H3C 製品基本操作トレーニング
実習ガイド v3.3

内容

課題一覧

Lab1 H3Cネットワークの学びを始めましょう

実習内容と目標

このラボでは以下のことを学びます:

- コンソールポートから装置にログインする方法を習得します。
- telnet でログインする方法を習得します。
- システムを操作する基本的なコマンドを習得します。
- ファイルを操作する基本的なコマンドを習得します。
- ftp、tftp でファイルのアップロード、ダウンロードの方法を習得します。

ネットワーク図

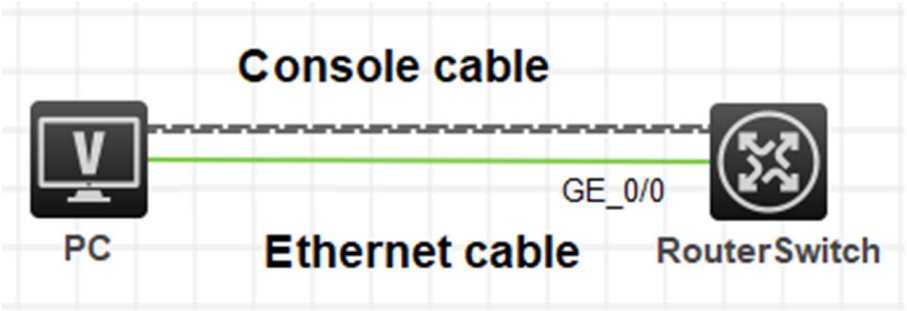


図 1.1 実習ネットワーク

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
コンソールシリアルケーブル	-	1	
ネットワークケーブルの接続	--	1	なし

実習手順

このタスクは、ルーターをテスト装置として使いますが、スイッチでも構いません。

タスク1:コンソールケーブルを使ってログインする

このタスクは、ユーザーがコンソール接続を介してデバイスを構成する方法を理解し、習得できるようにすることです。

注:シュミレーターでの実習では手順3から始めます

手順1:PCとルーターをケーブルで接続する

図1.1のようにPC(端末)のシリアルポートとMSRのコンソールポートをコンソールケーブルで接続します。 ケーブルのRJ-45の端はMSRのコンソールポートに接続され、9ピンRS-232の端はPCのシリアルポートに接続されます。

手順2:PCを起動しputty(tera termなどターミナルソフト)を起動します

次の図に示すように、PCデスクトップでputtyを実行して、接続セッションページを表示します。

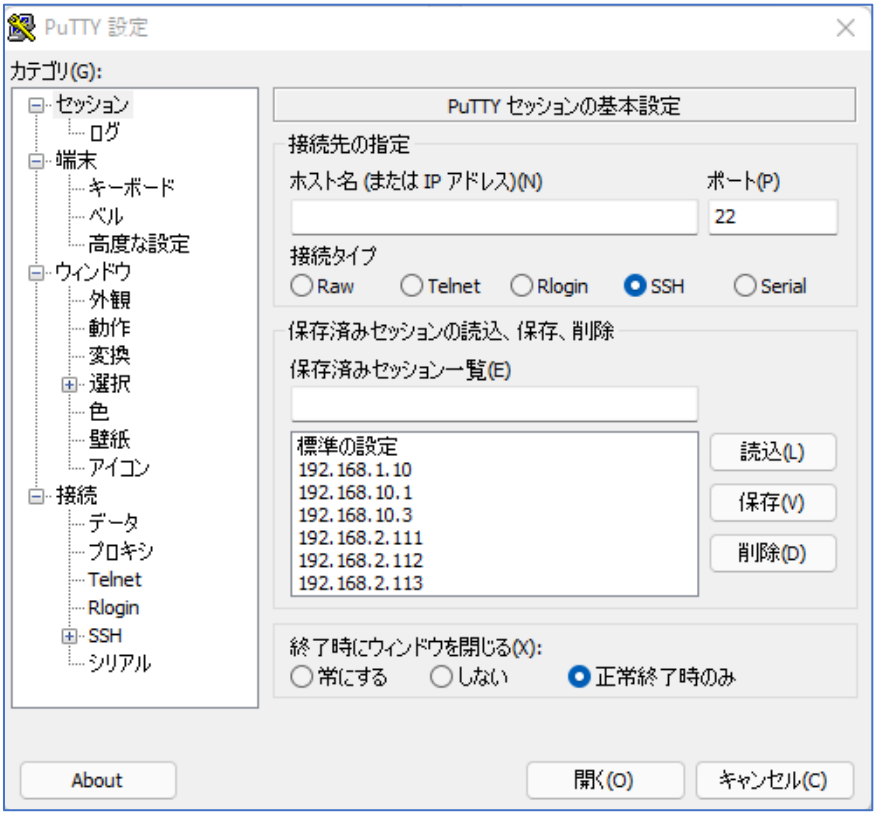


図 1-2 putty 起動画面

接続タイプでシリアルを選択します。 COMポートを選択します。 このラボでは、COM4を選択してPCをコンソールケーブルに接続します。 次の図に示すように、ボーレートをデフォルト値9600に設定します。

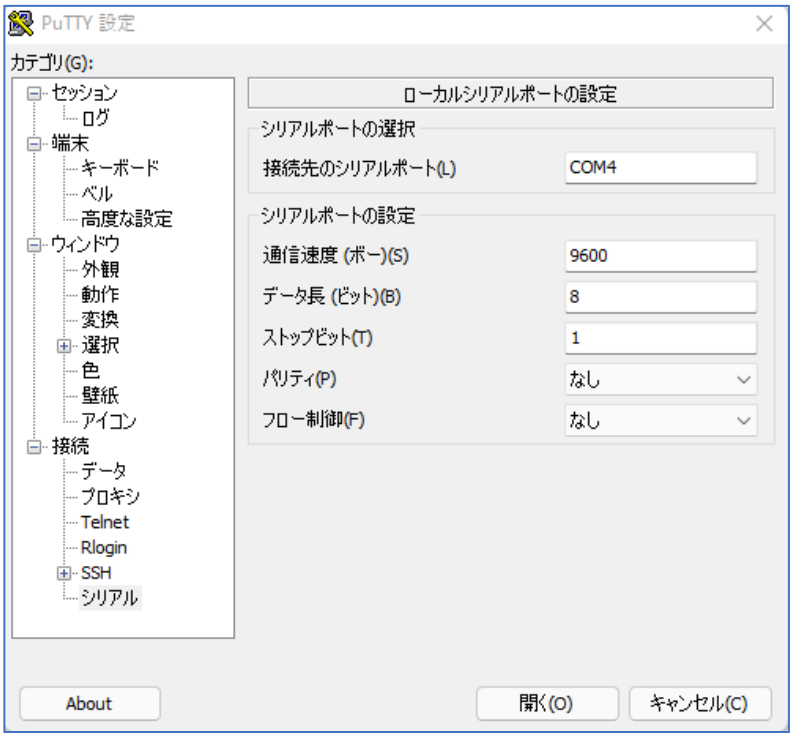


図 1.3 シリアルポートの設定画面

以下はtera termの起動画面でシリアルポートを選択します。

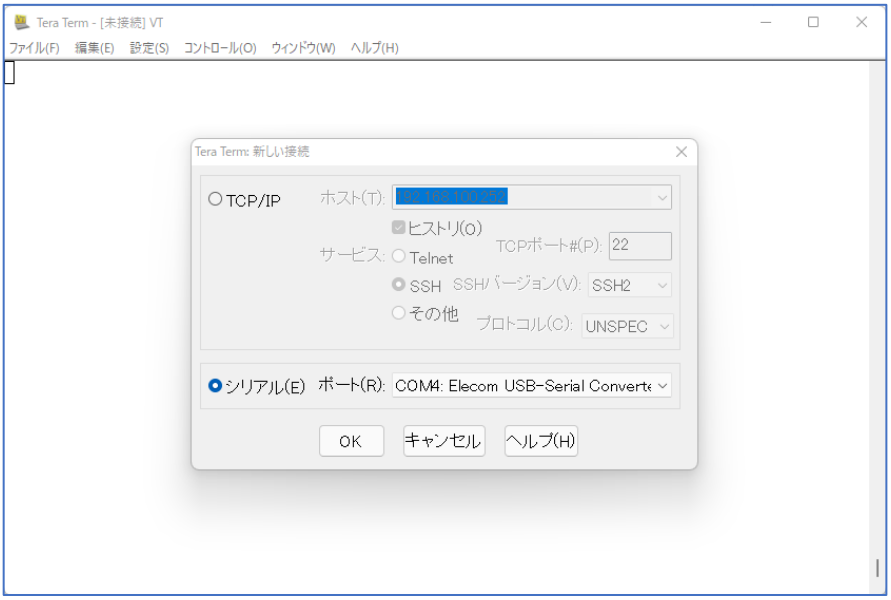


図 1.4 tera term 起動画面

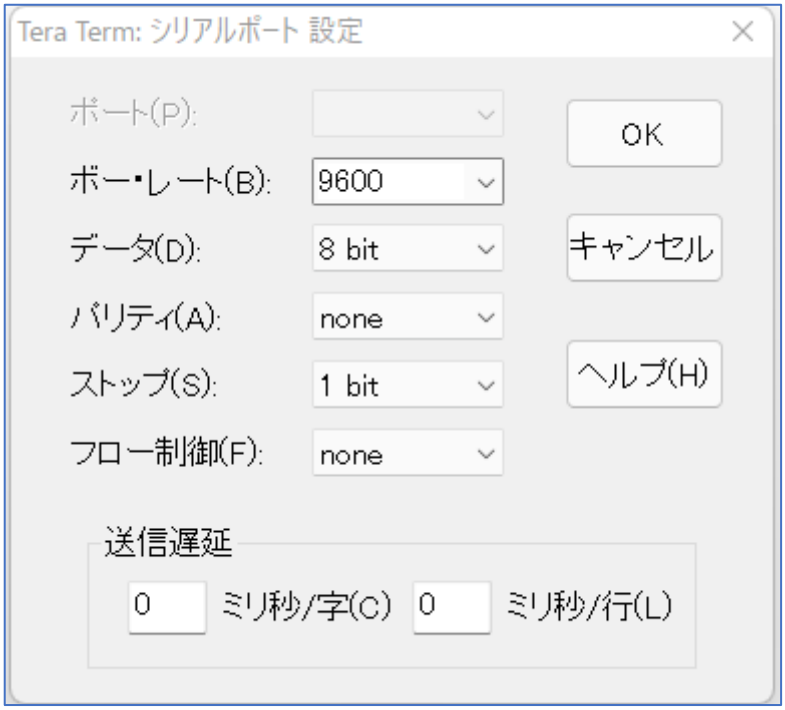
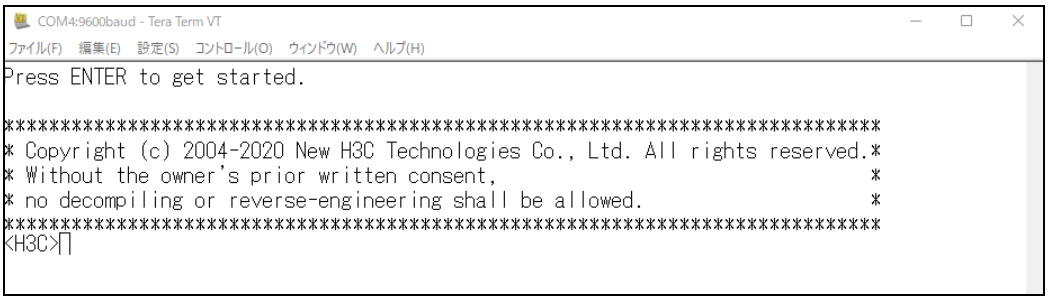


図 1.5 tera term シリアルポートの設定画面

OKをクリックすると装置のコンフィギュレーション画面が以下のように表示されます。

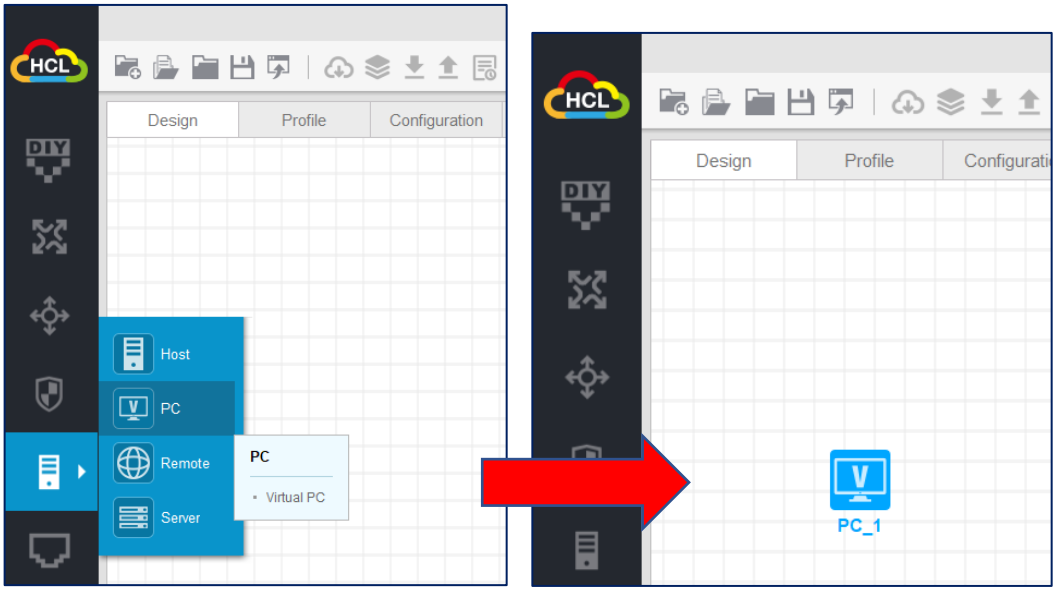


手順3:シュミレーターの場合はここから始めます。

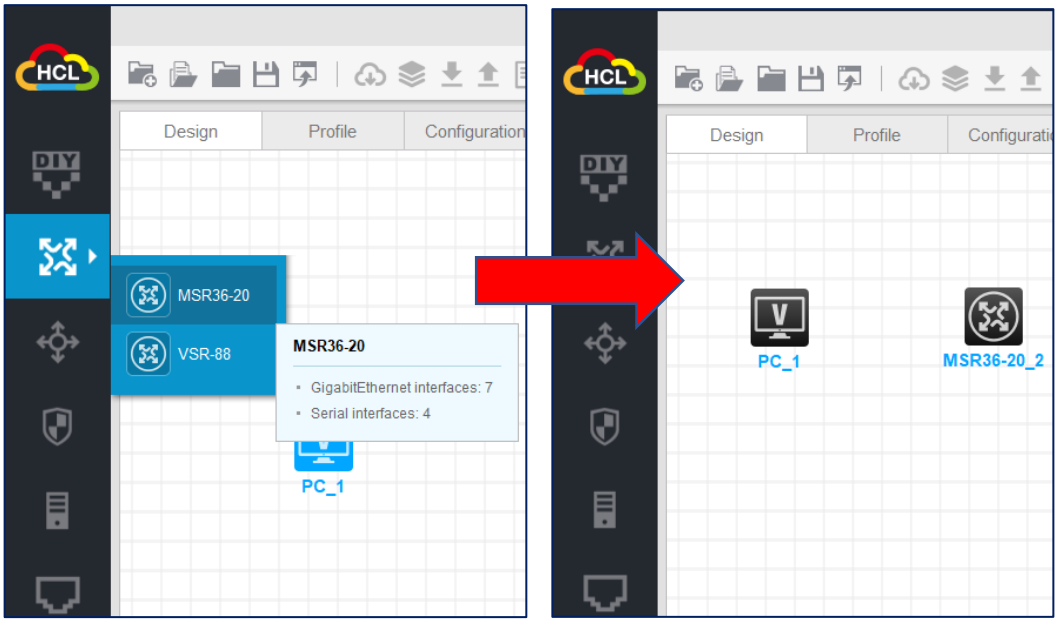
注意:HCLではコンソールケーブルは必要なく、直接装置を起動し、CLIで接続できます。

以下にHCLでのコンソールログインのケースを示します。

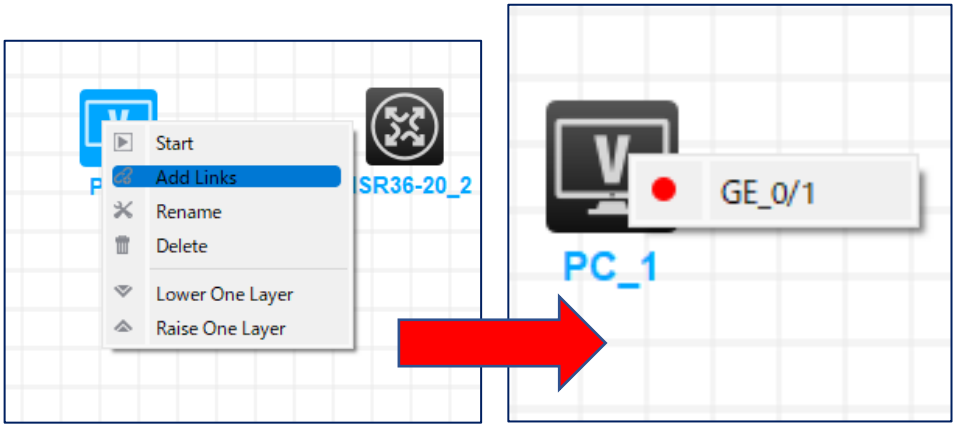
左側のメニューからPCを選択しワークスペースへ置きます。

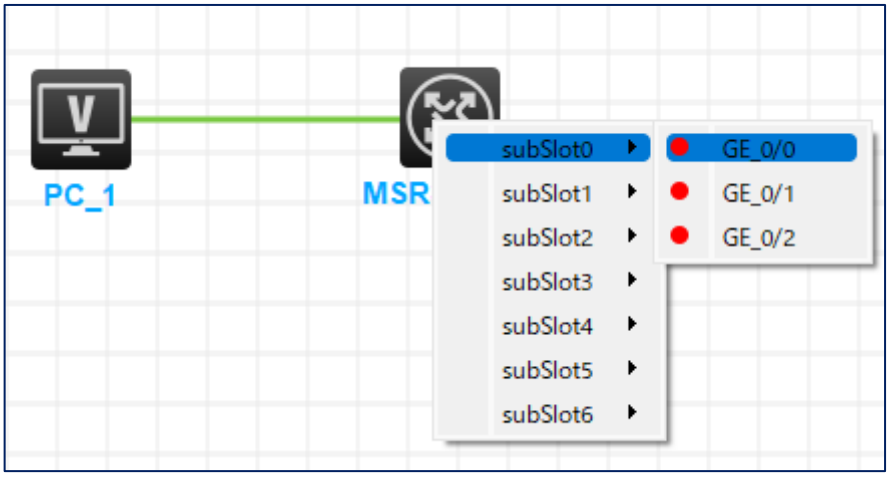


同様にルーターを選択し、ワークスペースへ置きます。

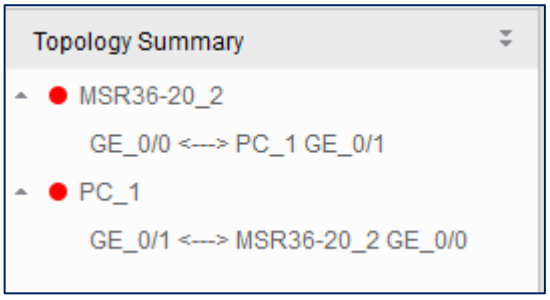


PCからルーターへケーブルをつなぎます。

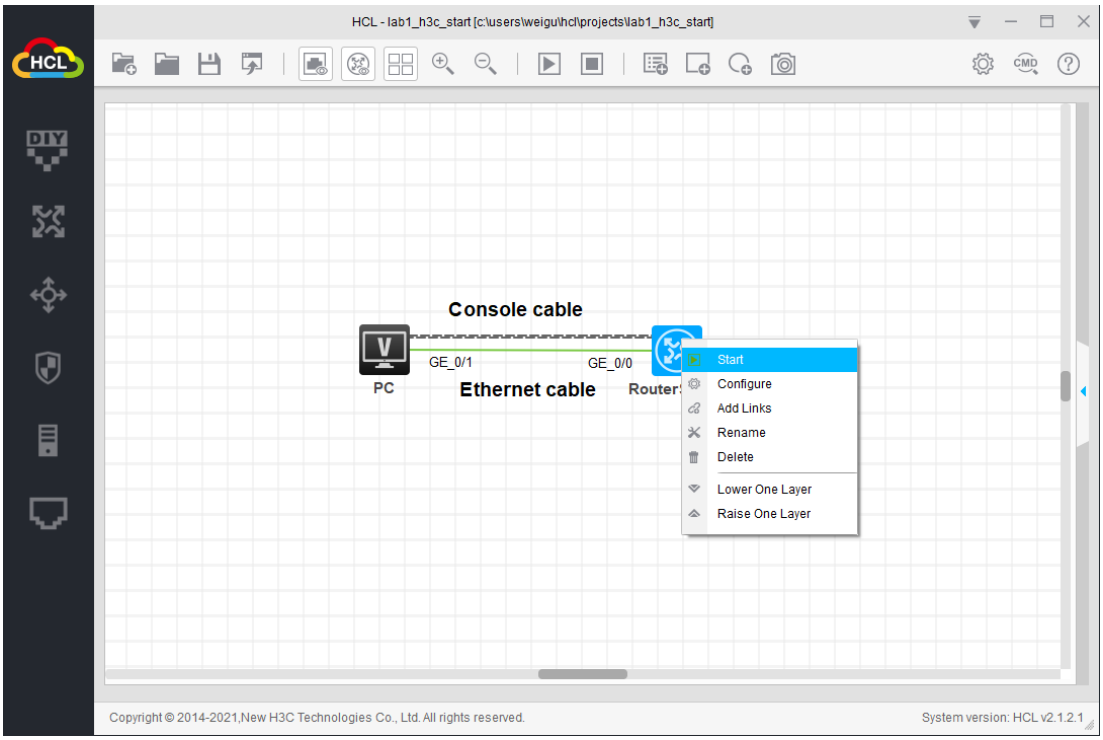




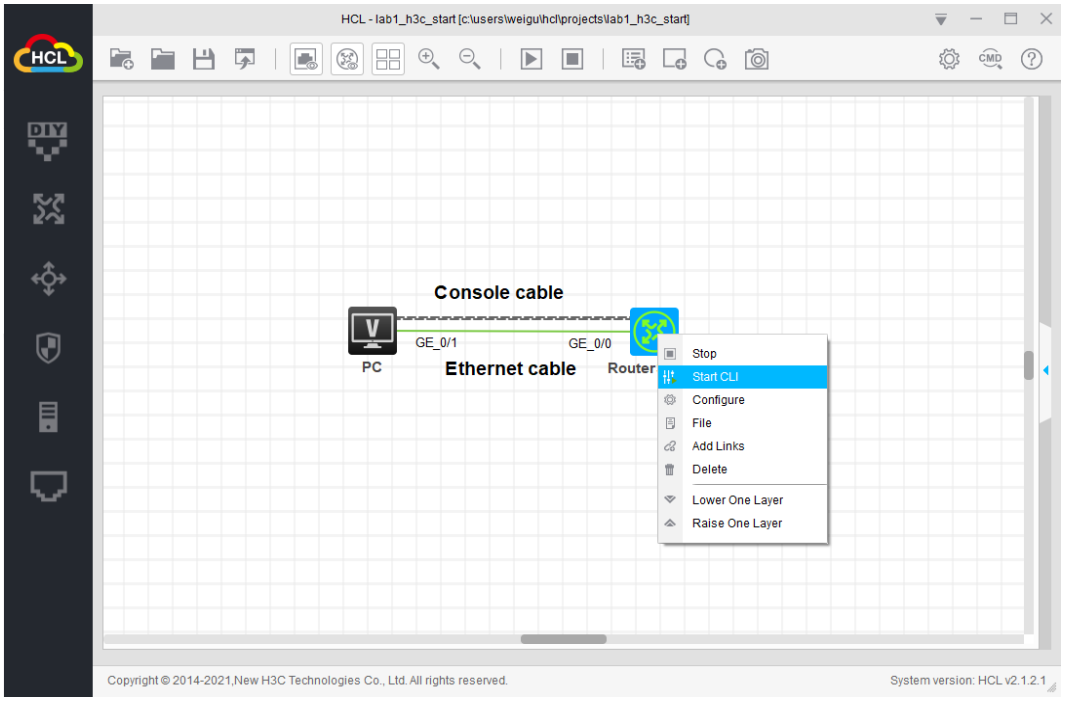
右端の下にトポロジーサマリーが表示され、PCとルーター間のどのインターフェースが接続されたか確認できます。



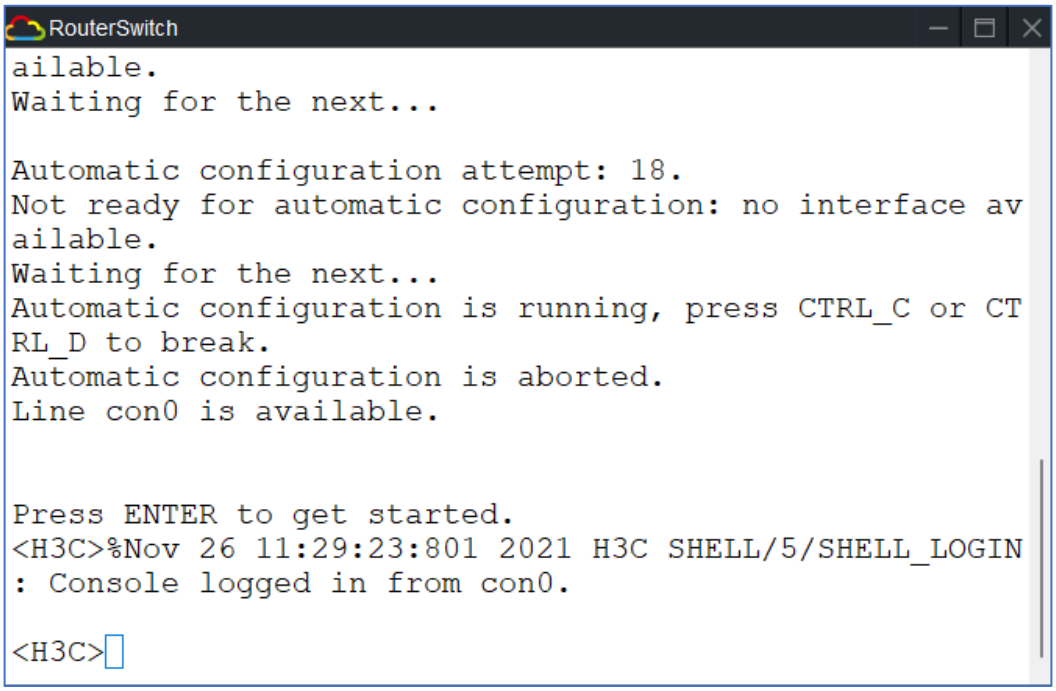
ルーターを起動するには、装置の上で右クリックしメニューから**Start**を選択します。



次に装置を右クリックし、メニューから**Start CLI**を選択するとコンソール画面が表示されます。



以下はHCLのコンソール画面です。



タスク2：システムとファイルを操作する基本的なコマンドを使う

手順1:システムビューに入る

タスク1が完了すると、構成インターフェイスがユーザービューに入ります。 system-viewコマンドを実行して、システムビューに入ります。

<H3C>sys

<H3C>system-view

System View: return to User View with Ctrl+Z.

[H3C]

プロンプトが[XXX]に変わってユーザーがシステムビューに入ったことが分かります。

システムビューでquitコマンドを実行するとユーザービューに戻ります。

[H3C]quit

<H3C>

手順2: ヘルプ機能と補完機能を使用します。

H3C Comwareプラットフォームは、CLI入力に応じてヘルプとインテリジェントな補完機能を提供します。

入力ヘルプ機能：コマンドを入力するときに、コマンド名を忘れた場合は、構成ビューでコマンドの最初の文字を入力してから、？を押すことができます。 システムは、最初の文字で始まるすべてのコマンドを自動的にリストします。 コマンドのキーワードまたはパラメーターを入力するときは、？を押します。 次の利用可能なキーワードとパラメーターを検索します。

システムビューで、sysと入力し、？を押します。 システムには、**sys**で始まるすべてのコ

マンドが一覧表示されます。

[H3C]sys?

sysname Specify the host name

system-working-mode System working mode

システムビューで、**sysname**と入力し、スペースと？を押します。 システムは、以下の使用可能なすべてのキーワードとパラメーターをリストします。

[H3C]sysname ?

TEXT Host name (1 to 64 characters)

インテリジェント補体機能：コマンドを入力するときに、コマンドの最初の文字を入力してからTabキーを押すことができます。 システムは自動的にコマンドを補完します。 複数のコマンドが同じプレフィックスを共有している場合は、Tabキーを繰り返し押してコマンドを切り替えます。

システムビューで、**sys**と入力します。

[H3C]sys

タブを押します。 システムは自動的にコマンドを補完します。

[H3C]sysname

システムビューで**in**と入力します。

[H3C]in

タブを押します。システムは自動的に**in**で始まる最初のコマンドを補完します：

[H3C]interface

タブを繰り返します。システムは自動的に**in**で始まるコマンドを繰り返します。

[H3C]info-center

手順3: システム名を変更します

Sysnameを変更するために**sysname**コマンドを実行します。

[H3C]sysname YourName

[YourName]

システム名はH3CからYourNameに変更されました。

手順4: システム時刻を変更します

現在のシステム時刻を問い合わせます。時刻はユーザービューでもシステムビューでも問い合わせることができます。

[YourName]display clock

11:46:17 UTC Fri 11/26/2021

quitコマンドを実行してシステムビューから抜け、システム時間を変更します。

[YourName]quit

<YourName>clock datetime 10:10:10 11/26/2021

To manually set the system time, execute the clock protocol none command first.

このエラーメッセージは、デフォルトでは時間をntpから取得するようになっているので、マニュアルで時間を変更することはできません。システムビューに戻って**clock**のプロトコルを**none**に変更します。

< YourName >system-view

System View: return to User View with Ctrl+Z.

[YourName]clock protocol none

時刻を変更するためにユーザービューへ戻るために**quit**を押して、ユーザービューでマニュアルで時刻を設定します。

[YourName]quit

<YourName>clock datetime 10:10:10 11/26/2021

現在のシステム時間を確認します。

<YourName>display clock

10:10:15 UTC Fri 11/26/2021

システム時刻は変更されておりました。

システムには自動識別機能があり、最初の文字がコマンドを一意に表すことができる場合、コマンドを識別します。

<YourName>dis clo

10:10:26 UTC Fri 11/26/2021

手順5: システムの現在のコンフィギュレーションを表示します

display current-configurationコマンドを実行して、システムの現在の構成を表示します。 特定の表示コンテンツは、使用中のデバイスとモジュールの対象となります。 次の構成で、インターフェイス情報を確認し、その情報をデバイスの実際のインターフェイスおよびモジュールと比較します。

<YourName>display current-configuration

#

 version 7.1.075, Alpha 7571

#

 sysname YourName

#

 clock protocol none

#

 system-working-mode standard

 xbar load-single

 password-recovery enable

 lpu-type f-series

#

vlan 1
#
interface Serial1/0
#
interface Serial2/0
#
interface Serial3/0
#
interface Serial4/0
#
interface NULL0
---- More ----
Spaceを押すと、次のページが表示されます。 Enterキーを押して次の行を表示し、**Ctrl+C**
を押して表示を閉じます。 このラボでは、**Space**を押します。
interface NULL0
#
interface GigabitEthernet0/0
port link-mode route
combo enable copper
#
interface GigabitEthernet0/1
port link-mode route
combo enable copper
#
interface GigabitEthernet0/2
port link-mode route
combo enable copper
#
interface GigabitEthernet5/0
port link-mode route
combo enable copper
#
interface GigabitEthernet5/1
port link-mode route
combo enable copper

#
interface GigabitEthernet6/0
port link-mode route
---- More ----

設定に基づいて、ルーターにはインターフェイスGigabitEthernet0/0、インターフェイスGigabitEthernet0/1、およびインターフェイスGigabitEthernet0/2があります。 特定のインターフェイス番号とタイプは、挿入されるデバイスモデルとボードによって異なります。

手順6: セーブされているコンフィギュレーションを表示します

display saved-configurationコマンドを実行してシステムのセーブされているコンフィギュレーションを表示します。

<YourName>display saved-configuration
<YourName>

構成ファイルは保存されません。 **display current-configuration**コマンドの実行後に構成があるのはなぜですか？ 現在の構成は永続ストレージではなく一時ストレージに保存されるためです。 デバイスを再起動すると、現在の構成が失われます。 正しい現在の構成をタイムリーに保存する必要があります。 保存された構成は、フラッシュ（またはCFカード、ハードディスクなど）に保存されます。 ここに保存された情報はありません。 そのため、フラッシュには設定ファイルは保存されません。

手順7: コンフィギュレーションをセーブします

コンフィギュレーションをセーブするために**save**コマンドを実行します。

<YourName>save
The current configuration will be written to the device. Are you sure? [Y/N]:**y**

装置のストレージに現在のコンフィギュレーションを書き込むのを承認するように**y**を選択します。

Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):

システムは、構成ファイルの名前を入力するように通知します。 ファイル名の形式は*** .cfg**であることに注意してください。 このラボでは、設定ファイルは、デフォルトで**startup.cfg**としてフラッシュに保存されます。

デフォルトのファイル名を使用するには、Enterキーを押します

Validating file. Please wait...
Configuration is saved to device successfully.

上記の情報は、構成ファイルを初めて保存する手順を示しています。 設定ファイルを再度保存すると、次のような表示内容が表示されます。

<YourName>save
The current configuration will be written to the device. Are you sure? [Y/N]:y

Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait...
Configuration is saved to device successfully.

Enterキーを押すと、デフォルトのファイル名**startup.cfg**を選択したため、システムは前の構成ファイルを上書きするかどうかを通知します。 保存した構成を再度表示します。

```
<YourName>display saved-configuration
#
 version 7.1.075, Alpha 7571
#
 sysname YourName
#
 clock protocol none
#
 system-working-mode standard
 xbar load-single
 password-recovery enable
 lpu-type f-series
#
vlan 1
#
interface Serial1/0
#
interface Serial2/0
#
interface Serial3/0
#
interface Serial4/0
#
interface NULL0
…
<YourName>
```

saveコマンドを実行すると、保存された構成は現在の構成と一致します。

手順6: コンフィギュレーションの削除と初期化

コマンドを削除するには、**undo**コマンドを実行してコマンドを削除します。 たとえば、

sysnameコマンドが削除された後、デバイス名はH3Cに復元されます。

[YourName]undo sysname

[H3C]

工場出荷時の設定に戻すには、ユーザービューで**reset saved-configuration**コマンドを実行して、保存された構成をクリアします（保存された構成をクリアするだけです。現在の構成は引き続き使用できます）。 次に、**reboot**コマンドを実行してsystmを再起動します。 システムは工場出荷時の設定に復元されます。

[H3C]quit

<H3C>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.

<H3C>reboot

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

保存されて構成はクリアされましたが、現在のコンフィギュレーションをクリアされたファイルに上書きしたのでは、意味がないので上書きしないという**n**を選択します。

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):

Validating file. Please wait...

Configuration is saved to device successfully.

This command will reboot the device. Continue? [Y/N]:**y**

手順7: ファイルのディレクトリーを表示します

pwdコマンドを実行して、現在のパスを表示します。

<YourName>pwd

flash:

<YourName>

現在のパスはflash:/です。 フラッシュは他のファイルディレクトリを保存し、一部のルーターには複数のハードディスクとCFカードが搭載されている場合があります。 **pwd**コマンドを実行すると、現在のパスが表示されます。

次に、**dir**コマンドを実行して、フラッシュ上のすべてのファイルを表示します。

<YourName>dir

Directory of flash:

```
   0 drw-           - Nov 26 2021 11:20:23   diagfile
   1 -rw-         253 Nov 26 2021 10:13:20   ifindex.dat
   2 -rw-       43136 Nov 26 2021 11:20:23   licbackup
   3 drw-           - Nov 26 2021 11:20:23   license
   4 -rw-       43136 Nov 26 2021 11:20:23   licnormal
   5 drw-           - Nov 26 2021 11:20:23   logfile
   6 -rw-           0 Nov 26 2021 11:20:23   msr36-cmw710-boot-a7514.bin
   7 -rw-           0 Nov 26 2021 11:20:23   msr36-cmw710-system-
a7514.bin
   8 drw-           - Nov 26 2021 11:20:30   pki
   9 drw-           - Nov 26 2021 11:20:23   seclog
  10 -rw-        2204 Nov 26 2021 10:13:20   startup.cfg
  11 -rw-       41214 Nov 26 2021 10:13:20   startup.mdb
1046512 KB total (1046328 KB free)
```

前の例では、dirコマンドの行の最初に行番号が表示されています。 2番目のカラムには属性が表示されます（drw-ディレクトリーを示し、-rw-は読み取りおよび書き込み可能なファイルを示します）。 3カラム目はファイルサイズを示します。 5行目は属性に基づいて、logfileが実際にはディレクトリーであることがわかります。

手順8: テキストファイルの中身を表示します

moreコマンドを使うとテキストファイルの中身を表示できます。

```
<YourName>more startup.cfg
#
 version 7.1.075, Alpha 7571
#
 sysname H3C
#
 clock protocol none
#
 system-working-mode standard
 xbar load-single
 password-recovery enable
 lpu-type f-series
#
vlan 1
#
interface Serial1/0
```

```
#
interface Serial2/0
#
interface Serial3/0
#
interface Serial4/0
#
interface NULL0
#
interface GigabitEthernet0/0
 port link-mode route
 combo enable copper
#
interface GigabitEthernet0/1
 port link-mode route
 combo enable copper
#
interface GigabitEthernet0/2
 port link-mode route
 combo enable copper
#
interface GigabitEthernet5/0
 port link-mode route
 combo enable copper
#
interface GigabitEthernet5/1
 port link-mode route
 combo enable copper
#
....
<YourName>
```

手順9: 現在のファイルパスを変更します

cdコマンドを使って現在のパスを変更することができます。

logfileのサブディレクトリーに移動します。

```
<YourName>cd logfile/
<YourName>dir
```

Directory of flash:/logfile

The directory is empty.

1046512 KB total (1046328 KB free)

現在のディレクトリーから一つ上のディレクトリーに移動します。

<YourName>cd ..

<YourName>pwd

flash:

<YourName>

手順10: ファイルを削除します

saveコマンドを実行して構成ファイルを20211126.cfgという名前を付けて保存し、

deleteコマンドを実行して構成ファイルを削除します。

<YourName>save 20211126.cfg

The current configuration will be saved to flash:/20211126.cfg. Continue? [Y/N]:y

Now saving current configuration to the device.

Saving configuration flash:/20211126.cfg.Please wait...

Configuration is saved to device successfully.

<YourName>dir

Directory of flash:

```
  0 -rw-        2209 Nov 26 2021 14:08:46    20211126.cfg
  1 -rw-       41214 Nov 26 2021 14:08:46    20211126.mdb
  2 drw-           - Nov 26 2021 11:20:23    diagfile
  3 -rw-         253 Nov 26 2021 14:08:46    ifindex.dat
  4 -rw-       43136 Nov 26 2021 11:20:23    licbackup
  5 drw-           - Nov 26 2021 11:20:23    license
  6 -rw-       43136 Nov 26 2021 11:20:23    licnormal
  7 drw-           - Nov 26 2021 11:20:23    logfile
  8 -rw-           0 Nov 26 2021 11:20:23    msr36-cmw710-boot-a7514.bin
  9 -rw-           0 Nov 26 2021 11:20:23    msr36-cmw710-system-
a7514.bin
 10 drw-           - Nov 26 2021 11:20:30    pki
 11 drw-           - Nov 26 2021 11:20:23    seclog
 12 -rw-        2204 Nov 26 2021 10:13:20    startup.cfg
 13 -rw-       41214 Nov 26 2021 10:13:20    startup.mdb
1046512 KB total (1046276 KB free)
```

<YourName>delete 20211126.cfg

Delete flash:/20211126.cfg? [Y/N]:**y**
Deleting file flash:/20211126.cfg... Done.
20211126.cfgファイルが削除された後、ファイルリストを照会して、ファイルが削除されたことを確認します。
<YourName>dir
Directory of flash:

0	-rw-	41214	Nov 26 2021 14:08:46	20211126.mdb
1	drw-	-	Nov 26 2021 11:20:23	diagfile
2	-rw-	253	Nov 26 2021 14:08:46	ifindex.dat
3	-rw-	43136	Nov 26 2021 11:20:23	licbackup
4	drw-	-	Nov 26 2021 11:20:23	license
5	-rw-	43136	Nov 26 2021 11:20:23	licnormal
6	drw-	-	Nov 26 2021 11:20:23	logfile
7	-rw-	0	Nov 26 2021 11:20:23	msr36-cmw710-boot-a7514.bin
8	-rw-	0	Nov 26 2021 11:20:23	msr36-cmw710-system-a7514.bin
9	drw-	-	Nov 26 2021 11:20:30	pki
10	drw-	-	Nov 26 2021 11:20:23	seclog
11	-rw-	2204	Nov 26 2021 10:13:20	startup.cfg
12	-rw-	41214	Nov 26 2021 10:13:20	startup.mdb

1046512 KB total (1046272 KB free)
yを選択してファイルを削除したにもかかわらず、ファイル内の使用可能なスペースが1046272KBの空き容量のままです。 どうして？
ファイルが削除されると、ごみ箱フォルダーが作成され、追加されたファイルがストレージスペースを占有します。 さらに、削除されたファイルは引き続きごみ箱に保存され、ストレージスペースを占有します。 ユーザーがこのコマンドを頻繁に使用してファイルを削除すると、デバイスのストレージ容量が減少します。 ごみ箱から廃棄ファイルを完全に削除し、ストレージスペースをリサイクルするには、ファイルの元のディレクトリーで**reset recycle-bin**コマンドを実行します。
dir / allコマンドを実行して、現在のディレクトリーの下にあるすべてのファイルとサブフォルダを表示します。 表示コンテンツには、非表示のファイル、非表示のフォルダー、非表示のファイル、および非表示のフォルダーが含まれます。
ごみ箱フォルダーの名前は.trashで、このフォルダー内のファイルは**dir / all .trash**コマンドを実行してクエリできます。
<YourName>dir /all
Directory of flash:

```
     0 -rw-          41214 Nov 26 2021 14:08:46     20211126.mdb
     1 drw-              - Nov 26 2021 11:20:23     diagfile
     2 -rw-            253 Nov 26 2021 14:08:46     ifindex.dat
     3 -rw-          43136 Nov 26 2021 11:20:23     licbackup
     4 drw-              - Nov 26 2021 11:20:23     license
     5 -rw-          43136 Nov 26 2021 11:20:23     licnormal
     6 drw-              - Nov 26 2021 11:20:23     logfile
     7 -rw-              0 Nov 26 2021 11:20:23     msr36-cmw710-boot-a7514.bin
     8 -rw-              0 Nov 26 2021 11:20:23     msr36-cmw710-system-
a7514.bin
     9 drw-              - Nov 26 2021 11:20:30     pki
    10 drw-              - Nov 26 2021 11:20:23     seclog
    11 -rw-           2204 Nov 26 2021 10:13:20     startup.cfg
    12 -rw-          41214 Nov 26 2021 10:13:20     startup.mdb
1046512 KB total (1046272 KB free)
<YourName>dir /all .trash
Directory of flash:/.trash
     0 -rw-           2209 Nov 26 2021 14:08:46     20211126.cfg_0001
     1 -rwh             52 Nov 26 2021 14:09:11     .trashinfo
1046512 KB total (1046272 KB free)
```

ファイル20211126.cfgは引き続きフラッシュで使用できます。 **reset recycle-bin**コマンドを実行して、ごみ箱をクリアし、ストレージスペースをリサイクルします。

```
<YourName>reset recycle-bin
Clear flash:/20211126.cfg? [Y/N]:y
Clearing file flash:/20211126.cfg... Done.

<YourName>dir /all .trash
Directory of flash:/.trash
     0 -rwh             0 Nov 26 2021 14:12:26     .trashinfo
1046512 KB total (1046280 KB free)
```

ごみ箱がクリアされた後、20211126.cfgファイルが削除され、使用可能なストレージスペースが1046280KBの空き容量に変更されます。

ごみ箱を使用せずにファイルを削除する別の方法があります。 **delete / unreserved**コマンドを実行して、ファイルを完全に削除します。 このコマンドは、コマンド**delete** を実行後 **reset recycle-bin**を実行したのと同等です。

```
<YourName>delete /unreserved  20211126.mdb
```

The file cannot be restored. Delete flash:/20211126.mdb? [Y/N]:y
Deleting the file permanently will take a long time. Please wait...
Deleting file flash:/20211126.mdb... Done.
<YourName>

タスク3：telnetでログインする

注意：HCLのPCはtelnetの機能がありません。そこで、PCを削除してPCの代わりにRouterやswitchを利用します。このラボではswitchを利用してtelnetを行います。
その場合の、switchのコンフィグは以下の通りです。

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]interface Vlan-interface 1
[H3C-Vlan-interface1]ip address 192.168.1.2 24
[H3C-Vlan-interface1]quit
[H3C]ping 192.168.1.1
Ping 192.168.1.1 (192.168.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=3.000 ms
56 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=3.000 ms
56 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for 192.168.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 2.000/2.400/3.000/0.490 ms
%Nov 26 18:14:17:722 2021 H3C PING/6/PING_STATISTICS: Ping statistics for
192.168.1.1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss,
round-trip min/avg/max/std-dev = 2.000/2.400/3.000/0.490 ms.

[H3C]save f
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
```

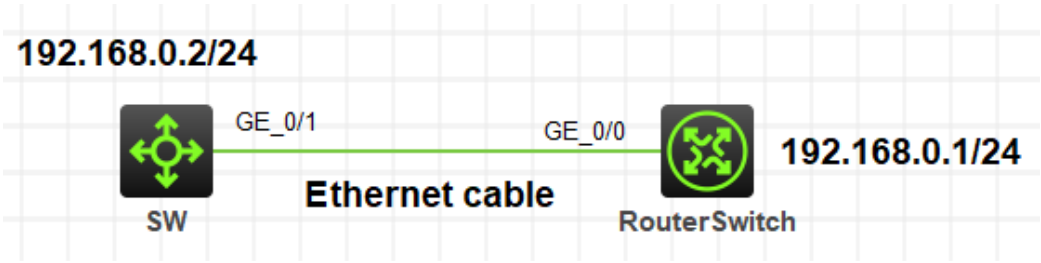


図 1.4 HCL の場合のネットワーク

手順1:コンソールポートからtelnetユーザーのコンフィギュレーションをする

<YourName>sys

System View: return to User View with Ctrl+Z.

testという名前のユーザーを作成します。

[YourName]local-user test

New local user added.

ログインパスワードをtestに設定します。 passwordコマンドを実行して、パスワードの構成方法を指定できます。 プレーンテキストのパスワードを構成するために示されるキーワードsimpleと、暗号パスワードを構成するために示されるキーワードcipher。

[YourName-luser-manage-test]password simple test

ユーザーのTelnetサービスタイプを設定します。 使用ロールはlevel 0です。レベル番号の数値が小さいほど、ユーザー権限は低くなります。

[YourName-luser-manage-test]service-type telnet

[YourName-luser-manage-test]authorization-attribute user-role level-0

[YourName-luser-manage-test]quit

手順2: superパスワードを設定します。

スーパーパスワードは、ユーザーロールを指定されたレベルに変更するために使用されます。 ユーザーロールをレベル15に変更するには、プレーンテキストモードでパスワードをH3Cに設定します。

[YourName]super password role level-15 simple H3C

手順3: welcome 情報を設定します。

ウェルカム情報を ”Welcome to H3C world!” に設定します。 文字 ”%” はテキストの終了文字です。 “%” と入力してテキストを終了し、ヘッダーコマンドを終了します。

[YourName]header login

Please input banner content, and quit with the character '%'.

Welcome to H3C world!%

[YourName]

手順4: telnetユーザーのローカル認証を設定する

VTY 0～63ユーザー行を入力します。 システムは、最大64のVTYユーザーの同時アクセスをサポートします。 VTYポートは論理端末回線であり、telnetまたはSSHを介してルーターにアクセスするために使用されます。

[YourName]line vty 0 63

ルーターは、ローカルサーバーまたはサードパーティサーバーを使用してユーザーを認証できます。 このラボでは、ローカル認証が採用されています（認証モードはschemeです）。

[YourName-line-vty0-63]authentication-mode scheme

[YourName-line-vty0-63]quit

手順5: インタフェースビューに入ってEthernetインタフェースにIPアドレスを設定する

interfaceコマンドを実行してイーサネットビューに入り、IPアドレスコマンドを実行してルータのイーサネットIPアドレスを設定します。

[YourName]interface GigabitEthernet 0/0

[YourName-GigabitEthernet0/0]ip address 192.168.0.1 255.255.255.0

[YourName-GigabitEthernet0/0]quit

PCのIPアドレスをルーターポートと同じネットワークセグメント上にある192.168.0.10/24に設定します。

PCを構成した後、PuTTYでルーターポートのGigabitEthernet0 / 1アップ情報を確認できます。

%Nov 26 15:33:00:860 2021 YourName IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet0/0 changed to up.

%Nov 26 15:33:00:860 2021 YourName IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet0/0 changed to up.

手順6: telnetサービスをenableにする

[YourName]telnet server enable

[YourName]save f

Validating file. Please wait...

Configuration is saved to device successfully.

手順7: telnetでログインする

クロスネットワークケーブルを使用してPCをルーターのイーサネットポートGigabitEthernet 0/0に接続し、PC CLIウィンドウでルーターポートのイーサネットIPアドレスをtelnetして、Enterキーを押します。

C:¥Users¥YourName>telnet 192.168.0.1

telnetのユーザー名とパスワードを入力して、構成ページに入ります。 ？を入力するとユーザーが使用できるコマンド（レベル0）を表示します。 ユーザーは最低レベルです。そのため、使用者はコマンドを表示し、いくつかのコマンドを使用することしかできません。

```
接続中  192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

******************************************************************************
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. All rights reserved.*
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

Welcome to H3C world!

login: test
Password: test
<YourName>?
User view commands:
  display        Display current system information
  erase          Alias for 'delete'
  exit           Alias for 'quit'
  no             Alias for 'undo'
  quit           Exit from current command view
  show           Alias for 'display'
  system-view    Enter System View
  write          Alias for 'save'
  xml            Enter XML view
<YourName>
```

次の情報がPuTTYに表示されます。これは、ユーザーがPC経由でルーターにログインしていることを示しています。

```
<YourName>
%Nov 29 10:21:18:727 2021 YourName SHELL/5/SHELL_LOGIN: Console logged
in from con0.
```

手順8: ユーザーrole(役割と権限)を変更する

superコマンドを実行してユーザーロールを変更し、スーパーパスワードを入力してレベル15に入ります。ユーザーレベル15で使用できるコマンドとユーザーレベル0で使用できるコマンドを比較します。

```
<YourName>super level-15 ?
  <cr>

<YourName>super level-15
Password: H3C
User privilege role is level-15, and only those commands that authorized to the
role can be used.
<YourName>?
User view commands:
  archive                 Archive configuration
  arp                     Address Resolution Protocol (ARP) module
  backup                  Backup operation
  boot-loader             Software image file management
  bootrom                 Update/read/backup/restore bootrom
  bootrom-access          Bootrom access control
  cd                      Change current directory
  clock                   Specify the system clock
  copy                    Copy a file
  debugging               Enable system debugging functions
  delete                  Delete a file
  diagnostic-logfile      Diagnostic log file configuration
  dialer                  Specify Dial-on-Demand Routing(DDR) configuration
                          information
  dir                     Display files and directories on the storage media

.....中略
                          algorithm
  show                    Alias for 'display'
  ssh2                    Establish a secure shell client connection
  startup                 Specify system startup parameters
  super                   Switch to a user role
  system-view             Enter System View
```

```
tar                  Archive management
tclquit              Exit from TCL shell
tclsh                Enter the TCL shell
telnet               Establish a telnet connection
terminal             Set the terminal line characteristics
tftp                 Open a TFTP connection
tracert              Tracert function
umount               Unmount a storage medium
undelete             Recover a deleted file
undo                 Cancel current setting
write                Alias for 'save'
xml                  Enter XML view
```

手順9: 設定をセーブしてルーターをリスタートします。

saveコマンドを実行して、現在の情報をルーターストレージに保存します。 次に、**5**コマンドを実行してシステムを再起動します。

```
<YourName>save force
Validating file. Please wait...
Configuration is saved to device successfully.
<YourName>reboot
Start to check configuration with next startup configuration file, please
wait.....DONE!
This command will reboot the device. Continue? [Y/N]:

Now rebooting, please wait...
```

タスク4：ftpを使ってシステムファイルをアップロード、ダウンロードする

手順1: コンソールポートからftpユーザーの設定をする

```
<YourName>system-view
System View: return to User View with Ctrl+Z.
[YourName]local-user test_ftp
New local user added.
[YourName-luser-manage-test_ftp]password simple test_ftp
```

手順2: ユーザーのためにftpサービスタイプを設定して、ユーザーのroleをlevel 15に設定する

```
[YourName-luser-manage-test_ftp]service-type ftp
[YourName-luser-manage-test_ftp]authorization-attribute user-role level-15
[YourName-luser-manage-test_ftp]quit
```

手順3: ftpサービスをenableにする

[YourName]ftp server enable

手順4: ftpにログインする

<H3C>ftp 192.168.0.1

Press CTRL+C to abort.

Connected to 192.168.0.1 (192.168.0.1).

220-

220-Welcome to H3C world!

220 FTP service ready.

User (192.168.0.1:(none)): test_ftp

331 Password required for test_ftp.

Password: test_ftp

230 User logged in.

Remote system type is UNIX.

Using binary mode to transfer files.

手順5: ftpを使ってファイルをアップロードする

ftp> put test.txt

227 Entering Passive Mode (192,168,0,1,220,127)

150 Accepted data connection

.

226 File successfully transferred

6187 bytes sent in 0.000 seconds (6.04 Kbytes/s)

手順6: ftpを使ってファイルをダウンロードする

ftp> get startup.cfg

startup.cfg already exists. Overwrite it? [Y/N]:y

227 Entering Passive Mode (192,168,0,1,222,13)

150 Accepted data connection

.

226 File successfully transferred

3080 bytes received in 0.002 seconds (1.47 Mbytes/s)

ftp> quit

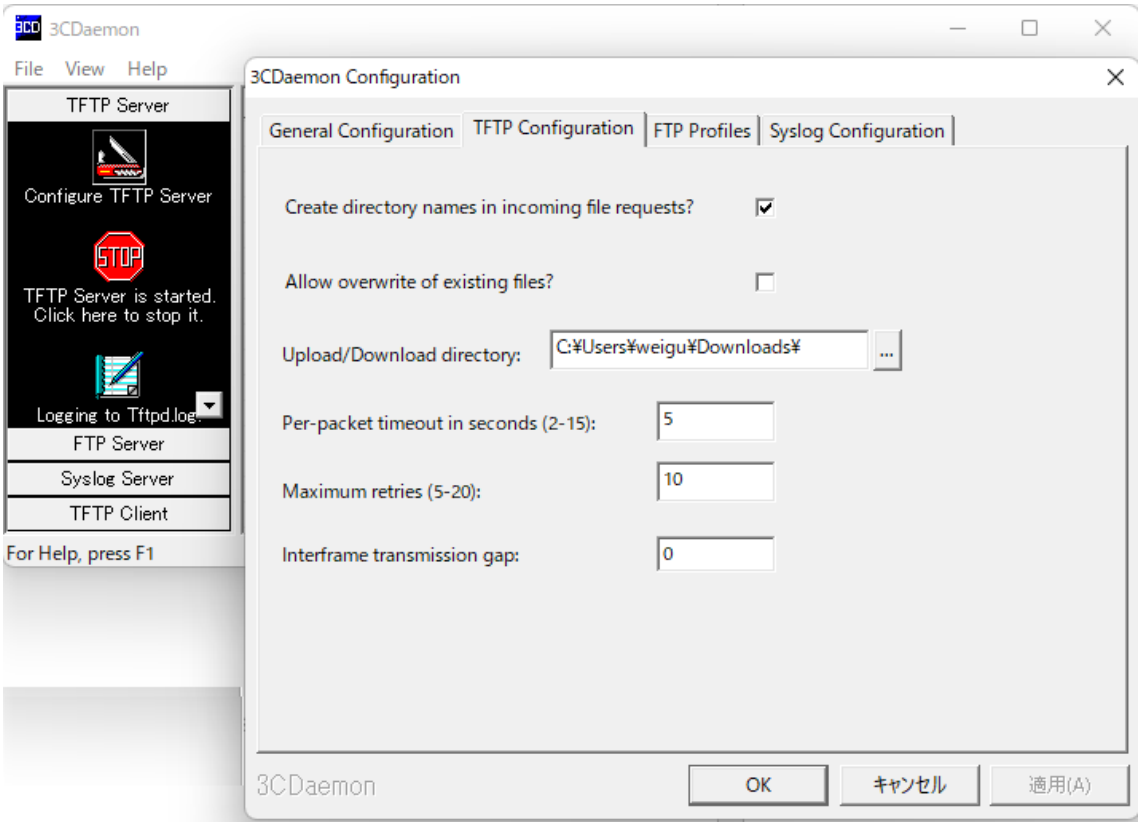
221-Goodbye. You uploaded 7 and downloaded 4 kbytes.

221 Logout.

タスク5：tftpを使ってシステムファイルをアップロード、ダウンロードする

手順1: tftpサーバーをenableにする

このラボではTFTPサーバーアプリケーションとして3CDaemonを使います。TFTPサーバーのパラメーターを設定し、ファイルのアップロード、ダウンロードのローカルディレクトリー(c:¥)を設定します。



手順2: tftpを使ってファイルをアップロードする

<YourName>tftp 192.168.0.2 get test.cfg

Press CTRL+C to abort.

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   598  100   598    0     0      0      0 --:--:--  0:00:40 --:--:--  116k
```

手順3: tftpを使ってファイルをダウンロードする

<YourName>tftp 192.168.0.2 put test.txt

Press CTRL+C to abort.

