# Problemen met fragmentatie oplossen: Beïnvloeding van c9800 draadloze controller met Azure

## Inhoud



## Inleiding

Dit document beschrijft een bekend probleem met het Azure-platform dat leidt tot pakketverlies als gevolg van de mishandeling van fragmenten die buiten de reeks vallen.

## Symptomen

getroffen producten: Catalyst 9800-CL draadloze controller die wordt gehost op Azure of Identity Service Engine die wordt gehost in Azure.

Instellen SSID: Geconfigureerd voor 802.1x EAP-TLS met centrale verificatie.

Gedrag : Bij gebruik van de 9800-CL die op het Azure-platform met een op EAP-TLS gebaseerde SSID wordt gehost, kunt u problemen met de connectiviteit ondervinden. De cliënten kunnen tijdens de authentificatiefase moeilijkheden ondervinden.

## Fout op ISE-server

Foutcode 5411 die aangeeft dat de aanvrager tijdens de uitwisseling van EAP-TLS-certificaten niet meer met ISE communiceert.

## Gedetailleerde loganalyse:

Hier is een illustratie van een van de getroffen configuraties: In de 9800 draadloze controller is de SSID ingesteld voor 802.1x en is de AAA-server geconfigureerd voor EAP-TLS. Wanneer een client verificatie probeert, met name tijdens de fase van de certificaatuitwisseling, stuurt de client een certificaat dat de maximale grootte van de transmissieeenheid (MTU) op de draadloze controller overschrijdt. De 9800 draadloze controller fragmenteert vervolgens dit grote pakket en stuurt de fragmenten sequentieel naar de AAA-server. Deze fragmenten komen echter niet in de juiste volgorde op de fysieke host aan, wat tot pakketverlies leidt.

Hier is de RA sporen van draadloze controller wanneer de client probeert verbinding te maken: De client voert de verificatiestatus van L2 in en er wordt een EAP-proces gestart

```
2023/04/12 16:51:27.606414 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] Invoeren van aanvraagstatus
2023/04/12 16:51:27.606425 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[0000.000.000:capwap_90000004] EAPOL-pakket verzenden
2023/04/12 16:51:27.606494 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] Verzonden EAPOL-pakket - versie : 3,EAPOL-
type : EAP, payloadlengte: 1008, EAP-Type = EAP-TLS
2023/04/12 16:51:27.606496 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] EAP-pakket - VERZOEK, ID : 0x25
2023/04/12 16:51:27.606536 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] EAPOL-pakket verzonden naar client
2023/04/12 16:51:27.640768 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] Ontvangen EAPOL-pakket - versie : 1,EAPOL-
type : EAP, payloadlengte: 6, EAP-Type = EAP-TLS
2023/04/12 16:51:27.640781 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] EAP-pakket - RESPONS, ID : 0x25
```

Wanneer de draadloze controller de toegangsaanvraag naar de AAA-server verstuurt en de pakketgrootte kleiner is dan 1500 bytes (wat de standaard MTU is op de draadloze controller), wordt de toegangsuitdaging zonder enige complicaties ontvangen.

```
2023/04/12 16:51:27.641094 {wncd_x_r0-0}{1}: [straal] [19224]: (info):
RADIUS: Verzend toegangsaanvraag naar 172.16.26.235:1812 id 0/6, len 552
2023/04/12 16:51:27.644693 {wncd_x_r0-0}{1}: [straal] [19224]: (info):
RADIUS: Ontvangen van ID 1812/6 172.16.26.235:0, Access-Challenge, len
1141
```

Soms kan een client zijn certificaat voor verificatie verzenden. Als de pakketgrootte MTU overschrijdt, zal het worden versplinterd alvorens verder wordt verzonden.

```
2023/04/12 16:51:27.758366 {wncd_x_r0-0}{1}: [straal] [19224]: (info):
RADIUS: Verzend toegangsaanvraag naar 172.16.26.235:1812 id 0/8, len
2048
2023/04/12 16:51:37.761885 {wncd_x_r0-0}{1}: [straal] [19224]: (info):
RADIUS: Time-out 5 seconden gestart
```

```
2023/04/12 16:51:42.762096 {wncd_x_r0-0}{1}: [straal] [19224]: (info):
RADIUS: Opnieuw verzenden naar (172.16.26.235:1812.1813) voor id 0/8
2023/04/12 16:51:32.759255 {wncd_x_r0-0}{1}: [straal] [19224]: (info):
RADIUS: Opnieuw verzenden naar (172.16.26.235:1812.1813) voor id 0/8
2023/04/12 16:51:32.760328 {wncd_x_r0-0}{1}: [straal] [19224]: (info):
RADIUS: Time-out 5 seconden gestart
2023/04/12 16:51:37.760552 {wncd_x_r0-0}{1}: [straal] [19224]: (info):
RADIUS: Opnieuw verzenden naar (172.16.26.235:1812.1813) voor id 0/8
2023/04/12 16:51:42.762096 {wncd_x_r0-0}{1}: [straal] [19224]: (info):
RADIUS: Opnieuw verzenden naar (172.16.26.235:1812.1813) voor id 0/8
```

