

了解AnyConnect网络访问管理器日志

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[Enable \(event\) NAM记录](#)

[配置NAM数据包捕获](#)

[记录集](#)

[读NAM日志](#)

[记录网络连接的摘要，不用802.1x启用的验证](#)

[使用802.1x和PEAP在有线网络，记录网络连接的摘要](#)

简介

本文描述如何启用AnyConnect网络访问管理器(NAM)记录日志以及收集和解释日志。在本文包括的示例描述反射网络访问管理器采取的步骤验证客户端的不同的验证方案和日志。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

启用NAM记录

如果可能与NAM模块涉及的问题识别，第一步将启用延长的操作日志功能。当NAM模块运行时，在客户端终端必须执行这。

步骤1.打开AnyConnect窗口并且确保它在重点。

步骤2.按此密钥组合，**左岸堤防班次+留下艾尔特+ L**。没有无响应。

步骤3.在AnyConnect图标右键单击在Windows系统托盘。菜单冒出。

步骤4.选择**延长记录**，因此安排一个复选标记显示。被选派的NAM日志当前调试消息。

配置NAM数据包捕获

当延长的记录日志启用时，NAM也保持一数据包捕获缓冲区去。缓冲区默认情况下对1MB大约被限制。如果数据包捕获是需要的，增加缓冲区大小也许是有利的，因此捕获更多活动。要扩大缓冲区，必须手工修改XML设置文件。

步骤1:在Windows PC，请浏览对：

C:\ProgramData\Cisco\Cisco AnyConnect安全移动性客户端\网络访问管理器\系统\

步骤2.打开文件internalConfiguration.xml。

步骤3.找出XML标记<packetCaptureFileSize>1</packetCaptureFileSize>并且调整值到10 10MB缓冲区大小的，等等。

步骤4.重新启动客户端PC使更改生效。

记录集

NAM日志集通过诊断和报告工具(箭)完成，是AnyConnect套件模块。在安装程序中，请选择模块并且请使用AnnyConnect全双工安装ISO安装。Cisco媒介服务接口(MSI)安装程序可能也被找到在ISO里面。

在您启用延长的记录日志并且执行测验，运行箭并且通过对话后，默认情况下日志套件在Windows桌面查找。

除箭套件之外，NAM消息日志也是有用找出在NAM日志的相关数据。为了查找NAM消息日志，请导航对**Settings**窗口的AnyConnect >网络访问Manager>消息历史记录。消息日志包含每个网络连接事件时间戳，可以用于发现日志相关与事件。

读NAM日志

NAM日志，特别是在您启用延长的记录日志后，包含很多数据，多数是毫不相关的，并且可以忽略。此部分列出调试线路展示每个步骤NAM采取建立网络连接。当您通过日志时工作，这些关键短语可能是有用设置一部分的日志与问题有关。

记录网络连接的摘要，不用802.1x启用的验证

```
2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123: AccessStateMachine
current state = ACCESS_STOPPED, received userEvent = START
```

说明：这表明用户选择从NAM模块的网络，并且NAM接收userEvent开始。

538: TESTPC: May 16 2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123: AccessStateMachine new state = ACCESS_STARTED

539: TESTPC: May 16 2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123: NetworkStateMachine current state USER_T_DISCONNECTED, received access event ACCESS_STARTED

说明：访问状态机和网络状况系统开始。

545: TESTPC: May 16 2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Ipv4 {EFD4F0F0-CF25-4D88-B125-E748CD539DFF}: received Cancel event [state: COMPLETE]

说明：IPv4实例获得已取消为了重置状态。

547: TESTPC: May 16 2016 17:20:37.974 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: starting makeMatches...

549: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-6-INFO_MSG: %[tid=1412]: matching adapter {484E4FEF-392C-436F-97F0-CD7206CD7D48} and network test123 ...

说明：有ID的484E4FEF-392C-436F-97F0-CD7206CD7D48适配器选择连接到网络test123，是在NAM配置的网络连接名称。

551: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123: AccessStateMachine new state = ACCESS_ATTACHED

557: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123: AccessStateMachine current state = ACCESS_ATTACHED, received userEvent = CONNECT

说明：NAM顺利地从事此网络的适配器。现在NAM设法联合(连接)到偶然是无线)的此网络(：

561: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM current: state(STATE_DISCONNECTED_LINK_DOWN), event(EVENT_CONNECT)

562: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM state change: STATE_DISCONNECTED_LINK_DOWN -> STATE_ASSOCIATING

567: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Starting wifi connection, trying ssid test123 ...

