Ejemplo de Configuración de Autenticación por Cable 802.1x en un Switch Catalyst Serie 3550 y ACS Versión 4.2

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Ejemplo de configuración del switch Configuración de ACS Verificación Troubleshoot

Introducción

Este documento proporciona un ejemplo de configuración básica de IEEE 802.1x con Cisco Access Control Server (ACS) versión 4.2 y el protocolo de servicio de usuario de acceso telefónico de acceso remoto (RADIUS) para la autenticación por cable.

Prerequisites

Requirements

Cisco recomienda que:

- Confirme la disponibilidad de IP entre ACS y el switch.
- Asegúrese de que los puertos de protocolo de datagramas de usuario (UDP) 1645 y 1646 estén abiertos entre ACS y el switch.

Componentes Utilizados

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

Cisco Catalyst 3550 Series Switches

Cisco Secure ACS versión 4.2

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). If your network is live, make sure that you understand the potential impact of any command.

Configurar

Ejemplo de configuración del switch

1. Para definir el servidor RADIUS y la clave previamente compartida, ingrese este comando:

Switch(config)# radius-server host 192.168.1.3 key cisco123

2. Para habilitar la funcionalidad 802.1x, ingrese este comando:

Switch(config)# dot1x system-auth-control

 Para habilitar globalmente la autenticación, autorización y administración de cuentas (AAA) y la autenticación y autorización RADIUS, ingrese estos comandos: Nota: Esto es necesario si necesita pasar atributos desde el servidor RADIUS; de lo contrario, puede omitirlo.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
awitch(Config)# aaa authorization network default group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config-if)# switchport mode acces
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
Switch(config-if)# dot1x timeout quiet-period
Switch(config-if)# dot1x timeout tx-period
```

Configuración de ACS

 Para agregar el switch como un cliente AAA en ACS, navegue hasta Configuración de red > Agregar cliente AAA de entrada, e ingrese esta información: Dirección IP: </P>Secreto compartido:
 Clave>Autenticar mediante: Radius (Cisco IOS[®]/PIX 6.0)

cisco	Network Configuration		•
	AAA Client Hostname	switch	octet in the IP address. For example, if you used access the direct in the IP address. For example, if you
Uper Setap	AAA Client IP Address	192.168.1.2	C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.
SharedDroffle Components	FOR GREAT PROFESS	d	You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.12
Network Configuration	Shared Secret	and 152.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.	
Cardige stion	RADIUS Key Wrap	(Beck to Top)	
Configuration	Key Encryption Key		Shared Secret
Administration Castrol	Message Authenticator Code Key Key Input Format	ASCII Hexadecimal	The Shared Secret is used to encrypt TACACS+ or the RADIUS AAA client and ACS. The shared secret must be configured in the AAA client and ACS identically, including case secret/bits.
J Databases			(Back to Top)
Validation	Authenticate Using RADIUS (Cisco 105/PIX 6.0) •		Network Device Group
Profiles	Single Connect TACACS+ AAA	From the list, dick the name of the Network Device Group (NDG) to which this AAA client belongs.	
Activity	Log Update/Watchdog Packets	Note: To enable NDGs, click Interface	
Documentation	Log RADIUS Tunneling Packets	Canfiguration: Advanced Options: Network Device Groups.	
	E Replace RADIUS Port info with	[Back to Top]	
	Match Framed-IP-Address with	RADIUS Key Wrap	

2. Para configurar la configuración de autenticación, navegue hasta Configuración del sistema
 > Configuración de autenticación global, y verifique que la casilla de verificación Permitir autenticación MS-CHAP versión 2 esté marcada:

alate	System Configuration				
CISCO	EAP-ILS session timeout (minutes): 120	-			
Uter Setup Setup Setup Setup Setup Components Endigenation	Select one of the following options for setting username during authentication:	Use this page to specify settings for various subhentication protocols. EAP Configuration EAP-FAST EAP-TLS EAP-TLS EAP EAP-PROVE Timeout HS-CUAP Configuration			
