

Solución de problemas de fragmentación: Afecta al controlador inalámbrico c9800 con Azure

Contenido

[Introducción](#)

[Síntomas](#)

[Error en el servidor ISE](#)

[Análisis de registro detallado:](#)

[Controlador inalámbrico EPC:](#)

[Volcados de ISE TCP](#)

[Azure Side Capture con análisis:](#)

[Solución sugerida desde el extremo del controlador inalámbrico:](#)

[Solución:](#)

Introducción

Este documento describe un problema conocido con la plataforma de Azure que conduce a la pérdida de paquetes debido al mal manejo de fragmentos fuera de secuencia.

Síntomas

Productos afectados: Controlador inalámbrico Catalyst 9800-CL alojado en Azure o Identity Service Engine alojado en Azure.

Configuración de SSID: Configurado para 802.1x EAP-TLS con autenticación central.

Conducta: Mientras utiliza el 9800-CL alojado en la plataforma Azure con un SSID basado en EAP-TLS, puede encontrar problemas de conectividad. Los clientes pueden encontrar dificultades durante la fase de autenticación.

Error en el servidor ISE

Código de error 5411 que indica que el solicitante ha dejado de comunicarse con ISE durante el intercambio de certificados EAP-TLS.

Análisis de registro detallado:

A continuación se muestra una ilustración de una de las configuraciones afectadas: En el controlador inalámbrico 9800, el SSID se configura para 802.1x y el servidor AAA se configura

para EAP-TLS. Cuando un cliente intenta la autenticación, especialmente durante la fase de intercambio de certificados, el cliente envía un certificado que excede el tamaño de la unidad de transmisión máxima (MTU) en el controlador inalámbrico. A continuación, el controlador inalámbrico 9800 fragmenta este paquete grande y envía los fragmentos secuencialmente al servidor AAA. Sin embargo, estos fragmentos no llegan en el orden correcto al host físico, lo que lleva a la caída de paquetes.

Estos son los rastros de RA del controlador inalámbrico cuando el cliente intenta conectarse:
El cliente ingresa en el estado de autenticación L2 y se inicia el proceso EAP

```
2023/04/12 16:51:27.606414 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(información): [Client_MAC:capwap_900000004] Ingresando el estado de la  
solicitud  
2023/04/12 16:51:27.606425 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(información): [0000.0000.0000:capwap_900000004] Enviando paquetes EAPOL  
2023/04/12 16:51:27.606494 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(información): [Client_MAC:capwap_900000004] Paquete EAPOL enviado -  
Versión: 3,Tipo EAPOL: EAP, longitud de carga útil: 1008, EAP-Tipo =  
EAP-TLS  
2023/04/12 16:51:27.606496 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(información): [Client_MAC:capwap_900000004] Paquete EAP - REQUEST, ID:  
0x25  
2023/04/12 16:51:27.606536 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(información): [Client_MAC:capwap_900000004] Paquete EAPOL enviado al  
cliente  
2023/04/12 16:51:27.640768 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(información): [Client_MAC:capwap_900000004] Paquete EAPOL recibido -  
Versión: 1,Tipo EAPOL: EAP, longitud de carga útil: 6, EAP-Tipo = EAP-  
TLS  
2023/04/12 16:51:27.640781 {wncd_x_R0-0}{1}: [dot1x] [19224]:  
(información): [Client_MAC:capwap_900000004] Paquete EAP - RESPUESTA, ID:  
0x25
```

Cuando el controlador inalámbrico envía la solicitud de acceso al servidor AAA y el tamaño del paquete es inferior a 1500 bytes (que es la MTU predeterminada en el controlador inalámbrico), el desafío de acceso se recibe sin ninguna complicación.

```
2023/04/12 16:51:27.641094 {wncd_x_R0-0}{1}: [radius] [19224]:  
(información): RADIUS: Send Access-Request to 172.16.26.235:1812 id 0/6,  
len 552  
2023/04/12 16:51:27.644693 {wncd_x_R0-0}{1}: [radius] [19224]:  
(información): RADIUS: Recibido desde id 1812/6 172.16.26.235:0, Access-  
Challenge, len 1141
```

A veces, un cliente puede enviar su certificado para la autenticación. Si el tamaño del paquete excede la MTU, se fragmentará antes de enviarse más lejos.