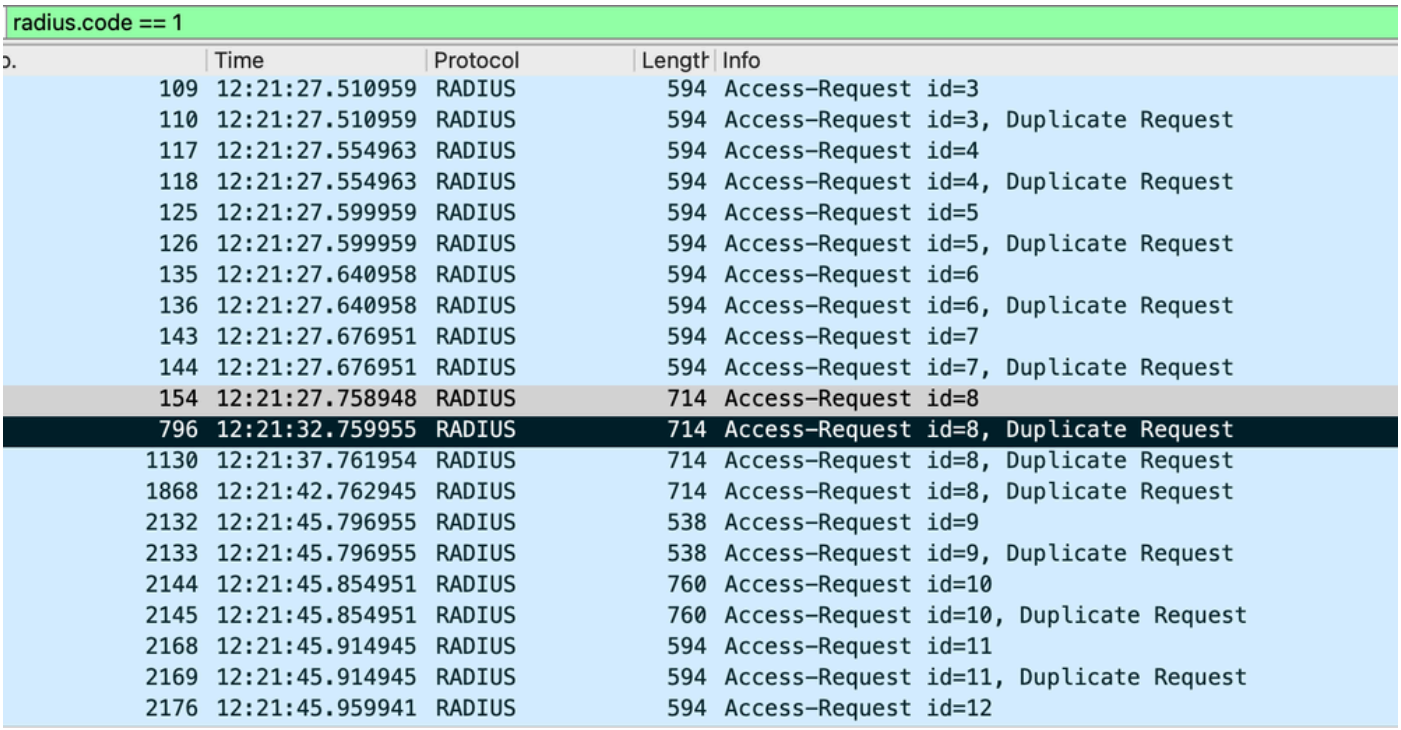
We hebben gemerkt dat de pakketgrootte 2048 is, wat de standaard MTU overtreft. Er is dus geen reactie van de AAA-server. De draadloze controller verstuurt de toegangsaanvraag voortdurend opnieuw tot het maximale aantal herhalingen is bereikt. Omdat er geen respons is, zal de draadloze controller uiteindelijk het EAPOL-proces opnieuw instellen.

```
2023/04/12 16:51:45.762890 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] Publicatie van EAPOL_START op client
2023/04/12 16:51:45.762956 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] Invoeren status
2023/04/12 16:51:45.762965 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] Posting!AUTH_ABORT op client
2023/04/12 16:51:45.762969 {wncd_x_r0-0}{1}: [dot1x] [19224]: (info):
[Client_MAC:capwap_90000004] Opnieuw opstarten inschakelen
```

Dit proces gaat in lijn en de client is alleen in de verificatiefase vastgezet.

De ingesloten pakketvastlegging die op de draadloze controller is opgenomen, toont aan dat de draadloze controller na verschillende toegangsaanvragen en uitwisselingen met een MTU van minder dan 1500 bytes een toegangsaanvraag van meer dan 1500 bytes verstuurt, die het certificaat van de client bevat. Dit grotere pakket ondergaat fragmentatie. Er wordt echter geen antwoord gegeven op dit specifieke verzoek om toegang. De draadloze controller blijft dit verzoek opnieuw verzenden tot het maximale aantal herhalingen is bereikt, waarna de EAP-TLS-sessie opnieuw wordt gestart. Deze opeenvolging van gebeurtenissen blijft zich herhalen, wat aangeeft dat er een EAP-TLS-lus optreedt terwijl de client probeert te verifiëren. Raadpleeg de gelijktijdige pakketopnamen van zowel de draadloze controller als de ISE-module hieronder voor een beter begrip.

