
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Diving into AP Path MTU

Sara Elsharayheh, Wireless Technical Leader
Benedict Jojo Arthur, Wireless Technical Consulting Engineer

TACENT-2009

Agenda

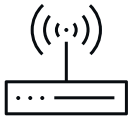
- Facts
- PMTU Discovery Mechanism
- EAP Authentication
- Client TCP MSS
- Q&A

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

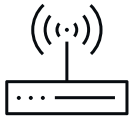
FACTs

A wireless client sends a packet with 1500 Bytes (IP MTU)

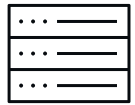
= 1524 Bytes



= 1560-1568 Bytes



Access Point



Wireless Controller

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

PMTU Discovery Mechanism

PMTU Discovery Mechanism

- Stands for Path Maximum Transmission Unit
- CAPWAP PMTU discovery initially occurs during the CAPWAP Join State
- The Access Point first negotiates the maximum value:1485 bytes
- Access point hard coded values to negotiate are 576, 1005, and 1485 bytes

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CAPWAP Discovery Mechanism

The AP attempts to negotiate at the maximum CAPWAP PMTU of 1485 bytes using the following equation:

DTLS + Outer IP + UDP = CAPWAP Packet

= 1485

CAPWAP + Ethernet = Total Packet Size

= 1499

Facts
Ethernet = 14 Bytes
Outer IP = 20 Bytes
UDP = 25 Bytes
DTLS = 1440 Bytes

Standard MTU of 1500 Bytes.

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CAPWAP PMTU at AP join

When the WLC sees the AP attempt with DF bit set and a corresponding response is sent back to the AP, this value becomes the initial CAPWAP PMTU.

If the WLC doesn't receive this from the AP, WLC and AP uses the minimum of 576 Bytes instead.

18:39:27.957010	0.018813	10.201.166.180	10.201.166.142	CAPWAP-…	282	Set	CAPWAP-Control - Discovery Request[Malformed Packet]
18:39:27.957231	0.000221	10.201.166.142	10.201.166.180	CAPWAP-…	190	Not set	CAPWAP-Control - Discovery Response
18:39:37.309225	9.351994	10.201.166.180	10.201.166.142	DTLSv1.2	231	Set	Client Hello
18:39:37.309600	0.000375	10.201.166.142	10.201.166.180	DTLSv1.2	106	Set	Hello Verify Request
18:39:37.310383	0.000783	10.201.166.180	10.201.166.142	DTLSv1.2	263	Set	Client Hello
18:39:37.310796	0.000413	10.201.166.142	10.201.166.180	DTLSv1.2	590	Set	Server Hello, Certificate (Fragment)
18:39:37.310823	0.000027	10.201.166.142	10.201.166.180	DTLSv1.2	590	Set	Certificate (Fragment)
18:39:37.310850	0.000027	10.201.166.142	10.201.166.180	DTLSv1.2	431	Set	Certificate (Reassembled), Certificate Request, Server Hello Done
18:39:37.327667	0.016817	10.201.166.180	10.201.166.142	DTLSv1.2	590	Set	Certificate (Fragment)
18:39:37.327715	0.000048	10.201.166.180	10.201.166.142	DTLSv1.2	527	Set	Certificate (Reassembled)
18:39:37.327755	0.000040	10.201.166.180	10.201.166.142	DTLSv1.2	329	Set	Client Key Exchange
18:39:38.004744	0.676989	10.201.166.180	10.201.166.142	DTLSv1.2	331	Set	Certificate Verify
18:39:38.004809	0.000065	10.201.166.180	10.201.166.142	DTLSv1.2	137	Set	Change Cipher Spec, Encrypted Handshake Message
18:39:38.005391	0.000582	10.201.166.142	10.201.166.180	DTLSv1.2	137	Set	Change Cipher Spec, Encrypted Handshake Message
18:39:38.062200	0.056809	10.201.166.180	10.201.166.142	DTLSv1.2	1499	Set	Application Data
18:39:42.628224	4.566024	10.201.166.180	10.201.166.142	DTLSv1.2	507	Set	Application Data
18:39:42.630516	0.002292	10.201.166.142	10.201.166.180	DTLSv1.2	219	Set	Application Data
18:39:42.883289	0.252773	10.201.166.180	10.201.166.142	DTLSv1.2	539	Set	Application Data

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CAPWAP PMTU at AP join Cont.

