配置Cisco Access Registrar和LEAP

目錄

簡介

Cisco Networking Services Access Registrar(AR)3.0支援精簡型可擴充驗證通訊協定(LEAP)（EAP-Cisco無線）。 本文檔介紹如何配置無線Aironet客戶端實用程式和Cisco Aironet 340、350或1200系列接入點(AP)，以便對Cisco AR進行LEAP身份驗證。

必要條件

需求

本文件沒有特定先決條件。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Aironet® 340、350或1200系列存取點
- 適用於Cisco LEAP的AP韌體11.21或更高版本
- Cisco Aironet 340或350系列網路介面卡(NIC)
- 適用於Cisco LEAP的韌體版本4.25.30或更高版本
- 適用於Cisco LEAP的網路驅動程式介面規範(NDIS)8.2.3或更高版本
- Aironet使用者端公用程式(ACU)版本5.02或更新版本
- 運行和驗證Cisco LEAP和MAC身份驗證請求需要Cisco Access Registrar 3.0或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

配置EAP-Cisco Wireless(Cisco LEAP)

本節介紹Cisco AR伺服器、AP以及各種客戶端上Cisco LEAP的基本配置。

逐步說明

按照以下說明配置LEAP:

1. 更改Cisco AR伺服器上的埠。AP在使用者資料包通訊協定(UDP)連線埠1812（驗證）和 1813（計量）上傳送RADIUS資訊。 由於預設情況下Cisco AR在UDP埠1645和1646上偵聽 ，因此您必須將Cisco AR配置為在UDP埠1812和1813上偵聽。發出**cd /radius/advanced/ports**命令。發出**add 1812**命令以新增埠1812。如果您計畫執行記帳，請發 出**add 1813**命令以新增埠1813。儲存配置，然後重新啟動服務。
2. 要將AP新增到Cisco AR伺服器，請發出以下命令：**cd /Radius/客戶端新增ap350-1cd ap350- 1set ipaddress 171.69.89.1set sharedsecret cisco**
3. 要配置有線等效保密(WEP)金鑰會話超時，請發出以下命令：**注意：**802.1x指定重新身份驗證 選項。Cisco LEAP演算法利用此選項為使用者終止當前WEP會話金鑰並發出新的WEP會話金 鑰。**cd /Radius/Profilesadd ap-profilecd ap-profilecd屬性set session-timeout 600**
4. 要建立使用步驟3中新增的配置檔案的使用者組，請發出以下命令：**cd /Radius/Usergroupsadd ap-groupcd ap-groupset baseprofile ap-profile**此使用者組中的使用者 將繼承配置檔案，並接收會話超時。
5. 要在使用者清單中建立使用者並將使用者新增到步驟4中定義的使用者組，請發出以下命令 ：**cd /Radius/Userlists新增ap使用者cd ap-usersadd user1cd使用者1set password Ciscoset group ap-group**
6. 要建立本地身份驗證和授權服務以使用UserService「ap-userservice」並將服務型別設定為「 eap-leap」，請發出以下命令：**cd /Radius/Servicesadd ap-localservicecd ap-localserviceset type eap-leapset UserService ap-userservice**
7. 要建立使用者服務「ap-userservice」以使用步驟5中定義的使用者清單，請發出以下命令：**cd /Radius/Servicesadd ap-userservicecd ap-localserviceset type localset userlist ap-users**
8. 要將Cisco AR使用的預設身份驗證和授權服務設定為步驟6中定義的服務，請發出以下命令 ：**cd /radiusset defaultauthenticationservice ap-localserviceset defaultauthorizationservice ap-localservice**
9. 若要儲存並重新載入組態，請發出以下命令：**儲存重新載入**

在AP上啟用EAP-Cisco(Cisco LEAP)

逐步說明

按照以下步驟在AP上啟用Cisco LEAP:

1. 瀏覽至AP。

2. 在「摘要狀態」頁中，按一下**設定**。
3. 在「服務」選單中，按一下**安全>身份驗證伺服器**。
4. 在802.1x協定版本下拉選單中，選擇要在此無線接入點上運行的802.1x版本。
5. 在Server Name/IP文本框中配置Cisco AR的IP地址。
6. 驗證「Server Type（伺服器型別）」下拉選單是否設定為**RADIUS**。
7. 將「埠」文本框更改為**1812**。這是與Cisco AR一起使用的正確IP埠號。
8. 使用Cisco AR上使用的值配置Shared Secret文本框。
9. 選中**EAP Authentication**覈取方塊。
10. 如果需要，請修改「超時」文本框。這是Cisco AR身份驗證請求的超時值。
11. 按一下**OK**返回到「Security Setup（安全設定）」螢幕。如果您也在執行RADIUS記帳，請驗證Accounting Setup頁面上的埠是否與Cisco AR（為1813設定）中配置的埠一致。
12. 按一下「**Radio Data Encryption(WEP)**」。
13. 通過在WEP金鑰1文本框中鍵入40位或128位金鑰值來配置廣播WEP金鑰。
14. 選擇要使用的身份驗證型別。確保至少選中**Network-EAP**覈取方塊。
15. 驗證「Use of Data Encryption」下拉選單是否設定為「**Optional**」或「**Full Encryption**」。可選：允許在相同的AP上使用非WEP和WEP客戶端。請注意，這是一種不安全的操作模式。儘可能使用完全加密。
16. 按一下**OK**完成。

配置ACU 6.00

逐步說明

按照以下步驟配置ACU:

1. 開啟ACU。
2. 按一下工具欄上的**配置檔案管理器**。
3. 按一下**Add**建立新配置檔案。
4. 在文本框中輸入配置檔名稱，然後按一下**OK**。
5. 在SSID1文本框中輸入相應的服務集識別符號(SSID)。
6. 按一下「**Network Security**」。
7. 從Network Security Type下拉選單中選擇**LEAP**。
8. 按一下「**Configure**」。
9. 根據需要配置密碼設定。
10. 按一下「**OK**」（確定）。
11. 在Network Security螢幕上按一下**OK**。

