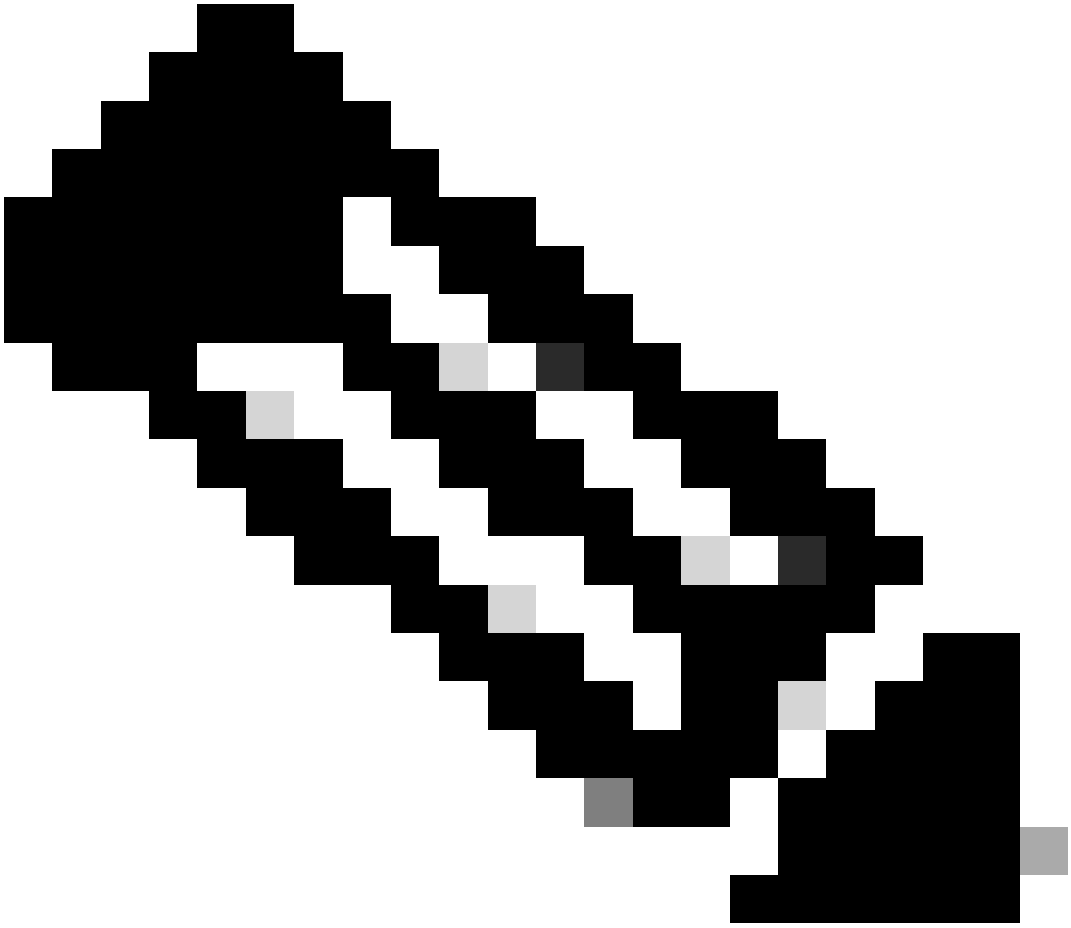
在這裡，它只是指向ISE伺服器的普通伺服器組。新增的源介面命令指向未設定MTU的WMI。以下是配置的外觀。

```
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
```

您可以看到，NoMTU伺服器組已新增到與WLAN關聯的身份驗證方法清單中。ip radius source-interface VLAN260 命令用於此伺服器群組，而VLAN 260未指定MTU，表示其使用的是1500。要確認，MTU為1500，可以使用show run all 命令並在輸出中查詢介面。

