Comprendre le MTU RADIUS et la fragmentation sur le WLC 9800

Table des matières

Introduction

Ce document décrit comment configurer le MTU des paquets RADIUS que le WLC envoie au serveur RADIUS.

Conditions préalables

Exigences

Cisco recommande que vous ayez une compréhension de base de ces sujets :

- Configuration AAA du contrôleur LAN sans fil (WLC) 9800
- Concepts RADIUS AAA (Authentication, Authorization and Accounting)
- Protocole EAP (Extensible Authentication Protocol)
- Unité de transmission maximale (MTU)

Composants utilisés

- Ingénieur Cisco Identity Service (ISE) 3.2
- Gamme de contrôleurs sans fil Catalyst 9800 (Catalyst 9800-L)
- Cisco IOS® XE 17.15.2
- Client sans fil Windows 11

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Fond

Dans le cadre de ce document, le serveur RADIUS (Remote Authentication Dial-In User Service) utilisé est Cisco ISE. Tout d'abord, il est démontré comment les paquets circuleraient sans aucune intervention extérieure pendant le processus EAP (extensible authentication protocol). Ensuite, il y a l'option de configuration pour changer la taille de la requête d'accès que le WLC envoie à n'importe quel serveur RADIUS. Cette option a été ajoutée dans la version 17.11 d'IOS-XE.

MTU RADIUS 9800

Généralement, le MTU des paquets RADIUS n'a pas d'importance car ils sont généralement petits et n'atteignent pas le MTU de toute façon. Cependant, lorsqu'un côté doit envoyer un certificat, qui est généralement de 2 à 5 Ko, le périphérique doit fragmenter ce certificat pour l'obtenir sous sa MTU.

Lorsque le client doit envoyer un certificat au serveur RADIUS, comme c'est le cas avec la sécurité de la couche de transport EAP (EAP-TLS), il présente au WLC une situation où le paquet doit être fragmenté à nouveau en raison de la quantité de données RADIUS qui doit être envoyée avec lui. Jusqu'à 17.11, l'administrateur réseau avait peu de contrôle sur ce processus, mais maintenant les ingénieurs ont la possibilité de manipuler la taille de la demande d'accès envoyée par le WLC.

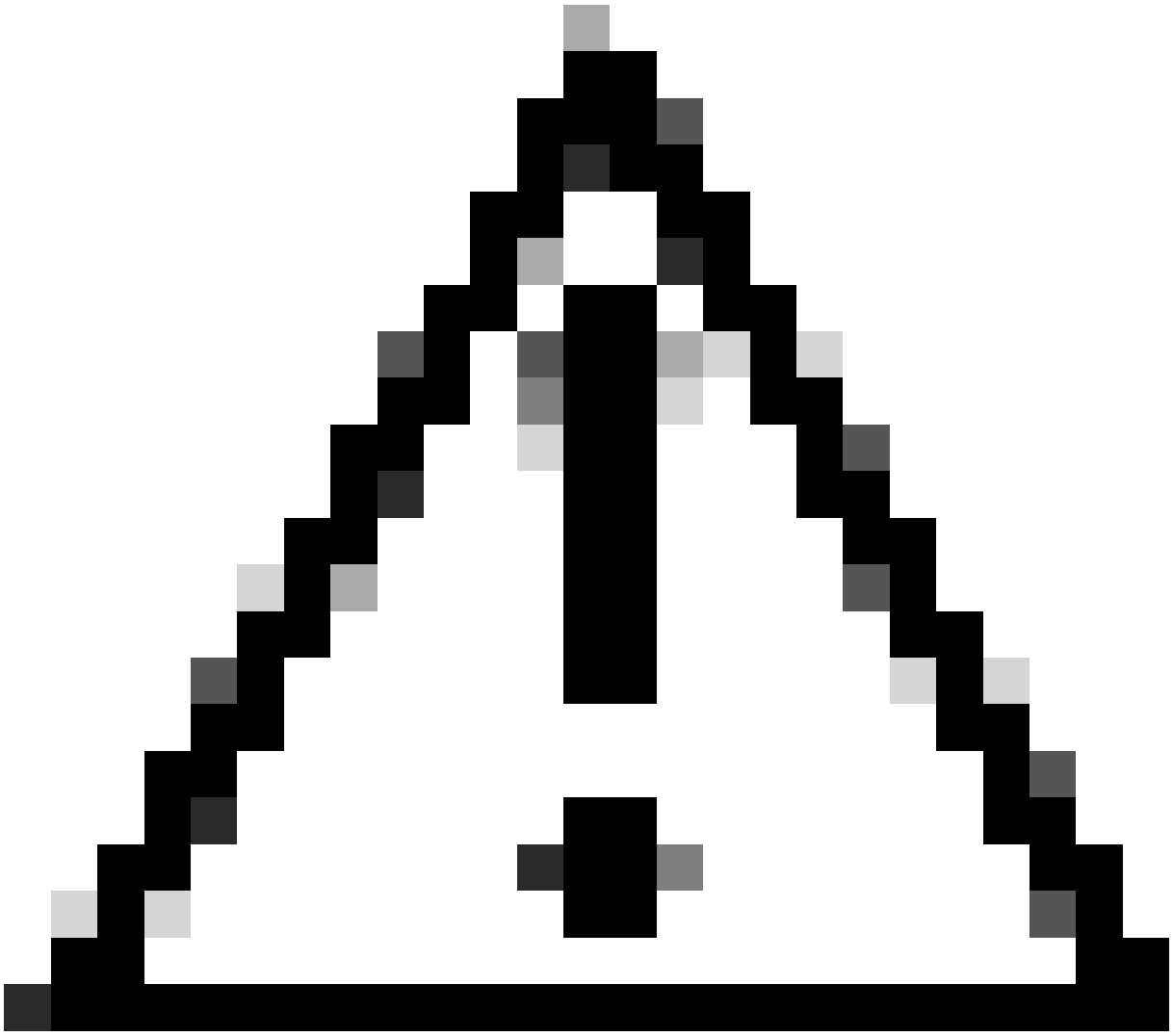
Flux de paquets EAP-TLS

Il s'agit d'une étude approfondie de l'aspect des paquets et de la manière dont ils sont traités par l'infrastructure sans fil. Pour que les modifications présentées dans ce document soient parfaitement comprises, il est important de connaître le flux des paquets pendant le processus d'authentification sans fil lors de l'utilisation de dot1x et plus particulièrement d'EAP-TLS.

Si vous avez déjà une compréhension approfondie de la façon dont le flux de paquets EAP et RADIUS fonctionne avec dans l'infrastructure sans fil Cisco, passez à la section de changement de comportement qui explique ce qui a été ajouté dans 17.11, donnant aux administrateurs réseau plus de contrôle sur le MTU RADIUS. Tout d'abord, examinez l'identification EAP (EAP-ID).

EAP-ID

L'EAP-ID est initié par l'authentificateur, dans ce cas le WLC. Il doit s'agir de la première partie du processus du PAE. Parfois, le client sans fil envoie un EAPOL-Start. Cela signifie normalement que le client n'a jamais reçu la requête EAP-ID ou qu'il veut recommencer.



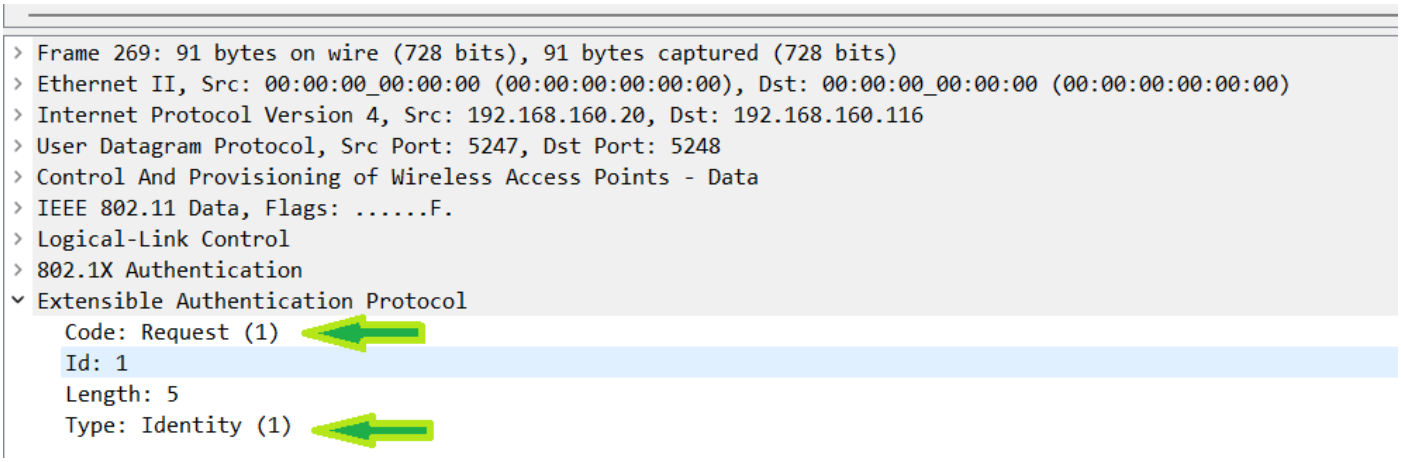
Mise en garde : Il existe une différence entre le paquet EAP-ID et l'ID de paquet EAP. Le paquet EAP-ID est utilisé pour identifier le demandeur où l'ID de paquet EAP est un numéro utilisé pour suivre le paquet spécifique lorsqu'il se déplace sur le réseau.

Demande EAP-ID

Tout d'abord, le périphérique client sans fil se connecte au réseau en utilisant le processus d'association normal. Lorsque le réseau local sans fil (WLAN) est configuré pour dot1x, le WLC doit d'abord savoir qui est le client avant de pouvoir demander l'accès au serveur RADIUS. Pour trouver ces informations, le WLC envoie la requête client et EAP-ID.

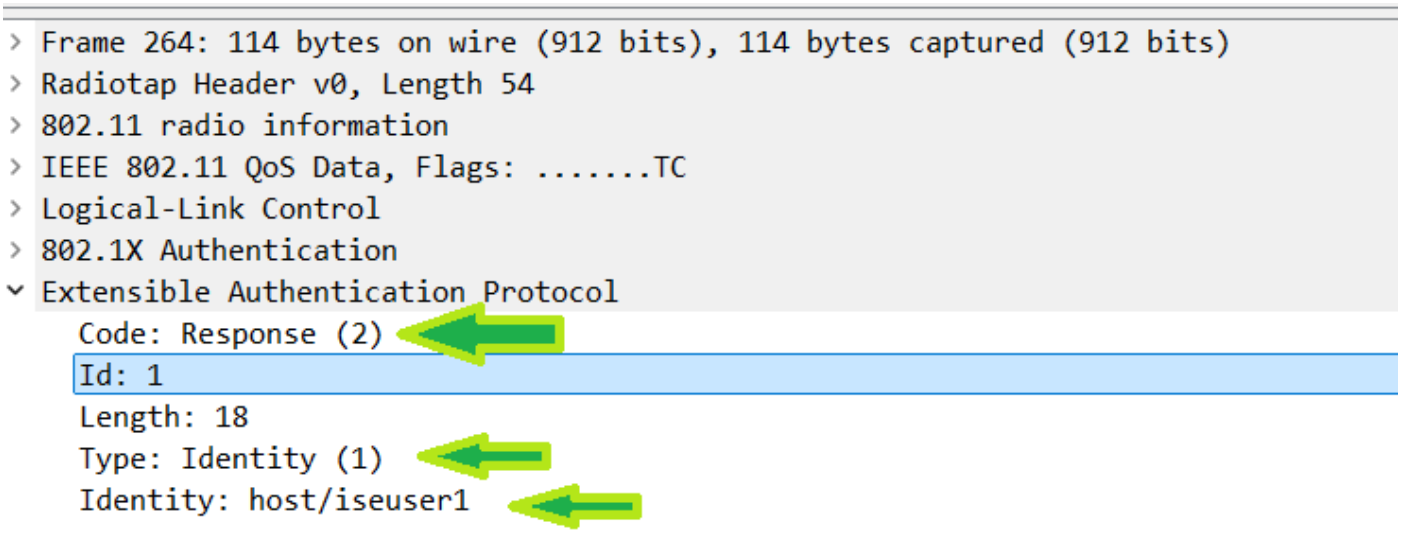
Le client est censé répondre avec la réponse EAP-ID. Cela donne au WLC ce dont il a besoin pour pouvoir construire la requête d'accès et l'envoyer à l'ISE. La requête EAP-ID est une requête qui demande au client d'entrer son nom d'utilisateur et son mot de passe dans une authentification PEAP normale.

