RADIUS-MTU und -Fragmentierung auf dem 9800 WLC

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die MTU der RADIUS-Pakete konfiguriert wird, die der WLC an den RADIUS-Server sendet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit den folgenden Themen grundsätzlich vertraut sind:

- AAA-Konfiguration für den Wireless LAN Controller (WLC) 9800
- Authentication, Authorization and Accounting (AAA) RADIUS-Konzepte
- Extensible Authentication Protocol EAP
- Maximum Transmission Unit (MTU)

Verwendete Komponenten

- Cisco Identity Service Engineer (ISE) 3.2
- Catalyst Wireless Controller der Serie 9800 (Catalyst 9800-L)
- Cisco IOS® XE 17.15.2
- Windows 11 Wireless-Client

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrund

Für die Zwecke dieses Dokuments wird als RADIUS-Server (Remote Authentication Dial-In User Service) die Cisco ISE verwendet. Zunächst wird demonstriert, wie die Pakete während des EAP-Prozesses (Extensible Authentication Protocol) ohne einen Eingriff von außen fließen würden. Als Nächstes müssen Sie die Größe der Zugriffsanforderung ändern, die der WLC an einen beliebigen RADIUS-Server sendet. Diese Option wurde in IOS-XE Version 17.11 hinzugefügt.

9800 RADIUS-MTU

In der Regel spielt die MTU der RADIUS-Pakete keine Rolle, da sie in der Regel klein sind und die MTU-Größe nicht erreichen. Wenn jedoch eine Seite ein Zertifikat senden muss, das in der Regel 2-5 KB groß ist, muss das Gerät dieses Zertifikat fragmentieren, um es unter ihre MTU zu bekommen.

Wenn der Client ein Zertifikat an den RADIUS-Server senden muss, wie dies bei EAP Transport Layer Security (EAP-TLS) der Fall ist, führt dies dazu, dass der WLC aufgrund der Menge an RADIUS-Daten, die mit ihm gesendet werden müssen, erneut fragmentiert werden muss. Bis zum 17.11 hatte der Netzwerkadministrator wenig Kontrolle über diesen Prozess, aber jetzt haben die Techniker die Möglichkeit, die Größe der vom WLC gesendeten Zugriffsanfrage zu ändern.

EAP-TLS-Paketfluss

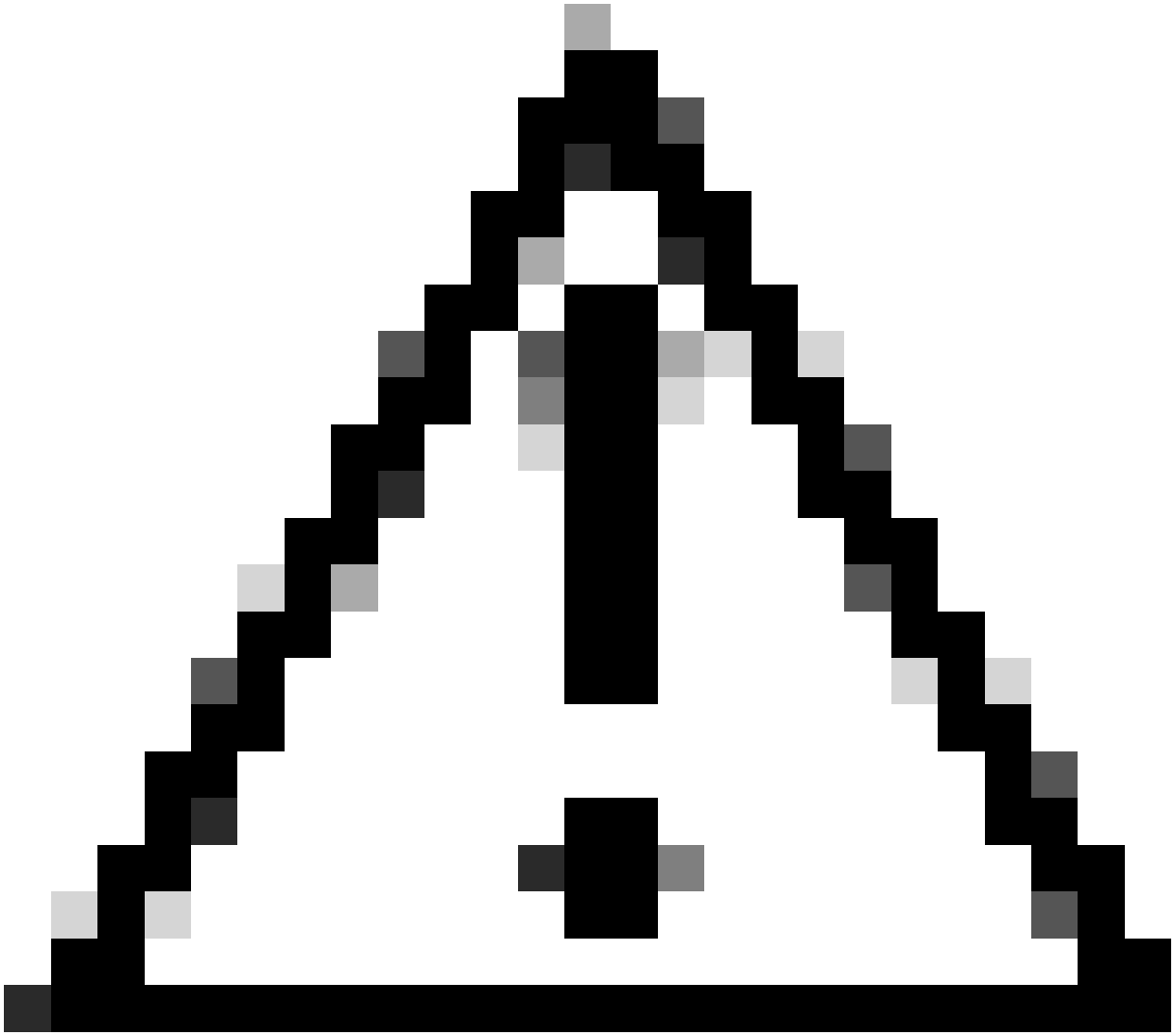
Auf diese Weise können wir das Aussehen von Paketen und ihre Behandlung durch die Wireless-Infrastruktur näher untersuchen. Damit die in diesem Dokument eingeführten Änderungen vollständig verstanden werden, ist es wichtig, den Paketfluss während des Wireless-Authentifizierungsprozesses bei Verwendung von dot1x und insbesondere von EAP-TLS zu

kennen.

Wenn Sie bereits genau wissen, wie der EAP- und RADIUS-Paketfluss in der Cisco Wireless-Infrastruktur funktioniert, fahren Sie mit dem Abschnitt über die Verhaltensänderung fort, in dem erläutert wird, was in 17.11 hinzugefügt wurde. So erhalten die Netzwerkadministratoren mehr Kontrolle über die RADIUS-MTU. Sehen Sie sich zunächst die EAP-ID (EAP-ID) an.

EAP-ID

Die EAP-ID wird vom Authentifikator, in diesem Fall dem WLC, initiiert. Dies muss der erste Teil des EAP-Prozesses sein. Manchmal sendet der Wireless-Client einen EAPOL-Start. Normalerweise bedeutet dies, dass der Client die EAP-ID-Anfrage nie erhalten hat oder einen Neustart durchführen möchte.



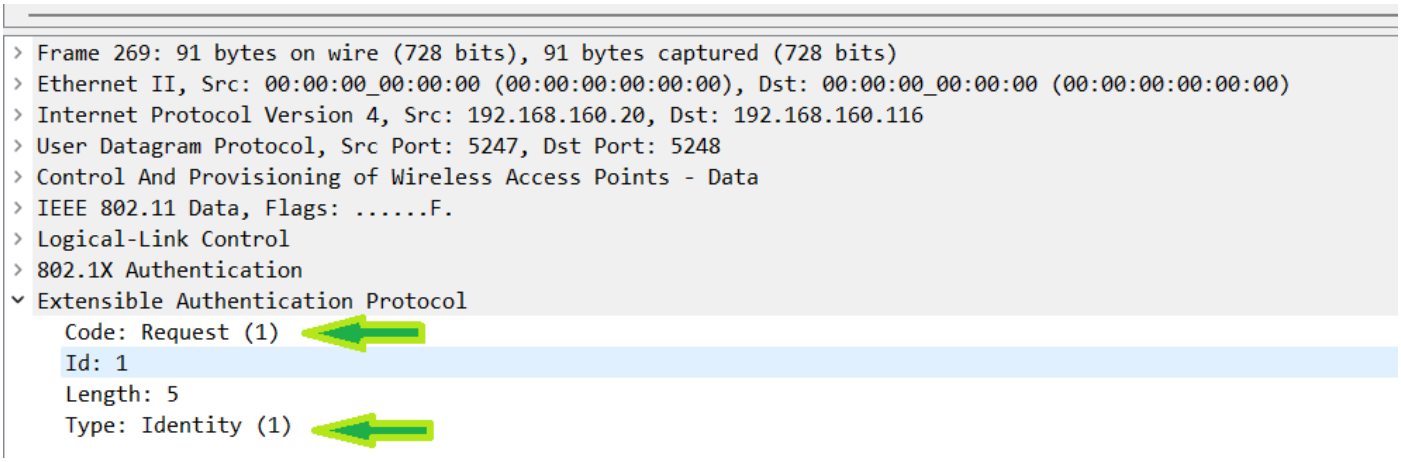
Vorsicht: Es besteht ein Unterschied zwischen dem EAP-ID-Paket und der EAP-Paket-ID. Das EAP-ID-Paket wird verwendet, um den Supplicant zu identifizieren, bei dem die EAP-Paket-ID eine Nummer ist, die verwendet wird, um das spezifische Paket zu verfolgen, während es sich durch das Netzwerk bewegt.

EAP-ID-Anforderung

Zunächst stellt das Wireless-Client-Gerät über den normalen Zuordnungsprozess eine Verbindung mit dem Netzwerk her. Wenn das Wireless Local Area Network (WLAN) für dot1x konfiguriert ist, muss der WLC zunächst wissen, wer der Client ist, bevor er Zugriff vom RADIUS-Server anfordern kann. Um diese Informationen zu finden, sendet der WLC die Client- und EAP-ID-Anforderung.

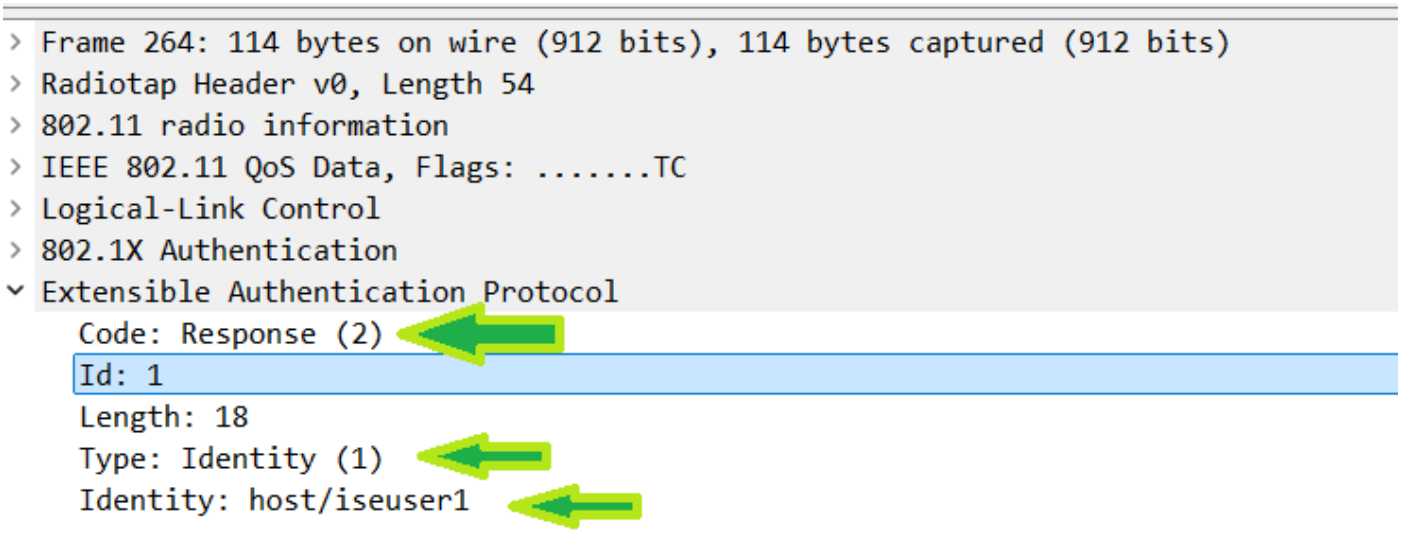
Es wird erwartet, dass der Client mit der EAP-ID-Antwort antwortet. Dadurch erhält der WLC die Informationen, die er benötigt, um die Zugriffsanfrage erstellen und an die ISE senden zu können. Die EAP-ID-Anfrage ist der Zeitpunkt, an dem der Client aufgefordert wird, seinen Benutzernamen und sein Passwort in eine normale PEAP-Authentifizierung einzugeben.

