与Microsoft NP配置示例的5760/3850系列WLC PEAP验证

文档ID117684

已更新：2014年5月05日

贡献用Surendra BG， Cisco TAC工程师。

下载 pdf文档
打印
反馈

相关产品

- Cisco 5700系列无线局域网控制器
- 远程用户拨入认证系统(RADIUS)

目录

简介

本文描述如何配置与微软询问握手认证协议版本2 (MS-CHAP v2)验证的Protected Extensible Authentication Protocol (PEAP)在一思科聚合的访问无线局域网(WLAN)部署用Microsoft网络策略服务器(NP)作为RADIUS服务器。

先决条件

要求

思科建议您有这些主题知识，在您尝试在本文前描述的配置：

- 基本Microsoft Windows版本2008安装
- 思科聚合访问WLAN控制器安装

保证这些需求符合，在您尝试此配置前：

- 安装在其中每一个的MS Windows服务器版本2008操作系统(OS)在测试实验室的服务器。
- 更新所有服务包。
- 安装控制器和轻量级接入点(拉普)。
- 配置最新的软件更新。

注意：对于初始安装和配置信息思科的聚合访问WLAN控制器，参考CT5760控制器和Catalyst 3850交换机配置示例Cisco条款。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 5760系列WLAN控制器版本3.3.2 (下一代配线间(NGWC))
- Cisco 3602系列LAP
- 有英特尔PROset请求方的Microsoft Windows XP
- Microsoft Windows运行NP以域控制器角色的版本2008服务器
- Cisco Catalyst 3560系列交换机

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。

背景信息

PEAP使用传输级安全性(TLS)为了创建在一个验证的PEAP客户端之间的一个已加密信道，例如一无线笔记本电脑和一PEAP验证器，例如Microsoft NP或所有RADIUS服务器。PEAP不指定认证方法，然而其他扩展验证协议的(EAPs)提供附加安全性，例如EAP-MS-CHAP v2，能通过Tls加密的信道运行PEAP提供。PEAP认证过程包括两个主要阶段。

PEAP 第一阶段：Tls加密的信道

有接入点(AP)的无线客户端关联。在一个安全关联创建在客户端和AP之间前， IEEE 802.11根据关联提供开放式系统或共享密钥认证。在IEEE基于802.11的关联成功设立在客户端和AP之间后，TLS会话协商与AP。

在验证顺利地完成在无线客户端和NP之间后， TLS会话协商在客户端和NP之间。在此协商内派生的密钥用于为了加密所有随后的通信。

PEAP 第二阶段：采用 EAP 身份验证的通信

EAP通信，包括EAP协商，发生在PEAP认证过程的第一阶段的内PEAP创建的TLS信道里面。NP验证有EAP-MS-CHAP v2的无线客户端。LAP和仅控制器转发消息在无线客户端和RADIUS服务器之间。WLAN控制器(WLC)和LAP不能解密消息，因为WLC不是TLS终端。

这是成功认证尝试的RADIUS数据顺序，用户把PEAP-MS-CHAP v2供给有效基于密码的凭证：

1. NP发送Request信息的标识给客户端：
   `EAP-Request/Identity`
2. 客户端回复一个身份响应消息：
   `EAP-Response/Identity`
3. NP传送MS-CHAP v2询问消息：
   `EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge)`
4. 客户端回复一个 MS-CHAP v2 质询和响应：
   `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response)`
5. 当服务器成功验证客户端时， NP回应MS-CHAP v2成功数据包：
   `EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success)`
6. 当客户端成功验证服务器时，客户端回应MS-CHAP v2成功数据包：
   `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success)`
7. NP发送指示成功认证的EAP类型长度值(TLV)。

