RADIUS MTU en Fragmentation op 9800 WLC begrijpen

Inhoud

Inleiding

Dit document beschrijft hoe de MTU van de RADIUS-pakketten die het WLC naar de RADIUS-server stuurt, moet worden geconfigureerd.

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis van deze onderwerpen te hebben:

- 9800 configuratie van draadloze LAN-controller (WLC) AAA
- Verificatie, autorisatie en accounting (AAA) RADIUS-concepten
- Uitbreidbaar verificatieprotocol - EAP
- Max. transmissieeenheid (MTU)

Gebruikte componenten

- Cisco Identity Service Engineer (ISE) 3.2
- Catalyst 9800 draadloze controller Series (Catalyst 9800-L)
- Cisco IOS® XE 17.15.2
- Windows 11 draadloze client

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrond

Voor de toepassing van dit document is de RADIUS-server (Remote Verification Dial-In User Service) die wordt gebruikt Cisco ISE. Eerst wordt aangetoond hoe de pakketten zonder enige interventie van buitenaf zouden lopen tijdens het EAP-proces (Extensible Authentication Protocol). Daarna is de configuratieoptie om de grootte van het toegangsverzoek te veranderen WLC naar om het even welke server van de RADIUS verzendt. Deze optie werd toegevoegd in IOS-XE versie 17.11.

9800 RADIUS-MTU

Meestal maakt de MTU van de RADIUS-pakketten niet uit, omdat ze meestal klein zijn en toch niet de MTU raken. Echter, als een kant een certificaat moet verzenden, wat meestal 2-5KB zijn, moet het apparaat dat certificaat fragmenteren om het onder hun MTU te krijgen.

Wanneer de client een certificaat naar de RADIUS-server moet sturen, zoals bij EAP Transport Layer Security (EAP-TLS) het geval is, stelt het de WLC voor met een situatie waarin het pakket opnieuw moet worden gefragmenteerd vanwege de hoeveelheid RADIUS-gegevens die ermee moeten worden verzonden. Tot 17.11 had de netwerkbeheerder weinig controle over dit proces, maar nu krijgen ingenieurs de optie om de grootte van het toegang-verzoek te manipuleren dat door WLC wordt verzonden.

EAP-TLS-pakketstroom

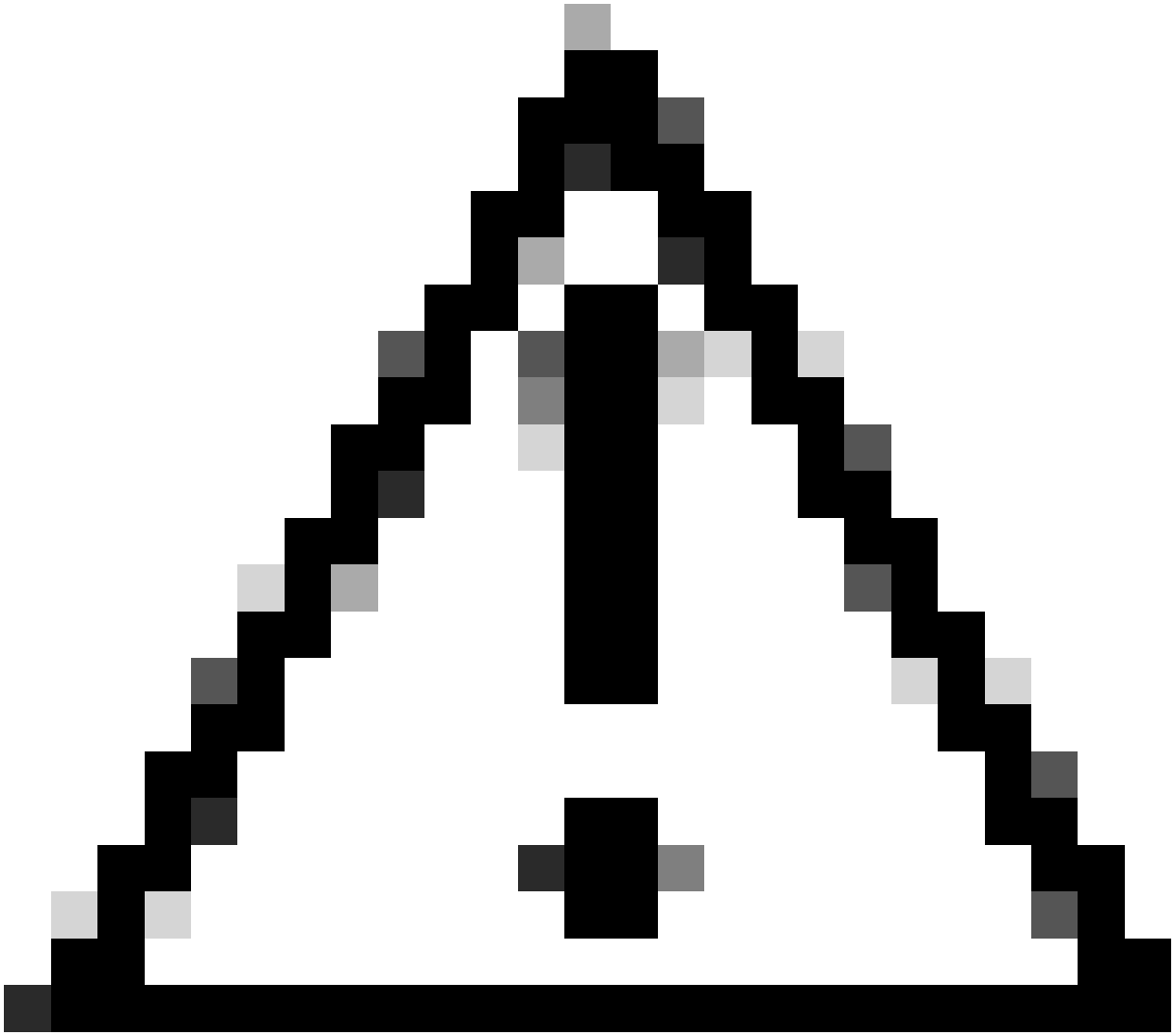
Dit is een beetje een diepe duik in hoe de pakketten eruit zien en hoe ze worden behandeld door de draadloze infrastructuur. Om de in dit document geïntroduceerde veranderingen volledig te kunnen begrijpen, is het belangrijk om te weten wat de pakketstroom is tijdens het draadloze

verificatieproces bij gebruik van dot1x en meer specifiek EAP-TLS.

Als u al een diepgaand begrip hebt van hoe de EAP- en RADIUS-pakketstroom werkt met in de draadloze infrastructuur van Cisco, ga dan naar de sectie gedragsverandering die uitlegt wat in 17.11 is toegevoegd, zodat de netwerkbeheerders meer controle hebben over de RADIUS MTU. Kijk eerst eens naar de EAP Identification (EAP-ID).

EAP-ID

De EAP-ID wordt geïnitieerd door de verificator, in dit geval de WLC. Dit moet het eerste deel van het EAP-proces zijn. Soms stuurt de draadloze client een EAPOL-start. Dit betekent normaal dat de client nooit de EAP-ID-aanvraag heeft ontvangen of opnieuw wil starten.



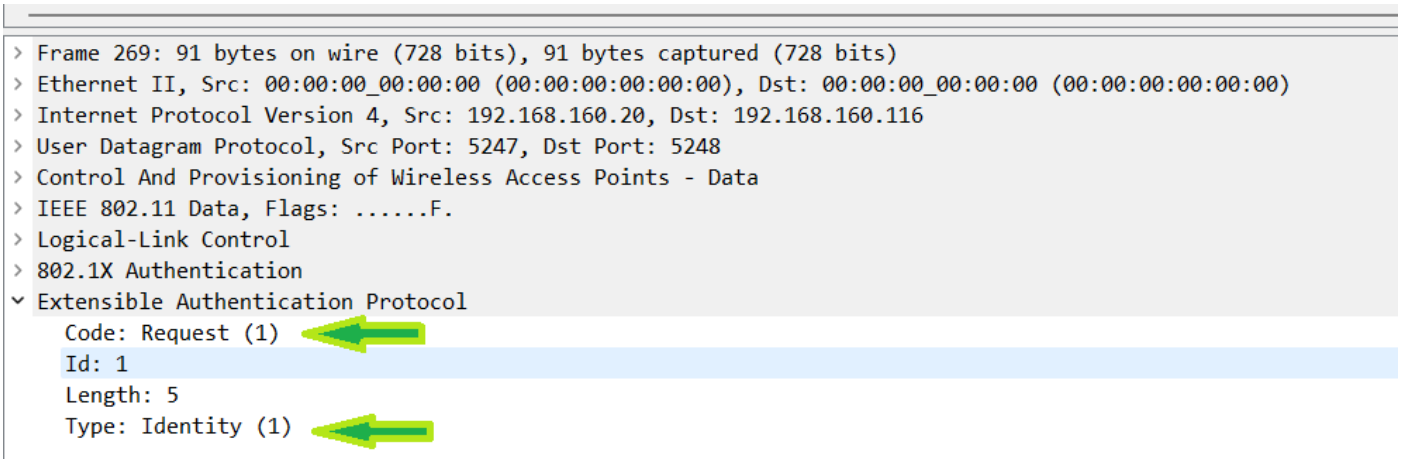
Voorzichtig: Er is een verschil tussen het EAP-ID-pakket en de EAP-pakket-ID. Het EAP-ID-pakket wordt gebruikt om de aanvrager te identificeren waar de EAP-pakket-ID een nummer is dat wordt gebruikt om het specifieke pakket te volgen terwijl het door het netwerk wordt verplaatst.

EAP-ID-aanvraag

Eerst maakt het draadloze clientapparaat verbinding met het netwerk via het normale associatieproces. Wanneer het Wireless Local Area Network (WLAN) is geconfigureerd voor dot1x, moet de WLC eerst weten wie de client is voordat deze toegang kan aanvragen bij de RADIUS-server. Om deze informatie te vinden stuurt de WLC de client en EAP-ID-verzoek.

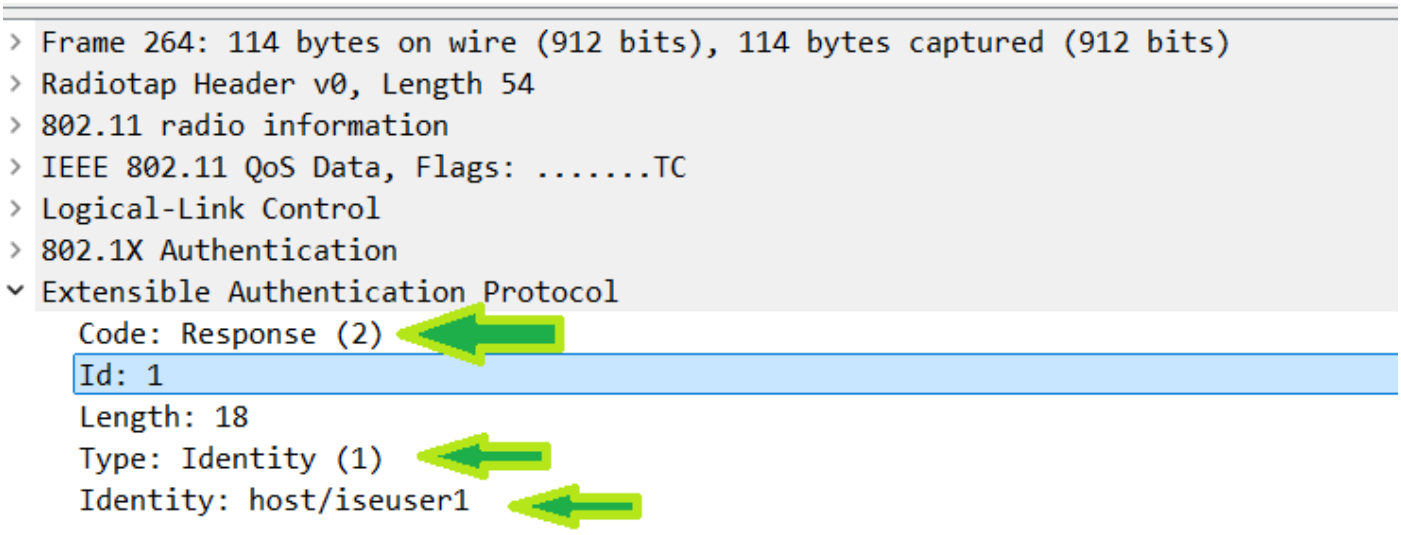
Verwacht wordt dat de client zal reageren met de EAP-ID-respons. Dit geeft de WLC wat het nodig heeft om het access-request te kunnen bouwen en naar de ISE te sturen. De EAP-ID-aanvraag is wanneer de client wordt gevraagd om zijn gebruikersnaam en wachtwoord in te voeren bij een normale PEAP-verificatie.

