Risoluzione dei problemi di frammentazione: Interessi sul controller wireless c9800 con Azure

Sommario

Introduzione

In questo documento viene descritto un problema noto della piattaforma Azure che comporta la perdita di pacchetti a causa di una gestione errata dei frammenti fuori sequenza.

Sintomi

Prodotti interessati: Catalyst 9800-CL Wireless Controller ospitato in Azure o Identity Service Engine ospitato in Azure.

Configurazione SSID: Configurato per 802.1x EAP-TLS con autenticazione centrale.

Condotta: Durante l'utilizzo di 9800-CL ospitato nella piattaforma Azure con un SSID basato su EAP-TLS è possibile riscontrare problemi di connettività. Durante la fase di autenticazione i client potrebbero incontrare problemi.

Errore sul server ISE

Codice di errore 5411 che indica che il supplicant ha cessato la comunicazione con ISE durante lo scambio del certificato EAP-TLS.

Analisi dettagliata registro:

Di seguito è riportata l'illustrazione di una delle configurazioni interessate: Nel controller wireless 9800, l'SSID è configurato per 802.1x e il server AAA è configurato per EAP-TLS. Quando un

client tenta di eseguire l'autenticazione, in particolare durante la fase di scambio dei certificati, invia un certificato che supera le dimensioni MTU (Maximum Transmission Unit) sul controller wireless. Il controller wireless 9800 frammenta quindi questo pacchetto di grandi dimensioni e invia i frammenti in sequenza al server AAA. Tuttavia, questi frammenti non arrivano nell'ordine corretto all'host fisico, causando il rifiuto del pacchetto.

Tracce dell'Autorità registrazione dal controller wireless durante il tentativo di connessione del client:
Il client entra nello stato di autenticazione L2 e il processo EAP è avviato

```
2023/04/12 16:51:27.606414 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[Client_MAC:capwap_90000004] Attivazione dello stato della richiesta in
corso
2023/04/12 16:51:27.606425 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[0000.0000.0000:capwap_90000004] Invio del pacchetto EAPOL in corso
2023/04/12 16:51:27.606494 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[Client_MAC:capwap_90000004] Pacchetto EAPOL inviato - Versione: 3,Tipo
EAPOL: Lunghezza payload EAP: 1008, tipo EAP = EAP-TLS
2023/04/12 16:51:27.606496 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[MAC_client:capwap_90000004] Pacchetto EAP - RICHIESTA, ID: 0x25
2023/04/12 16:51:27.606536 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[Client_MAC:capwap_90000004] Pacchetto EAPOL inviato al client
2023/04/12 16:51:27.640768 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[Client_MAC:capwap_90000004] Ricevuto pacchetto EAPOL - Versione: 1,Tipo
EAPOL: Lunghezza payload EAP: 6, tipo EAP = EAP-TLS
2023/04/12 16:51:27.640781 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[MAC_client:capwap_90000004] Pacchetto EAP - RISPOSTA, ID: 0x25
```

Quando il controller wireless invia la richiesta di accesso al server AAA e le dimensioni del pacchetto sono inferiori a 1500 byte (ossia l'MTU predefinita sul controller wireless), la richiesta di accesso viene ricevuta senza complicazioni.

```
2023/04/12 16:51:27.641094 {wncd_x_R0-0}{1}: [raggio] [1924]: (info):
RAGGIO: Invia richiesta di accesso a 172.16.26.235:1812 id 0/6, len 552
2023/04/12 16:51:27.644693 {wncd_x_R0-0}{1}: [raggio] [1924]: (info):
RAGGIO: Ricevuto da id 1812/6 172.16.26.235:0, Access-Challenge, len
1141
```

