17　小規模ネットワークの構築 実習

クラス　SK2A　No.　03　氏名　　文家俊

指示に従い、ルータの設定し、設定の確認を行いなさい。

設定に必要なもの：ルータ、電源ケーブル、クロスオーバーケーブル、コンソールケーブル、USB toシリアル変換ケーブル　まず講師の指示に従い、実習に必要な物品を揃えなさい．

コンソールケーブルとUSB to シリアル変換ケーブルで接続

アイコン が含まれている画像

自動的に生成された説明

各教室のLANコネクタに接続します

(自分自身のLANケーブルを使って接続)

なければ予備のクロスケーブルで接続

クロスケーブルを使って接続

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| デバイス（デバイス名） | インターフェイス(ルータ別) | | | IPアドレス | サブネットマスク | デフォルトゲートウェイ (デフォルトルート) |
| 1921/1941 | 4331 | 800M |
| ルータ(クラス出席番号)LANコネクタ | G0/0 | G0/0/0 | G0/4 | 10.16.10.x(出席番号) | 255.255.255.0 | 10.16.10.254 |
| ルータ(クラス出席番号) PCと接続 | G0/1 | G0/0/1 | G0/5 | 192.168.1.30 | 255.255.255.224 | 設定しない |
| PC | NIC | | | 192.168.1.？ 動的に取得 | 255.255.255.224 （動的に取得） | 192.168.1.30 （動的に取得） |

## ■作成トポロジ：図のように、ルータ（1921/1941/4331/800Mのいずれか）1台、PC1台を配置し、指定されたインターフェイスをケーブルで接続する。

あなたの設定するルータは[**800M**　]

## ■機器の設定（ [ ] 内にコマンドや結果を記入すること）

* PCの設定とLAN接続

PCとルータのPCと接続するインターフェイスを**クロスケーブル**で接続する

ルータ側の接続したインターフェイスは、  
[**800M→GIG 5**　]

PCのIP設定は、DHCPで動的に取得するため、今回は手動で設定しません

* ルータの設定1（ルータでインターフェイスが異なる　ルータは**800M**）
  1. 設定のためグローバルコンフィグモードに移動する。  
     **Would you like to enter the initial configuration dialog? [yes/no]:**と聞かれたら**no**と入力しEnter → **Press RETURN to get started!**と表示されたら再度Enter  
     Router > **en** 特権EXECモードに移動  
     Router# **conf t** グローバルコンフィグモードに移動  
     Router(config)#
  2. ルータのホスト名を**クラス出席番号**（ex. IE2A01,IE2B11,SK1A21,SK2B06,SE2A31）に設定する  
     Router(config)# [　hostname SK2A03　]
  3. 特権パスワードを設定する パスワード・・・**cisco**Router(config)# [　　enable secret cisco　]

1. 設定ファイル全てのパスワードを保護します(パスワードを暗号化する)  
   Router(config)# [　service password-encryption　　]
   1. PCと接続しているインターフェイスにIPアドレス192.168.1.30とサブネットマスク255.255.255.224を設定し、有効化する。  
      設定するインターフェイスは、[**800M→G0/5**]  
      Router(config)# [　int G0/5　]設定するインターフェイスへ  
      Router(config-if)# [　　ip address 192.168.1.30 255.255.255.224　　]  
       IPアドレスとサブネットマスク  
      Router(config-if)#[　　no shutdown　　] インターフェイスの有効化  
      Router(config-if)#[　description　Link to PC　　　　　]**インターフェイスの説明「Link to PC」を記述**  
      Router(config-if)# **exit**
   2. 教室のLANコネクタと接続予定のインターフェイスにIPアドレス10.16.10.ｘ(出席番号)とサブネットマスク255.255.255.0を設定し、有効化する。  
      　設定するインターフェイスは、[ **800M→G0/4**]  
      Router(config)# [　　int G0/4　　] 設定するインターフェイスへ  
      Router(config-if)# [　ip address 10.16.10.3 255.255.255.0　]  
       IPアドレスとサブネットマスク  
      Router(config-if)#[　no shutdown　] インターフェイスの有効化  
      Router(config-if)# [　　description　Link to LAN　] **インターフェイスの説明「Link to LAN」を記述**  
      Router(config-if)# **exit**
   3. デフォルトルートの設定  
      Router(config)# **ip route 0.0.0.0 0.0.0.0 10.16.10.254**
   4. SSHの有効化(①ホスト名は2.で設定しているため、5ステップ)
      1. ドメイン名として **ecccomp.com** を使用します。  
         **Router (config)#** [ 　ip domain-name ecccomp.com　]
      2. **1024**のモジュラスを使用します。  
         **Router (config)#** [ 　crypto key generate rsa general-keys modulus 1024 ]
   5. 暗号化されたパスワードClassを持つユーザCiscoを設定  
      Router (config)# [ 　username *Cisco* secret *Class*  ]
      1. VTY 回線では、ログインを認証するように設定されたユーザ名とパスワードを使用する必要があります。  
         Router (config)# line vty 0 4　　※ルータの場合vty回線は0～4の5回線   
         RTR-A (config-line)# [ 　login local　　 ]
      2. VTY 回線では、着信接続に SSH を使用する必要があります。  
         Router (config-line)# [ 　　transport input ssh ]
   6. DHCPとして機能設定する  
      Router(config)# **ip dhcp pool *クラス出席番号*(ex．Ie2a01)**Router(config-dhcp)# **network 192.168.1.0 255.255.255.224**Router(config-dhcp)# **default-router 192.168.1.30**Router(config-dhcp)# **dns-server 10.201.10.1**Router(config-dhcp)# **exit**

