在ISE中配置RADIUS KeyWrap

目录

简介

本文档介绍在思科ISE和思科交换机中配置RADIUS KeyWrap的过程。

先决条件

- dot1x知识
- RADIUS协议知识
- EAP知识

使用的组件

- ISE 3.2
- 软件版本为17.09.04a的思科C9300-24U
- Windows 10 PC

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

密钥包装是一种使用另一个密钥加密一个密钥值的技术。在RADIUS中使用相同的机制来加密密钥材料。此材料通常作为可扩展身份验证协议(EAP)身份验证的副产品生成，并在身份验证成功后返回到“访问接受”消息中。如果ISE在FIPS模式下运行，则此功能是必需的。

这提供了一个保护层，该层将实际的关键材料隔离起来，以防范潜在的攻击。基本上，威胁发起者根本无法访问底层关键材料，即使是在数据拦截的情况下。RADIUS密钥包装的主要目的是防止安

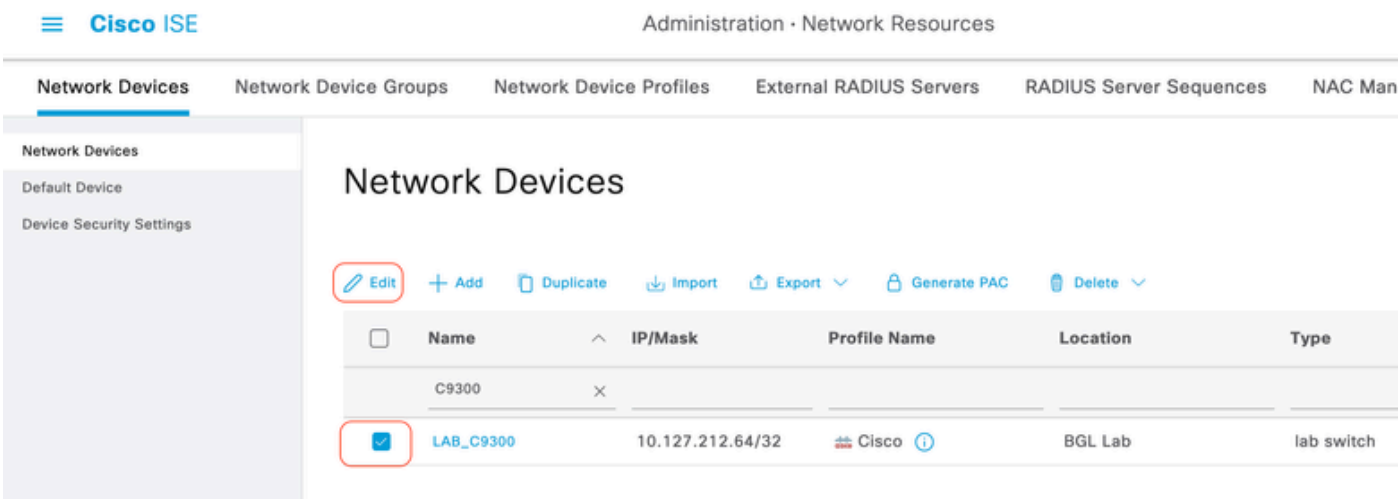
全数字内容的关键材料的曝光，特别是在大规模的企业级网络中。

在ISE中，密钥加密密钥用于使用AES加密和从RADIUS共享密钥分离的消息身份验证器代码密钥来加密密钥材料，以生成消息身份验证器代码。

配置

ISE

步骤 1：导航到Administration > Network Resources > Network Devices。点击要为其配置RADIUS KeyWrap的网络设备的复选框。单击Edit（如果已添加网络设备）。



步骤 2：展开RADIUS身份验证设置。单击Enable KeyWrap复选框。输入密钥加密密钥(Key Encryption Key)和消息验证器代码密钥(Message Authenticator Code Key)。Click Save.