8. 客户端回复一个 EAP-TLV 状态成功消息。

9. 服务器完成验证并且传送在纯文本的EAP成功信息。如果部署了 VLAN 用于客户端隔离，则此消息中还包含 VLAN 属性。

配置

请使用此部分为了配置与MS-CHAP v2验证的PEAP在与Microsoft NP的一思科聚合的访问WLC部署作为RADIUS服务器。

网络图

在本例中， Microsoft Windows版本2008服务器执行这些角色：

- **wireless.com**域的域控制器
- 域名系统 (DNS) 服务器
- Certificate Authority (CA)服务器
- NP为了验证无线用户
- 激活目录(AD)为了维护用户数据库

服务器连接对有线网络通过Layer2 (L2)交换机，如显示。 WLC和已注册LAP也连接对网络通过L2交换机。

无线客户端使用wi-fi受保护的访问2 (WPA2) - PEAP-MS-CHAP v2验证为了连接到无线网络。

配置

在此部分描述的配置在两个步骤完成：

1. 配置与CLI或GUI的5760/3850系列WLC。
2. 配置NP、域控制器和用户帐户的Microsoft Windows版本2008服务器在AD。

配置与CLI的聚合的访问WLCs

完成这些步骤为了配置需要的客户端的VLAN WLAN和映射它到与CLI的验证方法列表：

> **注意**：保证**dot1x系统验证控制**在WLC启用，或者dot1x不工作。

1. 启用**AAA新模型**功能。
2. 配置 RADIUS 服务器。
3. 添加服务器到服务器组。
4. 映射服务器组对方法列表。
5. 映射方法列表对WLAN。

```
aaa new-model
!
!
aaa group server radius Microsoft_NPS
 server name Microsoft_NPS
!
aaa authentication dot1x Microsoft_NPS group Microsoft_NPS aaa authorization network
Microsoft_NPS group Microsoft_NPS
radius server Microsoft_NPS
 address ipv4 10.104.208.96 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 10
 key Cisco123 wlan Microsoft_NPS 8 Microsoft_NPS
 client vlan VLAN0020
 no exclusionlist
 security dot1x authentication-list Microsoft_NPS
 session-timeout 1800
 no shutdown
```

配置与GUI的聚合的访问WLCs

完成这些步骤为了配置与GUI的聚合的访问WLCs ：

1. 启用**dot1x系统验证控制**：

2. 导航对**Configuration>安全>**AAA为了添加RADIUS服务器：

3. 导航到**RADIUS>服务器**，点击**新**，并且与共享机密一起更新RADIUS服务器的IP地址。共享机密应该匹配在RADIUS服务器配置的共享机密。

   在您配置RADIUS服务器后， Server选项应该看起来与此相似：

4. 配置服务器组并且选择组类型的**Radius**。然后，请添加该的RADIUS服务器您创建在上一步：

   服务器组应该看起来与此相似在配置以后：

5. 验证方法列表类型和**组的**挑选**dot1x**组类型的。然后，请映射该的服务器组您配置在上一步：

   验证方法列表应该看起来与此相似在配置以后：

6. 选择授权方法列表类型和**组的网络**组类型的。然后，请映射该的服务器组您配置在上一步：

   授权方法列表应该看起来与此相似在配置以后：

7. 导航**配置>无线**和点击**WLAN**选项卡。配置用户能连接和变得已验证通过有EAP验证的Microsoft NP服务器的一新的WLAN ：

   安全L2选项卡应该看起来与此相似在配置以后：

8. 映射该的方法列表您配置在上一个步骤。这帮助验证客户端到正确服务器。

在Microsoft Windows版本2008服务器的配置

此部分描述Microsoft Windows版本2008服务器的完整的配置。配置在六个步骤完成：

1. 配置服务器作为域控制器。
2. 安装并且配置服务器作为CA服务器。
3. 安装NP。
4. 安装证书。
5. 配置PEAP验证的NP。
6. 添加用户到AD。