Cependant, cette discussion porte sur EAP-TLS, de sorte que la réponse EAP-ID ne contienne que l'ID utilisateur. Dans la démonstration, l'ID d'utilisateur est iseuser1. Dans ce paquet, vous pouvez voir la requête EAP-ID que le WLC envoie au client sans fil en lui demandant qui ils sont. Puisqu'il s'agit d'un client sans fil, le WLC encapsule la requête dans CAPWAP et l'envoie au point d'accès (AP) pour être envoyé par voie hertzienne. Dans les données EAP, le code 1 signifie qu'il s'agit d'une requête et le type 1 signifie qu'il s'agit de l'identité.



Réponse EAP-ID

Ensuite, le client sans fil doit répondre avec la réponse EAP-ID. Dans les données EAP, le code est passé à 2, ce qui signifie qu'il s'agit d'une réponse, mais le type reste 1, ce qui indique toujours qu'il s'agit de l'identité. Ici, vous pouvez même voir le nom d'utilisateur que le client utilise. Une autre chose à vérifier sur ces paquets est le numéro d'ID du paquet EAP. Pour l'échange EAP-ID, il est toujours 1, mais ce nombre change par la suite en autre chose une fois qu'ISE est impliqué.



Vous pouvez voir que les deux paquets sont plutôt petits, de sorte que la MTU n'a pas d'incidence ici puisqu'elle est bien inférieure aux 1500 octets utilisés dans le réseau.

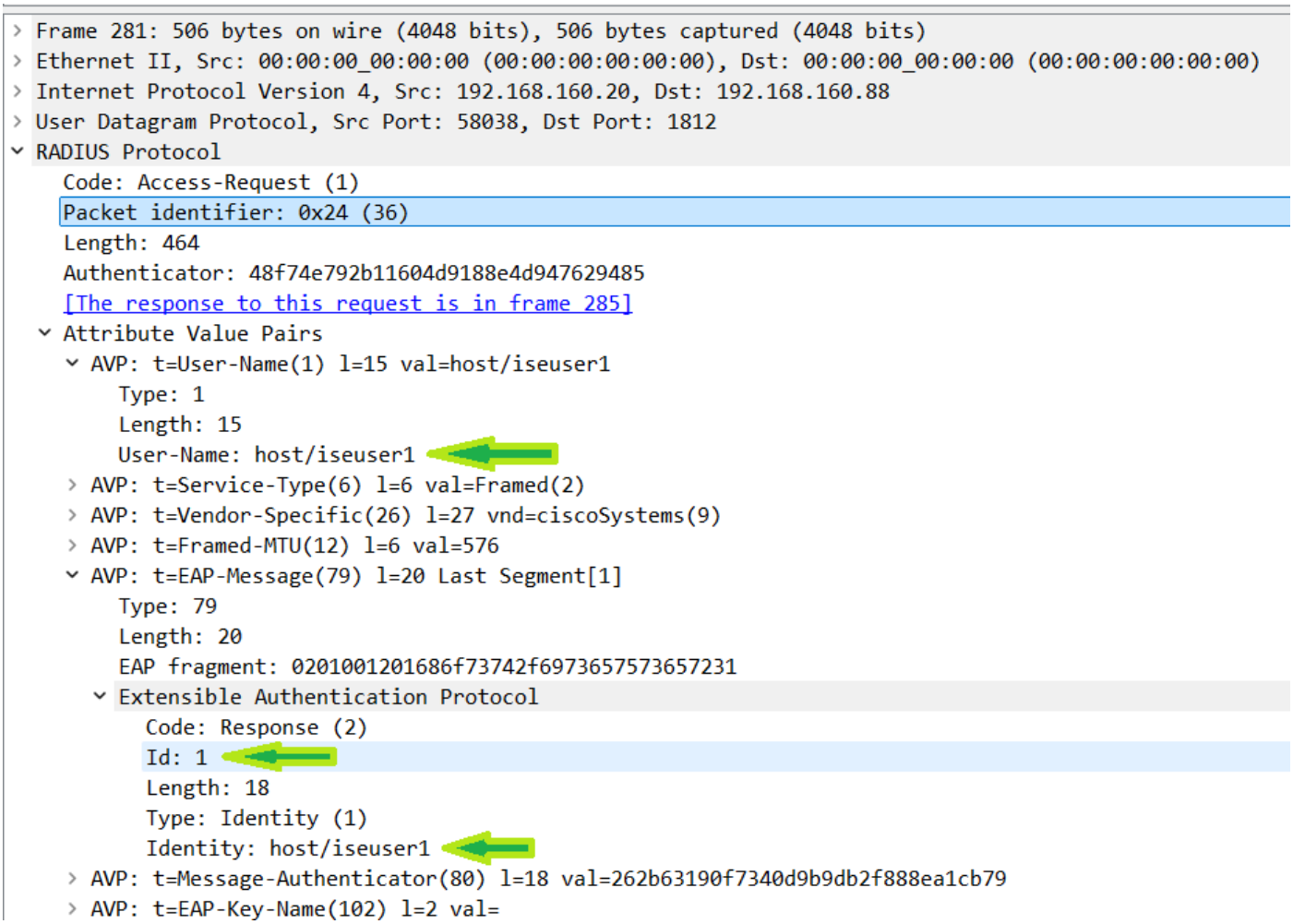
Access-Request et Access-Challenge

La communication avec le client est EAP et la communication entre le WLC et ISE est RADIUS. Pour la communication RADIUS, les paquets access-request et access-challenge sont utilisés. Le WLC reçoit le paquet EAP du demandeur et le transfère à ISE à l'aide de la requête d'accès RADIUS. Dans un réseau opérationnel, ISE répond par un défi d'accès.

Access-Request

Maintenant que le WLC connaît l'identité du client, il doit demander au serveur RADIUS si ce client est autorisé sur le réseau. Pour ce faire, le WLC demande l'accès pour ce client en envoyant le paquet de demande d'accès. Il y a d'autres parties de données que le WLC va envoyer avec les données EAP. Collectivement, elles sont appelées paires de valeurs d'attribut, AVP ou paires AV selon qui parle.

Ce document n'ira pas loin dans les PAV, car il n'entre pas dans le cadre de cette discussion. Ici, vous devez juste voir que le nom d'utilisateur (données EAP) est inclus et envoyé au serveur RADIUS, qui, dans ce cas, est ISE. En outre, vous pouvez voir que le numéro EAP-ID 1 est également envoyé à ISE. Souvenez-vous que lorsque vous avez regardé l'ID de paquet EAP par voie hertzienne, il y avait également 1. La dernière chose importante à noter ici est que puisque le WLC a ajouté tous ces AVP, le paquet de 114 octets envoyé par le client est maintenant transformé en un paquet de 488 octets avant d'être envoyé à ISE.

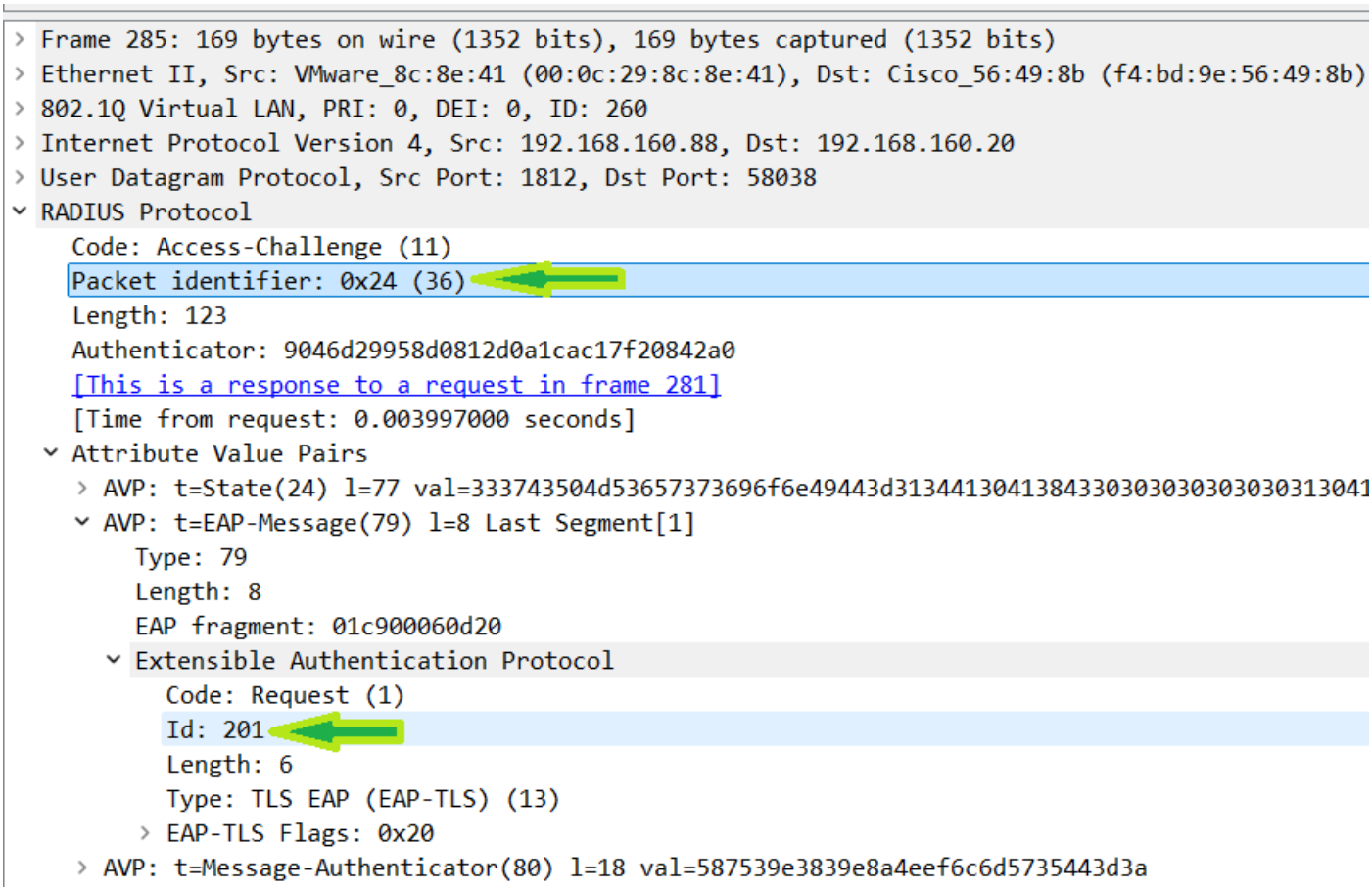


Confirmation d'accès

En supposant qu'ISE reçoive la demande d'accès et décide de répondre, cette réponse doit provenir d'ISE en tant que défi d'accès. En regardant en arrière à la requête d'accès, vous verriez l'ID de paquet RADIUS de 36 avant que les AVP ne commencent.

