|  |  |  |
| --- | --- | --- |
| Nom : PROFESSEUR | Prénom : CORRECTION | Date : \_ \_ / \_ \_ / 2 0 \_ \_ |

Configuration d'un réseau Routeur, Switch, VLAN, VLSM, ACL

Table des matières

[Découverte de Packet Tracer 3](#_Toc168254745)

[Rappel sur l’IP 8](#_Toc168254746)

[Service DNS et DHCP 12](#_Toc168254747)

[Configuration des adresses IP et passerelles 14](#_Toc168254748)

[Configuration d'un routeur PT (Activité 1/3) 16](#_Toc168254749)

[Ressources - Commandes CISCO 20](#_Toc168254750)

[Configuration d'un routeur PT Console (Activité 2/3) 22](#_Toc168254751)

[Configuration d'un routeur Cisco 1721 (Activité 3/3) 23](#_Toc168254752)

[Configuration des routes d’un réseau 26](#_Toc168254753)

[Configuration d'un réseau PT 27](#_Toc168254754)

[Bilan configuration d’un routeur 31](#_Toc168254755)

[Synthèse de la configuration d'un réseau PT (IP, Passerelles, Routeurs, Routes) 32](#_Toc168254756)

[Configuration d’un réseau avec des VLAN 36](#_Toc168254757)

[Révision d’un réseau avec des VLAN 48](#_Toc168254758)

[VLSM 51](#_Toc168254759)

[Synthèse VLSM 57](#_Toc168254760)

[ACL : Access Control List 59](#_Toc168254761)

[Exercices ACL : Access Control List 65](#_Toc168254762)

[ACL Réseau à configurer 71](#_Toc168254763)

[Exercices simulation PT : Configurer les ACLs IPv4 standard numérotées 75](#_Toc168254764)

[Exercices simulation PT : Configurer les ACLs IPv4 standard nommées 77](#_Toc168254765)

[77](#_Toc168254766)

[Exercices simulation PT : Configurer les ACLs IPv4 étendues 78](#_Toc168254767)

[78](#_Toc168254768)

Dossiers ressources utiles :

[\\polonium\Ressources\](file:///\\polonium\Ressources\) (id : ciel , mdp : ciel) : Cisco

ou nlardon.github.io : Cisco

Compte NetAcad (Cisco)

* Login :
* Mot de passe :

# Découverte de Packet Tracer

*Source Activité 1 BTS SIO Louise Michel*

L’objectif de cette activité est d’être capable d’utiliser le logiciel de simulation réseau Packet Tracer de Cisco.

## Quelques prérequis

Définissez l'acronyme DHCP.

Définir simplement le rôle du DHCP.

Définir simplement le rôle de la passerelle.

Définissez l'acronyme DNS.

Définir simplement le rôle du DNS.

Définir simplement le rôle du routeur.

## Plan réseau

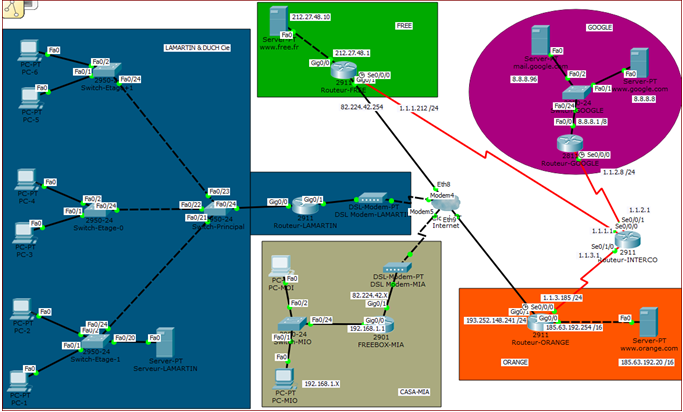
Copier le fichier SI2-Activite-1-PT-ve.pkt sur votre PC. Ouvrir ce fichier.

**PRESENTATION DE LA MAQUETTE**

La maquette proposée comporte :

* Le réseau (privé) de l’entreprise « LAMARTIN & DUCH Cie » (réseau bleu)
* Une représentation partielle de ce que pourrait être Internet :
  + Deux fournisseurs d’accès (Orange et Free : respectivement rectangles « orange » et « vert »)
  + La connexion d’un internaute via une BOX (rectangle gris)
  + Un 3ème réseau présent sur Internet, une reproduction simpliste du réseau de Google, composé de 2 serveurs : google.com et mail.google.com

Le fournisseur d’accès Internet (FAI) de la société LAMARTIN & DUCH est ORANGE, alors que l’internaute possède un abonnement FREE.



Le schéma ci-dessus présente la maquette finale. Le fichier qui vous est fournie contient la maquette avec quelques éléments en moins. Ne figurent pas sur le schéma initial :

* PC-5 et PC-6 -> Réseau LAMARTIN & DUCH
* Switch-Etage+1 -> Réseau LAMARTIN & DUCH
* PC-MOI -> Réseau CASA-MIA

Par ailleurs la maquette est opérationnelle, comme vous pourrez le constater, dès que les voyants des switchs sont au vert. A l’ouverture ils sont momentanément de couleur orange.

