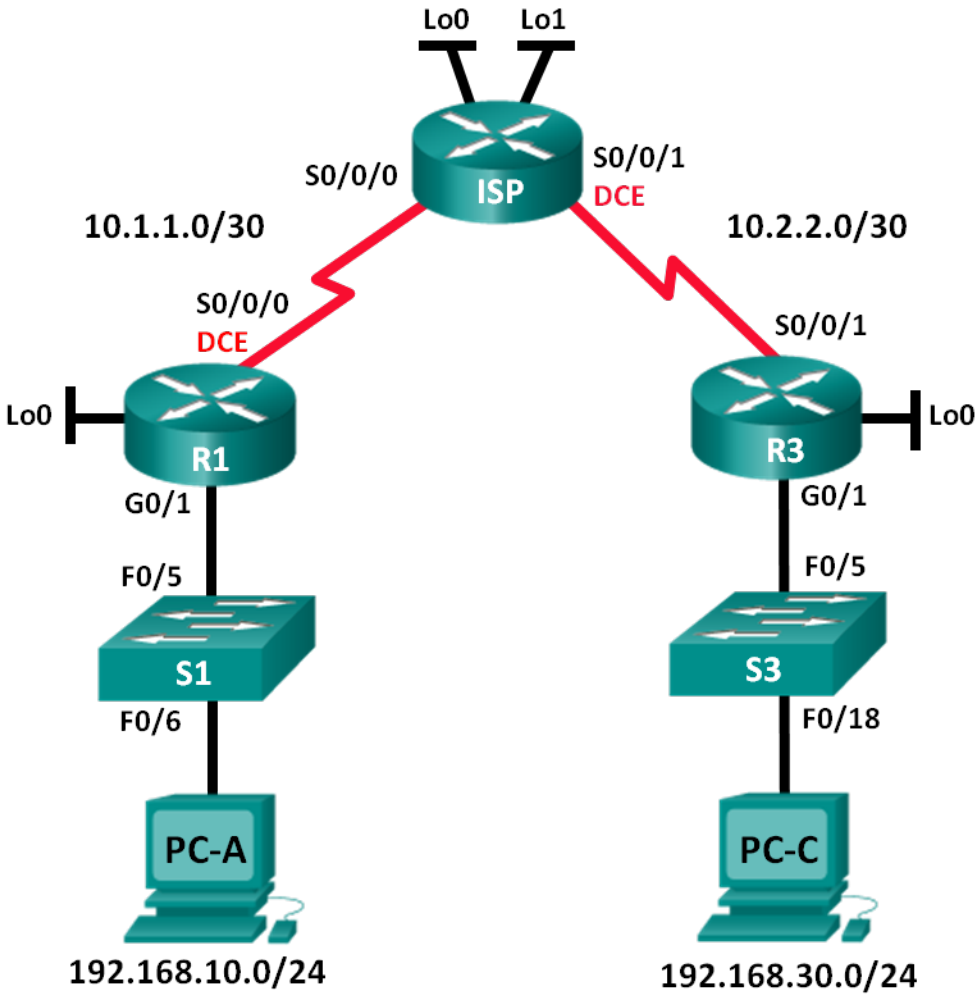
実習：拡張 ACL の設定と確認

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	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	209.165.201.1	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

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：デバイスの設定および接続の確認

- PC、ルータ、およびスイッチの基本設定を行います。
- R1、ISP、および R3 に RIP ルーティングを設定します。

パート 3：拡張番号付きおよび名前付き ACL の設定と確認

- 番号付き拡張 ACL を設定、適用、および確認します。
- 名前付き拡張 ACL を設定、適用、および確認します。

パート 4：拡張 ACL の修正および確認

背景/シナリオ

拡張アクセス コントロール リスト（ACL）は非常に強力です。これらは、フィルタ可能なトラフィックのタイプ、トラフィックの発信元および宛先に関して、標準 ACL よりもはるかに強力な制御を提供します。

この実習では、R1 と R3 によって表される 2 か所のオフィスのフィルタリング ルールをセットアップします。管理者は R1 と R3 の LAN 間のアクセス ポリシーを確立していて、これを実装する必要があります。