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   598  100   598    0     0      0      0 --:--:--  0:00:40 --:--:--  116k
```

質問:

1. このラボでは、システム時刻がコンフィギュレーションされているのを確認できない(コンフィギュレーションの中にclock時間が表示されない)のはなぜですか？

答え:

clockコマンドは、システムのハードウェアパラメータを変更するために使用されるコマンドであり、すぐに有効になります。 そのため、クロックは現在の構成ファイルまたは保存された構成ファイルに表示されません。

Lab2 ネットワーク機器の結線とデバッグ

実習内容と目標

このラボでは以下のことを学びます：

- ルーターをシリアルケーブルで接続する方法を習得します。
- Ping と tracert コマンドでシステムの接続性を試験する方法を習得します。
- デバッギングコマンドを使う方法を習得します。

ネットワーク図

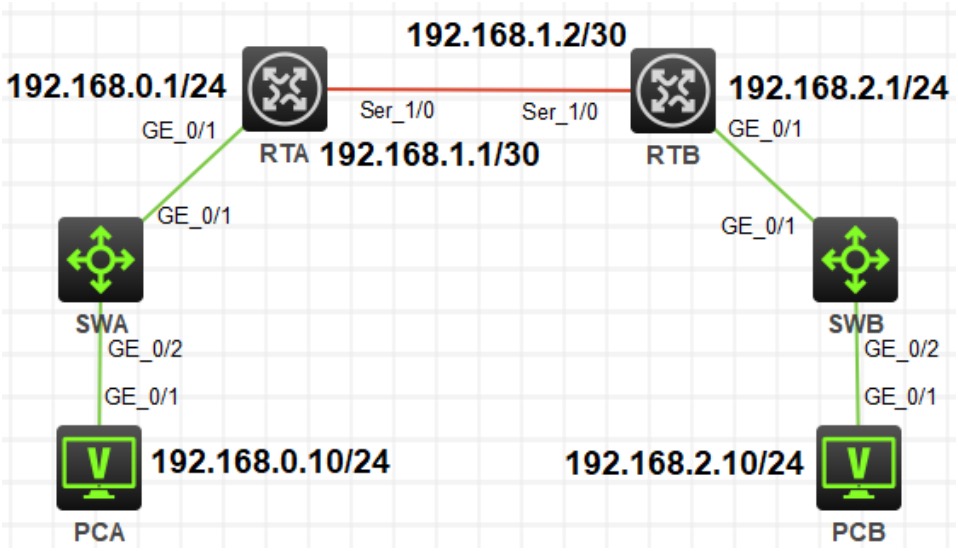


図 2.1 実習ネットワーク

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
S5820V2	Version7.1		
PC	Windows 7	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	
ネットワークケーブルの接続	--	4	なし

実習手順

タスク1：IPアドレスを設定してケーブルを接続する

このタスクは、ユーザーがルーター、スイッチ、PCを接続する方法に慣れるようにします。

手順1：PCとルーターをケーブルで接続する

図2.1のように2つのルーターを1つのケーブルで接続します。ルーターをそれぞれのスイッチS5820V2へ接続します。 PCとスイッチをケーブルで接続します。

手順2：IPアドレスを設定する

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2.1 IPアドレス割り当てスキーマ

装置	**インターフェース**	**IPアドレス**	**ゲートウェイ**
RTA	S1/0	192.168.1.1/30	-
	G0/0	192.168.0.1/24	-
RTB	S1/0	192.168.1.2/30	-
	G0/0	192.168.2.1/24	-
PCA		192.168.0.10/24	192.168.0.1
PCB		192.168.2.10/24	192.168.2.1

以下のようにRTAにIPアドレスを割り当てます：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname RTA
Configuration is saved to device successfully.
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ip address 192.168.0.1 24
[RTA-GigabitEthernet0/1]quit
[RTA]interface Serial 1/0
[RTA-Serial1/0]ip address 192.168.1.1 30
[RTA-Serial1/0]quit
[RTA]save f
Validating file. Please wait...
Configuration is saved to device successfully.
```

RTBのコンフィギュレーションは以下の通りです：

```
<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]sysname RTB
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ip address 192.168.2.1 24
[RTB-GigabitEthernet0/1]quit
[RTB]interface Serial 1/0
[RTB-Serial1/0]ip address 192.168.1.2 30
[RTB-Serial1/0]quit
```

タスク2：pingコマンドで装置の接続性をチェックします

このタスクは、ユーザーがルーター、スイッチ、PCの接続性をチェックする方法に慣れるようにします。

手順1：RTAからRTBへpingする

RTAへログインしてルーターの接続性をチェックするためにRTBのシリアルポートS1/0へpingします。

```
<RTA>ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=2.000 ms
```

56 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=2.000 ms

RTAはICMPエコー応答パケットを受信し、RTAがRTBにpingできることを示します。

RTAは、デフォルトで5つの**56バイト**ICMP要求パケットを送信します。 pingが成功すると、RTAは5つの応答パケットを受信します。 Windowsデバイスは、デフォルトで4つの32バイトICMP要求パケットを送信します。

手順2：pingコマンドのパラメーターをチェックします

```
<RTA>ping ?
  -a                  Specify the source IP address
  -c                  Specify the number of echo requests
  -f                  Specify packets not to be fragmented
  -h                  Specify the TTL value
  -i                  Specify an outgoing interface
  -m                  Specify the interval for sending echo requests
  -n                  Numeric output only. No attempt will be made to lookup host
                      addresses for symbolic names
  -p                  No more than 8 "pad" hexadecimal characters to fill out the
                      sent packet. For example, -p f2 will fill the sent packet with
                      000000f2 repeatedly
  -q                  Display only summary
  -r                  Record route. Include the RECORD_ROUTE option in the
                      ECHO_REQUEST packets and display the route
  -s                  Specify the payload length
  -t                  Specify the wait time for each reply
  -topology           Specify a topology
  -tos                Specify the TOS value
  -v                  Display the received ICMP packets other than ECHO-
RESPONSE
                      packets
  -vpn-instance       Specify a VPN instance
  STRING<1-253>       IP address or hostname of remote system
  ip                  IP information
  ipv6                IPv6 information
  mpls                MPLS ping
```

例えば、**-c**パラメーターを使ってpingパケットを50回送信します。

```
<RTA>ping -c 50 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
```

56 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=3.000 ms
-sパラメーターを使って、送信するパケットのサイズを512バイトにします。
<RTA>ping -s 512 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 512 data bytes, press CTRL_C to break
512 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=1.000 ms
512 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=2.000 ms
512 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=2.000 ms
パラメーター **-a**を使用して、pingパケットの送信元IPアドレスを設定します。 ネットワークのデバッグ中に、送信元IPアドレスを追加してネットワーク接続を確認します。 このラボでは、送信元IPアドレスはRTA G0/1ポートであり、pingオブジェクトはPCBです。
<RTA>ping -a 192.168.0.1 192.168.2.10
Ping 192.168.2.10 (192.168.2.10) from 192.168.0.1: 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
送信元IPアドレスとして使用できるのはローカルポートアドレスのみです。pingが失敗した場合は、次の手順に進みます。

手順3：PCAでRTAにpingします
<PCA>ping 192.168.0.1
Ping 192.168.0.1 (192.168.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=3.000 ms
56 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=3.000 ms

<PCA>ping 192.168.1.1
Ping 192.168.1.1 (192.168.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=3.000 ms
56 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=1.000 ms

手順4：PCAでRTBにpingします
<PCA>ping 192.168.1.2

Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

手順5：PCAでPCBにpingします

<H3C>ping 192.168.2.10

Ping 192.168.2.10 (192.168.2.10): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

PCAがPCBへのpingに失敗するのはなぜですか？

以下の手順に従って、原因を確認してください

1. PCA の RTA ポート GigabitEthernet0/1 および Serial1/0 に ping を実行します。 ポートに ping を実行できます。
2. PCA の RTB ポート Serial1/0 に ping を実行します。 ポートに ping を実行することはできません。
3. PCA で PCB に ping を実行します。 PCB に ping を実行することはできません。

RTBおよびPCBに送信されるICMP要求パケット（エコー要求）には、応答パケット（エコー応答）がありません。

RTAでdisplay ip routing-tableコマンドを実行して、ルーティングテーブルを確認します。

<RTA>display ip routing-table

Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/1
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/1
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/1
192.168.1.0/30	Direct	0	0	192.168.1.1	Ser1/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser1/0

192.168.1.1/32 Direct 0 0 127.0.0.1 InLoop0
192.168.1.2/32 Direct 0 0 192.168.1.2 Ser1/0
192.168.1.3/32 Direct 0 0 192.168.1.1 Ser1/0
224.0.0.0/4 Direct 0 0 0.0.0.0 NULL0
224.0.0.0/24 Direct 0 0 0.0.0.0 NULL0
255.255.255.255/32 Direct 0 0 127.0.0.1 InLoop0

ルーティングテーブルの宛先列で、エントリ192.168.2.0は使用できません。 そのため、PCB宛てのpingパケットを受信するRTAは、パケットをPCBに転送せず、直接パケットを破棄します。 その結果、PCAはPCBへのpingに失敗します。

エントリ192.168.1.2が使用可能ですが、PCAはどのようにしてRTBポートSerial1 / 0へのpingに失敗しますか？ RTBのルーティングテーブルでは、エントリ192.168.0.0は使用できません。 ただし、RTAはPCA ping要求パケットをRTBに送信します。 RTBは、ping応答パケットをPCAに転送しません。 その結果、PCAはRTBポートserial1 / 0へのpingに失敗します。

分析に基づいて、ステップ1の最後のテスト項目の原因は明らかです。 RTAにはIPアドレス192.168.2.0/24へのルーターがなく、RTBにもIPアドレス192.168.2.0/24へのルートがありません。

手順6：static routeを設定します

ip route-staticコマンドを実行して、宛先ネットワークセグメントをピアルータとPCを接続するものに設定し、ネクストホップをピアルータのポートに設定して、RTAおよびRTBに静的ルートを設定します。

RTAの構成は次のとおりです。

[RTA]ip route-static 192.168.2.0 255.255.255.0 192.168.1.2

RTBの構成は次のとおりです。

[RTB]ip route-static 192.168.0.0 255.255.255.0 192.168.1.1

PCAでPCBにpingします。

<PCA>ping 192.168.2.10
Ping 192.168.2.10 (192.168.2.10): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.2.10: icmp_seq=0 ttl=253 time=5.000 ms
56 bytes from 192.168.2.10: icmp_seq=1 ttl=253 time=4.000 ms
56 bytes from 192.168.2.10: icmp_seq=2 ttl=253 time=8.000 ms
56 bytes from 192.168.2.10: icmp_seq=3 ttl=253 time=6.000 ms

静的ルートがRTAおよびRTBで設定された後、PCAはPCBにpingを実行できます。

PCBにpingを実行するための送信元IPアドレスとしてRTAポートGigabitEthernet0 / 1を使用します。

[RTA]ping -a 192.168.0.1 192.168.2.10

Ping 192.168.2.10 (192.168.2.10) from 192.168.0.1: 56 data bytes, press CTRL_C to break

56 bytes from 192.168.2.10: icmp_seq=0 ttl=254 time=3.000 ms

56 bytes from 192.168.2.10: icmp_seq=1 ttl=254 time=6.000 ms

56 bytes from 192.168.2.10: icmp_seq=2 ttl=254 time=6.000 ms

56 bytes from 192.168.2.10: icmp_seq=3 ttl=254 time=5.000 ms

タスク3：tracertコマンドで装置の接続性をチェックします

tracertコマンドを実行して、パケットが送信元デバイスから宛先デバイスに通過するルートノードを表示します。 ネットワークに障害が発生した場合は、このコマンドを実行して障害のあるノードを特定します。

手順1：PCAでPCBへtracertする

PCAでCLIに入って、PCBのIPアドレスへtracertする。

C:¥Users¥HCL>tracert 192.168.2.10

PCAは3つのTTLICMPパケットを受け取ります。 最初のホップは192.168.0.1であり、最初のパケットがRTAによって返されることを示します。 類推により、2番目のパケットはRTBによって返され、3番目のパケットはPCBによって返されます。 3つのネットワークノードに到達可能です。 ネットワークノードの1つに到達できない場合、対応するTTLパケットは再送信されません。 これに基づいて、障害のあるノードを特定できます。

手順2：RTAでPCBへtracertする

RTAでPCBのIPアドレスへtracertする。

<RTA>tracert 192.168.2.10

traceroute to 192.168.2.10 (192.168.2.10), 30 hops at most, 52 bytes each packet, press CTRL_C to break

1 192.168.1.2 (192.168.1.2) 16.691 ms 16.620 ms 16.556 ms

2 192.168.2.10 (192.168.2.10) 16.636 ms 16.624 ms 16.569 ms

最初のホップはRTBで、次のホップはPCBです。

注意：HCLではtracertの機能が実現されておりませんので、以下のような出力になります。

<RTA>tracert 192.168.2.10

traceroute to 192.168.2.10 (192.168.2.10), 30 hops at most, 40 bytes each packet, press CTRL_C to break

1 * * *

2 * * *

tracertコマンドのパラメーターをチェックします。

```
<RTA>tracert ?
  -a                Specify the source IP address used by TRACERT
  -f                Specify the TTL value for the first packet
  -m                Specify the maximum TTL value
  -p                Specify the destination UDP port number
  -q                Specify the number of probe packets sent each time
  -t                Set the Type of Service (ToS) value
  -topology         Specify a topology
  -vpn-instance     Specify a VPN instance
  -w                Set the timeout to wait for each reply
  STRING<1-253>     IP address or hostname of the destination device
  ipv6              IPv6 information
  mpls              MPLS trace route
```

debuggingコマンドを実行して、デバッグ情報を表示します。

RTBの情報のmonitoringおよびdisplay機能を有効にします。

RTBでterminal monitorコマンドを実行して、システムmonitoring機能を有効にし、terminal debuggingコマンドを実行して、デバッグ情報表示機能を有効にします。

```
<RTB>terminal monitor
The current terminal is enabled to display logs.
<RTB>terminal debugging
The current terminal is enabled to display debugging logs.
```

手順3：RTBでICMP debugging switchをenableにします

RTBでdebugging ip icmp コマンドを実行してICMPモジュールのデバッキング機能をenableにします。

```
<RTB>debugging ip icmp
```

手順4：RTAでRTBにpingし、RTBでデバッグ情報を見ます

```
<RTA>ping -c 10 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=2.000 ms
```

56 bytes from 192.168.1.2: icmp_seq=5 ttl=255 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=6 ttl=255 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=7 ttl=255 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=8 ttl=255 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=9 ttl=255 time=3.000 ms

--- Ping statistics for 192.168.1.2 ---
10 packet(s) transmitted, 10 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/2.300/3.000/0.781 ms

RTBでバッギング情報を見ます。
*Nov 24 18:00:03:206 2021 RTB SOCKET/7/ICMP:
ICMP Input:
  ICMP Packet: vpn = PUBLIC(0), src = 192.168.1.1, dst = 192.168.1.2
               type = 8, code = 0 (echo)

*Nov 24 18:00:03:206 2021 RTB SOCKET/7/ICMP:
ICMP Output:
  ICMP Packet: vpn = PUBLIC(0), src = 192.168.1.2, dst = 192.168.1.1
               type = 0, code = 0 (echo-reply)

*Nov 24 18:00:03:410 2021 RTB SOCKET/7/ICMP:
ICMP Input:
  ICMP Packet: vpn = PUBLIC(0), src = 192.168.1.1, dst = 192.168.1.2
               type = 8, code = 0 (echo)

*Nov 24 18:00:03:410 2021 RTB SOCKET/7/ICMP:
ICMP Output:
  ICMP Packet: vpn = PUBLIC(0), src = 192.168.1.2, dst = 192.168.1.1
               type = 0, code = 0 (echo-reply)

手順5：スイッチのでバッギングをdisableにします。

Undo debugging allコマンドで全てのモジュールのスイッチのでバッキングをdisableにします。

<RTB>undo debugging all
All possible debugging has been turned off.
<RTB>undo terminal monitor

The current terminal is disabled to display logs.

質問:

1． 手順1のタスク2では、ping 192.168.1.2基本コマンドを使用しますが、ping -a 192.168.0.1 192.168.1.2拡張コマンドを使用すると、結果が異なります。 ルーターはどのようにパケットを処理しますか？

答え:

基本コマンドを使用する場合、ICMP応答パケットの送信元IPアドレスは192.168.1.1です。 拡張コマンドを使用する場合、送信元IPアドレスは192.168.0.1として指定されます。 そのため、ICMP応答パケットの宛先IPアドレスは異なります。

Lab3 VLANの設定

実習内容と目標

このラボを修了すると以下のことができるようになります：

- ホスト間のレイヤー2トラフィックを分離するためにVLANを設定します。
- アクセスポートとトランクポートを設定します。

ネットワーク図

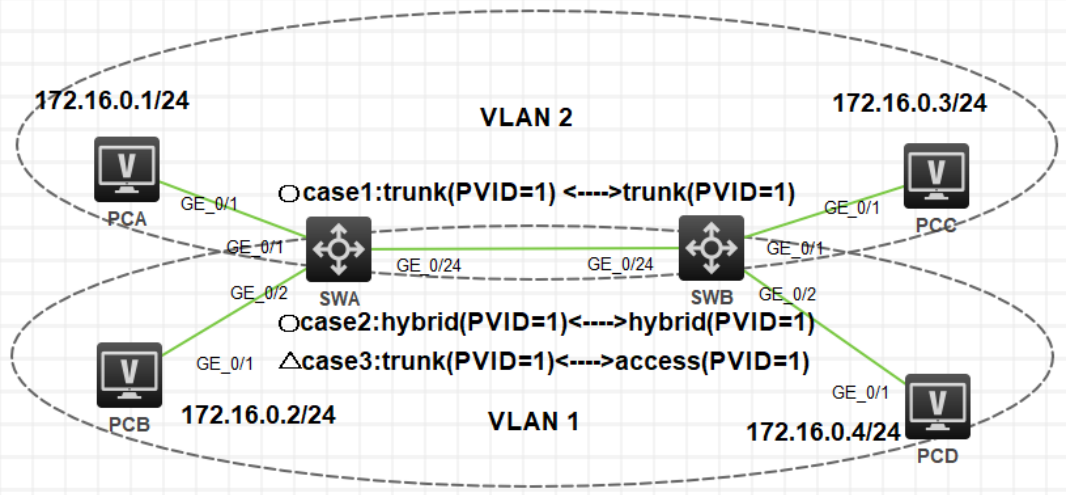


図 3.1 実習ネットワーク

現状

- スイッチ SWA、スイッチ SWB、PCA、PCB、PCC、PCD は、上の図のように配線されています。

最後に設定されたプロトコルが機能するかどうかをチェックします。

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
スイッチS5820v2	7571	2	なし
PC	Windows 7	4	なし
ネットワークケーブルの接続	--	5	なし

実習手順

タスク1：アクセスポートのコンフィギュレーション

このタスクはリンクタイプがアクセスのポートをどのように設定するかを表しています。そして、PC間のレイヤー2コミュニケーションを不可能にするためにどのようにPCをVLANにアサインするかを理解することです。

手順1：ケーブルの接続

図3.1のようにスイッチ間、スイッチとPC間のケーブルを接続します。

SWA、SWB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。

```
<SWA>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.
<SWA>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
.....
```

手順2：それぞれのスイッチのデフォルトVLANのコンフィギュレーションをチェックする

```
# SWA の VLAN の表示例
<SWA>display vlan
 Total VLANs: 1
 The VLANs include:
 1(default)

#システムのデフォルト VLAN である VLAN 1 のコンフィギュレーションをチェックします。
<SWA>display vlan 1
 VLAN ID: 1
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:     None
 Untagged ports:
     FortyGigE1/0/53                 FortyGigE1/0/54
     GigabitEthernet1/0/1            GigabitEthernet1/0/2
     GigabitEthernet1/0/3            GigabitEthernet1/0/4
```

GigabitEthernet1/0/5 GigabitEthernet1/0/6
GigabitEthernet1/0/7 GigabitEthernet1/0/8
GigabitEthernet1/0/9 GigabitEthernet1/0/10
GigabitEthernet1/0/11 GigabitEthernet1/0/12
GigabitEthernet1/0/13 GigabitEthernet1/0/14
GigabitEthernet1/0/15 GigabitEthernet1/0/16
GigabitEthernet1/0/17 GigabitEthernet1/0/18
GigabitEthernet1/0/19 GigabitEthernet1/0/20
GigabitEthernet1/0/21 GigabitEthernet1/0/22
GigabitEthernet1/0/23 GigabitEthernet1/0/24

#それぞれのポートのコンフィギュレーションをチェックします。例えば GigabitEthernet 1/0/1。

<H3C>display interface GigabitEthernet 1/0/1
GigabitEthernet1/0/1
Current state: UP
Line protocol state: UP
IP packet frame type: Ethernet II, hardware address: a61c-99cb-0100
Description: GigabitEthernet1/0/1 Interface
Bandwidth: 1000000 kbps
Loopback is not set
1000Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
Maximum frame length: 9216
Allow jumbo frames to pass
Broadcast max-ratio: 100%
Multicast max-ratio: 100%
Unicast max-ratio: 100%
PVID: 1
MDI type: Automdix
Port link-type: Access
  Tagged VLANs: None
  Untagged VLANs: 1
Port priority: 2
Last link flapping: 0 hours 17 minutes 35 seconds
Last clearing of counters: Never
Current system time:2021-10-29 17:22:21
Last time when physical state changed to up:2021-10-29 17:04:46
Last time when physical state changed to down:2021-10-29 17:04:41
  Peak input rate: 0 bytes/sec, at 00-00-00 00:00:00
  Peak output rate: 0 bytes/sec, at 00-00-00 00:00:00
  Last 300 second input: 0 packets/sec 0 bytes/sec 0%
  Last 300 second output: 0 packets/sec 0 bytes/sec 0%
  Input (total): 0 packets, 0 bytes
            0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
  Input (normal): 0 packets, 0 bytes
            0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
  Input: 0 input errors, 0 runts, 0 giants, 0 throttles
            0 CRC, 0 frame, 0 overruns, 0 aborts
            0 ignored, 0 parity errors
  Output (total): 0 packets, 0 bytes
            0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses

```
  Output (normal): 0 packets, 0 bytes
           0 unicasts, 0 broadcasts, 0 multicasts, 0 pauses
  Output: 0 output errors, 0 underruns, 0 buffer failures
           0 aborts, 0 deferred, 0 collisions, 0 late collisions
           0 lost carrier, 0 no carrier
```

SWA 上のすべてのポートはデフォルト VLAN である VLAN 1 に属していて、PVID 1 である。

手順3：VLANを作成してそれにポートを割り当てます。

```
# SWA のコンフィギュレーションをします
[SWA]vlan 2
[SWA-vlan2]port GigabitEthernet 1/0/1
[SWA-vlan2]quit

# SWB のコンフィギュレーションをします
[SWB]vlan 2
[SWB-vlan2]port GigabitEthernet 1/0/1
[SWB-vlan2]quit

#コンフィギュレーションをチェックします。
[SWA]display vlan
  Total VLANs: 2
  The VLANs include:
  1(default), 2

[SWA]display vlan 2
  VLAN ID: 2
  VLAN type: Static
  Route interface: Not configured
  Description: VLAN 0002
  Name: VLAN 0002
  Tagged ports:     None
  Untagged ports:
      GigabitEthernet1/0/1

[SWB]display vlan
  Total VLANs: 2
  The VLANs include:
  1(default), 2

[SWB]display vlan 2
  VLAN ID: 2
  VLAN type: Static
  Route interface: Not configured
  Description: VLAN 0002
  Name: VLAN 0002
  Tagged ports:     None
  Untagged ports:
      GigabitEthernet1/0/1
```

手順4：VLAN間の分離効果を試験する。

表3-1 IPアドレスアサインスキーム

装置名	IPアドレス
PCA	172.16.0.1/24
PCB	172.16.0.2/24
PCC	172.16.0.3/24
PCD	172.16.0.4/24

PC間でpingコマンドを実行して、異なるVLAN間での接続を試験してください。

例えば、PCAからPCBへping

<PCA>ping 172.16.0.2

Ping 172.16.0.2 (172.16.0.2): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

タスク2：Trunk portのコンフィギュレーション

このタスクでは、スイッチ間で同じVLANに属するPC同士でトラフィックを転送できるようにするためにtrunk port (802.1Qタグポート)をどのように設定するかを示しています。

手順1：Trunk portを設定する

異なるスイッチ上の同一VLANに属するPC同士で（PCAとPCC）でpingにより疎通確認をします。

<PCA>ping 172.16.0.3

Ping 172.16.0.3 (172.16.0.3): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

以上の結果は、PCCがpingに答えなかったことを表しています。この結果はSWAとSWB間のポートがaccess portであり、VLAN 1に属しているので、VLAN 2からのフレームを通しません。この問題を解決するために2つのスイッチ間のGigabitEternet 1/0/24ポートをtrunk portに設定します。

手順2: スイッチ間のポートのタイプをTrunk portに設定する

SWAをコンフィギュレーションします。

```
[SWA]interface GigabitEthernet 1/0/24
[SWA-GigabitEthernet1/0/24]port link-type trunk
[SWA-GigabitEthernet1/0/24]port trunk permit vlan all
[SWA-GigabitEthernet1/0/24]quit
```

SWBをコンフィギュレーションします。

```
[SWB]interface GigabitEthernet 1/0/24
[SWB-GigabitEthernet1/0/24]port link-type trunk
[SWB-GigabitEthernet1/0/24]port trunk permit vlan all
[SWB-GigabitEthernet1/0/24]quit
```

SWAのコンフィギュレーションを確認します。

```
[SWA]display vlan 2
 VLAN ID: 2
 VLAN type: Static
 Route interface: Not configured
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:
     GigabitEthernet1/0/24
 Untagged ports:
     GigabitEthernet1/0/1
```

この結果はGigabitEthernet 1/0/24がVLAN 2にあり、VLAN 2 からのフレームをタグを外さずに送信することを表しています。

スイッチ間のポートの情報を表示します。例えば、SWAのGigabitEthernet 1/0/24では:

```
<SWA>display interface GigabitEthernet 1/0/24
......
PVID: 1
MDI type: Automdix
Port link-type: Trunk
 VLAN Passing:     1(default vlan), 2
```

VLAN permitted: 1(default vlan), 2-4094

Trunk port encapsulation: IEEE 802.1q

出力はこのポートのPVIDが1、リンクタイプがtrunkであることを示しています。ポートはVLAN 1から4094のフレームを通します。

手順3: スイッチをまたがるVLAN通信をテストする

PCAでPCCに対してpingコマンドを使います。

<H3C>ping 172.16.0.3

Ping 172.16.0.3 (172.16.0.3): 56 data bytes, press CTRL_C to break

56 bytes from 172.16.0.3: icmp_seq=0 ttl=255 time=6.000 ms

56 bytes from 172.16.0.3: icmp_seq=1 ttl=255 time=7.000 ms

56 bytes from 172.16.0.3: icmp_seq=2 ttl=255 time=4.000 ms

56 bytes from 172.16.0.3: icmp_seq=3 ttl=255 time=6.000 ms

56 bytes from 172.16.0.3: icmp_seq=4 ttl=255 time=5.000 ms

同じVLANの2つのPCがスイッチをまたがってコミュニケートしていることを表している。

質問:

1. タスク2でSWAとSWBのポートGigabitEthernet 1/0/24でVLAN 2のフレームを通すのはどのリンクタイプでしょうか？

答え: hybrid

SWAをコンフィギュレーションします。

[SWA]interface GigabitEthernet 1/0/24

[SWA-GigabitEthernet1/0/24]port link-type hybrid

[SWA-GigabitEthernet1/0/24]port hybrid vlan 1 2 tagged

[SWA-GigabitEthernet1/0/24]quit

SWBをコンフィギュレーションします。

[SWB]interface GigabitEthernet 1/0/24

[SWB-GigabitEthernet1/0/24]port link-type hybrid

[SWB-GigabitEthernet1/0/24] port hybrid vlan 1 2 tagged

[SWB-GigabitEthernet1/0/24]quit

2. SWAのGigabitEthernet 1/0/24はPVID 1をもつtrunkポートだと仮定し、SWBのGigabitEthernet 1/0/24はPVID 1を持つaccessポートだとすると、タスク2のPCBは

PCDとコミュニケーションできますか？また、PCAはPCCとコミュニケーションできますか？
SWAをコンフィギュレーションします。
[SWA]interface GigabitEthernet 1/0/24
[SWA-GigabitEthernet1/0/24]port link-type trunk
[SWA-GigabitEthernet1/0/24] port trunk permit vlan all
[SWA-GigabitEthernet1/0/24]quit
SWBをコンフィギュレーションします(デフォルトはaccess)。
[SWB]interface GigabitEthernet 1/0/24
[SWB-GigabitEthernet1/0/24]port link-type access
[SWB-GigabitEthernet1/0/24]quit

答え：PCAとPCCはコミュニケーションできませんが、PCBとPCDはコミュニケーション出来ます。
<PCA>ping 172.16.0.3
Ping 172.16.0.3 (172.16.0.3): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

<PCB>ping 172.16.0.4
Ping 172.16.0.4 (172.16.0.4): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.0.4: icmp_seq=0 ttl=255 time=3.000 ms
56 bytes from 172.16.0.4: icmp_seq=1 ttl=255 time=4.000 ms
56 bytes from 172.16.0.4: icmp_seq=2 ttl=255 time=4.000 ms
56 bytes from 172.16.0.4: icmp_seq=3 ttl=255 time=5.000 ms
56 bytes from 172.16.0.4: icmp_seq=4 ttl=255 time=5.000 ms

Link-typeのおさらい：

パケットの向かう方向	Access	Trunk	Hybrid
タグなしフレームのインバウンド方向	フレームにPVIDタグを付けます。	・ポートで PVID が許可されている場合は、フレームに PVID タグを付けます。 ・そうでない場合は、フレームをドロップします。	
タグ付きフレームのインバウンド方向	・VLAN ID が PVID と同じであれば、フレームを受信します。 ・VLAN IDがPVIDと異なる場合は、フレームをドロップします。	・VLAN がポートで許可されている場合は、フレームを受信します。 ・VLANがポートで許可されていない場合は、フレームをドロップします。	
アウトバウンド方向	VLANタグを削除し、フレームを送信します。	•フレームが PVID タグを持ち、ポートが PVID に属している場合は、タグを削除してフレームを送信します。 •VLANがポート上で伝送されているがPVIDと異なる場合、タグを削除せずにフレームを送信します。	VLANがポートで許可されている場合にフレームを送信します。フレームのタギングステータスは、**port hybrid** *vlanvlan-id-list* **{ tagged | untagged }**コマンドの設定によって異なります。デフォルトは**untagged**です。

Lab4 Spanning Treeの設定

実習内容と目標

このラボを修了すると以下のことができるようになります：

- STP の基本的な概念を理解します
- STP の基本的な設定方法を理解します。

このタスクは、スイッチのSTPルートブリッジとエッジポートを設定して、リーダーがSTPルートブリッジとエッジポートの設定コマンドとクエリメソッドをマスターできるようにし、ポートの移行を表示してRSTP / MSTPのクイックコンバージェンス機能を理解することです。

ネットワーク図

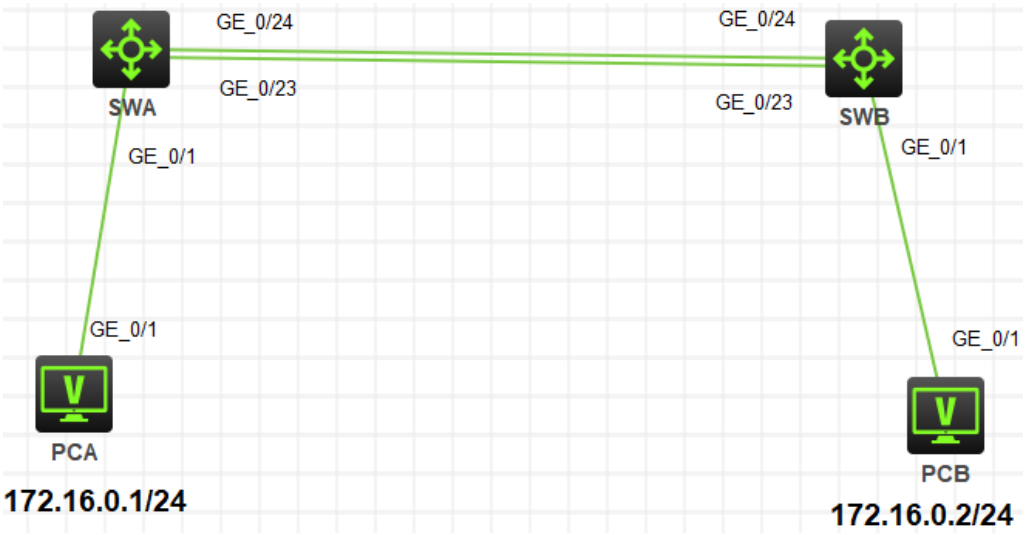


図 4.1 実習ネットワーク

現状

- スイッチ SWA、スイッチ SWB、PCA、PCB は、上の図のように配線されています。
- PCA、PCB は異なるスイッチに接続されていてそれぞれのスイッチ間は spanning tree の設定がされています。

最後に設定されたプロトコルが機能するかどうかをチェックします。

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
スイッチS5820v2	7571	2	なし
PC	Windows 7	2	なし
ネットワークケーブルの接続	--	4	なし

実習手順

手順1：ケーブルの接続

図4.1のようにスイッチ間、スイッチとPC間のケーブルを接続します。なお、この時点でスイッチをstartさせるとスイッチ間でループが発生するので、交互にstartさせてコンフィグをします。両方のコンフィグが完了したら、両方のスイッチをstartさせてください。SWA、SWB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。

<SWA>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.
<SWA>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
.....

手順2：Spanning treeの構成

リンクアグリゲーションは、静的アグリゲーションモードまたは動的アグリゲーションモードで動作します。 このラボタスクは、静的リンクアグリゲーションを検証することです。 システムビューでレイヤ2アグリゲートインターフェースを作成します。 次に、アグリゲーションインターフェースに対応するリンクアグリゲーショングループに物理ポート

を割り当てます。 このリンクアグリゲーショングループには、アグリゲーションインターフェースと同じ番号が付けられ、アグリゲーションインターフェースの作成時に自動的に作成されます。

 # SWA の設定

```
<SWA>sys
System View: return to User View with Ctrl+Z.
[SWA]stp global enable
[SWA]stp priority 0
[SWA]interface GigabitEthernet 1/0/1
[SWA-GigabitEthernet1/0/1]stp edged-port
Edge port should only be connected to terminal. It will cause temporary loops if port
GigabitEthernet1/0/1 is connected to bridges. Please use it carefully.
[SWA-GigabitEthernet1/0/1]quit
[SWA]
```

 # SWB の設定

```
<SWB>sys
System View: return to User View with Ctrl+Z.
[SWB]stp global enable
[SWB]stp priority 0
[SWB]interface GigabitEthernet 1/0/1
[SWB-GigabitEthernet1/0/1]stp edged-port
Edge port should only be connected to terminal. It will cause temporary loops if port
GigabitEthernet1/0/1 is connected to bridges. Please use it carefully.
[SWB-GigabitEthernet1/0/1]quit
[SWB]
```

手順2：Spanning treeの状態の確認

SWA と SWB の STP 情報を確認する。以下に例を示す。

```
  <SWA>dis stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID              : 32768.9c19-1eaa-0100
 Bridge times           : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC           : 4096.9c19-2e97-0200, 20
 RegRoot ID/IRPC        : 32768.9c19-1eaa-0100, 0
 RootPort ID            : 128.24
 BPDU-Protection        : Disabled
 Bridge Config-
 Digest-Snooping        : Disabled
 TC or TCN received     : 4
 Time since last TC     : 0 days 0h:0m:30s

<SWA>dis stp brief
 MST ID    Port                        Role  STP State     Protection
 0         GigabitEthernet1/0/1        DESI  FORWARDING    NONE
 0         GigabitEthernet1/0/23       ROOT  FORWARDING    NONE
 0         GigabitEthernet1/0/24       ALTE  DISCARDING    NONE
```

以上の情報によると、SWA はルートブリッジではありません。 ポート G1/0/23 はルートポートであり、転送状態です（スイッチ間でデータを転送する役割を果たします）。 ポート G/ 1/0/24 は、スタンバイルートポート(alternate)であり、ブロック状態です。 PC に接続し

ているポート G1/0/1 は、指定ポート(designate)であり、転送状態です。

```
<SWB>dis stp
-------[CIST Global Info][Mode MSTP]-------
 Bridge ID                : 4096.9c19-2e97-0200
 Bridge times             : Hello 2s MaxAge 20s FwdDelay 15s MaxHops 20
 Root ID/ERPC               : 4096.9c19-2e97-0200, 0
 RegRoot ID/IRPC          : 4096.9c19-2e97-0200, 0
 RootPort ID              : 0.0
 BPDU-Protection          : Disabled
 Bridge Config-
 Digest-Snooping          : Disabled
 TC or TCN received       : 3
 Time since last TC       : 0 days 0h:4m:19s

<SWB>dis stp brief
 MST ID     Port                                    Role    STP State     Protection
 0          GigabitEthernet1/0/1                    DESI    FORWARDING    NONE
 0          GigabitEthernet1/0/23                   DESI    FORWARDING    NONE
 0          GigabitEthernet1/0/24                   DESI    FORWARDING    NONE
```

前の情報によると、SWB はルートブリッジであり、その上のすべてのポートは指定されたポート（DESI）であり、転送状態にあります。

手順3：Spanning tree冗長機能の確認

STPは冗長リンクをブロックできます。 アクティブなリンクが切断された場合にネットワーク接続を復元するためにアクティブ化します。

装置名	IPアドレス	gateway
PCA	172.16.0.1/24	
PCB	172.16.0.2/24	

PCBでping172.16.0.1コマンドを実行して、PCBがICMPパケットをPCAに送信するようにします。

```
<PCB>ping 172.16.0.1
Ping 172.16.0.1 (172.16.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.0.1: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 172.16.0.1: icmp_seq=1 ttl=255 time=5.000 ms
56 bytes from 172.16.0.1: icmp_seq=2 ttl=255 time=5.000 ms
56 bytes from 172.16.0.1: icmp_seq=3 ttl=255 time=5.000 ms
56 bytes from 172.16.0.1: icmp_seq=4 ttl=255 time=5.000 ms
```

SWAのSTP状態を照会します。 そして、どのポート（このラボではG1/0/23）がforwarding

状態にあるかを確認します。 スイッチを接続しているforwading状態のケーブルを外し、PCBから送信されたICMPパケットが失われていないかどうかを確認します。 通常の場合、失われるパケットはないか、1つのパケットだけが失われます。

SWAでSTPポートの状態を再度照会します。 出力は次のとおりです。

<SWA>dis stp brief

MST ID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/24	ROOT	FORWARDING	NONE

前の情報に従って、元のブロックポートG1/0/24がforward状態に変更されます。
失われたパケットはありません。 収束速度が速いことを示します。 これは、STPと比較したRSTP/MSTPの改善です。 デフォルトでは、スイッチはMSTPで実行されます。 SWAの2つのポートは、1つのルートポートともう1つのスタンバイルートポートです。 アクティブなルートポートがブロックされている場合、スタンバイルートポートはすぐにforward状態に変更されます。

ノート:
PCBでping 172.16.0.1コマンドを実行します。 “request timed out”と表示された場合、PCAは応答しません。 PCAのファイアウォール機能または対応するスイッチの構成を確認してください。

手順4:ポートの状態の確認

SWポートG1 / 0/1に接続されているケーブルを外し、ケーブルを再接続します。 SWAの出力情報は以下の通りです

<SWA>%Oct 28 14:30:13:203 2021 H3C IFNET/3/PHY_UPDOWN:
Physical state on the interface GigabitEthernet1/0/1 changed to down.
%Oct 28 14:30:13:204 2021 H3C IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/1
changed to down.

<SWA>%Oct 28 14:39:39:057 2021 H3C IFNET/3/PHY_UPDOWN:
Physical state on the interface GigabitEthernet1/0/1 changed to up.
%Oct 28 14:39:39:057 2021 H3C IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/1
changed to up.

以前の情報によると、ポートは再接続された直後にforward状態に変更されます。 ポートはエッジポートとして構成されます。 そのため、遅延せず、forward状態になります。 これは、STPと比較したRSTP/MSTPのもう1つの改善点です。

ポートの移行は迅速です。 ポートの状態を明確に観察します。 PCに接続されているポートG1/0/1のエッジポート設定をキャンセルします。

手順5：SWAの設定

[SWA]interface GigabitEthernet 1/0/1

[SWA-GigabitEthernet1/0/1]undo stp edged-port

[SWA-GigabitEthernet1/0/1]quit

SWBポートG1/0/1に接続されているケーブルを外し、ケーブルを再接続します。 SWBでポートの状態を表示します。 数秒間隔でコマンドを実行して、ポートの移行状態を表示します。 出力情報は次のとおりです。

<SWB>dis stp brief

MST ID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	DISCARDING	NONE
0	GigabitEthernet1/0/24	DESI	FORWARDING	NONE

<SWB>dis stp brief

MST ID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	LEARNING	NONE
0	GigabitEthernet1/0/24	DESI	FORWARDING	NONE

<SWB>dis stp brief

MST ID	Port	Role	STP State	Protection
0	GigabitEthernet1/0/1	DESI	FORWARDING	NONE
0	GigabitEthernet1/0/24	DESI	FORWARDING	NONE

ポートの状態は次の順序で変更されます。 Discarding < learning < forwarding。 以前の情報によるとエッジポートの設定がキャンセルされた後、STPコンバージェンス速度が低下します。

質問:

ラボではSWBはデータを転送するルートポートをG1/0/23に選びました。ルートポートをG1/0/24に変更することができますか？

答え：

はい。デフォルトのポートのコストは200(100Mポートのデフォルト値)です。ポートG1/ 0/24からSWAへのSWBオーバーヘッドが、ポートG1 / 0/23からSWAへのオーバーヘッドよりも少なくなるように、ポートG1/0/24のコスト値を100に変更します。 設定後、スイッチはデ

ータ転送用のルートポートとしてポートG1/0/24を選択します。

Lab5 Port Securityの設定

実習内容と目標

このラボを修了すると以下のことができるようになります：

- Port isolation の基本機能を習得します。

注意：この機能はハードウェアで実現するためにHCLでは動作しませんので、設定の確認のみとなります。

ネットワーク図

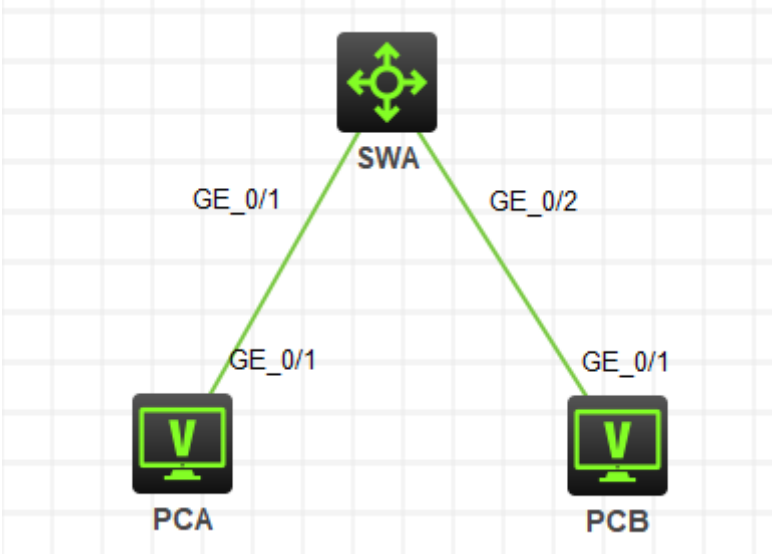


図 5.1 実習ネットワーク

現状

- スイッチ SWA、、PCA、PCB 上の図のように配線されています。

最後に設定されたプロトコルが機能するかどうかをチェックします。

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
スイッチS5820v2	7571	1	なし
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

ポートアイソレーションのコンフィギュレーション

このタスクは、スイッチのポート分離を構成して、2台のPCの通信をブロックし、PCがアップリンクポートを介してもう一方のPCにアクセスできるようにすることです。 テストの後、ポート分離の基本原理と構成を理解します。

手順1：ケーブルの接続

図5.1のようにスイッチ間、スイッチとPC間のケーブルを接続します。

SWA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。

```
<SWA>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.
<SWA>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
.....
```

手順2：port isolation実施前の確認

両方のPCにIPアドレスをアサインします。

PCAのIPアドレスを172.16.0.1/24

PCBのIPアドレスを172.16.0.2/24

ポートアイソレーションの機能を確認する前に、PC間の疎通を確認します。PCAはPCBへpingすることができます。その出力は以下の通りです。

```
<PCA>ping 172.16.0.2
Ping 172.16.0.2 (172.16.0.2): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.0.2: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 172.16.0.2: icmp_seq=1 ttl=255 time=4.000 ms
56 bytes from 172.16.0.2: icmp_seq=2 ttl=255 time=4.000 ms
```

56 bytes from 172.16.0.2: icmp_seq=3 ttl=255 time=4.000 ms
56 bytes from 172.16.0.2: icmp_seq=4 ttl=255 time=4.000 ms

手順3：port isolationのコンフィグレーション

SWAでポート分離を有効にします。ポートGigabitEthernet 1/0/1とGigabitEthernet 1/0/2を分離グループに追加し、ポートGigabitEthernet 1/0/24を分離グループのアップリンクポートとして構成します。

SWAをコンフィギュレーションします。

```
[SWA]port-isolate group 1
[SWA]interface GigabitEthernet 1/0/1
[SWA-GigabitEthernet1/0/1]port-isolate enable group 1
[SWA-GigabitEthernet1/0/1]quit
[SWA]interface GigabitEthernet 1/0/2
[SWA-GigabitEthernet1/0/2]port-isolate enable group 1
[SWA-GigabitEthernet1/0/2]quit
```

アイソレーショングループの情報を表示するために以下のコマンドを実行します。

```
[SWA]display port-isolate group 1
 Port isolation group information:
 Group ID: 1
 Group members:
     GigabitEthernet1/0/1              GigabitEthernet1/0/2
```

手順4：port isolation実施後の確認

注意：HCLではハードウェア機能は利用できませんので、以下の結果は変わります（ping出来てしまいます）。

ポートアイソレーションの機能を設定した後に、PC間の疎通を確認します。PCAはPCBへpingすることができません。その出力は以下の通りです。

```
<PCA>ping 172.16.0.2
Ping 172.16.0.2 (172.16.0.2): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
```

Lab6 Link aggregationの設定

実習内容と目標

このラボタスクでは、スイッチとユーザー表示コマンドで静的リンクアグリゲーションを構成して構成を確認する方法を示します。 さらに、ラボタスクで作成されたリンクアグリゲーショングループ内のリンクが切断され、リンクアグリゲーションがどのように機能してリンクの信頼性が確保されるかがテストされます。

ネットワーク図

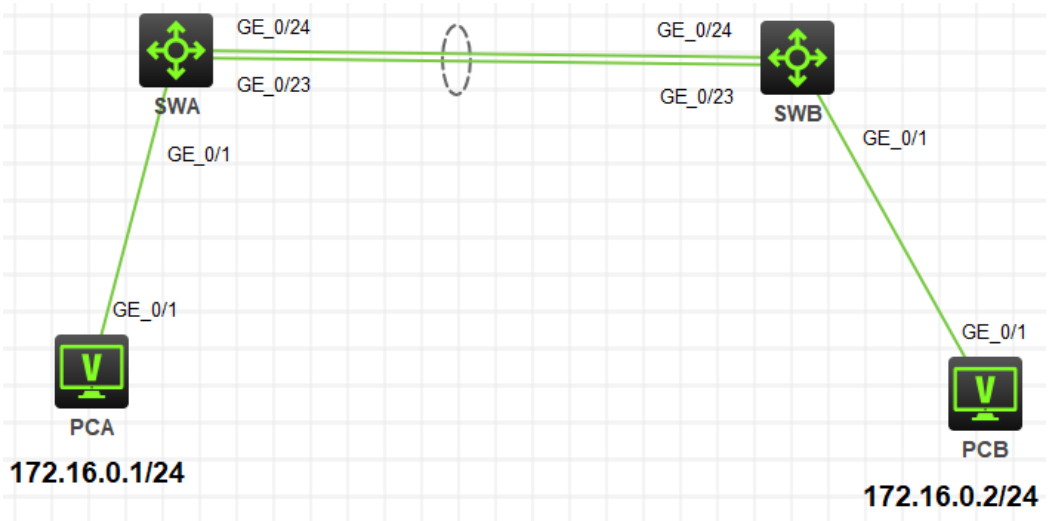


図 6.1 実習ネットワーク

現状

- スイッチ SWA、スイッチ SWB、PCA、PCB は、上の図のように配線されています。
- PCA、PCB は異なるスイッチに接続されていてそれぞれのスイッチ間は link aggregation で接続されています。

最後に設定されたプロトコルが機能するかどうかをチェックします。

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
スイッチS5820v2	7571	2	なし

PC	Windows 7	2	なし
ネットワークケーブルの接続	--	4	なし

実習手順

手順1：ケーブルの接続

図6.1のようにスイッチ間、スイッチとPC間のケーブルを接続します。なお、この時点でスイッチをstartさせるとスイッチ間でループが発生するので、交互にstartさせてコンフィグをします。両方のコンフィグが完了したら、両方のスイッチをstartさせてください。SWA、SWB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。

<SWA>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.
<SWA>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
.....

手順2：Static link aggregationの構成

リンクアグリゲーションは、静的アグリゲーションモードまたは動的アグリゲーションモードで動作します。 このラボタスクは、静的リンクアグリゲーションを検証することです。 システムビューでレイヤ2アグリゲートインターフェースを作成します。 次に、アグリゲーションインターフェースに対応するリンクアグリゲーショングループに物理ポートを割り当てます。 このリンクアグリゲーショングループには、アグリゲーションインターフェースと同じ番号が付けられ、アグリゲーションインターフェースの作成時に自動的に作成されます。

SWA の設定
<SWA>sys
System View: return to User View with Ctrl+Z.
[SWA]interface Bridge-Aggregation 1

```
[SWA-Bridge-Aggregation1]quit
[SWA]int GigabitEthernet 1/0/23
[SWA-GigabitEthernet1/0/23]port link-aggregation group 1
[SWA-GigabitEthernet1/0/23]quit
[SWA]interface GigabitEthernet 1/0/24
[SWA-GigabitEthernet1/0/24]port link-aggregation group 1
[SWA-GigabitEthernet1/0/24]quit
```

SWB の設定

```
<SWB>sys
System View: return to User View with Ctrl+Z.
[SWB]interface Bridge-Aggregation 1
[SWB-Bridge-Aggregation1]quit
[SWB]int GigabitEthernet 1/0/23
[SWB-GigabitEthernet1/0/23]port link-aggregation group 1
[SWB-GigabitEthernet1/0/23]quit
[SWB]interface GigabitEthernet 1/0/24
[SWB-GigabitEthernet1/0/24]port link-aggregation group 1
[SWB-GigabitEthernet1/0/24]quit
```

手順 3:コンフィグレーションの確認

SWA と SWB のそれぞれで link-aggregation group 情報を表示します。

```
<SWA>display link-aggregation summary
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, BLAGG -- Blade-Aggregation, RAGG -- Route-
Aggregation, SCH-B -- Schannel-Bundle
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 441a-fac6-9f5e

AGG          AGG     Partner ID      Selected  Unselected  Individual  Share
Interface    Mode                    Ports     Ports       Ports       Type
--------------------------------------------------------------------------------
BAGG1        S       None            0         2           0           Shar
```

```
<SWB>display link-aggregation summary
Aggregation Interface Type:
BAGG -- Bridge-Aggregation, BLAGG -- Blade-Aggregation, RAGG -- Route-
Aggregation, SCH-B -- Schannel-Bundle
Aggregation Mode: S -- Static, D -- Dynamic
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor System ID: 0x8000, 441a-fac6-9f5e

AGG          AGG     Partner ID      Selected  Unselected  Individual  Share
Interface    Mode                    Ports     Ports       Ports       Type
--------------------------------------------------------------------------------
BAGG1        S       None            0         2           0           Shar
```

手順4：リンクアグリゲーションの機能確認

両方のPCにIPアドレスをアサインします。

PCAのIPアドレスを172.16.0.124

PCBのIPアドレスを172.16.0.2/24

PCBからPCAへpingします。

<H3C>ping 172.16.0.2

Ping 172.16.0.2 (172.16.0.2): 56 data bytes, press CTRL_C to break

56 bytes from 172.16.0.2: icmp_seq=0 ttl=255 time=3.000 ms

56 bytes from 172.16.0.2: icmp_seq=1 ttl=255 time=5.000 ms

56 bytes from 172.16.0.2: icmp_seq=2 ttl=255 time=5.000 ms

SWAのGE0/23とSWBのGE0/23間のケーブルを外します。

そして、再び上記のpingを実行してpingが成功することを確認してください。

質問:

1．1つのスイッチに複数のリンクアグリゲーショングループを作ることができますか？

2．1つのポートが複数のリンクアグリゲーショングループに属することができますか？

答え：

1．アグリゲーションインターフェースを作成することにより、複数のリンクアグリゲーショングループを作成することができます。

2．1つのポートはただ1つのリンクアグリゲーショングループにしか属することができません。

Lab7 ARP

実習内容と目標

このラボでは以下のことを学びます：

- ARP の操作。
- ARP Proxy の操作とコンフィギュレーション。

ネットワーク図

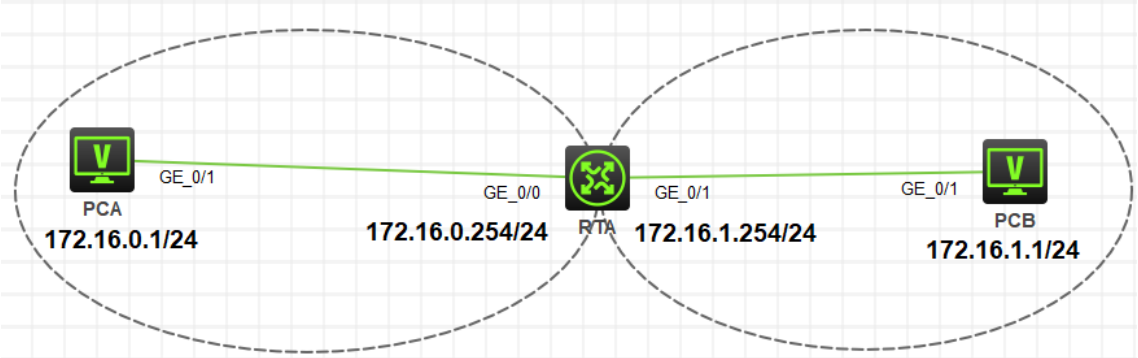


図 7.1 実習ネットワーク

現状

- ルーターRTA、PCA、PCB は、上の図のように配線されています。

最後に設定されたプロトコルが機能するかどうかをチェックします。

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	1	なし
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：ARPエントリーの表示

このタスクはどのようにARPエントリーが作成されるかを示しています。

手順1：PCAとRTAをケーブルで接続する

図7.1のようにルーターとPC間のケーブルを接続します。

RTA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。

```
<H3C>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.
<H3C>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
.....
```

手順2：PCAとRTAにIPアドレスをアサインする

それぞれの装置にIPアドレスをアサインします。

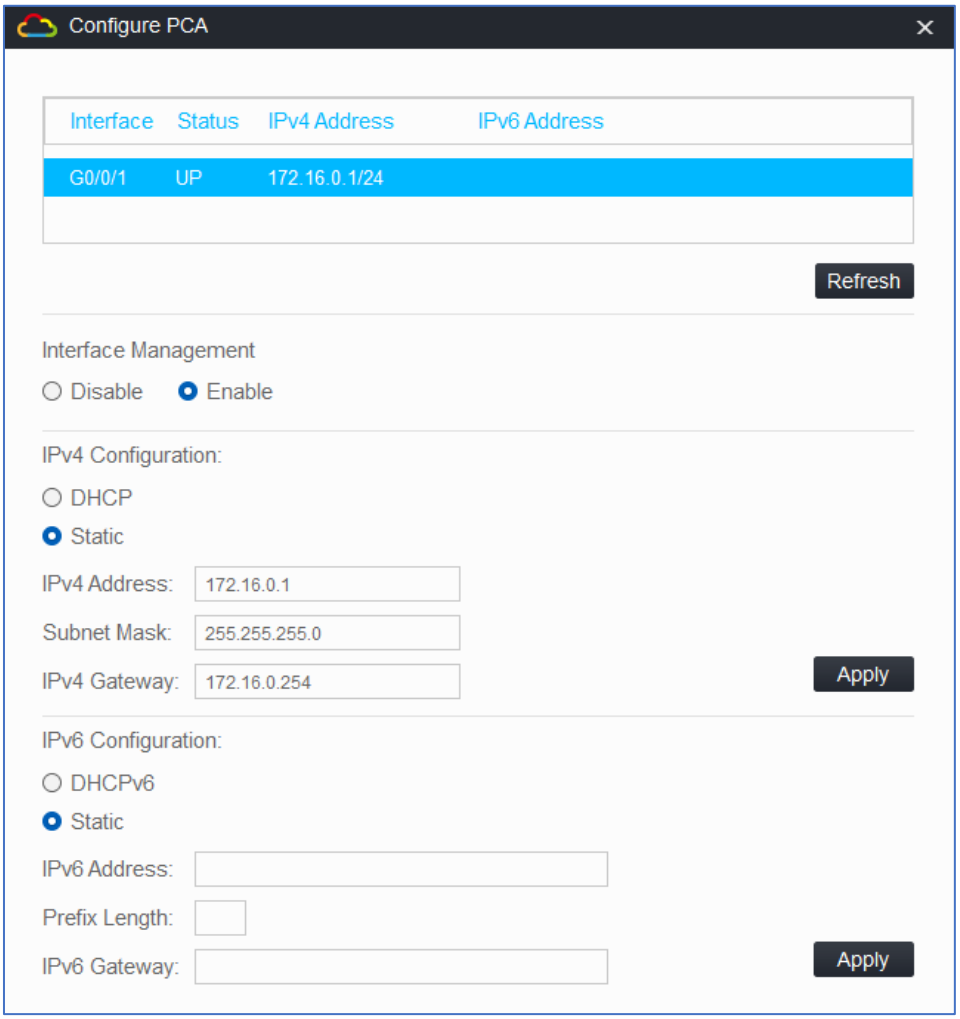
PCAのIPアドレスを172.16.0.1/24

PCBのIPアドレスを172.16.1.1/24

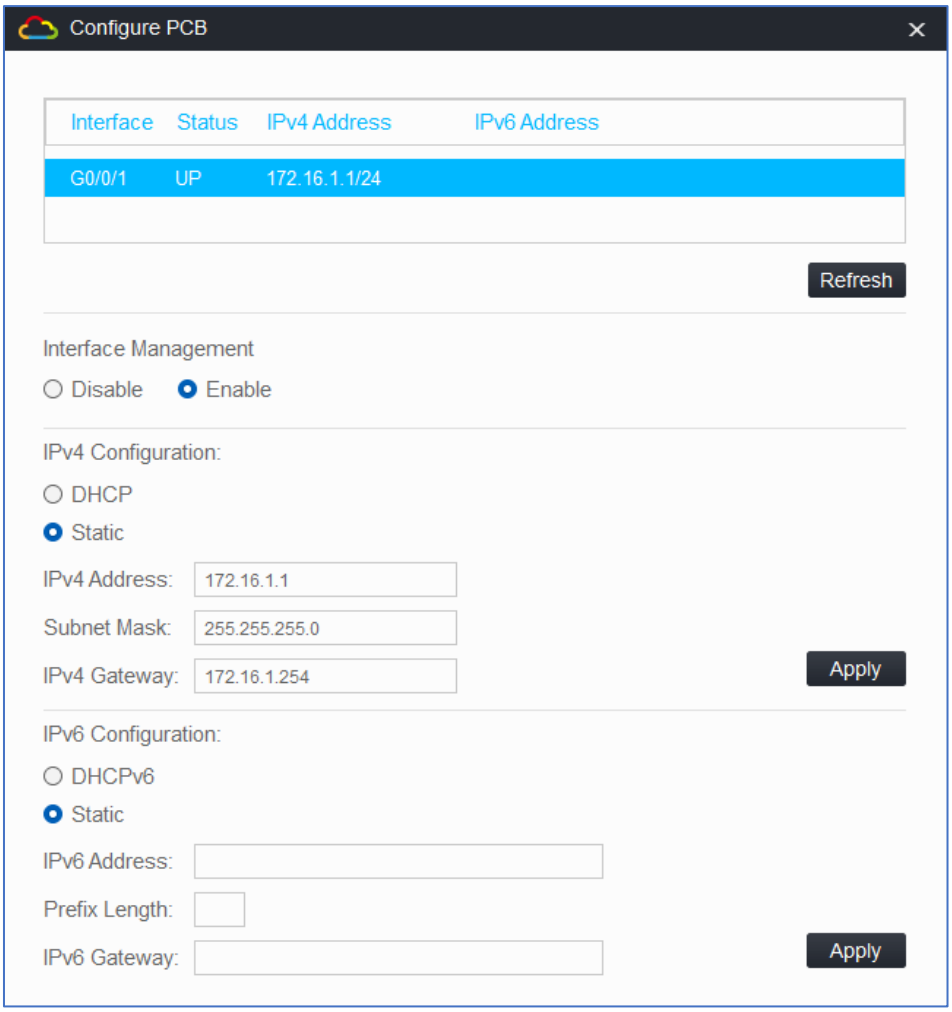
RTAのGigabitEthernet 0/0のIPアドレスを172.16.0.254/24

RTAのGigabitEthernet 0/1のIPアドレスを172.16.1.254/24

PCA の IP アドレスの設定


Configure PCA
Interface
Status
IPv4 Address
IPv6 Address
G0/0/1
UP
172.16.0.1/24
Refresh
Interface Management
Disable
Enable
IPv4 Configuration:
DHCP
Static
IPv4 Address:
172.16.0.1
Subnet Mask:
255.255.255.0
IPv4 Gateway:
172.16.0.254
Apply
IPv6 Configuration:
DHCPv6
Static
IPv6 Address:
Prefix Length:
IPv6 Gateway:
Apply

PCB の IP アドレスの設定



手順3：ARPエントリーを表示する

RTA、PCAとPCBのそれぞれのIPアドレスとMACアドレスを表示します。

RTAのインターフェースのIPアドレスとMACアドレスです。

<RTA>display interface GigabitEthernet 0/0

GigabitEthernet0/0

Current state: UP

Line protocol state: UP

Description: GigabitEthernet0/0 Interface

Bandwidth: 1000000 kbps

Maximum transmission unit: 1500

Allow jumbo frames to pass

Broadcast max-ratio: 100%

Multicast max-ratio: 100%

Unicast max-ratio: 100%

Internet address: 172.16.0.254/24 (primary)

IP packet frame type: Ethernet II, hardware address: **4681-b4cd-0105**

….