Votre mission, si vous l’acceptez (et idem si vous ne l’acceptez pas ;-) consiste à faire quelques vérifications / opérations de découverte, puis à ajouter les éléments manquants.

**PARTIE 1 – VERIFICATIONS**

**Vérification de l’adresse IP de PC1 et PC2**

|  |  |
| --- | --- |
|  | Cliquer sur PC-1 |
|  | Accéder à l’onglet « Desktop » qui vous montre les applications disponibles sur le « bureau » ;-)  Choisir l’invite de commandes (Command Prompt) |
|  | Taper « ipconfig » puis « ipconfig /all » et examiner les informations fournies.  L’adresse IP est-elle :   statique ? dynamique ?  Si l’adresse est obtenue dynamiquement, quelle est l’adresse du serveur DHCP ?    Quelle est l’adresse de la passerelle par défaut ?   |
| Indiquer l’adresse IP obtenue si différente de la copie d’écran ci-dessus : |  |

Procéder de même pour PC2.

|  |
| --- |
| Taper « ipconfig » puis « ipconfig /all » et examiner les informations fournies.  L’adresse IP est-elle :   statique ?  dynamique ?  Si l’adresse est obtenue dynamiquement, quelle est l’adresse du serveur DHCP ?    Quelle est l’adresse de la passerelle par défaut ?   |

**Vérification de la connexion avec ORANGE et FREE**

|  |  |
| --- | --- |
| Depuis le PC-1 connexion OK vers Orange et Free : | Depuis le PC-2 connexion OK vers Orange et Free : |

**Vérification de l’accès aux serveurs WEB de GOOGLE**

Vous allez utiliser maintenant l’outil de navigation (web browser)

|  |  |
| --- | --- |
| Accès à **www.google.com** | Accès à **mail.google.com** |
|  |  |

Faites la vérification sur PC2

**Vérification de la communication de PC-MIO avec FREE**

|  |  |
| --- | --- |
| Vérification de l’accès à **www.free.fr** | Vérification de l’accès à **www.orange.com** |

**Comparaison du nombre de sauts effectués par PC-MIO et PC-1 pour joindre www.google.com**

*Utiliser l’invite de commandes*

|  |  |
| --- | --- |
|  |  |
| Cocher la case correspondant au PC concerné :   PC-MIO PC-1 Impossible de savoir | Cocher la case correspondant au PC concerné :   PC-MIO PC-1 Impossible de savoir |

Conclusion : Même nombre de sauts ?  OUI NON

Combien de sauts ?

**Comparaison de la route empruntée par PC-MIO et PC-1 pour joindre www.google.com**

*Toujours dans l’invite de commande, mais en utilisant la commande* ***tracert***

|  |  |
| --- | --- |
|  |  |
| Cocher la case correspondant au PC concerné :   PC-MIO PC-1 | Cocher la case correspondant au PC concerné :   PC-MIO PC-1 |

Empruntent-ils le même chemin ?  OUI NON

Donner précisément le nom de tous actifs (switchs et routeurs) traversés par les paquets pour chaque PC pour atteindre le serveur GOOGLE.COM :

|  |  |
| --- | --- |
| **PC-MIO** | **PC-1** |
|  |  |

**Modifier la configuration IP de PC-3 et PC-4 pour qu’ils obtiennent une adresse IP dynamique**

Utiliser l’outil « **IP Configuration** »

|  |  |
| --- | --- |
|  |  |
| Cliquer sur « DHCP » et noter l’adresse IP si différente :   | Cliquer sur « DHCP » et noter l’adresse IP si différente :   |

Depuis **PC-3**, pinguer **PC-1** (avec son adresse IP) et **www.orange.com**. Effectuer une copie d’écran

# Rappel sur l’IP

## Rappel

* LAN : Local Area Network (réseau local)
* WAN : Wide area network (réseau étendu)
* Adresse IP : Une adresse IP (Internet Protocol) est un numéro d'identification qui est attribué de façon permanente ou provisoire.
* Adresse MAC : Une adresse MAC (Media Access Control) ou adresse physique est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire. Elle est unique au monde.