Da es sich hierbei jedoch um EAP-TLS handelt, hat die EAP-ID-Antwort hier nur die Benutzer-ID. In der Demo lautet die Benutzer-ID iseuser1. In diesem Paket können Sie die EAP-ID-Anforderung sehen, die der WLC an den Wireless-Client sendet und ihn fragt, wer er ist. Da es sich um einen Wireless-Client handelt, kapselt der WLC die Anforderung in CAPWAP und sendet sie zur Übertragung per Funk an den Access Point (AP). In den EAP-Daten gibt Code 1 an, dass es sich um eine Anforderung handelt, und Typ 1 bedeutet, dass es sich um eine Anforderung für die Identität handelt.



EAP-ID-Antwort

Als Nächstes wird erwartet, dass der Wireless-Client mit der EAP-ID-Antwort reagiert. In den EAP-Daten hat sich der Code in 2 geändert, was bedeutet, dass es sich um eine Antwort handelt, der Typ jedoch als 1 bleibt und weiterhin anzeigt, dass er für die Identität gilt. Hier sehen Sie sogar den Benutzernamen, den der Client verwendet. Bei diesen Paketen muss außerdem die ID-Nummer des EAP-Pakets überprüft werden. Für den EAP-ID-Austausch ist es immer 1, aber diese Zahl ändert sich später in etwas Anderes, sobald ISE beteiligt ist.



Sie können sehen, dass beide Pakete relativ klein sind, sodass die MTU hier keine Rolle spielt, da sie deutlich unter den 1500 Byte liegt, die im Netzwerk verwendet werden.

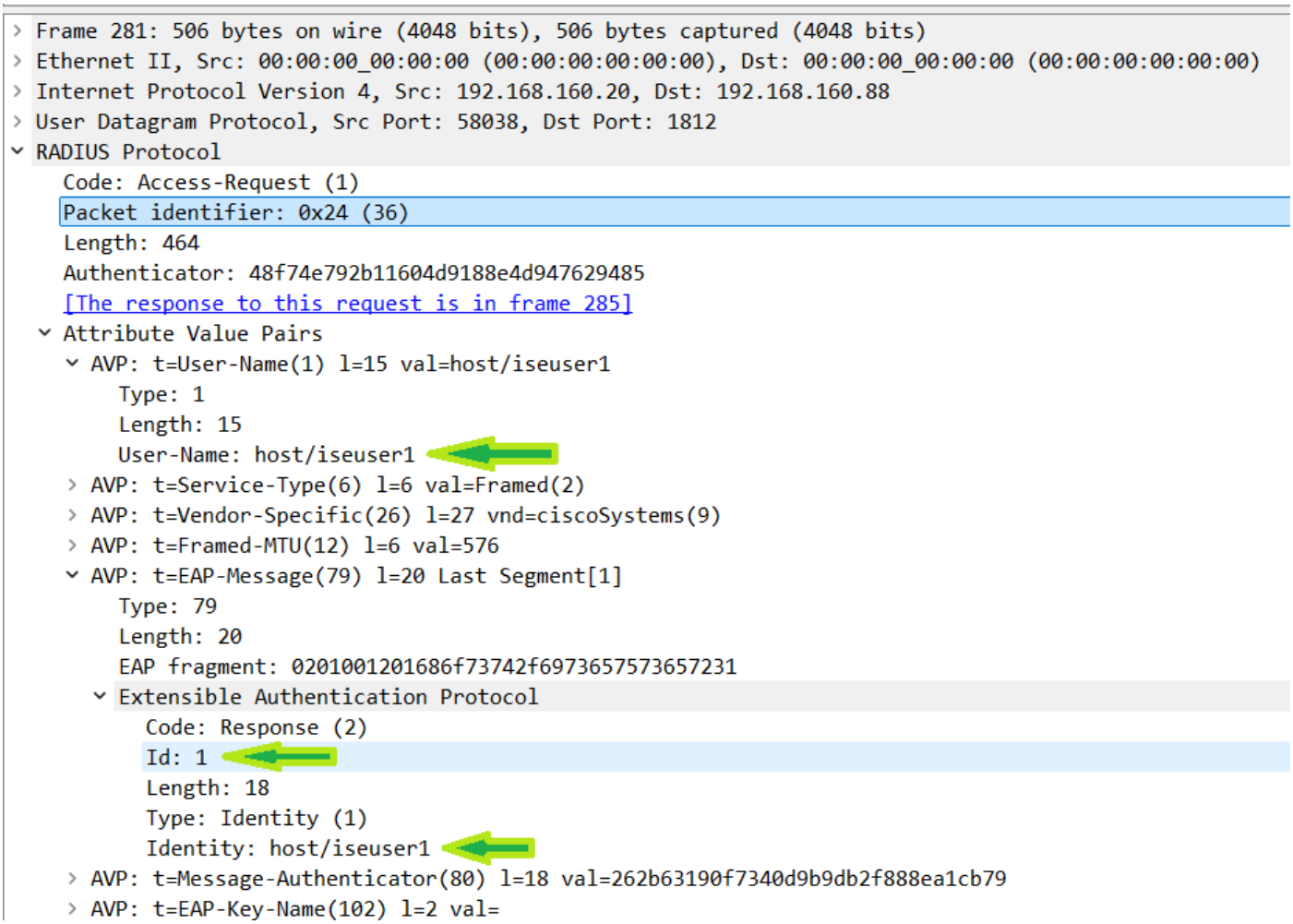
Access-Request und Access-Challenge

Die Kommunikation mit dem Client erfolgt über EAP, die Kommunikation zwischen dem WLC und der ISE über RADIUS. Für die RADIUS-Kommunikation werden die Access-Request- und Access-Challenge-Pakete verwendet. Der WLC empfängt das EAP-Paket vom Supplicant und leitet es über die RADIUS-Zugriffsanforderung an die ISE weiter. In einem funktionierenden Netzwerk reagierte die ISE mit einer Zugriffsherausforderung.

Zugriffsanfrage

Da der WLC nun die Identität des Clients kennt, muss er den RADIUS-Server fragen, ob dieser Client im Netzwerk zugelassen ist. Dazu fordert der WLC den Zugriff für diesen Client durch Senden des Access-Request-Pakets an. Es gibt weitere Daten, die der WLC zusammen mit den EAP-Daten senden wird. Diese werden zusammen als Attributwertpaare, AVPs oder AV-Paare bezeichnet, je nachdem, wer gerade spricht.

Dieses Dokument wird nicht weit in die AVPs eingehen, da dies außerhalb des Rahmens dieser Diskussion liegt. Hier müssen Sie nur sehen, dass der Benutzername (EAP-Daten) enthalten ist und an den RADIUS-Server, in diesem Fall die ISE, gesendet wird. Sie sehen auch, dass die EAP-ID Nummer 1 an die ISE gesendet wird. Denken Sie daran, dass die EAP-Paket-ID auf dem Funkweg dort ebenfalls 1 lautete. Der letzte wichtige Hinweis ist, dass, da der WLC alle diese AVPs hinzugefügt hat, das vom Client gesendete 114-Byte-Paket jetzt in ein 488-Byte-Paket umgewandelt wird, bevor es an die ISE gesendet wird.

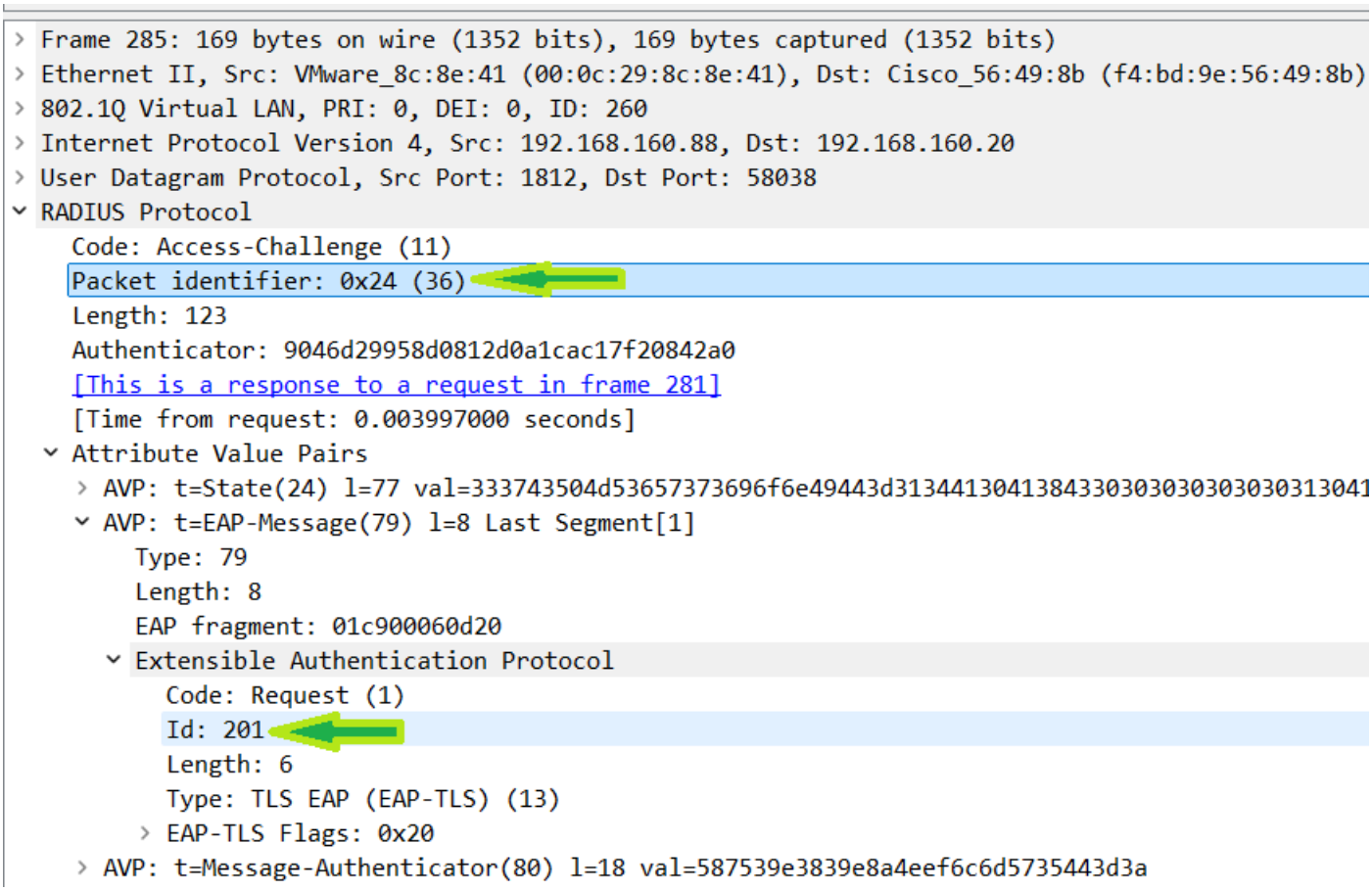


Herausforderung: Zugriff

Unter der Annahme, dass die ISE die Zugriffsanfrage erhält und beschließt, darauf zu reagieren, wird erwartet, dass diese Antwort von der ISE als Herausforderung für den Zugriff erkannt wird. Wenn Sie auf die Zugriffsanforderung zurückblicken, sehen Sie die RADIUS-Paket-ID 36, bevor die AVPs beginnen.

Wenn der WLC die Zugriffsanforderung empfängt, muss die RADIUS-ID mit der Paket-ID der Zugriffsanforderung übereinstimmen. Die RADIUS-Paket-ID ist für die RADIUS-Kommunikation zwischen der ISE und dem WLC bestimmt. Sie können in diesem Paket auch sehen, dass die ISE eine neue EAP-ID von 201 festgelegt hat, die zum Verfolgen der Kommunikation zwischen der ISE und dem Client verwendet wird. An dieser Stelle ist der WLC nur ein Pass-Through für die Kommunikation zwischen der ISE und dem Client.

Es ist wichtig, alle diese Paket-IDs hier zu notieren, damit Sie den Kommunikationsfluss verstehen und wissen, wie Sie diese Pakete über das Netzwerk verfolgen können. In einer Produktionsumgebung finden in der Regel mehrere Authentifizierungen gleichzeitig statt. Verwenden Sie den Befehl calling-station-id, um das Paket der MAC-Adresse des Clients zuzuordnen. Anschließend können Sie die RADIUS-Paket-ID und die EAP-Paket-ID verwenden, um den Paketfluss für diesen speziellen Client zu verfolgen. Bis jetzt hat keine der beiden Seiten Zertifikate gesendet, sodass die MTU-Größe weiterhin kein Problem darstellt.



