Entender o RADIUS MTU e a fragmentação no 9800 WLC

Contents

Introdução

Este documento descreve como configurar a MTU dos pacotes RADIUS que a WLC envia ao servidor RADIUS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha uma compreensão básica destes tópicos:

- Configuração de AAA da controladora Wireless LAN (WLC) 9800
- Conceitos de Autenticação, Autorização e Contabilização (AAA - Authentication, Authorization and Accounting) RADIUS
- Protocolo de autenticação extensível EAP
- Unidade máxima de transmissão (MTU)

Componentes Utilizados

- Cisco Identity Service Engineer (ISE) 3.2
- Catalyst 9800 Wireless Controller Series (Catalyst 9800-L)
- Cisco IOS® XE 17.15.2
- Cliente sem fio do Windows 11

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Background

Para os fins deste documento, o servidor Remote Authentication Dial-In User Service (RADIUS) usado é o Cisco ISE. Primeiro, é demonstrado como os pacotes fluiriam sem qualquer intervenção externa durante o processo do protocolo de autenticação extensível (EAP). A seguir está a opção de configuração para alterar o tamanho da solicitação de acesso que a WLC envia a qualquer servidor RADIUS. Essa opção foi adicionada no IOS-XE versão 17.11.

9800 RADIUS MTU

Geralmente, o MTU dos pacotes RADIUS não importa, pois eles são geralmente pequenos e não atingem o MTU mesmo assim. No entanto, quando um lado precisa enviar um certificado, que geralmente tem de 2 a 5 KB, o dispositivo precisa fragmentar esse certificado para obtê-lo sob sua MTU.

Quando o cliente precisa enviar um certificado ao servidor RADIUS, como é o caso do EAP Transport Layer Security (EAP-TLS), ele apresenta à WLC uma situação em que o pacote precisa ser fragmentado novamente devido à quantidade de dados RADIUS que precisa ser enviada com ele. Até 17.11, o administrador de rede tinha pouco controle sobre esse processo, mas agora os engenheiros têm a opção de manipular o tamanho da solicitação de acesso enviada pela WLC.

Fluxo de pacote EAP-TLS

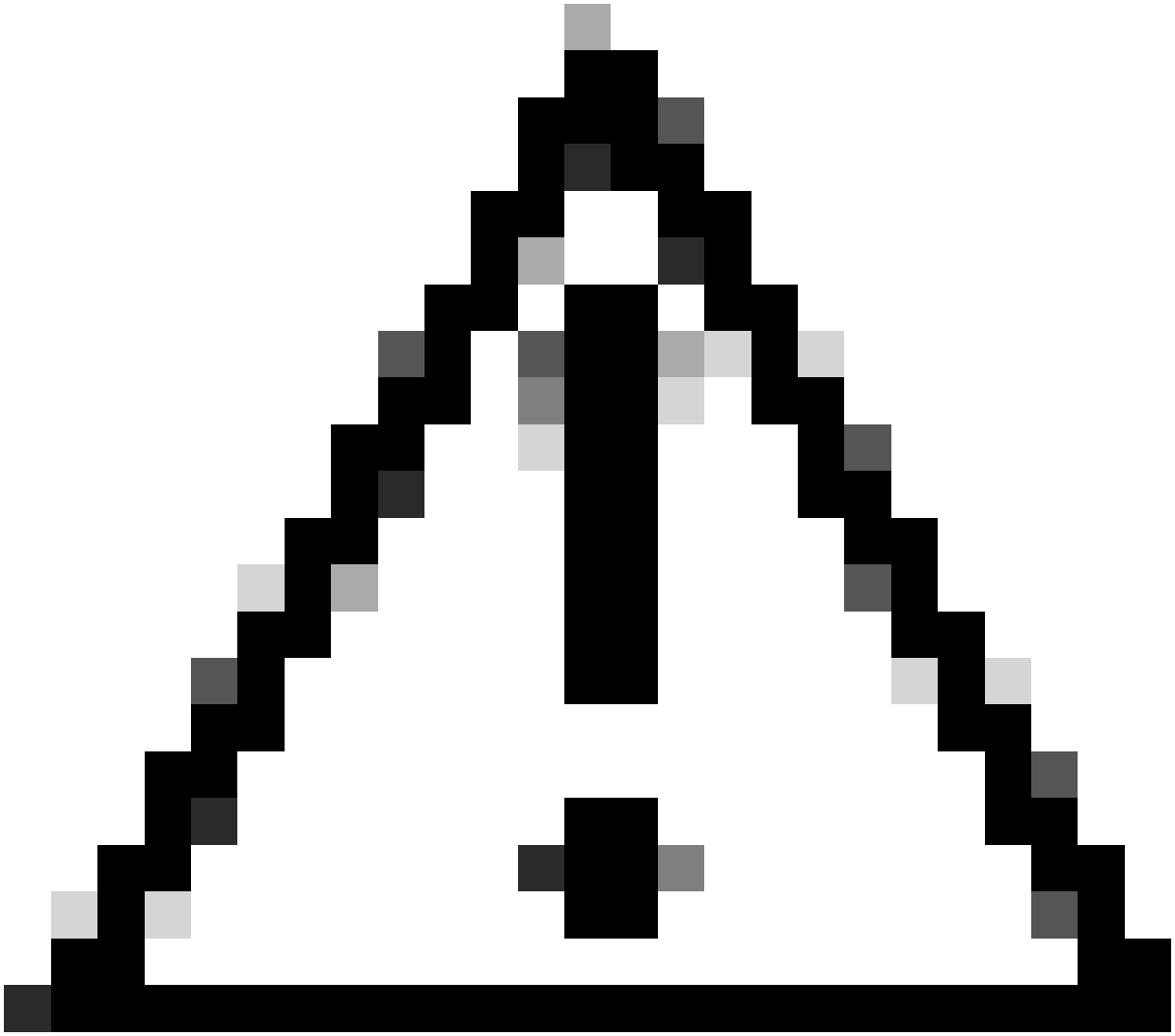
Este é um pouco de um aprofundamento em como os pacotes se parecem e como eles são tratados pela infraestrutura sem fio. Para que as alterações introduzidas neste documento sejam totalmente compreendidas, é importante saber o fluxo do pacote durante o processo de

autenticação sem fio ao usar dot1x e mais especificamente EAP-TLS.

Se você já tiver um profundo entendimento de como o fluxo de pacotes EAP e RADIUS funciona na infraestrutura sem fio da Cisco, vá para a seção de alteração de comportamento que explica o que foi adicionado em 17.11, dando aos administradores de rede mais controle sobre o RADIUS MTU. Primeiro, observe a Identificação EAP (EAP-ID).

EAP-ID

O EAP-ID é iniciado pelo autenticador, neste caso a WLC. Essa deve ser a primeira parte do processo EAP. Às vezes, o cliente sem fio envia um EAPOL-Start. Isso normalmente significa que o cliente nunca recebeu a solicitação de EAP-ID ou deseja recomeçar.



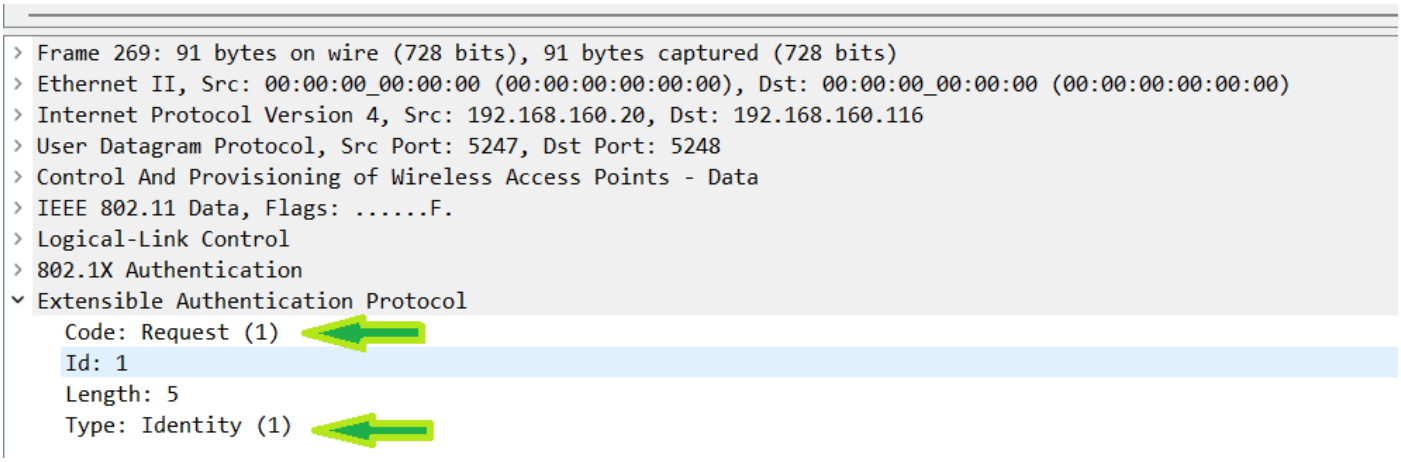
Caution: Há uma diferença entre o pacote EAP-ID e o pacote EAP ID. O pacote EAP-ID é usado para identificar o solicitante, onde o ID do pacote EAP é um número usado para rastrear o pacote específico à medida que ele se move pela rede.

Solicitação de EAP-ID

Primeiro, o dispositivo cliente sem fio se conecta à rede usando o processo de associação normal. Quando a rede local sem fio (WLAN) é configurada para dot1x, a WLC primeiro precisa saber quem é o cliente antes de solicitar acesso do servidor RADIUS. Para encontrar essas informações, a WLC envia o cliente e a solicitação EAP-ID.

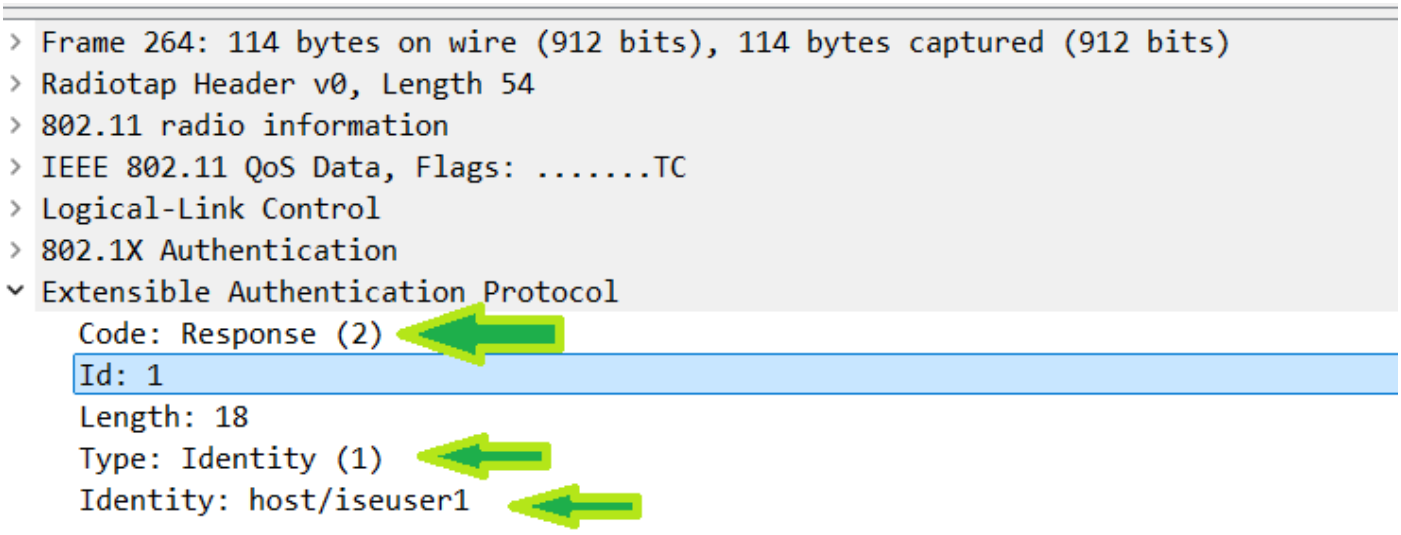
Espera-se que o cliente responda com a resposta EAP-ID. Isso fornece à WLC o que ela precisa para criar a solicitação de acesso e enviá-la ao ISE. A solicitação EAP-ID é quando o cliente é solicitado a inserir seu nome de usuário e senha em uma autenticação PEAP normal.

