

Problembehebung bei Fragmentierung: Affecting c9800 Wireless Controller mit Azure

Inhalt

[Einleitung](#)

[Symptome](#)

[Fehler auf ISE-Server](#)

[Detaillierte Protokollanalyse:](#)

[Wireless Controller-EPC:](#)

[ISE TCP-Dumps](#)

[Azure Side Capture mit Analyse:](#)

[Lösung vorgeschlagen vom Ende des Wireless-Controllers:](#)

[Lösung:](#)

Einleitung

In diesem Dokument wird ein bekanntes Problem mit der Azure-Plattform beschrieben, das zu Paketverlusten aufgrund der fehlerhaften Behandlung von nicht sequenzierten Fragmenten führt.

Symptome

Betroffene Produkte: Catalyst 9800-CL Wireless Controller auf Azure oder Identity Service Engine auf Azure gehostet.

SSID-Einrichtung: Konfiguriert für 802.1x EAP-TLS mit zentraler Authentifizierung.

Durchführung: Bei der Verwendung des auf der Azure-Plattform gehosteten 9800-CL mit einer EAP-TLS-basierten SSID können Verbindungsprobleme auftreten. Die Clients können während der Authentifizierungsphase auf Schwierigkeiten stoßen.

Fehler auf ISE-Server

Fehlercode 5411, der angibt, dass der Supplicant während des EAP-TLS-Zertifikataustauschs nicht mehr mit der ISE kommuniziert.

Detaillierte Protokollanalyse:

Nachfolgend finden Sie eine Abbildung einer der betroffenen Konfigurationen: Im Wireless-Controller 9800 ist die SSID für 802.1x eingerichtet, und der AAA-Server ist für EAP-TLS

konfiguriert. Wenn ein Client die Authentifizierung versucht, insbesondere während der Phase des Zertifikataustauschs, sendet der Client ein Zertifikat, das die maximale Größe der Übertragungseinheit (MTU) auf dem Wireless-Controller überschreitet. Der Wireless-Controller 9800 fragmentiert dann dieses große Paket und sendet die Fragmente der Reihe nach an den AAA-Server. Diese Fragmente gelangen jedoch nicht in der richtigen Reihenfolge an den physischen Host, was zu Paketverlusten führt.

Hier sind die RA-Ablaufverfolgungen des Wireless Controllers, wenn der Client versucht, eine Verbindung herzustellen:

Client wechselt in L2-Authentifizierungsstatus, und der EAP-Prozess wurde gestartet

```
2023/04/12 16:51:27.606414 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):  
[Client_MAC:capwap_90000004] Eingeben des Anforderungsstatus  
2023/04/12 16:51:27.606425 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):  
[0000.0000.0000:capwap_90000004] EAPOL-Paket wird gesendet  
2023/04/12 16:51:27.606494 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):  
[Client_MAC:capwap_90000004] EAPOL-Paket gesendet - Version: 3, EAPOL-  
Typ: EAP, Nutzlastlänge: 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-Paket - ANFORDERUNG, ID: 0 x 25  
2023/04/12 16:51:27.606536 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):  
[Client_MAC:capwap_90000004] EAPOL-Paket an Client gesendet  
2023/04/12 16:51:27.640768 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):  
[Client_MAC:capwap_90000004] EAPOL-Paket empfangen - Version: 1, EAPOL-  
Typ: EAP, Nutzlastlänge: 6, EAP-Typ = EAP-TLS  
2023/04/12 16:51:27.640781 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):  
[Client_MAC:capwap_90000004] EAP-Paket - ANTWORT, ID: 0 x 25
```

Wenn der Wireless-Controller die Zugriffsanforderung an den AAA-Server sendet und die Paketgröße weniger als 1500 Byte beträgt (dies ist die Standard-MTU auf dem Wireless-Controller), wird die Zugriffsanforderung ohne Komplikationen empfangen.

```
2023/04/12 16:51:27.641094 {wncd_x_R0-0}{1}: [Radius] [19224]: (Info):  
RADIUS: Senden Sie eine Zugriffsanfrage an 172.16.26.235:1812 id 0/6,  
len 552  
2023/04/12 16:51:27.644693 {wncd_x_R0-0}{1}: [Radius] [19224]: (Info):  
RADIUS: Empfangen von ID 1812/6 172.16.26.235:0, Access-Challenge, len  
1141
```