568: TESTPC: May 16 2016 17:20:37.989 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Connection Association Started(openNoEncryption)

说明：openNoEncryption表明网络配置如开放。在无线局域网控制器上它使用MAC验证旁路(MAB)验证。

234: TESTPC: May 16 2016 17:20:38.020 +0600: %NAMSSO-7-DEBUG_MSG: %[tid=1912]: waiting for cs...

说明：电缆敷设船在NAM日志能被看到很多。这些是毫不相关的日志，并且应该忽略。

575: TESTPC: May 16 2016 17:20:38.020 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123: NetworkStateMachine new state USER_T_DISCONNECTED 236: TESTPC: May 16 2016 17:20:38.020 +0600: %NAMSSO-7-DEBUG_MSG: %[tid=1912]: Tx CP Msg: <?xml version="1.0" encoding="UTF-8"?><SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:ssc="http://www.cisco.com/ssc" encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"><SOAP-ENV:Body> <networkStateEvent> <sequenceNumber>16</sequenceNumber> <groupName>Local networks</groupName> <networkName>test123</networkName> <networkState>Associating</networkState> <adapterName>Intel(R) Centrino(R) Ultimate-N 6300 AGN</adapterName> <serverVerifiedName></serverVerifiedName> </networkStateEvent> </SOAP-ENV:Body></SOAP-ENV:Envelope>

说明：这些是用于的简单对象访问协议(SOAP)消息告诉AnyConnect GUI显示连接状态消息例如在这种情况下关联。在NAM窗口显示的所有错误消息可以在其中一个在可以用于容易地找出问题的日志的SOAP消息找到。

```
582: TESTPC: May 16 2016 17:20:38.020 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: {484E4FEF-392C-436F-97F0-CD7206CD7D48} - Received STATE_AUTHENTICATED
583: TESTPC: May 16 2016 17:20:38.020 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM
current: state(STATE_ASSOCIATING), event(EVENT_AUTH_SUCCESS)
```

说明：NAM接收AUTH_SUCCESS事件，误导，因为没有当前发生的验证。您是获得此事件，因为您连接对开放式网络，那么默认情况下验证是成功的。

```
595: TESTPC: May 16 2016 17:20:38.738 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network test123:
AccessStateMachine current state = ACCESS_ASSOCIATING, received adapterState = associated
```

说明：服务集标识(SSID)的关联是成功的，计时处理验证。

```
603: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-6-INFO_MSG:
%[tid=1412][mac=1,6,3c:a9:f4:33:ab:50]: Authentication not required.
604: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM
current: state(STATE_ASSOCIATED), event(EVENT_AUTH_SUCCESS)
605: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM
state change: STATE_ASSOCIATED -> STATE_AUTHENTICATED
```

说明：因为这是开放式网络，默认情况下验证。这时，NAM连接对网络和当前开始DHCP过程：

```
610: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: {484E4FEF-392C-436F-97F0-CD7206CD7D48} creating a new DHCP work
612: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-6-INFO_MSG:
%[tid=1412][mac=1,6,3c:a9:f4:33:ab:50]: {484E4FEF-392C-436F-97F0-CD7206CD7D48}: DHCP: Sending
DHCP request
613: TESTPC: May 16 2016 17:20:38.754 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: queueing DHCP work
642: TESTPC: May 16 2016 17:20:40.830 +0600: %NAM-7-DEBUG_MSG: %[tid=1448]: Ipv4 {484E4FEF-392C-436F-97F0-CD7206CD7D48}: connectivity test[03]: IP:10.201.230.196(255.255.255.224)
GW:10.201.230.193 [Success]
643: TESTPC: May 16 2016 17:20:40.830 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Ipv4 {484E4FEF-392C-436F-97F0-CD7206CD7D48}: received Success event [state: WAIT_FOR_CONNECTIVITY]
645: TESTPC: May 16 2016 17:20:40.845 +0600: %NAM-6-INFO_MSG:
%[tid=1412][mac=1,6,3c:a9:f4:33:ab:50]: {484E4FEF-392C-436F-97F0-CD7206CD7D48}: IP Address
Received: 10.201.230.196
646: TESTPC: May 16 2016 17:20:40.845 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Ipv4 Connectivity
Result: SUCCESS
```

说明：NAM成功地获取一个IP地址。

```
648: TESTPC: May 16 2016 17:20:40.845 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM
current: state(STATE_AUTHENTICATED), event(EVENT_IP_CONNECTIVITY)
649: TESTPC: May 16 2016 17:20:40.845 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: ACE: adapter SM
state change: STATE_AUTHENTICATED -> STATE_CONNECTED
```

说明：一旦IP地址接收NAM将发送ARP (地址解析协议)请求到网关(GET连接)。一旦ARP响应接收客户端连接。

使用802.1x和PEAP在有线网络，记录网络连接的摘要

```
1286: TESTPC: May 16 2016 17:55:17.138 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network WiredPEAP:
AccessStateMachine new state = ACCESS_STARTED
```