No entanto, essa discussão gira em torno de EAP-TLS, portanto, a resposta de EAP-ID aqui teria apenas a ID de usuário. Na demonstração, o ID de usuário é iseuser1. Neste pacote, você pode ver a solicitação EAP-ID que o WLC envia ao cliente sem fio perguntando quem eles são. Como esse é um cliente sem fio, a WLC encapsula a solicitação no CAPWAP e a envia ao Ponto de Acesso (AP) para ser enviada pelo ar. Nos dados EAP, o código 1 significa que é uma solicitação e o tipo 1 significa que é para a identidade.



Resposta de EAP-ID

Em seguida, espera-se que o cliente sem fio responda com a resposta EAP-ID. Nos dados EAP, o código foi alterado para 2, significando que é uma resposta, mas o tipo permanece como 1, ainda mostrando que é para a identidade. Aqui, você pode até ver o nome de usuário que o cliente está usando. Outra coisa a ser verificada nesses pacotes é o número de ID do pacote EAP. Para a troca de EAP-ID, é sempre 1, mas esse número depois muda para outra coisa quando o ISE se envolve.



Você pode ver que ambos os pacotes são bem pequenos, portanto o MTU não tem nenhuma influência aqui, já que está bem abaixo dos 1500 bytes usados na rede.

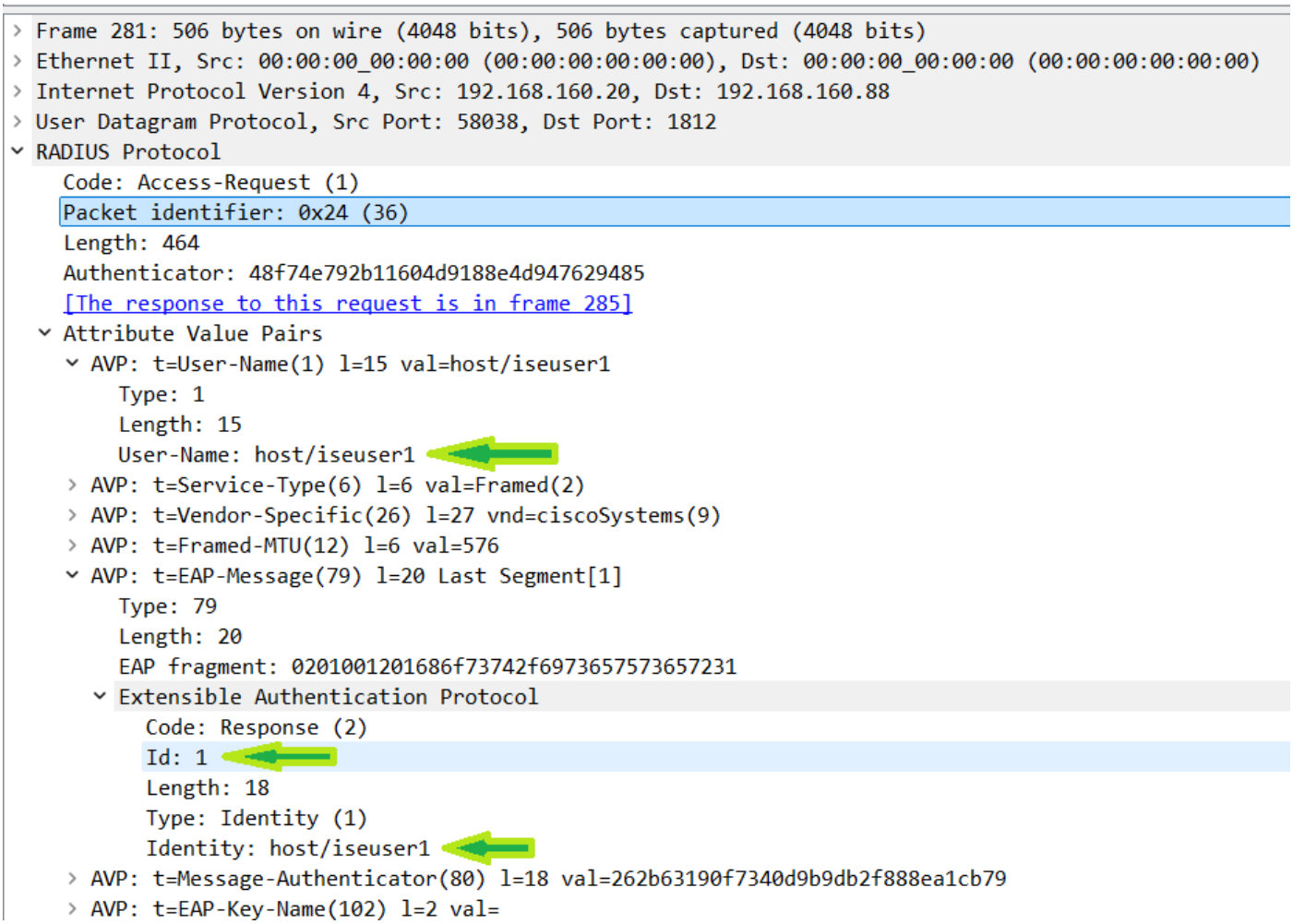
Access-Request e Access-Challenge

A comunicação com o cliente é EAP e a comunicação entre a WLC e o ISE é RADIUS. Para a comunicação RADIUS, os pacotes de solicitação de acesso e desafio de acesso são usados. A WLC recebe o pacote EAP do solicitante e o encaminha para o ISE usando a solicitação de acesso RADIUS. Em uma rede em funcionamento, o ISE responderia com um desafio de acesso.

Solicitação de acesso

Agora que a WLC sabe a identidade do cliente, ela precisa perguntar ao servidor RADIUS se esse cliente tem permissão na rede. Para fazer isso, a WLC solicita acesso para esse cliente enviando o pacote de solicitação de acesso. Há outros pedaços de dados que a WLC enviará junto com os dados EAP. Coletivamente, eles são chamados de pares de valores de atributo, AVPs ou pares AV, dependendo de quem está falando.

Este documento não vai muito além dos AVPs, pois isso está fora do escopo desta discussão. Aqui você só precisa ver que o nome de usuário (dados EAP) é incluído e enviado para o servidor RADIUS, que, neste caso, é ISE. Além disso, você pode ver que o número de ID de EAP 1 também é enviado ao ISE. Lembre-se de que quando você observou o ID do pacote EAP pelo ar, ele também estava em 1. A última coisa importante a ser observada aqui é que como a WLC adicionou todos esses AVPs, o pacote de 114 bytes que o cliente enviou agora é transformado em um pacote de 488 bytes antes de ser enviado ao ISE.

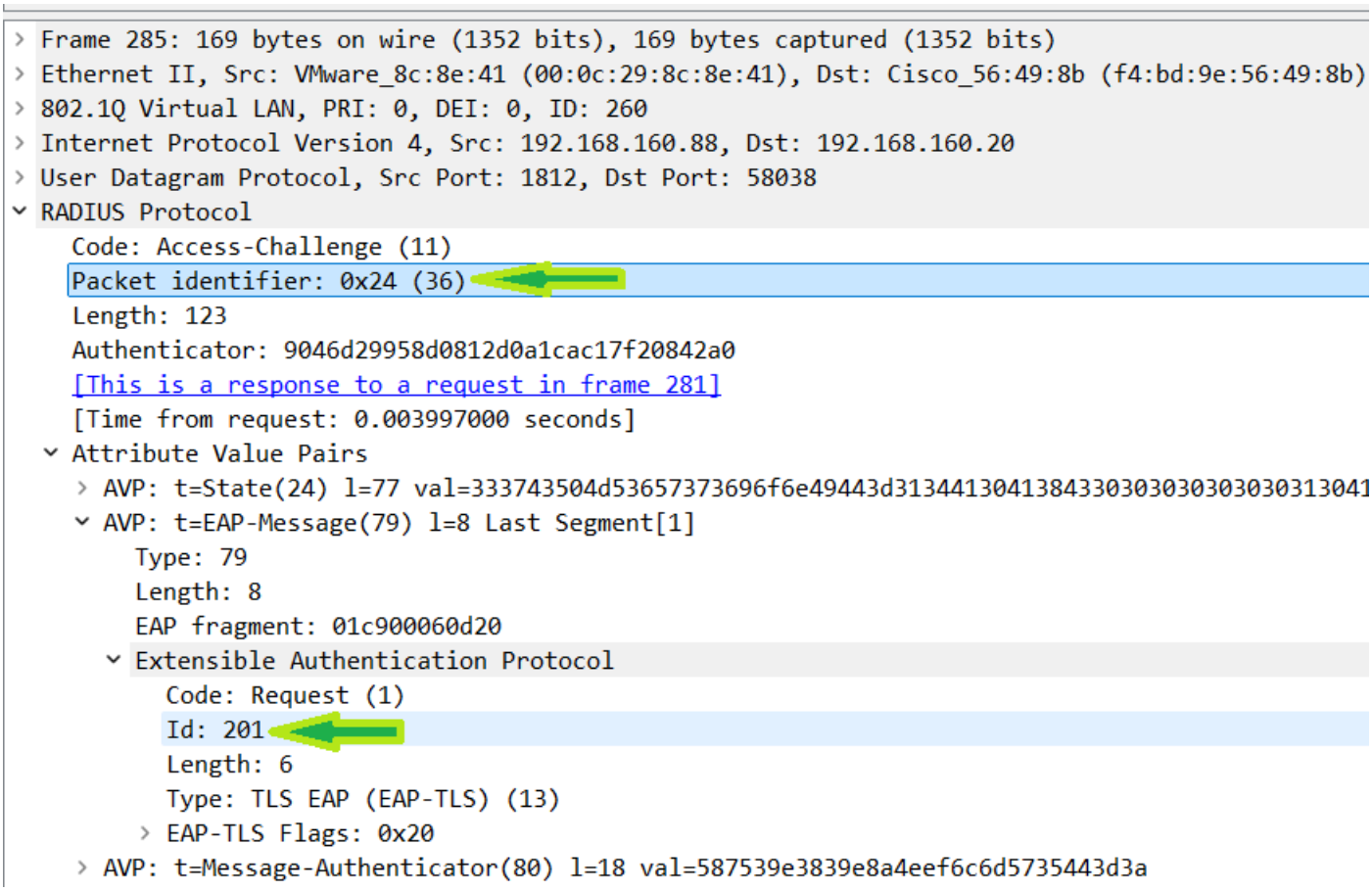


Desafio de acesso

Supondo que o ISE receba a solicitação de acesso e decida responder, espera-se que essa resposta venha como um desafio de acesso do ISE. Olhando para trás na solicitação de acesso, você veria o ID do pacote RADIUS de 36 antes dos AVPs começarem.

Quando a WLC recebe o desafio de acesso, o ID do RADIUS deve corresponder ao ID do pacote da solicitação de acesso. O ID do pacote RADIUS é para a comunicação RADIUS entre o ISE e a WLC. Você também pode ver neste pacote que o ISE definiu um novo EAP ID de 201 que é usado para rastrear a comunicação entre o ISE e o cliente. Neste ponto, a WLC é apenas uma passagem para a comunicação entre o ISE e o cliente.

