مصادقة IEEE 802.1x مع Catalyst 6500/6000 التي تشغل برنامج CatOS مثال تكوين Software

المحتويات

المقدمة

يشرح هذا المستند كيفية تكوين IEEE 802.1x على محول Catalyst 6500/6000 يعمل في الوضع المختلط (CatOS على Supervisor Engine (المحرك المشرف) وبرنامج Cisco IOS® على MSFC) وخادم خدمة طلب اتصال المستخدم البعيد (RADIUS) للمصادقة وتعيين VLAN.

المتطلبات الأساسية

المتطلبات

يجب أن يكون لدى قراء هذا المستند معرفة بالمواضيع التالية:

- دليل تثبيت Cisco Secure ACS ل Windows 4.1
- دليل المستخدم لخادم التحكم في الوصول الآمن من Cisco، الإصدار 4.1
- كيف يعمل RADIUS؟
- دليل نشر تحويل Catalyst و ACS

المكونات المستخدمة

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

- مادة حفازة 6500 أن يركض CatOS برمجية إطلاق 8.5(6) على المشرف محرك و cisco ios برمجية إطلاق 12.2(18)sxf على ال MSFC**ملاحظة:** تحتاج إلى الإصدار 6.2 من CatOS أو إصدار أحدث لدعم المصادقة المستندة إلى المنفذ 802.1x.**ملاحظة:** قبل إصدار البرنامج 7.2(2)، بمجرد مصادقة مضيف 802.1x، ينضم إلى شبكة VLAN مكونة من NVRAM. باستخدام الإصدار 7.2(2) من البرنامج والإصدارات الأحدث، بعد المصادقة، يمكن لمضيف 802.1x تلقي تعيين شبكة VLAN الخاصة به من خادم RADIUS.
- يستخدم هذا المثال خادم التحكم في الوصول الآمن (ACS 4.1) 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.

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.

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 مميزتين 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 ربطت إلى مفتاح ميناء ويعين الميناء إلى VLAN قبل أن يجعل يتوفر أي خدمة أن يكون قدمت بالمفتاح أو ال LAN. إلى أن تتم مصادقة الجهاز، يسمح التحكم في الوصول إلى 802.1x فقط لحركة مرور بروتوكول المصادقة المتوسع (EAP) عبر الشبكة المحلية (LAN) (EAPOL) من خلال المنفذ الذي يتم توصيل الجهاز به. بعد أن تكون المصادقة ناجحة، يمكن لحركة المرور العادية أن تمر عبر المنفذ.

التكوين

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

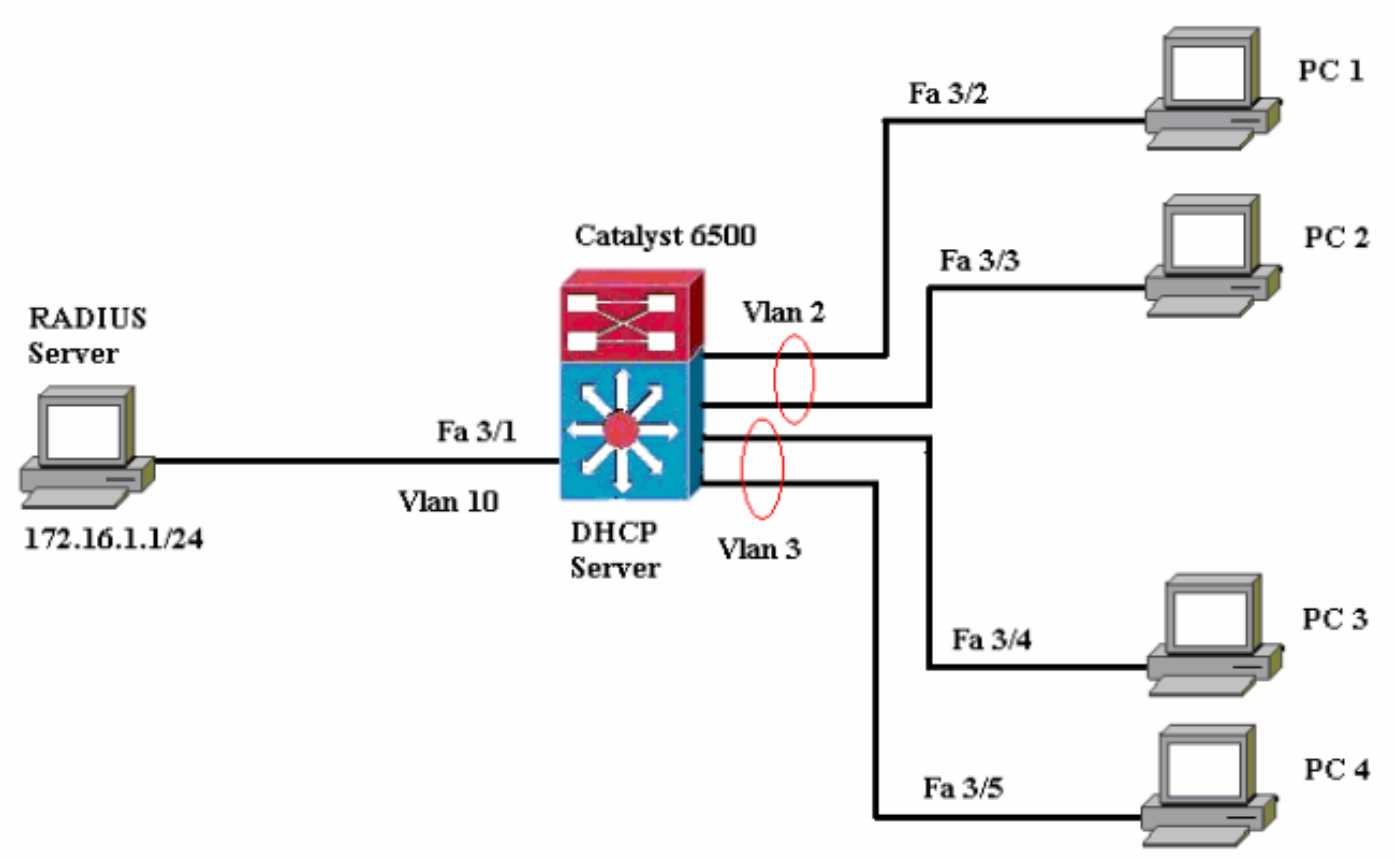
ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

يتطلب هذا التكوين الخطوات التالية:

- شكلت المادة حفازة مفتاح ل 802.1x صحة هوية
- تكوين خادم RADIUS
- قم بتكوين عملاء الكمبيوتر لاستخدام مصادقة 802.1x

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



- خادم RADIUS—يقوم بإجراء المصادقة الفعلية للعميل. يتحقق خادم RADIUS من هوية العميل ويخطر المحول بما إذا كان العميل مخولا للوصول إلى خدمات الشبكة المحلية والمحولات أم لا. هنا، شكلت ال RADIUS نادل للمصادقة و VLAN تنازل.
- المحول—يتحكم في الوصول المادي إلى الشبكة استنادا إلى حالة مصادقة العميل. ويعمل المحول كوسيط (وكيل) بين العميل وخادم RADIUS، حيث يطلب معلومات الهوية من العميل ويتحقق من هذه المعلومات باستخدام خادم RADIUS وإرسال إستجابة إلى العميل. هنا، المادة حفازة 6500 شكلت مفتاح أيضا ك DHCP نادل. يسمح دعم مصادقة 802.1x لبروتوكول التكوين الديناميكي للمضيف (DHCP) لخادم DHCP بتعيين عناوين IP إلى فئات مختلفة من المستخدمين النهائيين من خلال إضافة هوية المستخدم التي تمت مصادقتها في عملية اكتشاف DHCP.
- العملاء—الأجهزة (محطات العمل) التي تطلب الوصول إلى خدمات الشبكة المحلية (LAN) والمحولات والاستجابة للطلبات من المحول. فيما يلي، أجهزة الكمبيوتر من 1 إلى 4 هي العملاء الذين يطلبون الوصول إلى الشبكة المصادق عليها. سيستخدم PCs 1 و 2 نفس بيانات اعتماد تسجيل الدخول لتكون في شبكة VLAN رقم 2. وبالمثل، يستخدم جهازا الكمبيوتر 3 و 4 بيانات اعتماد تسجيل دخول لشبكة VLAN رقم 3. تم تكوين عملاء الكمبيوتر الشخصي للحصول على عنوان IP من خادم DHCP.**ملاحظة:** في هذا التكوين، يتم رفض أي عميل يفشل في المصادقة أو أي عميل قادر على الاتصال بالمحول ليس 802.1x الوصول إلى الشبكة عن طريق نقلهم إلى شبكة VLAN غير المستخدمة (4 VLAN أو 5) باستخدام فشل المصادقة وميزات شبكة VLAN الضيف.

شكلت المادة حفازة مفتاح ل 802.1x صحة هوية

يتضمن تكوين المحول العينة هذا:

- قم بتمكين مصادقة 802.1x والميزات المقترنة على منافذ FastEthernet.
- قم بتوصيل خادم RADIUS بشبكة VLAN رقم 10 خلف منفذ FastEthernet رقم 1/3.
- تكوين خادم DHCP لمجموعتي IP، واحدة للعملاء في شبكة VLAN رقم 2 وأخرى للعملاء في شبكة VLAN رقم 3.

• التوجيه بين شبكات VLAN للحصول على اتصال بين العملاء بعد المصادقة.

ارجع إلى إرشادات تكوين المصادقة للحصول على الإرشادات حول كيفية تكوين مصادقة 802.1x.

ملاحظة: تأكد من اتصال خادم RADIUS دائما خلف منفذ معتمد.

Catalyst 6500

```
Console (enable) set system name Cat6K
.System name set
Sets the hostname for the switch. Cat6K> (enable) ---!
set localuser user admin password cisco
.Added local user admin
Cat6K> (enable) set localuser authentication enable
LocalUser authentication enabled
Uses local user authentication to access the ---!
switch. Cat6K> (enable) set vtp domain cisco
VTP domain cisco modified
Domain name must be configured for VLAN ---!
configuration. Cat6K> (enable) set vlan 2 name VLAN2
,VTP advertisements transmitting temporarily stopped
.and will resume after the command finishes
Vlan 2 configuration successful
VLAN should be existing in the switch !--- for a ---!
successsful authentication. Cat6K> (enable) set vlan 3
name VLAN3
,VTP advertisements transmitting temporarily stopped
.and will resume after the command finishes
Vlan 3 configuration successful
VLAN names will be used in RADIUS server for VLAN ---!
assignment. Cat6K> (enable) set vlan 4 name
AUTHFAIL_VLAN
,VTP advertisements transmitting temporarily stopped
.and will resume after the command finishes
Vlan 4 configuration successful
A VLAN for non-802.1x capable hosts. Cat6K> ---!
(enable) set vlan 5 name GUEST_VLAN
,VTP advertisements transmitting temporarily stopped
.and will resume after the command finishes
Vlan 4 configuration successful
A VLAN for failed authentication hosts. Cat6K> ---!
(enable) set vlan 10 name RADIUS_SERVER
,VTP advertisements transmitting temporarily stopped
.and will resume after the command finishes
Vlan 10 configuration successful
This is a dedicated VLAN for the RADIUS Server. ---!
Cat6K> (enable) set interface sc0 10 172.16.1.2
255.255.255.0
.Interface sc0 vlan set, IP address and netmask set
Note: 802.1x authentication always uses the !--- ---!
sc0 interface as the identifier for the authenticator !-
.-- when communicating with the RADIUS server

Cat6K> (enable) set vlan 10 3/1
.VLAN 10 modified
.VLAN 1 modified
 VLAN  Mod/Ports
---------------------- ----
                       3/1    10
Assigns port connecting to RADIUS server to VLAN ---!
10. Cat6K> (enable) set radius server 172.16.1.1 primary
with auth-port 1812 acct-port 1813 172.16.1.1
```

```
.added to radius server table as primary server
Sets the IP address of the RADIUS server. Cat6K> ---!
(enable) set radius key cisco
Radius key set to cisco
The key must match the key used on the RADIUS ---!
server. Cat6K> (enable) set dot1x system-auth-control
enable
.dot1x system-auth-control enabled
Configured RADIUS servers will be used for dot1x
.authentication
Globally enables 802.1x. !--- You must specify at ---!
least one RADIUS server before !--- you can enable
802.1x authentication on the switch. Cat6K> (enable) set
port dot1x 3/2-48 port-control auto
.Port 3/2-48 dot1x port-control is set to auto
.Trunking disabled for port 3/2-48 due to Dot1x feature
.Spantree port fast start option enabled for port 3/2-48
Enables 802.1x on all FastEthernet ports. !--- This ---!
disables trunking and enables portfast automatically.
Cat6K> (enable) set port dot1x 3/2-48 auth-fail-vlan 4
Port 3/2-48 Auth Fail Vlan is set to 4
Ports will be put in VLAN 4 after three !--- failed ---!
authentication attempts. Cat6K> (enable) set port dot1x
3/2-48 guest-vlan 5
Ports 3/2-48 Guest Vlan is set to 5
Any non-802.1x capable host connecting or 802.1x !- ---!
-- capable host failing to respond to the username and
password !--- authentication requests from the
Authenticator is placed in the !--- guest VLAN after 60
seconds. !--- Note: An authentication failure VLAN is
independent !--- of the guest VLAN. However, the guest
VLAN can be the same !--- VLAN as the authentication
failure VLAN. If you do not want to !--- differentiate
between the non-802.1x capable hosts and the !---
authentication failed hosts, you can configure both
hosts to !--- the same VLAN (either a guest VLAN or an
authentication failure VLAN). !--- For more information,
refer to !--- Understanding How 802.1x Authentication
for the Guest VLAN Works. Cat6K> (enable) switch console
...Trying Router-16
.Connected to Router-16
...Type ^C^C^C to switch back
Transfers control to the routing module (MSFC). ---!
Router>enable
Router#conf t
Enter configuration commands, one per line.  End with
.CNTL/Z
Router(config)#interface vlan 10
Router(config-if)#ip address 172.16.1.3 255.255.255.0
This is used as the gateway address in RADIUS ---!
server. Router(config-if)#no shut
Router(config-if)#interface vlan 2
Router(config-if)#ip address 172.16.2.1 255.255.255.0
Router(config-if)#no shut
This is the gateway address for clients in VLAN 2. ---!
Router(config-if)#interface vlan 3
Router(config-if)#ip address 172.16.3.1 255.255.255.0
Router(config-if)#no shut
This is the gateway address for clients in VLAN 3. ---!
Router(config-if)#exit
Router(config)#ip dhcp pool vlan2_clients
Router(dhcp-config)#network 172.16.2.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.2.1
This pool assigns ip address for clients in VLAN 2. ---!
```

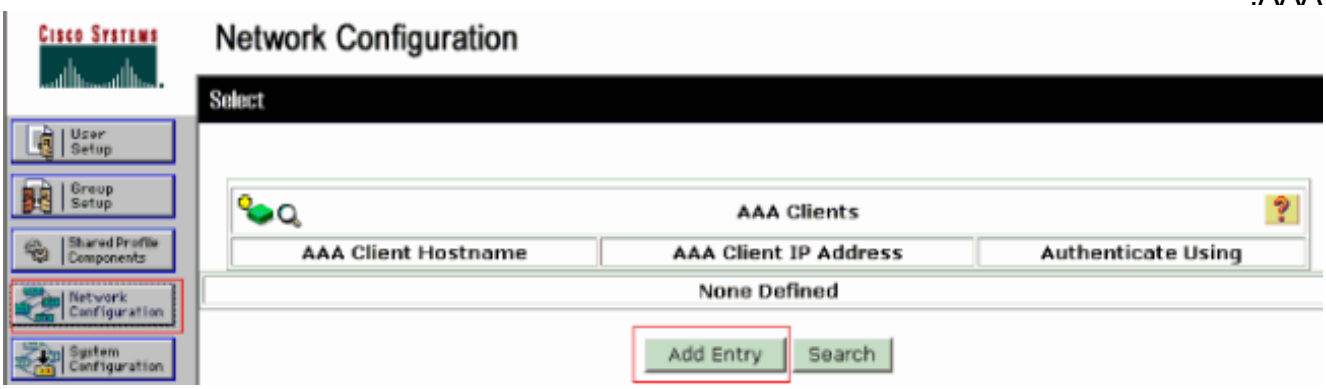
```
          Router(dhcp-config)#ip dhcp pool vlan3_clients
    Router(dhcp-config)#network 172.16.3.0 255.255.255.0
          Router(dhcp-config)#default-router 172.16.3.1
This pool assigns ip address for clients in VLAN 3. ---!
                                Router(dhcp-config)#exit
      Router(config)#ip dhcp excluded-address 172.16.2.1
      Router(config)#ip dhcp excluded-address 172.16.3.1
  In order to go back to the Switching module, !--- ---!
     enter Ctrl-C three times. Router# Router#^C Cat6K>
    (enable) Cat6K> (enable) show vlan VLAN Name Status
IfIndex Mod/Ports, Vlans ---- ------------------ -------
        -- ------- ------------------------ 1    default
                                  active    6      2/1-2

                                                   3/2-48
      VLAN2                             active    83    2
      VLAN3                             active    84    3
      AUTHFAIL_VLAN                     active    85    4
      GUEST_VLAN                        active    86    5
      RADIUS_SERVER                     active    87   10
                                                      3/1
      fddi-default                      active    78 1002
      token-ring-default                active    81 1003
      fddinet-default                   active    79 1004
      trnet-default                     active    80 1005
Output suppressed. !--- All active ports will be in ---!
       VLAN 1 (except 3/1) before authentication. Cat6K>
                                (enable) show dot1x
          PAE Capability             Authenticator Only
                        Protocol Version              1
                    system-auth-control           enabled
                            max-req                   2
                  quiet-period                 60 seconds
                re-authperiod                3600 seconds
                  server-timeout               30 seconds
                shutdown-timeout              300 seconds
                  supp-timeout                 30 seconds
                  tx-period                    30 seconds
Verifies dot1x status before authentication. Cat6K> ---!
                                                ((enable
```

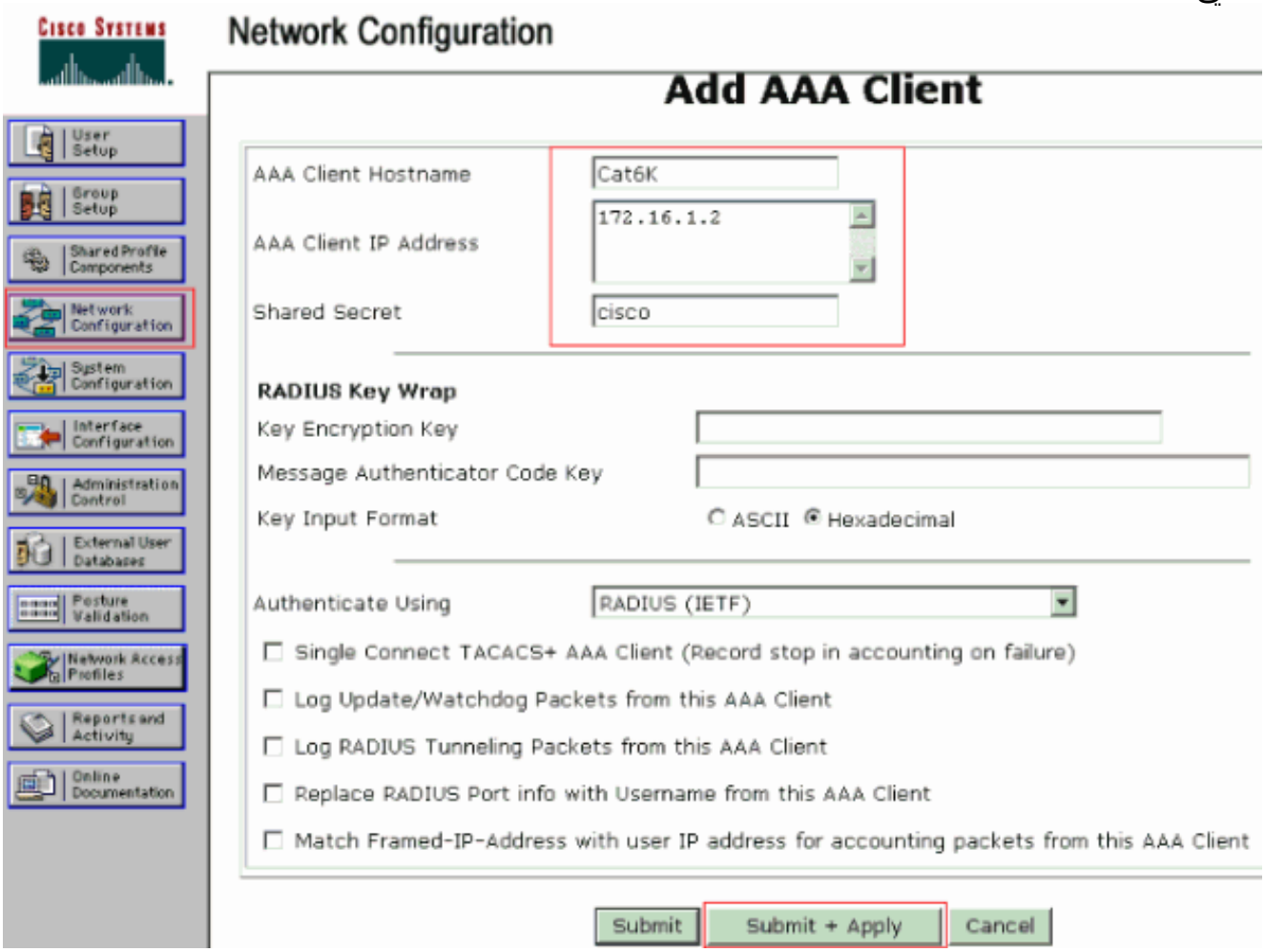
تكوين خادم RADIUS

تم تكوين خادم RADIUS باستخدام عنوان IP ثابت بقيمة 24/172.16.1.1. أكمل الخطوات التالية لتكوين خادم RADIUS لعميل AAA:

1. طقطقت in order to شكلت AAA زبون، **شبكة تشكيل** على ال ACS إدارة نافذة.
2. انقر فوق **إضافة إدخال** ضمن قسم عملاء AAA.



3. قم بتكوين اسم مضيف عميل AAA وعنوان IP والمفتاح السري المشترك ونوع المصادقة كما يلي:اسم مضيف عميل AAA = اسم المضيف للمحول (**Cat6K**).عنوان IP لعميل AAA = واجهة الإدارة (sc0)عنوان IP الخاص بالمحول (**172.16.1.2**).كلمة سر مشتركة = مفتاح RADIUS الذي تم تكوينه على المحول (**Cisco**).المصادقة باستخدام = RADIUS IETF.**ملاحظة:** لإجراء العملية الصحيحة، يجب أن يكون المفتاح السري المشترك مطابقا على عميل AAA و ACS. المفاتيح حساسة لحالة الأحرف.
4. انقر فوق **إرسال + تطبيق** لجعل هذه التغييرات فعالة، كما يوضح المثال التالي:

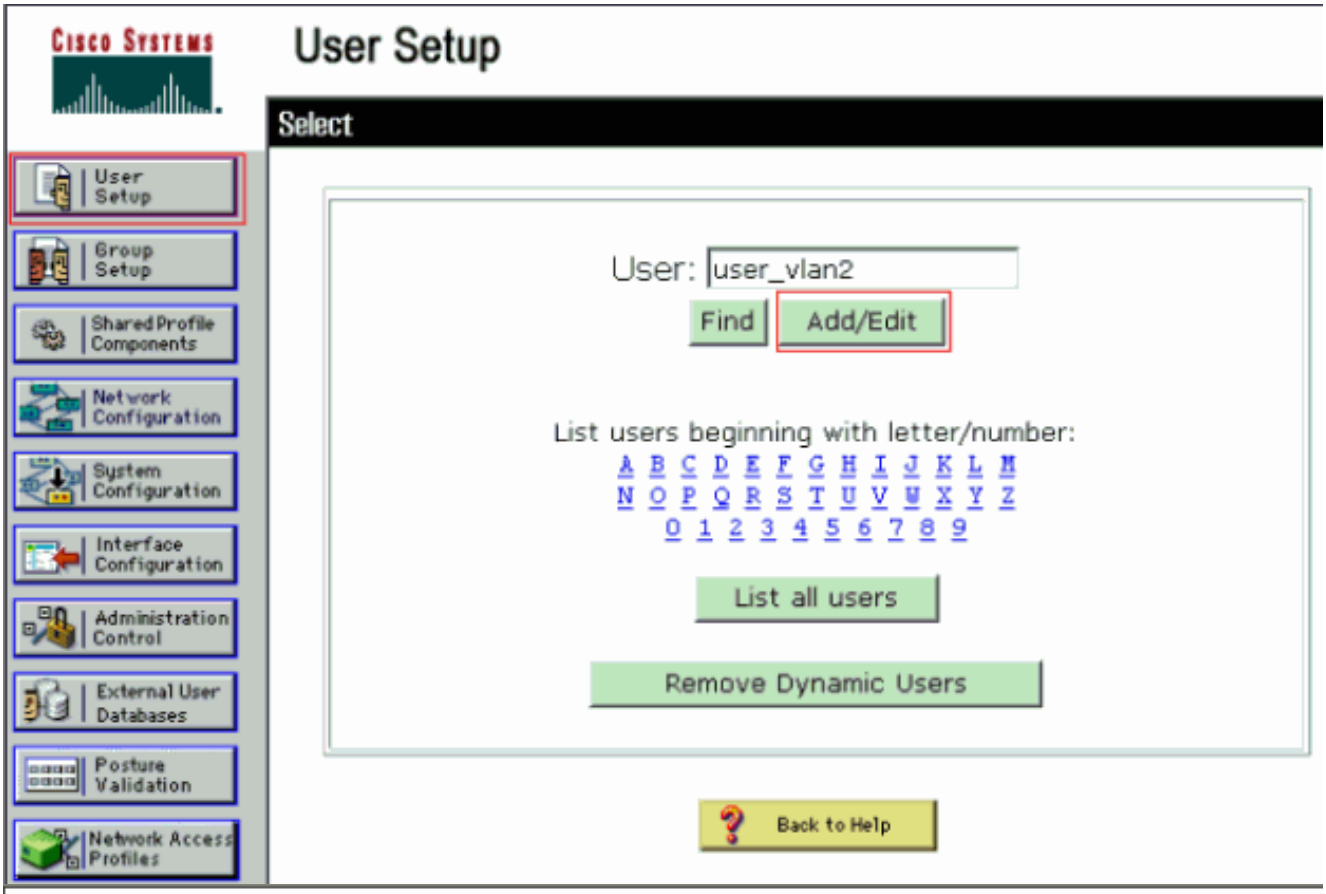


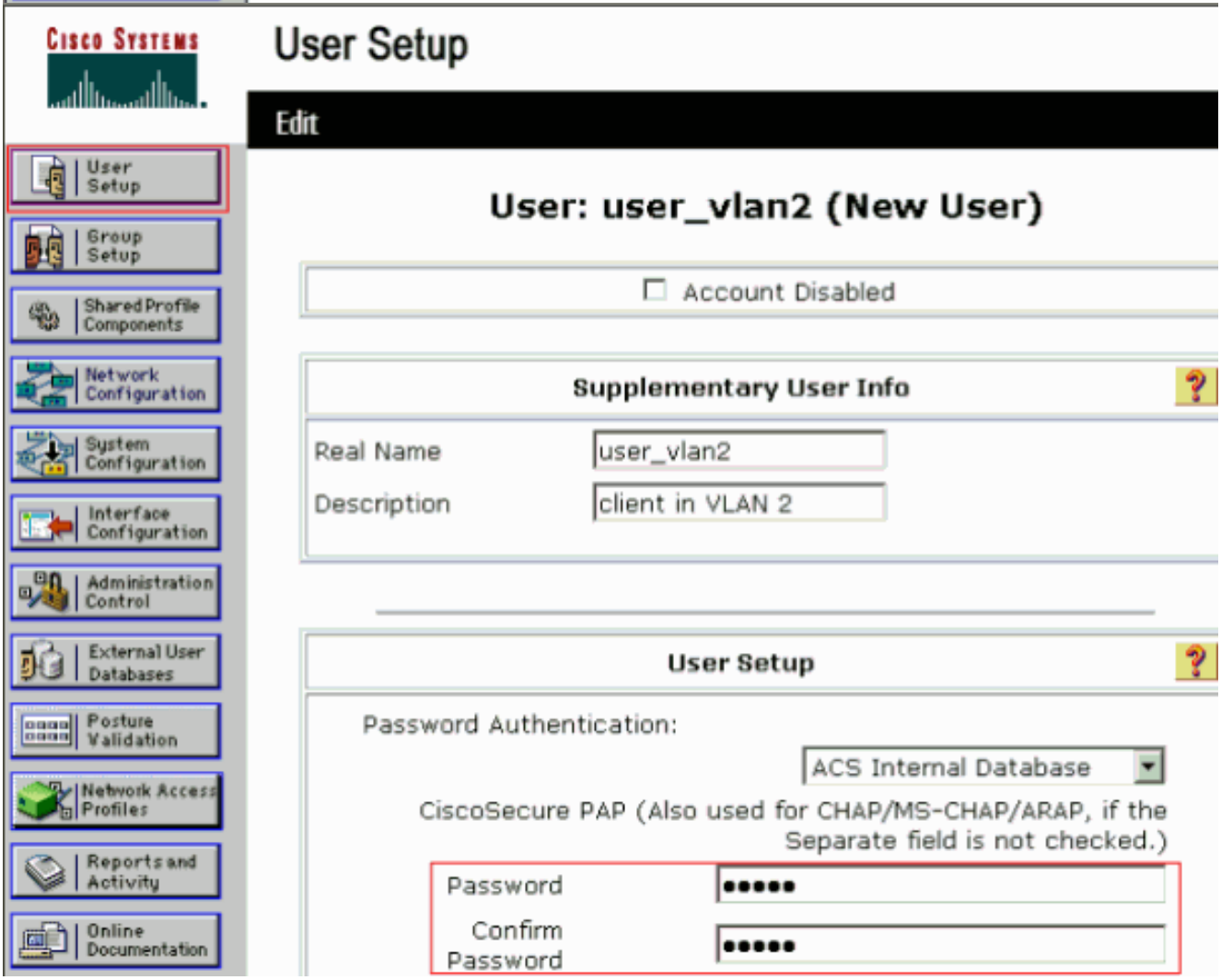
أتمت هذا steps in order to شكلت ال RADIUS نادل للمصادقة، VLAN و IP عنوان تنازل:

ينبغي خلقت إثنان مستعمل إسم بشكل مستقل لزبون أن يربط إلى VLAN 3 as well as VLAN 2. هنا، **خلقت** مستعمل_**vlan2** ل زبون يربط إلى VLAN 2 وآخر مستعمل **user_vlan3** لزبون يربط إلى VLAN 3 ل هذا الغرض.

ملاحظة: هنا، يظهر تكوين المستخدم للعملاء الذين يقومون بالاتصال بشبكة VLAN رقم 2 فقط. بالنسبة للمستخدمين الذين يقومون بالاتصال بشبكة VLAN رقم 3، أكمل الإجراء نفسه.

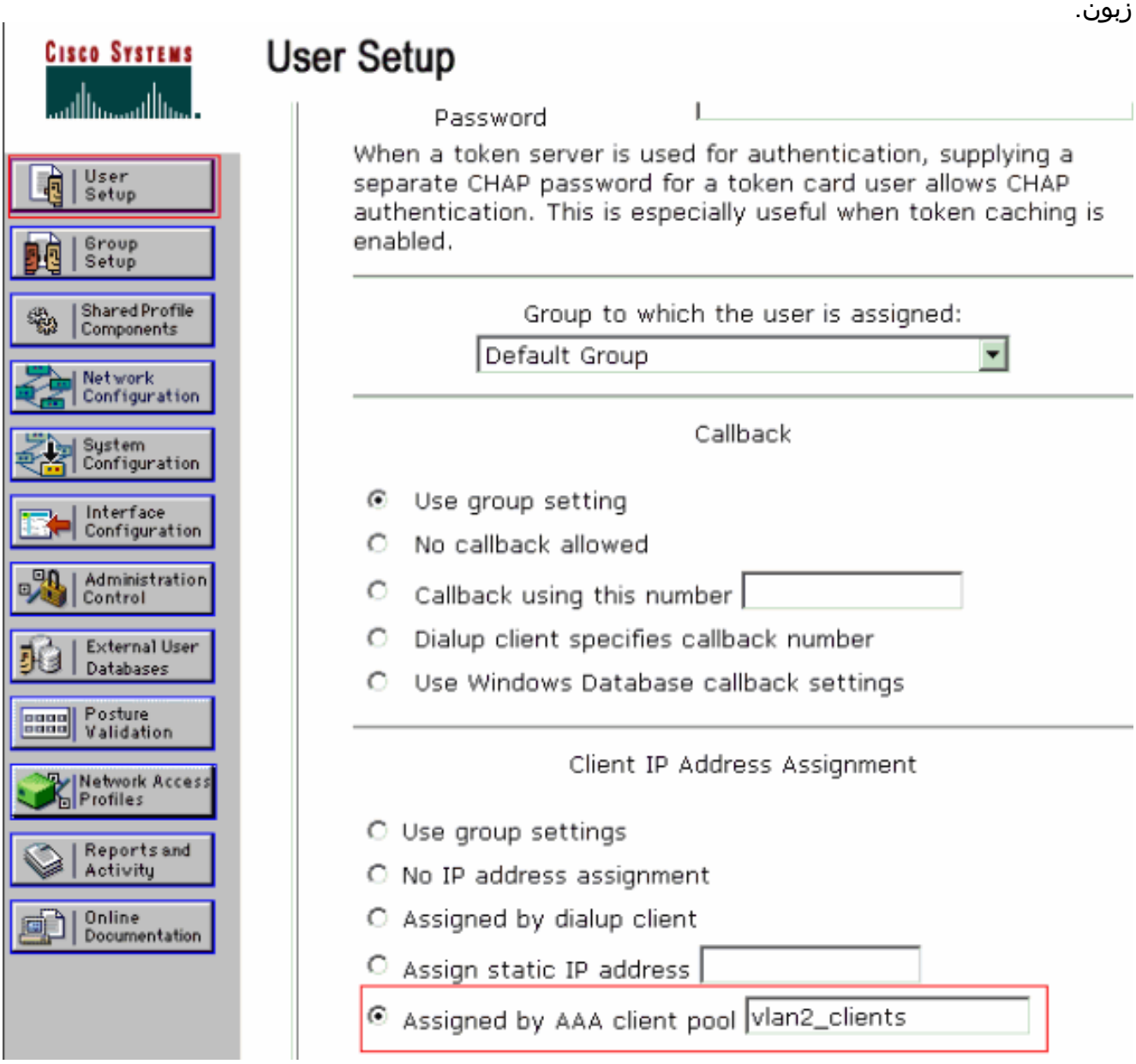
1. طقطقت in order to أضفت وشكلت مستعمل، **مستعمل setup** وعينت ال username وكلمة.





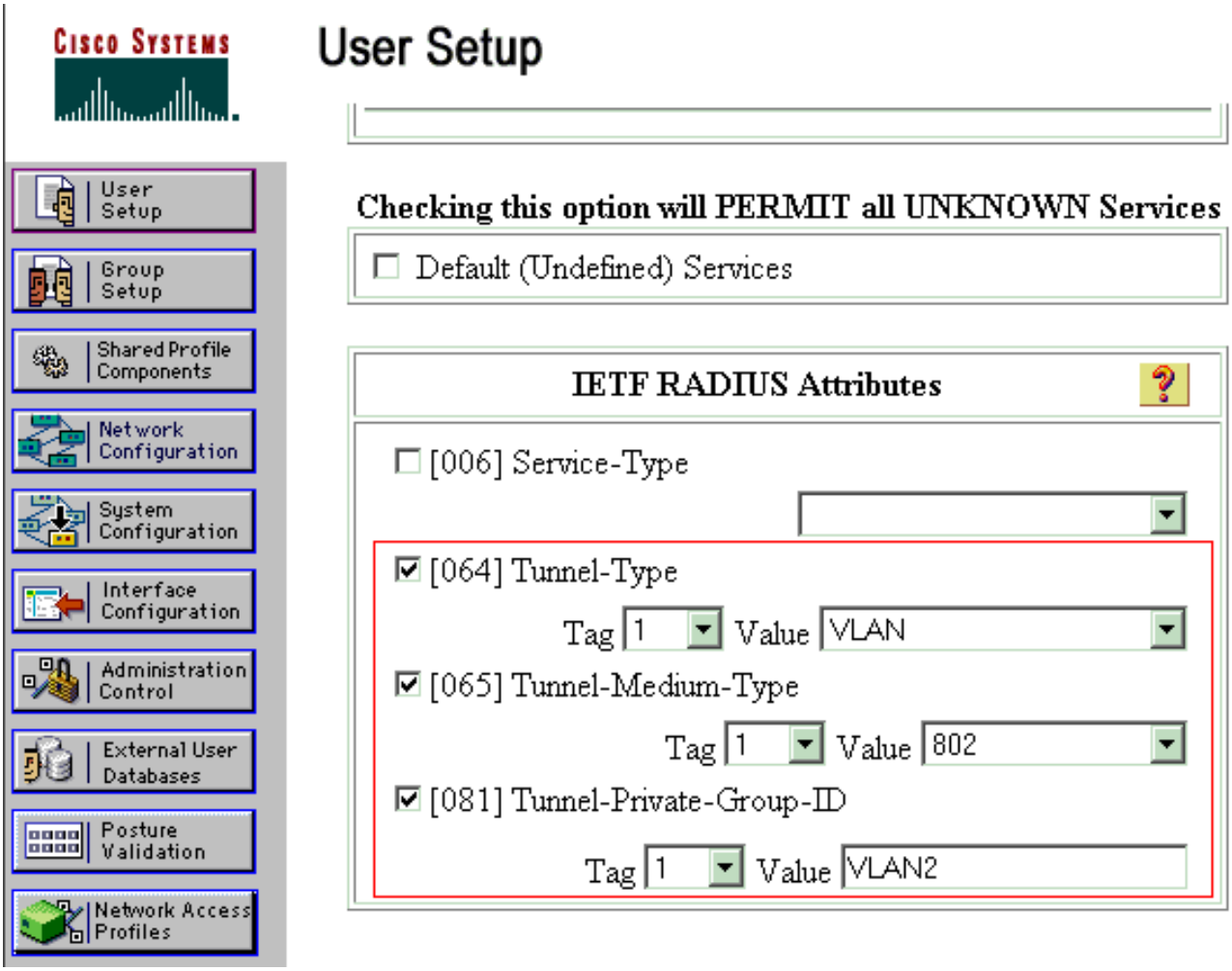
2. قم بتعريف تعيين عنوان IP للعميل **كمعين بواسطة تجمع عملاء AAA**. دخلت الاسم من العنوان بركة يشكل على المفتاح ل VLAN 2

زبون.



ملاحظة: حدد هذا الخيار واكتب اسم تجمع IP لعميل AAA في المربع، فقط إذا كان لهذا المستخدم أن يقوم بتعيين عنوان IP بواسطة تجمع عناوين IP تم تكوينه على عميل AAA.

3. قم بتعريف سمات فريق عمل هندسة الإنترنت (64 (IETF و 65.تأكد من أن علامات تمييز القيم مضبوطة 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 *إسم* أن يماثل.**ملاحظة:** يجب أن يكون *اسم* شبكة VLAN مماثلا تماما للاسم الذي تم تكوينه في المحول.**ملاحظة:** لا يدعم تعيين شبكة VLAN مع CatOS استنادا إلى *رقم* شبكة VLAN.

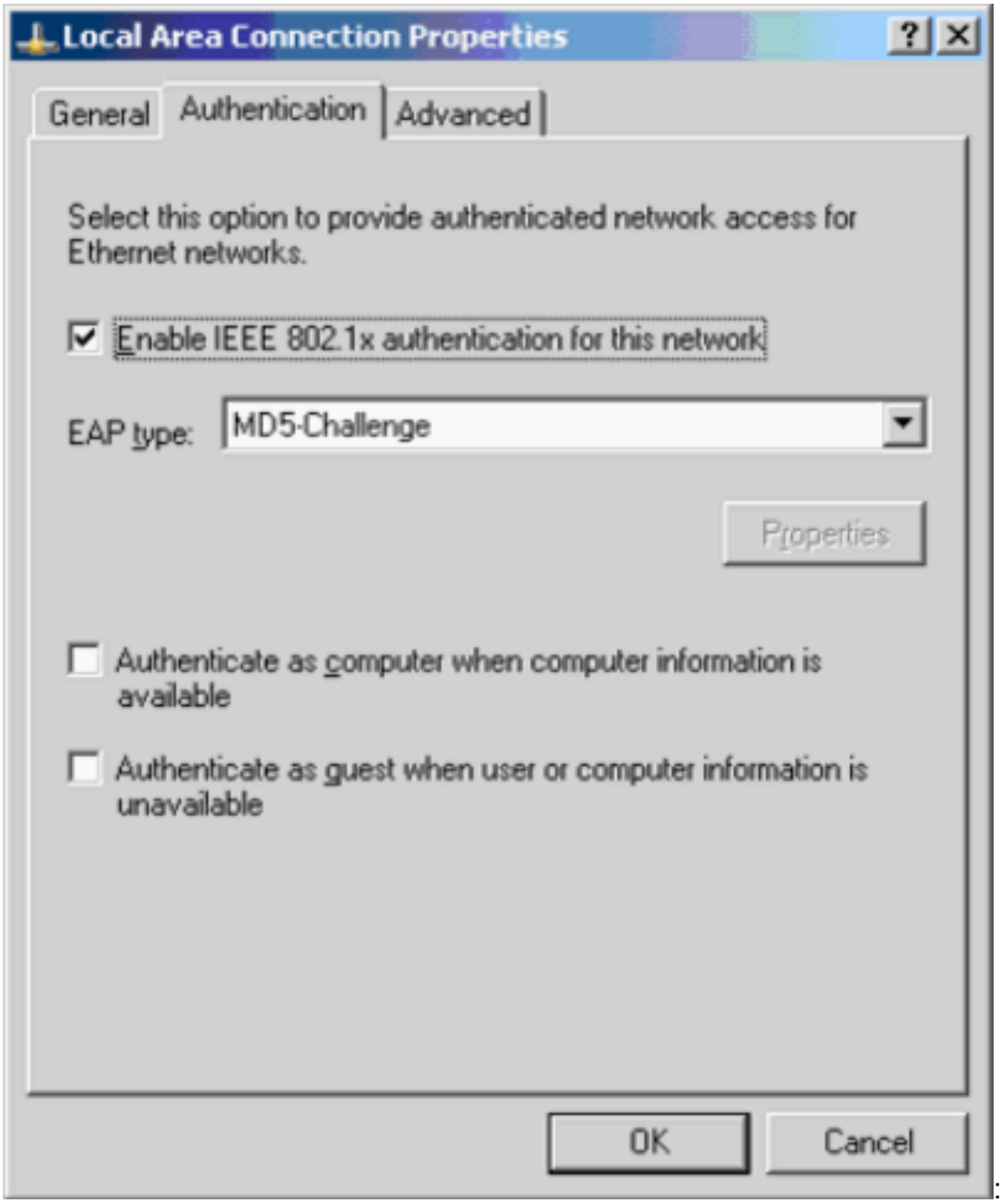


راجع RFC 2868: سمات RADIUS لدعم بروتوكول النفق للحصول على مزيد من المعلومات حول سمات IETF هذه.**ملاحظة:** في التكوين الأولي لخادم ACS، يمكن أن تفشل سمات IETF RADIUS في العرض في **إعداد المستخدم**. أخترت **قارن تشكيل>**in order to **RADIUS (IETF)** مكنت سمة IETF في مستعمل تشكيل شاشة. بعد ذلك، تحقق من السمات **64** و**65** و**81** في أعمدة المستخدم والمجموعة.

قم بتكوين عملاء الكمبيوتر لاستخدام مصادقة 802.1x

هذا المثال خاص ببروتوكول المصادقة المتوسع (EAP) ل Microsoft Windows XP عبر عميل شبكة LAN EAPOL)). أكمل الخطوات التالية:

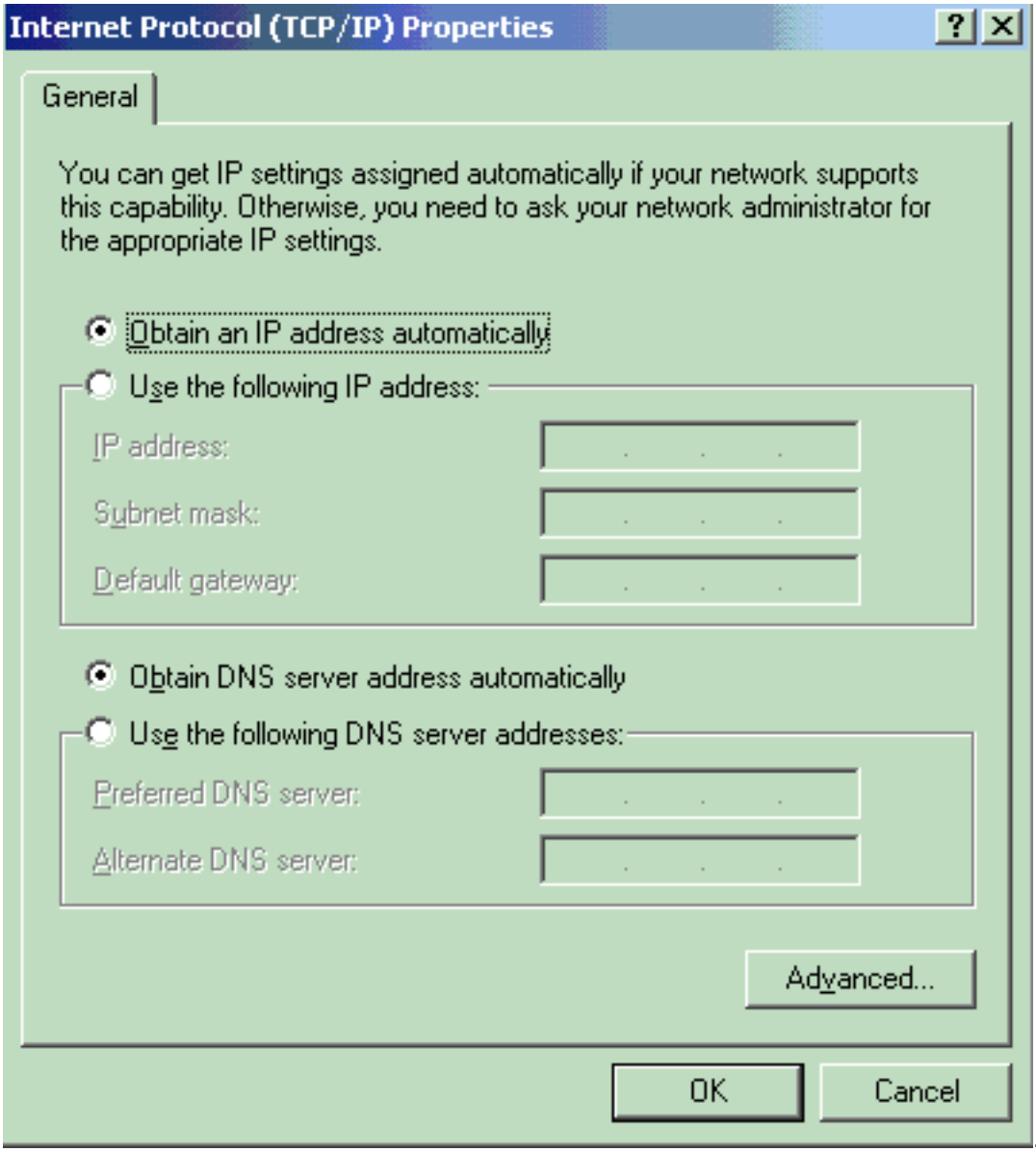
1. أختر **ابدأ > لوحة التحكم > إتصالات الشبكة**، ثم انقر بزر الماوس الأيمن فوق **اتصال المنطقة المحلية** واختر **الخصائص**.
2. تحقق من **رمز العرض في منطقة الإعلام عند إتصاله** ضمن علامة التبويب "عام".
3. تحت علامة تبويب المصادقة، تحقق من **تمكين مصادقة IEEE 802.1x لهذه الشبكة**.
4. ثبت ال EAP نوع إلى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



يوضح:

أتمت هذا steps in order to شكلت الزبون أن يحصل عنوان من DHCP نادل:

1. أختر **ابدأ > لوحة التحكم > إتصالات الشبكة**، ثم انقر بزر الماوس الأيمن فوق **اتصال المنطقة المحلية** واختر **الخصائص**.
2. تحت علامة التبويب "عام"، انقر فوق **بروتوكول الإنترنت (TCP/IP)** ثم **خصائص**.
3. أختر **الحصول على عنوان IP**



تلقائيا.

التحقق من الصحة

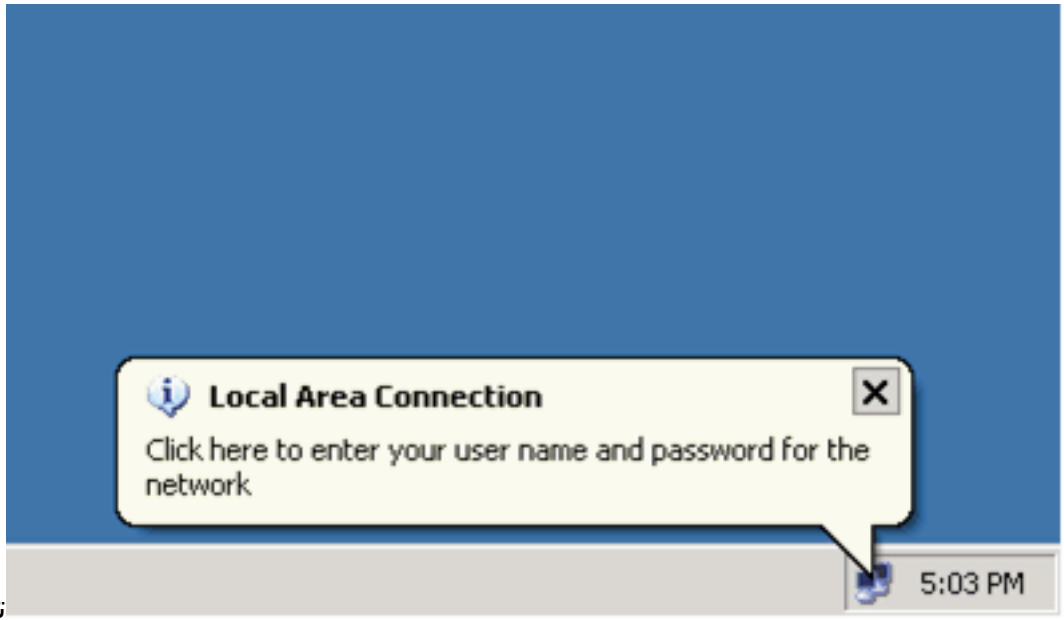
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

أجهزة الكمبيوتر العميلة

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

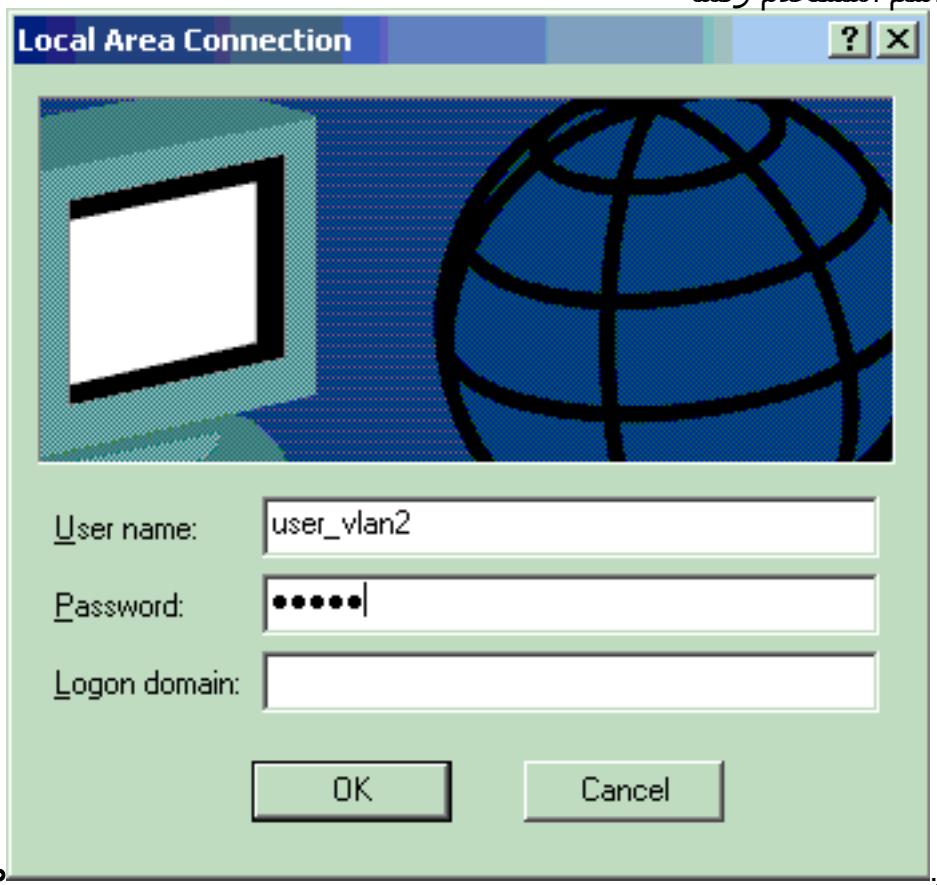
1. انقر فوق المطالبة، التي يظهرها هذا



المثال: تظهر نافذة

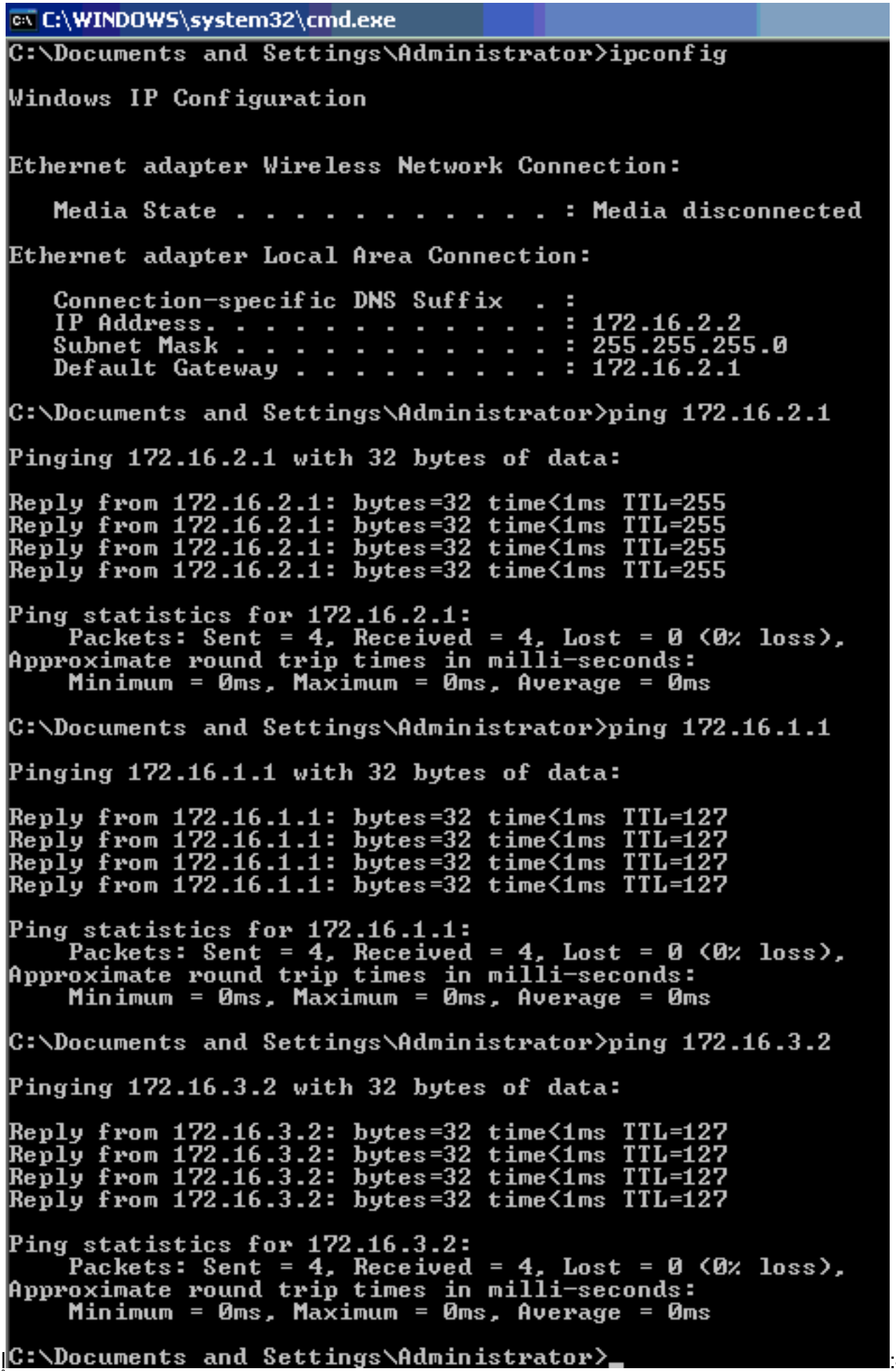
إدخال اسم مستخدم وكلمة مرور.

2. أدخل اسم المستخدم وكلمة

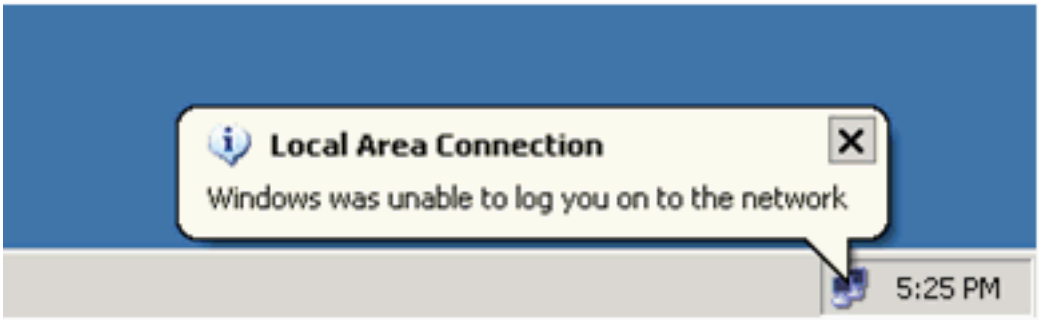


المرور. **ملاحظة:** في PC 1 و 2، أدخل مسوغات مستخدم VLAN 2. في PC 3 و 4، أدخل مسوغات مستخدم VLAN 3.

3. إذا لم تظهر رسائل خطأ، فتحقق من الاتصال بالطرق المعتادة، مثل من خلال الوصول إلى موارد الشبكة باستخدام الأمر **ping**. هذا مخرج من PC 1، الذي يظهر **إختبار اتصال** ناجح إلى PC



4: إذا ظهر هذا خطأ، فتحقق من صحة اسم المستخدم وكلمة



المرور:

Catalyst 6500

إذا ظهرت كلمة المرور واسم المستخدم صحيحين، دققت ال 802.1x ميناء دولة على المفتاح.

1. ابحث عن حالة المنفذ التي تشير إلى .

```
Cat6K> (enable) show port dot1x 3/1-5

  Port  Auth-State          BEnd-State Port-Control        Port-Status
------------ ------------------ ---------- ------------------- -----
    force-authorized   idle       force-authorized    authorized  3/1
This is the port to which RADIUS server is connected. 3/2 authenticated       idle ---!
                                                 auto               authorized
  authenticated       idle       auto                authorized  3/3
  authenticated       idle       auto                authorized  3/4
  authenticated       idle       auto                authorized  3/5

           Port  Port-Mode     Re-authentication    Shutdown-timeout
           ----------------    ----------------- ------------- -----
                   SingleAuth    disabled              disabled  3/1
                   SingleAuth    disabled              disabled  3/2
                   SingleAuth    disabled              disabled  3/3
                   SingleAuth    disabled              disabled  3/4
                   SingleAuth    disabled              disabled  3/5
```

تحقق من حالة شبكة VLAN بعد المصادقة الناجحة.

```
                                                Cat6K> (enable) show vlan
 VLAN Name                                Status    IfIndex Mod/Ports, Vlans
----------------------- ------- --------- ------------------------------- ----

                  default                          active    6       2/1-2    1
                 3/6-48
                  VLAN2                            active    83      3/2-3    2
                  VLAN3                            active    84      3/4-5    3
                           AUTHFAIL_VLAN                      active    85    4
                           GUEST_VLAN                         active    86    5
                     RADIUS_SERVER                    active    87      3/1   10
                           fddi-default                       active    78 1002
                           token-ring-default                 active    81 1003
                           fddinet-default                    active    79 1004
                           trnet-default                      active    80 1005
                                                        .Output suppressed ---!
```

2. تحقق من حالة ربط DHCP من وحدة التوجيه النمطية (MSFC) بعد المصادقة الناجحة.

```
                                                Router#show ip dhcp binding
     IP address       Hardware address        Lease expiration        Type
0100.1636.3333.9c      Feb 14 2007 03:00 AM    Automatic       172.16.2.2
0100.166F.3CA3.42      Feb 14 2007 03:03 AM    Automatic       172.16.2.3
0100.145e.945f.99      Feb 14 2007 03:05 AM    Automatic       172.16.3.2
0100.1185.8D9A.F9      Feb 14 2007 03:07 AM    Automatic       172.16.3.3
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- مصادقة IEEE 802.1x مع Catalyst 6500/6000 التي تشغل مثال تكوين برنامج Cisco IOS Software
- دليل نشر تحويل Catalyst و ACS
- المعيار RFC 2868: سمات بروتوكول RADIUS لدعم بروتوكول النفق
- تكوين مصادقة 802.1x
- صفحات دعم منتجات شبكة LAN
- صفحة دعم تحويل شبكة LAN
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).