

Catalyst 6500/6000 عم IEEE 802.1x ةقداصم Cisco IOS جم انرب نيوكت لاثم لغشت يتل Software

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [شكلت المادة حفازة مفتاح ل 802.1x صحة هوية](#)
- [تكوين خادم RADIUS](#)
- [قم بتكوين عملاء الكمبيوتر لاستخدام مصادقة 802.1x](#)
- [التحقق من الصحة](#)
- [أجهزة الكمبيوتر العملية](#)
- [Catalyst 6500](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يشرح هذا المستند كيفية تكوين IEEE 802.1x على محول Catalyst 6500/6000 يعمل في الوضع الأصلي (صورة برنامج Cisco IOS © واحدة للمحرك المشرف و 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 Cisco IOS برمجية إطلاق 12.2(18)SXF على مشرف محرك ملاحظة: تحتاج إلى برنامج Cisco IOS الإصدار 12.1(13)E أو إصدار أحدث لدعم المصادقة المستندة إلى المنفذ 802.1x.
- 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 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.

ملاحظة: إذا كان المحول يتلقى حزم EAPOL من المنفذ الذي لم يتم تكوينه لمصادقة 802.1x أو إذا كان المحول لا يدعم مصادقة 802.1x، فيتم إسقاط حزم EAPOL ولا تتم إعادة توجيهها إلى أي أجهزة تدفق البيانات.

التكوين

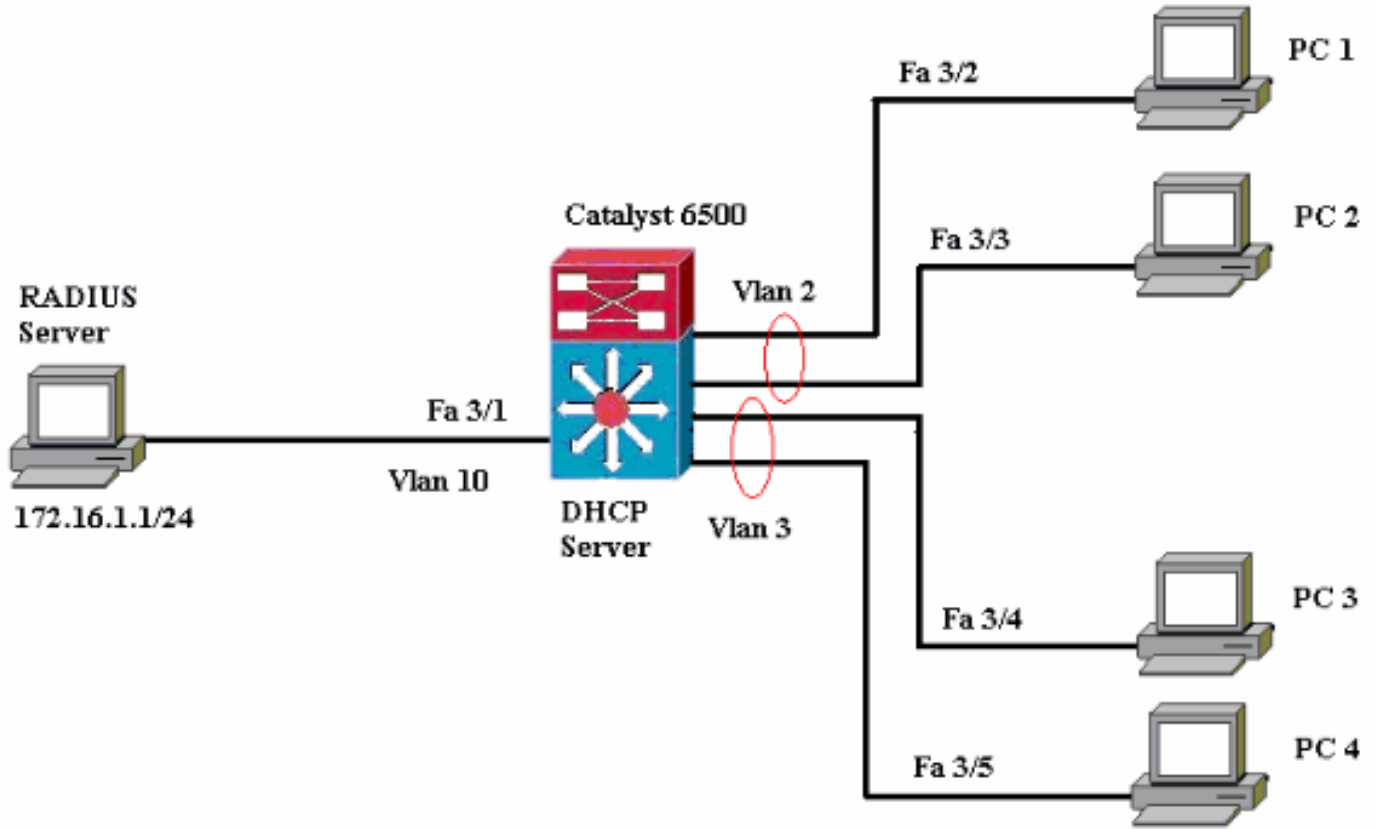
في هذا القسم، تقدم لك معلومات تكوين ميزة 802.1x الموضحة في هذا المستند.

يتطلب هذا التكوين الخطوات التالية:

- [شكلت المادة حفازة مفتاح ل 802.1x صحة هوية.](#)
- [قم بتكوين 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 مخولاً للوصول إلى خدمات الشبكة المحلية والمحولات أم لا. هنا، شكلت ال RADIUS نادل للمصادقة و VLAN تنازل.
- المحول—يتحكم 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 6500 شكلت مفتاح أيضاً 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. يستخدم 1 PCs و 2 نفس بيانات اعتماد تسجيل الدخول الموجودة في شبكة VLAN 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.

