Esempio di autenticazione cablata 802.1x su uno switch Catalyst serie 3550 e su una configurazione ACS versione 4.2

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Configurazione Esempio di configurazione dello switch Configurazione ACS Verifica Risoluzione dei problemi

Introduzione

In questo documento viene illustrato un esempio di configurazione di base di IEEE 802.1x con Cisco Access Control Server (ACS) versione 4.2 e il protocollo RADIUS (Remote Access Dial In User Service) per l'autenticazione cablata.

Prerequisiti

Requisiti

Cisco consiglia di:

- Confermare la raggiungibilità IP tra ACS e lo switch.
- Verificare che le porte UDP (User Datagram Protocol) 1645 e 1646 siano aperte tra ACS e lo switch.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Switch Cisco Catalyst serie 3550

Cisco Secure ACS versione 4.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di configurazione dello switch

1. Per definire il server RADIUS e la chiave già condivisa, immettere questo comando:

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

2. Per abilitare la funzionalità 802.1x, immettere questo comando:

Switch(config)# dot1x system-auth-control

 Per abilitare l'autenticazione, l'autorizzazione e l'autorizzazione AAA (Authentication, Authorization, and Accounting) e RADIUS a livello globale, immettere i seguenti comandi: Nota: questa operazione è necessaria se è necessario passare attributi dal server RADIUS. In caso contrario, è possibile ignorarla.

```
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)# awitchport 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
```

Configurazione ACS

 Per aggiungere lo switch come client AAA in ACS, selezionare Configurazione di rete > Aggiungi voce client AAA, quindi immettere le seguenti informazioni: Indirizzo IP: </l>
 IP>Segreto condiviso:
 Chiave>Autenticazione tramite: Radius (Cisco IOS[®]/PIX 6.0)

cisco	Network Configuration		×1
	AAA Client Hostname	switch	You can use the wildcard asterisk (*) for an octat in the IP address. For exercise, if you work every Add. direct in your 192, 168, 13.1 Class
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	And client if highest		You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.166.13.12
Network Configuration	Shared Secret	cisco123	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 string	RADIUS Key Wrap	[Beck to Top]	
Coeffiguration	Key Encryption Key		Shared Secret
Advaluation	Message Authenticator Code Key		The Shared Secret is used to encrypt TACACS+ or the RADIUS AAA diant and ACS. The shared
Control Uper	Key Input Format	ASCII Hexadecimal	E secret must be configured in the AAA dient and ACS identically, including case constituity.
Front Partase			(Beck to Top)
Process Validation	Authenticate Using	RADIUS (Cisco IDS/PDX 6.0) ·	Network Device Group
Profiles	Single Connect TACACS+ AAA	Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	
Activity	Log Update/Watchdog Packets	from this AAA Client	Notes To enable NDGs, click Interface
Cocumentation	E Log RADIUS Tunneling Packets	from this AAA Client	Canfiguration: Advanced Options: Network Device Groups.
	Replace RADIUS Port info with	Username from this AAA Client	[Back to Tool]
	Match Framed-IP-Address with	RADIUS Key Wrap	

2. Per configurare l'impostazione dell'autenticazione, passare a **Configurazione di sistema > Impostazione autenticazione globale** e verificare che la casella di controllo **Consenti autenticazione MS-CHAP versione 2** sia selezionata:

cisco	System Configuration EAP-ILS session timeout (minutes): 120	4
Untrop Series Series Series Series Composition For Watterst Configuration	Select one of the following options for setting username during authentication:	Use this page to specify settings for various authentication protocols. EAP Configuration EAP Configuration EAP-INS EAP-INS EAP-INS AP EAP Report Timeout INS CAP CAP Configuration INS
Sprien Carrigeration Configuration Configuration Carried Carri	LEAP Allow LEAP (For Aironet only) EAP-MD5 Allow EAP-MD5	EAP Configuration EAP is a flexible request-response protocol for arbitrary authentication information (8PC 2264). EAP is layered on top of another protocol auch as UCP, 802.1x or RADIUS and supports multiple "authentication" types. [Back to Top] PEAP
Pastane Validation	AP EAP request timeout (seconds): 20	PBAP is the outer layer protocol for the secure tunnel. Neter PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after
Reportand Reportand Documentation	MS-CHAP Configuration ? Station MS-CHAP Version 1 Authentication Allow MS-CHAP Version 2 Authentication Set to Help	 Provide the required steps on the ACS Certificate Setup page. Allow EAP-NBCNAPV2 — Use to enable EAP-NBCOAPV2 within NSI PEAP automation. Enable this protocol for any repository that supports MS-CHAPV2, such as Microsoft AD, and the ACS Internal Database. Allow EAP-CTC — Use to enable EAP-OTC within Case FEAP automatization. Enable this protocol to supports that supports MR-CHAPV2. Allow EAP-CTC — Use to enable EAP-OTC within Case FEAP automatization. Enable this protocol to supports that supports MR-CHAPV2. Allow EAP-CTC — Use to enable EAP-OTC within Case FEAP automatization. Enable this protocol to supports that supports MR-CHAPV2. Allow EAP-CTC — Use to enable EAP-OTC within Case FEAP automatization. Enable this protocol to supports MR-CHAPV2. Allow EAP-CTC — Use to enable EAP-OTC within Case FEAP automatization. Enable this protocol to supports MR-CHAPV2.

3. Per configurare un utente, scegliere **Configurazione utente** dal menu e attenersi alla seguente procedura:

Immettere le informazioni **utente**: Network-Admin *<nomeutente>*.Fare clic su Aggiungi/Modifica.Immettere il nome reale: Network-Admin *<nome descrittivo>*.Aggiungere una descrizione: *<scelta>*.Selezionare Autenticazione password: Database interno ACS.Inserire la password: *<password>*.Confermare la password: *<password>*.Fare clic su Invia.

adrada	User Setup				
CISCO	User: Network-Admin (New User)		Callback Chent IP Address Assignment Advanced Settings		
Cal Setto	E /	Account Disabled	Betwork Access Restrictions Base Sections Unsee Contex		
Baredirofie	Supplem	entary User Info	Account Deaths Describe adds ACLs Advanced TACACS+ Settings TaCACS- London County of the Settings		
Composents Composents Convigoration Convigoration Convigoration Convigoration Loterface	Real Name Description		Inclust - Linker Schuld Inclust - Linker Schuld		
Adroibistration Central	U	ser Setup	Time Round Alternate Scoup Account Disabled Status		
Portane Pertane Patidation	Password Authentication	ACS Internal Database • o used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)	. Select the Account Dirabled check box to dirable this account; dear the chec the account. [Reck to Top] Deleting a Username	k bax to enable	
Artivity Activity Online Doomentation	Password Confirm Password	••••••	The Delete button appears only when you are editing an existing user account you are adding a new user account. To delete the current user account from disk Delete. When asked to confirm your action, disk OK. [Back to Top]	nt, not when the detailese.	
	Separate (CHAP/MS-CHAP/ARAP)		Supplementary User Info		

Verifica

Lo <u>strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi</u> **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

Per verificare che la configurazione funzioni correttamente, immettere questi comandi:

- mostra punto1x
- mostra riepilogo dot1x
- interfaccia show dot1x
- 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

Risoluzione dei problemi

In questa sezione vengono forniti i comandi di debug che è possibile utilizzare per risolvere i problemi relativi alla configurazione.

Nota: consultare le <u>informazioni importanti sui comandi di debug</u> prima di usare i comandi di **debug**.

- debug dot1x all
- debug authentication all
- debug radius (fornisce le informazioni sul raggio a livello di debug)
- debug autenticazione aaa (debug per l'autenticazione)
- autorizzazione debug aaa (debug per autorizzazione)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).