Contenido

Introducción

Este documento proporciona una configuración de muestra para la autenticación del protocolo lightweight extensible authentication (SALTO) en un Punto de acceso basado en IOS®, que sirve a los clientes de red inalámbrica, así como actúa como servidor de RADIUS local. Esto es aplicable a un Punto de acceso IOS que ejecute 12.2(11)JA o más adelante.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Estar familiarizado con GUI o CLI de IOS
- Familiaridad con los conceptos relacionados con la autenticación de LEAP

Componentes

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

- Punto de acceso de la serie del Cisco Aironet 1240AG
- Cisco IOS Software Release 12.3(8)JA2
- Adaptador de red inalámbrica del 802.11 a/b/g/del Cisco Aironet que funcionamientos utilidad Aironet Desktop 3.6.0.122
- Se supone que hay sólo una VLAN en la red.

La información que contiene este documento se creó a partir de los dispositivos en 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 cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Descripción de la característica local del servidor de RADIUS

Utilizan generalmente a un servidor RADIUS externo para autenticar a los usuarios. En algunos casos, esto no es una solución factible. En estas situaciones, un Punto de acceso se puede hacer para actuar como servidor de RADIUS. Aquí, autentican a los usuarios contra la base de datos local configurada en el Punto de acceso. Esto se llama una característica local del servidor de RADIUS. Usted puede también hacer otros Puntos de acceso en el uso de la red que el servidor de RADIUS local ofrece en un Punto de acceso. Para más información sobre esto, refiera a configurar otros Puntos de acceso para utilizar el autenticador local.

Configurar

La configuración describe cómo configurar el SALTO y la característica local del servidor de RADIUS en un Punto de acceso. La característica local del servidor de RADIUS fue introducida en el Cisco IOS Software Release 12.2(11)JA. Refiera a la autenticación LEAP con el servidor de RADIUS para la información previa en cómo configurar el SALTO con un servidor RADIUS externo.

Como ocurre con la mayoría de los algoritmos de autenticación basados en contraseñas, Cisco LEAP es vulnerable a los ataques del diccionario. Este no es un ataque o vulnerabilidad nueva del LEAP de Cisco. Usted debe crear una política de contraseña fuerte para atenuar los establecimientos de diccionario, eso incluiría las contraseñas fuertes y frecuentaría las nuevas contraseñas. Refiera al establecimiento de diccionario en el Cisco LEAP para más información sobre los establecimientos de diccionario y cómo prevenirlos.

Este documento asume esta configuración para el CLI y el GUI:

1. La dirección IP del Punto de acceso es **10.77.244.194**.
2. El SSID usado es **Cisco**, que se asocia al **VLAN1.**
3. Los nombres de usuario son **user1** y **user2**, que se asocian al **testuser del** grupo.

Configuración de CLI

Punto de Acceso

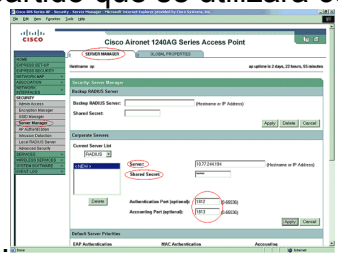
```
ap#show running-config Building configuration......aaa new-
model !--- This command reinitializes the authentication, !--
- authorization and accounting functions.!!aaa group server
radius rad_eap  server 10.77.244.194 auth-port 1812 acct-port
1813!--- A server group for RADIUS is created called
"rad_eap" !--- that uses the server at 10.77.244.194 on ports
1812 and 1813....aaa authentication login eap_methods group
rad_eap!--- Authentication [user validation] is to be done
for !--- users in a group called "eap_methods" who use server
group "rad_eap"....! bridge irb!interface Dot11Radio0 no ip
address no ip route-cache ! encryption vlan 1 key 1 size
128bit    12345678901234567890123456 transmit-key!This step
is optional----!--- This value seeds the initial key for use
with !--- broadcast [255.255.255.255] traffic. If more than
one VLAN is !--- used, then keys must be set for each VLAN.
```

```
encryption vlan 1 mode wep mandatory !--- This defines the
policy for the use of Wired Equivalent Privacy (WEP). !--- If
more than one VLAN is used, !--- the policy must be set to
mandatory for each VLAN. broadcast-key vlan 1 change 300  !--
- You can also enable Broadcast Key Rotation for each vlan
and Specify the time after which Brodacst key is changed. If
it is disabled Broadcast Key is still used but not
changed.ssid cisco           vlan 1!--- Create a SSID Assign
a vlan to this SSID              authentication open eap
eap_methods           authentication network-eap eap_methods
!--- Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and Network
EAP authentication !--- bit set in the headers of those
requests, and group those users into !--- a group called
"eap_methods." ! speed basic-1.0 basic-2.0 basic-5.5 basic-
11.0 rts threshold 2312 channel 2437 station-role root
bridge-group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group 1
spanning-disabled...interface FastEthernet0 no ip address no
ip route-cache duplex auto speed auto bridge-group 1 no
bridge-group 1 source-learning bridge-group 1 spanning-
disabled!interface BVI1 ip address 10.77.244.194
255.255.255.0 !--- The address of this unit. no ip route-
cache!ip default-gateway 10.77.244.194ip http serverip http
help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/ea
g/ivory/1100ip radius source-interface BVI1snmp-server
community cable ROsnmp-server enable traps ttyradius-server
local !--- Engages the Local RADIUS Server feature. nas
10.77.244.194 key shared_secret !--- Identifies itself as a
RADIUS server, reiterates !--- "localness" and defines the
key between the server (itself) and the access point. ! group
testuser !--- Groups are optional. ! user user1 nthash
password1 group testuser !--- Individual user user user2
nthash password2 group testuser !--- Individual user!---
These individual users comprise the Local Database!radius-
server host 10.77.244.194 auth-port 1812 acct-port    1813
key shared_secret!--- Defines where the RADIUS server is and
the key between !--- the access point (itself) and the
server.radius-server retransmit 3radius-server attribute 32
include-in-access-req format %hradius-server authorization
permit missing Service-Typeradius-server vsa send
accountingbridge 1 route ip!!line con 0line vty 5 15!end
```