## Adresse IP

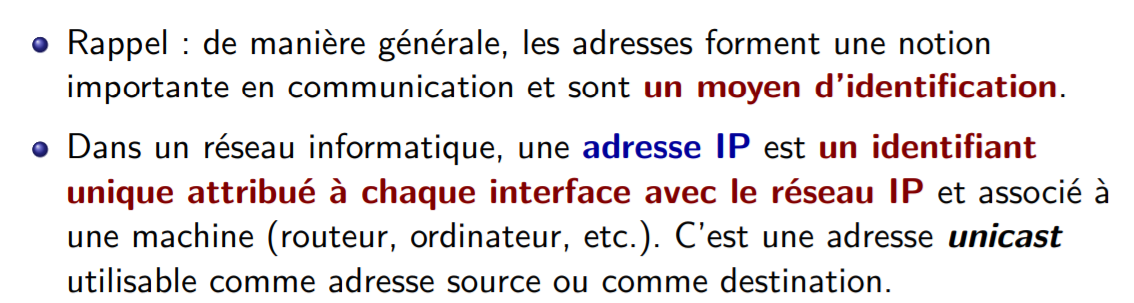
* Décimal : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
* Binaire : 0, 1
* 1 bit est l’unité la plus simple dans un système binaire
* 1 octet = 8 bits

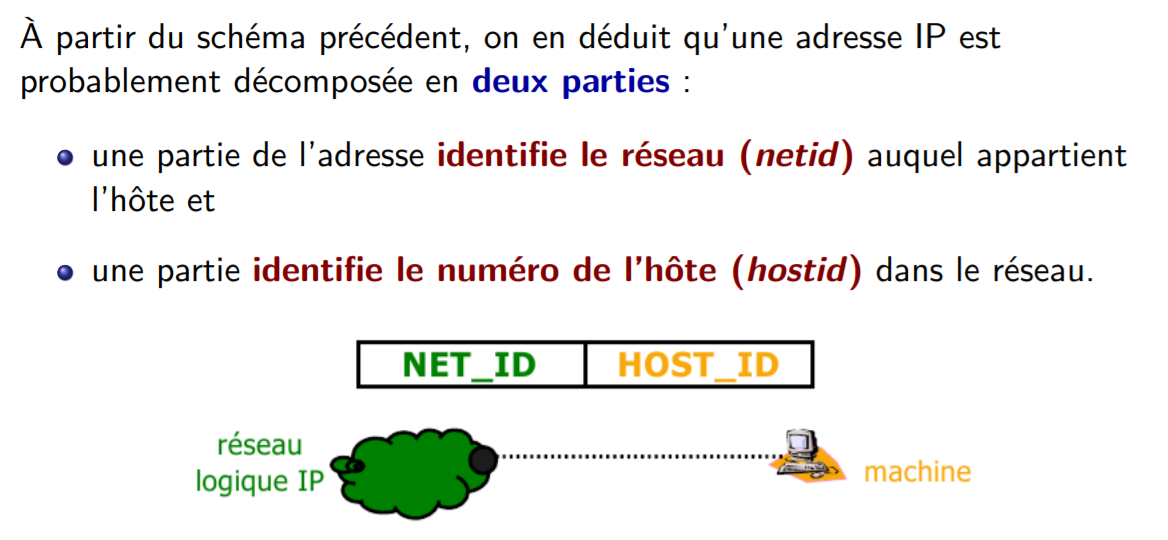
Conversion Décimal <-> Binaire



Opérations en binaire







* **Adresse Réseau = Adresse IP && Masque**
* **1er Adresse = Adresse Réseau + 1**
* **Dernière Adresse = Adresse de Diffusion – 1**
* **Adresse de diffusion = Adresse Réseau + Masque inversé**
* **Masque inversé = M̃ = 255.255.255.255 - Masque**

*Exemple : Nous cherchons l’adresse réseau de cette adresse IP :* ***10.5.100.16 / 20***

Etape 1 : On écrit le masque en décimal pointé

/20 = en binaire 1111 1111 . 1111 1111 . 1111 0000 . 0000 0000 soit 255.255.240.0

Etape 2 : On réalise l’opération ET bit à bit entre l’adresse réseau et le masque, où le masque est différent de 0 ou 255.

* Si 0, le résultat = 0
* Si 255, le résultat = le nombre de l’adresse réseau
* Si autre opération ET bit à bit

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Addresse IP | 10 | 5 | **100**  **binaire 0110 0100** | 16 |
| Masque | 255 | 255 | **240**  **binaire 1111 0000** | 0 |
| Adresse Réseau | 10 | 5 | **résultat ET 0110 0000**  **96** | 0 |

On obtient l’adresse réseau : **10 . 5 . 96 . 0 / 20**

Nous cherchons maintenant : l’adresse de diffusion, la première et la dernière adresse attribuable.

Etape 3 : On calcule le masque inversé

* Masque inversé = M̃ = 255.255.255.255 - 255.255.240.0 = **0.0.15.255**

Etape 4 : On calcule l’adresse de diffusion

* Adresse de diffusion = Adresse Réseau + M̃ = 10.5.96.0 + 0.0.15.255 = **10.5.111.255**

