Informazioni sul rilevamento della PMTU del punto di accesso CAPWAP

Sommario

Introduzione

In questo documento viene descritto il meccanismo di rilevamento della PMTU (Maximum Transmission Unit) del punto di accesso CAPWAP su IOS® XE e COS, nonché i problemi e la risoluzione.

Scenario e ambito

In genere, i problemi di PMTU si verificano quando un punto di accesso CAPWAP (AP) in un sito remoto si registra su un controller WLC (Wireless LAN Controller) su una WAN, in particolare quando il percorso include una VPN, un GRE o un segmento di rete con MTU inferiore ai 1500 byte standard.

Viene inoltre esaminata l'autenticazione con EAP-TLS (Extensible Authentication Protocol Transport Layer Security). Poiché EAP-TLS scambia certificati di grandi dimensioni, una MTU del percorso ridotta aumenta il rischio di frammentazione.

Tutti i registri sono stati acquisiti in base al codice versione 17.9.3. Gli output vengono troncati per mostrare solo le righe pertinenti.

Confronto tra controllo CAPWAP e dati (Elementi negoziati)

Controllo CAPWAP:

Il canale di controllo gestisce i messaggi di gestione critici, quali le richieste di join, gli scambi di configurazione e i segnali keepalive. Questi messaggi sono protetti tramite DTLS e rappresentano l'obiettivo principale del processo di negoziazione della PMTU (Path MTU) per garantire una comunicazione del control plane affidabile ed efficiente.

Dati CAPWAP:
Questo canale trasmette il traffico client incapsulato, in genere protetto anche da DTLS nella maggior parte delle distribuzioni. Mentre la negoziazione PMTU si verifica sul canale di controllo, i valori PMTU risultanti determinano indirettamente le dimensioni massime del pacchetto per l'incapsulamento del piano dati, influendo sull'affidabilità della trasmissione e sulla frammentazione dei dati del client.

Esempi

- Pacchetti di controllo: Richieste e risposte di join, aggiornamenti della configurazione e messaggi echo/keepalive.
- Pacchetti dati: Frame client incapsulati trasmessi tra il punto di accesso (AP) e il controller WLC.

Fatti: Dimensioni massime pacchetto CAPWAP

IOS AP (esempio)

Dimensioni pacchetto PMTU inviato: 1499 byte = Ethernet + CAPWAP PMTU

- Ethernet = 14 byte
- CAPWAP PMTU = 1485 byte
    - IP esterno = 20 byte
    - UDP = 25 byte
    - DTLS = 1440 byte

AP-COS (esempio)

Dimensioni pacchetto PMTU inviato: 1483 byte = Ethernet + CAPWAP PMTU

- Ethernet = 14 byte
- CAPWAP PMTU = 1469 byte
    - IP esterno = 20 byte
    - UDP = 25 byte
    - DTLS = 1424 byte

Controlli PMTU a tre fasi

Entrambe le piattaforme richiedono tre valori PMTU hardcoded: 576, 1005 e 1485. La differenza sta nel modo in cui ciascuna piattaforma conta l'intestazione Ethernet:

- I punti di accesso IOS non includono l'intestazione Ethernet nei valori 576/1005/1485.

- Frame totale = Ethernet (14) + PMTU (576/1005/1485)⇒ 590, 1019, 1499 byte (dimensioni del filo).

- AP-COS non include l'intestazione Ethernet nei valori 576/1005/1485.
  - Frame totale = PMTU (include già Ethernet). Questi pacchetti sono più piccoli di 14 byte su cavo degli equivalenti IOS AP.

Meccanismo di rilevamento CAPWAP PMTU

Comportamento di IOS AP

Fase di join AP

Durante il join CAPWAP, l'access point negozia una PMTU CAPWAP massima di 1485 byte con il bit DF impostato. Attende una risposta di 5 secondi.

- Se non arriva alcuna risposta o viene visualizzata la dicitura "Frammentazione richiesta" ICMP, l'access point torna a 576 byte per completare rapidamente l'unione, quindi cerca di aumentare la PMTU dopo aver raggiunto il valore RUN.

Acquisizione pacchetti (esempio)

Pacchetto numero 106 Viene visualizzata una sonda da 1499 byte (DF impostato). Nessuna risposta delle stesse dimensioni indica che il pacchetto non può attraversare il percorso senza frammentazione. In questo modo viene visualizzato il messaggio ICMP "Frammentazione richiesta".