配置Microsoft Windows 2008服务器作为域控制器

完成这些步骤为了配置Microsoft Windows版本2008服务器作为域控制器：

1. 导航**开始**>Server **Manager>角色**>Add**角色**。

2. 单击 **Next**。

3. 检查**活动目录域Services复选框**并且**其次**单击。

4. 查看**介绍对活动目录域服务**并且**其次**单击。

5. 点击**安装**为了开始安装过程。

   安装继续并且完成。

6. 点击Close此向导并且启动活动目录域服务安装向导(dcpromo.exe)为了继续AD的安装和配置。

7. 其次单击为了运行活动目录域服务安装向导。

8. 查看关于操作系统的兼容性的信息并且其次单击。

9. 点击创建在一个新的森林单选按钮的一新域并且其次单击为了创建新域。

10. 输入全双工DNS名对于新域(在本例中的wireless.com)并且其次单击。

11. 选择您的域的森林功能级并且其次单击。

12. 选择您的域的域功能级并且其次单击。

13. 检查DNS服务器复选框并且其次单击。

14. 当活动目录域服务安装向导弹出窗口出现为了创建在DNS的一新区域域的时，请点击是。

15. 选择文件夹您希望AD使用文件并且其次单击。

16. 输入管理员密码并且其次单击。

17. 查看您的选择并且其次单击。

安装收益。

18. 点击**芬通社**为了关闭向导。

19. 重新启动服务器为了更改能生效。

安装并且配置Microsoft Windows版本2008服务器作为CA服务器

与EAP-MS-CHAP v2的PEAP验证RADIUS服务器根据是存在服务器的证书。另外，由客户端计算机委托必须由公共CA发出的服务器证书。即公共CA证书在客户端计算机证书存储的可靠的根证书颁发机构文件夹已经存在。

完成这些步骤为了配置Microsoft Windows版本2008服务器作为发行证书对NP的CA服务器：

1. 导航**开始**>Server **Manager>角色**>Add**角色**。

2. 单击 **Next**。

3. 检查**活动目录证书服务**复选框并且**其次**单击。

4. 查看**介绍对活动目录证书服务**并且**其次**单击。

5. 检查**认证机关**复选框并且**其次**单击。

6. 点击**企业**单选按钮并且**其次**单击。

7. 点击**根CA**单选按钮并且**其次**单击。

8. 点击**创建一个新的专用密钥**单选按钮并且**其次**单击。

9. 单击**其次**在**CA**窗口的**配置的加密算法**。

10. **其次**单击为了接受**此CA**默认名称的**公用名称**。

11. 选择CA证书是有效的时间长度并且**其次**单击。

12. **其次**单击为了接受**证书数据库位置**默认位置。

13. 查看配置并且点击**安装**为了开始**活动目录证书服务**。

14. 在安装完成后，请点击**Close**。

安装在Microsoft Windows版本2008服务器的NP

> **注意**：使用在此部分描述的设置， NP用于，当RADIUS服务器为了验证有PEAP验证的无线客户端。

完成这些步骤为了安装和配置在Microsoft Windows版本2008服务器的NP ：

1. 导航**开始**>Server **Manager>角色**>Add**角色**。

2. 单击 **Next**。

3. 检查**网络策略并且访问Services复选框**并且**其次**单击。

4. 查看**介绍对网络策略并且访问服务**并且**其次**单击。

5. 检查**网络策略服务器**复选框并且**其次**单击。

6. 查看确认并且点击**安装**。

在安装完成后，屏幕类似于此应该出现：

7. 单击 **Close**。

安装证书

完成这些步骤为了安装NP的计算机证书：

1. 点击**开始**，输入微软管理控制台(MMC)，并且按回车。
2. 导航对**File>添加/删除管理单元**。
3. 选择**证书**并且单击**添加**。