The corresponding debug seen on the AP (debug capwap client pmtu)

```
[*05/18/2023 03:29:56.7089] wtpEncodePathMTUPayload: Total Packet Size: 1485

[*05/18/2023 03:29:56.7089] wtpEncodePathMTUPayload: Capwap Size is 1376.
[*05/18/2023 03:29:56.7089] [ENC]AP_PATH_MTU_PAYLOAD: pmtu 1485, len 1352, buffer len 1376
[*05/18/2023 03:29:56.7089] capwap_build_and_send_pmtu_packet: packet length = 1485 for current path MTU discovery

[*05/18/2023 03:33:24.6724] Join req: encodeLen = 1368 len = 8.

[*05/18/2023 03:33:24.6724] Sending Join Request Path MTU payload, Length 1376

[*05/18/2023 03:33:24.6724] SingleFragPkt:Len of pkt 1376

[*05/18/2023 03:33:24.6731] pmtu icmp pkt(ICMP_NEED_FRAG) from click received

[*05/18/2023 03:33:29.3176] Join req: encodeLen = 489 len = 8.

[*05/18/2023 03:33:29.3206] Msg Type = CAPWAP_JOIN_RESPONSE(4) Capwap State = Join(5).
[*05/18/2023 03:33:29.3206] Join Response from 10.201.166.142
[*05/18/2023 03:33:29.3206] Join Response: Total msgEleLen = 106.
[*05/18/2023 03:33:29.3206] AC accepted join request with result code: 0
[*05/18/2023 03:33:29.3246] Received wlcType 0, timer 30
```


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CAPWAP PMTU at AP join Cont.

The corresponding show command on the AP

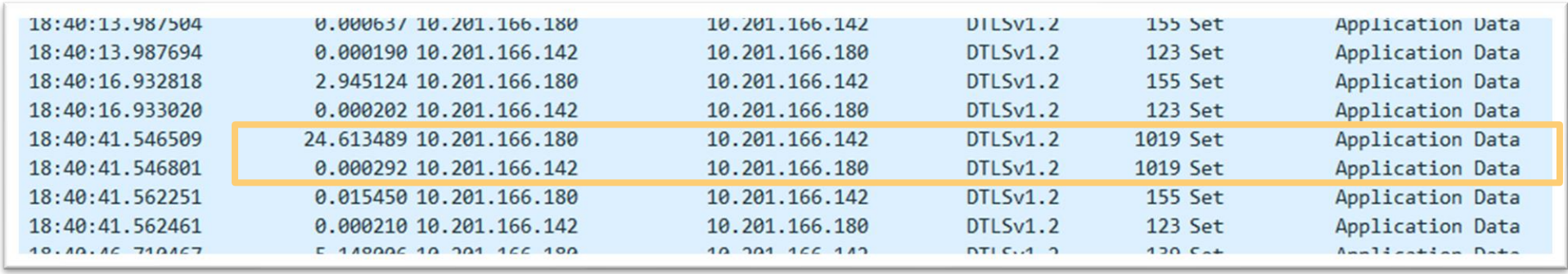
#show capwap client rcb

```
9130AP#show capwap client rcb
AdminState                              : ADMIN_ENABLED
OperationState                          : UP
Name                                    : AP70F0.96C6.4A34
SwVer                                   : 8.10.185.0
HwVer                                   : 1.0.0.0
MwarApMgrIp                             : 10.201.166.142
MwarName                                : 8540-F29-1
MwarHwVer                               : 0.0.0.0
Location                                : default location
ApMode                                  : Local
ApSubMode                               : Not Configured
CAPWAP Path MTU                         : 576
Software Initiated Reload Reason        : Factory Reset
CAPWAP Sliding Window
Active Window Size                      : 0
CAPWAP UDP-Lite                         : Enabled
IP Prefer-mode                          : IPv4
AP Link DTLS Encryption                 : OFF
AP TCP MSS Adjust                       : Enabled
AP TCP MSS size                         : 1250
```


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CAPWAP PMTU After AP join

- During the RUN state, AP attempts to periodically improve the CAPWAP PMTU.
- The AP Sends the next highest CAPWAP PMTU value every 30 seconds with DF bit set.
  - If AP receives response from the WLC, the current value gets adjusted.
  - If it doesn't, AP waits another 30 seconds before repeating the attempt



