Guía de configuración atada con alambre de la versión 1.05 del dot1x

Contenido

Introducción

Este documento suministra una configuración de ejemplo para la versión 1.05 de dot1x cableado.

Esta guía cubre los Certificados creados con Microsoft CA y los Certificados del auto firms, que se soportan a partir del Access Control Server (ACS) 3.3. Usando un certificado del auto firms aerodinamiza la instalación inicial PEAP considerablemente puesto que no se requiere ningún externo CA. Ahora, el período predeterminado de la expiración del certificado del auto firms es solamente un año y no puede ser cambiado. Esto es bastante estándar cuando se trata de los certificados de servidor, pero puesto que el certificado autofirmado también actúa como certificado raíz CA, éste puede significar instalar el nuevo certificado en cada cliente, cada año al usar al solicitante de Microsoft (a menos que usted no selecciona “valida la opción del certificado de servidor”). Es recomienda que usted utiliza los Certificados de un auto firms solamente como medida temporal hasta que CA tradicional pueda ser utilizado. Si usted desea utilizar un certificado del auto firms, vea la sección.

el 802.1x fue diseñado para autenticar los host en una red alámbrica en vez de los usuarios reales. El intentar autenticar a los usuarios vía el 802.1x en una red alámbrica puede dar lugar al comportamiento no deseado tal como un usuario autenticado del 802.1x que no es terminado una sesión la red hasta que el indicador luminoso LED amarillo de la placa muestra gravedad menor NIC libere el puerto.

prerrequisitos

Requisitos

Antes de utilizar esta configuración, asegúrese de que cumple con estos requisitos:

- Switches que ejecuta el Software Release 12.1(12c)EA1 y Posterior de Cisco IOS® (E-I solamente) o CatOS 6.2 y posterior
- ACS 3.2
- Windows 2000 SP3 (con el hotfix), SP4, o XP SP1

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Instalación de los servicios de certificados de Microsoft

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: El Internet Information Server (IIS) debe ser instalado antes de que usted instale CA. Avoid que da al CA el mismo nombre que un servidor ACS; el hacer tan puede hacer a los clientes PEAP fallar la autenticación porque consiguen confusos cuando a certificado raíz CA se encuentra con el mismo nombre que el certificado de servidor. Este problema no es único a los clientes de Cisco.

Instale el servidor del certificado de Microsoft (CA)

Complete estos pasos:

1. Elija el **Start (Inicio)> Settings (Configuración) > Control panel (Panel de control)**.
2. Dentro del panel de control, abierto **agregue/quite los programas**.
3. En agregue/quite los programas, eligen **agregan/quitan a los componentes de Windows**.
4. Elija los **servicios de certificados**.
5. Haga clic en Next (Siguiente).
6. Haga clic **sí al** mensaje IIS.
7. Elija un independiente (o la empresa) raíz CA.
8. Haga clic en Next (Siguiente).
9. Nombre CA.**Nota:** El resto de cuadros son opcionales.**Nota:** Avoid que da al CA el mismo nombre que el servidor ACS. Esto puede hacer a los clientes PEAP fallar la autenticación porque hacen confusos cuando a certificado raíz CA se encuentra con el mismo nombre que el certificado de servidor. Este problema no es único a los clientes de Cisco. Por supuesto, si usted no planea en usar el PEAP, esto no se aplica.
10. Haga clic en Next (Siguiente).
11. El valor por defecto de la base de datos está correcto.
12. Haga clic en Next (Siguiente).El IIS debe ser instalado antes de que usted instale CA.

ACS para la configuración del certificado de Windows

Cree un certificado de servidor

Complete estos pasos:

1. De su servidor ACS, hojee a CA (http://IP_of_CA_server/certsrv/).
2. Marque la **petición un** cuadro del **certificado**.
3. Haga clic en Next (Siguiente).
4. Elija el **pedido avanzado**.
5. Haga clic en Next (Siguiente).
6. Elija **presentan un pedido de certificado a este CA usando una forma**.
7. Haga clic en Next (Siguiente).
8. Teclee un nombre en el cuadro del nombre (CN).
9. Para el propósito previsto, elija el **Certificado de autenticación de servidor**.**Nota:** Si usted está utilizando la empresa CA, elija al **servidor Web de la** primera lista desplegable.
10. Elija éstos bajo opción dominante para crear una nueva plantilla:**CSP — V1.0 del Proveedor criptográfico de la base de MicrosoftTamaño de clave — 1024Nota:** Los Certificados creados con un tamaño de clave mayor de 1024 pueden trabajar para el HTTPS pero no trabajarán para el PEAP.**Nota:** La empresa CA de Windows 2003 permite los tamaños de clave mayores de 1024, pero usar un dominante más en gran parte de

