Konfigurieren von Cisco Access Registrar und LEAP

Inhalt

Einführung

Cisco Networking Services Access Registrar (AR) 3.0 unterstützt LEAP (Light Extensible Authentication Protocol) (EAP-Cisco Wireless). In diesem Dokument wird die Konfiguration der Wireless Aironet Client Utilities und der Cisco Aironet Access Points der Serien 340, 350 oder 1200 für die LEAP-Authentifizierung zum Cisco AR erläutert.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Aironet® Access Points der Serien 340, 350 oder 1200
- AP-Firmware 11.21 oder höher für Cisco LEAP
- Cisco Aironet Network Interface Cards (NICs) der Serien 340 oder 350
- Firmware-Versionen 4.25.30 oder höher für Cisco LEAP

- Network Driver Interface Specification (NDIS) 8.2.3 oder höher für Cisco LEAP
- Aironet Client Utilities (ACU) Version 5.02 oder höher
- Cisco Access Registrar 3.0 oder höher ist erforderlich, um Cisco LEAP- und MAC-Authentifizierungsanforderungen ausführen und authentifizieren zu können.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Konfigurieren von EAP-Cisco Wireless (Cisco LEAP)

In diesem Abschnitt werden die grundlegenden Konfigurationen von Cisco LEAP auf dem Cisco AR-Server, dem AP und verschiedenen Clients erläutert.

Schrittweise Anleitung

Befolgen Sie diese Anweisungen zur Konfiguration von LEAP:

1. Ändern Sie den Port auf dem Cisco AR-Server.Der Access Point sendet RADIUS-Informationen über die UDP-Ports 1812 (Authentifizierung) und 1813 (Accounting) des User Datagram Protocol. Da die Cisco AR standardmäßig auf den UDP-Ports 1645 und 1646 lauscht, müssen Sie die Cisco AR so konfigurieren, dass sie die UDP-Ports 1812 und 1813 überwacht.Geben Sie den Befehl **cd /radius/advanced/ports ein**.Geben Sie den Befehl **1812 hinzufügen** ein, um Port 1812 hinzuzufügen.Wenn Sie eine Abrechnung planen, geben Sie den Befehl **add 1813** zum Hinzufügen von Port 1813 ein.Speichern Sie die Konfiguration, und starten Sie die Dienste neu.
2. Führen Sie folgende Befehle aus, um den Access Point zum Cisco AR-Server hinzuzufügen:**cd /Radius/Clientsap350-1 hinzufügencd ap350-1set ipaddress 171.69.89.1set sharedsecret Cisco**
3. Führen Sie folgende Befehle aus, um das Timeout für die WEP-Schlüssellaufzeit (Wired Equivalent Privacy) zu konfigurieren:**Hinweis:** 802.1x gibt eine Reauthentifizierungsoption an. Der Cisco LEAP-Algorithmus verwendet diese Option, um den aktuellen WEP-Sitzungsschlüssel für den Benutzer zu löschen und einen neuen WEP-Sitzungsschlüssel auszugeben.**cd/Radius/ProfileAdd-AP-Profilcd AP-ProfilCD-AttributeSitzungs-Timeout 600 festlegen**
4. Führen Sie die folgenden Befehle aus, um eine Benutzergruppe zu erstellen, die die in Schritt 3 hinzugefügten Profile verwendet:**cd /Radius/BenutzergruppenHinzufügen einer AP-Gruppecd AP-GruppeFestlegen des Baseprofil-Map-Profils**Benutzer in dieser Benutzergruppe erben das Profil und erhalten dann das Sitzungs-Timeout.
5. Führen Sie folgende Befehle aus, um Benutzer in einer Benutzerliste zu erstellen und die Benutzer der in Schritt 4 definierten Benutzergruppe hinzuzufügen:**cd /Radius/BenutzerlistenAdd-AP-Benutzercd ap-benutzerBenutzer hinzufügen1cd user1Kennwort festlegen CiscoGruppe AP-Gruppe festlegen**

6. Führen Sie folgende Befehle aus, um einen lokalen Authentifizierungs- und Autorisierungsdienst zur Verwendung von UserService "ap-userservice" zu erstellen und den Servicetyp auf "eap-leap" festzulegen:**cd/Radius/Servicesadd apLocalservicecd ap-localserviceset type eap-sprungFestlegen von UserService ap-UserService**
7. Führen Sie folgende Befehle aus, um einen Benutzerdienst "ap-userservice" zu erstellen, der die in Schritt 5 definierte Benutzerliste verwendet:**cd/Radius/ServicesAdd-ap-User-Servicecd ap-localserviceFeststelltyp lokalset userlist ap users**
8. Führen Sie folgende Befehle aus, um den standardmäßigen Authentifizierungs- und Autorisierungsdienst festzulegen, den Cisco AR für den in Schritt 6 definierten Dienst verwendet:**cd /radiusset defaultauthenticationService ap-localserviceset defaultautorisierungService ap-localservice**
9. Führen Sie folgende Befehle aus, um die Konfiguration zu speichern und erneut zu laden:**speichernnachladen**