شكلت المادة حفازة مفتاح ل 802.1x صحة هوية

يتضمن تكوين المحول العينة هذا:

- كيفية تمكين مصادقة 802.1x على منافذ FastEthernet.
 - كيفية توصيل خادم RADIUS بشبكة VLAN رقم 10 خلف منفذ FastEthernet رقم 1/3.
 - DHCP نادل تشكيل ل إثتان ip بركة، واحد لزيون في VLAN 2 والآخر لزيون في VLAN 3.
 - التوجيه بين شبكات VLAN للحصول على اتصال بين العملاء بعد المصادقة.
- ارجع إلى [إرشادات وقيود المصادقة المستندة إلى المنفذ 802.1x](#) للحصول على الإرشادات حول كيفية تكوين مصادقة 802.1x.

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

```
Router#configure terminal
Enter configuration commands, one per line.  End with
.CNTL/Z

Router(config)#hostname Cat6K
Sets the hostname for the switch. ---!
Cat6K(config)#vlan 2
Cat6K(config-vlan)#name VLAN2
Cat6K(config-vlan)#vlan 3
Cat6K(config-vlan)#name VLAN3
VLAN should be existing in the switch for a ---!
successful authentication. Cat6K(config-vlan)#vlan 10
Cat6K(config-vlan)#name RADIUS_SERVER
This is a dedicated VLAN for the RADIUS server. ---!
Cat6K(config-vlan)#exit
Cat6K(config-if)#interface fastEthernet3/1
Cat6K(config-if)#switchport
Cat6K(config-if)#switchport mode access
Cat6K(config-if)#switchport access vlan 10
Cat6K(config-if)#no shut
Assigns the port connected to the RADIUS server to ---!
VLAN 10. !--- Note:- All the active access ports are in
.VLAN 1 by default

Cat6K(config-if)#exit
Cat6K(config)#dot1x system-auth-control
Globally enables 802.1x. Cat6K(config)#interface ---!
range fastEthernet3/2-48
Cat6K(config-if-range)#switchport
Cat6K(config-if-range)#switchport mode access
Cat6K(config-if-range)#dot1x port-control auto
Cat6K(config-if-range)#no shut
Enables 802.1x on all the FastEthernet interfaces. ---!
Cat6K(config-if-range)#exit
Cat6K(config)#aaa new-model
Enables AAA. Cat6K(config)#aaa authentication dot1x ---!
default group radius
Method list should be default. Otherwise dot1x does ---!
not work. Cat6K(config)#aaa authorization network
default group radius
You need authorization for dynamic VLAN assignment ---!
to work with RADIUS. Cat6K(config)#radius-server host
172.16.1.1
Sets the IP address of the RADIUS server. ---!
Cat6K(config)#radius-server key cisco
The key must match the key used on the RADIUS ---!
server. Cat6K(config)#interface vlan 10
Cat6K(config-if)#ip address 172.16.1.2 255.255.255.0
Cat6K(config-if)#no shut
This is used as the gateway address in RADIUS ---!
server !--- and also as the client identifier in the
RADIUS server. Cat6K(config-if)#interface vlan 2
Cat6K(config-if)#ip address 172.16.2.1 255.255.255.0
Cat6K(config-if)#no shut
This is the gateway address for clients in VLAN 2. ---!
Cat6K(config-if)#interface vlan 3
Cat6K(config-if)#ip address 172.16.3.1 255.255.255.0
Cat6K(config-if)#no shut
This is the gateway address for clients in VLAN 3. ---!
Cat6K(config-if)#exit
Cat6K(config)#ip dhcp pool vlan2_clients
Cat6K(dhcp-config)#network 172.16.2.0 255.255.255.0
```

```

Cat6K(dhcp-config)#default-router 172.16.2.1
This pool assigns ip address for clients in VLAN 2. ---!
Cat6K(dhcp-config)#ip dhcp pool vlan3_clients
Cat6K(dhcp-config)#network 172.16.3.0 255.255.255.0
Cat6K(dhcp-config)#default-router 172.16.3.1
This pool assigns ip address for clients in VLAN 3. ---!
Cat6K(dhcp-config)#exit
Cat6K(config)#ip dhcp excluded-address 172.16.2.1
Cat6K(config)#ip dhcp excluded-address 172.16.3.1
Cat6K(config-if)#end
Cat6K#show vlan

```

VLAN Name	Status	Ports
default	active	Fa3/2, Fa3/3, Fa3/4, Fa3/5, Fa3/6, Fa3/7, Fa3/8, Fa3/9, Fa3/10, Fa3/11, Fa3/12, Fa3/13, Fa3/14, Fa3/15, Fa3/16, Fa3/17, Fa3/18, Fa3/19, Fa3/20, Fa3/21, Fa3/22, Fa3/23, Fa3/24, Fa3/25, Fa3/26, Fa3/27, Fa3/28, Fa3/29, Fa3/30, Fa3/31, Fa3/32, Fa3/33, Fa3/34, Fa3/35, Fa3/36, Fa3/37, Fa3/38, Fa3/39, Fa3/40, Fa3/41, Fa3/42, Fa3/43, Fa3/44, Fa3/45, Fa3/46, Fa3/47, Fa3/48
VLAN2	active	2
VLAN3	active	3
RADIUS_SERVER	active	Fa3/1 10
fddi-default	act/unsup	1002
token-ring-default	act/unsup	1003
fddinet-default	act/unsup	1004
trnet-default	act/unsup	1005

Output suppressed. !--- All active ports are in ---!
.VLAN 1 (except 3/1) before authentication

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

RADIUS تكوين خادم

تم تكوين خادم RADIUS باستخدام عنوان IP ثابت بقيمة 24/172.16.1.1. 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.

CISCO SYSTEMS Network Configuration

Select

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		

Add Entry Search

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 = عنوان IP لواجهة الإدارة للمحول (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 مطابقاً على عميل AAA و ACS. المفاتيح حساسة لحالة الأحرف.