Lorsque le WLC reçoit la demande d'accès, l'ID RADIUS doit correspondre à l'ID de paquet de la demande d'accès. L'ID de paquet RADIUS correspond à la communication RADIUS entre ISE et le WLC. Vous pouvez également voir dans ce paquet que l'ISE a défini un nouvel ID EAP de 201 qui est utilisé pour suivre la communication entre l'ISE et le client. À ce stade, le WLC n'est qu'un passage pour la communication entre ISE et le client.

Il est important de noter tous ces ID de paquets ici afin de comprendre le flux de communication et la façon de suivre ces paquets sur le réseau. Dans un environnement de production, il y a généralement plusieurs authentifications simultanées. Utilisez la commande calling-station-id pour faire correspondre le paquet à l'adresse MAC du client. Ensuite, vous pouvez utiliser l'ID de paquet RADIUS et l'ID de paquet EAP pour suivre le flux de paquets pour ce client spécifique. Jusqu'à présent, aucune des parties n'a envoyé de certificats, il n'y a donc toujours pas lieu de s'inquiéter de la MTU.



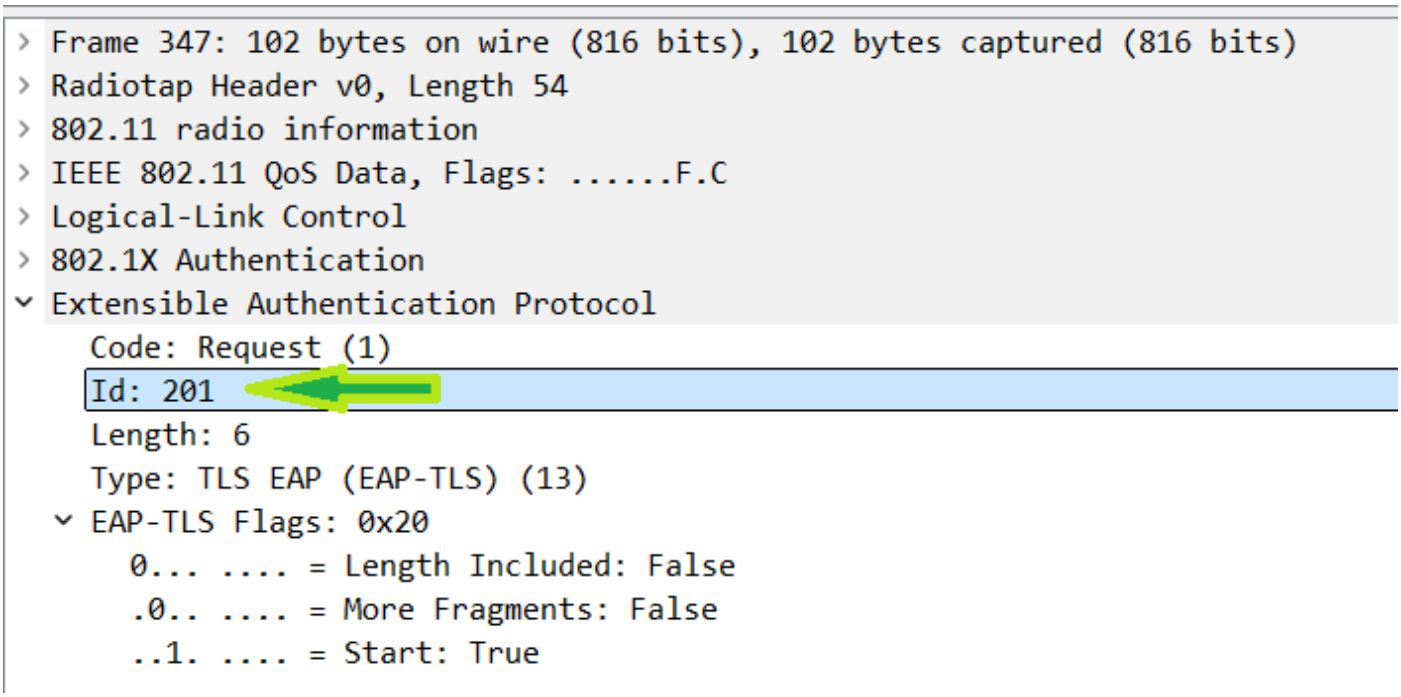
Requête EAP et réponse EAP

Pour rappel, le client parle EAP et non RADIUS. Cela dit, quand le WLC reçoit la demande d'accès, il doit supprimer les données RADIUS et retirer la demande EAP afin qu'elle puisse être envoyée au client.

Demande EAP

Cela doit ressembler exactement à ce qu'il a fait à l'intérieur du défi d'accès quand le WLC l'a reçu. Cependant, tous les éléments RADIUS ont été supprimés et seule la partie EAP est envoyée au client.

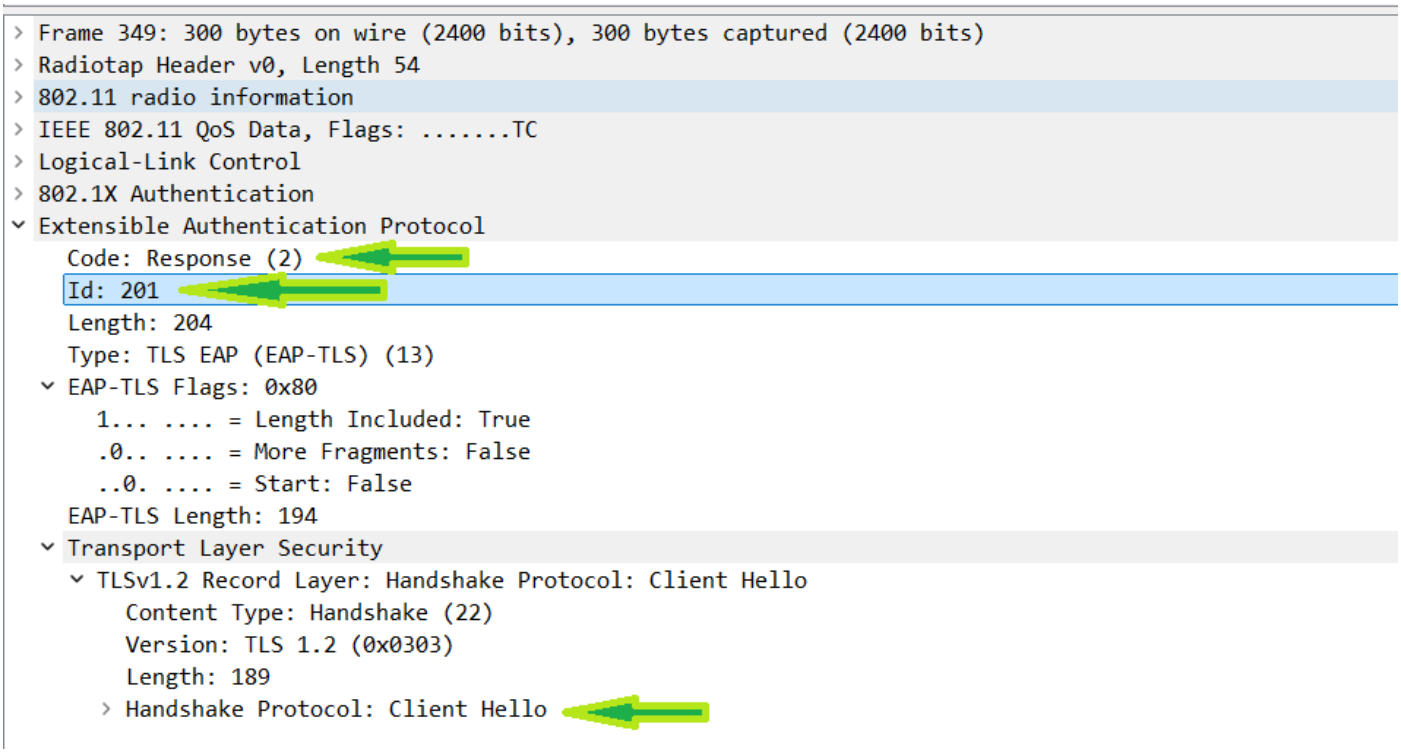
Vous pouvez toujours voir l'ID de paquet EAP de 201 ici exactement comme il était dans le défi d'accès parce que c'est les mêmes données que le WLC a reçu d'ISE. Le flux ici est le même qu'avec l'EAP-ID, seulement maintenant il ne vient pas du WLC et il est utilisé pour établir la méthode EAP. Ce paquet est encore assez petit parce qu'il est juste pour établir le début d'une session EAP-TLS.



Réponse EAP

Lorsque le client reçoit la requête EAP, il doit répondre par une réponse EAP. Dans la réponse EAP, le client commence à établir la session TLS. Cela ressemble à ce qu'il serait dans n'importe quelle autre situation où TLS est utilisé. Il commence par le message « client hello ». Ce document ne va pas creuser dans ce qui va dans le bonjour du client car il n'est pas pertinent pour ce sujet. Ce que vous devez remarquer ici est juste qu'une session TLS est en cours de configuration.

Vous pouvez voir les données dans les paquets ici comme vous le feriez avec n'importe quelle autre configuration TLS. Tout comme avec la réponse EAP-ID, ce paquet atteint le WLC et est converti en requête d'accès. ISE répond avec une requête EAP incluse dans un défi d'accès. C'est toujours le même courant à partir de maintenant.



Certificats TLS

Voici le point où vous allez voir la taille de paquet augmenter. Les certificats peuvent être assez volumineux en fonction de la présence d'une ou de plusieurs autorités de certification intermédiaires. S'il s'agit d'un certificat auto-signé, il serait évidemment plus petit qu'un certificat avec un certificat de périphérique enchaîné à 2 CA intermédiaires et une CA racine. Dans les deux cas, le propriétaire du certificat commence normalement à fragmenter ses propres paquets ici.

