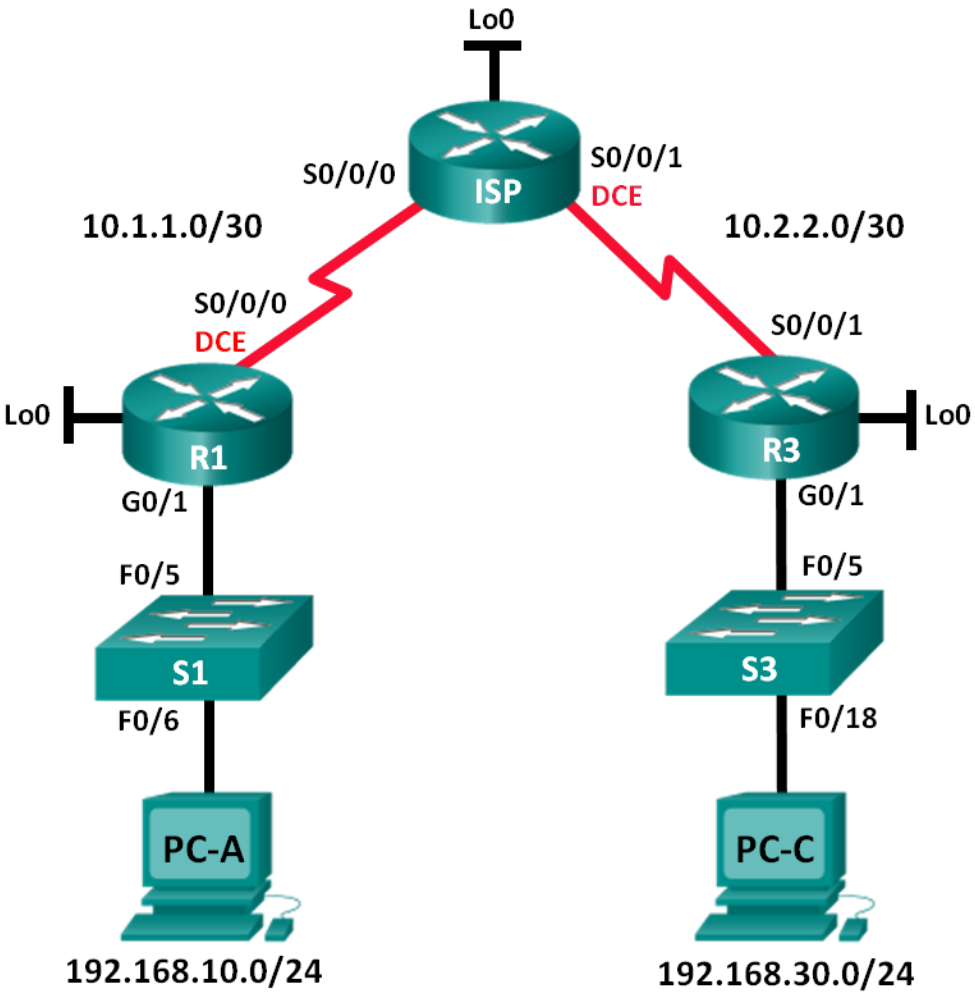
実習：標準 ACL の設定と確認

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
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

- ネットワーク トポロジに適合するように機器をセットアップします。
- ルータとスイッチを初期設定し、リロードします。

パート 2：デバイスの設定および接続の確認

- PC に固定 IP アドレスを割り当てます。
- ルータの基本設定を行います。
- 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。
- デバイス間の接続を確認します。

パート 3：標準番号付きおよび名前付き ACL の設定と確認

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

パート 4：標準 ACL の修正

- 名前付き標準 ACL を修正および確認します。

- ACL をテストします。

背景/シナリオ

ネットワーク セキュリティは、IP ネットワークを設計および管理する際に重要な問題となります。確立されたセキュリティ ポリシーに基づいてパケットをフィルタする適切なルールを設定する能力は、貴重なスキルです。

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. ルータ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. アドレス テーブルに示されるように、各ルータのループバック 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. DCE シリアル 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. コンソールのパスワードとして **cisco** を割り当てます。

h. 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。

3. （オプション）スイッチ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. 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。

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 ゲートウェイを設定します。

f. コンソールのパスワードとして **cisco** を割り当てます。

g. 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。

4. R1、ISP、および R3 に RIP ルーティングを設定します。

a. 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**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。