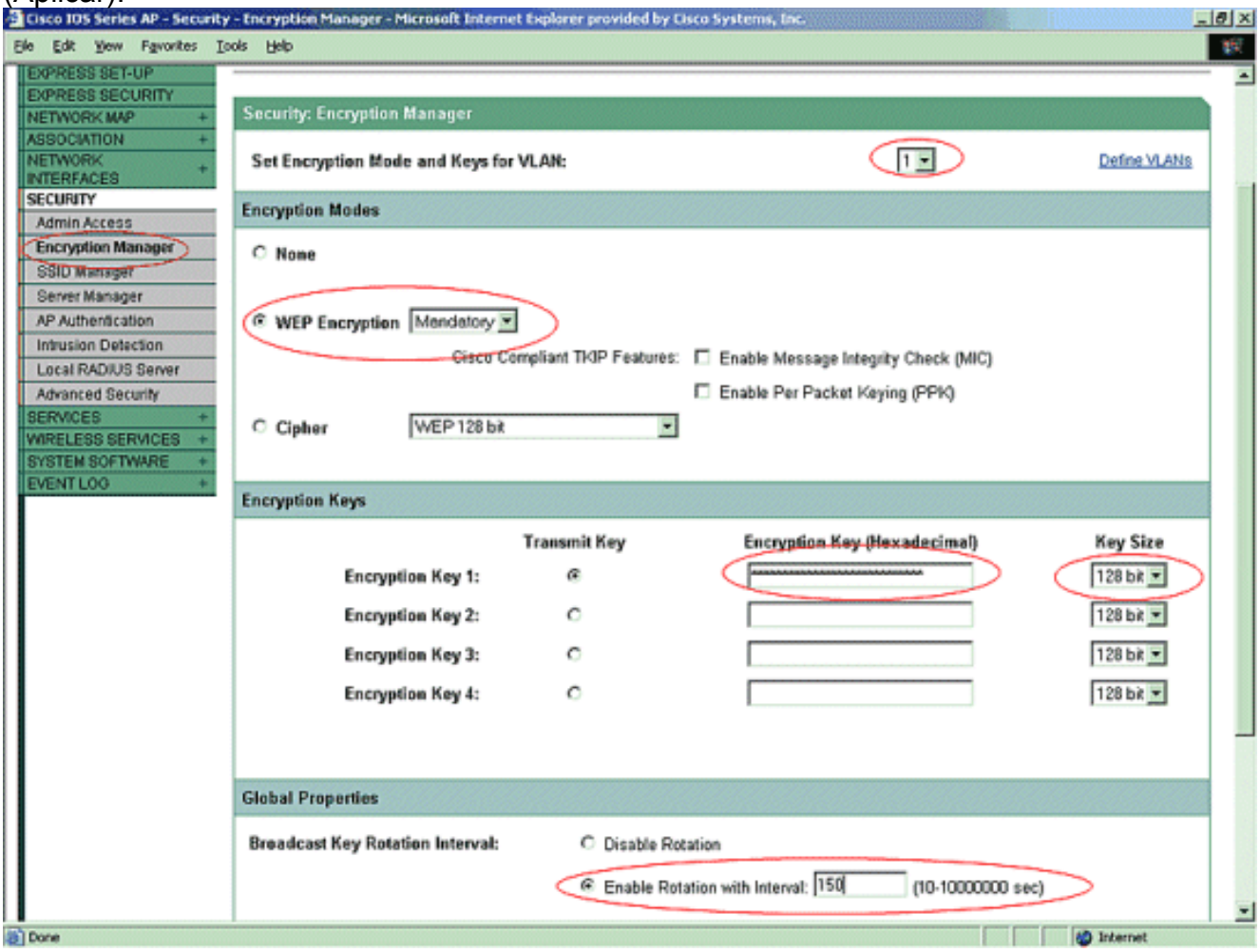
Configuración de la interfaz gráfica para el usuario