R1 と R3 の間に存在する ISP ルータには ACL は実装されません。制御および管理できるのは所有する機器のみであるため、ISP ルータへの管理アクセスは許可されていません。

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。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、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。不明な場合は、インストラクターに相談してください。

必要なリソース

- ルータ 3 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 2 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 2 台（Tera Term など、ターミナル エミュレーション プログラムを備えた Windows 7、Vista、または XP 搭載 PC）
- 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 ケーブルとシリアル 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設定し、リロードします。

2. デバイスの設定と接続の確認

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。デバイス名およびアドレス情報についてはトポロジとアドレス テーブルを参照してください。

1. PC-A と PC-C 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. DNS lookup をディセーブルにします。

b. トポロジに示すようにデバイス名を設定します。

c. R1 のループバック インターフェイスを作成します。

d. トポロジとアドレス テーブルに示されているように、インターフェイスの IP アドレスを設定します。

e. 特権 EXEC モードのパスワードとして **class** を設定します。

f. S0/0/0 インターフェイスのクロック レートを **128000** に割り当てます。

g. コンソールと VTY パスワードとして **cisco** を割り当て、Telnet アクセスをイネーブルにします。コンソールおよび VTY 回線の両方の**ロギングの同期**を設定します。

h. ~~**admin** ユーザのローカル認証で Web サーバをシミュレートするため、R1 の Web アクセスをイネーブルにします。~~

```
R1(config)# ip http server
R1(config)# ip http authentication local
R1(config)# username admin privilege 15 secret class
```

3. ISP の基本設定を行います。

a. トポロジに示すようにデバイス名を設定します。

b. ISP のループバック インターフェイスを作成します。

c. トポロジとアドレス テーブルに示されているように、インターフェイスの IP アドレスを設定します。

d. DNS lookup をディセーブルにします。

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

f. S0/0/1 インターフェイスのクロック レートを **128000** に割り当てます。

g. コンソールと VTY パスワードとして **cisco** を割り当て、Telnet アクセスをイネーブルにします。コンソールおよび VTY 回線の両方の**ロギングの同期**を設定します。