General Settings

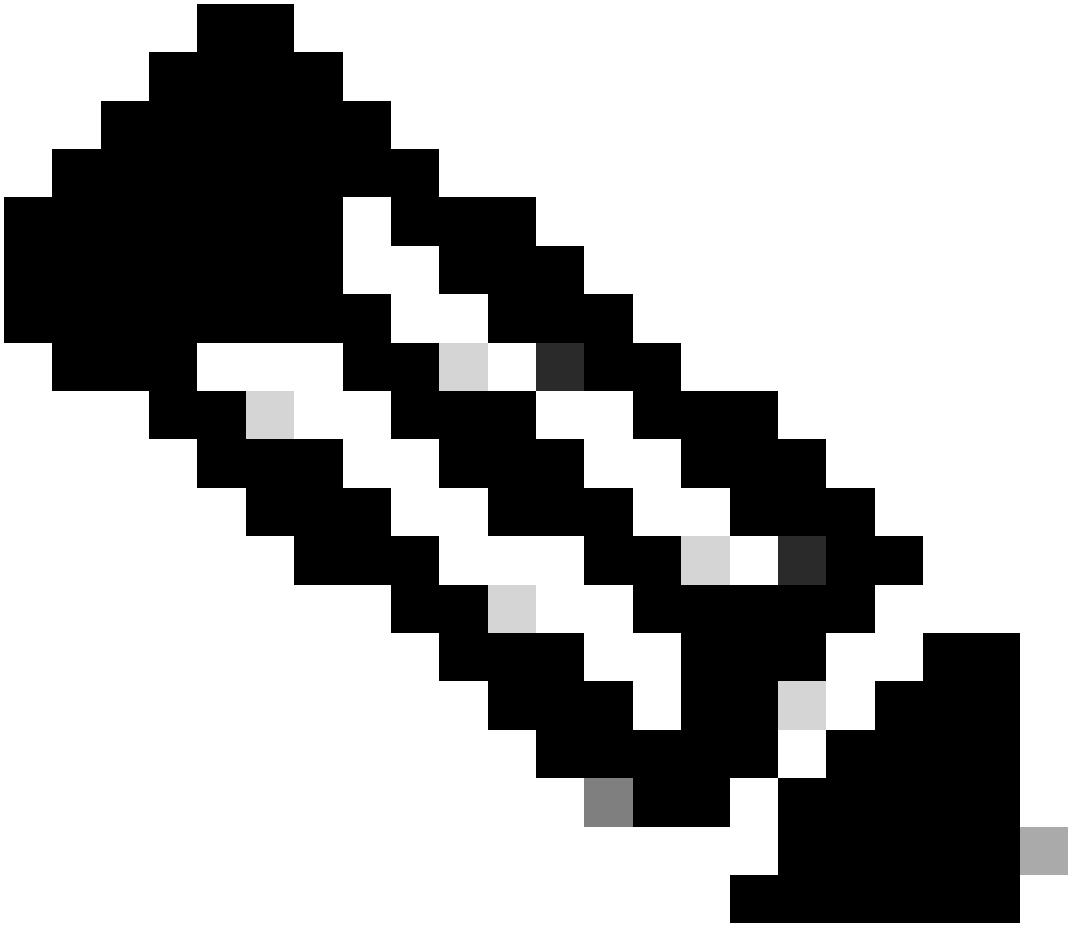
Enable KeyWrap

Key Encryption Key 22AB0###CA#1b2b1 Hide

Message Authenticator Code Key 12b1CcB202#2Cb1#bCa# Hide

Key Input Format

ASCII HEXADECIMAL



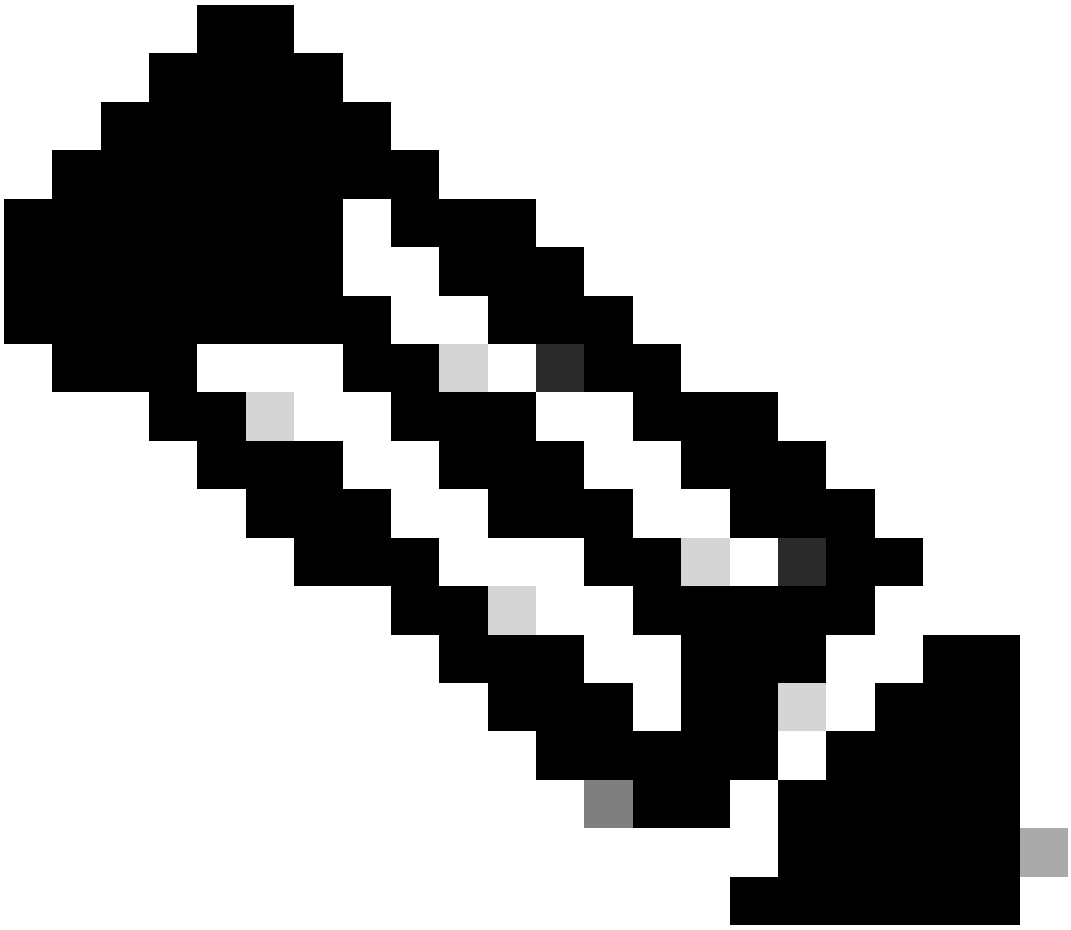
注意：密钥加密密钥和消息身份验证器代码密钥必须不同。

交换机

交换机中的AAA配置，以启用RADIUS KeyWrap功能。

```
aaa authentication dot1x default group RADGRP
aaa authorization network default group RADGRP
aaa accounting dot1x default start-stop group RADGRP

radius server ISERAD
 address ipv4 10.127.197.165 auth-port 1812 acct-port 1813
 key-wrap encryption-key 0 22AB0###CA#1b2b1 message-auth-code-key 0 12b1CcB202#2Cb1#bCa# format ascii
 key Iselab@123

aaa group server radius RADGRP
 server name ISERAD
 key-wrap enable
```

