Configuración de Cisco Access Registrar y LEAP

Contenido

Introducción

El 3.0 del Access Registrar del Cisco Networking Services (AR) soporta el protocolo light extensible authentication (SALTO) (Tecnología inalámbrica del EAP Cisco). Este documento muestra cómo configurar el Aironet Client Utilities inalámbrico y Cisco Aironet 340, 350, o (APS) de los Puntos de acceso de las 1200 Series para la autenticación LEAP a Cisco AR.

prerrequisitos

Requisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Aironet® 340 de Cisco, 350, o Puntos de acceso de las 1200 Series
- Firmware AP 11.21 o más adelante para el Cisco LEAP
- Cisco Aironet 340 o Network Interface Cards de las 350 Series (NIC)
- Versiones de firmware 4.25.30 o más adelante para el Cisco LEAP
- Network Driver Interface Specification (NDIS) 8.2.3 o más adelante para el Cisco LEAP
- Versiones 5.02 del Aironet Client Utilities (ACU) o más adelante

- Se requiere el Cisco Access Registrar 3.0 o más adelante ejecutar y autenticar las peticiones del Cisco LEAP y de la autenticación de MAC

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Configuración de EAP-Cisco Wireless (Cisco LEAP)

Esta sección cubre las configuraciones básicas del Cisco LEAP en el servidor de Cisco AR, el AP, y los diversos clientes.

Step-by-Step Instructions

Siga estas instrucciones de configurar el SALTO:

1. Cambie el puerto en el servidor de Cisco AR.El AP envía la información de RADIUS en los puertos 1812 (autenticación) y 1813 del User Datagram Protocol (UDP) (las estadísticas). Puesto que Cisco AR escucha en los puertos 1645 y 1646 UDP por abandono, usted debe configurar Cisco AR para escuchar en los puertos 1812 y 1813 UDP.Publique el comando **cd de /radius/advanced/ports**.Publique el **comando add 1812** de agregar el puerto 1812.Si usted planea hacer las estadísticas, publique el **comando add 1813** de agregar el puerto 1813.Salve la configuración, y después recomience los servicios.
2. Para agregar el AP al servidor de Cisco AR, publique estos comandos:**/Radius/Clients cdagregue ap350-1ap350-1 cdfije el IP address 171.69.89.1fije el sharedsecret Cisco**
3. Para configurar el tiempo de espera de la sesión de la clave del Wired Equivalent Privacy (WEP), publique estos comandos:**Nota:** el 802.1x especifica una opción de reautenticación. El algoritmo del Cisco LEAP utiliza esta opción para expirar la clave de la sesión actual WEP para el usuario y para publicar una nueva clave de la sesión WEP.**/Radius/Profiles cdagregue el ap-perfilap-perfil cdatributos del Cdfije el sesión-descanso 600**
4. Para crear a un grupo de usuarios que utiliza los perfiles agregó en el paso 3, publican estos comandos:**/Radius/Usergroups cdagregue el grupo apgrupo ap cdfije el ap-perfil baseprofile**Los usuarios en este grupo de usuarios heredan el perfil y a su vez reciben el tiempo de espera de la sesión.
5. Para crear a los usuarios en una lista de usuario y agregar a los usuarios al grupo de usuarios definido en el paso 4, publique estos comandos:**/Radius/Userlists cdagregue a los ap-usuariosap-usuarios cdagregue el user1user1 cdfije la palabra clave Ciscofije el grupo ap del grupo**
6. Para crear un servicio de la autenticación local y de la autorización para utilizar UserService “ap-userservice” y para fijar el tipo de servicio “EAP-salto”, publique estos comandos:**/Radius/Services cdagregue el ap-localserviceap-localservice cdfije el EAP-salto del tipofije UserService ap-userservice**
7. Para crear un servicio de usuario “ap-userservice” para utilizar la lista de usuario definida en

el paso 5, publique estos comandos:**/Radius/Services cdagregue el ap-userserviceap-localservice cdset type localfije a los ap-usuarios del userlist**
8. Para fijar la autenticación predeterminada y la autorización mantenga que las aplicaciones de Cisco AR al servicio definido en el paso 6, publican estos comandos:**/radius cdfije el defaultauthenticationservice ap-localservicefije el defaultauthorizationservice ap-localservice**
9. Para salvar y recargar la configuración, publique estos comandos:**guardarrecargar**

