

分段疑難排解：影響使用Azure的c9800無線控制器

目錄

[簡介](#)

[症狀](#)

[ISE伺服器出錯](#)

[詳細日誌分析：](#)

[無線控制器EPC:](#)

[ISE TCP轉儲](#)

[Azure Side Capture with analysis:](#)

[無線控制器端建議的解決方法：](#)

[解決方案：](#)

簡介

本文檔描述了Azure平台的一個已知問題，該問題導致由於處理亂序片段錯誤而導致資料包丟失。

症狀

受影響的產品：託管在Azure上的Catalyst 9800-CL無線控制器或託管在Azure上的身份服務引擎。

SSID設定：配置為使用中央身份驗證的802.1x EAP-TLS。

行為：在使用基於EAP-TLS的SSID的Azure平台上託管的9800-CL時，您可能會遇到連線問題。客戶端在身份驗證階段可能會遇到困難。

ISE伺服器出錯

錯誤代碼5411，指示請求方在EAP-TLS證書交換期間已停止與ISE的通訊。

詳細日誌分析：

以下是其中一個受影響配置的圖示：在9800無線控制器中，為802.1x設定SSID，並將AAA伺服器配置為EAP-TLS。當客戶端嘗試身份驗證時，特別是在證書交換階段，客戶端傳送超過無線控制器上最大傳輸單位(MTU)大小的證書。9800無線控制器接著將此大型封包分段，並將分段順序傳送到AAA伺服器。但是，這些片段未能以正確順序到達實體主機，因此導致封包捨棄。

以下是在使用者端嘗試連線時來自無線控制器的RA追蹤：

進入L2身份驗證狀態和EAP進程的客戶端已啟動

```
2023/04/12 16:51:27.606414 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004] 進入請求狀態
2023/04/12 16:51:27.606425 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [0000.0000.0000:capwap_900000004] 傳送EAPOL資料包
2023/04/12 16:51:27.606494 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004] 傳送的EAPOL資料包 — 版本 : 3,EAPOL型別 : EAP , 負載長度 : 1008,EAP-Type = EAP-TLS
2023/04/12 16:51:27.606496 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004] EAP資料包 — 請求 , ID:0x25
2023/04/12 16:51:27.606536 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004] EAPOL資料包傳送到客戶端
2023/04/12 16:51:27.640768 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004] 收到的EAPOL資料包 — 版本 : 1,EAPOL型別 : EAP , 負載長度 : 6,EAP-Type = EAP-TLS
2023/04/12 16:51:27.640781 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004] EAP資料包 — 響應 , ID :0x25
```

當無線控制器向AAA伺服器傳送存取要求，且封包大小低於1500位元組（這是無線控制器上的預設MTU）時，會收到存取質詢，而不會出現任何複雜情況。

```
2023/04/12 16:51:27.641094 {wncd_x_R0-0}{1}:[radius] [19224]: ( 資訊 ) : RADIUS:將訪問請求傳送到172.16.26.235:1812 id 0/6,len 552
2023/04/12 16:51:27.644693 {wncd_x_R0-0}{1}:[radius] [19224]: ( 資訊 ) : RADIUS:接收自id 1812/6 172.16.26.235:0, Access-Challenge , len 1141
```

有時，客戶端可能會傳送其證書以進行身份驗證。如果封包大小超過MTU，會在進一步傳送之前將其分段。

```
2023/04/12 16:51:27.758366 {wncd_x_R0-0}{1}:[radius] [19224]: ( 資訊 ) : RADIUS:傳送訪問請求到172.16.26.235:1812 id 0/8,len 2048
2023/04/12 16:51:37.761885 {wncd_x_R0-0}{1}:[radius] [19224]: ( 資訊 ) : RADIUS:已啟動5秒超時
2023/04/12 16:51:42.762096 {wncd_x_R0-0}{1}:[radius] [19224]: ( 資訊 ) : RADIUS:ID 0/8重新傳輸到(172.16.26.235:1812,1813)
2023/04/12 16:51:32.759255 {wncd_x_R0-0}{1}:[radius] [19224]: ( 資訊 ) : RADIUS:ID 0/8重新傳輸到(172.16.26.235:1812,1813)
2023/04/12 16:51:32.760328 {wncd_x_R0-0}{1}:[radius] [19224]: ( 資訊 ) : RADIUS:已啟動5秒超時
2023/04/12 16:51:37.760552 {wncd_x_R0-0}{1}:[radius] [19224]: ( 資訊 ) : RADIUS:ID 0/8重新傳輸到(172.16.26.235:1812,1813)
2023/04/12 16:51:42.762096 {wncd_x_R0-0}{1}:[radius] [19224]: ( 資訊 ) : RADIUS:ID 0/8重新傳輸到(172.16.26.235:1812,1813)
```

