Configuración de Funk RADIUS para Autenticar Clientes Inalámbricos de Cisco con LEAP

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Convenciones Configuración Configuración del punto de acceso o puente Configuración del producto Funk Software, Inc., Steel-Belted Radius Creación de usuarios en radios con correa de acero Información Relacionada

Introducción

Este documento describe cómo configurar los puntos de acceso 340 y 350 Series y los bridges 350 Series. También describe cómo el <u>producto Funk Software, Inc.</u>, Steel-Belted Radius, funciona junto con Light Extensible Authentication Protocol (LEAP) para autenticar un cliente inalámbrico de Cisco.

Nota: Las partes de este documento que se refieren a productos ajenos a Cisco se escribieron en base a la experiencia que el autor tuvo con ese producto ajeno a Cisco, no en formación formal. Están pensados para la comodidad de los clientes de Cisco, no como soporte técnico. Para obtener asistencia técnica autorizada sobre productos ajenos a Cisco, póngase en contacto con el servicio de asistencia técnica del producto del proveedor.

Prerequisites

Requirements

La información presentada en este documento supone que el producto Funk Software, Inc., Steel-Belted Radius, se instala y funciona correctamente. También supone que está obteniendo acceso administrativo al punto de acceso o al puente a través de la interfaz del navegador.

Componentes Utilizados

La información de este documento se basa en los puntos de acceso Cisco Aironet serie 340 y 350 y en los puentes serie 350. La información de este documento se aplica a todas las versiones de firmware 12.01T y posteriores de VxWorks.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Configuración

Configuración del punto de acceso o puente

Complete estos pasos para configurar el punto de acceso o el puente.

 En la página Summary Status (Estado de resumen), siga estos pasos:Haga clic en Setup (Configuración).Haga clic en Seguridad.Haga clic en Radio Data Encryption (WEP) (Cifrado de datos de Radio (WEP)).Introduzca una clave WEP aleatoria (26 caracteres hexadecimales) en la ranura WEP Key 1 (Clave WEP 1).Establezca el tamaño de la clave en 128 bits.Haga clic en Apply (Aplicar).

BR350-CLEAR	Root Radio	Data Encry	ption [ISCO SYSTEMS	
Cisco 350 Series Bridg	e 12.03T				
<u>Map</u> <u>Help</u>				Uptime: 01:45:05	
If VLANs are not en	abled, set Radio Data	a Encryption on this	page. If VLAN	s are enabled, Radio	
Data Encryption is set	t independently for ea	ach enabled VLAN	through <u>VLAN</u>	Setup.	
Use of Data Encryptic Must se	on by Stations is: at an Encryption Ke	Not Availab y or enable Broadd	le ast Key Rotatio	on first	
		Open	Shared	Network-EAP	
Accept Authentication	n Type:	v			
Require EAP:					
	Transmit		**	77 61	
NUTED IZ 1	With Key	Encryption	n Key	Key Size	
WEP Key I:	-			128 bit 👻	
WEP Key 2:	-			not set 💌	
WEP Key 3:	-			not set 💌	
WEP Key 4:	-			not set 💌	
Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F). Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F). This radio supports Encryption for all Data Rates.					
		Apply OK	Cancel	Restore Defaults	
[Map][[ogin][Help]					
Cisco 350 Series Bridge 12.03	r © Copyright	2002 Cisco Systems, Inc.		credits	

Click OK.Cambie la opción **El uso del cifrado de datos por estaciones es:** a **Cifrado completo**.Active las casillas **Open** y **Network EAP** en la línea **Aceptar Tipo de Autenticación**.

