

دليل تالاجم لاددعتم IEEE 802.1x ةقداصم تباتل لانيوكتل لادالوحم لانيوكت لاثم Cisco Catalyst Layer 3

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [المنتجات ذات الصلة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [شكلت المادة حفازة مفتاح ل 802.1x Multi-domain صحة هوية](#)
- [تكوين خادم RADIUS](#)
- [قم بتكوين عملاء الكمبيوتر لاستخدام مصادقة 802.1x](#)
- [قم بتكوين هواتف IP لاستخدام مصادقة 802.1x](#)
- [التحقق من الصحة](#)
- [أجهزة الكمبيوتر العميلة](#)
- [هواتف بروتوكول الإنترنت](#)
- [محول من الطبقة 3](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [فشل مصادقة هاتف IP](#)
- [معلومات ذات صلة](#)

المقدمة

تسمح المصادقة متعددة المجالات لهاتف IP وجهاز كمبيوتر شخصي بالمصادقة على منفذ المحول نفسه بينما تضعهم على شبكات VLAN الصوتية والبيانات المناسبة. يشرح هذا المستند كيفية تكوين مصادقة IEEE 802.1x متعددة المجالات (MDA) على محولات Cisco Catalyst Layer 3 ذات التكوين الثابت.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- [كيف يعمل RADIUS؟](#)

- دليل نشر تحويل ACS و Catalyst
- دليل المستخدم لخدام التحكم في الوصول الآمن من Cisco، الإصدار 4.1
- نظرة عامة على هاتف بروتوكول الإنترنت الموحد من Cisco

المكونات المستخدمة

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

- Cisco مادة حفازة 3560 sery مفتاح أن يركض Cisco IOS[®] برمجية إطلاق 12.2(37)SE1 ملاحظة: يتوفر دعم المصادقة متعددة المجالات فقط من برنامج Cisco IOS الإصدار 12.2(35)SE والإصدارات الأحدث.
- يستخدم هذا المثال خادم التحكم في الوصول الآمن (4.1 ACS) من Cisco كخادم RADIUS. ملاحظة: يجب تحديد خادم RADIUS قبل تمكين 802.1x على المحول.
- أجهزة الكمبيوتر العميلة التي تدعم مصادقة 802.1x ملاحظة: يستخدم هذا المثال عملاء Microsoft Windows XP.
- هاتف بروتوكول الإنترنت الموحد من Cisco طراز 7970G مع البرنامج الثابت SCCP، الإصدار 8.2(1)
- هاتف بروتوكول الإنترنت الموحد من Cisco طراز 7961G مع البرنامج الثابت SCCP، الإصدار 8.2(2)
- خادم تقارب الوسائط (MCS) مع Cisco Unified Communications Manager (Cisco CallManager) 4.1(3)SR2

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 أمر.

المنتجات ذات الصلة

يمكن استخدام هذا التكوين أيضا مع الأجهزة الصلبة التالية:

- سلسلة محول Cisco Catalyst 3560-E من Cisco
 - المحول سلسلة Cisco Catalyst 3750
 - المحول Cisco Catalyst 3750-E Series Switch
- ملاحظة: لا يدعم المحول Cisco Catalyst 3550 Series Switch المصادقة متعددة المجالات 802.1X.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يحدد معيار IEEE 802.1x بروتوكول التحكم في الوصول والمصادقة المستند إلى خادم العميل الذي يقيد الأجهزة غير المصرح بها من الاتصال بشبكة LAN من خلال منافذ يمكن الوصول إليها بشكل عام. يتحكم معيار 802.1x في الوصول إلى الشبكة من خلال إنشاء نقطتي وصول ظاهريتين متميزتين في كل منفذ. نقطة وصول واحدة هي ميناء غير خاضع للتحكم، في حين أن الأخرى هي ميناء خاضع للتحكم. تتوفر جميع حركات المرور عبر المنفذ الواحد لكل من نقطتي الوصول. يصادق 802.1x كل جهاز مستخدم أن يكون مرتبط إلى مفتاح ميناء ويعين الميناء إلى VLAN قبل أن يجعل هو يتوفر أي خدمة أن يكون قدمت بالمفتاح أو ال LAN. إلى أن تتم مصادقة الجهاز، يسمح التحكم في الوصول إلى شبكة 802.1x فقط لحركة مرور بروتوكول المصادقة المتوسع عبر شبكة (EAPOL) LAN من خلال المنفذ الذي يتم توصيل الجهاز به. بعد أن تكون المصادقة ناجحة، يمكن لحركة المرور العادية أن تمر عبر المنفذ.

يتكون الطراز 802.1x من ثلاثة مكونات أساسية. ويشار إلى كل منها باسم كيان الوصول إلى المنفذ (PAE).

- جهاز عميل يتطلب الوصول إلى الشبكة، على سبيل المثال، هواتف بروتوكول الإنترنت وأجهزة الكمبيوتر المتصلة
- جهاز الشبكة المصدق الذي يسهل طلبات تفويض الطالب، على سبيل المثال، Cisco Catalyst 3560
- خادم المصادقة — خادم مصادقة طلب اتصال المستخدم البعيد (RADIUS)، الذي يوفر خدمة المصادقة، على سبيل المثال، خادم التحكم في الوصول الآمن من Cisco

تحتوي هواتف بروتوكول الإنترنت (IP) الموحدة من Cisco أيضا على عميل 802.1X. يتيح هذا الطلب لمسؤولي الشبكة التحكم في اتصال هواتف IP بمنافذ محول شبكة LAN. ينفذ الإصدار الأولي من هاتف IP 802.1X الملحق خيار EAP-MD5 لمصادقة 802.1X. في تكوين متعدد المجالات، يجب أن يطلب هاتف IP وجهاز الكمبيوتر المرفق الوصول إلى الشبكة بشكل مستقل بواسطة مواصفات اسم المستخدم وكلمة المرور. قد يتطلب جهاز المصدق معلومات من سمات RADIUS المسماة. تحدد السمات معلومات تحويل إضافية مثل ما إذا كان يتم السماح بالوصول إلى شبكة VLAN معينة للمطالب. يمكن أن تكون هذه السمات خاصة بالمورد. تستخدم Cisco سمات RADIUS Cisco-AV-pair لإعلام المصدق (Cisco Catalyst 3560) بأن مسبب (IP Phone) مسموح به على شبكة VLAN الصوتية.

التكوين

في هذا القسم، تقدم لك معلومات تكوين ميزة المصادقة متعددة المجالات 802.1x الموضحة في هذا المستند.