1024 no trabaja con el PEAP. La autenticación pudo aparecer pasar en el ACS, pero el cliente apenas colgará mientras que intenta la autenticación.**Claves como exportablesNota:** Microsoft ha cambiado la plantilla del servidor Web con la versión de la empresa CA de Windows 2003. Con este cambio de la plantilla, las claves son no más exportables, y la opción es greyed hacia fuera. No hay otros Certificate Template plantilla de certificado suministrados los servicios de certificados que están para la autenticación de servidor, o que dan la capacidad de marcar las claves como exportables en el menú desplegable. Para crear una nueva plantilla que lo hace así pues, ver el crear una nueva sección del Certificate Template plantilla de certificado.**Utilice el almacenamiento de máquina localNota:** El resto de las opciones se deben dejar como valor por defecto.
11. Haga clic en Submit (Enviar).
12. Usted debe conseguir este mensaje: Se ha recibido su pedido de certificado.

Cree un nuevo Certificate Template plantilla de certificado

Complete estos pasos:

1. Elija el **Start (Inicio) > Run (Ejecutar) > el certmpl.msc.**
2. Haga clic con el botón derecho del ratón la **plantilla del servidor Web**.
3. Elija la **plantilla duplicado**.
4. Dé a plantilla un nombre, tal como ACS.
5. Haga clic la lengueta de la **dirección de petición**.
6. Elija **permiten que la clave privada sea exportada**.
7. Haga clic el botón **CSP**.
8. Elija el **v1.0 del Proveedor criptográfico de la base de Microsoft**.
9. Haga clic en OK.**Nota:** Todas las otras opciones se deben dejar como valor por defecto.
10. Haga clic en Apply (Aplicar).
11. Haga clic en OK.
12. Abra CA MMC broche-en.
13. Haga clic con el botón derecho del ratón los **Certificate Template plantilla de certificado**.
14. Elija **nuevo > Certificate Template plantilla de certificado a publicar**.
15. Elija la nueva plantilla que usted creó.
16. Haga clic en OK.
17. Recomience CA.La nueva plantilla se incluye en la lista desplegable del Certificate Template plantilla de certificado.

Apruebe el certificado de CA

Complete estos pasos:

1. Elija el **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > el Certificate Authority**.
2. En el cristal izquierdo, amplíe el certificado.
3. Elija **hasta que finalicen las peticiones**.
4. Haga clic con el botón derecho del ratón en el certificado.
5. Elija **todas las tareas**.
6. Elija el **problema**.

Descargue el certificado de servidor al servidor ACS

Complete estos pasos:

1. De su servidor ACS, hojee a CA (http://IP_of_CA_server/certsrv/).
2. Elija el **control en un certificado pendiente**.
3. Haga clic en Next (Siguiente).
4. Seleccione el certificado.
5. Haga clic en Next (Siguiente).
6. El tecleo **instala**.

Instale el certificado de CA en el servidor ACS

Nota: Estos pasos no se requieren si el ACS y CA están instalados en el mismo servidor.

1. Complete estos pasos:

2. De su servidor ACS, hojee a CA (http://IP_of_CA_server/certsrv/).
3. Elija **extraen el certificado de CA o el Lista de revocación de certificados (CRL)**.
4. Haga clic en Next (Siguiente).
5. Elija el **base 64 codificado**.
6. Haga clic el **certificado de CA de la descarga**.
7. Haga clic **abierto**.
8. El tecleo **instala el certificado**.
9. Haga clic en Next (Siguiente).
10. Elija el **lugar todos los Certificados en el almacén siguiente**.
11. El tecleo **hojea**.
12. Marque el cuadro de los **almacenes del show physical**.
13. En el cristal izquierdo, amplíe los **Trusted Root Certification Authority**.
14. Elija la **computadora local**.
15. Haga clic en OK.
16. Haga clic en Next (Siguiente).
17. Haga clic en Finish (Finalizar).
18. El Haga Click en OK en la importación era cuadro acertado.