Certificat ISE

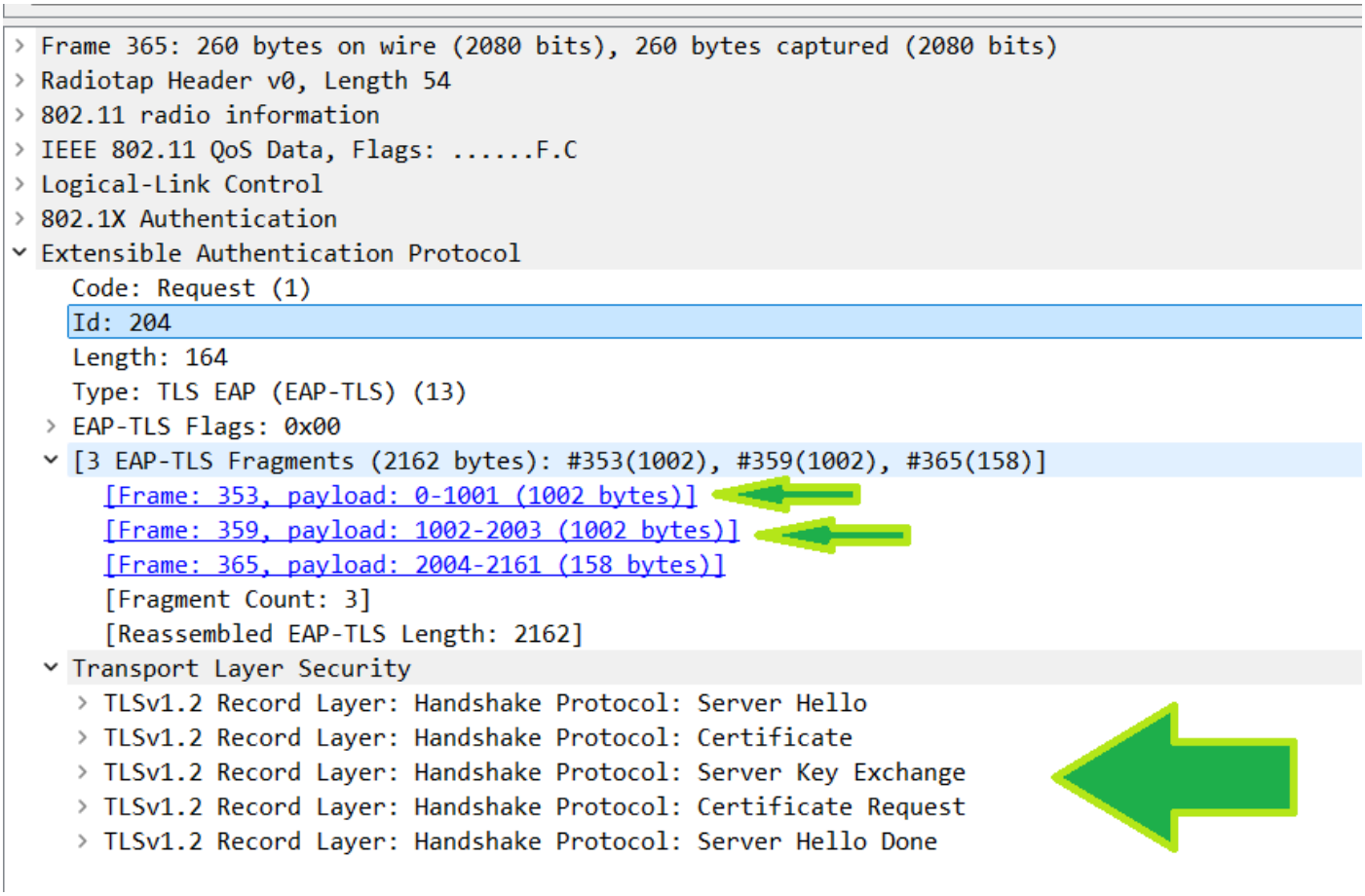
Maintenant qu'ISE a reçu le bonjour du client TLS, il répond avec une autre requête EAP. Dans cette nouvelle requête EAP, ISE envoie simultanément le message « server hello », son certificat, l'« échange de clés de serveur », la « certificate request » et les messages « server hello done ». S'il envoyait tout cela en un seul paquet, le paquet passerait par le MTU pour le réseau. Ainsi, ISE fragmente le paquet lui-même pour l'obtenir sous la MTU. Avec ISE, il fragmente la partie données du paquet de sorte qu'elle ne dépasse pas 1 002 octets dans l'espoir d'éviter une double fragmentation.

Qu'entend-on par double fragmentation ? La première fragmentation se produit sur ISE, car les données qu'il veut envoyer sont trop volumineuses pour tenir dans la MTU du réseau. Cependant, il peut y avoir d'autres endroits sur le réseau où, même si la MTU est la même, en raison de la façon dont le réseau est configuré, un périphérique doit peut-être fragmenter le paquet afin qu'il ajoute ses en-têtes et reste sous la MTU. Cela peut être vrai même si le bit ne pas fragmenter est vérifié.

Un bon exemple en est un tunnel VPN, ou n'importe quel tunnel d'ailleurs. Pour placer des données dans un tunnel VPN, les routeurs VPN doivent ajouter leurs en-têtes au trafic. Si ce trafic

RADIUS était fragmenté au niveau de la MTU ou à proximité de celle-ci, il n'y aurait aucun moyen de conserver les données sous la MTU et d'ajouter des en-têtes supplémentaires lorsqu'il s'agit de ce VPN. Ceci est vrai aussi pour les tunnels CAPWAP que vous pouvez voir un peu plus tard.

Ainsi, pour éviter que ces paquets ne se retrouvent dans une situation où un autre périphérique peut les fragmenter à nouveau, ISE fragmente le paquet à un endroit où cela peut être évité dans la plupart des réseaux. Cela signifie qu'ISE envoie ces données dans plusieurs requêtes EAP en attente d'une réponse EAP vide à chaque fois. L'ID EAP augmente avec chaque fragment envoyé. Du point de vue du WLC, il s'agirait d'un défi d'accès et d'un échange de demande d'accès pour chaque fragment et l'ID de paquet RADIUS augmenterait avec chaque fragment envoyé.



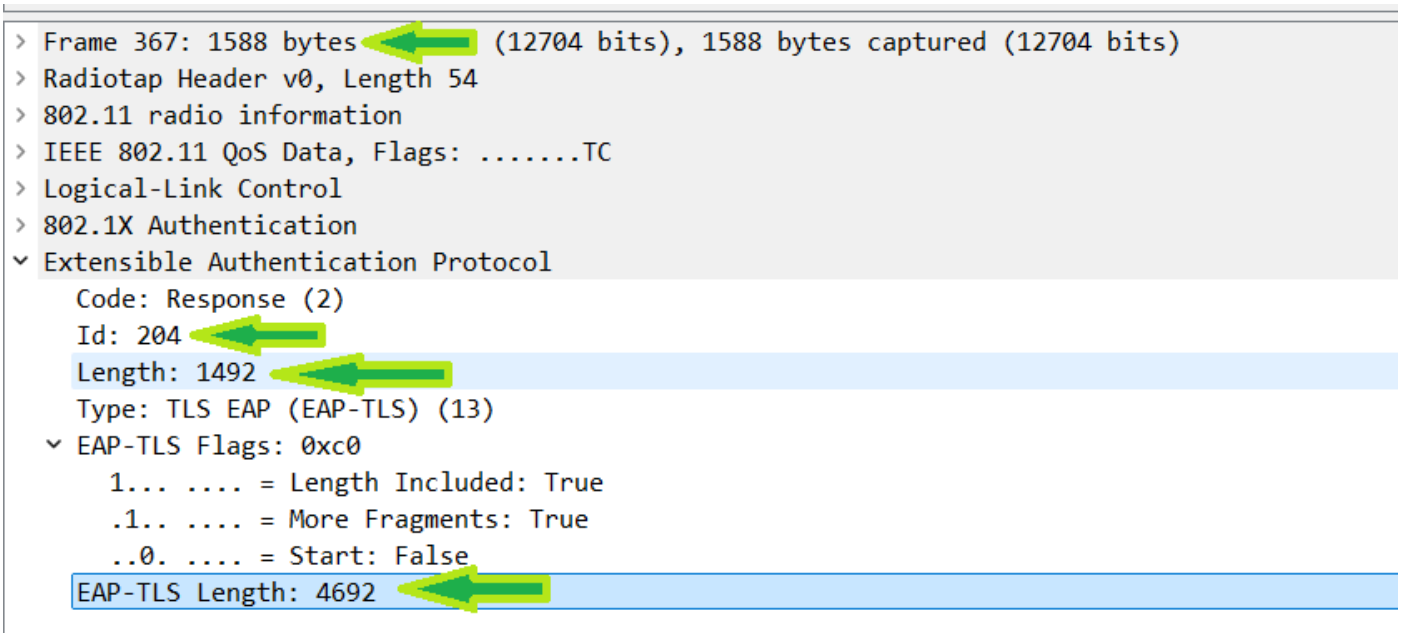
certificat client

Une fois qu'ISE envoie tous les fragments et qu'ils sont réassemblés par le client, le flux de paquets passe au client pour envoyer quelque chose. Dans TLS, il est prévu que le client envoie son propre certificat à ce stade afin de terminer l'authentification. C'est là que les choses deviennent plus complexes. Tout comme ISE, le client va envoyer plusieurs parties TLS en même temps, l'une d'entre elles étant son certificat.

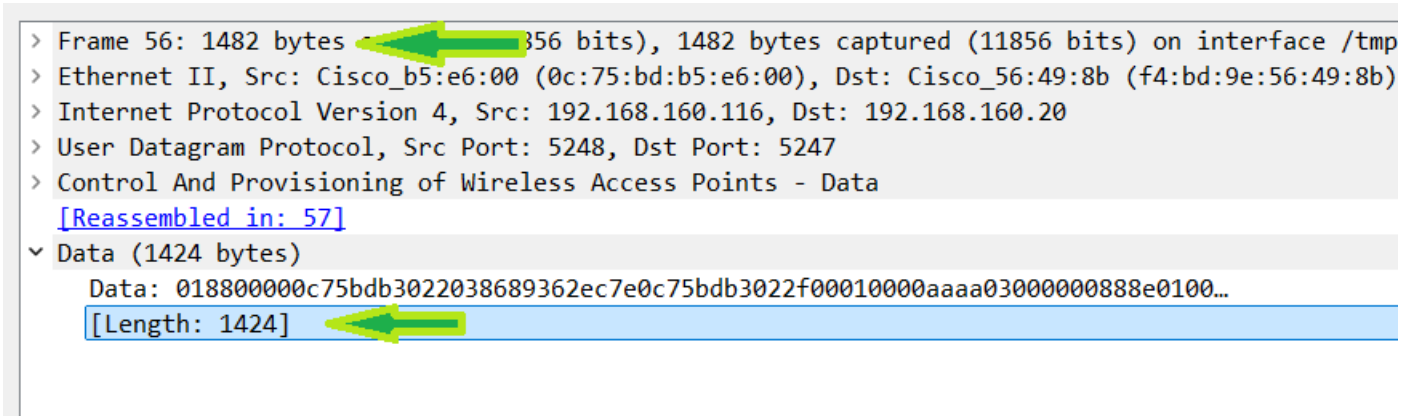
Contrairement à ce qui a été observé avec ISE, la plupart des clients envoient leurs données EAP juste en dessous de la MTU. Dans cette démonstration, les données 802.1x sont 1492. Le problème avec cela est que l'AP doit ajouter les en-têtes CAPWAP afin qu'il puisse être envoyé au WLC.

Comment cela peut-il être fait ? L'AP va devoir fragmenter le paquet pour qu'il puisse ajouter les en-têtes et l'envoyer au WLC. Il n'y a aucun moyen pour l'AP d'obtenir le paquet au WLC sans le fragmenter. Cela dit, ici, le paquet est doublement fragmenté, d'abord à partir du client, puis à nouveau à partir du point d'accès. Cependant, cette fragmentation n'est généralement pas un problème, comme on peut s'y attendre avec CAPWAP.