5. デバイス間の接続を確認します。

注：アクセス リストを設定して適用する**前に**、接続が動作しているかどうかをテスト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 インターフェイスへ ping を実行します。ping は成功しましたか? _____

3. 標準の番号付き ACL および名前付き ACL の設定と確認

1. 番号付き標準 ACL を設定します。

標準 ACL は、発信元の IP アドレスのみに基づいてトラフィックをフィルタします。標準 ACL の典型的なベスト プラクティスは、できるだけ宛先の近くで ACL を設定し適用することです。最初のアクセス リストでは、192.168.10.0/24 ネットワーク上のすべてのホストおよび 192.168.20.0/24 ネットワーク上のすべてのホストからのトラフィックに 192.168.30.0/24 ネットワーク上のすべてのホストへのアクセスを許可する標準番号付き ACL を作成します。また、セキュリティ ポリシーによって、すべての ACL の最後に ACL 文とも呼ばれる「**deny any** アクセス コントロール エントリ（ACE）」を入れることが定められています。

192.168.10.0/24 ネットワーク上のすべてのホストに 192.168.30.0/24 ネットワークへのアクセスを許可するために、どのワイルドカード マスクを使用しますか?

_____

シスコが推奨するベスト プラクティスに従う場合、この ACL をどのルータに配置しますか? _____

この ACL をどのインターフェイスに配置しますか? どの方向で適用しますか?

_____

a. R3 に ACL を設定します。アクセス リスト番号に 1 を使用します。

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b. 適切なインターフェイスに正しい方向で ACL を適用します。

```
R3(config)# interface g0/1
R3(config-if)# ip access-group 1 out
```

c. 番号付き ACL を確認します。

さまざまな **show** コマンドの使用は、ルータでの ACL のシンタックスと配置の両方の確認に役立ちます。

すべての ACE と共にアクセス リスト 1 を完全に表示するには、どのコマンドを使用しますか?

_____

アクセス リストが適用された場所とその方向を表示するには、どのコマンドを使用しますか?

_____

1) R3 で、**show access-lists 1** コマンドを実行します。

```
R3# show access-list 1
Standard IP access list 1
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
    30 deny   any
```

2) R3 で、**show ip interface g0/1** のコマンドを実行します。

```
R3# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.30.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 1
  Inbound access list is not set
  Output omitted
```

3) ACL をテストして、192.168.10.0/24 ネットワークからのトラフィックに 192.168.30.0/24 ネットワークへのアクセスを許可しているかどうか確認します。PC-A コマンド プロンプトから、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? _____

4) ACL をテストして、192.168.20.0/24 ネットワークからのトラフィックに 192.168.30.0/24 ネットワークへのアクセスを許可しているかどうか確認します。発信元として R1 のループバック 0 アドレスを使用して、拡張 ping を実行する必要があります。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? _____

```
R1# ping
Protocol [ip]:
Target IP address: 192.168.30.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
```

```
Extended commands [n]: y
Source address or interface: 192.168.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.20.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

d. R1 プロンプトから、PC-C の IP アドレスへ再度 ping を実行します。

```
R1# ping 192.168.3.3
```

ping は成功しましたか? その理由を述べてください。

_____

_____

_____

2. 名前付き標準 ACL を設定します。

次のポリシーに準拠する名前付き標準 ACL を作成します。192.168.40.0/24 ネットワーク上のすべてのホストからのトラフィックに 192.168.10.0/24 ネットワーク上のすべてのホストへのアクセスを許可します。また、ホスト PC-C に 192.168.10.0/24 ネットワークへのアクセスのみを許可します。このアクセス リストの名前は、BRANCH-OFFICE-POLICY とする必要があります。

シスコが推奨するベスト プラクティスに従う場合、この ACL をどのルータに配置しますか? _____

この ACL をどのインターフェイスに配置しますか? どの方向で適用しますか?

_____

a. R1 で標準名前付き ACL の BRANCH-OFFICE-POLICY を作成します。

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

アクセス リストの最初の許可される ACE を見つけます。これを記述する別の方法は何ですか?

_____

b. 適切なインターフェイスに正しい方向で ACL を適用します。

```
R1# config t
R1(config)# interface g0/1
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c. 名前付き ACL を確認します。

