ACL によるパケットフィルタリング

実習内容と目標

このラボでは以下のことを学びます：

- ACL の原理を学びます。
- ACL の基本的なコンフィギュレーションを習得します。
- ACL の共通のコンフィギュレーションコマンドを習得します。

ネットワーク図

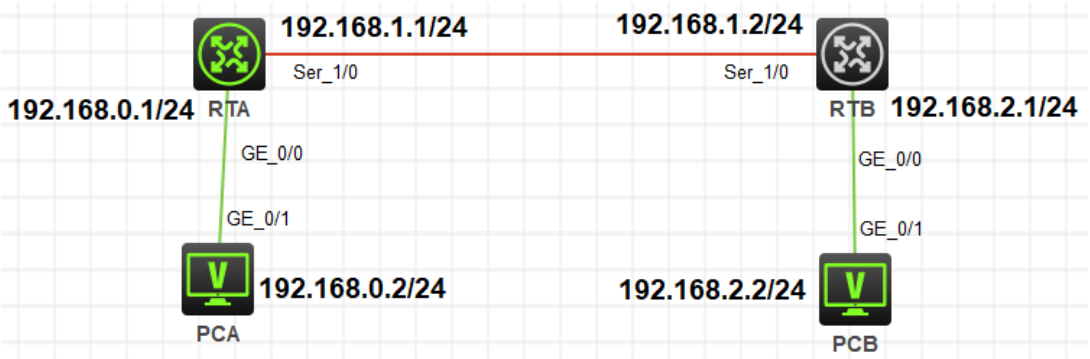


図 13.1 実習ネットワーク

実習装置

本実験に必要な主な設備機材 実験装置名前とモデル番号	バージョン	数量	特記事項
MSR36-20	Version7.1	2	なし
V35 DTEシリアルケーブル	-	1	
V35 DCEシリアルケーブル	-	1	
PC	Windows 7	2	なし
ネットワークケーブルの接続	--	2	なし

実習手順

タスク 1：ACL の基本的な設定をする

このタスクは、PCA がローカルネットワークセグメントを除く他のネットワークにアクセスすることを禁止するように、ルーターに基本的な ACL を構成することです。 このタスクの後、基本 ACL の構成方法と機能をマスターします。

手順 1：PC とルーターをケーブルで接続する

図 10.1のようにルーターと PC 間のケーブルを接続します。

RTA、RTB の設定がデフォルトであることを確実にするには **reset saved-configuration** コマンドでデフォルトのコンフィギュレーションへ戻します。

<RTA>reset saved-configuration

The saved configuration file will be erased. Are you sure? [Y/N]:y

Configuration file in flash: is being cleared.

Please wait ...

Configuration file is cleared.

<RTA>reboot

Start to check configuration with next startup configuration file, please wait.....DONE!

Current configuration may be lost after the reboot, save current configuration? [Y/N]:n

Please input the file name(*.cfg)[flash:/startup.cfg]

(To leave the existing filename unchanged, press the enter key):y

.....

表 13-1 IP アドレス割り当てスキーマ

装置	**インターフェイス**	**IP アドレス**	**ゲートウェイ**
RTA	S3/0	192.168.1.1/24	-
	G0/0	192.168.0.1/24	-
RTB	S3/0	192.168.1.2/24	-
	G0/0	192.168.2.1/24	-
PCA		192.168.0.2/24	192.168.0.1
PCB		192.168.2.2/24	192.168.2.1

表 13-1 に従って PC の IP アドレスとゲートウェイを構成します。Windows の「スタート」から「ファイル名を指定して実行」を選択します。 表示されるウィンドウで、CMD と入力します。 コマンドプ

ロンプトウィンドウで ipconfig コマンドを実行して、設定されているすべての IP アドレスを表示し、表 13-1 に従って RTA ポートと RTB ポートに IP アドレスとゲートウェイを設定します。

RTA を設定します。
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ip address 192.168.0.1 24
[RTA-GigabitEthernet0/0]quit
[RTA]interface Serial 1/0
[RTA-Serial1/0]ip address 192.168.1.1 24
[RTA-Serial1/0]quit

RTB を設定します。
[RTB]interface GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ip address 192.168.2.1 24
[RTB-GigabitEthernet0/0]quit
[RTB]interface Serial 1/0
[RTB-Serial1/0]ip address 192.168.1.2 24
[RTB-Serial1/0]quit

ネットワーク接続を実現するために、ルーターに静的ルートまたは任意のタイプの動的ルートを構成できます。 たとえば、RIP を使用する場合、構成は次のようになります。
RTA を設定します。
[RTA]rip
[RTA-rip-1]network 192.168.0.0
[RTA-rip-1]network 192.168.1.0
[RTA-rip-1]quit