Talvolta un client può inviare il proprio certificato per l'autenticazione. Se le dimensioni del pacchetto superano l'MTU, il pacchetto verrà frammentato prima di essere inviato ulteriormente.

```
2023/04/12 16:51:27.758366 {wncd_x_R0-0}{1}: [raggio] [1924]: (info):
RAGGIO: Invia richiesta di accesso a 172.16.26.235:1812 id 0/8, len 2048
2023/04/12 16:51:37.761885 {wncd_x_R0-0}{1}: [raggio] [1924]: (info):
RAGGIO: Timeout 5 sec avviato
2023/04/12 16:51:42.762096 {wncd_x_R0-0}{1}: [raggio] [1924]: (info):
```

```
RAGGIO: Ritrasmissione a (172.16.26.235:1812,1813) per id 0/8
2023/04/12 16:51:32.759255 {wncd_x_R0-0}{1}: [raggio] [1924]: (info):
RAGGIO: Ritrasmissione a (172.16.26.235:1812,1813) per id 0/8
2023/04/12 16:51:32.760328 {wncd_x_R0-0}{1}: [raggio] [1924]: (info):
RAGGIO: Timeout 5 sec avviato
2023/04/12 16:51:37.760552 {wncd_x_R0-0}{1}: [raggio] [1924]: (info):
RAGGIO: Ritrasmissione a (172.16.26.235:1812,1813) per id 0/8
2023/04/12 16:51:42.762096 {wncd_x_R0-0}{1}: [raggio] [1924]: (info):
RAGGIO: Ritrasmissione a (172.16.26.235:1812,1813) per id 0/8
```

Abbiamo notato che le dimensioni del pacchetto sono 2048, il che supera l'MTU predefinita. Di conseguenza, non è pervenuta alcuna risposta dal server AAA. Il controller wireless invierà in modo permanente la richiesta di accesso fino a raggiungere il numero massimo di tentativi. A causa dell'assenza di risposta, il controller wireless reimposterà il processo EAPOL.

```
2023/04/12 16:51:45.762890 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[Client_MAC:capwap_90000004] Invio di EAPOL_START sul client
2023/04/12 16:51:45.762956 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[Client_MAC:capwap_90000004] Attivazione dello stato iniziale in corso
2023/04/12 16:51:45.762965 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[MAC_client:capwap_90000004] Invio di !AUTH_ABORT sul client
2023/04/12 16:51:45.762969 {wncd_x_R0-0}{1}: [dot1x] [1924]: (info):
[Client_MAC:capwap_90000004] Attivazione dello stato di riavvio
```

Questo processo viene eseguito in loop e il client è bloccato solo nella fase di autenticazione.

L'acquisizione integrata dei pacchetti acquisita sul controller wireless mostra che dopo diverse richieste di accesso e scambi di richiesta con MTU inferiore a 1500 byte, il controller wireless invia una richiesta di accesso superiore a 1500 byte, che contiene il certificato del client. Questo pacchetto più grande viene frammentato. Non è tuttavia disponibile alcuna risposta a questa specifica richiesta di accesso. Il controller wireless continua a inviare questa richiesta finché non raggiunge il numero massimo di tentativi, dopodiché la sessione EAP-TLS viene riavviata. Questa sequenza di eventi continua a ripetersi, a indicare che si verifica un loop EAP-TLS quando il client tenta di eseguire l'autenticazione. Per una comprensione più chiara, fare riferimento alle acquisizioni simultanee di pacchetti dal controller wireless e dall'ISE forniti di seguito.