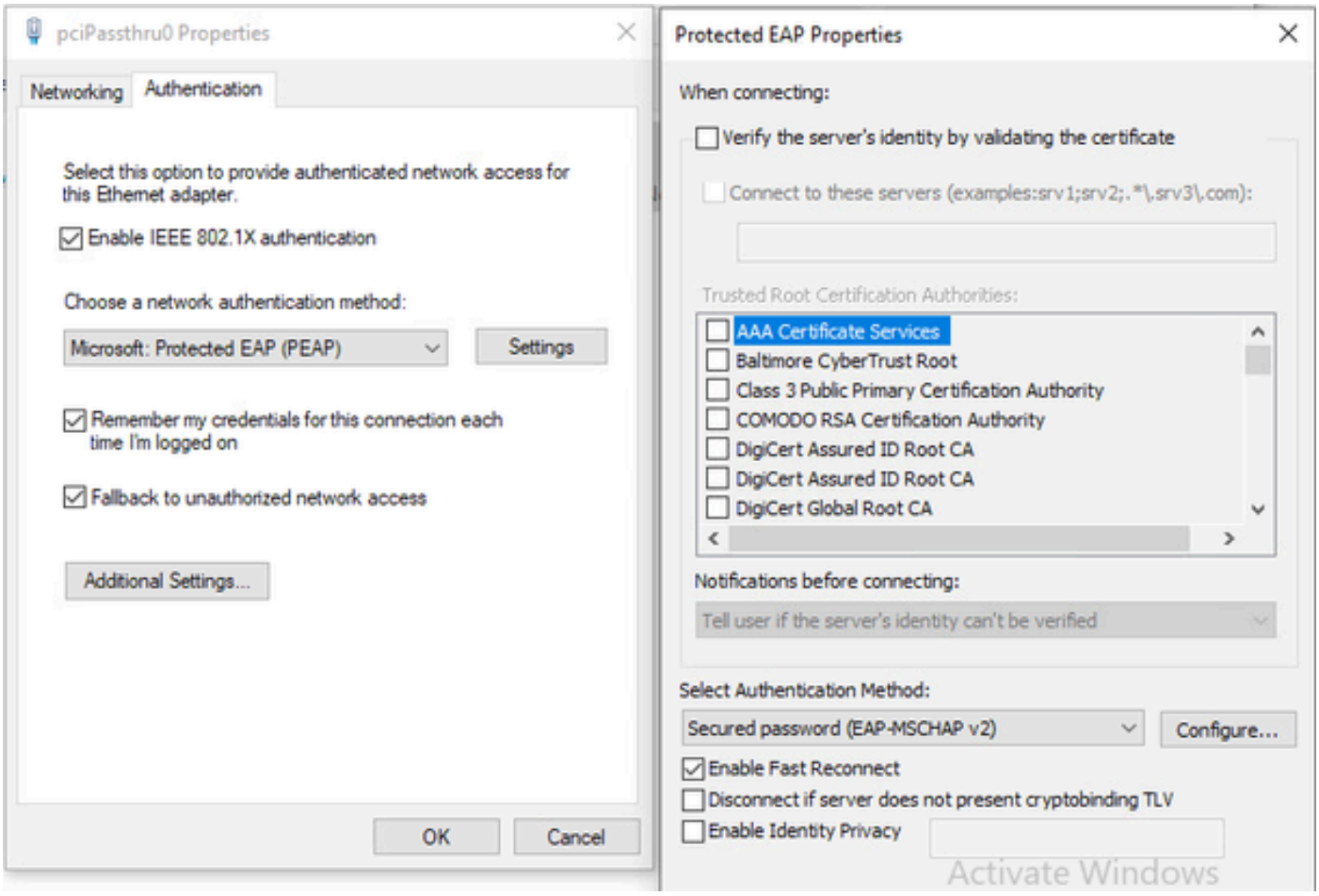
```
interface GigabitEthernet1/0/22
 switchport access vlan 302
 switchport mode access
 device-tracking attach-policy IPDT
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 dot1x pae authenticator
end
```