….

<RTA>display interface GigabitEthernet 0/1

GigabitEthernet0/1

Current state: UP

Line protocol state: UP

Description: GigabitEthernet0/1 Interface

Bandwidth: 1000000 kbps

Maximum transmission unit: 1500

Allow jumbo frames to pass

Broadcast max-ratio: 100%

Multicast max-ratio: 100%

Unicast max-ratio: 100%

Internet address: 172.16.1.254/24 (primary)

IP packet frame type: Ethernet II, hardware address: **4681-b4cd-0106**

….

….

PCAのIPアドレスとMACアドレス:

C:¥Users¥admin>ipconfig/all

イーサネット アダプター イーサネット 1:

接続固有の DNS サフィックス . . . . .:

説明. . . . . .: Realtek USB GbE Family Controller #1

物理アドレス. . . . . .: **A4-5D-36-59-26-4F**

DHCP 有効 . . . . . .: はい

自動構成有効. . . . . .: はい

リンクローカル IPv6 アドレス. . . . .: fe80::dc0d:609c:17d1:19ee%5(優先)

IPv4 アドレス . . . . . .: 172.16.0.1(優先)

サブネット マスク . . . . . .: 255.255.255.0

リース取得. . . . . .: 2021年11月2日 14:50:40

リースの有効期限. . . . . .: 2021年11月3日 14:50:40

PCBのIPアドレスとMACアドレス:

C:¥Users¥admin>ipconfig/all

イーサネット アダプター イーサネット 1:

接続固有の DNS サフィックス . . . . .:

説明. . . . . .: Realtek USB GbE Family Controller #1

物理アドレス. . . . . .: **44-37-E6-AB-7D-F0**

DHCP 有効 . . . . . .: はい

自動構成有効. . . . . .: はい

リンクローカル IPv6 アドレス. . . . .: fe80::dc0d:609c:17d1:19ee%5(優先)

IPv4 アドレス . . . . . .: 172.16.0.1(優先)

サブネット マスク . . . . . .: 255.255.255.0

リース取得. . . . . .: 2021年11月2日 14:50:40

リースの有効期限. . . . . .: 2021年11月3日 14:50:40

RTAと両方のPCが到達可能かpingコマンドにより確認します。その結果、RTAと両方のARPエントリーが作成されます。

PCAのping操作の結果は:

[PCA]ping 172.16.0.254

Ping 172.16.0.254 (172.16.0.254): 56 data bytes, press CTRL_C to break

56 bytes from 172.16.0.254: icmp_seq=0 ttl=255 time=1.000 ms

56 bytes from 172.16.0.254: icmp_seq=1 ttl=255 time=1.000 ms

56 bytes from 172.16.0.254: icmp_seq=2 ttl=255 time=2.000 ms

56 bytes from 172.16.0.254: icmp_seq=3 ttl=255 time=1.000 ms

56 bytes from 172.16.0.254: icmp_seq=4 ttl=255 time=2.000 ms

PCBのping操作の結果は:

<PCB>ping 172.16.1.254

Ping 172.16.1.254 (172.16.1.254): 56 data bytes, press CTRL_C to break

56 bytes from 172.16.1.254: icmp_seq=0 ttl=255 time=1.000 ms

56 bytes from 172.16.1.254: icmp_seq=1 ttl=255 time=1.000 ms

56 bytes from 172.16.1.254: icmp_seq=2 ttl=255 time=3.000 ms

56 bytes from 172.16.1.254: icmp_seq=3 ttl=255 time=2.000 ms

56 bytes from 172.16.1.254: icmp_seq=4 ttl=255 time=2.000 ms

PCA, PCB, RTAのARPエントリーをそれぞれ表示します。

PCAのARPエントリーは：

C:¥Users¥admin>arp -a

インターフェース: 172.16.0.1 --- 0x5

インターネット アドレス	物理アドレス	種類
172.16.0.254	**46-81-b4-cd-01-05**	動的

PCBのARPエントリーは：

C:¥Users¥admin>arp -a

インターフェース: 172.16.1.1 --- 0x5

インターネット アドレス	物理アドレス	種類
172.16.1.254	**46-81-b4-cd-0106**	動的

RTAのARPエントリーは：

<RTA>display arp all

Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid

IP address	MAC address	SVLAN/VSI Interface/Link ID	Aging	Type
172.16.0.1	**a45d-3659-264f** --	GE0/0	15	D
172.16.1.1	**4437-e6ab-7df0** --	GE0/1	17	D

ARPエントリーを比較すると両PCとRTAのARPエントリーが同じであることが分かります。

タスク2：ARP Proxyのコンフィグレーション

このタスクはどのようにARP proxyを設定するかを示しています。

手順1：PCAとRTAをケーブルで接続する

RTA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。

<H3C>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.

<H3C>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

.....

手順2：PCAとPCBのIPアドレスを変更する

図7.2のようにPCのIPアドレスのサブネットマスクを16ビット(172.16.0.0/16)に変更します。その結果、両PCは同じセグメントに存在することになります。しかし、両PCと接続されているRTAのインターフェースのアドレスは24ビット(172.16.0.0/24と172.16.1.0/24)のままですので、両PC間はコミュニケーションができません。

ネットワーク図

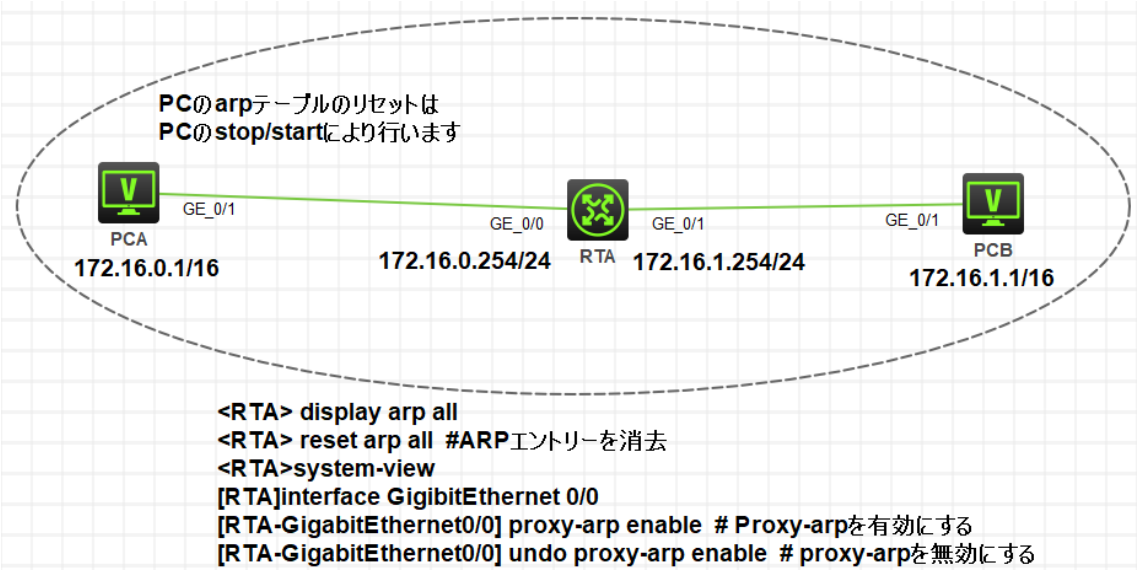
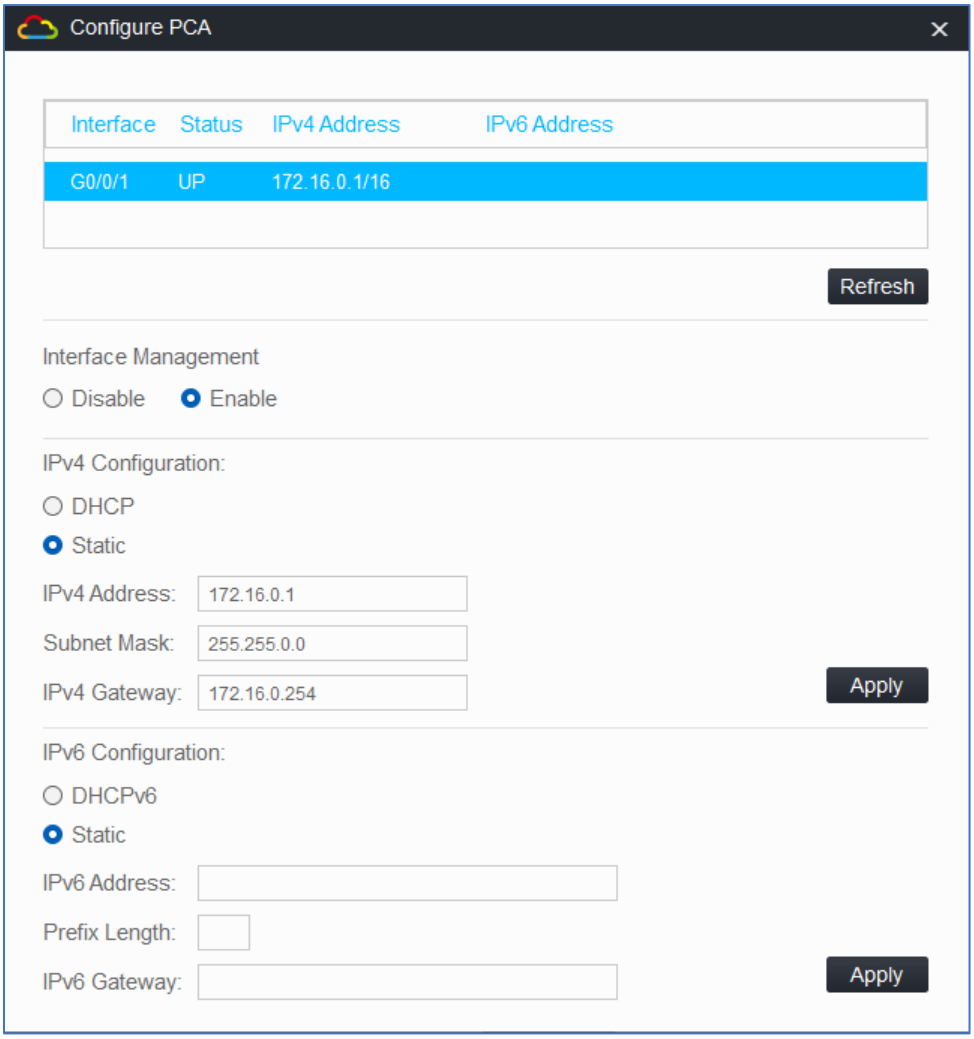
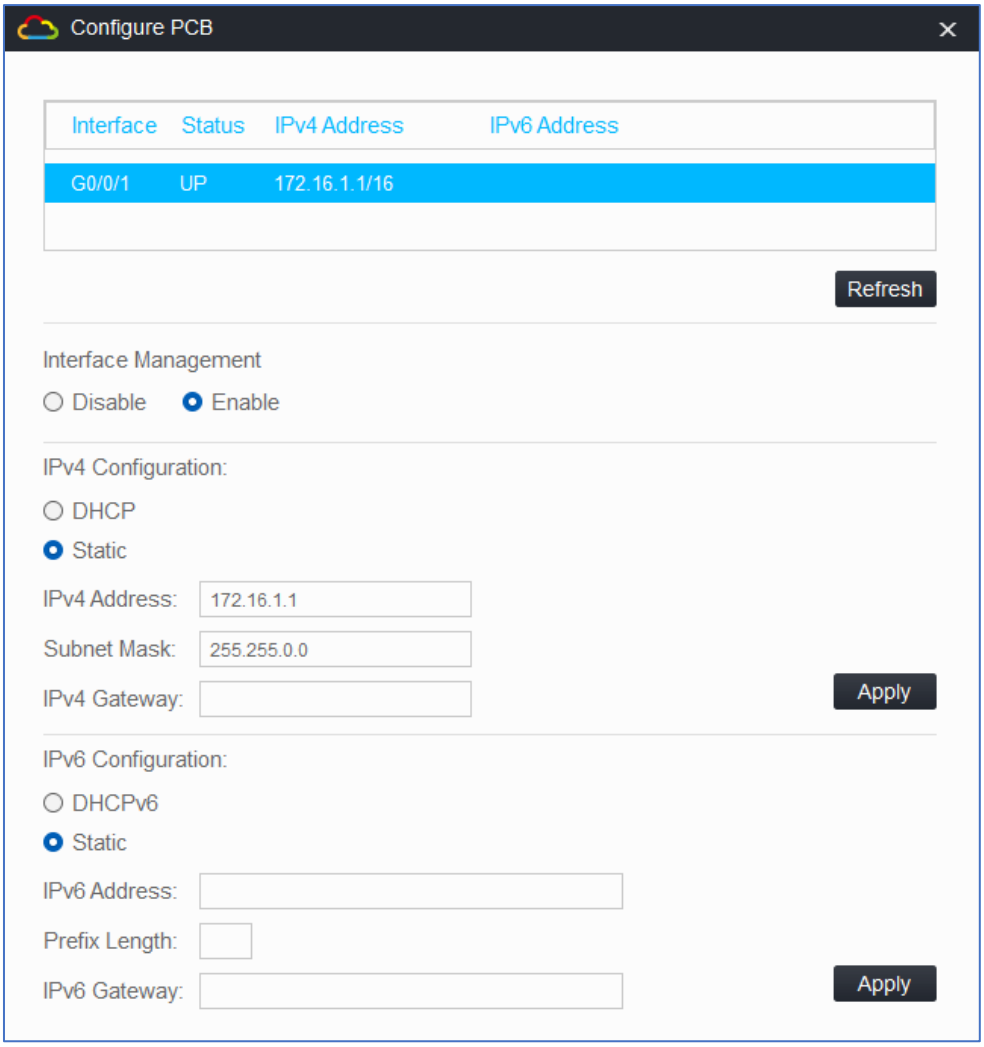


図 7.2 実習ネットワーク

PCA の IP アドレスの設定



PCB の IP アドレスの設定



RTAのIPアドレスとサブネットマスクの設定

<RTA>system-view

[RTA]interface GigabitEthernet 0/0

[RTA -GigabitEthernet0/0]ip address 172.16.0.254 24

[RTA -GigabitEthernet0/0]quit

[RTA]interface GigabitEthernet 0/1

[RTA -GigabitEthernet0/1]ip address 172.16.1.254 24

[RTA -GigabitEthernet0/1]quit

[RTA]display interface brief

Brief information on interfaces in route mode:

Link: ADM - administratively down; Stby - standby

Protocol: (s) - spoofing

Interface	Link	Protocol	Primary IP	Description
GE0/0	UP	UP	172.16.0.254	
GE0/1	UP	UP	172.16.1.254	

手順3：ARP proxyの設定をする

RTAにARP proxyの設定をする前に、両PC間のコミュニケーションができないことを確認します。

PCAからRTAのGigabitEthernet 0/0へのコミュニケーションはできます。

```
<PCA>ping 172.16.0.254
Ping 172.16.0.254 (172.16.0.254): 56 data bytes, press CTRL_C to break
56 bytes from 172.16.0.254: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 172.16.0.254: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 172.16.0.254: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 172.16.0.254: icmp_seq=3 ttl=255 time=3.000 ms
56 bytes from 172.16.0.254: icmp_seq=4 ttl=255 time=2.000 ms
```

PCAからRTAのGigabitEthernet 0/1へのコミュニケーションはサブネットが異なるのでコミュニケーションができません。

```
<PCA>ping 172.16.1.254
Ping 172.16.1.254 (172.16.1.254): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
```

当然、PCAからPCBへのpingはできません。

```
<PCA>ping 172.16.1.1
Ping 172.16.1.1 (172.16.1.1): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
```

PCAとPCBは同じサブネット上にありますが、異なるサブネットに属するインターフェースに接続されているため、相互にアクセスすることはできません。 ただし、ARPプロキシが設定されている場合、ルーターはPCAからのARP要求にルーター自体のMACアドレスで応答します。 次に、PCAはPCBの将来のパケットをルーターに送信し、ルーターはLayter2スイッチと同様にパケットをPCBに転送します。

RTAにARP proxyの設定をします。

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]proxy-arp enable

[RTA-GigabitEthernet0/0]quit

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]proxy-arp enable

[RTA-GigabitEthernet0/1]quit

PCAからPCBへpingします。

<PCA>ping 172.16.1.1

Ping 172.16.1.1 (172.16.1.1): 56 data bytes, press CTRL_C to break

56 bytes from 172.16.1.1: icmp_seq=0 ttl=254 time=3.000 ms

56 bytes from 172.16.1.1: icmp_seq=1 ttl=254 time=4.000 ms

56 bytes from 172.16.1.1: icmp_seq=2 ttl=254 time=4.000 ms

56 bytes from 172.16.1.1: icmp_seq=3 ttl=254 time=4.000 ms

手順4：ARPエントリーを表示する

RTA上のARPエントリーを表示する

[RTA]display arp all

Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid

IP address	MAC address	SVLAN/VSI Interface/Link ID	Aging	Type
172.16.0.1	**a45d-3659-264f** --	GE0/0	18	D
172.16.1.1	**4437-e6ab-7df0** --	GE0/1	18	D

質問:

上のRTAのARPエントリーの表示で18と表示されている”Aging”とは何ですか？

答え：

それぞれのIPアドレスのエージング時間が18秒であることを表しています。したがって、RTAがそれぞれのPCのIPアドレスに対応して学習したMACアドレスは18秒後には削除されます。

Lab8 DHCP

実習内容と目標

このラボでは以下のことを学びます：

- DHCP の操作。
- DHCP サーバーのコンフィギュレーション。
- DHCP relay agent のコンフィギュレーション。

ネットワーク図

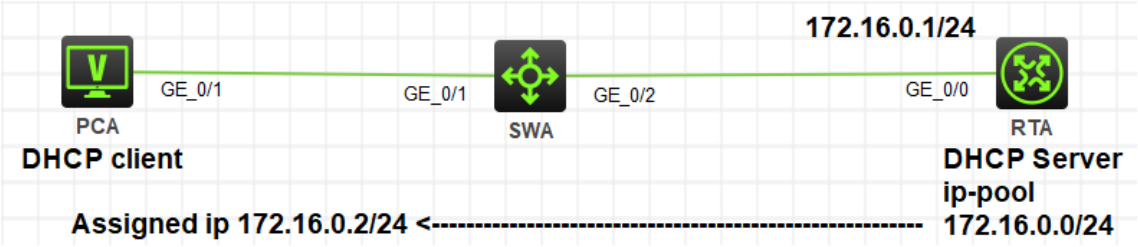


図 8.1 実習ネットワーク

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	1	なし
S5820V2	Version7.1	1	なし
PC	Windows 7	1	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：PCAがRTAのDHCPサーバー機能によりIPアドレスを取得する

このタスクでは、ルーターでDHCPサーバーを構成する方法と、DHCPクライアントが同じサブネット上のDHCPサーバーからIPアドレス、ゲートウェイアドレス、およびその他の構成情報を取得する方法を示します。

手順1：PCAとRTAをケーブルで接続する

図8.1のようにルーターとPC間のケーブルを接続します。

SWA、RTA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。

```
<H3C>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.
<H3C>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
.....
```

手順2：RTAのGigabitEthernet 0/0にIPアドレス172.16.0.1/24をアサインする

```
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ip address 172.16.0.1 24
[RTA-GigabitEthernet0/0]quit
```

手順3：RTAにDHCPサーバーのコンフィギュレーションをする

```
[RTA]dhcp enable
[RTA]dhcp server forbidden-ip 172.16.0.1
[RTA]dhcp server ip-pool 1
[RTA-dhcp-pool-1]network 172.16.0.0 mask 255.255.255.0
[RTA-dhcp-pool-1]gateway-list 172.16.0.1
[RTA-dhcp-pool-1]quit
```

RTAにコンフィグレーションしたDHCPアドレスプールの情報を表示する

```
[RTA]display dhcp server pool
Pool name: 1
  Network: 172.16.0.0 mask 255.255.255.0
  expired day 1 hour 0 minute 0 second 0
  reserve expired-ip enable
```

reserve expired-ip mode client-id time 4294967295 limit 256000
gateway-list 172.16.0.1

手順4：PCAのNICにDHCPサーバーからIPアドレスを取得するように設定する

コントロールパネルでネットワーク接続を開きます。 ローカルエリア接続を選択し、右クリックメニューからプロパティを選択します。 ポップアップダイアログボックスで、インターネットプロトコル（TCP / IP）を選択し、プロパティをクリックします。 図8-2のようにダイアログボックスが表示されます。

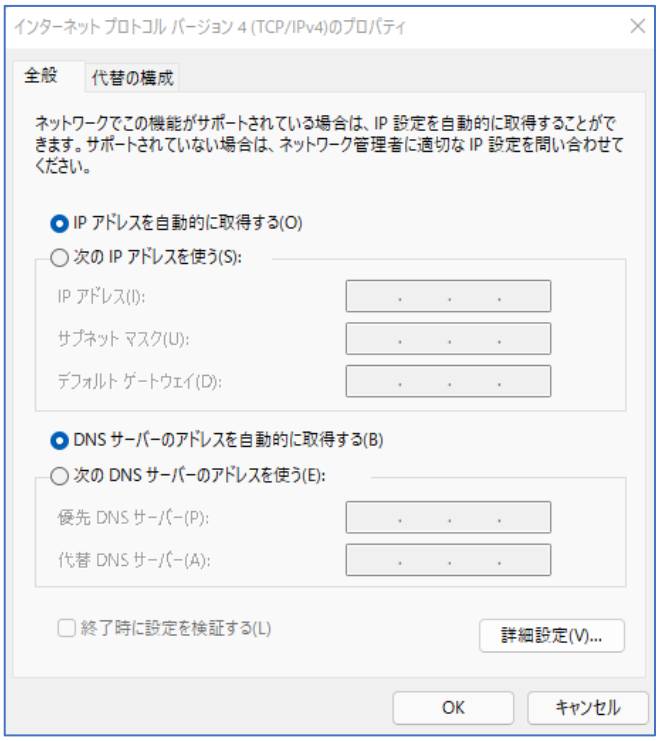


図 8.2 Windows PC の Internet protocol(TCP/IP)プロパティ

HCLでは以下のようにDHCPを選択します。

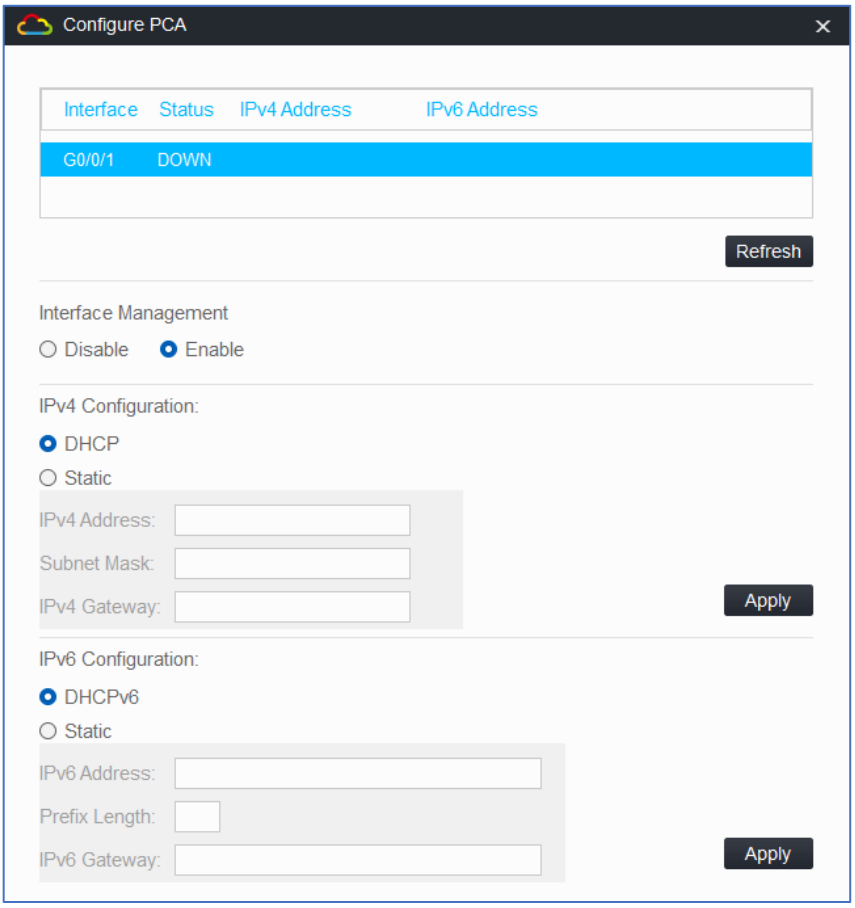


図 8.3 HCL の場合

PCAが取得したIPアドレス、マスク、ゲートウェイアドレスを確認するにはコマンドプロンプトでipconfigコマンドを入力します。

C:¥Users¥admin>ipconfig

Windows IP 構成

イーサネット アダプター イーサネット 1:

接続固有の DNS サフィックス . . . . .:

リンクローカル IPv6 アドレス. . . . .: fe80::dc0d:609c:17d1:19ee%5

IPv4 アドレス . . . . . .: 172.16.0.2

サブネット マスク . . . . . .: 255.255.255.0

デフォルト ゲートウェイ . . . . . .: 172.16.0.1

もし、PCAがIPアドレスの取得に失敗したら、ケーブルの接続を確認し、さらにコマンドプロンプトでipconfig/renewコマンドを入力します。

HCLの場合、configureのパネルの一番上に現在のIPアドレスが表示されますのでそこで確認します。

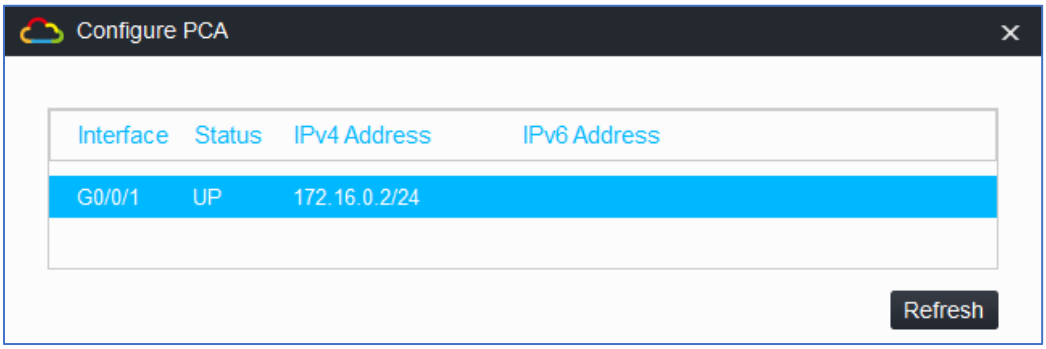


図 8.4 DHCP サーバーから割り当てられた IP アドレス

手順5：RTAのDHCPサーバーの状態を確認する

RTA上のDHCPサーバーの統計情報を表示します。

```
<RTA>display dhcp server statistics
    Pool number:                    1
    Pool utilization:               0.78%
    Bindings:
      Automatic:                    1
      Manual:                       0
      Expired:                      1
    Conflict:                       0
    Messages received:              143
      DHCPDISCOVER:                 48
      DHCPREQUEST:                  48
      DHCPDECLINE:                  0
      DHCPRELEASE:                  47
      DHCPINFORM:                   0
      BOOTPREQUEST:                 0
    Messages sent:                          96
      DHCPOFFER:                    48
      DHCPACK:                      48
      DHCPNAK:                      0
      BOOTPREPLY:                   0
    Bad Messages:                   0
```

この出力はルーターのアドレスプールの統計情報を表しています。

DHCPクライアントへ割り当てられているIPアドレスを確認するのは以下のコマンドで確認できます。

```
<RTA>display dhcp server ip-in-use
```

IP address　　Client identifier/　　Lease expiration　　Type
　　Hardware address
172.16.0.2　　0031-3836-632e-6430-　Nov　5 13:02:42 2021　Auto(C)

この結果、PCAには172.16.0.2が割り当てられていることが分かります。

DHCPサーバーが割り当て可能なIPアドレスは以下のコマンドで確認できます。

<RTA>display dhcp server free-ip

Pool name: 1

　Network: 172.16.0.0 mask 255.255.255.0

　　IP ranges from 172.16.0.3 to 172.16.0.254

出力は、IPアドレス172.16.0.2、172.16.0.1、および172.16.0.0が割り当て可能ではないことを示しています。 172.16.0.1は割り当てることができず、172.16.0.2がPCAに割り当てられており、172.16.0.0がネットワークアドレスです。

タスク2：PCAがRTAからDHCP relayによりIPアドレスを取得する

このラボタスクでは、SWAでDHCPリレーエージェントを構成する方法と、DHCPクライアントがリレーエージェントを介して別のサブネット上のDHCPサーバーからIPアドレス、ゲートウェイアドレス、およびその他の構成情報を取得する方法を示します。

ネットワーク図

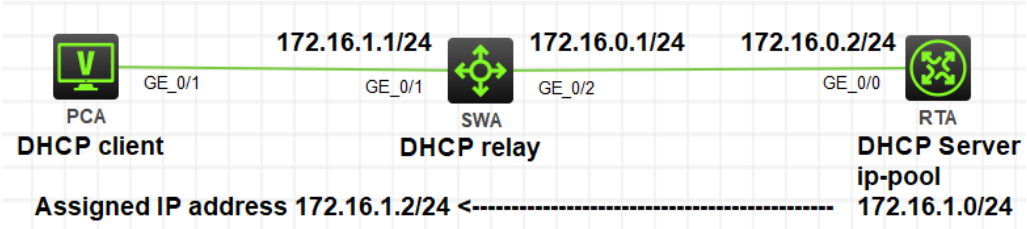


図 8.5 実習ネットワーク

手順1：PCAとRTAをケーブルで接続する

図8.1のようにルーターとPC間のケーブルを接続します。

SWA、RTA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。

<H3C>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.

<H3C>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

.....

手順2：SWAとRTAのIPアドレスを設定する

表8-1 SWAとRTAに割り当てるIPアドレススキーム

装置名	物理インターフェース	IPアドレス	VLANインターフェース
SWA	G1/0/1	172.16.1.1/24	VLAN-interface 1
	G1/0/2	172.16.0.1/24	VLAN-interface 2
RTA	G0/0	172.16.0.2/24	

表8-1のようにSWAとRTAにIPアドレスを割り当てます。

[SWA]vlan 2

[SWA-vlan2]quit

[SWA]interface GigabitEthernet 1/0/2

[SWA-GigabitEthernet1/0/2]port access vlan 2

[SWA-GigabitEthernet1/0/2]quit

[SWA]interface Vlan-interface 1

%Nov　4 15:41:15:621 2021 SWA IFNET/3/PHY_UPDOWN: Physical state on the interface Vlan-interface1 changed to up.

%Nov　4 15:41:15:621 2021 SWA IFNET/5/LINK_UPDOWN: Line protocol state on the interface Vlan-interface1 changed to up.

ip address 172.16.1.1 24

[SWA-Vlan-interface1]quit

[SWA]interface Vlan-interface 2

%Nov　4 15:41:57:485 2021 SWA IFNET/3/PHY_UPDOWN: Physical state on the interface Vlan-interface2 changed to up.

%Nov　4 15:41:57:485 2021 SWA IFNET/5/LINK_UPDOWN: Line protocol state on the interface Vlan-interface2 changed to up.

[SWA-Vlan-interface2]ip address 172.16.0.1 24

[SWA-Vlan-interface2]quit

SWAでVLAN, interface, IPアドレスが正しく割り当てられているか確認します。

```
[SWA]display ip interface brief
*down: administratively down
(s): spoofing    (l): loopback
Interface                   Physical Protocol IP Address          Description
MGE0/0/0                      down       down       --                    --
Vlan1                         up         up         172.16.1.1          --
Vlan2                         up         up         172.16.0.1          --

[SWA]display vlan all
 VLAN ID: 1
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 172.16.1.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0001
 Name: VLAN 0001
 Tagged ports:     None
 Untagged ports:
     GigabitEthernet1/0/1    ...
     ...........................

 VLAN ID: 2
 VLAN type: Static
 Route interface: Configured
 IPv4 address: 172.16.0.1
 IPv4 subnet mask: 255.255.255.0
 Description: VLAN 0002
 Name: VLAN 0002
 Tagged ports:     None
 Untagged ports:
     GigabitEthernet1/0/2
```

RTAでIPアドレスとStatic routeを設定します。

```
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ip address 172.16.0.2 24
[RTA-GigabitEthernet0/0]quit
```

[RTA]ip route-static 172.16.1.0 24 172.16.0.1

ルーティングテーブルを確認します。

[RTA]dis ip routing-table

Destinations : 13 Routes : 13

Destination/Mask Proto Pre Cost NextHop Interface

.....

172.16.1.0/24 Static 60 0 172.16.0.1 GE0/0

.....

手順3：PCAとRTAをケーブルで接続する

RTAにDHCPサーバーを設定し、SWAにDHCP relay agentを設定します。

RTAを設定します。

[RTA]dhcp enable

[RTA]dhcp server forbidden-ip 172.16.1.1

[RTA]dhcp server ip-pool pool1

[RTA-dhcp-pool-pool1]network 172.16.1.0 mask 255.255.255.0

[RTA-dhcp-pool-pool1]gateway-list 172.16.1.1

[RTA-dhcp-pool-pool1]quit

SWAを設定します。

[SWA]dhcp enable

[SWA]interface Vlan-interface 1

[SWA-Vlan-interface1]dhcp select relay

[SWA-Vlan-interface1]dhcp relay server-address 172.16.0.2

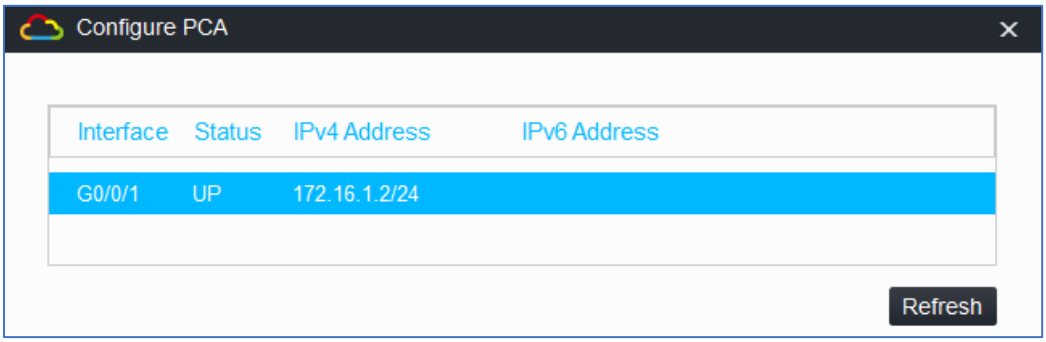
[SWA-Vlan-interface1]quit

手順4：PCAがRTAからDHCP relayによりIPアドレスを取得する

PCAとSWA間のケーブルを外します(HCLの場合、ケーブル上で右クリックし、プルダウンメニューからdeleteをクリックしてケーブルを削除します)。そして、再びケーブルを接続します(HCLの場合、再びAdd linkによりケーブルをつなぎます)。

PCAがSWAを経由(relay)して、RTAのDHCPサーバーから取得したIPアドレスを先ほどと同じように確認します。

HCLの場合、以下のようになります。割り当てられたIPアドレスは172.16.1.2/24でした。



手順5：DHCP relay agentの情報を表示する

SWA上のDHCPサーバーのアドレスを確認します。

```
<SWA>display dhcp relay server-address
Interface name                  Server IP address
Vlan1                           172.16.0.2
```

DHCP relayパケットの情報を表示します。

```
<SWA>display dhcp relay statistics
DHCP packets dropped:                   0
DHCP packets received from clients:     2
    DHCPDISCOVER:                       1
    DHCPREQUEST:                        1
    DHCPINFORM:                         0
    DHCPRELEASE:                        0
    DHCPDECLINE:                                0
    BOOTPREQUEST:                       0
DHCP packets received from servers:     2
    DHCPOFFER:                          1
    DHCPACK:                            1
    DHCPNAK:                            0
    BOOTPREPLY:                         0
DHCP packets relayed to servers:        2
    DHCPDISCOVER:                       1
    DHCPREQUEST:                        1
    DHCPINFORM:                         0
    DHCPRELEASE:                        0
    DHCPDECLINE:                                0
    BOOTPREQUEST:                       0
```

DHCP packets relayed to clients:	2	
DHCPOFFER:	1	
DHCPACK:	1	
DHCPNAK:	0	
BOOTPREPLY:	0	
DHCP packets sent to servers:	0	
DHCPDISCOVER:	0	
DHCPREQUEST:	0	
DHCPINFORM:		0
DHCPRELEASE:	0	
DHCPDECLINE:		0
BOOTPREQUEST:	0	
DHCP packets sent to clients:	0	
DHCPOFFER:	0	
DHCPACK:	0	
DHCPNAK:	0	
BOOTPREPLY:	0	

質問:

1. ラボタスク1で、DHCPアドレスプールがRTAで192.168.0.0/24として構成されている場合、PCAはRTAからIPアドレスを取得しますか？ どうして？

答え:

いいえ。

PCAはサブネット192.168.0.0/24のIPアドレスを取得できません。 ネットワークデバイスは、チェックメカニズムを使用して、無効なIPアドレスの割り当てを防ぎます。 ラボタスク1では、RTAはDHCPサーバーとPCAのゲートウェイの両方として機能してデータを転送します。 RTAは、PCAに接続されているインターフェースとは異なるサブネットに属するIPアドレスを割り当てません。 そうしないと、PCAはRTAと通信できません。 実際、DHCPアドレスプールとは異なるサブネット上で再利用されるインターフェース上のDCHP要求とは異なるサブネット上にあるインターフェースでDHCP要求を受信すると、RTAは要求を無視し、クライアントの要求にIPアドレスを割り当てません。

2. ラボタスク2で、DHCPアドレスプールがRTAで192.168.0.0./24として構成されている場合、PCAはRTAからIPアドレスを取得しますか？ どうして？

答え：
いいえ。PCAはサブネット192.168.0.0/24のIPアドレスを取得できません。 DHCPリレーエージェントは、パケットをDHCPサーバーに転送する前に、受信インターフェースのIPアドレスをDHCPクライアントからDHCPパケットに追加します。 DHCPサーバーは、DHCPリレーエージェントの受信インターフェースのサブネットにIPアドレスを割り当てます。 DHCPアドレスプールがそのサブネット上にないためです。 DHCPはIPアドレスを割り当てません。

Lab9 IPv6

実習内容と目標

このラボでは以下のことを学びます：

- ルーターに IPv6 のアドレスを設定します。
- IPv6 アドレスに ping します。
- IPv6 アドレスの設定とネイバーの情報をチェックします。

ネットワーク図

図 9.1 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
PC	Windows 7	1	なし
ネットワークケーブルの接続	--	1	なし

実習手順

タスク：IPv6アドレスの設定と表示

このタスクは、IPアドレスを構成する方法を示しています。 IPv6ネイバーエントリを確認し、IPv6ネイバーへの接続をテストします。 このタスクを完了すると、neighbor discovery（ND）プロトコルがどのように機能するかを説明できるようになります。 このラボタスクのすべてのコマンドについては、コマンドリファレンスのセクションを参照してください。

手順1：ルーターをケーブルで接続する

図9.1のようにルーター間をケーブルで接続します。

display versionコマンドを使用して、RTAおよびRTBが予期されたソフトウェアバージョンを実行していることを確認します。 どちらにも構成が行われていないことを確認してください。 RTAまたはRTBの設定が変更された場合は、reset saved-configurationコマンドを使用してデフォルト設定を復元し、rebootコマンドを使用してルーターをリブートして変更を検証します。 これらすべてのコマンドをユーザービューで実行します。

手順2：リンクローカルIPv6アドレスを自動的に生成し、接続をテストし、ネイバーを表示する

RTAを設定します。

インターフェース GigabitEthernet 0/0を自動的にリンクローカルIPv6アドレスを生成するように設定します。

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]ipv6 address auto link-local

[RTA-GigabitEthernet0/0]quit

RTBを設定します。

インターフェース GigabitEthernet 0/0を自動的にリンクローカルIPv6アドレスを生成するように設定します。

[RTB]interface GigabitEthernet 0/0

[RTB-GigabitEthernet0/0]ipv6 address auto link-local

[RTB-GigabitEthernet0/0]quit

上記の設定が完了すると、各インターフェースはリンクローカルアドレスを生成します。 各ルーターのリンクローカルアドレスを表示し、以下に示すように接続をテストします。

[RTA]display ipv6 interface GigabitEthernet 0/0 brief

*down: administratively down

(s): spoofing

Interface Physical Protocol IPv6 Address

GigabitEthernet0/0 up up

FE80::3E23:ACFF:FECA:105

[RTB]display ipv6 interface GigabitEthernet 0/0 brief

*down: administratively down

(s): spoofing

Interface Physical Protocol IPv6 Address

GigabitEthernet0/0 up up

FE80::3E23:B6FF:FE74:205

[RTA]ping ipv6 -i GigabitEthernet 0/0 FE80::3E23:ACFF:FECA:105
Ping6(56 data bytes) FE80::3E23:ACFF:FECA:105 --> FE80::3E23:ACFF:FECA:105,
press CTRL_C to break
56 bytes from FE80::3E23:ACFF:FECA:105, icmp_seq=0 hlim=64 time=0.000 ms
56 bytes from FE80::3E23:ACFF:FECA:105, icmp_seq=1 hlim=64 time=0.000 ms
56 bytes from FE80::3E23:ACFF:FECA:105, icmp_seq=2 hlim=64 time=0.000 ms
56 bytes from FE80::3E23:ACFF:FECA:105, icmp_seq=3 hlim=64 time=0.000 ms
56 bytes from FE80::3E23:ACFF:FECA:105, icmp_seq=4 hlim=64 time=0.000 ms

--- Ping6 statistics for FE80::3E23:ACFF:FECA:105 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.000/0.000/0.000 ms

RTAのネイバー情報を表示します。
[RTA]display ipv6 neighbors all
Type: S-Static D-Dynamic O-Openflow R-Rule I-Invalid
IPv6 address Link layer VID Interface/Link ID State T Age
3001::2 3c23-b674-0205 N/A GE0/0 STALE D
619
FE80::3E23:B6FF:FE74:205 3c23-b674-0205 N/A GE0/0 STALE D
609

手順3：インターフェースがグローバルユニキャストアドレスを生成するように設定し、接続確認をしてネイバーを表示します。
RTAを設定します。
interface G0/0にグローバルユニキャストアドレス 3001::1を設定します。
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ipv6 address 3001::1/64
[RTA-GigabitEthernet0/0]quit

RTBを設定します。
interface G0/0にグローバルユニキャストアドレス 3001::2を設定します。
[RTB]interface GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ipv6 address 3001::2/64

[RTB-GigabitEthernet0/0]quit

上記の構成が完了すると、各インターフェースはグローバルIPv6ユニキャストアドレスを生成します。 各ルーターのグローバルIPv6ユニキャストアドレスを表示し、以下に示すように接続をテストします。

```
[RTA]dis ipv6 interface GigabitEthernet 0/0 brief
*down: administratively down
(s): spoofing
Interface                                  Physical Protocol IPv6 Address
GigabitEthernet0/0                         up       up       3001::1
[RTB]display ipv6 interface GigabitEthernet 0/0 brief
*down: administratively down
(s): spoofing
Interface                                  Physical Protocol IPv6 Address
GigabitEthernet0/0                         up       up       3001::2

[RTA]ping ipv6 3001::2
Ping6(56 data bytes) 3001::1 --> 3001::2, press CTRL_C to break
56 bytes from 3001::2, icmp_seq=0 hlim=64 time=2.000 ms
56 bytes from 3001::2, icmp_seq=1 hlim=64 time=1.000 ms
56 bytes from 3001::2, icmp_seq=2 hlim=64 time=3.000 ms
56 bytes from 3001::2, icmp_seq=3 hlim=64 time=1.000 ms
56 bytes from 3001::2, icmp_seq=4 hlim=64 time=2.000 ms

--- Ping6 statistics for 3001::2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.800/3.000/0.748 ms
```

IPv6ネイバーを表示します。

```
[RTA]display ipv6 neighbors all
Type: S-Static       D-Dynamic       O-Openflow       R-Rule       I-Invalid
IPv6 address                 Link layer        VID  Interface/Link ID     State T  Age
3001::2                      3c23-b674-0205 N/A    GE0/0                    REACH D
23
FE80::3E23:B6FF:FE74:205     3c23-b674-0205 N/A    GE0/0                    REACH
D  13
```

質問:

1. IPv6ネイバーテーブルにはどのネイバー状態が含まれ、それらはどういう意味ですか？

答え:

隣接する状態には、INCMP、REACH、STALE、DELAY、およびPROBEが含まれます。 INCMPは、ネイバーアドレスが解決中であり、ネイバーのリンク層アドレスが不明であることを示しました。 REACHは、ネイバーが到達可能であることを示します。 STALE、DELAY、またはPROBEは、ネイバーの到達可能性が検証されていないことを示します。 NDプロトコルは、これらの状態を使用してネイバーの信頼性を示し、より多くの操作をサポートすることで、ARPよりも高いセキュリティを提供します。

Lab10 IPルーティング基礎

実習内容と目標

このラボでは以下のことを学びます：

- Static と default route のコンフィグレーション。
- ルーティングテーブルの表示。

ネットワーク図

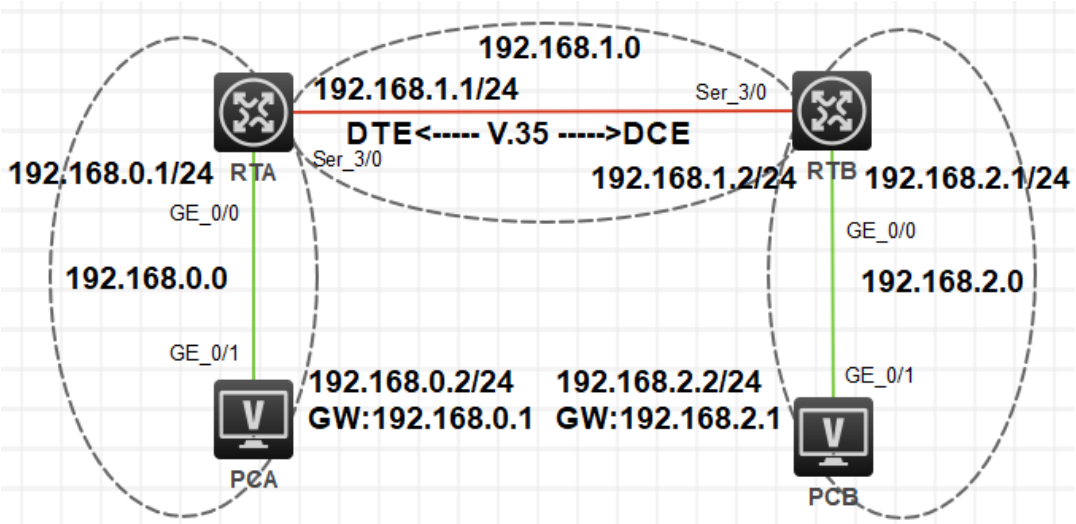


図 10.1 実習ネットワーク

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
V.35 DCEシリアルケーブル	-	1	
V.35 DTEシリアルケーブル		1	
PC	Windows 7	1	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：ルーティングテーブルを表示する

このタスクでは、ルーティングテーブルの表示法、ルーティングエントリーの項目を確認します。

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
.....
```

手順2：ルーティングテーブルを表示します

RTAのルーティングテーブルを表示します。

```
<RTA>display ip routing-table
Destinations : 8        Routes : 8
Destination/Mask    Proto   Pre  Cost      NextHop         Interface
0.0.0.0/32          Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0         127.0.0.1       InLoop0
224.0.0.0/4         Direct  0    0         0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0         0.0.0.0         NULL0
255.255.255.255/32  Direct  0    0         127.0.0.1       InLoop0
```

この結果は、ルーターが8つのダイレクトルートを持ち、1つのループバックアドレス
127.0.0.0と1つの別のループバックアドレス 127.0.0.1を持っています。

表10-1 IPアドレス割り当てスキーマ

装置	インターフェース	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

スキーマ毎にIPアドレスを割り当てます。

RTAをコンフィギュレーションします。

[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ip address 192.168.0.1 24
[RTA-GigabitEthernet0/0]quit
[RTA]interface Serial 3/0
[RTA-Serial3/0]ip address 192.168.1.1 24
[RTA-Serial3/0]quit

RTBをコンフィギュレーションします。

[RTB]interface GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ip address 192.168.2.1 24
[RTB-GigabitEthernet0/0]quit
[RTB]interface Serial 3/0
[RTB-Serial3/0]ip address 192.168.1.2 24
[RTB-Serial3/0]quit

RTAのルーティングテーブルを表示します。

<RTA>display ip routing-table
Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0

127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

出力は、RTAに宛先192.168.0.0/24、192.168.0.1/32、192.168.1.0/24、192.168.1.1/32、および192.168.1.2/32への新しい直接ルートがあることを示しています。これらのルートのうち192.168.0.1/ 32、192.168.1.1 / 32、および192.168.1.2/32はサブネットルートです。直接ルートは、リンク層プロトコルがアップすると検出されます。ポートのリンク層プロトコルがダウンすると、それに接続されている直接ルートは削除されます。

RTAのGigabitEthernet 0/0をshut downします。

```
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]shutdown
%Nov  5 17:56:32:962 2021 RTA IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet0/0 changed to down.
%Nov  5 17:56:32:962 2021 RTA IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet0/0 changed to down.
[RTA-GigabitEthernet0/0]quit
```

RTAの最新のルーティングテーブルを表示します。

```
[RTA]display ip routing-table
Destinations : 13        Routes : 13
```

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0

127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

GigabitEthernet 0/0のリンク層プロトコルがdisableになったのでこのポートに接続されているダイレクトルートが削除されます。

GigabitEthernet 0/0 を元に戻します。

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]undo shutdown

[RTA-GigabitEthernet0/0]%Nov 5 17:57:15:834 2021 RTA IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet0/0 changed to up.

%Nov 5 17:57:15:835 2021 RTA IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet0/0 changed to up.

[RTA-GigabitEthernet0/0]quit

リンク層プロトコルがアップした後、GigabitEthernet 0/0のダイレクトルートが追加されます。

タスク2：static routeの設定をします

このタスクではPC間のコミュニケーションを可能にするstatic routeの設定を行います。そして、どのようにしてルーティングループが発生するかを説明します。

手順1：PCのIPアドレスを設定する

表10-1に従って、PCのIPアドレスとゲートウェイを構成します。 次に、WindowsOSからStart > Runをクリックし、テキストボックスにcmdと入力して、OKをクリックし、ipconfigコマンドを使用して、構成されたIPアドレスとゲートウェイが正しいことを確認します。

接続をテストするために各PCのゲートウェイを使用します。 たとえば、PCAでゲートウェイ192.168.0.1にpingを実行します。

<PCA>ping 192.168.0.1

Ping 192.168.0.1 (192.168.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.0.1: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=3.000 ms
56 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.0.1: icmp_seq=4 ttl=255 time=2.000 ms

--- Ping statistics for 192.168.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/1.600/3.000/1.020 ms

お互いのPCへpingを行います。例えば、PCAからPCBへpingします。
[RTA]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

出力は、宛先に到達できないことを示しています。 これは、RTAが192.168.2.2のPCBへのルートを持っていないためです。

RTAのルーティングテーブルを表示
[RTA]display ip routing-table
Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0

192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

出力は、RTAにサブネット192.168.2.0/24へのルートがないことを示しています。 この問題を解決するために、各ルーターに静的ルートを構成できます。

手順2：static routeの計画を立てる

ネクストホップが2つのルーターで構成された静的ルートに含まれることを考慮してください。

手順3：static routeを設定する

RTAを設定する。

[RTA]ip route-static 192.168.2.0 24 192.168.1.2

RTBを設定する。

[RTB]ip route-static 192.168.0.0 24 192.168.1.1

RTAのルーティングテーブルを表示する

[RTA]display ip routing-table

Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0

192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.2.0/24	Static	60	0	192.168.1.2	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

PC間の接続性を確認する。例えば、PCAからPCBへpingする。

<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=3.000 ms

56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=5.000 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=5.000 ms

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

PCAからPCBへtracerouteする(HCLではtracertコマンドは用意されていません)

C:¥Users¥PCA>tracert 192.168.2.2

192.168.2.2 へのルートをトレースしています。経由するホップ数は最大 30 です

1	<1 ms	<1 ms	<1 ms	192.168.0.1
2	23 ms	23 ms	23 ms	192.168.1.2
3	28 ms	27 ms	28 ms	192.168.2.2

トレースを完了しました。

出力結果はPCAからPCBへの経路がPCA -> RTA -> RTB -> PCBであることを示しています。

手順4：ルーティングループを作成し、ルーターの転送動作を観察します。

ルーティングループを作成するには、ネクストホップがRTAとRTBのそれぞれの他のルーターを指すようにデフォルトルートを構成します。 ルーターはシリアルポートを介して接続されているためです。 ネクストホップはローカルシリアルポートとして設定されます。

RTAを設定します。

[RTA]ip route-static 0.0.0.0 0.0.0.0 s3/0

RTBを設定します。
[RTB]ip route-static 0.0.0.0 0.0.0.0 s3/0

それぞれのルーターのルーティングテーブルを表示します。例えば、RTAのルーティングテーブルを表示します。
[RTA]display ip routing-table

Destinations : 19 Routes : 19

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/0	Static	60	0	0.0.0.0	Ser3/0
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.2.0/24	Static	60	0	192.168.1.2	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

PCAから3.3.3.3へTracerouteします(HCLではtracertコマンドは用意されていません)。
C:¥Users¥PCA>tracert 3.3.3.3
3.3.3.3 へのルートをトレースしています。経由するホップ数は最大 30 です

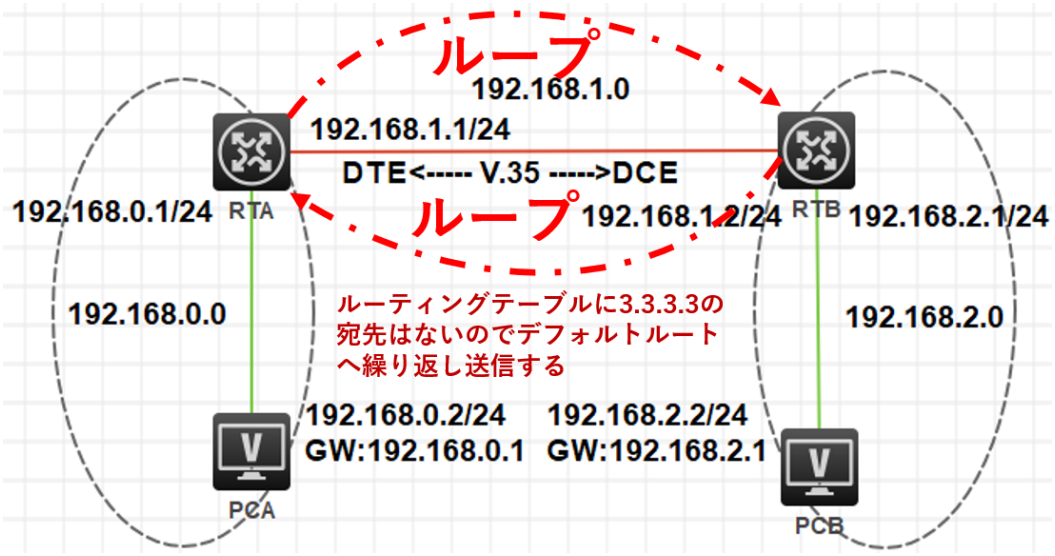
1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	23 ms	23 ms	23 ms	192.168.1.2
3	27 ms	27 ms	27 ms	192.168.1.1
4	31 ms	31 ms	31 ms	192.168.1.2
5	56 ms	56 ms	56 ms	192.168.1.1

.....

29	386 ms	387 ms	386 ms	192.168.1.1
30	409 ms	409 ms	409 ms	192.168.1.2

トレースを完了しました。

宛先3.3.3.3はデフォルトルートと一致するため、宛先3.3.3.3にアドレス指定されたパケットはRTBに送信されます。 その後、RTAに送り返します。 ルーティングループが発生します。パケットは、TTLが0に低下するまで、2つのルーター間で継続的に送信されます。



したがって、同じ宛先にアドレス指定され、ネクストホップが2つの接続されたルーター上の他のルーターを指す静的ルートを構成することはできません。 そうしないと、ルーティングループが発生します。

質問:

1. このラボでRTAに静的ルートのみを構成するとします。PCAからPCBへ送信されたパケットはPCBに到達できますか？ PCBはPCAからpingできましたか？

答え:

PCAからPCBに送信されたパケットはPCBに到達できます。 RTAで設定された静的ルートは、パケットをRTBに転送します。 次に、直接サブネットルートを介してパケットをPCBに送信

します。

RTBにはPCAへのルートがないため、PCAからPCBへのping操作は成功せず、PCBからのping応答パケットはRTBによって破棄されます。
実際には、ほとんどのネットワークアプリケーションは双方向通信を必要とします。 たとえば、HTTP、FTP、および電子メールは、双方向接続を確立するTCPを採用しています。

2. PCとルーターの間でルーティングループが発生する可能性はありますか？

答え:
いいえ、できません。 PCにはルーティング機能がないため、PC宛てではない着信パケットが破棄されます。

Lab11 RIPルーティング

実習内容と目標

このラボでは以下のことを学びます:

- RIP のコンフィグレーション。
- ルーティングテーブルの表示。

ネットワーク図

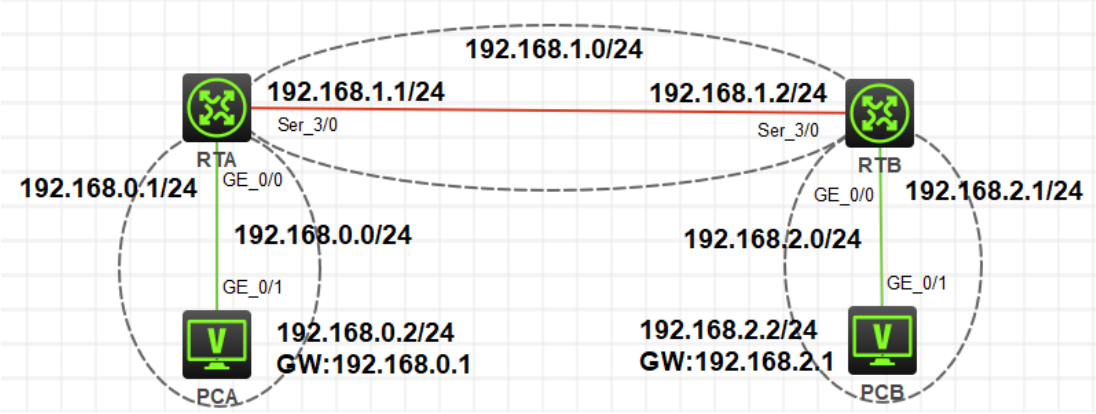


図 11.1 実習ネットワーク

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
PC	Windows 7	1	なし
V.35 DCEシリアルケーブル	-	1	
V.35 DTEシリアルケーブル		1	
ネットワークケーブルの接続	--	2	なし

実習手順

タスク1:RIPv1に設定する

このタスクでは、PC間のコミュニケーションができるようにRIPv1をどのように設定するかを確認します。

手順1：PCとルーターをケーブルで接続する

図11.1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

.....

手順2：PCとルーターにIPアドレスをアサインします

表11-1 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 11-1 のようにルーターに IP アドレスをアサインします。

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 3/0

[RTA-Serial3/0]ip address 192.168.1.1 24
[RTA-Serial3/0]quit

RTBを設定します。
[RTB]int GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ip address 192.168.2.1 24
[RTB-GigabitEthernet0/0]quit
[RTB]interface Serial 3/0
[RTB-Serial3/0]ip address 192.168.1.2 24
[RTB-Serial3/0]quit

- 表 11-1 で、PC の IP アドレスを構成し、ゲートウェイを指定します。 構成が完了したら、Windows オペレーティングシステムからスタート> ファイル名を指定して実行を選択し、ポップアップウィンドウに cmd と入力します。 次に、CLI で ipconfig と入力して、構成された IP アドレスと指定されたゲートウェイを確認します。
- ping コマンドを使用して、PC とゲートウェイ間の到達可能性をテストします。 たとえば、PCA のゲートウェイ（192.168.0.1）に ping を実行して、次の情報を出力します。
  <PCA>ping 192.168.0.1
  Ping 192.168.0.1 (192.168.0.1): 56 data bytes, press CTRL_C to break
  56 bytes from 192.168.0.1: icmp_seq=0 ttl=255 time=2.000 ms
  56 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=2.000 ms
  56 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=2.000 ms
  56 bytes from 192.168.0.1: icmp_seq=3 ttl=255 time=2.000 ms
  56 bytes from 192.168.0.1: icmp_seq=4 ttl=255 time=1.000 ms

- PC 間の到達可能性をテストします。 たとえば、次の出力のために PCA で PCB に ping を実行します。
  <H3C>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

出力は、ゲートウェイが宛先到達不能メッセージを返すことを示し、ping要求が宛先に転送されなかったことを示します。 ルーターのルーティングテーブルを表示します。 たとえば、次の出力のRTAのルーティングテーブルを表示します。

[RTA]display ip routing-table

Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

出力は、ネットワーク192.168.2.0/24（PCBが存在する場所）へのルートがRTAのルーティングテーブルで利用できないことを示しています。 したがって、PCAからping要求を受信すると、RTAはそれらを破棄し、宛先到達不能メッセージをPCAに返します。 この問題を解決するために、ルーターでRIPを構成できます。

手順3：RIPの設定をします。

RTAでは：

[RTA]rip

[RTA-rip-1]network 192.168.0.0

[RTA-rip-1]network 192.168.1.0

[RTA-rip-1]quit

RTBでは：

[RTB]rip
[RTB-rip-1]network 192.168.1.0
[RTB-rip-1]network 192.168.2.0
[RTB-rip-1]quit

ルーターのルーティングテーブルを表示します。 たとえば、RTAのルーティングテーブルを表示します。

[RTA]display ip routing-table
Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.2.0/24	RIP	100	1	192.168.1.2	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

出力は、ネットワーク192.168.2.0/24へのルートが利用可能であり、RIPによって学習されていることを示しています。 次に、PC間の到達可能性をテストします。 たとえば、PCAでPCBにpingを実行すると、次の情報が出力されます。

<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=3.000 ms
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=4.000 ms

56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=6.000 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=5.000 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=5.000 ms

手順4:RIPの状態をチェックします。
Display ripコマンドをRTAで実行します。