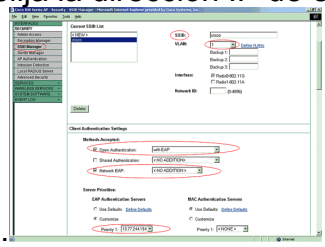
Complete estos pasos para configurar la característica local del servidor de RADIUS con el GUI:

1. Del menú en el lado izquierdo, elija la lengueta del administrador de servidor bajo menú de seguridad.Configure el servidor y mencione la dirección IP de este Punto de acceso, que es 10.77.244.194 en este ejemplo.Mencione los números del puerto 1812 y 1813 en los cuales el servidor de RADIUS local escuche.Especifique el secreto compartido que se utilizará con el servidor de RADIUS local tal y como se muestra en de la figura.

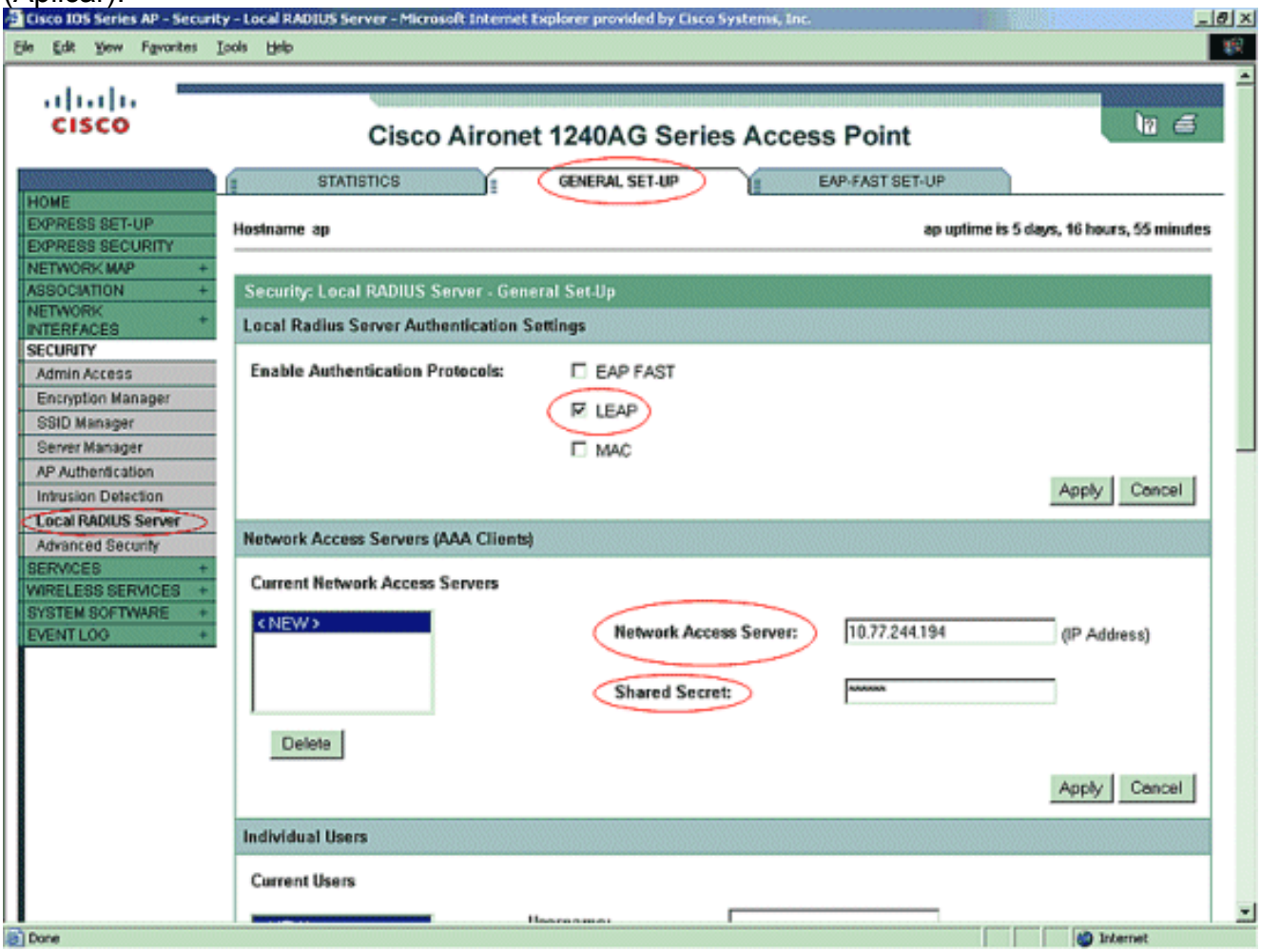


2. Del menú en el lado izquierdo, haga clic la ficha Manager del cifrado bajo menú de seguridad.Especifique el VLA N que se aplicará.Especifique que se usará el encripción WEP.Especifique que su uso es OBLIGATORIO.Inicialice cualquier clave WEP con un carácter hexadecimal 26-digit. Esta clave se utiliza para cifrar el broadcast y los paquetes de multidifusión. Este paso es opcional.Fije el tamaño de clave a los bits 128. Usted puede también elegir 40 bits. En este caso, el tamaño de la clave WEP en el paso