Deze discussie gaat echter over EAP-TLS, zodat de EAP-ID-respons hier alleen de gebruikers-ID zou hebben. In de demo is de gebruikers-id iseuser1. In dit pakket kunt u de EAP-ID-aanvraag zien die de WLC naar de draadloze client stuurt om te vragen wie ze zijn. Aangezien dit een draadloze client is, kapselt de WLC het verzoek in CAPWAP in en stuurt het naar het access point (AP) dat via de ether wordt verzonden. In de EAP-gegevens betekent code 1 dat het een verzoek is en type 1 dat het een verzoek voor de identiteit is.



EAP-ID-respons

Vervolgens wordt verwacht dat de draadloze client zal reageren met de EAP-ID-respons. In de EAP-gegevens is de code veranderd in 2, wat aangeeft dat het een reactie is, maar het type blijft als 1, nog steeds zichtbaar voor de identiteit. Hier kunt u zelfs de gebruikersnaam zien die de client gebruikt. Nog iets om deze pakketten te controleren is het ID-nummer van het EAP-pakket. Voor de EAP-ID-uitwisseling is het altijd 1, maar dit nummer verandert later in iets anders zodra ISE betrokken raakt.



Je kunt zien dat beide pakketten vrij klein zijn, dus de MTU heeft hier geen invloed, omdat het veel minder is dan de 1500 bytes die in het netwerk worden gebruikt.

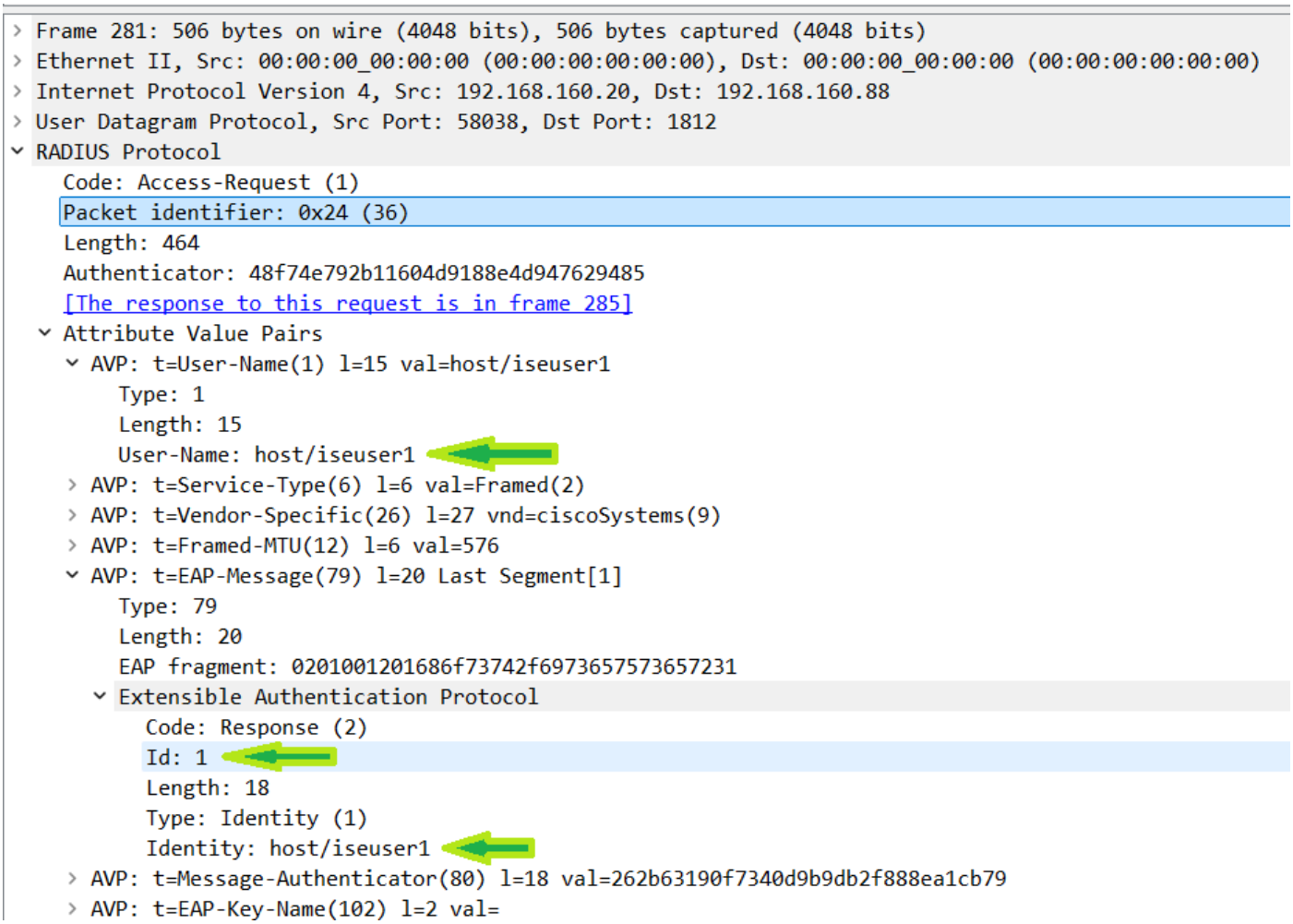
Access-request en access-Challenge

De communicatie met de client is EAP en de communicatie tussen de WLC en ISE is RADIUS. Voor de RADIUS-communicatie worden de pakketten access-request en access-challenge gebruikt. De WLC ontvangt het EAP-pakket van de aanvrager en stuurt het door naar ISE met behulp van het RADIUS-toegangsverzoek. In een werkend netwerk zou ISE reageren met een access-challenge.

Access-request

Nu de WLC de identiteit van de client kent, moet het de RADIUS-server vragen of die client is toegestaan op het netwerk. Om dat te doen, vraagt WLC toegang voor die cliënt door het toegang-verzoek pakket te verzenden. Er zijn andere gegevens die de WLC samen met de EAP-gegevens gaat verzenden. Deze worden gezamenlijk attribuutwaardeparen, AVP's of AV-paren genoemd, afhankelijk van wie er aan het woord is.

Dit document gaat niet ver in de AVP's, aangezien dat buiten het kader van deze discussie valt. Hier hoeft u alleen maar te zien dat de gebruikersnaam (EAP-gegevens) is opgenomen en naar de RADIUS-server is verzonden, die in dit geval ISE is. U kunt ook zien dat EAP-ID-nummer 1 ook naar ISE wordt verzonden. Vergeet niet dat toen je de EAP-pakketID via de lucht bekeek, het daar ook 1 was. Het laatste belangrijke dat hier opgemerkt moet worden is dat sinds de WLC al deze AVP's heeft toegevoegd, het 114-byte pakket dat de client verzonden wordt nu omgezet in een 488-byte pakket voordat het naar ISE wordt verzonden.

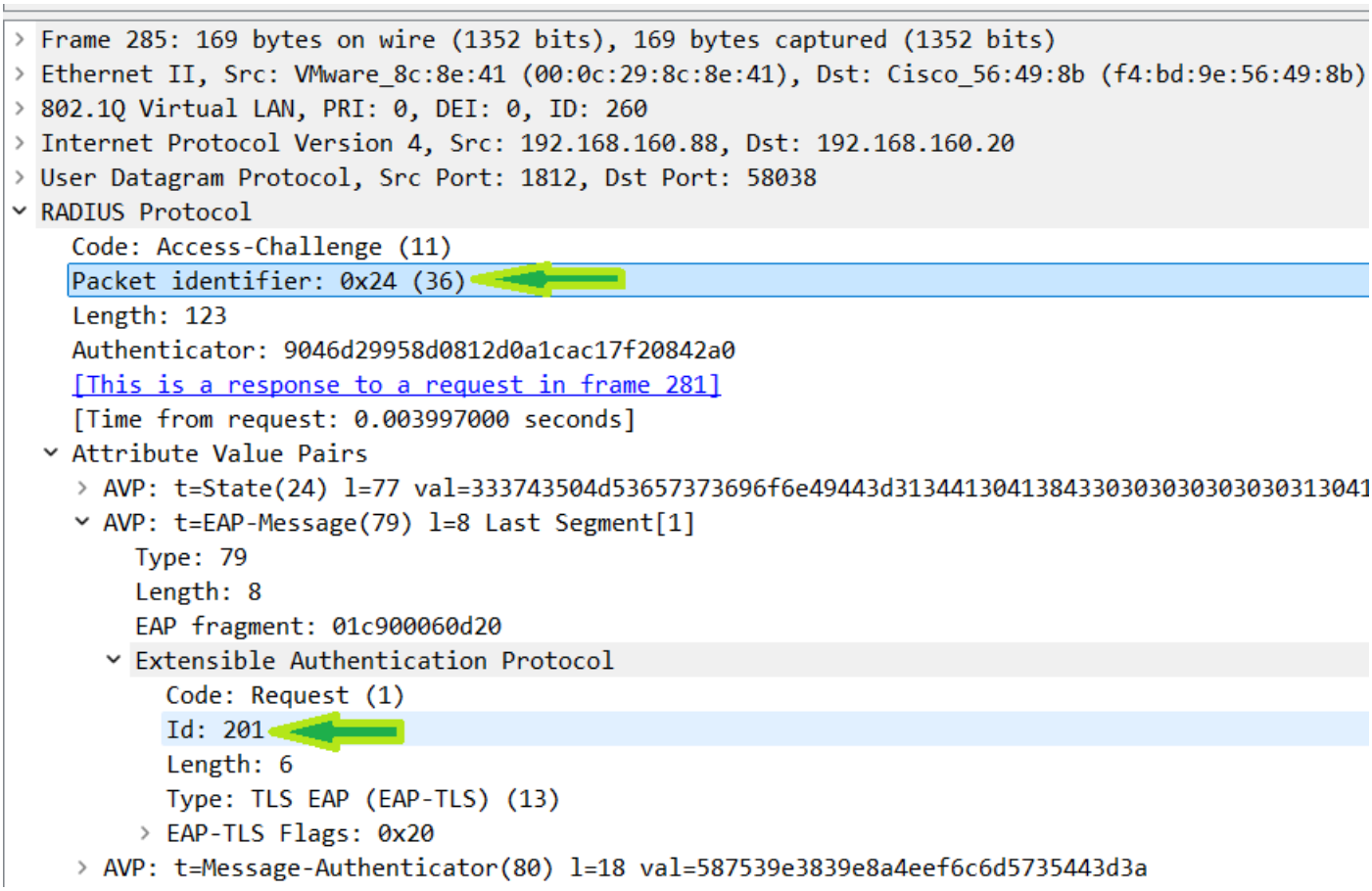


Access-Challenge

Aangenomen dat ISE het toegangsverzoek ontvangt en besluit te reageren, wordt verwacht dat deze reactie als een toegangsuitdaging van ISE komt. Als u terugkijkt op het toegangsverzoek, ziet u de RADIUS-pakketid van 36 voordat de AVP's beginnen.