17	07:41:47.427848	0.002187	10.201.166.185	10.201.234.34	CAPWAP-Cont…	264	Set	CAPWAP-Control - Discovery Request[Malformed Packet]
88	07:42:45.435367	58.0075…	10.201.166.185	10.201.234.34	DTLSv1.0	117	Set	Client Hello
92	07:42:45.437784	0.002417	10.201.166.185	10.201.234.34	DTLSv1.0	137	Set	Client Hello
98	07:42:45.667215	0.229431	10.201.166.185	10.201.234.34	DTLSv1.0	590	Set	Certificate (Fragment)
99	07:42:45.667260	0.000045	10.201.166.185	10.201.234.34	DTLSv1.0	590	Set	Certificate (Fragment)
100	07:42:45.667293	0.000033	10.201.166.185	10.201.234.34	DTLSv1.0	178	Set	Certificate (Reassembled)
101	07:42:45.667316	0.000023	10.201.166.185	10.201.234.34	DTLSv1.0	329	Set	Client Key Exchange
102	07:42:45.667347	0.000031	10.201.166.185	10.201.234.34	DTLSv1.0	329	Set	Certificate Verify
103	07:42:45.667372	0.000025	10.201.166.185	10.201.234.34	DTLSv1.0	60	Set	Change Cipher Spec
104	07:42:45.667394	0.000022	10.201.166.185	10.201.234.34	DTLSv1.0	123	Set	Encrypted Handshake Message
106	07:42:45.674895	0.007501	10.201.166.185	10.201.234.34	DTLSv1.0	1499	Set	Application Data
107	07:42:45.675288	0.000393	10.201.166.161	10.201.166.185	ICMP	70	Not set,Set	Destination unreachable (Fragmentation needed)
112	07:42:50.671019	4.995731	10.201.166.185	10.201.234.34	DTLSv1.0	411	Set	Application Data
114	07:42:50.718532	0.047513	10.201.166.185	10.201.234.34	DTLSv1.0	539	Set	Application Data
115	07:42:50.718571	0.000039	10.201.166.185	10.201.234.34	DTLSv1.0	539	Set	Application Data

Il corrispondente comando debug a livello AP ("debug capwap client path-mtu") mostra che l'access point ha provato per primo con 1485 byte e ha atteso una risposta per 5 secondi. In assenza di risposta, viene inviato un altro pacchetto di richiesta di unione di lunghezza inferiore, in quanto si trova ancora nella fase di unione e non c'è tempo da perdere. Per fare in modo che l'access point si colleghi al WLC, viene raggiunto il valore minimo indicato nel log di debug:

```
*Jul 11 18:27:15.000: CAPWAP_PATHMTU: CAPWAP_DTLS_SETUP: MTU = 1485
*Jul 11 18:27:15.000: CAPWAP_PATHMTU: Setting default MTU: MTU discovery can start with 576
*Jul 11 18:27:15.235: %CAPWAP-5-DTLSREQSUCC: DTLS connection created sucessfully peer_ip: 10.201.234.34
*Jul 11 18:27:15.235: CAPWAP_PATHMTU: Sending Join Request Path MTU payload, Length 1376, MTU 576
*Jul 11 18:27:15.235: %CAPWAP-5-SENDJOIN: sending Join Request to 10.201.234.34
...
```

```
*Jul 11 18:27:20.235: %CAPWAP-5-SENDJOIN: sending Join Request to 10.201.234.34
*Jul 11 18:27:21.479: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller c9800-CL
```

E se si esegue #show capwap client rcb in questo momento, si osserverà che l'MTU del CAPWAP è di 576 byte:

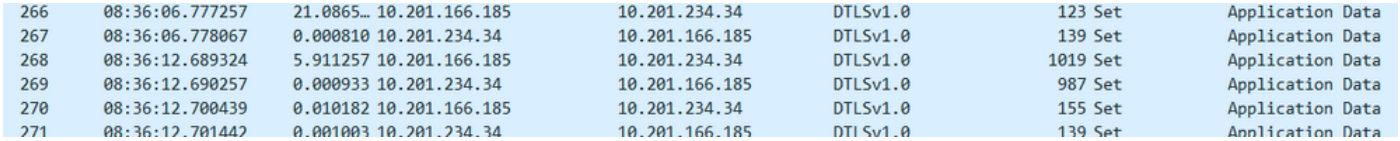
```
3702-AP#show capwap client rcb
AdminState : ADMIN_ENABLED
Primary SwVer : 17.9.3.50
..
MwarName : c9800-CL
MwarApMgrIp : 10.201.234.34
OperationState : JOIN
CAPWAP Path MTU : 576
```

Fase stato di esecuzione

Dopo che l'access point si è unito correttamente al controller LAN wireless. è in corso la verifica del meccanismo di rilevamento della PMTU. Dopo 30 secondi, l'access point può negoziare un valore PMTU più alto inviando un altro pacchetto CAPWAP il cui bit DF sia impostato sulle dimensioni del successivo valore PMTU più alto.