É importante observar todos esses IDs de pacote aqui para que você compreenda o fluxo de comunicação e como rastrear esses pacotes pela rede. Em um ambiente de produção, geralmente há várias autenticações ocorrendo ao mesmo tempo. Use o comando calling-station-id para associar o pacote ao endereço MAC do cliente. Em seguida, você pode usar o ID do pacote RADIUS e o ID do pacote EAP para rastrear o fluxo do pacote para esse cliente específico. Até este ponto, nenhum dos lados enviou certificados, portanto, ainda não houve necessidade de se preocupar com o MTU.



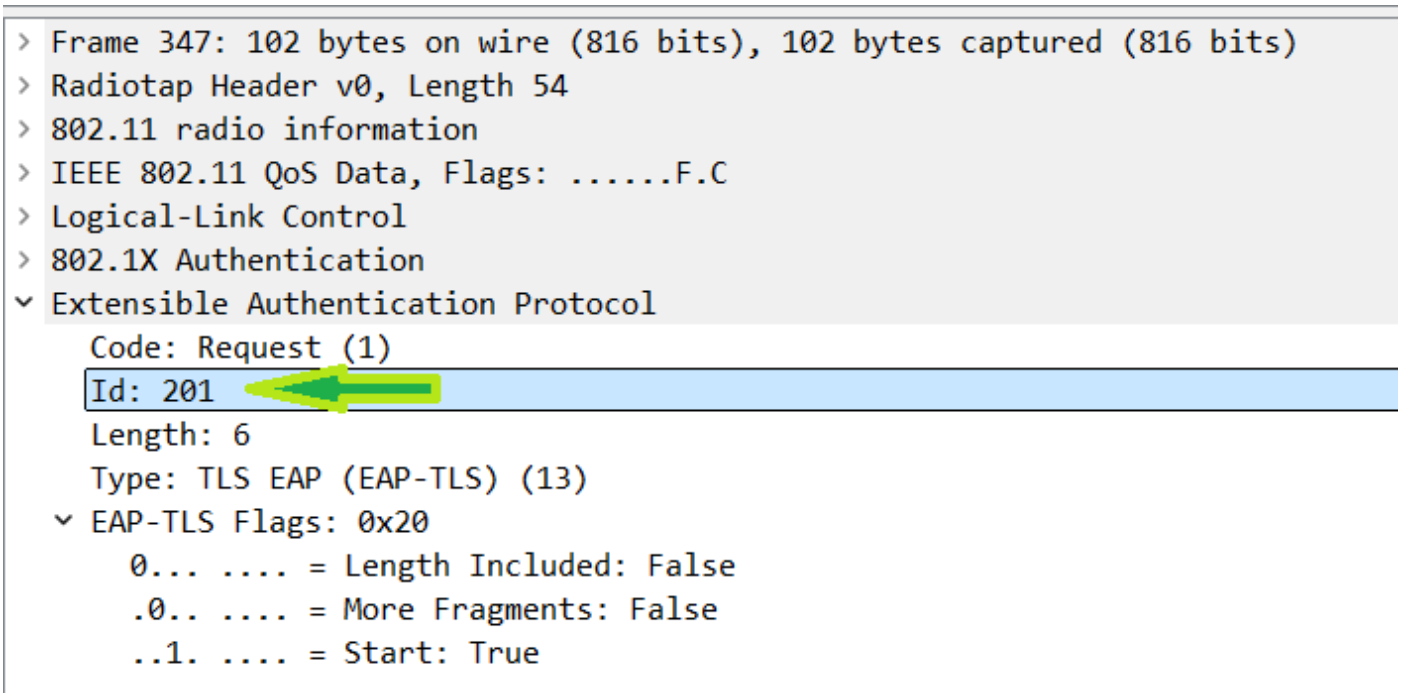
Solicitação EAP e Resposta EAP

Apenas um lembrete, o cliente fala EAP e não RADIUS. Ou seja, quando a WLC recebe o desafio de acesso, ela precisa remover os dados RADIUS e retirar a solicitação EAP para que ela possa ser enviada ao cliente.

Solicitação EAP

Isso deve parecer exatamente como dentro do desafio de acesso quando a WLC o recebeu. No entanto, todos os itens RADIUS foram removidos e apenas a parte EAP é enviada ao cliente.

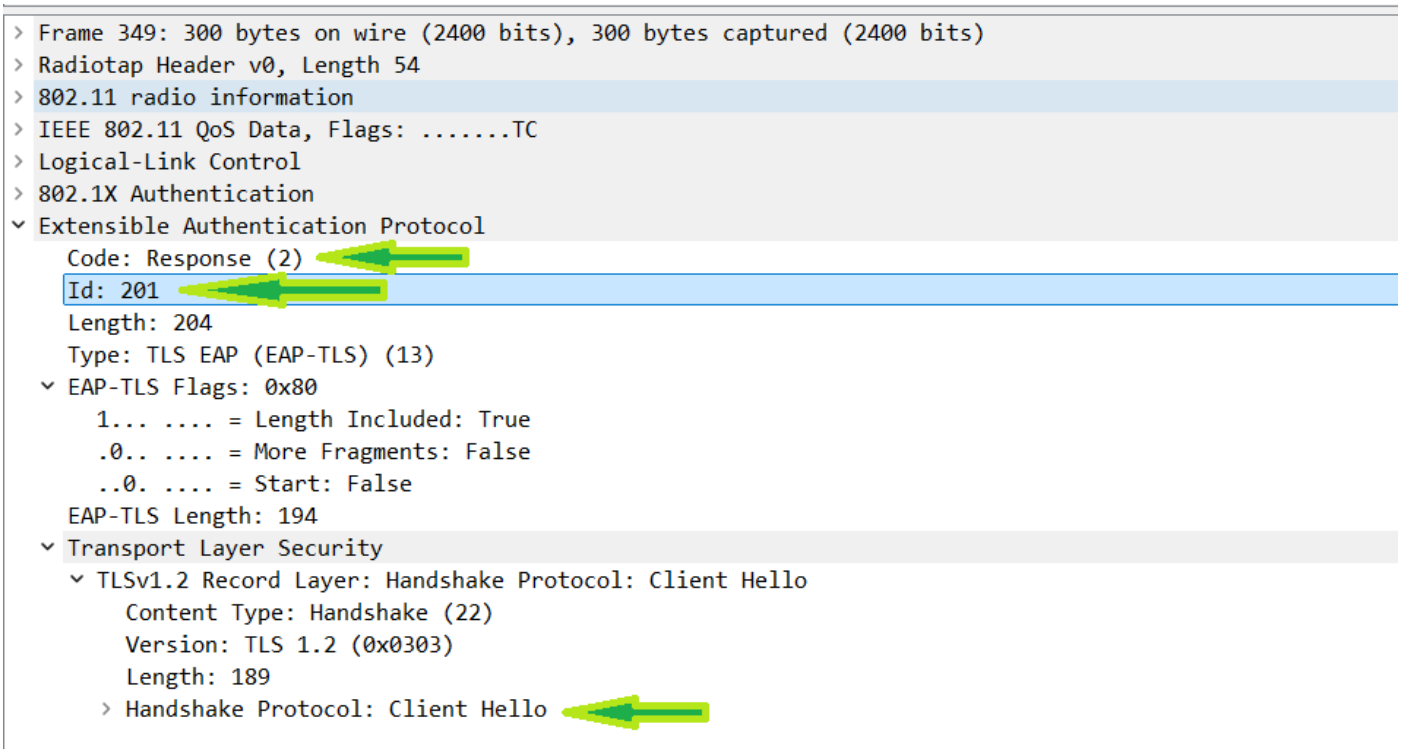
Você ainda pode ver o ID de pacote EAP 201 aqui, assim como no desafio de acesso, pois são os mesmos dados que o WLC recebeu do ISE. O fluxo aqui é o mesmo que com o EAP-ID, só que agora ele não vem da WLC e é usado para estabelecer o método EAP. Esse pacote ainda é muito pequeno porque é apenas para estabelecer o início de uma sessão EAP-TLS.



Resposta EAP

Quando o cliente recebe a EAP-Request, ele deve responder com uma EAP-Response. No EAP-Response, o cliente começa a estabelecer a sessão TLS. Isso parece o mesmo que em qualquer outra situação em que o TLS é usado. Ele começa com a mensagem "cliente hello". Este documento não vai detalhar o que entra no hello do cliente, pois é irrelevante para este tópico. O que você precisa observar aqui é apenas que uma sessão TLS está sendo configurada.

Você pode ver os dados nos pacotes aqui como faria com qualquer outra configuração de TLS. Assim como ocorre com a resposta EAP-ID, esse pacote atinge a WLC e é convertido em uma solicitação de acesso. O ISE responde com uma solicitação de EAP em um desafio de acesso. Este continua a ser o fluxo a partir de agora.



Certificados TLS

Este é o ponto onde você verá o aumento do tamanho do pacote. Os certificados podem ser bastante grandes dependendo da presença de uma ou mais autoridades de certificação intermediárias (CAs). Se for um certificado autoassinado, obviamente ele seria menor que um certificado com um certificado de dispositivo encadeado a 2 CAs intermediárias e uma CA raiz. De qualquer forma, você normalmente vê o proprietário do certificado começar a fragmentar seus próprios pacotes aqui.

Certificado ISE

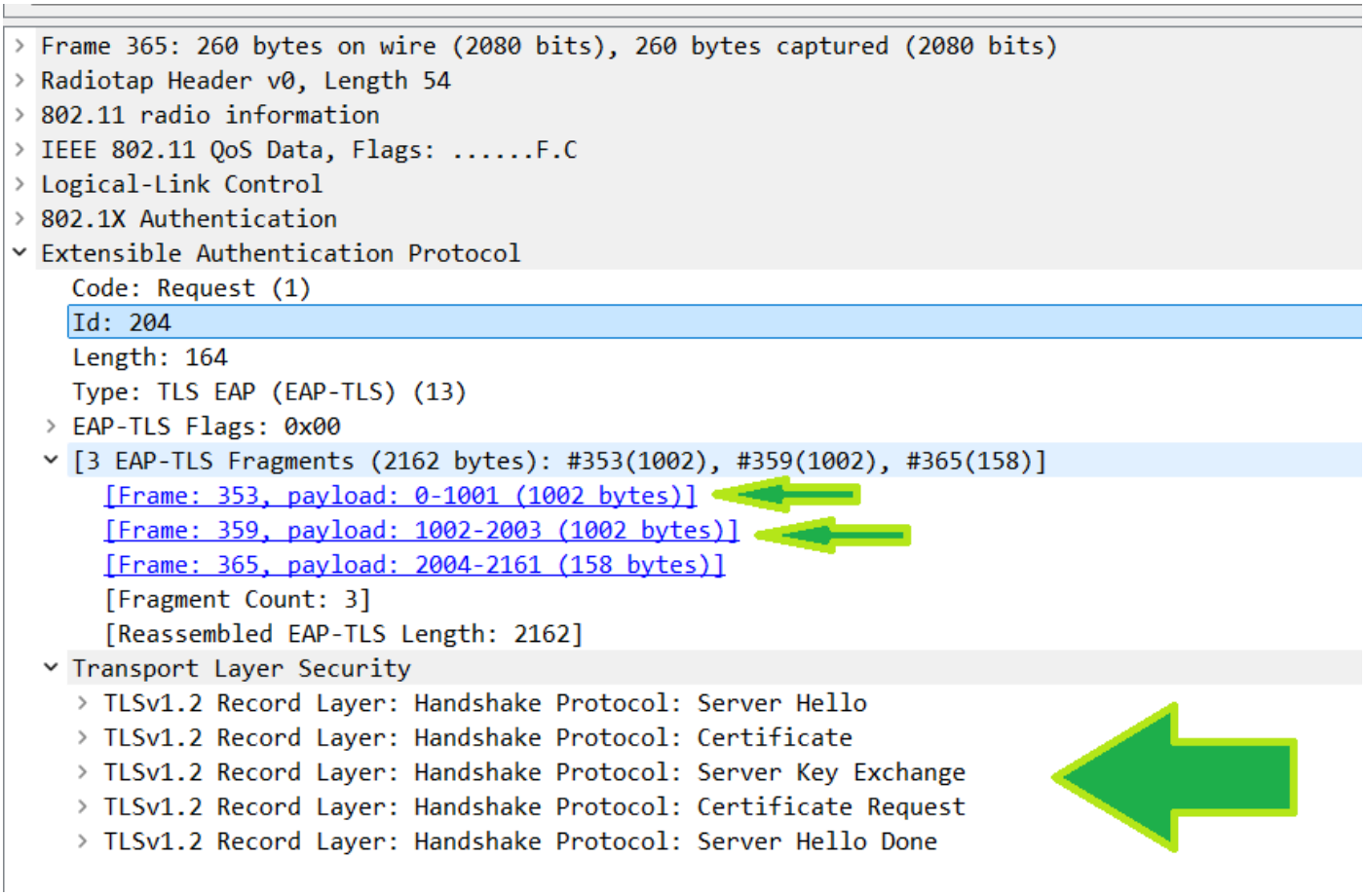
Agora que o ISE recebeu a saudação do cliente TLS, ele responde com outra solicitação EAP. Nessa nova solicitação de EAP, o ISE envia a mensagem "server hello", seu certificado, a "troca de chave do servidor", a "certificate request" e as mensagens "server hello done" todas de uma vez. Se enviasse tudo isso em um pacote, o pacote estaria sobre a MTU para a rede. Assim, o ISE fragmenta o próprio pacote para obtê-lo sob a MTU. Com o ISE, ele fragmenta a parte de dados do pacote de modo que não seja maior que 1002 bytes, na esperança de evitar a fragmentação dupla.

