# Maximize Your 9800 Wireless Controller Capabilities: Troubleshoot 802.1x and Gain Radius Fragment Control with MTU

Jaydeep Patel
Technical Consulting Engineer

Carlos Socorro
Technical Consulting Engineer
CCIE #66297

June 11, 2025

# AGENDA

01 802.1X & EAP-TLS Overview

02 EAP-TLS Most Common Errors

03 Troubleshoot Fragments and MTU

I. Server-Side Certificate lifecycle

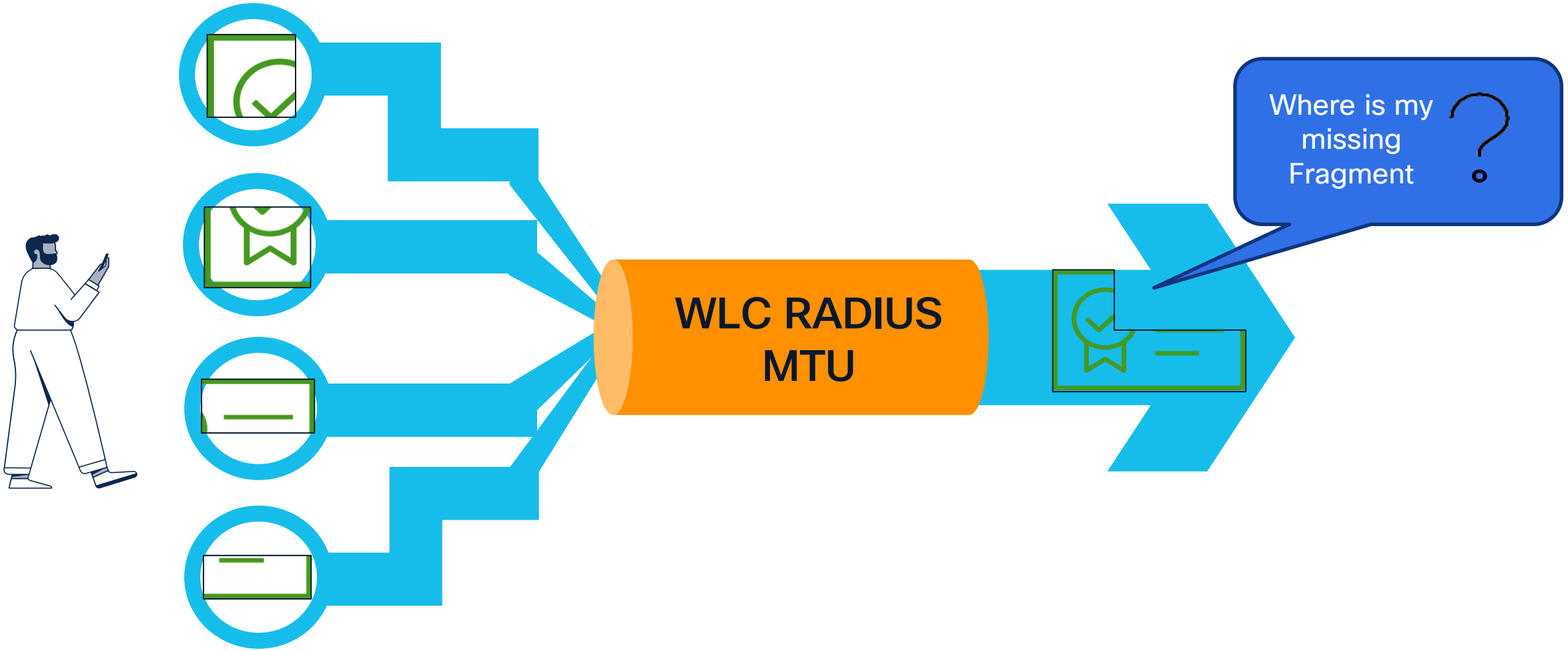
II. Client-Side Certificate lifecycle

04 Utilize RADIUS MTU Feature for Fragment Control

05 RADIUS Jumbo Frames

© 2025 Cisco and/or its affiliates. All rights reserved.

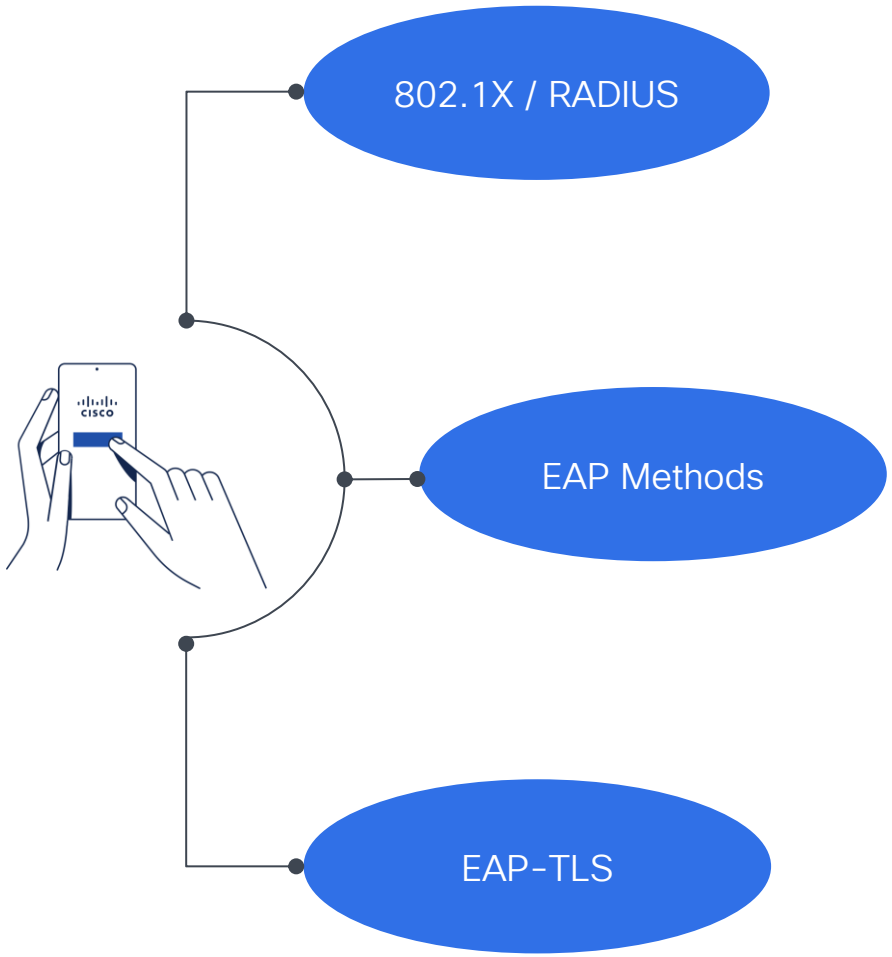
# The Importance of MTU and Fragmentation




© 2025 Cisco and/or its affiliates. All rights reserved.

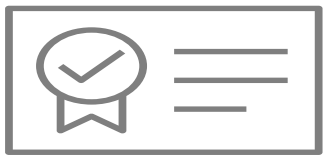
# 802.1X & EAP-TLS Overview

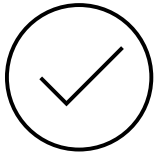
# 802.1X & EAP-TLS Overview





| EAP Method | Server Certificate | Client Certificate |
|---|---|---|
| LEAP | X | X |
| EAP-FAST | X | X |
| PEAP |  | X |
| EAP-TLS |  |  |

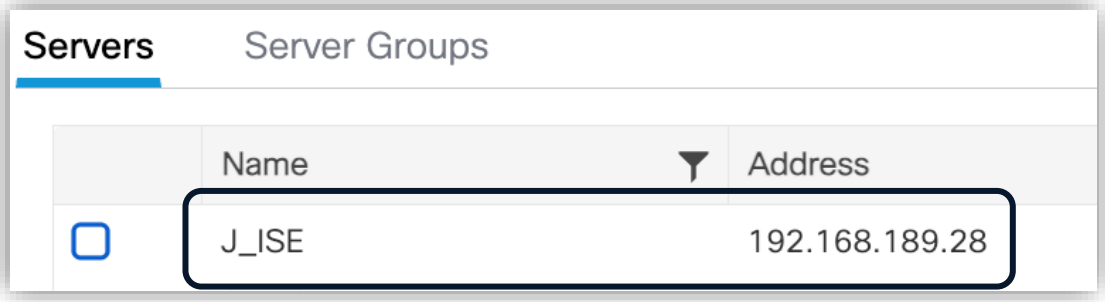





© 2025 Cisco and/or its affiliates. All rights reserved.

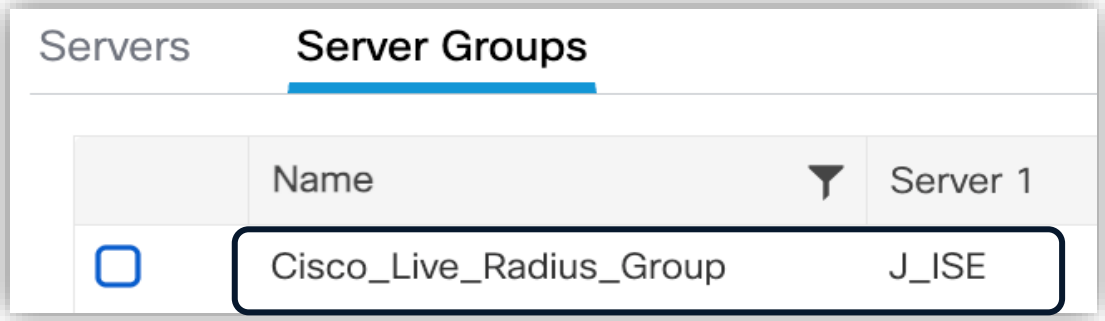
# WLC Configuration Overview

## 1. Configure ISE Server



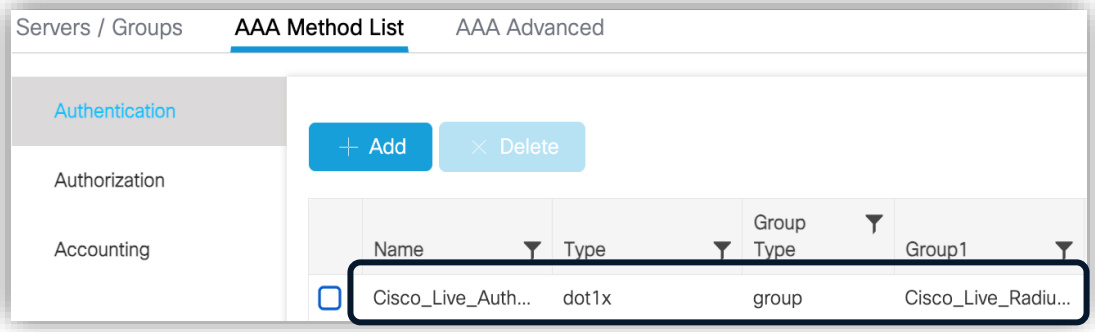

```
!
radius server J_ISE
 address ipv4 192.168.189.28 auth-port 1812 acct-port 1813
 key <secret>
!
```