## Draadloze controller EPC:

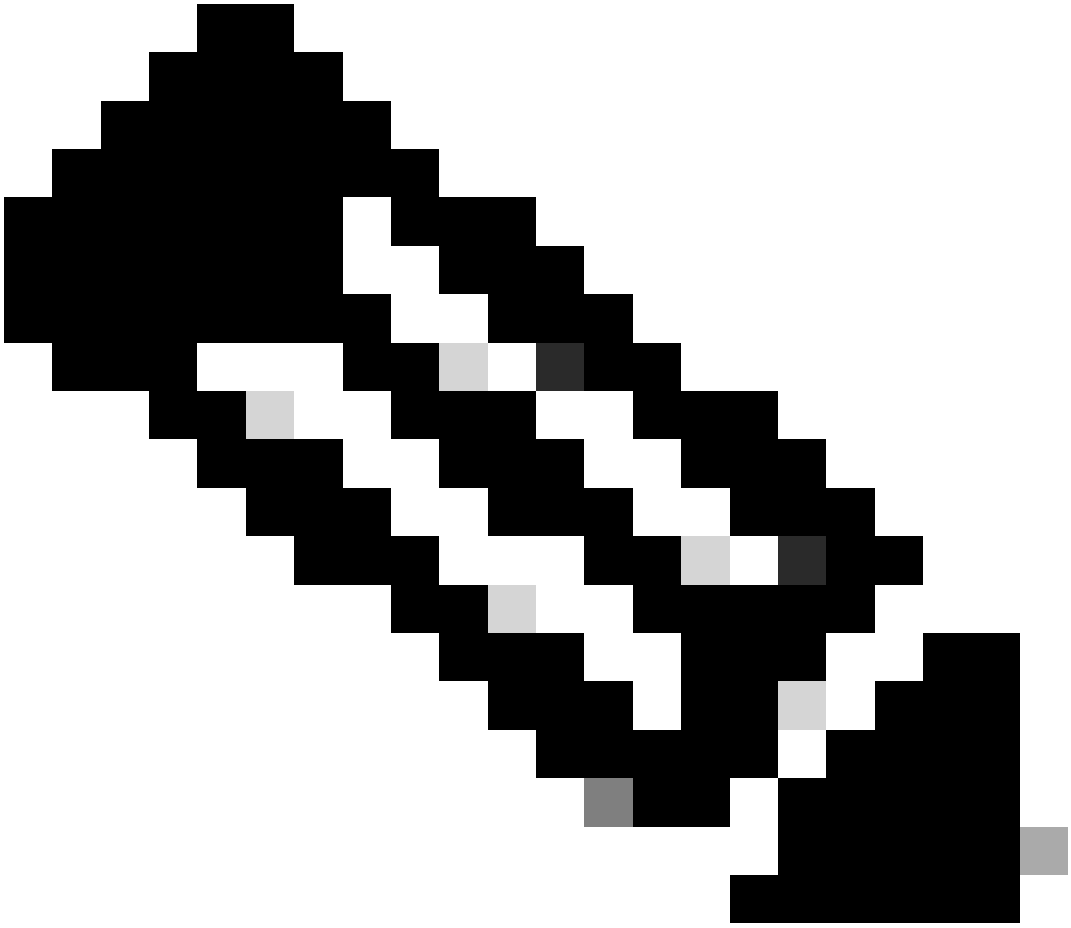


radius.code == 1

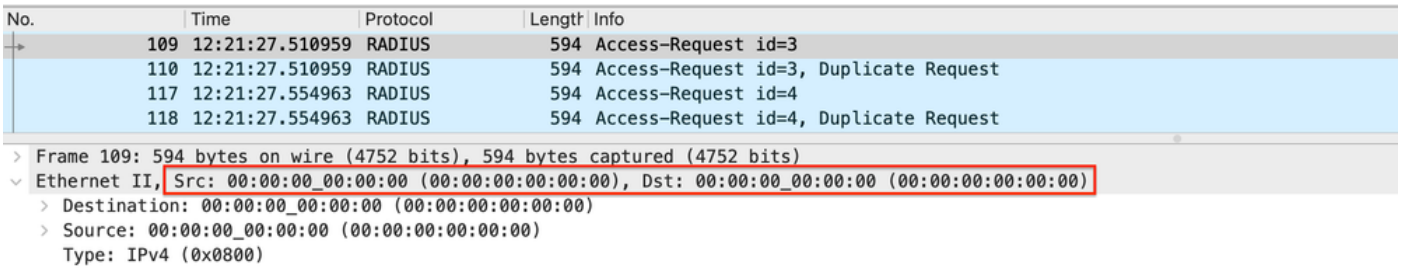
| ). | Time | Protocol | Length | Info |
|---|---|---|---|---|
| 109 | 12:21:27.510959 | RADIUS | 594 | Access-Request id=3 |
| 110 | 12:21:27.510959 | RADIUS | 594 | Access-Request id=3, Duplicate Request |
| 117 | 12:21:27.554963 | RADIUS | 594 | Access-Request id=4 |
| 118 | 12:21:27.554963 | RADIUS | 594 | Access-Request id=4, Duplicate Request |
| 125 | 12:21:27.599959 | RADIUS | 594 | Access-Request id=5 |
| 126 | 12:21:27.599959 | RADIUS | 594 | Access-Request id=5, Duplicate Request |
| 135 | 12:21:27.640958 | RADIUS | 594 | Access-Request id=6 |
| 136 | 12:21:27.640958 | RADIUS | 594 | Access-Request id=6, Duplicate Request |
| 143 | 12:21:27.676951 | RADIUS | 594 | Access-Request id=7 |
| 144 | 12:21:27.676951 | RADIUS | 594 | Access-Request id=7, Duplicate Request |
| 154 | 12:21:27.758948 | RADIUS | 714 | Access-Request id=8 |
| 796 | 12:21:32.759955 | RADIUS | 714 | Access-Request id=8, Duplicate Request |
| 1130 | 12:21:37.761954 | RADIUS | 714 | Access-Request id=8, Duplicate Request |
| 1868 | 12:21:42.762945 | RADIUS | 714 | Access-Request id=8, Duplicate Request |
| 2132 | 12:21:45.796955 | RADIUS | 538 | Access-Request id=9 |
| 2133 | 12:21:45.796955 | RADIUS | 538 | Access-Request id=9, Duplicate Request |
| 2144 | 12:21:45.854951 | RADIUS | 760 | Access-Request id=10 |
| 2145 | 12:21:45.854951 | RADIUS | 760 | Access-Request id=10, Duplicate Request |
| 2168 | 12:21:45.914945 | RADIUS | 594 | Access-Request id=11 |
| 2169 | 12:21:45.914945 | RADIUS | 594 | Access-Request id=11, Duplicate Request |
| 2176 | 12:21:45.959941 | RADIUS | 594 | Access-Request id=12 |

