実習：スイッチのセキュリティ機能の設定

トポロジ

アドレス 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
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

学習目標

パート 1：トポロジの設定およびデバイスの初期化

パート 2：デバイスの基本設定と接続の確認

パート 3：S1 の SSH アクセスの設定と確認

- SSH アクセスを設定します。
- SSH パラメータを変更する。
- SSH の設定を確認します。

パート 4：S1 のセキュリティ機能の設定と確認

- 一般的なセキュリティ機能を設定および確認します。
- ポート セキュリティを設定および確認します。

背景/シナリオ

PC やサーバでアクセスをロック ダウンし、優れたセキュリティ機能をインストールすることは非常に一般的です。スイッチやルータなどのネットワーク インフラストラクチャ デバイスにもセキュリティ機能を設定する必要があります。

この実習では、いくつかのベスト プラクティスに従って、LAN スイッチにセキュリティ機能を設定します。SSH とセキュアな HTTPS セッションのみを許可します。また、スイッチによって認識されていない MAC アドレスを持つデバイスをロック アウトするためにポート セキュリティを設定して確認します。

注：CCNA の実習で使用するルータは、Cisco IOS Release 15.2（4）M3（universalk9 イメージ）を搭載した Cisco 1941 Integrated Services Router（ISR）です。使用するスイッチは、Cisco IOS Release 15.0(2)（lanbasek9 イメージ）を搭載した Cisco Catalyst 2960 です。他のルータ、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、使用できるコマンドと生成される出力が、実習とは異なる場合があります。正しいインターフェイス ID については、この実習の最後にあるルータインターフェイスの集約表を参照してください。

注：ルータとスイッチが消去され、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。わからない場合は、インストラクターに問い合わせるか、デバイスを初期化してリロードするための前の実習の手順を参照してください。

必要なリソース

- ルータ 1 台（Cisco IOS Release 15.2（4）M3 ユニバーサル イメージまたは同等イメージを搭載した Cisco 1941）
- スイッチ 1 台（Cisco IOS Release 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
- トポロジに示すようなイーサネット ケーブル

1. トポロジのセットアップとデバイスの初期化

パート 1 では、ネットワーク トポロジを設定し、必要に応じて構成をクリアします。

1. トポロジに示すようにネットワークを配線します。

2. ルータとスイッチを初期化してリロードします。

コンフィギュレーション ファイルがルータやスイッチに以前に保存されている場合は、デバイスを初期化してリロードし、基本設定に戻します。

2. デバイスの基本設定と接続の確認

パート 2 では、ルータ、スイッチ、および PC の基本設定を行います。デバイス名とアドレス情報については、この実習の最初にあるトポロジおよびアドレス テーブルを参照してください。

1. PC-A の IP アドレスを設定します。

2. R1 の基本設定を行います。

a. デバイス名を設定します。

b. DNS lookup をディセーブルにします。

c. アドレス テーブルに示されるように、インターフェイスの IP アドレスを設定します。

d. 特権 EXEC モード パスワードとして **class** を割り当てます。

e. コンソールおよび VTY パスワードとして **cisco** を割り当て、ログインをイネーブルにします。

f. プレーン テキスト パスワードを暗号化します。

g. 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

3. S1 の基本設定を行います。

優れたセキュリティ プラクティスでは、スイッチの管理 IP アドレスを VLAN 1 以外の VLAN（またはエンド ユーザが存在する他のデータ VLAN）に割り当てます。この手順では、スイッチの VLAN 99 を作成して、それに IP アドレスを割り当てます。

a. デバイス名を設定します。

b. DNS lookup をディセーブルにします。

c. 特権 EXEC モード パスワードとして **class** を割り当てます。

d. コンソールおよび VTY パスワードとして **cisco** を割り当て、ログインをイネーブルにします。

e. R1 の IP アドレスを使用して S1 のデフォルト ゲートウェイを設定します。

f. プレーン テキスト パスワードを暗号化します。

g. 実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

h. スイッチの VLAN 99 を作成し、**Management** という名前を付けます。

```
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

i. アドレス テーブルに示されるように、VLAN 99 の管理インターフェイスの IP アドレスを設定し、インターフェイスをイネーブルにします。