O que significa fragmentação dupla? A primeira fragmentação está acontecendo no ISE, pois os dados que ele deseja enviar são muito grandes para caber dentro da MTU da rede. Ainda assim, pode haver outros lugares na rede onde, mesmo que o MTU seja o mesmo, por causa de como a rede é configurada, um dispositivo possivelmente precise fragmentar o pacote para que ele adicione seus cabeçalhos e permaneça sob o MTU. Isso pode ser verdadeiro mesmo se o bit do not fragment estiver marcado.

Um bom exemplo disso é com um túnel VPN, ou qualquer túnel. Para colocar dados em um túnel VPN, os roteadores VPN precisam adicionar seus cabeçalhos ao tráfego. Se esse tráfego

RADIUS fosse fragmentado na MTU ou próximo a ela, quando se trata dessa VPN não haveria como manter os dados sob a MTU e adicionar cabeçalhos extras. Isso também é verdadeiro para túneis CAPWAP, que você pode ver um pouco mais tarde.

Portanto, para evitar que esses pacotes cheguem a uma situação em que outro dispositivo possa fragmentá-lo novamente, o ISE fragmenta o pacote em um local onde isso possa ser evitado na maioria das redes. Isso significa que o ISE envia esses dados em várias Solicitações EAP aguardando uma resposta EAP vazia a cada vez. O ID de EAP aumenta com cada fragmento enviado. Do ponto de vista da WLC, isso seria um desafio de acesso e uma troca de solicitação de acesso para cada fragmento e o ID do pacote RADIUS aumentaria com cada fragmento enviado.



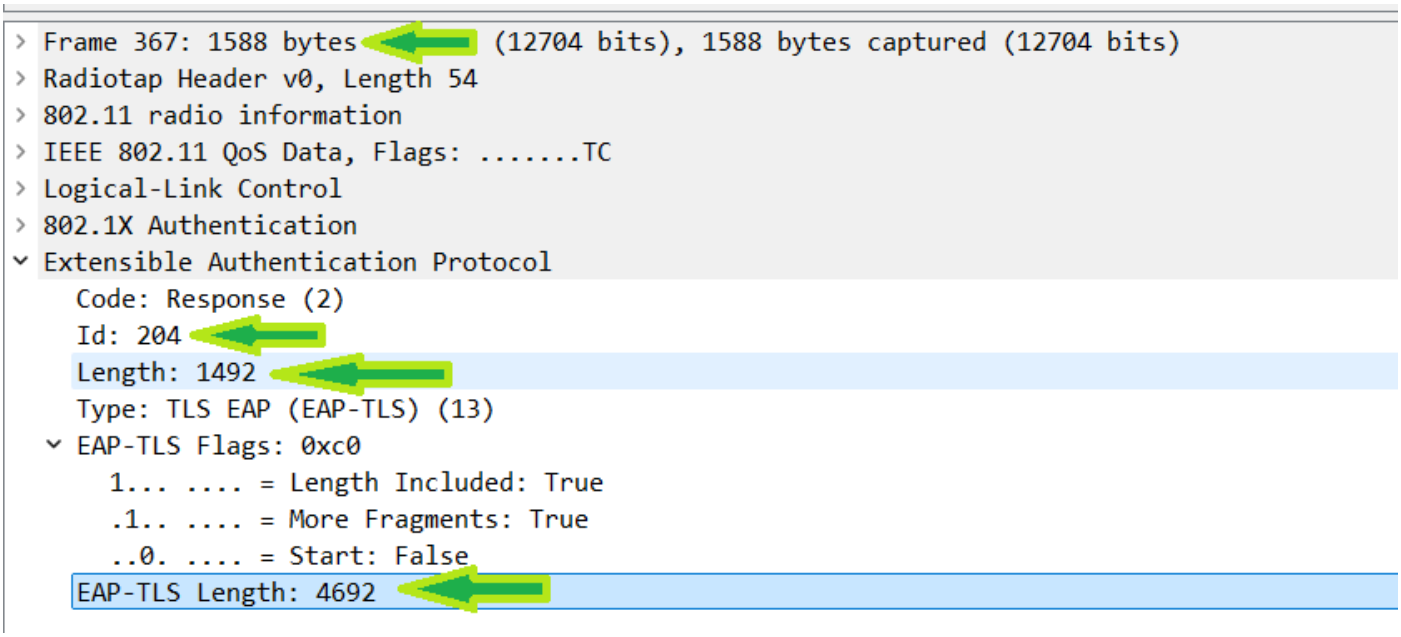
Client Certificate

Depois que o ISE envia todos os fragmentos e eles são reagrupados pelo cliente, o fluxo de pacotes segue para o cliente para enviar algo. No TLS, espera-se que o cliente envie seu próprio certificado neste ponto para concluir a autenticação. É aqui que as coisas se tornam mais complexas. Assim como o ISE, o cliente enviará várias peças TLS de uma só vez, sendo uma delas seu certificado.

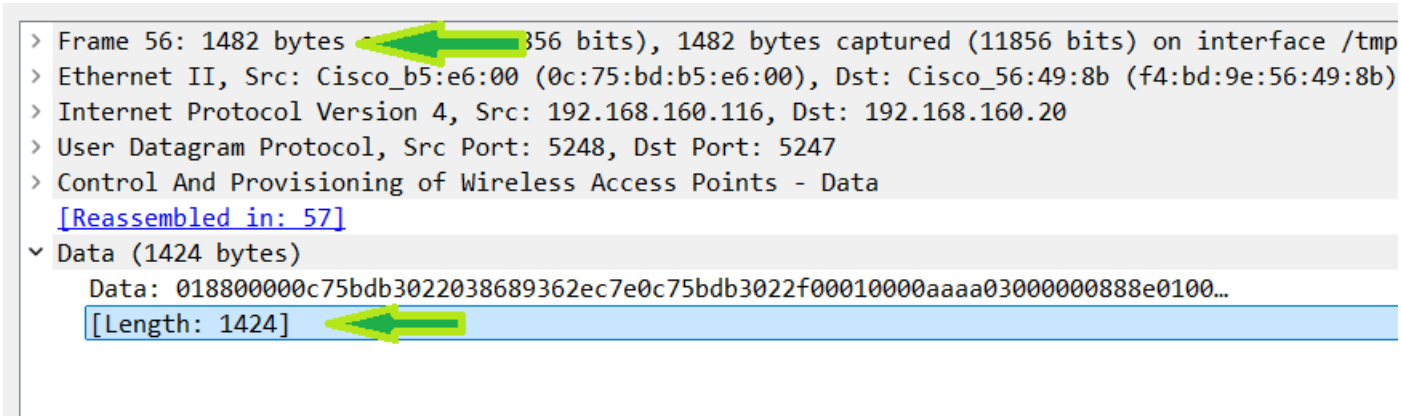
Diferentemente do que foi visto com o ISE, a maioria dos clientes envia seus dados EAP logo abaixo da MTU. Nesta demonstração, os dados 802.1x são 1492. O problema com isso é que o AP precisa adicionar os cabeçalhos CAPWAP para que ele possa ser enviado para a WLC.

Como isso pode ser feito? O AP terá que fragmentar o pacote para que possa adicionar os cabeçalhos e enviá-lo para a WLC. Não há como o AP obter o pacote para a WLC sem fragmentá-lo. Dito isso, aqui o pacote é fragmentado duas vezes, primeiro a partir do cliente e, em seguida, novamente a partir do AP. No entanto, essa fragmentação geralmente não é um problema, como esperado com o CAPWAP.

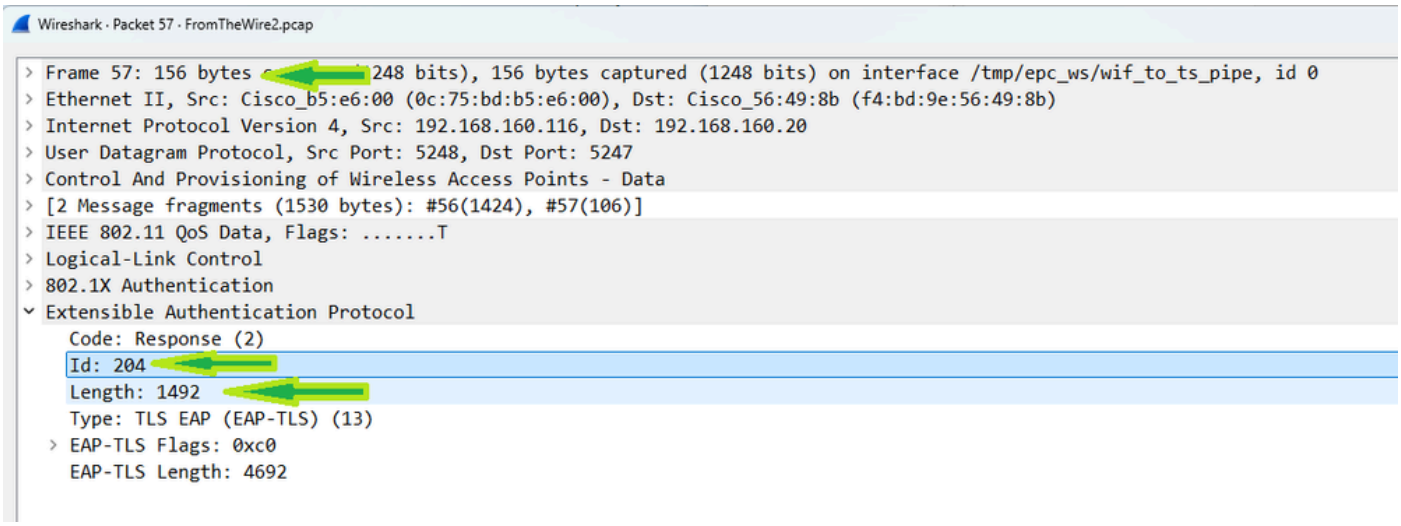
O pacote no ar:



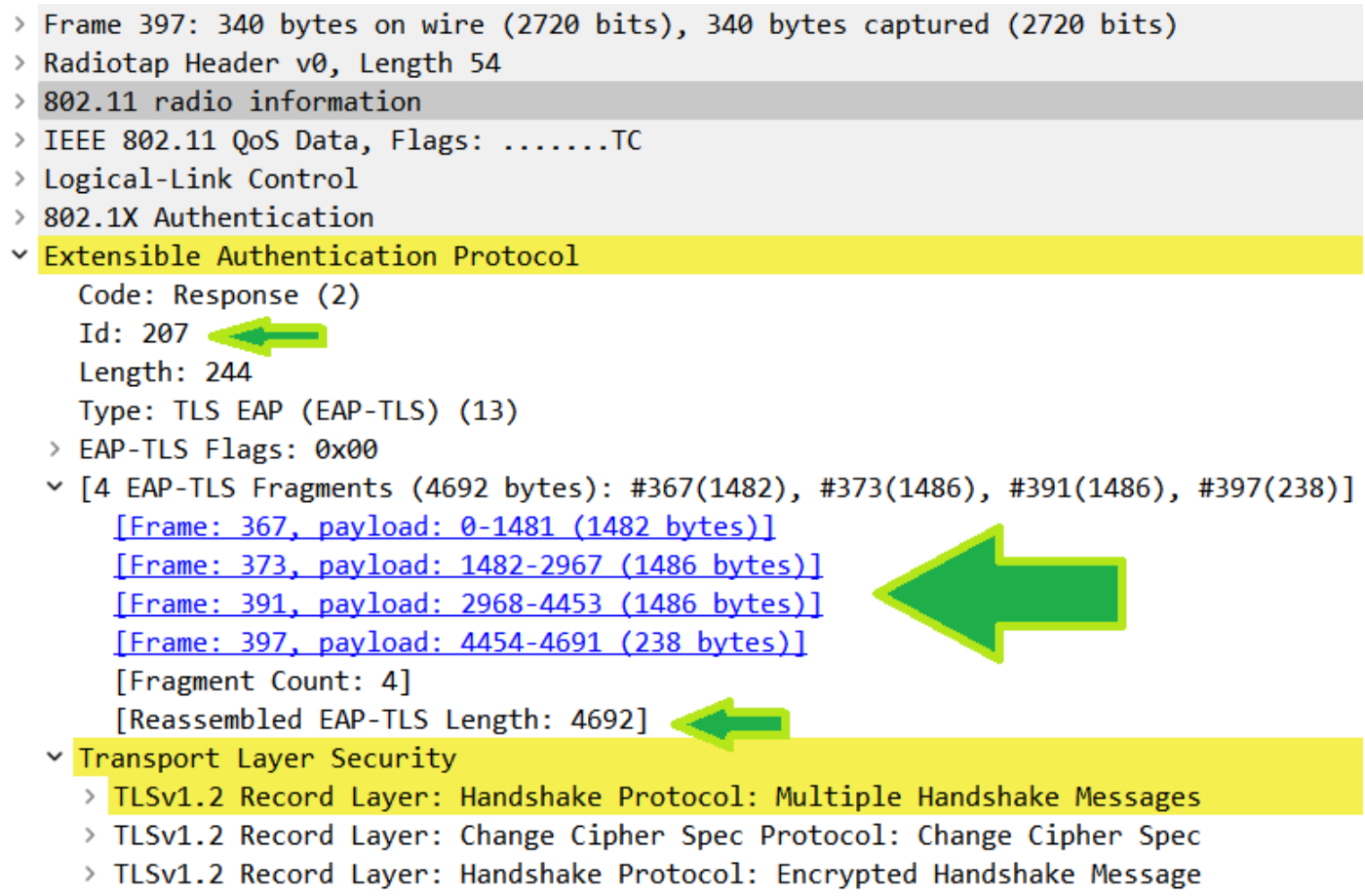
O fragmento do pacote no fio:



O pacote remontado no fio:



Todos os fragmentos do cliente reagrupados no ar:



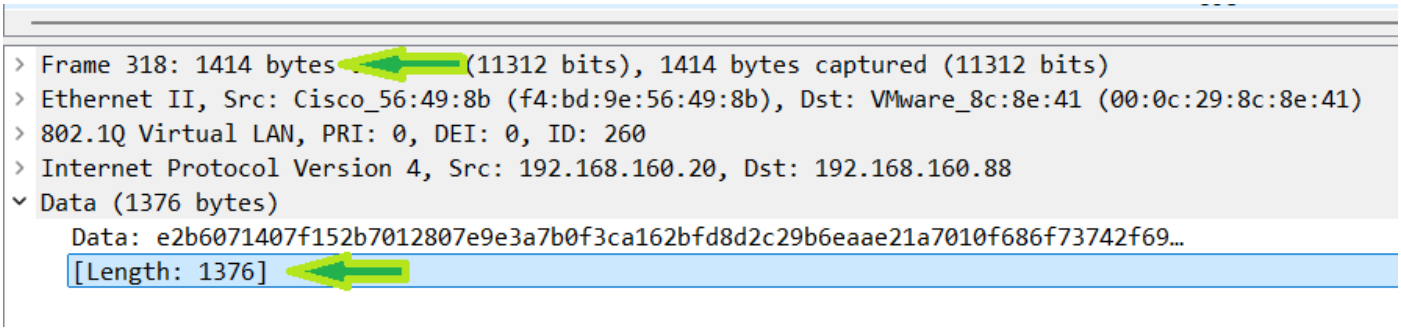
Certificado do cliente no WLC

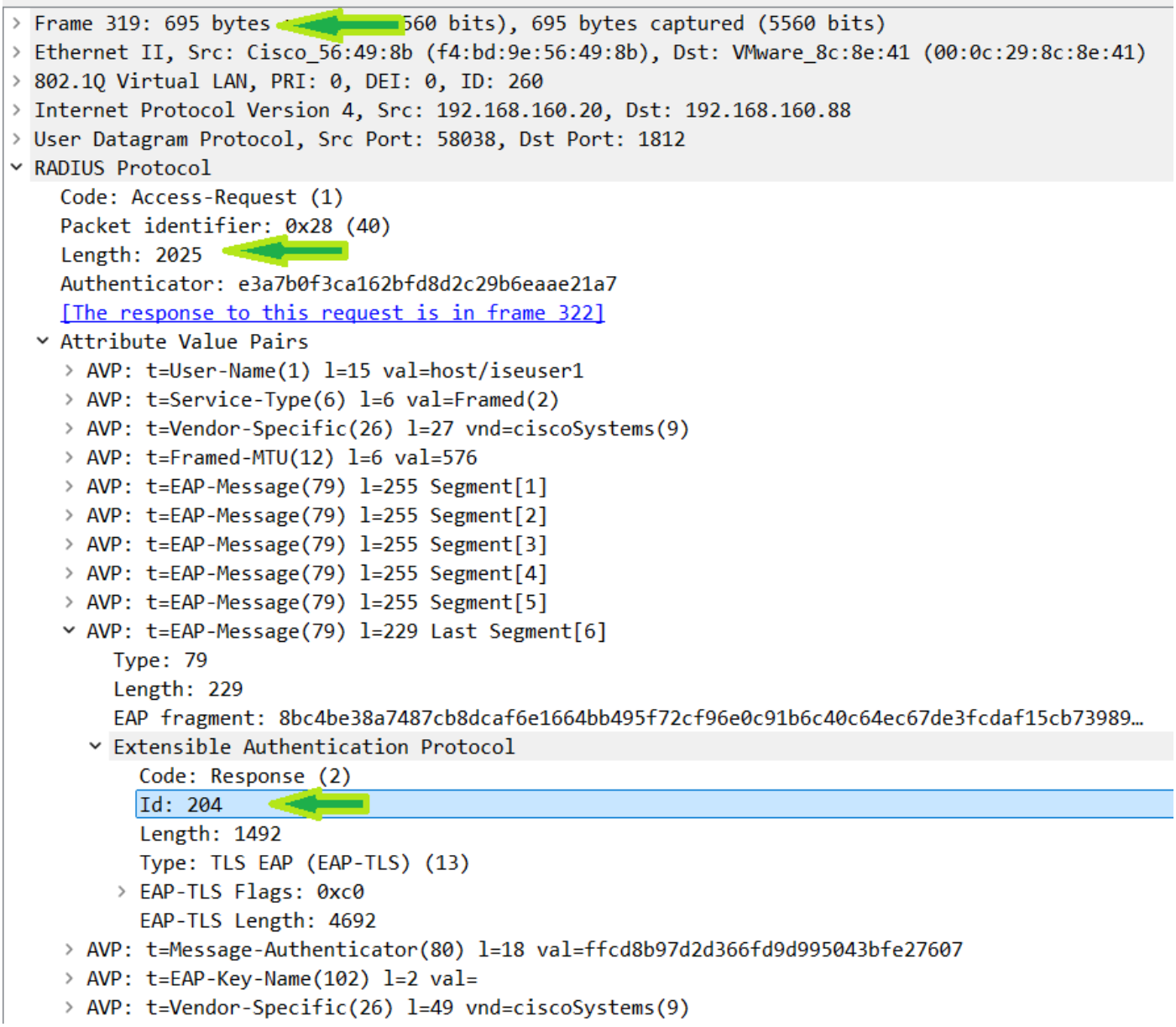
A WLC recebe os dois fragmentos CAPWAP e os remonta para ter o pacote de 1.492 bytes inteiro do cliente, restaurando o pacote - mas não por muito tempo. Essa restauração é de curta duração porque, se você olhar para trás para como o WLC envia a solicitação de acesso, você deve lembrar que ele tem que adicionar cerca de 400 bytes de AVPs RADIUS ao pacote antes que ele possa enviar os dados ao ISE.

Para matemática simples, suponha que a WLC adicione 408 bytes, elevando o tamanho total do pacote para 1900. Isso está bem acima do MTU de 1500, então o que a WLC vai fazer? Fragmente o pacote novamente.

Neste ponto, a WLC vai fragmentar o pacote em 1396 por padrão. A ideia aqui é a mesma do ISE. A esperança é tornar o pacote pequeno o suficiente para que, se ele tiver que passar por outro túnel, não precise ser fragmentado novamente para adicionar os cabeçalhos. No entanto, a WLC não é tão cautelosa quanto o ISE, portanto, 1396 é bom o suficiente aqui.