anterior debe ser un carácter hexadecimal 10-digit. Este paso es opcional.Usted puede también habilitar la rotación dominante del broadcast y especificar el tiempo después de lo cual se cambia la clave del broadcast. Si se inhabilita, la clave del broadcast todavía se utiliza pero no se cambia. Este paso es opcional.**Nota:** Estos pasos se relanzan para cada VLA N que utilice la autenticación LEAPHaga clic en Apply (Aplicar).

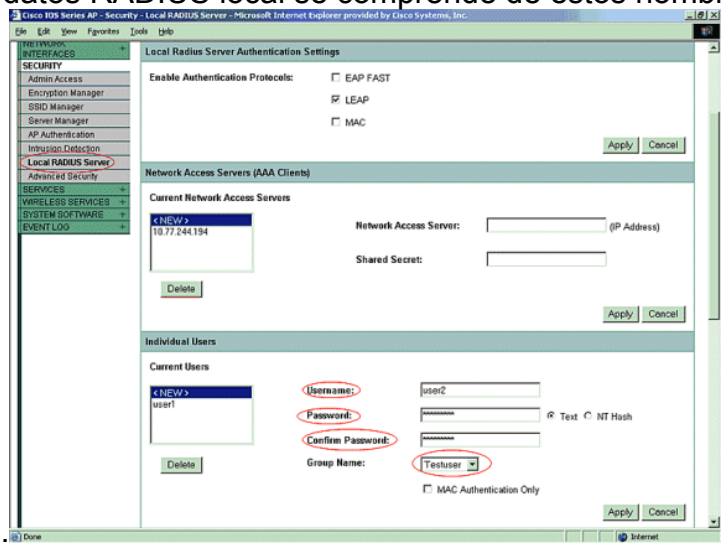


3. Bajo menú de seguridad, de la lengueta del administrador SSID, realice estas acciones:**Nota:** Usted puede agregar las características adicionales y la administración de claves más adelante, una vez que usted confirma que la configuración baja trabaja correctamente.Defina un nuevo SSID y asocíelo a un VLA N. En este ejemplo, el SSID se asocia al VLAN1.**Autenticación abierta del** control **(con el EAP).Red EAP (ninguna adición) del** control.**De los servidores de las prioridades > de la autenticación EAP del servidor**, elija **personalizan**; elija la dirección IP de este forPriority **1. del** Punto de acceso.Haga clic en Apply (Aplicar). 