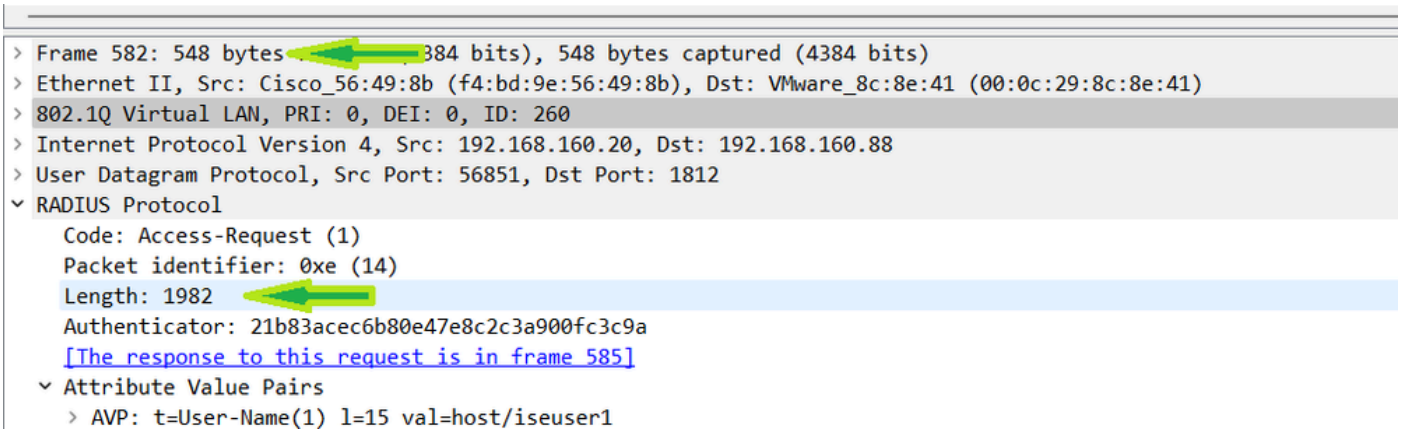
```
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
 no ip clear-dont-fragment
 ip redirects
 ip unreachables
 no ip proxy-arp
 ip mtu 1500
```