Etape 5 : On calcule la première et la dernière adresse attribuable

* 1er Adresse = Adresse Réseau + 1 = 10.5.96.0 + 1 = **10.5.96.1**
* Dernière Adresse = Adresse de Diffusion – 1 = 10.5.111.255 - 1 = **10.5.111.254**

|  |  |
| --- | --- |
| Nombre de machine sur notre réseau :   * 2^(Nombre “1” dans le masque inversé) - 2:   + 0.0.15.255 = 00000000.00000000.00001111.11111111 soit 12 “1”   + 212 - 2 soit 4094 machines * 2^(32 - préfixe) - 2   + 32 - préfixe = 32 – 20 = 12   + 212 - 2 soit 4094 machines | 1111 1111 = 255  1111 1110 = 254  1111 1100 = 252  1111 1000 = 248  1111 0000 = 240  1110 0000 = 224  1100 0000 = 192  1000 0000 = 128 |

#### Exercice 1

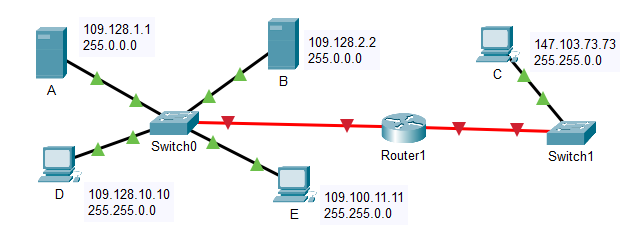
Une machine faisant partie d’un réseau local est reliée à l’Internet, sa configuration est la suivante :

Adresse IP : 192.168.54.53 Netmask : 255.255.255.224

1.1 Quelle est l’adresse de sous-réseau (adresse réseau) ?

1.2 Quel le numéro de la machine dans ce sous-réseau ?

#### Exercice 2



2.1 Précisez la plage du réseau pour les machines A – B – D – E. (1ère adresse à la dernière adresse).

2.2 Quelles sont les machines qui peuvent se voire entre elles ?

2.3 En quoi un masque de sous-réseau invalide affecte-t-il ces hôtes ?

2.4 Quel est le masque de sous-réseau correct pour que toutes les machines (sauf C) puissent se voir ?

#### Exercice 3

Soit l’adresse 192.16.5.133/29

3.1 Combien de bits sont utilisés pour identifier la partie réseau ?

3.2 Combien de bits sont utilisés pour identifier la partie hôte ?

3.3 Quel est le masque réseau correspondant (en décimal pointé) ?

3.4 Quel est l’adresse réseau ?

#### Exercice 4

Soit l’adresse 172.16.5.10/28

4.1 Quel est le masque réseau correspondant (en décimal pointé) ?

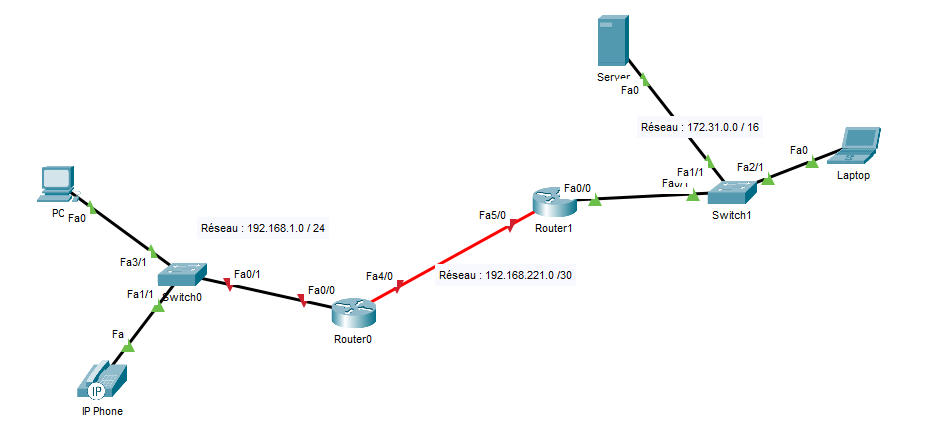
4.2 Quel est le masque réseau correspondant (en décimal pointé) ?

4.3 Quel est l’adresse réseau ?

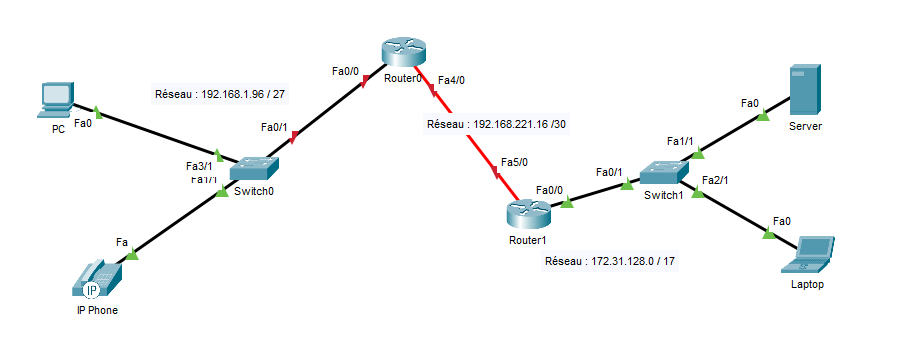
## Exemples de réseau

## 

Exemple réseau 1 : « Exemple réseau 1.pkt »