4. انقر فوق إرسال + تطبيق لجعل هذه التغييرات فعالة، كما يوضح المثال التالي:

CISCO SYSTEMS Network Configuration

Add AAA Client

AAA Client Hostname: Cat6K

AAA Client IP Address: 172.16.1.2

Shared Secret: cisco

RADIUS Key Wrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ASCII Hexadecimal

Authenticate Using: RADIUS (IETF)

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


Submit Submit + Apply Cancel

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 2 as well as VLAN 3. هنا، خلقت مستعمل_vlan2 ل زبون أن يربط إلى VLAN 2 وآخر مستعمل user_vlan3 لزبون أن يربط إلى VLAN 3 ل هذا غرض.

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

1. لإضافة مستخدمين وتكوينهم، انقر فوق إعداد المستخدم وحدد اسم المستخدم وكلمة المرور.




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](#)



User Setup

Edit

User: user_vlan2 (New User)

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

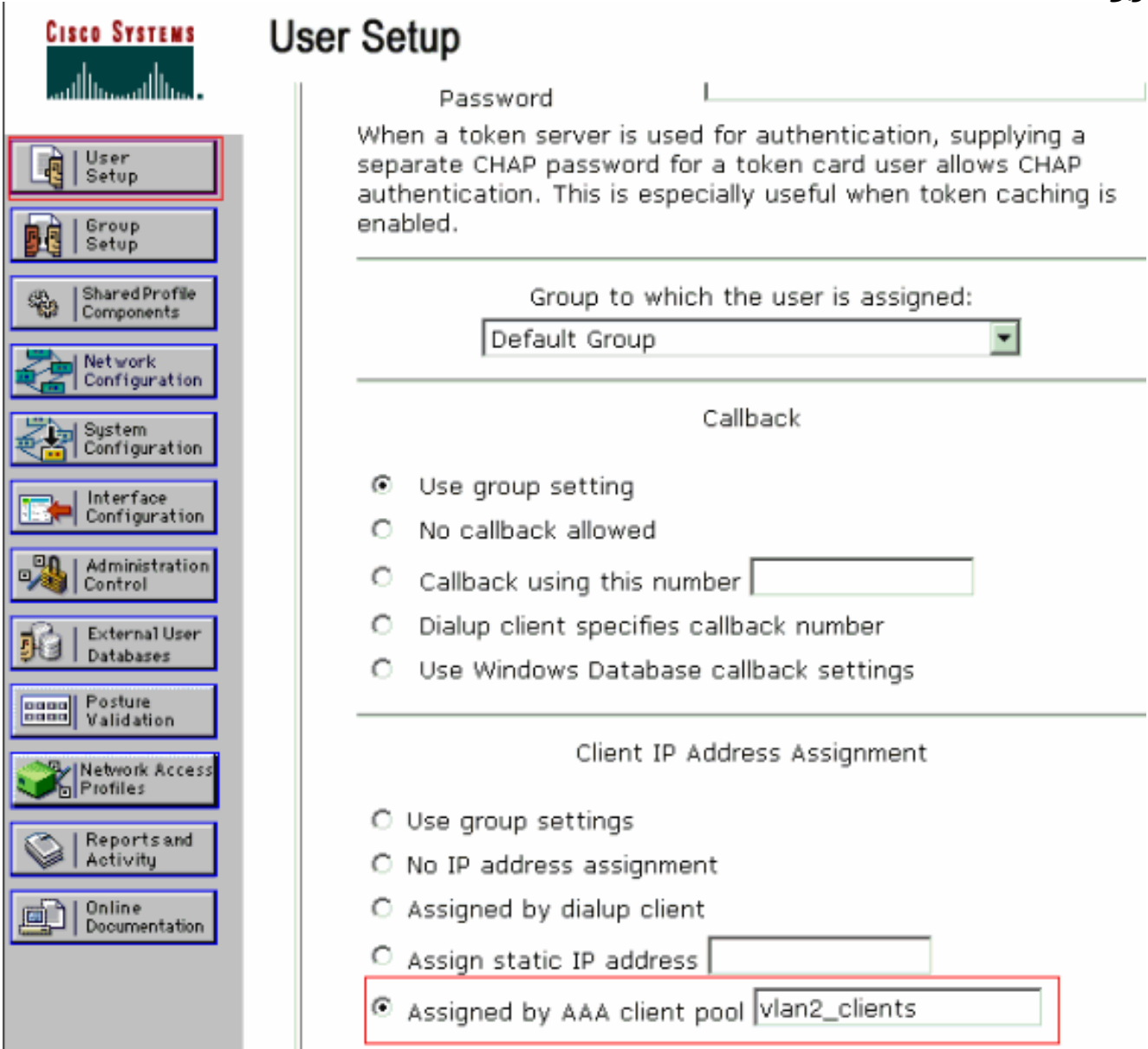
Password Authentication:

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

Password

Confirm Password

2. قم بتعريف تعيين عنوان IP للعميل كـ **جمع عملاء AAA**. دخلت الاسم من العنوان بركة بشكل على المفتاح لـ VLAN 2 زيون.



CISCO SYSTEMS

User Setup

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:

Callback

Use group setting

No callback allowed

Callback using this number

Dialup client specifies callback number

Use Windows Database callback settings

Client IP Address Assignment

Use group settings

No IP address assignment

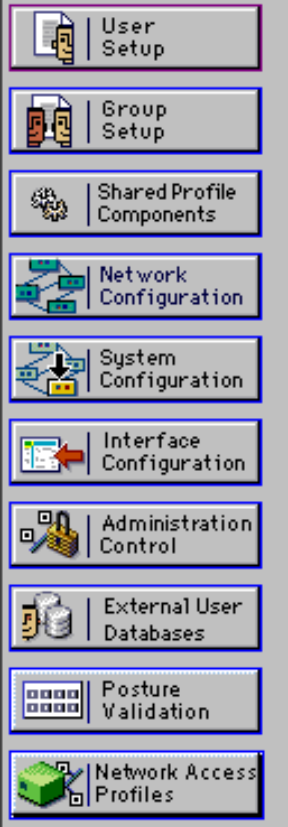
Assigned by dialup client

Assign static IP address

Assigned by AAA client pool

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) و65. 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 المحول.