Manchmal sendet ein Client sein Zertifikat zur Authentifizierung. Wenn die Paketgröße die MTU überschreitet, wird sie fragmentiert, bevor sie weiter gesendet wird.

```
2023/04/12 16:51:27.758366 {wncd_x_R0-0}{1}: [Radius] [19224]: (Info):  
RADIUS: Senden Sie eine Zugriffsanfrage an 172.16.26.235:1812 id 0/8,  
len 2048  
2023/04/12 16:51:37.761885 {wncd_x_R0-0}{1}: [Radius] [19224]: (Info):
```

```
RADIUS: Timeout nach 5 Sekunden gestartet
2023/04/12 16:51:42.762096 {wncd_x_R0-0}{1}: [Radius] [19224]: (Info):
RADIUS: Erneut übertragen an (172.16.26.235:1812,1813) für ID 0/8
2023/04/12 16:51:32.759255 {wncd_x_R0-0}{1}: [Radius] [19224]: (Info):
RADIUS: Erneut übertragen an (172.16.26.235:1812,1813) für ID 0/8
2023/04/12 16:51:32.760328 {wncd_x_R0-0}{1}: [Radius] [19224]: (Info):
RADIUS: Timeout nach 5 Sekunden gestartet
2023/04/12 16:51:37.760552 {wncd_x_R0-0}{1}: [Radius] [19224]: (Info):
RADIUS: Erneut übertragen an (172.16.26.235:1812,1813) für ID 0/8
2023/04/12 16:51:42.762096 {wncd_x_R0-0}{1}: [Radius] [19224]: (Info):
RADIUS: Erneut übertragen an (172.16.26.235:1812,1813) für ID 0/8
```

Wir haben festgestellt, dass die Paketgröße 2048 beträgt und damit die Standard-MTU übersteigt. Folglich hat der AAA-Server nicht geantwortet. Der Wireless-Controller sendet die Zugriffsanforderung erneut, bis die maximale Anzahl von Wiederholungsversuchen erreicht ist. Da keine Antwort eingeht, setzt der Wireless-Controller den EAPOL-Prozess zurück.

```
2023/04/12 16:51:45.762890 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):
[Client_MAC:capwap_900000004] EAPOL_START auf Client veröffentlichen
2023/04/12 16:51:45.762956 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):
[Client_MAC:capwap_900000004] Eintritt in den Initialstatus
2023/04/12 16:51:45.762965 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):
[Client_MAC:capwap_900000004] !AUTH_ABORT auf Client veröffentlichen
2023/04/12 16:51:45.762969 {wncd_x_R0-0}{1}: [dot1x] [19224]: (Info):
[Client_MAC:capwap_900000004] Neustartstatus wird eingegeben
```

Dieser Prozess läuft in einer Schleife ab, und der Client befindet sich nur in der Authentifizierungsphase.

Die auf dem Wireless-Controller erfasste Embedded Packet Capture (Integrierte Paketerfassung) zeigt, dass der Wireless-Controller nach mehreren Zugriffsanforderungen und Challenge-Austauschen mit einer MTU von weniger als 1500 Byte eine Zugriffsanforderung sendet, die 1500 Byte überschreitet und das Zertifikat des Clients enthält. Dieses größere Paket wird fragmentiert. Es gibt jedoch keine Antwort auf diese spezielle Zugriffsanfrage. Der Wireless-Controller sendet diese Anforderung erneut, bis die maximale Anzahl von Wiederholungen erreicht ist. Danach wird die EAP-TLS-Sitzung neu gestartet. Diese Ereignissequenz wiederholt sich immer wieder, was darauf hinweist, dass beim Authentifizierungsversuch des Clients eine EAP-TLS-Schleife auftritt. Weitere Informationen finden Sie in den nachfolgenden Informationen zur gleichzeitigen Paketerfassung vom Wireless-Controller und der ISE.

Wireless Controller-EPC:

radius.code == 1				
o.	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

Paketerfassung auf WLC

Wir stellen fest, dass der Wireless Controller mehrere doppelte Anforderungen für eine bestimmte Zugriffsanforderungs-ID sendet = 8



Anmerkung: Beim EPC stellen wir auch fest, dass es eine einzige Duplikatanforderung für andere IDs gibt. Daraus ergibt sich die Frage: Ist mit einer solchen Doppelarbeit zu rechnen? Die Antwort auf die Frage, ob diese Verdoppelung zu erwarten ist, lautet ja, ja. Der Grund hierfür ist, dass die Erfassung über die grafische Benutzeroberfläche des Wireless-Controllers erfolgt und die Option "Kontrollebene überwachen" ausgewählt wurde. Daher ist es normal, mehrere Instanzen von RADIUS-Paketen zu beobachten, da sie an die CPU weitergeleitet werden. In solchen Fällen müssen für Access-Anforderungen sowohl die Quell- als auch die Ziel-MAC-Adresse auf 00:00:00 eingestellt sein.