```
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
S1#
```

j. S1 で **show vlan** コマンドを実行します。VLAN 99 のステータスは何ですか?

_____

k. S1 に対して **show ip interface brief** コマンドを発行します。管理インターフェイス VLAN 99 のステータスとプロトコルは何ですか?

_____

VLAN 99 インターフェイスに対して **no shutdown** コマンドを実行しても、プロトコルがダウンしているのはなぜですか?

_____

l. ポート F0/5 および F0/6 をスイッチの VLAN 99 に割り当てます。

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
```

m. S1 に対して **show ip interface brief** コマンドを発行します。VLAN 99 インターフェイスのステータスとプロトコルはどのように示されていますか? _____

注：ポート ステートが収束するまでに遅延が生じることがあります。

4. デバイス間の接続を確認します。

a. PC-A から、R1 のデフォルト ゲートウェイ アドレスへ ping を実行します。ping は成功しましたか?

_____

b. PC-A から、S1 の管理アドレスへ ping を実行します。ping は成功しましたか? _____

c. S1 から、R1 のデフォルト ゲートウェイ アドレスへ ping を実行します。ping は成功しましたか?

_____

d. ~~PC-A で Web ブラウザを開き、http://172.16.99.11 に移動します。ユーザ名とパスワードの入力を求められたら、ユーザ名を空白のままにし、パスワードとして **class** を使用します。セキュリティ保護された接続であるか確認が求められたら、**No** と答えます。S1 の Web インターフェイスにアクセスできましたか?~~ _____

e. ~~PC-A のブラウザ セッションを閉じます。~~

~~**注**：Cisco 2960 スイッチのノンセキュア Web インターフェイス（HTTP サーバ）はデフォルトではイネーブルです。一般的なセキュリティ対策として、パート 4 で説明されているとおり、このサービスはディセーブルにします。~~

3. S1 の SSH アクセスの設定と確認

1. S1 の SSH アクセスを設定します。

a. S1 で SSH をイネーブルにします。グローバル コンフィギュレーション モードで、**CCNA-Lab.com** のドメイン名を作成します。

```
S1(config)# ip domain-name CCNA-Lab.com
```

b. SSH を介してスイッチに接続するときに使用するローカル ユーザ データベース エントリを作成します。ユーザには、管理レベルのアクセス権が必要です。

注：ここで使用するパスワードは強力なパスワードではありません。これは実習の目的でのみ使用されます。

```
S1(config)# username admin privilege 15 secret sshadmin
```

c. SSH 接続だけを許可するように VTY 回線の transport input を設定し、認証にローカル データベースを使用します。

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

d. 1024 ビットのモジュラスを使用して RSA 暗号キーを生成します。

```
S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

S1(config)#
S1(config)# end
```

e. SSH の設定を確認し、次の質問に答えてください。

```
S1# show ip ssh
```

スイッチが使用している SSH のバージョンはいくつですか? _____

SSH で許される認証試行は何回ですか? _____

SSH のデフォルトのタイムアウト設定はいくつですか? _____

2. S1 で SSH 設定を変更します。

デフォルトの SSH 設定を変更します。

```
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
```

SSH で許される認証試行は何回ですか? _____

SSH のタイムアウト設定はいくつですか? _____

3. S1 で SSH 設定を確認します。

a. PC-A で SSH クライアント ソフトウェアを使用して（Tera Term など）、S1 への SSH 接続を開きます。ホスト キーに関する SSH クライアントのメッセージが表示されたら、それを受け入れます。ユーザ名を **admin**、パスワードを **cisco** としてログインします。