我們注意到封包大小為2048，超過預設MTU。因此，沒有來自AAA伺服器的響應。無線控制器將持續重新傳送訪問請求，直到達到最大重試次數。由於沒有響應，無線控制器將最終重置EAPOL進程。

```
2023/04/12 16:51:45.762890 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004]在客戶端上發佈EAPOL_START
2023/04/12 16:51:45.762956 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004]進入init狀態
2023/04/12 16:51:45.762965 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004]在客戶端上發佈！AUTH_ABORT
2023/04/12 16:51:45.762969 {wncd_x_R0-0}{1}:[dot1x] [19224]: ( 資訊 ) : [Client_MAC:capwap_900000004]進入重新啟動狀態
```

此程式處於循環中，並且客戶端僅停滯在身份驗證階段。

在無線控制器上捕獲的嵌入式資料包捕獲顯示，在與小於1500位元組的MTU進行多次訪問請求和質詢交換後，無線控制器將傳送一個大於1500位元組的訪問請求，該請求包含客戶端證書。此較大封包將進行分段。但是，沒有響應此特定訪問請求。無線控制器將繼續重新傳送此請求，直到達到最大重試次數，之後EAP-TLS會話將重新啟動。此事件序列不斷重複，表明客戶端嘗試進行身份驗證時出現EAP-TLS環路。請參閱下面提供的無線控制器和ISE的併發資料包捕獲，以瞭解更清楚的資訊。

無線控制器EPC:

radius.code == 1				
No.	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

WLC上的封包擷取

我們觀察到無線控制器正在傳送對特定訪問請求ID = 8的多個重複請求



附註：在EPC上，我們還注意到有一個對其他ID的重複請求。這就引出了一個問題：是否應該出現這種重複？對於這種重複是否應該出現，答案是肯定的。原因是在選擇了「Monitor Control Plane」選項的情況下，從無線控制器的GUI擷取擷取。因此，觀察幾個RADIUS封包的範例是正常的，因為這些封包是導向到CPU。在這種情況下，訪問請求必須同時包含源和目標MAC地址設定為00:00:00。

No.	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

> Frame 109: 594 bytes on wire (4752 bits), 594 bytes captured (4752 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)

> Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)

> Source: 00:00:00_00:00:00 (00:00:00:00:00:00)

Type: IPv4 (0x0800)

傳送到WLC上CPU的Radius存取要求

實際上只有具有指定來源和目的地MAC位址的存取要求才能從無線控制器發出。

No.	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

> Frame 110: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits)

▼ 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)

傳送到AAA伺服器的Radius訪問請求

有問題的Access請求（由ID = 8標識），這些請求被多次傳送，並且沒有從AAA伺服器看到響應。進一步調查後，我們發現對於Access-request ID=8,UDP分段是由於大小超出MTU造成的，如下所示：

147	12:21:27.683955	TLSv1.2	104	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
148	12:21:27.683955	EAP	104	Request, TLS EAP (EAP-TLS)
149	12:21:27.756949	CAPWAP-Data	1450	CAPWAP-Data (Fragment ID: 50383, Fragment Offset: 0)
150	12:21:27.756949	EAP	188	Response, TLS EAP (EAP-TLS)
151	12:21:27.756949	EAP	1580	Response, TLS EAP (EAP-TLS)
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)
156	12:21:28.084987	TLSv1.2	1070	Application Data

WLC封包擷取時發生分段

> Frame 152: 1410 bytes on wire (11280 bits), 1410 bytes captured (11280 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)

> Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)

> Source: 00:00:00_00:00:00 (00:00:00:00:00:00)

Type: IPv4 (0x0800)

▼ 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

[\[Reassembled IPv4 in frame: 154\]](#)

> Data (1376 bytes)

分段的資料包 — I

```

> Frame 153: 1410 bytes on wire (11280 bits), 1410 bytes captured (11280 bits)
√ 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)
√ 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]