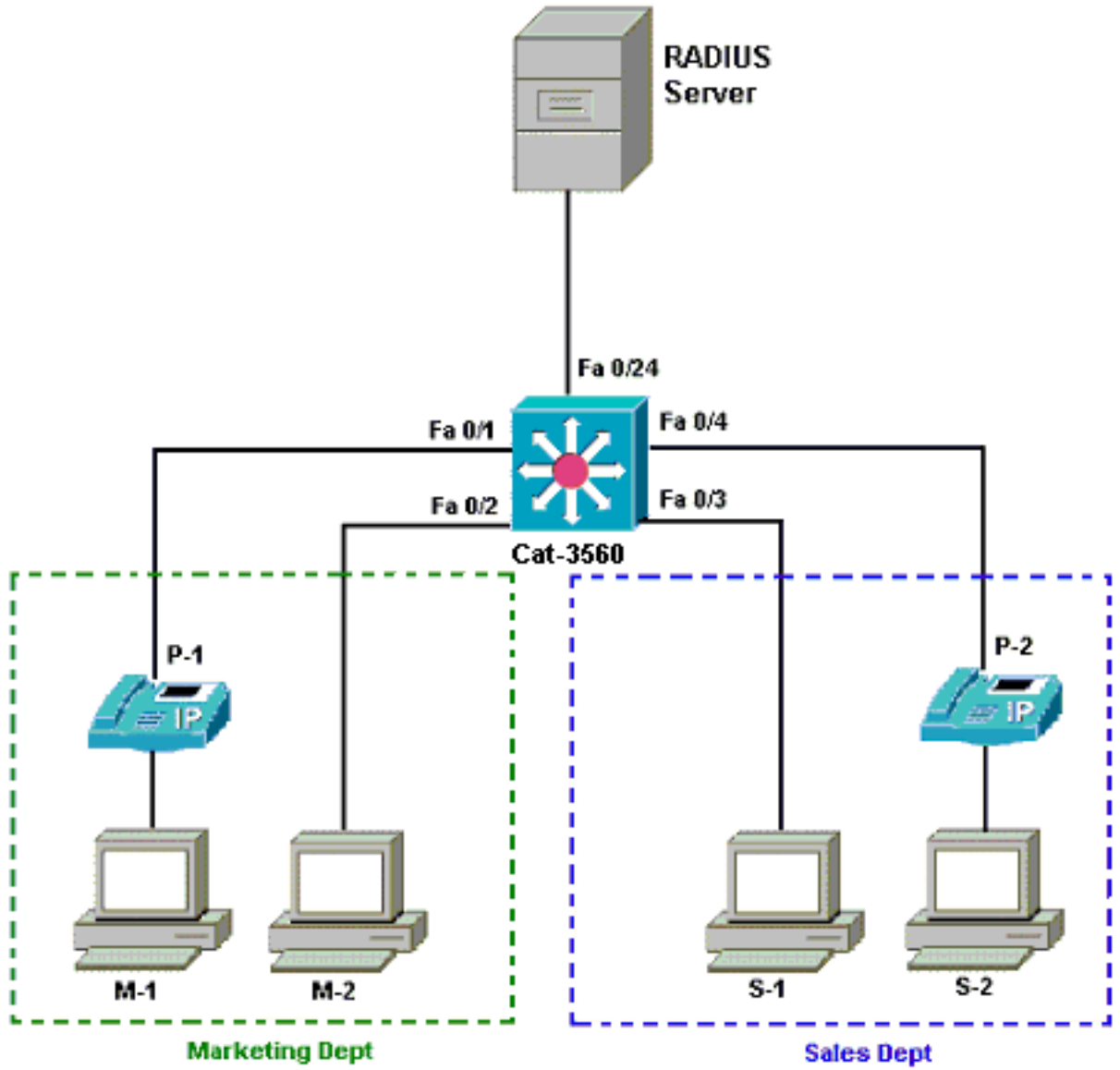
يتطلب هذا التكوين الخطوات التالية:

- [شكّلت المادة حفازة مفتاح ل 802.1x Multi-domain صحة هوية.](#)
- [قم بتكوين خادم RADIUS.](#)
- [قم بتكوين عملاء الكمبيوتر لاستخدام مصادقة 802.1x.](#)
- [قم بتكوين هواتف IP لاستخدام مصادقة 802.1x.](#)

ملاحظة: أستخدم أداة بحث الأوامر (للعلماء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



- خادم RADIUS—يقوم هذا بتنفيذ المصادقة الفعلية للعميل. يتحقق خادم RADIUS من هوية العميل ويخطر المحول بما إذا كان العميل مخولاً للوصول إلى خدمات الشبكة المحلية والمحولات أم لا. هنا، ركبت ال Cisco ACS وشكلت على وسائط تشكيل نادل (MCS) للمصادقة و VLAN تنازل. كما أن MCS هو خادم TFTP ومدير الاتصالات الموحدة من Cisco CallManager (Cisco) لهواتف IP.
- المحول—يتحكم هذا في الوصول المادي إلى الشبكة استناداً إلى حالة مصادقة العميل. يعمل المحول كوسيط (وكيل) بين العميل وخادم RADIUS. وهو يطلب معلومات الهوية من العميل، ويتحقق من هذه المعلومات باستخدام خادم RADIUS، ويرسل إستجابة إلى العميل. هنا، المادة حفازة 3560 شكلت مفتاح أيضاً ك DHCP نادل. يسمح دعم مصادقة 802.1x لبروتوكول التكوين الديناميكي للمضيف (DHCP) لخادم DHCP بتعيين عناوين IP إلى الفئات المختلفة للمستخدمين النهائيين. للقيام بذلك، يضيف معرف المستخدم الذي تمت مصادقته إلى عملية اكتشاف DHCP. المنافذ FastEthernet 0/1 و 4/0 هي المنافذ الوحيدة التي تم تكوينها للمصادقة متعددة المجالات 802.1x. توجد المنافذ FastEthernet 0/2 و 3/0 في الوضع الافتراضي 802.1x للمضيف الواحد. يتصل Port FastEthernet 0/24 بخادم RADIUS. ملاحظة: إذا كنت تستخدم خادم DHCP خارجي، فلا تنس إضافة الأمر ip helper-address على وجه (VLAN) (SVI)، التي يتواجد فيها العميل، والتي تشير إلى خادم DHCP.
- العملاء—هذه أجهزة، على سبيل المثال، هواتف IP أو محطات العمل، التي تطلب الوصول إلى خدمات الشبكة المحلية والمحولات والاستجابة إلى الطلبات من المحول. هنا، شكلت زبون in order to حققت العنوان من DHCP نادل. الأجهزة M-1 و M-2 و S-1 و S-2 هي أجهزة محطات العمل العملية التي تطلب الوصول إلى الشبكة. P-1 و P-2 هما عملاء هاتف IP الذين يطلبون الوصول إلى الشبكة. M-1 و M-2 و P-1 هي أجهزة عميلة في قسم التسويق. S-1 و S-2 و P-2 هي أجهزة عميلة في قسم المبيعات. تم تكوين هواتف IP P-1 و

P-2 لتكون في شبكة VLAN الصوتية نفسها (VLAN 3). يتم تكوين محطات العمل M-1 و M-2 لتكون في شبكة VLAN الخاصة بالبيانات نفسها (VLAN 4) بعد مصادقة ناجحة. كما تم تكوين محطات العمل S-1 و S-2 لتكون في شبكة VLAN نفسها للبيانات (VLAN 5) بعد مصادقة ناجحة. ملاحظة: يمكنك استخدام تعيين شبكة VLAN ديناميكي من خادم RADIUS لأجهزة البيانات فقط.

شكلت المادة حفازة مفتاح ل 802.1x Multi-domain صحة هوية

يتضمن تكوين المحول العينة هذا:

- كيفية تمكين مصادقة 802.1x متعددة المجالات على منافذ المحول
 - التكوين المرتبط بخادم RADIUS
 - تكوين خادم DHCP لتعيين عنوان IP
 - التوجيه بين شبكات VLAN للحصول على اتصال بين العملاء بعد المصادقة
- راجع [إستخدام مصادقة Multidomain](#) للحصول على مزيد من المعلومات حول الإرشادات حول كيفية تكوين MDA.
- ملاحظة: تأكد من اتصال خادم RADIUS دائما خلف منفذ معتمد.
- ملاحظة: يتم عرض التكوين ذي الصلة فقط هنا.

كات-3560

```
Switch#configure terminal
Switch(config)#hostname Cat-3560
Sets the hostname for the switch. Cat- ---!
3560 (config)#vlan 2
Cat-3560 (config-vlan)#name SERVER
Cat-3560 (config-vlan)#vlan 3
Cat-3560 (config-vlan)#name VOICE
Cat-3560 (config-vlan)#vlan 4
Cat-3560 (config-vlan)#name MARKETING
Cat-3560 (config-vlan)#vlan 5
Cat-3560 (config-vlan)#name SALES
Cat-3560 (config-vlan)#vlan 6
Cat-3560 (config-vlan)#name GUEST_and_AUTHFAIL
VLAN should already exist in the switch for a ---!
successful authentication. Cat-3560 (config-vlan)#exit
Cat-3560 (config)#interface vlan 2
Cat-3560 (config-if)#ip address 172.16.2.1 255.255.255.0
Cat-3560 (config-if)#no shut
This is the gateway address for the RADIUS Server. ---!
Cat-3560 (config-if)#interface vlan 3
Cat-3560 (config-if)#ip address 172.16.3.1 255.255.255.0
Cat-3560 (config-if)#no shut
This is the gateway address for IP Phone clients in ---!
VLAN 3. Cat-3560 (config-if)#interface vlan 4
Cat-3560 (config-if)#ip address 172.16.4.1 255.255.255.0
Cat-3560 (config-if)#no shut
This is the gateway address for PC clients in VLAN ---!
4. Cat-3560 (config-if)#interface vlan 5
Cat-3560 (config-if)#ip address 172.16.5.1 255.255.255.0
Cat-3560 (config-if)#no shut
This is the gateway address for PC clients in VLAN ---!
5. Cat-3560 (config-if)#exit
Cat-3560 (config)#ip routing
Enables IP routing for interVLAN routing. Cat- ---!
3560 (config)#interface range fastEthernet 0/1 - 4
Cat-3560 (config-if-range)#shut
```

```

Cat-3560(config-if-range)#exit
Cat-3560(config)#interface fastEthernet 0/24
Cat-3560(config-if)#switchport mode access
Cat-3560(config-if)#switchport access vlan 2
This is a dedicated VLAN for the RADIUS server. ---!
Cat-3560(config-if)#spanning-tree portfast
Cat-3560(config-if)#exit
Cat-3560(config)#interface range fastEthernet 0/1 ,
fastEthernet 0/4
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#switchport voice vlan 3
You must configure the voice VLAN for the IP phone ---!
when the !--- host mode is set to multidomain. !---
Note: If you use a dynamic VLAN in order to assign a
voice VLAN !--- on an MDA-enabled switch port, the voice
.device fails authorization

Cat-3560(config-if-range)#dot1x port-control auto
Enables IEEE 802.1x authentication on the port. ---!
Cat-3560(config-if-range)#dot1x host-mode multi-domain
Allow both a host and a voice device to be !--- ---!
authenticated on an IEEE 802.1x-authorized port. Cat-
3560(config-if-range)#dot1x guest-vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
The guest VLAN and restricted VLAN features only ---!
apply to the data devices !--- on an MDA enabled port.
Cat-3560(config-if-range)#dot1x reauthentication
Enables periodic re-authentication of the client. ---!
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
Set the number of seconds between re-authentication ---!
attempts. Cat-3560(config-if-range)#dot1x auth-fail max-
attempts 2
Specifies the number of authentication attempts to ---!
allow !--- before a port moves to the restricted VLAN.
Cat-3560(config-if-range)#exit
Cat-3560(config)#interface range fastEthernet 0/2 - 3
Cat-3560(config-if-range)#switchport mode access
Cat-3560(config-if-range)#dot1x port-control auto
By default a 802.1x authorized port allows only a ---!
single client. Cat-3560(config-if-range)#dot1x guest-
vlan 6
Cat-3560(config-if-range)#dot1x auth-fail vlan 6
Cat-3560(config-if-range)#dot1x reauthentication
Cat-3560(config-if-range)#dot1x timeout reauth-period 60
Cat-3560(config-if-range)#dot1x auth-fail max-attempts 2
Cat-3560(config-if-range)#spanning-tree portfast
Cat-3560(config)#ip dhcp pool IP-Phones
Cat-3560(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.3.1
Cat-3560(dhcp-config)#option 150 ip 172.16.2.201
This pool assigns ip address for IP Phones. !--- ---!
Option 150 is for the TFTP server. Cat-3560(dhcp-
config)#ip dhcp pool Marketing
Cat-3560(dhcp-config)#network 172.16.4.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.4.1
This pool assigns ip address for PC clients in ---!
Marketing Dept. Cat-3560(dhcp-config)#ip dhcp pool Sales
Cat-3560(dhcp-config)#network 172.16.5.0 255.255.255.0
Cat-3560(dhcp-config)#default-router 172.16.5.1
This pool assigns ip address for PC clients in ---!
Sales Dept. Cat-3560(dhcp-config)#exit
Cat-3560(config)#ip dhcp excluded-address 172.16.3.1
Cat-3560(config)#ip dhcp excluded-address 172.16.4.1
Cat-3560(config)#ip dhcp excluded-address 172.16.5.1

```

```

Cat-3560(config)#aaa new-model
Cat-3560(config)#aaa authentication dot1x default group
radius
Method list should be default. Otherwise dot1x does ---!
not work. Cat-3560(config)#aaa authorization network
default group radius
You need authorization for dynamic VLAN assignment ---!
to work with RADIUS. Cat-3560(config)#radius-server host
172.16.2.201 key CisCo123
The key must match the key used on the RADIUS ---!
server. Cat-3560(config)#dot1x system-auth-control
Globally enables 802.1x. Cat-3560(config)#interface ---!
range fastEthernet 0/1 - 4
Cat-3560(config-if-range)#no shut
Cat-3560(config-if-range)#^Z
Cat-3560#show vlan

```

VLAN Name	Status	Ports
default	active	Fa0/1, 1 Fa0/2, Fa0/3, Fa0/4
Fa0/5,		Fa0/6, Fa0/7, Fa0/8
Fa0/9,		Fa0/10, Fa0/11, Fa0/12
Fa0/13,		Fa0/14, Fa0/15, Fa0/16
Fa0/17,		Fa0/18, Fa0/19, Fa0/20
Fa0/21,		Fa0/22, Fa0/23, Gi0/1
Gi0/2		
SERVER	active	Fa0/24 2
VOICE	active	Fa0/1, 3 Fa0/4
MARKETING	active	4
SALES	active	5
GUEST_and_AUTHFAIL	active	6
fddi-default	act/unsup	1002
token-ring-default	act/unsup	1003
fddinet-default	act/unsup	1004
trnet-default	act/unsup	1005

ملاحظة: أستخدم أداة بحث الأوامر (للعلماء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

RADIUS خادم تكوين

تم تكوين خادم RADIUS باستخدام عنوان IP ثابت بقيمة 24/172.16.2.201. أكمل الخطوات التالية لتكوين خادم RADIUS لعمل AAA:

1. انقر فوق تكوين الشبكة على نافذة إدارة ACS لتكوين عميل AAA.
2. انقر فوق إضافة إدخال ضمن قسم عملاء AAA.

Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration**
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Personal Posture

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using

None Defined

Add Entry Search

AAA Servers		
AAA Server Name	AAA Server IP Address	AAA Server Type
CCM-4	172.16.2.201	CiscoSecure ACS

3. قم بتكوين اسم مضيف عميل AAA وعنوان IP والمفتاح السري المشترك ونوع المصادقة كما يلي: اسم مضيف عميل AAA = اسم المضيف للمحول (CAT-3560). عنوان IP لعميل AAA = عنوان IP لواجهة الإدارة للمحول (172.16.2.1). Shared Secret = مفتاح RADIUS الذي تم تكوينه على المحول (CisCo123). ملاحظة: لإجراء العملية الصحيحة، يجب أن يكون المفتاح السري المشترك مطابقاً على عميل AAA و ACS. المفاتيح حساسة لحالة الأحرف. المصادقة باستخدام RADIUS (Cisco IOS/PIX 6.0). ملاحظة: تتوفر سمة زوج سمة-قيمة (AV) من Cisco ضمن هذا الخيار.
4. انقر فوق إرسال + تطبيق لجعل هذه التغييرات فعالة، كما يوضح المثال التالي:

Add AAA Client

AAA Client Hostname

AAA Client IP Address

Shared Secret

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format ASCII Hexadecimal

Authenticate Using

- 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

إعداد المجموعة

ارجع إلى هذا الجدول لتكوين خادم RADIUS للمصادقة.

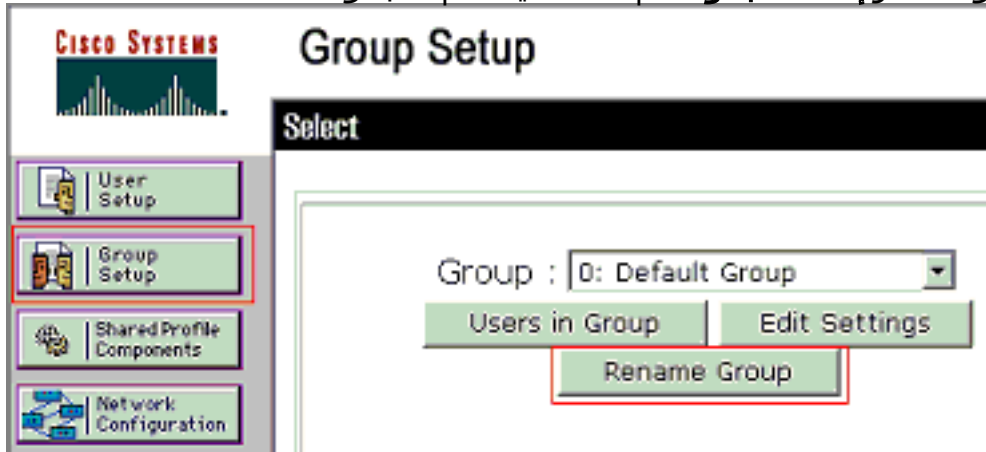
تجمع DHCP	VLAN	كلمة المرور	مستعمل	مجموعة	ديت	في المتال التالي
تسويق	تسويق	Cisco	mkt-manager	تسويق	تسويق	إم-1
تسويق	تسويق	شركة MScisco	طاقم القيادة	تسويق	تسويق	إم-2
المبيعات	المبيعات	Cisco	مدير المبيعات	المبيعات	المبيعات	إس-2
المبيعات	المبيعات	Cisco	موظفو	المبيعات	المبيعات	إس-

			المبيعات			1
هواتف بروتوكول الإنترنت	الصوت	P1Cisco	cp-7970g-sep001759e7492c	هواتف بروتوكول الإنترنت	التسويق	ف-1
هواتف بروتوكول الإنترنت	الصوت	P2Cisco	cp-7961g-sep001a2f80381f	هواتف بروتوكول الإنترنت	المبيعات	ف-2

قم بإنشاء مجموعات للعملاء الذين يتصلون بشبكات VLAN أرقام 3 (الصوت) و 4 (التسويق) و 5 (المبيعات). هنا، يتم إنشاء مجموعات هواتف IP والتسويق والمبيعات لهذا الغرض.

ملاحظة: هذا هو تكوين مجموعات التسويق و هواتف IP. لتكوين مجموعة المبيعات، أكمل خطوات مجموعة التسويق.

1. لإنشاء مجموعة، اختر إعداد المجموعة ثم أعد تسمية اسم المجموعة




الافتراضي.

2. اخترت in order to شكلت مجموعة، المجموعة من القائمة وطققة يحرر عملية



إعداد

3. قم بتعريف تعيين عنوان IP للعميل كمعين بواسطة تجمع عملاء AAA. أدخل اسم تجمع عناوين IP الذي تم تكوينه على المحول لعملاء هذه



Group Setup

Jump To Access Restrictions

IP Assignment ?


No IP address assignment
 Assigned by dialup client
 Assigned from AAA Client pool

ملاحظة

المجموعة.

: أختار هذا الخيار واكتب اسم تجمع IP لعميل AAA في المربع، فقط إذا كان لهذا المستخدم أن يتم تعيين عنوان IP بواسطة تجمع عناوين IP تم تكوينه على عميل AAA. ملاحظة: بالنسبة لتكوين مجموعة هواتف IP فقط، تجاوز الخطوة التالية، الخطوة 4، وانتقل إلى الخطوة 5.

4. قم بتعريف سمات فريق عمل هندسة الإنترنت (64 IETF) و65 و81 ثم انقر فوق إرسال + إعادة تشغيل. تأكد من أن علامات تمييز القيم يتم ضبطها على 1، كما يوضح هذا المثال. يتجاهل Catalyst أي علامة أخرى غير 1. in order to عينت مستعمل إلى VLAN خاص، أنت ينبغي أيضا عينت سمة 81 مع VLAN / اسم أو VLAN رقم أن يماثل. ملاحظة: إذا كنت تستخدم اسم شبكة VLAN، فيجب أن يكون هو نفسه تماما مثل الذي تم تكوينه في



Group Setup

Jump To Access Restrictions

IETF RADIUS Attributes ?

[064] Tunnel-Type
 Tag 1 Value VLAN
 [065] Tunnel-Medium-Type
 Tag 1 Value 802
 [081] Tunnel-Private-Group-ID
 Tag 1 Value MARKETING

[Back to Help](#)

ملاحظة:

المحول.

راجع RFC 2868: سمات RADIUS لدعم بروتوكول النفق للحصول على مزيد من المعلومات حول سمات IETF هذه. ملاحظة: في التكوين الأولي لخادم ACS، يمكن أن تفشل سمات IETF RADIUS في العرض في إعداد المستخدم. لتمكين سمات IETF في شاشات تكوين المستخدم، اختر تكوين الواجهة < RADIUS IETF)). بعد ذلك، تحقق من السمات 64 و65 و81 في أعمدة المستخدم والمجموعة. ملاحظة: إذا لم يتم تحديد سمة 81 IETF وكان المنفذ منفذ محول في وضع الوصول، فسيتم تخصيص العميل لشبكة VLAN الخاصة بالوصول الخاصة بالمنفذ. إذا قمت بتعريف السمة 81 للتعين الديناميكي لشبكة VLAN وكان المنفذ منفذ محول في وضع الوصول، فأنت بحاجة إلى إصدار الأمر AAA authorization network default group radius على المحول. يعين هذا أمر الميناء إلى ال VLAN أن ال RADIUS نادل يزيد. وإلا، فإن 802.1x ينقل المنفذ إلى الدولة بعد مصادقة المستخدم؛ ولكن المنفذ لا يزال في شبكة VLAN الافتراضية للمنفذ، ويمكن أن يفشل الاتصال. ملاحظة: تنطبق الخطوة التالية فقط على مجموعة هواتف بروتوكول الإنترنت.

5. قم بتكوين خادم RADIUS لإرسال سمة زوج (AV) سمة سمة سمة-قيمة Cisco لتحويل جهاز صوتي. وبدون ذلك، يتعامل المحول مع جهاز الصوت كجهاز بيانات. قم بتعريف سمة زوج سمة-قيمة (AV) من Cisco بقيمة device-traffic-class=voice وانقر إرسال + إعادة

The screenshot shows the Cisco Group Setup configuration page. The 'Group Setup' section is active, and the 'IP Assignment' is set to 'Assigned from AAA Client pool' with the value 'IP-Phones'. The 'Cisco IOS/PIX 6.x RADIUS Attributes' section has the attribute '[009\001] cisco-av-pair' checked, with the value 'device-traffic-class=voice' entered in the text box. Other attributes like 'cisco-h323-credit-amount', 'cisco-h323-credit-time', and 'cisco-h323-return-code' are unchecked. The 'Submit + Restart' button is highlighted with a red box.

تشغيل.

إعداد المستخدم

أكمل هذه الخطوات لإضافة مستخدم وتكوينه.

1. اخترت in order to أضفت وشكلت مستعمل، مستعمل setup. دخلت ال username وطققة



User Setup

Select



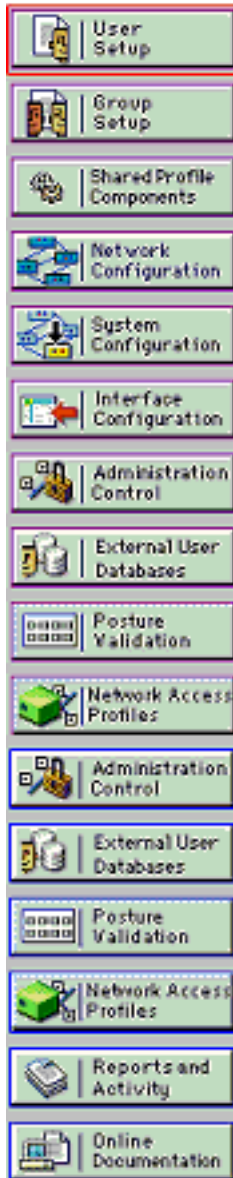
User:

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

يضيف/يحرر

2. قم بتعريف اسم المستخدم وكلمة المرور والمجموعة



User: mkt-manager (New User)

Account Disabled

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)

Password: *****
 Confirm Password: *****

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Marketing

Callback

Use group setting

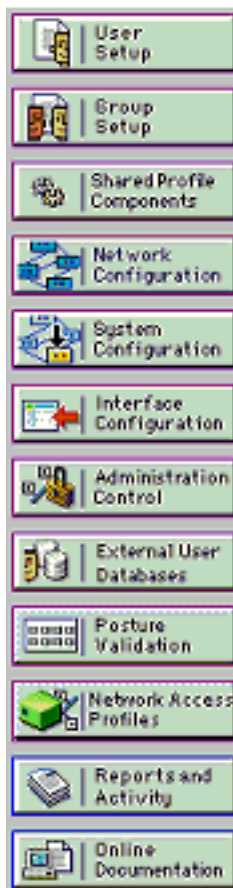
Submit

Delete

Cancel

للمستخدم.

- يستخدم هاتف IP معرف الجهاز الخاص به كاسم مستخدم والسر المشترك ككلمة مرور للمصادقة. يجب أن تتطابق هذه القيم مع خادم RADIUS. بالنسبة لهواتف IP P-1 و P-2، قم بإنشاء أسماء مستخدمين مثل معرف الجهاز وكلمة المرور الخاصين به مثل معرف الجهاز المشترك الذي تم تكوينه. راجع قسم [تكوين هواتف IP لاستخدام قسم مصادقة 802.1x](#) للحصول على مزيد من المعلومات حول معرف الجهاز والسر المشترك



User: CP-7961G-SEP001A2F80381F

Account Disabled

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)

Password *****

Confirm Password *****

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

IP Phones

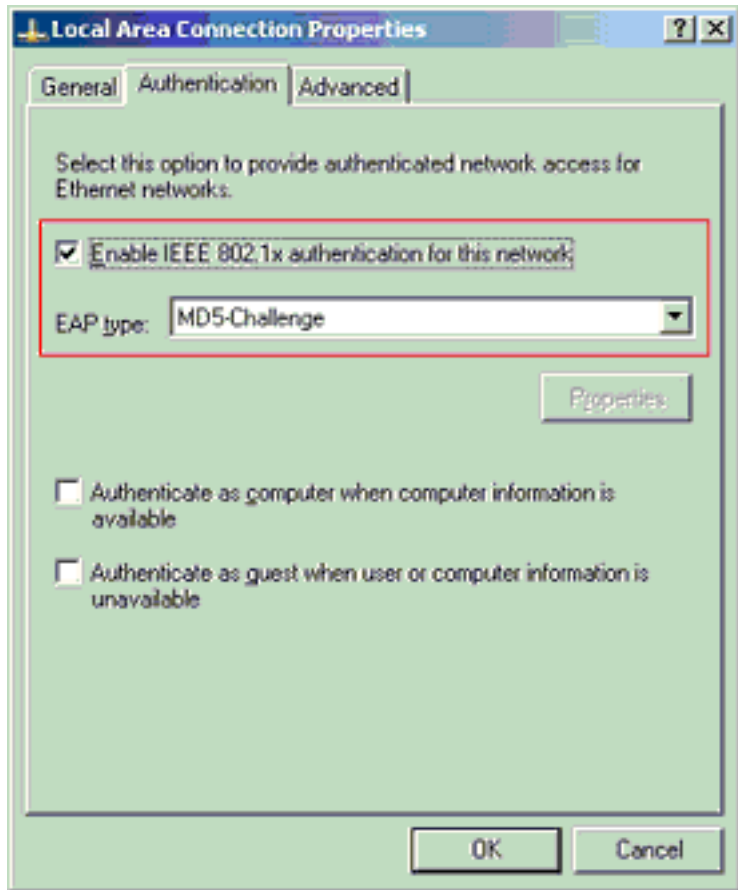
Submit Delete Cancel

على هاتف IP.

قم بتكوين عملاء الكمبيوتر لاستخدام مصادقة 802.1x

هذا المثال خاص بعميل بروتوكول المصادقة المتوسع (EAP) لـ Microsoft Windows XP عبر شبكة LAN ((EAPOL:

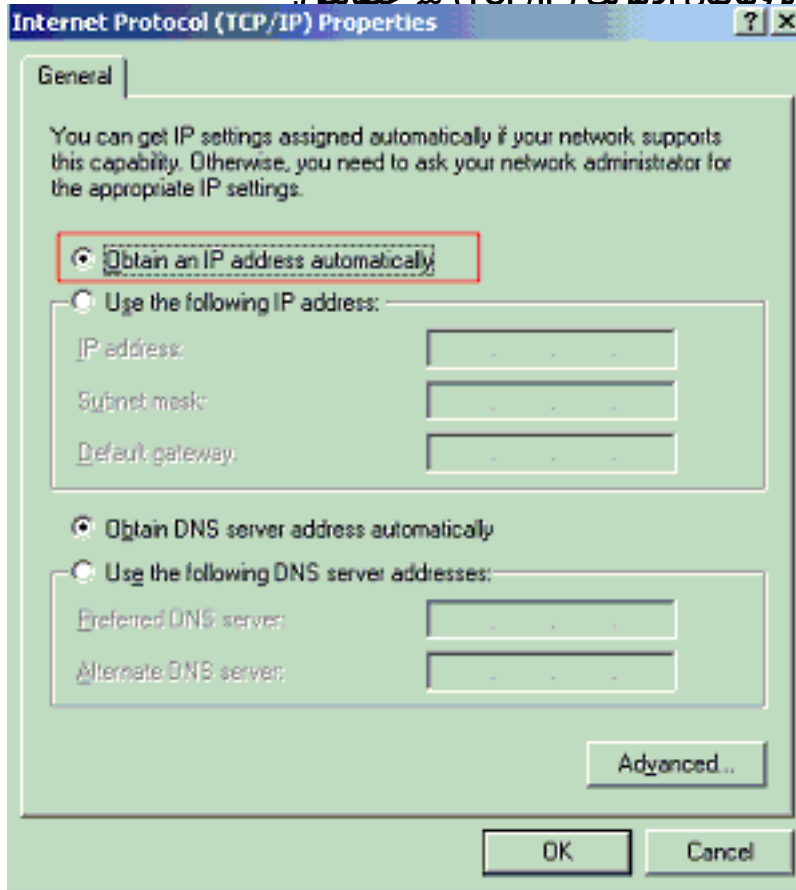
1. اختر ابدأ < لوحة التحكم < اتصالات الشبكة، ثم انقر بزر الماوس الأيمن فوق اتصال المنطقة المحلية واختر الخصائص.
2. تحقق من رمز العرض في منطقة الإعلام عند إتصاله ضمن علامة التبويب "عام".
3. تحت علامة تبويب المصادقة، تحقق من تمكين مصادقة IEEE 802.1x لهذه الشبكة.
4. ثبت ال EAP نوع إلى MD5-challenge، بما أن هذا مثال



يوضح:

أتمت هذا steps in order to شكلت الزبون أن يحصل العنوان من DHCP نادل.

1. أختار ابدأ < لوحة التحكم > إتصالات الشبكة، ثم انقر بزر الماوس الأيمن فوق اتصال المنطقة المحلية واختر الخصائص.
2. تحت علامة التبويب "عام"، انقر فوق **بوتوكول الإنترنت (TCP/IP)** ثم خصائص.



3. أختار الحصول على عنوان IP تلقائياً.

قم بتكوين هواتف IP لاستخدام مصادقة 802.1x

أكمل هذه الخطوات لتكوين هواتف IP لمصادقة 802.1x.

1. اضغط على زر الإعدادات للوصول إلى إعدادات مصادقة 802.1X واختر تكوين التأمين < مصادقة 802.1X > مصادقة الجهاز.
2. قم بتعيين خيار مصادقة الجهاز إلى ممكن.
3. اضغط على برنامج حفظ.
4. اختر مصادقة EAP-MD5 < 802.1X > سر مشترك لتعيين كلمة مرور على الهاتف.
5. أدخل السر المشترك واضغط على حفظ. ملاحظة: يجب أن تتراوح كلمة المرور بين ستة و 32 حرفاً، والتي تتكون من أي مجموعة من الأرقام أو الحروف. رسالة أبدت وكلمة مرور لا ينفذ إن هذا شرط لا يفى. ملاحظة: إذا قمت بتعطيل مصادقة 802.1X أو قمت بإعادة ضبط المصنع على الهاتف، فسيتم حذف سر MD5 المشترك الذي تم تكوينه مسبقاً. ملاحظة: يتعذر تكوين الخيارات الأخرى ومعرف الجهاز والنطاق. يتم استخدام معرف الجهاز كاسم مستخدم لمصادقة 802.1x. هذا مشتق من رقم نموذج الهاتف وعنوان MAC الفريد المعروض بهذا التنسيق: <MAC>-SEP-<model>-cp. على سبيل المثال، CP-7970G-SEP001759E7492C. راجع إعدادات مصادقة 802.1X للحصول على مزيد من المعلومات. أتمت هذا steps in order to شكلت ال ip هاتف أن يحصل العنوان من DHCP نادل.

1. اضغط على زر الإعدادات للوصول إلى إعدادات تكوين الشبكة واختر تكوين الشبكة.
2. إلغاء تأمين خيارات تكوين الشبكة. لإلغاء التأمين، اضغط على ***. ملاحظة: لا تضغط على *** لإلغاء تأمين الخيارات ثم اضغط على الفور *** مرة أخرى لتأمين الخيارات. يفسر الهاتف هذا التسلسل على أنه ***، الذي يعيد ضبط الهاتف. لتأمين الخيارات بعد إلغاء تأمينها، انتظر 10 ثوان على الأقل قبل أن تضغط على *** مرة أخرى.
3. قم بالتمرير إلى الخيار تمكين DHCP واضغط برنامج نعم لتمكين DHCP.
4. اضغط على برنامج حفظ.

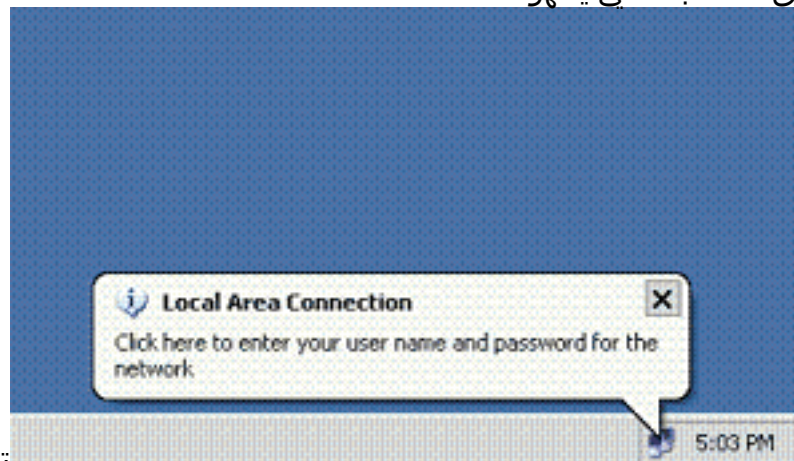
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

أجهزة الكمبيوتر العملية

إذا قمت بإكمال التكوين بشكل صحيح، فسيعرض عملاء الكمبيوتر الشخصي مطالبة منبثقة لإدخال اسم مستخدم وكلمة مرور.

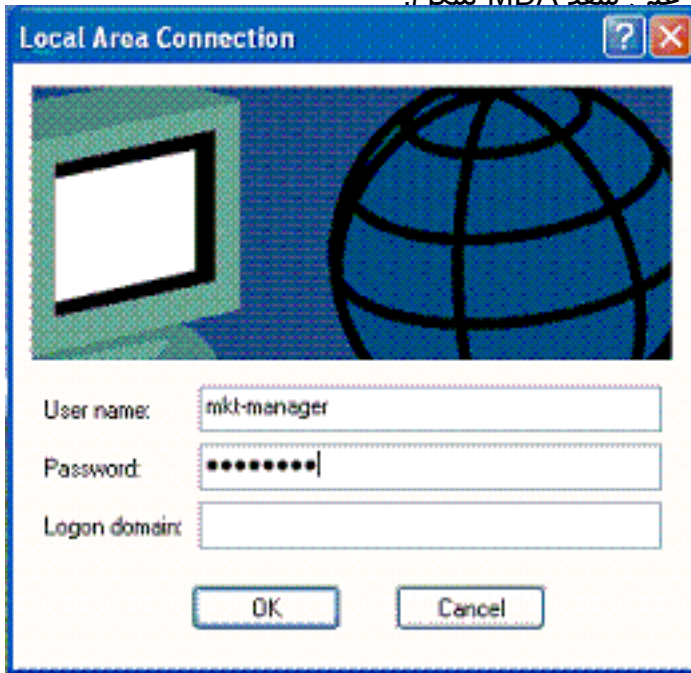
1. انقر فوق المطالبة، التي يظهرها هذا



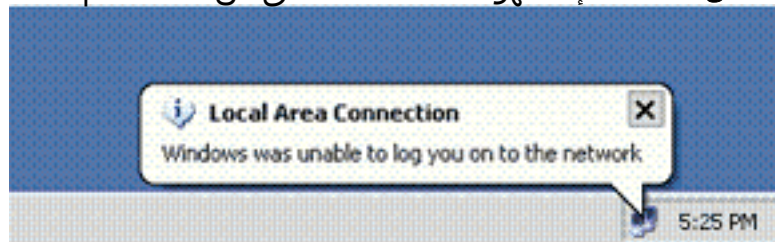
تظهر نافذة إدخال اسم المستخدم

المثال:

وكلمة المرور. ملاحظة: لا يفرض MDA ترتيب مصادقة الجهاز. ولكن، للحصول على أفضل النتائج، توصي Cisco بمصادقة جهاز صوت قبل جهاز بيانات على منفذ MDA يمكن.