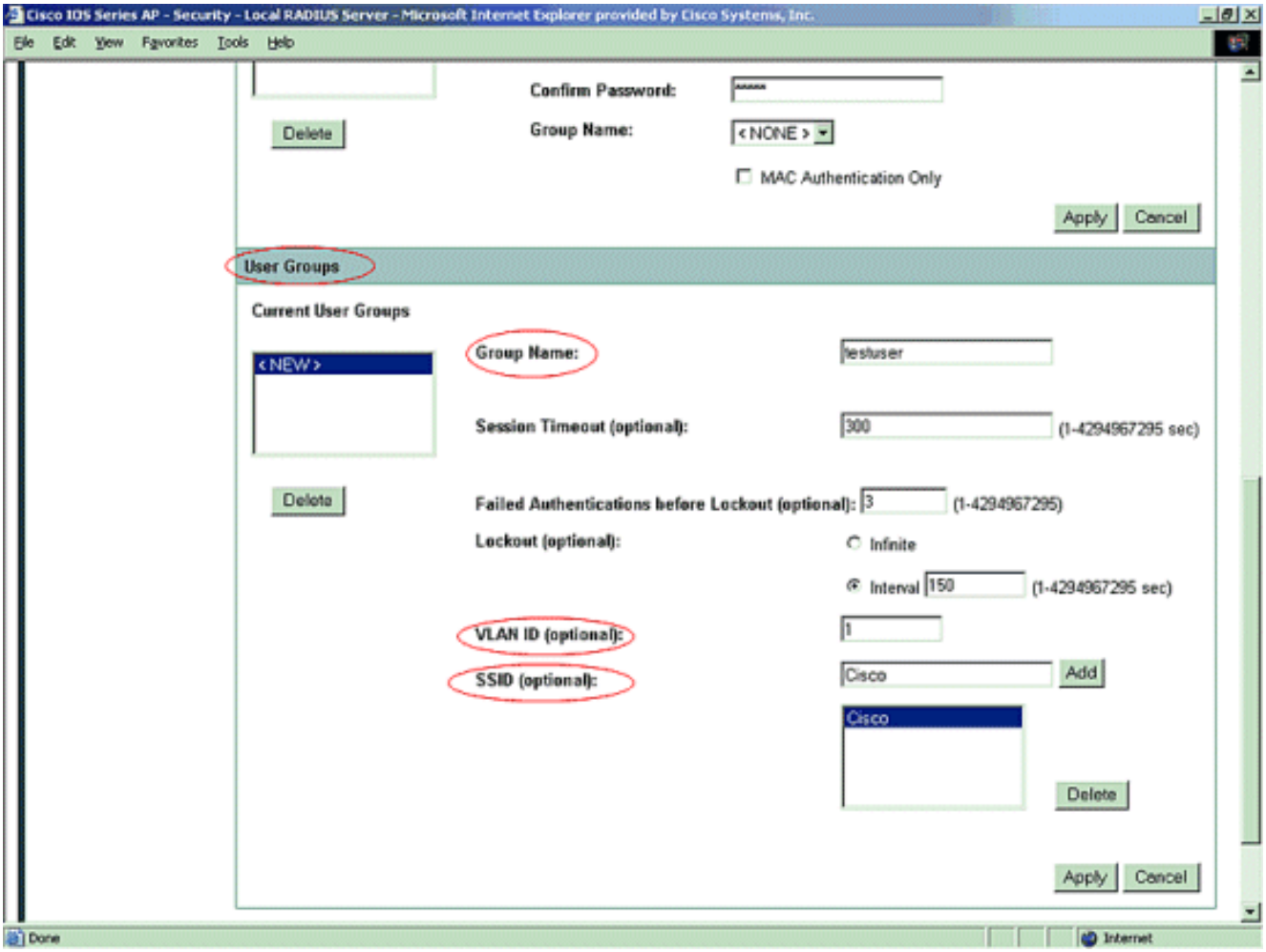
4. Bajo Seguridad, haga clic al servidor de RADIUS local de la lengueta general de la configuraciónBajo configuraciones locales de la autenticación de servidor de RADIUS, **SALTO del** control a aseegurarse que las peticiones de la autenticación LEAP están validadas.Defina la dirección IP y el secreto compartido del servidor RADIUS. Para el servidor de RADIUS local, ésta es la dirección IP de este AP (10.77.244.194).Haga clic en Apply
(Aplicar).



5. Navegue hacia abajo del servidor de RADIUS local bajo lengueta general de la configuración y defina a los usuarios individuales con sus nombres de usuario y contraseña. Opcionalmente, los usuarios pueden ser asociados a los grupos, que se define en el siguiente paso. Esto se aseegura ese solamente registro de ciertos usuarios en un SSID.**Nota:** La base de datos RADIUS local se comprende de estos nombres de usuario y contraseña individuales.



6. Navegue más lejos abajo en la misma página, otra vez del servidor de RADIUS local bajo lengueta general del submarino de la configuración a los grupos de usuarios; defina a los grupos de usuarios y asocíelos a un VLA N o a un SSID.



Nota: Los grupos son optativos. Los atributos de grupo no se envían a Active Directory y son relevantes sólo a nivel local. Usted puede agregar a los grupos más adelante, una vez que usted confirma que la configuración baja trabaja correctamente.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

