

نم لوجم ىلع 802.1x ةيكل سلا ةقداصم ل ACS نيوكت لاثم و Catalyst 3550 ةلسلسلا 4.2 رادصإلا

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [مثال على تكوين المحول](#)
- [تكوين ACS](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)

المقدمة

يقدم هذا المستند مثال تكوين IEEE 802.1x الأساسي مع الإصدار 4.2 من خادم التحكم في الوصول (ACS) من Cisco وروتوكول خدمة الوصول عن بعد في المستخدم (RADIUS) للمصادقة السلكية.

المتطلبات الأساسية

المتطلبات

Cisco يوصي أن أنت:

- قم بتأكيد إمكانية الوصول إلى IP بين ACS والمحول.
- تأكد من أن منافذ بروتوكول مخطط بيانات المستخدم (1645 UDP و 1646 مفتوحة بين ACS والمحول).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- المحولات Cisco Catalyst 3550 Series Switches
- Cisco Secure ACS، الإصدار 4.2

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي

التكوين

مثال على تكوين المحول

1. دخلت in order to عينت ال RADIUS نادل ومفتاح مشترك مسبقا، هذا أمر:

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

2. لتمكين وظيفة 802.1x، أدخل هذا الأمر:

```
Switch(config)# dot1x system-auth-control
```

3. لتمكين المصادقة والتفويض والمحاسبة (AAA) ومصادقة RADIUS والتفويض بشكل عام، أدخل الأوامر التالية:

ملاحظة: هذا ضروري إذا احتجت إلى تمرير السمات من خادم RADIUS؛ وإلا، يمكنك تخطيه.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(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
```

تكوين ACS

1. لإضافة المحول كعميل AAA في ACS، انتقل إلى تكوين الشبكة < إضافة إدخال AAA client، وأدخل هذه المعلومات:

عنوان <IP>: IP: <سر مشترك>: <key> المصادقة باستخدام: (RADIUS (Cisco IOS®/PIX 6.0

Network Configuration

AAA Client Hostname: switch
 AAA Client IP Address: 192.168.1.2
 Shared Secret: cisco123

RADIUS Key Wrap
 Key Encryption Key:
 Message Authenticator Code Key:
 Key Input Format: ASCII Hexadecimal

Authenticate Using: RADIUS (Cisco IOS/PDX 6.0)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
 Log Update/Watchdog Packets from this AAA Client
 Log RADIUS Tunneling Packets from this AAA Client
 Replace RADIUS Port info with Username from this AAA Client
 Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

You can use the wildcard asterisk (*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.* in the AAA Client IP Address box.

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 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.

[\[Back to Top\]](#)

Shared Secret
 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 sensitivity.

[\[Back to Top\]](#)

Network Device Group
 From the list, click the name of the Network Device Group (NDG) to which this AAA client belongs.

Note: To enable NDGs, click [Interface Configuration: Advanced Options: Network Device Groups](#).

[\[Back to Top\]](#)

RADIUS Key Wrap

لتكوين إعداد المصادقة، انتقل إلى تكوين النظام < إعداد المصادقة العامة، وتحقق من تحديد خانة الاختيار 2. السماح بمصادقة MS-CHAP الإصدار 2:

System Configuration

EAP-TLS session timeout (minutes): 120

Select one of the following options for setting username during authentication:
 Use Outer Identity
 Use CN as Identity
 Use SAN as Identity

LEAP
 Allow LEAP (For Aironet only)

EAP-MD5
 Allow EAP-MD5

AP EAP request timeout (seconds): 20

MS-CHAP Configuration

Allow MS-CHAP Version 1 Authentication
 Allow MS-CHAP Version 2 Authentication

[Back to Help](#)

Use this page to specify settings for various authentication protocols.

- EAP Configuration
- LEAP
- EAP-EAP
- EAP-TLS
- LEAP
- EAP-MD5
- AP EAP Request Timeout
- MS-CHAP Configuration

EAP Configuration
 EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.

[\[Back to Top\]](#)

PEAP
 PEAP is the outer layer protocol for the secure tunnel.

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the [ACS Certificate Setup](#) page.

- Allow EAP-MSCHAPv2 — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPv2, such as Microsoft AD, and the ACS Internal Database.
- Allow EAP-GTC — Use to enable EAP-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, DTP Servers, and the ACS Internal Database.
- Allow EAP-FAST — Use to enable the EAP (EAP-TLV) method for remote validation of

3. لتكوين مستخدم، انقر فوق إعداد المستخدم في القائمة، ثم أكمل الخطوات التالية:
 أدخل معلومات المستخدم: مسؤول الشبكة <username>. قطعة يضيف/يحرر. أدخل الاسم الحقيقي: مسؤول الشبكة <اسم وصفي>. إضافة وصف: <إختيارك>. حدد مصادقة كلمة المرور: قاعدة بيانات ACS الداخلية. أدخل كلمة المرور: <password>. أكد كلمة المرور: <password>. انقر على إرسال.

User Setup

User: Network-Admin (New User)

Account Disabled

Supplementary User Info

Real Name:
 Description:

User Setup

Password Authentication: ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password:
 Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

[Back to Top](#)

Account Disabled Status
 Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[\[Back to Top\]](#)

Deleting a Username
 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 database, click **Delete**. When asked to confirm your action, click **OK**.

[\[Back to Top\]](#)

Supplementary User Info
 This the available information in any supplementary user information boxes that appear

التحقق من الصحة

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر `show`. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرج الأمر `show`.

دخلت هذا أمر `in order to` أكدت أن تشكيكك يعمل بشكل صحيح:

- `show dot1x`
- `show dot1x` ملخص
- `show dot1x` قارن
- `<show authentication session 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
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم أوامر تصحيح الأخطاء التي يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: ارجع إلى [معلومات مهمة حول أوامر التصحيح](#) قبل استخدام أوامر `debug`.

- `debug dot1x all`
- تصحيح أخطاء المصادقة الكل
- `debug radius` (يوفر معلومات عن RADIUS على مستوى تصحيح الأخطاء)
- مصادقة `debug aaa` (تصحيح الأخطاء للمصادقة)
- `debug aaa` تخويل (تصحيح الأخطاء للتخويل)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد عوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) ي لصلأل يزي لچنل دن تسمل