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)

Radius-Zugriffsanfrage auf CPU auf WLC gestartet

Nur die Zugriffsanforderungen mit den angegebenen Quell- und Ziel-MAC-Adressen müssen tatsächlich vom Wireless-Controller gesendet werden.

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: 1 [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)

RADIUS-Zugriffsanfrage an AAA-Server gesendet

Es handelt sich um Access-Anfragen, die mit ID = 8 identifiziert werden und mehrfach versendet werden und für die keine Antwort vom AAA-Server einging. Bei der weiteren Untersuchung stellten wir fest, dass bei der Zugriffsanforderungs-ID=8 eine UDP-Fragmentierung auftritt, weil die Größe die MTU übersteigt, wie unten dargestellt:

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

Fragmentierung bei der WLC-Paketerfassung

> 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)

Fragmentiertes Paket - 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]

```

Fragmentiertes Paket - 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]

```

Reassembliertes Paket

Um eine Gegenprüfung vorzunehmen, überprüften wir die ISE-Protokolle und stellten fest, dass die Zugriffsanforderung, die auf dem Wireless-Controller fragmentiert war, von der ISE überhaupt nicht empfangen wurde.

ISE TCP-Dumps

radius.code == 1

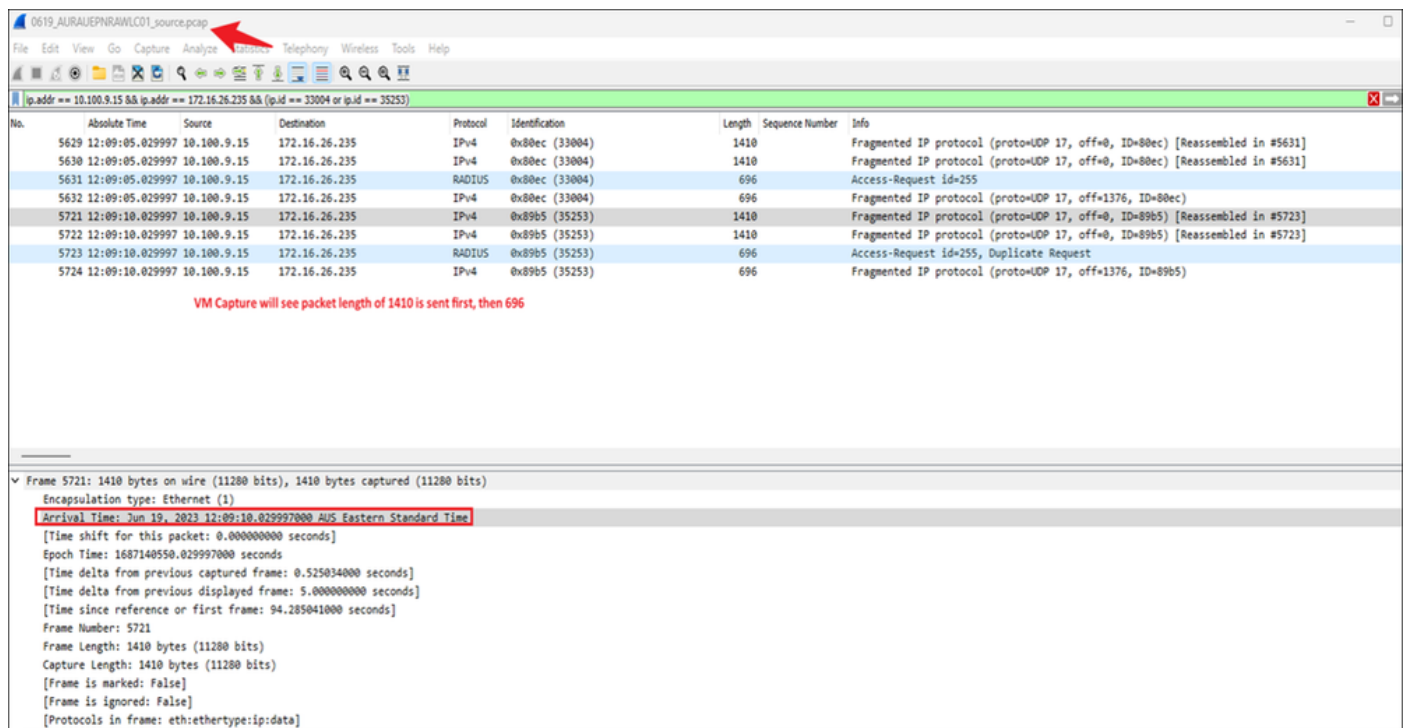
o.	Time	Protocol	Length	Info
1	12:21:27.387158	RADIUS	538	Access-Request id=0
3	12:21:27.428304	RADIUS	760	Access-Request id=1
5	12:21:27.492019	RADIUS	594	Access-Request id=2
7	12:21:27.527949	RADIUS	594	Access-Request id=3
9	12:21:27.572272	RADIUS	594	Access-Request id=4
11	12:21:27.617147	RADIUS	594	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