現在，檢視一旦WLC新增RADIUS資料，客戶端證書必須傳送到ISE的資料包：



附註：這裡，該行的位元組數為1518。這包括乙太網路負載以外的標頭，例如VLAN標頭和第2層標頭。這些不計入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]
```



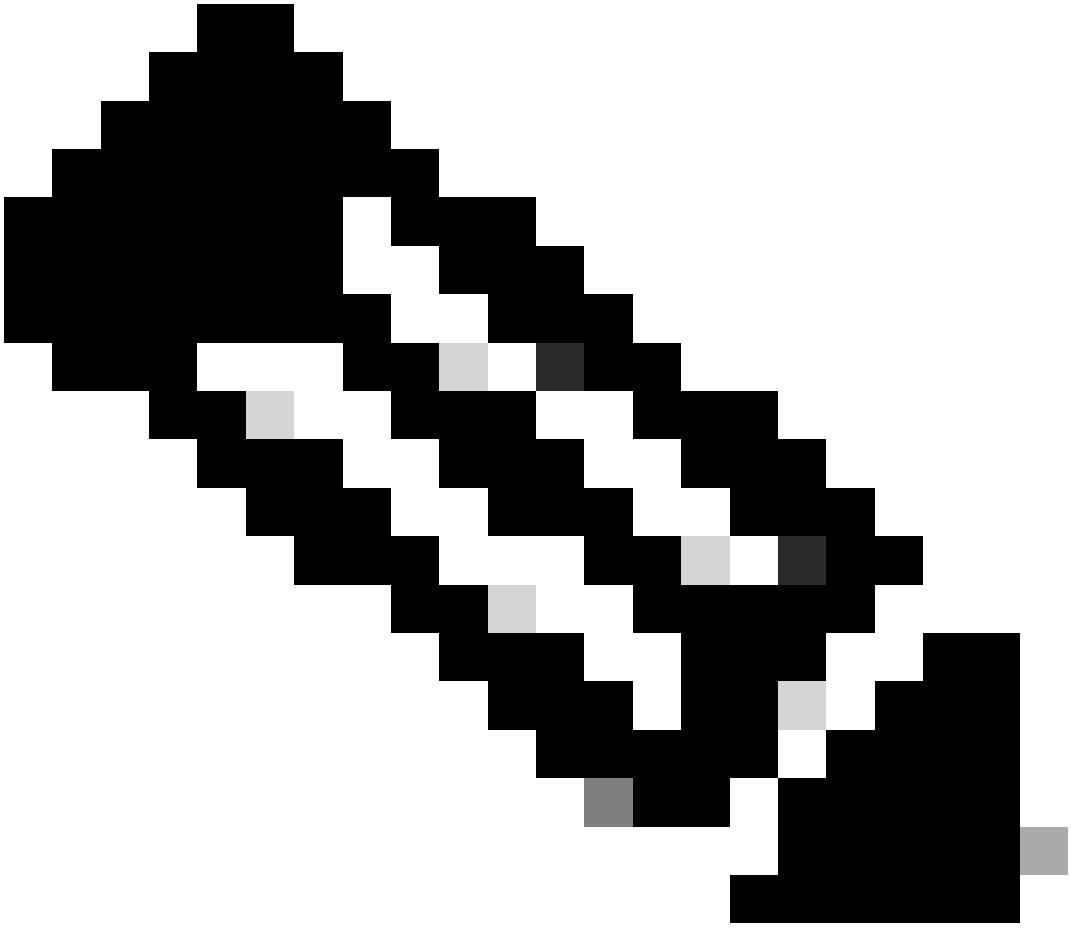
在這裡，您可以看到資料部分在1480進行分段。您可以在WMI上將該片段獲取到1500 MTU下。下一個封包小於550位元組，但您可以看到RADIUS資料的總大小為1982。話雖如此，但使用新MTU進行分段現在能夠正常運作。

使用MTU為1200的非WMI介面

現在，假設您要以較小的MTU進行分段，但不想讓此更改影響任何其他流量。此處沒有問題，配置保持不變，只是源介面配置將指向僅為此目的建立的SVI。更改方法清單以指向此新伺服器組，並且此伺服器組使用的源介面不是我的WMI，並且MTU設定為1200。以下是配置的外觀：

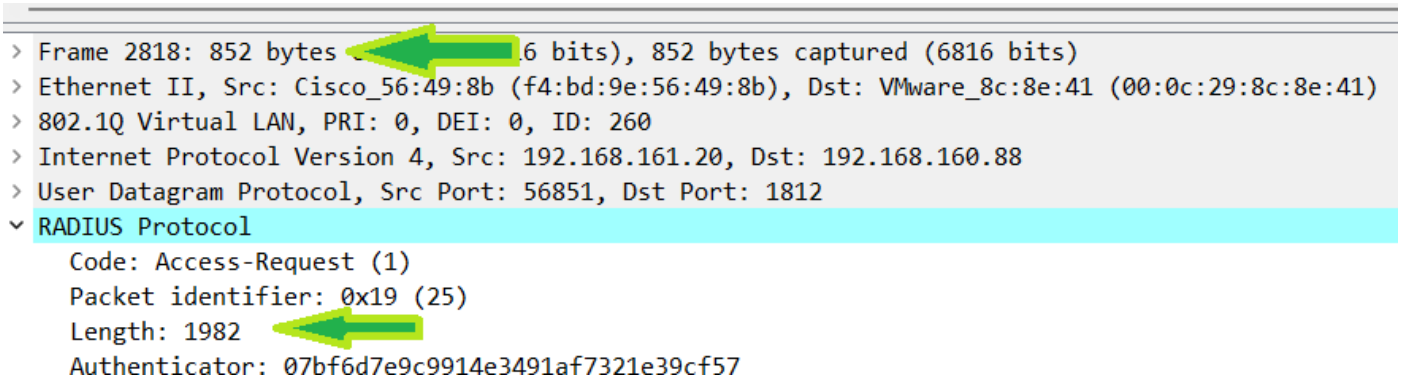
```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group MTU1200
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObFibbBMhNMFAbKUAAB
!
aaa group server radius MTU1200
 server name ISE
 ip radius source-interface Vlan261
 deadtime 5
!
9800#show run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

接下來，看看使用這個較低的MTU時封包的外觀。



附註：降低MTU和更改分段點並不是新行為的一部分。這一直都是事實。如果在1396進行分段的預設行為不適合MTU，則始終會在不同的點進行分段。本部分中的內容只是為了幫助解釋可用的選項。

```
> Frame 2817: 1214 bytes c      2 bits), 1214 bytes captured (9712 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: 192.168.161.20, Dst: 192.168.160.88
v Data (1176 bytes)
    Data: de13071407c6b995011907be07bf6d7e9c9914e3491af7321e39cf57010f686f73742f69…
    [Length: 1176]
```