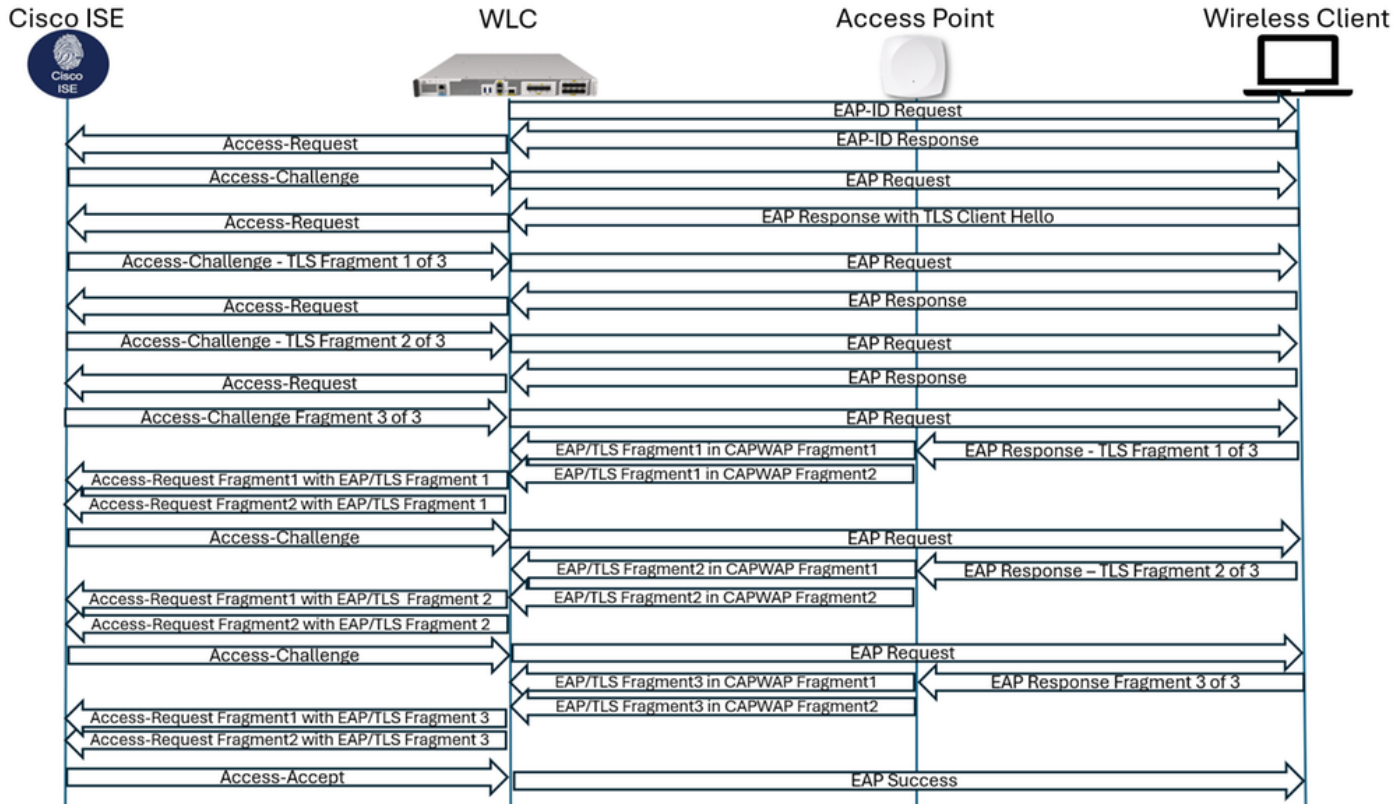
O pacote fragmentado saindo da WLC:





Fluxo de pacote TL;DR

Quando o ISE envia seu certificado, ele fragmenta os pacotes TLS em 1002 bytes. Não há problemas. Quando os clientes enviam seu certificado, eles geralmente se fragmentam próximo à MTU. Como o AP precisa adicionar os cabeçalhos CAPWAP ao pacote, ele também precisa fragmentar esse pacote. Uma vez que o WLc recebe os fragmentos, ele tem que remontar o pacote, mas então tem que adicionar os AVPs RADIUS para que o pacote seja fragmentado novamente. O fluxo de pacotes se parece com algo assim:



Alteração de Comportamento de RADIUS MTU

Ao observar o fluxo de pacotes para qualquer tráfego de dados de cliente sem fio, você pode ver que a infraestrutura sem fio tem influência apenas sobre ele em alguns lugares. O primeiro lugar é quando o tráfego deixa o AP e o segundo lugar é quando o tráfego deixa a WLC. A exceção é o tráfego TCP, em que a infraestrutura sem fio pode ajustar o MSS do cliente. No entanto, o EAP não se enquadra no TCP; na verdade, ele é seu próprio protocolo.

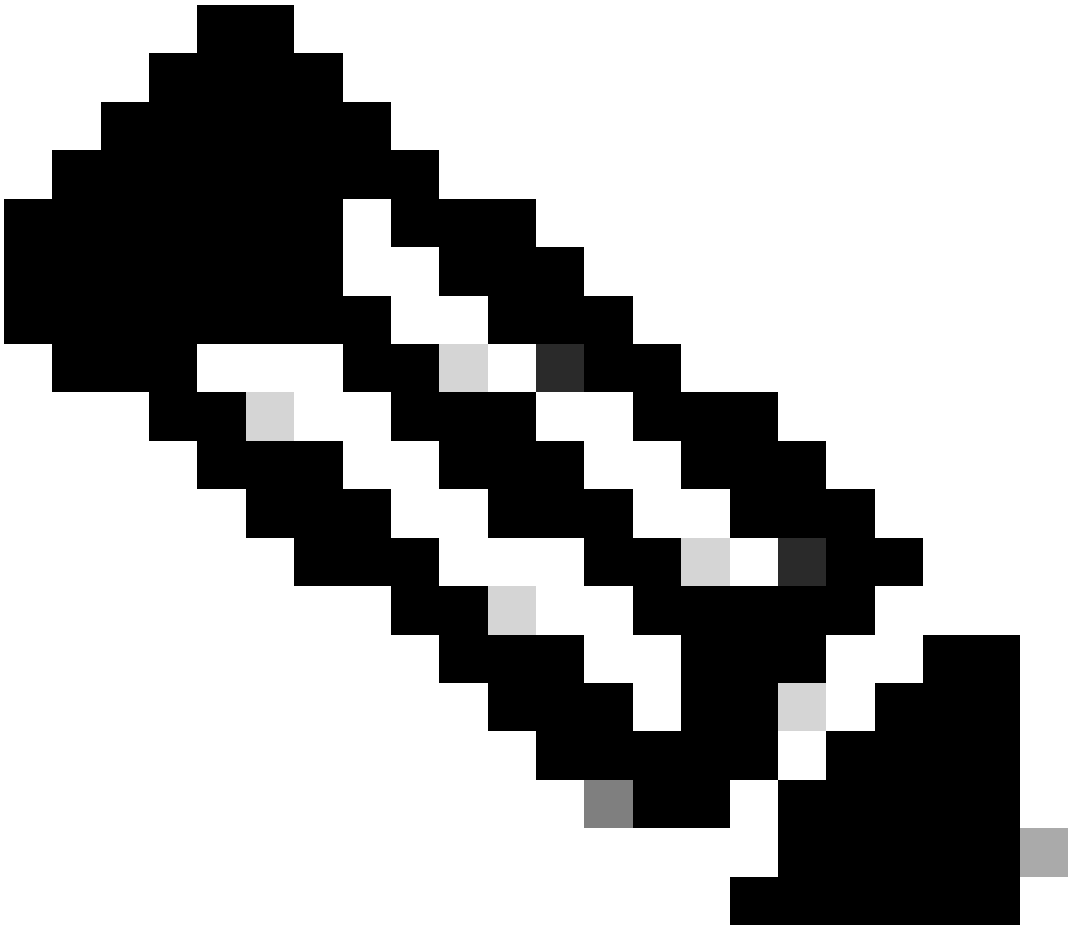
Ao observar os fluxos de tráfego EAP e RADIUS, você também pode ver que a rede de fato influencia o tamanho do tráfego no AP e na WLC quando o tamanho do pacote original fica muito próximo da MTU. Com uma compreensão adequada da função da WLC nessa troca, você pode ver que há apenas um lugar onde ela tem influência do tamanho do pacote RADIUS. Isso ocorreria quando uma resposta EAP entrasse e você a alterasse para uma solicitação de acesso RADIUS.

O que mudou

Se a resposta EAP estiver sobre a MTU, depois de adicionar os AVPs RADIUS, você terá que fragmentá-la. Como você já tem que fragmentar este pacote, não importa o tamanho, você pode pelo menos decidir em que tamanho deseja fragmentá-lo. É aí que entra a alteração de comportamento introduzida em 17.11.

Na solicitação de recurso rastreada no bug da Cisco id CSCwc81849, você deseja adicionar suporte para pacotes RADIUS Jumbo. A maneira como isso foi feito é que o pacote RADIUS não era mais fragmentado automaticamente em 1396. Agora, se você adicionar o comando ip radius source-interface <interface X>, a solicitação de acesso RADIUS será enviada na MTU dessa

interface.



Note: Se você estiver usando o Cisco Catalyst Center, ao provisionar configurações AAA, ele adicionará automaticamente a interface de origem ao grupo de servidores. Isso altera o comportamento padrão para fragmentar no tamanho de MTU da interface usada nesse comando.

Como essa alteração pode ser usada

Como o MTU padrão de todas as interfaces seria 1500, esse seria o novo MTU para fragmentar. A interface padrão usada para todo o tráfego RADIUS é a interface de gerenciamento sem fio (WMI). Quando você examina a configuração do grupo de servidores, se não houver uma interface de origem especificada, a WLC envia o tráfego RADIUS em 1396 usando a WMI. No entanto, se você entrar na configuração do grupo de servidores e informar que a interface de origem é a WMI, a WLC enviará o tráfego RADIUS em 1500 e ainda usará a WMI.

Agora, suponha que haja um dispositivo na rede como a VPN discutida anteriormente. Você não

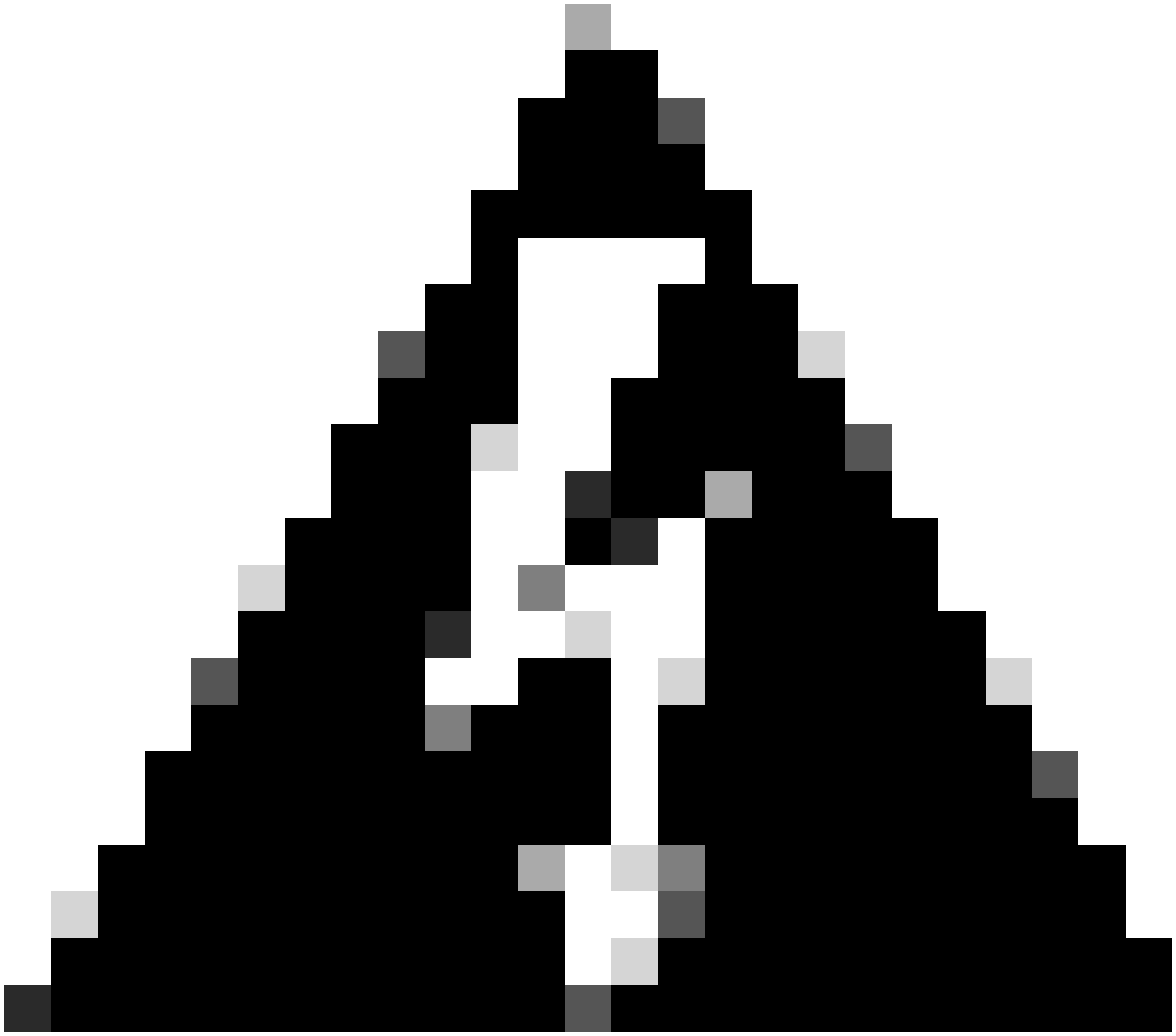
deseja que o tráfego seja fragmentado duas vezes, de modo que você possa alterar o MTU da interface para algo menor a fim de fragmentar os pacotes em um lugar diferente. Você pode alterar o MTU para algo como 1200 para que os pacotes sejam fragmentados na marca de 1200 bytes em vez de 1500.

aviso: Alterar a MTU da WMI afeta todo o tráfego que entra e sai do endereço IP de gerenciamento da WLC.

