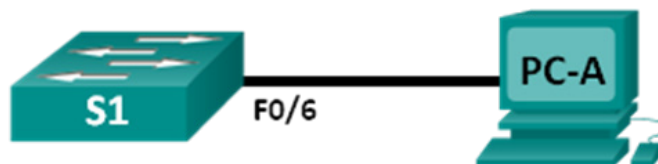


実習 - スイッチ管理アドレスの設定

トポロジ



アドレッシング テーブル

デバイス	インターフェイス	IP アドレス	サブネット マスク	デフォルト ゲートウェイ
S1	VLAN 1	192.168.1.2	255.255.255.0	該当なし
PC-A	NIC	192.168.1.10	255.255.255.0	該当なし

目的

パート 1: 基本的なネットワーク デバイスを設定する

- トポロジに示すようにネットワークを配線する。
- ホスト名、管理アドレス、Telnet アクセスなど、スイッチの基本設定を構成します。
- PC の IP アドレスを設定します。

パート 2: ネットワーク接続を確認およびテストする

- デバイスの設定を表示します。
- ping でエンドツーエンド接続をテストします。
- Telnet のリモート管理機能をテストします。
- スイッチの実行コンフィギュレーション ファイルを保存します。

背景/シナリオ

シスコ スイッチには、Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) と呼ばれる特殊なインターフェイスがあります。SVI には IP アドレスを設定できます。IP アドレスは、一般には管理アドレスと呼ばれ、スイッチにリモートアクセスして設定の表示や構成を行うのに使用されます。

この実習では、イーサネット LAN 配線を使用したシンプルなネットワークを構築し、コンソール方式とリモート アクセス方式を使用してシスコ スイッチにアクセスします。スイッチの基本設定と IP アドレスを設定したら、スイッチのリモート管理に管理 IP アドレスを使用する例を実際に示します。トポロジは、イーサネット ポートとコンソール ポートのみを使用するスイッチ 1 台とホスト 1 台で構成されます。

注: 使用するスイッチは、Cisco IOS リリース 15.0(2) (lanbasek9 イメージ) を搭載した Cisco catalyst 2960 です。他のスイッチおよび Cisco IOS バージョンを使用できます。モデルと Cisco IOS バージョンによっては、使用可能なコマンドと生成される出力が、この実習で示すものと異なる場合があります。

注: スイッチが消去されており、スタートアップ コンフィギュレーションがないことを確認してください。不明な場合は、インストラクタに相談してください。

実習に必要なリソースや機器

- スイッチ 1 台 (Cisco IOS リリース 15.0(2) の lanbasek9 イメージを搭載した Cisco 2960 または同等機器)
- PC 1 台 (Tera Term などのターミナル エミュレーション プログラムをインストールした Windows 7、Vista、または XP)
- コンソール ポート経由で Cisco IOS デバイスを設定するためのコンソール ケーブル
- トポロジで指定されているイーサネット ケーブル

パート 1: 基本的なネットワーク デバイスを設定する

パート 1 では、ネットワークを設定し、ホスト名、インターフェイス IP アドレス、パスワードなどの基本設定を構成します。

手順 1: ネットワークのケーブル配線を行います。

- a. トポロジに示すようにネットワークを配線する。
- b. PC-A からスイッチへのコンソール接続を確立します。

手順 2: スイッチの基本設定を構成する

この手順では、ホスト名や SVI への IP アドレスの設定など、スイッチの基本設定を構成します。スイッチへの IP アドレスの割り当ては、単なる最初の手順にすぎません。ネットワーク管理者は、スイッチの管理方法を指定する必要があります。Telnet と Secure Shell (SSH; セキュア シェル) は最も一般的に使われる管理手法ですが、Telnet は安全性が著しく低いプロトコルです。2 台のデバイス間でやり取りされる情報がすべてプレーン テキストで送信されます。パスワードや他の機密情報がパケット スニファによってキャプチャされると簡単に見られてしまいます。

- a. スイッチのコンフィギュレーション ファイルが NVRAM (NonVolatile Random-Access Memory; 不揮発性 RAM) に保存されていないものとし、スイッチのユーザ EXEC モード プロンプトで `Switch>` プロンプトが表示されるとします。特権 EXEC モードに切り替える。

```
Switch> enable
Switch#
```
- b. 特権 EXEC コマンド `show running-config` を使用してクリーン コンフィギュレーション ファイルを確認します。コンフィギュレーション ファイルが保存されている場合は削除してください。スイッチのモデルと IOS バージョンによっては、設定が少し異なることがあります。ただし、パスワードや IP アドレスが設定されていることはありません。スイッチにデフォルト設定が構成されていない場合は、インストラクタに問い合わせてください。
- c. グローバル コンフィギュレーション モードに入って、スイッチのホスト名を割り当てます。