2. أدخل اسم المستخدم وكلمة المرور.
3. إذا لم تظهر رسائل خطأ، فتتحقق من الاتصال بالطرق المعتادة، مثل من خلال الوصول إلى موارد الشبكة ومع اختبار الاتصال. ملاحظة: إذا ظهر هذا الخطأ، فتتحقق من صحة اسم المستخدم وكلمة



المرون:

هواتف بروتوكول الإنترنت

تتيح قائمة حالة المصادقة 802.1X في هواتف IP إمكانية مراقبة حالة المصادقة.

1. اضغط على زر الإعدادات للوصول إلى حالات مصادقة 802.1X في الوقت الفعلي واختر تكوين التأمين < حالة مصادقة 802.1X.
2. يجب أن تكون حالة الحركة مصدق عليها. راجع حالة مصادقة 802.1X في الوقت الفعلي للحصول على مزيد من المعلومات. ملاحظة: يمكن أيضا التحقق من حالة المصادقة من الإعدادات < الحالة < رسائل الحالة.

محول من الطبقة 3

إن يظهر الكلمة واسم مستعمل أن يكون صحيح، دقت ال 802.1x ميناء دولة على المفتاح.

.1

ابحث عن حالة المنفذ التي تشير إلى .

Cat-3560#show dot1x all summary

Interface	PAE	Client	Status
Fa0/1	AUTH	0016.3633.339c	AUTHORIZED
0017.59e7.492c	AUTHORIZED		
Fa0/2	AUTH	0014.5e94.5f99	AUTHORIZED
Fa0/3	AUTH	0011.858D.9AF9	AUTHORIZED
Fa0/4	AUTH	0016.6F3C.A342	AUTHORIZED
001a.2f80.381f	AUTHORIZED		

Cat-3560#show dot1x interface fastEthernet 0/1 details

```
Dot1x Info for FastEthernet0/1
-----
PAE                               = AUTHENTICATOR
PortControl                       = AUTO
ControlDirection                 = Both
HostMode                         = MULTI_DOMAIN
ReAuthentication                 = Enabled
QuietPeriod                      = 10
ServerTimeout                   = 30
SuppTimeout                      = 30
(ReAuthPeriod)                  = 60 (Locally configured)
ReAuthMax                       = 2
MaxReq                          = 2
TxPeriod                        = 30
RateLimitPeriod                 = 0
Auth-Fail-Vlan                  = 6
Auth-Fail-Max-attempts          = 2
Guest-Vlan                      = 6
```

Dot1x Authenticator Client List

```
-----
Domain                           = DATA
Supplicant                       = 0016.3633.339c
Auth SM State                    = AUTHENTICATED
Auth BEND SM State               = IDLE
Port Status                      = AUTHORIZED
ReAuthPeriod                    = 60
ReAuthAction                    = Reauthenticate
TimeToNextReauth                = 29
Authentication Method           = Dot1x
Authorized By                    = Authentication Server
Vlan Policy                      = 4
```

```
Domain                           = VOICE
Supplicant                       = 0017.59e7.492c
Auth SM State                    = AUTHENTICATED
Auth BEND SM State               = IDLE
Port Status                      = AUTHORIZED
ReAuthPeriod                    = 60
ReAuthAction                    = Reauthenticate
TimeToNextReauth                = 15
Authentication Method           = Dot1x
Authorized By                    = Authentication Server
```

تحقق من حالة شبكة VLAN بعد المصادقة الناجحة.

Cat-3560#show vlan

VLAN Name	Status	Ports
default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Gi0/1 Gi0/2		1
SERVER	active	Fa0/24
VOICE	active	Fa0/1, Fa0/4
MARKETING	active	Fa0/1, Fa0/2
SALES	active	Fa0/3, Fa0/4
GUEST_and_AUTHFAIL	active	6
fddi-default	act/unsup	1002

```
token-ring-default      act/unsup 1003
fddinet-default         act/unsup 1004
trnet-default           act/unsup 1005
```

.Output suppressed ---!

2. تحقق من حالة ربط DHCP بعد مصادقة ناجحة.

```
Router#show ip dhcp binding
IP address      Hardware address      Lease expiration      Type
e749.2c         Aug 24 2007 06:35 AM  Automatic.0100.1759   172.16.3.2
0100.1a2f.8038.1f Aug 24 2007 06:43 AM  Automatic              172.16.3.3
0100.1636.3333.9c Aug 24 2007 06:50 AM  Automatic              172.16.4.2
0100.145e.945f.99 Aug 24 2007 08:17 AM  Automatic              172.16.4.3
0100.166F.3CA3.42 Aug 24 2007 08:23 AM  Automatic              172.16.5.2
0100.1185.8D9A.F9 Aug 24 2007 08:51 AM  Automatic              172.16.5.3
```

تدعم أداة مترجم الإخراج (للعملاء المسجلين فقط) بعض أوامر **show**. استعملت ال OIT in order to شاهدت تحليل من عرض أمر إنتاج.

استكشاف الأخطاء وإصلاحها

فشل مصادقة هاتف IP

تعرض حالة هاتف IP أو في حالة فشل مصادقة 802.1x. أتمت هذا steps in order to تحريرت هذا إصدار:

- تأكد من تمكين 802.1x على هاتف IP.
- تحقق من إدخال معرف الجهاز على خادم المصادقة (RADIUS) كاسم مستخدم.
- تأكد من تكوين السر المشترك على هاتف IP.
- إذا تم تكوين السر المشترك، فتتحقق من أن لديك نفس السر المشترك الذي تم إدخاله على خادم المصادقة.
- تحقق من تكوين الأجهزة الأخرى المطلوبة بشكل صحيح، على سبيل المثال، المحول وخادم المصادقة.

معلومات ذات صلة

- [تكوين المصادقة المستندة إلى المنفذ IEEE 802.1x](#)
- [قم بتكوين هاتف IP لاستخدام مصادقة 802.1x](#)
- [إرشادات لنشر مصدر المحتوى الإضافي الآمن من Cisco لخوادم Windows NT/2000 في بيئة محول Cisco Catalyst Switch](#)
- [المعيار RFC 2868: سمات بروتوكول RADIUS لدعم بروتوكول النفق](#)
- [مصادقة IEEE 802.1x مع Catalyst 6500/6000 التي تشغل مثال تكوين برنامج Cisco IOS Software](#)
- [مصادقة IEEE 802.1x مع Catalyst 6500/6000 التي تشغل مثال تكوين البرنامج CatOS Software](#)
- [صفحات دعم منتجات شبكة LAN](#)
- [صفحة دعم تحويل شبكة LAN](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إلل دن تسمل