RTB を設定します。
[RTB]rip
[RTB-rip-1]network 192.168.1.0
[RTB-rip-1]network 192.168.2.0
[RTB-rip-1]quit

PCA で ping コマンドを実行して、PCA とルーター間の接続、および PCA と PCB 間の接続をテストします。 PCA はルーターと PCB に ping を実行する必要があります。
出力は次のとおりです。

<PCA>ping 192.168.2.2

Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break

56 bytes from 192.168.2.2: icmp_seq=0 ttl=253 time=5.000 ms

56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=6.000 ms

56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=5.000 ms

56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=6.000 ms

56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=6.000 ms

ルートに到達できない場合は、関連する章を参照して、ルーティングプロトコルが正しく設定されているかどうかを確認してください。

手順 2：ACL を計画する

このテストは、PCA がローカルネットワーク以外の他のネットワークにアクセスすることを禁止するためのものです。ACL の計画中に次の質問を考慮する必要があります。

- どのタイプの ACL を使用する必要がありますか？
- ACL ルールのアクションは拒否または許可ですか？
- ACL ルールの逆マスクはどうあるべきですか？
- ACL を適用するルーターポートと方向はどれですか。

答えは次のとおりです。

- 送信元 IP アドレスに基づいて PCA パケットを識別できる場合は、基本的な ACL が適用されます。
- PCA がローカルネットワーク以外の他のネットワークにアクセスすることを禁止する目的。したがって、ACL アクションは拒否する必要があります。
- PC から送信されたパケットのみを制御する必要があるため、リバースマスクは 0.0.0.0(192.168.0.2 に限定)に設定されます。
- ACL は、PCA に接続するインバウンド RTA ポート GigibitEtherenet0/0 に適用して、PCA がローカルネットワーク以外の他のネットワークにアクセスすることを禁止する必要があります。

手順 3：basic ACL を構成し、それを適用します。

RTA で ACL を次のように定義します。

[RTA]acl basic 2001

[RTA-acl-ipv4-basic-2001]rule deny source 192.168.0.2 0.0.0.0

[RTA-acl-ipv4-basic-2001]quit

RTA のパケットフィルタリングファイアウォール機能はデフォルトで有効になっており、デフォルトのアクションは許可です。

ACL を RTA のポート GigabitEthernet0/0 に適用します。

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]packet-filter 2001 inbound

[RTA-GigabitEthernet0/0]quit

手順 4:ファイアウォール機能を確認します。

PCA で ping コマンドを実行して、PCA と PCB の接続をテストします。 PCA は PCB に ping ができません。出力情報は次のとおりです。

<PCA>ping 192.168.2.2

Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

ACL とパケットフィルタリングファイアウォールの状態と RTA の統計を表示します。上の ping が 5 回 deny 条件に合致したことを示しています(5 times matched)。

[RTA]display acl 2001

Basic IPv4 ACL 2001, 1 rule,

ACL's step is 5

 rule 0 deny source 192.168.0.2 0 (5 times matched)

手順 5:一部のパケットは ACL ルールにヒットします。

[RTA]display packet-filter interface inbound

Interface: GigabitEthernet0/0

 Inbound policy:

  IPv4 ACL 2001

[RTA]display packet-filter statistics sum inbound 2001

Sum:

 Inbound policy:

  IPv4 ACL 2001

   rule 0 deny source 192.168.0.2 0

Totally 0 packets permitted, 0 packets denied

Totally 0% permitted, 0% denied

パケットフィルタリングファイアウォールは RTA で有効になっています。 ACL 2001 を使用して、ポート GigabitEthernet0 / 0 宛てのインバウンドパケットを照合およびフィルタリングします。

タスク 2:ACL の高度な構成

このタスクは、PCA とネットワーク 192.168.2.0/24 の間の FTP フローを禁止するように、ルーターに高度な ACL を構成することです。このタスクの後、高度な ACL の構成方法と機能を習得します。

設定の前に、ルーターの ACL およびパケットフィルタリング設定をクリアして、元のルーターを設定に復元することは、タスク 2 の手順 1 です。

手順 1:タスク 1 で設定した ACL を削除する

[RTA]undo acl basic 2001

手順 2:ACL を計画する

このテストは、PCA とネットワーク 192.168.2.0/24 の間の FTP フローを禁止するためのものです。ACL の計画時には、次の質問を検討する必要があります。

- どのタイプの ACL を使用する必要がありますか？
- ACL ルールのアクションは拒否または許可ですか？
- ACL ルールの逆マスクはどうあるべきですか？
- どのルーター部分とどの方向に ACL を適用する必要がありますか？

