

瞭解CAPWAP AP PMTU發現

目錄

[簡介](#)

[場景和範圍](#)

[CAPWAP控制與資料 \(協商內容 \)](#)

[事實：最大大小的CAPWAP資料包](#)

[三階段PMTU檢查](#)

[CAPWAP PMTU探索機制](#)

[IOS AP行為](#)

[AP加入階段](#)

[運行狀態階段](#)

[COS AP行為](#)

[AP加入階段](#)

[運行狀態階段](#)

[結論 \(演算法摘要 \)](#)

[相關CDET](#)

簡介

本檔案介紹IOS® XE和COS上的CAPWAP存取點路徑最大傳輸單元(PMTU)探索機制、問題和解決方案。

場景和範圍

當遠端站點的CAPWAP存取點(AP)跨WAN註冊到無線LAN控制器(WLC)時，尤其是當路徑包括VPN、GRE或MTU低於標準1500位元組的網段時，通常會看到PMTU問題。

我們還檢查使用可擴展身份驗證協定傳輸層安全(EAP-TLS)的身份驗證。因為EAP-TLS交換大型證書，所以減少的路徑MTU會增加分段風險。

在代碼版本17.9.3上捕獲所有日誌。輸出被截斷為僅顯示相關行。

CAPWAP控制與資料 (協商內容)

CAPWAP控制：

控制通道處理關鍵管理消息，例如加入請求、配置交換和keepalive訊號。這些消息使用DTLS進行保護，並且是路徑MTU(PMTU)協商過程的主要焦點，以確保可靠、有效的控制平面通訊。

CAPWAP資料：

此通道傳輸封裝的客戶端流量，在大多數部署中通常也受DTLS保護。控制通道上發生PMTU交涉時，產生的PMTU值會間接判斷資料平面封裝的最大封包大小，這會影響使用者端資料傳輸可靠性和分段。

範例

- 控制資料包：加入請求和響應、配置更新以及回應/保持連線消息。
- 資料包：在存取點(AP)和無線LAN控制器(WLC)之間傳輸的封裝使用者端訊框。

事實：最大大小的CAPWAP資料包

IOS AP (示例)

傳送的PMTU封包大小：1499位元組=乙太網+ CAPWAP PMTU

- 乙太網= 14位元組
- CAPWAP PMTU = 1485位元組
 - 外部IP = 20位元組
 - UDP = 25位元組
 - DTLS = 1440位元組

AP-COS (示例)

傳送的PMTU封包大小：1483位元組=乙太網+ CAPWAP PMTU

- 乙太網= 14位元組
- CAPWAP PMTU = 1469位元組
 - 外部IP = 20位元組
 - UDP = 25位元組
 - DTLS = 1424位元組

三階段PMTU檢查

兩個平台都會探測三個硬編碼PMTU值：576、1005和1485。不同之處在於每個平台對乙太網報頭計數的方式：

- IOS AP在576/1005/1485值中不包括乙太網報頭。
 - 幀總數=乙太網(14)+ PMTU(576/1005/1485)⇒ 590、1019、1499位元組 (線大小)。
- AP-COS在576/1005/1485值中包括乙太網報頭。
 - 幀總數= PMTU (已包含乙太網)。這些資料包線路上的大小比IOS AP等效資料包小14位元組。

CAPWAP PMTU探索機制

IOS AP行為

AP加入階段

在CAPWAP連線期間，AP會使用DF位元集協商最大1485位元組的CAPWAP PMTU。它會等待5秒鐘，等待響應。

- 如果沒有回應或ICMP「需要分段」到達，AP將回退到576位元組以快速完成加入，然後嘗試在達到RUN後提高PMTU。

資料包捕獲 (示例)

封包編號106您會看到一個1499位元組的探測 (DF設定)。 沒有大小相同的響應表示資料包無法在不進行分段的情況下遍歷路徑。然後會看到ICMP「需要分段」。

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

對應的AP級別調試(「debug capwap client path-mtu」)顯示，AP首先嘗試了1485個位元組，然後等待5秒進行響應。如果沒有回應，它會傳送另一個長度較小的加入請求封包，因為此封包仍處於加入階段且我們沒有時間浪費。它轉到最小值以使AP加入WLC，如調試日誌所示：

```
*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
```