Aktivierung von EAP-Cisco (Cisco LEAP) am AP

Schrittweise Anleitung

Gehen Sie folgendermaßen vor, um Cisco LEAP auf dem AP zu aktivieren:

1. Navigieren Sie zum AP.
2. Klicken Sie auf der Seite "Summary Status" (Zusammengefasster Status) auf **SETUP**.
3. Klicken Sie im Menü Dienste auf **Sicherheit > Authentifizierungsserver**.
4. Wählen Sie im Dropdown-Menü 802.1x Protocol Version (802.1x-Protokollversion) die Version von 802.1x aus, die auf diesem AP ausgeführt werden soll.
5. Konfigurieren Sie die IP-Adresse der Cisco AR im Textfeld Servername/IP.
6. Überprüfen Sie, ob das Dropdown-Menü Servertyp auf **RADIUS** eingestellt ist.
7. Ändern Sie das Textfeld Port in **1812**. Dies ist die richtige IP-Portnummer für die Cisco AR.
8. Konfigurieren Sie das Textfeld "Shared Secret" mit dem in der Cisco AR verwendeten Wert.
9. Aktivieren Sie das Kontrollkästchen **EAP-Authentifizierung**.
10. Ändern Sie ggf. das Textfeld Timeout. Dies ist der Timeout-Wert für eine Authentifizierungsanfrage für die Cisco AR.
11. Klicken Sie auf **OK**, um zum Bildschirm "Security Setup" zurückzukehren.Wenn Sie auch RADIUS Accounting (RADIUS-Accounting) durchführen, überprüfen Sie, ob der Port auf der Seite für die Accounting-Einrichtung mit dem in der Cisco AR konfigurierten Port (für 1813 festgelegt) übereinstimmt.
12. Klicken Sie auf **Radio Data Encryption (WEP)**.
13. Konfigurieren Sie einen Broadcast-WEP-Schlüssel, indem Sie im Textfeld WEP-Schlüssel 1 einen 40- oder 128-Bit-Schlüsselwert eingeben.
14. Wählen Sie die zu verwendenden Authentifizierungstypen aus. Stellen Sie sicher, dass mindestens das Kontrollkästchen **Network-EAP** aktiviert ist.
15. Überprüfen Sie, ob das Dropdown-Menü "Datenverschlüsselung verwenden" auf **Optional** oder **Vollverschlüsselung** eingestellt ist. Optional können WEP- und WEP-Clients auf demselben AP verwendet werden. Beachten Sie, dass es sich um einen unsicheren Betriebsmodus handelt. Verwenden Sie, wenn möglich, die vollständige Verschlüsselung.
16. Klicken Sie auf **OK**, um abzuschließen.

Konfigurieren der ACU 6.00

Schrittweise Anleitung

Führen Sie die folgenden Schritte aus, um die ACU zu konfigurieren:

1. Öffnen Sie die ACU.
2. Klicken Sie in der Symbolleiste auf **Profile Manager**.
3. Klicken Sie auf **Hinzufügen**, um ein neues Profil zu erstellen.
4. Geben Sie den Profilnamen in das Textfeld ein, und klicken Sie dann auf **OK**.
5. Geben Sie im Textfeld SSID1 den entsprechenden Service Set Identifier (SSID) ein.
6. Klicken Sie auf **Netzwerksicherheit**.
7. Wählen Sie **LEAP** im Dropdown-Menü Netzwerksicherheitstyp aus.
8. Klicken Sie auf **Konfigurieren**.
9. Konfigurieren Sie die Kennworteinstellungen nach Bedarf.
10. Klicken Sie auf **OK**.
11. Klicken Sie im Bildschirm "Netzwerksicherheit" auf **OK**.

Spuren von Cisco AR

Geben Sie **trace /r 5** ein, um die Ablaufverfolgungsausgabe auf der Cisco AR abzurufen. Wenn Sie AP-Debuggen benötigen, können Sie über Telnet eine Verbindung zum Access Point herstellen und die Befehle **eap_diag1_on** und **eap_diag2_on** ausgeben.

```
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
```

Zugehörige Informationen

- Support-Seite für Cisco Access Registrar
- Technischer Support und Dokumentation - Cisco Systems