CAPWAP AP PMTU 검색 이해

목차

소개

이 문서에서는 IOS® XE 및 COS의 CAPWAP PMTU(Access Point Path Maximum Transmission Unit) 검색 메커니즘, 문제 및 해결에 대해 설명합니다.

시나리오 및 범위

일반적으로 원격 사이트의 CAPWAP 액세스 포인트(AP)가 WAN을 통해 WLC(Wireless LAN Controller)에 등록할 때, 특히 경로에 표준 1500바이트보다 낮은 MTU를 갖는 VPN, GRE 또는 네트워크 세그먼트가 포함되어 있는 경우 PMTU 문제가 발생합니다.

또한 EAP-TLS(Extensible Authentication Protocol Transport Layer Security)를 사용한 인증도 검사합니다. EAP-TLS는 대형 인증서를 교환하므로 경로 MTU가 감소하면 프래그먼트화 위험이 증가합니다.

모든 로그는 코드 버전 17.9.3에서 캡처되었습니다. 관련 행만 표시하도록 출력이 잘립니다.

CAPWAP 제어 및 데이터(협상 내용)

CAPWAP 컨트롤:
제어 채널은 조인 요청, 컨피그레이션 교환 및 keepalive 신호와 같은 중요한 관리 메시지를 처리합니다. 이러한 메시지는 DTLS를 사용하여 보호되며 PMTU(Path MTU) 협상 프로세스에서 신뢰성과 효율적인 컨트롤 플레인 통신을 보장하는 데 주로 사용됩니다.

CAPWAP 데이터:

이 채널은 캡슐화된 클라이언트 트래픽을 전달하며, 대개 대부분의 구축에서 DTLS에 의해 보호됩니다. PMTU 협상이 제어 채널에서 발생하는 동안, 결과 PMTU 값은 간접적으로 데이터 평면 캡슐화를 위한 최대 패킷 크기를 결정하며, 클라이언트 데이터 전송 신뢰성 및 단편화에 영향을 줍니다.

예

- 제어 패킷: 요청 및 응답, 컨피그레이션 업데이트, 에코/킵얼라이브 메시지 가입
- 데이터 패킷: AP(액세스 포인트)와 WLC(무선 LAN 컨트롤러) 간에 전송되는 캡슐화된 클라이언트 프레임.

사실: 최대 크기 CAPWAP 패킷

IOS AP(예)

보낸 PMTU 패킷 크기: 1499바이트 = 이더넷 + CAPWAP PMTU

- 이더넷 = 14바이트
- CAPWAP PMTU = 1485바이트
    - 외부 IP = 20바이트
    - UDP = 25바이트
    - DTLS = 1440바이트

AP-COS(예)

보낸 PMTU 패킷 크기: 1483바이트 = 이더넷 + CAPWAP PMTU

- 이더넷 = 14바이트
- CAPWAP PMTU = 1469바이트
    - 외부 IP = 20바이트
    - UDP = 25바이트
    - DTLS = 1424바이트

3단계 PMTU 확인

두 플랫폼 모두 3개의 하드 코딩된 PMTU 값을 프로브합니다. 576, 1005 및 1485입니다. 차이점은 각 플랫폼이 이더넷 헤더를 계산하는 방법입니다.

- IOS AP는 576/1005/1485 값에 이더넷 헤더를 포함하지 않습니다.
    - 총 프레임 = 이더넷(14) + PMTU(576/1005/1485) ⇒ 590, 1019, 1499바이트(와이어 크기)
- AP-COS는 576/1005/1485 값에 이더넷 헤더를 포함하지 않습니다.
    - 총 프레임 = PMTU(이더넷이 이미 포함됨). 이러한 패킷은 IOS AP에 해당하는 패킷보다 유선에서 14바이트 더 작습니다.

CAPWAP PMTU 검색 메커니즘

IOS AP 동작

AP 조인 단계

CAPWAP 조인 중에 AP는 DF 비트가 설정된 최대 CAPWAP PMTU를 1485바이트로 협상합니다. 응답을 5초 기다립니다.

- 응답이 없거나 ICMP "Fragmentation Needed"가 도착하면 AP가 576바이트로 되돌아가 조인을 빠르게 완료한 다음 RUN에 도달하면 PMTU를 올리려고 시도합니다.

패킷 캡처(예)

패킷 번호 106 1499바이트 프로브(DF 집합)가 표시됩니다. No same-size response - 패킷이 단편화 없이 경로를 통과할 수 없음을 나타냅니다. 그런 다음 ICMP "Fragmentation Needed"가 표시됩니다.

