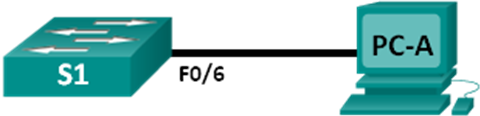
التمرين المعملي - تكوين عنوان إدارة المحول

الهيكل



جدول العنونة

|  |  |  |  |
| --- | --- | --- | --- |
| الجهاز | الواجهة | عنوان IP | قناع الشبكة الفرعية |
| S1 | VLAN 1 | 192.168.1.2 | 255.255.255.0 |
| PC-A | NIC | 192.168.1.10 | 255.255.255.0 |

الأهداف

الجزء الأول: تكوين جهاز شبكة أساسي

الجزء الثاني: التحقق من اتصال الشبكة واختباره

خلفية / سيناريو

يوجد بمحولات Cisco واجهة خاصة تعرف باسم واجهة المحول الافتراضية (SVI). يمكن تكوين واجهة المحول الافتراضية باستخدام عنوان IP، وعادةً ما يشار إليها بصفتها عنوان الإدارة. ويستخدم عنوان الإدارة للوصول عن بعد إلى المحول لعرض الإعدادات أو تكوينها.

وفي هذا التمرين المعملي، ستقوم بإنشاء شبكة بسيطة باستخدام كابلات شبكة Ethernet LAN، والوصول إلى محول Cisco باستخدام وحدة التحكم وطرق الوصول عن بعد. وستقوم بتكوين الإعدادات الأساسية للمحول، وعنوان IP وعرض استخدام عنوان IP لإدارة المحول عن بعد. يتكون المخطط من محول واحد ومضيف واحد باستخدام منافذ Ethernet ووحدة التحكم فقط.

**ملاحظة**: المحولات المستخدمة هي عبارة عن أجهزة Cisco Catalyst 2960 إلى جانب Cisco IOS الإصدار (2)15.0 ‏(صورة lanbasek9). ويمكن كذلك استخدام محولات وإصدارات Cisco IOS أخرى. طبقًا للطراز وإصدار Cisco IOS، قد تتباين الأوامر المتوفرة والإخراجات الناتجة عما هو موضح في التمارين المعملية.

**ملاحظة**: تأكد من مسح المحول وأنه لا يحتوي على أي تكوين لبدء التشغيل. وإذا لم تكن متأكدًا، فاتصل بالمعلم.

الموارد المطلوبة

* محول واحد (Cisco 2960 إلى جانب Cisco IOS Release 15.0(2) lanbasek9 صورة أو قابل للمقارنة)
* جهاز كمبيوتر واحد (يعمل بنظام Windows 7 أو 8 به برنامج محاكاة طرفي، مثل Tera Term)
* كابلات وحدة التحكم لتكوين أجهزة Cisco IOS عبر منافذ وحدة التحكم
* كابلات Ethernet كما هو موضح في الهيكل

1. تكوين جهاز شبكة أساسي

ستقوم في الجزء الأول بإعداد الشبكة وتكوين الإعدادات الأساسية، مثل أسماء المضيفين وعناوين IP للواجهة وكلمات المرور.

* 1. توصيل الشبكة.
     1. قم بتوصيل الشبكة كما هو موضح في الهيكل.
     2. قم بإنشاء اتصال وحدة تحكم بالمحول من الجهاز PC-A.
  2. قم بتكوين الإعدادات الأساسية للمحول.

ستقوم في هذه الخطوة بتكوين الإعدادات الأساسية للمحول، مثل اسم المضيف وتكوين عنوان IP للواجهة الظاهرية للمحول. تعيين عنوان IP على المحول هو الخطوة الأولى فقط. فبصفتك مسؤول الشبكة، يجب أن تحدد طريقة إدارة المحول. تعد Telnet وSSH طريقتين من طرق الإدارة الأكثر شيوعًا. ومع ذلك، تعد Telnet بروتوكولاً غير آمن للغاية. حيث ترسل جميع المعلومات التي تتدفق بين الجهازين بنص عادي. ويمكن الاطلاع على كلمات المرور والمعلومات الأخرى الحساسة بسهولة إذا تم التقاطها بواسطة مراقب الحزم.

* + 1. فإذا افترضنا أن المحول لا يشتمل على ملف تكوين مخزن في ذاكرة NVRAM، فستكون في مطالبة وضع EXEC الخاص بالمستخدم على المحول. ستكون المطالبة Switch>. ادخل إلى وضع EXEC ذي الامتيازات.

