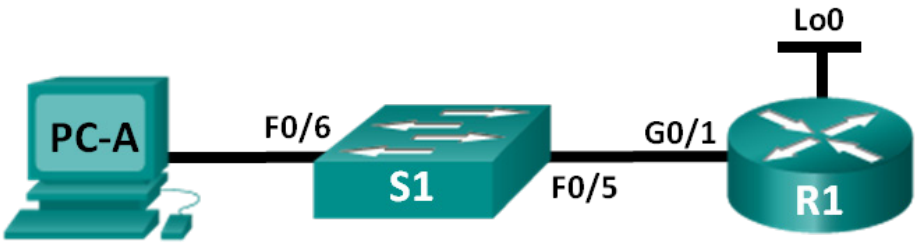
実習 - CLI を使用したネットワーク デバイス情報の収集

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
R1	G0/1	192.168.1.1	255.255.255.0	該当なし
	Lo0	209.165.200.225	255.255.255.224	該当なし
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

目的

パート 1:トポロジを設定してデバイスを初期化する

- ネットワーク トポロジに合わせて機器をセットアップします。
- ルータとスイッチを初期化してリロードします。

パート 2:デバイスを設定して接続を確認する

- PC-A NIC に固定 IP アドレスを割り当てます。
- R1 に基本情報を設定します。
- S1 の基本設定を行います。
- ネットワーク接続を確認します。

パート 3:ネットワーク デバイス情報を収集する

- IOS CLI コマンドを使用して R1 の情報を収集します。
- IOS CLI コマンドを使用して S1 の情報を収集します。
- コマンド プロンプト CLI を使用して PC-A の情報を収集します。

背景/シナリオ

稼働中のネットワークについて文書化することは、ネットワーク専門家が行う最も重要な作業の 1 つです。IP アドレス、モデル番号、IOS のバージョン、使用ポートを適切に文書化し、セキュリティのテストを行うことは、ネットワークのトラブルシューティングに大いに役立ちます。

この実習では、ルータ、スイッチ、PC 上でさまざまなコマンドを発行することで、小規模なネットワークを構築し、デバイスの設定、基本的なセキュリティ機能の追加、設定の文書化を行います。

注:CCNA のラボ演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。また、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、ラボ演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、このラボ演習の最後にあるルータ インターフェイスの要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。不明な場合は、インストラクタに問い合わせてください。

実習に必要なリソースや機器

- 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 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:　トポロジを設定し、デバイスを初期化する

パート 1 では、ネットワーク トポロジをセットアップし、必要に応じて設定をクリアし、ルータとスイッチの基本設定を行います。

手順 1:　トポロジに示すようにネットワークを配線します。

a. トポロジに示すようにデバイスを接続し、必要に応じてケーブル配線を行います。

b. トポロジ内のすべてのデバイスの電源を入れます。

手順 2:　ルータとスイッチを初期化してリロードします。

パート 2:　デバイスを設定し、接続を確認する

パート 2 では、ネットワーク トポロジを設定し、ルータとスイッチ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。