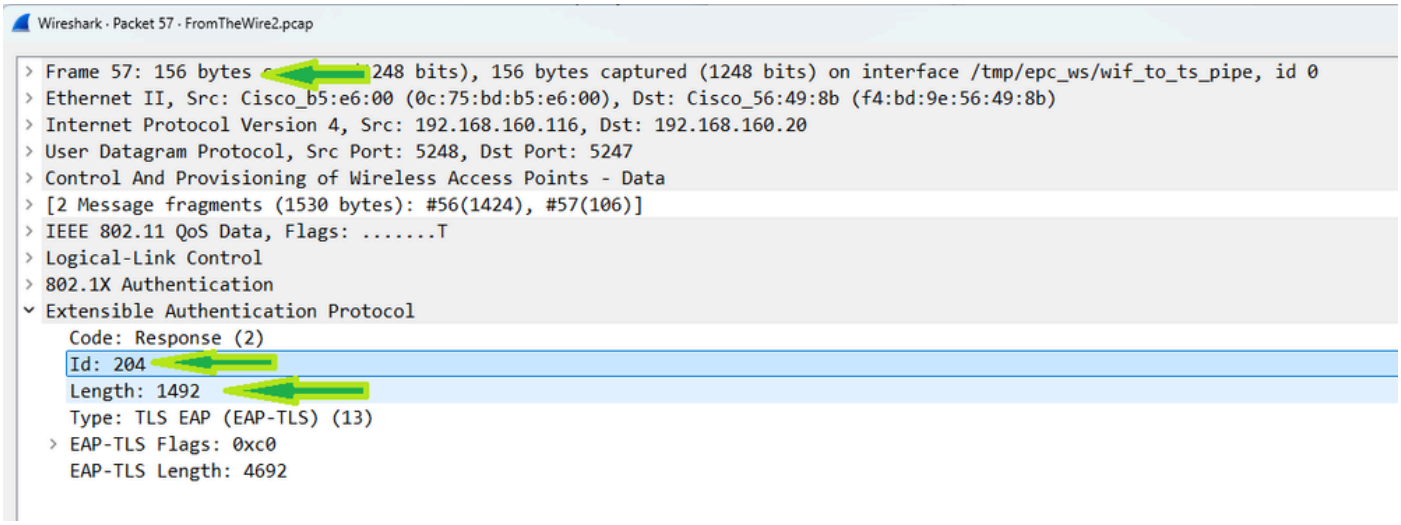
Le paquet transmis par voie aérienne :



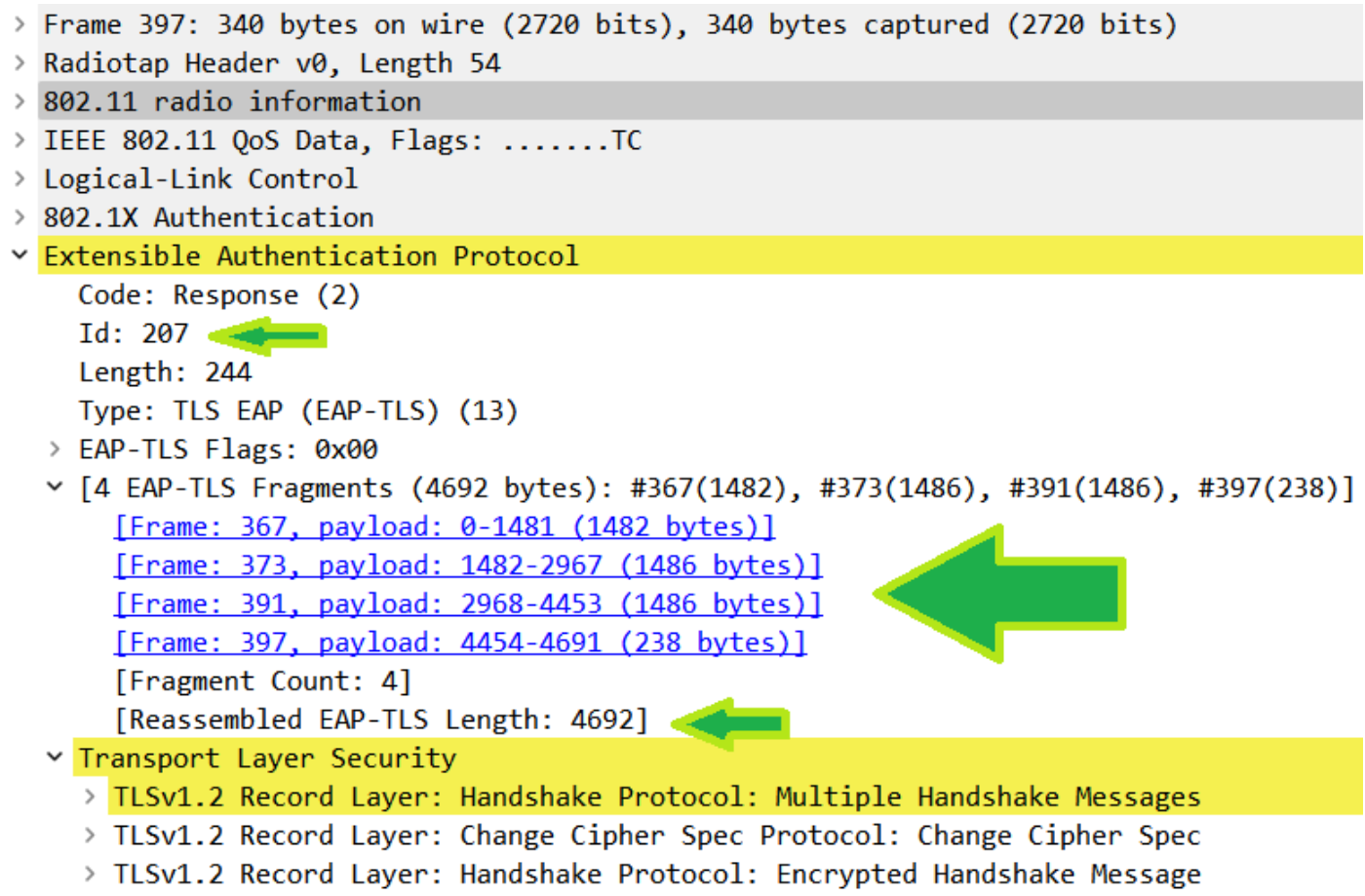
Fragment de paquet sur le fil :



Le paquet réassemblé sur le câble :



Tous les fragments de clients réassemblés par liaison radio :



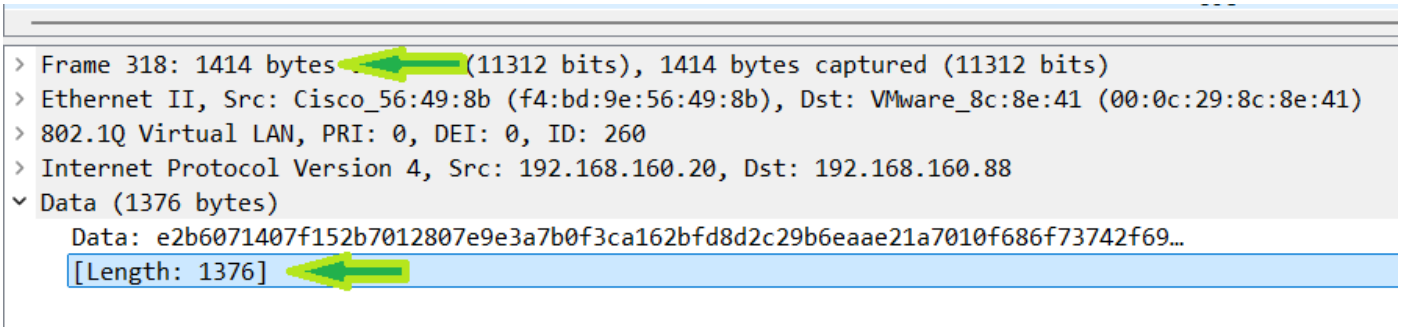
Certificat client au niveau du WLC

Le WLC reçoit les deux fragments CAPWAP et les réassemble pour avoir le paquet entier de 1492 octets du client, en restaurant le paquet - mais pas pour longtemps. Cette restauration est de courte durée car, si vous regardez comment le WLC envoie la requête d'accès, vous devez vous rappeler qu'il doit ajouter environ 400 octets de AVP RADIUS au paquet avant de pouvoir envoyer les données à ISE.

Pour des calculs simples, supposons que le WLC ajoute 408 octets, ce qui porte la taille totale du paquet à 1900. C'est bien au-dessus de la MTU 1500 donc que va faire le WLC ? Fragmentez à nouveau le paquet.

À ce stade, le WLC va fragmenter le paquet à 1396 par défaut. L'idée est la même qu'avec ISE. L'objectif est de rendre le paquet suffisamment petit pour que s'il doit passer par un autre tunnel, il n'ait pas besoin d'être fragmenté à nouveau pour ajouter les en-têtes. Cependant, le WLC n'est pas aussi prudent que l'ISE donc 1396 est assez bon ici.

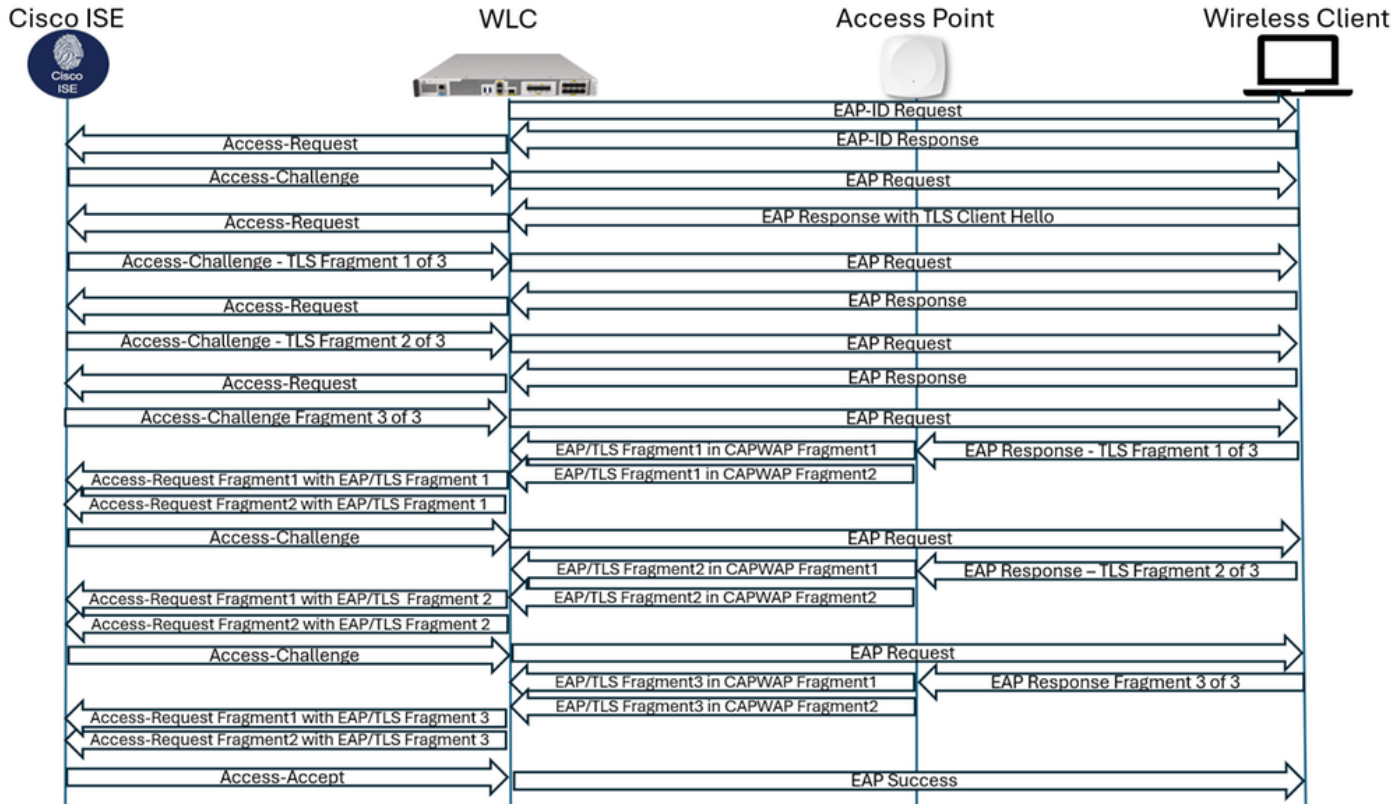
Le paquet fragmenté quittant le WLC :



```
> Frame 319: 695 bytes (5560 bits), 695 bytes captured (5560 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
> User Datagram Protocol, Src Port: 58038, Dst Port: 1812
v RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x28 (40)
    Length: 2025
    Authenticator: e3a7b0f3ca162bfd8d2c29b6eaae21a7
    [The response to this request is in frame 322]
  v Attribute Value Pairs
    > AVP: t=User-Name(1) l=15 val=host/iseuser1
    > AVP: t=Service-Type(6) l=6 val=Framed(2)
    > AVP: t=Vendor-Specific(26) l=27 vnd=ciscoSystems(9)
    > AVP: t=Framed-MTU(12) l=6 val=576
    > AVP: t=EAP-Message(79) l=255 Segment[1]
    > AVP: t=EAP-Message(79) l=255 Segment[2]
    > AVP: t=EAP-Message(79) l=255 Segment[3]
    > AVP: t=EAP-Message(79) l=255 Segment[4]
    > AVP: t=EAP-Message(79) l=255 Segment[5]
    v AVP: t=EAP-Message(79) l=229 Last Segment[6]
        Type: 79
        Length: 229
        EAP fragment: 8bc4be38a7487cb8dcaf6e1664bb495f72cf96e0c91b6c40c64ec67de3fcdaf15cb73989…
      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
    > AVP: t=Message-Authenticator(80) l=18 val=ffcd8b97d2d366fd9d995043bfe27607
    > AVP: t=EAP-Key-Name(102) l=2 val=
    > AVP: t=Vendor-Specific(26) l=49 vnd=ciscoSystems(9)
```