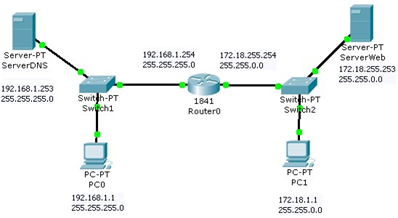
Exemple réseau 2 : « Exemple réseau 2.pkt »



# Service DNS et DHCP

## Service DNS

Pour accéder à un service hébergé sur un ordinateur distant, il faut adresser une requête à ce dernier. Les ordinateurs sont repérés grâce à leur adresse IP, ce qui pose un problème de mémorisation pour l'utilisateur. En effet, il est plus facile de se rappeler d'un nom que d'un numéro. C'est pourquoi on utilise le service DNS qui assure une correspondance entre les adresses IP des ordinateurs et les noms des domaines qu'il héberge.

Par exemple, www.google.fr = 74.125.43.99

Ouvrir le schéma « Activité DNS DHCP.pkt » :

Placer vous en mode simulation.

Ouvrer le navigateur web de PC0 et adresser une requête au serveur Web :

|  |  |
| --- | --- |
|  | Cliquer sur PC0, puis sur l'onglet Desktop, puis sur le bouton Web Browser.  Dans la barre d'adresse du navigateur, saisissez <http://172.18.255.253>  Cliquer sur Go et lancer la simulation.  Observer l'envoi de la requête (upload) et le retour d'information du serveur (download).  Vérifier que la page web envoyée par le serveur est bien affichée dans le navigateur de PC0. |

Renseigner le serveur DNS

|  |  |
| --- | --- |
|  | Cliquer sur le Serveur DNS, puis sur l'onglet Config, puis sur le bouton DNS.  Dans le champ Domain Name, saisissez [www.edison.com](http://www.edison.com)  Dans le champ IP Address, saisissez <http://172.18.255.253>  Cliquer sur le bouton Add |

Configurer les paramètres IP de PC0 pour lui indiquer l'adresse du serveur DNS.

En mode simulation : Dans le navigateur de PC0, adresser une nouvelle requête au serveur Web en utilisant directement son nom de domaine (http://www.edison.com dans la barre d'adresses).

Vérifier que la page web envoyée par le serveur est bien affichée dans le navigateur de PC0.

## Adressage automatique

Lorsque le réseau contient un très grand nombre d'ordinateurs, il est difficile de le paramétrer leurs adresses IP manuellement. On utilise alors un serveur DHCP.

1. Configurer le service DHCP, du serveur DHCP pour fournir les bonnes informations aux postes clients.

|  |  |
| --- | --- |
| Configuration DHCP | Adresse de départ : 172.18.255.1 |
| Nombre maximum d'hôtes : 255 |
| Passerelle : 172.18.255.254 |
| DNS : 192.168.1.253 |

Configurer l'adresse IP de PC1 en automatique (DHCP).

Placer Packet Tracer en Realtime et adresser une requête de renouvellement d'adresse IP au serveur DHCP :

* Exécuter la commande « ipconfig /renew » sur PC1 dans l'environnement « Command Prompt ».

1. Indiquer quelle est l'adresse fournie par le serveur à PC1 : Exécuter la commande « ipconfig /all » sur PC1 dans l'environnement « Command Prompt ».
2. Indiquer quelle est l'adresse fournie par le serveur à PC1 : Exécutez la commande « ipconfig /all » sur PC1 dans l'environnement « Command Prompt ».

|  |  |
| --- | --- |
| PC1 | Adresse IP : |
| Masque : |
| Passerelle : |
| DNS : |

# Configuration des adresses IP et passerelles

L’objectif de cette activité est d’être capable de configurer les adresses IP et les passerelles.

## Plan réseau

**Copier** le fichier « Config ip et passerelles.pka » sur votre PC.

**Ouvrir** ce fichier.

Réseau :

* VLAN221 : 192.168.221.0 / 24
* Pédago : 172.20.40.0 / 22
* Admin : 10.38.80.0 / 24
* MELEC : 172.24.0.0 / 16
* SSIHT : 172.31.0.0 / 16
* RISC : 10.0.0.0 / 8

**A faire :**

Routeur-Lycée :

* fa1/0 Dernière adresse attribuable du réseau Pédago
* fa2/0 Dernière adresse attribuable du réseau Admin
* fa3/0 Dernière adresse attribuable du réseau VLAN221

ServeurLycée :

* 2e adresse attribuable du réseau Pédago

Photocopieur :

* 123e adresse attribuable du réseau Pédago

PC-Proviseur :

* 8e adresse attribuable du réseau Admin

PC-DDF :

* 50e adresse attribuable du réseau Admin

Routeur-MELEC :

* fa0/0 24e adresse attribuable du réseau VLAN221
* fa1/ 1er adresse attribuable du réseau MELEC

Routeur-SSIHT :