## ■設定の確認と追加設定

* PCのIPアドレスを確認する  
  PCのコマンドプロントから、**ipconfig /all  
  PCに設定されているIPv4アドレス** [　　192.168.1.1　]←この後の設定必要

**PCに設定されているデフォルトゲートウェイ** [　192.168.1.31　]

* ルータの設定2（ルータでインターフェイスが異なる　ルータは、**1921　/　1941　/　4331　/　800M**）

1. NATの設定  
   Router(config)# **ip nat inside source static** **PCのIPv4アドレス 10.16.10.x**（xは出席番号）
2. PCと接続しているインターフェイスにNAT設定を適用する  
   設定するインターフェイスは、[**800M→G0/5**]  
   Router(config)# [　　int G0/5　　]設定するインターフェイスへ  
   Router(config-if)# **ip nat inside**Router(config-if)# **exit**
3. 教室のLANコネクタと接続予定のインターフェイスにNAT設定を適用する  
   設定するインターフェイスは、[**800M→G0/4**]  
   Router(config)# [　int G0/4　　]設定するインターフェイスへ  
   Router(config-if)# **ip nat outside**Router(config-if)# **exit**

## ■接続の確認 **※接続確認をする前に、無線LAN接続を切っておくこと。**

* PC → ルータの接続を確認する  
  PCのコマンドプロントから **ping *ルータのIPアドレス***（192.168.1.30） [　接続できた　]
* PC → JPNICの接続を確認する  
  PCのコマンドプロンプト **ping www.nic.ad.jp**
* グラフィカル ユーザー インターフェイス, テキスト

  自動的に生成された説明SSH接続の確認  
  Teratermでファイル→新しい接続　  
  ホスト：192.168.1.30  
  サービス：SSH  
  を入力・選択しOKを押す  
  続いて表示されるSSH認証画面で  
  ユーザ名：Cisco  
  パスフレーズ：Class  
  でOKを押す  
  ルータに、[　接続できた　・　接続できない　]
* pingを使用したネットワーク遅延のテスト
  1. コマンドプロンプトでダウンロードフォルダをカレントディレクトリとする。（PCのコマンドプロントで、[ **cd %HOMEPATH%\Downloads** ]と入力するか、ダウンロードフォルダのアドレスバーに「cmd」と入力しEnter）プロンプトがC:\Users\ユーザ名\Downloads>になっていればOK  
     接続確認を行う  
     **ping** [**www.lacnic.net**](http://www.lacnic.net)[　接続できた　]  
     **ping** [**www.afrinic.net**](http://www.afrinic.net)[　接続できた. ] **ping** [**www.apnic.net**](http://www.apnic.net)[　接続できた　]
  2. 全てについて確認できたら、リダイレクトを使って結果を出力します  
     **ping -n 25 www.lacnic.net > lacnic.txt  
     ping -n 25 www.afrinic.net > afrinic.txt  
     ping -n 25 www.apnic.net > apnic.txt**(pingの実行結果をリダイレクトしてテキストファイルにいるためただ固まっているようにも見えますが、しばらく見守りましょう)
  3. dir \*nic.txtでリダイレクトがファイルとして保存されていることを確認します  
      [　確認できた　]
  4. moreコマンドでpingの実行結果を確認する  
      [スペース] を押してファイルの残りの部分を表示するか、[q] を押して 終了します。  
     more lacnic.txt [　確認できた ]  
     more afrinic.txt [　確認できた ]  
     more apnic.txt [　確認できた ]
  5. 遅延の結果を比較します。

|  |  |  |  |
| --- | --- | --- | --- |
| 宛先 | 最小値 | 最大値 | 平均値 |
| **lacnic（ブラジル・サンパウロ）** | 275.108 | 277.549 | 275.470 |
| **afrinic（南アフリカ・ヨハネスバーグ）** | 184.176 | 199.965 | 186.240 |
| **apnic（日本国内・大阪と推定）** | 3.725 | 10.883 | 3.725 |