Nell'esempio, l'access point ha provato con un valore di 1005 byte. Poiché IOS esclude Ethernet dal campo PMTU, il cavo visualizza 1019 byte. Se il WLC risponde, l'access point aggiorna la PMTU a 1005 byte. In caso contrario, attende 30 secondi e riprova.

In questa schermata viene mostrata una negoziazione AP riuscita con 1005 PMTU (vedere i pacchetti #268 e #269). Notare che questi pacchetti hanno dimensioni diverse, il che è dovuto al fatto che il WLC ha un algoritmo diverso per il calcolo della PMTU.



266	08:36:06.777257	21.0865…	10.201.166.185	10.201.234.34	DTLSv1.0	123 Set	Application Data
267	08:36:06.778067	0.000810	10.201.234.34	10.201.166.185	DTLSv1.0	139 Set	Application Data
268	08:36:12.689324	5.911257	10.201.166.185	10.201.234.34	DTLSv1.0	1019 Set	Application Data
269	08:36:12.690257	0.000933	10.201.234.34	10.201.166.185	DTLSv1.0	987 Set	Application Data
270	08:36:12.700439	0.010182	10.201.166.185	10.201.234.34	DTLSv1.0	155 Set	Application Data
271	08:36:12.701442	0.001003	10.201.234.34	10.201.166.185	DTLSv1.0	139 Set	Application Data

In questo caso, il comando debug al livello AP corrispondente (debug capwap client pmtu) mostra dove l'access point ha negoziato correttamente la PMTU di 1005 byte e ha aggiornato il valore della PMTU dell'access point.

```
*Jul 11 18:28:39.911: CAPWAP_PATHMTU: PMTU Timer Expired: Trying to send higher MTU packet 576
*Jul 11 18:28:39.911: CAPWAP_PATHMTU: PMTU Timer:Sending Path MTU packet of size 1005
*Jul 11 18:28:39.911: CAPWAP_PATHMTU: MTU = 1005 for current MTU path discovery
*Jul 11 18:28:39.911: CAPWAP_PATHMTU: Ap Path MTU payload with MTU 1005 sent 888
*Jul 11 18:28:39.911: CAPWAP_PATHMTU: Stopping the message timeout timer
*Jul 11 18:28:39.911: CAPWAP_PATHMTU: Setting MTU to : 1005, it was 576
*Jul 11 18:28:39.911: CAPWAP_PATHMTU: Updating MTU to DPAA
*Jul 11 18:28:39.915: CAPWAP_PATHMTU: Sending MTU update to WLC
```

```
*Jul 11 18:28:39.915: CAPWAP_PATHMTU: MTU = 1005 for current MTU path discovery
*Jul 11 18:28:39.915: CAPWAP_PATHMTU: Ap Path MTU payload with MTU 1005 sent 21
```

Se invece si usa (#show capwap client rcb) in questo momento, si osserverà che l'MTU del punto di accesso CAPWAP è 1005 byte. Di seguito è riportato l'output del comando show:

```
3702-AP#show capwap client rcb
AdminState : ADMIN_ENABLED
Primary SwVer : 17.9.3.50
Name : 3702-AP
MwarName : c9800-CL
MwarApMgrIp : 10.201.234.34
OperationState : UP
CAPWAP Path MTU : 1005
```

Dopo 30 secondi, l'access point tenta di nuovo di negoziare il valore immediatamente superiore a 1485 byte, ma ha ricevuto un messaggio ICMP "destinazione irraggiungibile" mentre lo stato dell'access point è in stato RUN. L'ICMP unreachable ha un valore per l'hop successivo, che l'AP rispetta e usa per calcolare la propria PMTU, come mostrato nei debug.

```
*Jul 11 18:29:45.911: CAPWAP_PATHMTU: PMTU Timer:Sending Path MTU packet of size 1485
*Jul 11 18:29:45.911: CAPWAP_PATHMTU: MTU = 1485 for current MTU path discovery
*Jul 11 18:29:45.911: CAPWAP_PATHMTU: Ap Path MTU payload with MTU 1485 sent 1368
*Jul 11 18:29:45.911: CAPWAP_PATHMTU: Received ICMP Dst unreachable
*Jul 11 18:29:45.911: CAPWAP_PATHMTU: Src port:5246 Dst Port:60542, SrcAddr:10.201.166.185 Dst Addr:10.
*Jul 11 18:29:45.911: CAPWAP_PATHMTU: Calculated MTU 1293, last_icmp_mtu 1300
*Jul 11 18:29:48.911: CAPWAP_PATHMTU: Path MTU message could not reach WLC, Removing it from the Reliab
```

