Autenticación PEAP del WLC de las 5760/3850 Series con el ejemplo de configuración de Microsoft NP

ID del Documento: 117684

Actualizado: Mayo 05, 2014

Contribuido por Surendra BG, ingeniero de Cisco TAC.

Productos Relacionados

- Reguladores del Wireless LAN de las Cisco 5700 Series
- Remote Authentication Dial-In User Service (RADIUS)

Contenido

Introducción

Este documento describe cómo configurar el protocolo extensible authentication protegido (PEAP) con la autenticación del protocolo microsoft challenge handshake authentication versión 2 (v2 MS-CHAP) en Cisco convergió despliegue del Wireless LAN del acceso (red inalámbrica (WLAN)) con el servidor de políticas de la red de Microsoft (NP) como el servidor de RADIUS.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de estos temas antes de que usted intente la configuración descrita en este documento:

- Instalación básica de la versión 2008 de Microsoft Windows
- Cisco convergió instalación del controlador de WLAN del acceso

Asegúrese de que estos requisitos estén cumplidos antes de que usted intente esta configuración:

- Instale el operating system (OS) de la versión 2008 del Microsoft Windows server en cada uno de los servidores en el laboratorio de prueba.
- Ponga al día todos los paquetes de servicios.
- Instale los reguladores y los Puntos de acceso ligeros (revestimientos).
- Configure las actualizaciones de último software.

> Nota: Para la instalación inicial y la información de la configuración para Cisco convergieron los controladores de WLAN del acceso, refieren al artículo de Cisco del ejemplo de configuración del regulador CT5760 y del Catalyst 3850 Switch.

Componentes Utilizados

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

- Versión 3.3.2 del controlador de WLAN de las Cisco 5760 Series (Wiring Closet de la última generación (NGWC))
- REVESTIMIENTO de las Cisco 3602 Series
- Microsoft Windows XP con el supplicant de Intel PROset
- Servidor de la versión 2008 de Microsoft Windows que ejecuta los NP con los papeles del controlador de dominio
- Cisco Catalyst 3560 Series Switch

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.

Antecedentes

Seguridad del nivel del transporte de las aplicaciones PEAP (TLS) para crear un canal cifrado entre un cliente PEAP de autenticidad, tal como una laptop inalámbrica, y un authenticator PEAP, tal como Microsoft NP o cualquier servidor de RADIUS. El PEAP no especifica un método de autentificación sino proporciona la seguridad complementaria para otros protocolos extensible authentication (EAP), por ejemplo el v2 EAP-MS-CHAP, que puede actuar a través del canal TLS-cifrado que es proporcionado por el PEAP. El proceso de autenticación PEAP consiste en dos fases principales.

Fase uno PEAP: Canal TLS-cifrado

Los socios del cliente de red inalámbrica con el punto de acceso. Una asociación de IEEE 802.11-based proporciona un sistema operativo o una clave de autenticación compartida antes de que una asociación segura se cree entre el cliente y el AP. Después de que la asociación de IEEE 802.11-based se establezca con éxito entre el cliente y el AP, la sesión de TLS se negocia con el AP.

Después de que la autenticación se complete con éxito entre el cliente de red inalámbrica y los NP, la sesión de TLS se negocia entre el cliente y los NP. La clave que se deriva dentro de esta negociación se utiliza para cifrar toda la comunicación subsiguiente.

Fase dos PEAP: Comunicación EAP-autenticada

La comunicación EAP, que incluye la negociación EAP, ocurre dentro del canal de TLS que es creado por el PEAP dentro de la primera fase del proceso de autenticación PEAP. Los NP autentican al cliente de red inalámbrica con el v2 EAP-MS-CHAP. El REVESTIMIENTO y los mensajes delanteros del regulador solamente entre el cliente de red inalámbrica y el servidor de RADIUS. El controlador de WLAN (WLC) y el REVESTIMIENTO no pueden desencriptar los mensajes porque el WLC no es el punto final de TLS.