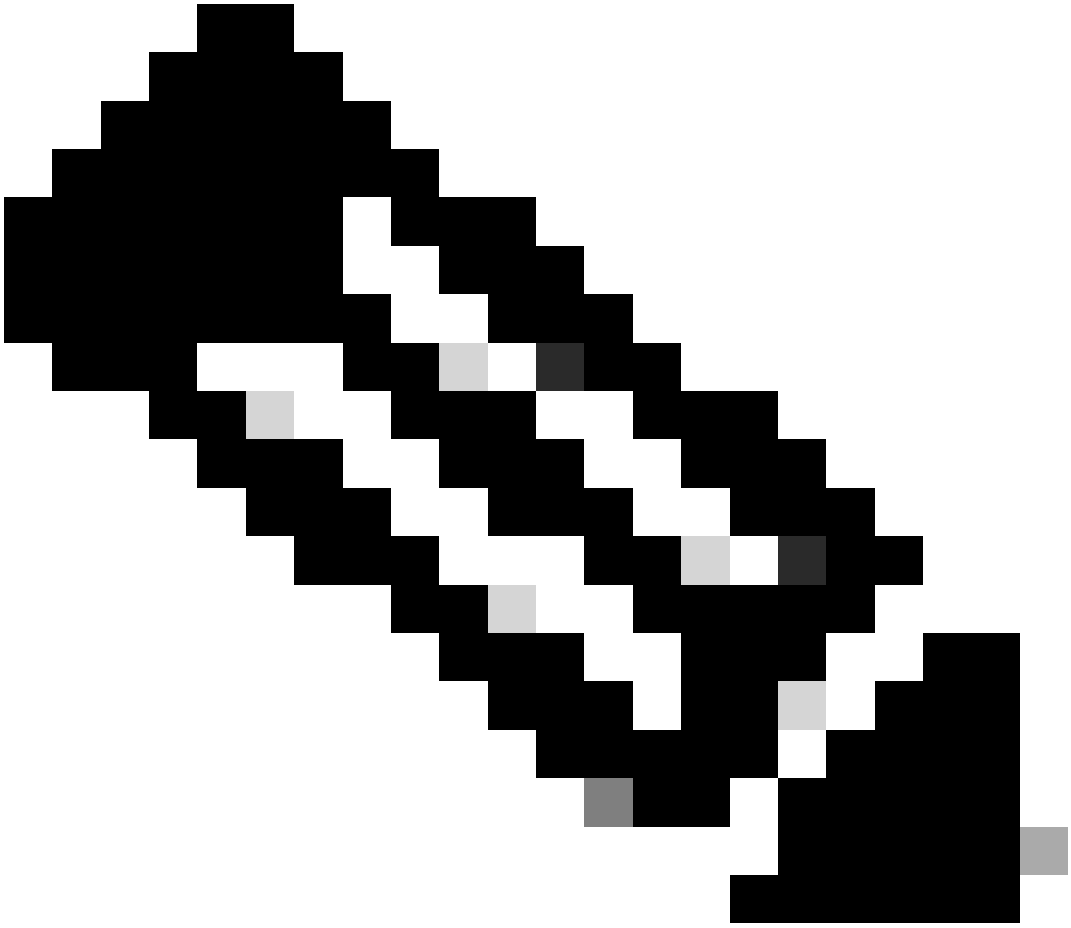
EPC controller wireless:

radius.code == 1

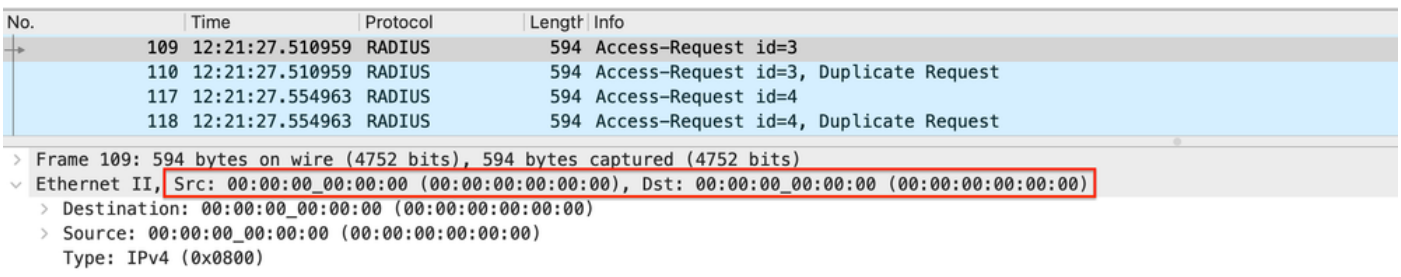
).	Time	Protocol	Length	Info
109	12:21:27.510959	RADIUS	594	Access-Request id=3
110	12:21:27.510959	RADIUS	594	Access-Request id=3, Duplicate Request
117	12:21:27.554963	RADIUS	594	Access-Request id=4
118	12:21:27.554963	RADIUS	594	Access-Request id=4, Duplicate Request
125	12:21:27.599959	RADIUS	594	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 su WLC