注: 付録 A にはパート 2 の各手順の設定の詳細が記されています。まずは、この付録を見ないでパート 2 を完了できるか試してください。

手順 1:　PC の IPv4 アドレスを設定します。

アドレス テーブルに基づいて、PC-A の IPv4 アドレス、サブネット マスク、デフォルト ゲートウェイ アドレスを設定します。

手順 2:　ルータを設定します。

手順 2 について詳しい説明が必要であれば、付録 A を参照してください。

a. ルータにコンソール接続し、特権 EXEC モードに入ります。

b. ルータに正しい時刻を設定します。

c. グローバル コンフィギュレーション モードに切り替えます。

   1) トポロジとアドレス テーブルに基づいて、ルータにデバイス名を割り当てます。

   2) DNS lookup を無効にします。

   3) デバイスにアクセスしようとする人に対して不正アクセスは許可されないと警告する MOTD バナーを作成します。

   4) 特権 EXEC の暗号化パスワードとして **class** を割り当てます。

   5) コンソール パスワードとして **cisco** を割り当て、コンソール ログイン アクセスを有効化します。

   6) クリア テキスト パスワードを暗号化します。

   7) SSH アクセス用に、**cisco.com** というドメイン名を作成します。

   8) SSH アクセス用に、**admin** という名前のユーザを作成して秘密のパスワードを **cisco** とします。

   9) RSA モジュール キーを生成します。ビット数は **512** とします。

d. vty 回線のアクセスを設定します。

   1) SSH 用の認証にはローカル データベースを使用します。

   2) ログイン アクセスには SSH のみを有効にします。

e. グローバル コンフィギュレーション モードに戻ります。

   1) ループバック 0 インターフェイスを作成し、アドレス テーブルに基づいて IP アドレスを割り当てます。

   2) ルータ上にインターフェイス G0/1 を設定し、アクティブにします。

   3) G0/1 および Lo0 のインターフェイス説明を設定します。

   4) 実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルに保存します。

手順 3:　スイッチを設定します。

手順 3 について詳しい説明が必要であれば、付録 A を参照してください。

a. スイッチにコンソール接続し、特権 EXEC モードに入ります。

b. スイッチに正しい時刻を設定します。

c. グローバル コンフィギュレーション モードに切り替えます。

   1) トポロジとアドレス テーブルに基づいて、スイッチにデバイス名を割り当てます。

   2) DNS lookup を無効にします。

   3) デバイスにアクセスしようとする人に対して不正アクセスは許可されないと警告する MOTD バナーを作成します。

   4) 特権 EXEC の暗号化パスワードとして **class** を割り当てます。

   5) クリア テキスト パスワードを暗号化します。

   6) SSH アクセス用に、**cisco.com** というドメイン名を作成します。

   7) SSH アクセス用に、**admin** という名前のユーザを作成して秘密のパスワードを **cisco** とします。

   8) RSA モジュール キーを生成します。ビット数は **512** とします。

   9) スイッチ上で、トポロジとアドレス テーブルに基づいて IP アドレスを作成し、アクティブにします。

   10) スイッチ上でデフォルト ゲートウェイを設定します。

   11) コンソール パスワードとして **cisco** を割り当て、コンソール ログイン アクセスを有効化します。

d. vty 回線のアクセスを設定します。

   1) SSH 用の認証にはローカル データベースを使用します。

   2) ログイン アクセスには SSH のみを有効にします。

   3) F0/5 および F0/6 のインターフェイス説明を設定するために適切なモードに入ります。

   4) 実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルに保存します。

手順 4:　ネットワーク接続を確認します。

a. PC-A 上のコマンド プロンプトから、S1 VLAN 1 の IP アドレスに対して ping を実行します。ping が成功しなかった場合は、物理設定と論理設定のトラブルシューティングをします。

b. PC-A のコマンド プロンプトから、R1 上のデフォルト ゲートウェイ IP アドレスに対して ping を実行します。ping が成功しなかった場合は、物理設定と論理設定のトラブルシューティングをします。

c. PC-A のコマンド プロンプトから、R1 上のループバック インターフェイスに対して ping を実行します。ping が成功しなかった場合は、物理設定と論理設定のトラブルシューティングをします。

d. スイッチにコンソール接続し、R1 上の G0/1 の IP アドレスに対して ping を実行します。ping が成功しなかった場合は、物理設定と論理設定のトラブルシューティングをします。

パート 3:　ネットワーク デバイス情報を収集する

パート 3 では、さまざまなコマンドを使用して、ネットワーク上のデバイスとパフォーマンス特性に関する情報を収集します。ネットワーク文書は、ネットワークを管理するうえで非常に重要な要素です。物理トポロジと論理トポロジの両方を文書化し、ネットワーク デバイスのプラットフォーム モデルと IOS のバージョンを確認することが重要です。こうした情報を収集する適切なコマンドを知っていることは、ネットワーク専門家にとっての必須条件です。

手順 1:　IOS コマンドを使用して R1 の情報を収集します。

最も基本的な手順の 1 つは、物理デバイスの情報と OS の情報を収集することです。

a. 適切なコマンドを発行して、次の情報を取得します。

ルータのモデル:

IOS のバージョン:

RAM の総容量:

NVRAM の総容量:

フラッシュ メモリの総容量:

IOS イメージ ファイル:

コンフィギュレーション レジスタ:

テクノロジー パッケージ:

この情報を収集するために、どのコマンドを発行しましたか。

b. ルータ インターフェイスに関する重要な情報の要約を表示するために、適切なコマンドを発行します。以下に、使用するコマンドと実行結果を記入してください。

注:IP アドレスを持つインターフェイスの情報のみを記入してください。

c. ルーティング テーブルを表示するために、適切なコマンドを発行します。以下に、使用するコマンドと実行結果を記入してください。

d. ルータ上で行われるレイヤ 2 からレイヤ 3 へのアドレス マッピングを表示するには、どのコマンドを使用しますか。以下に、使用するコマンドと実行結果を記入してください。

e. ルータ上のすべてのインターフェイスまたは特定のインターフェイスに関する詳しい情報を表示するには、どのコマンドを使用しますか。以下に、使用するコマンドを記入してください。

f. シスコは、OSI モデルのレイヤ 2 で機能する強力なプロトコルを提供しています。このプロトコルは、シスコ デバイスの物理的な接続を計画したり、モデル番号、IOS のバージョン、IP アドレスを特定する際に役立ちます。以下のテーブルの空欄を埋めるために、スイッチ S1 に関する情報を収集するには、ルータ R1 上でどのコマンドを使用しますか。

デバイス ID	ローカル インターフェイス	機能	モデル番号	リモート ポート ID	IP アドレス	IOS バージョン

コマンド:

g. ネットワーク デバイスのごく初歩的なテスト方法の 1 つに、Telnet で接続できるかどうかを確認するというものがあります。ただし、Telnet は安全なプロトコルではないので注意が必要です。通常は、Telnet を有効にすべきではありません。Tera Term や PuTTY などの Telnet クライアントを使用し、デフォルト ゲートウェイ IP アドレスを使用して R1 に Telnet で接続してみます。実行結果を以下に記入します。

h. PC-A から、SSH が正しく動作していることを確認するためのテストをします。Tera Term や PuTTY などの SSH クライアントを使用して、PC-A から R1 に SSH で接続します。キーが異なるという警告メッセージが表示された場合は、[**Continue**] をクリックします。パート 2 で作成した適切なユーザ名とパスワードを使用してログインします。正常にできましたか。

ルータに設定する各種パスワードは、できる限り強力で保護されたものにする必要があります。

注:実習で使用するパスワード(**cisco** および **class**)は、強力なパスワードに必要とされるベスト プラクティスに従っていません。これらは実習の利便性のみを考えて作成されたパスワードです。デフォルトでは、コンフィギュレーション ファイル内のコンソール パスワードと vty パスワードはクリアテキストで表示されます。

i. コンフィギュレーション ファイル内のすべてのパスワードが暗号化されていることを確認します。以下に、使用するコマンドと実行結果を記入してください。

コマンド:

コンソール パスワードは暗号化されていますか。

SSH パスワードは暗号化されていますか。

手順 2:　IOS コマンドを使用して S1 の情報を収集します。

R1 上で使用したコマンドの多くは、このスイッチでも使用できます。ただし、一部のコマンドには違いがあります。

a. 適切なコマンドを発行して、次の情報を取得します。

スイッチのモデル:

IOS のバージョン:

NVRAM の総容量:

IOS イメージ ファイル:

この情報を収集するために、どのコマンドを発行しましたか。

b. スイッチ インターフェイスに関する重要な情報の要約を表示するために、適切なコマンドを発行します。以下に、使用するコマンドと実行結果を記入してください。

注: アクティブなインターフェイスの情報だけを記入します。

c. スイッチの MAC アドレス テーブルを表示するための適切なコマンドを発行します。以下に、動的な MAC アドレスのみを記入してください。

d. S1 上で Telnet VTY アクセスが無効になっていることを確認します。Tera Term や PuTTY などの Telnet クライアントを使用し、アドレス 192.168.1.11 を使用して S1 に Telnet で接続してみます。実行結果を以下に記入します。

e. PC-A から、SSH が正しく動作していることを確認するためのテストをします。Tera Term や PuTTY などの SSH クライアントを使用して、PC-A から S1 に SSH で接続します。キーが異なるという警告メッセージが表示された場合は、[**Continue**] をクリックします。適切なユーザ名とパスワードを使用してログインします。正常にできましたか。

f. S1 上で適切なコマンドを使用して、ルータ R1 に関する情報を以下の表の空欄に記入します。

デバイス ID	ローカル インターフェイス	機能	モデル番号	リモート ポート ID	IP アドレス	IOS バージョン

g. コンフィギュレーション ファイル内のすべてのパスワードが暗号化されていることを確認します。以下に、使用するコマンドと実行結果を記入してください。

コマンド:

コンソール パスワードは暗号化されていますか。

手順 3: PC-A 上で情報を収集します。

さまざまな Windows ユーティリティ コマンドを使用して、PC-A に関する情報を収集します。

a. PC-A のコマンド プロンプトから **ipconfig /all** コマンドを発行し、以下に答えを記入します。

PC-A の IP アドレスは何ですか。

PC-A のサブネット マスクは何ですか。

PC-A のデフォルト ゲートウェイ アドレスは何ですか。

PC-A の MAC アドレスは何ですか。

b. この NIC で TCP/IP プロトコル スタックをテストするために、適切なコマンドを発行します。どのコマンドを使用しましたか。

c. PC-A のコマンド プロンプトから、R1 のループバック インターフェイスに対して ping を実行します。ping は成功しましたか。

d. PC-A から R1 上のループバック インターフェイスに向けて生成されるパケットのルータ ホップのリストをトレースするために、PC-A 上で適切なコマンドを発行します。以下に、使用するコマンドと出力を記入してください。どのコマンドを使用しましたか。

e. NIC 上で行われているレイヤ 2 からレイヤ 3 へのアドレス マッピングの情報を表示するために、PC-A 上で適切なコマンドを発行します。以下に答えを記入してください。192.168.1.0/24 ネットワークに関する情報のみを記入します。どのコマンドを使用しましたか。

復習

ネットワーク デバイスの文書化が重要である理由を説明してください。

ルータ インターフェイスの要約表

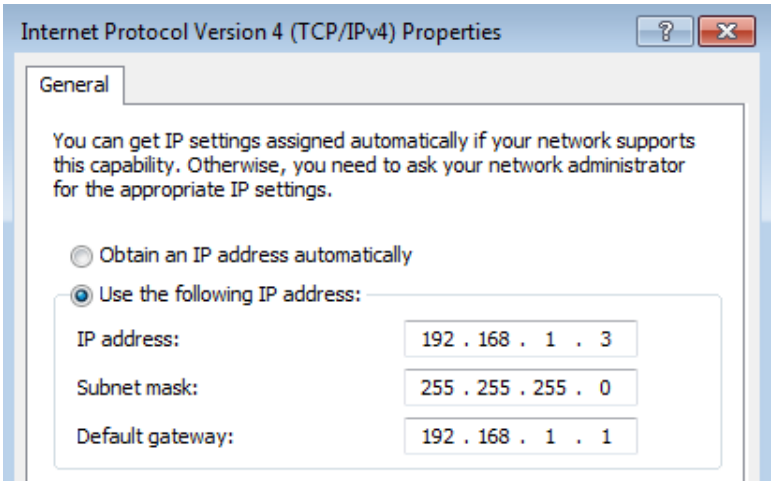
ルータ インターフェイスの要約				
ルータのモデル	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (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、インターフェイスに着目し、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リストする方法はありません。この表は、デバイス上のイーサネット インターフェイスとシリアル インターフェイスの考え得る組み合わせの識別情報を示しています。この表には他のタイプのインターフェイスは含まれていませんが、特定のルータにそうしたインターフェイスが装備される可能性はあります。ISDN BRI インターフェイスはその一例です。かっこ内の文字列は、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。

付録 A: パート 2 の各手順の設定の詳細

手順 1: PC の IPv4 アドレスを設定します。

この実習の最初にあるアドレス テーブルに基づいて、PC-A の IPv4 アドレス、サブネット マスク、デフォルト ゲートウェイ アドレスを設定します。



手順 2: ルータを設定します。

a. ルータにコンソール接続し、特権 EXEC モードに入ります。

```
Router> enable
Router#
```

b. ルータに正しい時刻を設定します。

```
Router# clock set 10:40:30 6 February 2013
Router#
```

c. グローバル コンフィギュレーション モードに切り替えます。

```
Router# config t
Router(config)#
```

1) ルータにホスト名を割り当てます。前掲のトポロジとアドレス テーブルに従ってください。

```
Router(config)# hostname R1
R1(config)#
```

2) DNS lookup を無効にします。

```
R1(config)# no ip domain-lookup
```

3) デバイスにアクセスしようとする人に対して不正アクセスは許可されないと警告する MOTD バナーを作成します。

```
R1(config)# banner motd #Warning! Unauthorized Access is prohibited.#
```