```
[RTA]display rip
  Public VPN-instance name:
    RIP process: 1
      RIP version: 1
      Preference: 100
      Checkzero: Enabled
      Default cost: 0
      Summary: Enabled
      Host routes: Enabled
      Maximum number of load balanced routes: 32
      Update time    :   30 secs   Timeout time          :   180 secs
      Suppress time :   120 secs   Garbage-collect time :   120 secs
      Update output delay:    20(ms)   Output count:      3
      TRIP retransmit time:      5(s)   Retransmit count: 36
      Graceful-restart interval:    60 secs
      Triggered Interval : 5 50 200
      BFD: Disabled
      Silent interfaces: None
      Default routes: Disabled
      Verify-source: Enabled
      Networks:
          192.168.0.0                 192.168.1.0
      Configured peers: None
      Triggered updates sent: 2
      Number of routes changes: 3
      Number of replies to queries: 1
```

出力はRIPv1が採用されていることを示し、ルート自動要約が有効になっています。 RIPの更新間隔は30秒で、ネットワーク192.168.0.0および192.168.1.0はRIPで有効になっています。

RIPパケットのデバッグを有効にして、受信/送信されたRIPパケットを確認します。

<RTA>terminal debugging

<RTA>debugging rip 1 packet

*Nov 16 16:02:40:904 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Sending response on interface GigabitEthernet0/0** from 192.168.0.1 to 255.255.255.255

*Nov 16 16:02:40:904 2021 RTA RIP/7/RIPDEBUG: Packet: version 1, cmd response, length 44

*Nov 16 16:02:40:904 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **192.168.1.0, cost 1**

*Nov 16 16:02:40:904 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **192.168.2.0, cost 2**

*Nov 16 16:02:40:904 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Sending response on interface Serial3/0** from 192.168.1.1 to 255.255.255.255

*Nov 16 16:02:40:904 2021 RTA RIP/7/RIPDEBUG: Packet: version 1, cmd response, length 24

*Nov 16 16:02:40:904 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **192.168.0.0, cost 1**

*Nov 16 16:03:05:339 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Receiving response from 192.168.1.2 on Serial3/0**

*Nov 16 16:03:05:339 2021 RTA RIP/7/RIPDEBUG: Packet: version 1, cmd response, length 24

*Nov 16 16:03:05:339 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **192.168.2.0, cost 1**

出力は、RTAがGigabitEthernet 0/0でルート192.168.1.0（コスト1）および192.168.2.0（コスト2）を含むルート更新を送信し、serial3/0でルート192.168.0.0（コスト1）を含むルート更新を送信することを示しています。 ルートの更新がブロードキャストされます。RTAは、ルート192.168.2.0（コスト1）を含むルート更新をserial3/0のRTB（192.168.1.2）から受信します。

serial3/0でルート192.168.2.0を受信した後、ルーターでRIPが有効になった後、スプリットホライズンがデフォルトで有効になっているため、RTAはserial3/0を介してルートを送信しません。

手順5:split horizonとpoison reverseをチェックします。

serial3/0またはRTAでsplit horizonを無効にしてから、送受信されたパケットを確認します。

[RTA-Serial3/0]undo rip split-horizon

*Nov 16 16:05:22:404 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Sending response on interface Serial3/0** from 192.168.1.1 to 255.255.255.255

*Nov 16 16:05:22:404 2021 RTA RIP/7/RIPDEBUG: Packet: version 1, cmd response, length 64

*Nov 16 16:05:22:404 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **192.168.0.0, cost 1**

*Nov 16 16:05:22:404 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **192.168.1.0, cost 1**

*Nov 16 16:05:22:405 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **192.168.2.0, cost 2**

出力は、split horizonが無効になった後を示しています。 RTAは、serial3/0でルート192.168.0.0、192.168.1.0、および192.168.2.0を含むルート更新を送信します。 RTAは、serial3/0で受信したルート192.168.2.0をserial3/0を介して送信します。 これにより、ルーティングループが発生する可能性があります。

ルーティングループを回避する別の方法は、poison reverseです。 RTAのserial3/0でポイズンリバースを有効にしてから、送受信されたパケットを確認します。

[RTA-Serial3/0]rip poison-reverse

*Nov 16 16:07:32:404 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Sending response on interface Serial3/0** from 192.168.1.1 to 255.255.255.255

*Nov 16 16:07:32:404 2021 RTA RIP/7/RIPDEBUG: Packet: version 1, cmd response, length 64

*Nov 16 16:07:32:404 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **192.168.0.0, cost 1**

*Nov 16 16:07:32:404 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **192.168.2.0, cost 16**

出力は、ポイズンリバースが有効になった後、RTAがルート192.168.2.0を含むルートアップデートをserial3/0経由で送信することを示していますが、ルートのコストは16です。したがって、RTBはネットワーク192.168.2.0宛てのパケットをRTAのserial3/0に転送しません。

手順6: silent-interfaceコマンドを使用して、RIPパケットの送信を制御します。

通常、ルーターは、PCがRIPパケットを受信する必要がない場合でも、PCに接続されているインターフェイスを含むすべてのインターフェイスを介してRIPプロトコルパケットを送信します。 silent-interfaceコマンドを使用して、インターフェイスがRIPパケットを送信できないようにすることができます。

RTAを設定

[RTA]rip

[RTA-rip-1]silent-interface GigabitEthernet 0/0

[RTA-rip-1]quit

RTBを設定

<RTB>sys

System View: return to User View with Ctrl+Z.

[RTB]rip

[RTB-rip-1]silent-interface GigabitEthernet 0/0

[RTB-rip-1]quit

構成が完了したら、debuggingコマンドを使用して、送受信されたRIPパケットを確認します。出力は、RIPパケットがGigabitEthernet0/0を介して送信されていないことを示しています。

この方法により、ルートリークによって引き起こされるネットワークセキュリティの問題を回避できます。 たとえば、会社のRIP対応ルートがインターフェイスを介してパブリックネットワークに接続されている場合、パブリックネットワークが内部ルート情報を取得しないようにインターフェイスでsilent-interfaceコマンドを設定できます。

このタスクを完了したら、ルーターのdebuggingを無効にします。

<RTA>undo debugging all

All possible debugging has been turned off.

<RTB>undo debugging all

All possible debugging has been turned off.

タスク2：RIPv2に設定する

このタスクは、RIPv1がその制限のためにサブネットルートを正しく学習できないことを示しています。 このタスクでは、RIPv2を構成する方法も示します。

手順1：PCとルーターをケーブルで接続する

図11.1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

.....

手順2：PCとルーターにIPアドレスを割り当てます。

表11-2 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	10.0.0.1/24	-
PCA		192.168.0.2/24	192.168.0.1
PCB		10.0.0.2/24	10.0.0.1

- 表 11-2 の IP アドレスをルーターに割り当てます。
  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 3/0
  [RTA-Serial3/0]ip address 192.168.1.1 24
  [RTA-Serial3/0]quit

  RTBを設定します。
  [RTB]interface GigabitEthernet 0/0
  [RTB-GigabitEthernet0/0]ip address 10.0.0.1 24
  [RTB-GigabitEthernet0/0]quit
  [RTB]interface Serial 3/0
  [RTB-Serial3/0]ip address 192.168.1.2 24
  [RTB-Serial3/0]quit
- 表 11-2 で、IP アドレスを構成し、PC のゲートウェイを指定します。構成が完了したら、Windows の操作システムからスタート > ファイル名を指定して実行を選択し、ポップアップウィンドウに **cmd** と入力します。 次に、CLI で ipconfig と入力して、構成済みの IP アドレスと指定されたゲートウェイを確認します。

手順3：RIPv1を構成し、ルーティングテーブルを表示します。
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 10.0.0.0
[RTB-rip-1]quit
```

構成が完了したら、RTAのルーティングテーブルを表示します。

```
[RTA]display ip routing-table
Destinations : 18        Routes : 18
Destination/Mask    Proto   Pre Cost      NextHop         Interface
0.0.0.0/32          Direct  0   0         127.0.0.1       InLoop0
10.0.0.0/8          RIP     100 1         192.168.1.2     Ser3/0
127.0.0.0/8         Direct  0   0         127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0         127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0         127.0.0.1       InLoop0
192.168.0.0/24      Direct  0   0         192.168.0.1     GE0/0
192.168.0.0/32      Direct  0   0         192.168.0.1     GE0/0
192.168.0.1/32      Direct  0   0         127.0.0.1       InLoop0
192.168.0.255/32    Direct  0   0         192.168.0.1     GE0/0
192.168.1.0/24      Direct  0   0         192.168.1.1     Ser3/0
192.168.1.0/32      Direct  0   0         192.168.1.1     Ser3/0
192.168.1.1/32      Direct  0   0         127.0.0.1       InLoop0
192.168.1.2/32      Direct  0   0         192.168.1.2     Ser3/0
192.168.1.255/32    Direct  0   0         192.168.1.1     Ser3/0
224.0.0.0/4         Direct  0   0         0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0         0.0.0.0         NULL0
255.255.255.255/32  Direct  0   0         127.0.0.1       InLoop0
```

出力は、RTAがRIPを介してルート10.0.0.0/8を学習したが、RTBのルートは10.0.0.0/24であることを示しています。 RTAはルートを正しく学習できませんでした。

RIPパケットのデバッグを有効にして、RTAで受信/送信されたRIPパケットをチェックします。

```
<RTA>terminal debugging
The current terminal is enabled to display debugging logs.
<RTA>debugging rip 1 packet
```

<RTA>*Nov 16 16:55:12:932 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Receiving response from 192.168.1.2 on Serial3/0**

*Nov 16 16:55:12:932 2021 RTA RIP/7/RIPDEBUG: Packet: version 1, cmd response, length 24

*Nov 16 16:55:12:932 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination 10.0.0.0, cost 1

出力は、RTAがサブネットマスクなしでルート10.0.0.0を含むRTBからルート更新を受信したことを示しています。 したがって、RTAはルートに自然なネットワークマスクを追加します。つまり、10.0.0.0/8です。

RIPv1メッセージにはサブネットマスクが含まれていないためです。 ルーターはルーターを正しく学習できない場合があります。 この問題を解決するには、RIPv2を使用します。

手順4：RIPv2を設定します。

RTAを設定します。

[RTA]rip

[RTA-rip-1]version 2

[RTA-rip-1]undo summary

[RTA-rip-1]quit

RTBを設定します。

[RTB]rip

[RTB-rip-1]version 2

[RTB-rip-1]undo summary

[RTB-rip-1]quit

設定が完了したら、RTAのルーティングテーブルを表示します。

[RTA]display ip routing-table

Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.0/24	RIP	100	1	192.168.1.2	Ser3/0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0

192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

出力は、RTAがルート10.0.0.0/24を正しく学習したことを示しています。
RIPルートのエージングタイムは180秒であるため、ルート10.0.0.0/8はルーティングテーブルにまだ存在します。 180秒以内にルートの更新が受信されない場合、ルートはルーティングテイルから削除されます。

RIPの動作状態を確認してください。 RTAの例;

```
[RTA]display rip
  Public VPN-instance name:
    RIP process: 1
        RIP version: 2
        Preference: 100
        Checkzero: Enabled
        Default cost: 0
        Summary: Disabled
        Host routes: Enabled
        Maximum number of load balanced routes: 32
        Update time    :   30 secs   Timeout time          :   180 secs
        Suppress time :   120 secs   Garbage-collect time :   120 secs
        Update output delay:    20(ms)   Output count:      3
        TRIP retransmit time:      5(s)   Retransmit count: 36
        Graceful-restart interval:    60 secs
        Triggered Interval : 5 50 200
        BFD: Disabled
        Silent interfaces: None
        Default routes: Disabled
        Verify-source: Enabled
```

Networks:

192.168.0.0 192.168.1.0

Configured peers: None

Triggered updates sent: 4

Number of routes changes: 5

Number of replies to queries: 1

出力は、現在のRIPバージョンがRIPv2であることを示しています。

RTAで送受信されたパケットを確認します。

<RTA>terminal debugging

The current terminal is enabled to display debugging logs.

<RTA>debugging rip 1 packet

*Nov 16 17:06:35:522 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Receiving response from 192.168.1.2 on Serial3/0**

*Nov 16 17:06:35:522 2021 RTA RIP/7/RIPDEBUG: Packet: version 2, cmd response, length 24

*Nov 16 17:06:35:522 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **10.0.0.0/255.255.255.0, nexthop 0.0.0.0, cost 1, tag 0**

出力は、RIPv2メッセージにサブネットマスク情報が含まれていることを示しています。

手順5：RIPv2認証を設定します。

RIPv2は、セキュリティを強化するための認証をサポートしています。 RTAとRTBに異なるパスワードを設定して、ルーティング情報を相互に正しく学習できるかどうかを確認します。

RTAを構成します。

[RTA]interface Serial 3/0

[RTA-Serial3/0]rip authentication-mode md5 rfc2453 plain aaaaa

[RTA-Serial3/0]quit

RTBを構成します。

[RTB]interface Serial 3/0

[RTB-Serial3/0]rip authentication-mode md5 rfc2453 plain abcde

[RTB-Serial3/0]quit

既存のルートが一定期間後に期限切れになるためです。 シャットダウンしてからインターフェイスを起動して、ルートの更新を高速化できます。 たとえば、シャットダウンしてから、RTAでSerial3/0を起動します。

[RTA]interface Serial 3/0

[RTA-Serial3/0]shutdown

[RTA-Serial3/0]quit

設定が完了したら、ルーターのルーティングテーブルを表示します。 たとえば、ルーティングテーブルまたはRTAを表示すると、次の情報が出力されます。

[RTA]display ip routing-table

Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

RTAで送受信されたパケットを確認してください。

<RTA>terminal debugging

The current terminal is enabled to display debugging logs.

<RTA>debugging rip 1 packet

<RTA>*Nov 16 17:29:15:595 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Ignored this packet on interface Serial3/0** from 192.168.1.2: **Authentication digest check failed**.

*Nov 16 17:29:15:595 2021 RTA RIP/7/RIPDEBUG: First RTE: ff ff 00 03 3c 20 5a a2 bf d0 69 87 25 c2 9d 1c 5e 5f 1f 2f

*Nov 16 17:29:38:365 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Sending response on interface Serial3/0** from 192.168.1.1 to 224.0.0.9
*Nov 16 17:29:38:365 2021 RTA RIP/7/RIPDEBUG: Packet: version 2, cmd response, length 48
*Nov 16 17:29:38:365 2021 RTA RIP/7/RIPDEBUG: Authentication mode: MD5 RFC2453
*Nov 16 17:29:38:366 2021 RTA RIP/7/RIPDEBUG: Digest: 1d23f8c8.74415840.3a34e8a3.0cf18041
*Nov 16 17:29:38:366 2021 RTA RIP/7/RIPDEBUG: Authentication sequence number: 2583
*Nov 16 17:29:38:366 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination 192.168.0.0/255.255.255.0, nexthop 0.0.0.0, cost 1, tag 0
*Nov 16 17:29:39:084 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Ignored this packet on interface Serial3/0** from 192.168.1.2: **Authentication digest check failed.**
*Nov 16 17:29:39:084 2021 RTA RIP/7/RIPDEBUG: First RTE: ff ff 00 03 8d 35 a9 62 a4 d7 29 35 fd 76 80 e0 84 ec e2 59

パスワードの設定に一貫性がないため、RTAはピアから送信されたルートを学習できません。
RTAのパスワードをRTBのパスワードに変更してから、ルーター間のルーティング情報の交換を確認します。

RTAを構成する
[RTA]interface Serial 3/0
[RTA-Serial3/0]rip authentication-mode md5 rfc2453 plain abcde
[RTA-Serial3/0]quit

設定後、RTAがRTBからルートアップデートを受信するまで待ってから、RTAのルーティングテーブルを表示します。
[RTA]display ip routing-table
Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.0/24	RIP	100	1	192.168.1.2	Ser3/0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0

127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.0/24	Direct	0	0	192.168.0.1	GE0/0
192.168.0.0/32	Direct	0	0	192.168.0.1	GE0/0
192.168.0.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.0.255/32	Direct	0	0	192.168.0.1	GE0/0
192.168.1.0/24	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.0/32	Direct	0	0	192.168.1.1	Ser3/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.2/32	Direct	0	0	192.168.1.2	Ser3/0
192.168.1.255/32	Direct	0	0	192.168.1.1	Ser3/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

ルーティングテーブルには、現在のルート10.0.0.0/24が含まれています。

RTAで送受信されたパケットを確認してください。

<RTA>

*Nov 16 17:34:43:533 2021 RTA RIP/7/RIPDEBUG: RIP 1 : **Receiving response from 192.168.1.2 on Serial3/0**

*Nov 16 17:34:43:533 2021 RTA RIP/7/RIPDEBUG: Packet: version 2, cmd response, length 48

*Nov 16 17:34:43:533 2021 RTA RIP/7/RIPDEBUG: Authentication mode: MD5 RFC2453

*Nov 16 17:34:43:533 2021 RTA RIP/7/RIPDEBUG: Digest: ccfcf958.d75a3e5a.57a561d7.1000f9f3

*Nov 16 17:34:43:533 2021 RTA RIP/7/RIPDEBUG: Authentication sequence number: 3074

*Nov 16 17:34:43:533 2021 RTA RIP/7/RIPDEBUG: AFI 2, destination **10.0.0.0/255.255.255.0, nexthop 0.0.0.0, cost 1, tag 0**

RTAは、RTBからルート更新を正しく受信できます。

質問:

1. ラボタスクでは、ルーターが180秒以内にルートのルート更新を受信しない場合、ルーターはルーティングテーブルからルートを削除します。 エージングタイムを短縮できますか？

答え:

エージングタイマーを小さい値に設定して、ネットワークコンバージェンスを高速化できます。

たとえば、エージングタイマーを60秒に設定します。

[RTA-rip-1] timers timeout 60

2. RIP認証ラボタスクで、設定されたパスワードが送受信されたRIPパケットの出力情報に表示されないのはなぜですか？

答え：
暗号文パスワードは、MD5認証用に構成されています。 プレーンテキストのパスワードが設定されている場合、パスワードは出力情報に表示できます。 ただし、プレーンテキストのパスワードは暗号文のパスワードほど安全ではありません。

Lab12 OSPFルーティング

実習内容と目標

このラボでは以下のことを学びます：

- OSPF area のコンフィグレーション。
- OSPF DR のコンフィグレーション。
- OSPF cost のコンフィグレーション。
- OSPF のルート選択について。
- 複数の OSPF area のコンフィギュレーション。

ネットワーク図

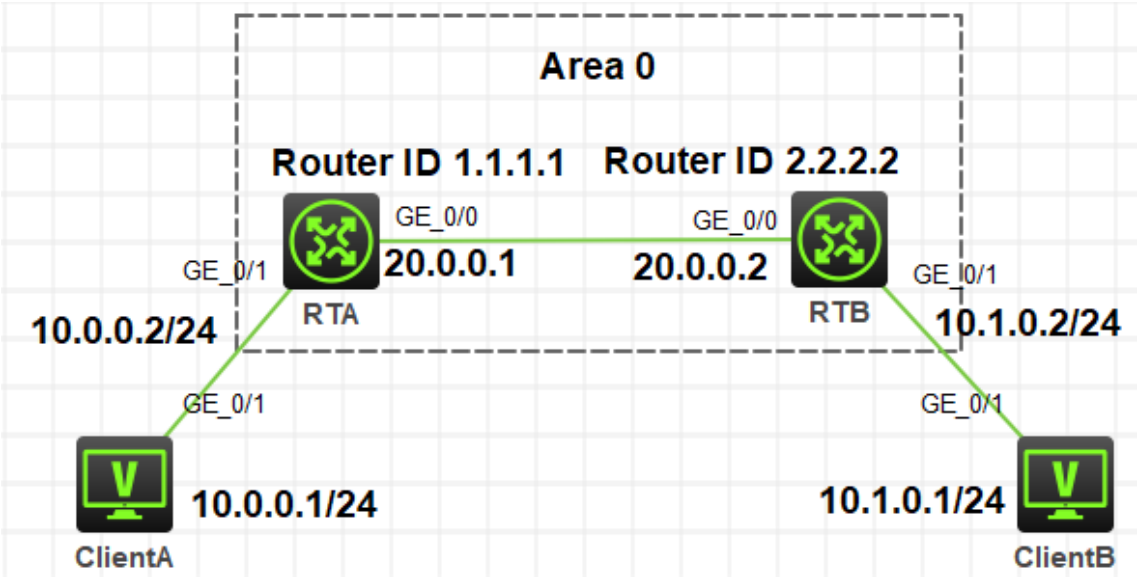


図 12.1 実習ネットワーク

図12-1は、単一のOSPFエリアを構成する方法を説明するlab task1のネットワーク図を示しています。 RTAとRTBは、それぞれクライアントAとクライアントBのゲートウェイです。 RTAのルーターIDはループバックインターフェースアドレス1.1.1.1であり、RTBのルーターIDはループバックインターフェースアドレス2.2.2.2です。 RTAとRTBはどちらもOSPFエリア0に属しています。RTAとRTBはネットワーク層で相互に到達でき、Client AとClient Bは相互に到達できます。

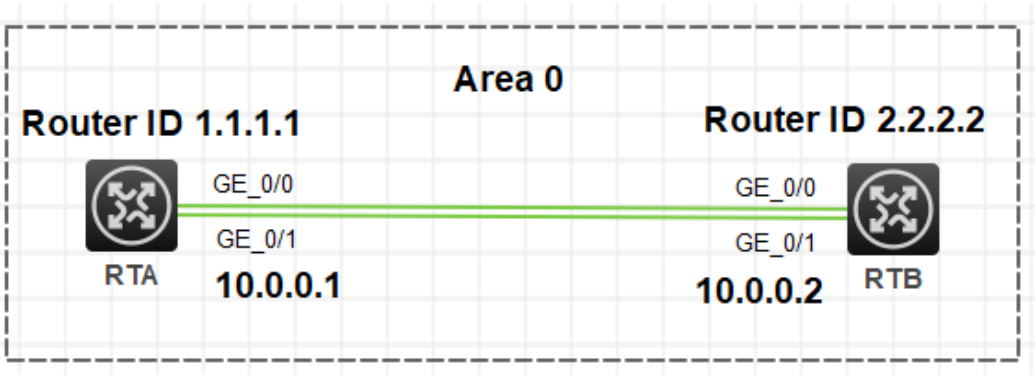


図12.2 実習ネットワーク

図12-2に、OSPFルートの選択を説明するラボタスク2のネットワーク図を示します。 このネットワークでは、2つのMSR30-20ルーターRTAおよびRTBがOSPFループバックインターフェースアドレス2.2.2.2に展開されています。 RTAとRTBはどちらもOSPFエリア0に属しています。RTAとRTBは2つのリンクを介して接続されています。

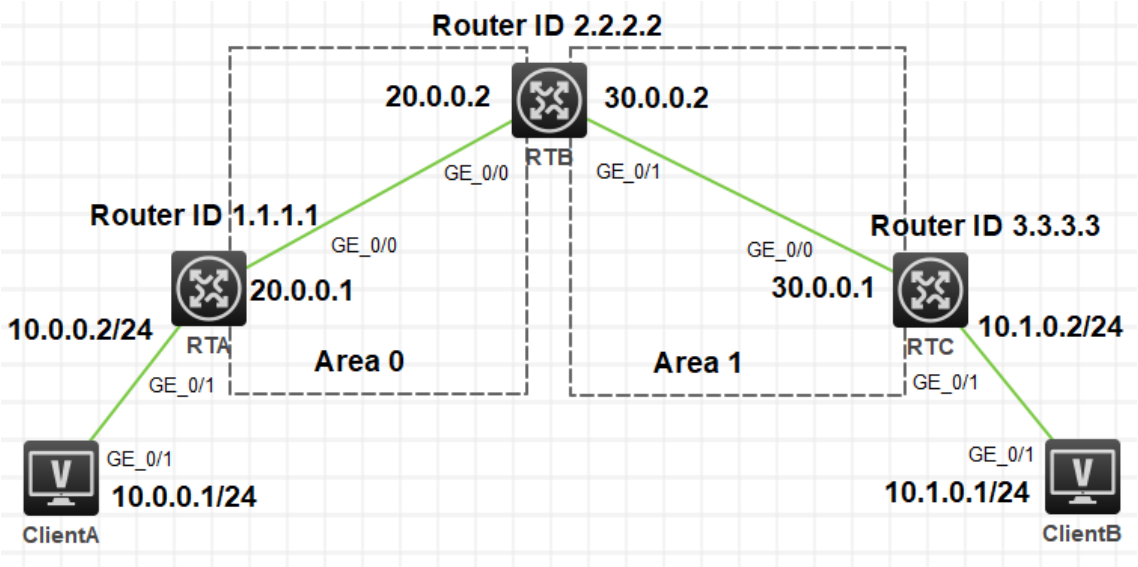


図 12.3 実習ネットワーク

図12-3に、lab task3のネットワーク図を示します。これは、複数のOSPFエリアを構成する方法を示しています。 3台のMSR30-20ルーター、RTA、RTB、RTC、および2台のPC、client Aとclient Bがネットワークに展開されています。 RTAとRTCは、それぞれclient Aとclient Bのゲートウェイです。 RTAのルーターIDはループバックインターフェースアドレス1.1.1.1であり、RTBのルーターIDはループバックインターフェースアドレス2.2.2.2であり、RTCのルーターIDはループバックインターフェースアドレス3.3.3.3です。 RTAとRTBのGigabitEthernet 0/0インターフェースは両方ともOSPFエリア0に属します。RTBとRTCのGigabitEthernet 0/1インターフェースは両方ともOSPFエリア1に属します。RTA、RTB、RTCは到達可能であり、クライアントAとクライアントBはお互いに到達可能です。

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	3	なし
PC	Windows 7	3	なし
ネットワークケーブルの接続	--	3	なし

実習手順

タスク1：基本的なOSPF単一エリアの設定をする

手順1：図12-1のように実習環境を構築する

まず、ラボ図に示すようにラボ環境を確立します。 次に、Client AのIPアドレスを10.0.0.1/24として構成し、ゲートウェイアドレスを10.0.0.2として指定します。 Client BのIPアドレスを10.1.0.1/24として構成し、ゲートウェイアドレスを10.1.0.2として指定します。

手順2：基本的な設定をします

ルーターインターフェースのIPアドレスを設定します。

```
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ip address 20.0.0.1 24
[RTA-GigabitEthernet0/0]quit
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ip address 10.0.0.2 24
[RTA-GigabitEthernet0/1]quit
[RTA]interface LoopBack 0
[RTA-LoopBack0]ip address 1.1.1.1 32
[RTA-LoopBack0]quit

[RTB]interface GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ip address 20.0.0.2 24
[RTB-GigabitEthernet0/0]quit
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ip address 10.1.0.2 24
[RTB-GigabitEthernet0/1]quit
[RTB]interface LoopBack 0
[RTB-LoopBack0]ip address 2.2.2.2 32
```

[RTB-LoopBack0]quit

手順3：ネットワークの接続性とルーティングテーブルをチェックします。
Client Aからclient Bへpingします。
<Client A>ping 10.1.0.1
Ping 10.1.0.1 (10.1.0.1): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
Client AはClient Bへping出来ませんでした。それは、RTAは10.1.0.1へのルートを学習していないからです。
RTAで**display ip routing-table**コマンドを実行してみましょう。
[RTA]display ip routing-table
Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.0/24	Direct	0	0	10.0.0.2	GE0/1
10.0.0.0/32	Direct	0	0	10.0.0.2	GE0/1
10.0.0.2/32	Direct	0	0	127.0.0.1	InLoop0
10.0.0.255/32	Direct	0	0	10.0.0.2	GE0/1
20.0.0.0/24	Direct	0	0	20.0.0.1	GE0/0
20.0.0.0/32	Direct	0	0	20.0.0.1	GE0/0
20.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
20.0.0.255/32	Direct	0	0	20.0.0.1	GE0/0
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

RTAはclient Bへのルートを持っていません。そのため、Client Bへのパケットを送信できません。

同じ情報をチェックするために、同じ操作をRTBで行ってみましょう。

手順4：OSPFを設定します。

OSPFをRTAに設定します。

```
[RTA]router id 1.1.1.1
[RTA]ospf 1
[RTA-ospf-1]area 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]quit
[RTA-ospf-1]quit
```

OSPFをRTBに設定します。

```
[RTB]router id 2.2.2.2
[RTB]ospf 1
[RTB-ospf-1]area 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 10.1.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]quit
[RTB-ospf-1]quit
```

手順5：OSPFのネイバーとルーティングテーブルをチェックします。

OSPFのネイバー状態をチェックするためにRTAで**display ospf peer**コマンドを実行します。

```
[RTA]display ospf peer

        OSPF Process 1 with Router ID 1.1.1.1
                Neighbor Brief Information

 Area: 0.0.0.0
 Router ID         Address         Pri Dead-Time   State             Interface
 2.2.2.2           20.0.0.2        1   35          Full/BDR          GE0/0
```

RTAとRTBの20.0.0.2のインターフェース（ルーターID 2.2.2.2）はネイバーです。 RTB

のインターフェース20.0.0.2は、ネットワークセグメントのDRでもあります。 ネイバー状態がfullで、RTAとRTBのLSDBが同期されていることを示しています。したがって、RTAにはRTBへのルートが必要です。

OSPFのルーティングテーブルをチェックするためにRTAで**display ospf routing**コマンドを実行します。

```
[RTA]display ospf routing
          OSPF Process 1 with Router ID 1.1.1.1
                    Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost      Type      NextHop          AdvRouter
Area
 20.0.0.0/24        1         Transit 0.0.0.0          1.1.1.1          0.0.0.0
 10.0.0.0/24        1         Stub      0.0.0.0          1.1.1.1          0.0.0.0
 2.2.2.2/32         1         Stub      20.0.0.2         2.2.2.2          0.0.0.0
 10.1.0.0/24        2         Stub      20.0.0.2         2.2.2.2          0.0.0.0
 1.1.1.1/32         0         Stub      0.0.0.0          1.1.1.1          0.0.0.0
 Total nets: 5
 Intra area: 5  Inter area: 0  ASE: 0  NSSA: 0
```

OSPFのグローバルなルーティングテーブルをチェックするためにRTAで**display ip routing-table**コマンドを実行します。

```
[RTA]display ip routing-table

Destinations : 19        Routes : 19

Destination/Mask    Proto   Pre Cost      NextHop         Interface
0.0.0.0/32          Direct  0   0         127.0.0.1       InLoop0
1.1.1.1/32          Direct  0   0         127.0.0.1       InLoop0
2.2.2.2/32          O_INTRA 10  1           20.0.0.2        GE0/0
10.0.0.0/24         Direct  0   0         10.0.0.2        GE0/1
10.0.0.0/32         Direct  0   0         10.0.0.2        GE0/1
10.0.0.2/32         Direct  0   0         127.0.0.1       InLoop0
```

```
10.0.0.255/32          Direct  0    0           10.0.0.2        GE0/1
10.1.0.0/24            O_INTRA 10   2           20.0.0.2        GE0/0
20.0.0.0/24            Direct  0    0           20.0.0.1        GE0/0
20.0.0.0/32            Direct  0    0           20.0.0.1        GE0/0
20.0.0.1/32            Direct  0    0           127.0.0.1       InLoop0
20.0.0.255/32          Direct  0    0           20.0.0.1        GE0/0
127.0.0.0/8            Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32           Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32           Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
224.0.0.0/4            Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24           Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
```

RTAはRTBの2.2.2.2/32と10.1.0.0/24へのルートを持っています。

同じような情報を得るためにRTBで同じような操作をしてください。

手順6：ネットワークの接続性をチェックします。

Client AからClient B(10.1.0.1)へpingします。

```
<Client A>ping 10.1.0.1
Ping 10.1.0.1 (10.1.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.0.1: icmp_seq=0 ttl=253 time=3.000 ms
56 bytes from 10.1.0.1: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 10.1.0.1: icmp_seq=2 ttl=253 time=2.000 ms
56 bytes from 10.1.0.1: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 10.1.0.1: icmp_seq=4 ttl=253 time=4.000 ms
```

Client BからClient A(10.0.0.1)へpingします。

```
<Client B>ping 10.0.0.1
Ping 10.0.0.1 (10.0.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.0.0.1: icmp_seq=0 ttl=253 time=3.000 ms
56 bytes from 10.0.0.1: icmp_seq=1 ttl=253 time=6.000 ms
56 bytes from 10.0.0.1: icmp_seq=2 ttl=253 time=6.000 ms
56 bytes from 10.0.0.1: icmp_seq=3 ttl=253 time=6.000 ms
56 bytes from 10.0.0.1: icmp_seq=4 ttl=253 time=5.000 ms
```

タスク2：上級OSPF単一エリアの設定をする

手順1：図12-2のようにlab環境を構築する

手順2：基本的な設定をする

ルーターインターフェースのIPアドレスの設定とOSPFの設定

RTAの設定：

```
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ip address 20.0.0.1 24
[RTA-GigabitEthernet0/0]quit
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ip address 10.0.0.1 24
[RTA-GigabitEthernet0/1]quit
[RTA]interface LoopBack 0
[RTA-LoopBack0]ip address 1.1.1.1 32
[RTA-LoopBack0]quit
[RTA]router id 1.1.1.1
[RTA]ospf 1
[RTA-ospf-1]area 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]quit
[RTA-ospf-1]quit
```

RTBの設定：

```
[RTB]interface GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ip address 20.0.0.2 24
[RTB-GigabitEthernet0/0]quit
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ip address 10.0.0.2 24
[RTB-GigabitEthernet0/1]quit
[RTB]interface LoopBack 0
[RTB-LoopBack0]ip address 2.2.2.2 32
[RTB-LoopBack0]quit
[RTB]router id 2.2.2.2
[RTB]ospf 1
[RTB-ospf-1]area 0.0.0.0
```

[RTB-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]quit
[RTB-ospf-1]quit
%Nov 18 12:32:18:343 2021 RTB OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.0.0.1(GigabitEthernet0/1) changed from LOADING to FULL.
%Nov 18 12:32:27:344 2021 RTB OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.1(GigabitEthernet0/0) changed from LOADING to FULL.

手順3：OSPFネイバーとルーティングテーブルをチェックする

OSPFネイバーの状態をチェックするためにRTAで**display ospf peer**コマンドを実行します。

[RTA]display ospf peer

OSPF Process 1 with Router ID 1.1.1.1

Neighbor Brief Information

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
2.2.2.2	20.0.0.2	1	40	Full/BDR	GE0/0
2.2.2.2	10.0.0.2	1	37	Full/BDR	GE0/1

RTAは、RTB（ルーターID 2.2.2.2）と2つのネイバーシップを確立しました。 RTAのインターフェースGigabitEthernet 0/0は、ネットワークのDRであるRTBの20.0.0.2/24にあるインターフェースとのネイバーシップを確立します。 RTAのインターフェースGigabitEthernet0/1は、そのネットワークのDRであるRTBの10.0.0.0/24にあるインターフェースとのネイバーシップを確立します。

RTAでdisplay ospf Routingコマンドを実行して、OSPFルーティングテーブルを確認します。

[RTA]display ospf routing

OSPF Process 1 with Router ID 1.1.1.1

Routing Table

Topology base (MTID 0)

```
 Routing for network
 Destination        Cost      Type      NextHop          AdvRouter
Area
 20.0.0.0/24        1         Transit 0.0.0.0          1.1.1.1          0.0.0.0
 10.0.0.0/24        1         Transit 0.0.0.0          1.1.1.1          0.0.0.0
 2.2.2.2/32         1         Stub      10.0.0.2         2.2.2.2          0.0.0.0
 2.2.2.2/32         1         Stub      20.0.0.2         2.2.2.2          0.0.0.0
 1.1.1.1/32         0         Stub      0.0.0.0          1.1.1.1          0.0.0.0
 Total nets: 5
 Intra area: 5    Inter area: 0    ASE: 0    NSSA: 0
```

出力は、RTAにネットワーク2.2.2.2/32への2つのルートがあることを示しています。 1つはネイバー20.0.0.2によってアドバタイズされ、もう1つはネイバー10.0.0.1によってアドバタイズされます。 2つのルートのコストは同じです。

RTAで**display ip routing-table**コマンドを実行して、グローバルルーティングテーブルを表示します。

```
[RTA]display ip routing-table
Destinations : 18        Routes : 19
Destination/Mask    Proto   Pre Cost      NextHop         Interface
0.0.0.0/32          Direct  0   0         127.0.0.1       InLoop0
1.1.1.1/32          Direct  0   0         127.0.0.1       InLoop0
2.2.2.2/32          O_INTRA 10  1           10.0.0.2        GE0/1
                                            20.0.0.2        GE0/0
10.0.0.0/24         Direct  0   0         10.0.0.1        GE0/1
10.0.0.0/32         Direct  0   0         10.0.0.1        GE0/1
10.0.0.1/32         Direct  0   0         127.0.0.1       InLoop0
10.0.0.255/32       Direct  0   0         10.0.0.1        GE0/1
20.0.0.0/24         Direct  0   0         20.0.0.1        GE0/0
20.0.0.0/32         Direct  0   0         20.0.0.1        GE0/0
20.0.0.1/32         Direct  0   0         127.0.0.1       InLoop0
20.0.0.255/32       Direct  0   0         20.0.0.1        GE0/0
127.0.0.0/8         Direct  0   0         127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0         127.0.0.1       InLoop0
```

127.255.255.255/32 Direct 0 0 127.0.0.1 InLoop0
224.0.0.0/4 Direct 0 0 0.0.0.0 NULL0
224.0.0.0/24 Direct 0 0 0.0.0.0 NULL0
255.255.255.255/32 Direct 0 0 127.0.0.1 InLoop0

出力は、RTAが同じコストでネットワーク2.2.2.2/32への2つのルートを持っていることを示しています。

RTBで同様の操作を実行して、関連情報を確認します。

手順4：インターフェースのOSPF costを変更する

RTAのGigabitEthernet 0/0のOSPF costを150に設定します。

```
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ospf cost 150
[RTA-GigabitEthernet0/0]quit
```

手順5：ルーティングテーブルをチェックする

RTAで**display ospf Routing**コマンドを実行して、OSPFルーティングテーブルを確認します。

```
[RTA]display ospf routing

        OSPF Process 1 with Router ID 1.1.1.1
                Routing Table

            Topology base (MTID 0)

 Routing for network
 Destination        Cost      Type      NextHop         AdvRouter
Area
 20.0.0.0/24        150       Transit 0.0.0.0           1.1.1.1         0.0.0.0
 10.0.0.0/24        1         Transit 0.0.0.0           1.1.1.1         0.0.0.0
 2.2.2.2/32         1         Stub      10.0.0.2        2.2.2.2         0.0.0.0
 1.1.1.1/32         0         Stub      0.0.0.0         1.1.1.1         0.0.0.0

 Total nets: 4
 Intra area: 4  Inter area: 0  ASE: 0  NSSA: 0
```

RTAのインターフェースGigabitEthernet 0/0のospfコストは150に変更されます。これは、GigabitEthernet 0/1よりも高くなります。 したがって、RTAには、ネイバー10.0.0.2（RTAのGigabitEthernet 0/1に接続）によってアドバタイズされたネットワーク2.2.2.2/32へのルートが1つしかありません。

RTAで**display ip routing-table**コマンドを実行して、グローバルルーティングテーブルを表示します。

```
[RTA-GigabitEthernet0/0]display ip routing-table
Destinations : 18        Routes : 18

Destination/Mask    Proto   Pre  Cost      NextHop         Interface
0.0.0.0/32          Direct  0    0         127.0.0.1       InLoop0
1.1.1.1/32          Direct  0    0         127.0.0.1       InLoop0
2.2.2.2/32          O_INTRA 10   1           10.0.0.2        GE0/1
10.0.0.0/24         Direct  0    0         10.0.0.1        GE0/1
10.0.0.0/32         Direct  0    0         10.0.0.1        GE0/1
10.0.0.1/32         Direct  0    0         127.0.0.1       InLoop0
10.0.0.255/32       Direct  0    0         10.0.0.1        GE0/1
20.0.0.0/24         Direct  0    0         20.0.0.1        GE0/0
20.0.0.0/32         Direct  0    0         20.0.0.1        GE0/0
20.0.0.1/32         Direct  0    0         127.0.0.1       InLoop0
20.0.0.255/32       Direct  0    0         20.0.0.1        GE0/0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.0/32        Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
127.255.255.255/32  Direct  0    0         127.0.0.1       InLoop0
224.0.0.0/4         Direct  0    0         0.0.0.0         NULL0
224.0.0.0/24        Direct  0    0         0.0.0.0         NULL0
255.255.255.255/32  Direct  0    0         127.0.0.1       InLoop0
[RTA-GigabitEthernet0/0]quit
```

出力は、RTAがネットワーク2.2.2.2/32へのルートを1つだけ持っており、出力インターフェースがGigabitEthernet 0/1であることを示しています。

手順6：インターフェースのOSPF DRプライオリティを変更します。

RTBのインターフェースGigabitEthernet0/0のOSPFDR優先度を0に変更します。

```
[RTB]interface GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ospf dr-priority 0
[RTB-GigabitEthernet0/0]quit
%Nov 18 12:43:07:837 2021 RTB OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor
20.0.0.1(GigabitEthernet0/0) changed from FULL to DOWN.
```

%Nov 18 12:43:17:548 2021 RTB OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.1(GigabitEthernet0/0) changed from LOADING to FULL.

手順7：ルーター上でOSPFプロセスをリスタートさせる

OSPFプロセスをRTBでリスタートさせ、次いでRTAでリスタートさせます。

<RTB>reset ospf 1 process

Reset OSPF process? [Y/N]:y

<RTB>%Nov 18 12:47:16:519 2021 RTB OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.1(GigabitEthernet0/0) changed from FULL to DOWN.

%Nov 18 12:47:16:520 2021 RTB OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.0.0.1(GigabitEthernet0/1) changed from FULL to DOWN.

%Nov 18 12:47:17:605 2021 RTB OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.1(GigabitEthernet0/0) changed from LOADING to FULL.

%Nov 18 12:47:18:612 2021 RTB OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.0.0.1(GigabitEthernet0/1) changed from LOADING to FULL.

<RTA>

%Nov 18 12:43:07:328 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.2(GigabitEthernet0/0) changed from FULL to INIT.

%Nov 18 12:43:17:035 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.2(GigabitEthernet0/0) changed from LOADING to FULL.

%Nov 18 12:47:15:952 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.2(GigabitEthernet0/0) changed from FULL to INIT.

%Nov 18 12:47:15:953 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.0.0.2(GigabitEthernet0/1) changed from FULL to INIT.

%Nov 18 12:47:17:035 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.2(GigabitEthernet0/0) changed from LOADING to FULL.

%Nov 18 12:47:18:041 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.0.0.2(GigabitEthernet0/1) changed from LOADING to FULL.

<RTA>reset ospf 1 process

Reset OSPF process? [Y/N]:y

%Nov 18 12:48:43:126 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.2(GigabitEthernet0/0) changed from FULL to DOWN.

%Nov 18 12:48:43:127 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 10.0.0.2(GigabitEthernet0/1) changed from FULL to DOWN.

%Nov 18 12:48:49:957 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor

10.0.0.2(GigabitEthernet0/1) changed from LOADING to FULL.

%Nov 18 12:49:27:040 2021 RTA OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 20.0.0.2(GigabitEthernet0/0) changed from LOADING to FULL.

手順8：OSPFネイバーのステータスをチェックする

RTAで**display ospf peer**コマンドを実行して、OSPFネイバーの状態情報を確認します。

[RTA]display ospf peer

OSPF Process 1 with Router ID 1.1.1.1

Neighbor Brief Information

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
2.2.2.2	20.0.0.2	0	34	Full/DROther	GE0/0
2.2.2.2	10.0.0.2	1	35	Full/DR	GE0/1

RTBのインターフェースGigabitEthernet 0/0のDR優先度が0であるため、インターフェースはDR/BDR選出に参加できません。 再起動後、RTAのインターフェースGigabitEthernet 0/0はネットワークセグメントのDRになり、RTBのインターフェースGigabitEthernet 0/0はDRotherになります。

RTBで同様の操作を実行して、関連情報を確認します。

タスク3：基本的なOSPF複数エリアの設定をする

手順1：図12-3のようにlab環境を構築する

最初に、ラボ図に示されているようにラボ環境を確立します。 次に、クライアントAのIPアドレスを10.0.0.1/24として構成し、ゲートウェイアドレスを10.0.0.2として指定します。クライアントBのIPアドレスを10.1.0.1/24として構成し、ゲートウェイアドレスを10.1.0.2として指定します。

手順2：基本的な設定をします

ルーターインターフェースのIPアドレスの設定とOSPFの設定

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]ip address 20.0.0.1 24

[RTA-GigabitEthernet0/0]quit

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]ip address 10.0.0.2 24

[RTA-GigabitEthernet0/1]quit

[RTA]int

[RTA]interface lo

```
[RTA]interface LoopBack 0
[RTA-LoopBack0]ip address 1.1.1.1 32
[RTA-LoopBack0]quit
[RTA]router
[RTA]router id 1.1.1.1
[RTA]ospf 1
[RTA-ospf-1]area 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 1.1.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0]network 10.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]quit
[RTA-ospf-1]quit

[RTB]interface GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ip address 20.0.0.2 24
[RTB-GigabitEthernet0/0]quit
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ip address 30.0.0.2 24
[RTB-GigabitEthernet0/1]quit
[RTB]interface LoopBack 0
[RTB-LoopBack0]ip address 2.2.2.2 32
[RTB-LoopBack0]quit
[RTB]router id 2.2.2.2
[RTB]ospf 1
[RTB-ospf-1]area 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 2.2.2.2 0.0.0.0
[RTB-ospf-1-area-0.0.0.0]network 20.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]quit
%Nov 18 14:46:19:795 2021 RTB OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor
20.0.0.1(GigabitEthernet0/0) changed from LOADING to FULL.
[RTB-ospf-1]area 1
[RTB-ospf-1-area-0.0.0.1]network 30.0.0.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.1]quit
[RTB-ospf-1]quit

[RTC]interface GigabitEthernet 0/0
```

[RTC-GigabitEthernet0/0]ip address 30.0.0.1 24
[RTC-GigabitEthernet0/0]quit
[RTC]interface GigabitEthernet 0/1
[RTC-GigabitEthernet0/1]ip address 10.1.0.2 24
[RTC-GigabitEthernet0/1]quit
[RTC]interface LoopBack 0
[RTC-LoopBack0]ip address 3.3.3.3 32
[RTC-LoopBack0]quit
[RTC]router id 3.3.3.3
[RTC]ospf 1
[RTC-ospf-1]area 1
[RTC-ospf-1-area-0.0.0.1]network 3.3.3.3 0.0.0.0
[RTC-ospf-1-area-0.0.0.1]network 10.1.0.0 0.0.0.255
[RTC-ospf-1-area-0.0.0.1]network 30.0.0.0 0.0.0.255
[RTC-ospf-1-area-0.0.0.1]quit
[RTC-ospf-1]quit

手順3：OSPFネイバーとルーティングテーブルをチェックする

RTAで**display ospf peer**コマンドを実行して、OSPFネイバーの状態情報を確認します。

[RTB]dis ospf peer

OSPF Process 1 with Router ID 2.2.2.2

Neighbor Brief Information

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
1.1.1.1	20.0.0.1	1	34	Full/DR	GE0/0

Area: 0.0.0.1

Router ID	Address	Pri	Dead-Time	State	Interface
3.3.3.3	30.0.0.1	1	32	Full/BDR	GE0/1

RTBとRTA（ルーターID 1.1.1.1）はエリア0にあります。RTBのインターフェースGigabitEthernet 0/0は、ネットワークのDRであるRTAの20.0.0.1/24にインターフェースとのネイバーシップを確立しました。

RTBとRTC（ルーターID 3.3.3.3）はエリア1にあります。RTBのインターフェースGigabitEthernet 0/1は、RTCの30.0.0.1/24のインターフェースとのネイバーシップを確

立します。 これはネットワークのDRです

RTBで**display ospf routing**コマンドを実行して、OSPFルーティングテーブルを確認します。

```
[RTB]display ospf routing
          OSPF Process 1 with Router ID 2.2.2.2
                    Routing Table

                Topology base (MTID 0)

 Routing for network
 Destination        Cost      Type      NextHop          AdvRouter
Area
 20.0.0.0/24        1         Transit 0.0.0.0          1.1.1.1          0.0.0.0
 10.0.0.0/24        2         Stub      20.0.0.1         1.1.1.1          0.0.0.0
 3.3.3.3/32         1         Stub      30.0.0.1         3.3.3.3          0.0.0.1
 2.2.2.2/32         0         Stub      0.0.0.0          2.2.2.2          0.0.0.0
 10.1.0.0/24        2         Stub      30.0.0.1         3.3.3.3          0.0.0.1
 30.0.0.0/24        1         Transit 0.0.0.0          2.2.2.2          0.0.0.1
 1.1.1.1/32         1         Stub      20.0.0.1         1.1.1.1          0.0.0.0

 Total nets: 7
 Intra area: 7  Inter area: 0  ASE: 0  NSSA: 0
```

RTBには、OSPFルーティングテーブル内のすべてのネットワークへのルートがあります。

RTBで**display ip routing-table**コマンドを実行して、グローバルルーティングテーブルを表示します。

```
[RTB]display ip routing-table
Destinations : 21        Routes : 21

Destination/Mask    Proto   Pre  Cost      NextHop         Interface
0.0.0.0/32          Direct  0    0         127.0.0.1       InLoop0
1.1.1.1/32          O_INTRA 10   1           20.0.0.1        GE0/0
2.2.2.2/32          Direct  0    0         127.0.0.1       InLoop0
3.3.3.3/32          O_INTRA 10   1           30.0.0.1        GE0/1
10.0.0.0/24         O_INTRA 10   2           20.0.0.1        GE0/0
```

10.1.0.0/24	O_INTRA	10	2	30.0.0.1	GE0/1
20.0.0.0/24	Direct	0	0	20.0.0.2	GE0/0
20.0.0.0/32	Direct	0	0	20.0.0.2	GE0/0
20.0.0.2/32	Direct	0	0	127.0.0.1	InLoop0
20.0.0.255/32	Direct	0	0	20.0.0.2	GE0/0
30.0.0.0/24	Direct	0	0	30.0.0.2	GE0/1
30.0.0.0/32	Direct	0	0	30.0.0.2	GE0/1
30.0.0.2/32	Direct	0	0	127.0.0.1	InLoop0
30.0.0.255/32	Direct	0	0	30.0.0.2	GE0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

RTBのグローバルルーティングテーブルには、すべてのネットワークへのルートがあります。 RTAで同様の操作を実行して、関連情報を確認します。

手順4：ネットワークの接続性をチェックする

次の出力について、Client AからClient B（10.1.0.1）にpingを実行します。

```
<Client A>ping 10.1.0.1
Ping 10.1.0.1 (10.1.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.0.1: icmp_seq=0 ttl=252 time=5.000 ms
56 bytes from 10.1.0.1: icmp_seq=1 ttl=252 time=7.000 ms
56 bytes from 10.1.0.1: icmp_seq=2 ttl=252 time=7.000 ms
56 bytes from 10.1.0.1: icmp_seq=3 ttl=252 time=8.000 ms
56 bytes from 10.1.0.1: icmp_seq=4 ttl=252 time=8.000 ms
```

次の出力について、Client BからClient A（10.0.0.1）にpingを実行します。

```
<Client B>ping 10.0.0.1
Ping 10.0.0.1 (10.0.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.0.0.1: icmp_seq=0 ttl=252 time=4.000 ms
56 bytes from 10.0.0.1: icmp_seq=1 ttl=252 time=7.000 ms
56 bytes from 10.0.0.1: icmp_seq=2 ttl=252 time=6.000 ms
56 bytes from 10.0.0.1: icmp_seq=3 ttl=252 time=6.000 ms
56 bytes from 10.0.0.1: icmp_seq=4 ttl=252 time=7.000 ms
```

質問:
1. ラボタスク2のステップ4で、RTAのインターフェースGigabitEthernet0 / 0のOSPFコストが変更されます。 RTBは、RTAに接続されたネットワーク1.1.1.1/32へのルーティングテーブルにいくつのルートを持っていますか。その理由は何ですか。

答え:
2つの等コストルートが利用可能です。 RTAのGigabitEthernet0 / 0で行われたコスト変更は、RTBではなくRTAでのルート計算にのみ影響します。

2. OSPFエリア内の指定されたネットワークに接続されたインターフェースでOSPFを有効にするには、ルーターID構成を含める必要がありますか？

答え:
いいえ。 指定されたルーターIDは、アドバタイズルーターのループバックインターフェースアドレスです。

3. インターフェースにOSPFコストを設定して、ルートバックアップを実装するにはどうすればよいですか。

答え:
ospf costコマンドを使用して、バックアップインターフェースのコストをプライマリインターフェースのコストよりも大きい値に設定します。 プライマリインターフェースに障害が発生すると、バックアップインターフェースが使用されます。

Lab13 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

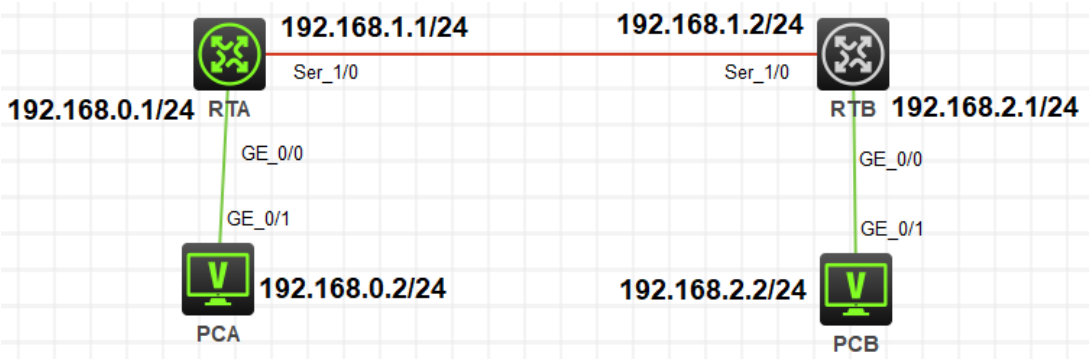


図 13.1 実習ネットワーク

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	**インターフェース**	**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？

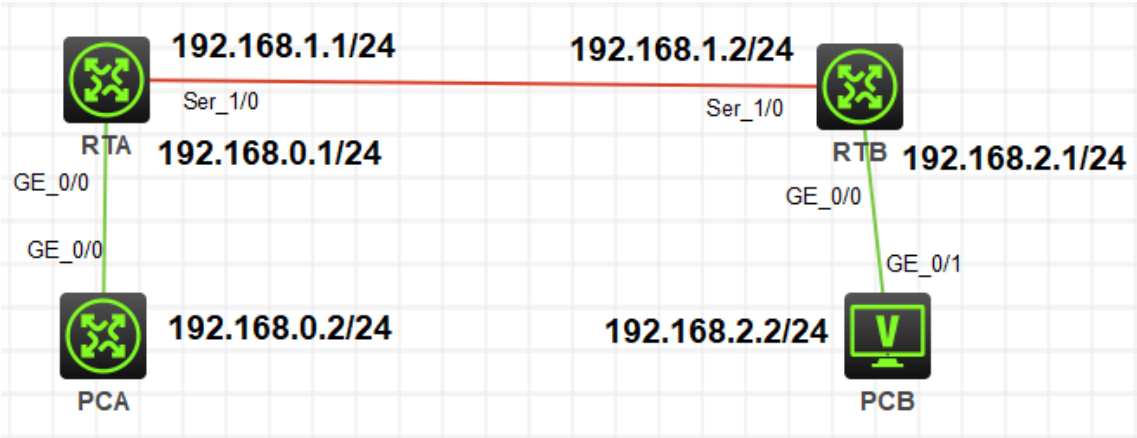
答え:

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



Lab14 Layer 3 マルチキャスト

実習内容と目標

このラボでは以下のことを学びます:

- 基本的な IGMP のコンフィグレーションを実行する。
- 基本的な PIM-DM のコンフィグレーションを実行する。
- 基本的な PIM-SM のコンフィグレーションを実行する。
- Layer 3 マルチキャストの表示と管理。