Wanneer de WLC de access-challenge ontvangt, moet de RADIUS-id overeenkomen met die pakketid van het toegangsverzoek. RADIUS-pakketid is voor de RADIUS-communicatie tussen ISE en WLC. In dit pakket kunt u ook zien dat de ISE een nieuwe EAP-ID van 2010 heeft ingesteld, die wordt gebruikt voor het bijhouden van de communicatie tussen ISE en de client. Op dit punt is de WLC slechts een doorvoerroute voor de communicatie tussen ISE en de klant.

Het is belangrijk om al deze pakket-ID's hier op te nemen, zodat u de communicatiestroom begrijpt en hoe u deze pakketten door het netwerk kunt volgen. In een productieomgeving zijn er meestal meerdere verificaties tegelijk. Gebruik de opdracht call-station-id om het pakket af te stemmen op het MAC-adres van de client. Vervolgens kunt u de RADIUS-pakket-ID en EAP-pakket-ID gebruiken om de pakketstroom voor deze specifieke client te volgen. Tot nu toe heeft geen van beide partijen certificaten verzonden, dus er is nog steeds geen reden om zich zorgen te maken over de MTU.



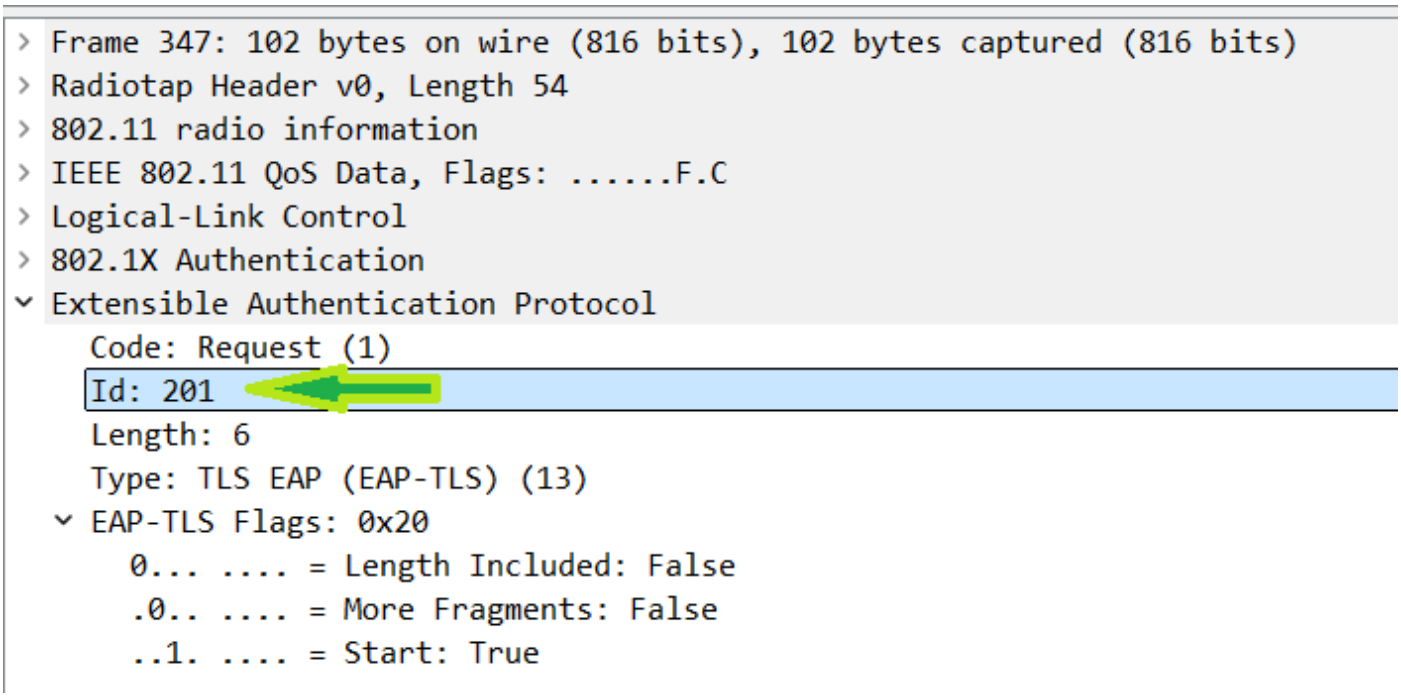
EAP-aanvraag en EAP-respons

Gewoon een herinnering, de client spreekt EAP niet RADIUS. Dat gezegd hebbende, wanneer de WLC de access-challenge ontvangt, moet het de RADIUS-gegevens verwijderen en het EAP-verzoek eruit halen zodat het naar de client kan worden verzonden.

EAP-aanvraag

Dit moet er precies zo uitzien als het binnen de access-challenge deed toen de WLC het ontving. Alle RADIUS-dingen zijn echter verwijderd en alleen het EAP-onderdeel wordt naar de client verzonden.

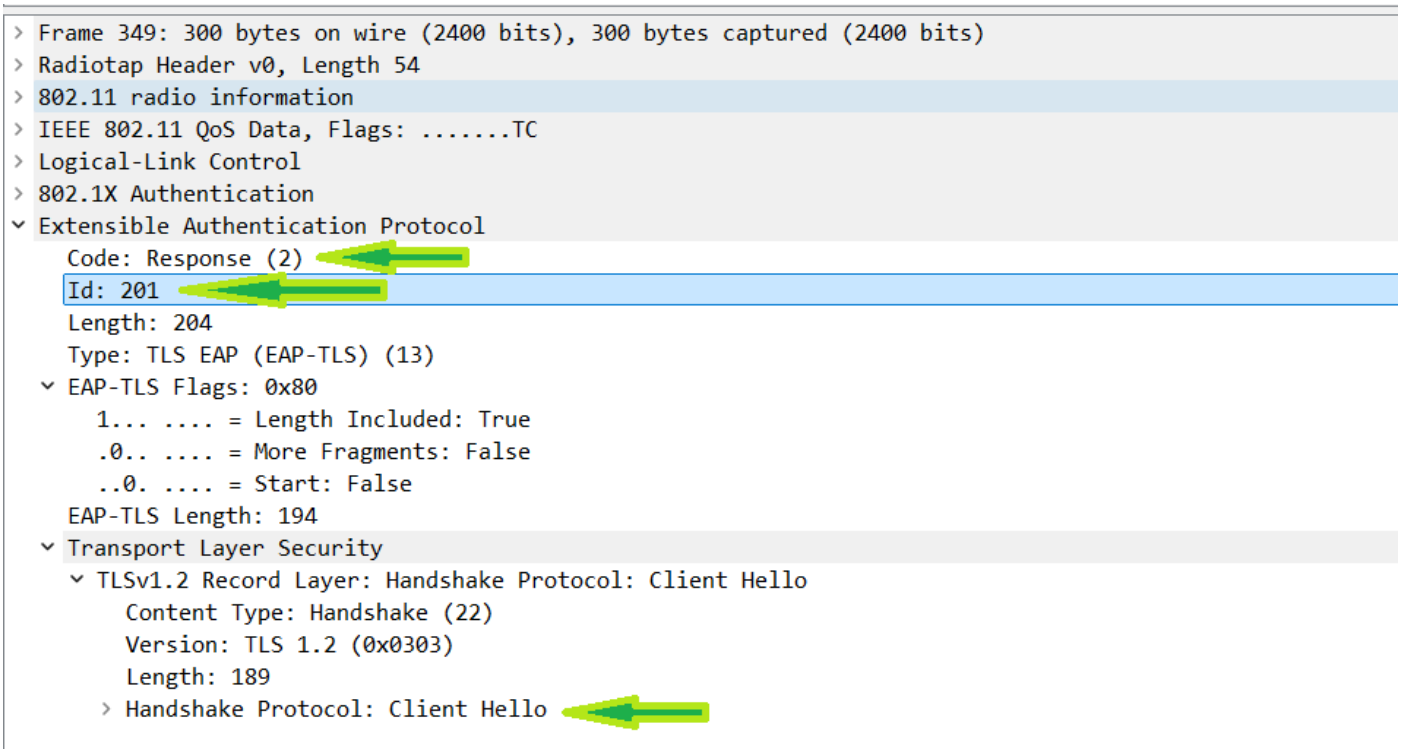
Je kunt hier nog steeds de EAP-pakketID van 201 zien, net zoals het was in de access-challenge omdat het dezelfde gegevens zijn die de WLC van ISE heeft ontvangen. De stroom hier is hetzelfde als met de EAP-ID, alleen nu komt het niet van de WLC en wordt het gebruikt voor het instellen van de EAP-methode. Dit pakket is nog steeds vrij klein, omdat het alleen maar het begin van een EAP-TLS-sessie moet vastleggen.



EAP-respons

Wanneer de client de EAP-Verzoek ontvangt, moet zij reageren met een EAP-Reactie. In de EAP-Response start de client de TLS-sessie. Dit ziet er hetzelfde uit als in elke andere situatie TLS wordt gebruikt. Het begint met het "client hello" bericht. Dit document gaat niet in wat gaat in de klant hallo omdat het irrelevant is voor dit onderwerp. Wat je hier moet opmerken is dat er een TLS sessie wordt ingesteld.

Hier kunt u de gegevens in de pakketten zien zoals bij elke andere TLS-instelling. Net als bij de EAP-ID-respons, raakt dit pakket de WLC en wordt het geconverteerd naar een toegangsaanvraag. ISE reageert met een EAP-aanvraag die is verpakt in een access-challenge. Dit blijft de flow van nu.



TLS-certificaten

Hier is het punt waar je de pakketgrootte gaat zien toenemen. De certificaten kunnen vrij groot zijn, afhankelijk van de aanwezigheid van een of meer tussenliggende certificeringsinstanties (CA's). Als het een zelf ondertekend certificaat is, zou het natuurlijk kleiner zijn dan een certificaat met een apparaatzekerheid geketend aan 2 tussenpersonen CA's en een wortel CA. Hoe dan ook, je ziet normaal gesproken dat de eigenaar van het certificaat zijn eigen pakketten hier begint te fragmenteren.