Switch> **enable**

Switch#

* + 1. استخدم أمر **show running-config** لوضع EXEC ذي الامتيازات للتحقق من ملف التكوين النظيف. إذا تم حفظ ملف تكوين من قبل، فستتعين إزالته. ووفقًا لطراز المحول وإصدار IOS، قد يبدو التكوين الخاص بك مختلفًا قليلاً. ومع ذلك، يجب ألا تكون هناك كلمات مرور تم تكوينها أو عنوان IP تم تعيينه. إذا كان المحول لا يشتمل على تكوين افتراضي، فاطلب المساعدة من معلمك.
    2. ادخل إلى وضع التكوين العام وقم بتعيين اسم مضيف المحول.

Switch# **configure terminal**

Switch(config)# **hostname S1**

S1(config)#

* + 1. قم بتكوين كلمة المرور الخاصة بالوصول إلى المحول.

S1(config)# **enable secret class**

S1(config)#

* + 1. امنع عمليات البحث غير المرغوب فيها الخاصة بنظام اسم المجال (DNS).

S1(config)# **no ip domain-lookup**

S1(config)#

* + 1. قم بتكوين شعار تسجيل دخول MOTD.

S1(config)# **banner motd #**

Enter Text message. End with the character ‘#’.

**Unauthorized access is strictly prohibited. #**

* + 1. تحقق من إعدادات الوصول عن طريق الانتقال بين الأوضاع.

S1(config)# **exit**

S1#

S1# **exit**

Unauthorized access is strictly prohibited.

S1>

ما مفاتيح الاختصار المستخدمة للانتقال مباشرة من وضع التكوين العام إلى وضع EXEC ذي الامتيازات؟

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. ارجع إلى وضع EXEC ذي الامتيازات من وضع EXEC الخاص بالمستخدم.

S1> **enable**

Password: **class**

S1#

**ملاحظة**: لن تظهر كلمة المرور على الشاشة عند الدخول.

* + 1. ادخل إلى وضع التكوين العام لضبط عنوان IP الخاص بالواجهة الظاهرية للمحول للسماح بإدارة المحول عن بعد.

S1# **config t**

S1#(config)# **interface vlan 1**

S1(config-if)# **ip address 192.168.1.2 255.255.255.0**

S1(config-if)# **no shut**

S1(config-if)# **exit**

S1(config)#

* + 1. قم بتقييد الوصول إلى منفذ وحدة التحكم. التكوين الافتراضي هو السماح بجميع اتصالات وحدة التحكم دون الحاجة إلى كلمة مرور.

S1(config)# **line con 0**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S1(config-line)# **exit**

S1(config)#

* + 1. قم بتكوين سطر VTY للمحول للسماح بوصول Telnet. إذا لم تقم بتكوين كلمة مرور VTY، فلن تتمكن من استخدام telnet مع المحول.

S1(config)# **line vty 0 4**

S1(config-line)# **password cisco**

S1(config-line)# **login**

S1(config-line)# **end**

S1#

\*Mar 1 00:06:11.590: %SYS-5-CONFIG\_I: Configured from console by console

* 1. تكوين عنوان IP على جهاز PC-A.
     1. قم بتخصيص عنوان IP وقناع الشبكة الفرعية بالكمبيوتر الشخصي كما هو موضح في جدول العنونة. فيما يلي توضيح لإجراء تعيين عنوان IP على جهاز كمبيوتر يعمل بنظام التشغيل Windows 7:
        1. انقر فوق رمز **قائمة ابدأ** بنظام التشغيل Windows > (**لوحة التحكم**).
        2. انقر فوق **عرض حسب:** > **الفئة**.
        3. اختر **عرض حالة الشبكة ومهامها** > **تغيير إعدادات المحول**.
        4. انقر بزر الماوس الأيمن فوق **اتصال شبكة المنطقة المحلية** وحدد **خصائص**.
        5. اختر **Internet Protocol Version 4 (TCP/IPv4)‎**، وانقر فوق خصائص > موافق.
        6. انقر فوق زر الخيار **استخدام عنوان IP التالي** وأدخل عنوان IP وقناع الشبكة الفرعية.

1. التحقق من اتصال الشبكة واختباره

ستقوم الآن بالتحقق من تكوين المحول وتوثيقه، واختبار الاتصال من طرف إلى طرف بين PC-A وS1، واختبار القدرة على إدارة المحول عن بعد.

* 1. اعرض تكوين جهاز S1.
     1. ارجع إلى اتصال وحدة التحكم لديك باستخدام برنامج Tera Term الموجود على PC-A. وأصدر الأمر **show run** لعرض تكوين المحول والتحقق منه. يتم توضيح عينة من التكوين أدناه. يتم تمييز الإعدادات التي قمت بتكوينها باللون الأصفر. إعدادات التكوين الأخرى هي إعدادات IOS افتراضية.