ネットワーク図

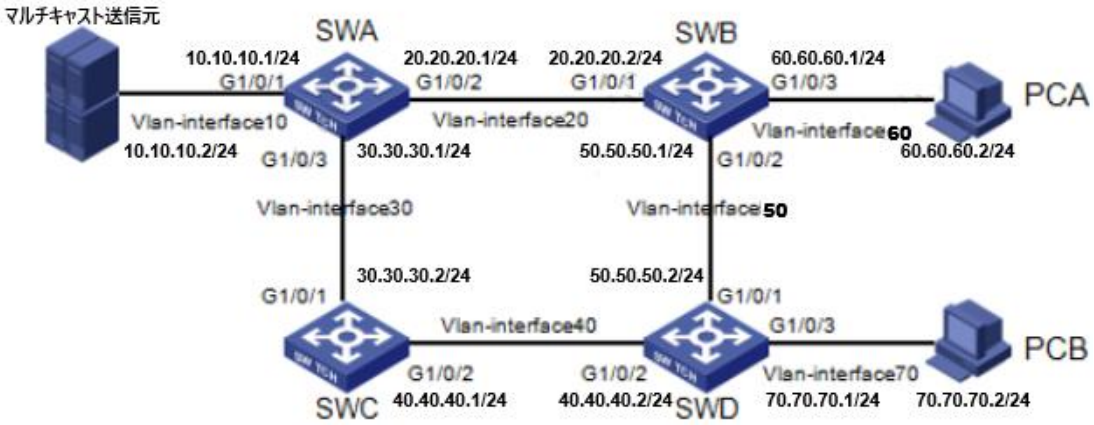


図 14.1 実習ネットワーク

表 14.1 インターフェースと IP アドレス

装置	インターフェース	IPアドレス	装置	インターフェース	IPアドレス
SWA	Vlan-int10	10.10.10.1/24	SWD	Vlan-int40	40.40.40.2/24
	Vlan-int20	20.20.20.1/24		Vlan-int50	50.50.50.2/24
	Vlan-int30	30.30.30.1/24		Vlan-int70	70.70.70.1/24
SWB	Vlan-int20	20.20.20.2/24	PCA		60.60.60.2
	Vlan-int50	50.50.50.1/24	PCB		70.70.70.2
	Vlan-int60	60.60.60.1/24	マルチキャスト送信元		10.10.10.2
SWC	Vlan-int30	30.30.30.2/24			
	Vlan-int40	40.40.40.1/24			

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
S5820V2-54QS-GE	Version7.10	4	なし
PC	Windows 11	3	なし
ネットワークケーブルの接続	--	7	なし

実習手順

タスク1: PIM-DMを構成します。

スイッチにPIM-DMを構成します。スイッチではIGMPv2が稼働しています。PIM-DMは受信者が多く存在することを前提として全方向に送信し、受信者がいないネットワークからは停止要求が送られ、不要な経路は停止されます。

手順1:IPアドレスとユニキャストルーティングを構成します。

- 図13-1に沿ってVLANインターフェースを作成し、IPアドレスとサブネットマスクを設定します。この作業の詳細は省略します。
- 全てのスイッチでOSPFを構成し、スイッチ間でPIM-DMドメインがネットワーク層で

到達可能で、ユニキャストルーティングプロトコルで動的なルーティングの更新が行われるようにします。

```
[SWA] interface LoopBack 0
[SWA-LoopBack0] ip address 1.1.1.1 32
[SWA-LoopBack0] quit
[SWA] router id 1.1.1.1
[SWA] ospf 1
[SWA-ospf-1] area 0
[SWA-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[SWA-ospf-1-area-0.0.0.0] network 10.10.10.0 0.0.0.255
[SWA-ospf-1-area-0.0.0.0] network 20.20.20.0 0.0.0.255
[SWA-ospf-1-area-0.0.0.0] network 30.30.30.0 0.0.0.255
[SWA-ospf-1-area-0.0.0.0] quit
[SWA-ospf-1] quit
[SWB]interface LoopBack 0
[SWB-LoopBack0] ip address 2.2.2.2 32
[SWB-LoopBack0] quit
[SWB] router id 2.2.2.2
[SWB] ospf 1
[SWB-ospf-1] area 0
[SWB-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[SWB-ospf-1-area-0.0.0.0] network 20.20.20.0 0.0.0.255
[SWB-ospf-1-area-0.0.0.0] network 50.50.50.0 0.0.0.255
[SWB-ospf-1-area-0.0.0.0] network 60.60.60.0 0.0.0.255
[SWB-ospf-1-area-0.0.0.0] quit
[SWB-ospf-1] quit
[SWC]interface LoopBack 0
[SWC-LoopBack0] ip address 3.3.3.3 32
[SWC-LoopBack0] quit
[SWC] router id 3.3.3.3
[SWC] ospf 1
[SWC-ospf-1] area 0
[SWC-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[SWC-ospf-1-area-0.0.0.0] network 30.30.30.0 0.0.0.255
[SWC-ospf-1-area-0.0.0.0] network 40.40.40.0 0.0.0.255
```

[SWC-ospf-1-area-0.0.0.0] quit
[SWC-ospf-1]quit
[SWD] interface LoopBack 0
[SWD-LoopBack0] ip address 4.4.4.4 32
[SWD-LoopBack0] quit
[SWD]router id 4.4.4.4
[SWD]ospf 1
[SWD-ospf-1]area 0
[SWD-ospf-1-area-0.0.0.0] network 4.4.4.4 0.0.0.0
[SWD-ospf-1-area-0.0.0.0] network 40.40.40.0 0.0.0.255
[SWD-ospf-1-area-0.0.0.0] network 50.50.50.0 0.0.0.255
[SWD-ospf-1-area-0.0.0.0] network 70.70.70.0 0.0.0.255
[SWD-ospf-1-area-0.0.0.0] quit

手順2：Layer 3マルチキャストを有効にする。

multicast routingコマンドを使って各スイッチでLayer 3マルチキャストルーティングを有効にする

[SWA] multicast routing
[SWB] multicast routing
[SWC] multicast routing
[SWD] multicast routing

手順3：IGMPを有効にする。

igmp enableコマンドを使って、受信者が接続されているVLANインターフェースでIGMPを有効にする

[SWB] interface vlan 60
[SWB-Vlan-interface60] igmp enable
[SWB-Vlan-interface60] quit
[SWD] interface vlan 70
[SWD-Vlan-interface70] igmp enable
[SWD-Vlan-interface70] quit

手順4：PIM-DMを有効にする。

pim dmコマンドを使って各スイッチのLayer 3インターフェースでPIM-DMを有効にする。

[SWA-Vlan-interface10] pim dm
[SWA-Vlan-interface20] pim dm
[SWA-Vlan-interface30] pim dm
[SWB-Vlan-interface20] pim dm
[SWB-Vlan-interface50] pim dm

[SWC-Vlan-interface30] pim dm

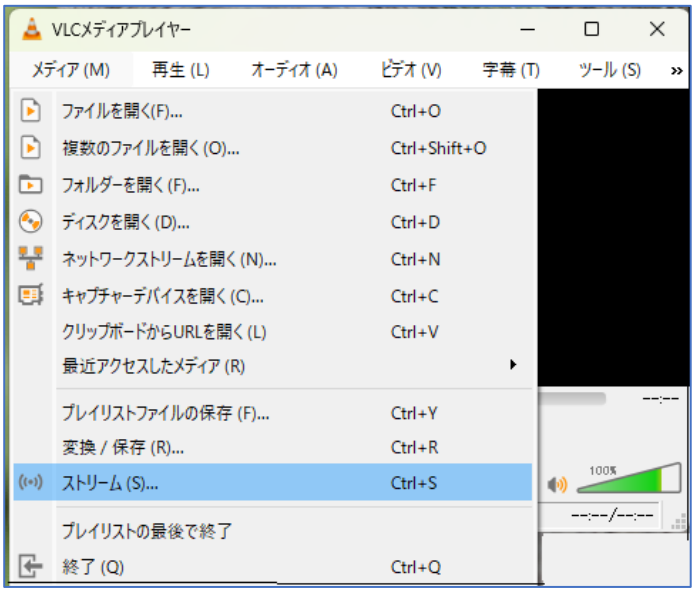
[SWC-Vlan-interface40] pim dm

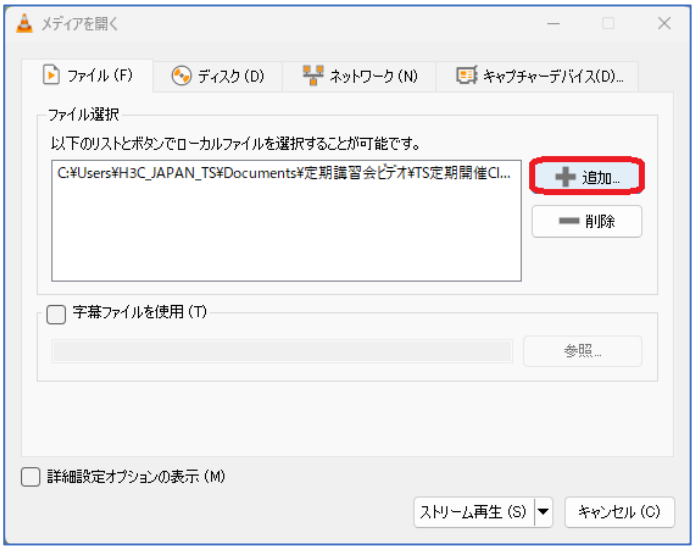
[SWD-Vlan-interface40] pim dm

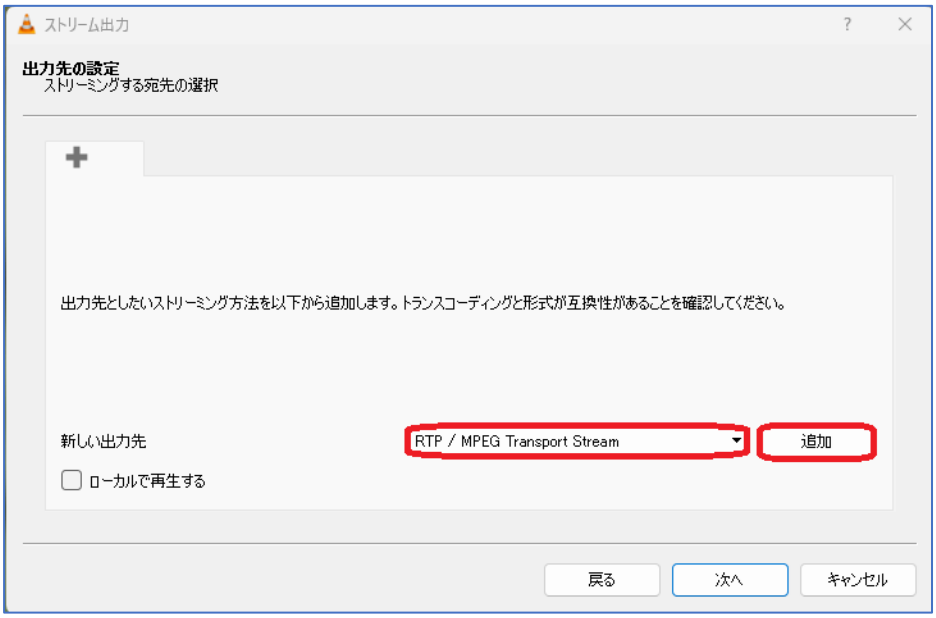
[SWD-Vlan-interface50] pim dm

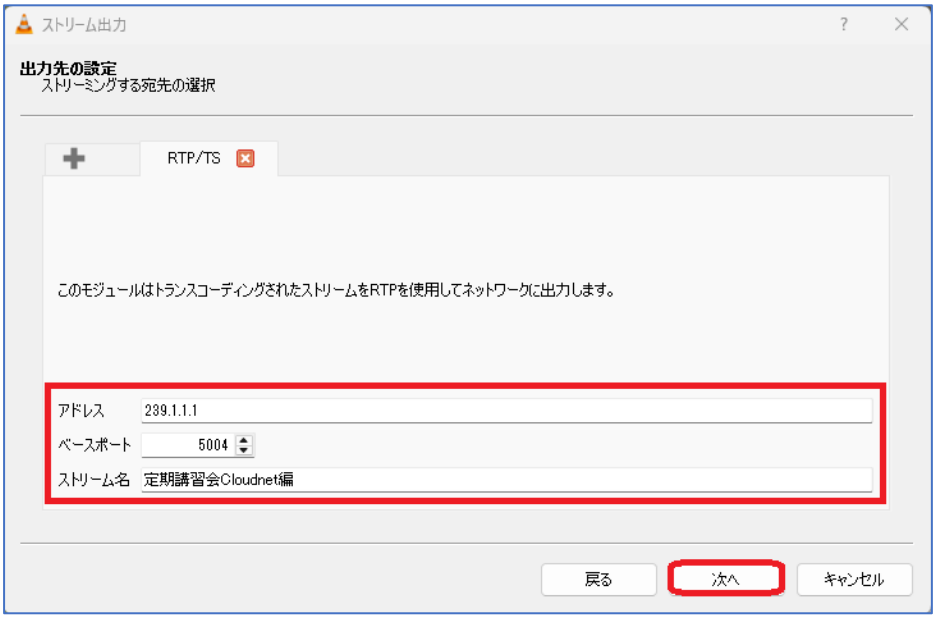
手順5:マルチキャストトラフィックの送受信。

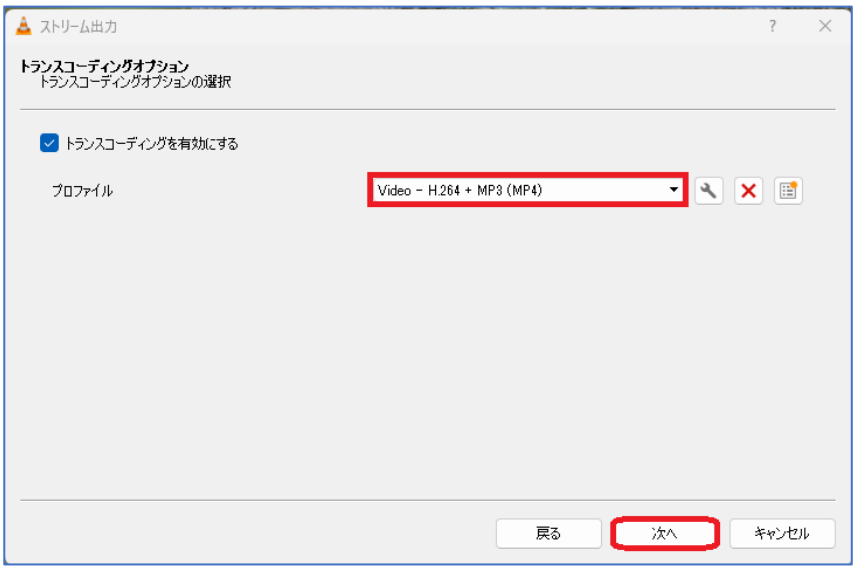
- マルチキャストの送信元装置でマルチキャストトラフィックを送信するのにVLCツールを使用します。また、マルチキャストトラフィックを受信するPCAとPCBでは、同じくVLCツールを使って行います。
- VLCで送信する手順は以下の通りです。

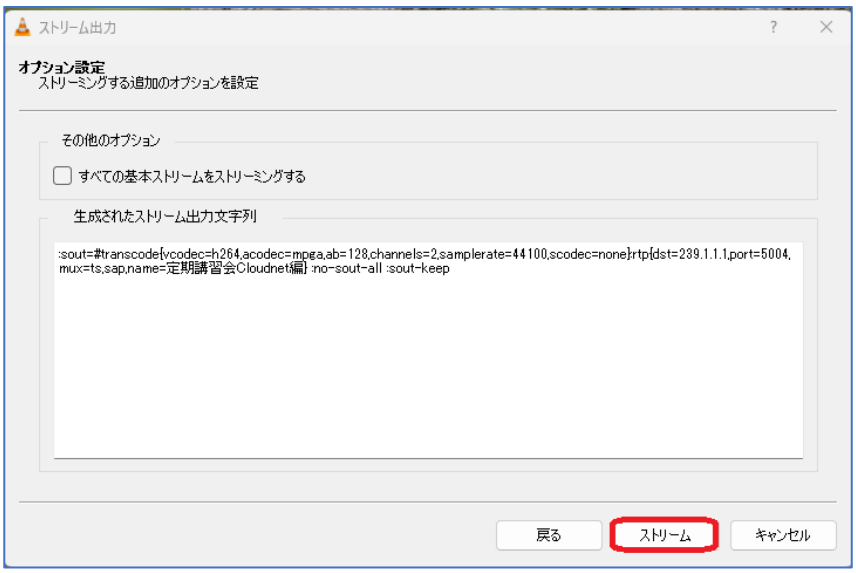




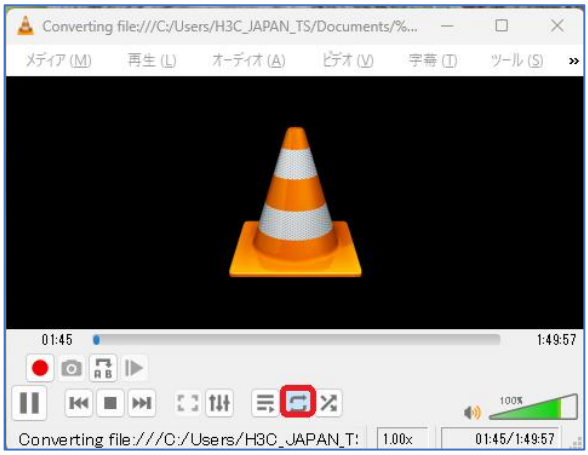

ストリーム出力
出力先の設定
ストリーミングする宛先の選択
出力先としたいストリーミング方法を以下から追加します。トランスコーディングと形式が互換性があることを確認してください。
新しい出力先
RTP / MPEG Transport Stream
追加
ローカルで再生する
戻る
次へ
キャンセル


ストリーム出力
出力先の設定
ストリーミングする宛先の選択
RTP/TS
このモジュールはトランスコーディングされたストリームをRTPを使用してネットワークに出力します。
アドレス
239.1.1.1
ベースポート
5004
ストリーム名
定期講習会Cloudnet編
戻る
次へ
キャンセル

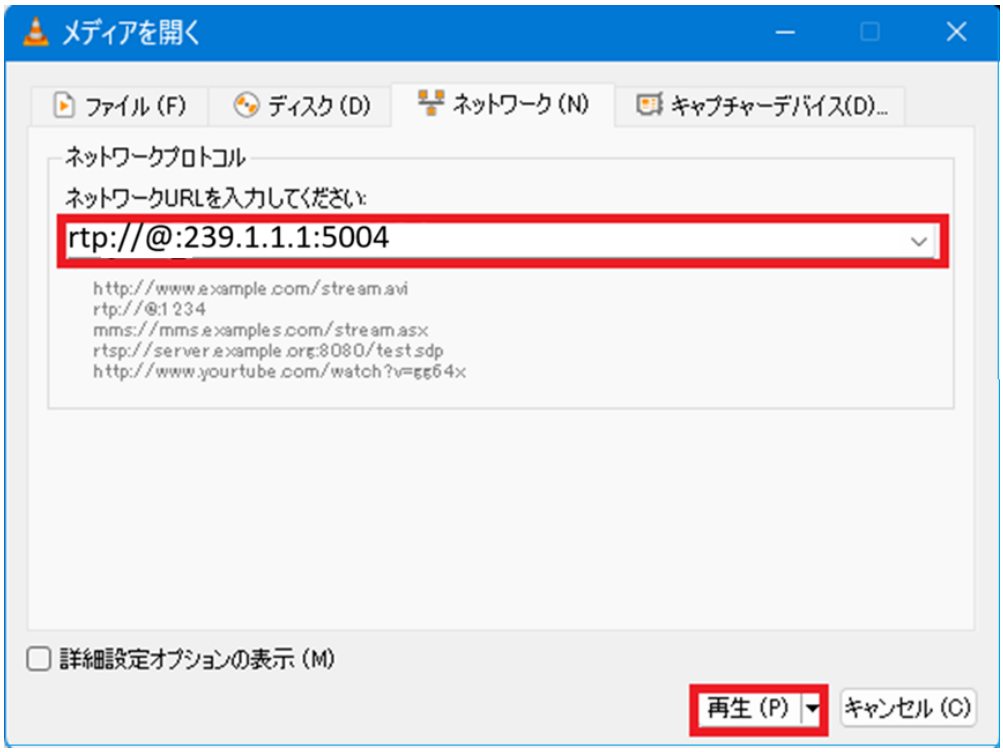

ストリーム出力
トランスコーディングオプション
トランスコーディングオプションの選択
トランスコーディングを有効にする
プロファイル
Video - H.264 + MP3 (MP4)
戻る
次へ
キャンセル


ストリーム出力
オプション設定
ストリーミングする追加のオプションを設定
その他のオプション
すべての基本ストリームをストリーミングする
生成されたストリーム出力文字列
:sout=#transcode{vcodec=h264,acodec=mpga,ab=128,channels=2,samplerate=44100,scodec=none}:rtp{dst=239.1.1.1,port=5004,mux=ts,sap,name=定期講習会Cloudnet編} :no-sout-all :sout-keep
戻る
ストリーム
キャンセル

配信中


Converting file:///C:/Users/H3C_JAPAN_TS/Documents/%...
メディア (M)
再生 (L)
オーディオ (A)
ビデオ (V)
字幕 (T)
ツール (S)
01:45
1:49:57
100%
Converting file:///C:/Users/H3C_JAPAN_T:
1.00x
01:45/1:49:57

- VLCで受信する手順は以下の通りです。



手順6：マルチキャスト関連の情報の表示。

VLCツールでマルチキャストデータを正常に受信出来たら、各スイッチでマルチキャスト関連の情報を表示します。

- SWBとSWDでdisplay igmp groupコマンドを使って、マルチキャストグループの情報を表示します。

<SWB>display igmp group

IGMP groups in total: 1

Vlan-interface60(60.60.60.1):

IGMP groups reported in total: 1

Group address	Last reporter	Uptime	Expires
239.255.255.250	60.60.60.2	00:11:07	00:03:35

<SWD>display igmp group

IGMP groups in total: 1

Vlan-interface70(70.70.70.1):

IGMP groups reported in total: 1

Group address	Last reporter	Uptime	Expires
239.255.255.250	70.70.70.2	00:11:07	00:03:35

結果はSWBとSWDマルチキャストグループ239.255.255.250でメンバーのIPアドレスが60.60.60.2と70.70.70.2です。

- Display pim neighborコマンドを使って、各スイッチのPIMネイバー情報を表示します。例えば、SWAの出力はSWAは2つのPIMネイバー(SWBとSWC)を持ち、VLAN-interface 20とVLAN-interface 30に接続されています。

<SWA>dis pim neighbor

Total Number of Neighbors = 2

Neighbor	Interface	Uptime	Expires	DR-Priority	Mode
20.20.20.2	Vlan20	00:08:29	00:01:22	1	P
30.30.30.2	Vlan30	00:05:50	00:01:38	1	P

- display pim routing-tableコマンドを使って、PIMのルーティングテーブル情報を表示します。PIMルーティングテーブルはPIMプロトコルによって作成され、テーブルは幾つかの(*, G)エントリーと(S, G)を含んでいます。

<SWB>display pim routing-table

Total 1 (*, G) entries; 2 (S, G) entries

(10.10.10.2, 239.1.1.1)

Protocol: pim-dm, Flag:

UpTime: 00:07:59

Upstream interface: Vlan-interface20

Upstream neighbor: 20.20.20.1

RPF prime neighbor: 20.20.20.1

Downstream interface information: None

(*, 239.255.255.250)
Protocol: pim-dm, Flag: WC
UpTime: 00:10:03
Upstream interface: NULL
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface information:
Total number of downstream interfaces: 1
1: Vlan-interface60
Protocol: igmp, UpTime: 00:10:03, Expires: -

(10.10.10.2, 239.255.255.250)
Protocol: pim-dm, Flag:
UpTime: 00:30:24
Upstream interface: Vlan-interface20
Upstream neighbor: 20.20.20.1
RPF prime neighbor: 20.20.20.1
Downstream interface information:
Total number of downstream interfaces: 1
1: Vlan-interface60
Protocol: pim-dm, UpTime: 00:10:03, Expires: -

SWDとSWBのPIMルーティングテーブルは同様です。なぜならば、SWAとSWCはどの受信者とも直接に接続されていないので、ルーティングテーブルは(*, G)のエントリーを含んでいません。

- display multicast routing-tableコマンドを使って、マルチキャストルーティングテーブルを表示します。以下の出力はSWAのものですが、他のスイッチの出力も同様です。

<SWA>dis multicast routing-table
Total 2 entries

00001. (10.10.10.2, 239.1.1.1)
Uptime: 00:05:20
Upstream Interface: Vlan-interface10

00002. (10.10.10.2, 239.255.255.250)
Uptime: 00:03:42

Upstream Interface: Vlan-interface10
List of 1 downstream interfaces
1: Vlan-interface20

- display multicast forwarding-tableコマンドを使って、マルチキャスト転送テーブルを表示します。以下の出力はSWAでのコマンドによるものですが、その他のスイッチの出力も同様です。

<SWA>dis multicast forwarding-table
Total 3 entries, 3 matched

00001. (10.10.10.2, 239.1.1.1)
Flags: 0x0
Uptime: 00:05:08, Timeout in: 00:03:24
Incoming interface: Vlan-interface10
Matched 13798 packets(18625400 bytes), Wrong If 0 packets
Forwarded 0 packets

00002. (10.10.10.2, 239.255.255.250)
Flags: 0x0
Uptime: 00:03:31, Timeout in: 00:02:09
Incoming interface: Vlan-interface10
List of 1 outgoing interfaces:
1: Vlan-interface20
Matched 22 packets(18567 bytes), Wrong If 0 packets
Forwarded 3 packets(495 bytes)

00003. (60.60.60.3, 239.255.255.250)
Flags: 0x0
Uptime: 00:03:31, Timeout in: 00:00:09
Incoming interface: Vlan-interface20
Matched 1 packets(165 bytes), Wrong If 0 packets
Forwarded 1 packets(165 bytes)

タスク2：PIM-SMを構成します。

スイッチにPIM-SMを構成します。スイッチではIGMPv2が稼働しています。PIM-SMは受信したいクライアントのみに送信するため無駄なトラフィックがないため、大規模なネットワークに適しています。受信したいクライアントはJoinメッセージを送信します。PIM-SMではルーターはRP（Rendezvous Point）に接続し、RPを中心にマルチキャストツリーを形成します。

手順1：IPアドレスとユニキャストルーティングを構成します。

- 図13-1に沿ってVLANインターフェースを作成し、IPアドレスとサブネットマスクを設定します。この作業の詳細は省略します。
- 全てのスイッチでOSPFを構成し、スイッチ間でPIM-DMドメインがネットワーク層で到達可能で、ユニキャストルーティングプロトコルで動的なルーティングの更新が行われるようにします。この手順はタスク1で示した構成と同じですので作業の説明は省略します。

手順2：Layer 3マルチキャストを有効にします。

Multicast routing-enableコマンドを使って、各スイッチでLayer 3マルチキャストルーティングを有効にします。

[SWA] multicast routing

[SWB] multicast routing

[SWC] multicast routing

[SWD] multicast routing

手順3：IGMPを有効にします。

受信者が接続されているVLAN InterfaceをIGMPを有効にします。

[SWB-Vlan-interface60] igmp enable

[SWD-Vlan-interface70] igmp enable

手順4：PIM-SMを構成します。

- pim smコマンドを使ってスイッチのLayer 3インターフェースでPIM-SMを有効にします。

[SWA-Vlan-interface10] pim sm

[SWA-Vlan-interface20] pim sm

[SWA-Vlan-interface30] pim sm

SWB, SWC, SWDも構成は同じです。従って、構成手順は省略します。

- PIMドメインでSWCをC-RPとC-BSRとして構成します。実際には、インターフェースがダウンしたときに開始される RP と BSR の再選択を回避するために、デバイスのループバック インターフェースを C-RP および C-BSR として設定します。

[SWC] pim
[SWC-pim] c-rp 3.3.3.3
[SWC-pim] c-bsr 3.3.3.3

手順5：マルチキャストトラフィックを送受信します。

この操作はタスク1の手順5と同じなので省略します。

手順6：マルチキャスト関連の情報を表示します。

[SWA]dis pim routing-table

Total 0 (*, G) entries; 2 (S, G) entries

(10.10.10.2, 239.1.1.1)
RP: NULL
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 00:20:57
Upstream interface: Vlan-interface10
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface information: None

(10.10.10.2, 239.255.255.250)
RP: NULL
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 00:01:49
Upstream interface: Vlan-interface10
Upstream neighbor: NULL
RPF prime neighbor: NULL
Downstream interface information: None

[SWA]dis multicast routing-table

Total 2 entries

00001. (10.10.10.2, 239.1.1.1)
Uptime: 00:21:58
Upstream Interface: Vlan-interface10

00002. (10.10.10.2, 239.255.255.250)
Uptime: 00:02:50
Upstream Interface: Vlan-interface10

[SWA]dis multicast forwarding-table

Total 2 entries, 2 matched

00001. (10.10.10.2, 239.1.1.1)

Flags: 0x0

Uptime: 00:22:29, Timeout in: 00:03:26

Incoming interface: Vlan-interface10

Matched 65933 packets(89010780 bytes), Wrong If 0 packets

Forwarded 0 packets

00002. (10.10.10.2, 239.255.255.250)

Flags: 0x0

Uptime: 00:03:21, Timeout in: 00:00:26

Incoming interface: Vlan-interface10

Matched 23 packets(11144 bytes), Wrong If 0 packets

Forwarded 12 packets(1928 bytes)

<SWB>display igmp group

IGMP groups in total: 1

Vlan-interface60(60.60.60.1):

IGMP groups reported in total: 1

Group address	Last reporter	Uptime	Expires
239.255.255.250	60.60.60.2	00:11:07	00:03:35

<SWD>display igmp group

IGMP groups in total: 1

Vlan-interface70(70.70.70.1):

IGMP groups reported in total: 1

Group address	Last reporter	Uptime	Expires
239.255.255.250	70.70.70.2	00:11:07	00:03:35

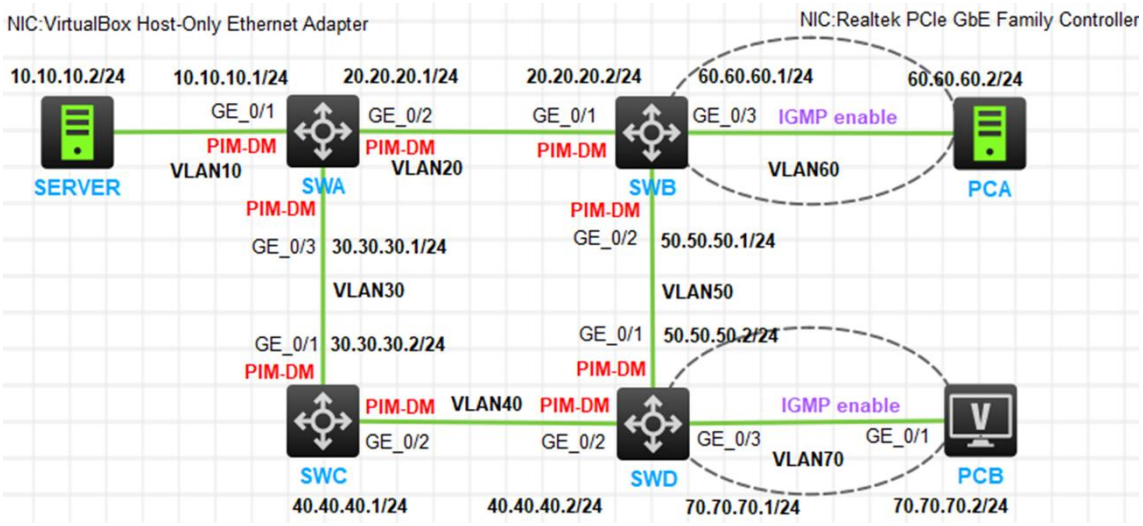
[SWA]display pim rp-info

[SWA]display pim bsr-info

Scope: non-scoped

State: Accept Any

構成サマリー(マルチキャスト部分を抽出)PIM-DM



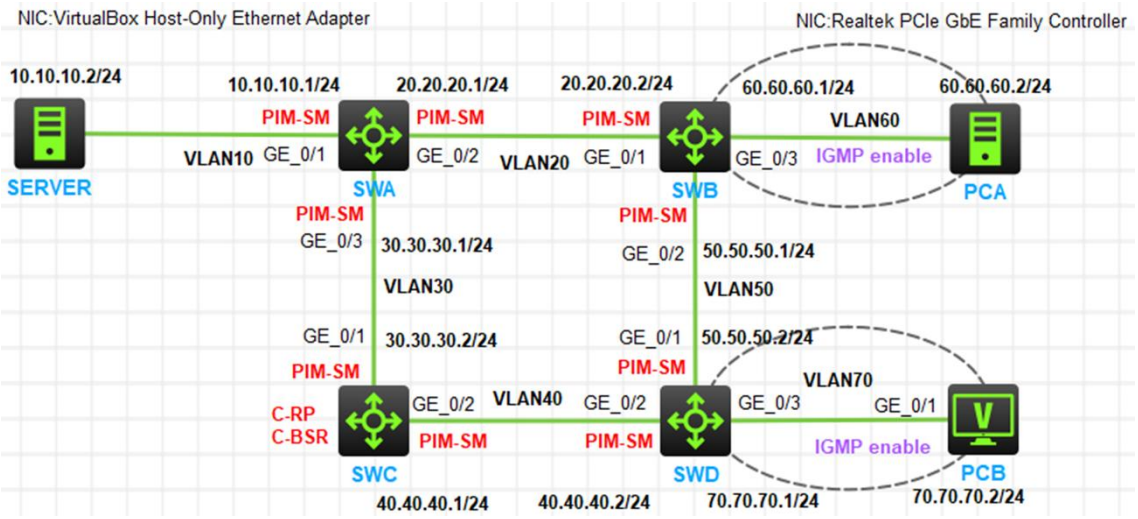

```
############################################################
# SWA
############################################################
vlan 1
vlan 10
vlan 20
vlan 30
#
interface Vlan-interface10
 ip address 10.10.10.1 255.255.255.0
 pim dm
#
interface Vlan-interface20
 ip address 20.20.20.1 255.255.255.0
 pim dm
#
interface Vlan-interface30
 ip address 30.30.30.1 255.255.255.0
 pim dm
#
interface GigabitEthernet1/0/1
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port access vlan 20
#
interface GigabitEthernet1/0/3
port access vlan 30
#
multicast routing
#
```

```
#########################################################
# SWB
#########################################################
vlan 1
vlan 20
vlan 50
vlan 60
#
interface Vlan-interface20
 ip address 20.20.20.2 255.255.255.0
 pim dm
#
interface Vlan-interface50
 ip address 50.50.50.1 255.255.255.0
 pim dm
#
interface Vlan-interface60
 ip address 60.60.60.1 255.255.255.0
 igmp enable
#
interface GigabitEthernet1/0/1
 port access vlan 20
#
interface GigabitEthernet1/0/2
 port access vlan 50
#
interface GigabitEthernet1/0/3
 port access vlan 60
#
multicast routing
#
```

```
#######################################################
# SWC
#######################################################
vlan 1
vlan 30
vlan 40
#
interface Vlan-interface30
 ip address 30.30.30.2 255.255.255.0
 pim dm
#
interface Vlan-interface40
 ip address 40.40.40.1 255.255.255.0
 pim dm
#
interface GigabitEthernet1/0/1
 port access vlan 30
#
interface GigabitEthernet1/0/2
 port access vlan 40
#
multicast routing
#
```

```
#############################################################
# SWD
#############################################################
vlan 1
vlan 40
vlan 50
vlan 70
#
interface Vlan-interface40
 ip address 40.40.40.2 255.255.255.0
 pim dm
#
interface Vlan-interface50
 ip address 50.50.50.2 255.255.255.0
 pim dm
#
interface Vlan-interface70
 ip address 70.70.70.1 255.255.255.0
 igmp enable
#
interface GigabitEthernet1/0/1
 port access vlan 50
#
interface GigabitEthernet1/0/2
 port access vlan 40
#
interface GigabitEthernet1/0/3
 port access vlan 70
#
multicast routing
#
```

構成サマリー(マルチキャスト部分を抽出)PIM-SM




```
############################################################
# SWA
############################################################
vlan 1
vlan 10
vlan 20
vlan 30
#
interface Vlan-interface10
 ip address 10.10.10.1 255.255.255.0
 pim sm
#
interface Vlan-interface20
 ip address 20.20.20.1 255.255.255.0
 pim sm
#
interface Vlan-interface30
 ip address 30.30.30.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/1
 port access vlan 10
#
interface GigabitEthernet1/0/2
 port access vlan 20
#
interface GigabitEthernet1/0/3
port access vlan 30
#
multicast routing
#
```

```
#########################################################
# SWB
#########################################################
vlan 1
vlan 20
vlan 50
vlan 60
#
interface Vlan-interface20
 ip address 20.20.20.2 255.255.255.0
 pim sm
#
interface Vlan-interface50
 ip address 50.50.50.1 255.255.255.0
 pim sm
#
interface Vlan-interface60
 ip address 60.60.60.1 255.255.255.0
 igmp enable
#
interface GigabitEthernet1/0/1
 port access vlan 20
#
interface GigabitEthernet1/0/2
 port access vlan 50
#
interface GigabitEthernet1/0/3
 port access vlan 60
#
multicast routing
#
```

```
#######################################################
# SWC
#######################################################
vlan 1
vlan 30
vlan 40
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
interface Vlan-interface30
 ip address 30.30.30.2 255.255.255.0
 pim sm
#
interface Vlan-interface40
 ip address 40.40.40.1 255.255.255.0
 pim sm
#
interface GigabitEthernet1/0/1
 port access vlan 30
#
interface GigabitEthernet1/0/2
 port access vlan 40
#
multicast routing
#
pim
 c-bsr 3.3.3.3
 c-rp 3.3.3.3
#
```

```
#############################################################
# SWD
#############################################################
vlan 1
vlan 40
vlan 50
vlan 70
#
interface Vlan-interface40
 ip address 40.40.40.2 255.255.255.0
 pim sm
#
interface Vlan-interface50
 ip address 50.50.50.2 255.255.255.0
 pim sm
#
interface Vlan-interface70
 ip address 70.70.70.1 255.255.255.0
 igmp enable
#
interface GigabitEthernet1/0/1
 port access vlan 50
#
interface GigabitEthernet1/0/2
 port access vlan 40
#
interface GigabitEthernet1/0/3
 port access vlan 70
#
multicast routing
#
```

Lab15 Layer 2 マルチキャスト

実習内容と目標

このラボでは以下のことを学びます:

- IGMP snooping のコンフィグレーション。
- マルチキャスト VLAN のコンフィグレーション。
- IGMP snooping querier(メンバー管理)のコンフィグレーション。
- Layer 2 マルチキャストの表示と管理。

ネットワーク図

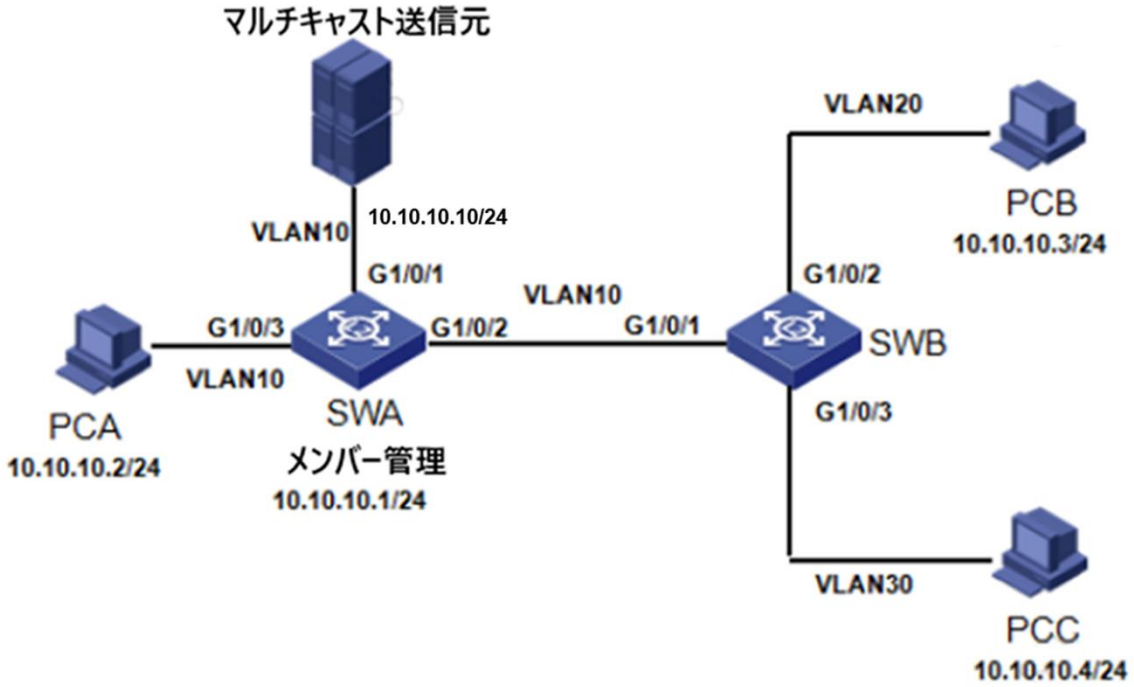


図 15.1 実習ネットワーク

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
S5820V2-54QS	Version7.10	2	なし
PC	Windows 11	4	なし
ネットワークケーブルの接続	--	5	なし

実習手順

タスク1： IGMP snoopingとマルチキャストVLANを構成します。

このタスクはIGMP snoopingを構成し、SWAをIGMP snooping querier(メンバー管理)に構成します。

手順1：基本的な設定

SWAとSWBにVLAN 10を作り、インターフェースVLAN 10をネットワーク図に基づいて作成します。SWAにVLAN-Interface 10を作成し10.10.10.1のIPアドレスを割り当てます。SWBにVLAN-Interface 10, VLAN-Interface 20, VLAN-Interface 30を作成し、それぞれのVLANにインターフェースを割り当てます。

<SWA> sys
System View: return to User View with Ctrl+Z.
[SWA] vlan 10
[SWA-vlan10] port GigabitEthernet 1/0/1 to GigabitEthernet 1/0/3
[SWA-vlan10] quit
[SWA] interface Vlan-interface 10
[SWA-Vlan-interface10] ip address 10.10.10.1 24
[SWA-Vlan-interface10] quit
<SWB> sys
System View: return to User View with Ctrl+Z.
[SWB] vlan 10
[SWB-vlan10] port GigabitEthernet 1/0/1
[SWB-vlan10] quit
[SWB] vlan 20
[SWB-vlan10] port GigabitEthernet 1/0/2
[SWB-vlan10] quit
[SWB] vlan 30

[SWB-vlan10] port GigabitEthernet 1/0/3
[SWB-vlan10] quit
[SWB] interface GigabitEthernet1/0/1
[SWB-GigabitEthernet1/0/1] port link-type hybrid
[SWB-GigabitEthernet1/0/1] port hybrid vlan 1 10 20 30 untagged
[SWB-GigabitEthernet1/0/1] quit
[SWB] interface GigabitEthernet1/0/2
[SWB-GigabitEthernet1/0/2] port link-type hybrid
[SWB-GigabitEthernet1/0/2] port hybrid vlan 1 10 20 30 untagged
[SWB-GigabitEthernet1/0/2] quit
[SWB] interface GigabitEthernet1/0/3
[SWB-GigabitEthernet1/0/3] port link-type hybrid
[SWB-GigabitEthernet1/0/3] port hybrid vlan 1 10 20 30 untagged
[SWB-GigabitEthernet1/0/3] quit

手順2：IGMP snoopingを構成します。

SWAとSWBでigmp-snooping enableコマンドでVLAN 10をグローバルでIGMP snoopingをenableにします。

[SWA] igmp-snooping
[SWA-igmp-snooping] quit
[SWA] vlan 10
[SWA-vlan10] igmp-snooping enable
[SWB] igmp-snooping
[SWB-igmp-snooping] quit
[SWB]vlan 10
[SWB-vlan10] igmp-snooping enable

手順3：IGMP snooping querierを構成します。

SWAのVLAN 10でIGMP querierをenableにして、igmp-snooping querier, igmp-snooping general-query source-ip *ip-address*, igmp-snooping special-query source-ip *ip-address*コマンドを使ってqueryメッセージの送信元IPアドレスを指定します。

[SWA-vlan10] igmp-snooping querier
[SWA-vlan10] igmp-snooping general-query source-ip 10.10.10.1
[SWA-vlan10] igmp-snooping special-query source-ip 10.10.10.1
[SWA-vlan10] quit

手順4：未確認マルチキャストデータを破棄する機能を構成します。

SWAとSWBでigmp-snooping drop-unknownコマンドを使ってVLAN 10への未確認マ

ルチキャストデータを破棄する機能を構成します。

[SWA-vlan10] igmp-snooping drop-unknown

[SWB-vlan10] igmp-snooping drop-unknown

タスク2：マルチキャストVLANを構成する

SWBでVLAN 10をマルチキャストVLANと定義し、VLAN 20とVLAN 30をマルチキャストVLANのsub-VLANとして追加します。

[SWB] multicast-vlan 10

[SWB-mvlan-10] subvlan 20 30

[SWB-mvlan-10] quit

手順1：マルチキャストVLANのsub-VLANでIGMP snoopingをenableにする。

[SWB] vlan 20

[SWB-vlan20] igmp-snooping enable

[SWB-vlan20] quit

[SWB] vlan 30

[SWB-vlan30] igmp-snooping enable

[SWB-vlan30] quit

手順2：マルチキャストトラフィックを送受信します。

マルチキャスト送信元装置でVLCツールを使ってマルチキャストトラフィックを送信します。PC A, PC B, PC CでVLCツールを使ってマルチキャストトラフィックを受信します。

- VLCで送受信する手順はLAB14と同様です。

手順3：SWBのマルチキャストVLANの情報を表示します。

[SWB] display multicast-vlan

Total 1 multicast VLANs.

Multicast VLAN 10:

Sub-VLAN list(2 in total):

20, 30

Port list(0 in total):

手順4：マルチキャストgroupの情報を表示します。

SWAとSWBで、display igmp-snooping groupコマンドを使って、ルーターポートとグループメンバーポートを含むLayer 2マルチキャストグループの情報を表示します。

<SWA>dis igmp-snooping group

Total 1 entries.

VLAN 10: Total 1 entries.

(0.0.0.0, 239.255.255.250)

Host slots (0 in total):

```
    Host ports (1 in total):
      GE1/0/1                                 (00:02:22)
```

[SWA]dis igmp-snooping

```
IGMP snooping information: Global
  IGMP snooping: Enabled
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-member-query-interval: 1s
  Report-aggregation: Enabled
  Host-tracking: Disabled
  Dot1p-priority: --

IGMP snooping information: VLAN 10
  IGMP snooping: Enabled
  Drop-unknown: Enabled
  Version: 2
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-member-query-interval: 1s
  Querier: Enabled
  Query-interval: 125s
  General-query source IP: 10.10.10.1
  Special-query source IP: 10.10.10.1
  Report source IP: 10.10.10.1
  Leave source IP: 10.10.10.1
  Host-tracking: Disabled
  Dot1p-priority: --
  Proxy: Disabled
```

[SWB]dis igmp-snooping

```
IGMP snooping information: Global
  IGMP snooping: Enabled
```

```
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-member-query-interval: 1s
  Report-aggregation: Enabled
  Host-tracking: Disabled
  Dot1p-priority: --

IGMP snooping information: VLAN 10
  IGMP snooping: Enabled
  Drop-unknown: Enabled
  Version: 2
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-member-query-interval: 1s
  Querier: Disabled
  Query-interval: 125s
  General-query source IP: 0.0.0.0
  Special-query source IP: 10.10.10.1
  Report source IP: 0.0.0.0
  Leave source IP: 0.0.0.0
  Host-tracking: Disabled
  Dot1p-priority: --
  Proxy: Disabled

IGMP snooping information: VLAN 20
  IGMP snooping: Enabled
  Drop-unknown: Disabled
  Version: 2
  Host-aging-time: 260s
  Router-aging-time: 260s
  Max-response-time: 10s
  Last-member-query-interval: 1s
  Querier: Disabled
  Query-interval: 125s
```

General-query source IP: 0.0.0.0
Special-query source IP: 10.10.10.1
Report source IP: 0.0.0.0
Leave source IP: 0.0.0.0
Host-tracking: Disabled
Dot1p-priority: --
Proxy: Disabled

IGMP snooping information: VLAN 30
IGMP snooping: Enabled
Drop-unknown: Disabled
Version: 2
Host-aging-time: 260s
Router-aging-time: 260s
Max-response-time: 10s
Last-member-query-interval: 1s
Querier: Disabled
Query-interval: 125s
General-query source IP: 0.0.0.0
Special-query source IP: 10.10.10.1
Report source IP: 0.0.0.0
Leave source IP: 0.0.0.0
Host-tracking: Disabled
Dot1p-priority: --
Proxy: Disabled

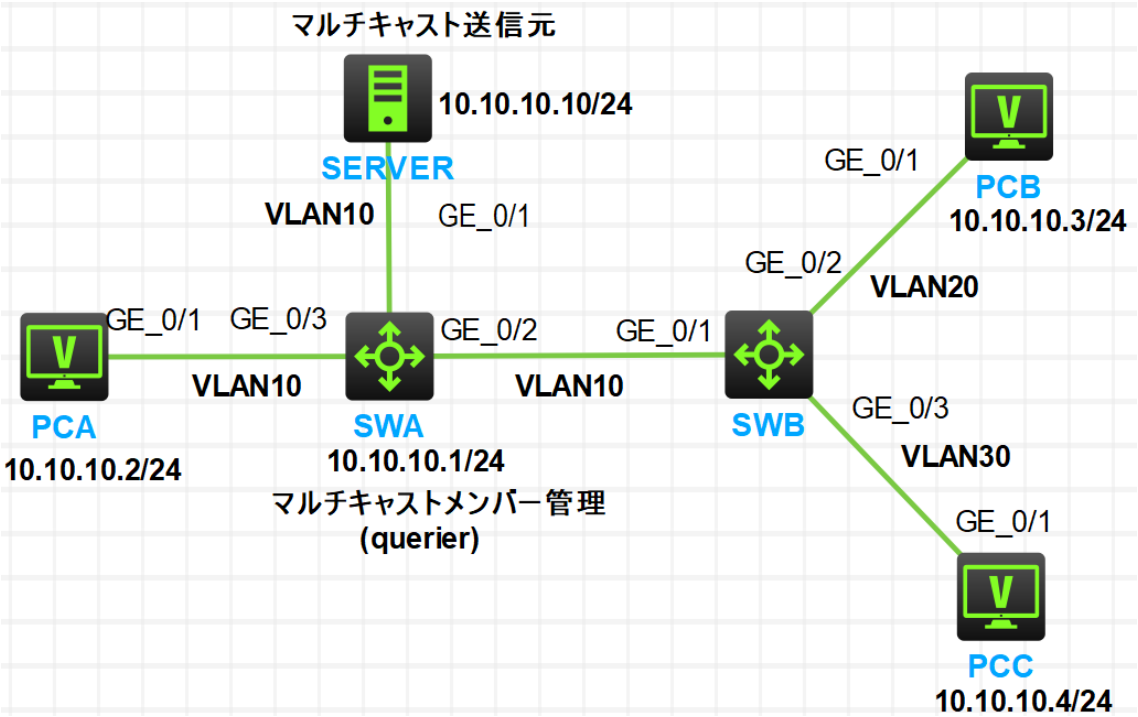
IGMP snoopingの出力はマルチキャストVLAN(VLAN 10)のルーターポートを管理し、sub-VLAN(VLAN 20とVLAN 30)のメンバーポートを管理しています。

コマンドリファレンス

コマンド	説明
igmp-snooping enable	VLAN または VSI の IGMP スヌーピングを有効にします。
igmp-snooping querier	IGMPスヌーピングクエリアを有効にする
igmp-snooping general-query source-ip *ip-address*	IGMP一般クエリの送信元IPアドレスを設定する
igmp-snooping special-query source-ip *ip-address*	IGMP グループ固有のクエリの送信元 IP アドレスを設定します。
igmp-snooping drop-unknown	VLANまたはVSIの不明なマルチキャストデータパケットのドロップを有効にする
multicast-vlan *vlan-id*	マルチキャストVLANを設定してそのビューに入るか、既存のマルチキャストVLANのビューに入る
subvlan *vlan-list*	マルチキャストVLANにサブVLANとしてVLANを割り当てる
display igmp-snooping group	ダイナミックIGMPスヌーピンググループエントリに関する情報を表示する
display multicast-vlan [*vlan-id*]	マルチキャスト VLAN に関する情報を表示します。

構成サマリー(マルチキャスト部分を抽出)

IGMP snooping




```
############################################################
# SWA
############################################################
#
igmp-snooping
#
vlan 1
#
vlan 10
 igmp-snooping enable
 igmp-snooping drop-unknown
 igmp-snooping querier
 igmp-snooping general-query source-ip 10.10.10.1
 igmp-snooping special-query source-ip 10.10.10.1
#
interface NULL0
#
interface Vlan-interface10
 ip address 10.10.10.1 255.255.255.0
#
interface GigabitEthernet1/0/1
port access vlan 10
#
interface GigabitEthernet1/0/2
port access vlan 10
#
```

```
interface GigabitEthernet1/0/3
port access vlan 10
#

############################################################
# SWB
############################################################
#
igmp-snooping
#
vlan 1
#
vlan 10
 igmp-snooping enable
 igmp-snooping drop-unknown
#
vlan 20
 igmp-snooping enable
#
vlan 30
 igmp-snooping enable
#
multicast-vlan 10
 subvlan 20 30
#
iinterface GigabitEthernet1/0/1
 port link-type hybrid
 port hybrid vlan 1 10 20 30 untagged
 port hybrid pvid vlan 10
#
interface GigabitEthernet1/0/2
 port link-type hybrid
 port hybrid vlan 1 10 20 30 untagged
 port hybrid pvid vlan 10
#
interface GigabitEthernet1/0/3
 port link-type hybrid
 port hybrid vlan 1 10 20 30 untagged
 port hybrid pvid vlan 10
#
```

Lab16 NATの設定

実習内容と目標

このラボでは以下のことを学びます：

- NAT の基本的なコンフィギュレーションを習得します。
- NAPT のコンフィギュレーション方法を習得します。
- Easy IP のコンフィギュレーション方法を習得します。
- NAT Server のコンフィギュレーション方法を習得します。

ネットワーク図

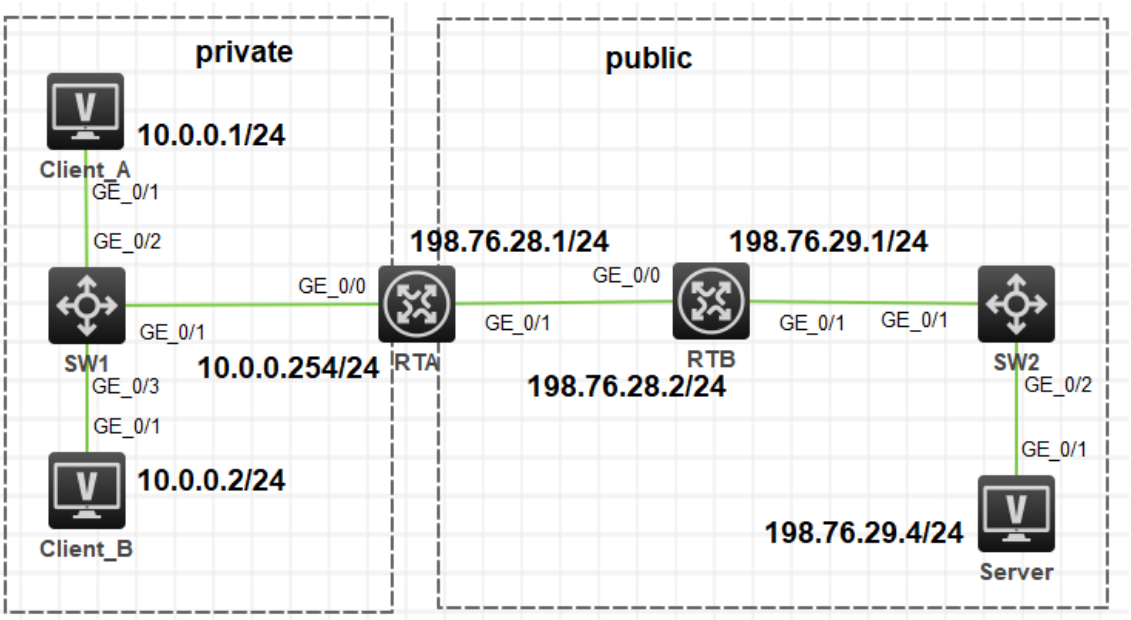


図 14.1 実習ネットワーク

上の図は、テストトポロジを示しています。2つのMSR3620（RTAとRTB）、2つのS5820V2（SW1とSW2）、および3つのPC（Client_A、Client_BとServer）です。

Client_AとClient_Bはプライベートネットワーク上にあり、RTAはゲートウェイとNATデバイスとして機能し、1つのプライベートネットワークポート（G0/0）と1つのパブリックネットワークを持ち、RTBがゲートウェイとして機能します。

トポロジには、いくつかのNATアプリケーションが含まれます。 Easy IPは最も単純で、主にダイヤルアップアクセスシナリオで使用されます。 基本的なNATはNAPTほど使われておりません。 NAPTは、パブリックネットワークIPアドレスの使用を改善でき、パブリ

ックサーバーシナリオへのプライベートクライアントアクセスに適用できます。 NATサーバーは、プライベートサービスからパブリックネットワークへのシナリオに適用できます。

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**	ルーター
S5820V2	**Version7.1**	**2**	スイッチ
PC	**Windows 7**	**3**	ホスト
ネットワークケーブルの接続	**--**	**6**	ストレートケーブル

実習手順

タスク1：基本的なNATの設定をする

このテストでは、プライベートネットワーククライアントのClient_AとClient_Bがパブリックネットワークサーバーにアクセスする必要があります。 RTBはプライベートネットワークルートを格納しないため、RTAで基本的なNATを構成して、パブリックネットワークアドレスをClient_AとClient_Bに動的に割り当てます。

手順1：テスト環境を構築する

ラボの図に従ってテスト環境を構築し、RTAおよびRTBポートにIPアドレスを構成します。 サーバー宛てのパケットをルーティングするには、ネクストホップRTB G0/0を使用して、RTBを指すようにRTAで静的ルートを構成します。 RTAはサーバーにpingを実行できます。 Client_AのIPアドレスを10.0.0.1/24として、ゲートウェイを10.0.0.254として構成します。 Client_B IPアドレスを10.0.0.2/24として構成し、ゲートウェイを10.0.0.254として構成します。

表14-1 IPアドレス割り当てスキーマ

装置	**インターフェース**	**IPアドレス**	**ゲートウェイ**
RTA	G0/0	10.0.0.254/24	-
	G0/1	198.76.28.1/24	-
RTB	G0/0	198.76.28.2/24	-
	G0/1	198.76.29.1/24	-
Client A		10.0.0.1	10.0.0.254

Client B		10.0.0.2	10.0.0.254
Server		198.76.29.4/24	198.76.29.1/24

手順2：基本的なコンフィギュレーション

IPアドレスとルートを設定します(RTBでは、あえてRTAへのstatic routeを設定しません)。

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]ip address 10.0.0.254 24

[RTA-GigabitEthernet0/0]quit

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]ip address 198.76.28.1 24

[RTA-GigabitEthernet0/1]quit

[RTA]ip route-static 0.0.0.0 0 198.76.28.2

[RTB]interface GigabitEthernet 0/0

[RTB-GigabitEthernet0/0]ip address 198.76.28.2 24

[RTB-GigabitEthernet0/0]quit

[RTB]interface GigabitEthernet 0/1

[RTB-GigabitEthernet0/1]ip address 198.76.29.1 24

[RTB-GigabitEthernet0/1]quit

手順3：接続性をチェックします

Client_AとClient_Bでそれぞれサーバー（IPアドレス198.76.29.4）にpingを実行します。出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

以前の情報に基づいて、Client_AとClient_Bはサーバーにpingを実行できません。RTBにはプライベートネットワークへのルートがないためです。 RTBは、サーバーから送信されたpingパケットのネットワークセグメント10.0.0.0宛てのルートを見つけることができません。

手順4：Basic NATを設定します

RTAでBasic NATを設定します。

ACLを使用して、ネットワークセグメント10.0.0.0/24にある送信元アドレスでフローを定

義します。

[RTA]acl basic 2000

[RTA-acl-ipv4-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255

[RTA-acl-ipv4-basic-2000]quit

アドレス変換のためのアドレスとして198.76.28.11から198.76.28.20を用意したNATアドレスプール1を作成します。

[RTA]nat address-group 1

[RTA-address-group-1]address 198.76.28.11 198.76.28.20

[RTA-address-group-1]quit

インターフェースビューに入り、ACL 2000とNAT アドレスプール1を結び付けてoutboundポート経由でアドレスを割り当てます。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]nat outbound 2000 address-group 1 no-pat