2023/04/12 16:51:27.758366 {wncd_x_R0-0}{1}: [radius] [19224]:
(información): RADIUS: Send Access-Request to 172.16.26.235:1812 id 0/8,
len 2048
2023/04/12 16:51:37.761885 {wncd_x_R0-0}{1}: [radius] [19224]:
(información): RADIUS: Tiempo de espera iniciado 5 s
2023/04/12 16:51:42.762096 {wncd_x_R0-0}{1}: [radius] [19224]:
(información): RADIUS: Retransmitir a (172.16.26.235:1812,1813) para id
0/8
2023/04/12 16:51:32.759255 {wncd_x_R0-0}{1}: [radius] [19224]:
(información): RADIUS: Retransmitir a (172.16.26.235:1812,1813) para id
0/8
2023/04/12 16:51:32.760328 {wncd_x_R0-0}{1}: [radius] [19224]:
(información): RADIUS: Tiempo de espera iniciado 5 s
2023/04/12 16:51:37.760552 {wncd_x_R0-0}{1}: [radius] [19224]:
(información): RADIUS: Retransmitir a (172.16.26.235:1812,1813) para id
0/8
2023/04/12 16:51:42.762096 {wncd_x_R0-0}{1}: [radius] [19224]:
(información): RADIUS: Retransmitir a (172.16.26.235:1812,1813) para id
0/8

Hemos observado que el tamaño del paquete es 2048, lo que supera la MTU predeterminada. En consecuencia, no ha habido respuesta del servidor AAA. El controlador inalámbrico volverá a enviar la solicitud de acceso de forma persistente hasta que alcance el número máximo de reintentos. Debido a la ausencia de una respuesta, el controlador inalámbrico restablecerá finalmente el proceso EAPOL.

2023/04/12 16:51:45.762890 {wncd_x_R0-0}{1}: [dot1x] [19224]:
(información): [Client_MAC:capwap_900000004] Publicando EAPOL_START en el
cliente
2023/04/12 16:51:45.762956 {wncd_x_R0-0}{1}: [dot1x] [19224]:
(información): [Client_MAC:capwap_900000004] Ingresando al estado de
inicialización
2023/04/12 16:51:45.762965 {wncd_x_R0-0}{1}: [dot1x] [19224]:
(información): [Client_MAC:capwap_900000004] Publicando !AUTH_ABORT en el
cliente
2023/04/12 16:51:45.762969 {wncd_x_R0-0}{1}: [dot1x] [19224]:
(información): [Client_MAC:capwap_900000004] Ingresando al estado de
reinicio

Este proceso entra en loop y el cliente está atascado en la fase de autenticación solamente.

La captura de paquetes incorporada capturada en el controlador inalámbrico muestra que después de varias solicitudes de acceso y de intercambios de desafío con una MTU inferior a 1500 bytes, el controlador inalámbrico envía una solicitud de acceso superior a 1500 bytes, que contiene el certificado del cliente. Este paquete más grande sufre fragmentación. Sin embargo, no