- **¿muestre las estadísticas del servidor local del radio**? Este comando visualiza las estadísticas recogidas por el autenticador local.`ap#show running-config Building configuration.....aaa new-model !--- This command reinitializes the authentication, !--- authorization and accounting functions.!!aaa group server radius rad_eap server 10.77.244.194 auth-port 1812 acct-port 1813!--- A server group for RADIUS is created called "rad_eap" !--- that uses the server at 10.77.244.194 on ports 1812 and 1813....aaa authentication login eap_methods group rad_eap!--- Authentication [user validation] is to be done for !--- users in a group called "eap_methods" who use server group "rad_eap"....! bridge irb!interface Dot11Radio0 no ip address no ip route-cache ! encryption vlan 1 key 1 size 128bit 12345678901234567890123456 transmit-key!This step is optional----!--- This value seeds the initial key for use with !--- broadcast [255.255.255.255] traffic. If more than one VLAN is !--- used, then keys must be set for each VLAN. encryption vlan 1 mode wep mandatory !--- This defines the policy for the use of Wired Equivalent Privacy (WEP). !--- If more than one VLAN is used, !--- the policy must be set to mandatory for each VLAN. broadcast-key vlan 1 change 300 !--- You can also enable Broadcast Key Rotation for each vlan and Specify the time after which Brodacst key is changed. If it is disabled Broadcast Key is still used but not changed.ssid cisco vlan 1!--`

```
- Create a SSID Assign a vlan to this SSID                authentication open eap eap_methods
authentication network-eap eap_methods  !--- Expect that users who attach to SSID "cisco" !---
request authentication with the type 128 Open EAP and Network EAP authentication !--- bit set in the
headers of those requests, and group those users into !--- a group called "eap_methods." ! speed
basic-1.0 basic-2.0 basic-5.5 basic-11.0 rts threshold 2312 channel 2437 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-group 1 block-unknown-source no bridge-group 1
source-learning no bridge-group 1 unicast-flooding bridge-group 1 spanning-disabled...interface
FastEthernet0 no ip address no ip route-cache duplex auto speed auto bridge-group 1 no bridge-group 1
source-learning bridge-group 1 spanning-disabled!interface BVI1 ip address 10.77.244.194
255.255.255.0 !--- The address of this unit. no ip route-cache!ip default-gateway 10.77.244.194ip
http serverip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100ip radius source-interface
BVI1snmp-server community cable ROsnmp-server enable traps ttyradius-server local !--- Engages the
Local RADIUS Server feature. nas 10.77.244.194 key shared_secret !--- Identifies itself as a RADIUS
server, reiterates !--- "localness" and defines the key between the server (itself) and the access
point. ! group testuser !--- Groups are optional. ! user user1 nthash password1 group testuser !---
Individual user user user2 nthash password2 group testuser !--- Individual user!--- These individual
users comprise the Local Database!radius-server host 10.77.244.194 auth-port 1812 acct-port    1813
key shared_secret!--- Defines where the RADIUS server is and the key between !--- the access point
(itself) and the server.radius-server retransmit 3radius-server attribute 32 include-in-access-req
format %hradius-server authorization permit missing Service-Typeradius-server vsa send
accountingbridge 1 route ip!!line con 0line vty 5 15!end
```

- **¿muestre el grupo de servidores todo del radio**? Este comando visualiza una lista de todos los grupos de servidores configurados RADIUS en el Punto de acceso.

Troubleshooting

Procedimiento de Troubleshooting

Esta sección proporciona la información de Troubleshooting relevante a esta configuración.

1. Para eliminar la posibilidad de los problemas RF que previenen la autenticación satisfactoria, fije el método en el SSID **para abrirse** para inhabilitar temporalmente la autenticación.¿Del GUI? En la página del administrador SSID, desmarque el **Network EAP** y marque **abierto**.¿De la línea de comando? Use los comandos authentication open y no authentication network-eap eap_methods.Si el cliente se asocia con éxito, el RF no contribuye al problema de asociación.
2. Verifique que todas las contraseñas secretas compartidas estén sincronizadas. Las líneas `clave del acct-puerto x del auténtico-puerto x del host de servidor RADIUS x.x.x.x <shared_secret> y clave` NAS `x.x.x.x <shared_secret> deben contener la` misma contraseña del secreto compartido.
3. Quite cualesquiera grupos de usuarios y configuración sobre los grupos de usuarios. Los conflictos pueden ocurrir a veces entre los grupos de usuarios definidos por el Punto de acceso, y los grupos de usuarios en el dominio.

Comandos para resolución de problemas

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- **¿haga el debug del authenticator todo aaa del dot11**? Este debug muestra a diversas negociaciones que va un cliente a través mientras que el cliente se asocia y autentica con el 802.1x o el proceso EAP desde la perspectiva del authenticator (Punto de acceso). Este