## 2. Configure Server Group




```
!
aaa group server radius Cisco_Live_Radius_Group
 server name J_ISE
!
```

## 3. Configure Authentication Method List

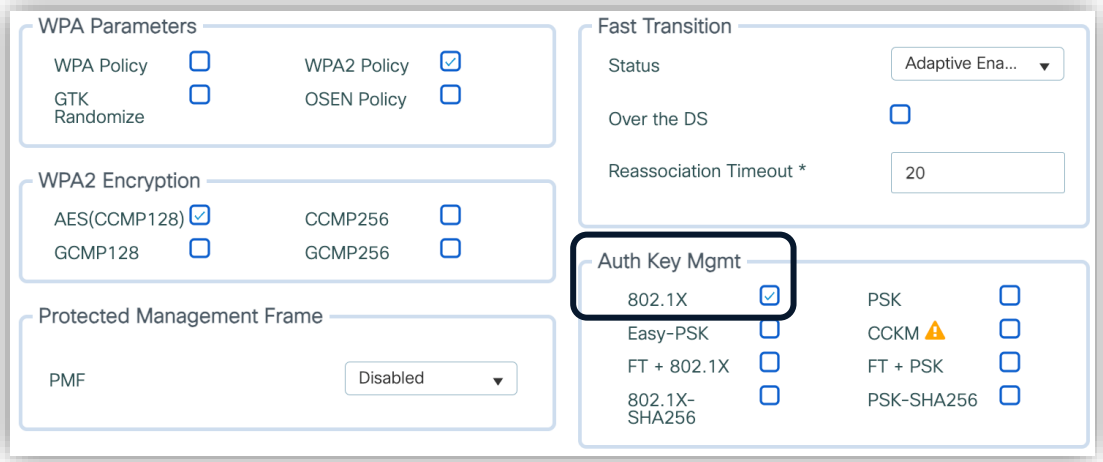



```
!
aaa authentication dot1x Cisco_Live_AuthC group Cisco_Live_Radius_Group
!
```

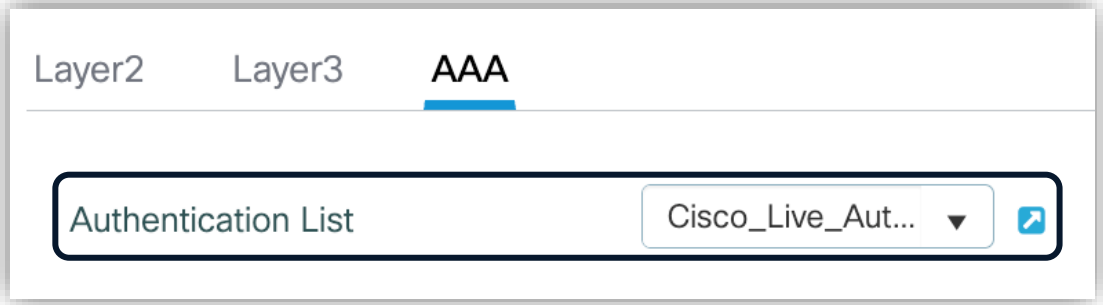
© 2025 Cisco and/or its affiliates. All rights reserved.

# WLC Configuration Overview

## 4. Configure WLAN with 802.1X Authentication




## 5. Map the Authentication Method List

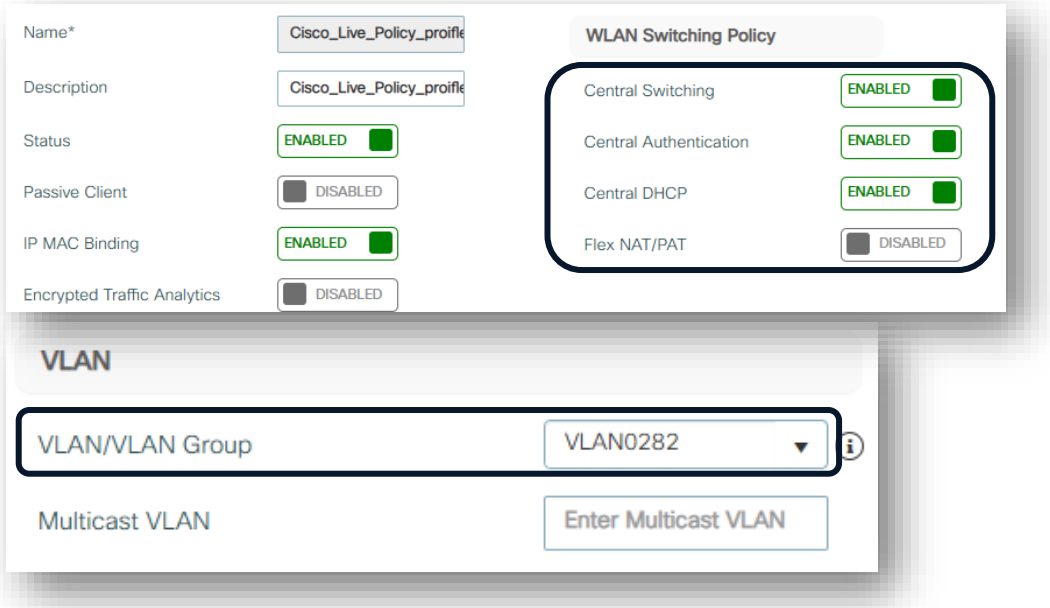



```
!
wlan Cisco_Live_Dot1x 9 Cisco_Live_Dot1x
radio policy dot11 24ghz
radio policy dot11 5ghz
security dot1x authentication-list Cisco_Live_Authe
!
```

© 2025 Cisco and/or its affiliates. All rights reserved.

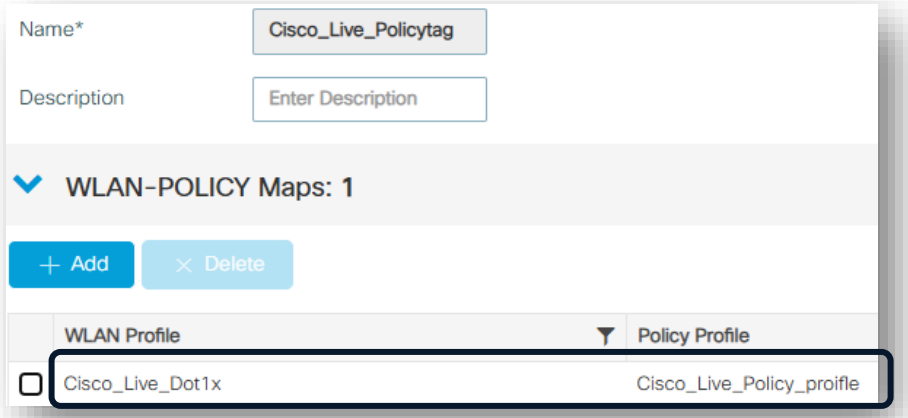
# WLC Configuration Overview

## 6. Configure Policy Profile




```
!
wireless profile policy Cisco_Live_Policy_proifle
description Cisco_Live_Policy_profile
vlan 282
no shutdown
!
```

## 7. Configure the Policy Tag to map the WLAN and Policy Profile




```
!
wireless tag policy Cisco_Live_Policytag
 description CL-PolicyTag
 wlan Cisco_Live_Dot1x policy Cisco_Live_Policy_profile
!
```

© 2025 Cisco and/or its affiliates. All rights reserved.

# EAP-TLS Common Error Logs

# EAP-TLS Common Errors

WLC

**Radioactive Traces**

2025/03/21 13:12:07.061330322 {wncd_x_R0-0}{1}: [client-orch-sm] [17707]: (note): MAC: ffff.ffff.ffff Client delete initiated. Reason: CO_CLIENT_DELETE_REASON_AAA_SERVER_UNAVAILABLE

2025/03/25 10:36:24.340001454 {wncd_x_R0-0}{1}: [client-orch-sm] [15664]: (note): MAC: ffff.ffff.ffff Client delete initiated. Reason: CO_CLIENT_DELETE_REASON_CLIENT_EAP_TIMEOUT_FAILURE

2025/03/25 10:21:48.492605329 {wncd_x_R0-0}{1}: [client-orch-sm] [15664]: (note): MAC: ffff.ffff.ffff Client delete initiated. Reason: CO_CLIENT_DELETE_REASON_L2AUTH_CONNECT_TIMEOUT

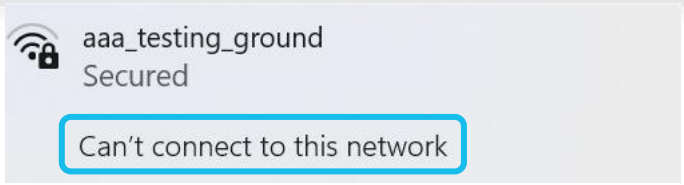
ISE

**Live Logs**

| | |
|---|---|
| Event | 5411 Supplicant stopped responding to ISE |
| Failure Reason | 12935 Supplicant stopped responding to ISE during EAP-TLS certificate exchange |

| | |
|---|---|
| Event | 5440 Endpoint abandoned EAP session and started new |
| Failure Reason | 5440 Endpoint abandoned EAP session and started new |