S1# **show run**

Building configuration...

Current configuration : 1508 bytes

!

! Last configuration change at 00:06:11 UTC Mon Mar 1 1993

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname S1

!

boot-start-marker

boot-end-marker

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

system mtu routing 1500

!

!

no ip domain-lookup

!

spanning-tree mode pvst

spanning-tree extend system-id

!

vlan internal allocation policy ascending

!

!

interface FastEthernet0/1

!

interface FastEthernet0/2

<output omitted>

interface FastEthernet0/24

!

interface GigabitEthernet0/1

!

interface GigabitEthernet0/2

!

interface Vlan1

ip address 192.168.1.2 255.255.255.0

!

ip http server

ip http secure-server

!

banner motd ^C

Unauthorized access is strictly prohibited. ^C

!

line con 0

password cisco

login

line vty 0 4

password cisco

login

line vty 5 15

login

!

end

* + 1. تحقق من حالة واجهة إدارة SVI. يجب أن تكون واجهة VLAN 1 لديك up/up (أعلى/ أعلى) وأن يكون عنوان IP معينًا. لاحظ أن منفذ المحول F0/6 لأعلى أيضًا نظرًا لاتصال PC-A به. ونظرًا لأن جميع منافذ المحول توجد أساسًا في VLAN 1، بشكل افتراضي، فيمكنك الاتصال بالمحول باستخدام عنوان IP الذي كونته من أجل VLAN 1.

S1# **show ip interface brief**

Interface IP-Address OK? Method Status Protocol

Vlan1 192.168.1.2 YES manual up up

FastEthernet0/1 unassigned YES unset down down

FastEthernet0/2 unassigned YES unset down down

FastEthernet0/3 unassigned YES unset down down

FastEthernet0/4 unassigned YES unset down down

FastEthernet0/5 unassigned YES unset down down

FastEthernet0/6 unassigned YES unset up up

FastEthernet0/7 unassigned YES unset down down

FastEthernet0/8 unassigned YES unset down down

FastEthernet0/9 unassigned YES unset down down

FastEthernet0/10 unassigned YES unset down down

FastEthernet0/11 unassigned YES unset down down

FastEthernet0/12 unassigned YES unset down down

FastEthernet0/13 unassigned YES unset down down

FastEthernet0/14 unassigned YES unset down down

FastEthernet0/15 unassigned YES unset down down

FastEthernet0/16 unassigned YES unset down down

FastEthernet0/17 unassigned YES unset down down

FastEthernet0/18 unassigned YES unset down down

FastEthernet0/19 unassigned YES unset down down

FastEthernet0/20 unassigned YES unset down down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

GigabitEthernet0/1 unassigned YES unset down down

GigabitEthernet0/2 unassigned YES unset down down

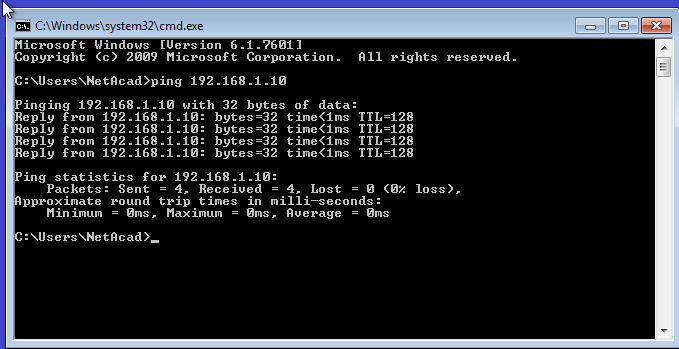
* 1. اختبار الاتصال من طرف إلى طرف.

افتح نافذة موجه الأوامر (cmd.exe) على الجهاز PC-A بالنقر فوق رمز **قائمة ابدأ بنظام التشغيل Windows** وإدخال **cmd** في حقل **بحث في البرامج والملفات**. تحقق من عنوان IP للجهاز PC-A باستخدام الأمر **ipconfig /all**. يعرض هذا الأمر اسم مضيف جهاز الكمبيوتر ومعلومات عنوان IPv4. اختبر اتصال الجهاز PC-A باستخدام الأمر Ping وعنوان الإدارة الخاص بالمحول S1.

* + 1. اختبر عنوان الجهاز PC-A باستخدام الأمر Ping أولاً.