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

- d. スイッチのパスワード アクセスを設定します。

```
S1(config)# enable secret class
S1(config)#
```
- e. 不要な DNS (Domain Name System) lookup を防止する

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

- f. ログインの Message of the Day (MOTD; 今日のお知らせ) バナーを設定します。

```
S1(config)# banner motd #  
Enter Text message. End with the character '#'.  
Unauthorized access is strictly prohibited. #
```

- g. モードを切り替えてアクセス設定を確認します。

```
S1(config)# exit  
S1#  
S1# exit  
Unauthorized access is strictly prohibited.  
S1>
```

グローバル コンフィギュレーション モードから特権 EXEC モードに直接移動するには、どのショートカット キーを使用しますか。

- h. ユーザ EXEC モードから特権 EXEC モードに戻ります。

```
S1> enable  
Password: class  
S1#
```

注: パスワードは入力時に画面に表示されません。

- i. グローバル コンフィギュレーション モードに入って、SVI の IP アドレスを設定してスイッチのリモート管理を可能にします。

```
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)#
```

- j. コンソール ポート アクセスを制限します。デフォルト設定では、すべてのコンソール接続をパスワードなしで行えるようになっています。

```
S1(config)# line con 0  
S1(config-line)# password cisco  
S1(config-line)# login  
S1(config-line)# exit  
S1(config)#
```

- k. スイッチの VTY (Virtual Terminal; 仮想端末) 回線を設定して、Telnet アクセスを許可します。VTY パスワードを設定していない場合、Telnet でスイッチにアクセスできません。

```
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
```

手順 3: PC-A の IP アドレスを設定する

- a. 1 ページの Addressing Table に示すように、PC に IP アドレスとサブネット マスクを割り当てます。Windows 7 を実行している PC に IP アドレスを割り当てる手順は、次のとおりです。
 - 1) Windows の [スタート] アイコン > [コントロール パネル] をクリックします。
 - 2) [表示方法] > [カテゴリ] をクリックします。
 - 3) [ネットワークの状態とタスクの表示] > [アダプタの設定の変更] を選択します。
 - 4) [ローカル エリア接続] を右クリックし、[プロパティ] を選択します。
 - 5) [インターネット プロトコル バージョン 4 (TCP/IPv4)] を選択し、[プロパティ] > [OK] をクリックします。
 - 6) [次の IP アドレスを使う] オプション ボタンをクリックし、IP アドレスとサブネット マスクを入力します。

パート 2: ネットワーク接続を確認およびテストする

次は、スイッチの設定を確認して文書を作成し、PC-A と S1 の間のエンドツーエンド接続をテストし、スイッチのリモート管理機能をテストします。

手順 1: S1 のデバイス設定を表示する

- a. PC-A で Tera Term を使用してコンソール接続に戻り、**show run** コマンドを発行してスイッチの設定を表示および確認します。次に示すのはサンプル設定です。ここで構成した設定は黄色で強調表示されています。それ以外は IOS のデフォルト設定です。

```
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 06YFDUHH6lwAE/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
```

- b. SVI 管理インターフェイスの状態を確認します。VLAN 1 インターフェイスは up/up で、IP アドレスが割り当てられている必要があります。また、スイッチ ポート F0/6 も PC-A が接続されているので up です。最初はすべてのスイッチ ポートが VLAN 1 内にあるので、デフォルトで、VLAN 1 用に設定した IP アドレスを使用してスイッチと通信できます。