如果此時運#showcapwap客戶端rcb，則會看到576位元組的CAPWAP AP MTU:

```
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
```

運行狀態階段

AP成功加入無線LAN控制器後。您會看到PMTU探索機制正在起作用，30秒後，您可以看到AP開始

透過傳送另一個CAPWAP封包 (其DF位元設定為下一個最高PMTU值的大小) 來交涉更高的PMTU值。

在本示例中，AP嘗試了1005位元組值。由於IOS將乙太網從PMTU欄位中排除，因此您會看到線路上的1019位元組。如果WLC回應，AP會將PMTU更新為1005位元組。如果不是，它會等待30秒並再次嘗試。

此截圖顯示1005 PMTU的成功的AP交涉(請參閱#268和#269包)。請注意，這些封包具有不同的大小，這是因為WLC具有不同的PMTU計算演演算法。

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

這裡，對應的AP層級偵錯(debug capwap client pmtu)顯示AP成功協商1005位元組PMTU並更新AP PMTU值的位置。

```
*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
```

而且如果您在此刻找到的(#show capwap使用者端rcb)是1005位元組的CAPWAP AP MTU，以下是show輸出：

```
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
```

30秒後，AP再次嘗試協商下一個較高值1485位元組，但是，當AP處於RUN狀態時，AP收到ICMP unreachable。ICMP無法連線具有下一個躍點值，AP認可此值，並使用該值計算其自己的PMTU (我們在偵錯中可看到)。

```
*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
```

相應的AP級別捕獲

請注意ICMP無法到達的封包編號281，然後AP嘗試協商PMTU，確認封包編號288上1300位元組的ICMP下一躍點值並在289上回應：

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	08:36:48.706461	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

COS AP行為

AP-COS AP的發現機制存在差異。我們從AP加入開始。

AP加入階段

在加入時，AP傳送一個最大值的加入請求，等待五秒。

如果沒有響應，它會再次嘗試並再等待五秒。

如果仍然沒有響應，它會傳送另一個包含1005位元組的加入請求。如果成功，則會更新PMTU並繼續（例如映像下載）。如果1005位元組的DF探測器仍無法到達控制器，便會降至最低576並重試。

以下是AP層級上的debug capwap client pmtu:

```
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
```

Ju1 11 19:06:20 kernel: [*07/11/2023 19:06:20.5816] CAPWAP State: Image Data
Ju1 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

請注意，封包大小為1483位元組，這是AP-COS預期的不含乙太網路標頭的pmtu值。以下是在封包編號1168上看到的：

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 fr
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 overl
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 overl
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 overl
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 overl
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 overl
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 overl
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 fragment
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

運行狀態階段

在AP達到RUN狀態後。它會繼續嘗試每30秒改善一次PMTU，並傳送帶有DF設定和下一個硬編碼值的CAPWAP資料包。

以下是AP層級調試(debug capwap client pmtu)

```
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1341] wtpEncodePathMTUPayload: Total Packet Size:
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1341] wtpEncodePathMTUPayload: Capwap Size is 137
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1341] [ENC]AP_PATH_MTU_PAYLOAD: pmtu 1485, len 13
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1341] capwap_build_and_send_pmtu_packet: packet 1
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1343] Ap Path MTU payload sent, length 1368
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1343] WTP Event Request: AP Path MTU payload sent
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1351] pmtu icmp pkt(ICMP_NEED_FRAG) from click re
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1351] chatter: chkcapwapicmpneedfrag :: CheckCapw
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1351] PMTU data: dcb->mtu 1005, pmtu_overhead:118
Ju1 11 19:08:15 kernel: [*07/11/2023 19:08:15.1351] PMTU: Last try for next hop MTU failed
Ju1 11 19:08:17 kernel: [*07/11/2023 19:08:17.9850] wtpCleanupPMTUPacket: PMTU: Found matching I
..
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6435] wtpEncodePathMTUPayload: Total Packet Size:
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6435] wtpEncodePathMTUPayload: Capwap Size is 137
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6436] [ENC]AP_PATH_MTU_PAYLOAD: pmtu 1485, len 13
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6436] capwap_build-and-send_pmtu_packet: packet 1
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6437] Ap Path MTU payload sent, length 1368
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6438] WTP Event Request: AP Path MTU payload sent
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6446] pmtu icmp pkt(ICMP_NEED_FRAG) from click re
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6446] chatter: chkcapwapicmpneedfrag :: CheckCapw
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6446] PMTU data: dcb->mtu 1005, pmtu_overhead:118
Ju1 11 19:08:43 kernel: [*07/11/2023 19:08:43.6447] PMTU: Last try for next hop MTU failed
Ju1 11 19:08:46 kernel: [*07/11/2023 19:08:46.4945] wtpCleanupPMTUPacket: PMTU: Found matching I
```

以下是對應的AP捕獲。檢視封包編號1427和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

結論 (演算法摘要)

總而言之，存取點上的CAPWAP PMTUD演算法是如此運作。

步驟1.在AP加入階段協商初始CAPWAP PMTU。

步驟2. 30秒後，AP嘗試通過傳送下一個預定義的較高值 (576、1005、1485位元組) 來改進當前CAPWAP PMTU。

步驟3 (選項1)。如果WLC響應，請將當前CAPWAP PMTU調整到新值並重複步驟2。

步驟3 (選項2)。如果沒有響應，則保留當前的CAPWAP PMTU並重複步驟2。

步驟3 (選項3)。如果沒有回應，且ICMP無法連線 (型別3，代碼4) 包括下一個躍點的MTU，請將CAPWAP PMTU調整到該值並重複步驟2。

附註：請參閱修復程式，確保在提供ICMP下一跳值時使用正確的CAPWAP PMTU。

相關CDET

問題編號 1:

思科錯誤ID [CSCwf52815](#)

當更高值探測失敗時，AP-COS AP不會認可ICMP不可達下一跳值。

修復：8.10.190.0、17.3.8、17.6.6、17.9.5、17.12.2。

IOS AP採用下一跳值並更新PMTU。

問題二：

思科錯誤ID [CSCwc05350](#)

當ICMP未反映最大→雙向PMTU時，非對稱MTU→WLC-AP不同於AP-WLC)會導致PMTU擺動。

修復：8.10.181.0、17.3.6、17.6.5、17.9.2、17.10.1。

因應措施：在WLC和AP之間控制MTU的裝置 (路由器、防火牆、VPN集中器) 上，在兩個方向上配置相同的MTU。

相關AP端思科錯誤ID [CSCwc05364](#):COS-AP改進PMTU機制，使其能夠識別非對稱MTU的最大方向MTU大小

相關WLC端思科錯誤ID [CSCwc48316](#):改善AP的PMTU計算，使其能夠有一個上游和另一個不同的MTU (標籤為Closed

by DE，因為它們沒有解決此問題的計畫)

問題三：

思科錯誤ID [CSCwf91557](#)

AP-COS在達到最大硬編碼值後停止PMTU發現。

在17.13.1中修復；另請透過思科錯誤ID [CSCwf52815](#) (於17.3.8、17.6.6、17.9.5、17.12.2中修正)。

問題四：

思科錯誤ID [CSCwk70785](#)

AP-COS未更新PMTU探測器的MTU值，導致斷開連線。

已在思科錯誤ID [CSCwk90660](#) - APSP6 17.9.5]中修復，目標為17.9.6、17.12.5、17.15.2、17.16。

問題五：

思科錯誤ID [CSCvw53456](#)

9800靜態CAPWAP路徑MTU配置 (與AireOS奇偶校驗)。

這允許9800在每個AP加入設定檔上設定靜態CAPWAP路徑MTU。 進入17.17。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。