注意：encryption-key的长度必须为16个字符，并且必须是message-auth-code和20个字符。

PC

为PEAP-MSCHAPv2配置的Windows 10请求方。



验证

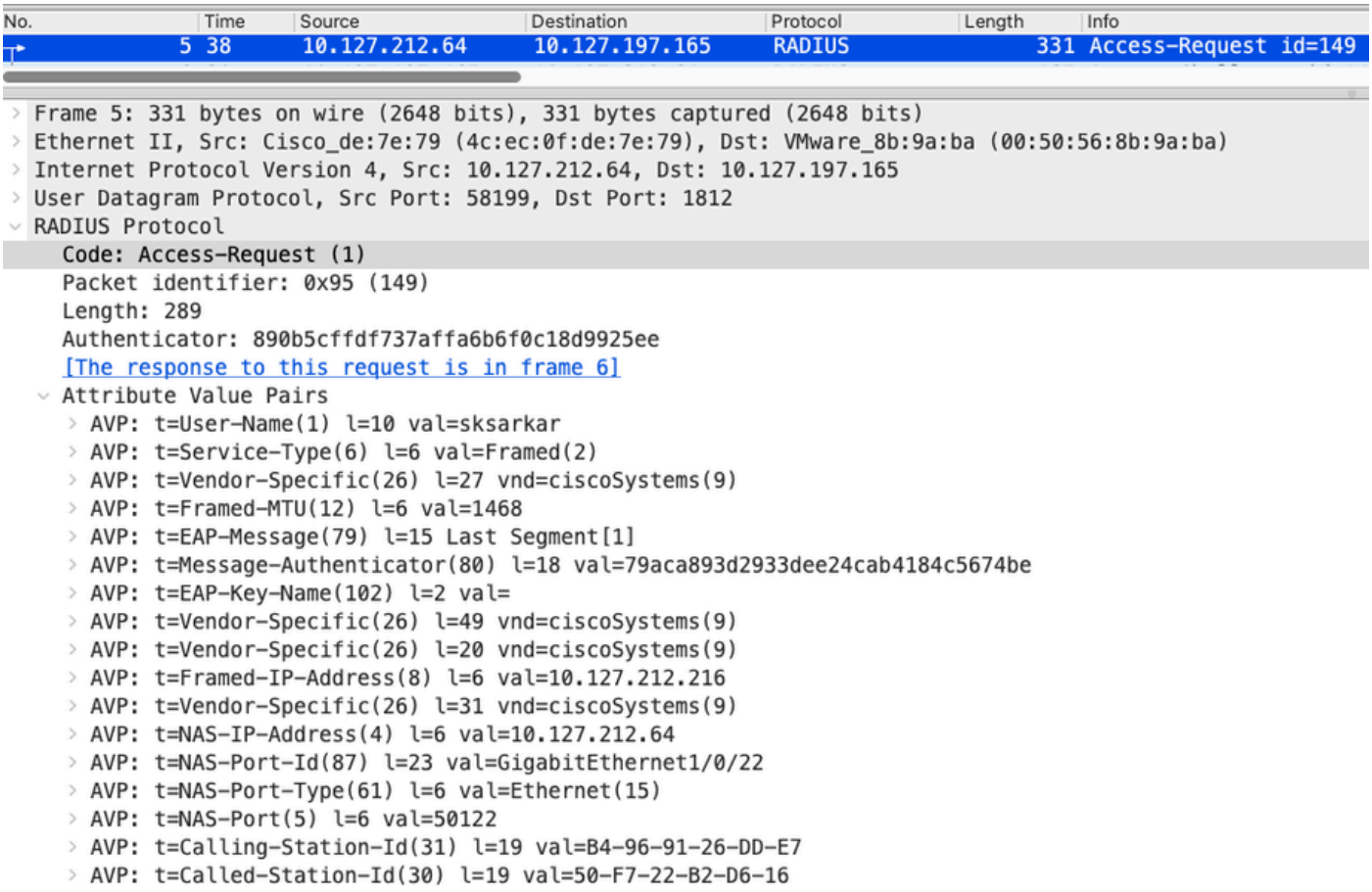
当交换机上未启用RADIUS KeyWrap功能时：

show radius server-group <服务器组名称>

命令输出必须显示Keywrap enabled:FALSE。

```
Switch#show radius server-group RADGRP
Server group RADGRP
Sharecount = 1 sg_unconfigured = FALSE
Type = standard Memlocks = 1
Server(10.127.197.165:1812,1813,ISERAD) Transactions:
Authen: 239 Author: 211 Acct: 200
Server_auto_test_enabled: FALSE
Keywrap enabled: FALSE
```

在数据包捕获中，您可以看到app-key、random-nonce和separate message-authenticator-code没有Cisco-AV-Pair属性。这表示交换机上禁用了RADIUS KeyWrap。