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

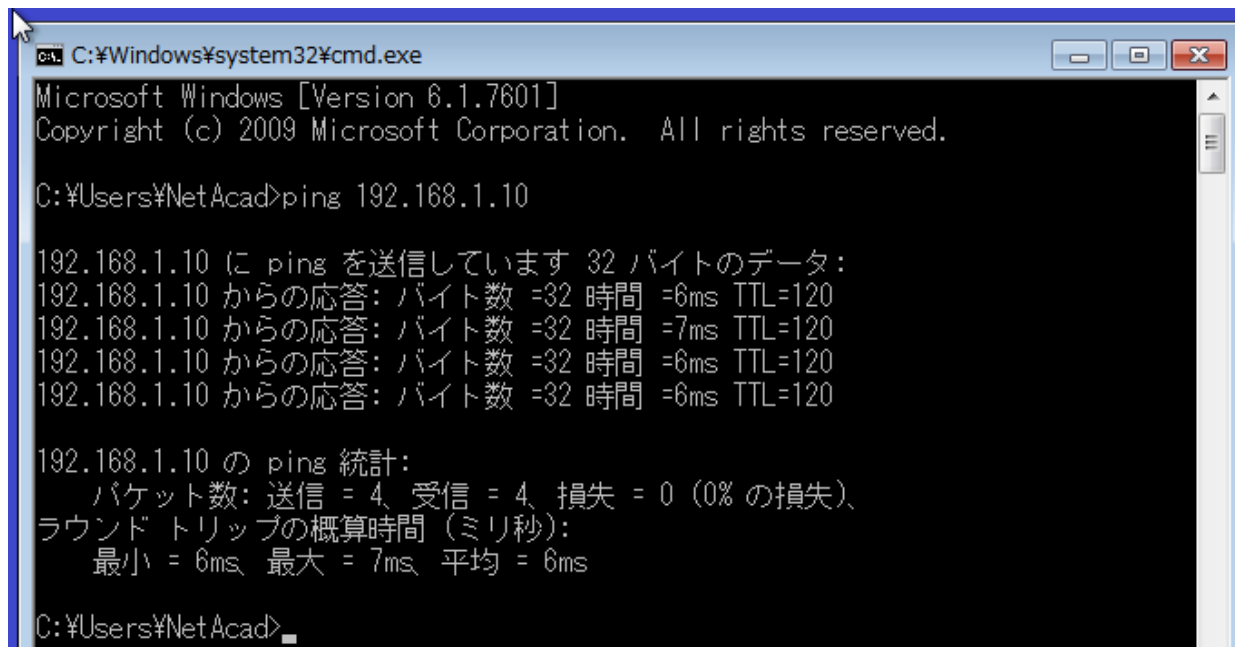
手順 2: エンドツーエンド接続をテストする。

PC-A で、Windows の [スタート] アイコンをクリックし、[プログラムとファイルの検索] フィールドに「cmd」と入力して、コマンド プロンプト ウィンドウ(cmd.exe)を開きます。ipconfig /all コマンドを使用して PC-A の IP アドレスを確認します。このコマンドは、PC のホスト名および IPv4 アドレスの情報を表示します。PC-A のアドレスと S1 の管理アドレスを ping します。

- a. 最初に PC-A のアドレスを ping します。

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

出力は次の画面のようになります。



```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.10

192.168.1.10 に ping を送信しています 32 バイトのデータ:
192.168.1.10 からの応答: バイト数 =32 時間 =6ms TTL=120
192.168.1.10 からの応答: バイト数 =32 時間 =7ms TTL=120
192.168.1.10 からの応答: バイト数 =32 時間 =6ms TTL=120
192.168.1.10 からの応答: バイト数 =32 時間 =6ms TTL=120

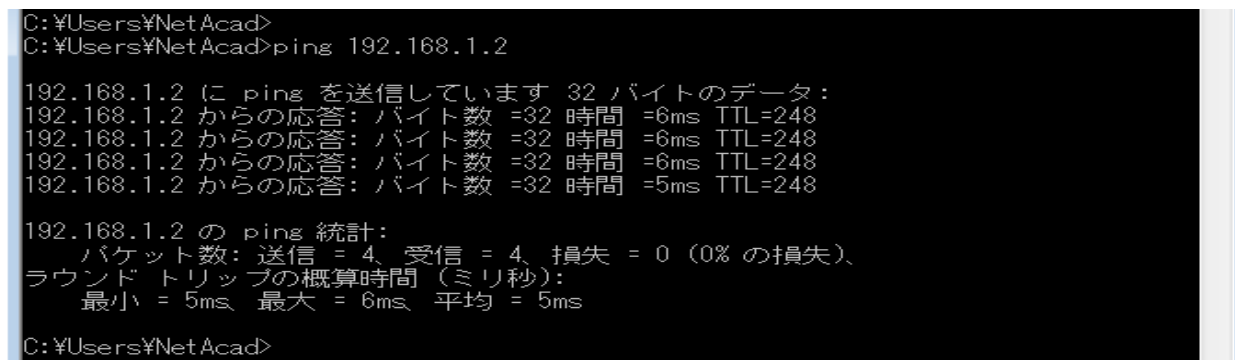
192.168.1.10 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 6ms、最大 = 7ms、平均 = 6ms

C:\Users\NetAcad>
  
```

- b. S1 の SVI 管理アドレスを ping します。

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

出力は次の画面のようになります。ping の結果が正しく得られない場合は、デバイスの基本設定のトラブルシューティングを行います。必要に応じて、物理的なケーブル配線と IP アドレスの両方を確認してください。



```

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

192.168.1.2 に ping を送信しています 32 バイトのデータ:
192.168.1.2 からの応答: バイト数 =32 時間 =6ms TTL=248
192.168.1.2 からの応答: バイト数 =32 時間 =6ms TTL=248
192.168.1.2 からの応答: バイト数 =32 時間 =6ms TTL=248
192.168.1.2 からの応答: バイト数 =32 時間 =5ms TTL=248

192.168.1.2 の ping 統計:
    パケット数: 送信 = 4、受信 = 4、損失 = 0 (0% の損失)、
ラウンド トリップの概算時間 (ミリ秒):
    最小 = 5ms、最大 = 6ms、平均 = 5ms

C:\Users\NetAcad>
  