Aquí está la secuencia del mensaje de RADIUS para una tentativa de la autenticación satisfactoria, donde el usuario suministra las credenciales basadas en la contraseña válidas el v2 PEAP-MS-CHAP:

1. Los NP envían un mensaje request de la identidad al cliente:
   `EAP-Request/Identity`
2. El cliente responde con un mensaje de respuesta de la identidad:
   `EAP-Response/Identity`
3. Los NP envían un mensaje de impugnación del v2 MS-CHAP:
   `EAP-Request/EAP-Type=EAP MS-CHAP-V2 (Challenge)`
4. El cliente responde con un desafío y una respuesta del v2 MS-CHAP:
   `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Response)`
5. Los NP responden con un paquete del éxito del v2 MS-CHAP cuando el servidor autentica con éxito al cliente:
   `EAP-Request/EAP-Type=EAP-MS-CHAP-V2 (Success)`
6. El cliente responde con un paquete del éxito del v2 MS-CHAP cuando el cliente autentica con éxito el servidor:
   `EAP-Response/EAP-Type=EAP-MS-CHAP-V2 (Success)`
7. Los NP envían un EAP-tipo-longitud-valor (TLV) que indique la autenticación satisfactoria.
8. El cliente responde con un Mensaje de éxito del estatus EAP-TLV.

9. El servidor completa la autenticación y envía un mensaje del EAP-éxito en el sólo texto. Si los VLA N se despliegan para el aislamiento del cliente, los atributos del VLA N se incluyen en este mensaje.

Configurar

Utilice esta sección para configurar el PEAP con la autenticación del v2 MS-CHAP en Cisco convergió despliegue del WLC del acceso con Microsoft NP como el servidor de RADIUS.

Diagrama de la red

En este ejemplo, el servidor de la versión 2008 de Microsoft Windows realiza estos papeles:

- Controlador de dominio para el dominio de **wireless.com**
- Servidor del Domain Name System (DNS)
- Servidor del Certificate Authority (CA)
- NP para autenticar a los usuarios de red inalámbrica
- Active Directory (AD) para mantener la base de datos de usuarios

El servidor conecta con la red alámbrica a través de un Switch de la capa 2 (L2), como se muestra. El WLC y el REVESTIMIENTO registrado también conectan con la red a través del Switch L2.

El Wi-Fi del uso de los clientes de red inalámbrica protegió el acceso 2 (WPA2) - autenticación del v2 PEAP-MS-CHAP para conectar con la red inalámbrica.

Configuraciones

La configuración que se describe en esta sección se completa en dos pasos:

1. Configure el WLC de las 5760/3850 Series con el CLI o el GUI.

2. Configure el servidor de la versión 2008 de Microsoft Windows para los NP, el controlador de dominio, y las cuentas de usuario en el AD.

Configure el WLCs convergido del acceso con el CLI

Complete estos pasos para configurar la red inalámbrica (WLAN) para el VLA N requerido del cliente y asociarla a la lista del método de autentificación con el CLI:

> Nota: Asegúrese de que el **control del auth del sistema del dot1x** esté habilitado en el WLC, o el dot1x no trabaja.

1. Habilite la característica del **modelo nuevo AAA**.

2. Configure al servidor de RADIUS.

3. Agregue el servidor en el grupo de servidores.

4. Asocie al grupo de servidores a la lista de métodos.

5. Asocie la lista de métodos a la red inalámbrica (WLAN).

```
aaa new-model
!
!
aaa group server radius Microsoft_NPS
 server name Microsoft_NPS
!
aaa authentication dot1x Microsoft_NPS group Microsoft_NPS aaa authorization network
Microsoft_NPS group Microsoft_NPS
radius server Microsoft_NPS
 address ipv4 10.104.208.96 auth-port 1645 acct-port 1646
 timeout 10
 retransmit 10
 key Cisco123 wlan Microsoft_NPS 8 Microsoft_NPS
 client vlan VLAN0020
 no exclusionlist
 security dot1x authentication-list Microsoft_NPS
 session-timeout 1800
 no shutdown
```

Configure el WLCs convergido del acceso con el GUI

Complete estos pasos para configurar el WLCs convergido del acceso con el GUI:

1. Habilite el sistema-auth-**control del dot1x**:

2. Navegue al > Security (Seguridad) de la **configuración** >AAA para agregar al servidor de RADIUS:

3. Navegue a **RADIUS > los servidores**, haga clic **NUEVO**, y ponga al día la dirección IP del servidor de RADIUS junto con el secreto compartido. El secreto compartido debe hacer juego el secreto compartido que se configura en el servidor de RADIUS también.