18:40:13.987504	0.000637	10.201.166.180	10.201.166.142	DTLSv1.2	155 Set	Application Data
18:40:13.987694	0.000190	10.201.166.142	10.201.166.180	DTLSv1.2	123 Set	Application Data
18:40:16.932818	2.945124	10.201.166.180	10.201.166.142	DTLSv1.2	155 Set	Application Data
18:40:16.933020	0.000202	10.201.166.142	10.201.166.180	DTLSv1.2	123 Set	Application Data
18:40:41.546509	24.613489	10.201.166.180	10.201.166.142	DTLSv1.2	1019 Set	Application Data
18:40:41.546801	0.000292	10.201.166.142	10.201.166.180	DTLSv1.2	1019 Set	Application Data
18:40:41.562251	0.015450	10.201.166.180	10.201.166.142	DTLSv1.2	155 Set	Application Data
18:40:41.562461	0.000210	10.201.166.142	10.201.166.180	DTLSv1.2	123 Set	Application Data

Successful CAPWAP PMTU negotiation to 1005 bytes

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CAPWAP PMTU After AP join Cont.

The corresponding debug seen on the AP (debug capwap client pmtu)

```
[*05/18/2023 03:57:31.0420] wtpEncodePathMTUPayload: Total Packet Size: 1005

[*05/18/2023 03:57:31.0420] wtpEncodePathMTUPayload: Capwap Size is 896.
[*05/18/2023 03:57:31.0420] [ENC]AP_PATH_MTU_PAYLOAD: pmtu 1005, len 872, buffer len 896
[*05/18/2023 03:57:31.0420] capwap build and send pmtu packet: packet length = 1005 for current path MTU discovery
[*05/18/2023 03:57:31.0423] Ap Path MTU payload sent, length 888

[*05/18/2023 03:57:31.0423] WTP Event Request: AP Path MTU payload sent to 10.201.166.142, seq num 49

[*05/18/2023 03:57:31.1884] WLC confirms PMTU 1005, updating MTU now.
[*05/18/2023 03:57:31.1884] PMTU: Stopping the pmtu message timeout timer
[*05/18/2023 03:57:31.1884] PMTU: Setting MTU to 1005, it was 576
[*05/18/2023 03:57:31.2148] PMTU: Sending MTU update to WLC..
[*05/18/2023 03:57:31.2148] wtpEncodePathMTUPayload: Total Packet Size: 1005

[*05/18/2023 03:57:31.2148] [ENC]AP_PATH_MTU_PAYLOAD: pmtu 1005, len 5, buffer len 29
[*05/18/2023 03:57:31.2148] capwap_build_and_send_pmtu_packet: packet length = 1005 for current path MTU discovery
[*05/18/2023 03:57:31.2148] Ap Path MTU payload sent, length 21

[*05/18/2023 03:57:31.2148] WTP Event Request: AP Path MTU payload sent to 10.201.166.142, seq num 53
```


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CAPWAP PMTU at AP join Cont.

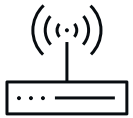
The corresponding show command on the AP

#show capwap client rcb

```
9130AP#show capwap client rcb
AdminState                              : ADMIN_ENABLED
OperationState                          : UP
Name                                    : AP70F0.96C6.4A34
SwVer                                   : 8.10.185.0
HwVer                                   : 1.0.0.0
MwarApMgrIp                             : 10.201.166.142
MwarName                                : 8540-F29-1
MwarHwVer                               : 0.0.0.0
Location                                : default location
ApMode                                  : Local
ApSubMode                               : Not Configured
CAPWAP Path MTU                         : 1005
Software Initiated Reload Reason        : Factory Reset
CAPWAP Sliding Window
Active Window Size                      : 0
CAPWAP UDP-Lite                         : Enabled
IP Prefer-mode                          : IPv4
AP Link DTLS Encryption                 : OFF
AP TCP MSS Adjust                       : Enabled
AP TCP MSS size                         : 1250
```


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

CAPWAP PMTU Conclusion



Access Point

CAPWAP Join **DF set**, PMTU= 1485

If Failed / No Response

CAPWAP Join **DF set**, PMTU = 576

30 seconds later

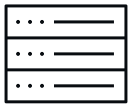
CAPWAP Packet **DF set**, PMTU = 1005

Corresponding CAPWAP Response

30 seconds later

CAPWAP Packet with **DF set**, PMTU = 1485

Corresponding CAPWAP Response



Wireless Controller

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

PMTU knowledge Check

- Standard MTU size for Ethernet 1500 Bytes before ethernet header applies.
- Tunnels like GRE / IPSEC use headers.
- SDWAN IPsec takes between 58-62 Bytes which leave MTU to 1438 /bytes.