4. 点击**计算机帐户**单选按钮并且**其次**单击。

5. 点击**本地计算机**单选按钮并且点击**芬通社**。

6. 点击OK键为了返回到MMC。

7. 展开**证书(本地计算机)**和**个人**文件夹，并且点击**证书**。

8. 用鼠标右键单击在CA证书的白色空间，并且选择**所有任务>请求新证书**。

9. 单击 **Next**。

10. 点击**域控制器**复选框，并且单击**登记**。

    注意：如果客户端验证发生故障由于EAP验证错误，则请保证所有复选框被检查此**证书登记**页，在您单击**登记前**。这创建大约三证书。

11. 一旦证书安装，请点击**芬通社**。

    NP证书当前安装。

12. 保证该**客户端验证，服务器验证**出现在证书的打算的目的列。

配置PEAP-MS-CHAP v2验证的网络策略服务器服务

完成这些步骤为了配置验证的NP ：

1. 导航到**Start > Administrative Tools >网络策略服务器**。
2. 用鼠标右键单击**NP (本地)**并且选择**在活动目录的寄存器服务器**。
3. 单击 **Ok**。
4. 单击 **Ok**。
5. 添加WLC作为NP的一个验证、授权和统计(AAA)客户端。
6. 扩展**RADIUS客户端和服务器**。用鼠标右键单击**RADIUS客户端**并且选择**新的RADIUS客户端**：
7. 输入名称(在本例中的**WLC**)， WLC (在本例中的**10.105.135.178的**)管理IP地址和一共享机密。

   注意：同样共享机密用于为了配置WLC。

8. 点击OK键为了返回到上一屏幕。

9. 创建无线用户的一个新的网络策略。展开**策略**，用鼠标右键单击**网络策略**，并且选择**新**：

10. 进入此规则的(在本例中的**PEAP**一策略名称)并且**其次**单击。

11. 为了配置此策略允许只有无线域用户，请添加这三个情况并且**其次**单击：

12. 点击**访问授权的**单选按钮为了授权匹配此策略的连接尝试并且**其次**单击。

13. 禁用所有**较不安全认证方法**：

14. 单击**添加**，选择**Microsoft ：Protected EAP (PEAP)** EAP类型，和点击OK键为了启用PEAP。

15. 选择**Microsoft ：Protected EAP (PEAP)**和单击**编辑**。保证早先创建的域控制器证书在证书发出的下拉列表选择并且点击OK键。

16. 单击 **Next**。

17. 单击 **Next**。

18. 单击 **Next**。

19. 单击 **完成**。

注意：从属在您的需要，您也许需要配置在NP的**连接请求策略**为了允许PEAP配置文件或策略。

将用户添加到 Active Directory

注意：在本例中，用户数据库在AD维护。

完成这些步骤为了添加用户到AD数据库：

1. 导航到**Start > Administrative Tools >激活目录用户和计算机。**
2. 在激活目录用户和计算机控制台结构树中，请展开域，用鼠标右键单击**用户**和**新建**，并且选择**用户**。
3. 在新的对象-用户对话框，输入无线用户的名称。此示例在First Name字段使用**Client1**和**Client1**在用户登录名字名称字段。单击 **Next**。
4. 在新的对象-用户对话框，输入您的在密码的选择密码并且确认密码字段。不选定**用户必须更改密码在下个登录**复选框并且**其次**单击。
5. 在新的对象-用户对话框，点击**芬通社**。
6. 重复步骤 2 到步骤 4，以便创建更多用户帐户。

验证

要验证配置，请完成以下步骤：

1. 搜索服务集设置识别(SSID)在客户端机器。
2. 保证客户端顺利地连接：

故障排除

注意：思科建议您使用跟踪为了排除故障无线问题。跟踪在圆的缓冲区保存并且不是密集的处理器。

使这些跟踪为了获取**L2验证日志**：

- **设置trace组无线安全级别调试**
- **设置trace组无线安全过滤器mac 0017.7C2F.B69A**

使这些跟踪为了得到**dot1x AAA事件**：

- **设置trace wcm-dot1x aaa级别调试**
- **设置trace wcm-dot1x aaa过滤器mac 0017.7C2F.B69A**

使这些跟踪为了接收**DHCP事件**：

- **设置trace dhcp事件级别调试**
- **设置trace dhcp事件过滤器mac 0017.7C2F.B69A**

使这些跟踪为了禁用跟踪和清楚缓冲区：

- **设置轨迹控制SYS已过滤跟踪结算**
- **设置trace wcm-dot1x aaa级别默认**
- **设置trace wcm-dot1x aaa过滤器无**
- **设置trace组无线安全级别默认**
- **设置trace组无线安全过滤器无**