ISE-certificaat

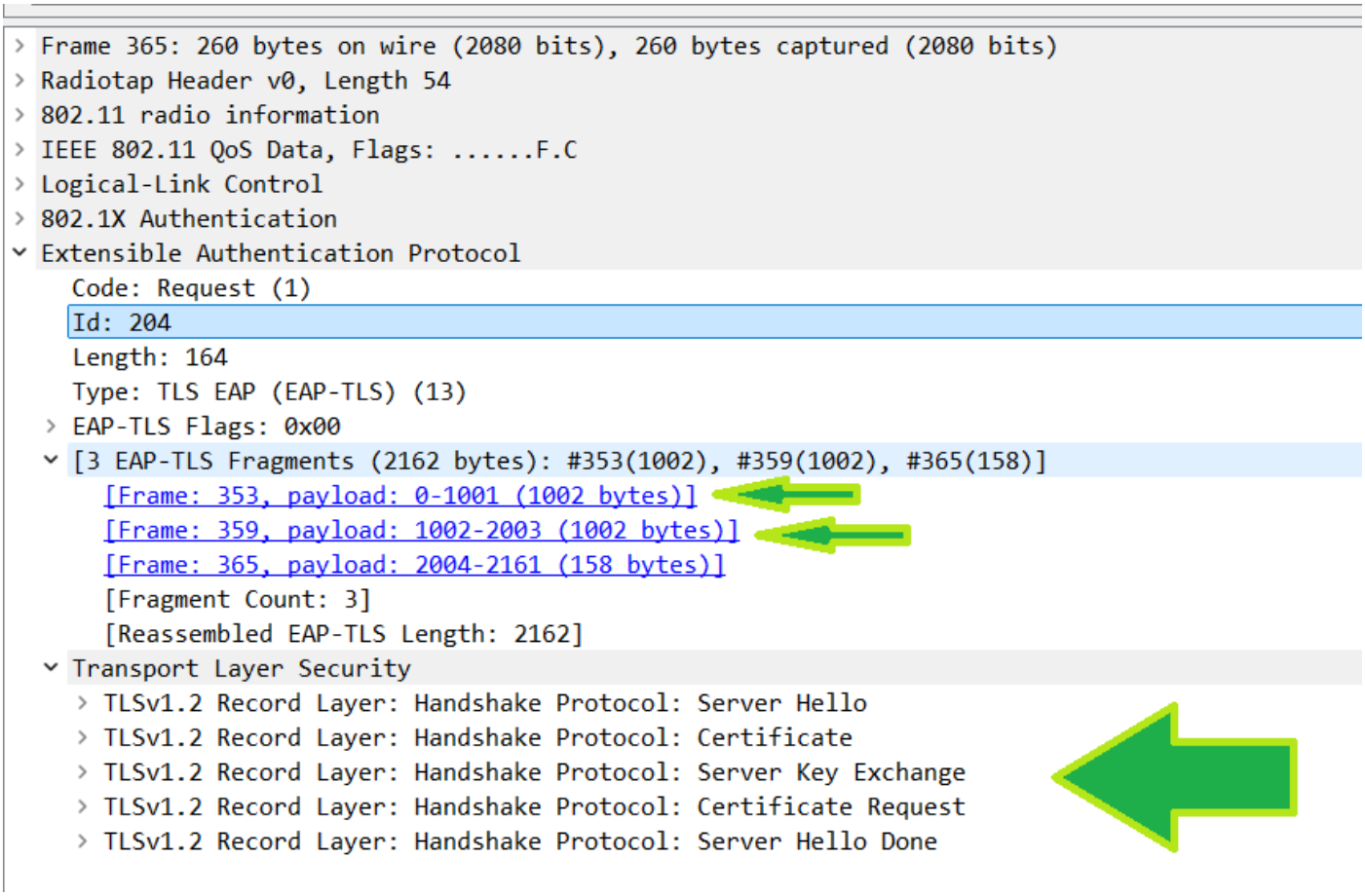
Nu ISE de TLS-client heeft ontvangen, reageert het met een andere EAP-aanvraag. In dit nieuwe EAP-verzoek stuurt ISE het "server hello"-bericht, het certificaat, de "server key exchange", het "certificaatverzoek" en de "server hello done"-berichten allemaal tegelijk. Als het dit alles in één pakket zou verzenden, zou het pakket over MTU voor het netwerk zijn. ISE fragmenteert het pakket om het onder de MTU te krijgen. Met ISE fragmenteert het het gegevensgedeelte van het pakket, zodat het niet groter is dan 1002 bytes in de hoop dubbele fragmentatie te voorkomen.

Wat wordt bedoeld met dubbele fragmentatie? De eerste fragmentatie gebeurt op ISE omdat de gegevens die het wil verzenden te groot zijn om binnen de MTU van het netwerk te passen. Toch kunnen er andere plaatsen in het netwerk zijn waar, zelfs als de MTU hetzelfde is, vanwege de manier waarop het netwerk is ingesteld, een apparaat mogelijk het pakket moet fragmenteren om het zijn kopregels toe te voegen en onder de MTU te blijven. Dit kan zelfs waar zijn als het fragment bit niet is ingeschakeld.

Een goed voorbeeld hiervan is een VPN-tunnel, of welke tunnel dan ook. Om gegevens in een VPN-tunnel te zetten, moeten de VPN-routers hun kopregels aan het verkeer toevoegen. Als dit RADIUS-verkeer gefragmenteerd was op of dicht bij de MTU, dan zou er met betrekking tot dit

VPN geen manier zijn om de gegevens onder de MTU te houden en extra kopregels toe te voegen. Dit geldt ook voor CAPWAP-tunnels, die je later ook kunt zien.

Om te voorkomen dat deze pakketten in een situatie terechtkomen waarin een ander apparaat het opnieuw kan fragmenteren, fragmenteert ISE het pakket op een plaats waar dit in de meeste netwerken kan worden vermeden. Dit betekent dat ISE deze gegevens in meerdere EAP-aanvragen verstuurt en elke keer wacht op een leeg EAP-antwoord. De EAP-ID neemt toe met elk verzonden fragment. Vanuit het oogpunt van de WLC, zou dit een access-challenge en toegangsaanvraag uitwisseling voor elk fragment zijn en de RADIUS pakket-ID zou toenemen met elk fragment verzonden.



Clientcertificaat

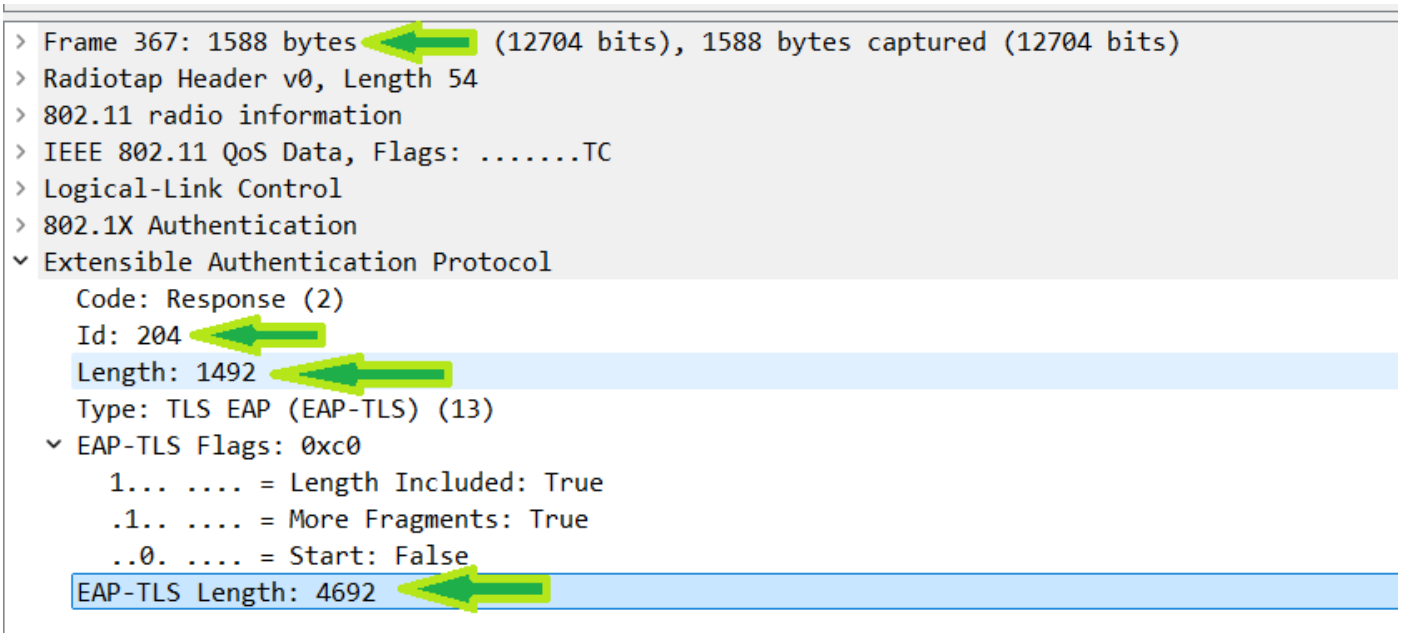
Zodra ISE alle fragmenten verstuurt en ze weer in elkaar gezet worden door de client, gaat de pakketstroom naar de client om iets te versturen. In TLS wordt verwacht dat de client op dit punt zijn eigen cert zal versturen om de authenticatie te voltooien. Dat is het punt waarop de zaken complexer worden. Net als ISE zal de client meerdere TLS-onderdelen tegelijk versturen, waarvan één het certificaat is.

In tegenstelling tot wat bij ISE werd gezien, sturen de meeste klanten hun EAP-gegevens net onder de MTU. In deze demo zijn de 802.1x-gegevens 1492. Het probleem met dat is dat de AP de CAPWAP kopballen moet toevoegen zodat het naar WLC kan worden verzonden.

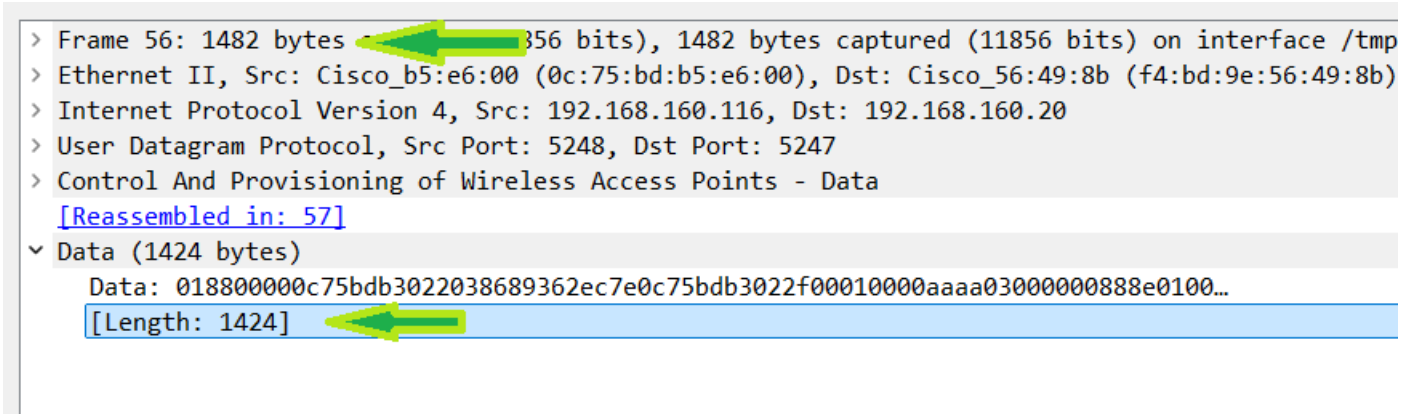
Hoe moet dat gebeuren? AP zal het pakket moeten fragmenteren zodat het de kopballen kan

toevoegen en het verzenden naar WLC. Er is geen manier voor AP om het pakket aan WLC te verkrijgen zonder het te fragmenteren. Dat gezegd hebbende, hier is het pakket dubbel gefragmenteerd, eerst van de client, dan weer van de AP. Deze fragmentatie is echter geen probleem zoals bij CAPWAP wordt verwacht.