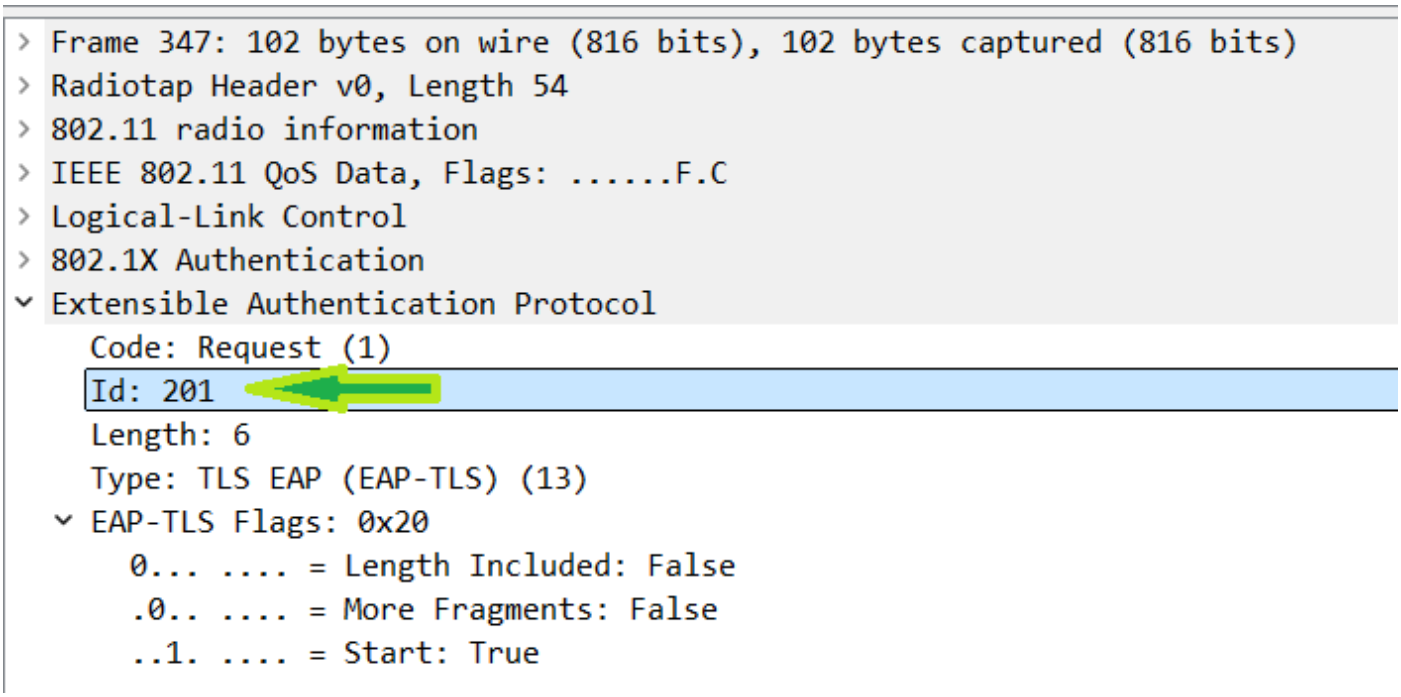
EAP-Anfrage und EAP-Antwort

Zur Erinnerung: Der Client spricht EAP, nicht RADIUS. Allerdings muss der WLC, wenn er die Access-Challenge erhält, die RADIUS-Daten entfernen und die EAP-Anfrage löschen, damit sie an den Client gesendet werden kann.

EAP-Anforderung

Dies muss genau so aussehen, wie es bei der Access-Challenge beim Empfang durch den WLC der Fall war. Alle RADIUS-Komponenten wurden jedoch entfernt, und nur der EAP-Teil wird an den Client gesendet.

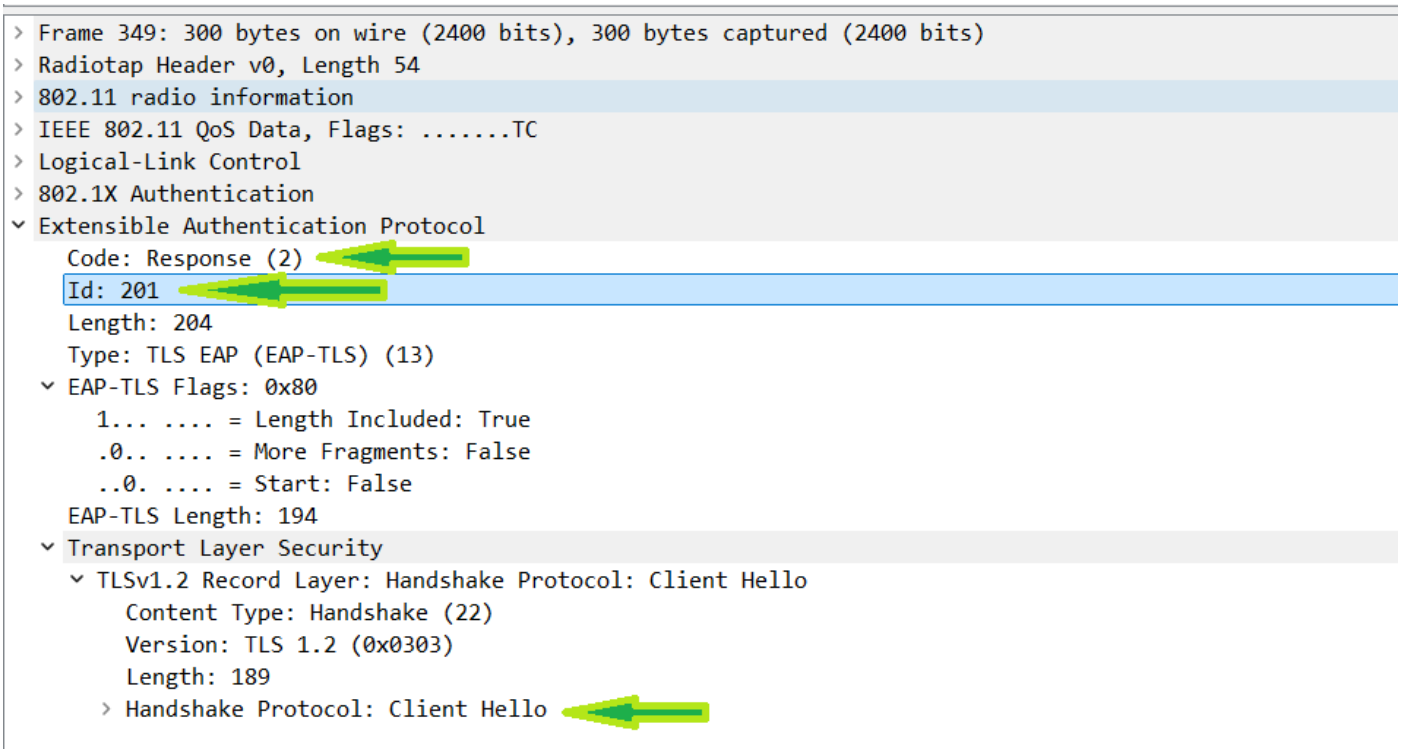
Die EAP-Paket-ID 201 sehen Sie hier genauso wie bei der Access-Challenge, da es sich um dieselben Daten handelt, die der WLC von der ISE erhalten hat. Der Ablauf ist hier der gleiche wie bei der EAP-ID, kommt aber jetzt nicht vom WLC und wird zur Erstellung der EAP-Methode verwendet. Dieses Paket ist noch ziemlich klein, da es nur den Start einer EAP-TLS-Sitzung festlegen soll.



EAP-Antwort

Wenn der Client die EAP-Anfrage empfängt, muss er mit einer EAP-Antwort antworten. In der EAP-Antwort beginnt der Client mit der Einrichtung der TLS-Sitzung. Dies entspricht in etwa dem Szenario, in dem TLS verwendet wird. Es beginnt mit der "client hello" Nachricht. In diesem Dokument wird nicht näher darauf eingegangen, was in die Begrüßung des Kunden einfließt, da es für dieses Thema irrelevant ist. Hier ist lediglich zu beachten, dass eine TLS-Sitzung eingerichtet wird.

Die Daten in den Paketen werden hier wie bei jeder anderen TLS-Konfiguration angezeigt. Wie bei der EAP-ID-Antwort trifft dieses Paket auf den WLC und wird in eine Zugriffsanfrage umgewandelt. Die ISE antwortet mit einer EAP-Anfrage, die als Access-Challenge verpackt ist. Das ist auch weiterhin der Fluss von jetzt an.



TLS-Zertifikate

An diesem Punkt wird die Paketgröße erhöht. Je nach Vorhandensein einer oder mehrerer zwischengeschalteter Zertifizierungsstellen können die Zertifikate relativ groß sein. Wenn es sich um ein selbstsigniertes Zertifikat handelt, wäre es natürlich kleiner als ein Zertifikat mit einem Gerätezertifikat, das mit zwei zwischengeschalteten Zertifizierungsstellen und einer Stamm-Zertifizierungsstelle verknüpft ist. In jedem Fall sehen Sie normalerweise, dass der Besitzer des Zertifikats hier seine eigenen Pakete fragmentiert.

ISE-Zertifikat

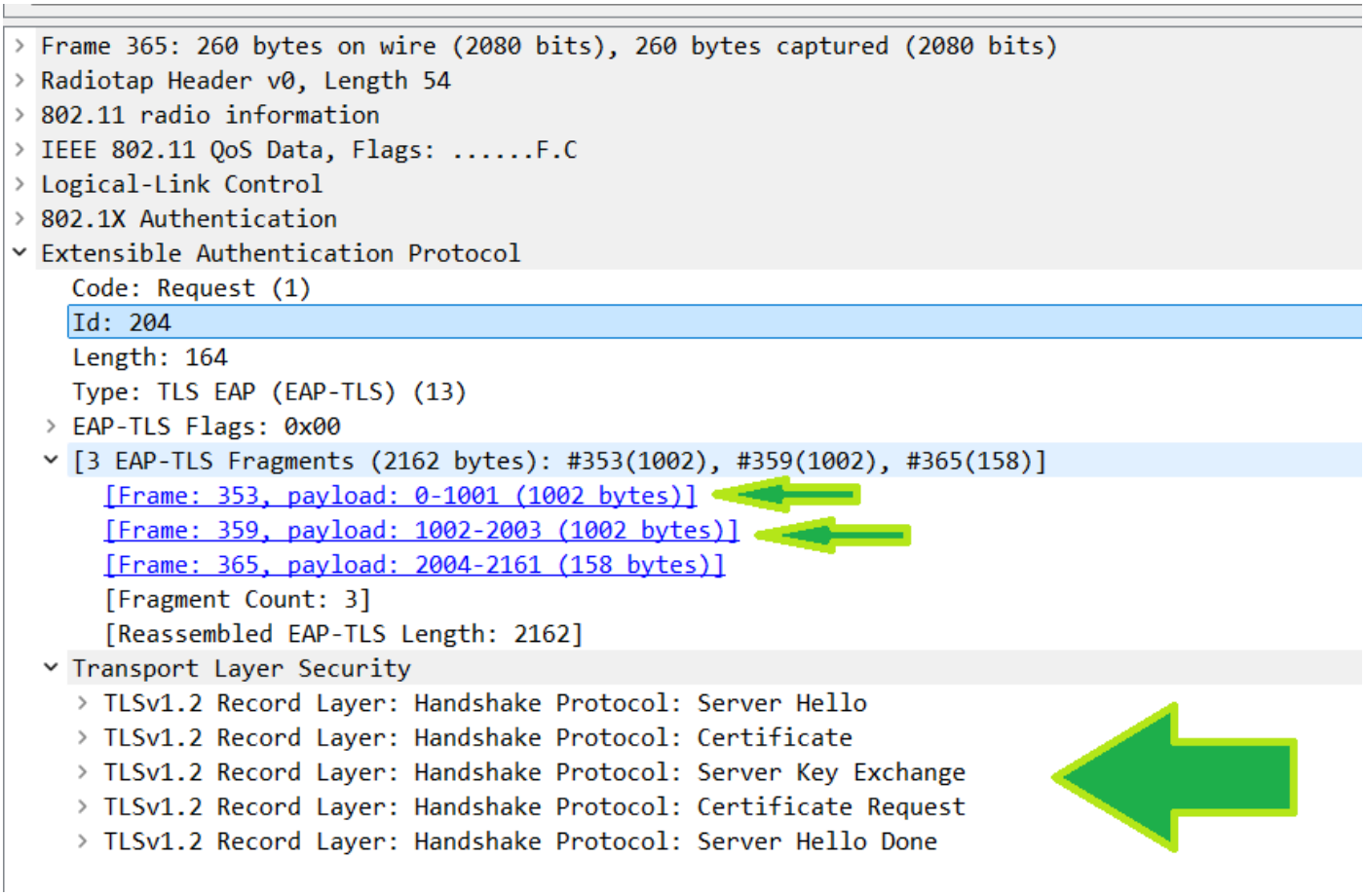
Nachdem die ISE den TLS-Client hello erhalten hat, antwortet sie mit einer weiteren EAP-Anforderung. In dieser neuen EAP-Anforderung sendet die ISE die "Server hello"-Nachricht, ihr Zertifikat, den "Server Key Exchange", die "Certificate Request" und die "Server hello done"-Nachricht auf einmal. Wenn diese Informationen in einem Paket gesendet werden, läuft das Paket über die MTU für das Netzwerk. Die ISE fragmentiert das Paket selbst, um es unter die MTU zu bringen. Bei der ISE wird der Datenteil des Pakets fragmentiert, sodass er nicht größer als 1002 Byte ist, um eine doppelte Fragmentierung zu vermeiden.