输入**显示trace SYS已过滤跟踪**命令为了查看跟踪：

```
[04/23/14 21:27:51.963 IST 1 8151] 0017.7c2f.b69a Adding mobile on LWAPP AP
 1caa.076f.9e10 (0)
[04/23/14 21:27:51.963 IST 2 8151] 0017.7c2f.b69a Local Policy:  Created MSCB
 Just AccessVLAN = 0 and SessionTimeout  is 0 and apfMsTimeout is 0

[04/23/14 21:27:51.963 IST 8 8151] 0017.7c2f.b69a Local Policy:Setting local
 bridging VLAN  name VLAN0020 and VLAN ID  20

[04/23/14 21:27:51.963 IST 9 8151] 0017.7c2f.b69a Applying WLAN ACL policies
 to client
[04/23/14 21:27:51.963 IST a 8151] 0017.7c2f.b69a No Interface ACL used for
 Wireless client in WCM(NGWC)
[04/23/14 21:27:51.963 IST b 8151] 0017.7c2f.b69a Applying site-specific IPv6
 override for station  0017.7c2f.b69a  - vapId 8, site 'test',
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST c 8151] 0017.7c2f.b69a Applying local bridging
 Interface Policy for station  0017.7c2f.b69a  - vlan 20,
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST d 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

04/23/14 21:27:51.963 IST f 8151] 0017.7c2f.b69a     Local Profiling Values :
 isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,
 applyPolicyAtRun= 0
[04/23/14 21:27:51.963 IST 10 8151] 0017.7c2f.b69a          ipv4ACL = [],
 ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[04/23/14 21:27:51.963 IST 11 8151] 0017.7c2f.b69a STA - rates (4):
 130 132 139 150 0 0 0 0 0 0 0 0 0 0 0 0
[04/23/14 21:27:51.963 IST 12 8151] 0017.7c2f.b69a STA - rates (12):
 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
[04/23/14 21:27:51.963 IST 13 8151] 0017.7c2f.b69a Processing RSN IE type 48,
 length 20 for mobile  0017.7c2f.b69a
[04/23/14 21:27:51.963 IST 14 8151] 0017.7c2f.b69a Received RSN IE with 0
 PMKIDsfrom mobile  0017.7c2f.b69a
```

[04/23/14 21:27:51.964 IST 1b 8151] 0017.7c2f.b69a **Change state to AUTHCHECK (2) last state START (0)**

[04/23/14 21:27:51.964 IST 1c 8151] 0017.7c2f.b69a Change state to 8021X_REQD (3) last state AUTHCHECK (2)

[04/23/14 21:27:51.964 IST 25 8151] 0017.7c2f.b69a apfProcessAssocReq (apf_80211.c:6272) **Changing state for mobile 0017.7c2f.b69a on AP 1caa.076f.9e10 from Associated to Associated**

[04/23/14 21:27:51.971 IST 26 8151] 0017.7c2f.b69a 1XA: Initiating authentication
[04/23/14 21:27:51.971 IST 27 8151] 0017.7c2f.b69a 1XA: Setting reauth timeout to 1800 seconds
[04/23/14 21:27:51.971 IST 28 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 0

[04/23/14 21:27:51.971 IST 29 8151] 0017.7c2f.b69a 1XA: Allocated uid 40
[04/23/14 21:27:51.971 IST 2a 8151] 0017.7c2f.b69a 1XA: **Calling Auth Mgr to authenticate client 4975000000003e uid 40**
[04/23/14 21:27:51.971 IST 2b 8151] 0017.7c2f.b69a 1XA: **Session Start from wireless client**