這裡，RADIUS資料仍為1982位元組，但這一次資料在1176進行分段，而不是在未使用來源介面時本來會在1376進行分段的預設值。請記得，將MTU設定為1500並使用source-interface指令時，您會在1480進行分段。使用此處的設定，可以控制流量到較低的MTU，而不會干擾WLC上的其他流量。

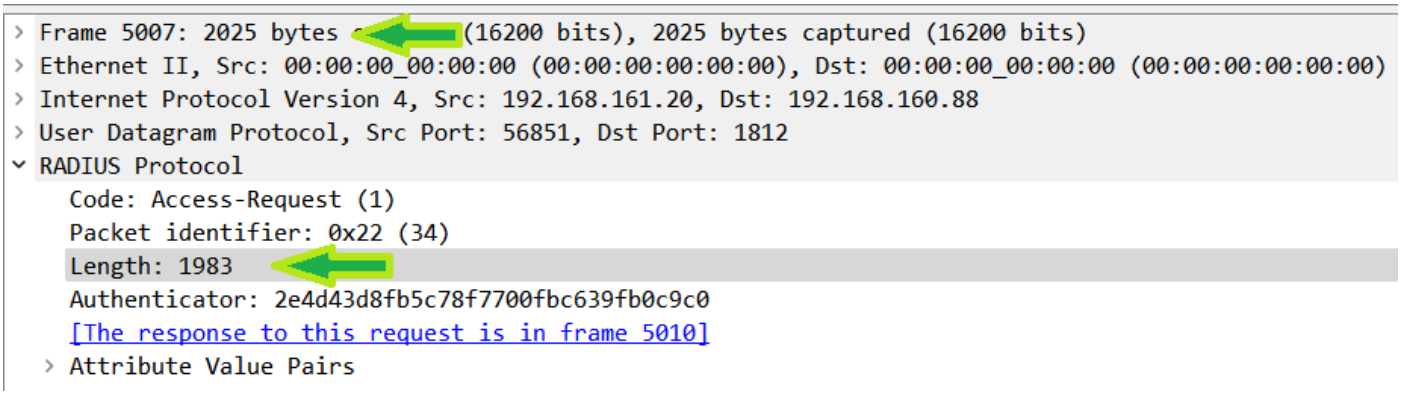
對巨量訊框使用9000的MTU

由於該功能是為傳送巨型幀的選項而設定的，因此如果不測試該功能，並且仍然使用VLAN 261的非WMI介面，將令人感到遺憾。但是，現在的IP MTU設定為9000。一個簡短的註釋，為了能夠在SVI上設定IP MTU，您必須將MTU設定為高於IP MTU的值。您可以在此配置中看到以下內容：

```
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
```

從這裡可以看到，捕獲的資料包從未分段。它以RADIUS資料大小為1983的一個完整資料包傳送。請記住，要使這種方法起作用，網路其餘部分需要配置為允許這樣大小的資料包通過。

此處需要注意的另一點是，客戶端MTU沒有更改，因此客戶端仍然在1492對EAP資料包進行分段。不同之處在於，WLC可以新增將封包傳送到ISE所需的所有RADIUS資料，而無需將使用者端資料分段。



結論

使用EAP-TLS時，客戶端需要將其證書傳送到AAA伺服器。這些憑證通常大於MTU，因此使用者端必須將其分段。客戶端對資料進行分段的點非常接近MTU。由於AP必須新增CAPWAP報頭，因此客戶端傳送的內容必須分段。WLC收到這兩個封包，並將其重新組合在一起，但必須再次分段以新增RADIUS資料。這時，網路管理員會獲得對使用者端傳送的EAP封包的WLC分段方式的部分控制。

如果您將ip radius source-interface <interface you want to use>命令新增到AAA伺服器組，WLC將使用您放在其中的任何介面，而不是（或包括）WMI。使用此命令還可以通知WLC在該介面的MTU而不是預設的1396處進行分段。這樣，您就可以更好地控制資料包在網路中的傳輸方式。

使用Cisco Catalyst Center時，會將source interface命令新增到伺服器組，從而更改預設行為。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。