Configuración ACS para utilizar el certificado de servidor

Complete estos pasos:

1. En el servidor ACS, elija la **configuración del sistema**.
2. Elija la **configuración del certificado ACS**.
3. Elija **instalan el certificado ACS**.
4. Elija el **certificado del uso del almacenamiento**.
5. Teclee adentro el nombre CN (el mismo nombre que fue utilizado en el paso 8 del crear una sección del certificado de servidor).
6. Haga clic en Submit (Enviar).
7. En el servidor ACS, **configuración del sistema del** tecleo.
8. Elija la **configuración del certificado ACS**.

9. Elija **editan Certificate Trust List (Lista de confianza del certificado)**.
10. Marque el cuadro para CA.
11. Haga clic en Submit (Enviar).

Configuración del certificado del dispositivo ACS

Cree y instale un certificado autofirmado

Nota: Esta sección se aplica solamente si usted no está utilizando CA externo.

Complete estos pasos:

1. En el servidor ACS, haga clic la **configuración del sistema**.
2. Haga clic la **configuración del certificado ACS**.
3. El tecleo **genera el certificado autofirmado**.
4. Teclee el tema del certificado en el de la forma. En este ejemplo, se utiliza cn=ACS33. Para más opciones de configuración del certificado autofirmado, refiera a la configuración del sistema: Autenticación y certificados.
5. Teclee la ruta completa y el nombre del certificado que se creará en el cuadro del archivo de certificado. Por ejemplo, `c:\acscerts\acs33.cer`.
6. Teclee la ruta completa y el nombre del archivo de clave privado que se creará en el cuadro del archivo de clave privado. Por ejemplo, `c:\acscerts\acs33.pvk`.
7. Ingrese y confirme la contraseña de la clave privada.
8. Elija **1024 de la** lista desplegable de la longitud de clave.**Nota:** Mientras que el ACS puede generar los tamaños de clave mayores de 1024, usando un dominante más en gran parte de 1024 no trabaja con el PEAP. La autenticación pudo aparecer pasar en el ACS, pero el cliente cuelga mientras que intenta la autenticación.
9. De la publicación a firmar con la lista, elija la publicación del hash que se utilizará para cifrar la clave. En este ejemplo, la publicación a firmar con en el SHA1 se utiliza.
10. **Certificado generado Install del** control.
11. Haga clic en Submit (Enviar).

Cree un certificado de servidor usando el CSR

Complete estos pasos:

1. De su servidor FTP, hojee a CA (http://IP_of_CA_server/certsrv/).
2. Elija la **petición un certificado**.
3. Haga clic en Next (Siguiente).
4. Elija el **pedido avanzado**.
5. Haga clic en Next (Siguiente).
6. Elija **presentan un pedido de certificado usando PKCS-10 un archivo codificado base64 o un pedido de renovación usando PKCS-7 un archivo codificado base64**.
7. Pegue la salida del paso 6 en el campo **codificado base64 del pedido de certificado**.
8. Haga clic en Submit (Enviar).
9. **Certificado de CA de la descarga del** tecleo.
10. Haga clic en Save (Guardar).

11. Nombre el certificado.
12. Salve el certificado a su directorio FTP

Descargue el certificado de CA al servidor FTP

Complete estos pasos:

1. De su servidor FTP, hojee a CA (http://IP_of_CA_server/certsrv/).
2. Elija **extraen el certificado de CA o el Lista de revocación de certificados (CRL)**.
3. Haga clic en Next (Siguiente).
4. Elija el **base 64 codificado**.
5. Haga clic el **certificado de CA de la descarga**.
6. Haga clic en Save (Guardar).
7. Nombre el certificado.
8. Salve el certificado a su directorio FTP

Instale el certificado de CA en el dispositivo

Complete estos pasos:

1. Elija la **configuración del sistema > el certificado ACS puestos > configuración de las autoridades de certificación ACS**.
2. Haga clic el **archivo del certificado de CA de la descarga**.
3. En el campo del servidor FTP, ingrese el IP Address o el nombre de host del servidor FTP
4. En el campo del login, ingrese un nombre de usuario válido que el Cisco Secure ACS pueda utilizar para acceder al servidor FTP.
5. Iin el campo de contraseña, ingresa la contraseña de usuario.
6. En el campo alejado del directorio FTP, ingrese la ruta relativo del directorio raíz del servidor FTP al directorio que contiene el archivo del certificado de CA.
7. En el campo de nombre del archivo alejado FTP, ingrese el nombre del archivo del certificado de CA.
8. Haga clic en Submit (Enviar).
9. Verifique el nombre de fichero en el campo.
10. Haga clic en Submit (Enviar).
11. Elija la **configuración del sistema > el control de servicio** para recomenzar los servicios ACS.