[04/23/14 21:27:51.971 IST 2c 8151] 0017.7c2f.b69a Session Manager Call Client 4975000000003e, uid 40, capwap id 7ae8c000000013,Flag 0, Audit-Session ID 0a6987b25357e2ff00000028, **method list Microsoft_NPS**, policy name (null)

[04/23/14 21:27:51.971 IST 2d 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca3] Session start request from Client[1] for 0017.7c2f.b69a (method: Dot1X, method list: Microsoft_NPS, aaa id: 0x00000028), policy
[04/23/14 21:27:51.971 IST 2e 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF: [0017.7c2f.b69a, Ca3] - client iif_id: 4975000000003E, session ID: 0a6987b25357e2ff00000028 for 0017.7c2f.b69a

[04/23/14 21:27:51.972 IST 43 284] ACCESS-METHOD-DOT1X-DEB: [0017.7c2f.b69a, Ca3] Posting !EAP_RESTART on Client 0x22000025
[04/23/14 21:27:51.972 IST 44 284] ACCESS-METHOD-DOT1X-DEB: [0017.7c2f.b69a, Ca3] 0x22000025:enter connecting state
[04/23/14 21:27:51.972 IST 45 284] ACCESS-METHOD-DOT1X-DEB: [0017.7c2f.b69a, Ca3] 0x22000025: restart connecting
[04/23/14 21:27:51.972 IST 46 284] ACCESS-METHOD-DOT1X-DEB: [0017.7c2f.b69a, Ca3] Posting RX_REQ on Client 0x22000025
[04/23/14 21:27:51.972 IST 47 284] ACCESS-METHOD-DOT1X-DEB: [0017.7c2f.b69a, Ca3] 0x22000025: authenticating state entered
[04/23/14 21:27:51.972 IST 48 284] ACCESS-METHOD-DOT1X-DEB: [0017.7c2f.b69a, Ca3] 0x22000025:connecting authenticating action
[04/23/14 21:27:51.972 IST 49 291] ACCESS-METHOD-DOT1X-DEB: [0017.7c2f.b69a, Ca3] **Posting AUTH_STAR**T for 0x22000025
[04/23/14 21:27:51.972 IST 4a 291] ACCESS-METHOD-DOT1X-DEB: [0017.7c2f.b69a, Ca3] 0x22000025:entering request state
[04/23/14 21:27:51.972 IST 4b 291] ACCESS-METHOD-DOT1X-NOTF: [0017.7c2f.b69a, Ca3] **Sending EAPOL packet**
[04/23/14 21:27:51.972 IST 4c 291] ACCESS-METHOD-DOT1X-INFO: [0017.7c2f.b69a, Ca3] Platform changed src mac of EAPOL packet
[04/23/14 21:27:51.972 IST 4d 291] ACCESS-METHOD-DOT1X-NOTF: [0017.7c2f.b69a, Ca3] **Sending out EAPOL packe**t
[04/23/14 21:27:51.972 IST 4e 291] ACCESS-METHOD-DOT1X-INFO: [0017.7c2f.b69a, Ca3] **EAPOL packet sent to clien**t 0x22000025

[04/23/14 21:27:52.112 IST 7d 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[04/23/14 21:27:52.112 IST 7e 211] AAA SRV(00000000): process authen req

[04/23/14 21:27:52.112 IST 7f 211] AAA SRV(00000000): **Authen method=SERVER_GROUP Microsoft_NP**S
[04/23/14 21:27:52.112 IST 80 211] AAA SRV(00000000): Selecting SG = DIAMETER
[04/23/14 21:27:52.113 IST 81 186] ACCESS-METHOD-DOT1X-INFO: [0017.7c2f.b69a, Ca3] **Queuing an EAPOL pkt on Authenticator Q**
[04/23/14 21:27:52.113 IST 82 291] ACCESS-METHOD-DOT1X-DEB: [0017.7c2f.b69a, Ca3] Posting EAPOL_EAP for **0x22000025**
[04/23/14 21:27:52.278 IST 83 220] AAA SRV(00000000): protocol reply GET_CHALLENGE_RESPONSE for Authentication
[04/23/14 21:27:52.278 IST 84 220] AAA SRV(00000000): Return Authentication status=GET_CHALLENGE_RESPONSE
[04/23/14 21:27:52.278 IST 85 291] ACCESS-METHOD-DOT1X-DEB:[0017.7c2f.b69a,Ca3] Posting EAP_REQ for 0x22000025