Aufzeichnungen am ISE-Ende

Azure Side Capture mit Analyse:

Das Azure-Team führte eine Erfassung auf dem physischen Host in Azure durch. Die auf dem vSwitch im Azure-Host erfassten Daten zeigen an, dass die UDP-Pakete nicht in der richtigen Reihenfolge ankommen. Da diese UDP-Fragmente nicht in der richtigen Reihenfolge sind, werden sie von Azure verworfen. Im Folgenden sind die gleichzeitigen Aufnahmen vom Azure-Ende und vom Wireless-Controller für die Zugriffsanforderungs-ID = 255 aufgeführt, bei denen das Problem der fehlerhaften Pakete deutlich wird:

Die Encapsulated Packet Capture (EPC) auf dem Wireless-Controller zeigt die Sequenz an, in der die fragmentierten Pakete vom Wireless-Controller zurückgelassen werden.



0619_AURAUENRAWLCO1_source.pcap

File Edit View Go Capture Analyze Packets Telephony Wireless Tools Help

ip.addr == 10.100.9.15 && ip.addr == 172.16.26.235 && (p.id == 33004 or p.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) on interface 0

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: 94.285041000 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]

Sequenz fragmentierter Pakete auf WLC

Auf dem physischen Host kommen die Pakete nicht in der richtigen Reihenfolge an

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

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	0x89b5 (35253)	696		Fragmented IP protocol (proto=UDP 17, off=1376, ID=89b5)
385	12:09:18.810391	10.100.9.15	172.16.26.235	RADIUS	0x89b5 (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), 0x89b5 (35253)	1460		Access-Request id=255, Duplicate Request[BoundErrorUnreassembled Packet]

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: Microsoft, Dst: 10.100.9.15
- > Internet Protocol Version 4, Src: 10.100.9.15, Dst: 172.16.26.235
- > Data (222 bytes)

Aufzeichnungen auf Azure End

Da die Pakete in der falschen Reihenfolge ankommen und der physische Knoten so programmiert ist, dass er alle nicht ordnungsgemäßen Frames zurückweist, werden die Pakete sofort verworfen. Durch diese Unterbrechung schlägt der Authentifizierungsprozess fehl, sodass der Client nicht mehr über die Authentifizierungsphase hinaus arbeiten kann.

Lösung vorgeschlagen vom Ende des Wireless-Controllers:

Ab Version 17.11.1 implementieren wir die Unterstützung für Jumbo Frames in Radius-/AAA-Paketen. Mit dieser Funktion kann der c9800-Controller die Fragmentierung von AAA-Paketen vermeiden, vorausgesetzt, die folgende Konfiguration ist auf dem Controller festgelegt. Um eine vollständige Fragmentierung dieser Pakete zu vermeiden, muss sichergestellt werden, dass jeder Netzwerk-Hop, einschließlich des AAA-Servers, mit Jumbo Frame-Paketen kompatibel ist. Für die ISE beginnt die Jumbo Frame-Unterstützung mit Version 3.1 und höher.

Schnittstellenkonfiguration des Wireless Controllers:

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

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

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

```
[1500 to 9000]
```

AAA-Serverkonfiguration auf dem Wireless-Controller:

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

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

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

Im Folgenden wird ein Radius-Paket kurz erläutert, wenn die MTU (Maximum Transmission Unit, maximale Übertragungseinheit) auf einem Wireless LAN Controller (WLC) auf 3.000 Byte konfiguriert ist. Pakete unter 3000 Byte wurden nahtlos und ohne Fragmentierung versendet:

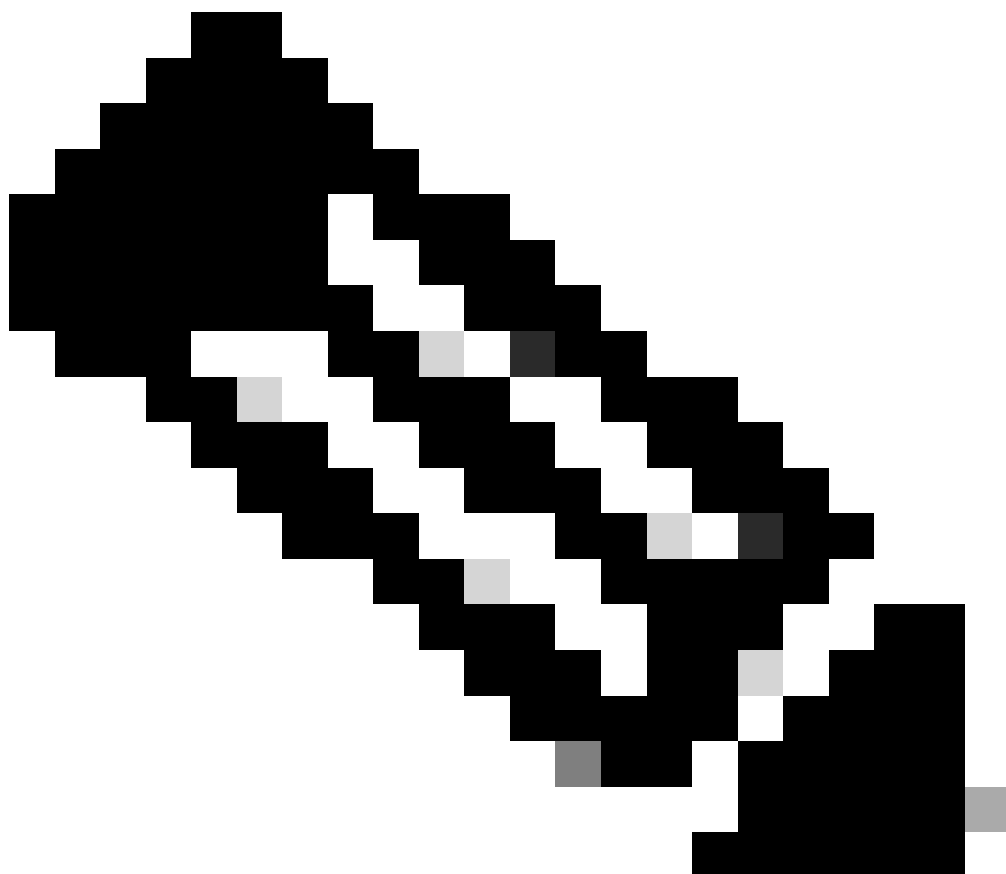
1020	10:08:11.177984	RADIUS	2075	Access-Request id=199
1021	10:08:11.177984	RADIUS	2075	Access-Request id=199, Duplicate Request
1119	10:08:16.194981	RADIUS	2075	Access-Request id=199, Duplicate Request
1120	10:08:16.194981	RADIUS	2075	Access-Request id=199, Duplicate Request
1223	10:08:21.179983	RADIUS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

Paketerfassung auf WLC mit erhöhter MTU

Durch diese Konfiguration überträgt der Wireless-Controller Pakete, ohne sie zu fragmentieren, und sendet sie intakt. Da Azure Cloud jedoch keine Jumbo Frames unterstützt, kann diese Lösung nicht implementiert werden.

Lösung:

- Aus der Encapsulated Packet Capture (EPC) des Wireless-Controllers konnten wir feststellen, dass die Pakete in der richtigen Reihenfolge gesendet wurden. Es liegt dann in der Verantwortung des empfangenden Hosts, diese korrekt wieder zusammenzubauen und mit der Verarbeitung fortzufahren, was in diesem Fall nicht auf Azure-Seite geschieht.
- Um das Problem von ungeordneten UDP-Paketen zu beheben, muss die `enable-udp-fragment-reordering` Option auf Azure aktiviert werden.
- Wenden Sie sich an das Azure-Supportteam, um Unterstützung in dieser Angelegenheit zu erhalten. Microsoft hat dieses Problem erkannt.



Anmerkung: Beachten Sie, dass sich dieses Problem nicht ausschließlich auf den Wireless LAN Controller (WLC) auswirkt. Ähnliche Probleme mit ungeordneten UDP-Paketen sind auf verschiedenen RADIUS-Servern aufgetreten, einschließlich ISE-, Forti Authenticator- und RTSP-Servern, insbesondere wenn diese in der Azure-Umgebung betrieben werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.