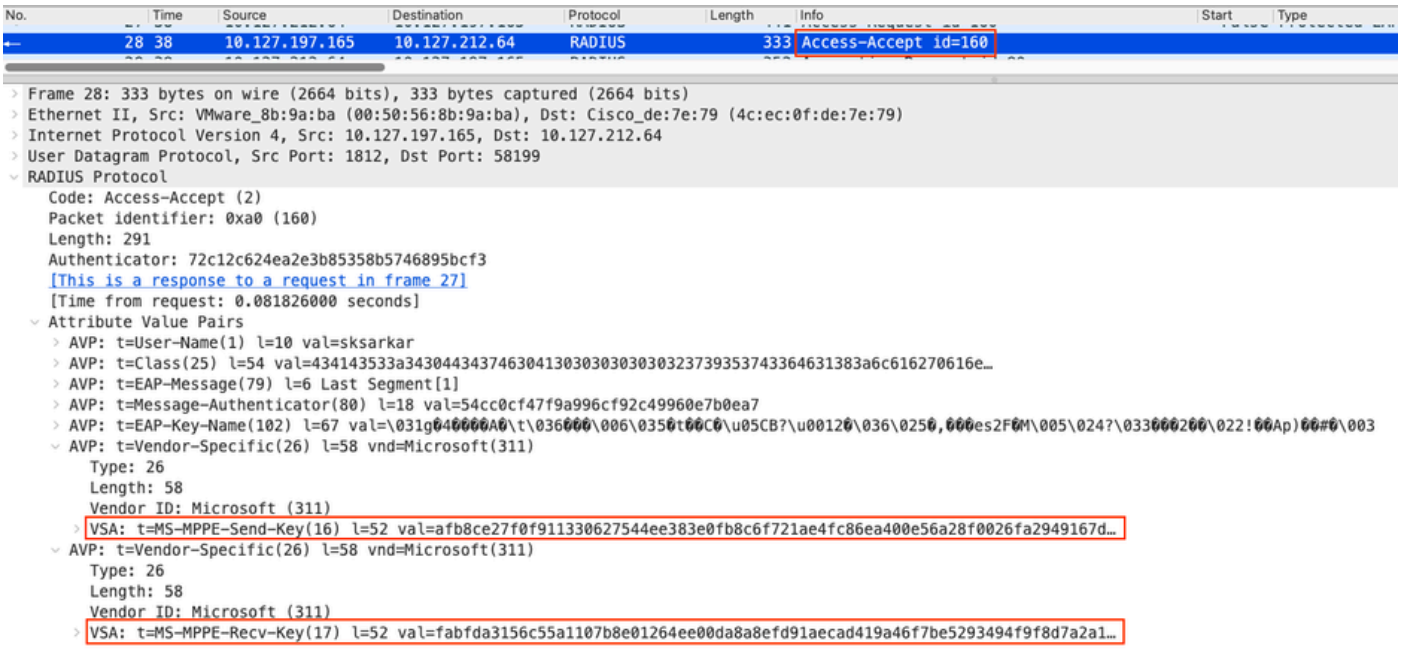


在ISE prrt-server.log中，您可以看到ISE仅验证完整性属性，即Message-Authenticator。

```
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
[1] User-Name - value: [sksarkar]
[4] NAS-IP-Address - value: [10.127.212.64]
[5] NAS-Port - value: [50122]
[6] Service-Type - value: [Framed]
[8] Framed-IP-Address - value: [10.127.212.216]
[12] Framed-MTU - value: [1468]
[30] Called-Station-ID - value: [50-F7-22-B2-D6-16]
[31] Calling-Station-ID - value: [B4-96-91-26-DD-E7]
[61] NAS-Port-Type - value: [Ethernet]
[79] EAP-Message - value: [<02><01><00><0d><01>sksarkar]
[80] Message-Authenticator - value: [<88>/`f

       |

        >

         <18><06>(

          ?
```

```
            ]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/22]
[102] EAP-Key-Name - value: []
[26] cisco-av-pair - value: [service-type=Framed]
[26] cisco-av-pair - value: [audit-session-id=40D47F0A0000002B9E06997E]
[26] cisco-av-pair - value: [method=dot1x]
[26] cisco-av-pair - value: [client-iif-id=292332370] ,RADIUSHandler.cpp:2455
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
Radius,2025-03-16 13:41:08,628,DEBUG,0x7f43b6e4b700,cntx=0000071664,sesn=labpan02/530700707/490,Calling
```

在Access-Accept数据包中，您可以看到MS-MPPE-Send-key和MS-MPPE-Recv-Key从RADIUS服务器发送到身份验证器。MS-MPPE指定EAP方法生成的密钥材料，可用于在对等方和身份验证器之间执行数据加密。这些32字节的密钥由RADIUS共享密钥、请求身份验证器和随机盐派生。