Acquisizioni del livello AP corrispondente

Notare il pacchetto ICMP "destinazione irraggiungibile" numero 281, quindi l'access point cerca di negoziare una PMTU rispettando il valore dell'hop successivo ICMP su 1300 byte sui pacchetti numero 288 e la risposta su 289:

280	08:36:42.691876	23.9733…	10.201.166.185	10.201.234.34	DTLSv1.0	1499 Set	Application Data
281	08:36:42.692200	0.000324	10.201.166.161	10.201.166.185	ICMP	70 Not set,Set	Destination unreachable (Fragmentation needed)
282	08:36:45.695098	3.002898	10.201.166.185	10.201.234.34	CAPWAP-Data	92 Set	CAPWAP-Data Keep-Alive[Malformed Packet]
283	08:36:45.695533	0.000435	10.201.166.185	10.201.234.34	DTLSv1.0	139 Set	Application Data
284	08:36:45.695785	0.000252	10.201.234.34	10.201.166.185	CAPWAP-Data	92 Set	CAPWAP-Data Keep-Alive[Malformed Packet]
285	08:36:45.695931	0.000146	10.201.234.34	10.201.166.185	DTLSv1.0	123 Set	Application Data
286	08:36:45.696416	0.000485	10.201.166.185	10.201.234.34	DTLSv1.0	155 Set	Application Data
287	08:36:45.696981	0.000565	10.201.234.34	10.201.166.185	DTLSv1.0	139 Set	Application Data
288	08:36:48.695568	2.998587	10.201.166.185	10.201.234.34	DTLSv1.0	1307 Set	Application Data
289	08:36:48.696456	0.000888	10.201.234.34	10.201.166.185	DTLSv1.0	1275 Set	Application Data
290	08:36:48.706641	0.010185	10.201.166.185	10.201.234.34	DTLSv1.0	155 Set	Application Data
291	08:36:48.707636	0.000995	10.201.234.34	10.201.166.185	DTLSv1.0	139 Set	Application Data

Comportamento COS AP

Esistono differenze nel meccanismo di rilevamento per i punti di accesso AP-COS. Iniziamo da AP join.

Fase di join AP

Al momento del join, l'access point invia una richiesta di join con il valore massimo e attende cinque secondi.

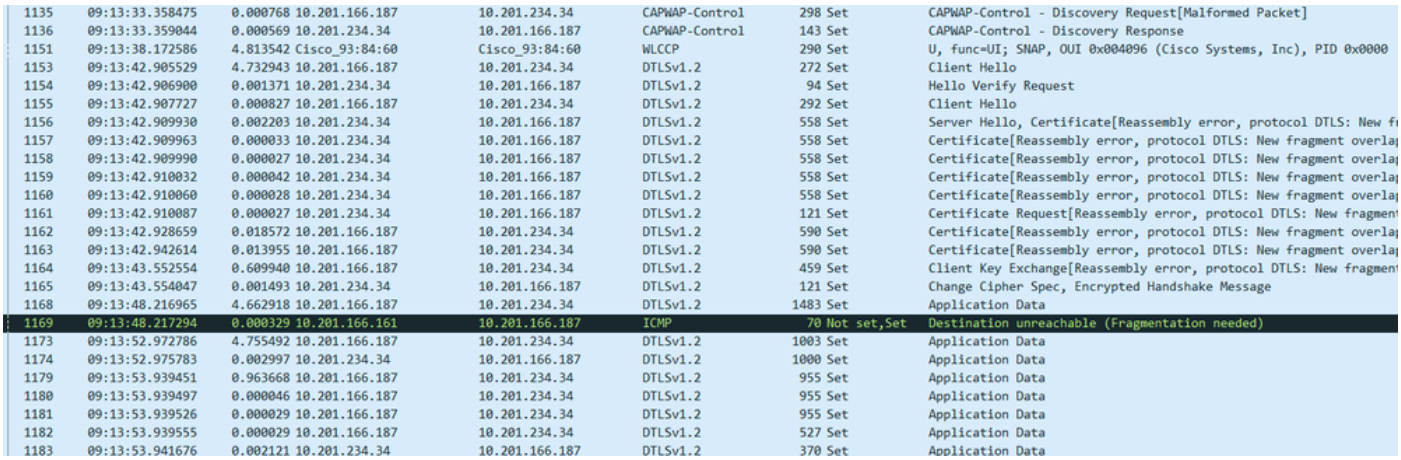
Se non viene fornita alcuna risposta, l'operazione verrà ripetuta e verranno attesi altri cinque secondi.