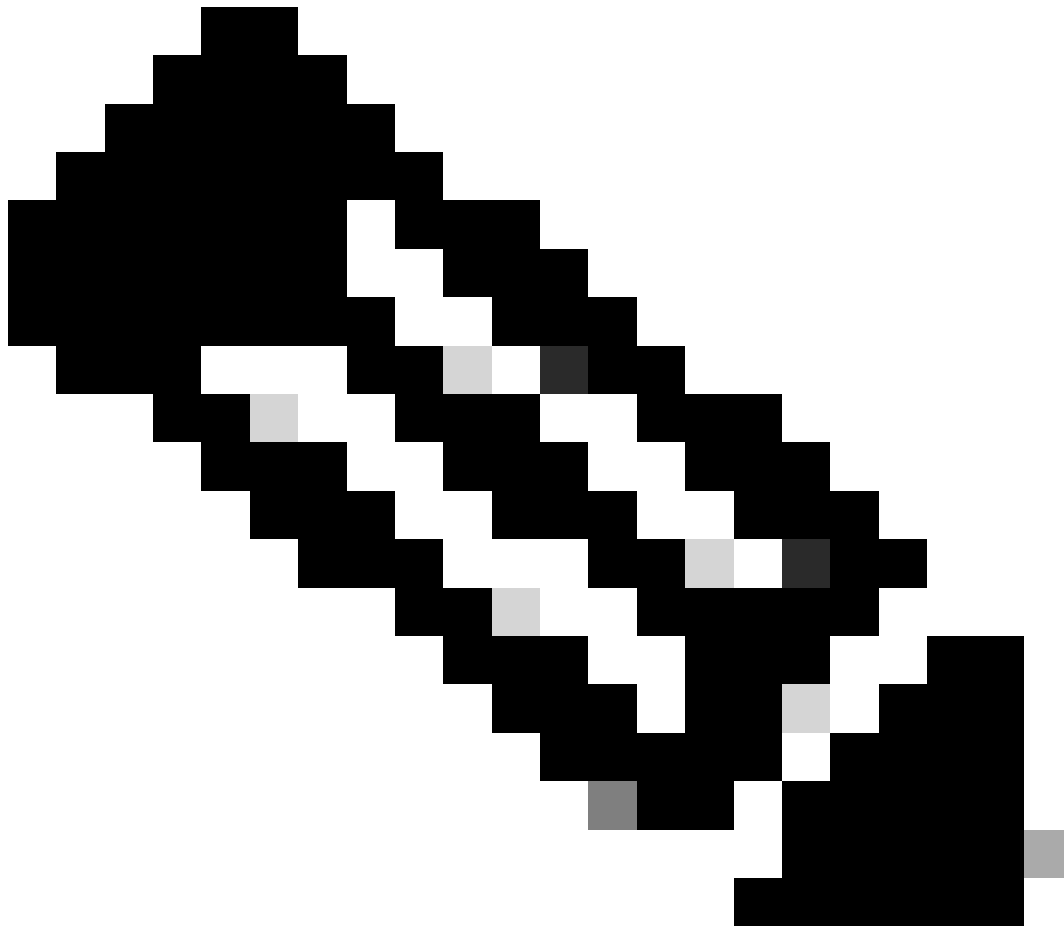
hay respuesta a esta solicitud de acceso en particular. El controlador inalámbrico continúa reenviando esta solicitud hasta que alcanza el número máximo de reintentos, después de lo cual se reinicia la sesión EAP-TLS. Esta secuencia de eventos se repite constantemente, lo que indica que se produce un loop EAP-TLS cuando el cliente intenta autenticarse. Consulte las capturas de paquetes simultáneas del controlador inalámbrico y de ISE que se proporcionan a continuación para obtener una comprensión más clara.

Controlador inalámbrico 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

Captura de paquetes en WLC

Observamos que el controlador inalámbrico está enviando varias solicitudes duplicadas para un ID de solicitud de acceso específico = 8



Nota: En el EPC, también observamos que hay una única solicitud duplicada para otras ID. Esto nos lleva a la pregunta: ¿Se prevé tal duplicación? La respuesta a si se espera esta duplicación es sí, lo es. La razón es que la captura se tomó de la GUI del controlador inalámbrico con la opción 'Monitor Control Plane' seleccionada. Como resultado, es normal observar varias instancias de paquetes RADIUS ya que están siendo dirigidos a la CPU. En estos casos, las solicitudes de acceso deben verse con las direcciones MAC de origen y destino establecidas en 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)

Radius Access-Request Punted to CPU on WLC

Sólo las solicitudes de acceso con las direcciones MAC de origen y destino especificadas deben enviarse realmente desde el controlador inalámbrico.

