Exemple de configuration de l'authentification câblée 802.1x sur un commutateur de la gamme Catalyst 3550 et un ACS version 4.2

Table des matières

Introduction Conditions préalables Exigences Composants utilisés Configurer Exemple de configuration de commutateur Configuration ACS Vérifier Dépannage

Introduction

Ce document fournit un exemple de configuration de base IEEE 802.1x avec Cisco Access Control Server (ACS) Version 4.2 et le protocole RADIUS (Remote Access Dial In User Service) pour l'authentification filaire.

Conditions préalables

Exigences

Cisco vous recommande de :

- Confirmez l'accessibilité IP entre ACS et le commutateur.
- Assurez-vous que les ports UDP (User Datagram Protocol) 1645 et 1646 sont ouverts entre ACS et le commutateur.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Commutateurs Cisco Catalyst, série 3550

Cisco Secure ACS version 4.2

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.

Configurer

Exemple de configuration de commutateur

1. Afin de définir le serveur RADIUS et la clé pré-partagée, entrez cette commande :

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

2. Afin d'activer la fonctionnalité 802.1x, entrez cette commande :

Switch(config)# dot1x system-auth-control

 Afin d'activer globalement l'authentification AAA (Authentication, Authorization, and Accounting) et l'authentification et l'autorisation RADIUS, entrez ces commandes : Remarque : ceci est nécessaire si vous devez passer des attributs à partir du serveur RADIUS ; sinon, vous pouvez l'ignorer.

```
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
```

Configuration ACS

 Afin d'ajouter le commutateur en tant que client AAA dans ACS, naviguez à Configuration du réseau > Ajouter l'entrée client AAA, et entrez ces informations : Adresse IP :
 Adresse IP :
 Adresse IP :
 Secret partagé :
 Authentification à l'aide de : Radius (Cisco IOS[®]/PIX 6.0)

cisco	Network Configuration		w.		
	AAA Client Hostname	switch	You can use the wildcard asterisk (*) for an octat in the IP address. For example, if you and direct the direct is an 100 100 100 100 100 100 100 100 100 10		
Uper Setap	AAA Client IP Address	192.168.1.2	C network to be represented by a single AAA clent entry, enter 192,168,13.* in the AAA Clent IP Address box.		
SuredProfile Components	Prot Client In Protiess	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 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.			
Cardigar Ation	RADIUS Key Wrap	[Beck to Too]			
Configuration	Key Encryption Key		Shared Secret		
Advanistration Central	Message Authenticator Code Key		The Shared Secret is used to encrypt TACACS+ or the RADIUS AAA dient and ACS. The shared secret must be configured in the AAA dient and		
30 Deternal Uper	Key Input Format	ASCII Hexadecimal	* ACS identically, including case sensitivity.		
Front Pastale		Authenticate Using RADIUS (Cisco 105/PIX 6.0) -			
Present Validation	Authenticate Using				
Profiles	Single Connect TACACS+ AAA	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)			
Activity	E Log Update/Watchdog Packets	Ander To enable Mildle click Interface			
Documentation	E Log RADIUS Tunneling Packets	Configuration: Advanced Options: Network Device Groups.			
	E Replace RADIUS Port info with	[Back to Tool]			
	Match Framed-IP-Address with	RADIUS Key Wrap			

2. Afin de configurer la configuration de l'authentification, naviguez vers System Configuration > Global Authentication Setup, et vérifiez que la case à cocher Allow MS-CHAP Version 2 Authentication est activée :

cisco	EAP-ILS session timeout (minutes): 120	4
Uter Serap Serap Serap Serap Seraposets Configuration	Select one of the following options for setting username during authentication:	Use this page to specify settings for various authentication protocols. EAP Configuration EEAP EAP-INS EAP-INS EAP-INS AP-EAP Request Timeout MS-CAAP Configuration
Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration	LEAP Allow LEAP (For Aironet only) EAP-MD5 Ø Allow EAP-MD5	EAP Configuration EAP is a flexible request-seponse protocol for arbitrary authentication information (RFC 2264). EAP is largered on top of another protocol such as UCP. 802.1x or RADIUS and supports multiple "authentication" types. [Back to Tap] PEAP
Perfame Validation	AP EAP request timeout (seconds): 20	PEAP is the outer layer protocol for the secure tunnel. Neter PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after
Reports and activity Desire	MS-CHAP Configuration ? Station MS-CHAP Version 1 Authentication Allow MS-CHAP Version 2 Authentication Rest to Help	 Provide the required steps on the ACS Certificate Setup page. Allow EAP-HECHAPV2 - Use to enable EAP-MECHAPV2 within MS PEAP authentication. Enable this protocol for any requiring the Set-MECHAPV2, such as Microsoft AB, and the ACS Internal Database. Allow EAP-GTC - Use to enable EAP-GTC within Cases PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database. Allow EAP-GTC - Use to enable EAP-GTC within Cases PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database. Allow Experts VabilitionThe to enable the DPAP (PAP-TIV) endered for mature vabilities of the support of

3. Afin de configurer un utilisateur, cliquez sur **User Setup** dans le menu, et complétez ces étapes :

Entrez les informations **utilisateur** : Network-Admin *<username>*.Cliquez sur **Add/Edit.**Entrez le **nom réel** : Network-Admin *<nom descriptif>*.Ajoutez une **description** : *<votre choix>*.Sélectionnez **Authentification par mot de passe** : Base de données interne ACS.Saisissez le **mot de passe** : *<mot de passe>*Confirmez le **mot de passe** : *<password>*.Cliquez sur Submit.

alada	User Setup				
cisco	User: Network-Admin (New User)			alback Jean IP Address Assignment Johancel Settings	
User Setup	Account Disabled			intwork Access Restrictions fax Sensions hear Outran	
(b) Shareditroffe	Supplementary User Info ?			Iscourt Disable Samhadaish ALa Maxaca JACACSE Sattings	
Network Configuration	Real Name Description			ACACI-1 Induk Paryong ACACI-1 United Rayong ACACI-1 United Sayong ACACI-1 United Sayong ACACI-1 United Sayong Autorization ACACI-1 Shell Command Autorization Ammand Autorization for Hetwork Device Hanagement Applications	
Configuration				ACACS+ Unknown Services ETF RADUUS Attributes Inte Bound Alternate Group Inte Bound Alternate Group	
Advalutration Central	User Setup 📍			Account Disabled Status	
Dutabacec	Password Authenticati	OD: ACS Internal Database	5	elect the Account Disabled check box to disable this account; clear the check box to enable he account.	
National Access Postilies	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)			(Beck to Too) Deleting a Username	
Arguette and Activity	Password Confirm	•••••		he Delete button appears only when you are editing an existing user account, not when ou are adding a nen user account. To delete the current user account from the detabese. Lisk better, when asked to confirm your action, disk DH.	
Bonumentation	Password	••••••	1	Back to Top]	
	Separate (CHAP/MS-CHAP/ARAP)			applementary User Info	
	Daceword			use the applicable information is not supplemental user information betwee that appear	

Vérifier

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Entrez ces commandes afin de confirmer que votre configuration fonctionne correctement :

- 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
```

Dépannage

Cette section fournit des commandes debug que vous pouvez utiliser afin de dépanner votre configuration.

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.

- debug dot1x all
- debug authentication all
- debug radius (fournit les informations de radius au niveau du débogage)
- debug aaa authentication (debug for authentication)
- debug aaa authorization (debug for authorization)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.