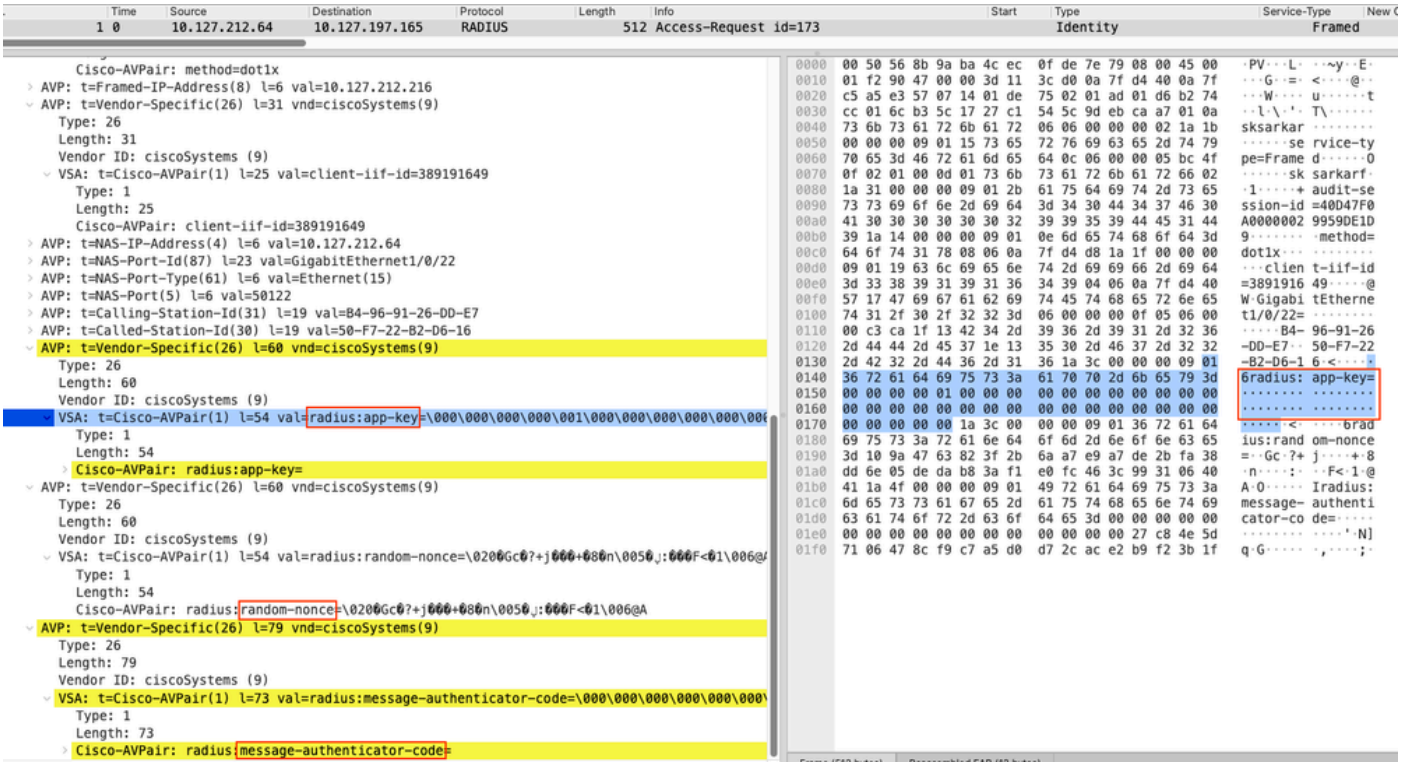
当在交换机和ISE上启用RADIUS KeyWrap功能时：

show radius server-group <服务器组名称>

命令输出必须显示Keywrap enabled:对。

```
Switch#show radius server-group RADGRP
Server group RADGRP
Sharecount = 1 sg_unconfigured = FALSE
Type = standard Memlocks = 1
Server(10.127.197.165:1812,1813,ISERAD) Transactions:
Authen: 239 Author: 211 Acct: 200
Server_auto_test_enabled: FALSE
Keywrap enabled: TRUE
```

在数据包捕获中，您可以看到app-key（无数据）、random-nonce和单独的消息 — authenticator-code存在Cisco-AV-Pair属性。这向RADIUS服务器指示身份验证器（交换机）支持RADIUS KeyWrap，并且服务器必须使用相同的身份验证。