4) 特権 EXEC の暗号化パスワードとして **class** を割り当てます。

```
R1(config)# enable secret class
```

5) コンソール パスワードとして **cisco** を割り当て、コンソール ログイン アクセスを有効化します。

```
R1(config)# line con 0
R1(config-line)# password cisco
R1(config-line)# login
```

6) クリア テキスト パスワードを暗号化します。

```
R1(config)# service password-encryption
```

7) SSH アクセス用に、**cisco.com** というドメイン名を作成します。

```
R1(config)# ip domain-name cisco.com
```

8) SSH アクセス用に、**admin** という名前のユーザを作成して秘密のパスワードを **cisco** とします。

```
R1(config)# username admin secret cisco
```

9) RSA モジュール キーを生成します。ビット数は **512** とします。

```
R1(config)# crypto key generate rsa modulus 512
```

d. vty 回線のアクセスを設定します。

1) SSH 用の認証にはローカル データベースを使用します。

```
R1(config)# line vty 0 4
R1(config-line)# login local
```

2) ログイン アクセスには SSH のみを有効にします。

```
R1(config-line)# transport input ssh
```

e. グローバル コンフィギュレーション モードに戻ります。

```
R1(config-line)# exit
```

1) ループバック 0 インターフェイスを作成し、アドレス テーブルに基づいて IP アドレスを割り当てます。

```
R1(config)# interface loopback 0
R1(config-if)# ip address 209.165.200.225 255.255.255.224
```

2) ルータ上にインターフェイス G0/1 を設定し、アクティブにします。

```
R1(config-if)# int g0/1
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shut
```

3) G0/1 および Lo0 のインターフェイス説明を設定します。

```
R1(config-if)# description Connected to LAN
R1(config-if)# int lo0
R1(config-if)# description Emulate ISP Connection
```

4) 実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルに保存します。

```
R1(config-if)# end
R1# copy run start
```

手順 3： スイッチを設定します。

a. スイッチにコンソール接続し、特権 EXEC モードに入ります。

```
Switch> enable
Switch#
```

b. スイッチに正しい時刻を設定します。

```
Switch# clock set 10:52:30 6 February 2013
```

c. グローバル コンフィギュレーション モードに切り替えます。

```
Switch# config t
```

1) トポロジとアドレス テーブルに基づいて、スイッチにホスト名を割り当てます。

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

2) DNS lookup を無効にします。

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

3) デバイスにアクセスしようとする人に対して不正アクセスは許可されないと警告する MOTD バナーを作成します。

```
S1(config)# banner motd #Warning! Unauthorized access is prohibited.#
```

4) 特権 EXEC の暗号化パスワードとして **class** を割り当てます。

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

5) クリア テキスト パスワードを暗号化します。

```
S1(config)# service password-encryption
```

6) SSH アクセス用に、**cisco.com** というドメイン名を作成します。

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

7) SSH アクセス用に、**admin** という名前のユーザを作成して秘密のパスワードを **cisco** とします。

```
S1(config)# username admin secret cisco
```

8) RSA モジュール キーを生成します。ビット数は **512** とします。

```
S1(config)# crypto key generate rsa modulus 512
```

9) スイッチ上で、トポロジとアドレス テーブルに基づいて IP アドレスを作成し、アクティブにします。

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.11 255.255.255.0
S1(config-if)# no shut
```

10) スイッチ上でデフォルト ゲートウェイを設定します。

```
S1(config)# ip default-gateway 192.168.1.1
```

11) コンソール パスワードとして **cisco** を割り当て、コンソール ログイン アクセスを有効化します。

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

d. vty 回線のアクセスを設定します。

1) SSH 用の認証にはローカル データベースを使用します。

```
S1(config-line)# line vty 0 15
S1(config-line)# login local
```

2) ログイン アクセスには SSH のみを有効にします。

```
S1(config-line)# transport input ssh
```

3) F0/5 および F0/6 のインターフェイス説明を設定するために適切なコンフィギュレーション モードに入ります。

```
S1(config-line)# int f0/5
S1(config-if)# description Connected to R1
S1(config-if)# int f0/6
S1(config-if)# description Connected to PC-A
```

4) 実行コンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルに保存します。

```
S1(config-if)# end
S1# copy run start
```