[RTA-GigabitEthernet0/1]quit

パブリックネットワークアドレスプールのアドレスグループ1は、RTAで構成され、アドレス範囲は198.76.28.11-198.76.28.20です。 パラメータno-patは、1対1のアドレス変換を示します。これは、ポート番号ではなく、アドレス指定されたアドレスを変換することを意味します。 この場合、RTAは、ACL2000ルールを変更するアウトバウンドパケットのアドレスを変換します。

手順5：接続性をチェックします

Client_AとClient_Bでそれぞれサーバー（IPアドレス198.76.29.4）にpingを実行します。出力情報は次のとおりです。

<H3C>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

56 bytes from 198.76.29.4: icmp_seq=0 ttl=253 time=4.000 ms

56 bytes from 198.76.29.4: icmp_seq=1 ttl=253 time=9.000 ms

56 bytes from 198.76.29.4: icmp_seq=2 ttl=253 time=9.000 ms

56 bytes from 198.76.29.4: icmp_seq=3 ttl=253 time=8.000 ms

56 bytes from 198.76.29.4: icmp_seq=4 ttl=253 time=8.000 ms

手順6：NATエントリーをチェックします

RTAでNATエントリーをチェックします。

[RTA]display nat session

Slot 0:

Initiator:

Source IP/port: 10.0.0.1/172

Destination IP/port: 198.76.29.4/2048

```
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet0/0
Initiator:
  Source           IP/port: 10.0.0.1/171
  Destination IP/port: 198.76.29.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet0/0
Total sessions found: 2

[RTA]display nat no-pat
Slot 0:
Total entries found: 0
[RTA]display nat no-pat
Slot 0:
Local     IP: 10.0.0.1
Global    IP: 198.76.28.17
Reversible: N
Type          : Outbound

Local     IP: 10.0.0.2
Global    IP: 198.76.28.16
Reversible: N
Type          : Outbound

Total entries found: 2
```

以前の情報に基づいて、このICMPパケットの送信元アドレス10.0.0.1は、送信元ポート番号249および宛先ポート番号2048のパブリックネットワークアドレス192.76.28.12に変換されました。送信元アドレス10.0.0.2は、 パブリックネットワークアドレス198.76.28.11、送信元ポート番号210、宛先ポート番号2048。1分後に全体を確認します。 最後のネットワークエントリは失われます。 4分後、すべてのエントリーが失われます。 出力情報は次のとおりです。

```
[RTA]display nat session
```

Slot 0:
Total sessions found: 0

NATエントリーにはエージングタイム（エージングタイム）があります。 エージング時間が経過すると、NATは対応するエントリーを削除します。Display session aging-time stateコマンドを実行して、セッションのデフォルトのエージングタイムを照会します。
[RTA]display session aging-time state
SESSION is not configured.
HCLのルーターではデフォルトのエージングタイムが設定されていないようなので、セッションの状態を確認します。
[RTA]display session statistics
Slot 0:
Current sessions: 4
TCP sessions: 0
UDP sessions: 0
ICMP sessions: 4
ICMPv6 sessions: 0
UDP-Lite sessions: 0
SCTP sessions: 0
DCCP sessions: 0
RAWIP sessions: 0

History average sessions per second:
Past hour: 0
Past 24 hours: 0
Past 30 days: 0
History average session establishment rate:
Past hour: 0/s
Past 24 hours: 0/s
Past 30 days: 0/s

Current relation-table entries: 0

Session establishment rate: 0/s
TCP: 0/s
UDP: 0/s

```
          ICMP:                    0/s
        ICMPv6:                    0/s
      UDP-Lite:                  0/s
          SCTP:                    0/s
          DCCP:                    0/s
         RAWIP:                    0/s

Received TCP       :                0 packets                0
bytes
Received UDP       :                0 packets                0
bytes
Received ICMP      :                0 packets                0
bytes
Received ICMPv6    :                0 packets                0
bytes
Received UDP-Lite :                 0 packets                0 bytes
Received SCTP      :                0 packets                0
bytes
Received DCCP      :                0 packets                0
bytes
Received RAWIP     :                0 packets                0
bytes
```

session aging-time コマンドを使ってNATセッションのエージングタイムを変更してみます。

NATでバッキング情報は以下の通りです:

```
<RTA>terminal monitor
The current terminal is enabled to display logs.
<RTA>terminal debugging
The current terminal is enabled to display debugging logs.
<RTA>debugging nat packet
<RTA>*Nov 22 12:09:21:244 2021 RTA NAT/7/COMMON:
  PACKET: (GigabitEthernet0/1-out) Protocol: ICMP
          10.0.0.2:      0 -      198.76.29.4:      0(VPN:      0) ------>
     198.76.28.12:      0 -      198.76.29.4:      0(VPN:      0)
*Nov 22 12:09:21:247 2021 RTA NAT/7/COMMON:
```

PACKET: (GigabitEthernet0/1-in) Protocol: ICMP

198.76.29.4: 0 - 198.76.28.12: 0(VPN: 0) ------>

198.76.29.4: 0 - 10.0.0.2: 0(VPN: 0)

以上のデバッキング情報によると、GigabitEthernet G0/1の出力で、ICMP 10.0.0.2の発信元アドレスのパケットは198.76.28.12に変換されていることが分かります。

ノート:

理論的には、各IPアドレスには65,536個のポートがあります。 占有ポートと予約ポートを除いて、使用可能なポートは理論値よりはるかに少なくなります。

手順7:コンフィギュレーションを元に戻します

RTAのBasic NAT設定を削除します。

NATアドレスプールを削除します。

[RTA]undo nat address-group 1

ポートに関連付けられたNATを削除します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo nat outbound 2000

[RTA-GigabitEthernet0/1]quit

タスク2:NAPTの設定をする

プライベートネットワーククライアントclient_AとClient_Bは、パブリックネットワークサーバーにアクセスする必要があります。 パブリックネットワークアドレスが制限されているため、RTAで構成されているパブリックネットワークアドレスの範囲は198.76.28.11-198.76.28.20です。 RTAでNAPTを構成して、パブリックネットワークアドレスとポートをClient_AとClient_Bに動的に割り当てます。

手順1:テスト環境を構築する

テスト環境を構築します。 タスク1のステップ1と2を参照してください。

手順2:接続性をチェックします

Client_AとClient_Bでそれぞれサーバー(IPアドレス198.76.29.4)にpingを実行します。出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

以前の情報に基づいて、Client_AとClient_Bはサーバーにpingを実行できません。

手順3：NAPTを設定します

ACLを使用して、ネットワークセグメント10.0.0.0/24にある送信元アドレスでフローを定義します。

[RTA]acl basic 2000

[RTA-acl-ipv4-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255

[RTA-acl-ipv4-basic-2000]quit

NATアドレスプール1を1つのアドレス198.76.28.11で構成します。

[RTA]nat address-group 1

[RTA-address-group-1]address 198.76.28.11 198.76.28.11

[RTA-address-group-1]quit

インターフェースビューでNATアドレスをacl 2000にバインドし、アドレスを提供します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]nat outbound 2000 address-group 1

[RTA-GigabitEthernet0/1]quit

パラメータno-patは伝送されず、NATがパケット内のポートを変換することを示します。

手順4：接続性をチェックします

Client_AとClient_Bでそれぞれサーバー（IPアドレス198.76.29.4）にpingを実行します。出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

56 bytes from 198.76.29.4: icmp_seq=0 ttl=253 time=5.000 ms

56 bytes from 198.76.29.4: icmp_seq=1 ttl=253 time=9.000 ms

56 bytes from 198.76.29.4: icmp_seq=2 ttl=253 time=8.000 ms

56 bytes from 198.76.29.4: icmp_seq=3 ttl=253 time=8.000 ms

56 bytes from 198.76.29.4: icmp_seq=4 ttl=253 time=7.000 ms

手順5：NATエントリーをチェックします

RTAのnatエントリーをチェックします。

[RTA]display nat session verbose

Slot 0:

Initiator:

Source IP/port: 10.0.0.1/191

Destination IP/port: 198.76.29.4/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/0
Responder:
Source IP/port: 198.76.29.4/3
Destination IP/port: 198.76.28.11/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/1
State: ICMP_REPLY
Application: OTHER
Role: -
Failover group ID: -
Start time: 2021-11-22 14:55:05 TTL: 22s
Initiator->Responder: 0 packets 0 bytes
Responder->Initiator: 0 packets 0 bytes
Initiator:
Source IP/port: 10.0.0.2/227
Destination IP/port: 198.76.29.4/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/0
Responder:
Source IP/port: 198.76.29.4/2
Destination IP/port: 198.76.28.11/0
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/1
State: ICMP_REPLY
Application: OTHER
Role: -
Failover group ID: -
Start time: 2021-11-22 14:54:53 TTL: 9s
Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 2

以前の情報に基づいて、送信元IPアドレス10.0.0.1と10.0.0.2は、同じパブリックネットワークアドレス198.76.28.11に変換されます。 ただし、10.0.0.1のポートは12289で、10.0.0.2のポートは12288です。RTAが198.76.28.11宛ての応答パケットを受信すると、RTAはパケットを変換用に指定されたポートにより10.0.0.1と10.0.0.2のどちらに転送するかを区別します。 NAPTはこのメソッドを使用して、IP層とトランスポート層でパケットを変換します。 これにより、パブリックIPアドレスの使用が大幅に改善されます。

手順6：コンフィギュレーションを元に戻します

RTAのNAPT設定を削除します。

NATアドレスプールを削除します。

[RTA]undo nat address-group 1

ポートに関連付けられたNATを削除します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo nat outbound 2000

[RTA-GigabitEthernet0/1]quit

タスク3：Easy IPの設定をする

プライベートネットワーククライアントClient_AおよびClient_Bは、パブリックネットワークサーバーにアクセスする必要があります。 パブリックネットワークポートのIPアドレスを使用して、パブリックネットワークアドレスとポートをClient_AとClient_Bに動的に割り当てます。

手順1：テスト環境を構築する

テスト環境を構築します。 タスク1のステップ1と2を参照してください。

手順2：接続性をチェックします

Client_AとClient_Bでそれぞれサーバー（IPアドレス198.76.29.4）にpingを実行します。出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

手順3：East IPを設定します

RTAでEasy IPを設定します。

ACLを使用して、ネットワークセグメント10.0.0.0/24にある送信元アドレスでフローを定

義します。

```
[RTA]acl basic 2000
[RTA-acl-ipv4-basic-2000]rule 0 permit source 10.0.0.0 0.0.0.255
[RTA-acl-ipv4-basic-2000]quit
```

インターフェースビューでNATアドレスをacl 2000にバインドし、アドレスを提供します。

```
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]nat outbound 2000
[RTA-GigabitEthernet0/1]quit
```

手順4：接続性をチェックします

Client_AとClient_Bでそれぞれサーバー（IPアドレス198.76.29.4）にpingを実行します。出力情報は次のとおりです。

```
<Client_A>ping 198.76.29.4
Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break
56 bytes from 198.76.29.4: icmp_seq=0 ttl=253 time=5.000 ms
56 bytes from 198.76.29.4: icmp_seq=1 ttl=253 time=9.000 ms
56 bytes from 198.76.29.4: icmp_seq=2 ttl=253 time=8.000 ms
56 bytes from 198.76.29.4: icmp_seq=3 ttl=253 time=8.000 ms
56 bytes from 198.76.29.4: icmp_seq=4 ttl=253 time=7.000 ms
```

手順5：NATエントリーをチェックします

RTAでNATエントリーをチェックします。

```
[RTA]display nat session verbose
Slot 0:
Initiator:
  Source          IP/port: 10.0.0.1/200
  Destination IP/port: 198.76.29.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet0/0
Responder:
  Source          IP/port: 198.76.29.4/5
  Destination IP/port: 198.76.28.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
```

```
  Inbound interface: GigabitEthernet0/1
State: ICMP_REPLY
Application: OTHER
Role: -
Failover group ID: -
Start time: 2021-11-22 15:56:36       TTL: 15s
Initiator->Responder:              0 packets          0 bytes
Responder->Initiator:              0 packets          0 bytes
Initiator:
  Source          IP/port: 10.0.0.2/238
  Destination IP/port: 198.76.29.4/2048
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet0/0
Responder:
  Source          IP/port: 198.76.29.4/4
  Destination IP/port: 198.76.28.1/0
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: -/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet0/1
State: ICMP_REPLY
Application: OTHER
Role: -
Failover group ID: -
Start time: 2021-11-22 15:56:30       TTL: 9s
Initiator->Responder:              0 packets          0 bytes
Responder->Initiator:              0 packets          0 bytes
Total sessions found: 2
[RTA]display nat session
Slot 0:
Total sessions found: 0
[RTA]display nat session
Slot 0:
Initiator:
```

Source IP/port: 10.0.0.1/202
Destination IP/port: 198.76.29.4/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/0
Initiator:
Source IP/port: 10.0.0.2/239
Destination IP/port: 198.76.29.4/2048
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: -/-/-
Protocol: ICMP(1)
Inbound interface: GigabitEthernet0/0
Total sessions found: 2
以前の情報に基づいて、10.0.0.1および10.0.0.2にアドレス指定された送信元IPは、RTAのアウトバウンドポートアドレス198.76.28.1に変換されました。
NAT構成後、Client_AがサーバーにpingをRTAできる場合、サーバーはClient_Aにpingを実行できますか？ 出力情報は次のとおりです。
<Server>ping 10.0.0.1
Ping 10.0.0.1 (10.0.0.1): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out
RTAには10.0.0.0/24へのルートがありません。 そのため、サーバーはClient_Aにpingを実行できません。 サーバーのICMP応答パケットはサーバーアドレス198.76.29.4を送信元アドレスとして使用し、RTAアウトバウンドアドレス198.76.28.1を宛先アドレスとして使用するため、Client_AはサーバーにpingをRTAを実行できます。 Client_Aの実際のソースアドレスは10.0.0.1です。 つまり、ICMP接続はClient_Aによって開始され、RTAがアドレスを変換してパケットを転送するようにトリガーする必要があります。 NATはRTAアウトバウンドポートGigibitEthernet0/1に対して有効であることに注意してください。 そのため、サーバーからクライアントにpingを実行するためにICMPパケットを送信しても、RTAをトリガーしてアドレスを変換することはできません。
サーバーでClient_Aにpingを実行する方法を知るには、タスク4に進みます。

手順6：コンフィギュレーションを元に戻します

RTAのEasy IP設定を削除します。

NATアドレスプールを削除します。

[RTA]undo nat address-group 1

ポートに関連付けられたNATを削除します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo nat outbound 2000

[RTA-GigabitEthernet0/1]quit

タスク4：NAT Serverの設定をする

Client_Aは、ICMPサービスを外部に提供する必要があります。 Client_Aを静的パブリックネットワークアドレス198.76.28.11およびRTAのポートにマップします。

手順1：接続性をチェックします

Client_AとClient_Bでそれぞれサーバー（IPアドレス198.76.29.4）にpingを実行します。出力情報は次のとおりです。

<Client_A>ping 198.76.29.4

Ping 198.76.29.4 (198.76.29.4): 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

手順2：NAT Serverを設定します

RTAにNAT Serverを設定します。

[RTA]interface GigabitEthernet 0/1

アウトバウンドポートのプライベートネットワークサーバーアドレスとパブリックネットワークアドレスに1対1のNATマッピングを実装します。

[RTA-GigabitEthernet0/1]nat server protocol icmp global 198.76.28.11 inside 10.0.0.1

[RTA-GigabitEthernet0/1]quit

手順3：接続性をチェックします

サーバーからClient_Aネットワークアドレス198.76.28.11にpingを実行します。

サーバーはClient_Aにpingを実行できます。

<Server>ping 198.76.28.11

Ping 198.76.28.11 (198.76.28.11): 56 data bytes, press CTRL_C to break

56 bytes from 198.76.28.11: icmp_seq=0 ttl=253 time=5.000 ms

56 bytes from 198.76.28.11: icmp_seq=1 ttl=253 time=8.000 ms

56 bytes from 198.76.28.11: icmp_seq=2 ttl=253 time=8.000 ms

56 bytes from 198.76.28.11: icmp_seq=3 ttl=253 time=5.000 ms

56 bytes from 198.76.28.11: icmp_seq=4 ttl=253 time=7.000 ms

手順4：NATエントリーをチェックします

RTAでNAT Serverエントリーをチェックします。

[RTA]dis nat session verbose

Slot 0:

Initiator:

Source IP/port: 198.76.29.4/191

Destination IP/port: 198.76.28.11/2048

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet0/1

Responder:

Source IP/port: 10.0.0.1/191

Destination IP/port: 198.76.29.4/0

DS-Lite tunnel peer: -

VPN instance/VLAN ID/Inline ID: -/-/-

Protocol: ICMP(1)

Inbound interface: GigabitEthernet0/0

State: ICMP_REPLY

Application: OTHER

Role: -

Failover group ID: -

Start time: 2021-11-22 16:45:42 TTL: 22s

Initiator->Responder: 0 packets 0 bytes

Responder->Initiator: 0 packets 0 bytes

Total sessions found: 1

手順5：コンフィギュレーションを元に戻します

RTAでNAT Server設定を削除します。

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo nat server protocol icmp global 198.76.28.11

NATアドレスプールを削除します。

[RTA]undo nat address-group 1

ポートに関連付けられたNATを削除します。

[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]undo nat outbound 2000
[RTA-GigabitEthernet0/1]quit
NATサーバーは、プライベートネットワークサーバーにアクセスするためのパブリックネットワーククライアントの要件を満たす必要があります。 NATサーバーは、パブリックネットワーククライアントがアクセスするプライベートネットワークアドレス/ポートをマップします。 実際のアプリケーションでは、プライベートネットワーク内のWebサーバーまたはFTPサーバーがパブリックネットワークの顧客にサービスを提供する必要がある場合、NATサーバーを使用してパブリックネットワークアドレスをプライベートネットワークサーバーにマップできます。 Client_Aがサーバーにpingを実行した場合、pingは正常に実行できますか？ Client_Bがサーバーにpingを実行した場合も、pingは正常に実行できますか？

RTAのNATサーバー構成コマンドに基づいて、Client_AがFTPサーバーの場合、FTPサービスを外部に提供できますか？ 答えはイエスです。 NATサーバー構成を変更します。 NATサーバーの構成は次のとおりです。
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]nat server protocol tcp global 198.76.28.11 ftp inside 10.0.0.1 ftp
[RTA-GigabitEthernet0/1]quit

質問:

1. このテストでは、パブリックネットワークアドレスプールにパブリックネットワークポートアドレスが含まれています。 別のアドレスセグメントが追加された場合、RTBをどのように構成する必要がありますか？

答え:
RTBのパブリックネットワークアドレスプール宛ての静的ルートを追加します。

2. nat serverコマンドのglobal-addressはインターネットアドレスである必要がありますか？

答え:
いいえ、実際には、グローバルアドレスは内部アドレスを基準にしています。 nat serverコマンドを実行して構成されたポートは、グローバルネットワークに接続されます。

Lab17 VRRPの設定

実習内容と目標

このラボでは以下のことを学びます：

- VRRP の基本的なコンフィギュレーションを習得します。
- VRRP と OSPF を組み合わせたコンフィギュレーション方法を習得します。
- VRRP の障害時の切り替えの確認をします。

ネットワーク図

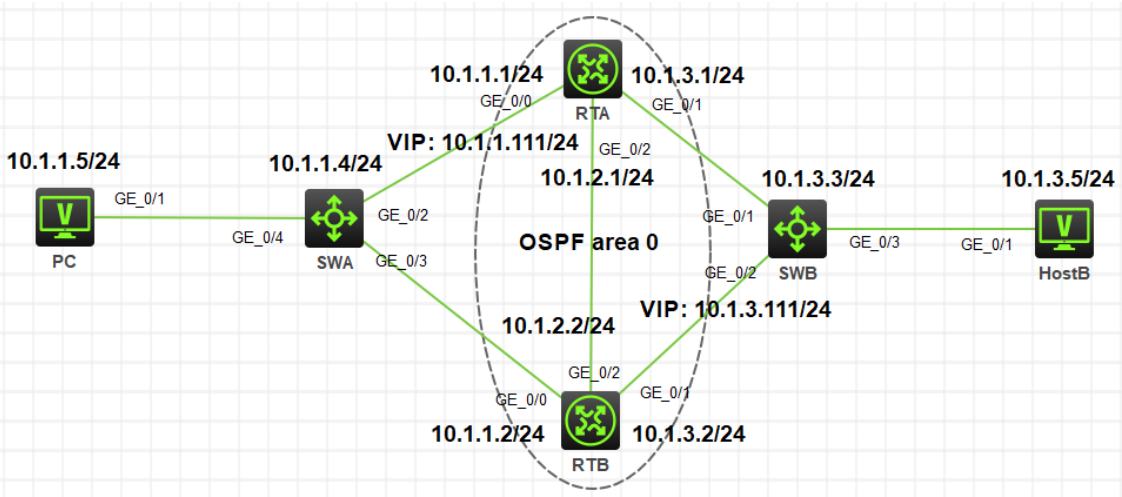


図 3.1 実習ネットワーク

上の図は、テストトポロジを示しています。2つのMSR3620（RTAとRTB）と、2つのS5820V2（SW1とSW2）、および2つのPC（PC、HostB）です。

PCからHostBへの経路を冗長化するためにVRRPを設定します。この場合、SWAからRTA, RTB間がVRRPにより冗長化され、仮想IPアドレスへ10.1.1.111となります。
また、HostBからPCへの経路を冗長化するためにRTBの右側にもSWBからの経路を冗長化するためにVRRPを設定します。

RTAのVRRPのプライオリティをRTBより高くしていると図3-2のように仮想IPは両方ともRTAに存在します。

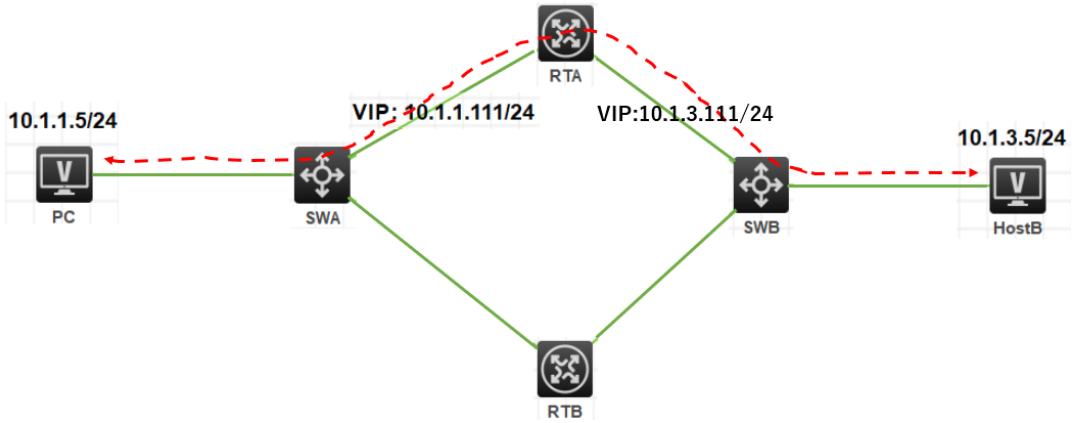


図3-2 RTA, RTBの両側にVRRPを構成

この場合、左側のVRRPでSWAからRTAへの経路に障害が発生しても図3-3のように右側の経路はSWBからRTAの経路のままです。

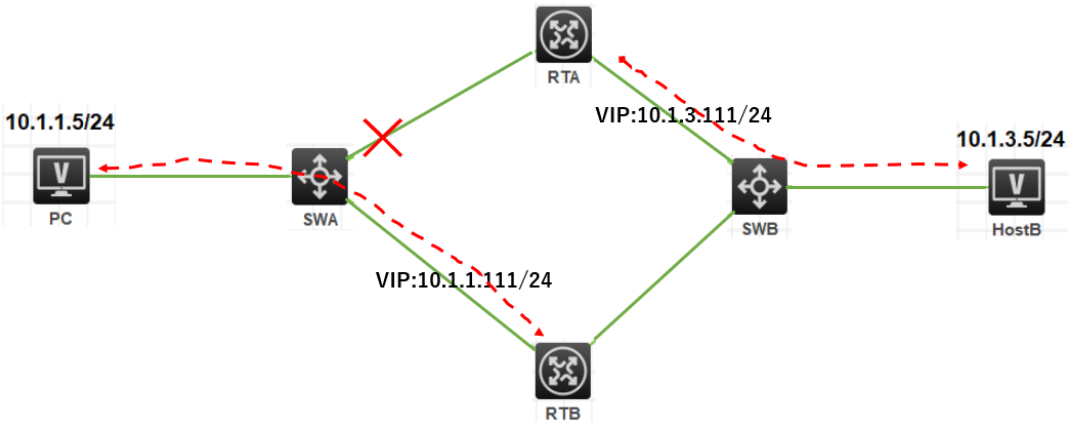


図3-3 SWA, RTA間に障害発生

したがって、PCからHostBへの通信は途切れてしまいます。

これを防ぐためにはRTAとRTBの間にルーティングプロトコルが必要となります。

今回はOSPFを使って、経路障害を検知して正しい経路を選択するようにします。

そうすると図3-4のように正しい迂回経路が選択されます。

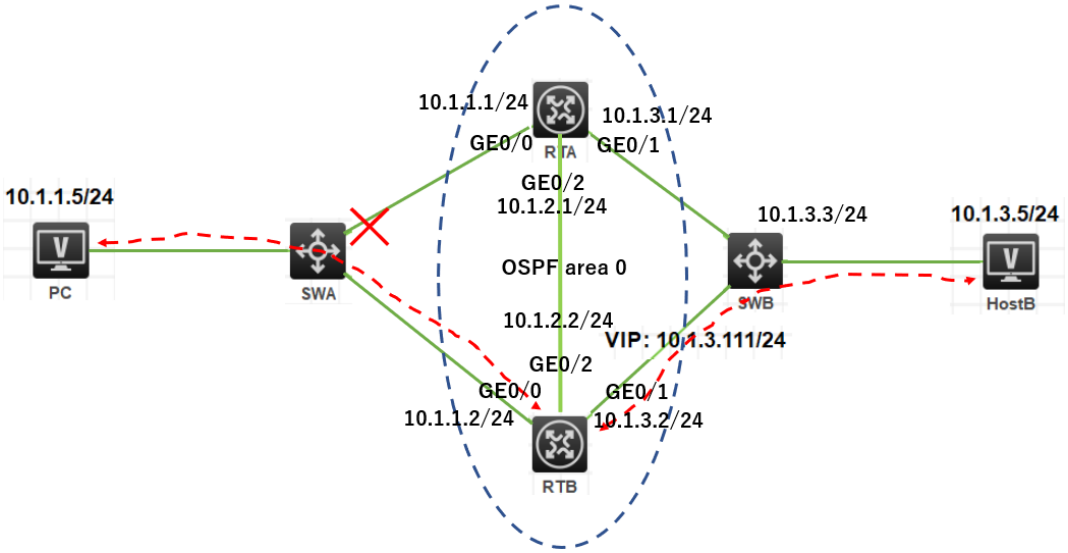


図3-4 OSPFにより経路障害に対応

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**	ルーター
S5820V2	**Version7.1**	**2**	スイッチ
PC	**Windows 7**	**2**	ホスト
ネットワークケーブルの接続	--	**7**	ストレートケーブル

実習手順

タスク1：それぞれの装置にIPアドレスを設定する

手順1：両PCにIPアドレス、ゲートウェイアドレスを設定する

アドレスおよびデフォルトゲートウェイは表3-1に従って設定します。

表3-1 IPアドレス割り当て

装置	インターフェイス	IPアドレス	ゲートウェイ
RTA	G0/0	10.1.1.1/24	-
	G0/1	10.1.3.1/24	-
	G0/2	10.1.2.1/24	
RTB	G0/0	10.1.1.2/24	-
	G0/1	10.1.3.2/24	-
	G0/2	10.1.2.2/24	
SWA	VLAN 1	10.1.1.4/24	10.1.1.111
SWB	VLAN 1	10.1.3.3/24	10.1.3.111
PC		10.1.1.5/24	10.1.1.111
HostB		10.1.3.5/24	10.1.3.111

手順2：SWA, SWBのSTPを無効にする

SWAのstpを無効にします

[SWA]undo stp global enable

[SWA]%Dec 21 17:55:46:538 2021 SWA STP/6/STP_DISABLE: STP is now disabled on the device.

SWBのstpを無効にします

[SWB]undo stp global enable

[SWB]%Dec 21 17:55:46:538 2021 SWB STP/6/STP_DISABLE: STP is now disabled on the device.

手順3：SWA, SWBにIPアドレス、デフォルトルートを設定する

PC、SWA間、HostB、SWB間にケーブルをつなぎます。そして、以下のようにSWA,SWBにIPアドレスとデフォルトルートを設定します。

SWAのVLAN 1にIPアドレス10.1.1.4/24を割り当てます。

[SWA]interface Vlan-interface 1

[SWA-Vlan-interface1]ip address 10.1.1.4 24

RTA, RTBの先にあるネットワークセグメントへのデフォルトゲートウェイ(仮想IPアドレス)を設定します。

[SWA]ip route-static 0.0.0.0 0.0.0.0 10.1.1.111

SWBのVLAN 1にIPアドレス10.1.3.3/24を割り当てます。

[SWB]interface Vlan-interface 1

[SWB-Vlan-interface1]ip address 10.1.3.3 24

RTA, RTBの先にあるネットワークセグメントへのデフォルトゲートウェイ(仮想IPアドレス)を設定します。

[SWB]ip route-static 0.0.0.0 0.0.0.0 10.1.3.111

手順4：SWAとRTA間、SWBとRTB間にケーブルを接続しRTA, RTBにIPアドレスを設定する

RTAにIPアドレスを割り当てます。

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]ip address 10.1.1.1 24

[RTA-GigabitEthernet0/0]quit

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]ip address 10.1.3.1 24

[RTA-GigabitEthernet0/1]quit

RTBにIPアドレスを割り当てます。

[RTB]interface GigabitEthernet 0/0

[RTB-GigabitEthernet0/0]ip address 10.1.1.2 24

[RTB-GigabitEthernet0/0]quit

[RTB]interface GigabitEthernet 0/1

[RTB-GigabitEthernet0/1]ip address 10.1.3.2 24

[RTB-GigabitEthernet0/1]quit

タスク2：RTA, RTBにVRRPを設定する

手順1：RTA, RTBにVRRPを設定する

RTAのVRID 1に仮想IP 10.1.1.111を設定し、VRID 2に仮想IP 10.1.3.111を設定します。

RTAが両VRIDのマスターにするためにプライオリティを110に設定します。

[RTA]interface GigabitEthernet 0/0

[RTA-GigabitEthernet0/0]vrrp vrid 1 virtual-ip 10.1.1.111

[RTA-GigabitEthernet0/0]vrrp vrid 1 priority 110

[RTA-GigabitEthernet0/0]vrrp vrid 1 preempt-mode delay 500

[RTA-GigabitEthernet0/0]quit

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]vrrp vrid 2 virtual-ip 10.1.3.111

[RTA-GigabitEthernet0/1]vrrp vrid 2 priority 110

[RTA-GigabitEthernet0/1]vrrp vrid 2 preempt-mode delay 500

[RTA-GigabitEthernet0/1]quit

RTBのVRID 1に仮想IP 10.1.1.111を設定し、VRID 2に仮想IP 10.1.3.111を設定します。

[RTB]int GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]vrrp vrid 1 virtual-ip 10.1.1.111
[RTB-GigabitEthernet0/0]vrrp vrid 1 priority 100
[RTB-GigabitEthernet0/0]vrrp vrid 1 preempt-mode delay 500
[RTB-GigabitEthernet0/0]quit
[RTB]int GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]vrrp vrid 2 virtual-ip 10.1.3.111
[RTB-GigabitEthernet0/1]vrrp vrid 2 priority 100
[RTB-GigabitEthernet0/1]vrrp vrid 2 preempt-mode delay 500
[RTB-GigabitEthernet0/1]quit

タスク3：RTA, RTBにOSPFを設定する

手順1：RTAとRTB間にケーブルを接続しRTA, RTBにIPアドレスを設定する

RTAにIPアドレスを割り当てます。

[RTA] interface GigabitEthernet 0/2
[RTA-GigabitEthernet0/2]ip address 10.1.2.1 24
[RTA-GigabitEthernet0/2]quit

#RTBにIPアドレスを割り当てます。

[RTB] interface GigabitEthernet 0/2
[RTB-GigabitEthernet0/2]ip address 10.1.2.2 24
[RTB-GigabitEthernet0/2]quit

手順2：RTA, RTBにOSPFを設定する

RTAにOSPFを設定します

[RTA]router id 1.1.1.1
[RTA]ospf 1
[RTA-ospf-1]area 0
[RTA-ospf-1-area-0.0.0.0]network 10.1.1.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]network 10.1.2.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]network 10.1.3.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0]quit
[RTA-ospf-1]quit

RTBにOSPFを設定します

[RTB]router id 2.2.2.2

[RTB]ospf 1

[RTB-ospf-1]area 0

[RTB-ospf-1-area-0.0.0.0]network 10.1.1.0 0.0.0.255

[RTB-ospf-1-area-0.0.0.0]network 10.1.2.0 0.0.0.255

[RTB-ospf-1-area-0.0.0.0]network 10.1.3.0 0.0.0.255

[RTB-ospf-1-area-0.0.0.0]quit

[RTB-ospf-1]quit

タスク4：OSPFの状態を確認する

RTAのOSPFの状態を確認します。

<RTA>dis ospf peer

OSPF Process 1 with Router ID 1.1.1.1

Neighbor Brief Information

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
2.2.2.2	10.1.1.2	1	38	Full/DR	GE0/0
2.2.2.2	10.1.3.2	1	40	Full/DR	GE0/1
2.2.2.2	10.1.2.2	1	39	Full/DR	GE0/2

RTBのOSPFの状態を確認します。

<RTB>display ospf peer

OSPF Process 1 with Router ID 2.2.2.2

Neighbor Brief Information

Area: 0.0.0.0

Router ID	Address	Pri	Dead-Time	State	Interface
1.1.1.1	10.1.1.1	1	38	Full/BDR	GE0/0
1.1.1.1	10.1.3.1	1	39	Full/BDR	GE0/1
1.1.1.1	10.1.2.1	1	31	Full/BDR	GE0/2

RTAのルーティングテーブルを表示します。

ここで分かるようにVRID 1の仮想IP 10.1.1.111、VRID 2の仮想IP 10.1.3.111の

マスターがRTAにあることが分かります(RTBのルーティングテーブルと比較してみてください)。

<RTA>dis ip routing-table

Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	Direct	0	0	10.1.1.1	GE0/0
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.111/32	Direct	1	0	127.0.0.1	InLoop0
10.1.1.255/32	Direct	0	0	10.1.1.1	GE0/0
10.1.2.0/24	Direct	0	0	10.1.2.1	GE0/2
10.1.2.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.2.255/32	Direct	0	0	10.1.2.1	GE0/2
10.1.3.0/24	Direct	0	0	10.1.3.1	GE0/1
10.1.3.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.3.111/32	Direct	1	0	127.0.0.1	InLoop0
10.1.3.255/32	Direct	0	0	10.1.3.1	GE0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

RTBのルーティングテーブルを表示します。

<RTB>display ip routing-table

Destinations : 16 Routes : 16

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	Direct	0	0	10.1.1.2	GE0/0
10.1.1.2/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.255/32	Direct	0	0	10.1.1.2	GE0/0
10.1.2.0/24	Direct	0	0	10.1.2.2	GE0/2
10.1.2.2/32	Direct	0	0	127.0.0.1	InLoop0
10.1.2.255/32	Direct	0	0	10.1.2.2	GE0/2
10.1.3.0/24	Direct	0	0	10.1.3.2	GE0/1
10.1.3.2/32	Direct	0	0	127.0.0.1	InLoop0
10.1.3.255/32	Direct	0	0	10.1.3.2	GE0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0

```
127.255.255.255/32 Direct  0    0          127.0.0.1       InLoop0
224.0.0.0/4        Direct  0    0          0.0.0.0         NULL0
224.0.0.0/24       Direct  0    0          0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0          127.0.0.1       InLoop0
```

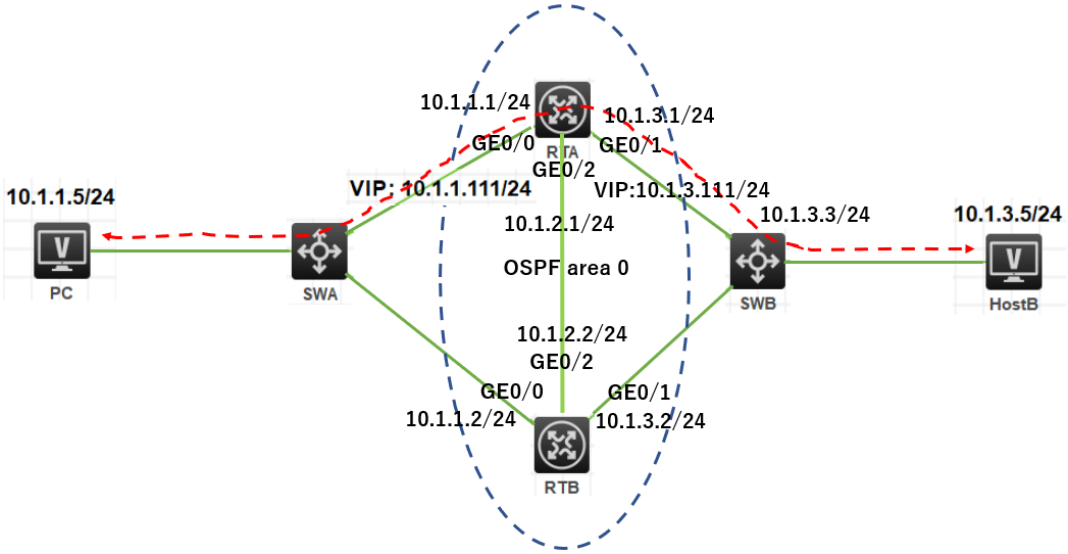
タスク5：VRRPの状態を確認する

```
# RTAのVRRPの状態を確認します。
# 先ほどのRTAのルーティングテーブルでRTAが仮想IPのマスターであることが分かり
# ましたが、ここでもそれが裏付けられました。
<RTA>display vrrp
IPv4 Virtual Router Information:
 Running mode          : Standard
 Total number of virtual routers : 2
 Interface             VRID   State        Running Adver   Auth
Virtual
                                           Pri     Timer   Type
IP
 ------------------------------------------------------------------------------
 GE0/0                 1      Master       110     100     Not supported
10.1.1.111
 GE0/1                 2      Master       110     100     Not supported
10.1.3.111

# RTBのVRRPの状態を確認します。
<RTB>display vrrp
IPv4 Virtual Router Information:
 Running mode          : Standard
 Total number of virtual routers : 2
 Interface             VRID   State        Running Adver   Auth
Virtual
                                           Pri     Timer   Type
IP
 ------------------------------------------------------------------------------
 GE0/0                 1      Backup       100     100     Not supported
10.1.1.111
 GE0/1                 2      Backup       100     100     Not supported
10.1.3.111
```

タスク6：PCとHostB間の疎通確認をします

現状は下図の通りです。



PCからHostBへpingします。

<PC>ping 10.1.3.5

Ping 10.1.3.5 (10.1.3.5): 56 data bytes, press CTRL_C to break

56 bytes from 10.1.3.5: icmp_seq=0 ttl=254 time=3.000 ms

56 bytes from 10.1.3.5: icmp_seq=1 ttl=254 time=5.000 ms

56 bytes from 10.1.3.5: icmp_seq=2 ttl=254 time=7.000 ms

56 bytes from 10.1.3.5: icmp_seq=3 ttl=254 time=4.000 ms

56 bytes from 10.1.3.5: icmp_seq=4 ttl=254 time=7.000 ms

HostBからPCへpingします。

<HostB>ping 10.1.1.5

Ping 10.1.1.5 (10.1.1.5): 56 data bytes, press CTRL_C to break

56 bytes from 10.1.1.5: icmp_seq=0 ttl=254 time=3.000 ms

56 bytes from 10.1.1.5: icmp_seq=1 ttl=254 time=7.000 ms

56 bytes from 10.1.1.5: icmp_seq=2 ttl=254 time=7.000 ms

56 bytes from 10.1.1.5: icmp_seq=3 ttl=254 time=7.000 ms

56 bytes from 10.1.1.5: icmp_seq=4 ttl=254 time=7.000 ms

タスク7：VRID 1のマスターに接続されているSWAのポートをshutdownして切り替えの状態を確認します。

手順1：PCからHostBへpingを続けます

手順2：SWAのG1/0/2をshutdownする

SWAのG1/0/2をshutdownします。

[SWA]interface GigabitEthernet 1/0/2

[SWA-GigabitEthernet1/0/2]shutdown

[SWA-GigabitEthernet1/0/2]%Dec 21 16:38:04:456 2021 SWA IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/2 changed to down.

%Dec 21 16:38:04:456 2021 SWA IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/2 changed to down.

手順3：PCからHostBへのpingの状態を確認します

手順1でG1/0/2をshutdownした直後に2つパケットが欠落しましたが、すぐにVRRPとOSPFにより代替ルートが用意されました。

<PC>ping -c 5000 10.1.3.5

Ping 10.1.3.5 (10.1.3.5): 56 data bytes, press CTRL_C to break

56 bytes from 10.1.3.5: icmp_seq=0 ttl=254 time=3.000 ms

56 bytes from 10.1.3.5: icmp_seq=1 ttl=254 time=8.000 ms

56 bytes from 10.1.3.5: icmp_seq=2 ttl=254 time=8.000 ms

56 bytes from 10.1.3.5: icmp_seq=3 ttl=254 time=7.000 ms

56 bytes from 10.1.3.5: icmp_seq=4 ttl=254 time=7.000 ms

56 bytes from 10.1.3.5: icmp_seq=5 ttl=254 time=6.000 ms

56 bytes from 10.1.3.5: icmp_seq=67 ttl=254 time=7.000 ms

56 bytes from 10.1.3.5: icmp_seq=68 ttl=254 time=7.000 ms

56 bytes from 10.1.3.5: icmp_seq=69 ttl=254 time=7.000 ms

Request time out

Request time out

56 bytes from 10.1.3.5: icmp_seq=72 ttl=253 time=8.000 ms

56 bytes from 10.1.3.5: icmp_seq=73 ttl=253 time=7.000 ms

56 bytes from 10.1.3.5: icmp_seq=74 ttl=253 time=7.000 ms

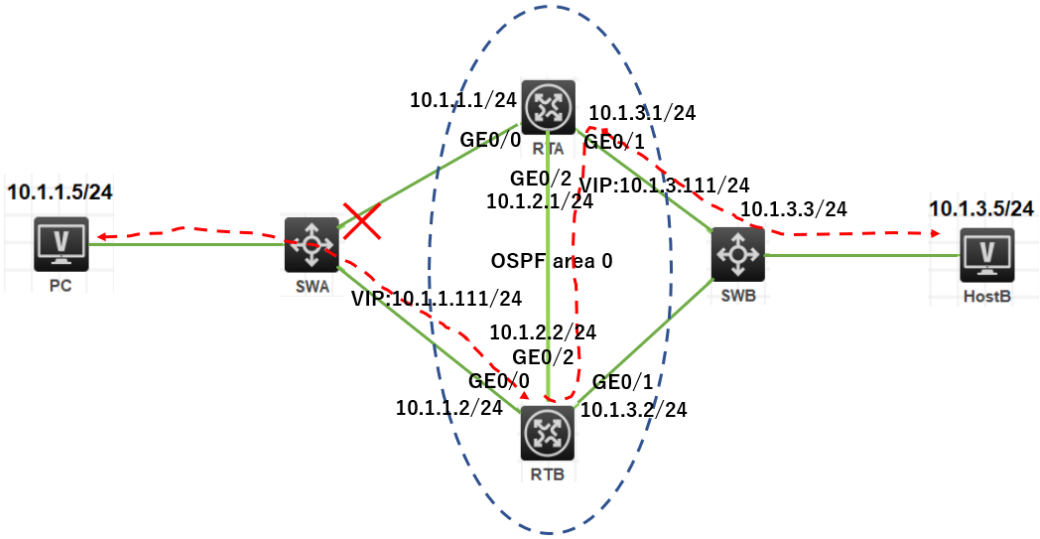
56 bytes from 10.1.3.5: icmp_seq=72 ttl=253 time=8.000 ms

56 bytes from 10.1.3.5: icmp_seq=73 ttl=253 time=7.000 ms

56 bytes from 10.1.3.5: icmp_seq=74 ttl=253 time=7.000 ms

手順4：RTA, RTBのルーティングテーブルを表示します

RTAのルーティングテーブルを表示します。RTAのルーティングテーブルから分かることは、仮想IP 10.1.1.111はRTBに移りましたが、仮想IP 10.1.3.111は相変わらずRTAにあります。そのためOSPFは経路障害後にRTBに到着した10.1.3.0宛のパケットをRTAに転送するルートを構築しました(VRRPによりRTBからSWBの経路は閉じていることを思い出してください)。



<RTA>dis ip routing-table

Destinations : 15 Routes : 16

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	O_INTRA	10	2	10.1.2.2	GE0/2
	O_INTRA	10	2	10.1.3.2	GE0/1
10.1.2.0/24	Direct	0	0	10.1.2.1	GE0/2
10.1.2.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.2.255/32	Direct	0	0	10.1.2.1	GE0/2
10.1.3.0/24	Direct	0	0	10.1.3.1	GE0/1
10.1.3.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.3.111/32	Direct	1	0	127.0.0.1	InLoop0
10.1.3.255/32	Direct	0	0	10.1.3.1	GE0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

RTBのルーティングテーブルを表示します

<RTB>display ip routing-table

Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface

```
0.0.0.0/32            Direct  0    0           127.0.0.1       InLoop0
10.1.1.0/24           Direct  0    0           10.1.1.2        GE0/0
10.1.1.2/32           Direct  0    0           127.0.0.1       InLoop0
10.1.1.111/32         Direct  1    0           127.0.0.1       InLoop0
10.1.1.255/32         Direct  0    0           10.1.1.2        GE0/0
10.1.2.0/24           Direct  0    0           10.1.2.2        GE0/2
10.1.2.2/32           Direct  0    0           127.0.0.1       InLoop0
10.1.2.255/32         Direct  0    0           10.1.2.2        GE0/2
10.1.3.0/24           Direct  0    0           10.1.3.2        GE0/1
10.1.3.2/32           Direct  0    0           127.0.0.1       InLoop0
10.1.3.255/32         Direct  0    0           10.1.3.2        GE0/1
127.0.0.0/8           Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32          Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
224.0.0.0/4           Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24          Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
```

手順5：RTA, RTBのvrrpの状態を表示します

RTAのvrrpの状態を表示します。

```
<RTA>display vrrp
IPv4 Virtual Router Information:
 Running mode          : Standard
 Total number of virtual routers : 2
 Interface             VRID   State        Running Adver    Auth
Virtual
                                           Pri      Timer    Type
IP
 ------------------------------------------------------------------------------
 GE0/0                 1      Initialize   110      100      Not supported
10.1.1.111
 GE0/1                 2      Master       110      100      Not supported
10.1.3.111
```

RTBのvrrpの状態を表示します。

```
<RTB>display vrrp
IPv4 Virtual Router Information:
 Running mode          : Standard
```

Total number of virtual routers : 2

Interface	VRID	State	Running Pri	Adver Timer	Auth Type	Virtual IP
GE0/0	1	Master	100	100	Not supported	10.1.1.111
GE0/1	2	Backup	100	100	Not supported	10.1.3.111

タスク8：VRID 2のマスターに接続されているSWAのポートをshutdownして切り替えの状態を確認します。

手順1：SWAのG1/0/2をundo shutdownする

手順2：PCからHostBへpingを続けます

手順3：SWAのG1/0/3をshutdownする

SWAのG1/0/3をshutdownします。

[SWA]interface GigabitEthernet 1/0/3

[SWA-GigabitEthernet1/0/3]shutdown

[SWA-GigabitEthernet1/0/3]%Dec 21 16:38:04:456 2021 SWA IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/3 changed to down.

%Dec 21 16:38:04:456 2021 SWA IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/3 changed to down.

手順4：PCからHostBへpingのpingの状態を確認します

手順2でG1/0/2をshutdownしましたが、すぐにVRRPとOSPFにより代替ルートが用意されパケットの欠落はみられませんでした。

<PC>ping -c 5000 10.1.3.5

Ping 10.1.3.5 (10.1.3.5): 56 data bytes, press CTRL_C to break

56 bytes from 10.1.3.5: icmp_seq=0 ttl=254 time=3.000 ms

56 bytes from 10.1.3.5: icmp_seq=1 ttl=254 time=8.000 ms

56 bytes from 10.1.3.5: icmp_seq=2 ttl=254 time=8.000 ms

56 bytes from 10.1.3.5: icmp_seq=0 ttl=254 time=3.000 ms

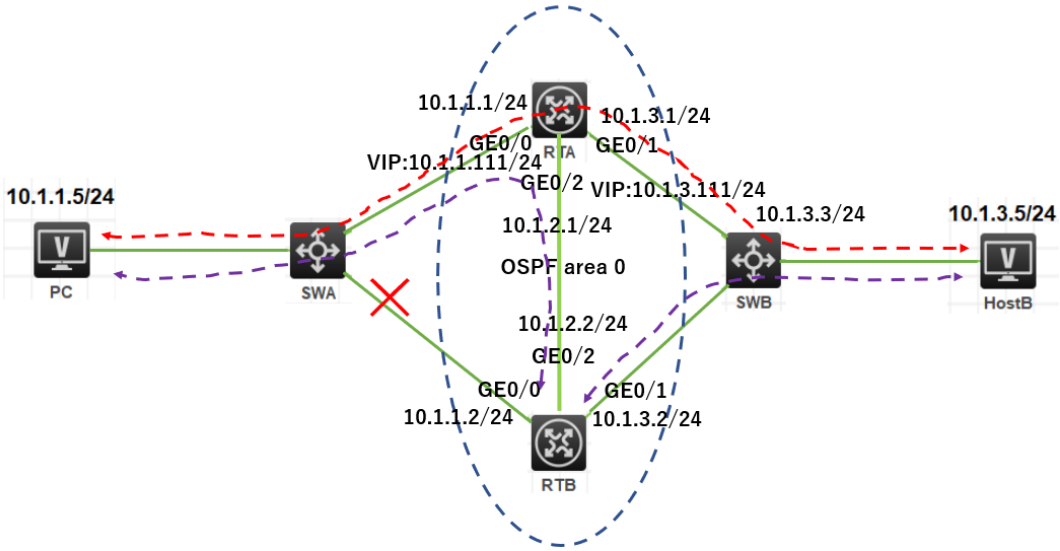
56 bytes from 10.1.3.5: icmp_seq=1 ttl=254 time=8.000 ms

56 bytes from 10.1.3.5: icmp_seq=2 ttl=254 time=8.000 ms

手順5：RTA, RTBのルーティングテーブルを表示します

RTAのルーティングテーブルを表示します

ここで分かるようにVRID 1の仮想IP 10.1.1.111、VRID 2の仮想IP 10.1.3.111の
マスターがRTAに戻ったことが分かります(RTBのルーティングテーブルと
比較してみてください)。



<RTA>dis ip routing-table
Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.0/24	Direct	0	0	10.1.1.1	GE0/0
10.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.1.111/32	Direct	1	0	127.0.0.1	InLoop0
10.1.1.255/32	Direct	0	0	10.1.1.1	GE0/0
10.1.2.0/24	Direct	0	0	10.1.2.1	GE0/2
10.1.2.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.2.255/32	Direct	0	0	10.1.2.1	GE0/2
10.1.3.0/24	Direct	0	0	10.1.3.1	GE0/1
10.1.3.1/32	Direct	0	0	127.0.0.1	InLoop0
10.1.3.111/32	Direct	1	0	127.0.0.1	InLoop0
10.1.3.255/32	Direct	0	0	10.1.3.1	GE0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0

```
255.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
```

RTBのルーティングテーブルを表示します

```
<RTB>display ip routing-table
Destinations : 14        Routes : 15
Destination/Mask    Proto   Pre Cost      NextHop         Interface
0.0.0.0/32          Direct  0   0         127.0.0.1       InLoop0
10.1.1.0/24         O_INTRA 10  2           10.1.2.1        GE0/2
                    O_INTRA 10  2           10.1.3.1        GE0/1
10.1.2.0/24         Direct  0   0         10.1.2.2        GE0/2
10.1.2.2/32         Direct  0   0         127.0.0.1       InLoop0
10.1.2.255/32       Direct  0   0         10.1.2.2        GE0/2
10.1.3.0/24         Direct  0   0         10.1.3.2        GE0/1
10.1.3.2/32         Direct  0   0         127.0.0.1       InLoop0
10.1.3.255/32       Direct  0   0         10.1.3.2        GE0/1
127.0.0.0/8         Direct  0   0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0         127.0.0.1       InLoop0
127.255.255.255/32 Direct  0    0         127.0.0.1       InLoop0
224.0.0.0/4         Direct  0   0         0.0.0.0         NULL0
224.0.0.0/24        Direct  0   0         0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0         127.0.0.1       InLoop0
```

手順6：RTA, RTBのvrrpの状態を表示します

RTAのvrrpの状態を表示します。

```
<RTA>display vrrp
IPv4 Virtual Router Information:
 Running mode          : Standard
 Total number of virtual routers : 2
 Interface             VRID   State        Running Adver   Auth
Virtual
                                           Pri      Timer   Type
IP
 ------------------------------------------------------------------------------
 GE0/0                 1      Master       110      100     Not supported
10.1.1.111
 GE0/1                 2      Master       110      100     Not supported
10.1.3.111
```

RTBのvrrpの状態を表示します。

```
<RTB>dis vrrp
IPv4 Virtual Router Information:
  Running mode            : Standard
  Total number of virtual routers : 2
  Interface                VRID   State        Running Adver   Auth
Virtual
                                                Pri      Timer    Type
IP
  --------------------------------------------------------------------------------
  GE0/0                    1      Initialize   100      100      Not supported
10.1.1.111
  GE0/1                    2      Backup       100      100      Not supported
10.1.3.111
```

Lab18 HDLC

実習内容と目標

このラボでは以下のことを学びます：

- HDLC のコンフィグレーションを習得します。

ネットワーク図

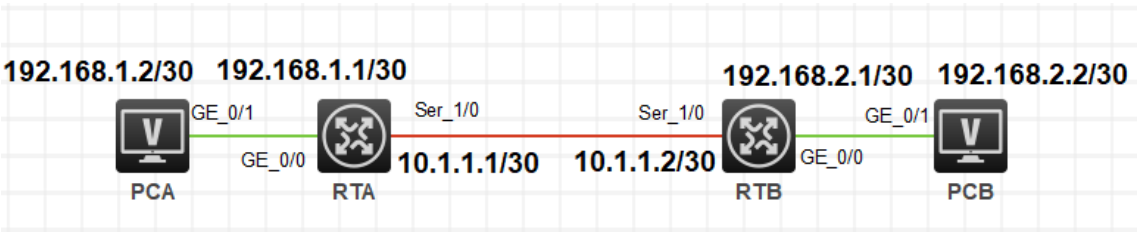


図 15.1 実習ネットワーク

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
PC	Windows 7	2	なし
V.35 DCEシリアルケーブル	-	1	
V.35 DTEシリアルケーブル		1	
ネットワークケーブルの接続	--	2	なし

実習手順

タスク1：PC間のコミュニケーションができるようにルーターでHDLCをenableにします

手順1：PCとルーターをケーブルで接続する

図15.1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

.....