C:\Users\NetAcad> **ping 192.168.1.10**

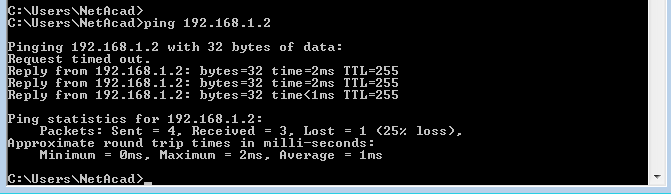
ينبغي أن تكون النتيجة لديك تشبه ما في الشاشة التالية:



* + 1. اختبر عنوان إدارة SVI باستخدام الأمر Ping بالمحول S1.

C:\Users\NetAcad> **ping 192.168.1.2**

ينبغي أن تكون النتيجة لديك تشبه ما في الشاشة التالية. إذا استمرت نتائج تنفيذ الأمر ping في الفشل، فقم باستكشاف أخطاء في تكوينات الجهاز الأساسية وإصلاحها. يجب أن تتحقق من كلٍ من الكابلات المادية وعنونة IP إذا لزم الأمر.



* 1. اختبر إدارة S1 عن بعد وتحقق منها.

ستستخدم الآن Telnet للوصول عن بُعد إلى المحول S1 باستخدام عنوان إدارة SVI. في هذا التمرين المعملي، يقع PC-A وS1 جنبًا إلى جنب. في شبكة الإنتاج، قد يكون المحول في صندوق أسلاك في الطابق العلوي بينما يوجد جهاز الكمبيوتر الخاص بالإدارة في الطابق الأرضي . ومع ذلك، لا يُعد Telnet بروتوكولاً آمنًا. ولكن ستستخدمه في هذا التمرين المعملي لاختبار الوصول عن بُعد. يتم إرسال جميع المعلومات المرسلة من خلال Telnet، بما في ذلك كلمات المرور والأوامر، عبر الجلسة بنص عادي. وفي التمارين المعملية اللاحقة، ستستخدم SSH للوصول عن بُعد إلى أجهزة الشبكة.

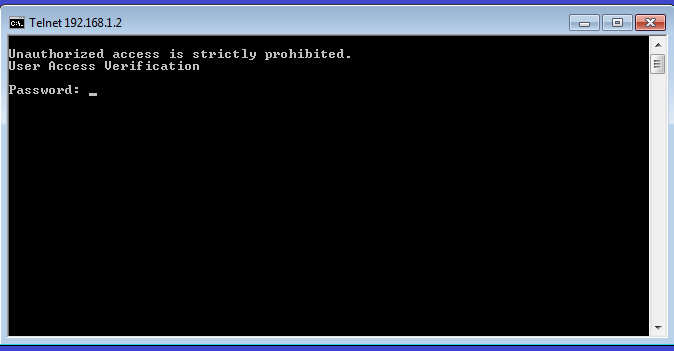
**ملاحظة**: لا يدعم Windows 7 وفق إعداداته الافتراضية بروتوكول Telnet. لذا يتعين على المسؤول تمكين هذا البروتوكول. لتثبيت عميل Telnet، افتح نافذة موجه الأوامر واكتب **”pkgmgr /iu:“TelnetClient**.

C:\Users\NetAcad> **pkgmgr /iu:”TelnetClient”**

* + 1. عندما تكون نافذة موجه الأوامر مفتوحة على الجهاز PC-A، أصدر أمر Telnet للاتصال بالمحول S1 عبر عنوان إدارة SVI. كلمة المرور هي **cisco**.

C:\Users\NetAcad> **telnet 192.168.1.2**

ينبغي أن تكون النتيجة لديك تشبه ما في الشاشة التالية:



* + 1. بعد إدخال كلمة المرور **cisco**، ستكون في مطالبة وضع EXEC الخاص بالمستخدم. اكتب **enable** في المطالبة. أدخل كلمة المرور **class** للدخول إلى وضع EXEC ذي الامتيازات وأصدر الأمر **show run**.
  1. احفظ ملف التكوين.
     1. من جلسة Telnet الخاصة بك، أصدِر الأمر **copy run start** على الموجه.

S1# **copy run start**

Destination filename [startup-config]? [**Enter**]

Building configuration ..

S1#

* + 1. اخرج من جلسة Telnet عن طريق كتابة **quit**. وستتم إعادتك إلى موجه أوامر Windows 7.

أسئلة تمرينية

لماذا يتعين عليك استخدام اتصال وحدة التحكم لتكوين المحول بصورة أولية؟ لماذا يتعذر الاتصال بالمحول عبر Telnet أو SSH؟

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_