Si noti che il controller wireless sta inviando diverse richieste duplicate per un particolare ID richiesta di accesso = 8

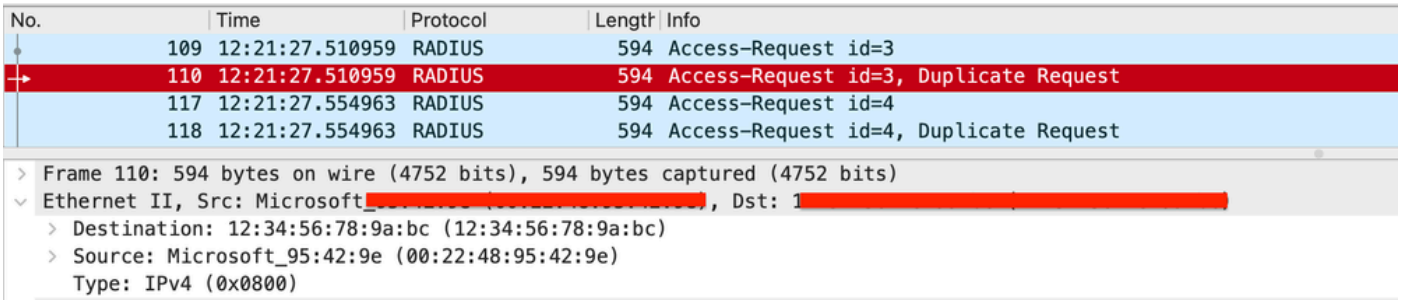


Nota: L'EPC rileva inoltre che esiste un'unica richiesta di duplicazione per altri codici di identificazione. Da qui la domanda: Si prevede una duplicazione di questo tipo? La risposta alla domanda se si prevede questa duplicazione è sì, lo è. Il motivo è che l'acquisizione è stata effettuata dalla GUI del controller wireless con l'opzione 'Monitor Control Plane' selezionata. Di conseguenza, è normale osservare diverse istanze di pacchetti RADIUS in quanto vengono indirizzati alla CPU. In questi casi, le richieste di accesso devono essere visualizzate con gli indirizzi MAC di origine e di destinazione impostati su 00:00:00.



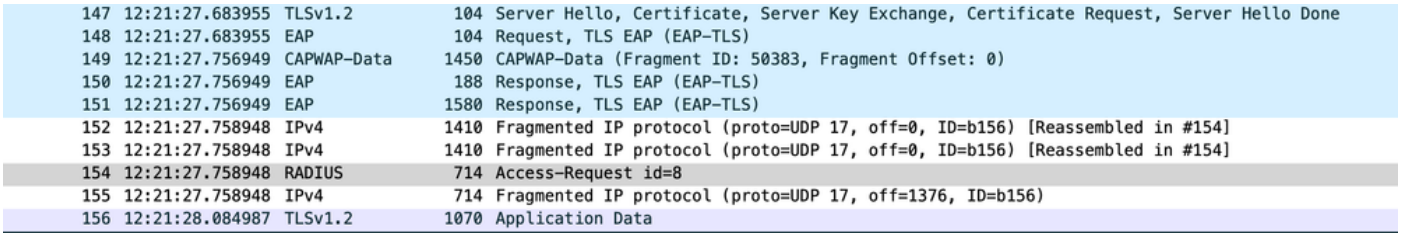
Richiesta di accesso Radius inoltrata alla CPU sul WLC

Solo le richieste di accesso con gli indirizzi MAC di origine e di destinazione specificati devono essere effettivamente inviate dal controller wireless.