手順2：PCとルーターにIPアドレスをアサインします

表15-1 IPアドレス割り当てスキーマ

装置	**インターフェース**	**IPアドレス**	**ゲートウェイ**
PCA		192.168.1.2/30	192.168.1.1
PCB		192.168.2.2/30	192.168.2.1
RTA	S1/0	10.1.1.1/30	-
	G0/0	192.168.1.1	
RTB	S1/0	10.1.1.2/30	-
	G0/0	192.168.2.1	

手順3：ルーターのWANインターフェースにHDLCのカプセル化とIPアドレスの割り当てを設定します

RTAのWANインターフェースSerial 1/0(DCE)を設定します

[RTA]interface Serial 1/0

[RTA-Serial1/0]link-protocol hdlc
%Nov 30 09:57:27:531 2021 RTA IFNET/5/LINK_UPDOWN: Line protocol state on the interface Serial1/0 changed to down.
%Nov 30 09:57:27:534 2021 RTA IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to down.
%Nov 30 09:57:31:861 2021 RTA IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to up.
[RTA-Serial1/0]baudrate 2048000
[RTA-Serial1/0]ip address 10.1.1.1 255.255.255.252
[RTA-Serial1/0]quit

RTBのWANインターフェースSerial 1/0(DTE)を設定します
[RTB]interface Serial 1/0
[RTB-Serial1/0]link-protocol hdlc
%Nov 30 10:00:01:880 2021 RTB IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to down.
%Nov 30 10:00:04:914 2021 RTB IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to up.
%Nov 30 10:00:04:918 2021 RTB IFNET/5/LINK_UPDOWN: Line protocol state on the interface Serial1/0 changed to up.
[RTB-Serial1/0]ip address 10.1.1.2 255.255.255.252
[RTB-Serial1/0]quit

ノート：シリアルインターフェースのボーレートを設定するためにドbaudrateコマンドを使用します。 ボーレート2048000は、シリアルインターフェースの物理速度が2048000bpsであることを意味します。
このコマンドは、DCEデバイスでのみ使用できます。

RTAで**display interface**コマンドにより設定を確認します。
[RTA]display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1500

Hold timer: 10 seconds, retry times: 5
Internet address: 10.1.1.1/30 (primary)
Link layer protocol: HDLC
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 10 minutes 33 seconds
Last clearing of counters: Never
Current system time:2021-11-30 10:10:39
Last time when physical state changed to up:2021-11-30 10:00:05
Last time when physical state changed to down:2021-11-30 10:00:02
上記の出力は、serial1/0の物理状態がUPであることを示しており、物理インターフェースが使用可能であることを示しています。

ノート: ルーターのインターフェースタイプは、接続されているケーブルによって異なります。 ケーブルがDCEの場合、ルータのインターフェースタイプはDCEです。 ケーブルがDTEの場合、ルーターのインターフェースタイプはDTEです。

手順4：ルーターのGigabitEthernetインターフェースにIPアドレスを割り当てます
RTAのGigabitEthernet0/0インターフェースにIPアドレスを割り当てます。
[RTA]interface GigabitEthernet 0/0
[RTA-GigabitEthernet0/0]ip address 192.168.1.1 30
[RTA-GigabitEthernet0/0]quit

RTBのGigabitEthernet0/0インターフェースにIPアドレスを割り当てます。
[RTB]interface GigabitEthernet 0/0
[RTB-GigabitEthernet0/0]ip address 192.168.2.1 30
[RTB-GigabitEthernet0/0]quit
手順5：ルーター、PCとゲートウェイ間の接続性をチェックします
RTAからPCAにpingします
<RTA>ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=2.000 ms

56 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=2.000 ms

RTAからRTBのWANインターフェースにpingします

<RTA>ping 10.1.1.2

Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL_C to break

56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=2.000 ms

56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=1.000 ms

56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.000 ms

56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms

56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=1.000 ms

手順6：2台のPCへのルートを設定します。

RTAでPCBへのルートを設定します。

[RTA]ip route-static 192.168.2.0 255.255.255.252 10.1.1.2

RTBでPCAへのルートを設定します。

[RTB]ip route-static 192.168.1.0 255.255.255.252 10.1.1.1

手順7：pingコマンドを使ってPCAとPCB間の接続性をチェックします。

PCAからPCBへpingします。もし、両者がお互いに到達できるなら、以下の出力を得ることができます。

<H3C>ping 192.168.1.2

Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break

56 bytes from 192.168.1.2: icmp_seq=0 ttl=253 time=2.000 ms

56 bytes from 192.168.1.2: icmp_seq=1 ttl=253 time=5.000 ms

56 bytes from 192.168.1.2: icmp_seq=2 ttl=253 time=5.000 ms

56 bytes from 192.168.1.2: icmp_seq=3 ttl=253 time=3.000 ms

56 bytes from 192.168.1.2: icmp_seq=4 ttl=253 time=2.000 ms

質問:

1．2つのHDLCピアが異なるキープアライブ間隔で設定されている場合、リンクは正常に機能しますか？

答え:

リンクが繰り返しup/downする場合があります。

Lab19 PPPのコンフィギュレーション

実習内容と目標

このラボでは以下のことを学びます：

- HDLC のコンフィグレーションを習得します。
- PPP 接続の完全な基本構成。
- PPP PAP 認証の完全な構成。
- PPP CHAP 認証の完全な構成。
- PPP の一般的な監視および保守コマンドに関する知識とスキルを理解し、理解する

ネットワーク図

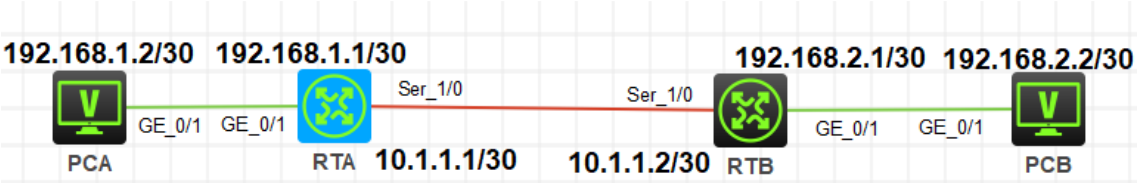


図 16.1 実習ネットワーク

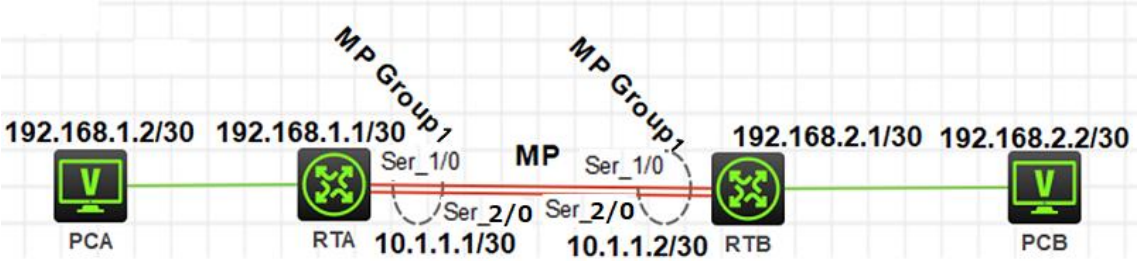


図 16.2 実習ネットワーク

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
PC	Windows 7	2	なし
V.35 DCEシリアルケーブル	-	2	

V.35 DTEシリアルケーブル		2	
ネットワークケーブルの接続	--	2	なし

実習手順

表16-1はPCとルーターに設定するIPアドレスです。

表16-1 IPアドレス割り当てスキーマ

装置	**インターフェース**	**IPアドレス**	**ゲートウェイ**
PCA		192.168.1.2/30	192.168.1.1
PCB		192.168.2.2/30	192.168.2.1
RTA	S1/0	10.1.1.1/30	PPP試験用
	MP-Group 1	10.1.1.1/30	PPP MP試験用
RTB	S1/0	10.1.1.2/30	PPP試験用
	MP-Group 2	10.1.1.2/30	PPP MP試験用

タスク1：PPPの基本的な設定をします

手順1：PCとルーターをケーブルで接続する

図15.1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
.....
```

手順2：PCとルーターにIPアドレスをアサインします

手順3： RTAのWANポートのためのPPPカプセル化の設定とIPアドレスの割り当て

```
[RTA]interface Serial 1/0
```

[RTA-Serial1/0]link-protocol ppp
[RTA-Serial1/0]ip address 10.1.1.1 255.255.255.252
[RTA-Serial1/0]baudrate 2048000
[RTA-Serial1/0]quit

PPPのカプセル化の後、主にLCPとIPCPの情報を見るためにdisplay interfaceコマンドを実行します。
[RTA]display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 10.1.1.1/30 (primary)
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 20 minutes 4 seconds
Last clearing of counters: Never
Current system time:2021-11-30 17:25:08
Last time when physical state changed to up:2021-11-30 17:05:03
Last time when physical state changed to down:2021-11-30 17:01:24

手順4：RTBのWANポートのためのPPPカプセル化の設定とIPアドレスの割り当て
[RTB]interface Serial 1/0
[RTB-Serial1/0]link-protocol ppp
[RTB-Serial1/0]ip address 10.1.1.2 255.255.255.252
[RTB-Serial1/0]quit

PPPのカプセル化の後、主にLCPとIPCPの情報を見るためにdisplay interfaceコマンドを実行します。
[RTB]display interface Serial 1/0
Serial1/0

Current state: UP
Line protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 10.1.1.2/30 (primary)
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 25 minutes 53 seconds
Last clearing of counters: Never
Current system time:2021-11-30 17:31:07
Last time when physical state changed to up:2021-11-30 17:05:15
Last time when physical state changed to down:2021-11-30 17:05:06

手順5：PC間とルーターのゲートウェイとの接続性をチェックします

RTAのLANポートにIPアドレスを割り当てます。

[RTA]int GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ip address 192.168.1.1 30
[RTA-GigabitEthernet0/1]quit

RTBのLANポートにIPアドレスを割り当てます。

[RTB]int GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ip address 192.168.2.1 30
[RTB-GigabitEthernet0/1]quit

RTAとPCA間の接続性をチェックするためにpingコマンドを実行します。

[RTA]ping 192.168.1.2
Ping 192.168.1.2 (192.168.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.2: icmp_seq=0 ttl=255 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 192.168.1.2: icmp_seq=2 ttl=255 time=0.000 ms
56 bytes from 192.168.1.2: icmp_seq=3 ttl=255 time=3.000 ms
56 bytes from 192.168.1.2: icmp_seq=4 ttl=255 time=1.000 ms

RTAとRTBのWANポートとの接続性をチェックします。

[RTA]ping 10.1.1.2

Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL_C to break

56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms

56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=2.000 ms

56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=2.000 ms

56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=0.000 ms

56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=1.000 ms

手順6：2つのルーターに隣接するLANセグメントへのルートをそれぞれ設定します

RTAでPCBネットワークセグメントへのルートを設定します。

[RTA]ip route-static 192.168.2.0 255.255.255.252 10.1.1.2

RTBでPCAネットワークセグメントへのルートを設定します。

[RTB]ip route-static 192.168.1.0 255.255.255.252 10.1.1.1

手順7：PCAまたはPCBで接続性をチェックするためにpingコマンドを実行します。

PCAでPCBのIPアドレスへpingします。正常であれば以下の出力を得ることができます。

<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=3.000 ms

56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=5.000 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=4.000 ms

56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=2.000 ms

タスク2：PPP PAPの設定をします

テストをする前に、タスク1のようにルーターを初期状態に戻します。

手順1：PC、ルーターのIPアドレスを設定し、接続性を確実にします

PCとルーターのLANIPアドレスを設定し、計画に基づいて接続を確認します。 特定のコマンドの詳細については、タスク1を参照してください。pingコマンドを実行して、PCとルーター間の接続を確認します。 デフォルトのカプセル化に基づいて、RTAはRTBにpingを実行できます。RTAとRTBでPCのあるセグメントへのstatic routeの設定をタスク1を参照して忘れずに設定してください。

手順2：RTAでローカルPAP認証に設定をします

RTAでローカルユーザーのユーザー名とパスワードを設定します。ユーザー名とパスワードはRTBと整合性があるようにします。

[RTA]local-user rtb class network

New local user added.
[RTA-luser-network-rtbclass]service-type ppp
[RTA-luser-network-rtbclass]password simple pwdpwd
[RTA-luser-network-rtbclass]quit

RTAでPAP認証を設定します。
[RTA]interface Serial 1/0
[RTA-Serial1/0]link-protocol ppp
[RTA-Serial1/0]ppp authentication-mode pap
[RTA-Serial1/0]ip address 10.1.1.1 255.255.255.252

認証モードの設定前にポートにIPアドレスが設定されていれば、認証設定を行った後にポートをリセットします。
[RTA-Serial1/0]shutdown
%Dec　1 10:11:47:246 2021 RTA IFNET/5/LINK_UPDOWN: Line protocol state on the interface Serial1/0 changed to down.
%Dec　1 10:11:47:246 2021 RTA IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to down.
[RTA-Serial1/0]undo shutdown
%Dec　1 10:11:55:175 2021 RTA IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to up.
[RTA-Serial1/0]quit

手順3：ポートの状態を表示し、接続性を確認します

display interfaceコマンドを使って設定したポートの情報を表示します。
[RTA]display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: DOWN
Description: Serial1/0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 10.1.1.1/30 (primary)
Link layer protocol: PPP
LCP: closed
Output queue - Urgent queuing: Size/Length/Discards 0/100/0

Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 0 minutes 16 seconds
Last clearing of counters: Never
Current system time:2021-12-01 10:12:10
Last time when physical state changed to up:2021-12-01 10:11:55
Last time when physical state changed to down:2021-12-01 10:11:47

そして、RTAでRTBへpingします。
[RTA]ping 10.1.1.2
Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

手順4：RTBでPAP認証のためにユーザー名とパスワードを設定します

RTBでPAP認証のユーザー名とパスワードを設定します。そして、IPアドレスを割り当てます。
[RTB]interface Serial 1/0
[RTB-Serial1/0]link-protocol ppp
[RTB-Serial1/0]ppp pap local-user rtb password simple pwdpwd
[RTB-Serial1/0]ip address 10.1.1.2 255.255.255.252
[RTB-Serial1/0]quit
PAP認証プロセスを思い出してください。 PAP認証は、2つのハンドシェイクで構成されています。 まず、認証されたパーティは、ユーザー名とパスワードをプレーンテキストモードで認証パーティに送信します。 このテストでは、RTBは認証されたパーティであり、ユーザー名rtbとパスワードpwdpwdを認証パーティRTAに送信します。 RTAは情報を確認します。
PAP認証は安全ではありません。

手順5：RTAとRTB間のポートの状態を確認し、接続性を確認します

pingコマンドで接続性をチェックし、display interface Serial 1/0コマンドで以下の情報を表示します。
[RTA]display interface Serial 1/0
Serial1/0
Current state: UP

Line protocol state: UP
Description: Serial1/0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 10.1.1.1/30 (primary)
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 32 minutes 35 seconds
Last clearing of counters: Never
Current system time:2021-12-01 10:44:29
Last time when physical state changed to up:2021-12-01 10:11:55
Last time when physical state changed to down:2021-12-01 10:11:47

RTAからRTBのWANインターフェースにpingします。
[RTA]ping 10.1.1.2
Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=3.000 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=3.000 ms

手順6：PCA又はPCBで接続性を確認するためにpingを実行します。

PCBのIPアドレスにPCAでpingします。ルーターの設定が正しければ、以下の結果を得られます。
<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=2.752 ms
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=2.891 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=5.876 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=5.945 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=3.580 ms

タスク3：PPP CHAPコンフィギュレーションを行う

テストをする前に、タスク1のようにルーターを初期状態に戻します。

手順1：PC、ルーターのIPアドレスを設定し、接続性を確実にします

PCとルーターのLANIPアドレスを設定し、計画に基づいて接続を確認します。 特定のコマンドの詳細については、タスク1を参照してください。デフォルトのPPPカプセル化に基づいて、2つのルーターが到達可能であるというpingコマンドを実行します。

手順2：RTBでCHAP認証のためにユーザー名とパスワードを設定します

[RTA]local-user rtb class network

New local user added.

[RTA-luser-network-rtbclass]service-type ppp

[RTA-luser-network-rtbclass]password simple pwdpwd

[RTA-luser-network-rtbclass]quit

CHAP認証モードを設定し、インターフェースにIPアドレスを割り当てます。

[RTA]interface Serial 1/0

[RTA-Serial1/0]ppp authentication-mode chap

[RTA-Serial1/0]ip address 10.1.1.1 255.255.255.252

認証モードの設定前にポートにIPアドレスが設定されていれば、認証設定を行った後にポートをリセットします。

[RTA-Serial1/0]shutdown

%Dec　1 11:17:34:121 2021 RTA IFNET/5/LINK_UPDOWN: Line protocol state on the interface Serial1/0 changed to down.

%Dec　1 11:17:34:122 2021 RTA IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to down.

[RTA-Serial1/0]undo shutdown

%Dec　1 11:17:45:686 2021 RTA IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to up.

[RTA-Serial1/0]quit

手順3：RTAとRTB間のポートの状態を確認し、接続性を確認します

display interfaceコマンドを使って設定したポートの情報を表示します。

[RTA]display interface Serial 1/0

Serial1/0

Current state: UP

Line protocol state: DOWN

Description: Serial1/0 Interface

Bandwidth: 64 kbps

Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 10.1.1.1/30 (primary)
Link layer protocol: PPP
LCP: closed
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 7 minutes 40 seconds
Last clearing of counters: Never
Current system time:2021-12-01 11:25:25
Last time when physical state changed to up:2021-12-01 11:17:45
Last time when physical state changed to down:2021-12-01 11:17:34

そして、RTAでRTBへpingします。
[RTA]ping 10.1.1.2
Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL_C to break
Request time out
Request time out
Request time out
Request time out
Request time out

手順4：RTBで認証モードをCHAPに設定し、認証のためにユーザー名とパスワードを設定します

RTBのコンフィギュレーションは以下の通りです。
[RTB]interface Serial 1/0
[RTB-Serial1/0]ppp chap user rtb
[RTB-Serial1/0]ppp chap password simple pwdpwd
[RTB-Serial1/0]quit

手順5：ポートの状態を表示し、接続性を確認します

pingコマンドで接続性をチェックし、display interface Serial 1/0コマンドで以下の情報を表示します。
[RTA]display interface Serial 1/0
Serial1/0
Current state: UP
Line protocol state: UP

Description: Serial1/0 Interface
Bandwidth: 64 kbps
Maximum transmission unit: 1500
Hold timer: 10 seconds, retry times: 5
Internet address: 10.1.1.1/30 (primary)
Link layer protocol: PPP
LCP: opened, IPCP: opened
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last link flapping: 0 hours 13 minutes 4 seconds
Last clearing of counters: Never
Current system time:2021-12-01 11:30:50
Last time when physical state changed to up:2021-12-01 11:17:45
Last time when physical state changed to down:2021-12-01 11:17:34

[RTA]ping 10.1.1.2
Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=2.000 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=1.000 ms

手順6：PCA又はPCBで接続性を確認するためにpingを実行します。

PCBのIPアドレスにPCAでpingします。ルーターの設定が正しければ、以下の結果を得られます。

<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=2.752 ms
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=2.891 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=5.876 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=5.945 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=3.580 ms

タスク4：PPP MPコンフィギュレーションを行う

テストをする前に、タスク1のようにルーターを初期状態に戻します。MPでは、RTAとRTB間を2本のV35ケーブルで接続します。

手順1： RTAとRTBでMP-Groupを作成し、IPアドレスを割り当てます。

RTAのコンフィギュレーションは以下の通りです。

[RTA]interface MP-group 1

[RTA-MP-group1]ip address 10.1.1.1 30

[RTA-MP-group1]quit

RTBのコンフィギュレーションは以下の通りです。

[RTB]interface MP-group 1

[RTB-MP-group1]ip address 10.1.1.2 30

[RTB-MP-group1]quit

手順2：RTAとRTBの物理ポートをMP-Groupに追加します

RTAとRTBの物理ポートをMP-Groupに追加します。そして、物理ポートにPPPカプセル化を設定します。

RTAのコンフィギュレーションは以下の通りです。

[RTA]interface Serial 1/0

[RTA-Serial1/0]link-protocol ppp

[RTA-Serial1/0]ppp mp MP-group 1

[RTA-Serial1/0]quit

%Dec 1 11:47:06:205 2021 RTA IFNET/5/LINK_UPDOWN: Line protocol state on the interface Serial1/0 changed to down.

%Dec 1 11:47:09:281 2021 RTA IFNET/5/LINK_UPDOWN: Line protocol state on the interface Serial1/0 changed to up.

[RTA]interface Serial 2/0

[RTA-Serial2/0]link-protocol ppp

[RTA-Serial2/0]ppp mp MP-group 1

[RTA-Serial2/0]quit

RTBのコンフィギュレーションは以下の通りです。

[RTB]interface Serial 1/0

[RTB-Serial1/0]ppp mp mp

[RTB-Serial1/0]link-protocol ppp

[RTB-Serial1/0]ppp mp MP-group 1

[RTB-Serial1/0]quit

%Dec 1 11:52:19:285 2021 RTB IFNET/5/LINK_UPDOWN: Line protocol state on the interface Serial1/0 changed to down.

%Dec 1 11:52:22:370 2021 RTB IFNET/5/LINK_UPDOWN: Line protocol state on the interface Serial1/0 changed to up.

%Dec　1 11:52:22:370 2021 RTB IFNET/5/LINK_UPDOWN: Line protocol state on the interface MP-group1 changed to up.

%Dec　1 11:52:22:372 2021 RTB IFNET/3/PHY_UPDOWN: Physical state on the interface MP-group1 changed to up.

[RTB]interface Serial 2/0

[RTB-Serial2/0]link-protocol ppp

[RTB-Serial2/0]ppp mp MP-group 1

[RTB-Serial2/0]quit

手順3：MPの状態を確認する

[RTA]display ppp mp

----------Slot0----------

Template: MP-group1

max-bind: 16, fragment: enabled, min-fragment: 128

Master link: MP-group1, Active members: 2, Bundle Multilink

Peer's endPoint descriptor: MP-group1

Sequence format: long (rcv)/long (sent)

Bundle Up Time: 2021/12/01　12:07:53:422

0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved

Sequence: 0 (rcv)/0 (sent)

Active member channels: 2 members

Serial1/0	Up-Time:2021/12/01　12:07:53:422
Serial2/0	Up-Time:2021/12/01　12:07:53:422

[RTA]display interface MP-group 1

MP-group1

Current state: UP

Line protocol state: UP

Description: MP-group1 Interface

Bandwidth: 128 kbps

Maximum transmission unit: 1500

Hold timer: 10 seconds, retry times: 5

Internet address: 10.1.1.1/30 (primary)

Link layer protocol: PPP

LCP: opened, MP: opened, IPCP: opened

Physical: MP, baudrate: 128000 bps

Output queue - Urgent queuing: Size/Length/Discards 0/100/0

Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
Last clearing of counters: Never
Last 300 seconds input rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 bits/sec, 0 packets/sec
Input: 4 packets, 48 bytes, 0 drops
Output: 6 packets, 72 bytes, 0 drops

RTAでRTBのIPアドレスにpingします。
[RTA]ping 10.1.1.2
Ping 10.1.1.2 (10.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 10.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 10.1.1.2: icmp_seq=1 ttl=255 time=3.000 ms
56 bytes from 10.1.1.2: icmp_seq=2 ttl=255 time=3.000 ms
56 bytes from 10.1.1.2: icmp_seq=3 ttl=255 time=3.000 ms
56 bytes from 10.1.1.2: icmp_seq=4 ttl=255 time=2.000 ms

質問:

1．CHAP認証中に、RTBポートS1 / 0がppp chap password simple pwdpwdで設定されていない場合、RTBがRTAから認証要求を受信したときに、RTBはCHAPの2回目のハンドシェイクを完了し、RTAに応答を返すにはどうすればよいですか。 RTBには追加の構成が必要ですか？

答え:

CHAPの原則に従って、認証されたパーティは、ローカルポートがデフォルトのCHAPパスワードで設定されていないことを検出すると、認証パーティのユーザー名に基づいて、ローカルテーブルからユーザー名に対応するパスワードを検索します。
したがって、RTBはローカルユーザー名とピアパスワードで設定する必要があります。
[RTB]local-user rta class network
New local user added.
[RTB-luser-network-rta]service-type ppp
[RTB-luser-network-rta]password simple pwdpwd
[RTB-luser-network-rta]quit

RTAでppp chap userコマンドを実行して、ユーザー名rtaを送信します。
[RTA]interface Serial 1/0
[RTA-Serial1/0]ppp chap user rta

[RTA-Serial1/0]quit

2. MPに認証が必要な場合、どのように構成できますか？

答え:
MP-gooupに追加された物理ポートの認証モードを構成します。例えば:
[RTB]interface Serial 1/0
[RTB-Serial1/0]link-protocol ppp
[RTB-Serial1/0]ppp authentication-mode pap
[RTB-Serial1/0]ppp pap local-user rtb password simple pwdpwd
[RTB-Serial1/0]quit

3. ステップ2とタスク1では、RTAボーレートは2048000 bpsですが、RTB仮想ボーレートは64000bpsです。どうして？

答え:
同期シリアルポートは、ケーブルタイプに応じて電気的機能を選択します。このテストでは、RTBはDTEデバイスです。同期されたシリアルポートはDTEデバイスとして機能し、DCEデバイスからクロックを受信します。ポートには、使用に影響を与えない仮想ボーレートが表示されます。実質的には、ボーレートはDCEデバイスのボーレートと一致しています。次のコマンドを実行して、仮想ボーレートをDCEデバイスのボーレートに変更します。

ノート: HCLの場合、virtualbaudrate 2048000はサポートされておりません。

[RTB]interface Serial 1/0
[RTB-Serial1/0]virtualbaudrate 2048000
[RTB-Serial1/0]shutdown
%Dec 1 13:14:37:548 2021 RTB IFNET/5/LINK_UPDOWN: Line protocol state on the interface Serial1/0 changed to down.
%Dec 1 13:14:37:551 2021 RTB IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to down.
[RTB-Serial1/0]undo shutdown
%Dec 1 13:14:41:927 2021 RTB IFNET/3/PHY_UPDOWN: Physical state on the interface Serial1/0 changed to up.
[RTB-Serial1/0]quit

Lab20 PPPoEのコンフィギュレーション

実習内容と目標

このラボでは以下のことを学びます：

- PPPoE 接続の基本構成。
- PPPoE CHAP 認証の完全な構成。
- PPPoE の一般的な監視および保守コマンドに関する知識とスキルを理解し、理解する

ネットワーク図

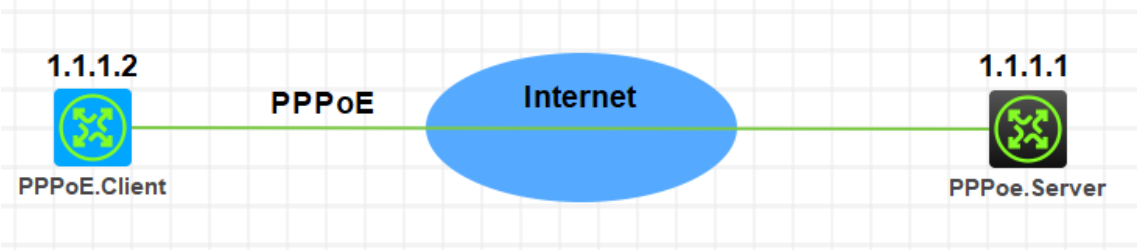


図 5.1 実習ネットワーク

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
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

表5.1はルーターに設定するIPアドレスです。

表5.1 IPアドレス割り当てスキーマ

装置	インターフェース	IPアドレス	ゲートウェイ
PPPoE.Server	Virtual template 1	1.1.1.1/8	
PPPoE.Client	dialer 1	ppp-negotiate	dialer 1

タスク1：PPPoEの基本的な設定をします

手順1：ルーター同士をLANケーブルで接続する

図5.1のようにルーター間のケーブルを接続します。

PPPoE Server、PPPoE Client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
.....
```

手順2：PPPoE ServerのWANポートのためのPPPカプセル化の設定とIPアドレスの割り当て

```
< H3C> system-view
[H3C] sysname PPPoE.Server
[PPPoE.Server]interface Virtual-Template 1
[PPPoE.Server-Virtual-Template1]ppp authentication-mode chap domain system
[PPPoE.Server-Virtual-Template1]ppp chap user h3c
[PPPoE.Server-Virtual-Template1]ip address 1.1.1.1 255.0.0.0
[PPPoE.Server-Virtual-Template1]remote address 1.1.1.2
```

[PPPoE.Server -Virtual-Template1]quit
[PPPoE.Server]interface GigabitEthernet 0/1
[PPPoE.Server-GigabitEthernet0/1]pppoe-server bind virtual-template 1
[PPPoE.Server-GigabitEthernet0/1]quit

手順3：PPPoE Serverのdomainの認証をppp loallにする
[PPPoE.Server]domain name system
[PPPoE.Server-isp-system]authentication ppp local
[PPPoE.Server-isp-system]quit
手順4：PPPoEのローカルユーザーを作成する
[PPPoE.Server]local-user h3c class network
New local user added.
[PPPoE.Server -luser-network-h3c]password simple h3c
[PPPoE.Server -luser-network-h3c]service-type ppp
[PPPoE.Server -luser-network-h3c]authorization-attribute user-role network-operator
[PPPoE.Server -luser-network-h3c]quit

PPPカプセル化後にLCPの情報を確認するためにdisplay interface virtual-Template 1コマンドを実行します。

<PPPoE.Server>display interface Virtual-Template 1
Virtual-Template1
Current state: DOWN
Line protocol state: DOWN
Description: Virtual-Template1 Interface
Bandwidth: 100000 kbps
Maximum transmission unit: 1454
Hold timer: 10 seconds, retry times: 5
Internet address: 1.1.1.1/8 (primary)
Link layer protocol: PPP
LCP: initial
Physical: None, baudrate: 100000000 bps
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0

タスク2：PPP CHAPの設定をします

テストをする前に、タスク1のようにルーターを初期状態に戻します。

手順1：PPPoE ClientのWANポートのためのPPPカプセル化の設定とIPアドレスの設定

```
< H3C> system-view
[H3C] sysname PPPoE.Client
[PPPoE.Client]interface Dialer 1
[PPPoE.Client]ppp chap user h3c
[PPPoE.Client]ppp chap password simple h3c
[PPPoE.Client]dialer bundle enable
[PPPoE.Client]dialer timer idle 0
[PPPoE.Client]dialer timer autodial 60
[PPPoE.Client]ip address ppp-negotiate
[PPPoE.Client]quit
[PPPoE.Client]interface GigabitEthernet 0/1
[PPPoE.Client -GigabitEthernet0/1]pppoe-client dial-bundle-number 1
%Mar 31 16:30:01:358 2022 H3C IFNET/5/LINK_UPDOWN: Line protocol state on
the interface Dialer1 changed to down.
[PPPoE.Client -GigabitEthernet0/1]quit
%Mar 31 16:31:07:856 2022 H3C IFNET/5/LINK_UPDOWN: Line protocol state on
the interface Dialer1 changed to up.
```

手順2： PPPoE Clientでデフォルトゲートウェイの設定をします

```
[PPPoE.Client]ip route-static 1.1.1.1 32 Dialer 1
[PPPoE.Client]quit
< PPPoE.Client>
```

ルーティングテーブルを表示します。

```
<PPPoE.Client>display ip routing-table
Destinations : 10          Routes : 10
Destination/Mask    Proto   Pre Cost        NextHop         Interface
0.0.0.0/32          Direct  0   0           127.0.0.1       InLoop0
1.1.1.1/32          Direct  0   0           1.1.1.1         Dia1
1.1.1.2/32          Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/8         Direct  0   0           127.0.0.1       InLoop0
127.0.0.0/32        Direct  0   0           127.0.0.1       InLoop0
127.0.0.1/32        Direct  0   0           127.0.0.1       InLoop0
127.255.255.255/32  Direct  0   0           127.0.0.1       InLoop0
```

```
224.0.0.0/4          Direct  0    0          0.0.0.0         NULL0
224.0.0.0/24         Direct  0    0          0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0          127.0.0.1       InLoop0
```

手順3：PPPoE ServerでPPPoEセッションのデバッグをします

```
<PPPoE.Server>debugging pppoe-server all
<PPPoE.Server>debugging dialer all
DDR is not configured.
<PPPoE.Server>display pppoe-server session summary
Total PPPoE sessions: 1
Local PPPoE sessions: 1

  Ethernet interface: GE0/1                Session ID: 1
  PPP index: 0x140000085                     State: OPEN
  Remote MAC: b238-66d3-0206                 Local MAC: b224-7e8e-
0106
  Service VLAN: N/A                          Customer VLAN: N/A
<PPPoE.Server>display pppoe-server session packet
Total PPPoE sessions: 1
Local PPPoE sessions: 1

  Ethernet interface: GE0/1                Session ID: 1
  InPackets: 79                              OutPackets: 82
  InBytes: 825                               OutBytes: 875
  InDrops: 0                                 OutDrops: 0
<PPPoE.Server>reset pppoe-server all
<PPPoE.Server>display pppoe-server session summary
<PPPoE.Server>display pppoe-server session packet
<PPPoE.Server>ping 1.1.1.2
Ping 1.1.1.2 (1.1.1.2): 56 data bytes, press CTRL_C to break
Request time out
Request time out
--- Ping statistics for 1.1.1.2 ---
3 packet(s) transmitted, 0 packet(s) received, 100.0% packet loss
<PPPoE.Server>%Mar 31 16:39:18:830 2022 H3C PING/6/PING_STATISTICS:
Ping statistics for 1.1.1.2: 3 packet(s) transmitted, 0 packet(s) received, 100.0%
```

packet loss.

手順4：PPPoE ClientからPPPoE ServerのIPアドレスに対しpingをします

```
<PPPoE.Client>ping 1.1.1.1
Ping 1.1.1.1 (1.1.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.1: icmp_seq=0 ttl=255 time=0.000 ms
56 bytes from 1.1.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 1.1.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 1.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 1.1.1.1: icmp_seq=4 ttl=255 time=0.000 ms

--- Ping statistics for 1.1.1.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.000/0.400/1.000/0.490 ms
%Mar 31 16:38:37:675 2022 H3C IFNET/5/LINK_UPDOWN: Line protocol state on the
```

手順5：PPPoE ClientでPPPoE Serverとの接続を確認します

```
<PPPoE.Client>debugging pppoe-client all
<PPPoE.Client>debugging dialer all
<PPPoE.Client>display pppoe-client session summary
Bundle ID       Interface       VA              RemoteMAC          LocalMAC
State
1          1        GE0/1           VA0             b224-7e8e-0106 b238-66d3-0206
SESSION
<PPPoE.Client>display pppoe-client session packet
Bundle:       1                          Interface:    GE0/1
InPackets: 5                          OutPackets: 4
InBytes:     230                       OutBytes:     78
InDrops:     0                         OutDrops:     0
<PPPoE.Client>display dialer
Dialer1
  Dialer Route:
  Dialer number:
  Dialer Timers(in seconds):
    Auto-dial: 60          Compete: 20             Enable: 5
    Idle: 0                Wait-for-Carrier: 60
  Total Channels: 1
  Free Channels: 0
```

手順6：PPPoE ServerでPPPoE Clientとの接続を確認します

```
<PPPoE.Server>debugging pppoe-server all
<PPPoE.Server >debugging dialer all
DDR is not configured.
<PPPoE.Server>display pppoe-server session summary
Total PPPoE sessions: 1
Local PPPoE sessions: 1

  Ethernet interface: GE0/1                Session ID: 1
  PPP index: 0x140000085                     State: OPEN
  Remote MAC: b238-66d3-0206                 Local MAC: b224-7e8e-0106
  Service VLAN: N/A                        Customer VLAN: N/A
<PPPoE.Server>display pppoe-server session packet
Total PPPoE sessions: 1
Local PPPoE sessions: 1

  Ethernet interface: GE0/1                Session ID: 1
  InPackets: 214                           OutPackets: 217
  InBytes: 3239                            OutBytes: 3509
  InDrops: 0                               OutDrops: 0
<PPPoE.Server>ping 1.1.1.2
Ping 1.1.1.2 (1.1.1.2): 56 data bytes, press CTRL_C to break
56 bytes from 1.1.1.2: icmp_seq=0 ttl=255 time=1.000 ms
56 bytes from 1.1.1.2: icmp_seq=1 ttl=255 time=0.000 ms
56 bytes from 1.1.1.2: icmp_seq=2 ttl=255 time=2.000 ms
56 bytes from 1.1.1.2: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 1.1.1.2: icmp_seq=4 ttl=255 time=0.000 ms
<PPPoE.Server>
```

Lab21 L2TP(LAC自動開始トンネリングモード)

実習内容と目標

このラボでは以下のことを学びます:

- L2TP のコンフィグレーションを習得します。
- LAC と LNS について学びます。
  - **LAC**: L2TP Access Concentrator(LAC)は、PPPとL2TPの両方に対応しています。通常は、ローカルISPに配置されたNetwork Access Server(NAS)で、主にPPPユーザーにアクセスサービスを提供します。

    LACは、L2TPトンネルのエンドポイントであり、LNSとリモートシステムの間にあります。L2TPを使用してリモートシステムから受信したパケットをカプセル化し、カプセル化されたパケットをLNSに送信します。LNSから受信したパケットをカプセル化解除し、カプセル化解除されたパケットを目的のリモートシステムに送信します。
  - **LNS**: L2TP Network Server(LNS)は、PPPおよびL2TPの両方に対応しています。通常、エンタープライズネットワーク上のエッジデバイスです。

    LNSは、L2TPトンネルのもう一方のエンドポイントです。これは、LACによってトンネリングされるPPPセッションの論理終端ポイントです。L2TPは、トンネルを確立することによって、PPPセッションの終端ポイントをNASからLNSに拡張します。
- LAC 自動開始トンネルについて学びます。
  - リモートシステムとLAC間の接続はダイヤルアップ接続に限定されず、任意のIPベースの接続にすることができます。
  - L2TPセッションは、L2TPトンネルが確立された直後に確立されます。次に、LACとLNSがそれぞれPPPoEクライアントとPPPoEサーバーとして動作し、PPPネゴシエーションを実行します。
  - LNSは、リモートシステムではなくLACにプライベートIPアドレスを割り当てます。

ネットワーク図

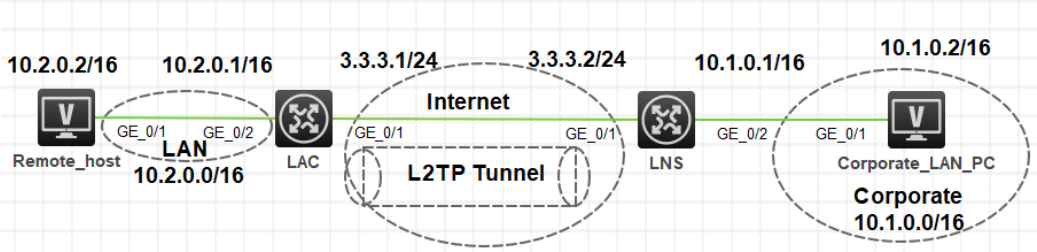


図 2.1 実習ネットワーク

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
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：LNSとのL2TPトンネルをLAC自動開始モードで確立するようにLACを設定します

手順1：PCとルーターをケーブルで接続する

図2.1のようにルーターとPC間のケーブルを接続します。

LAC、LNS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。

```
<LAC>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.
<LAC>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

.....

手順2：PCとルーターにIPアドレスをアサインします

表2-1 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
Remote host		10.2.0.2/16	10.2.0.1
Corporate_LAN_PC		10.1.0.2/16	10.1.0.1
NAC	G0/1	3.3.3.1/24	-
	G0/2	10.2.0.1/16	
LNS	G0/1	3.3.3.2/24	-
	G0/2	10.1.0.1/16	

手順3：LNSをコンフィギュレーションします

#インターフェイスのIPアドレスを設定します(詳細は省略します)。

#vpdnuserという名前のローカルユーザーを作成し、パスワードを設定して、PPPサービスを有効にします。

<LNS> system-view

[LNS] local-user vpdnuser class network

[LNS-luser-network-vpdnuser] password simple Hello

[LNS-luser-network-vpdnuser] service-type ppp

[LNS-luser-network-vpdnuser] quit

#Create Virtual-Template 1にIPアドレスを割り当て、PPP認証モードを次のように指定する。

PAPを使用し、IPアドレス192.168.0.10をPPPユーザーに割り当てます。

[LNS] interface virtual-template 1

[LNS-virtual-template1] ip address 192.168.0.1 24

[LNS-virtual-template1] ppp authentication-mode pap

[LNS-virtual-template1] remote address 192.168.0.10

[LNS-virtual-template1] quit

#ISPドメインシステムでPPPユーザーのローカル認証を設定します。

[LNS] domain system

[LNS-isp-system] authentication ppp local

[LNS-isp-system] quit

#L2TPをイネーブルにし、LNSモードでL2TPグループ1を作成します。

[LNS] l2tp enable

[LNS] l2tp-group 1 mode lns

#ローカルトンネル名をLNSとして設定し、LACからのトンネリング要求を受信するVirtual-Template 1を指定します。

[LNS-l2tp1] tunnel name LNS

[LNS-l2tp1] allow l2tp virtual-template 1 remote LAC

#トンネル認証をイネーブルにし、認証キーをaabbccとして設定します。

[LNS-l2tp1] tunnel authentication

[LNS-l2tp1] tunnel password simple aabbcc

[LNS-l2tp1] quit

#ネクストホップアドレスが192.168.0.10(LNSがLACのVirtual-PPP 1に割り当てるIPアドレス)のスタティックルートを設定して、PPPユーザー宛てのパケットがL2TPトンネル経由で転送されるようにします。

[LNS] ip route-static 10.2.0.0 16 192.168.0.10

手順4：LACをコンフィギュレーションします

#インターフェイスのIPアドレスを設定します(詳細は省略)。

#L2TPをイネーブルにします。

<LAC> system-view

[LAC] l2tp enable

#L2TPグループ1をLACモードで作成します。

[LAC] l2tp-group 1 mode lac

#ローカルトンネル名をLACとして設定し、トンネルピア(LNS)のIPアドレスを指定します。

[LAC-l2tp1] tunnel name LAC

[LAC-l2tp1] lns-ip 3.3.3.2

#トンネル認証をイネーブルにし、認証キーをaabbccとして設定します。

[LAC-l2tp1] tunnel authentication

[LAC-l2tp1] tunnel password simple aabbcc

[LAC-l2tp1] quit

#Virtual-PPP 1を作成し、ユーザー名とパスワードをvpdnuserとHelloとに設定し、PPP認証はPAPを使います。

[LAC] interface virtual-ppp 1

[LAC-Virtual-PPP1] ip address ppp-negotiate

[LAC-Virtual-PPP1] ppp pap local-user vpdnuser password simple Hello

[LAC-Virtual-PPP1] quit

#企業ネットワーク宛てのパケットがL2TPトンネルを介して転送されるように、スタティックルートを設定します。

[LAC] ip route-static 10.1.0.0 16 virtual-ppp 1

#LACをトリガーして、LNSとのL2TPトンネルを確立します。

[LAC] interface virtual-ppp 1

[LAC-Virtual-PPP1] l2tp-auto-client l2tp-group 1

手順5：リモートホストで、LACをゲートウェイとして設定します

手順6：設定の確認

#LNSで、display L2TP sessionコマンドを使用して、確立されたL2TPセッションを表示します。

[LNS] display l2tp session

LocalSID	RemoteSID	LocalTID	State
21409	3395	4501	Established

#LNSで、確立されたL2TPトンネルを表示するには、display L2TP tunnelコマンドを使用します。

[LNS] display l2tp tunnel

LocalTID	State	Sessions	RemotePort
RemoteTID		RemoteAddress	RemoteName

4501524Established13.3.3.11701LAC

#LNSで、LAC側のプライベートネットワークアドレスである10.2.0.1にpingできることを確認します。これは、10.2.0.0/16上のホストと10.1.0.0/16上のホストがL2TPトンネルを介して相互に通信できることを示します。

[LNS] ping -a 10.1.0.1 10.2.0.1

Ping 10.2.0.1 (10.2.0.1): 56 data bytes, press CTRL_C to break

56 bytes from 10.2.0.1: icmp_seq=0 ttl=128 time=1.000 ms

56 bytes from 10.2.0.1: icmp_seq=1 ttl=128 time=1.000 ms

56 bytes from 10.2.0.1: icmp_seq=2 ttl=128 time=1.000 ms

56 bytes from 10.2.0.1: icmp_seq=3 ttl=128 time=1.000 ms

56 bytes from 10.2.0.1: icmp_seq=4 ttl=128 time=1.000 ms

--- Ping statistics for 10.2.0.1 ---

5 packet(s) transmitted, 5 packet(s) received, 0.0%
packet loss round-trip min/avg/max/std-dev =
1.000/1.000/1.000/0.000 ms

Lab22 IPsecVPNの設定

実習内容と目標

このラボでは以下のことを学びます：

- IPsec で IKE メインモード、事前共有鍵認証方式を習得します。
- IPsec で IKE アグレッシブモード、事前共有鍵認証方式を習得します。

ネットワーク図

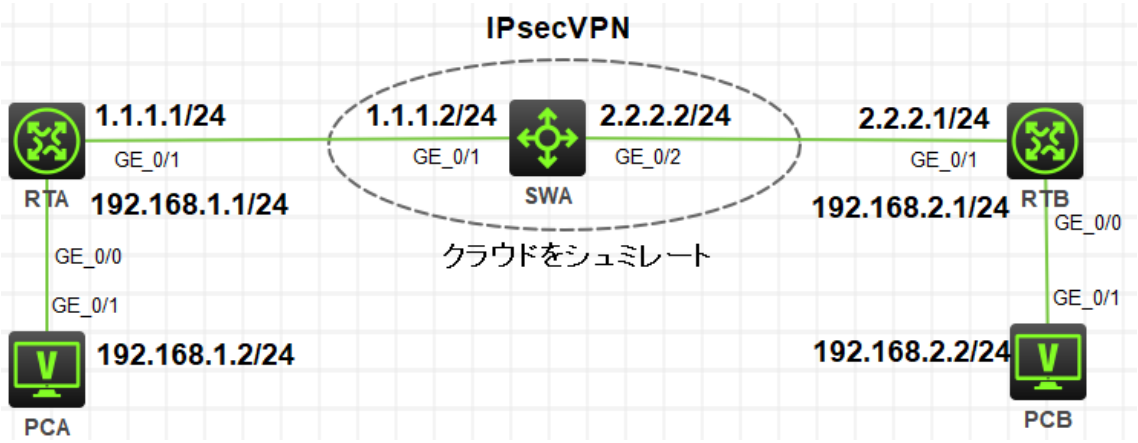


図 4.1 実習ネットワーク

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**	ルーター
S5820V2	**Version7.1**	**1**	スイッチ
PC	**Windows 7**	**2**	ホスト
ネットワークケーブルの接続	--	**4**	ストレートケーブル

実習手順

タスク1：それぞれの装置にIPアドレスを設定する

この実習ではRTAとRTB間IKE認証によるIPsecトンネルの接続をどのようにするかを示

します。そして、どのようにフェーズ1でメインモードを使い、事前共有鍵認証を行うIKEを設定するかを示します。

手順1：両PCにIPアドレス、ゲートウェイアドレスを設定する

PC、ルーター、そしてスイッチを図4-1のように接続します。そして、スイッチにはVLAN 2を作成し、VLAN 2にGE1/0/2を追加します。

[H3C]vlan 2

[H3C-vlan2]port gi

[H3C-vlan2]port GigabitEthernet 1/0/2

[H3C-vlan2]quit

アドレスおよびデフォルトゲートウェイは表3-1に従って設定します。RTAをPCAのデフォルトゲートウェイに、RTBをPCBのデフォルトゲートウェイに設定します。

表3-1 IPアドレス割り当て

装置	インターフェイス	IPアドレス	ゲートウェイ
RTA	G0/0	192.168.1.1/24	-
	G0/1	1.1.1.1/24	-
RTB	G0/0	192.168.2.1/24	-
	G0/1	2.2.2.1/24	-
SWA	VLAN 1	1.1.1.2/24	
	VLAN 2	2.2.2.2/24	
PCA		192.168.1.2/24	192.168.1.1/24
PCB		192.168.2.2/24	192.168.2.1/24

手順2：ルーティングプロトコルを設定する

RTA，RTB，SWAに以下のようにOSPFを設定します。

[RTA-ospf-1]area 0

[RTA-ospf-1-area-0.0.0.0]network 1.1.1.0 0.0.0.255

[RTA-ospf-1-area-0.0.0.0]quit

[RTA-ospf-1]quit

[SWA]ospf 1

[SWA-ospf-1]area 0

[SWA-ospf-1-area-0.0.0.0]network 1.1.1.0 0.0.0.255

[SWA-ospf-1-area-0.0.0.0]network 2.2.2.0 0.0.0.255

[SWA-ospf-1-area-0.0.0.0]quit

[SWA-ospf-1]quit

[RTB]ospf 1
[RTB-ospf-1]area 0
[RTB-ospf-1-area-0.0.0.0]network 2.2.2.0 0.0.0.255
[RTB-ospf-1-area-0.0.0.0]quit
[RTB-ospf-1]quit

上記のように設定後、SWAは公共ネットワークをシミュレートしていて、公共ネットワークルートのみ保存しています。これはサブネット192.168.1.0/24と192.168.2.0/24へのルートを持っていません。なぜならば、OSPFエリアPCAとPCBに接続されているルーターインタフェースへのルートを含んでいません。

各ルーターでリモートプライベートネットワークへのスタティックルートを以下のように設定します。
[RTA]ip route-static 192.168.2.0 255.255.255.0 1.1.1.2
[RTB]ip route-static 192.168.1.0 255.255.255.0 2.2.2.2

上記設定完了後、RTA，RTB，SWAのルーティングテーブルを表示します。
[RTA]display ip routing-table
Destinations : 18 Routes : 18

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	Direct	0	0	1.1.1.1	GE0/1
1.1.1.0/32	Direct	0	0	1.1.1.1	GE0/1
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.255/32	Direct	0	0	1.1.1.1	GE0/1
2.2.2.0/24	O_INTRA	10	2	1.1.1.2	GE0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.0/24	Direct	0	0	192.168.1.1	GE0/0
192.168.1.0/32	Direct	0	0	192.168.1.1	GE0/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.255/32	Direct	0	0	192.168.1.1	GE0/0
192.168.2.0/24	Static	60	0	1.1.1.2	GE0/1

```
224.0.0.0/4             Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24            Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0

<SWA>display ip routing-table
Destinations : 16        Routes : 16
Destination/Mask    Proto   Pre Cost      NextHop         Interface
0.0.0.0/32              Direct  0    0           127.0.0.1       InLoop0
1.1.1.0/24              Direct  0    0           1.1.1.2         Vlan1
1.1.1.0/32              Direct  0    0           1.1.1.2         Vlan1
1.1.1.2/32              Direct  0    0           127.0.0.1       InLoop0
1.1.1.255/32            Direct  0    0           1.1.1.2         Vlan1
2.2.2.0/24              Direct  0    0           2.2.2.2         Vlan2
2.2.2.0/32              Direct  0    0           2.2.2.2         Vlan2
2.2.2.2/32              Direct  0    0           127.0.0.1       InLoop0
2.2.2.255/32            Direct  0    0           2.2.2.2         Vlan2
127.0.0.0/8             Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32            Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32            Direct  0    0           127.0.0.1       InLoop0
127.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0
224.0.0.0/4             Direct  0    0           0.0.0.0         NULL0
224.0.0.0/24            Direct  0    0           0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0           127.0.0.1       InLoop0

[RTB]display ip routing-table
Destinations : 18        Routes : 18
Destination/Mask    Proto   Pre Cost      NextHop         Interface
0.0.0.0/32              Direct  0    0           127.0.0.1       InLoop0
1.1.1.0/24              O_INTRA 10   2           2.2.2.2         GE0/1
2.2.2.0/24              Direct  0    0           2.2.2.1         GE0/1
2.2.2.0/32              Direct  0    0           2.2.2.1         GE0/1
2.2.2.1/32              Direct  0    0           127.0.0.1       InLoop0
2.2.2.255/32            Direct  0    0           2.2.2.1         GE0/1
127.0.0.0/8             Direct  0    0           127.0.0.1       InLoop0
127.0.0.0/32            Direct  0    0           127.0.0.1       InLoop0
127.0.0.1/32            Direct  0    0           127.0.0.1       InLoop0
```

```
127.255.255.255/32 Direct  0    0          127.0.0.1       InLoop0
192.168.1.0/24     Static  60   0          2.2.2.2         GE0/1
192.168.2.0/24     Direct  0    0          192.168.2.1     GE0/0
192.168.2.0/32     Direct  0    0          192.168.2.1     GE0/0
192.168.2.1/32     Direct  0    0          127.0.0.1       InLoop0
192.168.2.255/32   Direct  0    0          192.168.2.1     GE0/0
224.0.0.0/4        Direct  0    0          0.0.0.0         NULL0
224.0.0.0/24       Direct  0    0          0.0.0.0         NULL0
255.255.255.255/32 Direct  0    0          127.0.0.1       InLoop0
```

この結果は、SWAのルーティングテーブルにはプライベートネットワークへのルートを持っていないことを表しています。

以下のように、PCAとPCB間の接続を確認します。

```
<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
```

この結果は、PCAはPCBにpingできないことを表しています。この結果の理由はSWAがPCBへのルートを持っていないからです。

手順3：IKEプロポーザルを設定する

```
[RTA]ike proposal 1
[RTA-ike-proposal-1]authentication-method pre-share
[RTA-ike-proposal-1]authentication-algorithm md5
[RTA-ike-proposal-1]encryption-algorithm 3des-cbc
[RTA-ike-proposal-1]quit

[RTB]ike proposal 1
[RTB-ike-proposal-1]authentication-method pre-share
[RTB-ike-proposal-1]authentication-algorithm md5
[RTB-ike-proposal-1]encryption-algorithm 3des-cbc
[RTB-ike-proposal-1]quit
```

手順4：IKE keychainを設定する

[RTA]ike keychain keychain1

[RTA-ike-keychain-keychain1]pre-shared-key address 2.2.2.1 255.255.255.0 key sim

ple h3c

[RTA-ike-keychain-keychain1]quit

[RTB]ike keychain keychain1

[RTB-ike-keychain-keychain1]pre-shared-key address 1.1.1.1 255.255.255.0 key sim

ple h3c

[RTB-ike-keychain-keychain1]quit

手順5：IKE profileを設定する

Pre-shared keyを使う

[RTA]ike profile profile1

[RTA-ike-profile-profile1]local-identity address 1.1.1.1

[RTA-ike-profile-profile1]match remote identity address 2.2.2.1 255.255.255.0

[RTA-ike-profile-profile1]keychain keychain1

[RTA-ike-profile-profile1]proposal 1

[RTA-ike-profile-profile1]quit

[RTB]ike profile profile1

[RTB-ike-profile-profile1]local-identity address 2.2.2.1

[RTB-ike-profile-profile1]match remote identity address 1.1.1.1 255.255.255.0

[RTB-ike-profile-profile1]keychain keychain1

[RTB-ike-profile-profile1]proposal 1

[RTB-ike-profile-profile1]quit

手順6：ACLを設定する

両ルーターがサブネット192.168.1.0/24と192.168.2.0/24との間のトラフィックを認識できるようにACLを設定します。

[RTA]acl advanced 3000

[RTA-acl-ipv4-adv-3000]rule 0 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255

[RTA-acl-ipv4-adv-3000]quit

[RTB]acl advanced 3000
[RTB-acl-ipv4-adv-3000]rule 0 permit ip source 192.168.2.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
[RTB-acl-ipv4-adv-3000]quit

手順7：IPsec proposalを設定する

[RTA]ipsec transform-set trans1
[RTA-ipsec-transform-set-trans1]esp authentication-algorithm sha1
[RTA-ipsec-transform-set-trans1]esp encryption-algorithm aes-cbc-128
[RTA-ipsec-transform-set-trans1]quit

[RTB]ipsec transform-set trans1
[RTB-ipsec-transform-set-trans1]esp authentication-algorithm sha1
[RTB-ipsec-transform-set-trans1]esp encryption-algorithm aes-cbc-128
[RTB-ipsec-transform-set-trans1]quit

手順8：IPsec policyの設定と適用

両ルーターにおいて、IPsec policyの設定と隣接する装置と接続されている物理インタフェースにそれを適用する。

[RTA]ipsec policy policy1 1 isakmp
[RTA-ipsec-policy-isakmp-policy1-1]remote-address 2.2.2.1
[RTA-ipsec-policy-isakmp-policy1-1]security acl 3000
[RTA-ipsec-policy-isakmp-policy1-1]transform-set trans1
[RTA-ipsec-policy-isakmp-policy1-1]ike-profile profile1
[RTA-ipsec-policy-isakmp-policy1-1]quit
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ipsec apply policy policy1
[RTA-GigabitEthernet0/1]quit

[RTB]ipsec policy policy1 1 isakmp
RTB-ipsec-policy-isakmp-policy1-1]remote-address 1.1.1.1
RTB-ipsec-policy-isakmp-policy1-1]security acl 3000
[RTB-ipsec-policy-isakmp-policy1-1]transform-set trans1
[RTB-ipsec-policy-isakmp-policy1-1]ike-profile profile1
[RTB-ipsec-policy-isakmp-policy1-1]quit
[RTB]interface GigabitEthernet 0/1

```
[RTB-GigabitEthernet0/1]ipsec apply policy policy1
[RTB-GigabitEthernet0/1]quit
```

手順9：設定を確認する

```
[RTA]display ike proposal
  Priority Authentication Authentication Encryption    Diffie-Hellman Duration
                     method           algorithm       algorithm           group
(seconds)
-------------------------------------------------------------------------------
  1        PRE-SHARED-KEY        MD5             3DES-CBC       Group 1
86400
  default  PRE-SHARED-KEY        SHA1            DES-CBC        Group 1
86400

[RTA]display ipsec transform-set
IPsec transform set: trans1
   State: complete
   Encapsulation mode: tunnel
   ESN: Disabled
   PFS:
   Transform: ESP
   ESP protocol:
      Integrity: SHA1
      Encryption: AES-CBC-128

[RTA]display ipsec policy
-----------------------------------------
IPsec Policy: policy1
Interface: GigabitEthernet0/1
-----------------------------------------

   ----------------------------
   Sequence number: 1
   Mode: ISAKMP
   ----------------------------
   Traffic Flow Confidentiality: Disabled
```

```
  Security data flow: 3000
  Selector mode: standard
  Local address:
  Remote address: 2.2.2.1
  Transform set:    tran1
  IKE profile: profile1
  IKEv2 profile:
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA idle time:

[RTB]display ike proposal
  Priority Authentication Authentication Encryption    Diffie-Hellman Duration
                     method           algorithm       algorithm           group
(seconds)
-------------------------------------------------------------------------------
  1        PRE-SHARED-KEY        MD5             3DES-CBC       Group 1
86400
  default  PRE-SHARED-KEY        SHA1            DES-CBC        Group 1
86400
[RTB]display ipsec transform-set
IPsec transform set: trans1
  State: complete
  Encapsulation mode: tunnel
  ESN: Disabled
  PFS:
  Transform: ESP
  ESP protocol:
    Integrity: SHA1
    Encryption: AES-CBC-128

[RTB]display ipsec policy
----------------------------------------
IPsec Policy: policy1
Interface: GigabitEthernet0/1
----------------------------------------
```

Sequence number: 1

Mode: ISAKMP

Traffic Flow Confidentiality: Disabled

Security data flow: 3000

Selector mode: standard

Local address:

Remote address: 1.1.1.1

Transform set: trans1

IKE profile: profile1

IKEv2 profile:

SA duration(time based): 3600 seconds

SA duration(traffic based): 1843200 kilobytes

SA idle time:

手順10:トンネルが確立されていて稼働しているかを確認する

PCAからPCBにpingして両PC間の接続を確認します。

<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

56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=2.000 ms

56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=9.000 ms

56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=2.000 ms

56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=4.000 ms

出力は、最初のICMPエコー要求がタイムアウトになり、他のすべての要求はタイムアウトしなかったことを示しています。 最初の要求がタイムアウトする前にIPsec SAsが使用できなかったため、最初の要求は破棄されました。 最初のリクエストがIKEネゴシエーションをトリガーし、次に予想されるIPsec SAsが推定され、後続のすべてのリクエストがIPsecトンネルを介して宛先に配信されました。

RTAとRTBのIPsecとIKE情報を表示します。

<RTA>display ike sa

<RTA>display ike sa

Connection-ID Remote Flag DOI

```
------------------------------------------------------------------
     2                2.2.2.1                RD              IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

<RTA>display ike sa verbose
<RTA>display ike sa verbose
    ----------------------------------------------
    Connection ID: 2
    Outside VPN:
    Inside VPN:
    Profile: profile1
    Transmitting entity: Initiator
    ----------------------------------------------
    Local IP: 1.1.1.1
    Local ID type: IPV4_ADDR
    Local ID: 1.1.1.1

    Remote IP: 2.2.2.1
    Remote ID type: IPV4_ADDR
    Remote ID: 2.2.2.1

    Authentication-method: PRE-SHARED-KEY
    Authentication-algorithm: MD5
    Encryption-algorithm: 3DES-CBC

    Life duration(sec): 86400
    Remaining key duration(sec): 85632
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected

    Extend authentication: Disabled
    Assigned IP address:

<RTA>display ipsec sa
```

```
<RTA>display ipsec sa
-------------------------------
Interface: GigabitEthernet0/1
-------------------------------

  ----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1428
    Tunnel:
        local    address: 1.1.1.1
        remote address: 2.2.2.1
    Flow:
        sour addr: 192.168.1.0/255.255.255.0    port: 0    protocol: ip
        dest addr: 192.168.2.0/255.255.255.0    port: 0    protocol: ip

    [Inbound ESP SAs]
      SPI: 2415685184 (0x8ffc6e40)
      Connection ID: 12884901889
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843199/2777
      Max received sequence-number: 4
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: N
      Status: Active
```

```
  [Outbound ESP SAs]
    SPI: 3646540216 (0xd959c9b8)
    Connection ID: 12884901888
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/2777
    Max sent sequence-number: 4
    UDP encapsulation used for NAT traversal: N
    Status: Active

<RTB>display ike sa
<RTB>display ike sa
  Connection-ID  Remote                  Flag          DOI
--------------------------------------------------------------------
  2              1.1.1.1                 RD            IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

<RTB>display ike sa verbose
<RTB>display ike sa verbose
  ----------------------------------------------
  Connection ID: 2
  Outside VPN:
  Inside VPN:
  Profile: profile1
  Transmitting entity: Responder
  ----------------------------------------------
  Local IP: 2.2.2.1
  Local ID type: IPV4_ADDR
  Local ID: 2.2.2.1

  Remote IP: 1.1.1.1
  Remote ID type: IPV4_ADDR
  Remote ID: 1.1.1.1

  Authentication-method: PRE-SHARED-KEY
```

```
    Authentication-algorithm: MD5
    Encryption-algorithm: 3DES-CBC

    Life duration(sec): 86400
    Remaining key duration(sec): 85506
    Exchange-mode: Main
    Diffie-Hellman group: Group 1
    NAT traversal: Not detected

    Extend authentication: Disabled
    Assigned IP address:

<RTB>display ipsec sa
<RTB>display ipsec sa
-------------------------------
Interface: GigabitEthernet0/1
-------------------------------

  -----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1428
    Tunnel:
        local    address: 2.2.2.1
        remote address: 1.1.1.1
    Flow:
        sour addr: 192.168.2.0/255.255.255.0    port: 0    protocol: ip
        dest addr: 192.168.1.0/255.255.255.0    port: 0    protocol: ip
```

[Inbound ESP SAs]
SPI: 1971329230 (0x758018ce)
Connection ID: 4294967296
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/2592
Max received sequence-number: 4
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 316893198 (0x12e3680e)
Connection ID: 4294967297
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/2592
Max sent sequence-number: 4
UDP encapsulation used for NAT traversal: N
Status: Active

IPsec policy: policy1
Sequence number: 1
Mode: ISAKMP

Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Path MTU: 1428
Tunnel:

```
    local    address: 2.2.2.1
    remote address: 1.1.1.1
  Flow:
    sour addr: 192.168.2.0/255.255.255.0    port: 0    protocol: ip
    dest addr: 192.168.1.0/255.255.255.0    port: 0    protocol: ip