h. ~~ISP の Web アクセスをイネーブルにします。手順 2h と同じパラメータを使用します。~~

4. R3 の基本設定を行います。

a. トポロジに示すようにデバイス名を設定します。

b. R3 ループバック インターフェイスを作成します。

c. トポロジとアドレス テーブルに示されているように、インターフェイスの IP アドレスを設定します。

d. DNS lookup をディセーブルにします。

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

f. コンソール パスワードとして **cisco** を割り当て、コンソール回線の**ロギングの同期**を設定します。

g. R3 で SSH をイネーブルにします。

```
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa          ← 対話モードで modulus を 1024 に設定
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

h. ~~R3 上で Web アクセスをイネーブルにします。手順 2h と同じパラメータを使用します。~~

5. （オプション）S1 および S3 の基本設定を行います。

a. トポロジに示すようにホスト名を設定します。

b. トポロジとアドレス テーブルに示されているように、管理インターフェイスの IP アドレスを設定します。

c. DNS lookup をディセーブルにします。

d. 特権 EXEC モードのパスワードとして **class** を設定します。

e. デフォルト ゲートウェイのアドレスを設定します。

6. R1、ISP、および R3 に RIP ルーティングを設定します。

a. 自律システム（AS）番号 10 を設定し、R1、ISP、および R3 上のすべてのネットワークにアドバタイズします。自動集約をディセーブルにします。

b. R1、ISP、および R3 に RIP を設定した後、すべてのルータにすべてのネットワークがリストされた完全なルーティング テーブルがあることを確認します。そうでない場合はトラブルシューティングします。

7. デバイス間の接続を確認します。

注：ACL を設定および適用する**前に**、接続を確認することが非常に重要です。トラフィックのフィルタを開始する前に、ネットワークが適切に機能していることを確認します。

a. PC-A から、PC-C および R3 のループバック インターフェイスとシリアル インターフェイスへ ping を実行します。

ping は成功しましたか? _____

b. R1 から、PC-C および R3 のループバック インターフェイスとシリアル インターフェイスへ ping を実行します。

ping は成功しましたか? _____

c. PC-C から、PC-A および R1 のループバック インターフェイスとシリアル インターフェイスへ ping を実行します。

ping は成功しましたか? _____

d. R3 から、PC-A および R1 のループバック インターフェイスとシリアル インターフェイスへ ping を実行します。

ping は成功しましたか? _____

e. PC-A から、ISP ルータのループバック インターフェイスへ ping を実行します。

ping は成功しましたか? _____

f. PC-C から、ISP ルータのループバック インターフェイスへ ping を実行します。

ping は成功しましたか? _____

g. ~~PC-A で Web ブラウザを開き、ISP の http://209.165.200.225 に移動します。ユーザ名とパスワードの入力を求められます。ユーザ名として **admin**、パスワードとして **class** を使用します。シグニチャを受け入れるように促すメッセージが表示されたら、これを受け入れます。ルータによって、別ウィンドウに~~

Cisco Configuration Professional（CCP）Express がロードされます。ユーザ名とパスワードの入力を求められます。ユーザ名として **admin**、パスワードとして **class** を使用します。

h. PC-C で Web ブラウザを開き、R1 の http://10.1.1.1 に移動します。ユーザ名とパスワードの入力を求められます。ユーザ名として **admin**、パスワードとして **class** を使用します。シグニチャを受け入れるように促すメッセージが表示されたら、これを受け入れます。ルータによって、別ウィンドウに CCP Express がロードされます。ユーザ名とパスワードの入力を求められます。ユーザ名として **admin**、パスワードとして **class** を使用します。

3. 拡張の番号付き ACL および名前付き ACL の設定と確認

拡張 ACL はさまざまな方法でトラフィックをフィルタできます。拡張 ACL は、発信元 IP アドレス、発信元ポート、宛先 IP アドレス、宛先ポート、およびさまざまなプロトコルとサービスに基づいてフィルタできます。

セキュリティ ポリシーは次のとおりです。

1. 192.168.10.0/24 ネットワークから任意のネットワーク宛てに発信された Web トラフィックを許可します。
2. PC-A から R3 のシリアル インターフェイスへの SSH 接続を許可します。
3. 192.168.10.0.24 ネットワークのユーザによる 192.168.20.0/24 ネットワークへのアクセスを許可します。
4. 192.168.30.0/24 ネットワークから発信された Web トラフィックによる ISP の Web インターフェイスおよび 209.165.200.224/27 ネットワークを介した R1 へのアクセスを許可します。192.168.30.0/24 ネットワークは、Web を介した他のネットワークへのアクセスは一切許可されません。

上記のセキュリティ ポリシーを見ると、セキュリティ ポリシーを満たすために少なくとも 2 つの ACL が必要です。ベスト プラクティスは、できるだけ発信元の近くに拡張 ACL を配置することです。これらのポリシーの場合も、このプラクティスに従います。

1. セキュリティ ポリシーの 1 および 2 に対応する番号付き拡張 ACL を R1 で設定します。

R1 で番号付き拡張 ACL を使用します。拡張 ACL の範囲はいくつですか?

_____

a. R1 に ACL を設定します。ACL 番号として 100 を使用します。

```
R1(config)# access-list 100 remark Allow Web & SSH Access
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
R1(config)# access-list 100 permit tcp any any eq 80
```

上記のコマンド出力で 80 は何を示していますか?

_____

ACL 100 は、どのインターフェイスに適用する必要がありますか?

_____

_____

ACL 100 は、どの方向に適用する必要がありますか?

_____

_____

b. ACL 100 を S0/0/0 インターフェイスに適用します。