   Después de que usted configure al servidor de RADIUS, la lengueta del servidor debe aparecer similar a esto:

4. Configure a un grupo de servidores y seleccione el **radio** para el Tipo de grupo. Entonces, agregue al servidor de RADIUS que usted creó en el paso anterior:

El grupo de servidores debe aparecer similar a esto después de la configuración:

5. **Dot1x** selecto para el tipo y el **grupo de la** lista del método de autentificación para el Tipo de grupo. Entonces, asocie al grupo de servidores que usted configuró en el paso anterior:

   La lista del método de autentificación debe aparecer similar a esto después de la configuración:

6. **Red** selecta para el tipo y el **grupo de la** lista del método de autorización para el Tipo de grupo. Entonces, asocie al grupo de servidores que usted configuró en el paso anterior:

   La lista del método de autorización debe aparecer similar a esto después de la configuración:

7. Navegue **para configurar > Tecnología inalámbrica** y para hacer clic la configuración de cuadro de la **red inalámbrica (WLAN) una** nueva red inalámbrica (WLAN) a la cual los usuarios puedan conectar y autenticarse a través del servidor de Microsoft NP con la autenticación EAP:

   La lengueta de la Seguridad L2 debe aparecer similar a esto después de la configuración:

8. Asocie la lista de métodos que usted configuró en los pasos anteriores. Esto ayuda a autenticar al cliente al servidor correcto.

Configuración en el servidor de la versión 2008 de Microsoft Windows

Esta sección describe una configuración completa del servidor de la versión 2008 de Microsoft Windows. La configuración se completa en seis pasos:

1. Configure el servidor como controlador de dominio.

2. Instale y configure el servidor como servidor de CA.

3. Instale los NP.

4. Instale un certificado.

5. Configure los NP para la autenticación PEAP.

6. Agregue a los usuarios al AD.

Configure el servidor de Microsoft Windows 2008 como controlador de dominio

Complete estos pasos para configurar el servidor de la versión 2008 de Microsoft Windows como controlador de dominio:

1. Navegue **para comenzar > administrador de servidor > los papeles de los papeles >** Add.

2. Haga clic en Next (Siguiente).

3. Marque la casilla de verificación de los **servicios del dominio de Active Directory** y haga clic **después**.

4. Revise la **introducción a los servicios del dominio de Active Directory** y haga clic **después**.

5. El tecleo **instala** para comenzar el proceso de instalación.

   La instalación procede y completa.

6. Haga clic **cerca a este Asisitente y inicie al asistente de instalación de los servicios del dominio de Active Directory (dcpromo.exe) para** continuar la instalación y la configuración del AD.

7. Haga clic **después** para funcionar con al **asistente de instalación de los servicios del dominio de Active Directory**.

8. Revise la información sobre la **compatibilidad del sistema operativo** y haga clic **después**.

9. Haga clic el **crear un nuevo dominio en un nuevo** botón de radio del **bosque** y haga clic **después** para crear un nuevo dominio.

10. Ingrese el nombre DNS completo para el nuevo dominio (**wireless.com** en este ejemplo) y haga clic **después**.

11. Seleccione el **nivel funcional del bosque** para su dominio y haga clic **después**.

12. Seleccione el **nivel funcional del dominio** para su dominio y haga clic **después**.

13. Marque la casilla de verificación del **servidor DNS** y haga clic **después**.

14. Haga clic **sí** cuando la ventana emergente del **asistente de instalación de los servicios del dominio de Active Directory** aparece para crear una nueva zona en el DNS para el dominio.

15. Seleccione las carpetas que usted quisiera que el AD utilice para los archivos e hiciera clic **después**.

16. Ingrese la contraseña del administrador y haga clic **después**.

17. Revise sus selecciones y haga clic **después**.

Los ingresos de la instalación.