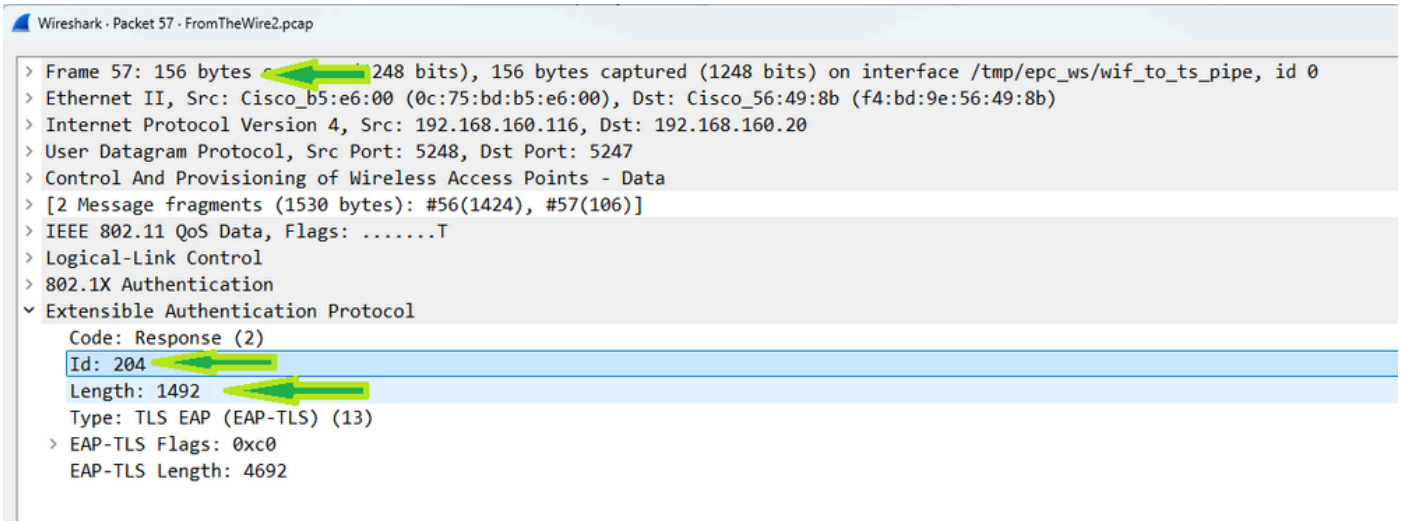
Het pakket via de ether:



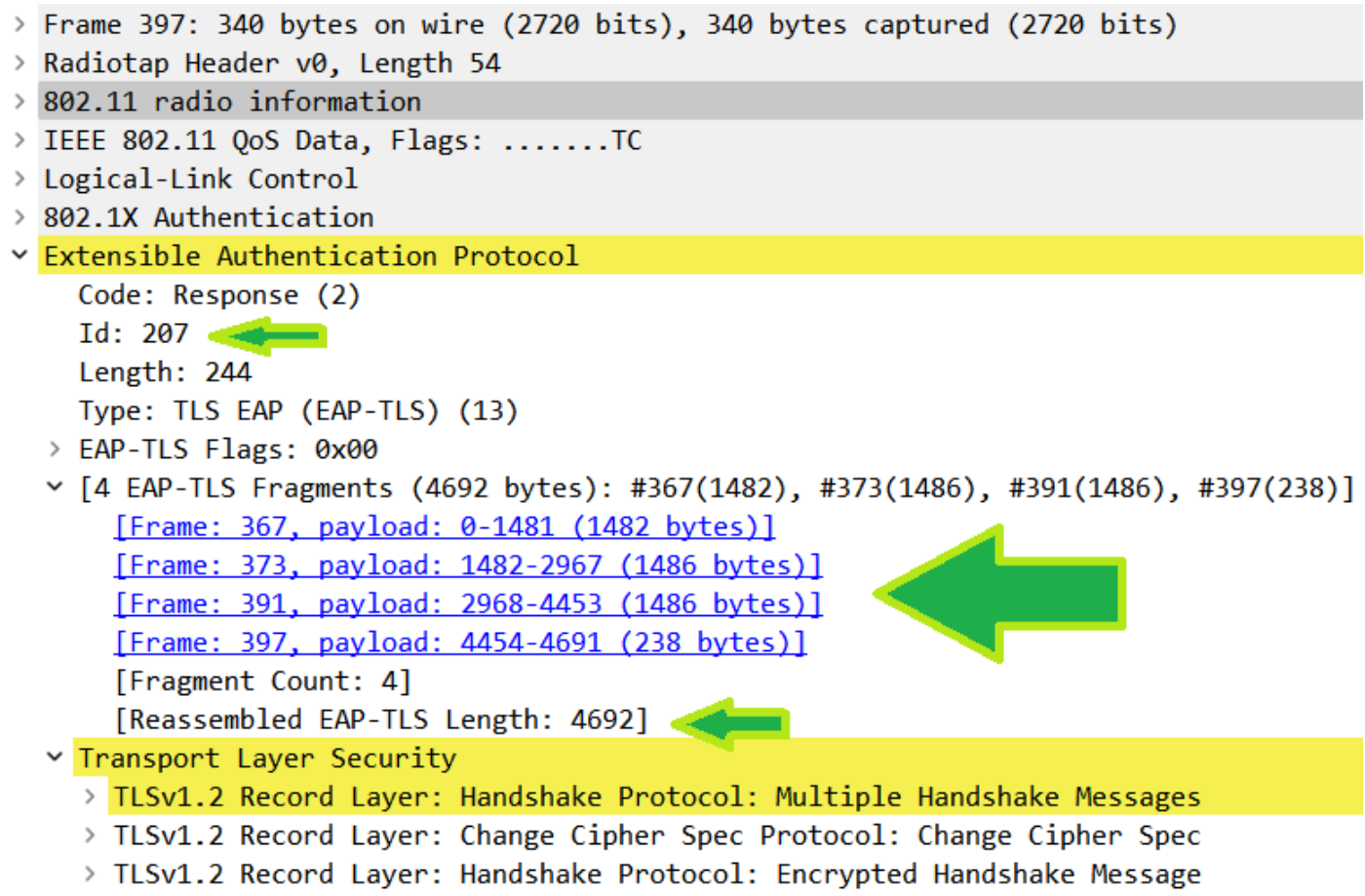
Het pakketfragment op de draad:



Het pakket dat op de draad opnieuw wordt geassembleerd:



Alle fragmenten van clients die via de ether worden geassembleerd:



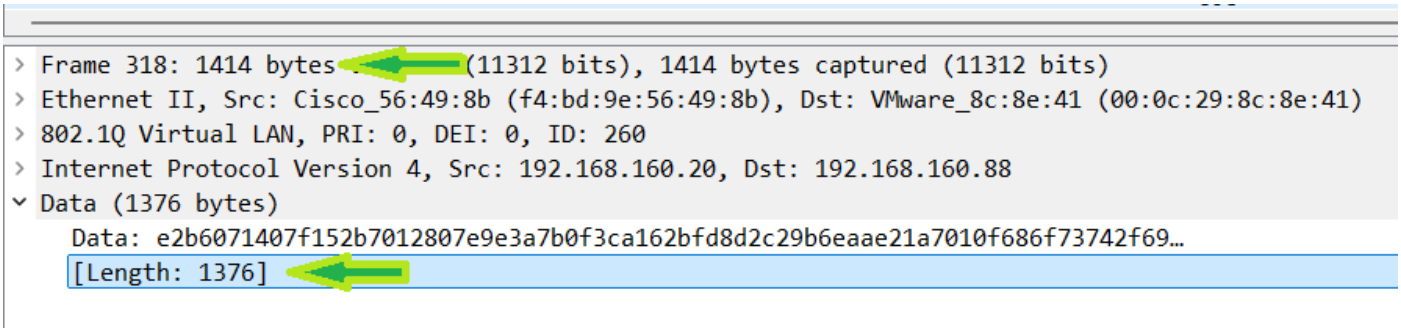
Client Cert bij de WLC

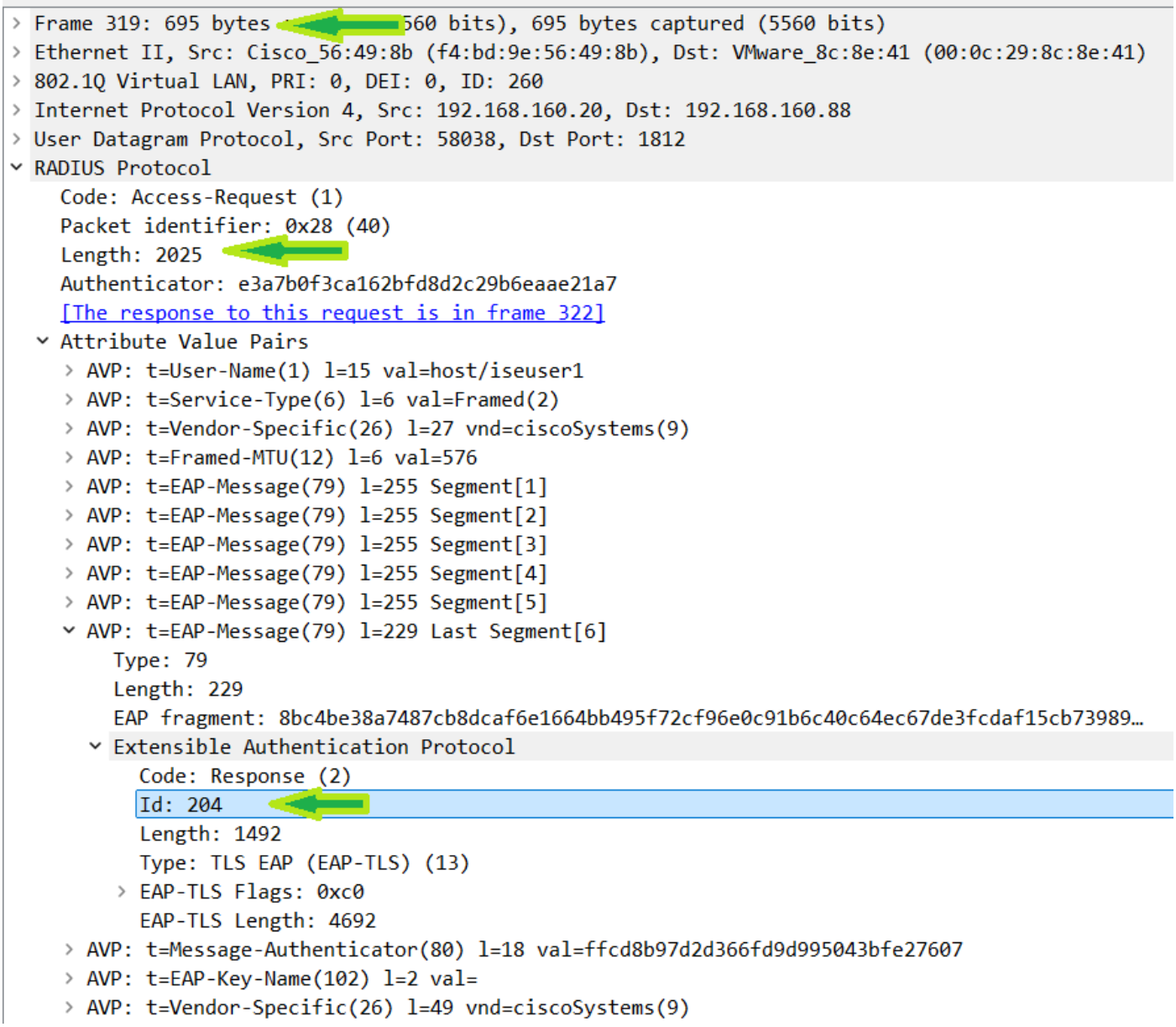
De WLC ontvangt de twee CAPWAP fragmenten en herassembleert ze om het hele 1492 byte pakket van de client, het herstellen van het pakket - maar niet voor lang. Deze restauratie is kort geleefd omdat, als u terugkijkt naar hoe de WLC het access-request verstuurt, u moet onthouden dat het ongeveer 400 bytes van RADIUS AVPs aan het pakket moet toevoegen voordat het de gegevens naar ISE kan versturen.

Voor eenvoudige wiskunde, veronderstel de WLC 408 bytes toevoegt brengend de totale pakketgrootte aan 1900. Dit is ruim boven de 1500 MTU dus wat gaat de WLC doen? Fragmenteer het pakket opnieuw.

Op dit punt, gaat WLC het pakket bij 1396 door gebrek fragmenteren. De gedachte hier is hetzelfde als bij ISE. De hoop is dat het pakket klein genoeg wordt gemaakt, zodat het, als het door een andere tunnel moet gaan, niet opnieuw gefragmenteerd hoeft te worden om de kopregels toe te voegen. Echter, de WLC is niet zo voorzichtig als ISE dus 1396 is hier goed genoeg.

