CiscoITN+2-3ACL実習

クラス　　　No.　　　氏名

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  
　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.x.254  xは出席番号 | 255.255.255.0 | 設定しない |
| PC | NIC | | | 動的に取得  192.168.x.1以降 xは出席番号 | 255.255.255.0 （動的に取得） | 192.168.ｘ.254 （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 **ここでは接続しません、ルータ設定の８の後で設定します**
* 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、**1921　/　1941　/　4331　/　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)#

* 1. 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　]
  2. 特権パスワードを設定する パスワード・・・**cisco**Router(config)# [　enable secret cisco　]
  3. 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**　]
  4. PCと接続しているインターフェイスにIPアドレス192.168.ｘ.254とサブネットマスク255.255.255.0を設定し、有効化する。、xは出席番号  
     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 192.168.3.254 255.255.255.0　]  
       
     Router(config-if)#[　no shutdown　] インターフェイスの有効化  
     Router(config-if)#[　ip nat inside　　]NATの内側として設定  
     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**
  5. 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)# [　ip nat outside　　]NATの外側として設定  
     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**
  6. DHCPでプールから除外するアドレスを設定（192.168.x.251～254を除外）xは出席番号  
     Router(config)# [　**ip dhcp excluded-address 192.168.3.251 192.168.3.254**]192.168.x. 251～254を除外、xは出席番号
  7. DHCPとして機能設定  
     プール名：クラス出席番号 使用ネットワーク：192.168.x.0/24 DG：192.168.x.254 xは出席番号  
     DNSサーバは10.201.10.1、リース時間は90分  
     Router(config)# [　ip dhcp pool sk2a03　　]DHCPプールの設定 プール名はクラス出席番号Router(config-dhcp)# [　network 192.168.3.0 255.255.255.0　]DHCPで使用するネットワークを指定Router(config-dhcp)# [　default-router 192.168.3.254　]DGの設定を指定  
     Router(config-dhcp)# [　dns-server 10.201.10.1　　]割り当てるDNSサーバのアドレスを指定  
     Router(config-dhcp)# [　**lease 0 1 30**　　]リース時間を1時間30分に設定Router(config-dhcp)# **exit**

ここで**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

1. IPv4ダイナミックルーティングの設定(OSPFv2) プロセスIDは１、エリアIDは0  
   Router(config)# [　　router ospf 1　] ospfのプロセスIDは１Router(config-router)#[ 　network 192.168.3.0 0.0.0.255 area 0　　]アドバタイズするネットワークの設定、エリアIDは0  
   Router(config-router)#[ 　 network 10.16.10.0 0.0.0.255 area 0　　] アドバタイズするネットワークの設定、エリアIDは0
2. SSHの設定  
   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)
3. ドメイン名として ecccomp.com を使用します。  
   Router (config)# [ 　ip domain-name ecccomp.com　　]
4. 暗号鍵の設定（1024で設定）  
   Router (config)# [ 　crypto key generate rsa general-keys modulus 1024　　 ]
5. ユーザ名：クラス出席番号(ex. IE2A01) パスワードCl@ssを設定  
   Router (config)# [ 　username *sk2a03* secret *Cl@ss*　 ]
6. VTY 回線では、設定されたユーザ名とパスワードを認証に使用  
   Router (config)# line vty 0 4  
   Router (config-line)# [ 　　login local　　 ]
7. VTY 回線では、リモート接続にSSHのみ使用する  
   Router (config-line)# [ 　transport input ssh ]
8. アクセスリストの設定1 リモート接続のアクセス制限  
   SSH（VTY）回線用に、名前付きの標準ACL(SSH-NAT)」を作成する（NATの設定にも適用）．  
   送信元は192.168.x.0/24のみを許可します(xは出席番号)、  
   作成したリストをVTY回線への接続(入力方向)に適用します  
   **Router (config)#** [ 　ip access-list standard SSH-NAT　] 標準アクセスリスト「SSH-NAT」を作成  
   **Router (config-std-nacl)#** [ permit 192.168.3.0 0.0.0.255　] 送信元は192.168.x.0/24のみを許可  
   **Router (config-std-nacl)#exit  
   Router (config)# line vty 0 4**  
   **Router (config-line)#** [ access-class SSH-NAT in　] アクセスリスト「SSH-NAT」を入力方向へ適用

NAPTの設定  
標準アクセスリスト「SSH-NAT」に一致するトラフィックをルータの外部側インターフェイスでNAT変換（複数の内部アドレスを単一の外部アドレスにマッピングすること）  
外部インターフェイスは、[ **800M→G0/4**]