* fa0/0 172e adresse attribuable du réseau VLAN221
* fa1/0 1er adresse attribuable du réseau SSIHT

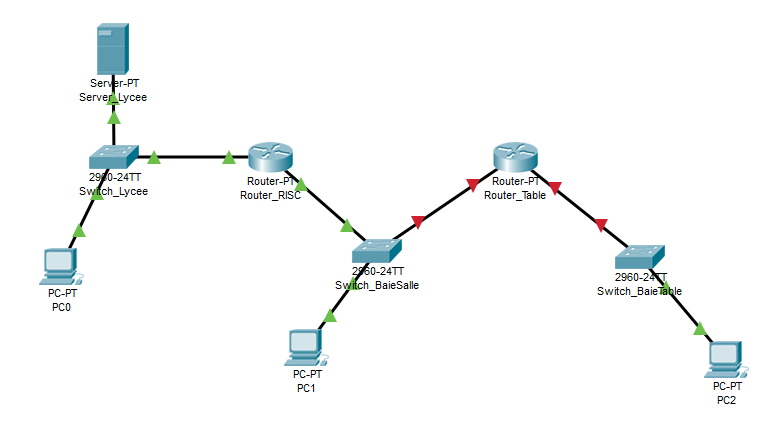
Configurer les passerelles des serveurs MELEC, SSIHT et RISC

# Configuration d'un routeur PT (Activité 1/3)

L’objectif de cette activité est d’être capable de configurer un routeur.

## Plan réseau

**Copier** le fichier activite-config-router.pkt sur votre PC.

**Ouvrir** ce fichier.

**Identifier** les 3 réseaux sur le plan réseau :

* Réseau Lycée
* Réseau SalleRISC
* Réseau Table

**Numéro de table :**

**Compléter** le tableau “Table des équipements” avec les informations dont vous disposez dans la simulation (toutes les informations ne sont pas encore configurées).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nom de l’équipement | Interface | Adresse IP | Masque de sous réseau | Adresse réseau | Passerelle |
| Server\_Lycée | fa0 | 172.16.80.10 | 255.255.0.0 | 172.16.0.0 | 172.16.130.10 |
| PC0 | fa0 | 172.16.130.30 | 255.255.0.0 | 172.16.0.0 | 172.16.130.10 |
| Router\_RISC | Fa0/0 | 10.0.0.1 | 255.0.0.0 | 10.0.0.0 |  |
| Router\_RISC | Fa0/1 | 172.16.130.10 | 255.255.0.0 | 172.16.0.0 |  |
| PC1 | fa0 | 10.0.2.2 | 255.0.0.0 | 10.0.0.0 | 10.0.0.1 |
| Router\_Table | Fa0/0 | 10.x.0.1 | 255.0.0.0 | 10.0.0.0 |  |
| Router\_Table | Fa0/1 | 192.168.x.1 | 255.255.255.0 | 192.168.x.0 |  |
| PC2 | fa0 | 192.168.x.10 | 255.255.255.0 | 192.168.x.0 | 192.168.x.10 |

Adresse DNS : 172.16.80.10

**Test du réseau Lycée**

|  |  |
| --- | --- |
| Tester la connexion entre : | OK / NOK |
| PC0 et Server\_Lycée | OK |
| PC0 et l’interface Fa1/0 de Router\_RISC | OK |
| PC0 et l’interface Fa0/0 de Router\_RISC | OK |
| Server\_Lycée et l’interface Fa1/0 de Router\_RISC | OK |
| Server\_Lycée et l’interface Fa0/0 de Router\_RISC | OK |

**Test du réseau SalleRISC**

|  |  |
| --- | --- |
| Tester la connexion entre : | OK / NOK |
| PC1 et Server\_Lycée | OK |
| PC1 et l’interface Fa1/0 de Router\_RISC | OK |
| PC1 et l’interface Fa0/0 de Router\_RISC | OK |

**Configuration du routeur entre le réseau SalleRISC et le réseau Table**

Interface fa0/0

**Donner** une adresse IP à l’interface fa0/0 du routeur “Router-Table”. Avec le deuxième octet de l’adresse IP votre numéro de table :

* Ex pour la table 9 : xxx.009.xxx.xxx

Activer l’interface “On”

Compléter le tableau.

Interface fa1/0

**Configurer** l’adresse IP de l’interface fa1/0 du routeur “Router-Table” par :

* Adresse IP : 192.168.x.1 (x le numéro de table)
* Masque sous réseau : 255.255.255.0

**Activer** l’interface “On”

**Compléter** le tableau.

PC2

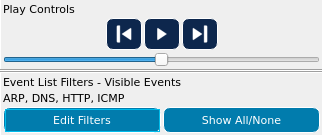
**Donner** une adresse IP à l’interface fa0 du PC “PC2”.

