

CAPWAP AP PMTU Discovery begrijpen

Inhoud

[Inleiding](#)

[Scenario en scope](#)

[CAPWAP Control vs. Data \(waarover wordt onderhandeld\)](#)

[Feiten: maximaal formaat CAPWAP-pakket](#)

[Driefasige PMTU-controles](#)

[CAPWAP PMTU Discovery Mechanism](#)

[IOS AP-gedrag](#)

[Fase AP-verbinding](#)

[RUN-toestandsfase](#)

[COSAP-gedrag](#)

[Fase AP-verbinding](#)

[RUN-toestandsfase](#)

[Conclusie \(algoritme samenvatting\)](#)

[Gerelateerde CDET's](#)

Inleiding

In dit document wordt het detectiemechanisme voor het CAPWAP Access Point Path Maximum Transmission Unit (PMTU) beschreven voor IOS® XE en COS, problemen en oplossingen.

Scenario en scope

PMTU-problemen worden meestal gezien wanneer een CAPWAP-toegangspunt (AP) op een externe locatie zich registreert bij een draadloze LAN-controller (WLC) via een WAN, vooral wanneer het pad VPN, GRE of een netwerksegment met een MTU lager dan de standaard 1500 bytes omvat.

We onderzoeken ook verificatie met Extensible Authentication Protocol Transport Layer Security (EAP-TLS). Omdat EAP-TLS grote certificaten uitwisselt, verhoogt een gereduceerd MTU-pad het risico op fragmentatie.

Alle logs zijn vastgelegd op codeversie 17.9.3. Uitgangen worden afgekapt om alleen relevante lijnen weer te geven.

CAPWAP Control vs. Data (waarover wordt onderhandeld)

CAPWAP-besturing:

Het controlekanaal behandelt kritieke beheerberichten zoals join-verzoeken, configuratieuitwisselingen en bewaar levende signalen. Deze berichten worden beveiligd met behulp van DTLS en zijn de primaire focus van het Path MTU (PMTU) onderhandelingsproces om

betrouwbare en efficiënte controle vliegtuig communicatie te garanderen.

CAPWAP-gegevens:

Dit kanaal draagt ingekapseld clientverkeer, meestal ook beschermd door DTLS in de meeste implementaties. Terwijl PMTU-onderhandeling plaatsvindt op het controlekanaal, bepalen de resulterende PMTU-waarden indirect de maximale pakketgrootte voor de inkapseling van het gegevensvlak, wat de betrouwbaarheid en fragmentatie van de datatransmissie van de client beïnvloedt.

Voorbeelden

- Controlepakketten: voeg verzoeken en antwoorden, configuratie-updates en echo / keepalive-berichten toe.
- Gegevenspakketten: ingekapselde clientframes die worden verzonden tussen het toegangspunt (AP) en de draadloze LAN-controller (WLC).

Feiten: maximaal formaat CAPWAP-pakket

IOS AP (voorbeeld)

Verzonden PMTU-pakketgrootte: 1499 bytes = Ethernet + CAPWAP PMTU

- Ethernet = 14 bytes
- CAPWAP PMTU = 1485 bytes
 - Externe IP = 20 bytes
 - UDP = 25 bytes
 - DTLS = 1440 bytes

AP-COS (voorbeeld)

Verzonden PMTU-pakketgrootte: 1483 bytes = Ethernet + CAPWAP PMTU

- Ethernet = 14 bytes
- CAPWAP PMTU = 1469 bytes
 - Buitenste IP = 20 bytes
 - UDP = 25 bytes
 - DTLS = 1424 bytes

Driefasige PMTU-controles

Beide platforms testen drie hardgecodeerde PMTU-waarden: 576, 1005 en 1485. Het verschil is hoe elk platform de Ethernet-header telt:

- IOS-toegangspunten bevatten de Ethernet-header niet in de 576/1005/1485-waarden.
 - Totaal frame = Ethernet (14) + PMTU (576/1005/1485) $\Rightarrow$ 590, 1019, 1499 bytes (draadgrootte).

- AP-COS bevat de Ethernet-header wel in de waarden 576/1005/1485.
 - Totaal frame = PMTU (bevat al Ethernet). Deze pakketten zijn 14 bytes kleiner op de draad dan IOS AP-equivalenten.

CAPWAP PMTU Discovery Mechanism

IOS AP-gedrag

Fase AP-verbinding

Tijdens de CAPWAP-join onderhandelt het toegangspunt over een maximale CAPWAP PMTU van 1485 bytes met de DF-bitset. 5 seconden wachten op een reactie.