Checking this option will PERMIT all UNKNOWN Services

Default (Undefined) Services

IETF RADIUS Attributes

[006] Service-Type

[064] Tunnel-Type

Tag 1 Value VLAN

[065] Tunnel-Medium-Type

Tag 1 Value 802

[081] Tunnel-Private-Group-ID

Tag 1 Value VLAN2

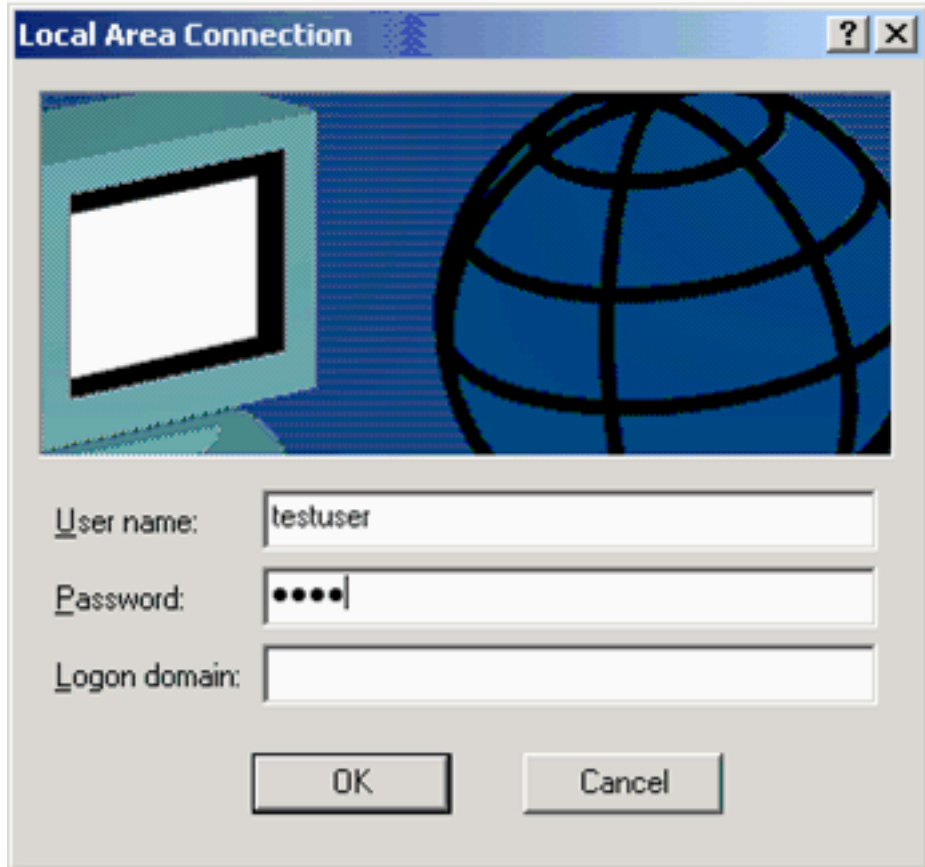
ملاحظة: للحصول على مزيد من المعلومات حول سمات IETF هذه، ارجع إلى [سمات RFC 2868](#): سمات RADIUS لدعم بروتوكول النفق. ملاحظة: في التكوين الأولي لخادم ACS، يمكن أن تفشل سمات IETF RADIUS في العرض في إعداد المستخدم. لتمكين سمات IETF في شاشات تكوين المستخدم، اختر تكوين الواجهة < IETF (RADIUS). بعد ذلك، تحقق من السمات 64 و 65 و 81 في أعمدة المستخدم والمجموعة. ملاحظة: إذا لم تقم بتحديد سمة 81 IETF وكان المنفذ منفذ محول في وضع الوصول، فسيكون للعميل تعيين إلى شبكة VLAN الخاصة بالوصول الخاصة بالمنفذ. إذا كنت قد قمت بتعريف السمة 81 للتعيين 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 يزود. وإلا، فإن 802.1x ينقل المنفذ إلى الدولة بعد مصادقة المستخدم؛ ولكن المنفذ لا يزال في شبكة VLAN الافتراضية للمنفذ، ويمكن أن يفشل الاتصال. إذا قمت بتعريف السمة 81، ولكنك قمت بتكوين المنفذ كمنفذ موجه، يحدث رفض الوصول. تظهر رسالة الخطأ هذه:

```
:DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE%
RADIUS attempted to assign a VLAN to Dot1x port FastEthernet3/4 whose
.VLAN cannot be assigned
```