18. Clic en Finalizar **para cerrar al Asisitente.**

19. Recomience el servidor para que los cambios tomen el efecto.

Instale y configure el servidor de la versión 2008 de Microsoft Windows como servidor de CA

El PEAP con el v2 EAP-MS-CHAP valida al servidor de RADIUS basado sobre el certificado que está presente en el servidor. Además, el certificado de servidor se debe publicar por un público CA que sea confiado en por la computadora cliente. Es decir, el certificado de CA público existe ya en la carpeta del Trusted Root Certification Authority en el almacén de certificados de la computadora cliente.

Complete estos pasos para configurar el servidor de la versión 2008 de Microsoft Windows como servidor de CA que publique el certificado a los NP:

1. Navegue **para comenzar > administrador de servidor > los papeles de los papeles >** Add.

2. Haga clic en Next (Siguiente).

3. Marque la casilla de verificación de los **servicios de certificados del Active Directory** y haga clic **después**.

4. Revise la **introducción a los servicios de certificados del Active Directory** y haga clic **después**.

5. Marque la casilla de verificación del **Certificate Authority** y haga clic **después**.

6. Haga clic el botón de radio de la **empresa** y haga clic **después**.

7. Haga clic **raíz CA el** botón de radio y haga clic **después**.

8. Haga clic el **crear un nuevo** botón de radio de la **clave privada** y haga clic **después**.

9. Haga clic **después** en la **criptografía que configura para la** ventana de **CA**.

10. Haga clic **después** para validar el **Common Name para este** nombre predeterminado de **CA**.

11. Seleccione la longitud del tiempo para la cual el certificado de CA es válido y haga clic **después**.

12. Haga clic **después** para validar la ubicación predeterminada de la **ubicación de la base de datos del certificado**.

13. Revise la configuración y el tecleo **instala** para comenzar los **servicios de certificados del Active Directory**.

14. Después de que se complete la instalación, **cierre del** tecleo.

Instale los NP en el servidor de la versión 2008 de Microsoft Windows

> Nota: Con la configuración que se describe en esta sección, los NP se utilizan mientras que un servidor de RADIUS para autenticar a los clientes de red inalámbrica con la autenticación PEAP.

Complete estos pasos para instalar y configurar los NP en el servidor de la versión 2008 de Microsoft Windows:

1. Navegue **para comenzar > administrador de servidor > los papeles de los papeles >** Add.

2. Haga clic en Next (Siguiente).

3. Marque la casilla de verificación de los **servicios de la política de red y del acceso** y haga clic **después**.

4. Revise la **introducción a los servicios de la política de red y del acceso** y haga clic **después**.

5. Marque la **política de red casilla de selección del servidor** y haga clic **después**.

6. Revise la confirmación y el tecleo **instala**.

   Después de que la instalación sea completa, una pantalla similar a esto debe aparecer:

7. Haga clic en Close (Cerrar).

Instale un certificado

Complete estos pasos para instalar el certificado del ordenador para los NP:

1. Haga clic el **comienzo**, ingrese el Microsoft Management Console (MMC), y el Presione ENTER.

2. Navegue **para clasifiar** > Add**/quite Broche-en**.

3. Elija los **Certificados** y el haga click en Add

4. Haga clic el botón de radio de la **cuenta de la Computadora** y haga clic **después**.

5. Haga clic el botón de radio y el clic en Finalizar de la **computadora local**.

6. Haga Click en OK para volver al MMC.

7. Amplíe los **Certificados (computadora local)** y las **carpetas personales**, y haga clic los **Certificados**.

8. Haga clic con el botón derecho del ratón el espacio blanco en el certificado de CA, y elija **todas las tareas > certificado de la petición nuevo**.

9. Haga clic en Next (Siguiente).

10. Haga clic la casilla de verificación del **controlador de dominio**, y el tecleo **alista**.

    Nota: Si la autenticación de cliente falla debido a un error del certificado EAP, después asegúrese de que todas las casillas de verificación estén comprobadas esta página de la **inscripción del certificado** antes de que usted tecleo **aliste**. Esto crea aproximadamente tres Certificados.

11. Clic en Finalizar una vez que el certificado está instalado.

    El certificado NP ahora está instalado.

12. Asegure esa **autenticación de cliente, autenticación de servidor** aparece en la columna prevista de los propósitos para el certificado.