```

分段的資料包 — 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)
√ 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
√ [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]

```

重組封包

為了交叉驗證，我們檢查了ISE日誌，發現無線控制器上已分段的訪問請求根本未被ISE接收。

ISE TCP轉儲

radius.code == 1					
o.	Time	Protocol	Length	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

在ISE終端捕獲

Azure Side Capture with analysis:

Azure團隊對Azure內的物理主機執行捕獲。在Azure主機內的vSwitch上捕獲的資料表明UDP資料包的到達順序有誤。由於這些UDP片段的順序不正確，Azure正在丟棄它們。下面是同時從Azure端和無線控制器捕獲的訪問請求ID = 255，其中明視訊記憶體在資料包順序錯誤的問題：無線控制器上的封裝封包擷取(EPC)會顯示分段封包從無線控制器中離開的順序。

0619_AURAUENRAWL01_source.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.100.9.15 && ip.addr == 172.16.26.235 && (ip.id == 33004 or ip.id == 35253)

No.	Absolute Time	Source	Destination	Protocol	Identification	Length	Sequence Number	Info
5629	12:09:05.029997	10.100.9.15	172.16.26.235	IPv4	0x80ec (33004)	1410		Fragmented IP protocol (proto=UDP 17, off=0, ID=80ec) [Reassembled in #5631]
5630	12:09:05.029997	10.100.9.15	172.16.26.235	IPv4	0x80ec (33004)	1410		Fragmented IP protocol (proto=UDP 17, off=0, ID=80ec) [Reassembled in #5631]
5631	12:09:05.029997	10.100.9.15	172.16.26.235	RADIUS	0x80ec (33004)	696		Access-Request id=255
5632	12:09:05.029997	10.100.9.15	172.16.26.235	IPv4	0x80ec (33004)	696		Fragmented IP protocol (proto=UDP 17, off=1376, ID=80ec)
5721	12:09:10.029997	10.100.9.15	172.16.26.235	IPv4	0x89b5 (35253)	1410		Fragmented IP protocol (proto=UDP 17, off=0, ID=89b5) [Reassembled in #5723]
5722	12:09:10.029997	10.100.9.15	172.16.26.235	IPv4	0x89b5 (35253)	1410		Fragmented IP protocol (proto=UDP 17, off=0, ID=89b5) [Reassembled in #5723]
5723	12:09:10.029997	10.100.9.15	172.16.26.235	RADIUS	0x89b5 (35253)	696		Access-Request id=255, Duplicate Request
5724	12:09:10.029997	10.100.9.15	172.16.26.235	IPv4	0x89b5 (35253)	696		Fragmented IP protocol (proto=UDP 17, off=1376, ID=89b5)

VM Capture will see packet length of 1410 is sent first, then 696

Frame 5721: 1410 bytes on wire (11280 bits), 1410 bytes captured (11280 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Jun 19, 2023 12:09:10.029997000 AUS Eastern Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1687140550.029997000 seconds