قم بتكوين عملاء الكمبيوتر لاستخدام مصادقة 802.1x

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

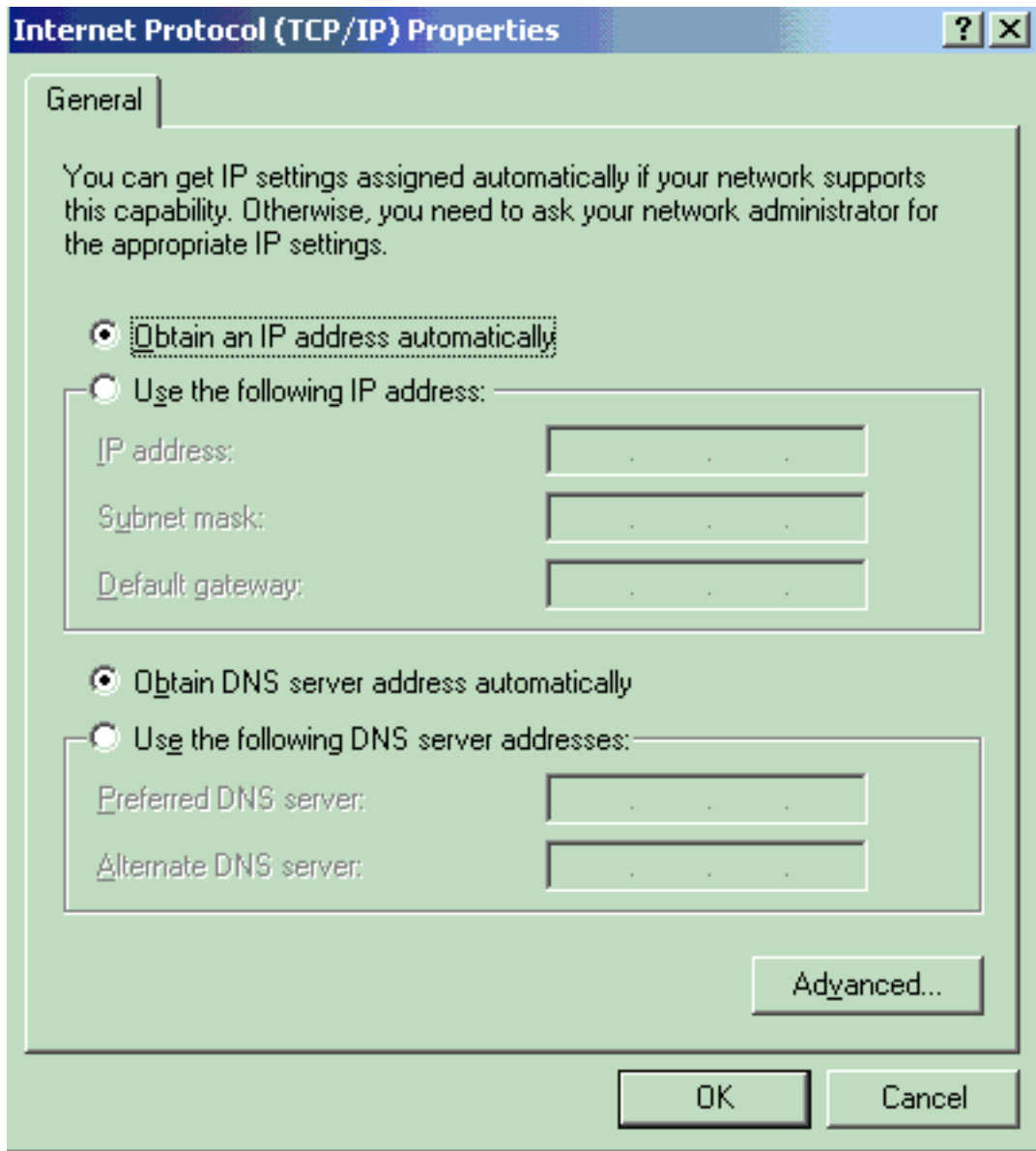
1. اختر ابدأ < لوحة التحكم < اتصالات الشبكة، ثم انقر بزر الماوس الأيمن فوق اتصال المنطقة المحلية واختر الخصائص.
2. تحقق من رمز العرض في منطقة الإعلام عند إتصاله ضمن علامة التبويب "عام".
3. تحت علامة تبويب المصادقة، تحقق من تمكين مصادقة IEEE 802.1x لهذه الشبكة.
4. ثبت ال EAP نوع إلى MD5-challenge، بما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



يوضح:

أكمل هذه الخطوات لتكوين العملاء للحصول على عنوان IP من خادم DHCP.

1. اختر ابدأ < لوحة التحكم < اتصالات 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. اختر الحصول على عنوان IP



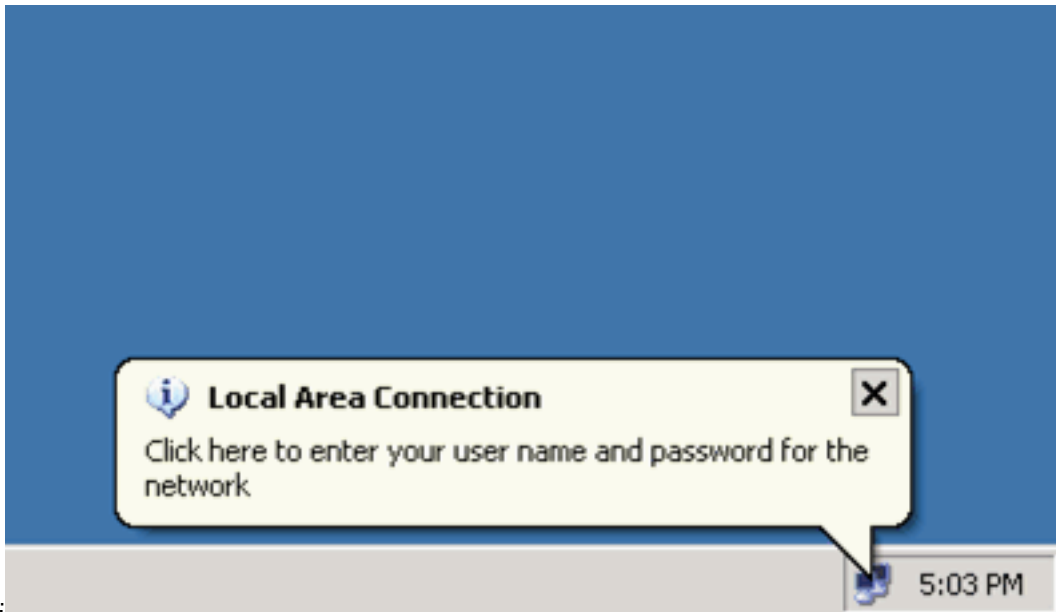
تلقائياً.