Se ancora non risponde, invia un'altra richiesta di join con 1005 byte. Se l'operazione ha esito positivo, la PMTU viene aggiornata e l'operazione prosegue (ad esempio, il download delle immagini). Se la sonda DF da 1005 byte non riesce ancora a raggiungere il controller, scende al minimo di 576 byte e riprova.

Di seguito è riportata la pmtu del client debug capwap sul livello AP:

```
Jul 11 19:06:10 kernel: [*07/11/2023 19:06:10.7065] AP_PATH_MTU_PAYLOAD_msg_enc_cb: request pmtu 1485, 
Jul 11 19:06:10 kernel: [*07/11/2023 19:06:10.7066] Sending Join request to 10.201.234.34 through port 
Jul 11 19:06:10 kernel: [*07/11/2023 19:06:10.7066] Sending Join Request Path MTU payload, Length 1376
..
Jul 11 19:06:15 kernel: [*07/11/2023 19:06:15.3235] AP_PATH_MTU_PAYLOAD_msg_enc_cb: request pmtu 1485, 
Jul 11 19:06:15 kernel: [*07/11/2023 19:06:15.3235] Sending Join request to 10.201.234.34 through port 
Jul 11 19:06:15 kernel: [*07/11/2023 19:06:15.3235] Sending Join Request Path MTU payload, Length 1376
Jul 11 19:06:15 kernel: [*07/11/2023 19:06:15.3245] chatter: chkcapwapicmpneedfrag :: CheckCapwapICMPNe
..
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.0794] AP_PATH_MTU_PAYLOAD_msg_enc_cb: request pmtu 1005, 
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.0794] Sending Join request to 10.201.234.34 through port 
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.0794] Sending Join Request Path MTU payload, Length 896
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.0831] Join Response from 10.201.234.34, packet size 917
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.0832] AC accepted previous sent request with result code:
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.0832] Received wlcType 0, timer 30
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.5280] WLC confirms PMTU 1005, updating MTU now.
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.5702] PMTU: Set capwap_init_mtu to TRUE and dcb's mtu to 
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.5816] CAPWAP State: Image Data
Jul 11 19:06:20 kernel: [*07/11/2023 19:06:20.5822] AP image version 17.9.3.50 backup 17.6.5.22, Contro
```

Si noti che le dimensioni del pacchetto sono di 1483 byte, ossia il valore pmtu senza l'intestazione ethernet come previsto per AP-COS. È possibile vedere questo sul pacchetto numero 1168 qui:



1135	09:13:33.358475	0.000768	10.201.166.187	10.201.234.34	CAPWAP-Control	298 Set	CAPWAP-Control - Discovery Request[Malformed Packet]
1136	09:13:33.359044	0.000569	10.201.234.34	10.201.166.187	CAPWAP-Control	143 Set	CAPWAP-Control - Discovery Response
1151	09:13:38.172586	4.813542	Cisco_93:84:60	Cisco_93:84:60	WLCCP	290 Set	U, func=UI; SNAP, OUI 0x004096 (Cisco Systems, Inc), PID 0x0000
1153	09:13:42.905529	4.732943	10.201.166.187	10.201.234.34	DTLSv1.2	272 Set	Client Hello
1154	09:13:42.906900	0.001371	10.201.234.34	10.201.166.187	DTLSv1.2	94 Set	Hello Verify Request
1155	09:13:42.907727	0.000827	10.201.166.187	10.201.234.34	DTLSv1.2	292 Set	Client Hello
1156	09:13:42.909930	0.002203	10.201.234.34	10.201.166.187	DTLSv1.2	558 Set	Server Hello, Certificate[Reassembly error, protocol DTLS: New f
1157	09:13:42.909963	0.000033	10.201.234.34	10.201.166.187	DTLSv1.2	558 Set	Certificate[Reassembly error, protocol DTLS: New fragment overla
1158	09:13:42.909990	0.000027	10.201.234.34	10.201.166.187	DTLSv1.2	558 Set	Certificate[Reassembly error, protocol DTLS: New fragment overla
1159	09:13:42.910032	0.000042	10.201.234.34	10.201.166.187	DTLSv1.2	558 Set	Certificate[Reassembly error, protocol DTLS: New fragment overla
1160	09:13:42.910060	0.000028	10.201.234.34	10.201.166.187	DTLSv1.2	558 Set	Certificate[Reassembly error, protocol DTLS: New fragment overla
1161	09:13:42.910087	0.000027	10.201.234.34	10.201.166.187	DTLSv1.2	121 Set	Certificate Request[Reassembly error, protocol DTLS: New fragmen
1162	09:13:42.928659	0.018572	10.201.166.187	10.201.234.34	DTLSv1.2	590 Set	Certificate[Reassembly error, protocol DTLS: New fragment overla
1163	09:13:42.942614	0.013955	10.201.166.187	10.201.234.34	DTLSv1.2	590 Set	Certificate[Reassembly error, protocol DTLS: New fragment overla
1164	09:13:43.552554	0.609940	10.201.166.187	10.201.234.34	DTLSv1.2	459 Set	Client Key Exchange[Reassembly error, protocol DTLS: New fragmen
1165	09:13:43.554047	0.001493	10.201.234.34	10.201.166.187	DTLSv1.2	121 Set	Change Cipher Spec, Encrypted Handshake Message
1168	09:13:48.216965	4.662918	10.201.166.187	10.201.234.34	DTLSv1.2	1483 Set	Application Data
1169	09:13:48.217294	0.000329	10.201.166.161	10.201.166.187	ICMP	70 Not set,Set	Destination unreachable (Fragmentation needed)
1173	09:13:52.972786	4.755492	10.201.166.187	10.201.234.34	DTLSv1.2	1003 Set	Application Data
1174	09:13:52.975783	0.002997	10.201.234.34	10.201.166.187	DTLSv1.2	1000 Set	Application Data
1179	09:13:53.939451	0.963668	10.201.166.187	10.201.234.34	DTLSv1.2	955 Set	Application Data
1180	09:13:53.939497	0.000046	10.201.166.187	10.201.234.34	DTLSv1.2	955 Set	Application Data
1181	09:13:53.939526	0.000029	10.201.166.187	10.201.234.34	DTLSv1.2	955 Set	Application Data
1182	09:13:53.939555	0.000029	10.201.166.187	10.201.234.34	DTLSv1.2	527 Set	Application Data
1183	09:13:53.941676	0.002121	10.201.234.34	10.201.166.187	DTLSv1.2	370 Set	Application Data

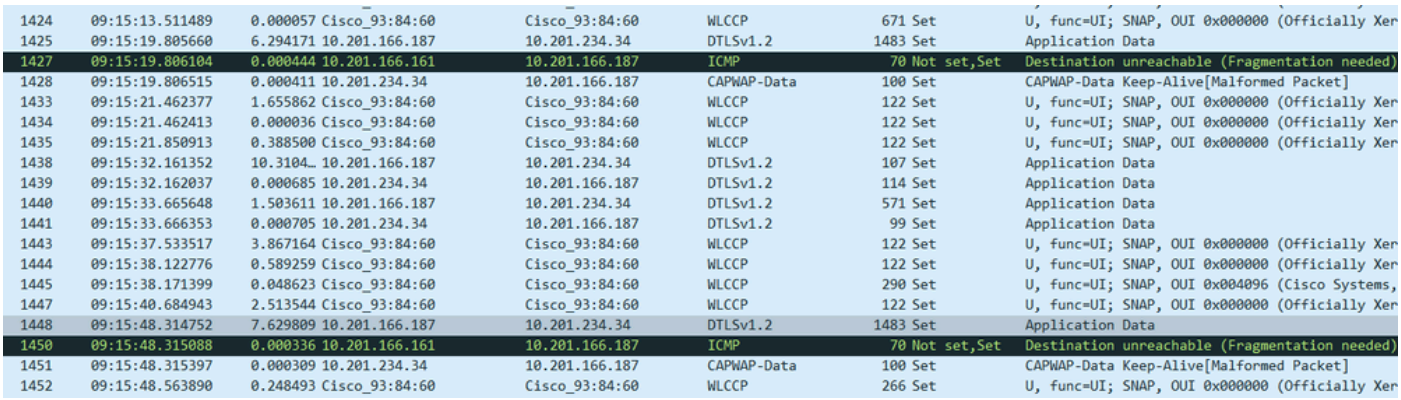
Fase stato di esecuzione

Quando l'access point raggiunge lo stato RUN. continua a cercare di migliorare la PMTU ogni 30 secondi, inviando pacchetti CAPWAP con DF impostato e il successivo valore hardcoded.