What would happen to the CAPWAP traveling in the IPsec Tunnel ? 1005 Bytes

- Static PMTU on AireOS available. C9800 coming soon.
  - WLC>config ap pmtu <ap name | all> disable <new mtu value>

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

EAP Authentication

EAP Authentication Facts

- EAP Certificate size average between 2,200 to 7,500 Bytes
- EAP-TLS is the only EAP type require both sides certificates that's why it is considered the heaviest

EAP Type/ Certificates	Server Side Required	Client Side Required
LEAP	No	No
PEAP	Yes	No
EAP-TLS	Yes	Yes
EAP-Fast	No	No

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

EAP-TLS Certificate Exchange Capturers

13:46:14.856950	2.098002	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	143	Request, Identity
13:46:14.867951	0.011001	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	137	Response, Identity
13:46:14.899947	0.031996	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	96	Request, TLS EAP (EAP-TLS)
13:46:14.933942	0.033995	IntelCor_32:98:ad	Cisco_85:3a:8a	TLSv1.2	270	Client Hello
13:46:14.971949	0.038007	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	1102	Request, TLS EAP (EAP-TLS)
13:46:14.974940	0.002991	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
13:46:15.004989	0.030049	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	1098	Request, TLS EAP (EAP-TLS)
13:46:15.007995	0.003006	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
13:46:15.037992	0.029997	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	1098	Request, TLS EAP (EAP-TLS)
13:46:15.052991	0.014999	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
13:46:15.082988	0.029997	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	1098	Request, TLS EAP (EAP-TLS)
13:46:15.086985	0.003997	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
13:46:15.116983	0.029998	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	1098	Request, TLS EAP (EAP-TLS)
13:46:15.119988	0.003005	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
13:46:15.149986	0.029998	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	1098	Request, TLS EAP (EAP-TLS)
13:46:15.154990	0.005004	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
13:46:15.185979	0.030989	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	1098	Request, TLS EAP (EAP-TLS)
13:46:15.187978	0.001999	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
13:46:15.217975	0.029997	Cisco_85:3a:8a	IntelCor_32:98:ad	TLSv1.2	572	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
13:46:15.542971	0.324996	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	294	Response, TLS EAP (EAP-TLS)
13:46:15.572968	0.029997	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	96	Request, TLS EAP (EAP-TLS)
13:46:15.575958	0.002990	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	294	Response, TLS EAP (EAP-TLS)
13:46:15.605956	0.029998	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	96	Request, TLS EAP (EAP-TLS)
13:46:15.610960	0.005004	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	294	Response, TLS EAP (EAP-TLS)
13:46:15.640958	0.029998	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	96	Request, TLS EAP (EAP-TLS)
13:46:15.643963	0.003005	IntelCor_32:98:ad	Cisco_85:3a:8a	TLSv1.2	969	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
13:46:15.677958	0.033995	Cisco_85:3a:8a	IntelCor_32:98:ad	TLSv1.2	147	Change Cipher Spec, Encrypted Handshake Message
13:46:15.682963	0.005005	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
13:46:15.729957	0.046994	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	94	Success
13:46:15.729957	0.000000	Cisco_85:3a:8a	IntelCor_32:98:ad	EAPOL	207	Key (Message 1 of 4)
13:46:15.747947	0.017990	IntelCor_32:98:ad	Cisco_85:3a:8a	EAPOL	233	Key (Message 2 of 4)
13:46:15.775945	0.027998	Cisco_85:3a:8a	IntelCor_32:98:ad	EAPOL	241	Key (Message 3 of 4)
13:46:15.777959	0.002014	IntelCor_32:98:ad	Cisco_85:3a:8a	EAPOL	193	Key (Message 4 of 4)

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

EAP Exchange Captures

This is the server certificate that got reassembled due to the size.