Configure las configuraciones de la autenticación global

Complete estos pasos:

1. En el servidor ACS, haga clic la **configuración del sistema**.
2. Haga clic la **configuración de la autenticación global**.

Complete estos pasos para el v3.2 ACS y posterior:

1. Marque el **EAP MSCHAPv2 de la permit si usa el** cuadro de **Microsoft PEAP**.
2. Marque la **permit EAP-GTC si usa el** cuadro de **Cisco PEAP**.
3. Marque la **versión MS-CHAP de la permit 1** cuadro de la **autenticación**.

4. Marque el cuadro de la **autenticación de la versión MS-CHAP 2 de la permit**.
5. Haga clic en Submit (Enviar).

Complete estos pasos para ACS v3.1 y posterior:

1. Marque el cuadro de la **permit PEAP**.
2. Marque la **versión MS-CHAP de la permit 1** cuadro de la **autenticación**.
3. Marque el cuadro de la **autenticación de la versión MS-CHAP 2 de la permit**.
4. Haga clic en Submit (Enviar).

Configure el ACS para permitir la autenticación de la máquina

Complete estos pasos:

1. Elija las **Bases de datos de usuarios externas > la configuración de la base de datos**.
2. Haga clic en base de datos de Windows.
3. Haga clic en Configure (Configurar).
4. Marque el cuadro de la **autenticación de la máquina PEAP del permiso**.
5. Haga clic en Submit (Enviar).

Configure el AP en el ACS

Complete estos pasos para configurar el AP en el ACS:

1. En el servidor ACS, haga clic la **configuración de red** a la izquierda.
2. Para agregar a un cliente AAA, el tecleo **agrega la entrada**.
3. Ingrese estos valores en los rectángulos:Dirección IP del cliente AAA — IP_of_your_APClave — Componga un dominante (aseegurese la clave hace juego la clave secreta compartida AP)Autentique usando — RADIUS (Cisco Aironet)
4. Haga clic en Submit (Enviar).
5. Reinicio.

Configure el Switch para el dot1x

Refiera a estos documentos para la configuración del dot1x:

- Catalyst 2950
- Catalyst 3550
- Catalyst 4500
- Catalyst 6500

Configuración de los temporizadores del dot1x

Complete estos pasos para configurar los temporizadores del dot1x como el RADIUS A/V empareja:

- Configure el atributo de RADIUS del Sesión-descanso (atributo [27]) que especifica el tiempo después de lo cual ocurre el reauthentication.
- Configure el atributo de RADIUS de la Terminación-acción (atributo [29]) que especifica Paso

a seguir durante el reauthentication. Cuando el valor de atributo se fija para omitir, la sesión del IEEE 802.1X termina, y la Conectividad se pierde durante el reauthentication. Cuando el valor de atributo se fija al pedido de RADIUS, la sesión no es afectada durante el reauthentication.

Nota: Los valores para los atributos 27 y 29 se pueden asignar en un para cada grupo, bajo sección RADIUS (IETF). Fije el atributo 27 al período del reauthentication, y 29 al pedido de RADIUS.

En el Switch, realice esta configuración para que el Switch valide los valores de los atributos de RADIUS del servidor de RADIUS:

```
(config-if)#dot1x reauthentication (config-if)#dot1x timeout reauth-period server
```

Configure al cliente para el PEAP con la autenticación de la máquina

Unirse al dominio

Complete estos pasos:

Nota: Para completar este paso, el ordenador debe tener una de estas conexiones a CA:

- conexión alámbrica
- conexión de red inalámbrica con la Seguridad del 802.1x inhabilitada

1. Login a Windows XP con una cuenta que tiene privilegios de administrador.
2. Click derecho en el **mi PC**.
3. Elija las **propiedades**.
4. Haga clic la lengueta del **nombre de computadora**.
5. Haga clic el **cambio**.
6. En el campo de nombre de la computadora, ingrese el nombre de host.
7. Elija el **dominio**.
8. Ingrese el nombre del dominio.
9. Haga clic en OK.
10. Se visualiza un diálogo del login. Inicie sesión con una cuenta que tenga permiso para unirse al dominio.
11. Una vez que el ordenador se ha unido a con éxito el dominio, recomience el ordenador. La máquina siente bien al miembro del dominio, tiene un certificado para CA instalado, y una contraseña para la autenticación de la máquina se genera automáticamente.

