Cisco Access Registrar およびLEAP の設定

目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[EAP Cisco Wireless（Cisco LEAP）の設定](#)
[手順説明](#)
[AP での EAP Cisco（Cisco LEAP）の有効化](#)
[手順説明](#)
[ACU 6.00 の設定](#)
[手順説明](#)
[Cisco AR からのトレース](#)
[関連情報](#)

概要

Cisco Networking Service Access Registrar（AR）3.0 は、Light Extensible Authentication Protocol（LEAP）（EAP-Cisco Wireless）をサポートしています。 このドキュメントでは、Cisco AR への LEAP 認証のためのワイヤレス Aironet クライアント ユーティリティおよび Cisco Aironet 340、350、または 1200 シリーズ アクセス ポイント（AP）の設定方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Aironet® 340、350、または 1200 シリーズのアクセス ポイント
- Cisco LEAPのAPのファームウェア11.21以降
- Cisco Aironet 340または350シリーズのネットワーク インターフェイス カード（NIC ）
- Cisco LEAPのファームウェア バージョン4.25.30以降
- Cisco LEAPのNetwork Driver Interface Specification （NDIS ）8.2.3以降
- Aironet Client Utility （ACU ）バージョン5.02以降

- Cisco Network Registrar 3.0以降では、Cisco LEAPおよびMAC認証要求を実行し、認証が必要です

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

EAP Cisco Wireless （ Cisco LEAP ）の設定

このセクションでは、Cisco ARサーバ、APとクライアントのさまざまなCisco LEAPの基本設定について説明します。

手順説明

LEAP の設定方法は次のとおりです。

1. Cisco ARサーバのポートを変更します。APはユーザ データグラム プロトコル（UDP ）ポート1812 （認証）および1813 RADIUS情報を送信します（アカウンティング） Cisco ARはUDPポート1645および1646でデフォルトにするため、1812と1813 Cisco ARをUDPポートで受信するように設定します。/radius/advanced/ports **cdコマンドを**発行します。ポート1812を**提供する1812コマンドを発行します。**アカウンティングを予定してポート1813を**提供する1813コマンドを発行します。**設定を保存してから、サービスを再起動します。
2. Cisco ARサーバにAPを追加するには、次のコマンドを実行する:**CD /Radius/Clientsap350-1を追加しますCD ap350-1set ipaddress 171.69.89.1sharedsecret ciscoを設定します**
3. Wired Equivalent Privacy （ WEP ）キーのセッション タイムアウトを設定するには、次のコマンドを実行する:**注:** 802.1xは再認証オプションを指定します。 Cisco LEAPアルゴリズムはユーザの損失、新たなWEPセッション キーを発行するときは、このオプションを現在のWEPのセッション キーを使用します。**CD /Radius/Profilesadd ap-profilecd ap-profilecd attributesset session-timeout 600**
4. プロファイルを使用するユーザ グループを作成するには、手順3で次のコマンドを発行します。追加:**CD /Radius/Usergroupsadd ap-groupcd ap-groupbaseprofile apプロファイルを設定します**このユーザ グループ内のユーザにプロファイルを継承し、結果としてセッション タイムアウトを受け取ります。
5. ユーザ リストでユーザを作成し、ステップ4で定義されたユーザ グループにユーザを追加するには、次のコマンドを実行します:**CD /Radius/Userlistsadd ap-userscd ap-usersadd user1CD user1Ciscoパスワードを設定しますグループのAPグループを設定します**
6. ローカル認証と認可サービスをUserService 「ap userservice」を使用し、「飛躍」eapにサービス タイプを設定するために作成するには、次のコマンドを実行します:**CD /Radius/Servicesadd ap-localservicecd ap-localserviceLEAPのEAPタイプを設定しますUserService ap userserviceを設定します**
7. ユーザを定義するステップ5でユーザ リストを使用するために作成するには「ap userservice」を次のコマンドを発行します。英語]:**CD /Radius/Servicesadd ap-userservicecd ap-localserviceローカル設定のタイプuserlist apのユーザを設定します**

8. 手順6で定義した、サービスへのCisco ARの使用が次のコマンドを発行してデフォルトの認証と認可を設定するには、[Service:**CD /radiusdefaultauthenticationservice ap localserviceを設定しますdefaultauthorizationservice ap localserviceを設定します**
9. 設定を保存してリロードするには、次のコマンドを実行します:**savereload**

AP での EAP Cisco （ Cisco LEAP ）の有効化

手順説明

APのCisco LEAPを有効にするには、次のステップを実行します:

1. AP をブラウズします。
2. [Summary Status]ページから、[Setup]をクリックします。
3. サービス メニューで、セキュリティ> Authentication Serversをクリックします。
4. 802.1x Protocol Versionドロップダウン メニューで、このAPで動作するように802.1xのバージョンを選択します。
5. [Server Name/IP] テキストボックスで、Cisco AR の IP アドレスを設定します。
6. サーバ タイプ)]ドロップダウン メニューでRADIUSに設定されていること**を確認します。**
7. [Port] テキストボックスを [1812] に変更します。 これはCisco ARで使用する、正しいIPポート番号です。
8. Cisco ARで使用される値とShared Secretテキスト ボックスを設定します。
9. [EAP Authentication] チェックボックスを選択します。
10. これとタイムアウトのテキスト ボックスを変更します。 これはCisco AR認証要求のタイムアウト値です。
11. [OK] をクリックし、[Security Setup] 画面に戻ります。また、RADIUSアカウンティングを設定したら、ページのアカウンティング ポートがCisco ARで設定されたポートと一致していることを確認します（1813に設定）。
12. [Radio Data Encryption (WEP)] をクリックします。
13. 40を入力して、ブロードキャストWEPキーがWEP Key 1]テキストボックスには、128またはビット ゲージ キー値設定します。
14. 使用する認証タイプを選択します。 、少なくとも、ネットワークEAP]チェックボックスが**選択されている**ことを確認します。
15. データ暗号化のドロップダウン メニューの使用はオプションまたは完全な暗号化**に設定されていることを確認します。** オプションでは、APの非WEPとWEPのクライアントの使用。 これが非セキュア モードであることに注意してください。 可能な限り、[Full Encryption] を使用してください。
16. 終了するには [OK] をクリックします。

ACU 6.00 の設定

手順説明

次の手順に従って、ACU を設定します。

1. ACU を開きます。
2. ツールバーの[Profile Managerをクリックします。
3. [Add] をクリックし、新規プロファイルを作成します。

4. テキストボックスにプロファイル名を入力し、[OK] をクリックします。
5. SSID1テキスト ボックスの適切なService Set Identifier （ SSID ）で入力します。
6. [Network Security] をクリックします。
7. Network Security Typeドロップダウン メニューからLEAPを選択します。
8. [Configure] をクリックします。
9. 必要に応じてパスワード設定を変更します。
10. [OK] をクリックします。
11. ネットワーク セキュリティ画面でOKをクリックします。

Cisco AR からのトレース

Cisco ARのトレース出力を得るためにトレースr 5を発行します。 APのデバッグが必要であれば、Telnet経由でAPに接続し、eap_diag1_onとeap_diag2_onコマンドを発行できます。

```
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
```

関連情報

- Cisco Access Registrar サポート ページ
- テクニカル サポートとドキュメント – Cisco Systems