[Time delta from previous captured frame: 0.525034000 seconds]

[Time delta from previous displayed frame: 5.000000000 seconds]

[Time since reference or first frame: 24.285041000 seconds]

Frame Number: 5721

Frame Length: 1410 bytes (11280 bits)

Capture Length: 1410 bytes (11280 bits)

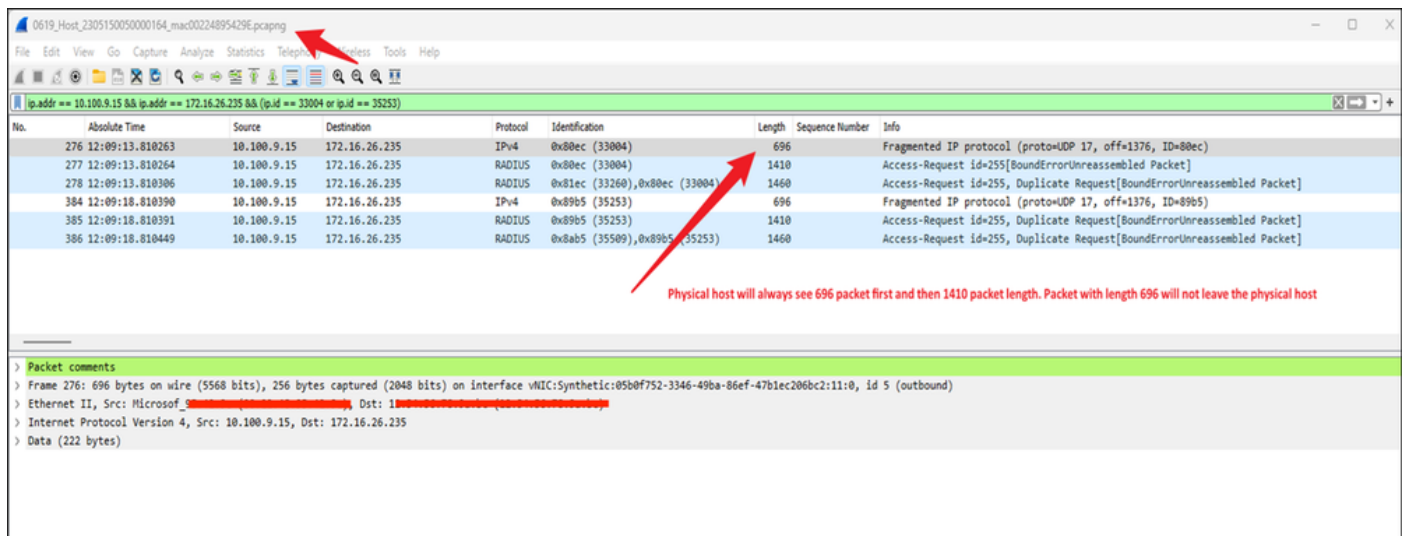
[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:data]

WLC上分段封包的序列

在實體主機上，封包到達的順序不正確



No.	Absolute Time	Source	Destination	Protocol	Identification	Length	Sequence Number	Info
276	12:09:13.810263	10.100.9.15	172.16.26.235	IPv4	0x80ec (33004)	696		Fragmented IP protocol (proto=UDP 17, off=1376, ID=80ec)
277	12:09:13.810264	10.100.9.15	172.16.26.235	RADIUS	0x80ec (33004)	1410		Access-Request id=255[BoundErrorUnreassembled Packet]
278	12:09:13.810306	10.100.9.15	172.16.26.235	RADIUS	0x81ec (33260), 0x80ec (33004)	1460		Access-Request id=255, Duplicate Request[BoundErrorUnreassembled Packet]
384	12:09:18.810390	10.100.9.15	172.16.26.235	IPv4	0x8905 (35253)	696		Fragmented IP protocol (proto=UDP 17, off=1376, ID=8905)
385	12:09:18.810391	10.100.9.15	172.16.26.235	RADIUS	0x8905 (35253)	1410		Access-Request id=255, Duplicate Request[BoundErrorUnreassembled Packet]
386	12:09:18.810449	10.100.9.15	172.16.26.235	RADIUS	0x8ab5 (35509), 0x8905 (35253)	1460		Access-Request id=255, Duplicate Request[BoundErrorUnreassembled Packet]

Physical host will always see 696 packet first and then 1410 packet length. Packet with length 696 will not leave the physical host

Packet comments

- > Frame 276: 696 bytes on wire (5568 bits), 256 bytes captured (2048 bits) on interface vNIC:Synthetic:05b0f752-3346-49ba-86ef-47b1ec206bc2:11:0, id 5 (outbound)
- > Ethernet II, Src: Microsof..., Dst: 1...
- > Internet Protocol Version 4, Src: 10.100.9.15, Dst: 172.16.26.235
- > Data (222 bytes)

Azure End上的捕獲

由於資料包以錯誤的順序到達，並且物理節點被程式設計為拒絕任何亂序幀，因此資料包會被立即丟棄。這種中斷會導致身份驗證過程失敗，使客戶端無法進入身份驗證階段。

無線控制器端建議的解決方法：

從版本17.11.1開始，我們正在實施對Radius/AAA資料包中的巨型幀的支援。此功能允許c9800控制器避免將AAA封包分段，前提是在控制器上設定了以下組態。請注意，要完全避免這些資料包的分段，必須確保每個網路躍點（包括AAA伺服器）都與巨型幀資料包相容。對於ISE，從3.1版本開始支援巨型幀。

無線控制器上的介面組態：