Si el cliente se unió al dominio antes de la instalación de CA, o el certificado de CA no fue instalado en el cliente, completa estos pasos:

Nota: La necesidad de esto es indicada por las fallas de autenticación a menudo (pero no siempre) con los errores tales como `autenticación fallada durante el contacto SSL`.

1. De su servidor ACS, hojee a CA (http://IP_of_CA_server/certsrv/).
2. Elija **extraen el certificado de CA o el Lista de revocación de certificados (CRL)**.
3. Haga clic en Next (Siguiente).
4. Elija el **base 64 codificado**.
5. Haga clic el **certificado de CA de la descarga**.
6. Haga clic **abierto**.

7. El tecleo **instala el certificado**.
8. Haga clic en Next (Siguiente).
9. Elija el **lugar todos los Certificados en el almacén siguiente**.
10. El tecleo **hojea**.
11. Marque el cuadro de los **almacenes del show physical**.
12. En el cristal izquierdo, amplíe el certificado.
13. Elija la **computadora local**.
14. Haga clic en OK.
15. Haga clic en Next (Siguiente).
16. Haga clic en Finish (Finalizar).
17. El Haga Click en OK en la importación era cuadro acertado.

Configuración XP SP1 para el PEAP con la autenticación de la máquina

Complete estos pasos:

1. Elija el **Start (Inicio) > Control Panel (Panel de control) > Network Connections (Conexiones de red)**.
2. Elija las **propiedades**.
3. Haga clic la lengueta de la **autenticación**.
4. Marque el cuadro del **IEEE 802.1X del permiso…**.
5. Para el tipo EAP, elija el **EAP protegido**.
6. Haga clic en Properties (Propiedades).
7. Marque la **autenticidad como ordenador….** cuadro.
8. Elija las **propiedades**.
9. Marque el cuadro para CA
10. Haga clic en OK.
11. Haga clic en OK.

Windows 2000 de la configuración para la autenticación de la máquina PEAP

Complete estos pasos:

1. Si usted está ejecutando el SP3, descargue y instale el hotfix del 802.1x: http://support.microsoft.com/default.aspx?kbid=313664 . Esto no se requiere para el SP4.
2. Elija el **Start (Inicio) > Configuration (Configuración) > Control Panel (Panel de control) > Network and dial-up connections (Conexiones de red y marcado manual)**.
3. Haga clic con el botón derecho del ratón la conexión de red.
4. Elija las **propiedades**.
5. Haga clic la lengueta de la **autenticación**.
6. Elija el **Control de acceso a la red del permiso usando el IEEE 802.1X**.
7. Elija **EAP protegido (PEAP) de la** lista desplegable del tipo EAP.
8. Marque la **autenticidad como** cuadro del **ordenador…**.
9. Elija las **propiedades**.
10. Marque el cuadro para CA
11. Haga clic en OK.
12. Haga clic en OK.

Nota: Si no hay lengueta de la **autenticación**, el servicio del 802.1x está instalado en un estado

inhabilitado. Para solucionar esto, usted debe habilitar el servicio de **configuración de red inalámbrica** en la lista de servicios.

Nota: Si la lengueta de la **autenticación** está presente, pero es inasequible, ésta indica que el driver del adaptador de red no soporta el 802.1x correctamente. Marque la página del hotfix del 802.1x o el sitio web del vendedor para los drivers soportados.

1. Complete estos pasos para habilitar la configuración de red inalámbrica:

2. Haga clic con el botón derecho del ratón el **mi PC**.
3. El tecleo **maneja**.
4. **Servicios y aplicaciones del** tecleo.
5. Haga clic en **Services**.
6. Fije el valor de lanzamiento para el servicio a automático.
7. Inicie el servicio.