Was ist unter doppelter Fragmentierung zu verstehen? Die erste Fragmentierung findet auf der ISE statt, da die zu sendenden Daten zu groß sind, um in die MTU des Netzwerks zu passen. Es kann jedoch auch andere Stellen im Netzwerk geben, an denen ein Gerät das Paket fragmentieren muss, um seine Header hinzuzufügen und unter der MTU zu bleiben, obwohl die MTU gleich ist. Dies kann auch dann der Fall sein, wenn das Bit nicht fragmentieren aktiviert ist.

Ein gutes Beispiel hierfür ist ein VPN-Tunnel oder ein anderer Tunnel. Um Daten in einen VPN-Tunnel zu übertragen, müssen die VPN-Router ihre Header zum Datenverkehr hinzufügen. Wenn dieser RADIUS-Datenverkehr bei oder nahe der MTU fragmentiert wäre, gäbe es bei diesem VPN

keine Möglichkeit, die Daten unter der MTU zu halten und zusätzliche Header hinzuzufügen. Dies gilt auch für CAPWAP-Tunnel, die man etwas später sehen kann.

Damit diese Pakete nicht erneut fragmentiert werden, fragmentiert die ISE das Paket an einer Stelle, an der dies in den meisten Netzwerken vermieden werden kann. Das bedeutet, dass die ISE diese Daten in mehreren EAP-Anfragen sendet, die jedes Mal auf eine leere EAP-Antwort warten. Die EAP-ID wird mit jedem gesendeten Fragment erhöht. Aus der Sicht des WLC würde dies eine Zugriffs-Herausforderung und einen Zugriffsanforderungs-Austausch für jedes Fragment darstellen, und die RADIUS-Paket-ID würde mit jedem gesendeten Fragment zunehmen.



Client-Zertifikat

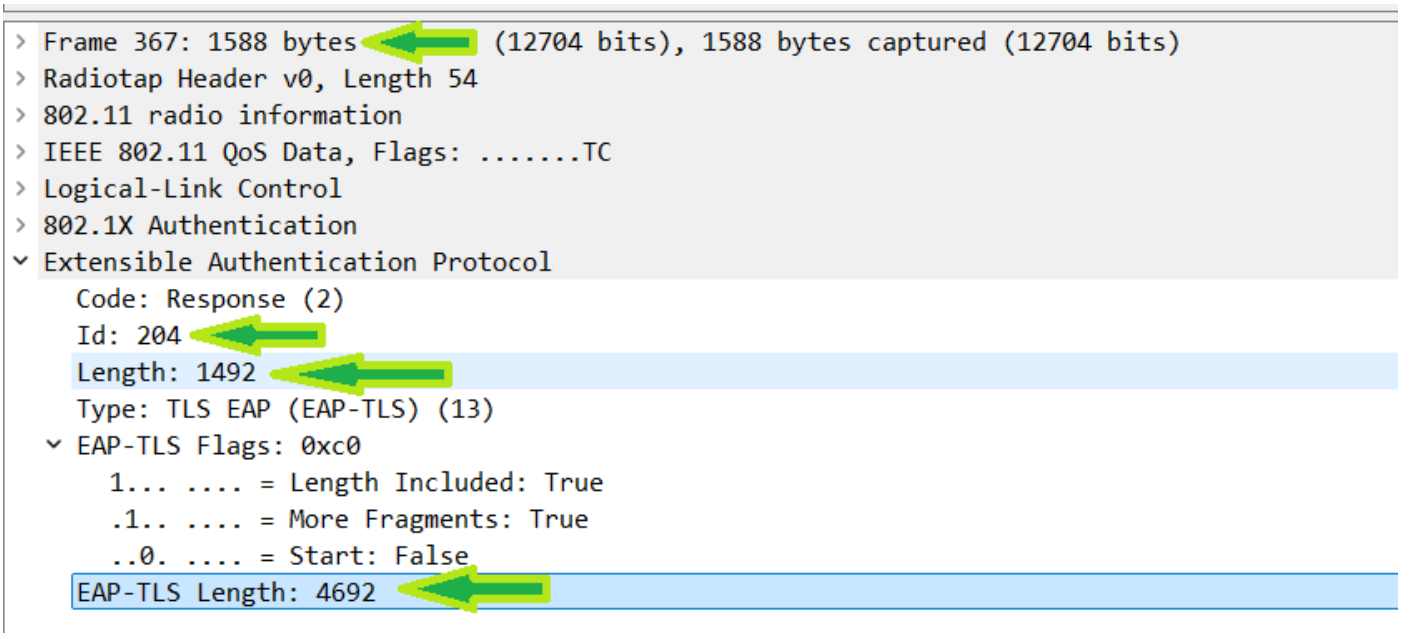
Sobald die ISE alle Fragmente sendet und sie vom Client wieder zusammengesetzt werden, wird der Paketfluss zum Client weitergeleitet, um etwas zu senden. Bei TLS wird erwartet, dass der Client an dieser Stelle ein eigenes Zertifikat sendet, um die Authentifizierung abzuschließen. An dieser Stelle werden die Dinge komplexer. Genau wie die ISE sendet der Client mehrere TLS-Komponenten gleichzeitig, von denen einer sein Zertifikat ist.

Anders als bei der ISE senden die meisten Clients ihre EAP-Daten knapp unter der MTU. In dieser Demo sind die 802.1x-Daten 1492. Das Problem dabei ist, dass der WAP die CAPWAP-Header hinzufügen muss, damit sie an den WLC gesendet werden können.

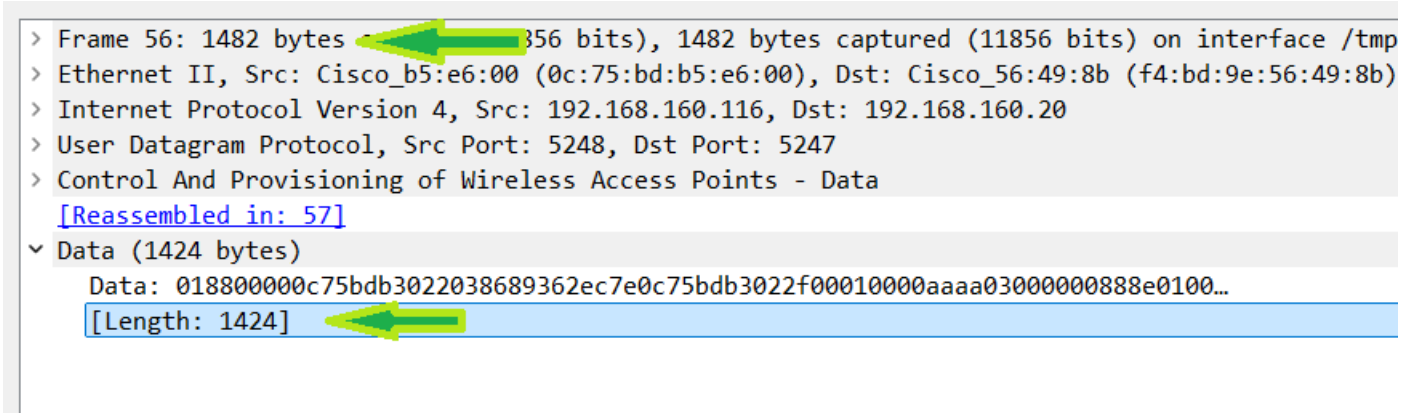
Wie soll das geschehen? Der WAP muss das Paket fragmentieren, damit er die Header hinzufügen und an den WLC senden kann. Der WAP kann das Paket nicht an den WLC abrufen,

ohne es zu fragmentieren. Das heißt, hier ist das Paket doppelt fragmentiert, zuerst vom Client, dann wieder vom AP. Diese Fragmentierung stellt jedoch in der Regel kein Problem dar, wie es bei CAPWAP erwartet wird.

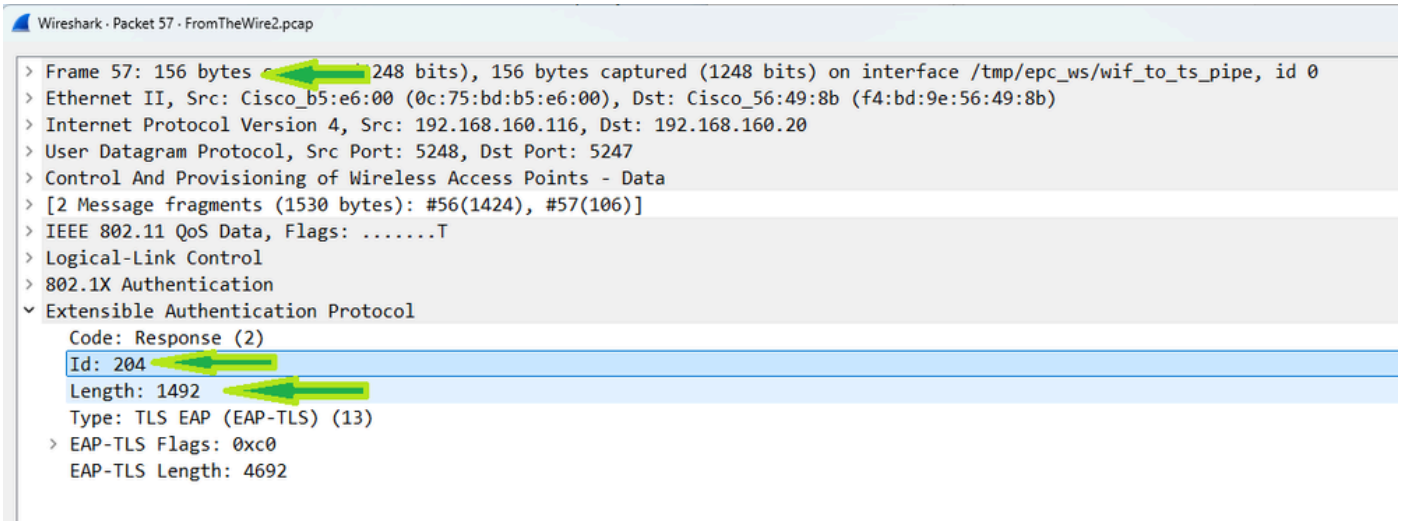
Das Paket über Funk:



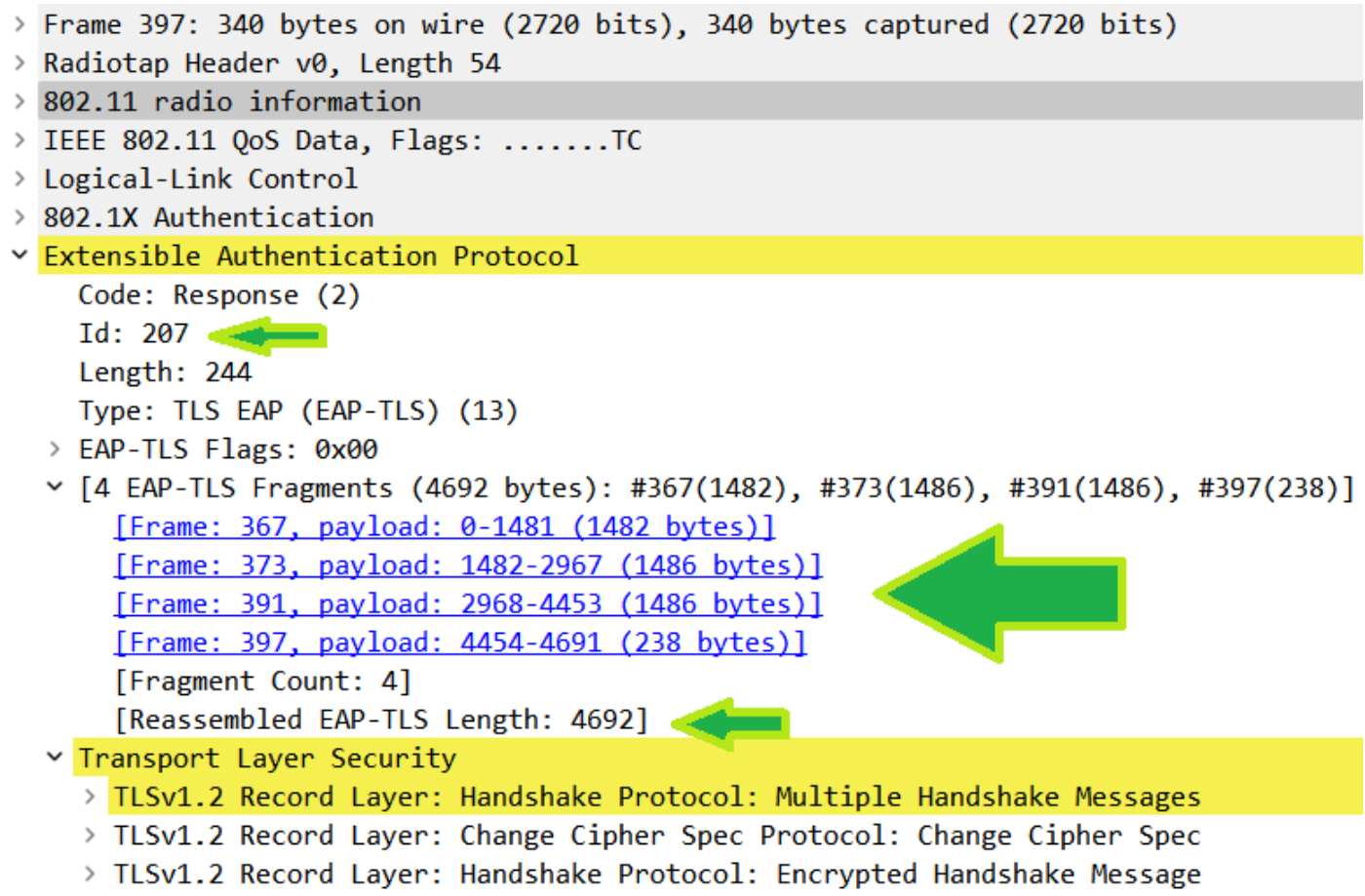
Das Paketfragment in der Leitung:



Das Paket wurde über den Draht wieder zusammengesetzt:



Alle Client-Fragmente werden per Funk reassembliert:



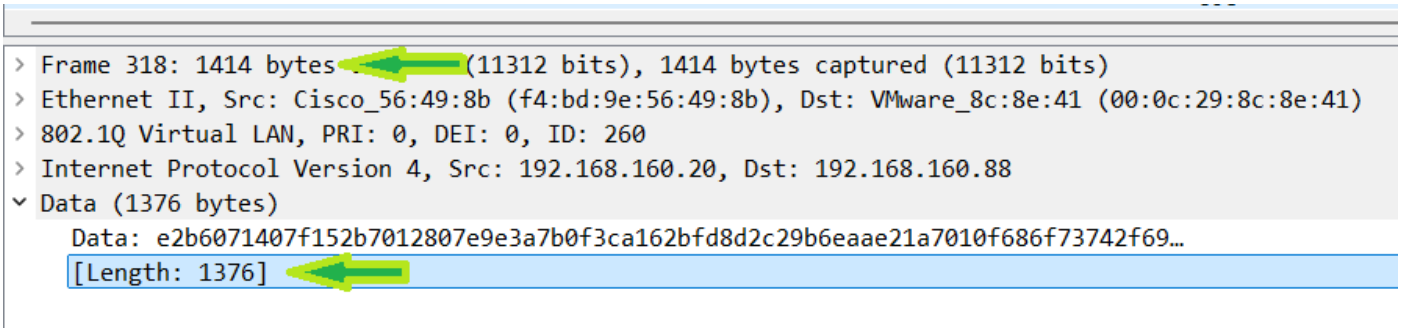
Client-Zertifikat am WLC

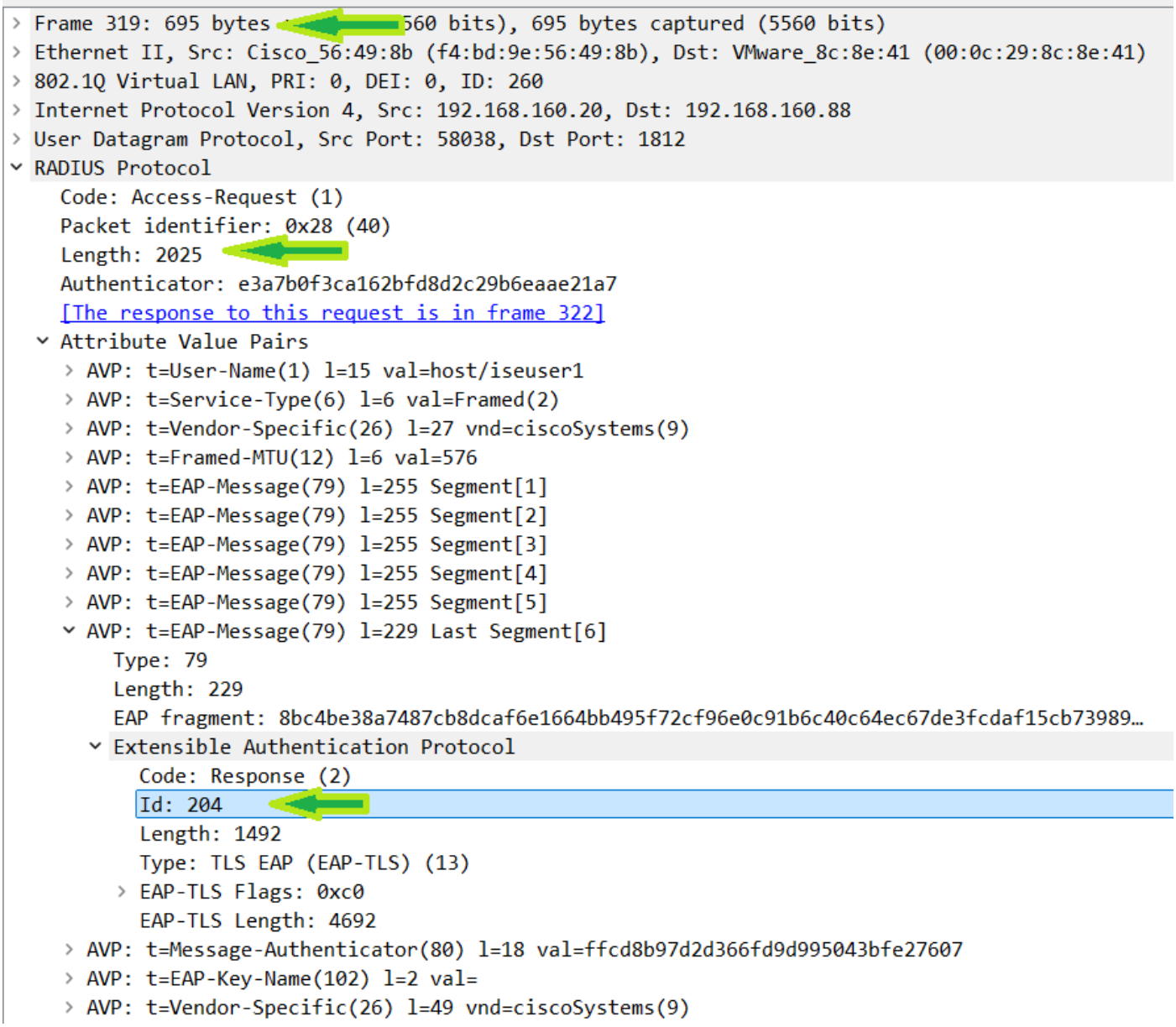
Der WLC empfängt die beiden CAPWAP-Fragmente und setzt sie wieder zusammen, um das gesamte 1492-Byte-Paket vom Client zu erhalten, wodurch das Paket wiederhergestellt wird - aber nicht lange. Diese Wiederherstellung ist von kurzer Dauer, denn wenn Sie darauf zurückblicken, wie der WLC die Zugriffsanfrage sendet, müssen Sie daran denken, dass er dem Paket RADIUS AVPs im Wert von etwa 400 Byte hinzufügen muss, bevor er die Daten an die ISE senden kann.

Rechnen Sie für einfache Berechnungen mit einem WLC, der 408 Byte hinzufügt, um die Gesamtpaketgröße auf 1900 zu erhöhen. Dieser Wert liegt deutlich über 1.500 MTU. Was wird der WLC also tun? Fragment Sie das Paket erneut.

An diesem Punkt fragmentiert der WLC das Paket standardmäßig mit 1396. Der Gedanke ist derselbe wie bei der ISE. Die Hoffnung besteht darin, das Paket so klein zu machen, dass es nicht erneut fragmentiert werden muss, um die Header hinzuzufügen, wenn es einen anderen Tunnel durchlaufen muss. Allerdings ist der WLC nicht so vorsichtig wie die ISE, daher ist 1396 hier gut genug.

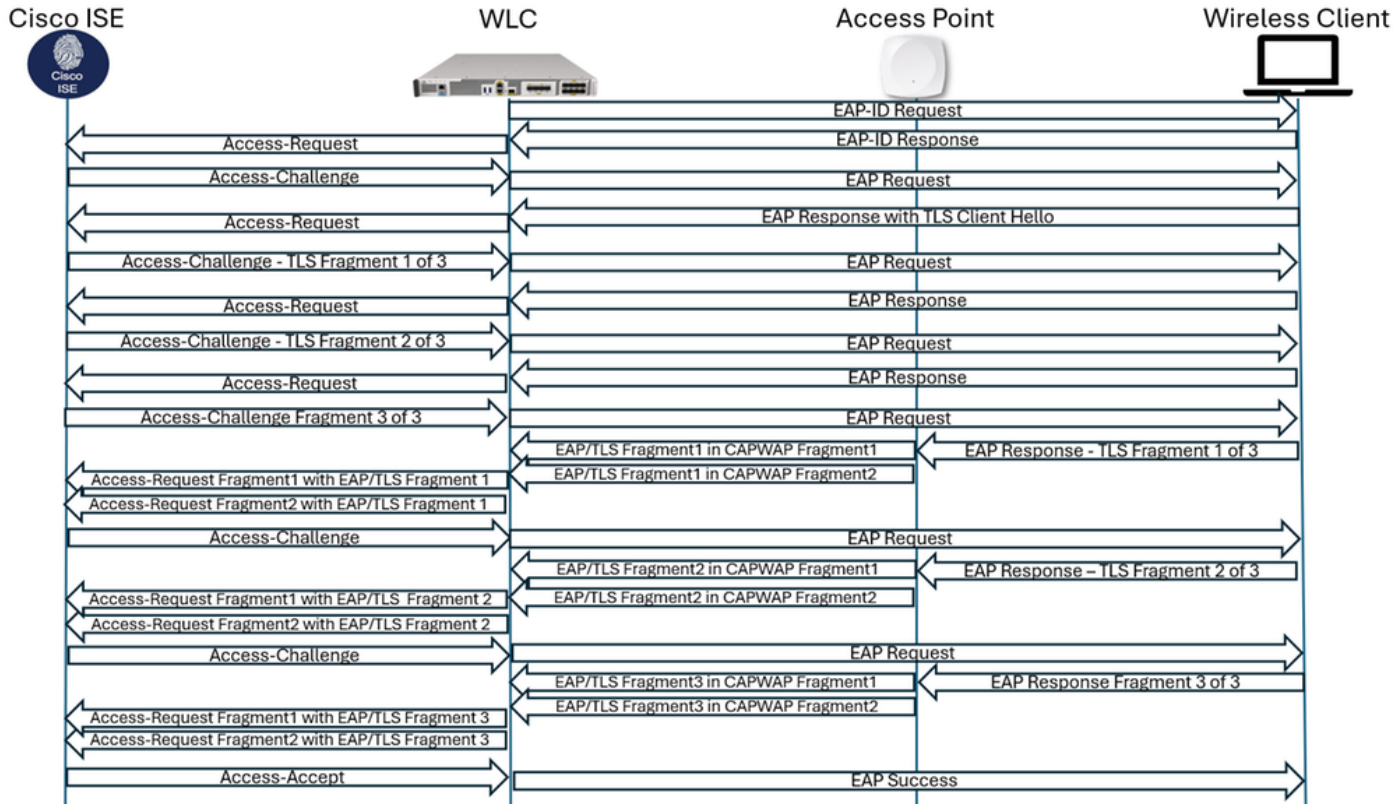
Das fragmentierte Paket verlässt den WLC:





Paketfluss TL;DR

Wenn die ISE ihr Zertifikat sendet, fragmentiert sie die TLS-Pakete mit 1002 Byte. Keine Probleme. Wenn die Clients ihr Zertifikat senden, fragmentieren sie in der Regel in der Nähe der MTU. Da der WAP die CAPWAP-Header dem Paket hinzufügen muss, muss auch dieses Paket fragmentiert werden. Sobald der WLc die Fragmente empfängt, muss er das Paket wieder zusammensetzen, aber dann die RADIUS AVPs hinzufügen, damit das Paket wieder fragmentiert wird. Der Paketfluss sieht in etwa wie folgt aus:



RADIUS-MTU - Verhaltensänderung

Wenn Sie sich den Paketfluss für den Datenverkehr der Wireless-Clients ansehen, sehen Sie, dass die Wireless-Infrastruktur nur an einigen Stellen Einfluss darauf hat. An erster Stelle steht, wenn der Datenverkehr den AP verlässt, und an zweiter Stelle, wenn der Datenverkehr den WLC verlässt. Eine Ausnahme bildet der TCP-Datenverkehr, bei dem die Wireless-Infrastruktur die Client-MSS anpassen kann. EAP fällt jedoch nicht unter TCP, sondern ist ein eigenes Protokoll.