debug fue introducido en el Cisco IOS Software Release 12.2(15)JA. Este comando toma obsoleto el comando debug dot11 aaa dot1x en esa versión y en las posteriores. *Mar 1 00:26:03.097: dot11_auth_add_client_entry: Create new client 0040.96af.3e93 for application 0x1 *Mar 1 00:26:03.097: dot11_auth_initialize_client: 0040.96af.3e93 is added to the client list for application 0x1---------- Lines Omitted for simplicity ----------*Mar 1 00:26:03.098: dot11_auth_dot1x_start: in the dot11_auth_dot1x_start*Mar 1 00:26:03.132: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,EAP_START) for 0040.96af.3e93*Mar 1 00:26:03.132: dot11_auth_dot1x_send_id_req_to_client: **Sending identity request to 0040.96af.3e93*(client)***Mar 1 00:26:03.133: *Mar 1 00:26:03.099: dot11_auth_dot1x_send_id_req_to_client: Client 0040.96af.3e93 timer started for 30 seconds *Mar 1 00:26:03.132: dot11_auth_parse_client_pak: **Received EAPOL packet from 0040.96af.3e93**---------- Lines Omitted----------*Mar 1 00:26:03.138: EAP code: 0x2 id: 0x1 length: 0x000A type: 0x1 01805BF0: 0100000A 0201000A 01757365 7231 .....**user1*(User Name of the client)*** *Mar1 00:26:03.146: dot11_auth_dot1x_run_rfsm: Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93*Mar1 00:26:03.147:dot11_auth_dot1x_send_response_to_server: **Sending client 0040.96af.3e93 data toserver** *Mar1 00:26:03.147: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds---------- Lines Omitted----------*Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp: **Received server response:GET_CHALLENGE_RESPONSE** *Mar1 00:26:03.150: dot11_auth_dot1x_parse_aaa_resp: found session timeout 10 sec*Mar 1 00:26:03.150: dot11_auth_dot1x_run_rfsm: Executing Action(SERVER_WAIT,SERVER_REPLY) for 0040.96af.3e93*Mar 1 00:26:03.150: dot11_auth_dot1x_send_response_to_client: **Forwarding server message to client 0040.96af.3e93**---------- Lines Omitted----------*Mar 1 00:26:03.151: dot11_auth_send_msg: **Sending EAPOL to requestor***Mar 1 00:26:03.151: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 10 seconds*Mar 1 00:26:03.166: dot11_auth_parse_client_pak: **Received EAPOL packet*(User Credentials)* from 0040.96af.3e93***Mar 1 00:26:03.166: EAP code: 0x2 id: 0x11 length: 0x0025 type: 0x1101805F90: 01000025 02110025...%...%01805FA0: 11010018 7B75E719 C5F3575E EFF64B27 **....{ug.EsW^ovK'** Executing Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96af.3e93*Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server: **Sending client 0040.96af.3e93 data *(User Credentials)* to server***Mar 1 00:26:03.186: dot11_auth_dot1x_send_response_to_server: Started timer server_timeout 60 seconds---------- Lines Omitted----------*Mar 1 00:26:03.196: dot11_auth_dot1x_parse_aaa_resp: **Received server response: PASS***Mar1 00:26:03.197: dot11_auth_dot1x_run_rfsm: ExecutingAction(SERVER_WAIT,SERVER_PASS) for 0040.96af.3e93 *Mar 1 00:26:03.197: dot11_auth_dot1x_send_response_to_client: **Forwarding server message*(Pass Message)* to client**---------- Lines Omitted----------*Mar 1 00:26:03.198: dot11_auth_send_msg: Sending EAPOL to requestor*Mar 1 00:26:03.199: dot11_auth_dot1x_send_response_to_client: Started timer client_timeout 30 second*Mar 1 00:26:03.199: dot11_auth_send_msg: **client authenticated 0040.96af.3e93,** node_type 64 for application 0x1*Mar 1 00:26:03.199: dot11_auth_delete_client_entry: 0040.96af.3e93 is deleted for application 0x1*Mar 1 00:26:03.200: %DOT11-6-ASSOC: **Interface Dot11Radio0, Station *Station Name* 0040.96af.3e93 Associated KEY_MGMT[NONE]**