**Configurer** l’adresse passerelle et l’adresse DNS.

**Compléter** le tableau.

**Test du réseau Table**

|  |  |
| --- | --- |
| Tester la connexion entre : | OK / NOK |
| PC2 et l’interface Fa1/0 de Router\_Table | OK |
| PC2 et l’interface Fa0/0 de Router\_Table | OK |
| PC2 et PC1 | NOK |
| PC2 et PC0 | NOK |
| PC2 et Server\_Lycee | NOK |

**Passer** en mode Simulation. Configurer les filtres comme ceci :

**Tester** la connexion entre PC2 et PC1.

**Lancer** la simulation (Symbole Play)

**Observer** l’échange et **identifier** où est le problème.

**STOP Appel professeur STOP**

**Configuration d’une route sur le routeur “Router\_RISC”**

**Configurer** une route dans le routeur “Router\_RISC” pour résoudre le problème de communication entre PC2 et PC1.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Network (destination) | Masque | Next Hop |
| Routeur : Router\_RISC | 192.168.x.0 | 255.255.255.0 | 10.x.0.0 |

**Passer** en mode Simulation.

**Observer** la connexion entre PC2 et PC1.

**Configuration d’une route sur le routeur “Router\_Table”**

**Passer** en mode Simulation.

**Tester** la connexion entre PC2 et PC0.

**Lancer** la simulation (Symbole Play)

**Observer** l’échange et identifier où est le problème.

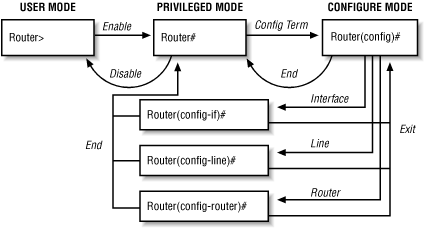
**Configurer** la route nécessaire.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Network (destination) | Masque | Next Hop |
| Routeur : Router\_Table | 172.16.0.0 | 255.255.0.0 | 10.0.0.1 |

**Compléter** le tableau table de routage.

**Tester** depuis le “Web Browser” de PC2 d’accéder au site : hello.fr

# Ressources - Commandes CISCO



« **enable** » ou « **ena** » ou « **en** » pour passer en mode administrateur sur l'équipement réseau.

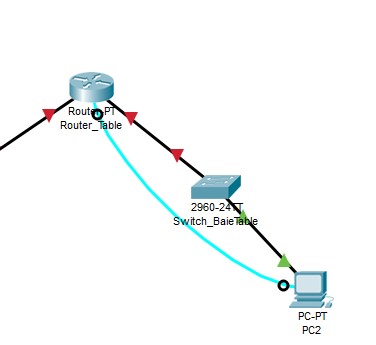
“ **configure terminal** ” ou “ **conf term** ” ou “ **conf t** ” pour passer en mode configuration globale.

|  |  |
| --- | --- |
| ***Commandes en Mode Configuration Globale = Configure Mode*** | |
| hostname <hostname> ou host <hostname> | Permet de modifier le nom de l'équipement réseau |
| enable secret <password> | Assigne un mot de passe encrypté à enable |
| no ip domain lookup | Désactiver la recherche DNS sur un routeur cisco |
| ip route <réseau distant> <masque réseau réseau distant> <passerelle d'accès> | Ajoute une route |
| ***Configuration d’une interface en le Mode Configuration Globale*** | |
| interface <interface>  int <interface> | Entre dans le mode de configuration de l'interface |
| ip address <address> <mask>  ip add <address> <mask> | Configure l'interface avec l'ip et le masque de réseau |
| no shutdown ou no shut | Active l'interface |
| shutdown ou shut | Désactive l'interface |
| ***Les commandes de sauvegarde en Mode Administration = Privileged Mode*** | |
| copy running-config startup-config | Sauvegarde la configuration courante en NVRAM |
| erase startup-config | Efface la configuration de la NVRAM |
| **Commandes show :** |  |
| show interfaces | Donne une description détaillée sur les interfaces |
| show ip interface brief | Affiche un résumé des interfaces |
| show running-config | Affiche la configuration courante |
| show startup-config | Affiche la configuration en NVRAM |
| show ip route | Affiche la table de routage |
| show ip protocols | Affiche des informations sur les protocoles utilisés |
| show ? | Donne toutes les commandes show disponibles |
| reload | Redémarre l'équipement réseau |
| ping [<address>] | ping |

# Configuration d'un routeur PT Console (Activité 2/3)

L’objectif de cette activité est d’être capable de configurer un routeur en mode console. Nous configurerons le réseau comme celui de l’activité Configuration d'un routeur PT (Activité 1/3). Mais la configuration du routeur sera faite par console. Certains éléments sont verrouillés.

## Plan réseau

**Copier** le fichier activite-config-router\_console.pka sur votre PC.

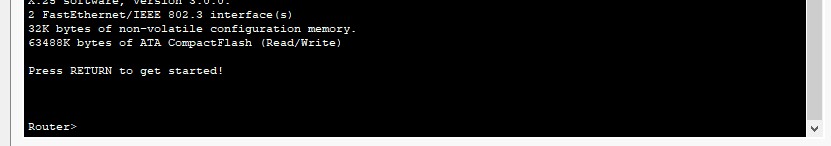
**Ouvrir** ce fichier.