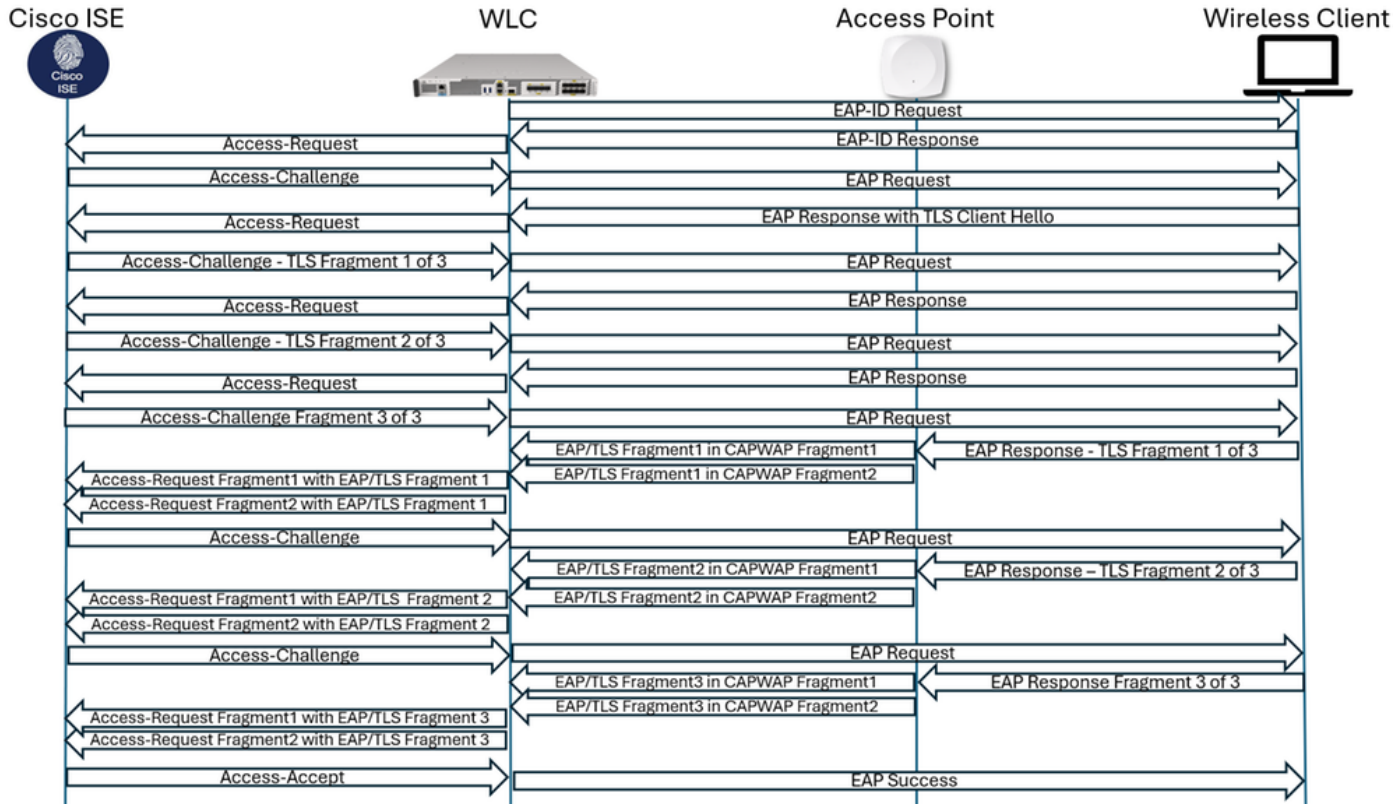
Het gefragmenteerde pakket dat WLC verlaat:





Packet Flow TL;DR

Wanneer ISE haar certificaat verstuurt, fragmenteert ze de TLS-pakketten met 1002 bytes. Geen problemen. Wanneer de opdrachtgevers hun certificaat versturen, versnipperen ze meestal dicht bij de MTU. Aangezien het toegangspunt de CAPWAP-kopregels aan het pakket moet toevoegen, moet het ook dit pakket fragmenteren. Zodra de WLc de fragmenten heeft ontvangen, moet het pakket opnieuw worden geassembleerd, maar dan moet het de RADIUS-AVP's toevoegen zodat het pakket opnieuw gefragmenteerd is. De pakketstroom ziet er ongeveer zo uit:



Gedragsverandering RADIUS MTU

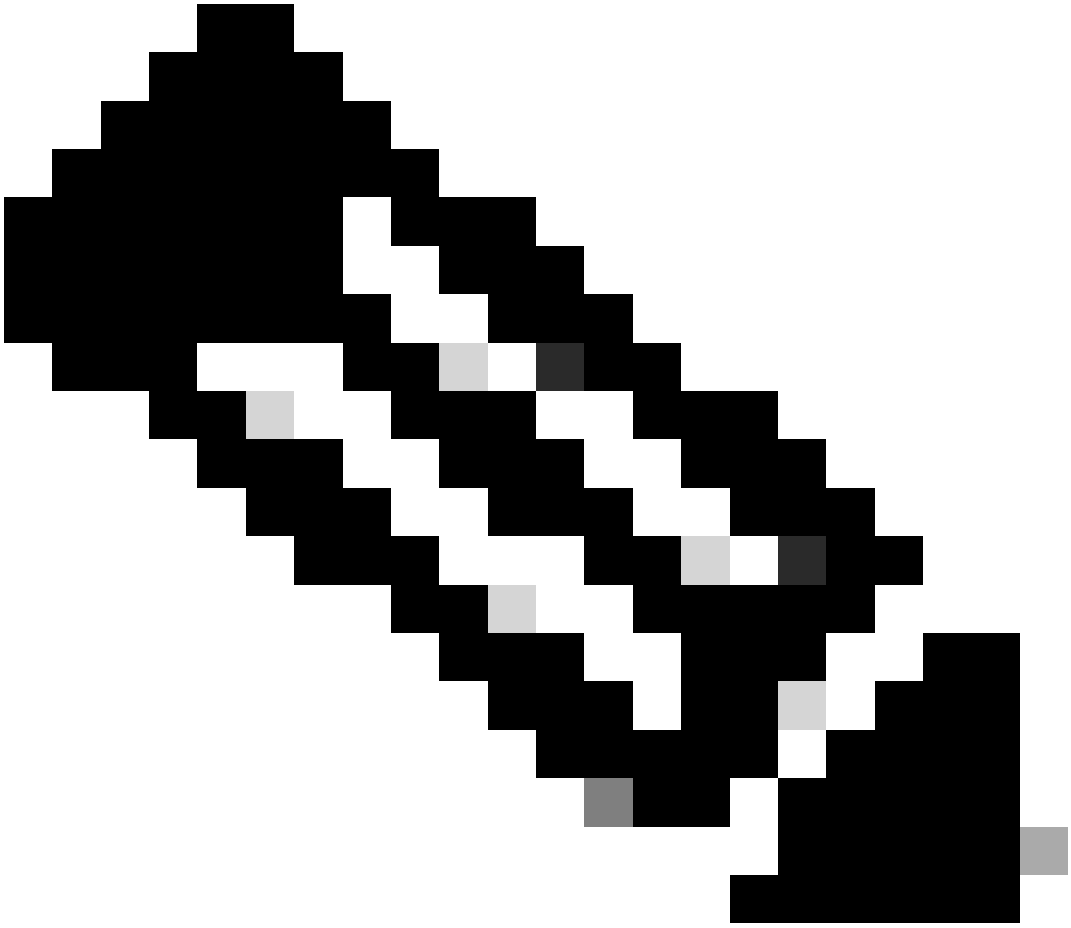
Wanneer u de pakketstroom voor elk draadloos client-dataverkeer bekijkt, kunt u zien dat de draadloze infrastructuur slechts invloed heeft op een paar plaatsen. De eerste plaats is wanneer het verkeer de AP verlaat en de tweede plaats is wanneer het verkeer de WLC verlaat. De uitzondering is met TCP-verkeer waar de draadloze infrastructuur de client-MSS kan aanpassen. EAP valt echter niet onder TCP, in feite is het zijn eigen protocol.

Wanneer u kijkt naar de EAP- en RADIUS-verkeersstromen, kunt u ook zien dat het netwerk in feite de verkeersgrootte beïnvloedt bij zowel de AP als de WLC wanneer de oorspronkelijke pakketgrootte te dicht bij de MTU komt. Met een goed begrip van de rol van de WLC in deze uitwisseling, kunt u zien dat er slechts één plaats is waar het invloed heeft op de grootte van het RADIUS-pakket. Dit is het geval als een EAP-respons wordt ontvangen en u deze wijzigt in een RADIUS-toegangsverzoek.

Wat veranderde

Als de EAP-respons via de MTU verloopt, moet u, zodra u de RADIUS AVP's toevoegt, deze fragmenteren. Omdat je dit pakket hoe dan ook al moet fragmenteren, kun je op zijn minst bepalen op welke grootte je het wilt fragmenteren. Dat is waar de gedragsverandering die in 17.11 geïntroduceerd wordt, om je heen komt.

In het functieverzoek dat in Cisco-bugid CSCwc81849 wordt bijgehouden, wilt u ondersteuning toevoegen voor RADIUS Jumbo-pakketten. Dat is gebeurd door het RADIUS-pakket niet meer automatisch te fragmenteren in 1396. Als u nu de opdracht IP radius source-interface <interface X> toevoegt, wordt het RADIUS-toegangsverzoek verzonden via de MTU van die interface.



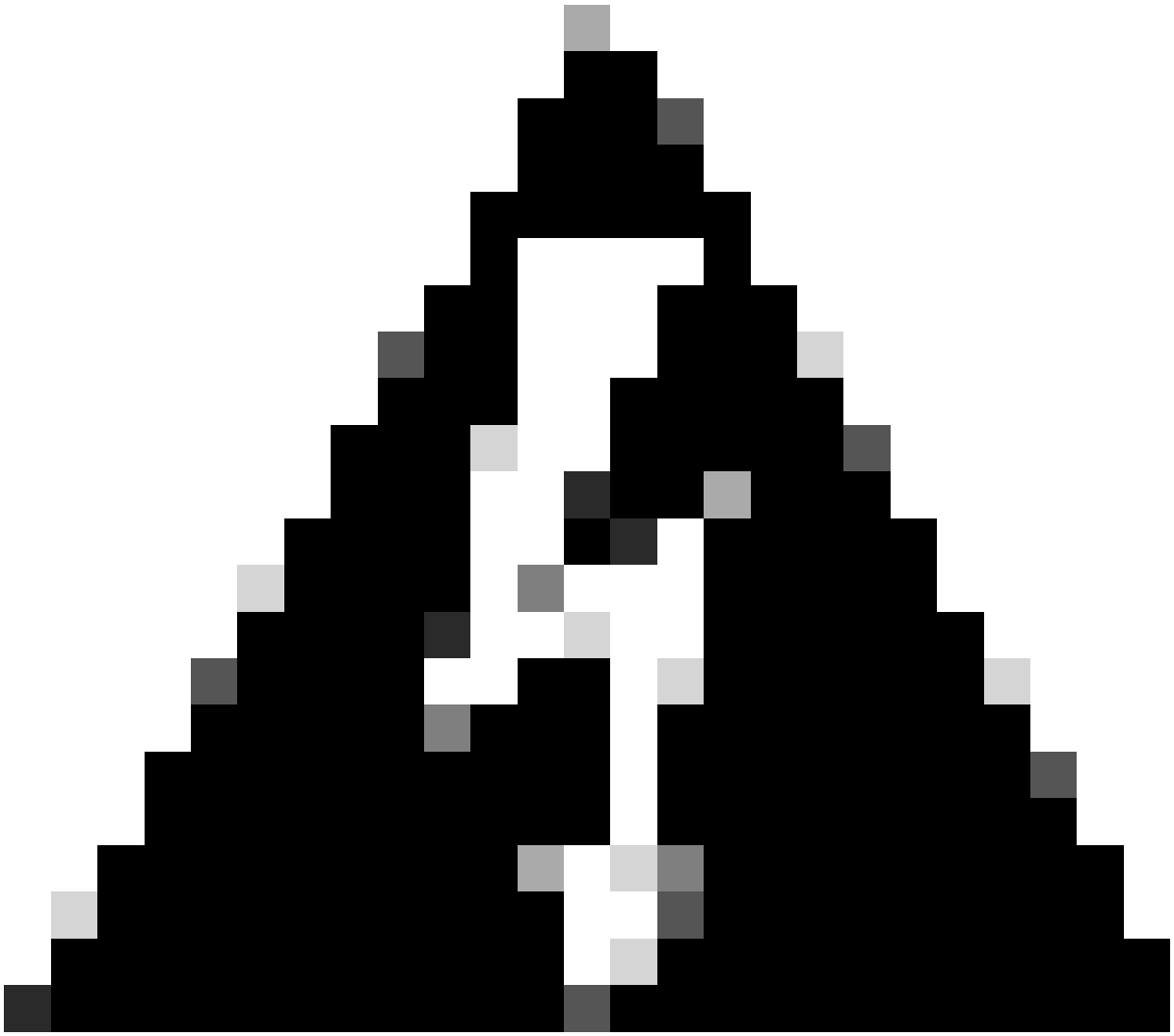
Opmerking: Als u Cisco Catalyst Center gebruikt en AAA-configuraties instelt, wordt automatisch de broninterface aan de servergroep toegevoegd. Dit verandert het standaardgedrag in fragment bij de grootte MTU van de interface die in dat bevel wordt gebruikt.