```
C9800-CL(config)#interface
```

```
C9800-CL(config-if) # mtu
```

```
C9800-CL(config-if) # ip mtu
```

```
[1500 to 9000]
```

無線控制器上的AAA伺服器配置：

```
C9800-CL(config)# aaa group server radius
```

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

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

以下簡要說明無線LAN控制器(WLC)上的MTU (最大傳輸單元) 設定為3000位元組時Radius封包。小於3000位元組的資料包無需分段即可無縫傳送：

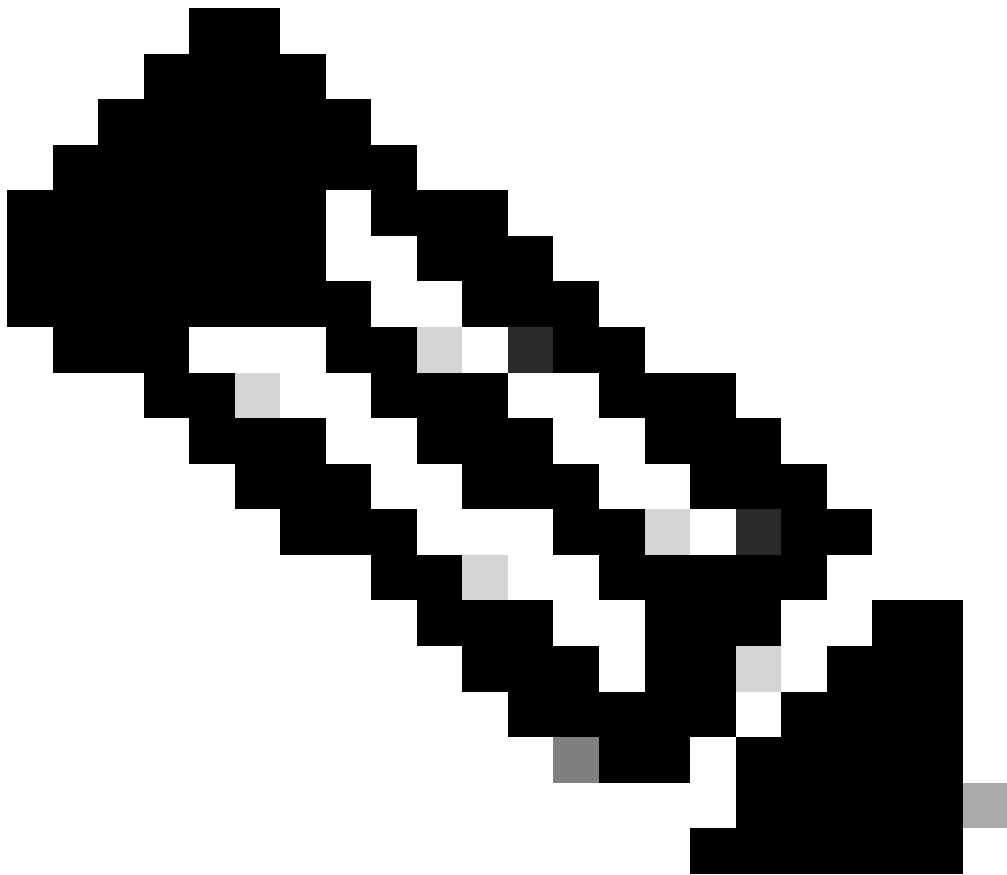
1020	10:08:11.177984	RADIUS	2075	Access-Request id=199
1021	10:08:11.177984	RADIUS	2075	Access-Request id=199, Duplicate Request
1119	10:08:16.194981	RADIUS	2075	Access-Request id=199, Duplicate Request
1120	10:08:16.194981	RADIUS	2075	Access-Request id=199, Duplicate Request
1223	10:08:21.179983	RADIUS	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

WLC上的封包擷取 (增加MTU)

透過以此方式設定組態，無線控制器可以傳輸封包，而不會將其分段，且完整傳送封包。但是，由於Azure雲不支援巨型幀，因此無法實施此解決方案。

解決方案：

- 從無線控制器的封裝封包擷取(EPC)中，我們觀察到封包是以正確的順序傳送的。然後，接收主機便有責任正確重組這些請求並繼續處理，在這種情況下，Azure端不會發生此類操作。
- 要解決UDP資料包順序錯誤的問題enable-udp-fragment-reordering，需要在Azure上啟用該選項。
- 您必須向Azure支援團隊尋求有關此問題的幫助。Microsoft已承認此問題。



附註：必須注意的是，此問題並非只有無線LAN控制器(WLC)獨有。不同的RADIUS伺服器（包括ISE、Forti Authenticator和RTSP伺服器）上也遇到類似的有序的UDP資料包問題，尤其是當這些伺服器在Azure環境中運行時。

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）。