Flux de paquets TL;DR

Lorsque ISE envoie son certificat, il fragmente les paquets TLS à 1002 octets. Pas de problème. Lorsque les clients envoient leur certificat, ils se fragmentent généralement à proximité de la MTU. Puisque le point d'accès doit ajouter les en-têtes CAPWAP au paquet, il doit fragmenter ce paquet également. Une fois que le WLC reçoit les fragments, il doit réassembler le paquet, mais il doit ensuite ajouter les AVP RADIUS afin que le paquet soit à nouveau fragmenté. Le flux de paquets ressemble à ceci :



Changement de comportement RADIUS MTU

Lorsque vous examinez le flux de paquets pour n'importe quel trafic de données client sans fil, vous pouvez constater que l'infrastructure sans fil n'a d'influence sur celui-ci qu'à quelques endroits. Le premier endroit est quand le trafic quitte le point d'accès et le second endroit est quand le trafic quitte le WLC. L'exception est le trafic TCP, où l'infrastructure sans fil peut ajuster la MSS du client. Cependant, EAP ne fait pas partie de TCP, en fait, c'est son propre protocole.

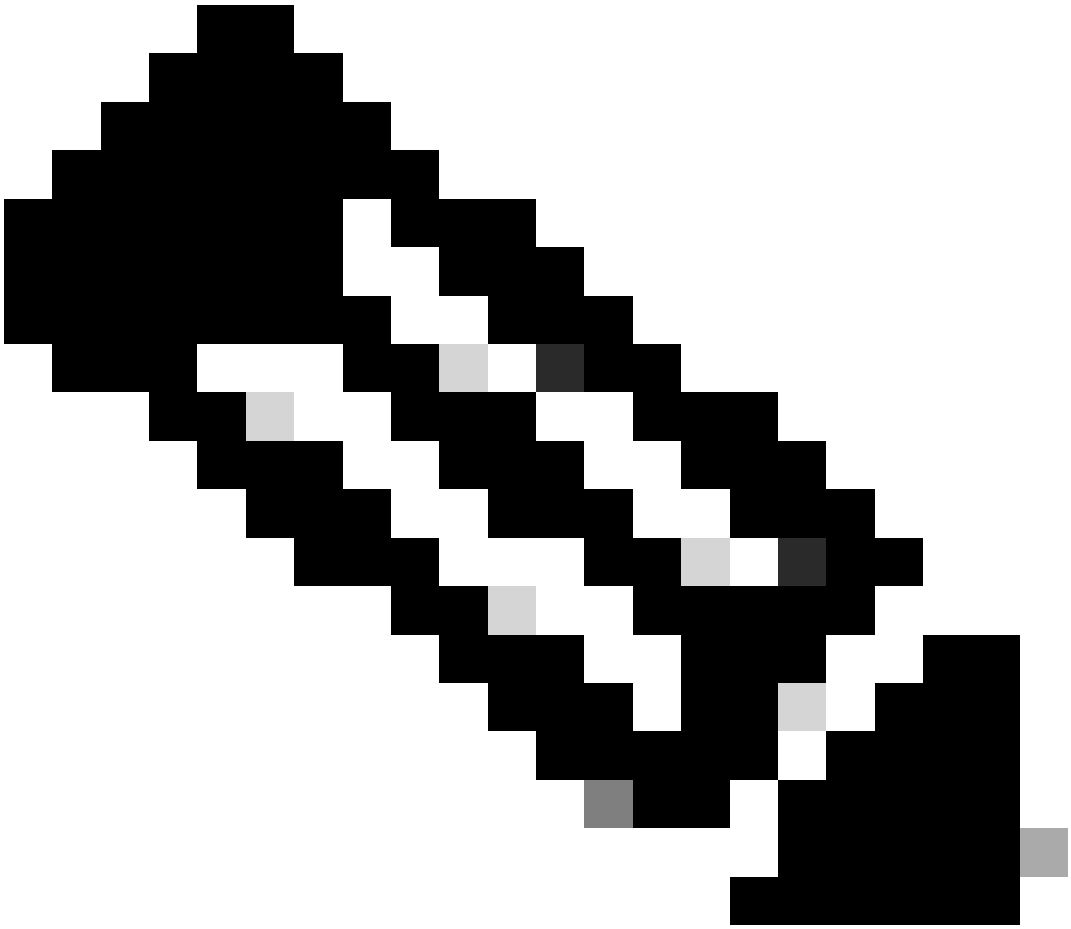
Lorsque vous examinez les flux de trafic EAP et RADIUS, vous pouvez également voir que le réseau influence en fait la taille du trafic à la fois au niveau de l'AP et du WLC lorsque la taille de paquet d'origine se rapproche trop de la MTU. Avec une bonne compréhension du rôle du WLC dans cet échange, vous pouvez voir qu'il n'y a vraiment qu'un seul endroit où il a une influence de la taille du paquet RADIUS. Cela se produit lorsqu'une réponse EAP arrive et que vous la changez en requête d'accès RADIUS.

Éléments modifiés

Si la réponse EAP est sur le MTU, une fois que vous ajoutez les AVP RADIUS, vous devez le fragmenter. Puisque vous devez déjà fragmenter ce paquet quoi qu'il arrive, vous pouvez au moins décider à quelle taille vous voulez le fragmenter. C'est là que le changement de comportement introduit dans 17.11 intervient.

Dans la demande de fonctionnalité suivie dans l'ID de bogue Cisco CSCwc81849, vous voulez ajouter la prise en charge des paquets Jumbo RADIUS. Pour ce faire, le paquet RADIUS n’a plus été automatiquement fragmenté à 1396. Maintenant, si vous ajoutez la commande ip radius source-interface <interface X>, la requête d'accès RADIUS est envoyée à la MTU de cette

interface.

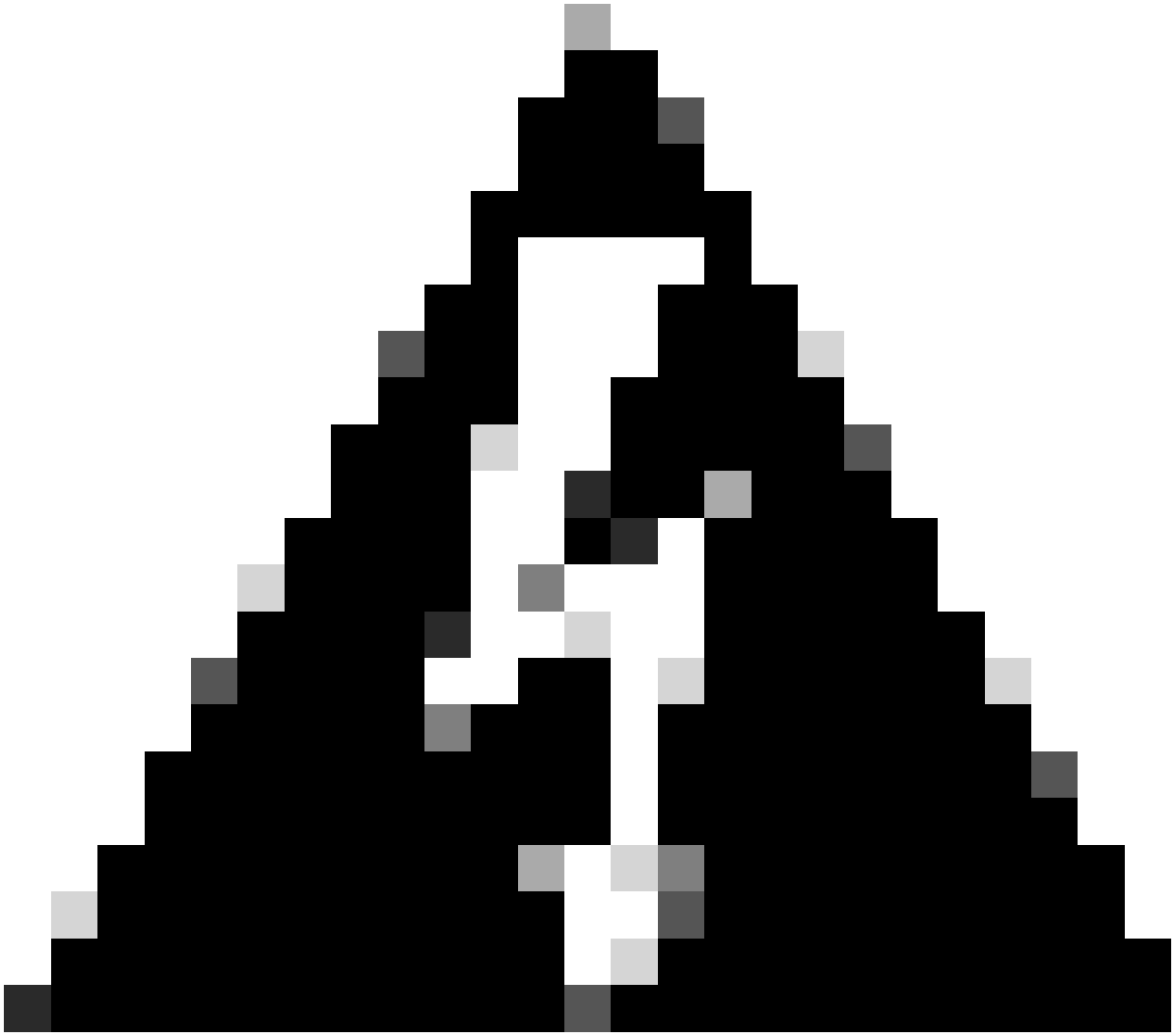


> Remarque : Si vous utilisez Cisco Catalyst Center, lorsque vous provisionnez des configurations AAA, il ajoute automatiquement l'interface source au groupe de serveurs. Cela modifie le comportement par défaut pour fragmenter à la taille MTU de l'interface utilisée dans cette commande.

Comment ce changement peut-il être utilisé ?

Puisque le MTU par défaut de toutes vos interfaces serait 1500, ce serait le nouveau MTU à fragmenter. L'interface par défaut utilisée pour tout le trafic RADIUS est l'interface de gestion sans fil (WMI). Lorsque vous examinez la configuration de votre groupe de serveurs, s'il n'y a aucune interface source spécifiée, le WLC envoie le trafic RADIUS à 1396 en utilisant le WMI. Cependant, si vous accédez à la configuration du groupe de serveurs et que vous lui dites que l'interface source est l'interface WMI, le WLC envoie maintenant le trafic RADIUS à 1500 toujours en utilisant l'interface WMI.