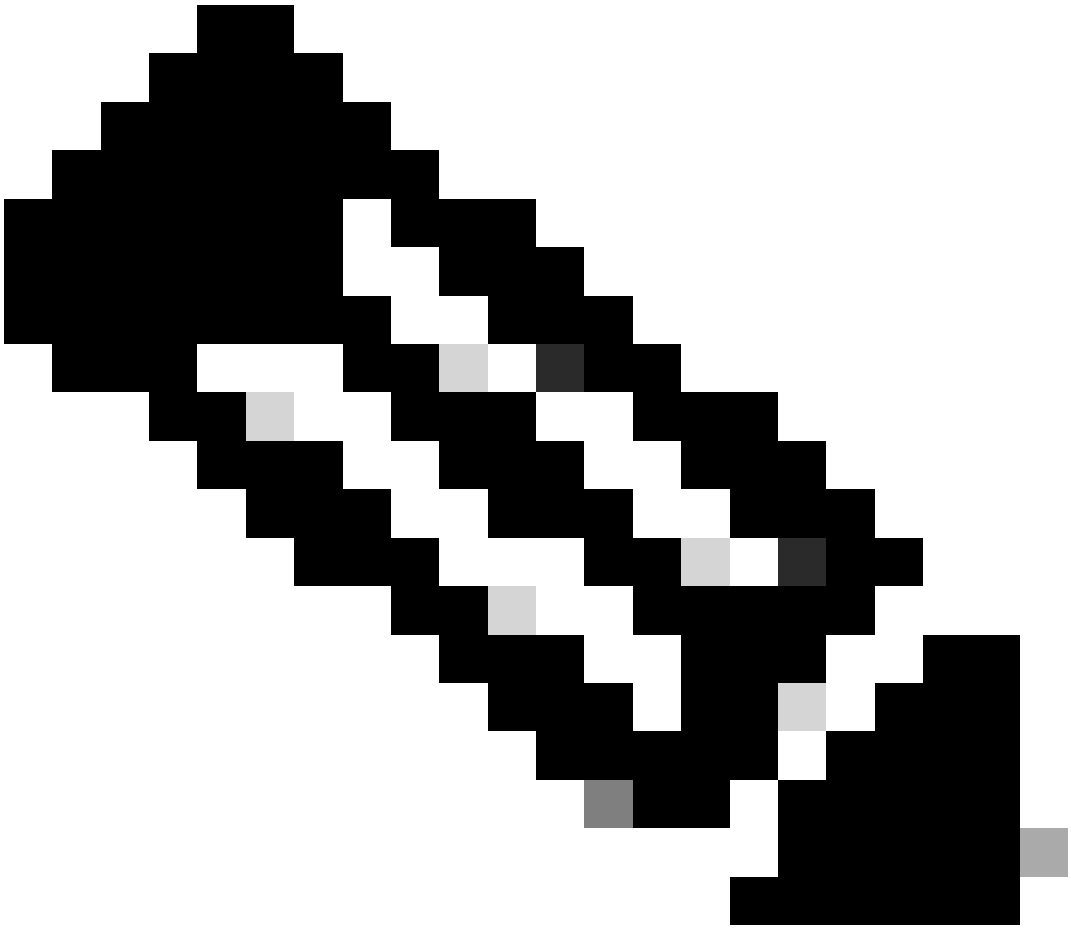
Wenn Sie sich die EAP- und RADIUS-Datenverkehrsflüsse anschauen, können Sie auch sehen, dass das Netzwerk tatsächlich die Datenverkehrsgröße sowohl am AP als auch am WLC beeinflusst, wenn die ursprüngliche Paketgröße zu nahe an die MTU herankommt. Wenn Sie die Rolle des WLC bei diesem Austausch richtig verstehen, können Sie sehen, dass es nur einen Ort gibt, an dem die Größe des RADIUS-Pakets beeinflusst wird. Dies ist der Fall, wenn eine EAP-Antwort eingeht und Sie sie in eine RADIUS-Zugriffsanforderung ändern.

Was hat sich geändert

Wenn die EAP-Antwort die MTU überschreitet, muss sie nach dem Hinzufügen der RADIUS AVPs fragmentiert werden. Da Sie dieses Paket bereits fragmentieren müssen, können Sie zumindest entscheiden, in welcher Größe Sie es fragmentieren möchten. An dieser Stelle kommt die in 17.11 eingeführte Verhaltensänderung ins Spiel.

In der Funktionsanforderung, die in der Cisco Bug-ID CSCwc81849 nachverfolgt wird, möchten Sie Unterstützung für RADIUS-Jumbo-Pakete hinzufügen. Dies wurde dadurch erreicht, dass das RADIUS-Paket bei 1396 nicht mehr automatisch fragmentiert wurde. Wenn Sie jetzt den Befehl ip radius source-interface <interface X> hinzufügen, wird die RADIUS-Zugriffsanforderung mit der

MTU dieser Schnittstelle gesendet.

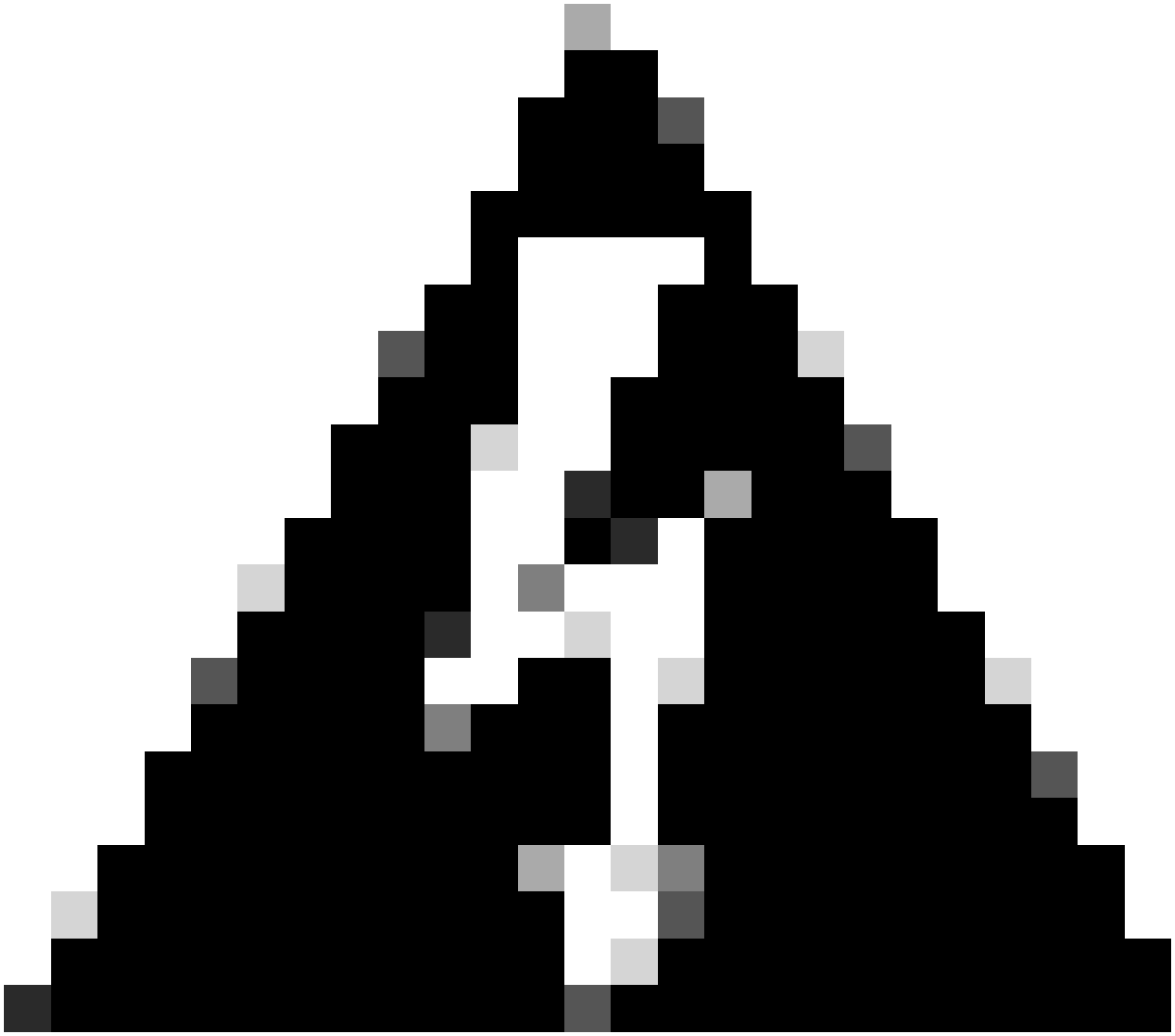


> Anmerkung: Wenn Sie Cisco Catalyst Center verwenden und AAA-Konfigurationen bereitstellen, wird der Servergruppe automatisch die Quellschnittstelle hinzugefügt. Dadurch wird das Standardverhalten so geändert, dass es bei der MTU-Größe der in diesem Befehl verwendeten Schnittstelle fragmentiert wird.

Wie kann diese Änderung verwendet werden?

Da die Standard-MTU aller Schnittstellen 1500 ist, würde dies die neue MTU für die Fragmentierung sein. Die Standardschnittstelle für den gesamten RADIUS-Datenverkehr ist die Wireless Management Interface (WMI). Wenn Sie die Konfiguration der Servergruppe betrachten und keine Quellschnittstelle angegeben ist, sendet der WLC den RADIUS-Datenverkehr unter 1396 mithilfe des WMI. Wenn Sie jedoch die Konfiguration der Servergruppe aufrufen und ihr mitteilen, dass die Quellschnittstelle die WMI ist, sendet der WLC jetzt den RADIUS-Datenverkehr mit der Nummer 1500, wobei die WMI weiterhin verwendet wird.

Nehmen wir nun an, es gibt ein Gerät im Netzwerk, wie das VPN zuvor beschrieben. Der Datenverkehr soll nicht doppelt fragmentiert werden, sodass Sie die MTU der Schnittstelle auf eine kleinere Größe ändern können, um die Pakete an einer anderen Stelle zu fragmentieren. Sie können die MTU-Größe auf etwa 1200 ändern, sodass die Pakete bei der 1200-Byte-Marke fragmentiert werden, anstatt bei 1500.

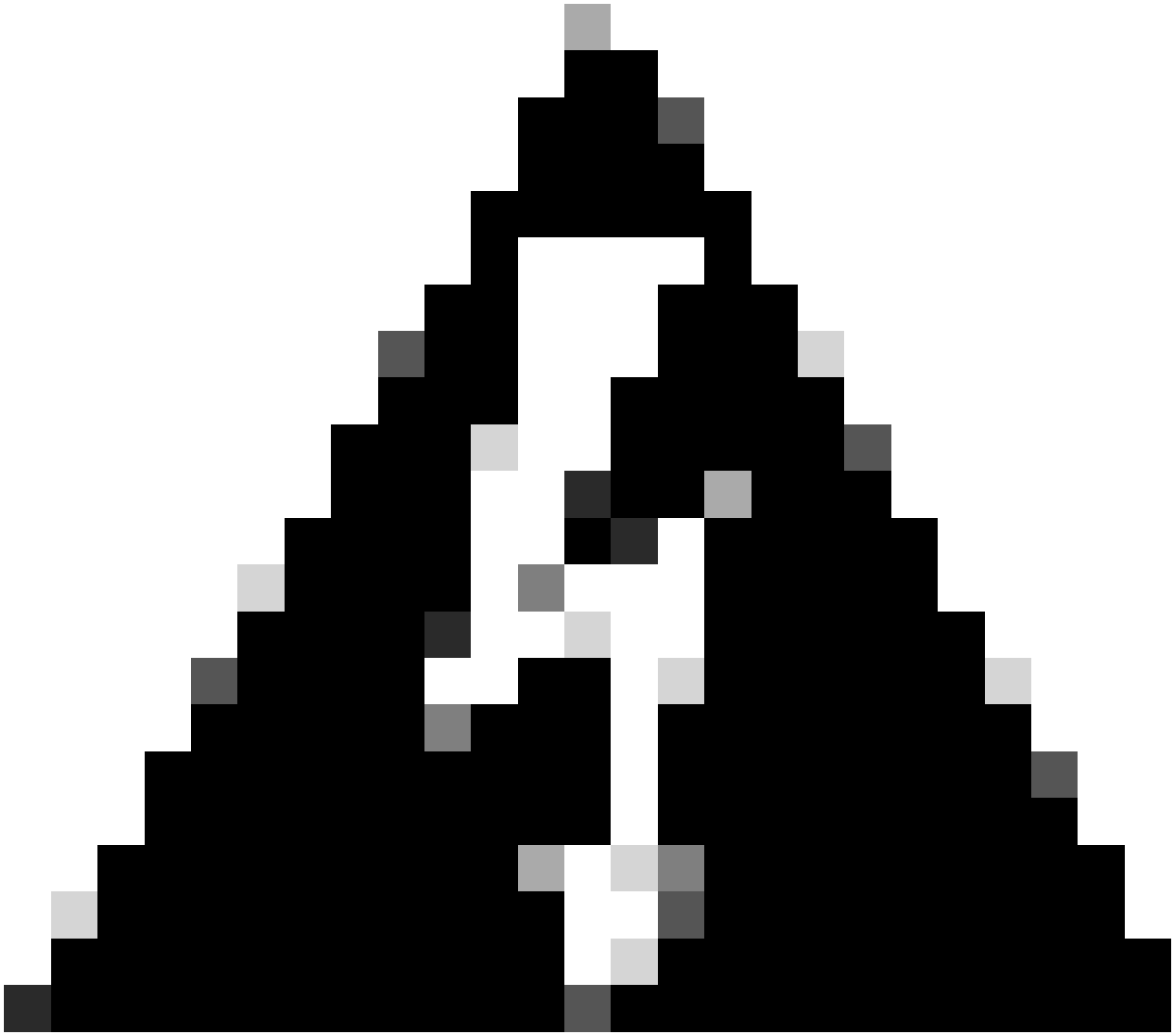


Warnung: Eine Änderung der MTU der WMI wirkt sich auf den gesamten Datenverkehr aus, der an die IP-Adresse der WLC-Verwaltung gesendet wird.