- ¿**autenticación de RADIUS del debug**? Este debug muestra las negociaciones RADIUS entre el servidor y el cliente, que, en este caso, son el Punto de acceso.
- ¿**cliente del servidor local del radio del debug**? Este debug muestra la autenticación del cliente desde la perspectiva del servidor de RADIUS. *Mar 1 00:30:00.742: RADIUS(0000001A): **SendAccess-Request*(Client's User Name)* to 10.77.244.194:1812*(Local Radius Server)*** id 1645/65, len 128 *Mar 1 00:30:00.742: RADIUS: **User-Name [1] 7 "user1"** *Mar 1 00:30:00.742: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0" *Mar 1 00:30:00.743: RADIUS: **Calling-Station-Id [31] 16 "0040.96af.3e93" *(Client)*** *Mar 1 00:30:00.743: RADIUS: Service-Type [6] 6 Login [1] *Mar 1 00:30:00.743: RADIUS: Message-Authenticato[80] *Mar 1 00:30:00.743: RADIUS: 23 2E F4 42 A4 A3 72 4B 28 44 6E 7A 58 CA 8F 7B [#.?B??rK(DnzX??{] *Mar 1 00:30:00.743: RADIUS: EAP-Message [79] 12 *Mar 1 00:30:00.743: **RADIUS: 02 02 00 0A 01 75 73 65 72 31 [?????user1]** *Mar 1 00:30:00.744: RADIUS: NAS-Port-Type [61] 6 802.11 wireless---------- Lines Omitted For Simplicity---------- *Mar 1 00:30:00.744: RADIUS: **NAS-IP-Address [4] 6 10.77.244.194*(Access Point IP)***Mar 1 00:30:00.744: RADIUS: Nas-Identifier [32] 4 "ap" ---------- Lines Omitted---------- *Mar 1 00:30:00.745: RADIUS: **Received from id 1645/65 10.77.244.194:1812, Access-Challenge**, len 117 *Mar 1 00:30:00.746: RADIUS: 75 73 65 72 31 **[user1]** *Mar 1 00:30:00.746: RADIUS: Session-Timeout [27] 6 10 *Mar 1 00:30:00.747: RADIUS: State [24] 50 *Mar 1 00:30:00.747: RADIUS:

```
BF 2A A0 7C 8265 76 AA 00 00 00 00 00 00 00 00    [?*?|?ev?????????]  ------------------------------
--------   Lines Omitted for simplicity ------------ *Mar 1 00:30:00.756:
RADIUS/ENCODE(0000001A):Orig. component type = DOT11*Mar 1 00:30:00.756: RADIUS: AAA Unsupported
Attr: ssid [264] 5  *Mar 100:30:00.756: RADIUS: 63 69 73 [cis]  *Mar 1 00:30:00.756: RADIUS: AAA
Unsupported Attr: interface [157] 3  *Mar 1 00:30:00.756: RADIUS: 32 [2]  *Mar 1 00:30:00.757:
RADIUS(0000001A): Config NAS IP: 10.77.244.194 *Mar 1 00:30:00.757: RADIUS/ENCODE(0000001A):
acct_session_id: 26  *Mar 1 00:30:00.757: RADIUS(0000001A): Config NAS IP: 10.77.244.194 *Mar 1
00:30:00.779: RADIUS(0000001A):    Send Access-Request to 10.77.244.194:1812 id 1645/67, len 189
*Mar 1 00:30:00.779: RADIUS:    authenticator B0 15 3C C1 BC F6 31 85 - 66 5D 41 F9 2E B4 48 7F  *Mar
1 00:30:00.779: RADIUS: User-Name [1] 7 "user1"  *Mar 1 00:30:00.780: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 00:30:00.780: RADIUS: Called-Station-Id [30] 16"0019.a956.55c0"  *Mar 1 00:30:00.780: RADIUS:
Calling-Station-Id [31] 16"0040.96af.3e93"  *Mar  1 00:30:00.758: RADIUS:      92 D4 24 49 04 C2 D2
0A C3 CE E9 00 6B F1 B2 AF  [??$I????????k???] *Mar  1 00:30:00.759: RADIUS:  EAP-Message
[79]  39   *Mar  1 00:30:00.759: RADIUS:      02 17 00 25 11 01 00 18 05 98 8B BE 09 E9 45 E2
[??????????????E?] *Mar  1 00:30:00.759: RADIUS:      73 5D 33 1D F0 2F DB 09 50 AF 38 9F F9 3B BD D4
[s]3??/??P?8??;??] *Mar  1 00:30:00.759: RADIUS:      75 73 65 72 31
[user1] ---------------------------------------   Lines Omitted-------------------------- *Mar 1
00:30:00.781: RADIUS: State [24] 50 RADIUS:    NAS-IP-Address [4] 6 10.77.244.194*Mar 1 00:30:00.783:
RADIUS: Nas-Identifier [32] 4 "ap" *Mar 1 00:30:00.822: RADIUS:    Received from id 1645/67
10.77.244.194:1812, Access-Accept, len 214  *Mar 1 00:30:00.822:    RADIUS: authenticator 10 0C B6 EE
7A 96 3A 46 - 36 49 FC D3 7A F4 42 2A  ------------------------------------   Lines Omitted-------
--------------------- *Mar 1 00:30:00.823: RADIUS: 75 73 65 72 31 [user1]*Mar 1 00:30:00.823: RADIUS:
Vendor, Cisco [26] 59  *Mar 1 00:30:00.823: RADIUS:    Cisco AVpair [1] 53 "leap:session-
key=?+*ve=];q,oi[d6|-z."  *Mar 1 00:30:00.823:    RADIUS: User-Name [1] 28 "user1 *Mar 1
00:30:00.824: RADIUS:    Message-Authenticato[80] 18  *Mar 1 00:30:00.824: RADIUS:    06 2D BA 93 10
C0 91 F8 B4 B8 A4 00 82 0E 11 36   [?-????????????6]    *Mar 1 00:30:00.826: RADIUS/DECODE: EAP-
Message fragments,37, total 37 bytes *Mar 1 00:30:00.826: found leap session key  *Mar 1
00:30:00.830: %DOT11-6-ASSOC:    Interface Dot11Radio0, Station Station Name Associated
KEY_MGMT[NONE]
```

- ¿**paquetes del servidor local del radio del debug**? Este debug muestra todos los procesos hechos por y desde la perspectiva del servidor de RADIUS.

Información Relacionada

- Configuración de un punto de acceso como un autenticador local
- Configuración de los tipos de autenticación
- Configuración de los servidores RADIUS y TACACS+
- Soporte Técnico y Documentación - Cisco Systems