Configure el servicio de servidor de la política de red para la autenticación del v2 PEAP-MS-CHAP

Complete estos pasos para configurar los NP para la autenticación:

1. Navegue al **Start (Inicio) > Administrative Tools (Herramientas administrativas)** > al **servidor de la política de red**.

2. Haga clic con el botón derecho del ratón los **NP (locales)** y elija el **servidor del registro en el Active Directory**.

3. Haga clic en OK.

4. Haga clic en OK.

5. Agregue el WLC como cliente del Authentication, Authorization, and Accounting (AAA) en los NP.

6. Amplíe los **clientes RADIUS y los servidores**. Haga clic con el botón derecho del ratón a los **clientes RADIUS** y elija al **nuevo cliente RADIUS**:

7. Ingrese un nombre (**WLC** en este ejemplo), el IP Address de administración del WLC (**10.105.135.178** en este ejemplo), y un secreto compartido.

   Nota: El mismo secreto compartido se utiliza para configurar el WLC.

8. Haga Click en OK para volver a la pantalla anterior.

9. Cree una nueva política de red para los usuarios de red inalámbrica. Amplíe las **directivas**, haga clic con el botón derecho del ratón las **políticas de red**, y elija **nuevo**:

10. Ingrese un nombre de la directiva para esta regla (**PEAP** en este ejemplo) y haga clic **después**.

11. Para configurar esta directiva para permitir solamente a los usuarios del dominio de red inalámbrica, agregue estas tres condiciones y haga clic **después**:

12. Haga clic el botón de radio **concedido acceso** para conceder los intentos de conexión que hacen juego esta directiva y haga clic **después**.

13. Inhabilite todos los **métodos de autentificación menos seguros**:

14. El tecleo **agrega**, selecciona **Microsoft:** Tipo **protegido EAP (PEAP)** EAP, y **AUTORIZACIÓN del** tecleo para habilitar el PEAP.

15. Seleccione **Microsoft: El EAP protegido (PEAP)** y el tecleo **editan**. Asegúrese de que el certificado anterior-creado del controlador de dominio esté seleccionado en la lista desplegable publicada certificado y haga clic la **autorización**.

16. Haga clic en Next (Siguiente).

17. Haga clic en Next (Siguiente).

18. Haga clic en Next (Siguiente).

19. Haga clic en Finish (Finalizar).

Nota: Dependiente sobre sus necesidades, usted puede ser que necesite configurar las **directivas del pedido de conexión** en los NP para permitir el perfil PEAP o la directiva.

Agregue a los usuarios al Active Directory

Nota: En este ejemplo, la base de datos de usuarios se mantiene en el AD.

Complete estos pasos para agregar a los usuarios a la base de datos AD:

1. Navegue al **Start (Inicio) > Administrative Tools (Herramientas administrativas) >** a los **usuarios de directorio activo y computadora**.

2. En el árbol de la consola de los usuarios de directorio activo y computadora, amplíe el dominio, haga clic con el botón derecho del ratón a los **usuarios** y **nuevo**, y elija al **usuario**.

3. En el nuevo objeto - El cuadro de diálogo del usuario, ingresa el nombre del usuario de red inalámbrica. Este ejemplo utiliza el **client1** en el campo de primer nombre y el **client1** en el campo de nombre de inicio del usuario. Haga clic en Next (Siguiente).

4. En el nuevo objeto - El cuadro de diálogo del usuario, ingresa una contraseña de su opción en la contraseña y confirma los campos de contraseña. Desmarque al **usuario debe cambiar la contraseña en la** casilla de verificación **siguiente del inicio** y hacer clic **después**.

5. En el nuevo objeto - Cuadro de diálogo del usuario, clic en Finalizar.

6. Relance los pasos 2 a 4 para crear las cuentas de usuario adicionales.

Verificación

Complete estos pasos para verificar su configuración:

1. Busque para la identificación de conjunto de servicio (SSID) en la máquina del cliente.

2. Asegúrese de que el cliente esté conectado con éxito:

Troubleshooting

> Nota: Cisco recomienda que usted utiliza las trazas para resolver problemas los problemas inalámbricos. Las trazas se guardan en el buffer circular y no son hace un uso intensivo del procesador.