[التحقق من الصحة](#)

[أجهزة الكمبيوتر العميلة](#)

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

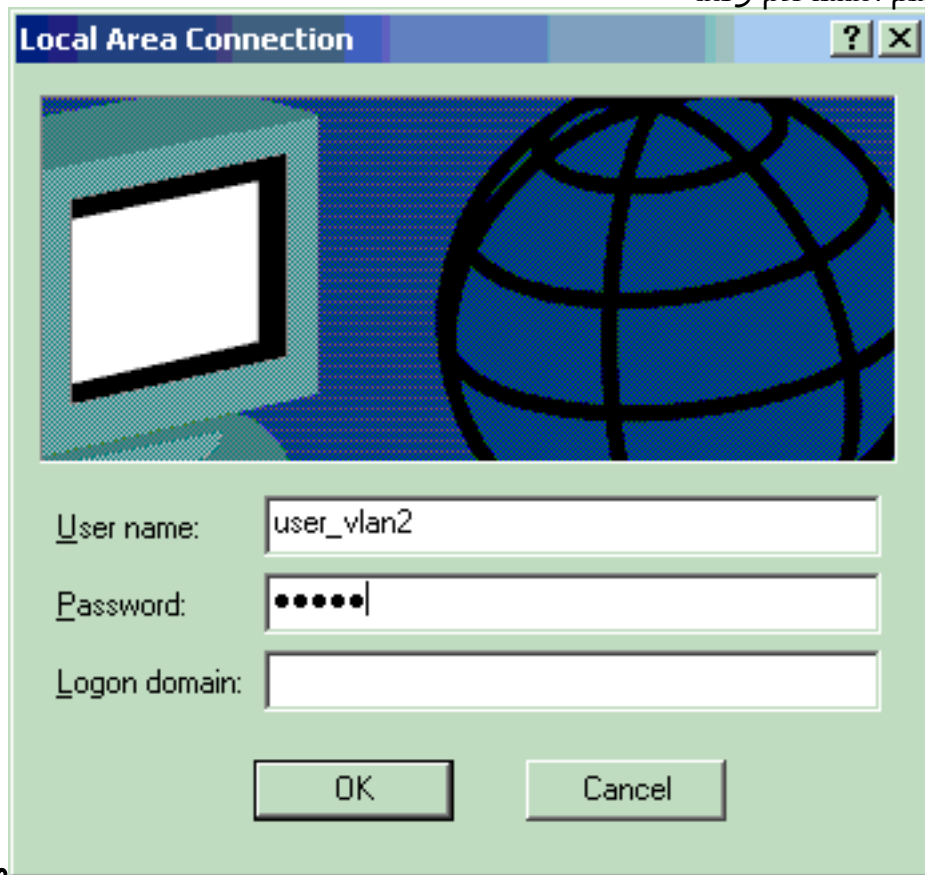
1. انقر فوق المطالبة، التي يظهرها هذا



تظهر نافذة

المثال:

إدخال اسم المستخدم وكلمة المرور.
2. أدخل اسم المستخدم وكلمة



ملاحظة: في PC 1 و 2،

المرور.

أدخل مسوغات مستخدم VLAN 2 وفي PC 3 و 4 أدخل مسوغات مستخدم VLAN 3.
3. إذا لم تظهر رسائل خطأ، فتتحقق من الاتصال بالطرق المعتادة، مثل من خلال الوصول إلى موارد الشبكة ومع
إختبار الاتصال. هذا المخرج من PC 1، وييدي إختبار اتصال ناجح إلى PC

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

    Media State . . . . . : Media disconnected
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . :
    IP Address . . . . . : 172.16.2.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 172.16.2.1

C:\Documents and Settings\Administrator>ping 172.16.2.1

Pinging 172.16.2.1 with 32 bytes of data:

Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255
Reply from 172.16.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.1.1

Pinging 172.16.1.1 with 32 bytes of data:

Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127
Reply from 172.16.1.1: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>ping 172.16.3.2

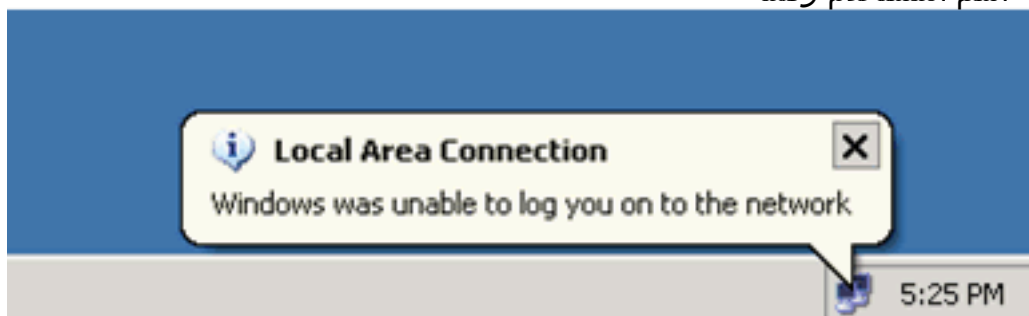
Pinging 172.16.3.2 with 32 bytes of data:

Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127
Reply from 172.16.3.2: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>
```

إذا ظهر هذا الخطأ، فتتحقق من صحة اسم المستخدم وكلمة المرور:



Catalyst 6500

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

1. ابحث عن حالة المنفذ التي تشير إلى .

Cat6K#show dot1x

```
Sysauthcontrol = Enabled
Dot1x Protocol Version = 1
Dot1x Oper Controlled Directions = Both
Dot1x Admin Controlled Directions = Both
```

Cat6K#show dot1x interface fastEthernet 3/2

```
AuthSM State = AUTHENTICATED
BendSM State = IDLE
PortStatus = AUTHORIZED
MaxReq = 2
MultiHosts = Enabled
Port Control = Auto
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
```

Cat6K#show dot1x interface fastEthernet 3/4

```
AuthSM State = AUTHENTICATED
BendSM State = IDLE
PortStatus = AUTHORIZED
MaxReq = 2
MultiHosts = Enabled
Port Control = Auto
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
```

Cat6K#show dot1x interface fastEthernet 3/1

Default Dot1x Configuration Exists for this interface FastEthernet3/1