**Router(config)# ip nat inside source list SSH-NAT int G0/4 overload**

※例は800Mの場合  
※内部インターフェイスの指定、外部インターフェイスの指定は5，6.で設定済み

1. アクセスリストの設定2  
   名前付きACL名前：STOP-PING-WEBを作成、適切なインターフェイスの適切な方向へ適用してください。  
   ACLの内容  
   ・PC(送信元：192.168.x.0/24)からルータ(宛先：192.168.ｘ.254/32)へのpingを拒否  
   ・PC(送信元：192.168.x.0/24)からＷｅｂサーバ(宛先：10.201.10.0/24)へのWeb通信を拒否  
   ・それ以外の通信は許可  
   **Router (config)#** [ ip access-list extended STOP-PING-WEB　] 名前付きの拡張ACL（名前：STOP-PING-WEB）を作成  
   **Router(config-ext-nacl)#** [ deny icmp 192.168.3.0 0.0.0.255 host 192.168.3.254　]   
   　　　　　　　　　　　　　　送信元：192.168.x.0/24から宛先：192.168.ｘ.254/32へのpingを拒否
2. **Router(config-ext-nacl)#** [ deny tcp 192.168.3.0 0.0.0.255 10.201.10.0 0.0.0.255 eq 80　]   
   　　　　　　　　　　　　　　送信元：192.168.x.0/24から宛先：10.201.10.0/24へのWeb通信を拒否
3. **Router(config-ext-nacl)#** [ permit ip any any　] それ以外の通信は許可  
   **Router(config-ext-nacl)#exit**  
   インターフェイスへの適用  
   設定すべきインターフェイスを選択、[**800M→G0/4・G0/5**]  
   設定すべき方向を選択[ **in / out**]  
   **Router(config)#** [　int g0/5　] 設定するインターフェイスへ  
   **Router(config-if)#** [　ip access-group STOP-PING-WEBc in　]  
   **Router(config-if)# exit**
4. アクセスリストの設定3  
   名前付きの拡張ACL（名前：STOP-GGL）を作成、適切なインターフェイスの適切な方向へ適用してください。  
   ACLの内容  
   ・ルータ(送信元：10.16.10.ｘ/32)からGoogleのＤＮＳサーバ(宛先：8.8.8.8/32)へのpingを拒否(xは出席番号)  
   ・それ以外の通信は許可  
   **Router (config)#** [ ip access-list extended STOP-GGL　　] 名前付きの拡張ACL（名前：STOP-GGL）を作成  
   **Router(config-ext-nacl)#** [ deny icmp host 10.16.10.3 host 8.8.8.8　] 送信元：10.16.10.ｘ/32から宛先：8.8.8.8/32へのpingを拒否  
   **Router(config-ext-nacl)#** [ permit ip any any　] それ以外の通信は許可  
   **Router(config-ext-nacl)#exit**
5. インターフェイスへの適用  
   設定すべきインターフェイスを選択、[ **800M→G0/4・G0/5**]  
   設定すべき方向を選択[ **in / out**]  
   **Router(config)#** [　int g0/4　] 設定するインターフェイスへ  
   **Router(config-if)#** [　ip access-group STOP-GGL out　　]  
   **Router(config-if)# exit**

接続の確認1

* 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.x.254）xは出席番号  
   [　接続できない　]  
  PCのコマンドプロントで、**arp -a**を実行し、***ルータのIPアドレス***（192.168.x.254）のMACアドレスを確認  
  192.168.x.254のMACアドレス：[　f8:f:6f:c8:13:12　]
* PCのコマンドプロントから **ping 10.201.10.24**を実行する  
   [　接続できた　]
* PCのブラウザで10.201.10.24を表示  
   [　表示できない　]
* グラフィカル ユーザー インターフェイス, テキスト, アプリケーション

  自動的に生成された説明SSH接続の確認1  
  Teratermでファイル→新しい接続　  
  ホスト：192.168.x.254(xは出席番号)  
  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：クラス出席番号  
  パスフレーズ：Cl@ss  
  でOKを押す  
  ルータに、[　接続できた　・　接続できない　]

接続の確認２

* ルータで**show access-lists**を実施し、表示内容を転記しなさい

Standard IP access list SSH-NAT

10 permit 192.168.3.0, wildcard bits 0.0.0.255 (562 matches)

Extended IP access list STOP-GGL

10 deny tcp host 10.16.10.3 host 8.8.8.8

20 permit ip any any (7259 matches)

Extended IP access list STOP-PING-WEBc

10 deny icmp 192.168.3.0 0.0.0.255 host 192.168.3.254 (7 matches)

20 deny tcp 192.168.3.0 0.0.0.255 10.201.10.0 0.0.0.255 eq www (5 matches)

30 permit ip any any (2462 matches)

**【チェック項目】上記「show access-lists」の出力をチェックしてもらうこと**

■提出　  
□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。

□チェックできなかった人

このWordファイル(docx)