Permita a estas trazas para obtener los **registros del auth L2**:

- **fije el debug llano grupo-Tecnología inalámbrica-seguro de la traza**
- **fije el mac grupo-Tecnología inalámbrica-seguro 0017.7C2F.B69A del filtro de la traza**

Permita a estas trazas para obtener los **eventos del dot1x AAA**:

- **fije el debug del nivel de la traza wcm-dot1x aaa**
- **fije el mac 0017.7C2F.B69A del filtro de la traza wcm-dot1x aaa**

Permita a estas trazas para recibir los **eventos del DHCP**:

- **fije el debug llano de los eventos DHCP de la traza**
- **fije el mac 0017.7C2F.B69A del filtro de los eventos DHCP de la traza**

Permita a estas trazas para inhabilitar las trazas y borrar el buffer:

- **fije las sys-filtrar-trazas del control de traza claras**
- **fije el valor por defecto del nivel de la traza wcm-dot1x aaa**
- **fije el filtro de la traza wcm-dot1x aaa ningunos**

- fije el valor por defecto grupo-Tecnología inalámbrica-seguro del nivel de la traza
- fije el filtro grupo-Tecnología inalámbrica-seguro de la traza ningunos

Ingrese las sys-filtrar-**trazas de la traza de la demostración** ordenan para ver las trazas:

```
[04/23/14 21:27:51.963 IST 1 8151] 0017.7c2f.b69a Adding mobile on LWAPP AP
 1caa.076f.9e10 (0)
[04/23/14 21:27:51.963 IST 2 8151] 0017.7c2f.b69a Local Policy:  Created MSCB
 Just AccessVLAN = 0 and SessionTimeout  is 0 and apfMsTimeout is 0

[04/23/14 21:27:51.963 IST 8 8151] 0017.7c2f.b69a Local Policy:Setting local
 bridging VLAN  name VLAN0020 and VLAN ID  20

[04/23/14 21:27:51.963 IST 9 8151] 0017.7c2f.b69a Applying WLAN ACL policies
 to client
[04/23/14 21:27:51.963 IST a 8151] 0017.7c2f.b69a No Interface ACL used for
 Wireless client in WCM(NGWC)
[04/23/14 21:27:51.963 IST b 8151] 0017.7c2f.b69a Applying site-specific IPv6
 override for station  0017.7c2f.b69a  - vapId 8, site 'test',
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST c 8151] 0017.7c2f.b69a Applying local bridging
 Interface Policy for station  0017.7c2f.b69a  - vlan 20,
 interface 'VLAN0020'
[04/23/14 21:27:51.963 IST d 8151] 0017.7c2f.b69a
 **** Inside applyLocalProfilingPolicyAction ****

04/23/14 21:27:51.963 IST f 8151] 0017.7c2f.b69a     Local Profiling Values :
 isValidVlan = 0, vlan = 0, isVlanRecdInDelete = 0, isValidSessionTimeout = 0,
 sessionTimeout=0, isSessionTORecdInDelete = 0  ProtocolMap = 0 ,
 applyPolicyAtRun= 0
[04/23/14 21:27:51.963 IST 10 8151] 0017.7c2f.b69a          ipv4ACL = [],
 ipv6ACL = [], inQoS = [unknown], outQoS = [unknown]
[04/23/14 21:27:51.963 IST 11 8151] 0017.7c2f.b69a STA - rates (4):
 130 132 139 150 0 0 0 0 0 0 0 0 0 0 0 0
[04/23/14 21:27:51.963 IST 12 8151] 0017.7c2f.b69a STA - rates (12):
 130 132 139 150 12 18 24 36 48 72 96 108 0 0 0 0
[04/23/14 21:27:51.963 IST 13 8151] 0017.7c2f.b69a Processing RSN IE type 48,
 length 20 for mobile  0017.7c2f.b69a
[04/23/14 21:27:51.963 IST 14 8151] 0017.7c2f.b69a Received RSN IE with 0
 PMKIDsfrom mobile  0017.7c2f.b69a


[04/23/14 21:27:51.964 IST 1b 8151] 0017.7c2f.b69a Change state to AUTHCHECK
 (2) last state START (0)

[04/23/14 21:27:51.964 IST 1c 8151] 0017.7c2f.b69a Change state to 8021X_REQD
 (3) last state AUTHCHECK (2)


[04/23/14 21:27:51.964 IST 25 8151] 0017.7c2f.b69a apfProcessAssocReq
 (apf_80211.c:6272) Changing state for mobile  0017.7c2f.b69a  on AP
 1caa.076f.9e10  from Associated to Associated

[04/23/14 21:27:51.971 IST 26 8151] 0017.7c2f.b69a 1XA: Initiating