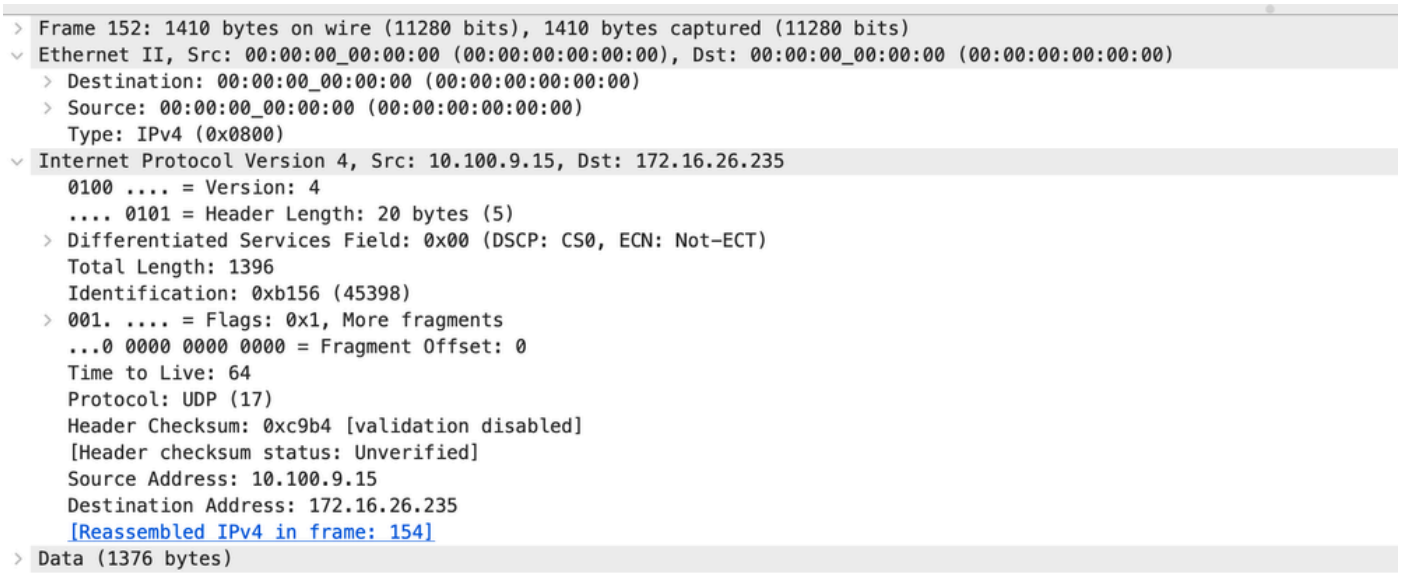


Richiesta di accesso Radius inviata al server AAA

Le richieste di accesso in questione, identificate da ID = 8, che vengono inviate più volte e per le quali non è stata vista alcuna risposta dal server AAA. In seguito a ulteriori indagini, è stato rilevato che per Access-request con ID=8 la frammentazione UDP è avvenuta a causa delle dimensioni superiori all'MTU, come mostrato di seguito:



Frammentazione all'acquisizione di pacchetti WLC



Pacchetto frammentato - 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]
```

Pacchetto frammentato - 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]
```

Pacchetto riassemblato

Per la verifica incrociata, abbiamo esaminato i log di ISE e abbiamo scoperto che la richiesta di accesso, che era stata frammentata sul controller wireless, non veniva ricevuta da ISE.