Auch wenn Sie die MTU der WMI nicht ändern möchten, ist der Punkt, an dem Sie eine Quellschnittstelle angeben, dass diese nicht die WMI-Schnittstelle ist, sondern eine andere Schnittstelle, und verwenden Sie diese Schnittstelle für den RADIUS-Datenverkehr sowie die MTU dieser Schnittstelle. Da diese Konfiguration auf Servergruppenebene vorgenommen wird, können Sie sehr genau festlegen, von welchem RADIUS-Datenverkehr diese Änderung betroffen sein soll.

Diese Konfiguration ist nicht an einen AAA-Server oder ein WLAN gebunden. Es ist möglich, mehrere Servergruppen mit denselben Servern zu verwenden und nur die Quellschnittstelle auf

einem von ihnen anzugeben, wenn Sie dies möchten. Diese Servergruppe wird einer Methodenliste hinzugefügt und dann einem WLAN hinzugefügt. Wenn es z. B. nur ein WLAN gibt, in dem diese Änderung vorgenommen werden soll, können Sie, auch wenn Sie nur einen AAA-Server haben, eine neue Servergruppe erstellen, den Befehl ip radius source-interface verwenden, der auf die Schnittstelle mit der gewünschten MTU verweist, den AAA-Server zu dieser neuen Gruppe hinzufügen, eine neue Methodenliste mit dieser neuen Gruppe erstellen und diese Methodenliste dann dem spezifischen WLAN hinzufügen, in dem dass diese Änderung vorgenommen wird.



Warnung: Es wird immer empfohlen, Änderungen an einem aktiven Netzwerk während eines Wartungsfensters vorzunehmen.

Der Beweis liegt in der Paketerfassung.

Es ist allgemein bekannt,Und wenn Sie das im Netzwerk nicht erfasst haben, können Sie es auch nicht beweisen. Nachfolgend finden Sie einige Konfigurationsbeispiele mit diesen

Änderungen, die zeigen, wie dies funktioniert.

Nachfolgend finden Sie eine WLAN-Konfiguration. Während des Tests wird nur die Servergruppe geändert, die in der Methodenliste verwendet wird.

```
9800#show run wlan
wlan TLS-Test 2 TLS-Test
 radio policy dot11 24ghz
 radio policy dot11 5ghz
 no security ft adaptive
 security dot1x authentication-list TLS-AuthC
 no shutdown
!
```

Hinzufügen des Befehls "source-interface" mit der Standard-MTU

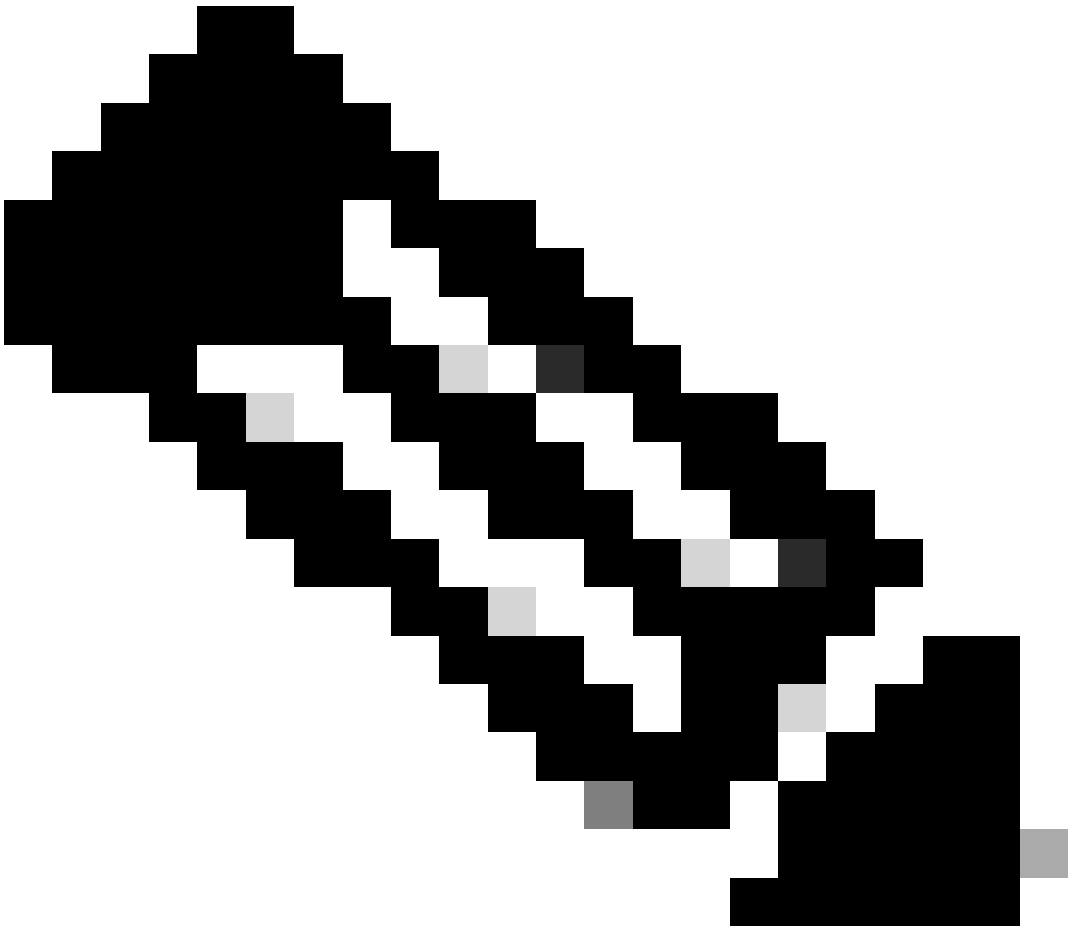
Hierbei handelt es sich lediglich um eine normale Servergruppe, die auf den ISE-Server verweist. Der Quellschnittstellenbefehl wurde hinzugefügt, der auf mein WMI zeigt, für das kein MTU festgelegt ist. So sieht die Konfiguration aus.

```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group NoMTU
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObF[^bPBVNaYibbBMhNMFAbKUAAB
!
aaa group server radius NoMTU
 server name ISE
 ip radius source-interface Vlan260
 deadtime 5
!
9800#show run inter vlan 260
!
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
 no ip proxy-arp
end
```

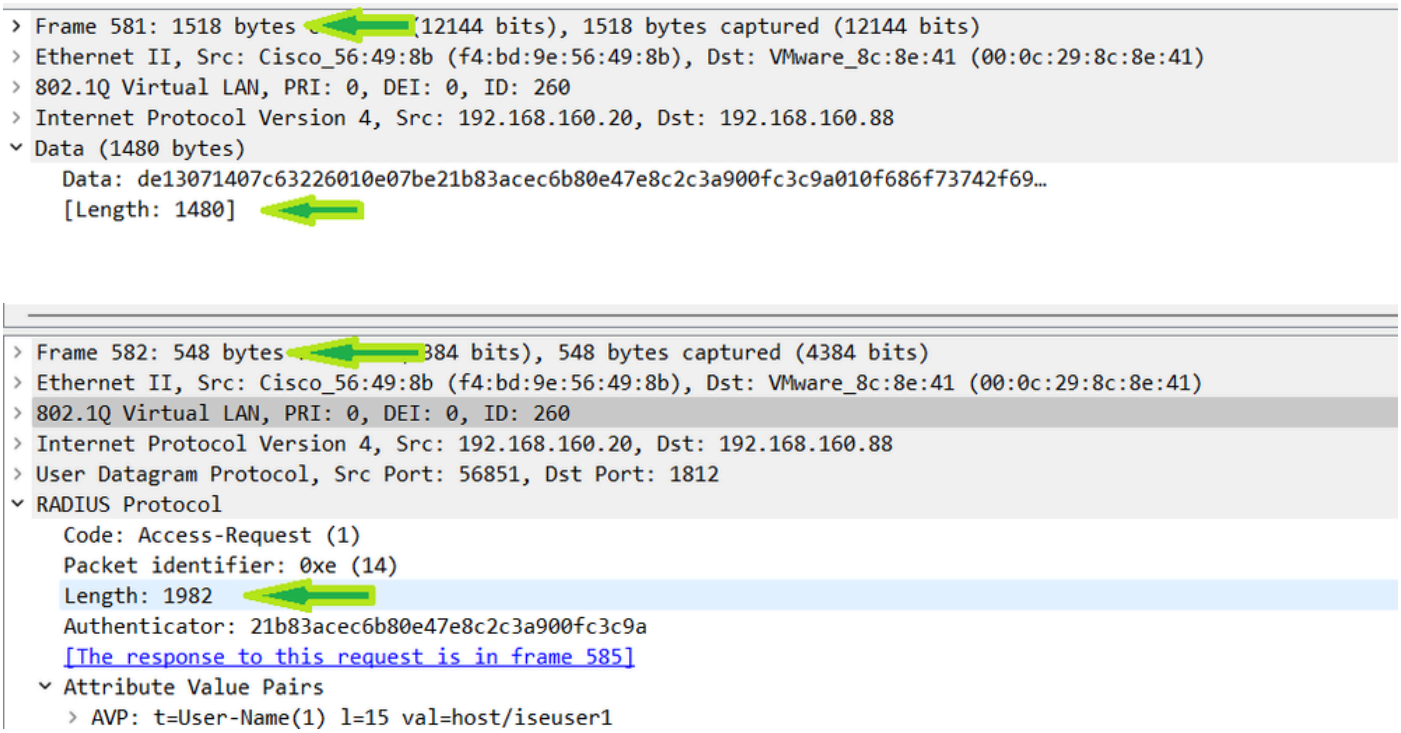
Wie Sie sehen, wurde die NoMTU-Servergruppe zur Liste der Authentifizierungsmethoden hinzugefügt, die mit dem WLAN verknüpft ist. Der Befehl ip radius source-interface VLAN260 wird für diese Servergruppe verwendet, und VLAN 260 gibt keine MTU an, d. h., es wird eine MTU von 1500 verwendet. Nur um zu bestätigen, die MTU von 1500 können Sie den Befehl show run all und suchen Sie nach der Schnittstelle in der Ausgabe.

```
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
 no ip clear-dont-fragment
 ip redirects
 ip unreachables
 no ip proxy-arp
 ip mtu 1500
```

Sehen Sie sich nun das Paket an, bei dem das Client-Zertifikat an die ISE gesendet werden muss, sobald der WLC die RADIUS-Daten hinzufügt:



Anmerkung: Hier sind die Bytes auf der Zeile 1518. Dies schließt Header außerhalb der Ethernet-Payload ein, wie den VLAN-Header und den Layer-2-Header. Diese werden nicht auf die MTU angerechnet.



Hier können Sie sehen, dass der Datenteil bei 1480 fragmentiert ist. Sie können dieses Fragment unter der 1500-MTU-Größe auf dem WMI abrufen. Das nächste Paket ist unter 550 Byte, aber Sie können sehen, dass die Gesamtgröße der RADIUS-Daten 1982 ist. Das heißt, die Fragmentierung mit der neuen MTU funktioniert jetzt.