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

해당 AP 레벨 Debug("debug capwap client path-mtu")는 AP가 1485바이트로 먼저 시도하고 응답을 5초 기다렸다는 것을 보여줍니다. 응답이 없을 경우, 더 작은 길이의 다른 가입 요청 패킷을 보냅니다. 아직 가입 단계에 있기 때문에 시간을 낭비할 필요가 없습니다. 디버그 로그에 표시된 대로 AP가 WLC에 조인하도록 하려면 최소값으로 이동합니다.

```
*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
```

이 시점에서 capwap 클라이언트 rcb#show 실행하면 CAPWAP AP MTU가 576바이트에 있음을 알 수 있습니다.

```
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
```

실행 상태 단계

AP가 성공적으로 무선 LAN 컨트롤러에 조인하면 30초 후에 AP가 다음으로 높은 PMTU 값의 크기의 DF 비트가 설정된 다른 CAPWAP 패킷을 전송하여 더 높은 PMTU 값을 협상하기 시작하는 PMTU 검색 메커니즘이 표시됩니다.

이 예에서 AP는 1005바이트 값을 시도했습니다. IOS에서는 이더넷을 PMTU 필드에서 제외하므로 와이어에 1019바이트가 표시됩니다. WLC가 응답하면 AP는 PMTU를 1005바이트로 업데이트합니다. 그렇지 않은 경우 30초를 기다린 후 다시 시도합니다.

이 스크린샷은 1005 PMTU의 성공적인 AP 협상을 보여줍니다(패킷 #268 및 #269 참조). 이러한 패킷의 크기는 서로 다르며, 이는 WLC가 PMTU 계산에 대해 서로 다른 알고리즘을 사용하기 때문입니다.

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

여기서 해당 AP 레벨 Debug(debug capwap client pmtu)는 AP가 성공적으로 1005바이트 PMTU를 협상하고 AP PMTU 값을 업데이트한 위치를 보여줍니다.

```
*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
```

이 순간에 CAPWAP 클라이언트 rcb를 #show CAPWAP AP MTU가 1005바이트에 있음을 알게 되면 show 출력입니다.

```
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
```

30초 후 AP는 1485바이트의 다음으로 높은 값을 협상하려고 다시 시도하지만, AP 상태가 RUN(실행) 상태인 동안 AP가 ICMP에 연결할 수 없는 ICMP를 수신했습니다. ICMP unreachable은 다음 홉 값을 가지며, AP는 이 값을 적용하고 디버그에서 볼 수 있는 것처럼 자체 PMTU를 계산하는 데 사용합니다.

```
*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
```

해당 AP 레벨 캡처

ICMP unreachable 패킷 번호 281을 확인한 다음 AP가 ICMP next hop 값을 1300바이트로 지정하고 응답을 289로 지정하여 PMTU를 협상합니다.

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 동작

AP-COS AP에 대한 검색 메커니즘에는 차이가 있습니다. 우리는 AP 가입에서 시작합니다.

AP 조인 단계

가입 시 AP는 최대값으로 가입 요청을 전송하고 5초를 기다립니다.

응답이 없으면 다시 시도하여 5초 더 기다립니다.

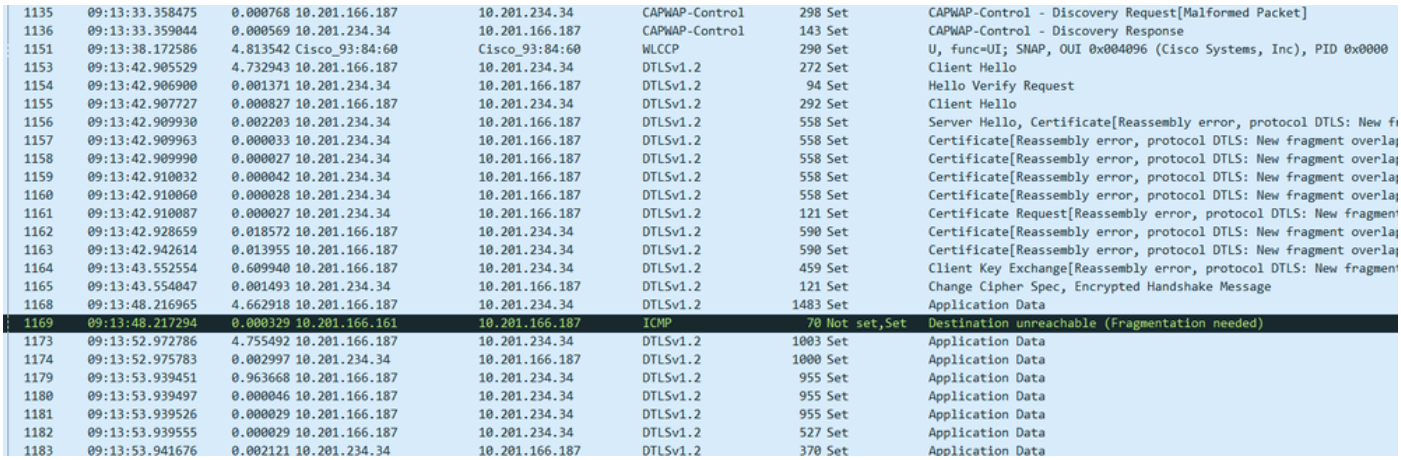
여전히 응답이 없는 경우 1005바이트의 또 다른 가입 요청을 보냅니다. 이 작업이 성공하면 PMTU가 업데이트되고 이미지 다운로드가 진행됩니다. 1005바이트 DF 프로브가 여전히 컨트롤러에 도달할 수 없는 경우 최소 576으로 드롭하고 재시도합니다.