BR350-to-Radius	Root R	adio Data	a Encryption	CISCO SYSTEMS		
Cisco 350 Series Bridge	12.03T					
Map Help				2003/07/10 09:30:53		
If VLANs are <i>not</i> enal	oled, set Radio	Data Encrypti	on on this page. If VL	ANs <i>are</i> enabled, Radio		
Data Encryption is set i	independently f	for each enable	d VLAN through <u>VL</u>	AN Setup.		
Use of Data Encryption	n by Stations is	Full Encrypt	ion 👻			
		,	_			
	-	Open	Shared	Network-EAP		
Accept Authentication	Туре:		H			
Require LAFE.						
	Fransmit					
	With Key	H	Incryption Key	Key Size		
WEP Key 1:	۲			128 bit 💌		
WEP Key 2:	-			not set 💌		
WEP Key 3:	-			not set -		
WEP Key 4:	-			not set 💌		
Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F). Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F). This radio supports Encryption for all Data Rates.						
		Apply	OK Cancel	Restore Defaults		
		[Map][Login	[Help]			
Cisco 350 Series Bridge 12.03 T	⊕ Co	pyright 2002 Cisco S	stems, Inc.	<u>credits</u>		

Click OK.

2. En la página Security Setup (Configuración de seguridad), haga clic en Authentication Server y realice estas entradas en la página:Nombre de servidor/IP: Introduzca la dirección IP o el nombre de host del servidor RADIUS.secreto compartido: Introduzca la cadena exacta como la del servidor RADIUS para este punto de acceso o puente.En el servidor Use para: para este servidor RADIUS, marque la casilla de verificación EAP Authentication.

BR350-to-Radius	Authentica	tor Co	onfiguration		Cisco	SYSTEMS
Cisco 350 Series Bridge	12.03T					
Map Help					2003/07/10 09:45	11
802.1X Protocol Vers	sion (for EAP Authe	entication):	802.1x-2001 💌			
Primary Server Reatte	mpt Period (Min.):		0			
Server Name/IP	Server Type	Port	Shared Secret	Retra	n Int (sec)	Retran
172.30.1.124	RADIUS -	1812	*****	5		3
Use server for: 🔽 EA	AP Authentication	MAC A	ddress Authentication	User Authentication	MIP Authenticat	ion
		1010		_		
The summer for DEF	RADIUS -	1812	danas Authentiation	D Harr Authoritation		3
Use server for.	SF Authentication	MACA	daress Admendication	U Oser Authentication	L MIF Authentical	ion
	RADIUS -	1812	*****	5		3
Use server for: 🔽 EA	AP Authentication	MAC A	ddress Authentication	User Authentication	MIP Authenticat	ion
	DADILIC	1010		-		6
Use server for JE	P Authentication	MAC A	ddress Authentication	D User Authentication	MIP Authenticat	ion
	in rioanenae anon	_ mino n	datess realization			
Note: For each aut	hentication function,	, the most	recently used server is	s shown in green text.		
				Apply OK	Cancel Restor	e Defaults
			MaplLoginlHelp]			
Cisco 350 Series Bridge 12.03T		© Copyright	2002 Cisco Systems, Inc.			credits

3. Cuando haya configurado los parámetros en el Paso 2, haga clic en **Aceptar**.Con esta configuración, el punto de acceso o el puente está listo para autenticar los clientes LEAP contra un servidor RADIUS.

Configuración del producto Funk Software, Inc., Steel-Belted Radius

Complete los pasos del siguiente procedimiento para configurar el producto Funk Software, Inc., Steel-Belted Radius, para comunicarse con el punto de acceso o puente. Para obtener información más completa sobre el servidor, consulte <u>Funk Software</u>.

Nota: Las partes de este documento que se refieren a productos ajenos a Cisco se escribieron en base a la experiencia que el autor tuvo con ese producto ajeno a Cisco, no en formación formal. Están pensados para la comodidad de los clientes de Cisco, no como soporte técnico. Para obtener asistencia técnica autorizada sobre productos ajenos a Cisco, póngase en contacto con el servicio de asistencia técnica del producto del proveedor.

1. En el menú Clientes RAS, haga clic en Agregar para crear un nuevo cliente

		<u> </u>	<u></u>		
	Add New RAS Client				
	Client name:				_
		🔲 Any RAS	client		
		0K.	Cancel		
RAS.					