```
AuthSM State = FORCE AUTHORIZED
BendSM State = IDLE
PortStatus = AUTHORIZED
MaxReq = 2
MultiHosts = Disabled
PortControl = Force Authorized
QuietPeriod = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod = 3600 Seconds
ServerTimeout = 30 Seconds
SuppTimeout = 30 Seconds
TxPeriod = 30 Seconds
```

تحقق من حالة شبكة VLAN بعد المصادقة الناجحة.

Cat6K#show vlan

VLAN Name	Status	Ports
,default	active	Fa3/6, Fa3/7, Fa3/8, Fa3/9
,Fa3/10, Fa3/11, Fa3/12, Fa3/13		
,Fa3/14, Fa3/15, Fa3/16, Fa3/17		
,Fa3/18, Fa3/19, Fa3/20, Fa3/21		
,Fa3/22, Fa3/23, Fa3/24, Fa3/25		
,Fa3/26, Fa3/27, Fa3/28, Fa3/29		
,Fa3/30, Fa3/31, Fa3/32, Fa3/33		

,Fa3/34, Fa3/35, Fa3/36, Fa3/37
 ,Fa3/38, Fa3/39, Fa3/40, Fa3/41
 ,Fa3/42, Fa3/43, Fa3/44, Fa3/45
 Fa3/46, Fa3/47, Fa3/48

```

VLAN2 active Fa3/2, Fa3/3 2
VLAN3 active Fa3/4, Fa3/5 3
RADIUS_SERVER active Fa3/1 10
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 من مصادقة ما بعد النجاح.

```

Router#show ip dhcp binding
IP address Hardware address Lease expiration Type
0100.1636.3333.9c Mar 04 2007 06:35 AM Automatic 172.16.2.2
0100.166F.3CA3.42 Mar 04 2007 06:43 AM Automatic 172.16.2.3
0100.145e.945f.99 Mar 04 2007 06:50 AM Automatic 172.16.3.2
0100.1185.8D9A.F9 Mar 04 2007 06:57 AM Automatic 172.16.3.3

```

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر **show**.

استكشاف الأخطاء وإصلاحها

يجمع الإنتاج من هذا يضبط أمر in order to تحريت:

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

• **debug dot1x events**—يمكن تصحيح بيانات الطباعة التي تحرسها علامة **dot1x events**.

```
Cat6K#debug dot1x events
```

```
Dot1x events debugging is on
```

```
#Cat6K
```

```

Debug output for PC 1 connected to Fa3/2. 00:13:36: dot1x-ev:Got a Request from SP to ---!
send it to Radius with id 14 00:13:36: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 3 00:13:36: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:13:36: dot1x-ev:Found a free slot at slot: 0
00:13:36: dot1x-ev:AAA Client process spawned at slot: 0 00:13:36: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/2, Request-Id = 14, Length = 15 00:13:36: dot1x-
ev:The Interface on which we got this AAA Request
is FastEthernet3/2
dot1x-ev:MAC Address is 0016.3633.339c 00:13:36
dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:13:36
dot1x-ev:going to send to backend on SP, length = 6 00:13:36
dot1x-ev:Sent to Bend 00:13:36
dot1x-ev:Got a Request from SP to send it to Radius with id 15 00:13:36
dot1x-ev:Found a process thats already handling therequest for 00:13:36
this id 12
dot1x-ev:Username is user_vlan2; eap packet length = 6 00:13:36
dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA 00:13:36
dot1x-ev:going to send to backend on SP, length = 31 00:13:36
dot1x-ev:Sent to Bend 00:13:36
dot1x-ev:Got a Request from SP to send it to Radius with id 16 00:13:36
dot1x-ev:Found a process thats already handling therequest for 00:13:36
this id 13
dot1x-ev:Username is user_vlan2; eap packet length = 32 00:13:36
dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS 00:13:36
dot1x-ev:Vlan name = VLAN2 00:13:36
- dot1x-ev:Sending Radius SUCCESS to Backend SM 00:13:37
id 16 EAP pkt len = 4
dot1x-ev:The process finished processing the request 00:13:37

```


will pick up any pending requests from the queue

#Cat6K

#Cat6K

Debug output for PC 3 connected to Fa3/4. 00:19:58: dot1x-ev:Got a Request from SP to ---!
send it to Radius with id 8 00:19:58: dot1x-ev:Couldn't Find a process thats already
handling the request for this id 1 00:19:58: dot1x-ev:Inserted the request on to list of
pending requests. Total requests = 1 00:19:58: dot1x-ev:Found a free slot at slot: 0
00:19:58: dot1x-ev:AAA Client process spawned at slot: 0 00:19:58: dot1x-ev:AAA Client-
process processing Request Interface= Fa3/4, Request-Id = 8, Length = 15 **00:19:58: dot1x-
ev:The Interface on which we got this AAA
Request is FastEthernet3/4**
dot1x-ev:MAC Address is 0014.5e94.5f99 :00:19:58
dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA :00:19:58
dot1x-ev:going to send to backend on SP, length = 6 :00:19:58
dot1x-ev:Sent to Bend :00:19:58
dot1x-ev:Got a Request from SP to send it to Radius with id 9 :00:19:58
dot1x-ev:Found a process thats already handling therequest :00:19:58
for this id 10
dot1x-ev:Username is user_vlan3; eap packet length = 6 :00:19:58
dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_GETDATA :00:19:58
dot1x-ev:going to send to backend on SP, length = 31 :00:19:58
dot1x-ev:Sent to Bend :00:19:58
dot1x-ev:Got a Request from SP to send it to Radius with id 10 :00:19:58
dot1x-ev:Found a process thats already handling therequest :00:19:58
for this id 11
dot1x-ev:Username is user_vlan3; eap packet length = 32 :00:19:58
dot1x-ev:Dot1x Authentication Status:AAA_AUTHEN_STATUS_PASS :00:19:58
dot1x-ev:Vlan name = 3 :00:19:58
dot1x-ev:Sending Radius SUCCESS to Backend SM - id 10 EAP pkt len = 4 :00:19:58
dot1x-ev:The process finished processing the request :00:19:58
will pick up any pending requests from the queue

#Cat6K

• debug radius—يعرض المعلومات المرتبطة بـ RADIUS.