System Cardigaration	LEAP Allow LEAP (For Aironet only)	EAP Configuration EAP is a flexible request-response protocol for arbitrary authentication information (RPC 2284). EAP is leaved on two of earther restored such as URC 822, to or BARUIS and			
Advancerretion Central Detabaser	EAP-MD5 ZAllow EAP-MD5	supports multiple "authentication" types. [Back to Top] PEAP			
Tabdation	AP EAP request timeout (seconds): 20	PEAP is the outer layer protocol for the secure tunnel.			
Hadwork Access Prefiles	MS-CHAP Configuration	Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required ateps on the ACS Certificate Setup page. Allow SAP-MSCIAPV2 — Use to enable SAP-MSCIAMV2 within MS PEAP authentication. Enable this protocol for some requirements MSC-MSCIAMV2 within MSI PEAP authentication. Enable this protocol for some requirements MSC-MSCIAMV2 within MSI PEAP authentication.			
Contractation	Allow MS-CHAP Version 1 Authentication Allow MS-CHAP Version 2 Authentication	Detabase. Allow EAP-CTC - Use to enable EAP-STC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.			
	E Own to help	Allers Desture Validation Una to snable the DPAD (PAD-TLV) protocol for posture validation of			

 Para configurar un usuario, haga clic en User Setup en el menú, y complete estos pasos: Ingrese la información de usuario: Network-Admin *<username>*.Haga clic en Agregar/Editar.Ingrese el Nombre real: Network-Admin *<nombre descriptivo>*.Añada una descripción: *<su elección>*.Seleccione la Password Authentication: ACS Internal Database.Introduzca la contraseña: *<contraseña>*.Confirme la contraseña: *<password>*.Haga clic en Submit (Enviar).

alada	User Setup				
CISCO	User: Network-Admin (New User)		Collect Control P Address Assignment Advanced Settings		
Call Series		Account Disabled	Hatwork Access Restrictions Hat Sension Unase Coving		
SharedProfile	Supplem	entary User Info 📑	Account Deable Deamlo able ACLs Advanced IACAS+ Settings Tel ACS+ Control Tel ACS+ Control		
Refuerb Carfigeration System Configuration	Real Name Description		TACACS1 Enable Parameter TACACS1 - United Summer TACACS1 - United Summar Authorization TACACS1 - United Summar Authorization Command Authorization for Network Banagement Applications TACACS1 - University Survival		
Configuration	· · · · · · ·	ser Setun	IACRUS Antonicos ANDUS Antonicos Inne Baund Alternate Group		
Dutabases	Password Authentication:		Account Disabled Status Select the Account Disabled check box to disable this account; clear the check box to enable the account.		
Telidation Network Access Postile:	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)		[Resk to Tau] Deleting a Username		
Artivity Activity Online Donmentation	Password Confirm Password	••••••	The Delete button appears only when you are editing an existing user account, not when you are adding a new user account. To delete the current user account from the detabase, disk Delete . When asked to confirm your action, disk OK .		
	Separate (CHAP/MS-CHAP/ARAP)		Supplementary User Info		

Verificación

La herramienta de interpretación de información de salida (disponible para clientes registrados únicamente) admite ciertos comandos show. Utilice la herramienta para ver una análisis de información de salida del comando show.

Ingrese estos comandos para confirmar que su configuración funciona correctamente:

- show dot1x
- show dot1x summary
- show dot1x interface
- show authentication sessions interface <interface>
- show authentication interface <interface>

Switch(config)# show dot1x

```
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

Switch(config)# show dot1x summary

```
Interface PAE Client Status
```

Fa0/4 AUTH

Switch(config)# show dot1x interface fa0/4 detail

Dot1x Info for FastEthernet0/4

```
PAE = AUTHENTICATOR
PortControl = FORCE_AUTHORIZED
ControlDirection = Both
HostMode = SINGLE_HOST
QuietPeriod = 5
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

Troubleshoot

Esta sección proporciona los comandos debug que puede utilizar para resolver problemas de su configuración.

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

- debug dot1x all
- debug authentication all
- debug radius (proporciona la información de radius en el nivel de depuración)
- debug aaa authentication (debug for authentication)
- debug aaa authorization (debug for authorization)

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).