來自Cisco AR的跟蹤

發出**trace /r 5**以獲取Cisco AR上的跟蹤輸出。如果需要AP調試，可以通過Telnet連線到AP並發出**eap_diag1_on**和**eap_diag2_on**命令。

```
06/28/2004 16:31:49: P1121: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1121: Checking Message-Authenticator
06/28/2004 16:31:49: P1121: Trace of Access-Request packet
06/28/2004 16:31:49: P1121: identifier = 5
06/28/2004 16:31:49: P1121: length = 146
```

```
06/28/2004 16:31:49: P1121:
   reqauth = e5:4f:91:27:0a:91:82:6b:a4:81:c1:cc:c8:11:86:0b
06/28/2004 16:31:49: P1121: User-Name = user1
06/28/2004 16:31:49: P1121: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1121: NAS-Port = 37
06/28/2004 16:31:49: P1121: Service-Type = Login
06/28/2004 16:31:49: P1121: Framed-MTU = 1400
06/28/2004 16:31:49: P1121: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1121: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1121: NAS-Identifier = frinket
06/28/2004 16:31:49: P1121: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1121: EAP-Message = 02:02:00:0a:01:75:73:65:72:31
06/28/2004 16:31:49: P1121:
   Message-Authenticator = f8:44:b9:3b:0f:33:34:a6:ed:7f:46:2d:83:62:40:30
06/28/2004 16:31:49: P1121: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1121: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1121: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1121: Authenticating and Authorizing with
   Service ap-localservice
06/28/2004 16:31:49: P1121: Response Type is Access-Challenge,
   skipping Remote Session Management.
06/28/2004 16:31:49: P1121: Response Type is Access-Challenge,
   skipping Local Session Management.
06/28/2004 16:31:49: P1121: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1121: Trace of Access-Challenge packet
06/28/2004 16:31:49: P1121: identifier = 5
06/28/2004 16:31:49: P1121: length = 61
06/28/2004 16:31:49: P1121:
   reqauth = 60:ae:19:8d:41:5e:a8:dc:4c:25:1b:8d:49:a3:47:c4
06/28/2004 16:31:49: P1121: EAP-Message =
   01:02:00:15:11:01:00:08:66:27:c3:47:d6:be:b3:67:75:73:65:72:31
06/28/2004 16:31:49: P1121: Message-Authenticator =
   59:d2:bc:ec:8d:85:36:0b:3a:98:b4:90:cc:af:16:2f
06/28/2004 16:31:49: P1121: Sending response to 10.48.86.230
06/28/2004 16:31:49: P1123: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1123: Checking Message-Authenticator
06/28/2004 16:31:49: P1123: Trace of Access-Request packet
06/28/2004 16:31:49: P1123: identifier = 6
06/28/2004 16:31:49: P1123: length = 173
06/28/2004 16:31:49: P1123:
   reqauth = ab:f1:0f:2d:ab:6e:b7:49:9e:9e:99:00:28:0f:08:80
06/28/2004 16:31:49: P1123: User-Name = user1
06/28/2004 16:31:49: P1123: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1123: NAS-Port = 37
06/28/2004 16:31:49: P1123: Service-Type = Login
06/28/2004 16:31:49: P1123: Framed-MTU = 1400
06/28/2004 16:31:49: P1123: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1123: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1123: NAS-Identifier = frinket
06/28/2004 16:31:49: P1123: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1123: EAP-Message =
   02:02:00:25:11:01:00:18:5e:26:d6:ab:3f:56:f7:db:21:96:f3:b0:fb:ec:6b:
   a7:58:6f:af:2c:60:f1:e3:3c:75:73:65:72:31
06/28/2004 16:31:49: P1123: Message-Authenticator =
   21:da:35:89:30:1e:e1:d6:18:0a:4f:3b:96:f4:f8:eb
06/28/2004 16:31:49: P1123: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1123: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1123: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1123: Authenticating and Authorizing
   with Service ap-localservice
06/28/2004 16:31:49: P1123: Calling external service ap-userservice
   for authentication and authorization
06/28/2004 16:31:49: P1123: Getting User user1's UserRecord
   from UserList ap-users
```

```
06/28/2004 16:31:49: P1123: User user1's MS-CHAP password matches
06/28/2004 16:31:49: P1123: Processing UserGroup ap-group's check items
06/28/2004 16:31:49: P1123: User user1 is part of UserGroup ap-group