Asignación del VLAN dinámico para el 802.1x y el ACS

Esta opción se soporta en IOS 12.1(12c)EA1 (E-I solamente) o 12.1(14)EA1 o CatOS 7.2 y posterior

Nota: el 802.1x fue diseñado para autenticar los host en una red alámbrica en vez de los usuarios reales. El intentar autenticar a los usuarios vía el 802.1x en una red alámbrica puede dar lugar al comportamiento no deseado tal como la asignación del VLAN dinámico asignada a un usuario que no es cambiado hasta que el indicador luminoso LED amarillo de la placa muestra gravedad menor NIC libere el puerto (se recomienza o powercycled el ordenador).

Complete estos pasos:

1. Elija la **configuración de la interfaz > RADIUS (IETF)**.
2. Marque el **Tipo de Túnel [064] para el usuario/la casilla de grupo**.
3. Marque el Túnel-Media-**tipo [065] para el usuario/la casilla de grupo**.
4. Marque el **[081] Túnel-Soldado-Grupo-ID para el usuario/la casilla de grupo**.
5. Haga clic en Submit (Enviar).
6. Elija el **usuario/la configuración de grupo**.
7. Marque el cuadro de **Tipo de Túnel [064]**.
8. Elija **1 de la** lista desplegable de la etiqueta.
9. Elija el **VLA N** para la lista desplegable de valores.
10. Elija **0** para todas las listas desplegables subsiguientes de la etiqueta.
11. Marque el cuadro del Túnel-Media-**tipo [065]**.
12. Elija **1 de la** lista desplegable de la etiqueta.
13. Elija **802 de la** lista desplegable de valores.
14. Elija **0** para todas las listas desplegables subsiguientes de la etiqueta.
15. Marque el cuadro **[081] Túnel-Soldado-Grupo-ID**.
16. Elija **1 de la** lista desplegable de la etiqueta.
17. Utilice el nombre del VLA N que necesita ser avanzado. Puede ser el nombre predeterminado y es encontrado publicando el **comando show vlan**.
18. Elija **0** para todas las listas desplegables subsiguientes de la etiqueta.
19. Haga clic en Submit (Enviar).

Verificación

No podido crear el mensaje de error del objeto del “CertificateAuthority.Request”

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

Complete estos pasos:

1. Elija el **Start (Inicio) > Administrative Tools (Herramientas administrativas) > el IIS**.
2. Elija los **sitios web > el Sitio Web predeterminado**.
3. Haga clic con el botón derecho del ratón **CertSrv**.
4. Elija las **propiedades**.
5. Haga clic el **botón de la configuración** en la sección de las configuraciones de aplicaciones de la lengueta del **directorio virtual**.
6. Haga clic la lengueta de las **opciones**.
7. Elija al **estado de la sesión del permiso**.**Nota:** Todas las otras opciones se deben dejar como valor por defecto.
8. Haga clic en OK.
9. Haga clic en OK.
10. Reinicio IIS.

Si su navegador bloquea con un ActiveX que descarga de mensaje de control, refiera a este artículo sobre el sitio Web de Microsoft: El Internet Explorer para el responder en “el mensaje del control ActiveX de la transferencia” cuando usted intenta utilizar a un servidor de certificados .

Troubleshooting

Problema

El Switch no puede entrar en contacto al servidor ACS secundario cuando el servidor ACS primario va abajo en la autenticación del dot1x; este error ocurre: `“Sesión de Authen medida el tiempo hacia fuera: Desafío no proporcionado por el cliente.”`

Solución

Este error ocurre cuando el temporizador de emergencia no se configura en el Switch, que hace el Switch continuar intentando al servidor primario que está abajo. Esto hace la autenticación fallar. Para resolver este problema, configure el temporizador de emergencia en el Switch de modo que el Switch entre en contacto al servidor ACS secundario después de que espere el tiempo configurado (en los segundos) o el número de recomprobaciones para alcanzar al servidor primario antes del considera al servidor primario ser declarado absolutamente o inasequible. Ahora la autenticación tiene éxito con el servidor secundario, que es activo. El tiempo muerto se puede configurar con este comando: [time seconds [tries number] de los muerto-criterios del radio-servidor | número de los intentos en el modo de configuración global.

Información Relacionada

- Cisco Secure Access Control Server para Unix

- Cisco Secure Access Control Server para Windows
- Guía de configuración Identificar-basada de los sistemas de interconexión de redes
- Soporte Técnico y Documentación - Cisco Systems