Mesmo que você não queira alterar a MTU da WMI, o ponto de especificar uma interface de origem é alterá-la de WMI para outra interface e usar essa interface para o tráfego RADIUS, bem como alterar a MTU nessa interface. Como essa configuração é feita no nível do grupo de servidores, você pode ser muito específico sobre qual tráfego RADIUS deseja que essa alteração seja afetada.

Esta configuração não está ligada a um servidor AAA ou WLAN. É possível ter vários grupos de servidores com os mesmos servidores e especificar somente a interface de origem em um deles se você assim escolher. Este grupo de servidores é adicionado a uma lista de métodos e, em

seguida, adicionado a uma WLAN. Assim, por exemplo, se houver apenas uma WLAN onde você deseja que essa alteração seja feita, mesmo que você tenha apenas um servidor AAA, você pode criar um novo grupo de servidores, usar o comando ip radius source-interface que aponta para a interface com a MTU que você deseja usar, adicionar o servidor AAA a esse novo grupo, criar uma nova lista de métodos usando esse novo grupo e, em seguida, adicionar essa lista de métodos à WLAN específica onde você deseja que essa alteração seja feita.



aviso: É sempre sugerido que, ao fazer QUAISQUER alterações em uma rede ativa, isso seja feito durante uma janela de manutenção.

A prova está na captura de pacotes

É comumente conhecidoEm redes, se você não a capturou, não poderá prová-la. Aqui estão alguns exemplos de configuração com essas alterações em vigor para mostrar como isso funciona.

Esta é uma configuração de WLAN. Durante o teste, somente o grupo de servidores usado na

lista de métodos é alterado.

```
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
!
```

Adicionando o comando Source-Interface com o MTU padrão

Aqui, é apenas um grupo de servidores normal que aponta para o servidor ISE. O comando source interface foi adicionado apontando para o meu WMI que não tem MTU definido. Esta é a aparência da configuração.

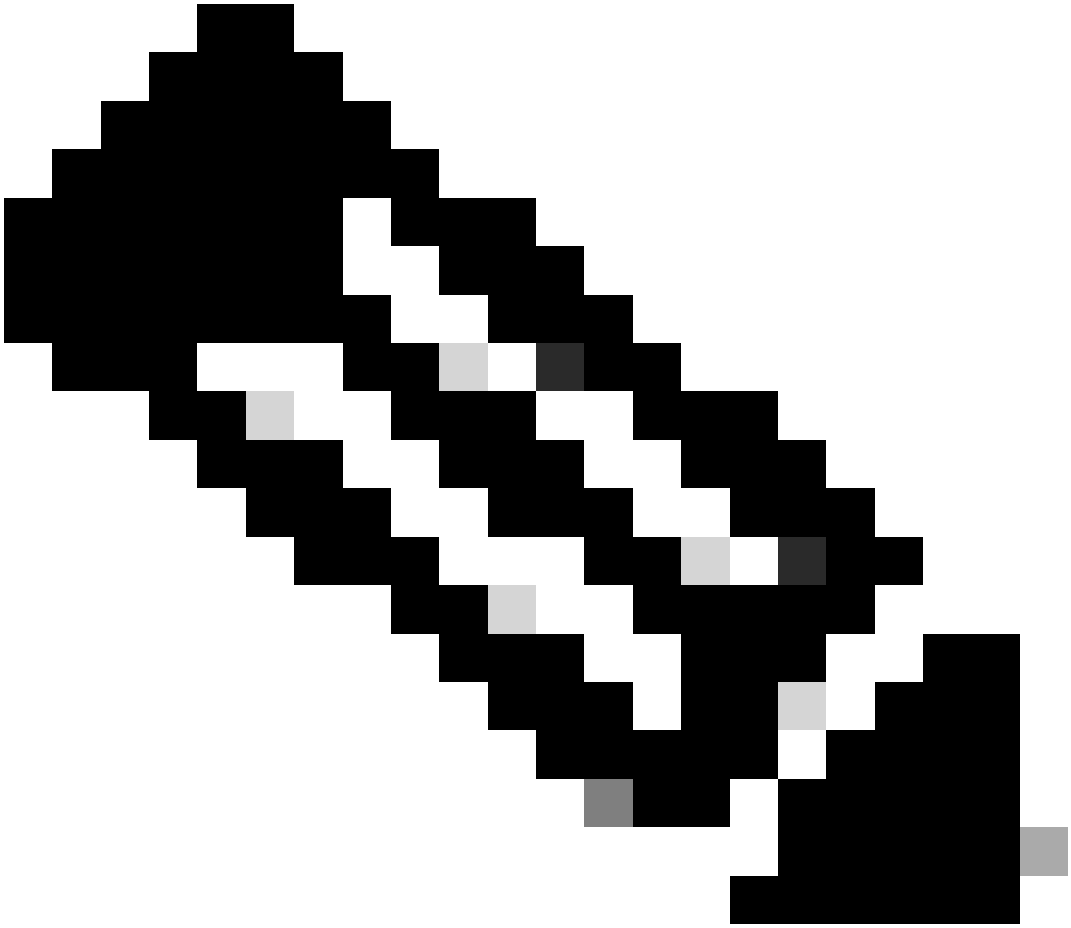
```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group NoMTU
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObF[^bPBVNaYibbBMhNMFAbKUAAB
!
aaa group server radius NoMTU
 server name ISE
 ip radius source-interface Vlan260
 deadtime 5
!
9800#show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

Como você pode ver, o grupo de servidores NoMTU foi adicionado à lista de métodos de autenticação vinculada à WLAN. O comando ip radius source-interface VLAN260 é usado para este grupo de servidores e a VLAN 260 não especifica uma MTU, o que significa que ela está usando a MTU de 1500. Apenas para confirmar, a MTU de 1500 você pode usar o comando show run all e procurar a interface na saída.

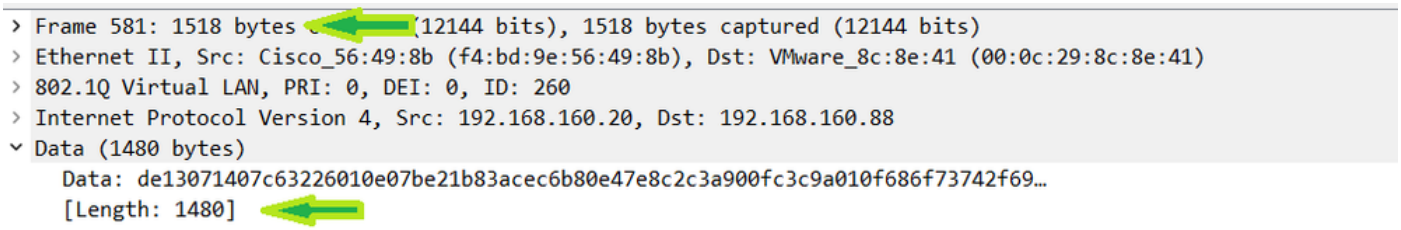
```
interface Vlan260
 ip address 192.168.160.20 255.255.255.0
 no ip clear-dont-fragment
```

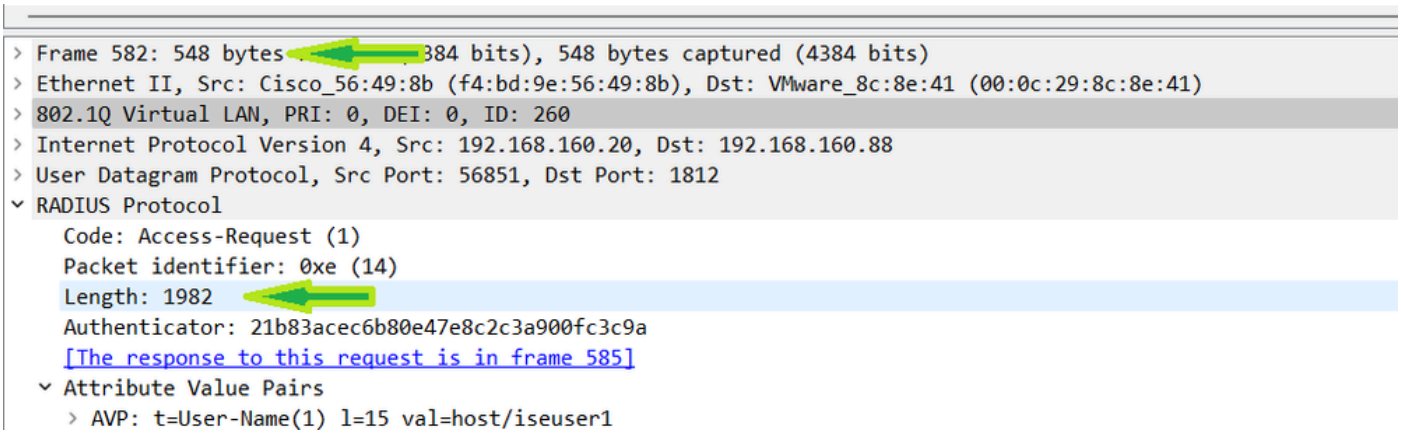
```
ip redirects
ip unreachables
no ip proxy-arp
ip mtu 1500
```

Agora examine o pacote em que o certificado de cliente deve ser enviado ao ISE quando a WLC adicionar os dados RADIUS:



Note: Aqui, os bytes na linha são 1518. Isso inclui cabeçalhos fora do payload Ethernet, como o cabeçalho de VLAN e o cabeçalho de camada 2. Eles não são contados para a MTU.





Aqui, você pode ver que a parte de dados está fragmentada em 1480. Você pode obter esse fragmento sob a MTU 1500 na WMI. O próximo pacote está abaixo de 550 bytes, mas você pode ver que o tamanho total dos dados RADIUS é 1982. Dito isso, a fragmentação com o novo MTU agora funciona.

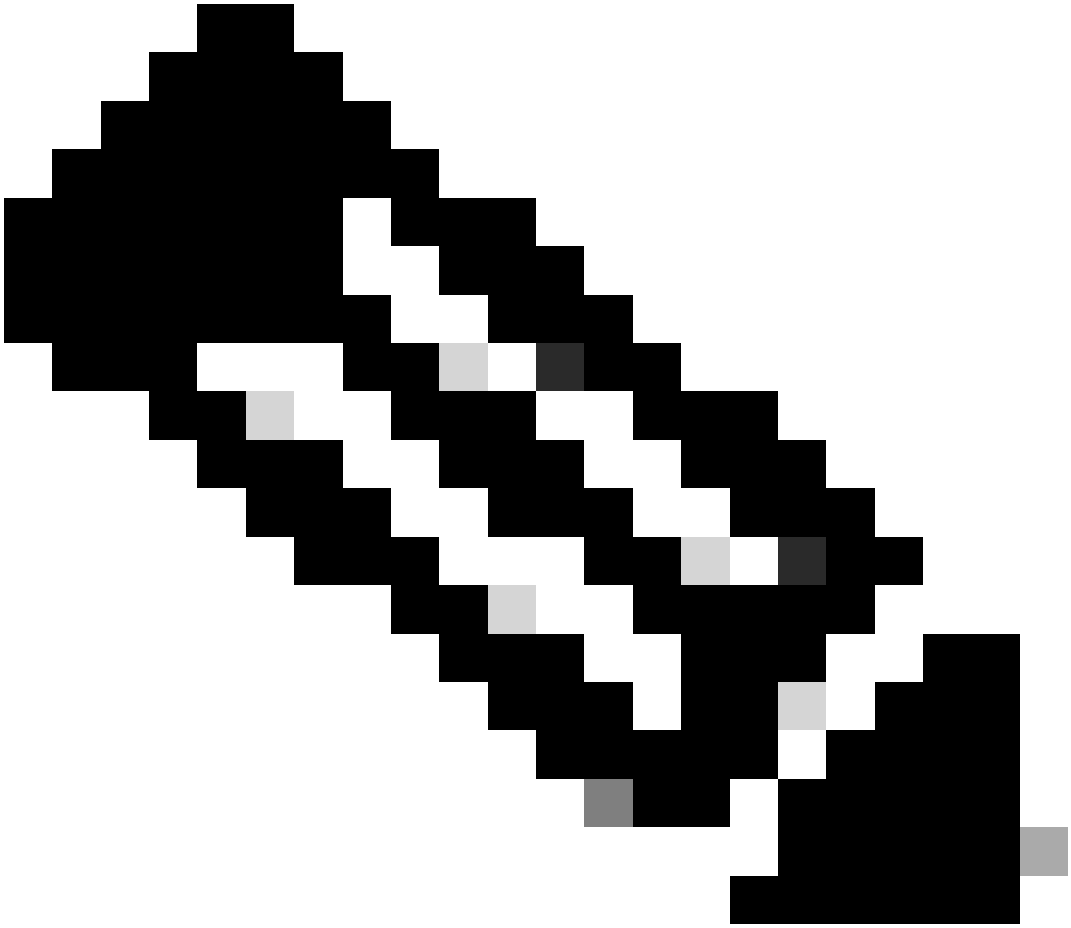
Usando uma Interface Não-WMI com uma MTU de 1200

Agora, suponha que você queira fragmentar em uma MTU menor, mas não queira que essa alteração afete nenhum outro tráfego. Sem problemas aqui, a configuração permanece a mesma somente a configuração da interface de origem apontará para uma SVI que foi criada apenas para essa finalidade. Altere a lista de métodos para apontar para esse novo grupo de servidores e esse grupo de servidores usa uma interface de origem que não é minha WMI e tem a MTU definida como 1200. Esta é a aparência da configuração:

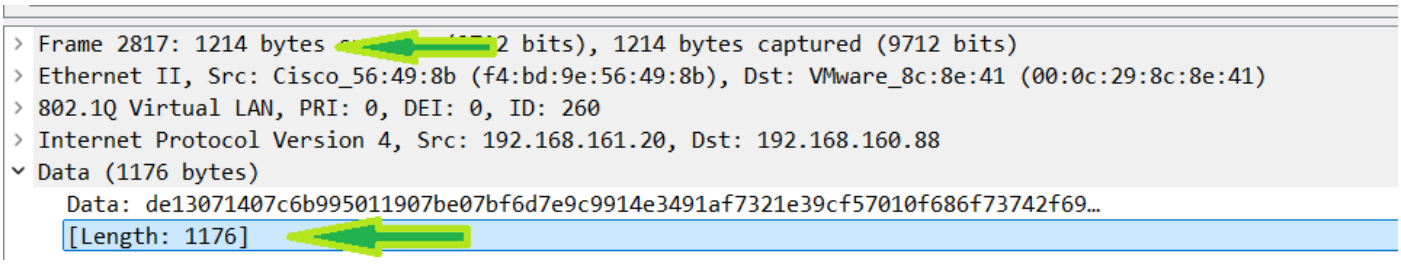
```
9800#show run aaa
!
aaa authentication dot1x TLS-AuthC group MTU1200
!
!
radius server ISE
 address ipv4 192.168.160.10 auth-port 1812 acct-port 1813
 key 6 _`gINMNXObFibbBMhNMFAbKUAAB
!
aaa group server radius MTU1200
 server name ISE
 ip radius source-interface Vlan261
 deadtime 5
!
9800#show run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