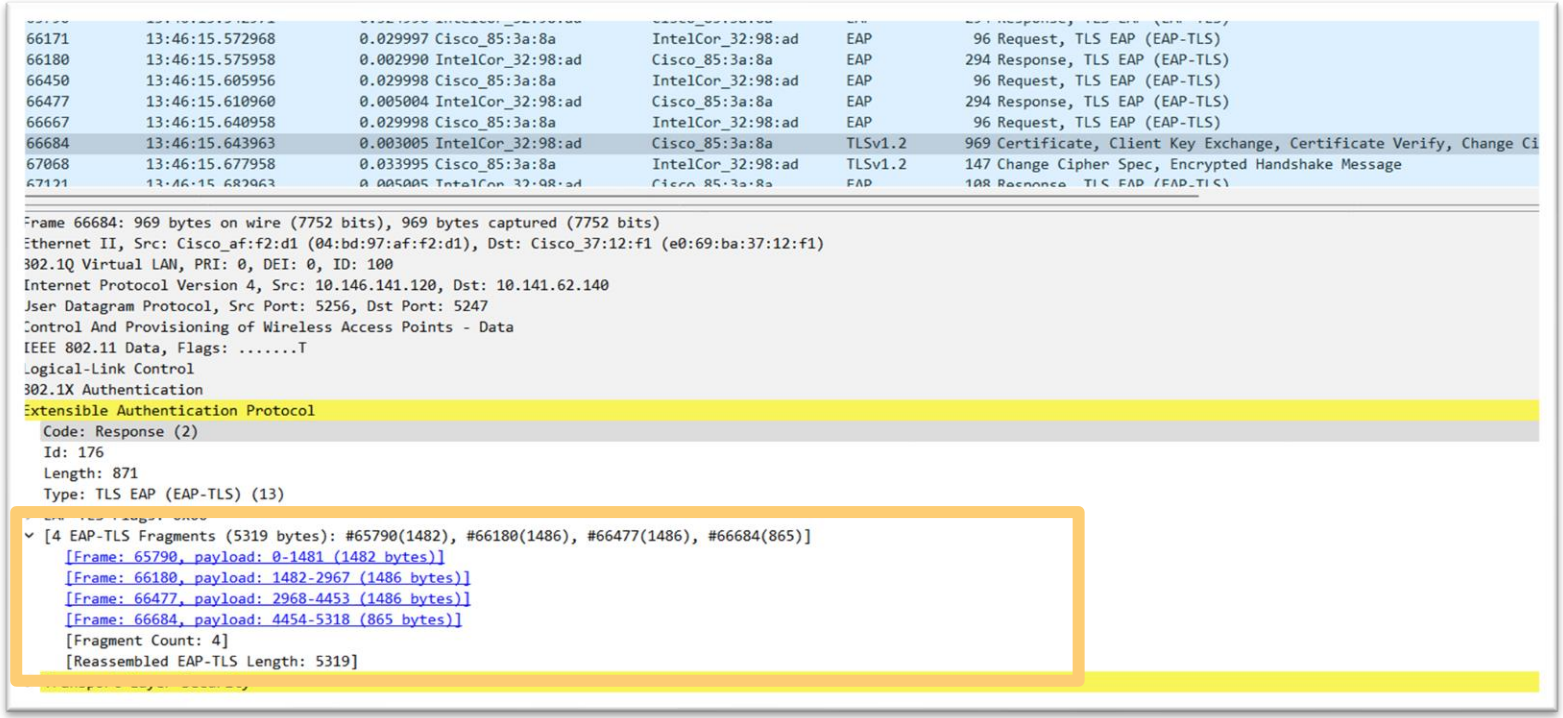
64684	13:46:15.149986	0.029998	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	1098	Request, TLS EAP (EAP-TLS)
64698	13:46:15.154990	0.005004	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
64753	13:46:15.185979	0.030989	Cisco_85:3a:8a	IntelCor_32:98:ad	EAP	1098	Request, TLS EAP (EAP-TLS)
64757	13:46:15.187978	0.001999	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	108	Response, TLS EAP (EAP-TLS)
64794	13:46:15.217975	0.029997	Cisco_85:3a:8a	IntelCor_32:98:ad	TLSv1.2	572	Server Hello, Certificate, Server Key Exchange, Cert
65790	13:46:15.542971	0.324996	IntelCor_32:98:ad	Cisco_85:3a:8a	EAP	294	Response, TLS EAP (EAP-TLS)

```
> Frame 64794: 572 bytes on wire (4576 bits), 572 bytes captured (4576 bits)
> Ethernet II, Src: Cisco_37:12:f1 (e0:69:ba:37:12:f1), Dst: Cisco_af:f2:d1 (04:bd:97:af:f2:d1)
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 100
> Internet Protocol Version 4, Src: 10.141.62.140, Dst: 10.146.141.120
> User Datagram Protocol, Src Port: 5247, Dst Port: 5256
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 Data, Flags: ......F.
> Logical-Link Control
> 802.1X Authentication
v Extensible Authentication Protocol
    Code: Request (1)
    Id: 173
    Length: 482
    Type: TLS EAP (EAP-TLS) (13)
v [8 EAP-TLS Fragments (7490 bytes): #64434(1002), #64502(1002), #64550(1002), #64619(1002), #64656(1002), #64684(1002), #64753(1002), #64794(476)]
      [Frame: 64434, payload: 0-1001 (1002 bytes)]
      [Frame: 64502, payload: 1002-2003 (1002 bytes)]
      [Frame: 64550, payload: 2004-3005 (1002 bytes)]
      [Frame: 64619, payload: 3006-4007 (1002 bytes)]
```