 authentication
[04/23/14 21:27:51.971 IST 27 8151] 0017.7c2f.b69a 1XA: Setting reauth
 timeout to 1800 seconds
[04/23/14 21:27:51.971 IST 28 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 0

[04/23/14 21:27:51.971 IST 29 8151] 0017.7c2f.b69a 1XA: Allocated uid 40
[04/23/14 21:27:51.971 IST 2a 8151] 0017.7c2f.b69a 1XA: Calling Auth Mgr
 to authenticate client 4975000000003e uid 40
[04/23/14 21:27:51.971 IST 2b 8151] 0017.7c2f.b69a 1XA: Session Start from
```

```
 wireless client

[04/23/14 21:27:51.971 IST 2c 8151] 0017.7c2f.b69a Session Manager Call Client
 4975000000003e, uid 40, capwap id 7ae8c000000013,Flag 0, Audit-Session ID
 0a6987b25357e2ff00000028, method list Microsoft_NPS, policy name (null)

[04/23/14 21:27:51.971 IST 2d 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca3] Session start request from Client[1] for 0017.7c2f.b69a
 (method: Dot1X, method list: Microsoft_NPS, aaa id: 0x00000028),  policy
[04/23/14 21:27:51.971 IST 2e 22] ACCESS-CORE-SM-CLIENT-SPI-NOTF:
 [0017.7c2f.b69a, Ca3]  - client iif_id: 4975000000003E, session ID:
 0a6987b25357e2ff00000028 for 0017.7c2f.b69a


[04/23/14 21:27:51.972 IST 43 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting !EAP_RESTART on Client 0x22000025
[04/23/14 21:27:51.972 IST 44 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:enter connecting state
[04/23/14 21:27:51.972 IST 45 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025: restart connecting
[04/23/14 21:27:51.972 IST 46 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting RX_REQ on Client 0x22000025
[04/23/14 21:27:51.972 IST 47 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025: authenticating state entered
[04/23/14 21:27:51.972 IST 48 284] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:connecting authenticating action
[04/23/14 21:27:51.972 IST 49 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting AUTH_START for 0x22000025
[04/23/14 21:27:51.972 IST 4a 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] 0x22000025:entering request state
[04/23/14 21:27:51.972 IST 4b 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending EAPOL packet
[04/23/14 21:27:51.972 IST 4c 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Platform changed src mac  of EAPOL packet
[04/23/14 21:27:51.972 IST 4d 291] ACCESS-METHOD-DOT1X-NOTF:
 [0017.7c2f.b69a, Ca3] Sending out EAPOL packet
[04/23/14 21:27:51.972 IST 4e 291] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] EAPOL packet sent to client 0x22000025


[04/23/14 21:27:52.112 IST 7d 211] Parsed CLID MAC Address = 0:23:124:47:182:154
[04/23/14 21:27:52.112 IST 7e 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:52.112 IST 7f 211] AAA SRV(00000000): Authen method=SERVER_GROUP
 Microsoft_NPS
[04/23/14 21:27:52.112 IST 80 211] AAA SRV(00000000): Selecting SG = DIAMETER
[04/23/14 21:27:52.113 IST 81 186] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Queuing an EAPOL pkt on Authenticator Q
[04/23/14 21:27:52.113 IST 82 291] ACCESS-METHOD-DOT1X-DEB:
 [0017.7c2f.b69a, Ca3] Posting EAPOL_EAP for 0x22000025
[04/23/14 21:27:52.278 IST 83 220] AAA SRV(00000000): protocol reply
 GET_CHALLENGE_RESPONSE for Authentication
[04/23/14 21:27:52.278 IST 84 220] AAA SRV(00000000): Return Authentication
 status=GET_CHALLENGE_RESPONSE
[04/23/14 21:27:52.278 IST 85 291] ACCESS-METHOD-DOT1X-DEB:[0017.7c2f.b69a,Ca3]
 Posting EAP_REQ for 0x22000025
```