答えは次のとおりです。

- このテストは、PCA とネットワーク 192.168.2.0/24 の間の FTP フローを禁止するためのものです。 FTP パケットはポート番号に基づいて識別される必要があるため、アドバンス ACL が適用されます。
- 目的は PC 通信を禁止することであるため、ACL アクションは拒否する必要があります。
- PC からネットワーク 192.168.2.0/24 に送信されるパケットを制御する必要があるため、送信元 IP アドレスのリバースマスクは 0.0.0.0(192.168.0.2 に限定)に設定され、宛先 IP アドレスのリバースマスクは 0.0.0.255(192.168.2.0 の全てのアドレス)に設定されます。 。
- ACL は、PCA に接続するインバウンド RTA のポート GigabitEthernet0/0 に適用して、PCA がパケットを送信しないようにする必要があります。

手順 3:アドバンス ACL を構成し、それを適用します。

RTA で ACL を次のように定義します。

[RTA]acl advanced 3002

[RTA-acl-ipv4-adv-3002]rule deny tcp source 192.168.0.2 0.0.0.0 destination 192.168.2.0 0.0.0.255 destination-port eq ftp

[RTA-acl-ipv4-adv-3002]rule permit ip source 192.168.0.2 0.0.0.0 destination 192.168.2.0 0.0.0.255

[RTA-acl-ipv4-adv-3002]quit

RTA のパケットフィルタリングファイアウォール機能はデフォルトで permit になっており、ping は許可されています。

ACL を RTA のポート GigabitEthernet0/0 に適用します。

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]packet-filter 3002 inbound

[RTA-GigabitEthernet0/0]quit

設定された ACL を確認してみます。

[RTA]display packet-filter verbose interface GigabitEthernet 0/0 inbound

Interface: GigabitEthernet0/0

Inbound policy:

IPv4 ACL 3002

rule 0 deny tcp source 192.168.0.2 0 destination 192.168.2.0 0.0.0.255 destination-port eq ftp

rule 5 permit ip source 192.168.0.2 0 destination 192.168.2.0 0.0.0.255

手順 4:ファイアウォール機能を確認します。

PCA で ping コマンドを実行して、PCA と PCB の接続をテストします。 PCA は PCB に ping を実行できる必要があります。出力情報は次のとおりです。

<PCA>ping 192.168.2.2

Ping 192.168.2.2 (192.168.2.2): 56 data bytes, press CTRL_C to break

56 bytes from 192.168.2.2: icmp_seq=0 ttl=253 time=2.000 ms

56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=1.000 ms

56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=1.000 ms

56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=1.000 ms

56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=1.000 ms

RTB で FTP サービスを有効にします。

[RTB]ftp server enable

[RTB]local-user admin class manage

New local user added.

[RTB-luser-manage-admin]password simple h3cjapan

[RTB-luser-manage-admin]service-type ftp

[RTB-luser-manage-admin]authorization-attribute user-role network-admin

[RTB-luser-manage-admin]quit

次に、PCA 上の FTP クライアントを使用して PCA から RTB に FTP 接続します。 FTP 接続は失敗するはずです。出力情報は次のとおりです。

<PCA>ftp 192.168.2.1

Press CTRL+C to abort.

ACL とファイアウォールの状態および RTA の統計を表示します。上の ftp が 1 回 deny 条件に合致したことを示しています(1 times matched)。

[RTA]display acl 3002

Advanced IPv4 ACL 3002, 2 rules,

ACL's step is 5

 rule 0 deny tcp source 192.168.0.2 0 destination 192.168.1.0 0.0.0.255 destination-port eq ftp (1 times matched)

 rule 5 permit ip source 192.168.0.2 0 destination 192.168.2.0 0.0.0.255 (1 times matched)

手順 5:一部のパケットは ACL 3002 ルールにヒットします。

パケットフィルタリングファイアウォールが RTA で有効になっている場合は、ACL 3002 を使用して、ポート gigabitEthernet0/0 宛てのパケットを照合およびフィルタリングします。

[RTA]display packet-filter interface inbound

Interface: GigabitEthernet0/0

 Inbound policy:

  IPv4 ACL 3002

[RTA]display packet-filter statistics sum inbound 3002

Sum:

 Inbound policy:

  IPv4 ACL 3002

   rule 0 deny tcp source 192.168.0.2 0 destination 192.168.2.0 0.0.0.255 destination-port

eq ftp

rule 5 permit ip source 192.168.0.2 0 destination 192.168.2.0 0.0.0.255

Totally 0 packets permitted, 0 packets denied

Totally 0% permitted, 0% denied

手順 6(オプション):RTA の ACL 3002 ルールを削除して、FTP が正しく利用できることを確認しましょう。

RTA の ACL 3002 を削除します。

[RTA]undo acl advanced 3002

PCA から RTB に対して ftp を実行します。

<PCA>ftp 192.168.2.1

Press CTRL+C to abort.