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

EAP Exchange Capturers

This is the client cert reassembled

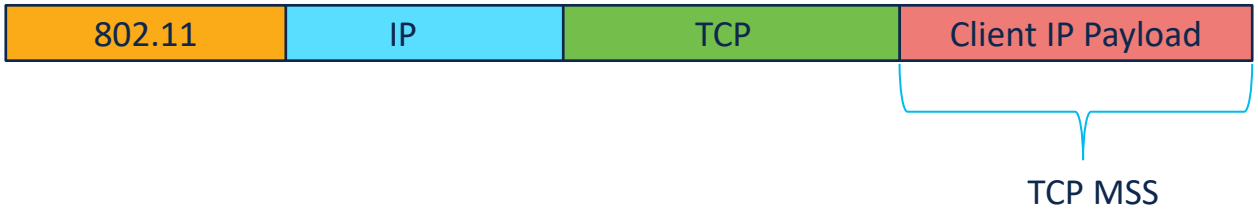


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Client TCP MSS

Client TCP MSS

- Most client connections are TCP-oriented
- TCP MSS options are decided during the 3-way handshake
- Payload of packet refers to TCP MSS

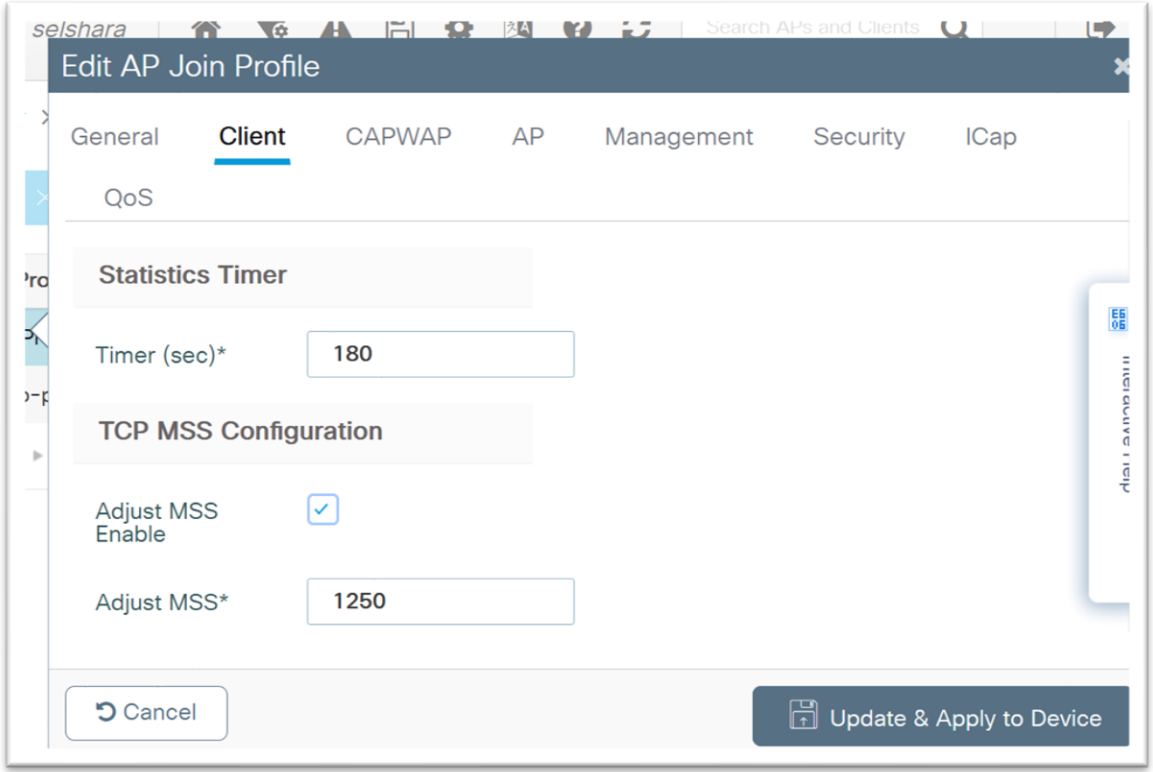


How is it then adjusted ?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