Aquí está el resto del EAP hecho salir:

```
[04/23/14 21:27:54.690 IST 12b 211] AAA SRV(00000000): process authen req
[04/23/14 21:27:54.690 IST 12c 211] AAA SRV(00000000): Authen
 method=SERVER_GROUP Microsoft_NPS
[04/23/14 21:27:54.690 IST 12d 211] AAA SRV(00000000): Selecting SG =
 DIAMETER
[04/23/14 21:27:54.694 IST 12e 220] AAA SRV(00000000): protocol reply PASS
```

```
 for Authentication
[04/23/14 21:27:54.694 IST 12f 220] AAA SRV(00000000): Return Authentication
 status=PASS
[04/23/14 21:27:54.694 IST 130 189] ACCESS-METHOD-DOT1X-INFO:
 [0017.7c2f.b69a, Ca3] Received an EAP Success


[04/23/14 21:27:54.695 IST 186 8151] 0017.7c2f.b69a Starting key exchange with
 mobile - data forwarding is disabled
[04/23/14 21:27:54.695 IST 187 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
 to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.706 IST 188 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
 message (len 121) from mobile
[04/23/14 21:27:54.706 IST 189 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
 from mobile
[04/23/14 21:27:54.706 IST 18a 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
 PTK_START state (msg 2) from mobile
[04/23/14 21:27:54.706 IST 18b 8151] 0017.7c2f.b69a 1XK: Stopping retransmission
 timer
[04/23/14 21:27:54.706 IST 18c 8151] 0017.7c2f.b69a 1XA: Sending EAPOL message
 to mobile, WLAN=8 AP WLAN=8
[04/23/14 21:27:54.717 IST 18d 8151] 0017.7c2f.b69a 1XA: Received 802.11 EAPOL
 message (len 99) from mobile
[04/23/14 21:27:54.717 IST 18e 8151] 0017.7c2f.b69a 1XA: Received EAPOL-Key
 from mobile
[04/23/14 21:27:54.717 IST 18f 8151] 0017.7c2f.b69a 1XK: Received EAPOL-key in
 PTKINITNEGOTIATING state (msg 4) from mobile
[04/23/14 21:27:54.717 IST 190 8151] 0017.7c2f.b69a 1XK: Set Link Secure: 1

[04/23/14 21:27:54.717 IST 191 8151] 0017.7c2f.b69a 1XK: Key exchange complete
 - updating PEM
[04/23/14 21:27:54.717 IST 192 8151] 0017.7c2f.b69a apfMs1xStateInc
[04/23/14 21:27:54.717 IST 193 8151] 0017.7c2f.b69a Change state to
 L2AUTHCOMPLETE (4) last state 8021X_REQD (3)


[04/23/14 21:27:58.277 IST 1df 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:27:58.277 IST 1e0 269] DHCPD: Sending notification of DISCOVER:
[04/23/14 21:28:05.279 IST 1e1 269] DHCPD: Adding binding to hash tree
[04/23/14 21:28:05.279 IST 1e2 269] DHCPD: DHCPOFFER notify setup address
 20.20.20.5 mask 255.255.255.0


[04/23/14 21:28:05.306 IST 1f4 8151] 0017.7c2f.b69a Change state to RUN (20)
 last state DHCP_REQD (7)
```

¿Era este documento útil? Sí ningún

Gracias por su feedback.

Abra un caso de soporte (requiere un contrato de servicios con Cisco.)

Discusiones relacionadas de la comunidad del soporte de Cisco

La comunidad del soporte de Cisco es un foro para que usted haga y conteste a las preguntas, las sugerencias de la parte, y colabora con sus pares.

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre los convenios usados en este documento.

Actualizado: Mayo 05, 2014
ID del Documento: 117684