  [Inbound ESP SAs]
    SPI: 3646540216 (0xd959c9b8)
    Connection ID: 4294967298
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/2677
    Max received sequence-number: 4
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 2415685184 (0x8ffc6e40)
    Connection ID: 4294967299
    Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843199/2677
    Max sent sequence-number: 4
    UDP encapsulation used for NAT traversal: N
    Status: Active
```

出力は、期待されるISAKMP SAとIOsec SAsがすべて確立されたことを示しています。RTAのインバウンドSAのSPIはRTBのアウトバウンドSAのSPIと一致し、RTAのアウトバウンドSAのSPIはRTAのインバウンドSAのSPIと一致します。 SAsは、同じ認証アルゴリズムと暗号化アルゴリズムを使用します。

手順11：IPsecの動作を監視する

存在する全てのIPsec SAとISAKMP SAをクリアする。

```
<RTA>reset ike sa
<RTA>reset ipsec sa
```

<RTB>reset ike sa
<RTB>reset ipsec sa

デバッグを有効にします。
<RTA>terminal monitor
The current terminal is enabled to display logs.
<RTA>terminal debugging
The current terminal is enabled to display debugging logs.
<RTA>debugging ike packet
<RTA>debugging ipsec packet

IPsecトンネルを確立するためにPCAからPCBへpingします。
<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
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=9.000 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=2.000 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=4.000 ms

デバッギング情報確認し、分析します。
<RTA>*Dec 27 10:59:36:781 2021 RTA IPSEC/7/PACKET:
Failed to find SA by SP, SP Index = 0, SP Convert-Seq = 65536.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Encryption algorithm is 3DES-CBC.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Hash algorithm is HMAC-MD5.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  DH group 1.
*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Authentication method is Pre-shared key.

*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Lifetime type is in seconds.

*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Life duration is 86400.

*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Construct transform payload for transform 1.

*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Constructed SA payload.

*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Construct NAT-T rfc3947 vendor ID payload.

*Dec 27 10:59:36:781 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Construct NAT-T draft3 vendor ID payload.

*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Construct NAT-T draft2 vendor ID payload.

*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Construct NAT-T draft1 vendor ID payload.

*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Construct XAUTH draft6 vendor ID payload.

*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Sending packet to 2.2.2.1 remote port 500, local port 500.

*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

I-Cookie: d5f7180aa563cf61

R-Cookie: 0000000000000000

next payload: SA

version: ISAKMP Version 1.0
exchange mode: Main
flags:
message ID: 0
length: 176
*Dec 27 10:59:36:782 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Sending an IPv4 packet.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received packet from 2.2.2.1 source port 500 destination port 500.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

I-Cookie: d5f7180aa563cf61
R-Cookie: 535bbbeaca951ab0
next payload: SA
version: ISAKMP Version 1.0
exchange mode: Main
flags:
message ID: 0
length: 116
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Security Association Payload.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Vendor ID Payload.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Vendor ID Payload.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process SA payload.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

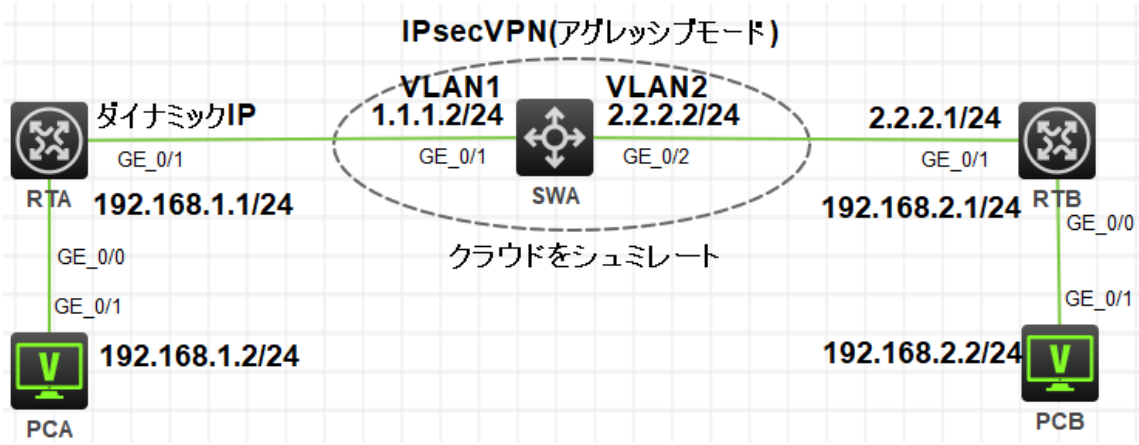
Check ISAKMP transform 1.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Encryption algorithm is 3DES-CBC.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  HASH algorithm is HMAC-MD5.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  DH group is 1.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Authentication method is Pre-shared key.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Lifetime type is 1.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Life duration is 86400.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Attributes is acceptable.
*Dec 27 10:59:36:783 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process vendor ID payload.
*Dec 27 10:59:36:788 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct KE payload.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NONCE payload.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-D payload.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Construct DPD vendor ID payload.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Sending packet to 2.2.2.1 remote port 500, local port 500.
*Dec 27 10:59:36:789 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

I-Cookie: d5f7180aa563cf61
R-Cookie: 535bbbeaca951ab0
next payload: KE
version: ISAKMP Version 1.0
exchange mode: Main
flags:
message ID: 0
length: 208

タスク2：IPsec+IKEアグレッシブモードを設定します

このラボタスクでは、IKEネゴシエーションを介してRTAとRTBの間にIPsecトンネルを確立する方法と、フェーズ1でアグレッシブモードを使用するようにIKEを構成する方法を示します。



手順1：IPアドレスを設定する

表3-3にようにIPアドレスを割り当てます。PCAのデフォルトゲートウェイとしてRTA、そしてPCBのデフォルトゲートウェイをRTBと設定します。

表3-3 IPアドレス割り当て

装置	インターフェイス	IPアドレス	ゲートウェイ

RTA	G0/0	192.168.1.1/24	-
	G0/1	ダイナミックにIPアドレスを取得	-
RTB	G0/0	192.168.2.1/24	-
	G0/1	2.2.2.1/24	-
SWA	VLAN 1	1.1.1.2/24	
	VLAN 2	2.2.2.2/24	
PCA		192.168.1.2/24	192.168.1.1/24
PCB		192.168.2.2/24	192.168.2.1/24

手順2：全てのIPsecとIKEのコンフィギュレーションをクリアします

[RTA]interface GigabitEthernet 0/1

[RTA-GigabitEthernet0/1]undo ipsec apply policy

[RTA-GigabitEthernet0/1]quit

[RTA]undo ipsec policy policy1

[RTA]undo ipsec transform-set trans1

[RTA]undo ike profile profile1

[RTA]undo ike keychain keychain1

[RTA]undo ike proposal 1

[RTA]undo acl advanced 3000

RTBのIPsecとIKE設定のクリアに必要なコマンドはRTA同様。

[RTB]interface GigabitEthernet 0/1

[RTB-GigabitEthernet0/1]undo ipsec apply policy

[RTB-GigabitEthernet0/1]quit

[RTB]undo ipsec policy policy1

[RTB]undo ipsec transform-set trans1

[RTB]undo ike profile profile1

[RTB]undo ike keychain keychain1

[RTB]undo ike proposal 1

[RTB]undo acl advanced 3000

手順3：公共のネットワーク接続を設定します

[SWA]dhcp enable

[SWA]dhcp server ip-pool 1

[SWA-dhcp-pool-1]network 1.1.1.0 mask 255.255.255.0

[SWA-dhcp-pool-1]gateway-list 1.1.1.2
[SWA-dhcp-pool-1]quit

[RTA]undo ospf 1
Undo OSPF process? [Y/N]:y
[RTA]undo ip route-static 192.168.2.0 255.255.255.0
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ip address dhcp-alloc
[RTA-GigabitEthernet0/1]quit

RTAのルーティング情報を表示します。この結果はRTAがIPアドレスとデフォルトルートを取得していることを表しています。

[RTA]display ip routing-table
Destinations : 17 Routes : 17

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
0.0.0.0/0	Static	70	0	1.1.1.2	GE0/1
0.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.0/24	Direct	0	0	1.1.1.1	GE0/1
1.1.1.0/32	Direct	0	0	1.1.1.1	GE0/1
1.1.1.1/32	Direct	0	0	127.0.0.1	InLoop0
1.1.1.255/32	Direct	0	0	1.1.1.1	GE0/1
127.0.0.0/8	Direct	0	0	127.0.0.1	InLoop0
127.0.0.0/32	Direct	0	0	127.0.0.1	InLoop0
127.0.0.1/32	Direct	0	0	127.0.0.1	InLoop0
127.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.0/24	Direct	0	0	192.168.1.1	GE0/0
192.168.1.0/32	Direct	0	0	192.168.1.1	GE0/0
192.168.1.1/32	Direct	0	0	127.0.0.1	InLoop0
192.168.1.255/32	Direct	0	0	192.168.1.1	GE0/0
224.0.0.0/4	Direct	0	0	0.0.0.0	NULL0
224.0.0.0/24	Direct	0	0	0.0.0.0	NULL0
255.255.255.255/32	Direct	0	0	127.0.0.1	InLoop0

PCAからPCBへpingします。PCAが何もプライベートネットワークへのルートを持っていないため、PCBへのpingはできません。

<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
手順4：IKE Proposalを設定します
[RTA]ike proposal 1
[RTA-ike-proposal-1]authentication-method pre-share
[RTA-ike-proposal-1]authentication-algorithm md5
[RTA-ike-proposal-1]encryption-algorithm 3des-cbc
[RTA-ike-proposal-1]quit

[RTB]ike proposal 1
[RTB-ike-proposal-1]authentication-method pre-share
[RTB-ike-proposal-1]authentication-algorithm md5
[RTB-ike-proposal-1]encryption-algorithm 3des-cbc
[RTB-ike-proposal-1]quit
手順5：IKE identifyを設定します
[RTA]ike identity fqdn rta
[RTB]ike identity fqdn rtb
手順6：IKE keychainを設定します
[RTA]ike keychain keychain1
[RTA-ike-keychain-keychain1]pre-shared-key address 2.2.2.1 255.255.255.0 key sim
ple h3c
[RTA-ike-keychain-keychain1]quit

[RTB]ike keychain keychain1
[RTB-ike-keychain-keychain1]pre-shared-key hostname rta key simple h3c
[RTB-ike-keychain-keychain1]quit
手順7：IKE Profileを設定します
[RTA]ike profile profile1
[RTA-ike-profile-profile1]exchange-mode aggressive
[RTA-ike-profile-profile1]match remote identity fqdn rtb
[RTA-ike-profile-profile1]keychain keychain1
[RTA-ike-profile-profile1]proposal 1

[RTA-ike-profile-profile1]quit

[RTB]ike profile profile1
[RTB-ike-profile-profile1]exchange-mode aggressive
[RTB-ike-profile-profile1]match remote identity fqdn rta
[RTB-ike-profile-profile1]keychain keychain1
[RTB-ike-profile-profile1]proposal 1
[RTB-ike-profile-profile1]quit
手順8：ACLを設定します
[RTA]acl advanced 3000
[RTA-acl-ipv4-adv-3000]rule 0 permit ip source 192.168.1.0 0.0.0.255 destination
192.168.2.0 0.0.0.255
[RTA-acl-ipv4-adv-3000]quit

[RTB]acl advanced 3000
[RTB-acl-ipv4-adv-3000]rule 0 permit ip source 192.168.2.0 0.0.0.255 destination
192.168.1.0 0.0.0.255
[RTB-acl-ipv4-adv-3000]quit

手順9：IPsec Proposalを設定します
[RTA]ipsec transform-set trans1
[RTA-ipsec-transform-set-trans1]esp authentication-algorithm sha1
[RTA-ipsec-transform-set-trans1]esp encryption-algorithm aes-cbc-128
[RTA-ipsec-transform-set-trans1]quit

[RTB]ipsec transform-set trans1
[RTB-ipsec-transform-set-trans1]esp authentication-algorithm sha1
[RTB-ipsec-transform-set-trans1]esp encryption-algorithm aes-cbc-128
[RTB-ipsec-transform-set-trans1]quit
手順10：IPsec Policyを設定して適用します
両方のルーターでIPsec Policyを設定し、それを隣接する装置に接続されているインタフェースへ適用します。
[RTA]ipsec policy policy1 1 isakmp
[RTA-ipsec-policy-isakmp-policy1-1]remote-address 2.2.2.1
[RTA-ipsec-policy-isakmp-policy1-1]security acl 3000

[RTA-ipsec-policy-isakmp-policy1-1]transform-set trans1
[RTA-ipsec-policy-isakmp-policy1-1]ike-profile profile1
[RTA-ipsec-policy-isakmp-policy1-1]quit
[RTA]interface GigabitEthernet 0/1
[RTA-GigabitEthernet0/1]ipsec apply policy policy1
[RTA-GigabitEthernet0/1]quit

応答者としてのRTBは、対抗側のIPアドレスを取得できないため、テンプレートとして構成する必要があります。
[RTB]ipsec policy-template template1 1
[RTB-ipsec-policy-template-template1-1]security acl 3000
[RTB-ipsec-policy-template-template1-1]transform-set trans1
[RTB-ipsec-policy-template-template1-1]ike-profile profile1
[RTB-ipsec-policy-template-template1-1]quit
[RTB]ipsec policy policy1 1 isakmp template template1
[RTB]interface GigabitEthernet 0/1
[RTB-GigabitEthernet0/1]ipsec apply policy policy1
[RTB-GigabitEthernet0/1]quit
手順11：設定を確認します
RTAとRTBでdisplayコマンドを使い設定情報を表示します。
<RTA>display ike proposal
  Priority Authentication Authentication Encryption   Diffie-Hellman Duration
                      method   algorithm   algorithm   group   (seconds)
----
  1   PRE-SHARED-KEY   MD5   3DES-CBC   Group 1
86400
  default PRE-SHARED-KEY   SHA1   DES-CBC   Group 1
86400

<RTA>display ipsec transform-set
IPsec transform set: trans1
   State: complete
   Encapsulation mode: tunnel
   ESN: Disabled
   PFS:
   Transform: ESP

```
  ESP protocol:
    Integrity: SHA1
    Encryption: AES-CBC-128

<RTA>display ipsec policy
-----------------------------------------
IPsec Policy: policy1
Interface: GigabitEthernet0/1
-----------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: ISAKMP
  ----------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow: 3000
  Selector mode: standard
  Local address:
  Remote address: 2.2.2.1
  Transform set:    trans1
  IKE profile: profile1
  IKEv2 profile:
  SA duration(time based): 3600 seconds
  SA duration(traffic based): 1843200 kilobytes
  SA idle time:

[RTB]display ike proposal
  Priority Authentication Authentication Encryption    Diffie-Hellman Duration
                     method           algorithm       algorithm           group          (seconds)
-------------------------------------------------------------------------------
  1              PRE-SHARED-KEY        MD5             3DES-CBC       Group 1
86400
  default    PRE-SHARED-KEY        SHA1            DES-CBC        Group 1
86400

[RTB]display ipsec policy-template
```

```
-------------------------------------------
IPsec Policy Template: template1
-------------------------------------------

  ----------------------------
  Sequence number: 1
  ----------------------------
  Traffic Flow Confidentiality: Disabled
  Security data flow : 3000
  Selector mode: standard
  Local address:
  IKE profile: profile1
  IKEv2 profile:
  Remote address:
  Transform set: trans1
  IPsec SA local duration(time based):
  IPsec SA local duration(traffic based):
  SA idle time:

[RTB]display ipsec policy
-------------------------------------------
IPsec Policy: policy1
Interface: GigabitEthernet0/1
-------------------------------------------

  ----------------------------
  Sequence number: 1
  Mode: Template
  ----------------------------
  Policy template name: template1
```

手順12:トンネルが確立されていて稼働しているかを確認します

PCAからPCBにpingして両方のPC間の接続性を確認します。

```
<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
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=2.000 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
出力は、最初のICMPエコー要求がタイムアウトになり、他のすべての要求はタイムアウトしなかったことを示しています。 最初のリクエストがタイムアウトする前にIPsec SAsが利用できなかったためです。 最初の要求は破棄され、後続のすべての要求はIPsecトンネルを介して宛先に配信されました。

RTAとRTBのIPsecとIKE情報を表示します。
<RTA>display ike sa
Connection-ID Remote Flag DOI
---
2 2.2.2.1 RD IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

<RTA>display ike sa verbose

Connection ID: 2
Outside VPN:
Inside VPN:
Profile: profile1
Transmitting entity: Initiator

Local IP: 1.1.1.1
Local ID type: FQDN
Local ID: rta

Remote IP: 2.2.2.1
Remote ID type: FQDN
Remote ID: rtb

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: MD5
Encryption-algorithm: 3DES-CBC

Life duration(sec): 86400
Remaining key duration(sec): 86080
Exchange-mode: Aggressive
Diffie-Hellman group: Group 1
NAT traversal: Not detected
Extend authentication: Disabled
Assigned IP address:

この出力結果はIKEがアグレッシブモードでの認証をしたことを表しています。

```
<RTA>display ipsec sa
-------------------------------
Interface: GigabitEthernet0/1
-------------------------------

  -----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: ISAKMP
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1428
    Tunnel:
        local  address: 1.1.1.1
        remote address: 2.2.2.1
    Flow:
        sour addr: 192.168.1.0/255.255.255.0  port: 0  protocol: ip
        dest addr: 192.168.2.0/255.255.255.0  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 3943816766 (0xeb11de3e)
      Connection ID: 12884901888
      Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
```

SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3269
Max received sequence-number: 9
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 2248163441 (0x86004071)
Connection ID: 4294967297
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3269
Max sent sequence-number: 9
UDP encapsulation used for NAT traversal: N
Status: Active

```
<RTB>display ike sa
    Connection-ID     Remote                Flag            DOI
-----------------------------------------------------------------
    2                 1.1.1.1               RD              IPsec
Flags:
RD--READY RL--REPLACED FD-FADING RK-REKEY

<RTB>display ike sa verbose
  ----------------------------------------------
  Connection ID: 2
  Outside VPN:
  Inside VPN:
  Profile: profile1
  Transmitting entity: Responder
  ----------------------------------------------
  Local IP: 2.2.2.1
  Local ID type: FQDN
  Local ID: rtb
```

Remote IP: 1.1.1.1
Remote ID type: FQDN
Remote ID: rta

Authentication-method: PRE-SHARED-KEY
Authentication-algorithm: MD5
Encryption-algorithm: 3DES-CBC

Life duration(sec): 86400
Remaining key duration(sec): 85645
Exchange-mode: Aggressive
Diffie-Hellman group: Group 1
NAT traversal: Not detected

Extend authentication: Disabled
Assigned IP address:

この出力結果はISAKMP SAがアグレッシブモードで認証されたことを表しています。

<RTB>display ipsec sa

```
-------------------------------
Interface: GigabitEthernet0/1
-------------------------------

  -----------------------------
  IPsec policy: policy1
  Sequence number: 1
  Mode: Template
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1428
    Tunnel:
```

local address: 2.2.2.1
remote address: 1.1.1.1
Flow:
sour addr: 192.168.2.0/255.255.255.0 port: 0 protocol: ip
dest addr: 192.168.1.0/255.255.255.0 port: 0 protocol: ip

[Inbound ESP SAs]
SPI: 2248163441 (0x86004071)
Connection ID: 4294967296
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/2792
Max received sequence-number: 9
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 3943816766 (0xeb11de3e)
Connection ID: 4294967297
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/2792
Max sent sequence-number: 9
UDP encapsulation used for NAT traversal: N
Status: Active

手順13：IPsecの操作を監視します

存在する全てのIPsec SAsとISAKMP SAsをクリアします。

<RTA>reset ike sa
<RTA>reset ipsec sa

<RTB>reset ike sa
<RTB>reset ipsec sa

デバッギングを有効にします

<RTA>debugging ike packet
<RTA>debugging ipsec packet

IPsecトンネルを確立するのをトリガーするためにPCAからPCBへpingします。
<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
56 bytes from 192.168.2.2: icmp_seq=1 ttl=253 time=5.000 ms
56 bytes from 192.168.2.2: icmp_seq=2 ttl=253 time=4.000 ms
56 bytes from 192.168.2.2: icmp_seq=3 ttl=253 time=3.000 ms
56 bytes from 192.168.2.2: icmp_seq=4 ttl=253 time=3.000 ms

デバッギング情報確認し、分析します。
<RTA>*Dec 27 17:41:06:235 2021 RTA IPSEC/7/PACKET:
Failed to find SA by SP, SP Index = 0, SP Convert-Seq = 65536.
*Dec 27 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
  Encryption algorithm is 3DES-CBC.
*Dec 27 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
  Hash algorithm is HMAC-MD5.
*Dec 27 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
  DH group 1.
*Dec 27 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
  Authentication method is Pre-shared key.
*Dec 27 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
  Lifetime type is in seconds.
*Dec 27 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
  Life duration is 86400.
*Dec 27 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
Construct transform payload for transform 1.

*Dec 27 17:41:06:235 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Constructed SA payload.
*Dec 27 17:41:06:241 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct KE payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NONCE payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Local ID type: FQDN (2).
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Local ID value: rta.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct ID payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct DPD vendor ID payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-T rfc3947 vendor ID payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-T draft3 vendor ID payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-T draft2 vendor ID payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct NAT-T draft1 vendor ID payload.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Construct XAUTH draft6 vendor ID payload.

*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Sending packet to 2.2.2.1 remote port 500, local port 500.
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

I-Cookie: bcded72f665242bf
R-Cookie: 0000000000000000
next payload: SA
version: ISAKMP Version 1.0
exchange mode: Aggressive
flags:
message ID: 0
length: 328
*Dec 27 17:41:06:242 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Sending an IPv4 packet.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received packet from 2.2.2.1 source port 500 destination port 500.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

I-Cookie: bcded72f665242bf
R-Cookie: f74c3eafc3262c64
next payload: SA
version: ISAKMP Version 1.0
exchange mode: Aggressive
flags:
message ID: 0
length: 328
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Security Association Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Received ISAKMP Key Exchange Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Nonce Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Identification Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Vendor ID Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Vendor ID Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Vendor ID Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP NAT-D Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP NAT-D Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Received ISAKMP Hash Payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process NONCE payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process KE payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process ID payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Peer ID type: FQDN (2).
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Peer ID value: FQDN rtb.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process SA payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Check ISAKMP transform 1.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Encryption algorithm is 3DES-CBC.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  HASH algorithm is HMAC-MD5.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  DH group is 1.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Authentication method is Pre-shared key.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Lifetime type is 1.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
  Life duration is 86400.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Attributes is acceptable.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500
Process vendor ID payload.
*Dec 27 17:41:06:251 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Received 2 NAT-D payload.
*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
Verify HASH payload.
*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
HASH:
 df75edf4 8f4bc628 a283abd1 b255633c
*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
Construct NAT-D payload.
*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
HASH:
 6a243a4a 79b85851 5372998f fdbfa6a1
*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
Construct authentication by pre-shared-key.
*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
Construct INITIAL-CONTACT payload.
*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
Encrypt the packet.
*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500
Sending packet to 2.2.2.1 remote port 500, local port 500.
*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst =
2.2.2.1/500

  I-Cookie: bcded72f665242bf
  R-Cookie: f74c3eafc3262c64
  next payload: NAT-D
  version: ISAKMP Version 1.0
  exchange mode: Aggressive
  flags: ENCRYPT

message ID: 0

length: 116

*Dec 27 17:41:06:256 2021 RTA IKE/7/PACKET: vrf = 0, src = 1.1.1.1, dst = 2.2.2.1/500

Lab23 IRFの設定

実習内容と目標

このラボでは以下のことを学びます：

- IRF の基本的なコンフィギュレーションを習得します。
- IRF での障害の状況と復旧の状況を習得します。
- IRF のケーブル全てに障害が発生した場合の IP アドレスの重複を防ぐための MAD 機能を習得します。

ネットワーク図

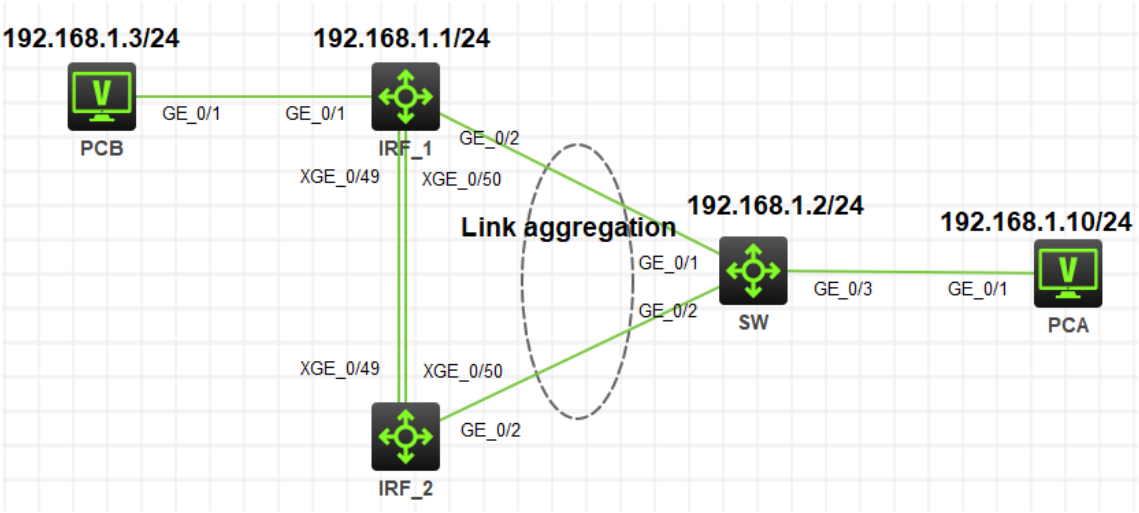


図 1.1 実習ネットワーク

上の図は、テストトポロジを示しています。2つのS5820V2（IRF_1とIRF_2）、1つのS5820V2（SW）、および2つのPC（PCA、PCB）です。

IRF_1とIRF_2でIRFの設定を行います。IRFとSWの間はlink aggregationを設定し経路の冗長化を実現しています。

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
S5820V2	**Version7.1**	**3**	スイッチ
PC	**Windows 7**	**2**	ホスト

ネットワークケーブルの接続	-	4	ストレートケーブル
IRFポートをつなぐファイバーケーブル	-	2	-

実習手順

タスク1：基本的なIRFの設定をする

このテストでは、2台のスイッチ（IRF_1とIRF_2）にIRFの設定を行います。

手順1：テスト構成

以下の表1-1はテストで使われる装置のインターフェース、IPアドレスを示しています。

表1-1 IPアドレス割り当てスキーマ

装置	インターフェース	IPアドレス	補足
IRF_1	G1/0/1		-
	G1/0/2	Link aggregationを設定	-
	XGE1/0/49	IRFを設定	
	XGE1/0/50		
IRF_2	G2/0/2	Link aggregationを設定	-
	XGE2/0/49	IRFを設定	-
	XGE2/0/50		-
SW	G0/1	VLAN 1 192.168.1.2/24	Link aggregationを設定
	G0/2		
	G0/3		
PCA		192.168.1.10/24	-
PCB		192.168.1.3/24	-

手順2：IRF_1の設定を行います。

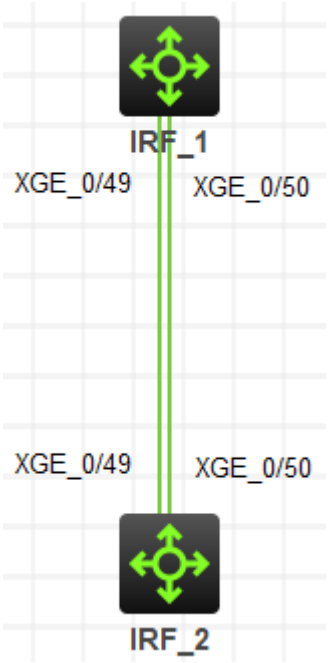


図 1.2 実習ネットワーク

共通の設定
<H3C>sys
System View: return to User View with Ctrl+Z.
[IRF]sysname IRF
[IRF]irf auto-update enable
IRFポートをshutdownして、STPをdisableにします。
[IRF]interface Ten-GigabitEthernet 1/0/49
[IRF-Ten-GigabitEthernet1/0/49]shutdown
[IRF-Ten-GigabitEthernet1/0/49]undo stp enable
[IRF-Ten-GigabitEthernet1/0/49]quit
[IRF]interface Ten-GigabitEthernet 1/0/50
[IRF-Ten-GigabitEthernet1/0/50]shutdown
[IRF-Ten-GigabitEthernet1/0/50]undo stp enable
[IRF-Ten-GigabitEthernet1/0/50]quit
IRFの論理スロット/論理ポート1/1を作成し、ポートTen-GibabitEternet1/0/49とTen-GibabitEternet1/0/50をIRF論理スロット/論理ポート1/1に追加します。
[IRF]irf-port 1/1
[IRF-irf-port1/1]port group interface Ten-GigabitEthernet 1/0/49
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.

Execute the "irf-port-configuration active" command to activate the IRF ports.
[IRF-irf-port1/1]port group interface Ten-GigabitEthernet 1/0/50
[IRF-irf-port1/1]quit
IRF_1をプライマリデバイスとして選択されるように、IRF_1のIRFプライオリティを32にします。
[IRF]irf member 1 priority 32
IRFに設定したポートをenableにします（IRF_2との結線はまだ行いません）
[IRF]interface Ten-GigabitEthernet 1/0/49
[IRF-Ten-GigabitEthernet1/0/49]undo shutdown
[IRF-Ten-GigabitEthernet1/0/49]quit
[IRF]interface Ten-GigabitEthernet 1/0/50
[IRF-Ten-GigabitEthernet1/0/50]undo shutdown
[IRF-Ten-GigabitEthernet1/0/50]quit
[IRF]irf-port-configuration active
[IRF]save force
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
IRFの設定を確認します。
IRFのプライオリティが32であることが確認できます。
[IRF]display irf

MemberID	Role	Priority	CPU-Mac	Description
*+1	Master	32	8459-1858-0104	----------

* indicates the device is the master.
+ indicates the device through which the user logs in.

The bridge MAC of the IRF is: 8459-1858-0100
Auto upgrade : yes
Mac persistent : 6 min
Domain ID : 11
IRFに使われるポートとしてTen-GigabitEthernet1/0/49とTen-GigabitEthernet1/0/50が設定されていることが確認できます。
[IRF]display irf link
Member 1

IRF Port	Interface	Status
1	Ten-GigabitEthernet1/0/49	DOWN
	Ten-GigabitEthernet1/0/50	DOWN

2 disable --

手順3：SW(IRF_2)のスロット番号を2に設定します。

#論理スロット番号を2にします

<H3C>sys

System View: return to User View with Ctrl+Z.

[H3C]sysname IRF

[IRF]irf domain 11

[IRF]irf member 1 renumber 2

Renumbering the member ID may result in configuration change or loss.

Continue?[Y/N]:y

[IRF]save force

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

[IRF]quit

<IRF>reboot

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

This command will reboot the device. Continue? [Y/N]:y

Now rebooting, please wait...

%Nov 23 17:23:49:144 2021 IRF_2 DEV/5/SYSTEM_REBOOT: System is rebooting now.

Cryptographic Algorithms Known-Answer Tests are running ...

CPU 0 of slot 2 in chassis :

Starting Known-Answer tests in the user space.

Cryptographic Algorithms Known-Answer Tests passed.

Line con1 is available.

スロット番号が2に変更されたことを確認します。

Press ENTER to get started.

<IRF>display irf

MemberID Role Priority CPU-Mac Description

***+2 Master 1 8459-2a32-0204 ----------**

* indicates the device is the master.

\+ indicates the device through which the user logs in.

The bridge MAC of the IRF is: 8459-2a32-0200

Auto upgrade : yes

Mac persistent : 6 min
Domain ID : 11

手順4：IRF_2の設定を行います。

共通の設定
[IRF]irf auto-update enable
IRFポートをshutdownして、STPをdisableにします。
[IRF]interface Ten-GigabitEthernet 2/0/49
[IRF-Ten-GigabitEthernet2/0/49]shutdown
[IRF-Ten-GigabitEthernet2/0/49]undo stp enable
[IRF-Ten-GigabitEthernet2/0/49]quit
[IRF]interface Ten-GigabitEthernet 2/0/50
[IRF-Ten-GigabitEthernet2/0/50]shutdown
[IRF-Ten-GigabitEthernet2/0/50]undo stp enable
[IRF-Ten-GigabitEthernet2/0/50]quit
IRFの論理スロット/論理ポート2/2を作成し、ポートTen-GibabitEternet2/0/49とTen-GibabitEternet2/0/50をIRF論理スロット/論理ポート2/2に追加します。
[IRF]irf-port 2/2
[IRF-irf-port2/2]port group interface Ten-GigabitEthernet 2/0/49
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[IRF-irf-port2/2]port group interface Ten-GigabitEthernet 2/0/50
[IRF-irf-port2/2]quit
IRF_2をプライマリデバイスとして選択されるように、IRF_2のIRFプライオリティを1(デフォルト)にします。
[IRF]irf member 2 priority 1
IRFポートをenableにします。
[IRF]interface Ten-GigabitEthernet 2/0/49
[IRF-Ten-GigabitEthernet2/0/49]undo shutdown
[IRF-Ten-GigabitEthernet2/0/49]quit
[IRF]interface Ten-GigabitEthernet 2/0/50
[IRF-Ten-GigabitEthernet2/0/50]undo shutdown
[IRF-Ten-GigabitEthernet2/0/50]quit
[IRF]irf-port-configuration active
[IRF]save force
Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

IRFの設定を確認します。

IRFのプライオリティが1であることが確認できます。

[IRF_2]display irf

MemberID	Role	Priority	CPU-Mac	Description
*+2	Master	1	8459-2a32-0204	----------

* indicates the device is the master.

+ indicates the device through which the user logs in.

The bridge MAC of the IRF is: 8459-2a32-0200

Auto upgrade : yes

Mac persistent : 6 min

Domain ID : 11

IRFに使われるポートとしてTen-GigabitEthernet2/0/49とTen-GigabitEthernet2/0/50が設定されていることが確認できます。

[IRF_2]display irf link

Member 2

IRF Port	Interface	Status
1	disable	--
2	Ten-GigabitEthernet2/0/49	DOWN
	Ten-GigabitEthernet2/0/50	DOWN

手順5：IRF SW間をケーブルで接続しIRFを確立する

注意：HCLではケーブルをつないだだけではIRFの確立が始まりません。一旦IRF_2のスイッチをstopさせ、再度startさせます。ついでIRF_1のスイッチをstopさせ、再度startさせると以下のようなメッセージが表示され、落ち着くとIRFが確立されています。

[IRF]%Nov 23 12:40:28:215 2021 IRF STM/6/STM_LINK_UP: IRF port 2 came up.

%Nov 23 12:40:28:215 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet2/0/49 changed to up.

%Nov 23 12:40:28:216 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet2/0/49 changed to up.

%Nov 23 12:40:28:536 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet2/0/50 changed to up.

%Nov 23 12:40:28:537 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet2/0/50 changed to up.

%Nov 23 12:40:50:018 2021 IRF DEV/2/BOARD_STATE_FAULT: Board state changed to Fault on slot 1, type is unknown.
%Nov 23 12:40:50:610 2021 IRF HA/5/HA_BATCHBACKUP_STARTED: Batch backup of standby board in slot 1 started.
%Nov 23 12:40:51:476 2021 IRF DEV/5/BOARD_STATE_NORMAL: Board state changed to Normal on slot 1, type is H3C S5820V2-54Q.
%Nov 23 12:40:52:273 2021 IRF IFNET/3/IF_WARN: -Slot=1; The jumboframe of the aggregate interface Bridge-Aggregation1 is not supported on the member port GigabitEthernet1/0/1
%Nov 23 12:40:55:431 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/1 changed to up.
%Nov 23 12:40:55:436 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet1/0/49 changed to up.
%Nov 23 12:40:55:442 2021 IRF LAGG/6/LAGG_ACTIVE: Member port GE1/0/1 of aggregation group BAGG1 changed to the active state.
%Nov 23 12:40:55:443 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet1/0/49 changed to up.
%Nov 23 12:40:55:443 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet1/0/50 changed to up.
%Nov 23 12:40:55:448 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet1/0/50 changed to up.
%Nov 23 12:40:55:448 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/2 changed to up.
%Nov 23 12:40:55:449 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/2 changed to up.
%Nov 23 12:40:55:462 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface Bridge-Aggregation1 changed to up.
%Nov 23 12:40:55:462 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/1 changed to up.
%Nov 23 12:40:55:462 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface Bridge-Aggregation1 changed to up.
%Nov 23 12:40:55:490 2021 IRF LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent neighbor created on port Ten-GigabitEthernet2/0/49 (IfIndex 178), neighbor's chassis ID is 4cf2-7c42-0200, port ID is Ten-GigabitEthernet1/0/49.
%Nov 23 12:40:55:246 2021 IRF LLDP/6/LLDP_CREATE_NEIGHBOR: -Slot=1; Nearest bridge agent neighbor created on port Ten-GigabitEthernet1/0/49 (IfIndex

50), neighbor's chassis ID is 4cf2-7c42-0200, port ID is Ten-GigabitEthernet2/0/49.
%Nov 23 12:40:55:495 2021 IRF LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent neighbor created on port Ten-GigabitEthernet2/0/50 (IfIndex 179), neighbor's chassis ID is 4cf2-7c42-0200, port ID is Ten-GigabitEthernet1/0/50.
%Nov 23 12:40:55:297 2021 IRF LLDP/6/LLDP_CREATE_NEIGHBOR: -Slot=1; Nearest bridge agent neighbor created on port Ten-GigabitEthernet1/0/50 (IfIndex 51), neighbor's chassis ID is 4cf2-7c42-0200, port ID is Ten-GigabitEthernet2/0/50.
%Nov 23 12:40:56:654 2021 IRF LLDP/6/LLDP_CREATE_NEIGHBOR: -Slot=1; Nearest bridge agent neighbor created on port GigabitEthernet1/0/2 (IfIndex 3), neighbor's chassis ID is 4cf2-8d1a-0300, port ID is GigabitEthernet1/0/1.
%Nov 23 12:40:56:912 2021 IRF HA/5/HA_BATCHBACKUP_FINISHED: Batch backup of standby board in slot 1 has finished.
%Nov 23 12:41:25:784 2021 IRF STP/6/STP_DETECTED_TC: Instance 0's port Bridge-Aggregation1 detected a topology change.
%Nov 23 12:41:25:736 2021 IRF STP/6/STP_DETECTED_TC: -Slot=1; Instance 0's port GigabitEthernet1/0/2 detected a topology change.

手順6：IRFの状態確認

```
[IRF]dis irf link
Member 1
 IRF Port   Interface                          Status
 1          Ten-GigabitEthernet1/0/49          UP
            Ten-GigabitEthernet1/0/50          UP
 2          disable                             --
Member 2
 IRF Port   Interface                          Status
 1          disable                             --
 2          Ten-GigabitEthernet2/0/49          UP
            Ten-GigabitEthernet2/0/50          UP

[IRF]display irf
MemberID      Role      Priority   CPU-Mac            Description
 *+1          Master    32         82ed-032d-0604     ---
   2          Standby   1          4cf2-7c42-0204     ---
-------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.
```

```
The bridge MAC of the IRF is: 4cf2-7c42-0200
Auto upgrade                : yes
Mac persistent              : 6 min
Domain ID                   : 0

[IRF]display irf topology
                                Topology Info
--------------------------------------------------------------------------
                IRF-Port1                IRF-Port2
MemberID    Link        neighbor    Link        neighbor    Belong To
2           DIS         ---         UP          1           82ed-032d-
0604
1           UP          2           DIS         ---         82ed-032d-
0604
```

手順7：IRFに管理用のIPアドレスをアサインします

```
[IRF]interface Vlan-interface 1
[IRF-Vlan-interface1]ip address 192.168.1.1 24
[IRF-Vlan-interface1]quit
[IRF]save f
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
```

タスク2：IRF装置と外部SWをlink aggregationで接続します

このテストでは、IRFのケーブルに障害が発生した時の冗長経路を用意するために外部SWとlink aggregationで接続します。

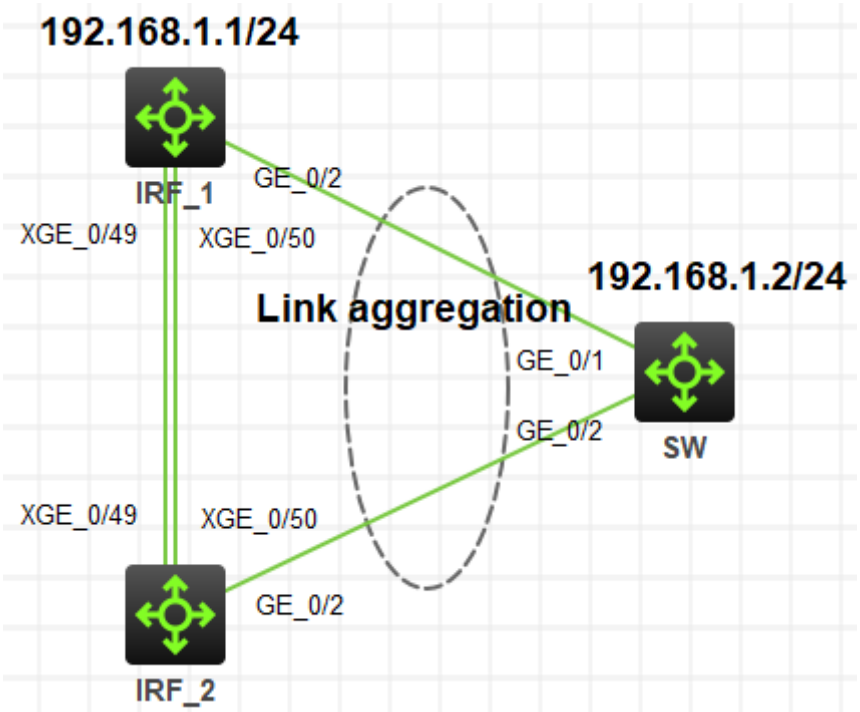


図 1.3 実習ネットワーク

手順1：IRF装置側にlink aggregationの設定をします

```
[IRF]interface Bridge-Aggregation 1
[IRF-Bridge-Aggregation1]quit
[IRF]interface GigabitEthernet 1/0/2
[IRF-GigabitEthernet1/0/2]port link-aggregation group 1
%Nov 23 18:15:23:685 2021 IRF IFNET/3/IF_WARN: -Slot=1; The jumboframe of
the aggregate interface Bridge-Aggregation1 is not supported on the member port
GigabitEthernet1/0/2
[IRF-GigabitEthernet1/0/2]quit
[IRF]interface GigabitEthernet 2/0/2
[IRF-GigabitEthernet2/0/2]port link-aggregation group 1
%Nov 23 18:15:41:339 2021 IRF IFNET/3/IF_WARN: The jumboframe of the
aggregate interface Bridge-Aggregation1 is not supported on the member port
GigabitEthernet2/0/2
[IRF-GigabitEthernet2/0/2]quit
[IRF]save f
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.
```

手順2：link aggregationの設定を確認します

[IRF]dis link-aggregation member-port

Flags: A -- LACP_Activity, B -- LACP_Timeout, C -- Aggregation,

D -- Synchronization, E -- Collecting, F -- Distributing,

G -- Defaulted, H -- Expired

GigabitEthernet1/0/2:

Aggregate Interface: Bridge-Aggregation1

Port Number: 3

Port Priority: 32768

Oper-Key: 1

GigabitEthernet2/0/2:

Aggregate Interface: Bridge-Aggregation1

Port Number: 131

Port Priority: 32768

Oper-Key: 1

手順2：外部SW側にlink aggregationの設定をします

[SW]interface Bridge-Aggregation 1

[SW]interface GigabitEthernet 1/0/1

[SW-GigabitEthernet1/0/1]port link-aggregation group 1

%Nov 23 19:09:48:044 2021 SW IFNET/3/IF_WARN: The jumboframe of the aggregate interface Bridge-Aggregation1 is not supported on the member port GigabitEthernet1/0/1

[SW-GigabitEthernet1/0/1]quit

[SW]interface GigabitEthernet 1/0/2

[SW-GigabitEthernet1/0/2]port link-aggregation group 1

[SW-GigabitEthernet1/0/2]quit

%Nov 23 19:09:55:976 2021 SW IFNET/3/IF_WARN: The jumboframe of the aggregate interface Bridge-Aggregation1 is not supported on the member port GigabitEthernet1/0/2

[SW]save f

Validating file. Please wait...

Saved the current configuration to mainboard device successfully.

手順3：IRF装置とSW間のケーブルを接続して管理用のIPをSWに設定し、IRF装置との接続

をpingで確認します。

注意：HCLではIRFの設定をされたSWが反応しなくなることがあります。その場合は一旦IRF_1またはIRF_2のスイッチをstopさせ、再度startさせます。

[SW]int vlan 1
[SW-Vlan-interface1]ip address 192.168.1.2 24
[SW-Vlan-interface1]quit
[SW]ping 192.168.1.1
Ping 192.168.1.1 (192.168.1.1): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=3.000 ms
56 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.000 ms
56 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.000 ms

手順4：IRF機能確認用のPCを設定

図1.4のようにPCAとPCBの設定をしてからそれぞれのPCからのケーブルを接続します。

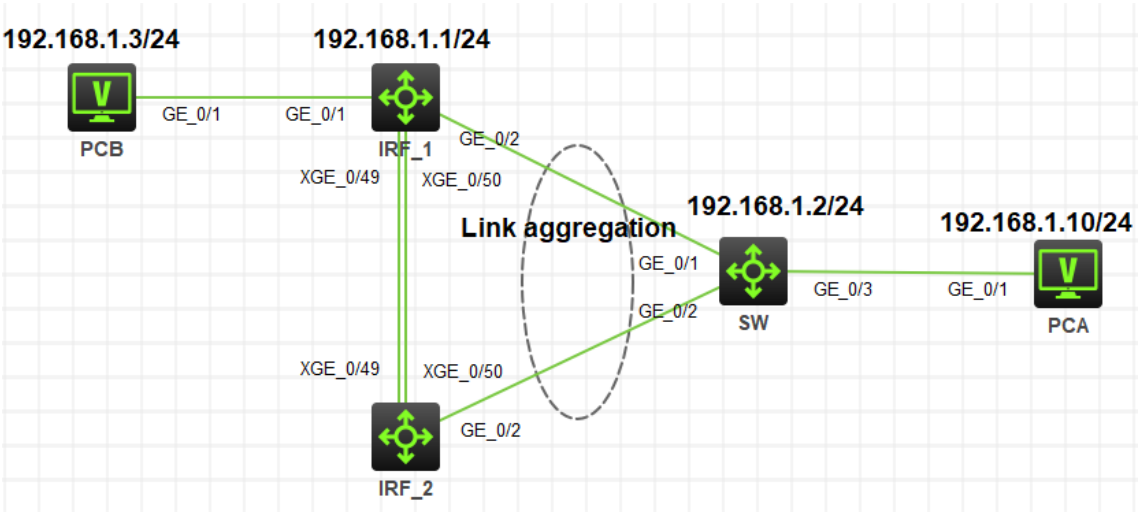


図 1.4 実習ネットワーク

手順5：IRFの障害再現

SWからPCBへ連続してpingを実行。

[SW]ping -c 10000 192.168.1.3
Ping 192.168.1.3 (192.168.1.3): 56 data bytes, press CTRL_C to break
56 bytes from 192.168.1.3: icmp_seq=0 ttl=255 time=3.000 ms
56 bytes from 192.168.1.3: icmp_seq=1 ttl=255 time=1.000 ms

56 bytes from 192.168.1.3: icmp_seq=2 ttl=255 time=1.000 ms
56 bytes from 192.168.1.3: icmp_seq=3 ttl=255 time=1.000 ms
56 bytes from 192.168.1.3: icmp_seq=4 ttl=255 time=1.000 ms
56 bytes from 192.168.1.3: icmp_seq=5 ttl=255 time=1.000 ms
56 bytes from 192.168.1.3: icmp_seq=6 ttl=255 time=1.000 ms
56 bytes from 192.168.1.3: icmp_seq=7 ttl=255 time=1.000 ms
56 bytes from 192.168.1.3: icmp_seq=8 ttl=255 time=1.000 ms
IRFインターフェースTen-GigabitEthernet1/0/49をshutdownする
[IRF]interface Ten-GigabitEthernet 1/0/49
[IRF-Ten-GigabitEthernet1/0/49]shutdown
[IRF-Ten-GigabitEthernet1/0/49]quit
%Nov 23 12:49:11:460 2021 IRF LLDP/6/LLDP_DELETE_NEIGHBOR: Nearest bridge agent neighbor deleted on port Ten-GigabitEthernet2/0/49 (IfIndex 178), neighbor's chassis ID is 4cf2-7c42-0200, port ID is Ten-GigabitEthernet1/0/49.
%Nov 23 12:49:11:464 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet2/0/49 changed to down.
%Nov 23 12:49:11:465 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet2/0/49 changed to down.
%Nov 23 12:49:11:466 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet1/0/49 changed to down.
%Nov 23 12:49:11:466 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet1/0/49 changed to down.
[IRF]display irf link
Member 1

IRF Port	Interface	Status
1	Ten-GigabitEthernet1/0/49	ADM
	Ten-GigabitEthernet1/0/50	UP
2	disable	--

Member 2

IRF Port	Interface	Status
1	disable	--
2	Ten-GigabitEthernet2/0/49	DOWN
	Ten-GigabitEthernet2/0/50	UP

SWからPCBへのpingにはパケットロスが見られなかった
56 bytes from 192.168.1.3: icmp_seq=1 ttl=255 time=1.000 ms
56 bytes from 192.168.1.3: icmp_seq=2 ttl=255 time=1.000 ms

56 bytes from 192.168.1.3: icmp_seq=3 ttl=255 time=1.000 ms

56 bytes from 192.168.1.3: icmp_seq=4 ttl=255 time=1.000 ms

56 bytes from 192.168.1.3: icmp_seq=5 ttl=255 time=1.000 ms

手順6：IRFの障害復旧再現

IRFインターフェースTen-GigabitEthernet1/0/49をundo shutdownする

[IRF]interface Ten-GigabitEthernet 1/0/49

[IRF-Ten-GigabitEthernet1/0/49]undo shutdown

[IRF-Ten-GigabitEthernet1/0/49]quit

%Nov 23 12:51:40:319 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet2/0/49 changed to up.

%Nov 23 12:51:40:319 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet2/0/49 changed to up.

%Nov 23 12:51:40:065 2021 IRF LLDP/6/LLDP_CREATE_NEIGHBOR: -Slot=1; Nearest bridge agent neighbor created on port Ten-GigabitEthernet1/0/49 (IfIndex 50), neighbor's chassis ID is 4cf2-7c42-0200, port ID is Ten-GigabitEthernet2/0/49.

%Nov 23 12:51:40:321 2021 IRF IFNET/3/PHY_UPDOWN: Physical state on the interface Ten-GigabitEthernet1/0/49 changed to up.

%Nov 23 12:51:40:321 2021 IRF IFNET/5/LINK_UPDOWN: Line protocol state on the interface Ten-GigabitEthernet1/0/49 changed to up.

%Nov 23 12:51:40:321 2021 IRF LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent neighbor created on port Ten-GigabitEthernet2/0/49 (IfIndex 178), neighbor's chassis ID is 4cf2-7c42-0200, port ID is Ten-GigabitEthernet1/0/49.

%Nov 23 12:52:04:067 2021 IRF SHELL/5/SHELL_LOGOUT: Console logged out from con1.

[IRF]display irf link

Member 1

IRF Port	Interface	Status
1	Ten-GigabitEthernet1/0/49	UP
	Ten-GigabitEthernet1/0/50	UP
2	disable	--

Member 2

IRF Port	Interface	Status
1	disable	--
2	Ten-GigabitEthernet2/0/49	UP
	Ten-GigabitEthernet2/0/50	UP

SWからPCBへのpingにはパケットロスが見られなかった

56 bytes from 192.168.1.3: icmp_seq=1 ttl=255 time=1.000 ms

56 bytes from 192.168.1.3: icmp_seq=2 ttl=255 time=1.000 ms

56 bytes from 192.168.1.3: icmp_seq=3 ttl=255 time=1.000 ms

56 bytes from 192.168.1.3: icmp_seq=4 ttl=255 time=1.000 ms

56 bytes from 192.168.1.3: icmp_seq=5 ttl=255 time=1.000 ms

タスク3：IRFケーブル全てに障害が発生した場合に備えて

このテストでは、2台のスイッチ（IRF_1とIRF_2）間の2本のIRFケーブルに障害が発生した場合、active/activeとなって、同じIPアドレスを持つ装置になってしまうことを防ぐために用意されているMADという機能を設定します。

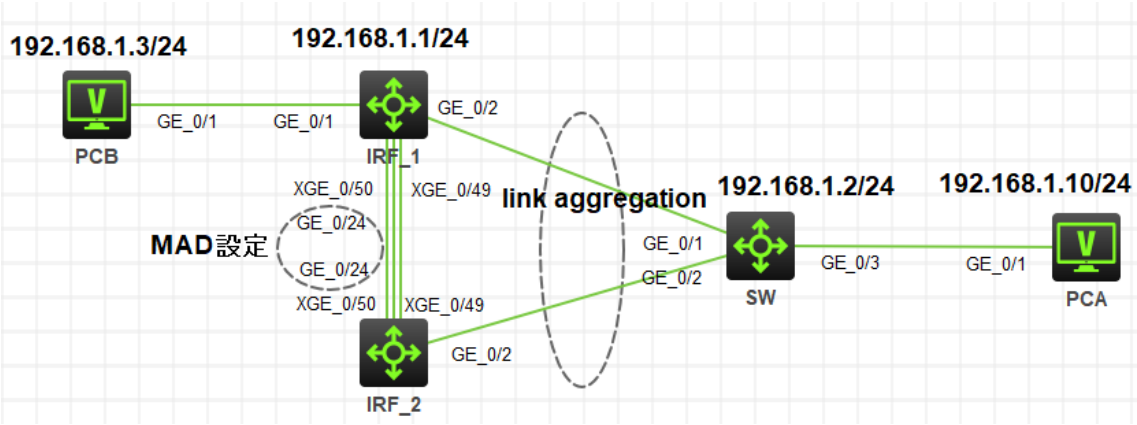


図 1.5 実習ネットワーク

手順1：IRF装置へBFD MADを設定します。

[IRF]vlan 99

[IRF-vlan99]quit

[IRF]interface vlan 99

[IRF-Vlan-interface99]mad bfd enable

[IRF-Vlan-interface99]mad ip address 172.16.0.1 24 member 1

[IRF-Vlan-interface99]mad ip address 172.16.0.2 24 member 2

[IRF-Vlan-interface99]quit

%Nov 23 21:04:48:548 2021 IRF

BFD/4/BFD_MAD_INTERFACE_CHANGE_STATE: BFD MAD function enabled

on Vlan-interface99 changed to the faulty state.

[IRF]interface GigabitEthernet 1/0/24

[IRF-GigabitEthernet1/0/24]port access vlan 99

[IRF-GigabitEthernet1/0/24]undo stp enable

[IRF-GigabitEthernet1/0/24]quit

[IRF]interface GigabitEthernet 2/0/24

[IRF-GigabitEthernet2/0/24]port access vlan 99

[IRF-GigabitEthernet2/0/24]undo stp enable
[IRF-GigabitEthernet2/0/24]quit
[IRF]save f
Validating file. Please wait...
Saved the current configuration to mainboard device successfully.
Slot 1:
Save next configuration file successfully.

手順2：BFD MADに設定したポートにケーブルを接続します。

ケーブル接続が完了したらMADの状態を確認します。

[IRF]display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
Ten-GigabitEthernet1/0/49
Ten-GigabitEthernet1/0/50
Ten-GigabitEthernet2/0/49
Ten-GigabitEthernet2/0/50
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Vlan-interface99
MAD status : Faulty
Member ID MAD IP address Neighbor MAD status
1 172.16.0.1/24 2 Faulty
2 172.16.0.2/24 1 Faulty
[IRF]display bfd session
Total Session Num: 1 Up Session Num: 0 Init Mode: Active

IPv4 session working in control packet mode:

LD/RD SourceAddr DestAddr State Holdtime
Interface
129/0 172.16.0.1 172.16.0.2 Down 0ms
Vlan99

手順3：IRFを構成するケーブルをshutdownしてMADの機能を確認します。

IRF_1のポートの状態はUPなので、こちらは192.168.1.1のアドレスでアクセスできま

す。

[IRF]display ip interface brief

*down: administratively down

(s): spoofing (l): loopback

Interface	Physical	Protocol	IP Address	Description
MGE0/0/0	down	down	--	--
Vlan1	**up**	**up**	**192.168.1.1**	**--**
Vlan99	down	down	172.16.0.1	--

IRF_2のポートの状態はDOWNなので、こちらは192.168.1.1のアドレスでアクセスできません。

[IRF]display ip interface brief

*down: administratively down

(s): spoofing (l): loopback

Interface	Physical	Protocol	IP Address	Description
MGE0/0/0	down	down	--	--
Vlan1	**down**	**down**	**192.168.1.1**	**--**
Vlan99	down	down	172.16.0.2	--

それぞれのコンフィギュレーション

IRFのコンフィギュレーション

```
#
 version 7.1.075, Alpha 7571
#
 sysname IRF
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 32
 irf member 2 priority 1
#
 lldp global enable
#
 system-working-mode standard
 xbar load-single
 password-recovery enable
 lpu-type f-series
```

```
#
vlan 1
#
Vlan 99
#
irf-port 1/1
 port group interface Ten-GigabitEthernet1/0/49
 port group interface Ten-GigabitEthernet1/0/50
#
irf-port 2/2
 port group interface Ten-GigabitEthernet2/0/49
 port group interface Ten-GigabitEthernet2/0/50
#
 stp global enable
#
interface Bridge-Aggregation1
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
#
interface Vlan-interface99
 mad bfd enable
 mad ip address 172.16.0.1 255.255.255.0 member 1
 mad ip address 172.16.0.2 255.255.255.0 member 2
#
…..一部省略
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet1/0/2
 port link-mode bridge
 combo enable fiber
```

```
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
 port link-mode bridge
 combo enable fiber
#
.....一部省略
#
interface GigabitEthernet1/0/24
 port link-mode bridge
 port access vlan 99
 combo enable fiber
 undo stp enable
#
.....一部省略
#
interface GigabitEthernet2/0/1
 port link-mode bridge
 combo enable fiber
#
interface GigabitEthernet2/0/2
 port link-mode bridge
 combo enable fiber
 port link-aggregation group 1
#
interface GigabitEthernet2/0/3
 port link-mode bridge
 combo enable fiber
#
.....一部省略
#
interface GigabitEthernet2/0/24
 port link-mode bridge
 port access vlan 99
 combo enable fiber
 undo stp enable
```

```
#
.....一部省略
#
interface Ten-GigabitEthernet1/0/51
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet1/0/52
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet2/0/51
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet2/0/52
 port link-mode bridge
 combo enable fiber
#
interface Ten-GigabitEthernet1/0/49
 combo enable fiber
#
interface Ten-GigabitEthernet1/0/50
 combo enable fiber
#
interface Ten-GigabitEthernet2/0/49
 combo enable fiber
#
interface Ten-GigabitEthernet2/0/50
 combo enable fiber
#
 scheduler logfile size 16
#
line class aux
 user-role network-operator
#
```

…..一部省略
#
return

SWのコンフィギュレーション
#
 version 7.1.075, Alpha 7571
#
 sysname SW
#
 irf mac-address persistent timer
 irf auto-update enable
 undo irf link-delay
 irf member 1 priority 1
#
 lldp global enable
#
 system-working-mode standard
 xbar load-single
 password-recovery enable
 lpu-type f-series
#
vlan 1
#
 stp global enable
#
interface Bridge-Aggregation1
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.1.2 255.255.255.0
#
...一部省略
#
interface GigabitEthernet1/0/1

port link-mode bridge
combo enable fiber
port link-aggregation group 1
#
interface GigabitEthernet1/0/2
port link-mode bridge
combo enable fiber
port link-aggregation group 1
#
interface GigabitEthernet1/0/3
port link-mode bridge
combo enable fiber
#
...一部省略
#
line class aux
user-role network-operator
#
...一部省略
#
return

質問:

1．IRFを構成するポートはactive/stand-byのようにいずれかのポートは正常の場合はデータが送受信されないでしょうか？

答え:

いいえ。IRFを構成するポートはload-sharingされていてそれぞれのポートがデータの送受信をしております。