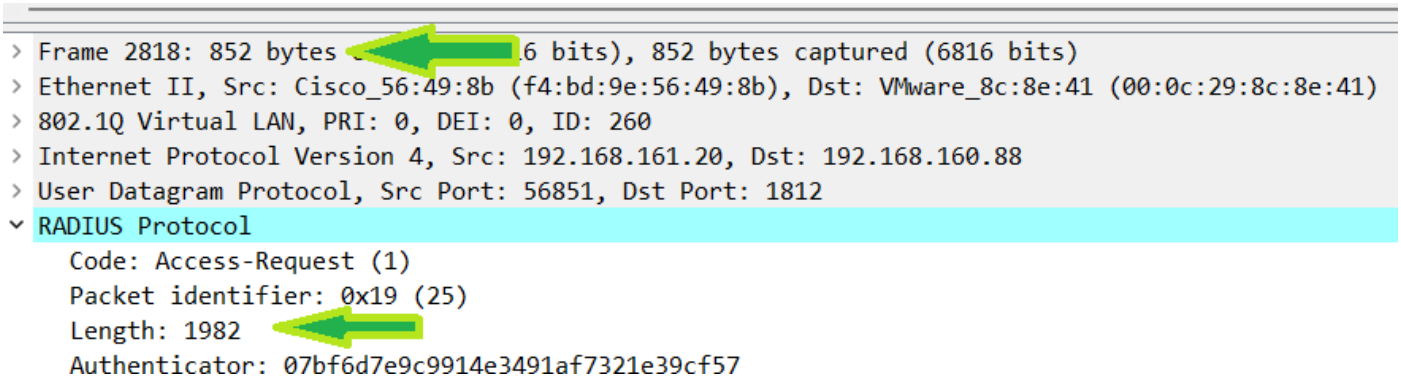
```
 ip address 192.168.161.20 255.255.255.0
 no ip proxy-arp
 ip mtu 1200
end
```

Em seguida, veja como os pacotes ficam com esse MTU mais baixo.



> Note: Reduzir a MTU e alterar o ponto de fragmentação não faz parte do novo comportamento. Isso sempre foi verdade. Se o comportamento padrão de fragmentação em 1396 não se encaixar no MTU, você sempre fragmentará em um ponto diferente. Ele faz parte desta seção apenas para ajudar a explicar as opções disponíveis.





Aqui, os dados RADIUS ainda são 1982 bytes, mas desta vez os dados foram fragmentados em 1176 em vez do padrão 1376 em que teriam sido fragmentados se a interface de origem não fosse usada. Lembre-se de que quando você define o MTU como 1500 e usa o comando source-interface, você fragmenta em 1480. Usar a configuração aqui permite que você manipule o tráfego para uma MTU mais baixa sem interferir com outro tráfego na WLC.

Usando um MTU de 9000 para Quadros Jumbo

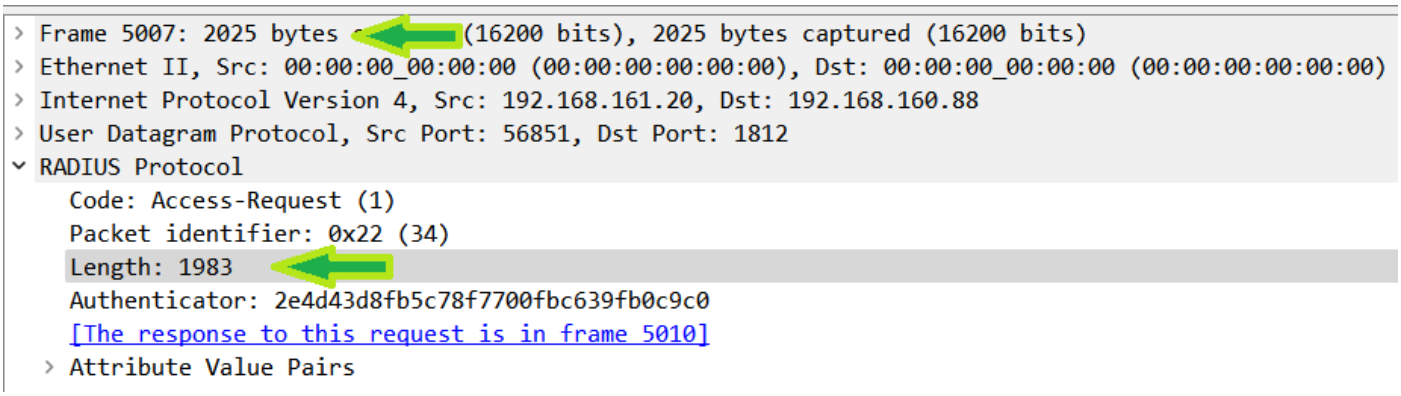
Como o recurso foi criado para a opção de enviar quadros jumbo, seria uma pena não testar isso também usando a interface não WMI da VLAN 261. No entanto, agora o MTU IP está definido como 9000. Uma observação rápida: para poder definir o MTU IP no SVI, você precisa definir o MTU para algo superior ao MTU IP. Você pode ver isso nesta configuração:

```
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
```

Aqui, observando a captura, você pode ver que o pacote nunca foi fragmentado. Ele foi enviado como um pacote inteiro com o tamanho de dados RADIUS em 1983. Lembre-se de que, para que isso funcione, o restante da rede precisa ser configurado para permitir a passagem de um pacote desse tamanho.

Outra coisa a ser observada aqui é que o MTU do cliente não mudou, de modo que o cliente ainda está fragmentando o pacote EAP em 1492. A diferença é que a WLC pode adicionar todos

os dados RADIUS necessários para enviar o pacote ao ISE sem precisar fragmentar os dados do cliente.



Conclusão

Quando você usa EAP-TLS, espera-se que o cliente envie seu certificado para o servidor AAA. Esses certificados são geralmente maiores que a MTU, portanto o cliente tem que fragmentá-la. O ponto no qual o cliente fragmenta os dados está muito próximo da MTU. Como o AP precisa adicionar o cabeçalho CAPWAP, o que o cliente está enviando deve ser fragmentado. A WLC recebe esses dois pacotes, os coloca juntos novamente, mas depois precisa fragmentá-los novamente para adicionar os dados RADIUS. Neste ponto, o administrador de rede recebe algum controle sobre como a WLC fragmenta o pacote EAP que o cliente enviou.

Se você adicionar o comando ip radius source-interface <interface que você deseja usar> ao grupo de servidores AAA, a WLC usará qualquer interface que você colocar em vez de (ou incluindo) a WMI. O uso desse comando também diz ao WLC para fragmentar em qualquer MTU dessa interface, em vez do padrão 1396. Dessa forma, você tem mais controle sobre como os pacotes estão se movendo pela rede.

Ao usar o Cisco Catalyst Center, o comando source interface é adicionado ao grupo de servidores, alterando assim o comportamento padrão.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.