Packet Capture op WLC

Wij merken op dat de draadloze controller meerdere dubbele aanvragen voor een bepaalde Access-request ID = 8 verstuurt

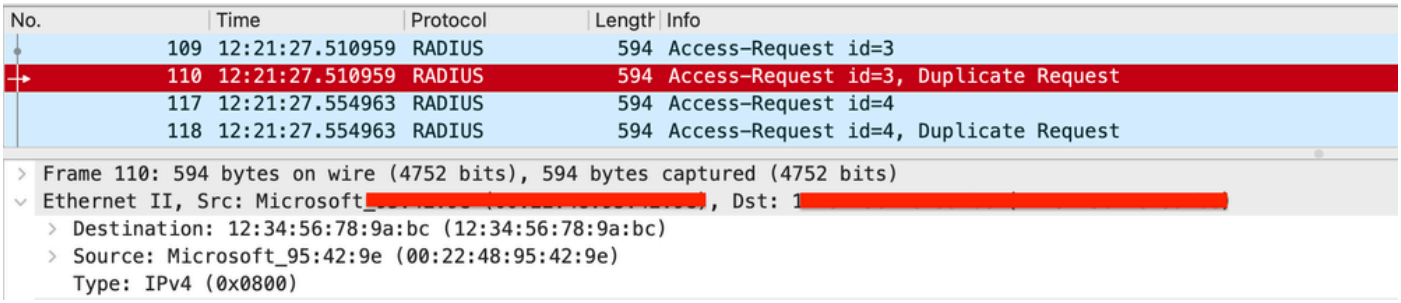


Opmerking: Wat de EPC betreft, merken we ook op dat er slechts één dubbel verzoek is voor andere ID's. Dit roept de vraag op: Verwacht u een dergelijke duplicatie? Het antwoord op de vraag of deze duplicatie wordt verwacht, is ja, dat is het. De reden is dat de opname is genomen van de GUI van de draadloze controller met de optie 'Monitor Control Plane' geselecteerd. Hierdoor is het normaal dat u meerdere RADIUS-pakketten waarneemt, omdat deze naar de CPU worden gestuurd. In dergelijke gevallen moeten toegangsaanvragen worden gezien met zowel de bron- als de doelMAC-adressen die zijn ingesteld op 00:00:00.



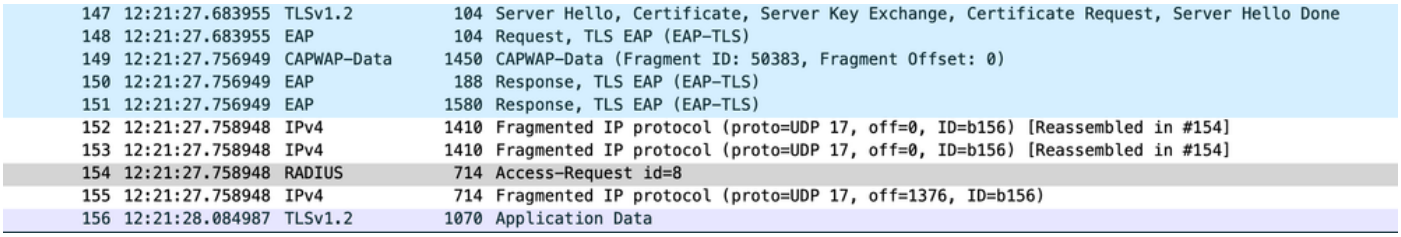

Radius access-aanvraag bestraft met CPU op WLC

Alleen de toegangsaanvragen met de opgegeven bron- en doelMAC-adressen moeten daadwerkelijk worden verzonden vanuit de draadloze controller.