* 1. 遅延の結果を比較して、遅延は地理的な場所によってどのように影響されると推測できますか？

できます

上記の結果を教員に確認してもらうこと。

■提出物  
□全員

提出物：TeraTermのlogファイル（今日の日付でサイズが最大のもの）またはshow runの出力  
ファイル名の最初をクラス番号氏名にしてください。

□最後のチェックまで行かなかった人

このWordファイル(docx)

設定に必要なコマンド（ルータとスイッチ）

1. ﾕｰｻﾞﾓｰﾄﾞから特権モードに　 　　　　 Router>enable (enに省略可)
2. 特権モードからﾕｰｻﾞﾓｰﾄﾞに戻る　 Router#disable
3. 特権モードからグローバル設定モードに　 Router#configure terminal (conf tに省略可)
4. 一つ上のモードに戻る　　　　　　　 Router(config)#exit
5. ホスト名をつける　　　　　　　　　 Router(config)# hostname *ホスト名*
6. 特権モードのパスワードを設定する 　 Router (config)#enable secret *パスワード*
7. コンソールのパスワードの設定 Router(config)#line cons 0

Router(config-line)#password *パスワード*

　　　　　　　　　　　　　　　　　　 Router(config-line)#login

1. VTY(telnet/ssh)のパスワードの設定 Router(config)#line vty 0 4

Router(config-line)#password *パスワード*

　　　　　　　　　　　　　　　　　　 Router(config-line)#login

　　　　　　　　　　SSH接続の有効化 Router(config-line)# transport input ssh

1. 設定画面のタイムアウト時間を設定　 Router(config-line)#exec-timeout*分　秒*
2. 入力中のログ出力を抑制する　　　　 Router(config-line)#logging　synchronous
3. パスワードを暗号化する 　　　　　 　 Router(config)# service password-encryption
4. DNS検索の無効化(入力ミスされたコマンドをドメイン名に解決することを防止) Router(config)# no ip domain-lookup
5. インターフェイスの設定(IPv4)　　　　　 Router(config)#int *インターフェイス名*

Router(config-if)#ip address *IPｱﾄﾞﾚｽ ｻﾌﾞﾈｯﾄﾏｽｸ*※今回のサブネットマスクは255.255.255.0のみ

　　　　　　　　　　　　　　　　　　　　 Router(config-if)#no shutdown(初回のみ実施)

　　　　　　インターフェイスの説明の記述 Router(config-if)#description 説明文

1. デフォルトルートの設定　　　　　　　 Router(config)# ip route 0.0.0.0 0.0.0.0 *IPｱﾄﾞﾚｽ*
2. デフォルトゲートウェイの設定(通常スイッチのみ) Switch(config)# ip default-gateway *IPｱﾄﾞﾚｽ*
3. SSHの設定（6ステップ）
   1. ホスト名を設定 Switch(config)# hostname *ホスト名*
   2. ドメイン名を設定 Switch (config)# ip domain-name *ドメイン名*
   3. 1024のモジュラスを使用（秘密鍵を生成）します。  
       Switch (config)# crypto key generate rsa general-keys modulus 1024
   4. ローカル データベースのユーザ名、暗号化されたパスワードを設定  
       Switch (config)# username *ユーザ名* secret *パスワード*
   5. VTY 回線で、ログイン時をローカル データベースのユーザ名、暗号化されたパスワードで認証するように設定  
       Switch (config) # line vty 0 15　※ルータの場合vty回線は0～4の5回線  
       Switch (config-line)# login local
   6. VTY 回線で、着信接続に SSH のみを限定します  
       Switch (config-line)# transport input ssh
4. 全てのパスワードの文字数の最小値を設定する Router(config )# security passwords min-length 10
5. ブルートフォースのログイン試行回数の制御  
    Router(config )# login block-for *ブロック(待機・ブロック)秒数* attempts *失敗回数* within *制限秒数(〇秒以内)*
6. MOTDバナー(不正アクセスへの警告) Router(config )# banner motd # *メッセージ* #