说明：开始的NAM连接到网络WiredPEAP。

```
1300: TESTPC: May 16 2016 17:55:17.138 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Binding adapter
Intel(R) 82579LM Gigabit Network Connection and user auth for network WiredPEAP
1303: TESTPC: May 16 2016 17:55:17.138 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network WiredPEAP:
AccessStateMachine new state = ACCESS_ATTACHED
```

说明：NAM匹配适配器对此网络。

```
1309: TESTPC: May 16 2016 17:55:17.138 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: Network WiredPEAP:
AccessStateMachine current state = ACCESS_ATTACHED, received userEvent = CONNECT
1342: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: STATE (4)
S_enterStateAux called with state = CONNECTING (dot1x_sm.c 142)
```

说明：NAM开始的连接对此有线网络。

```
1351: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
Sent start frame (dot1x_sm.c 117)
```

说明：客户端发送EAPOL_START。

```
1388: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: PORT (3)
net: RECV (status: UP, AUTO) (portMsg.c 658)
1389: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
recvd EAP IDENTITY frame (dot1x_util.c 264)
1397: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP State: EAP_STATE_IDENTITY (eap_auth_client.c 940)
```

说明：客户端收到从交换机的标识请求，它当前寻找凭证退还。

```
1406: TESTPC: May 16 2016 17:55:17.154 +0600: %NAM-7-DEBUG_MSG: %[tid=1464]: EAP-CB: credential
requested: sync=8, session-id=1, handle=00AE1FFC, type=AC_CRED_SESSION_START
1426: TESTPC: May 16 2016 17:55:17.169 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: EAP: processing
credential request: sync=8, session-id=1, eap-handle=00AE1FFC, eap-level=0, auth-level=0,
protected=0, type=CRED_REQ_SESSION_START
1458: TESTPC: May 16 2016 17:55:17.169 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Trying fast
reauthentication for unprotected identity anonymous
1464: TESTPC: May 16 2016 17:55:17.169 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: EAP: credential
request completed, response sent: sync=9
```

说明：默认情况下，Anyconnect发送匿名作为无保护的标识(outter标识)，那么此处它尝试匿名并且看到服务器是否对它是好的。事实标识是匿名的与主机/匿名相对表明它是用户认证，而不是计算机验证。

```
1492: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
recvd EAP TLS frame (dotlx_util.c 293)
```

说明：RADIUS服务器发送扩展验证传输层安全(EAP-TLS)帧，不用任何内容。其目的将协商与客户端的EAP-TLS协议。

```
1516: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-6-INFO_MSG: %[tid=1412]: EAP: EAP suggested
by server: eapTls
1517: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-6-INFO_MSG: %[tid=1412]: EAP: EAP requested
by client: eapPeap
1518: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: EAP: EAP methods
sent: sync=10
1519: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]: EAP: credential
request 10: state transition: PENDING -> RESPONDED
```

说明：NAM认可服务器的请求使用EAP-TLS，但是客户端配置使用Protected Extensible Authentication Protocol (PEAP)。这是原因NAM退还PEAP的一个还价。

```
1520: TESTPC: May 16 2016 17:55:17.185 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: Authentication state transition:
AUTH_STATE_UNPROTECTED_IDENTITY_SENT_FOR_FAST_REAUTHENTICATION ->
AUTH_STATE_UNPROTECTED_IDENTITY_ACCEPTED
```

说明：RADIUS服务器接受outter/无保护的标识。

```
1551: TESTPC: May 16 2016 17:55:17.200 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
recvd EAP PEAP frame (dotlx_util.c 305)
1563: TESTPC: May 16 2016 17:55:17.200 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP-PEAP: SSL handshake start (eap_auth_tls_p.c 409)
```

说明：PEAP的已保护部分(设立安全隧道交换内在凭证)开始，在客户端接收从RADIUS服务器的确认继续使用PEAP后。

```
1565: TESTPC: May 16 2016 17:55:17.200 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL STATE: SSLv3 write client hello A (eap_auth_tls_p.c 394)
1566: TESTPC: May 16 2016 17:55:17.200 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL STATE: SSLv3 read server hello A (eap_auth_tls_p.c 394)
```