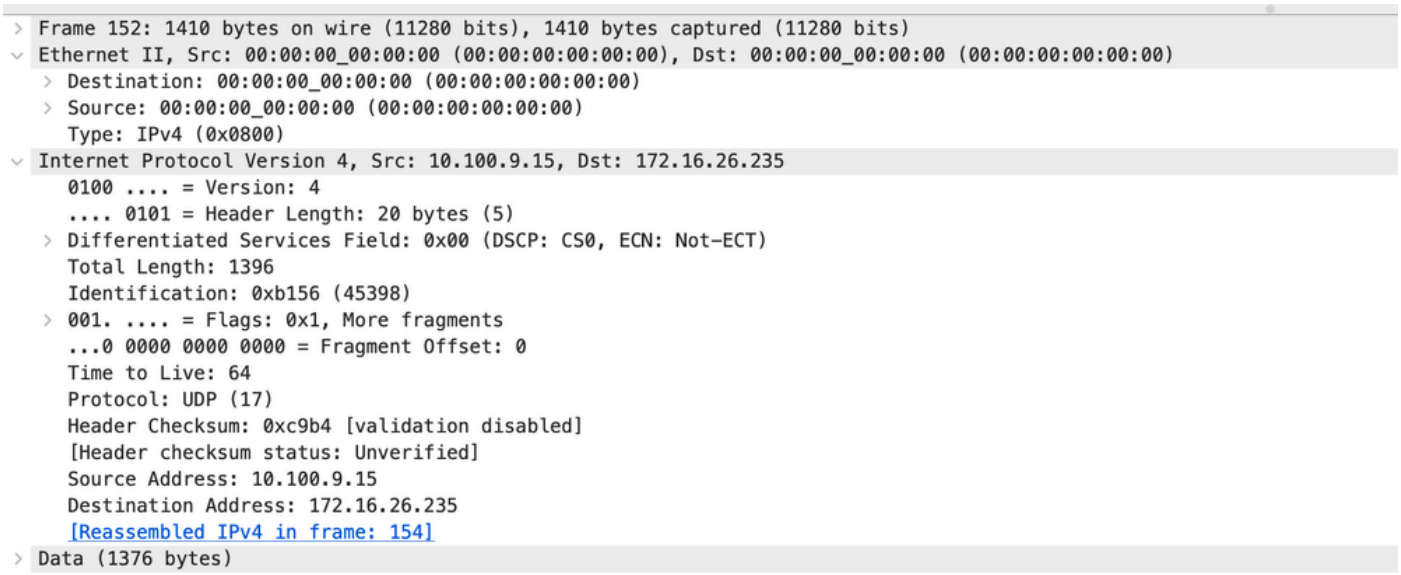



Radius access-aanvraag verzonden naar AAA-server

De toegangsaanvragen in kwestie, geïdentificeerd door ID = 8, die meerdere keren worden verzonden en waarvoor geen antwoord werd gezien vanaf AAA-server. Bij nader onderzoek hebben we vastgesteld dat voor Access-request ID=8 UDP-fragmentatie optreedt vanwege de grootte die de MTU overtreft, zoals hieronder wordt geïllustreerd:




Fragmentation die op WLC-pakketvastlegging plaatsvindt




Gefragmenteerd pakket - I

```
> Frame 153: 1410 bytes on wire (11280 bits), 1410 bytes captured (11280 bits)
v Ethernet II, Src: Microsoft_[redacted] Dst: [redacted]
  > Destination: 12:34:56:78:9a:bc (12:34:56:78:9a:bc)
  > Source: Microsoft_95:42:9e (00:22:48:95:42:9e)
    Type: IPv4 (0x0800)
v Internet Protocol Version 4, Src: 10.100.9.15, Dst: 172.16.26.235
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1396
    Identification: 0xb156 (45398)
  > 001. .... = Flags: 0x1, More fragments
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xc9b4 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.100.9.15
    Destination Address: 172.16.26.235
    [Reassembled IPv4 in frame: 154]
```

Gefragmenteerd pakket - II

```
        152 12:21:27.758948 IPv4          1410 Fragmented IP protocol (proto=UDP 17, off=0, ID=b156) [Reassembled in #154]
        153 12:21:27.758948 IPv4          1410 Fragmented IP protocol (proto=UDP 17, off=0, ID=b156) [Reassembled in #154]
        154 12:21:27.758948 RADIUS         714 Access-Request id=8
        155 12:21:27.758948 IPv4           714 Fragmented IP protocol (proto=UDP 17, off=1376, ID=b156)

> Frame 154: 714 bytes on wire (5712 bits), 714 bytes captured (5712 bits)
> Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
v Internet Protocol Version 4, Src: 10.100.9.15, Dst: 172.16.26.235
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 700
    Identification: 0xb156 (45398)
  > 000. .... = Flags: 0x0
    ...0 0000 1010 1100 = Fragment Offset: 1376
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0xebc0 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.100.9.15
    Destination Address: 172.16.26.235
v   [3 IPv4 Fragments (2056 bytes): #152(1376), #153(1376), #154(680)]
      [Frame: 152, payload: 0-1375 (1376 bytes)]
    > [Frame: 153, payload: 0-1375 (1376 bytes)]
      [Frame: 154, payload: 1376-2055 (680 bytes)]
      [Fragment count: 3]
      [Reassembled IPv4 length: 2056]
```

Hergemonteerd pakket

Om te verifiëren, hebben we de ISE-logboeken bekeken en ontdekt dat het toegangsverzoek, dat was gefragmenteerd op de draadloze controller, helemaal niet door de ISE werd ontvangen.