接続は成功しましたか? _____

S1 にどのようなプロンプトが表示されましたか? 理由

_____

_____

b. 「**exit**」と入力し、S1 の SSH セッションを終了します。

4. S1 のセキュリティ機能の設定と確認

パート 4 では、未使用ポートをシャットダウンしてスイッチで実行されている特定のサービスをオフにし、MAC アドレスに基づいてポート セキュリティを設定します。スイッチは、MAC アドレス テーブルのオーバーフロー攻撃、MAC スプーフィング攻撃、およびスイッチ ポートへの無許可の接続の対象となる可能性があります。スイッチ ポートで学習可能な MAC アドレス数を制限し、その数を超えた場合にポートをディセーブルにするためのポート セキュリティを設定します。

1. S1 に一般的なセキュリティ機能を設定します。

a. S1 に、適切なセキュリティ警告メッセージを示す Message of The Day（MOTD）バナーを設定します。

b. S1 で **show ip interface brief** コマンドを実行します。どの物理ポートがアップの状態ですか?

_____

c. スイッチの未使用の物理ポートをすべてシャットダウンします。**interface range** コマンドを使用します。

```
S1(config)# interface range f0/1 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 - 2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

d. S1 に対して **show ip interface brief** コマンドを発行します。ポート F0/1 ～ F0/4 のステータスは何ですか?

_____

e. ~~**show ip http server status** コマンドを実行します。~~

HTTP サーバのステータスは何ですか? _____

どのサーバ ポートを使用していますか? _____

HTTP セキュア サーバのステータスは何ですか? _____

どのセキュア サーバ ポートを使用していますか? _____

f. HTTP セッションはすべてをプレーン テキストで送信しました。S1 で実行されている HTTP サービスをディセーブルにします。

```
S1(config)# no ip http server
```

g. PC-A で、http://172.16.99.11 への Web ブラウザ セッションを開きます。結果はどうでしたか?

_____

h. PC-A で、https://172.16.99.11 へのセキュアな Web ブラウザ セッションを開きます。証明書を受け入れます。ユーザ名なしで、パスワードを **class** としてログインします。結果はどうでしたか?

_____

i. PC-A の Web セッションを閉じます。

2. S1 にポート セキュリティを設定し確認します。

a. R1 の G0/1 の MAC アドレスを記録します。R1 の CLI で、**show interface g0/1** コマンドを使用して、インターフェイスの MAC アドレスを記録します。

```
R1# show interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is 30f7.0da3.1821 (bia
3047.0da3.1821)
```

R1 の G0/1 インターフェイスの MAC アドレスは何ですか?

_____

b. S1 の CLI から、特権 EXEC モードで **show mac address-table** コマンドを実行します。ポート F0/5 および F0/6 のダイナミック エントリを検索します。それらを以下に記録します。

F0/5 MAC アドレス：_____

F0/6 MAC アドレス：_____

c. 基本的なポート セキュリティを設定します。

注：この手順は通常、スイッチのすべてのアクセス ポートで実行されます。ここでは、例として F0/5 を取り上げます。

1)S1 の CLI で、R1 に接続するポートのインターフェイス コンフィギュレーション モードに切り替えます。

```
S1(config)# interface f0/5
```

2)ポートをシャットダウンします。

```
S1(config-if)# shutdown
```

3)F0/5 のポート セキュリティをイネーブルにします。

```
S1(config-if)# switchport port-security
```

注：**switchport port-security** コマンドを入力すると、MAC アドレスの最大数は 1 に、違反処理がシャットダウンに設定されます。**switchport port-security maximum** および **switchport port-security violation** コマンドを使用してデフォルトの動作を変更できます。

4)手順 2a で記録された R1 の G0/1 インターフェイスの MAC アドレスに対応するスタティック エントリを設定します。

```
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
```

（xxxx.xxxx.xxxx は、ルータの G0/1 インターフェイスの実際の MAC アドレスです）

注：オプションで、**switchport port-security mac-address sticky** コマンドを使用して、ポートで動的に学習されたすべてのセキュア MAC アドレス（設定された最大数まで）をスイッチの実行コンフィギュレーションに追加することができます。

5)スイッチ ポートをイネーブルにします。