1) R1 で、**show access-lists** コマンドを発行します。

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3
    20 permit 192.168.40.0, wildcard bits 0.0.0.255
```

R1 のこの ACL と R3 の ACL の間に相違点はありますか? 設定されている場合、それは何ですか?

_____

_____

_____

_____

_____

2) R1 で **show ip interface g0/1** のコマンドを実行します。

```
R1# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.10.1/24
```

```
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is BRANCH-OFFICE-POLICY
  Inbound access list is not set
<出力を省略>
```

3) ACL をテストします。PC-C のコマンド プロンプトから、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? _____

4) ACL をテストして、PC-C のホストのみに 192.168.10.0/24 ネットワークへのアクセスが許可されることを確認します。発信元として R3 の G0/1 アドレスを使用して拡張 ping を実行する必要があります。ping PC-A の IP アドレス。ping は成功しましたか? _____

5) ACL をテストして、192.168.40.0/24 ネットワークからのトラフィックに 192.168.10.0/24 ネットワークへのアクセスを許可しているかどうか確認します。発信元として R3 のループバック 0 アドレスを使用して、拡張 ping を実行する必要があります。ping PC-A の IP アドレス。ping は成功しましたか? _____

4. 標準 ACL の修正

ビジネスにおいて、セキュリティ ポリシーが変更されるのは一般的です。このため、ACL を変更する必要が生じることがあります。パート 4 では、以前に設定された ACL のいずれかを、導入された新しい管理ポリシーに一致するように変更します。

管理部門は、209.165.200.224/27 ネットワークからのユーザに 192.168.10.0/24 ネットワークへのフル アクセスを許可する必要があると判断しました。また、管理部門は、すべてのルータの ACL を一貫したルールに準拠させることを望んでいます。すべての ACL の最後に **deny any** ACE を配置する必要があります。BRANCH-OFFICE-POLICY ACL を修正する必要があります。

この ACL に 2 行を追加します。これを実行するための 2 とおりの方法があります。

オプション 1：グローバル コンフィギュレーション モードで **no ip access-list standard BRANCH-OFFICE-POLICY** コマンドを実行します。これはルータから ACL 全体を効率的に取得します。ルータの IOS に応じて、次のシナリオのいずれかが起こります。パケットのすべてのフィルタリングがキャンセルされ、すべてのパケットがルータの経由を許可されるか、または、G0/1 インターフェイスで **ip access-group** コマンドを削除しなかったため、フィルタリングが引き続き実行されます。どちらにしろ、ACL がなくなっても、ACL 全体を再入力するか、テキスト エディタを使用してカット アンド ペーストできます。

オプション 2：ACL 自体に特定の行を追加または削除することで ACL を変更できます。これは、多くのコード行がある ACL では、特に役立つことがあります。ACL 全体の再入力やカット アンド ペーストはエラーを招きやすい傾向があります。ACL 内の特定の行の変更は簡単に達成されます。

注：この実習では、オプション 2 を使用します。

1. 名前付き標準 ACL を修正します。

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

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
```

b. ACL の最後に 2 行を追加します。グローバル コンフィギュレーション モードから、ACL の BRANCH-OFFICE-POLICY を変更します。

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

c. ACL を確認します。

1) R1 で、**show access-lists** コマンドを発行します。

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
    10 permit 192.168.30.3 (8 matches)
    20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
    30 permit 209.165.200.224, wildcard bits 0.0.0.31
    40 deny   any
```

R1 の G0/1 インターフェイスに BRANCH-OFFICE-POLICY を適用する必要がありますか?

_____

_____

2) ISP のコマンド プロンプトから、拡張 ping を実行します。ACL をテストして、209.165.200.224/27 ネットワークからのトラフィックに 192.168.10.0/24 ネットワークへのアクセスを許可しているかどうかを確認します。発信元として ISP のループバック 0 アドレスを使用して、拡張 ping を実行する必要があります。ping PC-A の IP アドレス。ping は成功しましたか? _____

復習

1. おわかりのとおり、標準 ACL は非常に強力で十分に動作しています。拡張 ACL を使用する必要があるのはなぜですか?

_____

_____

_____

_____

_____

2. 通常、番号付き ACL に比べ名前付き ACL の方が、より多くの入力が必要となります。番号付き ACL より名前付き ACL を選択するのはなぜですか?

_____

_____

_____

_____

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。