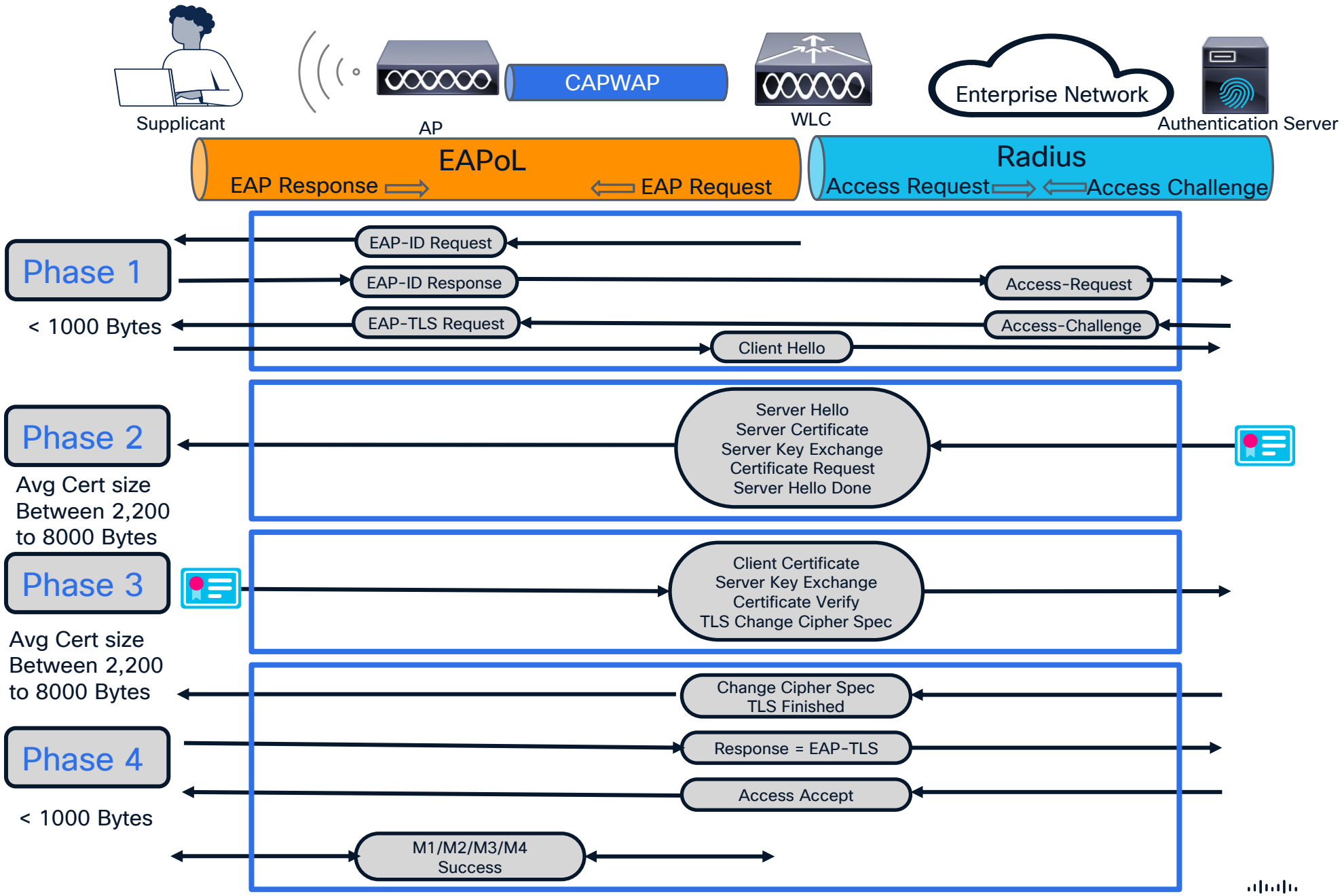
CLIENT




© 2025 Cisco and/or its affiliates. All rights reserved.

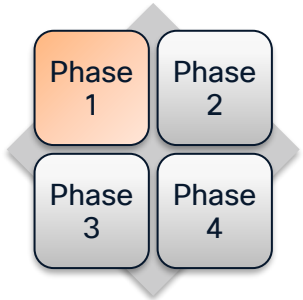
# Troubleshoot Fragments and MTU

# EAP-TLS Flow Diagram

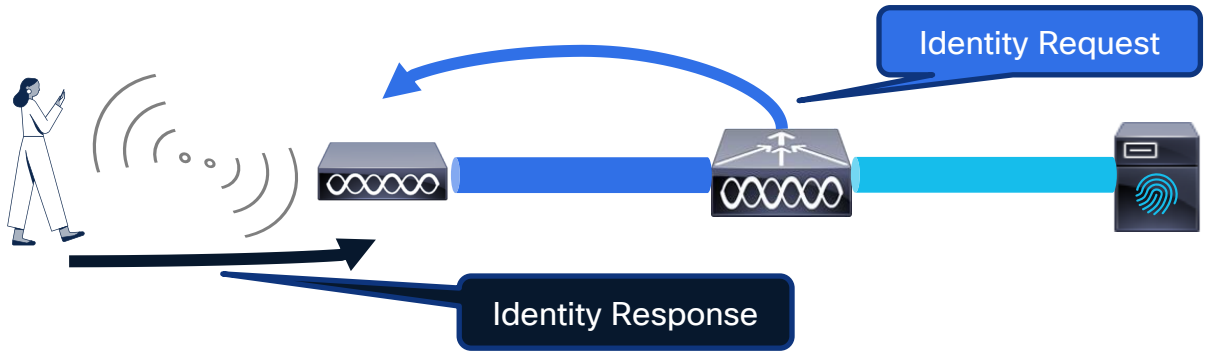



© 2025 Cisco and/or its affiliates. All rights reserved.

# Identity of Client




#3922 – WLC EPC PCAP
#388 – OTA




| Fragmentation Required | NO |
|---|---|

- Code 1 signifies it is a request and type 1 signifies it is for the identity request
- Code 2 signifies it is a response in identity response packet

```
3922 70:bc:48:80:ff:af   EAP  04:cf:4b:b1:c6:aa   Request, Identity
388  04:cf:4b:b1:c6:aa   EAP  70:bc:48:80:ff:af   Response, Identity
```

```
› User Datagram Protocol, Src Port: 5247, Dst Port: 5253
› Control And Provisioning of Wireless Access Points - Data
⌄ Extensible Authentication Protocol
    Code: Request (1)
    Id: 1
    Length: 5
    Type: Identity (1)
```

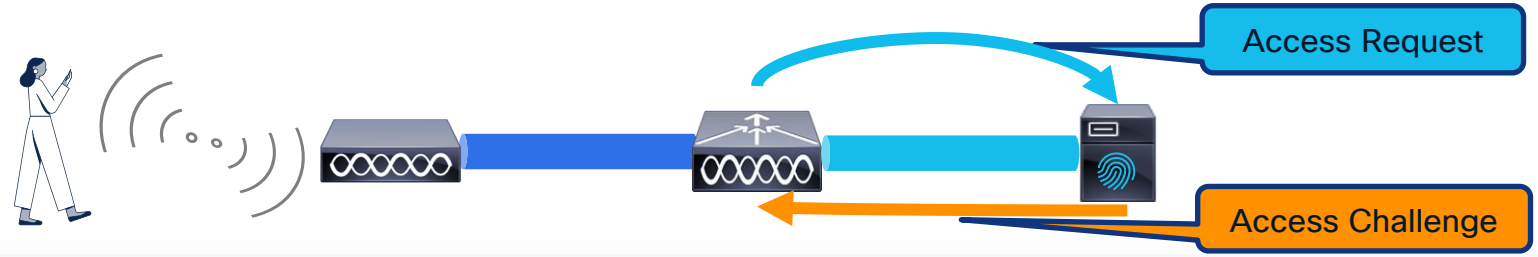
```
Extensible Authentication Protocol
  Code: Response (2)
  Id: 1
  Length: 19
  Type: Identity (1)
  Identity: host/Liveadmin
```

© 2025 Cisco and/or its affiliates. All rights reserved.

# Identity of Client in RADIUS

Phase 1 | Phase 2 | Phase 3 | Phase 4

WLC EPC PCAP




| Fragmentation Required | NO |
|---|---|

```
3967 192.168.182.17   RADIUS  192.168.189.28   Access-Request  id=143
3971 192.168.189.28   RADIUS  192.168.182.17   Access-Challenge id=143
```

```
RADIUS Protocol
    Code: Access-Request (1)
    Packet identifier: 0x8f (143)
    Length: 453
AVP: t=EAP-Message(79) l=21 Last Segment[1]
    Type: 79
  Extensible Authentication Protocol
      Code: Response (2)
      Id: 1
      Length: 19
      Type: Identity (1)
      Identity: host/Liveadmin
```

```
RADIUS Protocol
    Code: Access-Challenge (11)
    Packet identifier: 0x8f (143)
    Length: 120
AVP: t=EAP-Message(79) l=8 Last Segment
    Type: 79
  Extensible Authentication Protocol
    Code: Request (1)
    Id: 31
    Length: 6
    Type: TLS EAP (EAP-TLS) (13)
```

Radius Identifiers

© 2025 Cisco and/or its affiliates. All rights reserved.

# Understanding EAP Packet ID and RADIUS Identifier

## EAP Packet ID Consistency:

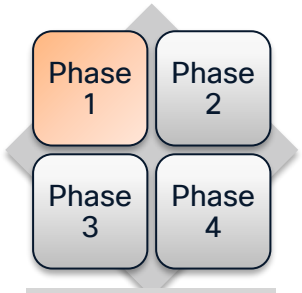
- When the RADIUS server sends an EAP message in AVP, Server assigns a new EAP Packet ID.
- This EAP Packet ID remains consistent throughout the entire communication flow until the next EAP message is initiated by the RADIUS server.
- For instance, as seen in the previous packet capture, the EAP Packet ID is 31. When the WLC forwards this EAP packet to the AP via CAPWAP, the same Packet ID (31) is retained, as shown in subsequent pcaps.

## RADIUS Identifier Consistency:

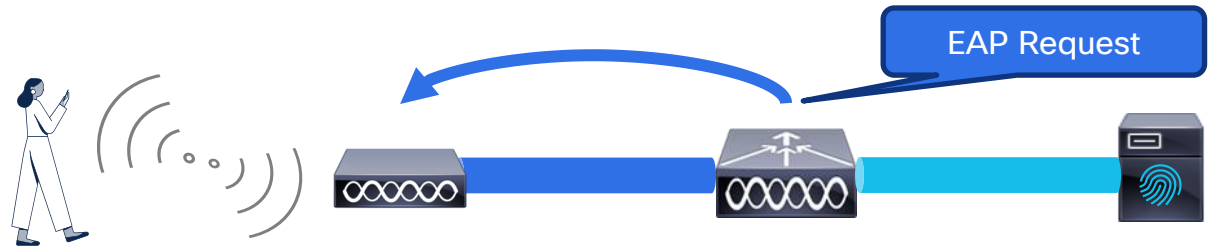
- The RADIUS Identifier remains consistent throughout a single transaction.
- The communication begins with an Access-Request sent from the WLC to the RADIUS server. The same Identifier is preserved when the RADIUS server responds with an Access-Challenge. So, WLC assigns new Radius Identifier in communications.
- For example, in the previous pcap, the RADIUS Identifier is 143 on both the Access-Request and Access-Challenge messages.

© 2025 Cisco and/or its affiliates. All rights reserved.

# Response on Identity




WLC EPC PCAP




| Fragmentation Required | NO |
|---|---|

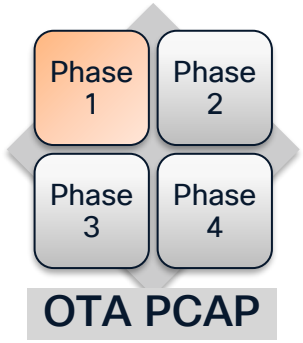
```
3973 70:bc:48:80:ff:af  EAP     04:cf:4b:b1:c6:aa  Request, TLS EAP (EAP-TLS)
```

```
› Internet Protocol Version 4, Src: 192.168.182.17, Dst: 192.168.182.146
› User Datagram Protocol, Src Port: 5247, Dst Port: 5253
› Control And Provisioning of Wireless Access Points - Data
› IEEE 802.11 Data, Flags: ......F.
› Logical-Link Control
› 802.1X Authentication
⌄ Extensible Authentication Protocol
    Code: Request (1)
    Id: 31
    Length: 6
    Type: TLS EAP (EAP-TLS) (13)
  › EAP-TLS Flags: 0x20
```

EAP Packet ID

© 2025 Cisco and/or its affiliates. All rights reserved.

# Response on Identity




| Fragmentation Required | NO |
|---|---|

- Below, we can observe the same EAP packet being transmitted over the air, maintaining the consistent EAP Packet ID of 31

```
392 70:bc:48:80:ff:af  EAP    04:cf:4b:b1:c6:aa  Request, TLS EAP (EAP-TLS)
```

```
Extensible Authentication Protocol
    Code: Request (1)
    Id: 31
    Length: 6
    Type: TLS EAP (EAP-TLS) (13)
  > EAP-TLS Flags: 0x20
```

© 2025 Cisco and/or its affiliates. All rights reserved.

# TLS Session Initiation

### Client Response to EAP-Request:

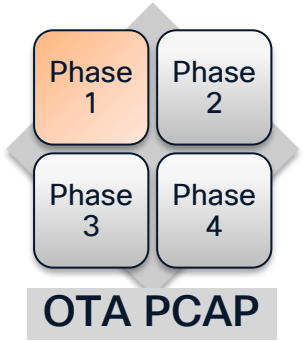
When the client receives the EAP-Request, it must respond with an EAP-Response. In this response, the client begins the process of establishing a TLS session.

### TLS Session Initialization:

The TLS session setup begins with the "Client Hello" message, and as seen in the next packet, the EAP Packet ID remains consistently set to 31.

© 2025 Cisco and/or its affiliates. All rights reserved.

# TLS Session Initiation





| Fragmentation Required | NO |
|---|---|

```
394 04:cf:4b:b1:c6:aa  TLSv1    70:bc:48:80:ff:af  Client Hello
```

```
› 802.1X Authentication
⌄ Extensible Authentication Protocol
    Code: Response (2)
    Id: 31
    Length: 437
    Type: TLS EAP (EAP-TLS) (13)
  › EAP-TLS Flags: 0x80
    EAP-TLS Length: 427
  ⌄ Transport Layer Security
      › TLSv1 Record Layer: Handshake Protocol: Client Hello
```

EAP Packet Id is same in Response as it was in request

© 2025 Cisco and/or its affiliates. All rights reserved.

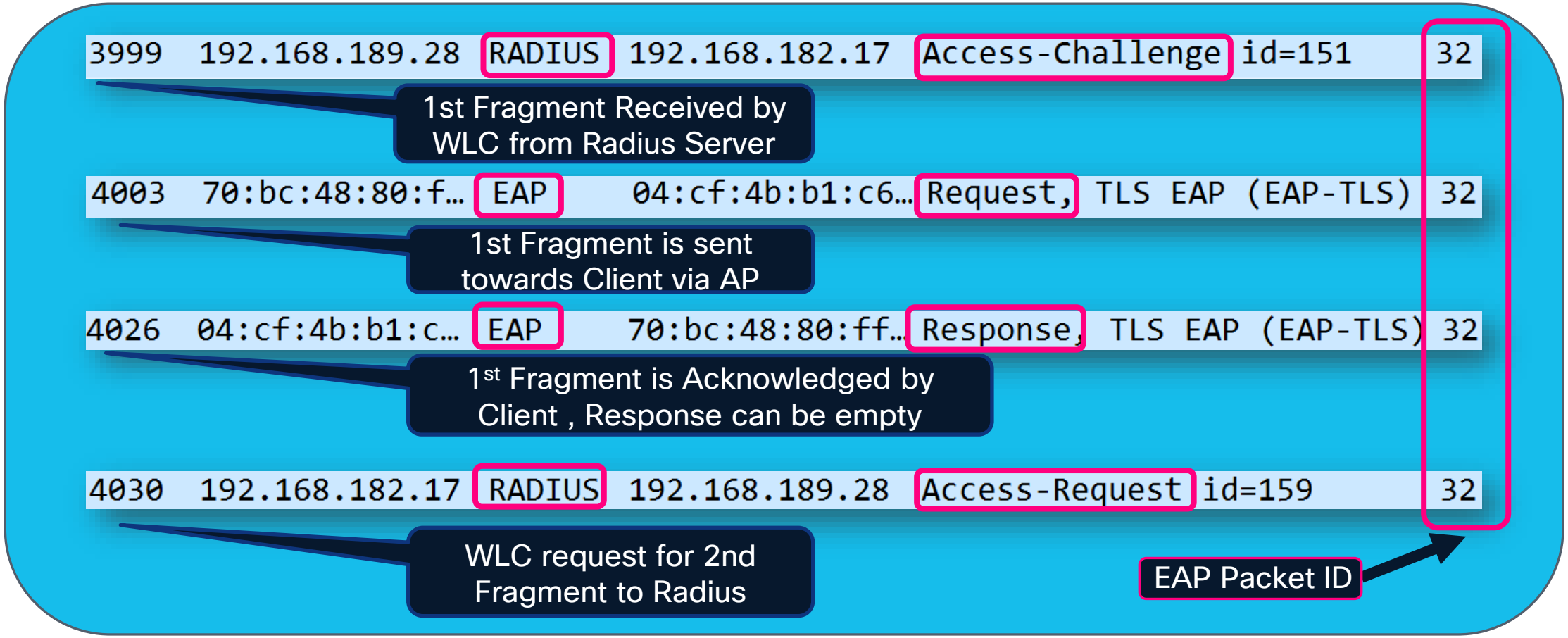
# Fragmentation Behavior

The Auth server MUST wait until it receives the EAP-Response before sending another fragment

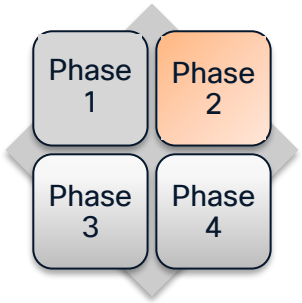
Same applies to the supplicant, it MUST wait until it receives the EAP-Request before sending another fragment.

WLC EPC PCAP

- Following shows one Fragment Behavior before sending another one from server side:




© 2025 Cisco and/or its affiliates. All rights reserved.




# Server Certificate

OTA PCAP

| Fragmentation Required | Yes |
|---|---|

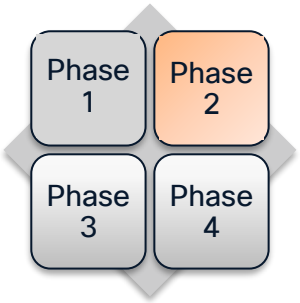
ISE intelligently sends packets sized at 1002 bytes, aiming to minimize the chances of further fragmentation within the network.

```
417  70:bc:48:80:ff:… TLSv1.2 04:cf:4b:b1:c6… Server Hello, Certificate,
▾ [3 EAP-TLS Fragments (2163 bytes): #408(1002), #413(1002), #417(159)]
    [Frame: 408, payload: 0-1001 (1002 bytes)]
    [Frame: 413, payload: 1002-2003 (1002 bytes)]
    [Frame: 417, payload: 2004-2162 (159 bytes)]
    [Fragment Count: 3]
    [Reassembled EAP-TLS Length: 2163]
  ▾ Transport Layer Security
    › TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    › TLSv1.2 Record Layer: Handshake Protocol: Certificate
    › TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
    › TLSv1.2 Record Layer: Handshake Protocol: Certificate Request
    › TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done
```

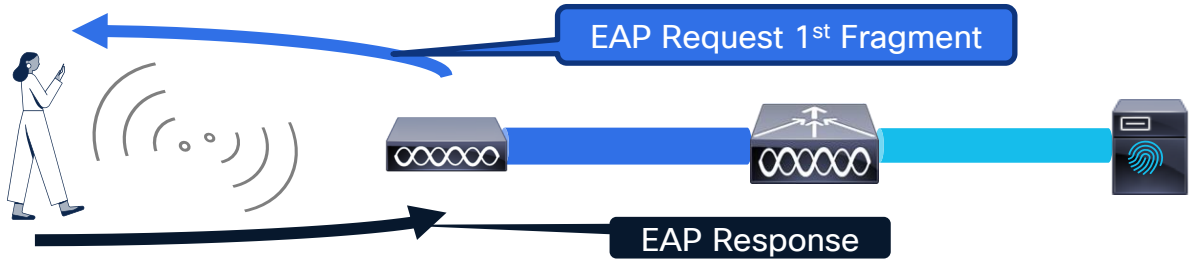
Zooming in on Fragment

© 2025 Cisco and/or its affiliates. All rights reserved.

# Server Certificate




OTA PCAP




| Fragmentation Required | Yes |
|---|---|

- ISE transmits the data in multiple Fragments, each time awaiting an empty EAP Response in return.

```
408  70:bc:48:80:ff:af  EAP  04:cf:4b:b1:c6:aa  Request, TLS EAP (EAP-TLS)
410  04:cf:4b:b1:c6:aa  EAP  70:bc:48:80:ff:af  Response, TLS EAP (EAP-TLS)
```

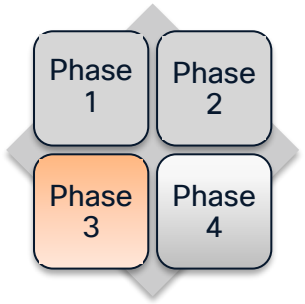
```
Extensible Authentication Protocol
  Code: Request (1)
  Id: 32
  Length: 1012
  Type: TLS EAP (EAP-TLS) (13)
  EAP-TLS Flags: 0xc0
    1... .... = Length Included: True
    .1.. .... = More Fragments: True
    ..0. .... = Start: False
  EAP-TLS Length: 2163
```

```
Extensible Authentication Protocol
  Code: Response (2)
  Id: 32
  Length: 6
  Type: TLS EAP (EAP-TLS) (13)
  EAP-TLS Flags: 0x00
    0... .... = Length Included: False
    .0.. .... = More Fragments: False
    ..0. .... = Start: False
```

Empty EAP Response

© 2025 Cisco and/or its affiliates. All rights reserved.

# Client Certificate




OTA PCAP


| Fragmentation Required | Yes |
|---|---|

- Client sends fragmented certificate to AP.
- The length of the Certificate is 4150 bytes

```
4134 04:cf:4b:b1:c6:aa  TLSv1.2    70:bc:48:80… Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
```

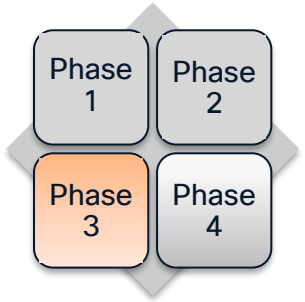
```
Extensible Authentication Protocol
 Code: Response (2)
 Id: 37
 Length: 131
 Type: TLS EAP (EAP-TLS) (13)
EAP-TLS Flags: 0x00
  0... .... = Length Included: False
  .0.. .... = More Fragments: False
  ..0. .... = Start: False
[4 EAP-TLS Fragments (4579 bytes): #4062(1482), #4091(1486), #4113(1486), #4134(125)]
  [Frame: 4062, payload: 0-1481 (1482 bytes)]
  [Frame: 4091, payload: 1482-2967 (1486 bytes)]
  [Frame: 4113, payload: 2968-4453 (1486 bytes)]
  [Frame: 4134, payload: 4454-4578 (125 bytes)]
  [Fragment Count: 4]
  [Reassembled EAP-TLS Length: 4579]
```

Zooming in on Fragment

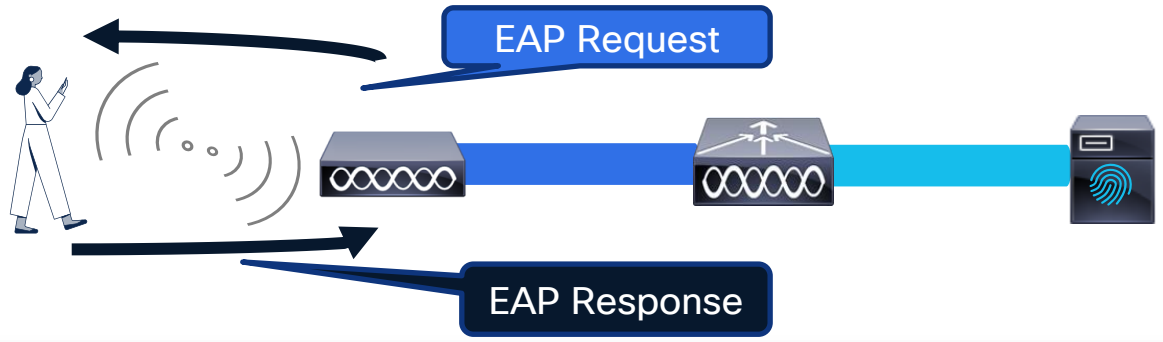
```
Transport Layer Security
TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 4523
  Handshake Protocol: Certificate
    Handshake Type: Certificate (11)
    Length: 4153
    Certificates Length: 4150
    Certificates (4150 bytes)
```

© 2025 Cisco and/or its affiliates. All rights reserved.

# Client Certificate




OTA PCAP




| Fragmentation Required | Yes |
|---|---|

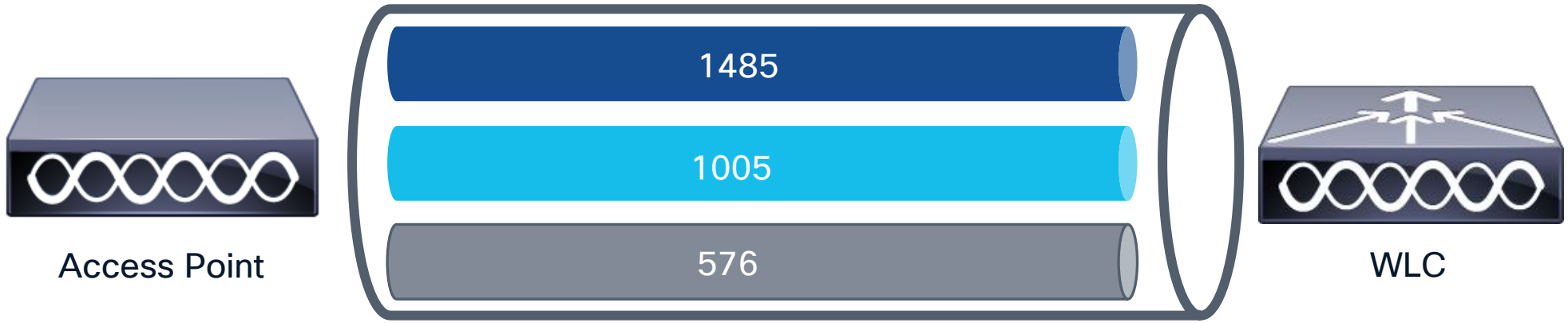
```
4062 04:cf:4b:b1:c6:aa        EAP        70:bc:48:80:ff:af Response, TLS EAP (EAP-TLS)
4082 70:bc:48:80:ff:af        EAP        04:cf:4b:b1:c6:aa Request, TLS EAP (EAP-TLS)
```

```
Extensible Authentication Protocol
 Code: Response (2)
 Id: 34
 Length: 1492
 Type: TLS EAP (EAP-TLS) (13)
 EAP-TLS Flags: 0xc0
  1... .... = Length Included: True
  .1.. .... = More Fragments: True
  ..0. .... = Start: False
 EAP-TLS Length: 4579
```

```
Extensible Authentication Protocol
 Code: Request (1)
 Id: 35
 Length: 6
 Type: TLS EAP (EAP-TLS) (13)
 EAP-TLS Flags: 0x00
  0... .... = Length Included: False
  .0.. .... = More Fragments: False
  ..0. .... = Start: False
```

© 2025 Cisco and/or its affiliates. All rights reserved.

# Fragmentation at AP Port for Client Certificate




PMTU (Path Maximum Transmission Unit) depends on these major factors:

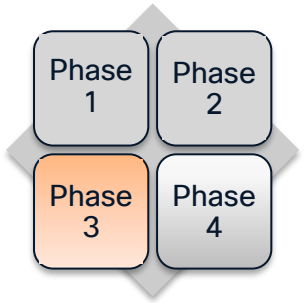
- Refers to the largest packet size that can be transmitted without fragmentation on a specific network path
- The Access Point is set to negotiate PMTU at 576, 1005 or 1485

- Verification can be done at WLC or AP level using the following commands:

```
c9800_40_new_1#show ap name C9120AXI-1 config general
Cisco AP Name                    : C9120AXI-1
MAC Address                      : 70bc.4829.3e48
IP Address Configuration         : DHCP
IP Address                       : 192.168.182.115
IP Netmask                       : 255.255.255.0
Gateway IP Address               : 192.168.182.1
CAPWAP Path MTU                  : 1485
```

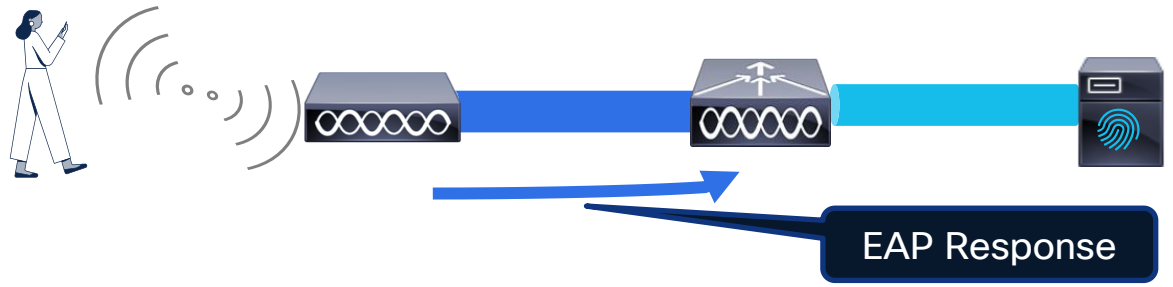
```
C9120AXI-1#show capwap client rcb
OperationState                   : UP
Name                             : C9120AXI-1
SwVer                            : 17.15.3.28
MwarApMgrIp                      : 192.168.182.17
MwarName                         : c9800_40_new_1
ApMode                           : Local
CAPWAP Path MTU                  : 1485
```

© 2025 Cisco and/or its affiliates. All rights reserved.




# Fragmentation at AP Port for Client Certificate

AP PCAP



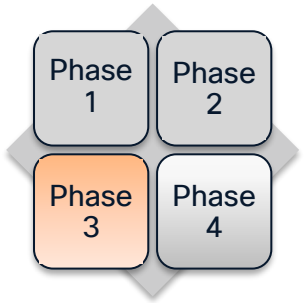

| Fragmentation Required | Yes |
|---|---|

- The AP encapsulates the frames in CAPWAP

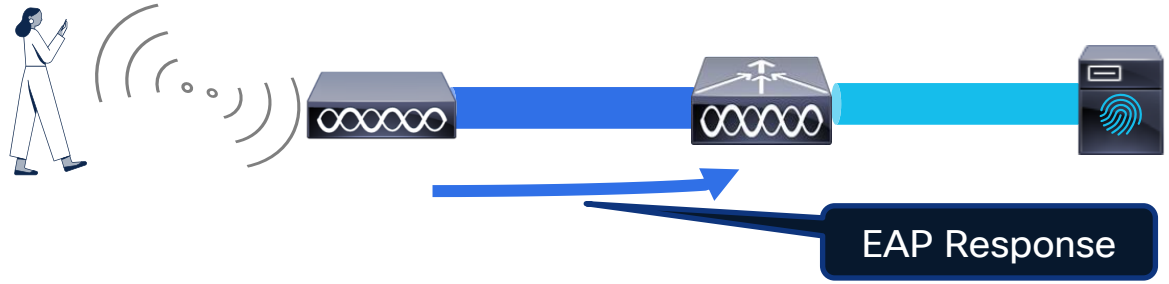
```
955 04:cf:4b:b1:c6:aa  TLSv1.2    70:bc:48:80.. Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
Control And Provisioning of Wireless Access Points - Data
Extensible Authentication Protocol
  Code: Response (2)
  Id: 37
  Length: 131
  Type: TLS EAP (EAP-TLS) (13)
> EAP-TLS Flags: 0x00
v [4 EAP-TLS Fragments (4579 bytes): #947(1482), #950(1486), #953(1486), #955(125)]
    [Frame: 947, payload: 0-1481 (1482 bytes)]
    [Frame: 950, payload: 1482-2967 (1486 bytes)]
    [Frame: 953, payload: 2968-4453 (1486 bytes)]
    [Frame: 955, payload: 4454-4578 (125 bytes)]
    [Fragment Count: 4]
    [Reassembled EAP-TLS Length: 4579]
```

CAPWAP Encapsulation

Zooming in on Fragment




# Fragmentation at AP Port for Client Certificate




| Fragmentation Required | Yes |
|---|---|

**AP PCAP**

- AP adds CAPWAP header and send fragments to the WLC

**TAC Tip** eap || eapol || data.data contains 04:cf:4b:b1:c6:aa

```
946 192.168.182.146   CAPWAP-Data  192.168.182… CAPWAP-Data (Fragment ID: 16271
Control And Provisioning of Wireless Access Points - Data
Reassembled in: 947
```

First Fragmentation

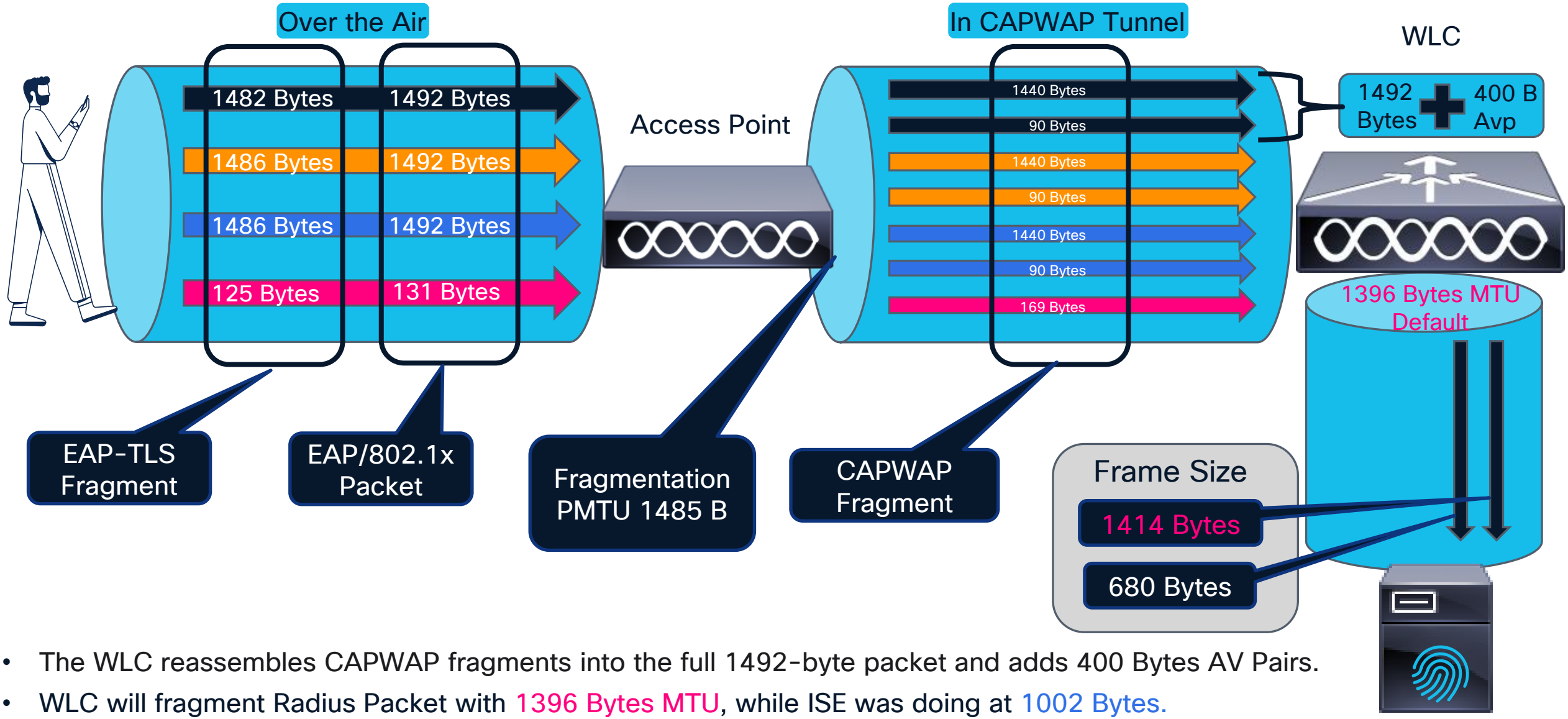
```
947 04:cf:4b:b1:c6:aa EAP          70:bc:48:80… Response, TLS EAP (EAP-TLS)
Control And Provisioning of Wireless Access Points - Data
[2 Message fragments (1530 bytes): #946(1440), #947(90)]
```

Second Fragmentation

- The packet is fragmented twice:
  - 1 – Fragmentation performed by the client to exchange the certificate
  - 2 – Fragmentation performed by the AP to add CAPWAP header

© 2025 Cisco and/or its affiliates. All rights reserved.

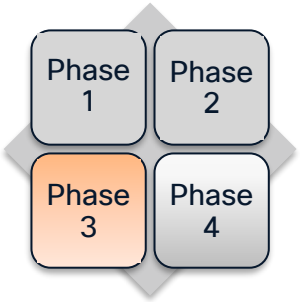
# Client Certificate




- The WLC reassembles CAPWAP fragments into the full 1492-byte packet and adds 400 Bytes AV Pairs.
- WLC will fragment Radius Packet with 1396 Bytes MTU, while ISE was doing at 1002 Bytes.

© 2025 Cisco and/or its affiliates. All rights reserved.

# Client Certificate




WLC PCAP


| Fragmentation Required | Yes |
|---|---|

TAC Tip

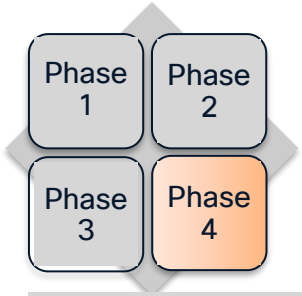
eap || eapol || data.data contains 04:cf:4b:b1:c6:aa || ip

```
4076  192.168.182.17     IPv4      192.168.189.28     Fragmented IP protocol
> Frame 4076: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits)
> Ethernet II, Src: 24:d5:e4:d9:fc:ab (24:d5:e4:d9:fc:ab), Dst: Cisco_ce:98:f3
> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 282
> Internet Protocol Version 4, Src: 192.168.182.17, Dst: 192.168.189.28
v Data (1376 bytes)
```

Can this value packet drop?

```
4077  192.168.182.17     RADIUS    192.168.189.28     Access-Request id=175
> Frame 4077: 680 bytes on wire (5440 bits), 680 bytes captured (5440 bits)
> Ethernet II, Src: 24:d5:e4:d9:fc:ab (24:d5:e4:d9:fc:ab), Dst: Cisco_ce:98:f3
v RADIUS Protocol
    > AVP: t=EAP-Message(79) l=255 Segment[1]
    > AVP: t=EAP-Message(79) l=255 Segment[2]
    > AVP: t=EAP-Message(79) l=255 Segment[3]
```

© 2025 Cisco and/or its affiliates. All rights reserved.




# TLS Session Established

WLC PCAP

- Let us review the Phase 4 packet flows before proceeding to the next section on the WLC's new feature.
- Once the RADIUS server receives the client certificates (all fragments), it responds with the cipher spec and TLS tunnel will be established with following communications.

1 After last Client cert Fragment in Access-Request this message arrives from ISE which contains Cipher Spec

EAP Packet Id is same for all side communications

```
4142 192.168.189.28     RADIUS   192.168.182.17     38 Access-Challenge id=199
4144 70:bc:48:80:ff:af  TLSv1.2  04:cf:4b:b1:c6:aa  38 Change Cipher Spec, Encrypted Handshake Message
4154 04:cf:4b:b1:c6:aa  EAP      70:bc:48:80:ff:af  38 Response, TLS EAP (EAP-TLS)
```

3 Client is acknowledging cipher spec
This is response arrived from AP in CAPWAP

2 This Cipher Spec is placed in CAPWAP from WLC to AP

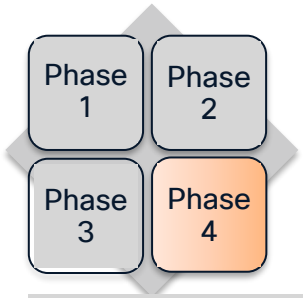
```
4156 192.168.182.17     RADIUS   192.168.189.28     38 Access-Request id=207
4175 192.168.189.28     RADIUS   192.168.182.17     38 Access-Accept id=207
```

5 ISE Responding back to WLC with Accept which contains Success message in EAP

EAP Packet Id is same for all side communications

4 Towards ISE

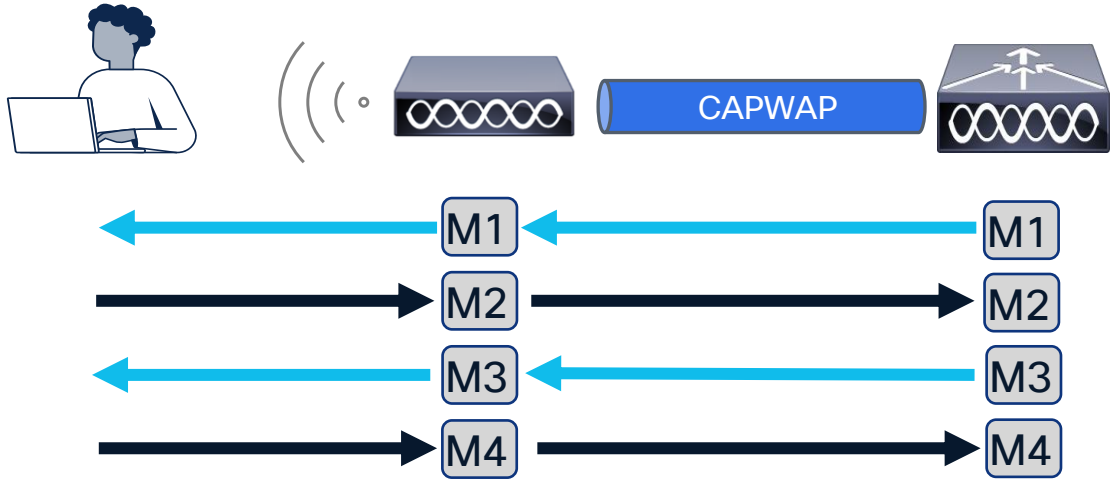
© 2025 Cisco and/or its affiliates. All rights reserved.




WLC PCAP

# TLS Session Established

- Now a critical 4-step handshake between the authenticator and the supplicant will occur. This handshake plays a vital role in generating encryption keys that secure the wireless connection.
- The successful completion of the EAP-TLS authentication process establishes a secure, encrypted communication channel



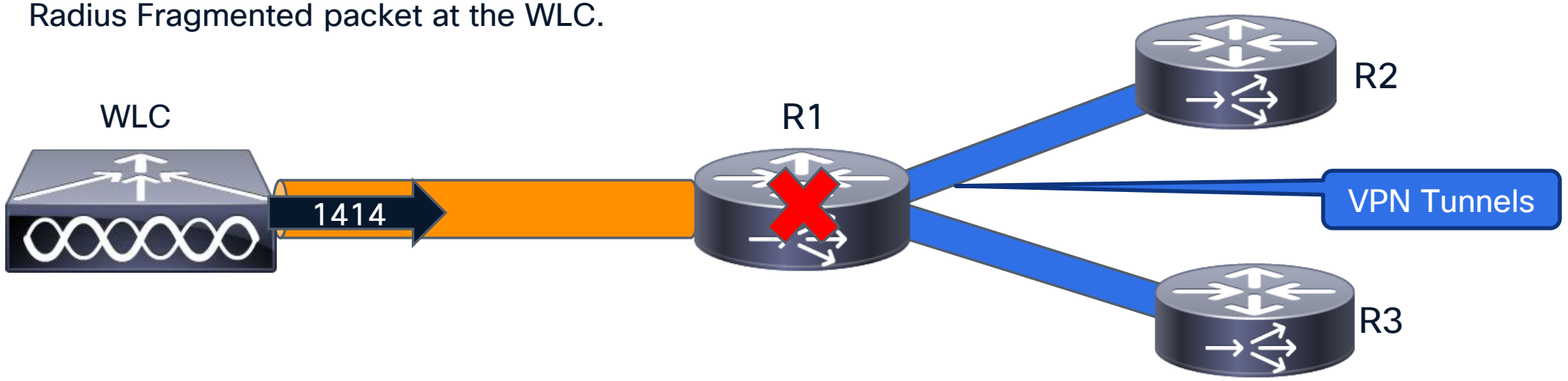

```
4197 70:bc:48:80:ff:af  EAPOL   04:cf:4b:b1:c6:aa     Key (Message 1 of 4)
4203 04:cf:4b:b1:c6:aa  EAPOL   70:bc:48:80:ff:af     Key (Message 2 of 4)
4209 70:bc:48:80:ff:af  EAPOL   04:cf:4b:b1:c6:aa     Key (Message 3 of 4)
4217 04:cf:4b:b1:c6:aa  EAPOL   70:bc:48:80:ff:af     Key (Message 4 of 4)
```

© 2025 Cisco and/or its affiliates. All rights reserved.

# Potential Cause for Fragments Drop

## Scenario 1: GRE/IPSEC VPN Tunnels in Routers between WLC and ISE

- Routers need to add additional header of tunneling protocols which end up increasing MTU close to Radius Fragmented packet at the WLC.




## Scenario 2: Don't Fragment is configured and device need to Fragment

- If the Don't Fragment flag config is set, then fragmentation of packet is NOT permitted, and it may drop.

## How can we overcome this issue from WLC?

© 2025 Cisco and/or its affiliates. All rights reserved.

# Utilize Radius MTU Feature for Fragment Control

# MTU Feature Introduction in 9800

Starting from version 17.11, the WLC has introduced behavior change where you can configure MTU for SVI and add them under AAA server groups for radius packets to Fragment.

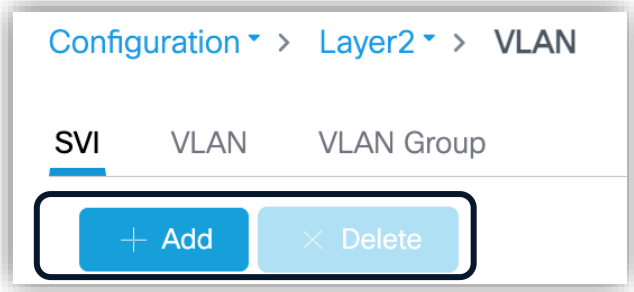
- This gives you more control and you do not need to make multiple changes in your infrastructure to accommodate Fragments.

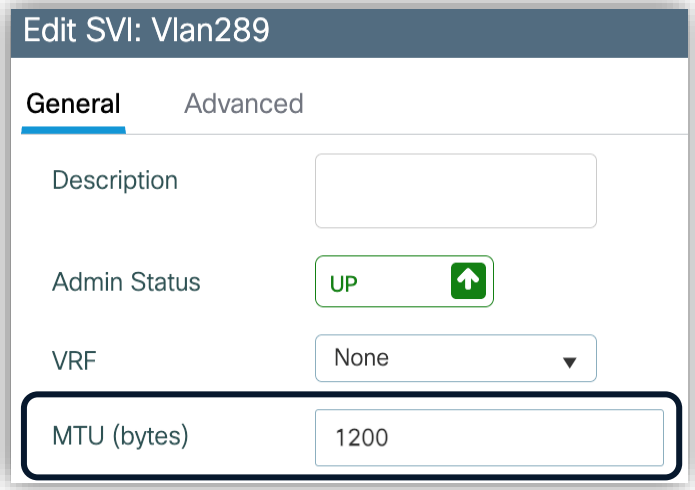
- Let us look ahead what configuration we need and how packets will look like after this.

© 2025 Cisco and/or its affiliates. All rights reserved.

# Layer 3 Interface in 9800 for MTU Feature

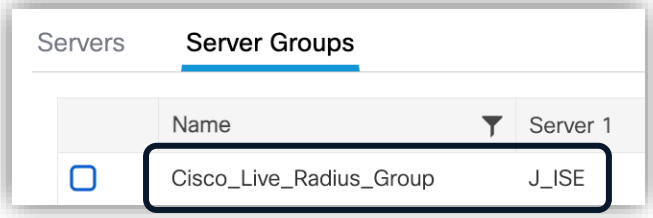
## 1. Configure SVI and set desired MTU value

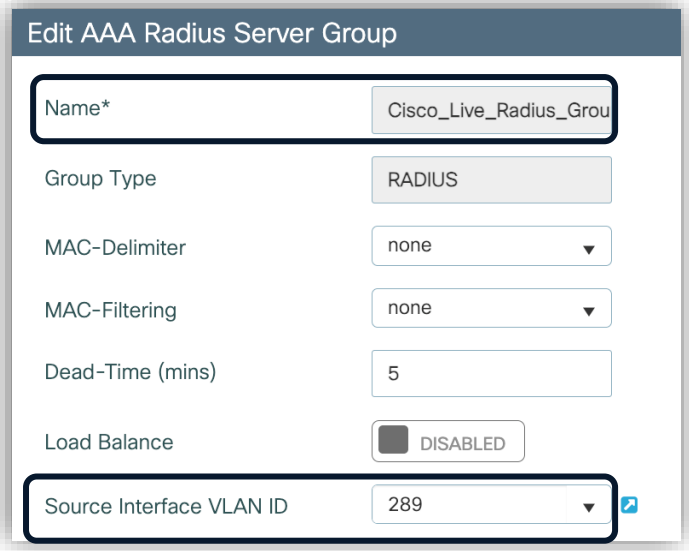



```
!
interface Vlan289
 ip address 192.168.189.31 255.255.255.0
 no ip proxy-arp
 ip mtu 1200
!
```

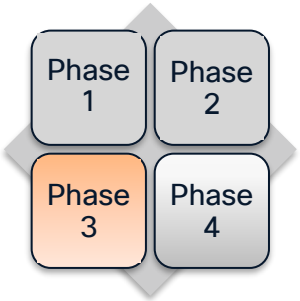
## 2. Map SVI with new MTU to RADIUS Server Group



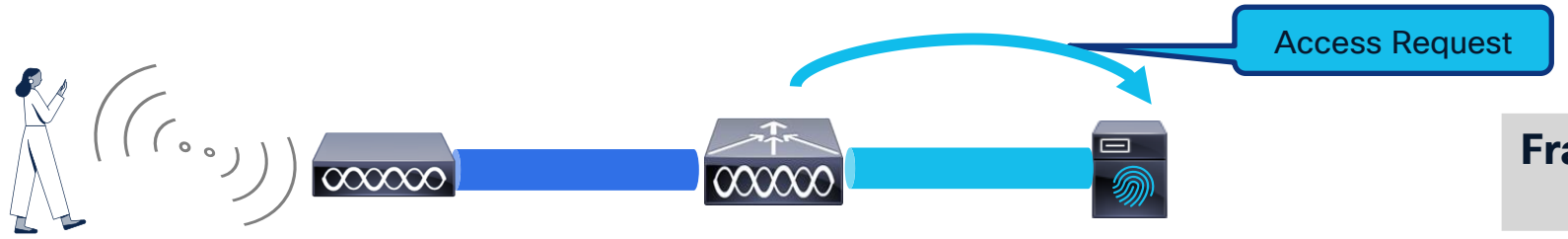

```
!
aaa group server radius Cisco_Live_Radius_Group
 ip radius source-interface Vlan289
!
```

© 2025 Cisco and/or its affiliates. All rights reserved.




WLC PCAP

# MTU Behavior Change




| Fragmentation Required | Yes |
|---|---|

- Gain control by setting MTU to match the network requirements.

```
2713 192.168.189.31     IPv4          192.168.189… Fragmented IP protocol
Frame 2713: 1210 bytes on wire (9680 bits), 1210 bytes captured (9680 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 192.168.189.31, Dst: 192.168.189.28
Data (1176 bytes)
```

```
2714 192.168.189.31     RADIUS        192.168.189… Access-Request id=223
Frame 2714: 877 bytes on wire (7016 bits), 877 bytes captured (7016 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 192.168.189.31, Dst: 192.168.189.28
User Datagram Protocol, Src Port: 56595, Dst Port: 1812
RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0xdf (223)
  Length: 2011
  Authenticator: 2d70752da6b76440abc2d7ea65ce138f
```

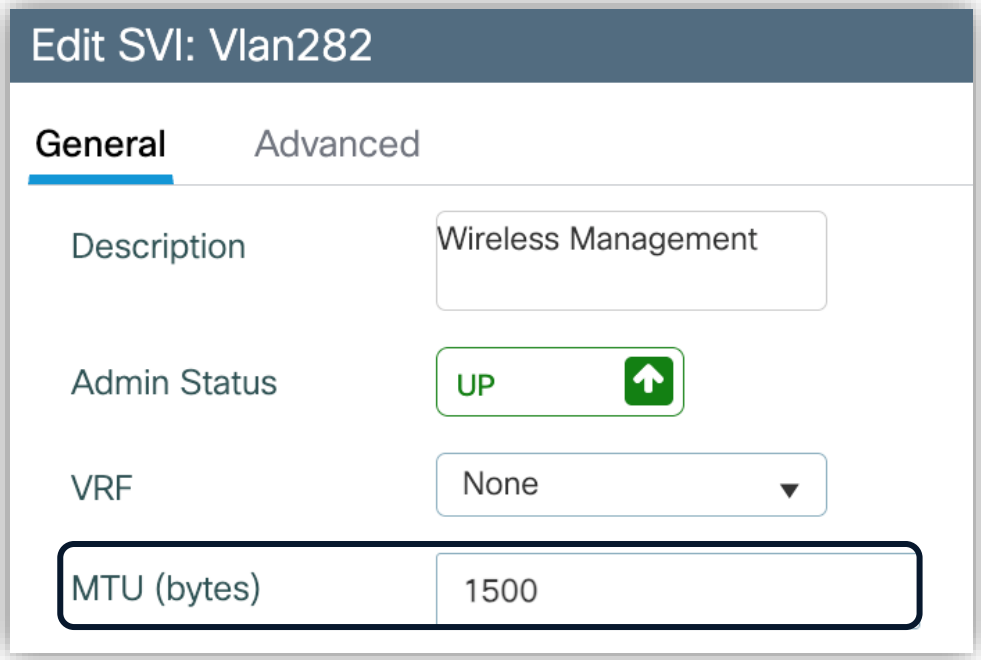
© 2025 Cisco and/or its affiliates. All rights reserved.

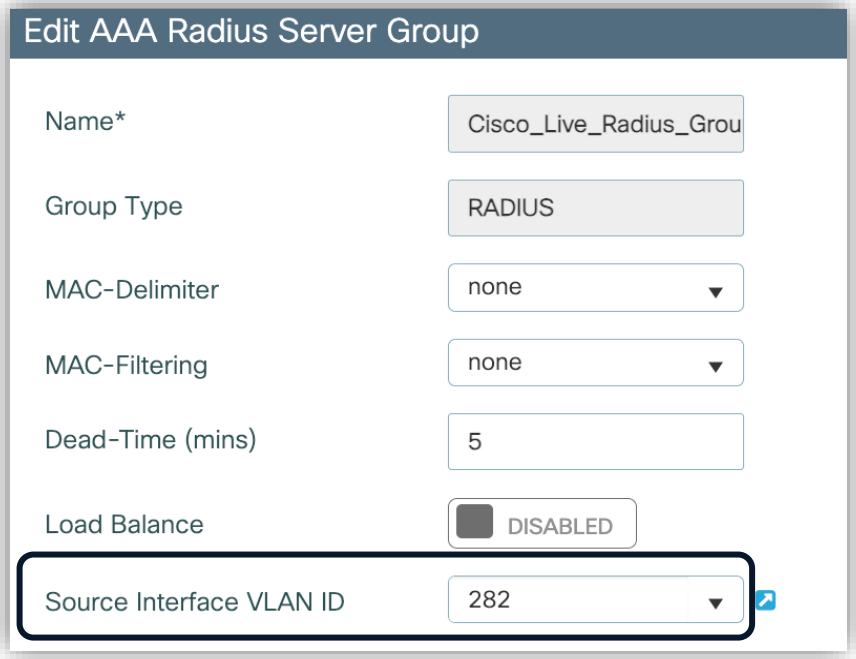
# What Happens If WMI is Used as RADIUS Source?

If you are using Cisco Catalyst Center to provision AAA configurations, it automatically includes the source interface in the server group.

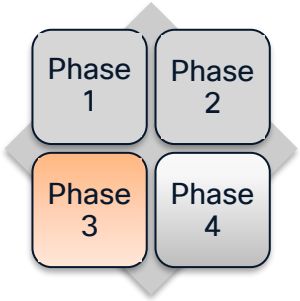
TAC Tip

- When you source WMI in Radius WLC will take that as 1500 MTU which is default value




© 2025 Cisco and/or its affiliates. All rights reserved.




# MTU Using WMI as RADIUS Source

- Client Certificate 1st Fragment Leaving WLC towards Radius Sever

WLC PCAP


```
468 2025-05-02 16:39:4…  192.168.182.…  IPv4   192.168.189.28  Fragmented IP protocol
  › Frame 468: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
  › Internet Protocol Version 4, Src: 192.168.182.17, Dst: 192.168.189.28
  › Data (1480 bytes)
```

1480 B Data + 20 B Ipv4 Header + 14 B Ethernet Header = 1514 B

```
469 2025-05-02 16:39:4…  192.168.182.17  RADIUS  192.168.189.28  Access-Request id=151
  › Frame 469: 572 bytes on wire (4576 bits), 572 bytes captured (4576 bits)
  ⌄ Internet Protocol Version 4, Src: 192.168.182.17, Dst: 192.168.189.28
    ⌄ [2 IPv4 Fragments (2018 bytes): #468(1480), #469(538)]
        [Frame: 468, payload: 0-1479 (1480 bytes)]
        [Frame: 469, payload: 1480-2017 (538 bytes)]
```

538 B Data + 20 B Ipv4 Header + 14 B Ethernet Header = 572 B

© 2025 Cisco and/or its affiliates. All rights reserved.

# Radius Jumbo Frames

# MTU Configuration for RADIUS Jumbo Frames

- Configure Jumbo MTU to enable big maximum transmission unit (MTU).
- Jumbo frames are frames that are bigger than the standard Ethernet frame size, which is 1518 bytes (including Layer 2 (L2) header and FCS).
- However, now the IP MTU is set to 9000, you can configure the MTU equal or higher than the IP MTU.
- You can see the configuration in the output below:

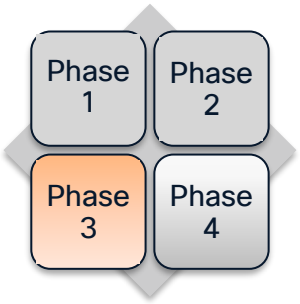
```
c9800_40_new_1#show run int vlan 289
Current configuration : 106 bytes
!
interface Vlan289
mtu 9100
ip address 192.168.189.31 255.255.255.0
no ip proxy-arp
ip mtu 9000
end
!
```

```
c9800_40_new_1#show interface vlan 289
Vlan289 is up, line protocol is down , Autostate Enabled
  Hardware is Ethernet SVI, address is ffff.ffff.fff (bia ffff.ffff.ffff)
  Internet address is 192.168.189.31/24
  MTU 9100 bytes, BW 1000000 Kbit/sec, DLY 10 usec
```

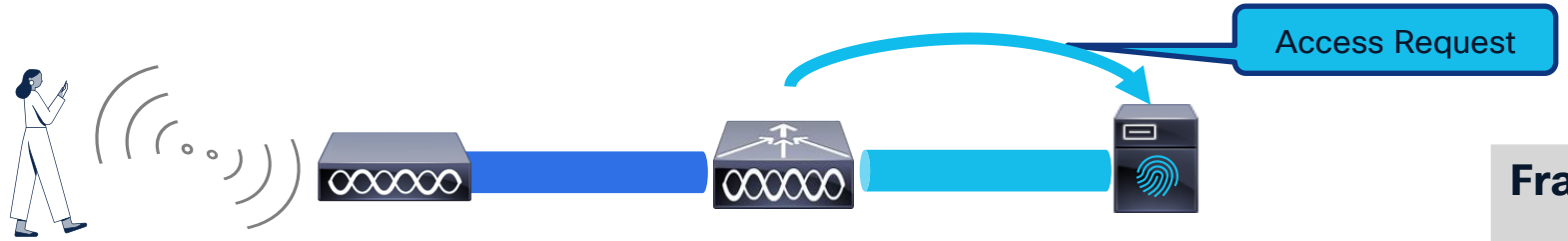
TAC Tip

- Feature was introduced on code 17.11
- Jumbo Frames are only supported for RADIUS frames

© 2025 Cisco and/or its affiliates. All rights reserved.




# MTU Behavior Change for Jumbo Frames



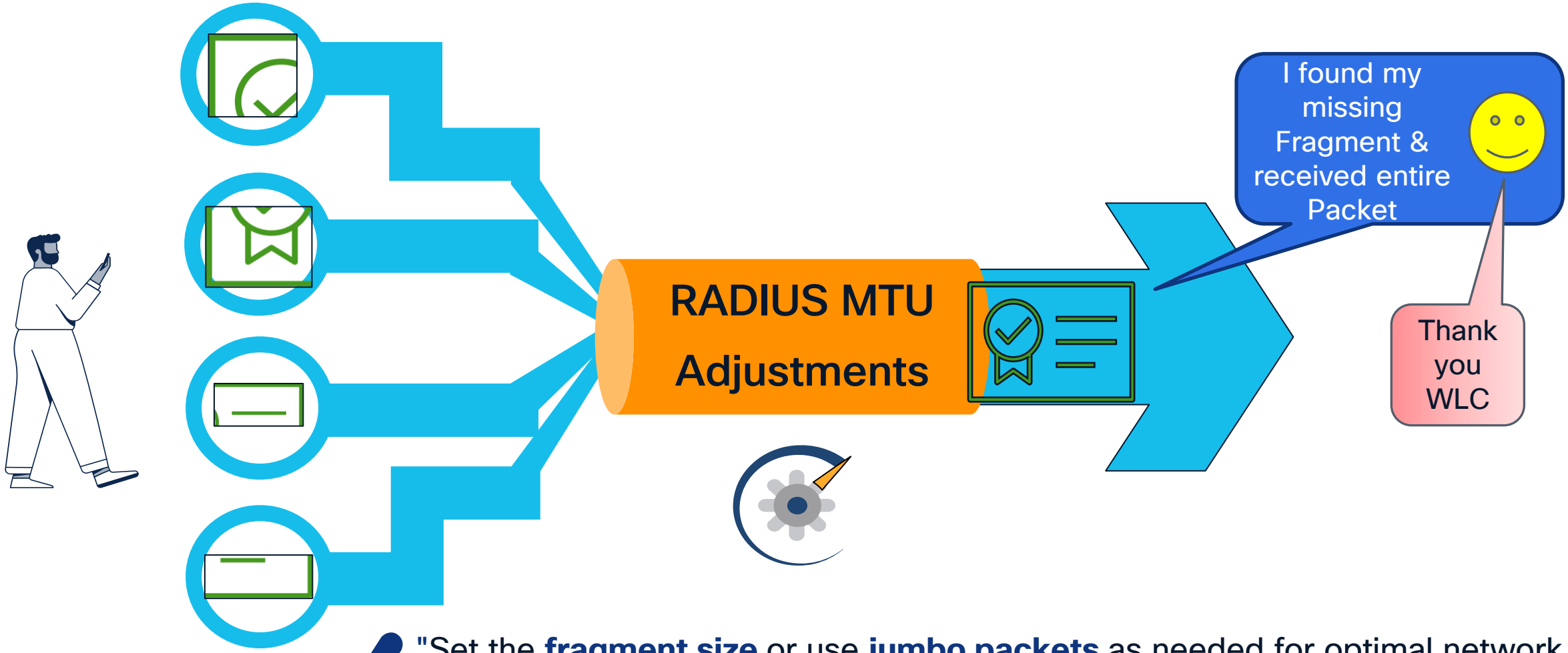

| Fragmentation Required | NO |
|---|---|

- The WLC sends Jumbo Frames for RADIUS traffic.
- There is no fragmentation required as MTU is set to 9000

```
11339 192.168.189.31     RADIUS        192.168.189…Access-Request id=119
Frame 11339: 2053 bytes on wire (16424 bits), 2053 bytes captured (16424 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 192.168.189.31, Dst: 192.168.189.28
User Datagram Protocol, Src Port: 56595, Dst Port: 1812
RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x77 (119)
  Length: 2011
  Authenticator: 124b73d5fbdd3081df644abc67339d28
```

© 2025 Cisco and/or its affiliates. All rights reserved.

# Think Big, Send Smart




"Set the **fragment size** or use **jumbo packets** as needed for optimal network **performance** using Radius MTU adjustment on the WLC!"

© 2025 Cisco and/or its affiliates. All rights reserved.

# Complete Your Session Evaluations

**Complete** a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

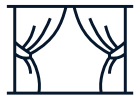
**Earn** 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

**Level up** and earn exclusive prizes!

**Complete your surveys** in the Cisco Live mobile app.

© 2025 Cisco and/or its affiliates. All rights reserved.

# Continue Your Education



**Visit** the Cisco Showcase for related demos

**Book** your one-on-one Meet the Engineer meeting

**Attend** the interactive education with DevNet, Capture the Flag, and Walk-in Labs

**Visit** the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

**Contact us at**: jaydepat@cisco.com, casocorr@cisco.com

© 2025 Cisco and/or its affiliates. All rights reserved.

# Q & A

CISCO Live !

# Thank you

cisco Live !