Cómo habilitar EAP-Cisco (Cisco LEAP) en AP

Step-by-Step Instructions

Siga los siguientes pasos para habilitar el Cisco LEAP en el AP:

1. Hojee al AP.
2. De la página del estado resumido, haga clic la **CONFIGURACIÓN**.
3. En el menú de los servicios, haga clic **Security > Authentication el servidor**.
4. Seleccione la versión del 802.1x para ejecutarse en este AP en el menú desplegable de la Versión del protocolo del 802.1x.
5. Configure la dirección IP de Cisco AR en el cuadro de texto del servidor Name/IP.
6. Verifique el tipo de servidor que el menú desplegable se fija al **RADIUS**.
7. Cambie el cuadro de texto del puerto a **1812**. Éste es el número del puerto correcto IP a utilizar con Cisco AR.
8. Configure el cuadro de texto del secreto compartido con el valor usado en Cisco AR.
9. Seleccione la casilla de verificación de la **autenticación EAP**.
10. Modifique timeout text (Texto de tiempo de espera) el cuadro si está deseado tan. Éste es el valor de agotamiento del tiempo para un pedido de autenticación para Cisco AR.
11. Haga Click en OK a volver a la pantalla de la configuración de seguridad.Si usted también está haciendo las estadísticas RADIUS, verifique que el puerto en la página de configuración de las estadísticas esté de acuerdo con el puerto configurado en Cisco AR (fija para 1813).
12. Haga clic en Radio Data Encryption (WEP) (Cifrado de datos de Radio (WEP)).
13. Configure una clave WEP del broadcast por teclear en un 40- o el valor de la clave del 128-bit en el cuadro de texto de la clave WEP 1.
14. Seleccione los tipos de autenticación utilizar. Aseegurese que, al mínimo, **Casilla de verificación EAP de la red.** está seleccionado.
15. Verifique Use of Data Encryption el menú desplegable se fija a la **encripción opcional o completa**. Opcional permite el uso del NON-WEP y de los clientes WEP en el mismo AP. Sea consciente que esto es un modo de operación inseguro. Utilice la encripción completa cuando es posible.
16. Haga Click en OK a acabar.

Configurar ACU 6.00

Step-by-Step Instructions

Siga los siguientes pasos para configurar el ACU:

1. Abra el ACU.
2. Haga clic al **administrador del perfil** en la barra de herramientas.
3. El tecleo **agrega** para crear un nuevo perfil.
4. Ingrese el nombre del perfil en el cuadro de texto, y después haga clic la **AUTORIZACIÓN**.
5. Ingrese en el Service Set Identifier (SSID) apropiado en el cuadro de texto SSID1.
6. Haga clic la **seguridad de la red**.
7. Seleccione el **SALTO del** menú desplegable del tipo de la seguridad de la red.
8. Haga clic en Configure (Configurar).
9. Configure las configuraciones de la contraseña según las necesidades.
10. Click OK.
11. Haga Click en OK en la pantalla de seguridad de la red.

Seguimientos de Cisco AR

Publique la **traza /r 5** para obtener el resultado de la traza en Cisco AR. Si usted necesita el debug AP, el usted puede conectarse al AP vía Telnet y publica los **comandos eap_diag1_on y eap_diag2_on**.

```
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
```

Información Relacionada

- Página de soporte del Cisco Access Registrar
- Soporte Técnico y Documentación - Cisco Systems