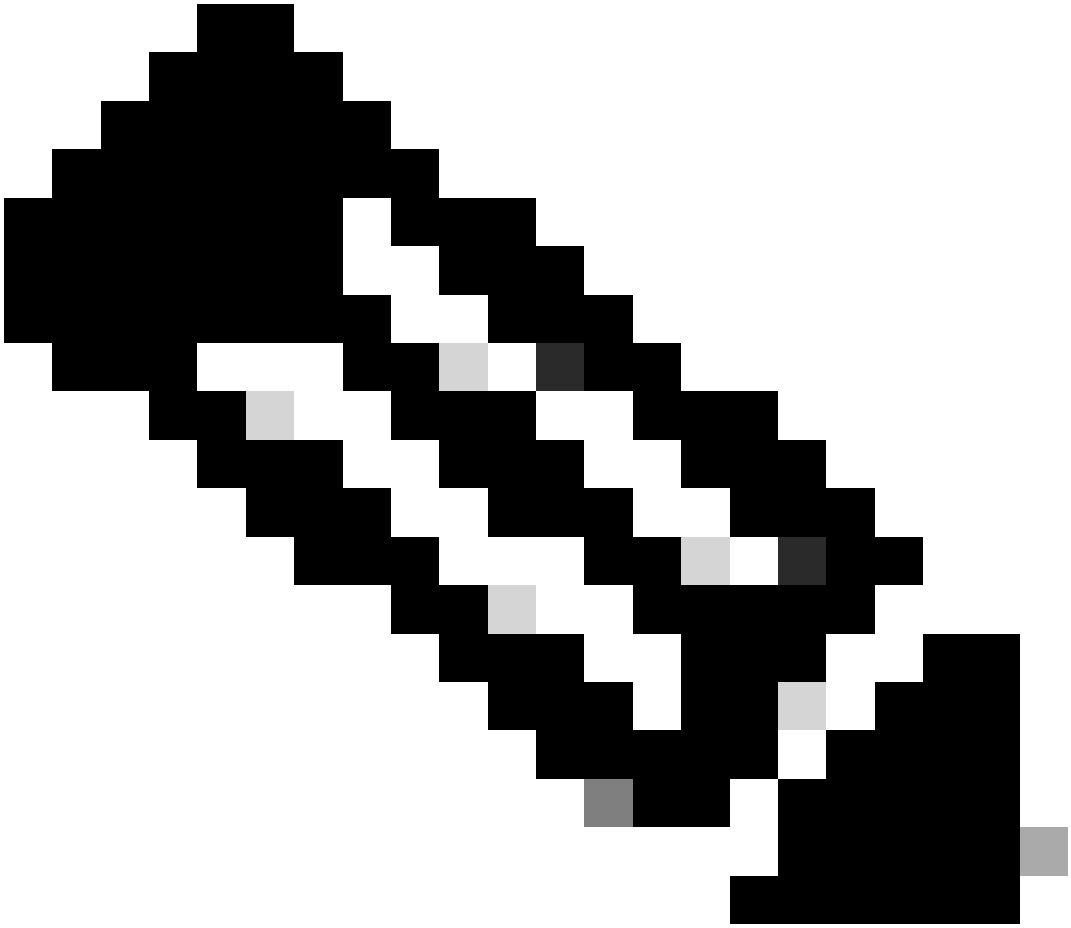
Verwenden einer Nicht-WMI-Schnittstelle mit einer MTU von 1200

Nehmen wir nun an, Sie möchten mit einer kleineren MTU fragmentieren, aber nicht, dass sich diese Änderung auf anderen Datenverkehr auswirkt. Kein Problem, die Konfiguration bleibt die gleiche, nur die Quellschnittstellenkonfiguration verweist auf eine SVI, die nur zu diesem Zweck erstellt wurde. Ändern Sie die Methodenliste so, dass sie auf diese neue Servergruppe verweist, und diese Servergruppe verwendet eine Quellschnittstelle, die nicht mein WMI ist und für die die MTU auf 1200 festgelegt ist. So sieht die Konfiguration aus:

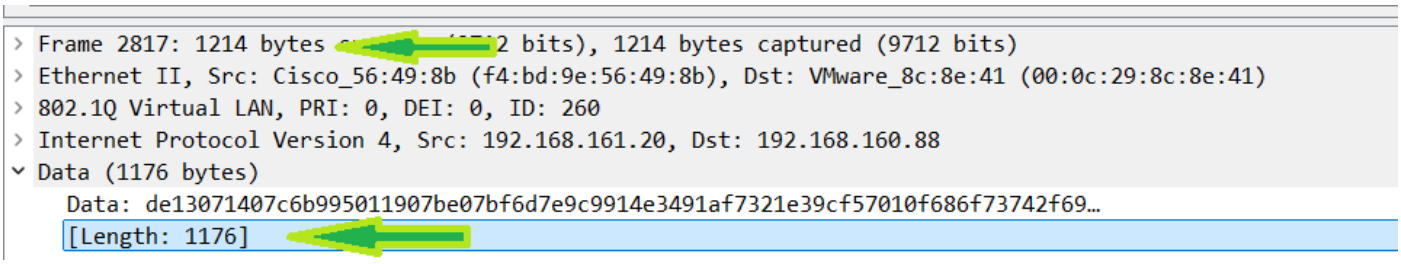
```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group MTU1200
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObFibbBMhNMFAbKUAAB
!
aaa group server radius MTU1200
 server name ISE
 ip radius source-interface Vlan261
 deadtime 5
!
9800#show run inter vlan 261
!
interface Vlan261
```

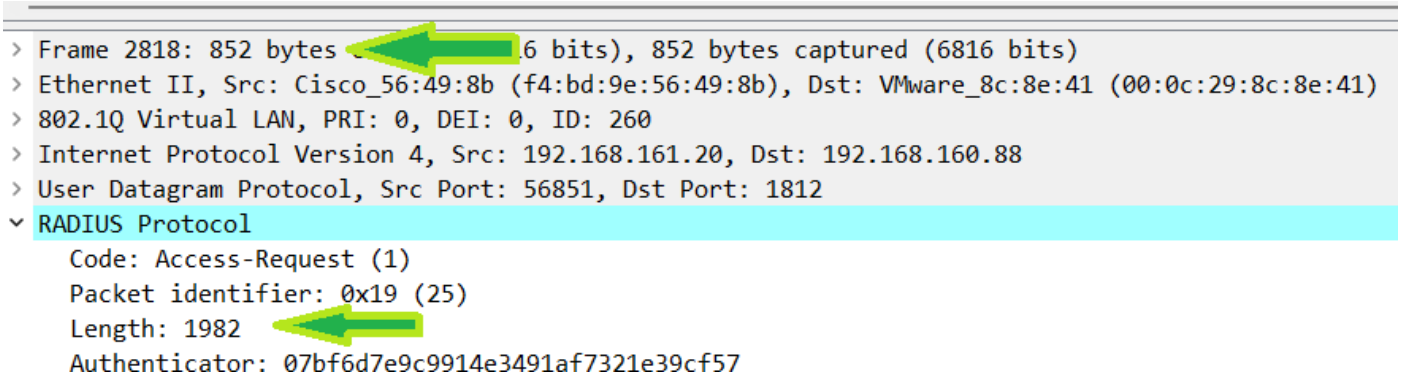
```
 ip address 192.168.161.20 255.255.255.0
 no ip proxy-arp
 ip mtu 1200
end
```

Sehen wir uns nun an, wie die Pakete mit dieser niedrigeren MTU aussehen.



Anmerkung: Die Senkung der MTU und die Änderung des Fragmentierungspunkts sind nicht Teil des neuen Verhaltens. Das war schon immer so. Wenn das Standardverhalten der Fragmentierung bei 1396 nicht unter die MTU passt, würden Sie immer an einem anderen Punkt fragmentieren. Es ist Teil dieses Abschnitts, nur um die verfügbaren Optionen zu erläutern.





Hier sind die RADIUS-Daten noch 1982 Byte groß, aber diesmal waren die Daten bei 1176 fragmentiert anstatt bei 1376, wenn die Quellschnittstelle nicht verwendet würde. Denken Sie daran, dass Sie bei 1480 fragmentieren, wenn Sie die MTU auf 1500 setzen und den Befehl source-interface verwenden. Mit der hier gezeigten Konfiguration kann der Datenverkehr auf eine niedrigere MTU geändert werden, ohne den Datenverkehr auf dem WLC zu beeinträchtigen.

Verwenden einer MTU von 9000 für Jumbo-Frames

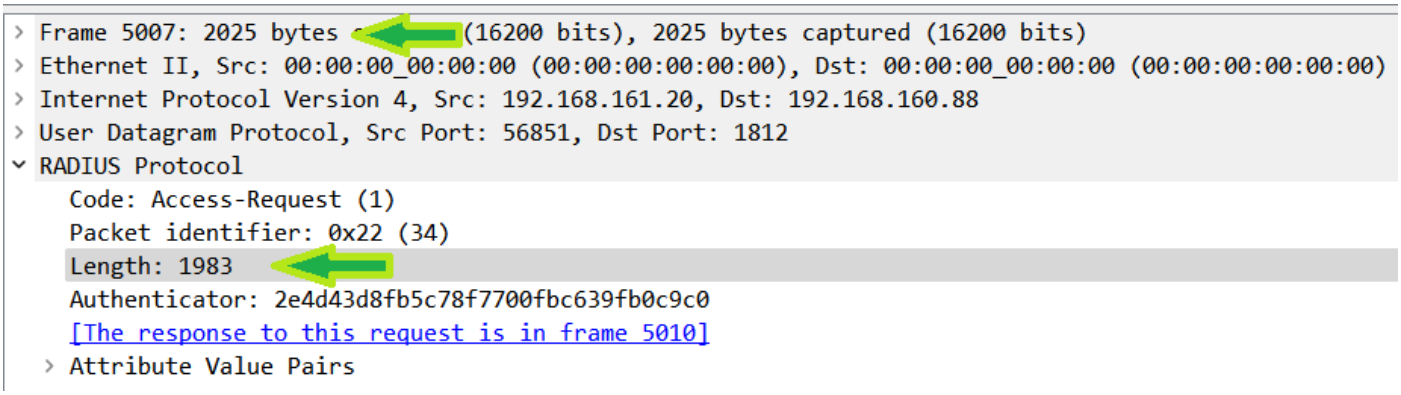
Da die Funktion für die Option zum Senden von Jumbo-Frames bereitgestellt wurde, wäre es bedauerlich, dies nicht auch noch mit der Nicht-WMI-Schnittstelle von VLAN 261 zu testen. Nun ist die IP-MTU jedoch auf 9000 festgelegt. Eine kurze Anmerkung: Um die IP-MTU auf der SVI einstellen zu können, muss die MTU auf einen Wert höher als die IP-MTU eingestellt werden. Sie können dies in dieser Konfiguration sehen:

```
9800(config-if)#do sho run inter vl 261
!
interface Vlan261
 mtu 9100
 ip address 192.168.161.20 255.255.255.0
 no ip proxy-arp
 ip mtu 9000
end
```

Wenn Sie sich die Aufzeichnung ansehen, sehen Sie, dass das Paket nie fragmentiert wurde. Es wurde als ein ganzes Paket mit der RADIUS-Datengröße von 1983 gesendet. Damit dies funktioniert, muss das übrige Netzwerk so konfiguriert werden, dass ein Paket dieser Größe durchgelassen wird.

Beachten Sie auch, dass sich die Client-MTU nicht geändert hat, sodass der Client das EAP-

Paket bei 1492 immer noch fragmentiert. Der Unterschied besteht darin, dass der WLC alle für das Senden des Pakets an die ISE erforderlichen RADIUS-Daten hinzufügen kann, ohne die Client-Daten fragmentieren zu müssen.



Schlussfolgerung

Wenn Sie EAP-TLS verwenden, wird vom Client erwartet, dass er sein Zertifikat an den AAA-Server sendet. Diese Zertifikate sind in der Regel größer als die MTU, sodass der Client sie fragmentieren muss. Der Punkt, an dem der Client die Daten fragmentiert, liegt ziemlich nahe an der MTU. Da der WAP den CAPWAP-Header hinzufügen muss, muss das, was der Client sendet, fragmentiert werden. Der WLC empfängt diese beiden Pakete und setzt sie wieder zusammen. Anschließend muss er sie jedoch erneut fragmentieren, um die RADIUS-Daten hinzuzufügen. An diesem Punkt erhält der Netzwerkadministrator eine gewisse Kontrolle darüber, wie der WLC das vom Client gesendete EAP-Paket fragmentiert.

Wenn Sie den Befehl ip radius source-interface <Schnittstelle, die Sie verwenden möchten> zur AAA-Servergruppe hinzufügen, verwendet der WLC die Schnittstelle, die Sie dort platziert haben, anstelle des WMI (oder einschließlich). Mit diesem Befehl wird der WLC außerdem angewiesen, mit einer MTU zu fragmentieren, die nicht der Standardeinstellung von 1396 entspricht. Auf diese Weise haben Sie mehr Kontrolle darüber, wie Pakete das Netzwerk durchlaufen.

Bei Verwendung von Cisco Catalyst Center wird der Server-Gruppe der Befehl source interface hinzugefügt, wodurch das Standardverhalten geändert wird.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.