Cat6K#**debug radius**

Radius protocol debugging is on

#Cat6K

Debug output for PC 1 connected to Fa3/2. 00:13:36: RADIUS: ustruct sharecount=1 ---!
00:13:36: RADIUS: Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-
login: length of radius packet = 85 code = 1 00:13:36: RADIUS: Initial Transmit
FastEthernet3/2 id 17 172.16.1.1:1812, Access-Request, len 85 00:13:36: Attribute 4 6
AC100201 00:13:36: Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36:
Attribute 12 6 000003E8 00:13:36: Attribute 79 17 0201000F 00:13:36: Attribute 80 18
CCEE4889 00:13:36: RADIUS: Received from id 17 172.16.1.1:1812, Access-Challenge, len 79
00:13:36: Attribute 79 8 010D0006 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80
18 C883376B 00:13:36: RADIUS: EAP-login: length of eap packet = 6 00:13:36: RADIUS: EAP-
login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS:
Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius
packet = 109 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 18
172.16.1.1:1812, Access-Request, len 109 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 8 020D0006 00:13:36: Attribute 80
18 15582484 00:13:36: RADIUS: Received from id 18 172.16.1.1:1812, Access-Challenge, len 104
00:13:36: Attribute 79 33 010E001F 00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 80
18 0643D234 00:13:36: RADIUS: EAP-login: length of eap packet = 31 00:13:36: RADIUS: EAP-
login: got challenge from radius 00:13:36: RADIUS: ustruct sharecount=1 00:13:36: RADIUS:
Unexpected interface type in nas_port_format_a 00:13:36: RADIUS: EAP-login: length of radius
packet = 135 code = 1 00:13:36: RADIUS: Initial Transmit FastEthernet3/2 id 19
172.16.1.1:1812, Access-Request, len 135 00:13:36: Attribute 4 6 AC100201 00:13:36:
Attribute 61 6 00000000 00:13:36: Attribute 1 12 75736572 00:13:36: Attribute 12 6 000003E8
00:13:36: Attribute 24 33 43495343 00:13:36: Attribute 79 34 020E0020 00:13:36: Attribute 80
18 E8A61751 00:13:36: RADIUS: Received from id 19 172.16.1.1:1812, Access-Accept, len 124
00:13:36: Attribute 64 6 0100000D 00:13:36: Attribute 65 6 01000006 00:13:36: Attribute 81 8
01564C41 00:13:36: Attribute 88 15 766C616E 00:13:36: Attribute 8 6 FFFFFFFF 00:13:36:

Attribute 79 6 030E0004 00:13:36: Attribute 25 39 43495343 00:13:36: Attribute 80 18 11A7DD44 00:13:36: RADIUS: EAP-login: length of eap packet = 4 Cat6K# Cat6K# !--- Debug output for PC 3 connected to Fa3/4. 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 85 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 11 172.16.1.1:1812, Access-Request, len 85 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 79 17 0201000F 00:19:58: Attribute 80 18 0001AC52 00:19:58: RADIUS: Received from id 11 172.16.1.1:1812, Access-Challenge, len 79 00:19:58: Attribute 79 8 010B0006 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 23B9C9E7 00:19:58: RADIUS: EAP-login: length of eap packet = 6 00:19:58: RADIUS: EAP-login: got challenge from radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 109 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 12 172.16.1.1:1812, Access-Request, len 109 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 79 8 020B0006 00:19:58: Attribute 80 18 F4C8832E 00:19:58: RADIUS: Received from id 12 172.16.1.1:1812, Access-Challenge, len 104 00:19:58: Attribute 79 33 010C001F 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 80 18 45472A93 00:19:58: RADIUS: EAP-login: length of eap packet = 31 00:19:58: RADIUS: EAP-login: got challenge from radius 00:19:58: RADIUS: ustruct sharecount=1 00:19:58: RADIUS: Unexpected interface type in nas_port_format_a 00:19:58: RADIUS: EAP-login: length of radius packet = 135 code = 1 00:19:58: RADIUS: Initial Transmit FastEthernet3/4 id 13 172.16.1.1:1812, Access-Request, len 135 00:19:58: Attribute 4 6 AC100201 00:19:58: Attribute 61 6 00000000 00:19:58: Attribute 1 12 75736572 00:19:58: Attribute 12 6 000003E8 00:19:58: Attribute 24 33 43495343 00:19:58: Attribute 79 34 020C0020 00:19:58: Attribute 80 18 37011E8F 00:19:58: RADIUS: Received from id 13 172.16.1.1:1812, Access-Accept, len 120 00:19:58: Attribute 64 6 0100000D 00:19:58: Attribute 65 6 01000006 00:19:58: Attribute 81 4 0133580F 00:19:58: Attribute 88 15 766C616E 00:19:58: Attribute 8 6 FFFFFFFE 00:19:58: Attribute 79 6 030C0004 00:19:58: Attribute 25 39 43495343 00:19:58: Attribute 80 18 F5520A95 00:19:58: RADIUS: EAP-#login: length of eap packet = 4 Cat6K

معلومات ذات صلة

- [مصادقة IEEE 802.1x مع Catalyst 6500/6000 التي تشغل مثال تكوين البرنامج CatOS Software](#)
- [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](#)
- [تكوين المصادقة المستندة إلى المنفذ IEEE 802.1X](#)
- [دعم منتجات الشبكات المحلية \(LAN\)](#)
- [دعم تقنية تحويل شبكات LAN](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ان ا عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا