Catalyst 3550 Series 스위치 및 ACS 버전 4.2의 802.1x 유선 인증 컨피그레이션 예

목차

<u>소개</u> <u>사전 요구 사항</u> <u>요구 사항</u> <u>사용되는 구성 요소</u> <u>구성</u> <u>스위치 설정 예시</u> <u>ACS 컨피그레이션</u> <u>다음을 확인합니다.</u> <u>문제 해결</u>

소개

이 문서에서는 유선 인증을 위한 Cisco ACS(Access Control Server) 버전 4.2 및 RADIUS(Remote Access Dial In User Service) 프로토콜의 기본 IEEE 802.1x 컨피그레이션 예를 제공합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 사항을 권장합니다.

- ACS와 스위치 간 IP 연결 가능성을 확인합니다.
- UDP(User Datagram Protocol) 포트 1645 및 1646이 ACS와 스위치 간에 열려 있는지 확인합 니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Catalyst 3550 Series Switches
- Cisco Secure ACS 버전 4.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바 이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

스위치 설정 예시

1. RADIUS 서버 및 사전 공유 키를 정의하려면 다음 명령을 입력합니다.

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

2.802.1x 기능을 활성화하려면 다음 명령을 입력합니다.

Switch(config)# dot1x system-auth-control

Switch(config-if)# dot1x timeout tx-period

 AAA(Authentication, Authorization, and Accounting) 및 RADIUS 인증 및 권한 부여를 전역적 으로 활성화하려면 다음 명령을 입력합니다.
 참고: RADIUS 서버에서 특성을 전달해야 하는 경우 이 작업이 필요합니다. 그렇지 않으면 건 너뛸 수 있습니다.

```
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-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
```

ACS 컨피그레이션

 ACS에서 스위치를 AAA 클라이언트로 추가하려면 Network Configuration(네트워크 컨피그레 이션) > Add entry AAA client(항목 AAA 클라이언트 추가)로 이동하여 다음 정보를 입력합니 다.

IP 주소: <*IP*>공유 암호: <*key*>다음을 사용하여 인증: Radius(Cisco IOS[®]/PIX 6.0)

CISCO			•
	AAA Client Hostname	witch	You can use the wildcard asteriak (*) for an other in the IP address. For example, if you yant every AAA diset in your 192.168,13.1 Class
Uper Setap	AAA Client IP Address	92.168.1.2	C network to be represented by a single AAA client entry, enter 192,168,13.* In the AAA Client IP Address box,
StaredDroffe Components	For Chence in Planets	a	You can define ranges within an octet of an JP address. For example, if you want every AAA client with an IP address between 192.168.13.12
Ref work Configuration	Shared Secret ci	scol23	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.
Configuration	RADIUS Key Wrap	[Beck to Top]	
Configuration	Key Encryption Key		Shared Secret
Advancestation Castrol	Message Authenticator Code Key Key Input Format	ASCII Hexadecimal	The Shared Secret is used to encrypt TACACS+ or the RADIUS AAA diant and ACS. The shared secret must be configured in the AAA diant and ACS identically, including case sensitivity.
Pastale			(Back to Top)
Validation	Authenticate Using R	ADIUS (Cisco 10S/PIX 6.0) ·	Network Device Group
Profiles	Single Connect TACACS+ AAA Clie	From the list, dick the name of the Network Device Group (NDG) to which this AAA client belongs.	
Activity	Log Update/Watchdog Packets fro	m this AAA Client	Notes To enable NDGs, click Interface
Booumentation	Log RADIUS Tunneling Packets fro	Canfiguration: Advanced Options: Network Device Groups.	
	Replace RADIUS Port info with Use	[Back to Top]	
	Match Framed-IP-Address with us	er IP address for accounting packets from this AAA Client	RADIUS Key Wrap

Network Continueation

2. 인증 설정을 구성하려면 System Configuration(시스템 구성) > Global Authentication Setup(전 역 인증 설정)으로 이동하여 Allow MS-CHAP Version 2 Authentication(MS-CHAP 버전 2 인증 허용) 확인란이 선택되었는지 확인합니다.

abada	System Configuration	
cisco	EAP-ILS session timeout (minutes): 120	
User Brisp Setap Setap Setap Setap Setap Setap Setap Setar Setap Setar Setap	Select one of the following options for setting username during authentication:	Use this page to specify settings for various suthentication protocols. EAP Configuration EAP-TAS EAP-TLS EAP EAP-TLS AP-SAP Recent Timeout HS-CAAP Configuration
Septem Cardigeration	LEAP Allow LEAP (For Aironet only)	EAP Configuration EAP is a Reachine request-response protocol for arbitrary authentication information (RPC 2294). EAD is leaved on two of earthur restored such as URE ADD to or BADUIS and
Adventoriation Castrol Detabases	EAP-MD5 ZAllow EAP-MD5	supports multiple "authentication" types. <u>Hilack to Tapi</u> PEAP
Talidation	AP EAP request timeout (seconds): 20	PEAP is the outer layer protocol for the secure tunnel.
Profiles	MS-CHAP Configuration	Neter FEAP is a certificate-based actientication protocol. FEAP authentication can occur only after you have completed the required ategs on the AES Certificate Setup page.
Cattor Consecution	Allow MS-CHAP Version 1 Authentication	Alive EAP-MICHAIPV2 — Use to enable EAP-MICHAIPV2 within this PEAP authentication. Enable this protocol for any repository that supports MS-CHAIPV2, such as Microsoft AD, and the ACS Internal Detabase.
	Allow MS-CHAP Version 2 Authentication Bet to Help	 Allow EAP-CTC — Use to enable EAP-GTC within Cisco FEAP authentication. Enable this protocol to support any distabase that supports PAP, including LOAP, OTP Servers, and the ACS External Database.
		• Allow Doubure Validation Use to enable the DPAD (PAD-TIV) perform for conture validation of

 사용자를 구성하려면 메뉴에서 User Setup(사용자 설정)을 클릭하고 다음 단계를 완료합니다. 사용자 정보 Network-Admin *<username>을 입력합니다*.Add/Edit를 클릭합니다.Real Name: Network-Admin *<*descriptive name>*을 입력합니다*.설명을 추가합니다. *<원하는 항목* Password Authentication: ACS Internal Database(비밀번호 인증: ACS 내부 데이터베이스) 를 선택합니다.비밀번호를 입력합니다. *<password>*.비밀번호를 확인합니다: *<password>*.Submit(제출)을 클릭합니다.

	User Setup			
CISCO	User: Network-Admin (New User)			Calibach Chent IP Address Assignment Advanced Settings
Settop	C Account Disabled			Hetmork Access Restrictions Hax Sensions Unact Outlan
Co Shareditoffe	Supplementary User Info ?			Account Disable Control Advanced JAACS+ Settings Advanced JAACS+ Settings TACACS+ Control
Network Configuration System Configuration	Real Name Description			1ACAC5 + Enable Parameter 1ACAC5 + Onebic Parameter 1ACAC5 + Onebic Announced Authorization 1ACAC5 + Shell Cannon Authorization Command Authorization for Herbook Device Management Applications 1ACAC5 + Unknown Services
Configuration		car Satun		EIT FACIUS Automutes Additus Yender Societas Time Bound Alternate Group
Contrast User	Password Authentication: ACS Internal Database CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)			Account Disabled Status Select the Account Disabled check box to disable this account; dear the check box to enable the account. [Back to Tap] Deleting a Username
Validation Network Access Postiec			ìf .)	
Calese Documentation	Password Confirm Password	••••••		The Delete button appears only when you are editing an existing user account, not when you are adding a ner user account. To delete the current user account from the database, disk bedter, when asked to confirm your action, disk CK . [Back to Too]
	Separate (CHAP/MS-CHAP/ARAP)			Supplementary User Info

다음을 확인합니다.

<u>아웃풋 인터프리터 툴(등록</u> 고객 전용)은 특정 show 명령을 지원합니다. show 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 다음 명령을 입력합니다.

- dot1x 표시
- show dot1x 요약
- show dot1x 인터페이스
- 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

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하기 위해 사용할 수 있는 debug 명령을 제공합니다.

참고: debug 명령<u>을</u> 사용하기 전에 Debug 명령에 대한 중요 정보**를** 참조하십시오.

- 모두 dot1x 디버그
- 모든 인증 디버그
- debug radius(디버그 레벨에서 radius 정보 제공)
- debug aaa authentication (debug for authentication)
- debug aaa authorization(권한 부여를 위한 디버그)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번 역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.