Maintenant, supposons qu'il y ait un périphérique dans le réseau comme le VPN mentionné précédemment. Vous ne voulez pas que le trafic soit fragmenté deux fois pour pouvoir changer la MTU de l'interface en quelque chose de plus petit afin de fragmenter les paquets à un endroit différent. Vous pouvez remplacer la valeur MTU par quelque chose comme 1200 afin que les paquets soient fragmentés au niveau de la marque de 1200 octets au lieu de 1500.



Avertissement : La modification de la MTU de la WMI affecte tout le trafic en provenance et à destination de l'adresse IP de gestion du WLC.

Même si vous ne voulez pas modifier la MTU de l'interface WMI, le point de spécifier une interface source est de la modifier d'être l'interface WMI à une autre interface, et d'utiliser cette interface pour le trafic RADIUS, ainsi que de modifier la MTU sur cette interface. Comme cette configuration est effectuée au niveau du groupe de serveurs, vous pouvez être très précis sur le trafic RADIUS dont vous voulez que cette modification soit affectée.

Cette configuration n'est pas liée à un serveur AAA ou à un WLAN. Il est possible d'avoir plusieurs groupes de serveurs avec les mêmes serveurs en eux et ne spécifier l'interface source sur l'un

d'eux que si vous le souhaitez. Ce groupe de serveurs est ajouté à une liste de méthodes, puis à un réseau local sans fil. Ainsi, par exemple, s'il n'y a qu'un seul WLAN où vous voulez que cette modification soit effectuée, même si vous n'avez qu'un seul serveur AAA, vous pouvez créer un nouveau groupe de serveurs, utiliser la commande ip radius source-interface qui pointe vers l'interface avec le MTU que vous voulez utiliser, ajouter le serveur AAA à ce nouveau groupe, créer une nouvelle liste de méthodes en utilisant ce nouveau groupe, puis ajouter cette liste de méthodes au WLAN spécifique où vous voulez que cette modification soit effectuée.

Avertissement : Il est toujours conseillé, lorsque vous apportez des modifications ANY à un réseau actif, de le faire au cours d’une fenêtre de maintenance.

La preuve se trouve dans la capture de paquets

Il est généralement connuDans le domaine des réseaux, si vous ne l'avez pas capturé, vous ne pouvez pas le prouver. Voici quelques exemples de configuration avec ces modifications en place pour vous montrer comment cela fonctionne.

Voici une configuration WLAN. Au cours du test, seul le groupe de serveurs utilisé dans la liste des méthodes est modifié.

```
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
!
```

Ajout De La Commande Source-Interface Avec La MTU Par Défaut

Ici, il s'agit simplement d'un groupe de serveurs normal pointant vers le serveur ISE. La commande d'interface source a été ajoutée pointant vers mon WMI qui n'a pas de MTU défini. Voici à quoi ressemble la configuration.