- Als er geen reactie of een ICMP "Fragmentatie nodig" arriveert, daalt het toegangspunt terug naar 576 bytes om snel te voltooien en probeert het vervolgens PMTU te verhogen nadat het RUN heeft bereikt.

Packet capture (voorbeeld)

Pakketnummer 106 U ziet een 1499-byte sonde (DF-set). Geen respons van dezelfde grootte geeft aan dat het pakket het pad niet kon doorkruisen zonder fragmentatie. U ziet dan ICMP "Fragmentatie nodig."

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	58.00751	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

Het bijbehorende foutopsporingsniveau op AP-niveau ("debug capwap client path-mtu") laat zien dat het toegangspunt het eerst probeerde met 1485 bytes en 5 seconden wachtte op een reactie. Als er geen reactie is, stuurt het een ander pakket met een kleinere lengte, omdat dit nog steeds in de join-fase zit en we geen tijd hebben om te verspillen. Het gaat naar de minimumwaarde om het toegangspunt te laten deelnemen aan de WLC, zoals aangegeven in het debug-log:

```
*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 successfully 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
```

En als je op dit moment `#show capwap client rcb` draait, zie je dat de CAPWAP AP MTU op 576 bytes staat:

```
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-toestandsfase

Nadat het toegangspunt zich met succes heeft aangesloten bij de draadloze LAN-controller, ziet u het PMTU Discovery Mechanism in het spel, waar u na 30 seconden kunt zien dat het toegangspunt begint te onderhandelen over een hogere PMTU-waarde door een ander CAPWAP-pakket te verzenden met een DF-bitset van die grootte van de volgende hoogste PMTU-waarde.

In dit voorbeeld heeft de AP de waarde 1005 bytes geprobeerd. Omdat IOS het Ethernet uitsluit van het PMTU-veld, ziet u 1019 bytes op de draad. Als de WLC reageert, wordt de PMTU bijgewerkt naar 1005 bytes. Als dat niet het geval is, wacht 30 seconden en probeert het opnieuw.

Deze screenshot toont een succesvolle AP-onderhandeling van 1005 PMTU (zie pakketten # 268 en # 269). Merk op dat deze pakketten verschillende groottes hebben, wat te wijten is aan het feit dat de WLC een ander algoritme heeft voor PMTU-berekening.

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

Hier toont het bijbehorende foutopsporingsniveau op AP-niveau (`debug capwap client pmtu`) waar de AP met succes de 1005 bytes PMTU heeft onderhandeld en de AP PMTU-waarde heeft bijgewerkt.

```
*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
```

En als je dat doet (#show capwap client rcb) op dit moment vind je dat de CAPWAP AP MTU op 1005 bytes, Hier is de show output:

```
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
```

Na 30 seconden probeert het toegangspunt opnieuw te onderhandelen over de volgende hogere waarde van 1485 bytes, maar het toegangspunt heeft ICMP onbereikbaar ontvangen terwijl de status van het toegangspunt is ingeschakeld. De ICMP onbereikbaar heeft een volgende hop waarde, en de AP eert deze waarde en gebruikt het om zijn eigen PMTU berekenen zoals we kunnen zien in de debugs.

```
*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
```

Het corresponderende AP-niveau vangt op

Let op het onbereikbare ICMP-pakketnummer 281 en vervolgens probeert de AP een PMTU te onderhandelen met het eren van de volgende ICMP-hopwaarde op 1300 bytes op pakketnummer 288 en respons op 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

COSAP-gedrag

Er zijn verschillen in het ontdekkingsmechanisme voor AP-COS AP's. We beginnen bij AP join.

Fase AP-verbinding

Bij join verzendt het toegangspunt een join-verzoek met de maximale waarde en wacht het vijf

seconden.

Als er geen reactie is, probeert het opnieuw en wacht het nog eens vijf seconden.

Als er nog steeds geen reactie is, stuurt het een ander Join Request met 1005 bytes. Als dat lukt, wordt PMTU bijgewerkt en gaat het verder (bijvoorbeeld het downloaden van afbeeldingen). Als de 1005-byte DF-sonde de controller nog steeds niet kan bereiken, zakt deze naar het minimum van 576 en probeert het opnieuw.

Hier is de debug capwap client pmtu op het AP-niveau:

```
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
```

Merk op dat de pakketgrootte 1483 bytes is, wat de pmtu-waarde is zonder de ethernetheader zoals verwacht voor AP-COS. U ziet dit op pakketnummer 1168 hier:

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 fragment overlay]
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 overlay]
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 overlay]
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 overlay]
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 overlay]
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 fragment overlay]
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 overlay]
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 overlay]
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 overlay]
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-toestandfase

Nadat het toegangspunt de status RUN heeft bereikt, probeert het elke 30 seconden de PMTU te verbeteren door

CAPWAP-pakketten met DF-set en de volgende harde gecodeerde waarde te verzenden.

Hier is de AP-niveau 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 1
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 I
..
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 1
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 I
```

Hier zijn de bijbehorende AP-opnames. kijk naar pakketnummer 1427 en 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

Conclusie (algoritme samenvatting)

Samengevat werkt het CAPWAP PMTUD-algoritme op Access Points als volgt.

Stap 1. De initiële CAPWAP PMTU wordt onderhandeld tijdens de AP join-fase.

Stap 2. 30 seconden later probeert het toegangspunt de huidige CAPWAP PMTU te verbeteren door de volgende vooraf gedefinieerde hogere waarde (576, 1005, 1485 bytes) te verzenden.

Stap 3 (optie 1). Als de WLC reageert, past u de huidige CAPWAP PMTU aan op de nieuwe waarde en herhaalt u stap 2.

Stap 3 (optie 2). Als er geen reactie is, houdt u de huidige CAPWAP PMTU en herhaalt u stap 2.

Stap 3 (optie 3). Als er geen respons is en een ICMP Unreach (Type 3, Code 4) een next-hop MTU bevat, past u de CAPWAP PMTU aan die waarde aan en herhaalt u stap 2.

OPMERKING: Zie de oplossingen om ervoor te zorgen dat de juiste CAPWAP PMTU wordt gebruikt wanneer een ICMP-waarde voor de volgende hop wordt opgegeven.

Gerelateerde CDET's

Afgiftenummer 1:

Cisco bug ID [CSCwf52815](#)

AP-COS AP's voldoen niet aan de waarde van ICMP Unreach next-hop wanneer sondes met een hogere waarde mislukken.

Oplossingen: 8.10.190.0, 17.3.8, 17.6.6, 17.9.5, 17.12.2.

IOS AP's eren de next-hop-waarde en updaten PMTU.

Afgiftenummer 2:

Cisco bug ID [CSCwc05350](#)

Asymmetrische MTU (WLC→AP verschilt van AP→WLC) leidde tot PMTU-flapperen wanneer ICMP de maximale bidirectionele PMTU niet weergaf.

Oplossingen: 8.10.181.0, 17.3.6, 17.6.5, 17.9.2, 17.10.1.

Oplossing: configureer dezelfde MTU in beide richtingen op apparaten die MTU (router, firewall, VPN-concentrator) tussen WLC en AP regelen.

Gerelateerde AP Side Cisco bug ID [CSCwc05364](#): COS-AP verbeteren PMTU mechanisme om te kunnen identificeren van de maximale directionele MTU grootte voor asymmetrische MTUs

Gerelateerde WLC-kant Cisco bug ID [CSCwc48316](#): verbeter PMTU-berekeningen voor AP om twee verschillende MTU's te kunnen hebben, de ene upstream en de andere (gemarkeerd als gesloten door DE omdat ze geen plannen hebben om dit aan te pakken)

Nummer van uitgifte 3:

Cisco bug ID [CSCwf91557](#)

AP-COS stopt PMTU-detectie na het bereiken van de maximale hardcodewaarde.

Fixed in 17.13.1; ook via Fixed via Cisco bug ID [CSCwf52815](#) in 17.3.8, 17.6.6, 17.9.5, 17.12.2.

Afgiftenummer 4:

Cisco bug ID [CSCwk70785](#)

AP-COS werkt de MTU-waarde voor de PMTU-sonde niet bij, waardoor verbindingen worden verbroken.

opgelost in Cisco bug ID [CSCwk90660](#) - APSP6 17.9.5] Target 17.9.6, 17.12.5, 17.15.2, 17.16.

Afgiftenummer 5:

Cisco bug ID [CSCvv53456](#)

9800 Statische configuratie van CAPWAP Path MTU (pariteit met AireOS).

Hierdoor kan voor de 9800 een statische MTU voor het CAPWAP-pad worden geconfigureerd op basis van het profiel voor een verbinding per toegangspunt. Op naar 17.17.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.