## ISE-TCP-dompels

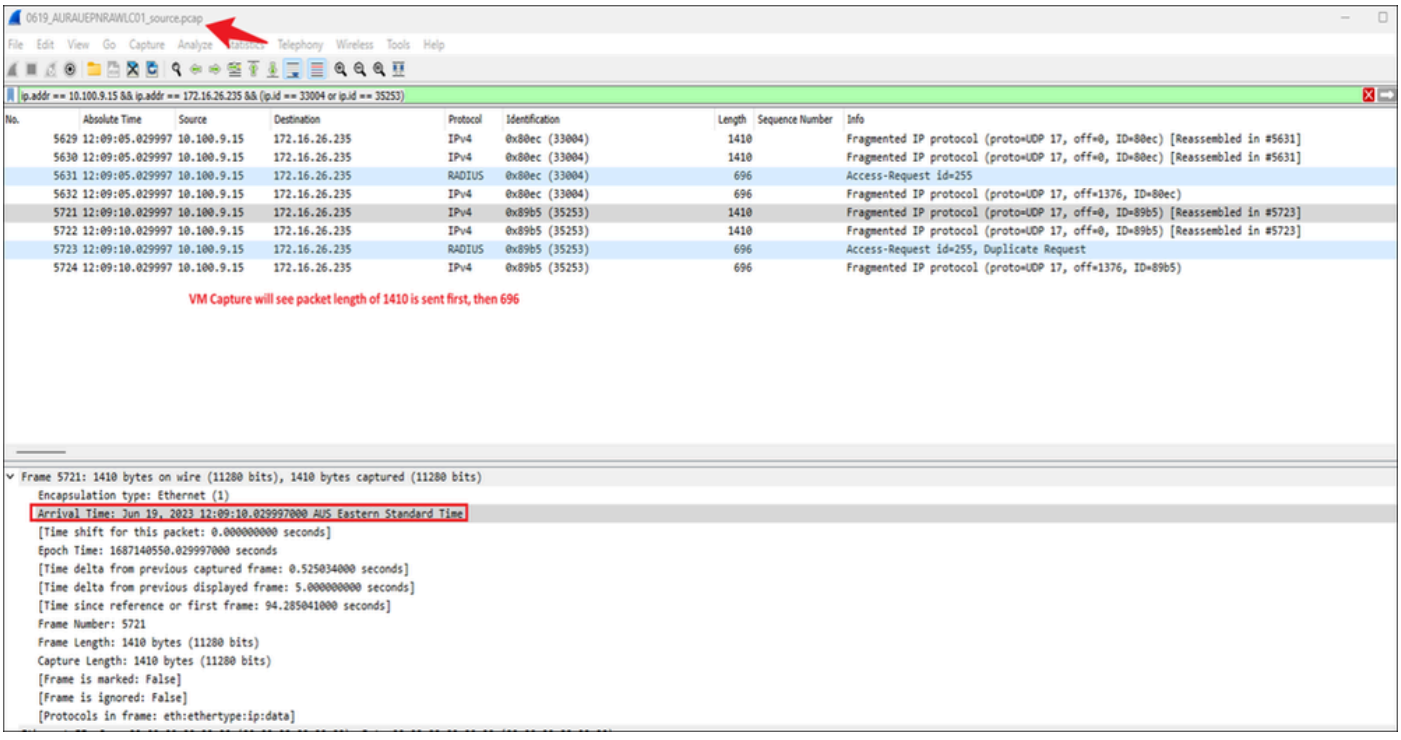
radius.code == 1

| o. | Time | Protocol | Lengtr | Info |
|---|---|---|---|---|
| 1 | 12:21:27.387158 | RADIUS | 538 | Access-Request id=0 |
| 3 | 12:21:27.428304 | RADIUS | 760 | Access-Request id=1 |
| 5 | 12:21:27.492019 | RADIUS | 594 | Access-Request id=2 |
| 7 | 12:21:27.527949 | RADIUS | 594 | Access-Request id=3 |
| 9 | 12:21:27.572272 | RADIUS | 594 | Access-Request id=4 |
| 11 | 12:21:27.617147 | RADIUS | 594 | Access-Request id=5 |
| 13 | 12:21:27.657917 | RADIUS | 594 | Access-Request id=6 |
| 15 | 12:21:27.694381 | RADIUS | 594 | Access-Request id=7 |
| 17 | 12:21:45.814195 | RADIUS | 538 | Access-Request id=9 |
| 19 | 12:21:45.871163 | RADIUS | 760 | Access-Request id=10 |
| 21 | 12:21:45.932076 | RADIUS | 594 | Access-Request id=11 |
| 23 | 12:21:45.977012 | RADIUS | 594 | Access-Request id=12 |
| 25 | 12:21:46.018562 | RADIUS | 594 | Access-Request id=13 |