Hoe kan deze wijziging worden gebruikt?

Aangezien de standaard MTU van al uw interfaces 1500 zou zijn, zou dat de nieuwe MTU zijn om fragment te fragmenteren. De standaardinterface die voor al het RADIUS-verkeer wordt gebruikt, is de Wireless Management Interface (WMI). Wanneer u de configuratie van uw servergroep bekijkt, als er geen bron-interface opgegeven is, verstuurt WLC het RADIUS-verkeer op 1396 met behulp van de WMI. Als u echter in de servergroep configuratie gaat en vertelt dat de bron-interface WMI is, stuurt WLC nu het RADIUS-verkeer op 1500 nog steeds met WMI.

Ga er nu vanuit dat er een apparaat in het netwerk is zoals de VPN die eerder besproken is. U wilt niet dat het verkeer dubbel gefragmenteerd is, zodat u de MTU van de interface kunt veranderen in iets kleiner om de pakketten op een andere plaats te fragmenteren. Je kunt de MTU zo'n 1200

maken, zodat de pakketten gefragmenteerd worden bij de 1200 bytes markering in plaats van 1500.



Waarschuwing: Verandering van de MTU van WMI beïnvloedt al verkeer dat naar en van het WLC beheer IP adres gaat.

Ook al wil je de MTU van de WMI niet wijzigen, het punt van het specificeren van een broninterface is om het te veranderen van de WMI naar een andere interface, en die interface te gebruiken voor RADIUS verkeer, evenals de MTU op die interface te veranderen. Aangezien deze configuratie wordt uitgevoerd op het niveau van de servergroep, kunt u zeer specifiek zijn over welk RADIUS-verkeer u wilt dat deze wijziging wordt beïnvloed door.

Dit configuratiebestand is niet gekoppeld aan een AAA-server of WLAN. Het is mogelijk om meerdere servergroepen met dezelfde servers in te hebben en alleen de broninterface op een van hen te specificeren als u dat kiest. Deze servergroep wordt toegevoegd aan een methodelijst en vervolgens toegevoegd aan een WLAN. Zo, bijvoorbeeld, als er slechts één WLAN is waar u deze verandering wilt aanbrengen, zelfs als u slechts één AAA server hebt, kunt u een nieuwe

servergroep creëren, de ip straal bron-interface opdracht gebruiken die aan de interface met de MTU richt u wilt gebruiken, de AAA server aan deze nieuwe groep toevoegen, een nieuwe methodelijst creëren die deze nieuwe groep gebruikt, en dan die methodelijst toevoegen aan het specifieke WLAN waar u deze verandering wilt aanbrengen.

Waarschuwing: Het wordt altijd voorgesteld, wanneer het maken van om het even welke veranderingen in een levend netwerk, het wordt gedaan tijdens een onderhoudsvenster.

Het bewijs wordt geleverd in de pakketvastlegging

Het is algemeen bekendAls je dat in netwerken niet kon vastleggen, kan je het niet bewijzen. Hier zijn een paar configuratievoorbeelden met deze veranderingen om u te tonen hoe dit werkt.

Hier is een WLAN-configuratie. Tijdens het testen wordt alleen de servergroep die in de methodelijst wordt gebruikt, gewijzigd.

```
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
!
```

Het toevoegen van de bron-interface opdracht met de standaard MTU

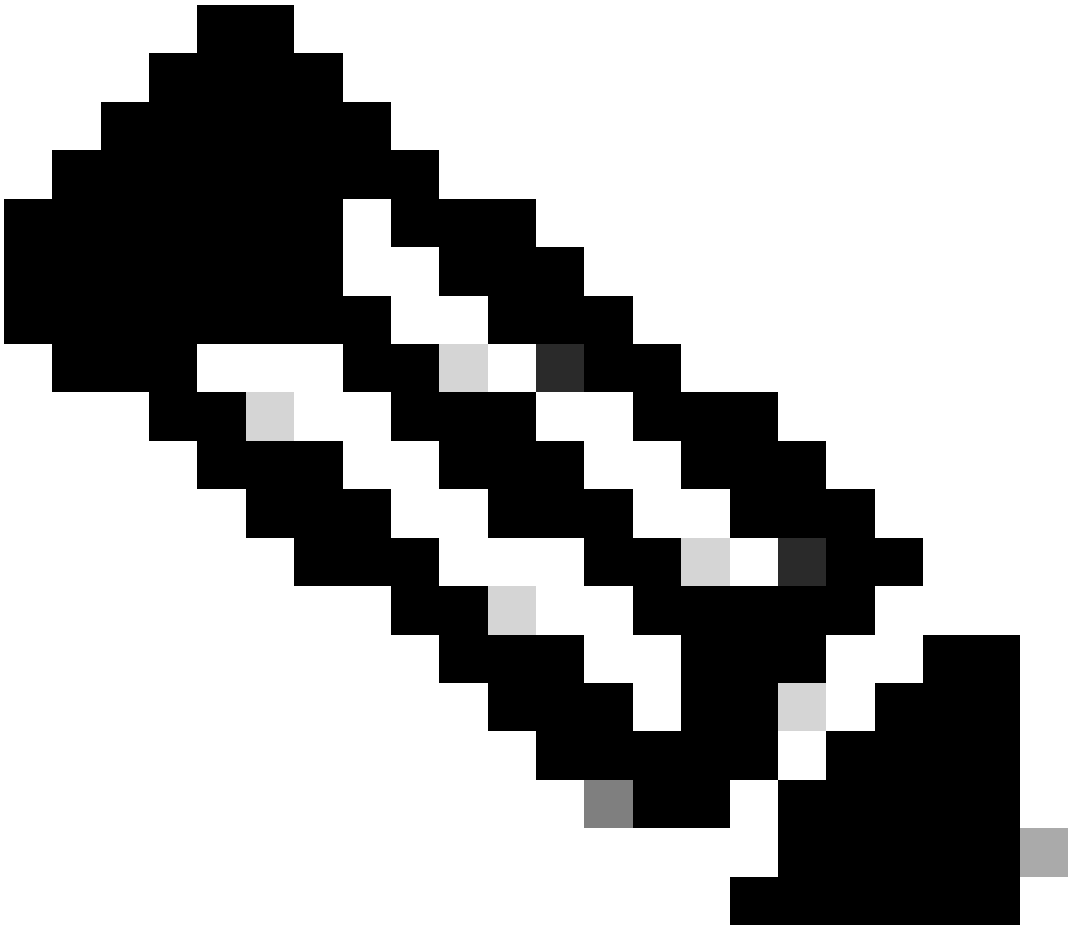
Hier is het gewoon een normale servergroep die naar de ISE-server wijst. De broninterface-opdracht is toegevoegd met aanwijzen naar mijn WMI die geen MTU-set heeft. Zo ziet de configuratie er uit.

```
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
```

Zoals u kunt zien, is de groep NoMTU-server toegevoegd aan de lijst met verificatiemethoden die aan het WLAN is gekoppeld. De opdracht IP radius source-interface VLAN260 wordt gebruikt voor deze servergroep en VLAN 260 geeft geen MTU-betekenis op, omdat het de MTU van 1500 gebruikt. Enkel om te bevestigen, kan MTU van 1500 u de show gebruiken in werking stelt al bevel en zoekt de interface in de output.

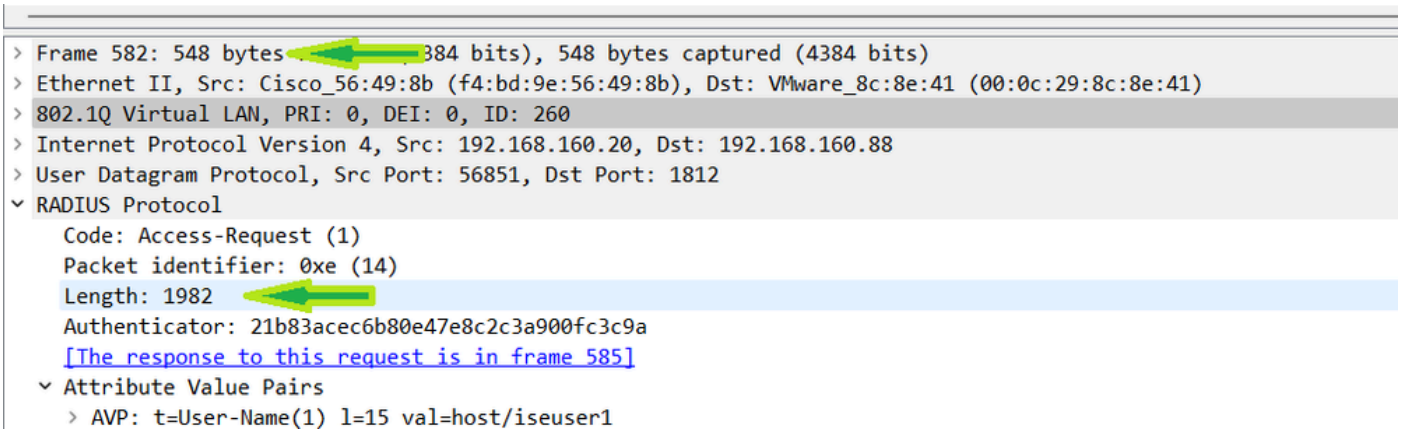
```
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
 no ip clear-dont-fragment
 ip redirects
 ip unreachables
 no ip proxy-arp
 ip mtu 1500
```

Bekijk nu het pakket waar de client cert naar ISE moet worden verzonden zodra de WLC de RADIUS-gegevens toevoegt:



Opmerking: Hier, de bytes op de lijn is 1518. Dit omvat kopballen buiten de nuttige lading Ethernet zoals de kopbal van VLAN en laag 2 kopbal. Deze worden niet meegeteld bij de 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]
```



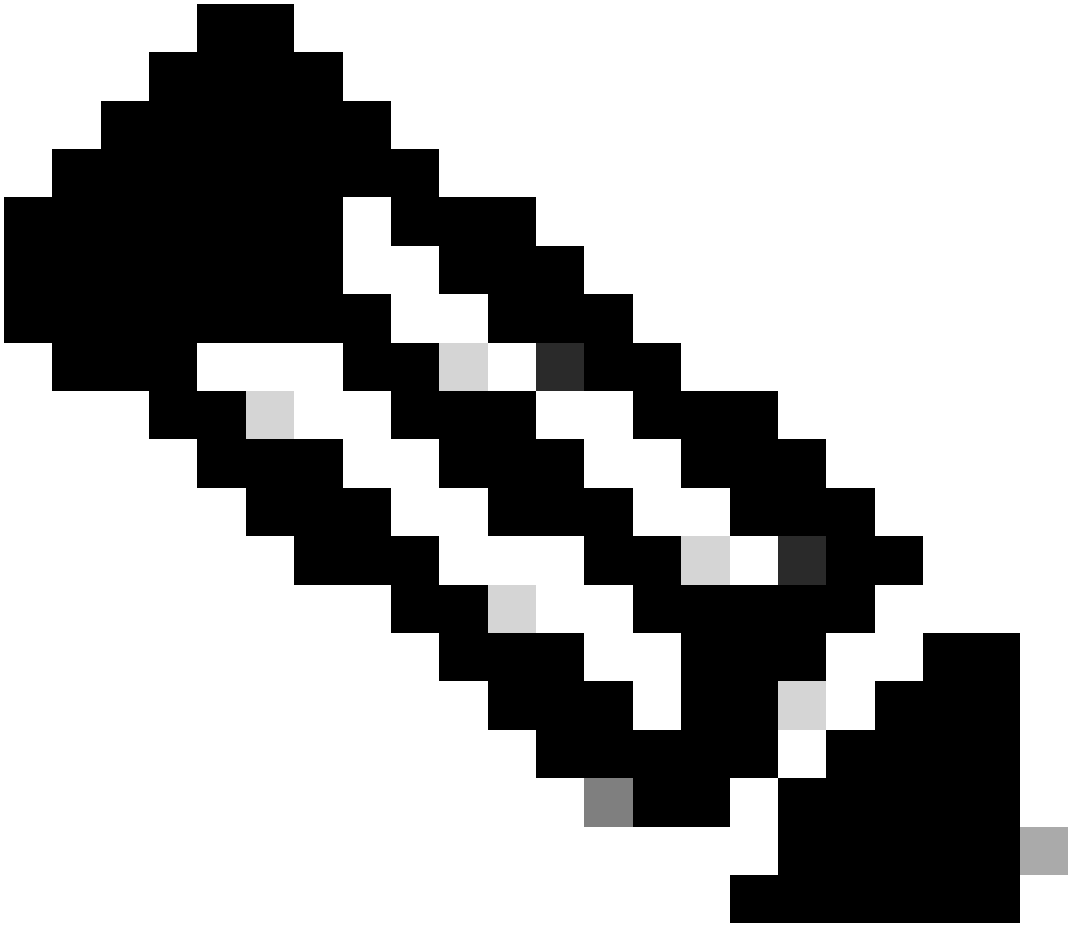
Hier kan je zien dat het gegevensgedeelte gefragmenteerd is op 1480. Je kunt dat fragment onder de 1500 MTU op de WMI krijgen. Het volgende pakket is minder dan 550 bytes, maar u kunt zien dat de totale grootte van de RADIUS-gegevens 1982 is. Dat gezegd hebbende, werkt het fragmenteren met de nieuwe MTU nu.

Een niet-WMI-interface met een MTU van 1200 gebruiken

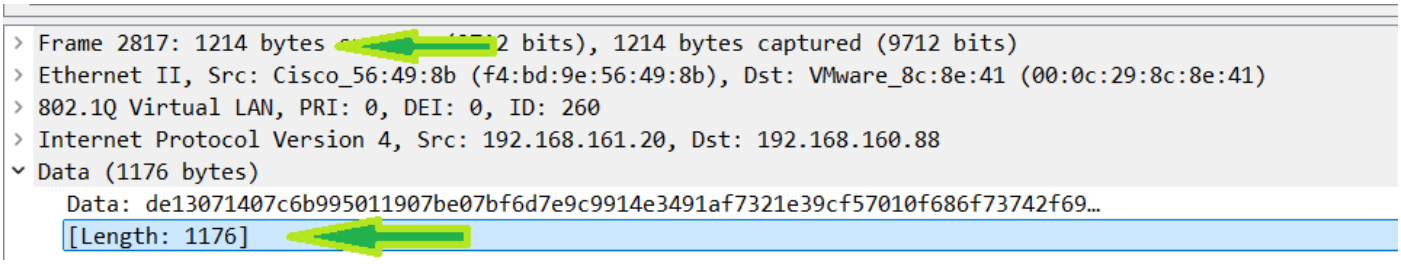
Stel nu dat je wilt fragmenteren bij een kleinere MTU, maar dat deze verandering geen invloed heeft op ander verkeer. Geen probleem hier, blijft de configuratie hetzelfde alleen de bron-interface-configuratie gaat naar een SVI die alleen voor dit doel is gemaakt. Verander de methodelijst om deze nieuwe servergroep aan te wijzen en deze servergroep gebruikt een bron-interface die niet mijn WMI is en MTU heeft ingesteld op 1200. Zo ziet de configuratie eruit:

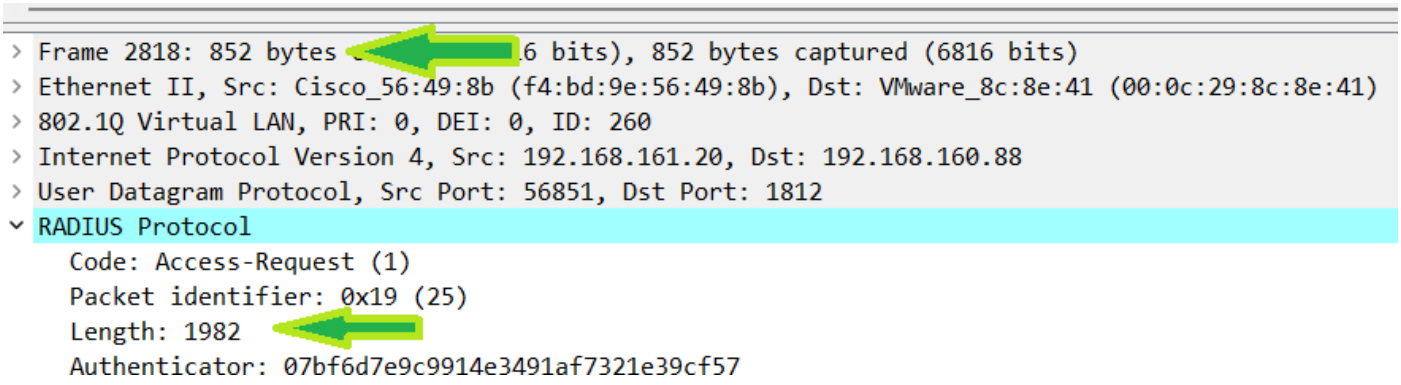
```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group MTU1200
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObFibbBMhNMFAbKUAAB
!
aaa group server radius MTU1200
 server name ISE
 ip radius source-interface Vlan261
 deadtime 5
!
9800#show run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

Zie vervolgens hoe de pakketten eruit zien met deze lagere MTU.



Opmerking: Het verlagen van de MTU en het veranderen van het fragmentatiepunt maakt geen deel uit van het nieuwe gedrag. Dit is altijd al waar geweest. Als het standaardgedrag van fragmenteren op 1396 niet onder MTU past, zou je altijd fragmenteren op een ander punt. Het maakt deel uit van deze sectie alleen maar om de beschikbare opties te helpen verklaren.





Hier zijn de RADIUS-gegevens nog steeds 1982 bytes, maar deze keer waren de gegevens gefragmenteerd op 1176 in plaats van de standaard 1376, het zou gefragmenteerd zijn op als de broninterface niet werd gebruikt. Herinner dat wanneer u MTU aan 1500 plaatst en het bron-interfacebevel gebruikt, u fragment op 1480 fragment. Met behulp van de configuratie hier kunt u het verkeer naar een lagere MTU manipuleren zonder te interfereren met ander verkeer op de WLC.

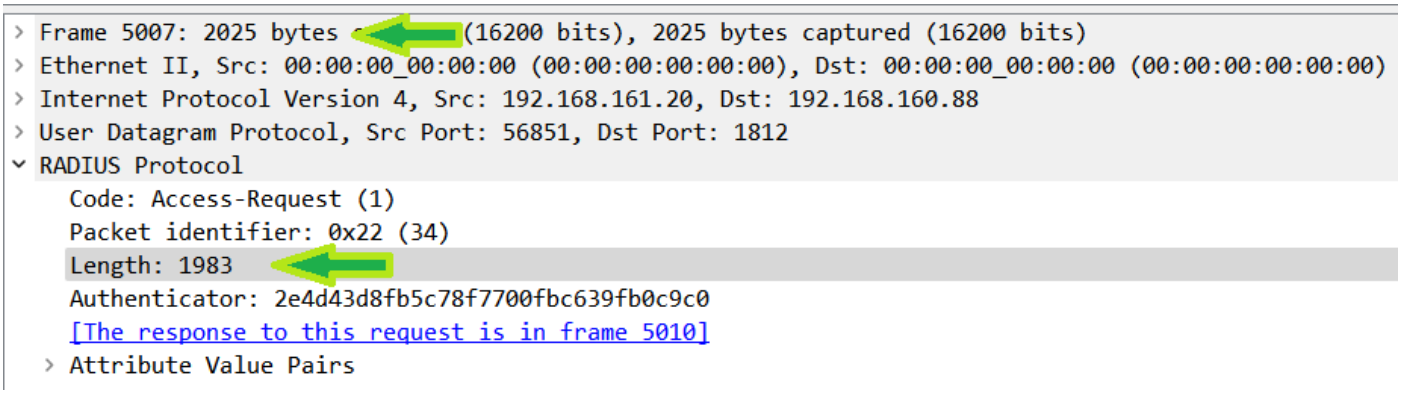
Een MTU van 9000 gebruiken voor jumboframes

Aangezien de optie werd gemaakt om jumboframes te verzenden, zou het een schande zijn om dat niet te testen ook nog steeds met behulp van de niet-WMI interface van VLAN 261. Nu is de IP MTU ingesteld op 9000. Een korte opmerking, om de IP MTU op de SVI te kunnen instellen, moet u de MTU op iets hoger dan de IP MTU instellen. U kunt dit zien in deze configuratie:

```
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
```

Hier, kijkend naar de opname, kun je zien dat het pakket nooit gefragmenteerd was. Het werd verzonden als één geheel pakket met de de gegevensgrootte van de RADIUS bij 1983. Houd in gedachten, om dit te werken de rest van het netwerk moet worden geconfigureerd om een pakket van deze grootte door toe te staan.

Een ander ding om hier op te merken is dat de client MTU niet is gewijzigd, zodat de client nog steeds het EAP-pakket fragmenteert op 1492. Het verschil is dat de WLC alle RADIUS-gegevens kan toevoegen die nodig zijn om het pakket naar ISE te verzenden, zonder dat de clientgegevens hoeven te worden gefragmenteerd.



Conclusie

Wanneer u EAP-TLS gebruikt, wordt verwacht dat de client zijn certificaat naar de AAA-server stuurt. Deze certificaten zijn meestal groter dan de MTU, dus de client moet ze fragmenteren. Het punt waarop de client de gegevens fragmenteert, ligt vrij dicht bij de MTU. Aangezien de AP de CAPWAP-header moet toevoegen, moet wat de client verzendt worden gefragmenteerd. De WLC ontvangt deze twee pakketten, zet ze weer samen maar moet het dan opnieuw fragmenteren om de RADIUS-gegevens toe te voegen. Op dit punt krijgt de netwerkbeheerder enige controle over hoe de WLC het EAP-pakket fragmenteert dat de client heeft verzonden.

Als u de IP straal bron-interface <interface u wilt gebruiken>opdracht toevoegt aan de AAA-servergroep, gebruikt de WLC de interface die u daar plaatst in plaats van (of inclusief) de WMI. Deze opdracht vertelt de WLC ook om fragment te fragmenteren bij wat de MTU van die interface is in plaats van de standaard 1396. Op deze manier heb je meer controle over hoe pakketten door het netwerk bewegen.

Wanneer u Cisco Catalyst Center gebruikt, wordt de opdracht broninterface toegevoegd aan de servergroep en verandert u dus het standaardgedrag.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.