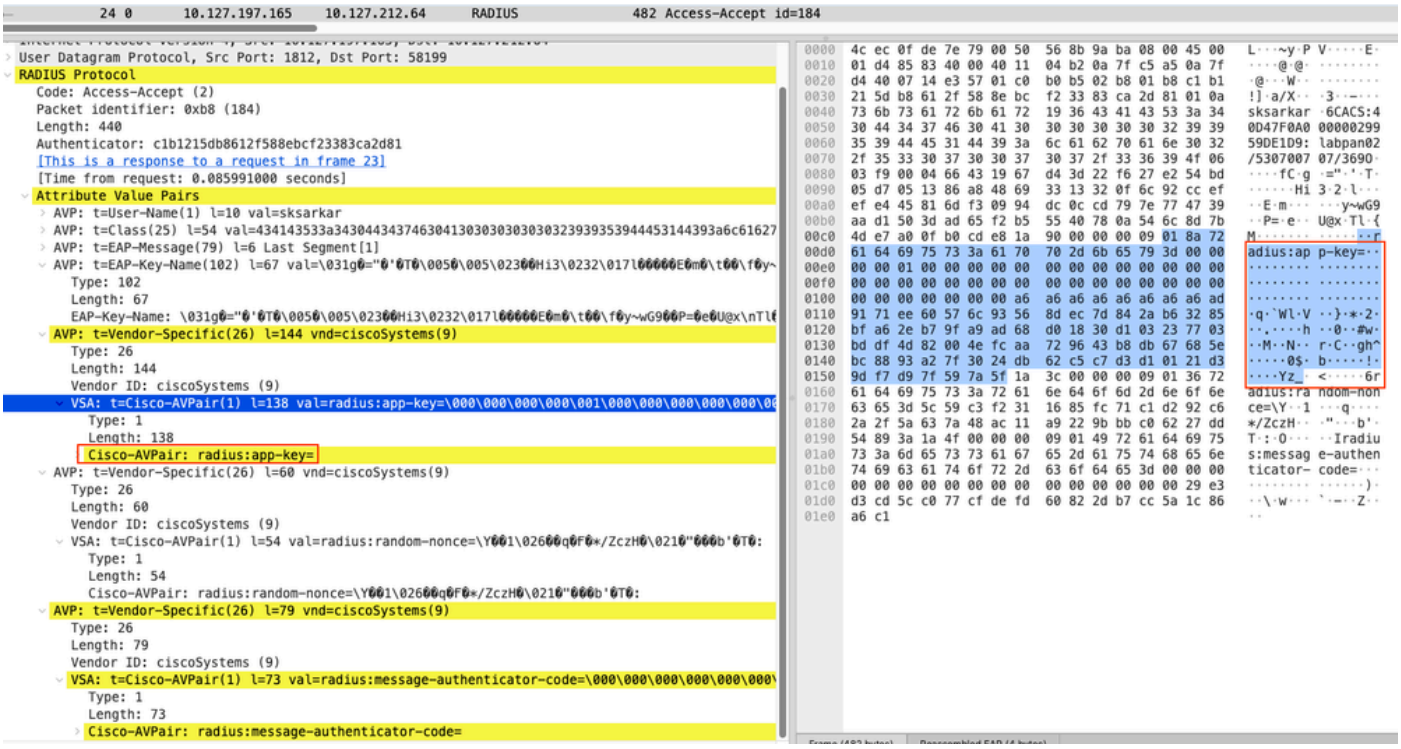


在ISE prrt-server.log中，您可以看到ISE验证属性app-key，并且random-nonce和message-authenticator-code出现在ACCESS-REQUEST数据包中。

```
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
[1] User-Name - value: [sksarkar]
[4] NAS-IP-Address - value: [10.127.212.64]
[5] NAS-Port - value: [50122]
[6] Service-Type - value: [Framed]
[12] Framed-MTU - value: [1468]
[30] Called-Station-ID - value: [50-F7-22-B2-D6-16]
[31] Calling-Station-ID - value: [B4-96-91-26-DD-E7]
[61] NAS-Port-Type - value: [Ethernet]
[79] EAP-Message - value: [<02><01><00><0d><01>sksarkar]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/22]
```

```
[102] EAP-Key-Name - value: []
[26] cisco-av-pair - value: [service-type=Framed]
[26] cisco-av-pair - value: [audit-session-id=40D47F0A000000319E1CAEFD]
[26] cisco-av-pair - value: [method=dot1x]
[26] cisco-av-pair - value: [client-iif-id=293712201]
[26] cisco-av-pair - value: [****]
[26] cisco-av-pair - value: [****]
[26] cisco-av-pair - value: [****] ,RADIUSHandler.cpp:2455
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
Radius,2025-03-16 14:05:20,882,DEBUG,0x7f43b704c700,cntx=0000072242,sesn=labpan02/530700707/539,Calling
```

在Access-Accept数据包中，您可以看到app-key属性中的加密密钥材料以及随机事件和消息身份验证器代码。这些属性旨在提供比当前定义的供应商特定MS-MPPE-Send-Key和MS-MPPE-Recv-Key属性更强的保护和更高的灵活性。



常见问题解答

1)是否需要在网络设备和ISE上启用RADIUS KeyWarp才能使其正常工作？

是，RADIUS KeyWrap需要在网络设备和ISE上启用才能正常运行。但是，如果仅在ISE上启用密钥绕行，但在网络设备上不启用，则身份验证仍然有效。但是，如果您在网络设备上启用它，但在ISE中未启用，则身份验证失败。

2)启用KeyWrap是否会增加ISE和网络设备的资源利用率？

否，启用KeyWrap后，ISE和网络设备的资源利用率不会显着提高。

3)RADIUS KeyWrap提供多少额外安全性？

由于RADIUS本身不为其负载提供任何加密，KeyWrap通过加密密钥材料提供额外的安全性。安全级别取决于使用哪种加密算法来加密密钥材料。在ISE中，AES用于加密密钥材料。

参考

- 用于交付密钥材料的思科供应商特定RADIUS属性

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。