2. Configure los parámetros para el nombre del cliente, la dirección IP y la marca/modelo.Nombre del cliente: Introduzca el nombre del punto de acceso o puente.IP Address: Introduzca la dirección del punto de acceso o el puente que se comunica con el radio de cinturón de acero.Nota: El servidor RADIUS ve el punto de acceso o el puente como un cliente RADIUS.Marca/modelo: Seleccione Punto de acceso Cisco Aironet.

Steel-Belted Ra	ndius Enterprise E	dition (CISCO-FHA0VD6BF)	
File Help			
C Servers	Client name:	CISCO AP	Add
RAS Clients	IP address:	172.30.1.103	Remove
C Users	Make/model:	Cisco Aironet Access Point	
C Profiles			
C Proxy		Vendor Info	
C Tunnels		Edit authentication shared secret	
C IP Pools		Use different shared secret for accounting	
O IPX Pools		Edit accounting shared secret	
C Access		Accurac dours if no keep slive	
C Configuration		packets after (seconds):	
C Statistics			
	IP address pool:	<none></none>	
			Save
			Reset

3. Haga clic en Editar secreto compartido de

En	ter shared secre	t		×
1	Enter shared secret:			
I	Unmask shared :	secret		
	Set	Validate	Cancel	
icación				

Introduzca la cadena

exacta como la del punto de acceso o puente para este servidor.Haga clic en **Establecer** para volver al cuadro de diálogo anterior.Click **Save**.

- Busque el archivo EAP.INI que se encuentra en la carpeta de instalación de Steel-Belted Radius (en un PC con Windows, este archivo se encuentra normalmente en C:\Radius\Services).
- 5. Verifique que LEAP sea una opción para EAP-Type.Un archivo de ejemplo tiene un aspecto similar al siguiente: [Native-User]

EAP-Only = 0

First-Handle-Via-Auto-EAP = 0
EAP-Type = LEAP, TTLS

- 6. Guarde el archivo EAP.INI modificado.
- 7. Detenga y reinicie el servicio RADIUS.

Creación de usuarios en radios con correa de acero

Esta sección describe cómo crear un nuevo usuario nativo (local) con el producto Funk Software, Inc., Steel-Belted Radius. Si es necesario agregar un usuario de dominio o grupo de trabajo, comuníquese con <u>Funk Software</u> para obtener ayuda. Las entradas de usuario nativas requieren que el nombre y la contraseña del usuario se introduzcan en la base de datos local de Steel-Belted Radius. Para todos los demás tipos de entradas de usuario, Steel-Belted Radius se basa en otra base de datos para validar las credenciales de un usuario.

🥝 Steel-Belt	ed Radius Enterprise Edition (CISCO-FHA0VD6BF)	
File Help		
C Servers	User name: TEST	Add
O RAS Clien	ts User type: Native User Set password	Remove
O Users		
C Profiles	Check list attributes Return list attributes	
O Proxy		
C Tunnels		~
C IP Pools		
C IPX Pools		
C Access		
C Configurat	ion	
C Statistics	Ins Edit Del	
	Maximum concurrent connections:	Save
	Profile name: <pre></pre>	Reset

Complete estos pasos para configurar un usuario nativo en el RADIUS con cinturón de acero:

1. En el menú Users (Usuarios), haga clic en Add para crear un nuevo

Add New User				X
Native	Domain	SecurID]	
Enter user na	me:			
	OK		Cancel	

usuario.

- 2. Haga clic en la ficha **Native**, introduzca el nombre de usuario en el campo y haga clic en **OK**.Se cierra el cuadro de diálogo Agregar nuevo usuario.
- 3. En el cuadro de diálogo Usuarios, seleccione el usuario y haga clic en Establecer

Enter User Password	×
Enter password:	
 Allow PAP or CHAP Allow PAP only (encrypt password in database)
Set Validate Cancel	

contraseña.

- 4. Introduzca la contraseña para el usuario y haga clic en Establecer.
- 5. En el cuadro de diálogo Usuarios, haga clic en Guardar y haya creado el usuario.

Información Relacionada

- <u>Configuración de seguridad</u>
- Software Funk
- LAN inalámbrica (WLAN)
- <u>Soporte Técnico Cisco Systems</u>

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).