Di seguito è riportato il comando AP level debug (debug capwap client pmtu)

```
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1341] wtpEncodePathMTUPayload: Total Packet Size:
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1341] wtpEncodePathMTUPayload: Capwap Size is 137
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1341] [ENC]AP_PATH_MTU_PAYLOAD: pmtu 1485, len 13
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1341] capwap_build_and_send_pmtu_packet: packet l
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1343] Ap Path MTU payload sent, length 1368
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1343] WTP Event Request: AP Path MTU payload sent
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1351] pmtu icmp pkt(ICMP_NEED_FRAG) from click re
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1351] chatter: chkcapwapicmpneedfrag :: CheckCapw
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1351] PMTU data: dcb->mtu 1005, pmtu_overhead:118
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1351] PMTU: Last try for next hop MTU failed
Jul 11 19:08:17 kernel: [*07/11/2023 19:08:17.9850] wtpCleanupPMTUPacket: PMTU: Found matching
..
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6435] wtpEncodePathMTUPayload: Total Packet Size:
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6435] wtpEncodePathMTUPayload: Capwap Size is 137
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6436] [ENC]AP_PATH_MTU_PAYLOAD: pmtu 1485, len 13
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6436] capwap_build-and-send_pmtu_packet: packet l
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6437] Ap Path MTU payload sent, length 1368
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6438] WTP Event Request: AP Path MTU payload sent
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6446] pmtu icmp pkt(ICMP_NEED_FRAG) from click re
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6446] chatter: chkcapwapicmpneedfrag :: CheckCapw
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6446] PMTU data: dcb->mtu 1005, pmtu_overhead:118
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6447] PMTU: Last try for next hop MTU failed
Jul 11 19:08:46 kernel: [*07/11/2023 19:08:46.4945] wtpCleanupPMTUPacket: PMTU: Found matching
```

Di seguito sono riportate le acquisizioni corrispondenti dell'access point. esaminare i pacchetti numero 1427 e 1448:



1424	09:15:13.511489	0.000057	Cisco_93:84:60	Cisco_93:84:60	WLCCP	671 Set	U, func=UI; SNAP, OUI 0x000000 (Officially Xer
1425	09:15:19.805660	6.294171	10.201.166.187	10.201.234.34	DTLSv1.2	1483 Set	Application Data
1427	09:15:19.806104	0.000444	10.201.166.161	10.201.166.187	ICMP	70 Not set,Set	Destination unreachable (Fragmentation needed)
1428	09:15:19.806515	0.000411	10.201.234.34	10.201.166.187	CAPWAP-Data	100 Set	CAPWAP-Data Keep-Alive[Malformed Packet]
1433	09:15:21.462377	1.655862	Cisco_93:84:60	Cisco_93:84:60	WLCCP	122 Set	U, func=UI; SNAP, OUI 0x000000 (Officially Xer
1434	09:15:21.462413	0.000036	Cisco_93:84:60	Cisco_93:84:60	WLCCP	122 Set	U, func=UI; SNAP, OUI 0x000000 (Officially Xer
1435	09:15:21.850913	0.388500	Cisco_93:84:60	Cisco_93:84:60	WLCCP	122 Set	U, func=UI; SNAP, OUI 0x000000 (Officially Xer
1438	09:15:32.161352	10.3104…	10.201.166.187	10.201.234.34	DTLSv1.2	107 Set	Application Data
1439	09:15:32.162037	0.000685	10.201.234.34	10.201.166.187	DTLSv1.2	114 Set	Application Data
1440	09:15:33.665648	1.503611	10.201.166.187	10.201.234.34	DTLSv1.2	571 Set	Application Data
1441	09:15:33.666353	0.000705	10.201.234.34	10.201.166.187	DTLSv1.2	99 Set	Application Data
1443	09:15:37.533517	3.867164	Cisco_93:84:60	Cisco_93:84:60	WLCCP	122 Set	U, func=UI; SNAP, OUI 0x000000 (Officially Xer
1444	09:15:38.122776	0.589259	Cisco_93:84:60	Cisco_93:84:60	WLCCP	122 Set	U, func=UI; SNAP, OUI 0x000000 (Officially Xer
1445	09:15:38.171399	0.048623	Cisco_93:84:60	Cisco_93:84:60	WLCCP	290 Set	U, func=UI; SNAP, OUI 0x004096 (Cisco Systems,
1447	09:15:40.684943	2.513544	Cisco_93:84:60	Cisco_93:84:60	WLCCP	122 Set	U, func=UI; SNAP, OUI 0x000000 (Officially Xer
1448	09:15:48.314752	7.629809	10.201.166.187	10.201.234.34	DTLSv1.2	1483 Set	Application Data
1450	09:15:48.315088	0.000336	10.201.166.161	10.201.166.187	ICMP	70 Not set,Set	Destination unreachable (Fragmentation needed)
1451	09:15:48.315397	0.000309	10.201.234.34	10.201.166.187	CAPWAP-Data	100 Set	CAPWAP-Data Keep-Alive[Malformed Packet]
1452	09:15:48.563890	0.248493	Cisco_93:84:60	Cisco_93:84:60	WLCCP	266 Set	U, func=UI; SNAP, OUI 0x000000 (Officially Xer