这是输出的EAP的其余：

[04/23/14 21:27:54.690 IST 12b 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:54.690 IST 12c 211] AAA SRV(00000000): Authen method=SERVER_GROUP Microsoft_NPS
[04/23/14 21:27:54.690 IST 12d 211] AAA SRV(00000000): Selecting SG = DIAMETER
[04/23/14 21:27:54.694 IST 12e 220] AAA SRV(00000000): **protocol reply PASS for Authentication**
[04/23/14 21:27:54.694 IST 12f 220] AAA SRV(00000000): **Return Authentication status=PASS**
[04/23/14 21:27:54.694 IST 130 189] ACCESS-METHOD-DOT1X-INFO: [0017.7c2f.b69a, Ca3] **Received an EAP Succe**ss

[04/23/14 21:27:54.695 IST 186 8151] 0017.7c2f.b69a **Starting key exchange with mobile - data forwarding is disable**d
[04/23/14 21:27:54.695 IST 187 8151] 0017.7c2f.b69a 1XA: **Sending EAPOL message to mobile, WLAN=8 AP WLAN=8**
[04/23/14 21:27:54.706 IST 188 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL message (len 121) from mobile
[04/23/14 21:27:54.706 IST 189 8151] 0017.7c2f.b69a 1XA: **Received EAPOL-Key from mobile**
[04/23/14 21:27:54.706 IST 18a 8151] 0017.7c2f.b69a 1XK: **Received EAPOL-key in PTK_START state (msg 2)** from mobile
[04/23/14 21:27:54.706 IST 18b 8151] 0017.7c2f.b69a 1XK: Stopping retransmission timer
[04/23/14 21:27:54.706 IST 18c 8151] 0017.7c2f.b69a 1XA: **Sending EAPOL message to mobile, WLAN=8 AP WLAN=8**
[04/23/14 21:27:54.717 IST 18d 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL message (len 99) from mobile
[04/23/14 21:27:54.717 IST 18e 8151] 0017.7c2f.b69a 1XA: **Received EAPOL-Key from mobile**
[04/23/14 21:27:54.717 IST 18f 8151] 0017.7c2f.b69a 1XK: **Received EAPOL-key in PTKINITNEGOTIATING state (msg 4) from mobile**
[04/23/14 21:27:54.717 IST 190 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 1

[04/23/14 21:27:54.717 IST 191 8151] 0017.7c2f.b69a 1XK: Key exchange complete - updating PEM
[04/23/14 21:27:54.717 IST 192 8151] 0017.7c2f.b69a apfMs1xStateInc
[04/23/14 21:27:54.717 IST 193 8151] 0017.7c2f.b69a **Change state to L2AUTHCOMPLETE (**4) last state 8021X_REQD (3)

[04/23/14 21:27:58.277 IST 1df 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:27:58.277 IST 1e0 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:28:05.279 IST 1e1 269] DHCPD: Adding binding to hash tree
[04/23/14 21:28:05.279 IST 1e2 269] DHCPD: DHCPOFFER notify setup address **20.20.20.5 mask 255.255.255.0**

```
[04/23/14 21:28:05.306 IST 1f4 8151] 0017.7c2f.b69a Change state to RUN (20)
 last state DHCP_REQD (7)
```

本文档是否是有用？有 没有

感谢您的反馈。

打开支持案例（需要思科服务合同。）

相关的思科支持社区讨论

思科支持社区是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 Cisco Technical Tips Conventions 。

已更新：2014年5月05日
文档ID117684