Opnamen op ISE-end

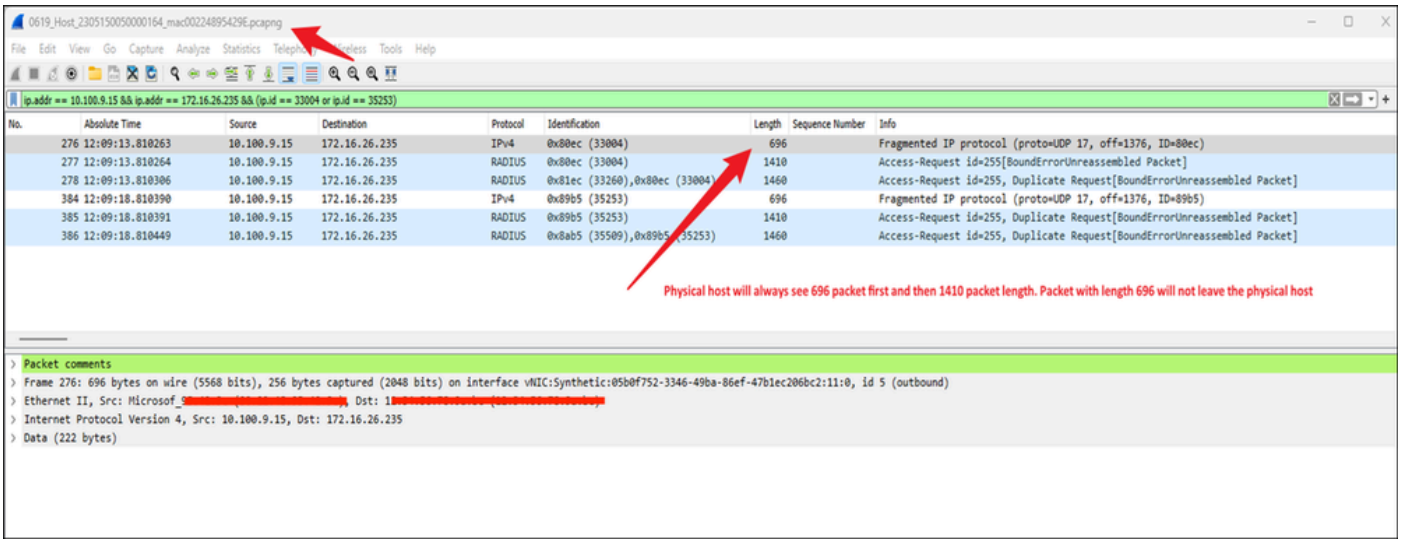
## Azure Side Capture met analyse:

Het Azure-team heeft een vastlegging uitgevoerd op de fysieke host in Azure. De gegevens die op de vSwitch in de Azure-host zijn opgenomen, geven aan dat de UDP-pakketten niet meer in volgorde van ontvangst zijn. Omdat deze UDP-fragmenten niet in de juiste volgorde staan, worden ze door Azure verwijderd. Hieronder staan de opnamen van zowel de Azure-eindapparatuur als de draadloze controller, die gelijktijdig worden genomen voor toegangsaanvraag ID = 255, waarbij de kwestie van pakketten die niet in orde zijn duidelijk is:
De Encapsulated Packet Capture (EPC) op de draadloze controller toont de volgorde waarin de gefragmenteerde pakketten van de draadloze controller vertrekken.




Sequentie van gefragmenteerde pakketten op WLC

Op de fysieke host komen de pakketten niet in de juiste volgorde aan




Opname op Azure End

Aangezien de pakketten in de verkeerde orde aankomen, en de fysieke knoop wordt geprogrammeerd om het even welke uit-van-ordekaders te verwerpen, worden de pakketten onmiddellijk gelaten vallen. Deze onderbreking veroorzaakt dat het verificatieproces mislukt, waardoor de client niet verder kan gaan dan de verificatiefase.

## Aanbevolen tijdelijke oplossing van eindpunt draadloze controller:

Vanaf versie 17.11.1 implementeren we ondersteuning voor Jumbo Frames in Radius/AAA-pakketten. Met deze functie kan de c9800-controller fragmentatie van AAA-pakketten voorkomen, mits de volgende configuratie op de controller is ingesteld. Houd er rekening mee dat om fragmentatie van deze pakketten volledig te voorkomen, het essentieel is om ervoor te zorgen dat elke netwerkhop, inclusief de AAA-server, compatibel is met Jumbo Frame-pakketten. Voor ISE begint de ondersteuning van Jumbo Frame met versie 3.1 en verder.
Interfaceconfiguratie op draadloze controller:

C9800-CL(config)#interface

C9800-CL(config-if) # mtu

C9800-CL(config-if) # ip mtu

[1500 to 9000]

AAA-serverconfiguratie op draadloze controller:

C9800-CL(config)# aaa group server radius

C9800-CL(config-sg-radius) # server name

```
C9800-CL(config-sg-radius) # ip radius source-interface
```

Hier is een korte blik op een pakket van de Straal wanneer de MTU (Maximum Transmission Unit) aan 3000 bytes op een Draadloze LAN Controller (WLC) wordt gevormd. Pakketten kleiner dan 3000 bytes werden naadloos verzonden zonder dat er fragmentatie nodig was:

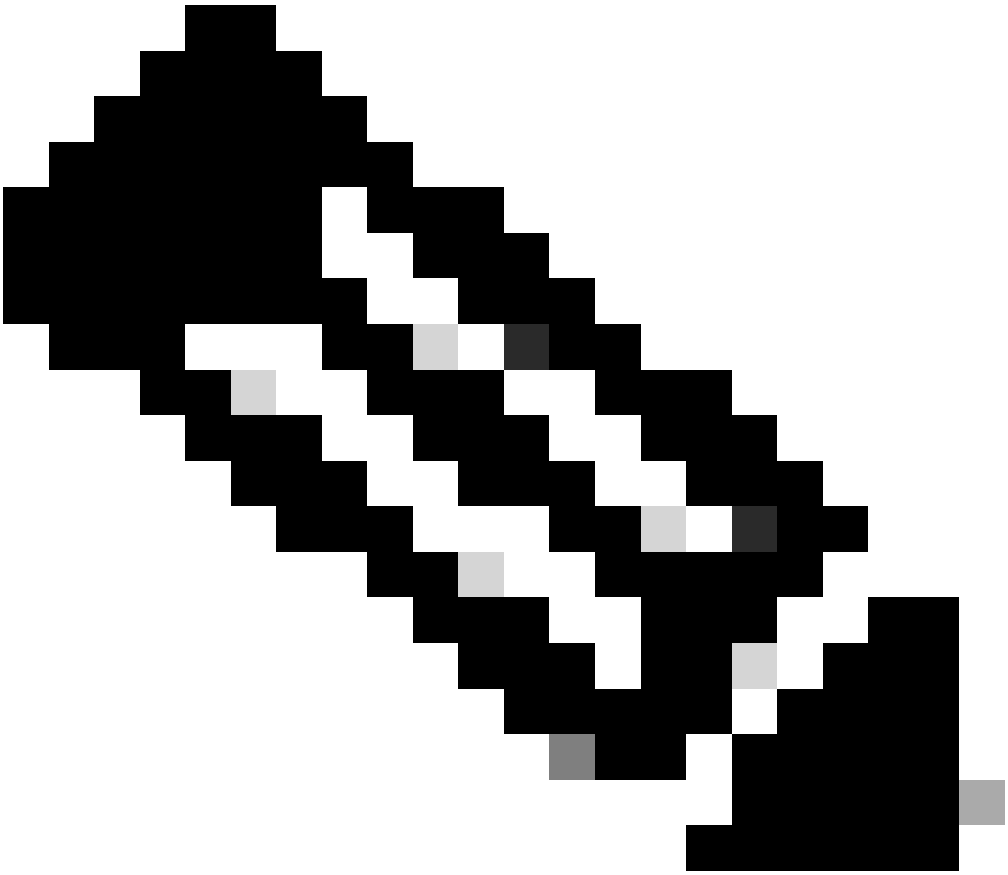
| | | | | |
|---|---|---|---|---|
| 1020 | 10:08:11.177984 | RADIUS | 2075 | Access-Request id=199 |
| 1021 | 10:08:11.177984 | RADIUS | 2075 | Access-Request id=199, Duplicate Request |
| 1119 | 10:08:16.194981 | RADIUS | 2075 | Access-Request id=199, Duplicate Request |
| 1120 | 10:08:16.194981 | RADIUS | 2075 | Access-Request id=199, Duplicate Request |
| 1223 | 10:08:21.179983 | RADIUS | 2075 | Access-Request id=199, Duplicate Request |
| 1224 | 10:08:21.179983 | RADIUS | 2075 | Access-Request id=199, Duplicate Request |
| 1451 | 10:08:26.180990 | RADIUS | 2075 | Access-Request id=199, Duplicate Request |
| 1452 | 10:08:26.180990 | RADIUS | 2075 | Access-Request id=199, Duplicate Request |
| 2470 | 10:08:31.181982 | RADIUS | 2075 | Access-Request id=199, Duplicate Request |

Packet Capture op WLC met verhoogde MTU

Door de configuratie op deze manier in te stellen, brengt de draadloze controller pakketten over zonder ze te fragmenteren, waardoor ze intact worden verzonden. Omdat Azure Cloud geen jumboframes ondersteunt, kan deze oplossing echter niet worden geïmplementeerd.

# Oplossing:

- Vanuit de EPC (Encapsulated Packet Capture) van de draadloze controller hebben we gemerkt dat de pakketten in de juiste volgorde worden verzonden. Het is dan de verantwoordelijkheid van de ontvangende host om ze correct te hermonteren en verder te gaan met de verwerking, wat in dit geval niet gebeurt aan de kant van Azure.
- Om de kwestie van out-of-order UDP-pakketten aan te pakken, moet het`enable-udp-fragment-reordering`optioneel worden geactiveerd op Azure.
- U moet contact opnemen met Azure-ondersteuningsteam voor hulp bij deze kwestie. Microsoft heeft dit probleem erkend.



Opmerking: Het moet worden opgemerkt dat dit probleem niet exclusief is voor de draadloze LAN-controller (WLC). Soortgelijke problemen met out-of-order UDP-pakketten zijn aangetroffen op verschillende radiusservers, waaronder ISE-, Forti Authenticator- en RTSP-servers, met name wanneer ze werken in de Azure-omgeving.

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.