다음은 AP 레벨의 디버그 capwap 클라이언트 pmtu입니다.

```
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
```

패킷 크기는 AP-COS에 대해 예상한 대로 이더넷 헤더가 없는 pmtu 값인 1483바이트입니다. 패킷 번호 1168에 표시되는 내용은 다음과 같습니다.



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

실행 상태 단계

AP가 RUN 상태에 도달한 후. 30초마다 PMTU를 개선하려고 계속 시도하면서 DF 세트와 다음 하드 코딩된 값이 포함된 CAPWAP 패킷을 전송합니다.

AP 레벨 디버그(debug capwap client pmtu)입니다

```
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: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
```

다음은 해당 AP 캡처입니다. 패킷 번호 1427 및 1448을 확인합니다.

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

결론(알고리즘 요약)

요약하면, 액세스 포인트의 CAPWAP PMTUD 알고리즘은 이와 같이 작동합니다.

1단계. 초기 CAPWAP PMTU는 AP 조인 단계 중에 협상됩니다.

2단계. 30초 후에 AP는 다음으로 미리 정의된 더 높은 값(576, 1005, 1485바이트)을 전송하여 현재 CAPWAP PMTU를 개선하려고 시도합니다.

3단계(옵션 1). WLC가 응답하면 현재 CAPWAP PMTU를 새 값으로 조정하고 2단계를 반복합니다.

3단계(옵션 2). 응답이 없으면 현재 CAPWAP PMTU를 유지하고 2단계를 반복합니다.

3단계(옵션 3). 응답이 없고 ICMP Unreachable(Type 3, Code 4)에 next-hop MTU가 포함된 경우 CAPWAP PMTU를 해당 값으로 조정하고 2단계를 반복합니다.

참고: ICMP next-hop 값이 제공될 때 올바른 CAPWAP PMTU가 사용되는지 확인하려면 수정을 참조하십시오.

관련 CDET

문제 번호 1:

Cisco 버그 ID CSCwf52815

AP-COS AP가 더 높은 값의 프로브가 실패할 경우 ICMP Unreachable next-hop 값을 준수하지 않습니다.
수정: 8.10.190.0, 17.3.8, 17.6.6, 17.9.5, 17.12.2.
IOS AP는 next-hop 값을 적용하고 PMTU를 업데이트합니다.

문제 번호 2:

Cisco 버그 ID CSCwc05350

ICMP가 최대 양방향 PMTU를 반영하지 않을 경우 비대칭 MTU(WLC→AP는 AP→WLC와 다름)가 PMTU 플래핑으로 이어집니다.
수정: 8.10.181.0, 17.3.6, 17.6.5, 17.9.2, 17.10.1.
해결 방법: WLC와 AP 간의 MTU(라우터, 방화벽, VPN Concentrator)를 제어하는 디바이스에서 양방향으로 동일한 MTU를 구성합니다.

관련 AP 측 Cisco 버그 ID CSCwc05364: COS-AP는 PMTU 메커니즘을 개선하여 비대칭 MTU에 대한 최대 방향 MTU 크기를 식별할 수 있습니다.

관련 WLC 측 Cisco 버그 ID CSCwc48316: 하나의 업스트림과 다른 두 개의 서로 다른 MTU를 가질 수 있도록 AP에 대한 PMTU 계산 개선(이를 해결할 계획이 없으므로 DE에서 닫음으로 표시)

문제 번호 3:

Cisco 버그 ID CSCwf91557

AP-COS는 최대 하드 코딩된 값에 도달한 후 PMTU 검색을 중지합니다.

17.13.1에서 수정됨. 17.3.8, 17.6.6, 17.9.5, 17.12.2에서 Cisco 버그 ID CSCwf52815를 통해 수정됨

문제 번호 4:

Cisco 버그 ID CSCwk70785

AP-COS가 PMTU 프로브에 대한 MTU 값을 업데이트하지 않아 연결이 끊어집니다.

fixed in Cisco 버그 ID CSCwk90660 - APSP6 17.9.5] Target 17.9.6, 17.12.5, 17.15.2, 17.16.

문제 번호 5:

Cisco 버그 ID CSCvv53456

9800 고정 CAPWAP 경로 MTU 컨피그레이션(AireOS와 동일).

이를 통해 9800은 AP 가입 프로필 단위로 고정 CAPWAP 경로 MTU를 구성할 수 있습니다. 17.17로 들어갑니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.