Connected to 192.168.2.1 (192.168.2.1).

220 FTP service ready.

User (192.168.2.1:(none)): admin

331 Password required for admin.

Password:

230 User logged in.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> dir

227 Entering Passive Mode (192,168,2,1,166,220)

150 Accepted data connection

drwxrwxrwx 2 0 0 4096 Nov 21 07:16 diagfile

-rwxrwxrwx 1 0 0 253 Nov 21 07:42 ifindex.dat

-rwxrwxrwx 1 0 0 43136 Nov 21 07:16 licbackup

drwxrwxrwx 3 0 0 4096 Nov 21 07:16 license

-rwxrwxrwx 1 0 0 43136 Nov 21 07:16 licnormal

drwxrwxrwx 2 0 0 4096 Nov 21 07:16 logfile

-rwxrwxrwx 1 0 0 0 Nov 21 07:16 msr36-cmw710-boot-a7514.bin

-rwxrwxrwx 1 0 0 0 Nov 21 07:16 msr36-cmw710-system-a7514.bin

drwxrwxrwx 2 0 0 4096 Nov 21 07:16 pki

drwxrwxrwx 2 0 0 4096 Nov 21 07:16 seclog

-rwxrwxrwx 1 0 0 2644 Nov 21 07:42 startup.cfg

-rwxrwxrwx 1 0 0 43964 Nov 21 07:42 startup.mdb

226 12 matches total

ftp> quit

221-Goodbye. You uploaded 0 and downloaded 0 kbytes.

221 Logout.

質問:

1. タスク 1 で、ACL 2001 の構成中に、他のパケットの通過を許可するために次のコンテンツを追加する必要がありますか？ どうして？

答え:

いいえ、ありません。 デフォルトの ACL アクションは permit です。 そのため、システムは ACL ルールに当てはまらないすべてのパケットを転送します。

2. タスク 2 で、ACL を RTB に適用できますか？

答え:

はい、できます。 コンフィギュレーション結果は同じです。 ただし、ACL を RTA に適用すると、フローの処理と転送の手順が短縮されます。

補足:

HCL の PC には ftp の機能はありませんので、PCA の代わりにルーターを利用します。

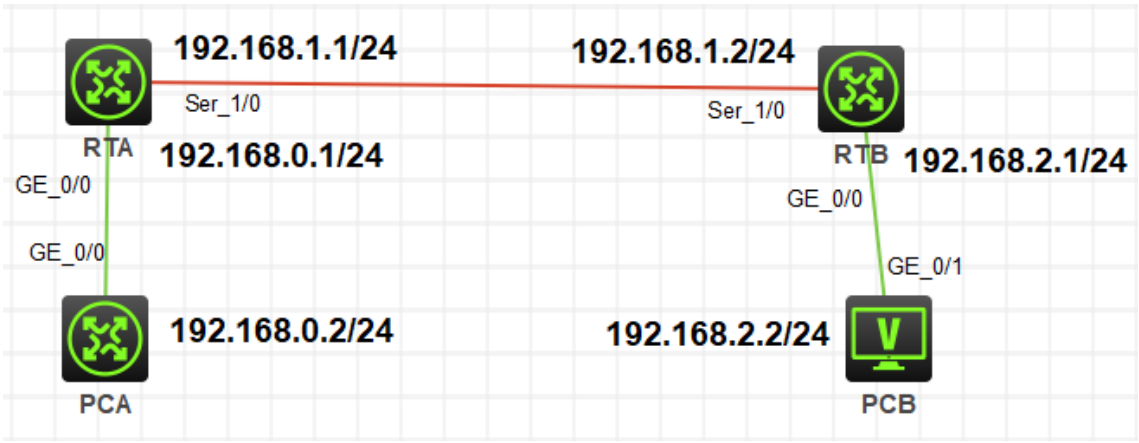
ルーターの設定は以下の通りです:

[PCA]interface GigabitEthernet 0/0

[PCA-GigabitEthernet0/0]ip address 192.168.0.2 255.255.255.0

[PCA-GigabitEthernet0/0]quit

[PCA] ip route-static 0.0.0.0 0 192.168.0.1


192.168.1.1/24
192.168.1.2/24
Ser_1/0
Ser_1/0
RTA
192.168.0.1/24
RTB
192.168.2.1/24
GE_0/0
GE_0/0
GE_0/0
GE_0/1
192.168.0.2/24
192.168.2.2/24
PCA
PCB