```
R1(config)# int s0/0/0
R1(config-if)# ip access-group 100 out
```

c. ACL 100 を確認します。

1) ~~PC-A で Web ブラウザを開き、http://209.165.200.225（ISP ルータ）にアクセスします。通常は成功します。成功しない場合は、トラブルシューティングします。~~

2) IP アドレスの 10.2.2.1 を使用して PC-A から R3 への SSH 接続を確立します。資格情報として、**admin** と **class** を使用してログインします。通常は成功します。成功しない場合は、トラブルシューティングします。

3) R1 で特権 EXEC モードのプロンプトから、**show access-lists** コマンドを実行します。

```
R1# show access-lists
Extended IP access list 100
    10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)
    20 permit tcp any any eq www (111 matches)
```

4) PC-A のコマンド プロンプトから、10.2.2.1 へ ping を実行します。結果を説明してください。

_____

_____

_____

2. R3 でセキュリティ ポリシー番号 3 に対応する名前付き拡張 ACL を設定します。

a. R3 にポリシーを設定します。ACL WEB-POLICY と名前を付けます。

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224
0.0.0.31 eq 80
```

b. ACL WEB-POLICY を S0/0/1 インターフェイスに適用します。

```
R3(config-ext-nacl)# int S0/0/1
R3(config-if)# ip access-group WEB-POLICY out
```

c. ACL WEB-POLICY を確認します。

1) R3 特権 EXEC モードのコマンド プロンプトから、**show ip interface s0/0/1** コマンドを実行します。

ACL の名前は何ですか（ある場合）。_____

ACL はどの方向に適用されますか? _____

2) ~~PC-C で Web ブラウザを開き、http://209.165.200.225（ISP ルータ）にアクセスします。通常は成功します。成功しない場合は、トラブルシューティングします。~~

3) ~~PC-C から、http://10.1.1.1（R1）への Web ブラウザ セッションを開きます。通常は成功します。成功しない場合は、トラブルシューティングします。~~

4) ~~PC-C から、http://209.165.201.1（ISP ルータ）への Web ブラウザ セッションを開きます。これは失敗します。失敗しない場合は、トラブルシューティングします。~~

5) PC-C のコマンド プロンプトから、PC-A へ ping を実行します。結果はどうなりますか?理由

_____

4. 拡張 ACL の修正および確認

ACL は R1 と R3 に適用されたため、R1 と R3 の LAN ネットワーク間では、ping や他のあらゆる種類のトラフィックは許可されません。管理部門は、192.168.10.0/24 と 192.168.30.0/24 ネットワークの間のすべてのトラフィックを許可する必要があると判断しました。R1 と R3 の両方の ACL を修正する必要があります。

1. R1 の ACL 100 を変更します。

a. R1 の特権 EXEC モードから、**show access-lists** コマンドを実行します。

このアクセス リストには何行ありますか? _____

b. グローバル コンフィギュレーション モードに入り、R1 の ACL を変更します。

```
R1(config)# ip access-list extended 100
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
R1(config-ext-nacl)# end
```

c. **show access-lists** コマンドを発行します。

追加した新しい行は ACL 100 のどこに表示されていますか?

_____

2. R3 の ACL WEB-POLICY を変更します。

a. R3 の特権 EXEC モードから、**show access-lists** コマンドを実行します。

このアクセス リストには何行ありますか? _____

b. グローバル コンフィギュレーション モードに入り、R3 の ACL を変更します。

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255
R3(config-ext-nacl)# end
```

c. **show access-lists** コマンドを実行し、新しい行が ACL の最後に追加されたことを確認します。

3. 変更された ACL を確認します。

a. PC-A から、PC-C の IP アドレスへ ping を実行します。ping は成功しましたか? _____

b. PC-C から、PC-A の IP アドレスへ ping を実行します。ping は成功しましたか? _____

ACL が、変更後すぐに ping に対して動作したのはなぜですか?

_____

復習

1. ACL を慎重に計画しテストする必要があるのはなぜですか?

_____

_____

2. 標準または拡張のどちらのタイプの ACL が適していますか?

_____

_____

_____

_____

_____

3. ~~EIGRP hello パケットとルーティング アップデートが、R1 と R3 に適用された ACL の暗黙の **deny any** アクセス コントロール エントリ（ACE）または ACL 文によってブロックされないのはなぜですか?~~

_____

_____

_____

_____

_____

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。