```
S1(config-if)# no shutdown
S1(config-if)# end
```

d. **show port-security interface** コマンドを実行して S1 の F0/5 のポート セキュリティを確認します。

```
S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
```

F0/5 のポート ステータスは何ですか?

_____

e. R1 のコマンド プロンプトから、PC-A に ping を実行して接続を確認します。

```
R1# ping 172.16.99.3
```

f. 次に、ルータ インターフェイスの MAC アドレスを変更して、セキュリティに違反します。G0/1 のインターフェイス コンフィギュレーション モードに切り替え、それをシャットダウンします。

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
```

g. アドレスとして **aaaa.bbbb.cccc** を使用して、インターフェイスの新しい MAC アドレスを設定します。

```
R1(config-if)# mac-address aaaa.bbbb.cccc
```

h. 可能な場合は、この手順の実行と同時に、S1 でコンソール接続を開きます。S1 へのコンソール接続に、セキュリティ違反を示すさまざまなメッセージが表示されます。R1 の G0/1 インターフェイスをイネーブルにします。

```
R1(config-if)# no shutdown
```

i. R1 の特権 EXEC モードから、PC-A へ ping を実行します。ping は成功しましたか? その理由を述べてください。

_____

j. スイッチで、次に示す次のコマンドを使用してポート セキュリティを確認します。

```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
---------------------------------------------------------------------
      Fa0/5            1           1                1         Shutdown
---------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : aaaa.bbbb.cccc:99
Security Violation Count   : 1

S1# show interface f0/5
FastEthernet0/5 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05)
  MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
<出力を省略>

S1# show port-security address
               Secure Mac Address Table
------------------------------------------------------------------------
Vlan     Mac Address       Type                  Ports      Remaining Age
                                                            (mins)
```

```
----     -----------       ----                  -----   -------------
  99     30f7.0da3.1821    SecureConfigured      Fa0/5         -
-------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     :0
Max Addresses limit in System (excluding one mac per port) :8192
```

k. ルータで、G0/1 インターフェイスをシャットダウンし、ルータからハードコードされた MAC アドレスを削除して、G0/1 インターフェイスを再度イネーブルにします。

```
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown
R1(config-if)# end
```

l. R1 から、172.16.99.3 にある PC-A へ再度 ping を実行します。ping は成功しましたか? _____

m. ping の失敗の原因を判別するため、**show interface f0/5** コマンドを実行します。結果を記録します。

_____

n. S1 の F0/5 の error disabled ステータスをクリアします。

```
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown
S1(config-if)# no shutdown
```

注：ポート ステートが収束するまでに遅延が生じることがあります。

o. F0/5 が error disabled モードでないことを確認するために、S1 で **show interface f0/5** コマンドを実行します。

```
S1# show interface f0/5
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

p. R1 のコマンド プロンプトから、PC-A へ再度 ping を実行します。問題なく実行されます。

復習

1. なぜスイッチのポート セキュリティをイネーブルにするのですか?

_____

_____

2. スイッチの未使用ポートをディセーブルにする必要があるのはなぜですか?

_____

_____

ルータ インターフェイスの集約表

ルータ インターフェイスの集約				
ルータのモデル	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

注：ルータがどのように設定されているかを確認するには、インターフェイスを調べ、ルータの種類とルータが持つインターフェイスの数を識別します。各ルータ クラスの設定のすべての組み合わせを効果的に示す方法はありません。この表には、デバイスにイーサネットおよびシリアル インターフェイスの取り得る組み合わせに対する ID が記されています。その他のタイプのインターフェイスは、たとえ特定のルータに含まれている可能性があるものであっても、表には一切含まれていません。ISDN BRI インターフェイスはその一例です。カッコ内の文字列は、インターフェイスを表すために Cisco IOS コマンドで使用できる正規の省略形です。