```

手順 3: S1 のリモート管理をテストおよび確認する

次は、SVI 管理アドレスを使用するスイッチ S1 に Telnet でリモート アクセスします。この実習では、PC-A と S1 は並んで配置されています。実稼働ネットワークでは、最上階のワイヤリング クローゼットにスイッチがあり、管理 PC は 1 階にあると考えられます。Telnet は安全なプロトコルではありません。ただし、この実習では Telnet を使用してリモート アクセスをテストします。Telnet のセッションでは、パスワードやコマンドなどの情報がすべてプレーン テキストで送信されます。後の実習では、ネットワーク デバイスへのアクセスにセキュア シェル (SSH) を使用します。

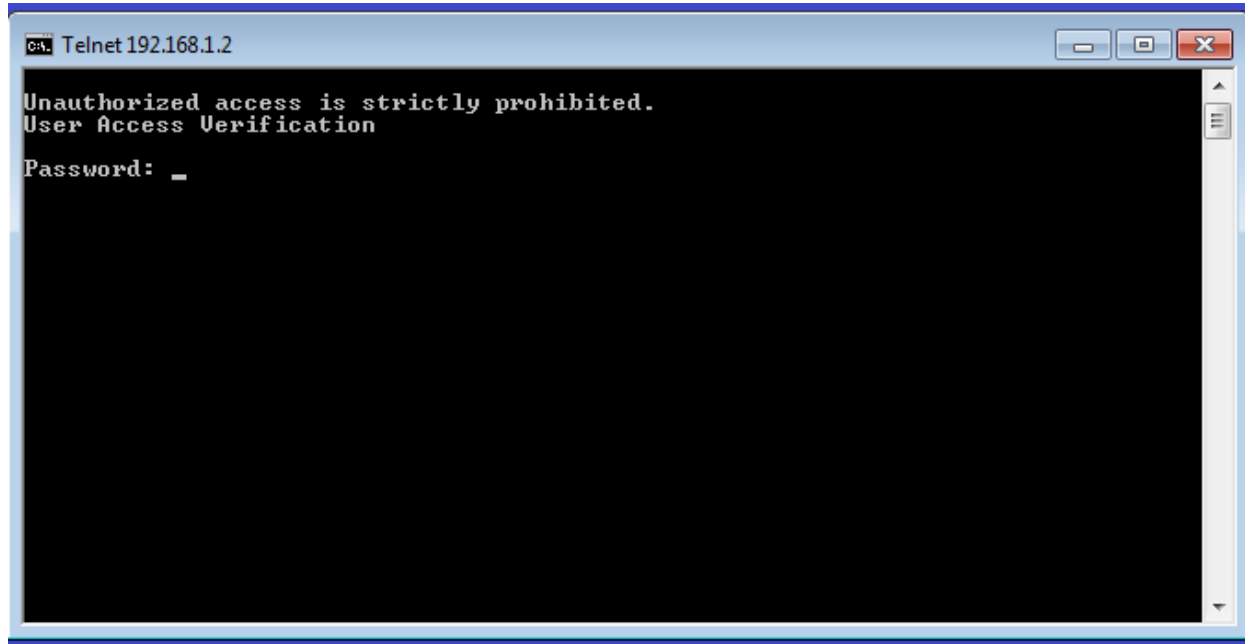
注: Windows 7 は、ネイティブで Telnet をサポートしていません。管理者はこのプロトコルを有効にする必要があります。Telnet クライアントをインストールするには、コマンド プロンプト ウィンドウを開き、「**pkgmgr /iu:"TelnetClient"**」と入力します。

```
C:\Users\NetAcad> pkgmgr /iu:"TelnetClient"
```

- a. PC-A でコマンド プロンプト ウィンドウを開いた状態で、Telnet コマンドを発行して、SVI 管理アドレスを介して S1 に接続します。パスワードは **cisco** です。

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

出力は次の画面のようになります。



- b. パスワード「**cisco**」を入力すると、ユーザ EXEC モード プロンプトが表示されます。プロンプトで「**enable**」と入力します。パスワード「**class**」と入力して特権 EXEC モードに入り、**show run** コマンドを発行します。

手順 4: コンフィギュレーション ファイルの保存

- a. Telnet セッションから、プロンプトで **copy run start** コマンドを発行します。

```
S1# copy run start
Destination filename [startup-config]? [Enter]
Building configuration ..
S1#
```

- b. 「**quit**」と入力して、Telnet セッションを終了します。Windows 7 コマンド プロンプトに戻ります。

復習

コンソール接続を使用して最初にスイッチを設定する必要があるのはなぜですか。Telnet または SSH を利用してスイッチに接続しないのはなぜですか。