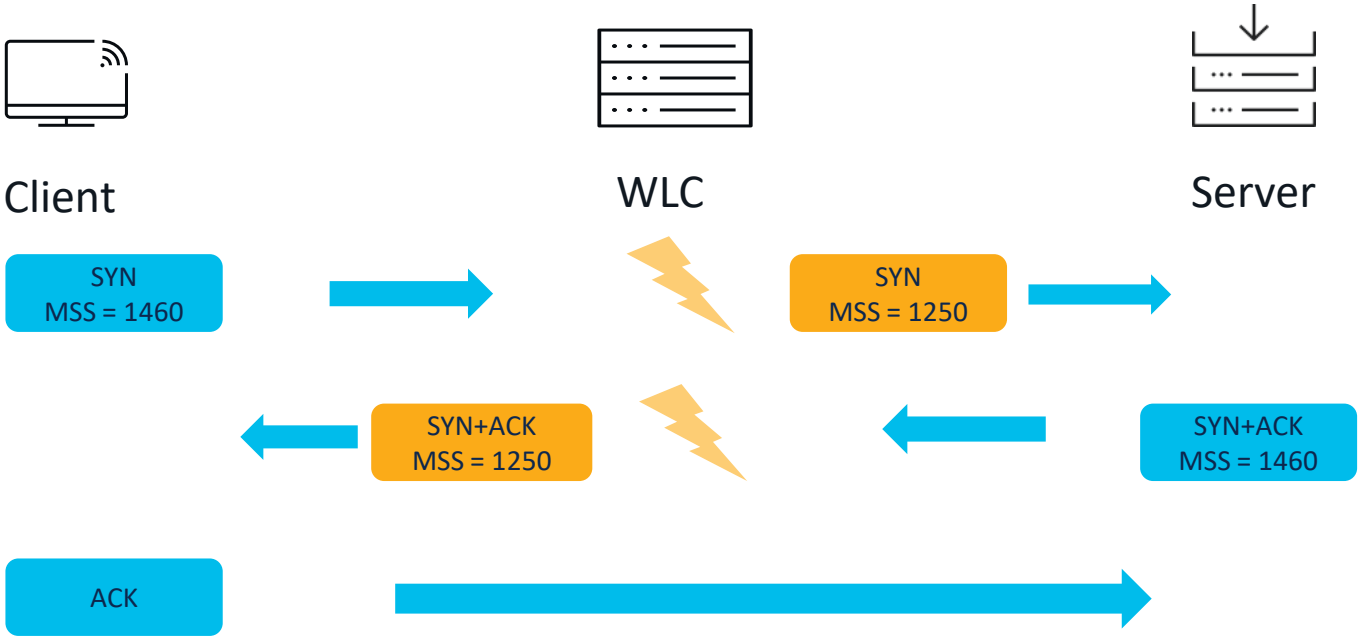
TCP MSS Adjust Feature

- Enabled by default and set to 1250 bytes.
- On 9800, accessed through AP Join profile.



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

TCP 3-way Handshake



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Questions ?

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live-branded socks (while supplies last)!

Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public