ISE TCP Dump

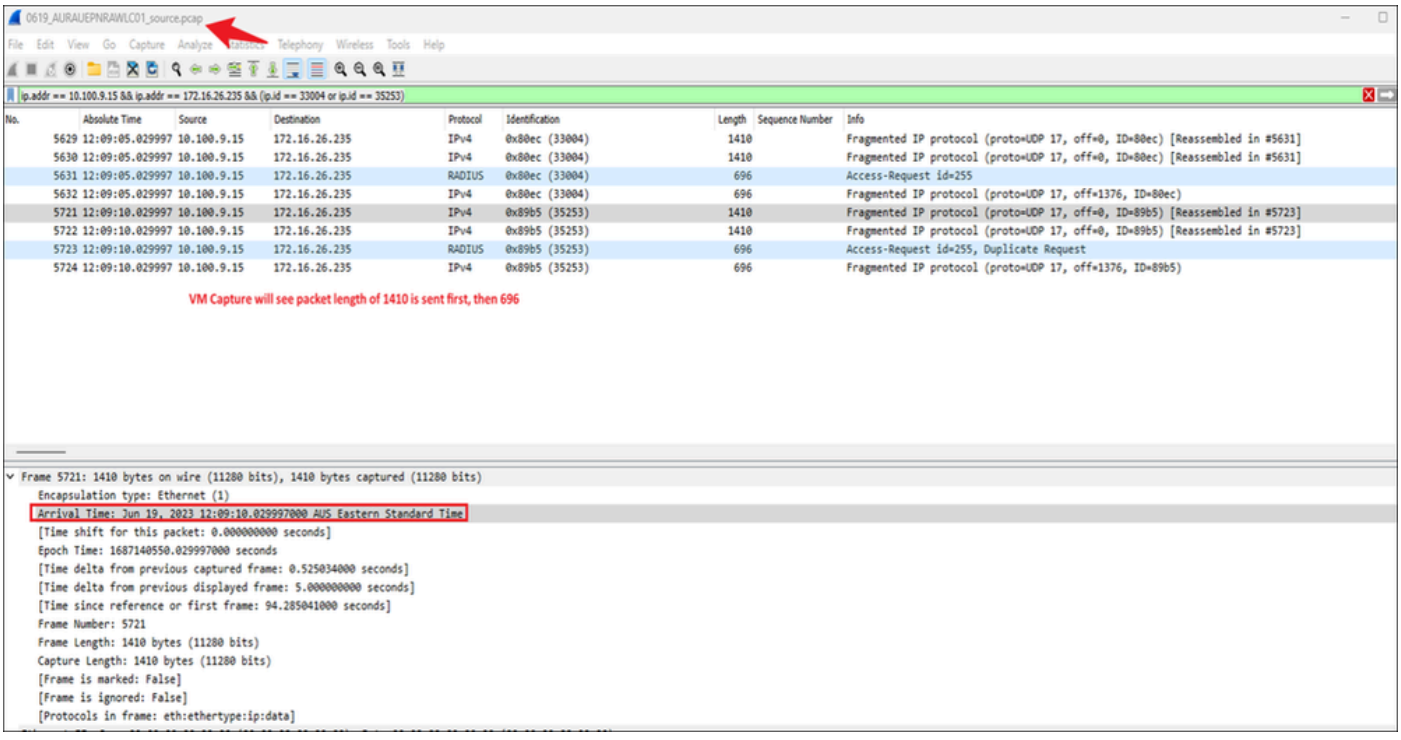
radius.code == 1

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

Clip su ISE End

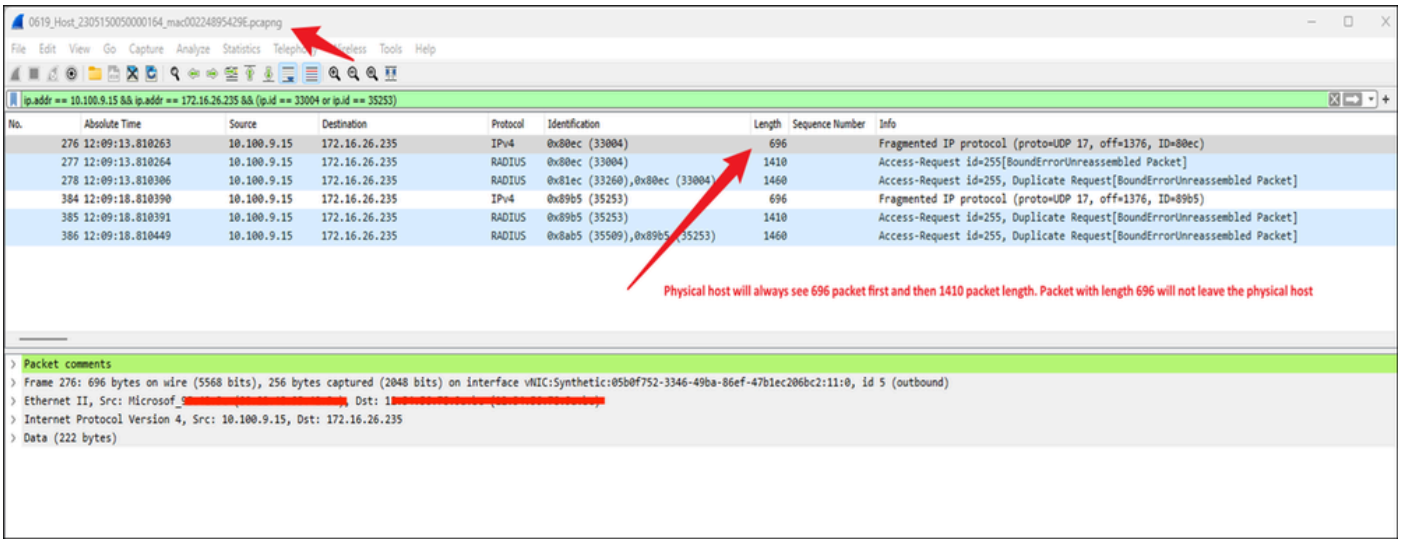
Azure Side Capture con analisi:

Il team di Azure ha eseguito un'acquisizione sull'host fisico in Azure. I dati acquisiti sullo switch vSwitch nell'host di Azure indicano che i pacchetti UDP stanno arrivando fuori sequenza. Questi frammenti UDP non sono nell'ordine corretto. Azure li sta eliminando. Di seguito sono riportate le clip acquisite sia dall'estremità di Azure che dal controller wireless, acquisite contemporaneamente per l'ID richiesta di accesso = 255, in cui il problema dei pacchetti non in ordine è evidente:
L'EPC (Encapsulated Packet Capture) sul controller wireless visualizza la sequenza in cui i pacchetti frammentati lasciano il controller wireless.



Sequenza di pacchetti frammentati sul WLC

Sull'host fisico, i pacchetti non arrivano nella sequenza corretta



Acquisizioni in Azure End

Poiché i pacchetti stanno arrivando nell'ordine sbagliato e il nodo fisico è programmato per rifiutare i frame non ordinati, i pacchetti vengono scartati immediatamente. L'interruzione causa il fallimento del processo di autenticazione e impedisce al client di superare la fase di autenticazione.

Soluzione suggerita dall'estremità del controller wireless:

A partire dalla versione 17.11.1, stiamo implementando il supporto per i frame jumbo nei pacchetti Radius/AAA. Questa funzione consente al controller c9800 di evitare la frammentazione dei pacchetti AAA, a condizione che sul controller sia impostata la seguente configurazione. Per evitare la frammentazione completa di questi pacchetti, è essenziale verificare che ogni hop di rete, incluso il server AAA, sia compatibile con i pacchetti Jumbo Frame. Per ISE, il supporto di Jumbo Frame inizia con la versione 3.1 in avanti.
Configurazione interfaccia sul controller wireless:

C9800-CL(config)#interface

C9800-CL(config-if) # mtu

C9800-CL(config-if) # ip mtu

[1500 to 9000]

Configurazione server AAA sul controller wireless:

C9800-CL(config)# aaa group server radius

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

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

Di seguito viene riportato un breve elenco di un pacchetto Radius quando l'MTU (Maximum Transmission Unit) è configurata su 3000 byte su un controller WLC. I pacchetti inferiori a 3000 byte sono stati inviati senza problemi senza bisogno di frammentazione:

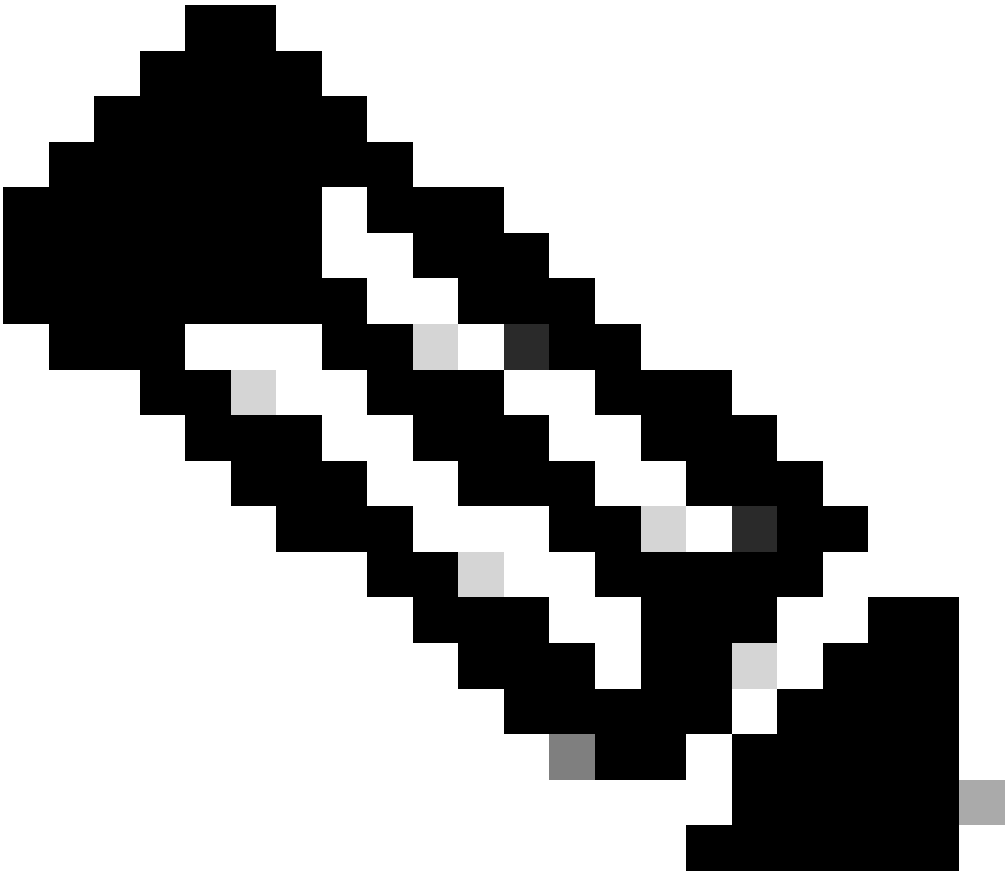
```
1020 10:08:11.177984 RADIUS          2075 Access-Request id=199
1021 10:08:11.177984 RADIUS          2075 Access-Request id=199, Duplicate Request
1119 10:08:16.194981 RADIUS          2075 Access-Request id=199, Duplicate Request
1120 10:08:16.194981 RADIUS          2075 Access-Request id=199, Duplicate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

Acquisizione dei pacchetti sul WLC con MTU aumentata

Impostando la configurazione in questo modo, il controller wireless trasmette i pacchetti senza frammentarli, inviandoli intatti. Tuttavia, poiché il cloud di Azure non supporta i frame jumbo, non è possibile implementare questa soluzione.

Soluzione:

- Da EPC (Encapsulated Packet Capture) del controller wireless è stato rilevato che i pacchetti vengono inviati nell'ordine corretto. Spetta quindi all'host ricevente ricomporre i frammenti in modo corretto e continuare l'elaborazione che, in questo caso, non viene eseguita sul lato di Azure.
- Per risolvere il problema dei pacchetti UDP non ordinati, è necessario attivare questa`enable-udp-fragment-reordering`opzione in Azure.
- È necessario rivolgersi al team di supporto di Azure per assistenza su questo argomento. Microsoft ha riconosciuto questo problema.



Nota: Si noti che questo problema non riguarda esclusivamente il controller WLC (Wireless LAN Controller). Problemi simili relativi a pacchetti UDP non ordinati sono stati riscontrati in server RADIUS diversi, inclusi i server ISE, Forti Authenticator e RTSP, in particolare quando operano nell'ambiente di Azure.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).