Catalyst 3550系列交換機和ACS 4.2版上的 802.1x有線身份驗證配置示例

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>設定</u> <u>交換機配置示例</u> <u>ACS配置</u> <u>驗證</u> <u>疑難排解</u>

簡介

本檔案將提供思科存取控制伺服器(ACS)版本4.2和用於有線驗證的遠端存取撥入使用者服務 (RADIUS)通訊協定的基本IEEE 802.1x組態範例。

必要條件

需求

思科建議您:

- 確認ACS和交換機之間的IP可達性。
- 確保ACS和交換機之間的使用者資料包協定(UDP)埠1645和1646處於開啟狀態。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco Catalyst 3550 系列交換器
- Cisco安全ACS版本4.2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

交換機配置示例

1. 若要定義RADIUS伺服器和預先共用金鑰,請輸入以下命令:

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

2. 若要啟用802.1x功能,請輸入以下命令:

Switch(config)# dot1x system-auth-control

若要全域性啟用身份驗證、授權和記帳(AAA)以及RADIUS身份驗證和授權,請輸入以下命令
 :
 註:如果需要從RADIUS伺服器傳遞屬性,則必須執行此操作;否則,您可以跳過它。

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-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
```

ACS配置

 要在ACS中將交換機新增為AAA客戶端,請導航到Network Configuration > Add entry AAA client,然後輸入以下資訊: IP地址:<IP>共用金鑰:<key>驗證使用:Radius(Cisco IOS[®]/PIX 6.0)

cisco	Network Configuration		A
	AAA Client Hostname	switch	You can use the wildcard asteriak (*) for an octet in the IP address. For example, if you want every AAA dist in your 192,164,121 Class
Uper Setap		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.
Setap SharedDroffle Community	AAA Client IP Address	4	You can define ranges within an octet of an JP address. For example, if you want every AAA
Network Configuration	Shared Secret	cisco123	client with an IP address between 172,160,13,12 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.
Sester Cardigeration	(Back to Top)		
Configuration	Key Encryption Key		Shared Secret
Administration Castrol	Message Authenticator Code Key	O ASCIL & Havadacimal	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
30 Dutabanes	key input romat	• ASCII • Hexadeciliai	ACs identically, including case sensitivity.
CODE Pattale Validation	Authenticate Using	RADIUS (Gisco IOS/PIX 6.0) *	Network Device Croup
Network Access Postiles	Single Connect TACACS+ AAA	From the list, dick the name of the Network Device Group (NDG) to which this AAA client belongs.	
Activity	E Log Update/Watchdog Packets	Notes To enable NDGs, click Interface	
Documentation	Log RADIUS Tunneling Packets from this AAA Client		Configuration: Advanced Options: Network Device Groups.
	Replace RADIUS Port info with	[Bask to Top]	
	E Match Framed-IP-Address with user IP address for accounting packets from this AAA Client		RADIUS Key Wrap

2. 要配置身份驗證設定,請導航到System Configuration > Global Authentication Setup,然後驗 證Allow MS-CHAP Version 2 Authentication覈取方塊是否已選中:

. dealer	System Configuration		
CISCO	EAP-ILS session timeout (minutes): 120		
Uter Stop Setop Setop Setop References References References	Select one of the following options for setting username during authentication:	Use this page to specify settings for various authentication protocols. EAP Configuration PEAP EAP-TAS EAP-	
System Configuration	LEAP Allow LEAP (For Aironet only)	EAP Configuration EAP is a field is request-response protocol for arbitrary authentication information (RPC 2294). Ref is learned on the of eacher protocol such as USP, 802, by or BADUIS and	
Advantation Control Detabases	EAP-MD5 ZAllow EAP-MD5	supports multiple "authentication" types. [Back to Top] PEAP	
Tabdation	AP EAP request timeout (seconds): 20	DEAD is the outer layer protocol for the secure tunnel.	
Native Accurate	MC-CHAD Configuration	Note: FEAP is a certificate-based authentication protocol. FEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.	
Activity	Allow MS-CHAP Version 1 Authentication	 Allow EAP-HICHAP+2 — Use to enable EAP-HICHAP+2 within HS FEAP authentication. Enable this protocol for any repository that supports MS-CHAP+2, such as Microsoft AD, and the ACS Internal Database. 	
	Allow M5-CHAP Version 2 Authentication	Alive EAP-GTC - Use to enable BAP-GTC within Class TEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database. Alive Enables: Validation - Use in analysis the EPAD (FAD-T1V) entrored for continue validation of	

3. 要配置使用者,請按一下選單上的User Setup,然後完成以下步驟:
 輸入User information: Network-Admin <username>。按一下「Add/Edit」。輸入Real Name:

Network-Admin *<descriptive name>。*新增**說明**: *<您的選擇>。*選擇**Password Authentication**: ACS Internal Database。輸入**密碼**: *<password>。*確認**Password**: *<password>。*按一下 「Submit」。

allada	User Setup	
CISCO	User: Network-Admin (New User)	Callack Chert IP Address Assistment Advected Settings
Ucar Setap	Account Disabled	Betwork Access Restrictions Max Sentions Unacc Outpan
Croup Tetap	Supplementary User Info	Account Deside Describe Described Advanced JACACS+ Settings TACACS+ Englisher TACACS+ Englisher
Surface Surface	Real Name Description	TACACS+ Enable Parament TACACS+ Conference of Parament TACACS+ Conference of Anthretization TACACS+ Shell Common of Anthretization TACACS+ Unknown of TACACS+ Unknown Services TACACS+ Unknown Services TACACS+ Unknown Services
Configuration		IETE RADIUS Attributes RADIUS Vendor Steacht Attributes Time Round Alternate Scope
Central	User Setup 1	Account Disabled Status
DG Dutabases	Password Authentication: ACS Internal Database	Select the Account Disabled check box to disable this account; dear the check box to enable the account.
Network Access Postilec	CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)	(Back to Tso) Deleting a Username
Activity	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.
Den Bonamentation	Confirm Password	dick Delete. When asked to confirm your action, dick OK. [Back to Top]
	Separate (CHAP/MS-CHAP/ARAP)	Supplementary User Tafo
	Decement	Tune the contrable information is not constanted user information house that annual

驗證

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)支援某些**show**命令。使用Output Interpreter工具檢視**show**指 令輸出的分析。

輸入以下命令以確認您的組態是否正常運作:

- 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 本節提供可用於對組態進行疑難排解的偵錯命令。

附註:使用 debug 指令之前,請先參閱有關 Debug 指令的重要資訊。

- debug dot1x all
- 調試全部身份驗證
- debug radius(提供偵錯層級的radius資訊)
- debug aaa authentication(調試以進行身份驗證)
- debug aaa authorization(debug for authorization)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。