说明：NAM发送客户端在EAP信息封装的Hello并且等待服务器问候来。服务器问候包含ISE证书，因此采取一些时间完成转接。

```
1622: TESTPC: May 16 2016 17:55:17.216 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: 8021X (4)
```

```
recvd EAP PEAP frame (dotlx_util.c 305)
1632: TESTPC: May 16 2016 17:55:17.216 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL STATE: SSLv3 read server hello A (eap_auth_tls_p.c 394)
1633: TESTPC: May 16 2016 17:55:17.216 +0600: %NAM-6-INFO_MSG: %[tid=1468][comp=SAE]: CERT (0)
looking up: "/CN=ISE20-1.kurmai.com" (lookup.c 100)
1634: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-6-INFO_MSG: %[tid=1468][comp=SAE]: CERT (0)
Certificate not found: "/CN=ISE20-1.kurmai.com" (lookup.c 133)
1646: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL_ERROR_WANT_X509_LOOKUP (eap_auth_tls_p.c 193)
```

说明：NAM解压缩ISE服务器的主题名称从服务器证书的。因为它没有在信任存储安装的服务器证书，您没找到它那里。

```
1649: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (5)
EAP_EVENT_CRED_REQUEST queued (eapCredProcess.c 496)
1650: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-7-DEBUG_MSG: %[tid=1464][comp=SAE]: EAP (5)
EAP: CRED_REQUEST (eapMessage.c 355)
1662: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Getting credentials
from logon.
1685: TESTPC: May 16 2016 17:55:17.232 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: ...resumed
```

说明：在通道设立后，NAM寻找内在/保护将发送的标识对RADIUS服务器。在这种情况下，“请自动地使用我的Windows登录名字，并且密码”选项在有线的适配器启用，因此NAM使用windows登录凭证而不是询问用户它。

```
1700: TESTPC: May 16 2016 17:55:17.247 +0600: %NAM-7-DEBUG_MSG: %[tid=1464][comp=SAE]: EAP (0)
SSL STATE: SSLv3 write client key exchange A (eap_auth_tls_p.c 394)
1701: TESTPC: May 16 2016 17:55:17.247 +0600: %NAM-7-DEBUG_MSG: %[tid=1464][comp=SAE]: EAP (0)
SSL STATE: SSLv3 write change cipher spec A (eap_auth_tls_p.c 394)
1750: TESTPC: May 16 2016 17:55:17.278 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
SSL STATE: SSL negotiation finished successfully (eap_auth_tls_p.c 394)
1751: TESTPC: May 16 2016 17:55:17.278 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP-PEAP: SSL handshake done (eap_auth_tls_p.c 425)
1752: TESTPC: May 16 2016 17:55:17.278 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP-PEAP: New session. (eap_auth_tls_p.c 433)
1753: TESTPC: May 16 2016 17:55:17.278 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: EAP (0)
EAP-PEAP: session cipher AES256-SHA. (eap_auth_tls_p.c 441)
```

说明：NAM发送客户端密钥和密码器spec到服务器并且接收确认。SSL协商是成功的，并且通道设立。

```
1810: TESTPC: May 16 2016 17:55:17.294 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Protected
identity/(Username) sent.
1814: TESTPC: May 16 2016 17:55:17.294 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: Authentication state transition:
AUTH_STATE_UNPROTECTED_IDENTITY_ACCEPTED -> AUTH_STATE_PROTECTED_IDENTITY_SENT
1883: TESTPC: May 16 2016 17:55:17.310 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: Authentication state transition: AUTH_STATE_PROTECTED_IDENTITY_SENT -
> AUTH_STATE_PROTECTED_IDENTITY_ACCEPTED
```

说明：已保护标识发送到服务器，接受标识。现在服务器请求密码。

```
1902: TESTPC: May 16 2016 17:55:17.310 +0600: %NAM-7-DEBUG_MSG: %[tid=1464][comp=SAE]: EAP (5)
deferred password request (eapRequest.c 147)
1918: TESTPC: May 16 2016 17:55:17.310 +0600: %NAM-6-INFO_MSG: %[tid=1412]: Protected password
sent.
1921: TESTPC: May 16 2016 17:55:17.325 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: Authentication state transition:
AUTH_STATE_PROTECTED_IDENTITY_ACCEPTED -> AUTH_STATE_CREDENTIAL_SENT
```

说明：NAM接收密码请求和发送密码对服务器。

```
2076: TESTPC: May 16 2016 17:55:17.856 +0600: %NAM-7-DEBUG_MSG: %[tid=1412]:
Auth[WiredPEAP:user-auth]: Authentication state transition: AUTH_STATE_CREDENTIAL_SENT ->
AUTH_STATE_SUCCESS
2077: TESTPC: May 16 2016 17:55:17.856 +0600: %NAM-7-DEBUG_MSG: %[tid=1468][comp=SAE]: STATE (4)
S_enterStateAux called with state = AUTHENTICATED (dot1x_sm.c 142)
```

说明：服务器接收密码，验证它并且发送EAP成功。验证这时是成功的，并且客户端继续作为它从DHCP获得IP地址。