06/28/2004 16:31:49: P1123: Merging UserGroup ap-group's BaseProfiles
   into response dictionary
06/28/2004 16:31:49: P1123: Merging BaseProfile ap-profile
   into response dictionary
06/28/2004 16:31:49: P1123: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1123: Adding attribute Session-Timeout, value = 600
06/28/2004 16:31:49: P1123: Merging UserGroup ap-group's Attributes
   into response Dictionary
06/28/2004 16:31:49: P1123: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1123: Removing all attributes except for
   EAP-Message from response - they will be sent back in the Access-Accept
06/28/2004 16:31:49: P1123: Response Type is Access-Challenge,
   skipping Remote Session Management.
06/28/2004 16:31:49: P1123: Response Type is Access-Challenge,
   skipping Local Session Management.
06/28/2004 16:31:49: P1123: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1123: Trace of Access-Challenge packet
06/28/2004 16:31:49: P1123: identifier = 6
06/28/2004 16:31:49: P1123: length = 44
06/28/2004 16:31:49: P1123:
   reqauth = 28:2e:a3:27:c6:44:9e:13:8d:b3:60:01:7f:da:8b:62
06/28/2004 16:31:49: P1123: EAP-Message = 03:02:00:04
06/28/2004 16:31:49: P1123: Message-Authenticator =
   2d:63:6a:12:fd:91:9e:7d:71:9d:8b:40:04:56:2e:90
06/28/2004 16:31:49: P1123: Sending response to 10.48.86.230
06/28/2004 16:31:49: P1125: Packet received from 10.48.86.230
06/28/2004 16:31:49: P1125: Checking Message-Authenticator
06/28/2004 16:31:49: P1125: Trace of Access-Request packet
06/28/2004 16:31:49: P1125: identifier = 7
06/28/2004 16:31:49: P1125: length = 157
06/28/2004 16:31:49: P1125:
   reqauth = 72:94:8c:34:4c:4a:ed:27:98:ba:71:33:88:0d:8a:f4
06/28/2004 16:31:49: P1125: User-Name = user1
06/28/2004 16:31:49: P1125: NAS-IP-Address = 10.48.86.230
06/28/2004 16:31:49: P1125: NAS-Port = 37
06/28/2004 16:31:49: P1125: Service-Type = Login
06/28/2004 16:31:49: P1125: Framed-MTU = 1400
06/28/2004 16:31:49: P1125: Called-Station-Id = 000d29e160f2
06/28/2004 16:31:49: P1125: Calling-Station-Id = 00028adc8f2e
06/28/2004 16:31:49: P1125: NAS-Identifier = frinket
06/28/2004 16:31:49: P1125: NAS-Port-Type = Wireless - IEEE 802.11
06/28/2004 16:31:49: P1125: EAP-Message =
   01:02:00:15:11:01:00:08:3e:b9:91:18:a8:dd:98:ee:75:73:65:72:31
06/28/2004 16:31:49: P1125: Message-Authenticator =
   8e:73:2b:a6:54:c6:f5:d9:ed:6d:f0:ce:bd:4f:f1:d6
06/28/2004 16:31:49: P1125: Cisco-AVPair = ssid=blackbird
06/28/2004 16:31:49: P1125: Using Client: ap1200-1 (10.48.86.230)
06/28/2004 16:31:49: P1125: Using Client ap1200-1 (10.48.86.230) as the NAS
06/28/2004 16:31:49: P1125: Authenticating and Authorizing
   with Service ap-localservice
06/28/2004 16:31:49: P1125: Merging attributes into the Response Dictionary:
06/28/2004 16:31:49: P1125: Adding attribute Session-Timeout, value = 600
06/28/2004 16:31:49: P1125: Restoring all attributes to response
   that were removed in the last Access-Challenge
06/28/2004 16:31:49: P1125: No default Remote Session Service defined.
06/28/2004 16:31:49: P1125: Adding Message-Authenticator to response
06/28/2004 16:31:49: P1125: Trace of Access-Accept packet
06/28/2004 16:31:49: P1125: identifier = 7
06/28/2004 16:31:49: P1125: length = 142
06/28/2004 16:31:49: P1125:
   reqauth = 71:f1:ef:b4:e6:e0:c2:4b:0a:d0:95:47:35:3d:a5:84
```

```
06/28/2004 16:31:49: P1125: Session-Timeout = 600
06/28/2004 16:31:49: P1125: EAP-Message =
02:02:00:25:11:01:00:18:86:5c:78:3d:82:f7:69:c7:96:70:35:31:bb:51:a7:ba:f8:48:8c:
45:66:00:e8:3c:75:73:65:72:31
06/28/2004 16:31:49: P1125: Message-Authenticator =
7b:48:c3:17:53:67:44:f3:af:5e:17:27:3d:3d:23:5f
06/28/2004 16:31:49: P1125: Cisco-AVPair =
6c:65:61:70:3a:73:65:73:73:69:6f:6e:2d:6b:65:79:3d:04:f2:c5:2a:de:fb:4e:1e:8a:8d
:b8:1b:e9:2c:f9:9a:3e:83:55:ff:ae:54:57:4b:60:e1:03:05:fd:22:95:4c:b4:62
06/28/2004 16:31:49: P1125: Sending response to 10.48.86.230
```

相關資訊

- [Cisco Access Registrar支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)