Conclusione (Riepilogo algoritmi)

In sintesi, l'algoritmo CAPWAP PMTUD sui punti di accesso funziona in questo modo.

Passaggio 1. La PMTU CAPWAP iniziale viene negoziata durante la fase di join dell'access point.

Passaggio 2. 30 secondi dopo, l'access point tenta di migliorare la PMTU del CAPWAP corrente inviando il successivo valore più alto predefinito (576, 1005, 1485 byte).

Passaggio 3 (opzione 1). Se il WLC risponde, regolare la PMTU del CAPWAP corrente sul nuovo valore e ripetere il passaggio 2.

Passaggio 3 (opzione 2). Se non viene fornita alcuna risposta, mantenere la PMTU CAPWAP corrente e ripetere il passaggio 2.

Passaggio 3 (opzione 3) Se non viene ricevuta alcuna risposta e un messaggio ICMP "destinazione irraggiungibile" (tipo 3, codice 4) include un'MTU dell'hop successivo, regolare la PMTU del CAPWAP su tale valore e ripetere il passaggio 2.

NOTA: Vedere le correzioni per assicurarsi che venga usata la PMTU CAPWAP corretta quando si fornisce un valore ICMP dell'hop successivo.

CDET correlati

Numero problema 1:

ID bug Cisco CSCwf52815

I punti di accesso AP-COS non rispettano il valore ICMP "destinazione irraggiungibile" dell'hop successivo quando le richieste di valore superiore hanno esito negativo.
Correzioni: 8.10.190.0, 17.3.8, 17.6.6, 17.9.5, 17.12.2.
Gli access point IOS rispettano il valore dell'hop successivo e aggiornano la PMTU.

Numero problema 2:

ID bug Cisco CSCwc05350

La MTU asimmetrica (WLC→AP diverso da AP→WLC) ha causato il flapping della PMTU quando l'ICMP non rifletteva la PMTU bidirezionale massima.

Correzioni: 8.10.181.0, 17.3.6, 17.6.5, 17.9.2, 17.10.1.
Soluzione temporanea: configurare la stessa MTU in entrambe le direzioni sui dispositivi che controllano l'MTU (router, firewall, concentratore VPN) tra il WLC e l'AP.

ID bug Cisco lato AP correlato CSCwc05364: I punti di accesso COS migliorano il meccanismo PMTU per essere in grado di identificare le dimensioni massime della MTU direzionale per le MTU asimmetriche

ID bug Cisco lato WLC CSCwc48316: Migliorare i calcoli della PMTU affinché l'access point sia in grado di avere due MTU diverse, una a monte e l'altra (contrassegnata come Chiusa da DE in quanto non è prevista alcuna soluzione)

Numero problema 3:

ID bug Cisco CSCwf91557

AP-COS interrompe il rilevamento della PMTU dopo aver raggiunto il valore massimo hardcoded.

Fissato al punto 17.13.1; anche via Fixed (Risolto) tramite Cisco bug ID CSCwf52815 in 17.3.8, 17.6.6, 17.9.5, 17.12.2.

Numero problema 4:

ID bug Cisco CSCwk70785

AP-COS: impossibile aggiornare il valore MTU della sonda PMTU. Causa della disconnessione.

risolto nell'ID bug Cisco CSCwk90660 - APSP6 17.9.5] Target 17.9.6, 17.12.5, 17.15.2, 17.16.

Numero 5:

ID bug Cisco CSCv53456

Configurazione MTU del percorso statico CAPWAP 9800 (parità con AireOS).

Ciò consente a 9800 di avere un'MTU del percorso CAPWAP statica configurata sulla base del profilo di join per access point. Passiamo alle 17.17.

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).