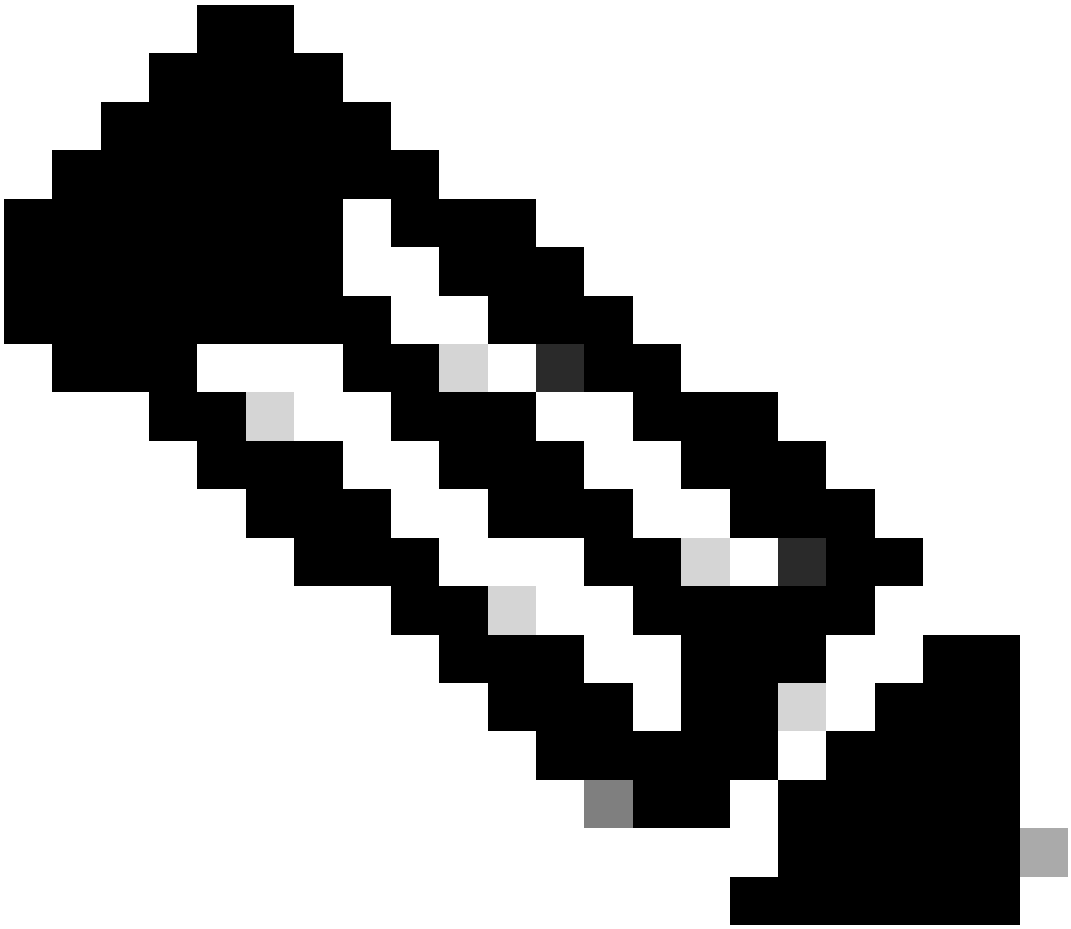
```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group NoMTU
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObF[^bPBVNaYibbBMhNMFAbKUAAB
!
aaa group server radius NoMTU
 server name ISE
 ip radius source-interface Vlan260
 deadtime 5
!
9800#show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

Comme vous pouvez le voir, le groupe de serveurs NoMTU a été ajouté à la liste des méthodes d'authentification liée au WLAN. La commande ip radius source-interface VLAN260 est utilisée pour ce groupe de serveurs et VLAN 260 ne spécifie pas de MTU, ce qui signifie qu'il utilise le MTU de 1500. Juste pour confirmer, le MTU de 1500 vous pouvez utiliser la commande show run all et rechercher l'interface dans la sortie.

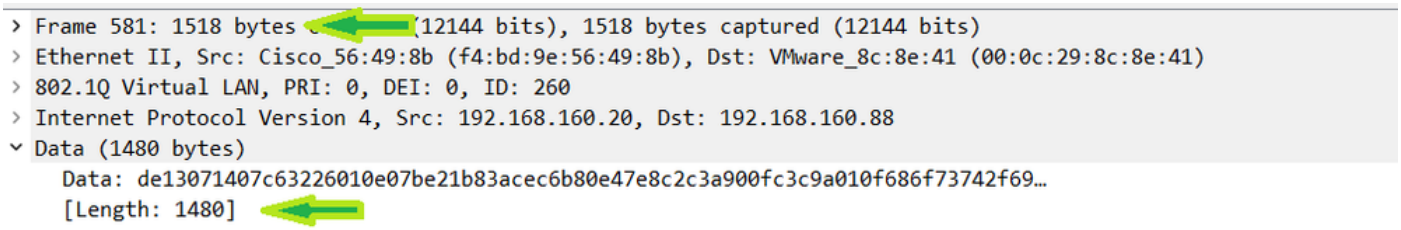
```
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
```

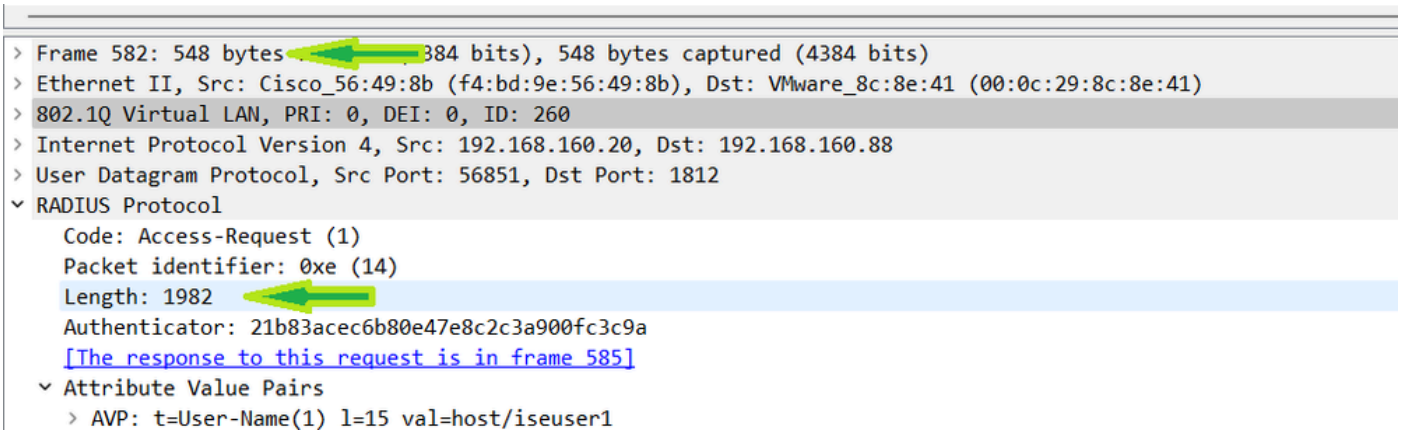
```
no ip clear-dont-fragment
ip redirects
ip unreachables
no ip proxy-arp
ip mtu 1500
```

Maintenant, regardez le paquet où le certificat client doit être envoyé à ISE une fois que le WLC ajoute les données RADIUS :



Remarque : Ici, les octets de la ligne sont 1518. Cela inclut les en-têtes en dehors de la charge utile Ethernet, comme l'en-tête VLAN et l'en-tête de couche 2. Ils ne sont pas comptabilisés dans le MTU.





Ici, vous pouvez voir que la partie données est fragmentée à 1480. Vous pouvez obtenir ce fragment sous la MTU 1500 sur le WMI. Le paquet suivant contient moins de 550 octets, mais vous pouvez voir que la taille totale des données RADIUS est 1982. Cela dit, la fragmentation avec le nouveau MTU fonctionne maintenant.

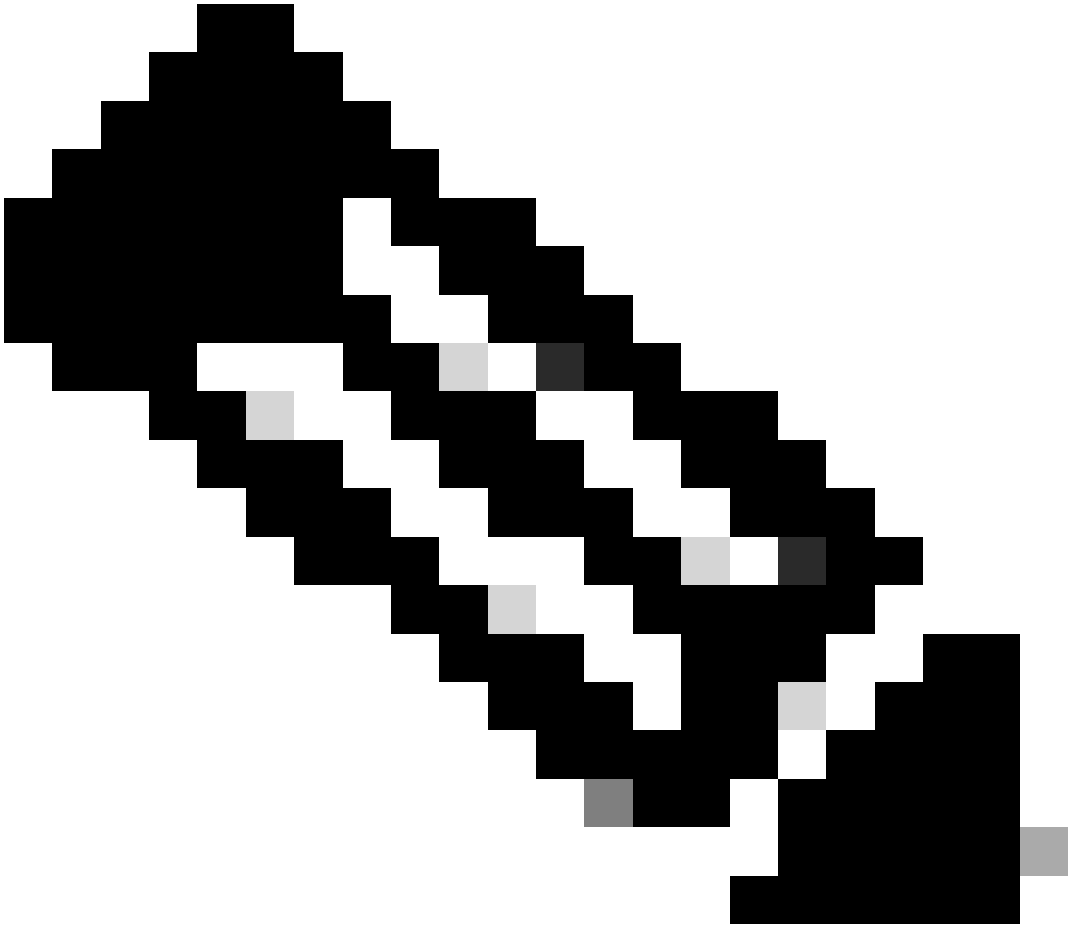
Utilisation d'une interface non WMI avec un MTU de 1200

Maintenant, supposons que vous voulez fragmenter à un MTU plus petit mais que vous ne voulez pas que cette modification affecte tout autre trafic. Aucun problème ici, la configuration reste la même, seule la configuration de l'interface source pointe vers une interface SVI créée à cet effet. Modifiez la liste de méthodes pour pointer vers ce nouveau groupe de serveurs et ce groupe de serveurs utilise une interface source qui n'est pas mon WMI et dont le MTU est défini sur 1200. Voici à quoi ressemble la configuration :

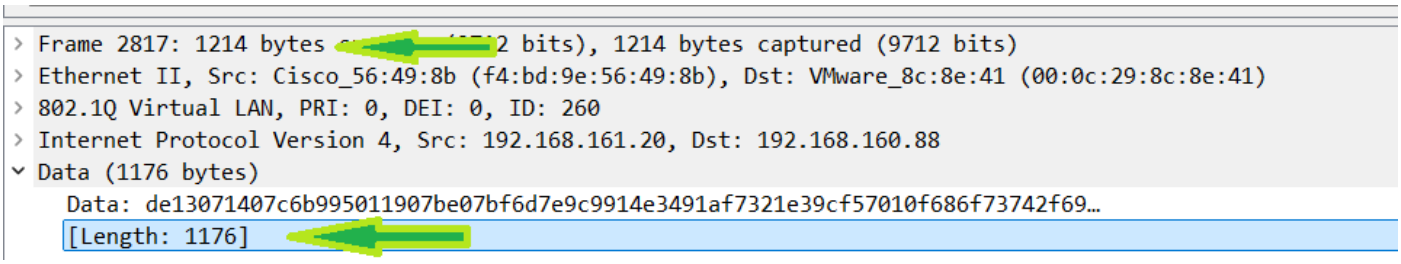
```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group MTU1200
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObFibbBMhNMFAbKUAAB
!
aaa group server radius MTU1200
 server name ISE
 ip radius source-interface Vlan261
 deadtime 5
!
9800#show run inter vlan 261
!
interface Vlan261
```

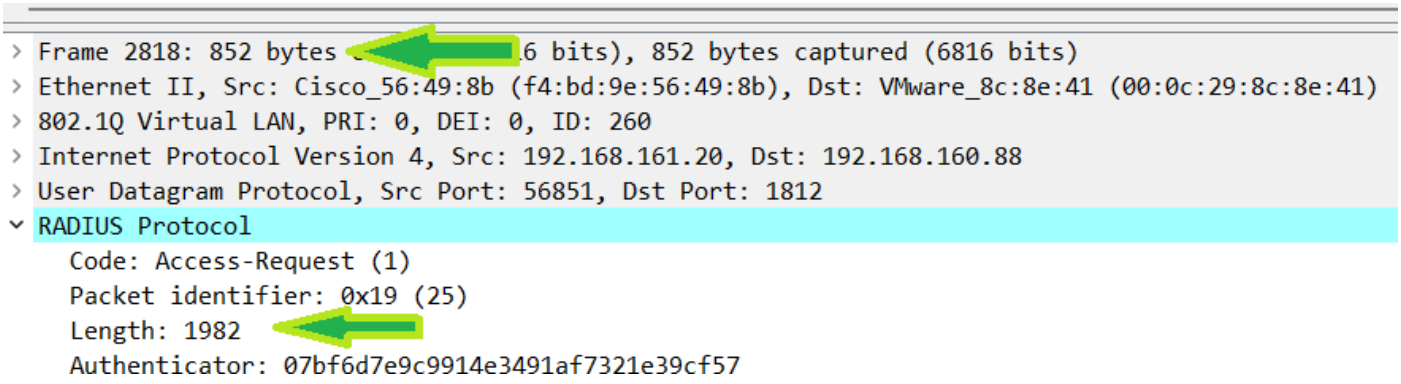
```
 ip address 192.168.161.20 255.255.255.0
 no ip proxy-arp
 ip mtu 1200
end
```

Voyez ensuite à quoi ressemblent les paquets avec ce MTU inférieur.



> Remarque : La diminution de la MTU et la modification du point de fragmentation ne font pas partie du nouveau comportement. Cela a toujours été vrai. Si le comportement par défaut de la fragmentation à 1396 ne correspond pas à la MTU, vous devez toujours fragmenter à un autre point. Elle fait partie de cette section uniquement pour vous aider à expliquer les options disponibles.





Ici, les données RADIUS sont toujours de 1982 octets, mais cette fois, les données ont été fragmentées à 1176 au lieu des 1376 par défaut, où elles auraient été fragmentées si l'interface source n'avait pas été utilisée. N'oubliez pas que lorsque vous définissez la MTU sur 1500 et que vous utilisez la commande source-interface, vous fragmentez à 1480. L'utilisation de la configuration ici vous permet de manipuler le trafic vers un MTU inférieur sans interférer avec d'autres trafics sur le WLC.

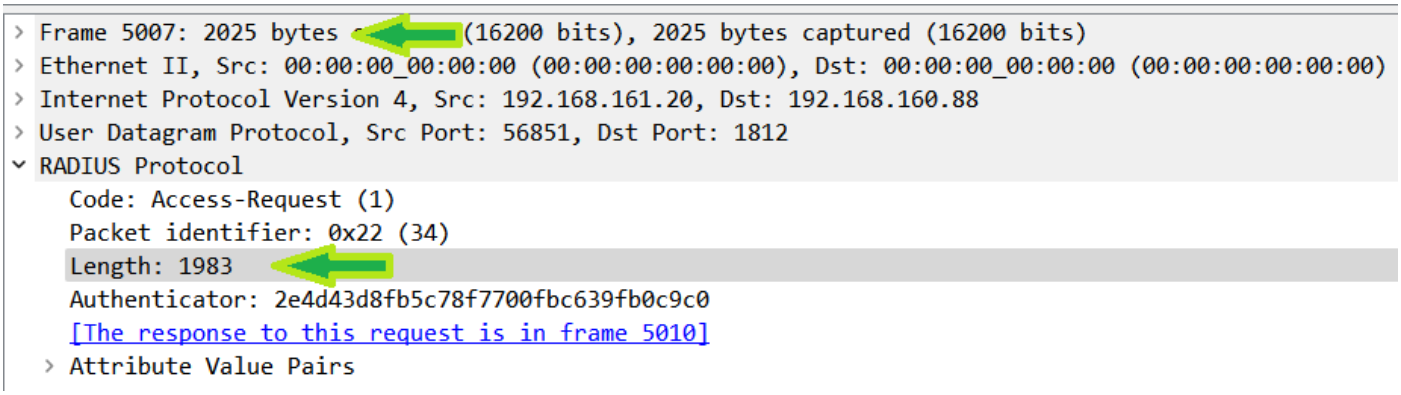
Utilisation d'un MTU de 9 000 pour les trames Jumbo

Étant donné que la fonctionnalité a été créée pour l'option d'envoi de trames Jumbo, il serait dommage de ne pas la tester également en utilisant l'interface non-WMI du VLAN 261. Cependant, maintenant le MTU IP est défini sur 9000. Une remarque rapide, afin de pouvoir définir le MTU IP sur l'interface SVI, vous devez définir le MTU à quelque chose de plus élevé que le MTU IP. Vous pouvez voir ceci dans cette configuration :

```
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
```

Ici, en regardant la capture, vous pouvez voir que le paquet n'a jamais été fragmenté. Il a été envoyé sous la forme d'un paquet entier avec la taille des données RADIUS à 1983. Gardez à l'esprit que pour que cela fonctionne, le reste du réseau doit être configuré pour permettre l'acheminement d'un paquet de cette taille.

Une autre chose à noter ici est que le MTU du client n'a pas changé, de sorte que le client fragmente toujours le paquet EAP à 1492. La différence est que le WLC peut ajouter toutes les données RADIUS nécessaires pour envoyer le paquet à ISE sans avoir à fragmenter les données du client.



Conclusion

Lorsque vous utilisez EAP-TLS, le client est censé envoyer son certificat au serveur AAA. Ces certificats sont généralement plus volumineux que le MTU, de sorte que le client doit les fragmenter. Le point auquel le client fragmente les données est assez proche de la MTU. Puisque l'AP doit ajouter l'en-tête CAPWAP, ce que le client envoie doit être fragmenté. Le WLC reçoit ces deux paquets, les remet ensemble, mais doit ensuite les fragmenter à nouveau pour ajouter les données RADIUS. À ce stade, l'administrateur réseau dispose d'un certain contrôle sur la façon dont le WLC fragmente le paquet EAP que le client a envoyé.

Si vous ajoutez la commande ip radius source-interface <interface you want to use> au groupe de serveurs AAA, le WLC utilise l'interface que vous y placez au lieu de (ou y compris) le WMI. L'utilisation de cette commande indique également au WLC de se fragmenter à n'importe quel MTU de cette interface au lieu de la valeur par défaut 1396. De cette façon, vous avez plus de contrôle sur la manière dont les paquets circulent sur le réseau.

Lorsque vous utilisez Cisco Catalyst Center, la commande d'interface source est ajoutée au groupe de serveurs, ce qui modifie le comportement par défaut.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.