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)

Solicitud de acceso Radius enviada al servidor AAA

Las solicitudes de acceso en cuestión, identificadas por ID = 8, que se envían varias veces y para las que no se ha visto ninguna respuesta del servidor AAA. Tras una investigación adicional, observamos que para Access-request ID=8, la fragmentación UDP se produce debido al tamaño que supera la MTU, como se ilustra a continuación:

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

Fragmentación que tiene lugar en la captura de paquetes WLC

>	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)

Paquete fragmentado: 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]

```

Paquete fragmentado - 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]

```

Paquete reensamblado

Para llevar a cabo la verificación cruzada, revisamos los registros de ISE y descubrimos que ISE no estaba recibiendo la solicitud de acceso, que se había fragmentado en el controlador inalámbrico.

Volcados de ISE TCP

radius.code == 1

No.	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

Capturas al final de ISE

Azure Side Capture con análisis:

El equipo de Azure realizó una captura en el host físico de Azure. Los datos capturados en el vSwitch dentro del host de Azure indican que los paquetes UDP están llegando fuera de secuencia. Debido a que estos fragmentos UDP no están en el orden correcto, Azure los está descartando. A continuación se muestran las capturas del extremo de Azure y del controlador inalámbrico, tomadas simultáneamente para el ID de solicitud de acceso = 255, donde el problema de los paquetes que están fuera de servicio es claramente evidente:

La captura de paquetes encapsulados (EPC) del controlador inalámbrico muestra la secuencia en la que los paquetes fragmentados salen del controlador inalámbrico.

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 && (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: 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]

Secuencia de paquetes fragmentados en WLC

En el host físico, los paquetes no llegan en la secuencia adecuada

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)

Capturas en Azure End

Dado que los paquetes llegan en el orden incorrecto y el nodo físico está programado para rechazar cualquier trama fuera de orden, los paquetes se descartan inmediatamente. Esta interrupción hace que el proceso de autenticación falle, dejando al cliente incapaz de avanzar más allá de la fase de autenticación.

Solución sugerida desde el extremo del controlador inalámbrico:

A partir de la versión 17.11.1, estamos implementando el soporte para tramas Jumbo en paquetes Radius/AAA. Esta función permite que el controlador c9800 evite la fragmentación de paquetes AAA, siempre que se establezca la siguiente configuración en el controlador. Tenga en cuenta que para evitar la fragmentación completa de estos paquetes, es esencial asegurarse de que cada salto de red, incluido el servidor AAA, sea compatible con los paquetes de tramas gigantes. Para ISE, la compatibilidad con tramas gigantes comienza a partir de la versión 3.1.

Configuración de la interfaz en el controlador inalámbrico:

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

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

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

```
[1500 to 9000]
```

Configuración de servidor AAA en controlador inalámbrico:

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

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

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

A continuación se presenta una breve descripción de un paquete Radius cuando la MTU (unidad de transmisión máxima) se configura en 3000 bytes en un controlador de LAN inalámbrica (WLC). Los paquetes menores de 3000 bytes se enviaron sin problemas sin necesidad de fragmentación:

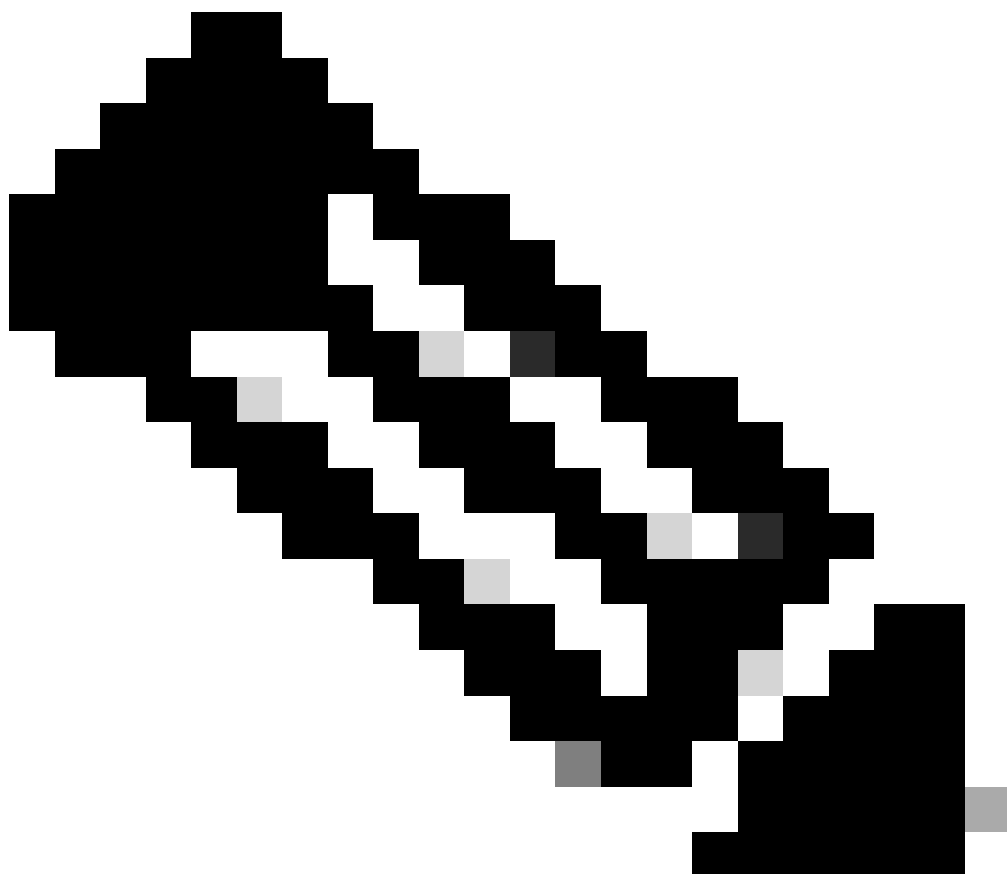
1020	10:08:11.177984	RADIUS	2075	Access-Request id=199
1021	10:08:11.177984	RADIUS	2075	Access-Request id=199, Duplicate Request
1119	10:08:16.194981	RADIUS	2075	Access-Request id=199, Duplicate Request
1120	10:08:16.194981	RADIUS	2075	Access-Request id=199, Duplicate Request
1223	10:08:21.179983	RADIUS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

Captura de paquetes en WLC con MTU aumentada

Al establecer la configuración de esta manera, el controlador inalámbrico transmite los paquetes sin fragmentarlos, enviándolos intactos. Sin embargo, como la nube de Azure no admite tramas jumbo, esta solución no se puede implementar.

Solución:

- En la captura de paquetes encapsulados (EPC) del controlador inalámbrico, observamos que los paquetes se envían en el orden correcto. Es responsabilidad del host receptor volver a ensamblarlos correctamente y continuar con el procesamiento, que, en este caso, no se produce en el lado de Azure.
- Para resolver el problema de los paquetes UDP fuera de servicio, `enable-udp-fragment-reordering` debe activarse la opción en Azure.
- Debe ponerse en contacto con el equipo de soporte técnico de Azure para obtener ayuda con este asunto. Microsoft ha reconocido este problema.



Nota: Debe tenerse en cuenta que este problema no es exclusivo del controlador de LAN inalámbrica (WLC). Problemas similares con paquetes UDP fuera de servicio se han encontrado en diferentes servidores RADIUS, incluidos los servidores ISE, Forti Authenticator y RTSP, especialmente cuando funcionan dentro del entorno de Azure.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).