CAPWAP AP PMTUディスカバリについて

内容

はじめに

このドキュメントでは、IOS® XEおよびCOSでのCAPWAPアクセスポイントパス最大伝送ユニット(PMTU)の検出メカニズム、問題、および解決策について説明します。

シナリオと範囲

リモートサイトのCAPWAPアクセスポイント(AP)がWAN経由でワイヤレスLANコントローラ(WLC)に登録する場合は通常、PMTUの問題が発生します。特に、パスにVPN、GRE、または標準の1500バイトよりも低いMTUを持つネットワークセグメントが含まれている場合に、問題が発生します。

また、Extensible Authentication Protocol(EAP)Transport Layer Security(EAP-TLS)による認証についても説明します。 EAP-TLSは大きな証明書を交換するため、パスMTUを減らすとフラグメンテーションリスクが増大します。

すべてのログは、コードバージョン17.9.3でキャプチャされました。出力は、関連する行だけを表示するように切り捨てられます。

CAPWAP制御とデータ（ネゴシエートされる内容）

CAPWAP制御：
制御チャネルは、加入要求、設定交換、キープアライブ信号などの重要な管理メッセージを処理します。これらのメッセージはDTLSを使用して保護され、コントロールプレーン通信の信頼性と効率性を確保するためのパスMTU(PMTU)ネゴシエーションプロセスの主な焦点となります。

CAPWAPデータ：
このチャネルはカプセル化されたクライアントトラフィックを伝送し、通常はほとんどの導入でDTLSによって保護されます。PMTUネゴシエーションがコントロールチャネルで発生している間、結果のPMTU値によって間接的にデータプレーンカプセル化の最大パケットサイズが決定され、クライアントのデータ伝送の信頼性とフラグメンテーションに影響を与えます。

例

- 制御パケット：接続要求と応答、設定の更新、およびエコー/キープアライブメッセージ。
- データパケット：アクセスポイント(AP)とワイヤレスLANコントローラ(WLC)の間で送信されるカプセル化されたクライアントフレーム。

事実：最大サイズのCAPWAPパケット

IOS AP（例）

送信されるPMTUパケットサイズ：1499バイト=イーサネット+ CAPWAP PMTU

- イーサネット= 14バイト
- CAPWAP PMTU = 1485バイト
    - 外部IP = 20バイト
    - UDP = 25バイト
    - DTLS = 1440バイト

AP-COS（例）

送信されるPMTUパケットサイズ：1483バイト=イーサネット+ CAPWAP PMTU

- イーサネット= 14バイト
- CAPWAP PMTU = 1469バイト
    - 外部IP = 20バイト
    - UDP = 25バイト
    - DTLS = 1424バイト

3段階PMTUチェック

両方のプラットフォームは、3つのハードコードされたPMTU値（576、1005、および1485）をプローブします。違いは、各プラットフォームでイーサネットヘッダーがどのようにカウントされるかです。

- IOS APでは、576/1005/1485の値にイーサネットヘッダーが含まれていません。
    - 合計フレーム=イーサネット(14) + PMTU(576/1005/1485) ⇒ 590、1019、1499バイト（配線サイズ）。
- AP-COSでは、イーサネットヘッダーが576/1005/1485の値に含まれています。
    - 合計フレーム= PMTU（すでにイーサネットを含む）。 これらのパケットは、ワイヤ

上ではIOS APの同等のパケットよりも14バイト小さくなります。

CAPWAP PMTUディスカバリメカニズム

IOS APの動作

AP加入フェーズ

CAPWAP加入時に、APはDFビットが設定された1485バイトの最大CAPWAP PMTUをネゴシエートします。応答を5秒間待機します。

- 応答がない場合、またはICMP「Fragmentation Needed」が到達した場合、APは576バイトにフォールバックして迅速に加入を完了し、RUNに到達した後でPMTUを引き上げようとします。

パケットキャプチャ（例）

パケット番号106 1499バイトのプローブ（DFセット）が表示されます。 同じサイズの応答は、パケットがフラグメンテーションなしでパスを通過できなかったことを示します。その後、ICMP「Fragmentation Needed」が表示されます。

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

対応するAPレベルのデバッグ(「debug capwap client path-mtu」)は、APが1485バイトで最初に試行し、応答を5秒間待機したことを示します。応答がない場合は、長さが短い別の接続要求パケットを送信します。これは結合段階のままであり、時間を無駄にしないためです。デバッグログに示されているように、APをWLCに加入させるための最小値に到達します。

```
*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
```

この時点で#show capwap client rcbを実行すると、576バイトのCAPWAP AP MTUが表示されます。

```
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
```

RUN状態フェーズ

APがワイヤレスLANコントローラに正常に加入した後、PMTUディスカバリメカニズムが動作していることがわかります。このメカニズムでは、30秒後に、次に大きいPMTU値のサイズが設定されたDFビットを設定した別のCAPWAPパケットを送信することで、APがより大きいPMTU値のネゴシエーションを開始します。

この例では、APは1005バイト値を試行しています。IOSではPMTUフィールドからイーサネットが除外されるため、回線上に1019バイトが表示されます。WLCが応答すると、APはPMTUを1005バイトに更新します。そうでない場合は、30秒間待機してから再試行します。

次のスクリーンショットは、1005 PMTUのAPネゴシエーションが成功した状態を示しています(パケット#268および#269を参照)。 これらのパケットのサイズは異なることに注意してください。これは、WLCにPMTU計算の異なるアルゴリズムが設定されているためです。

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

ここで、対応するAPレベルのデバッグ(debug capwap client pmtu)により、APが1005バイトのPMTUを正常にネゴシエートし、AP PMTU値を更新した場所が示されます。

```
*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
```

また、この時点で(#show capwap client rcb)を実行すると、1005バイトのCAPWAP AP MTUが表示されます。showの出力を次に示します。

```
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では次に高い値である1485バイトのネゴシエーションが再試行されますが、APステータスがRUN状態の間にAPでICMP unreachableが受信されました。ICMP unreachableにはネクストホップ値があり、APはこの値を承認して、デバッグでわかるように、自身のPMTUの計算に使用します。

```
*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
```

対応するAPレベルのキャプチャ

ICMP unreachableパケット番号281に注目してください。次に、APでは、パケット番号288で1300バイトのICMPネクストホップ値を考慮し、289で応答を考慮したPMTUのネゴシエーションが試行されます。

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

COS APの動作

AP-COS APの検出メカニズムには違いがあります。AP joinから開始します。

AP加入フェーズ

加入時に、APは最大値を設定した加入要求を送信し、5秒間待機します。

応答がない場合は、再試行してさらに5秒間待機します。

それでも応答がない場合は、1005バイトで別の参加要求を送信します。これが成功すると、PMTUが更新され（イメージのダウンロードなど）、処理が続行されます。 1005バイトのDFプローブがコントローラに到達できない場合は、576バイト未満まで低下し、再試行されます。

APレベルでのdebug capwap client pmtuを次に示します。

```
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
```

パケットサイズが1483バイトであることに注目してください。これは、AP-COSで期待されるイーサネットヘッダーのないpmtu値です。パケット番号1168に次のように表示されます。

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

RUN状態フェーズ

APはRUN状態に達した後、30秒ごとにPMTUの改善を試行し続け、DFが設定されたCAPWAPパケットと、次にハードコードされた値を送信します。

APレベルのデバッグ(debug capwap client pmtu)を次に示します

```
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 :: CheckCapwa
Jul 11 19:08:15 kernel: [*07/11/2023 19:08:15.1351] PMTU data: dcb->mtu 1005, pmtu_overhead:1184
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 :: CheckCapwa
Jul 11 19:08:43 kernel: [*07/11/2023 19:08:43.6446] PMTU data: dcb->mtu 1005, pmtu_overhead:1184
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
```

対応するAPキャプチャを次に示します。パケット番号1427と1448を確認してください。

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（アルゴリズムサマリ）

要約すると、アクセスポイントのCAPWAP PMTUDアルゴリズムは次のように動作します。

ステップ 1：最初のCAPWAP PMTUは、AP加入フェーズでネゴシエートされます。

ステップ2:30秒後、APは次の事前定義されたより高い値（576、1005、1485バイト）を送信して、現在のCAPWAP PMTUの改善を試みます。

ステップ3（オプション1）：WLCが応答する場合は、現在のCAPWAP PMTUを新しい値に調整し、ステップ2を繰り返します。

ステップ3（オプション2）：応答がない場合は、現在のCAPWAP PMTUを維持して、ステップ2を繰り返します。

ステップ3（オプション3）：応答がなく、ICMP到達不能（タイプ3、コード4）にネクストホップMTUが含まれる場合は、CAPWAP PMTUをその値に調整して、ステップ2を繰り返します。

注：ICMPネクストホップ値が提供されたときに正しいCAPWAP PMTUが使用されるようにするための修正を参照してください。

関連CDET

問題1:

Cisco Bug ID CSCwf52815

AP-COS APが、より高い値のプローブが失敗した場合に、ICMP到達不能ネクストホップ値を承認しない。
修正：8.10.190.0、17.3.8、17.6.6、17.9.5、17.12.2
IOS APはネクストホップ値を承認し、PMTUを更新します。

問題2:

Cisco Bug ID CSCwc05350

非対称MTU(WLC→APはAP→WLCとは異なる)では、ICMPに双方向PMTUの最大値が反映されなかった場合にPMTUフラッピングが発生します。
修正：8.10.181.0、17.3.6、17.6.5、17.9.2、17.10.1
回避策：WLCとAPの間のMTU（ルータ、ファイアウォール、VPNコンセントレータ）を制御するデバイスで、両方向に同じMTUを設定します。

関連するAP側のCisco Bug ID CSCwc05364:COS-APでは、非対称MTUの最大指向性MTUサイズを識別できるようにPMTUメカニズムが改善されています

関連するWLC側のCisco Bug ID CSCwc48316:APが1つのアップストリームと他の2つの異なるMTUを持つことができるように、PMTUの計算を改善します（これに対処する計画がないため、DEによってクローズとマークされています）

問題3:

Cisco Bug ID CSCwf91557

AP-COSは、最大ハードコード値に達した後、PMTUディスカバリを停止します。

17.13.1で修正されています。また、17.3.8、17.6.6、17.9.5、17.12.2のCisco Bug ID CSCwf52815でも修正されています。

問題4:

Cisco Bug ID CSCwk70785

AP-COSがPMTUプローブのMTU値を更新しないため、切断が発生します。

Cisco Bug ID CSCwk90660 - APSP6 17.9.5]ターゲット17.9.6、17.12.5、17.15.2、17.16で修正されています。

問題5:

Cisco Bug ID CSCvv53456

9800スタティックCAPWAPパスMTU設定（AireOSとパリティ）。

これにより、AP加入プロファイルごとに9800にスタティックCAPWAPパスMTUを設定できます。 17.17に進みます

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。