## Configurer un routeur depuis un PC

**Configurer** l’adresse IP, passerelles, DNS de PC2.

**Connecter** le PC PC2 au Routeur ”Router\_Table” à l’aide d’un câble console.

Dans le PC PC2, ouvrir un Terminal puis OK



Vous disposez d’une ressource “Commandes\_CISCO”, qui va vous permettre de configurer le routeur en commande.

**Entrer** les commandes suivantes, en **Mode Configuration** :

* no ip domain lookup
* exit
* exit

**Renommer** votre routeur hostname par Router\_Table.

**Mettre** le mot de passe “cisco” à votre routeur.

**Configurer** les 2 interfaces du routeur “Router\_Table”.

**Ajouter des tables de routage**

**Configurer** la route nécessaire sur le routeur “Router\_RISC”. (Attention il faut déplacer le câble console sur le bon routeur.)

**Tester** la connexion entre PC2 et PC1.

**Configurer** la route nécessaire sur le routeur “Router\_Table”. (Attention il faut déplacer le câble console sur le bon routeur.)

**Tester** la connexion entre PC2 et PC0.

**Tester** depuis le “Web Browser” d’accéder au site : [hello.fr](http://www.hello.fr)

# Configuration d'un routeur Cisco 1721 (Activité 3/3)



L’objectif de cette activité est d’être capable de configurer un routeur en mode console. Nous configurerons le réseau comme celui de l’activité Configuration d'un routeur PT. Mais la configuration du routeur sera faite par console et sur du matériel.

## Configurer un routeur depuis un PC

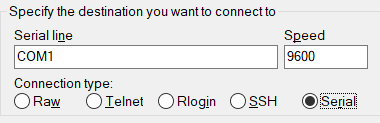
**Le routeur éteint**

**Connecter** un PC au Routeur ”Router\_Table” à l’aide d’un câble console.

* Coté PC, soit sur le port DB9 (port série) ou le port USB (adaptateur USB – DB9)
* Coté routeur, sur le port Console

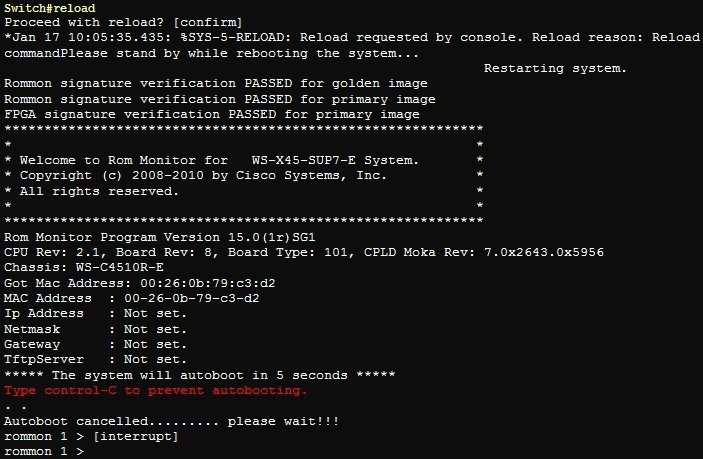
Sur le PC, ouvrir un Terminal (comme Putty), choisir le port COM puis Open.

*Dans le gestionnaire de périphérique de Windows, vous trouverez le port COM utilisé (COM1, COM2, …)*



**Nous allons procéder un factory reset du routeur.**

* Allumer le routeur
* Dans les premières secondes, appuyer sur Ctrl + Pause (Ctrl + Break)

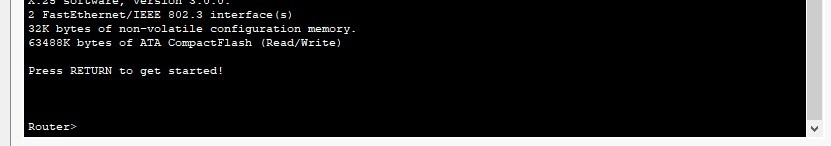
Vous devez entrer en menu ROMMON.

* Entrer la commande : **confreg 0x2142**
* Puis : **reset**

Le routeur va entrer dans sa phase d’initialisation (environ 1min).

* Répondre **no** aux questions si demandées

Appuyer sur la touche “Entrée”, si l’initialisation est finie vous devez avoir ceci :



*Remarque avant de commencer :*

* *La console peut vous afficher des informations alors que vous êtes en train d'écrire une commande. Appuyer sur la touche “Tab” pour continuer votre commande.*

**Entrer** les commandes suivantes, en **Mode Configuration** :

* no ip domain lookup
* exit
* exit

Vous disposez d’une ressource “Commandes\_CISCO”, qui va vous permettre de configurer le routeur en commande.

**Renommer** votre routeur hostname par Router\_Table#. (# numéro de table)

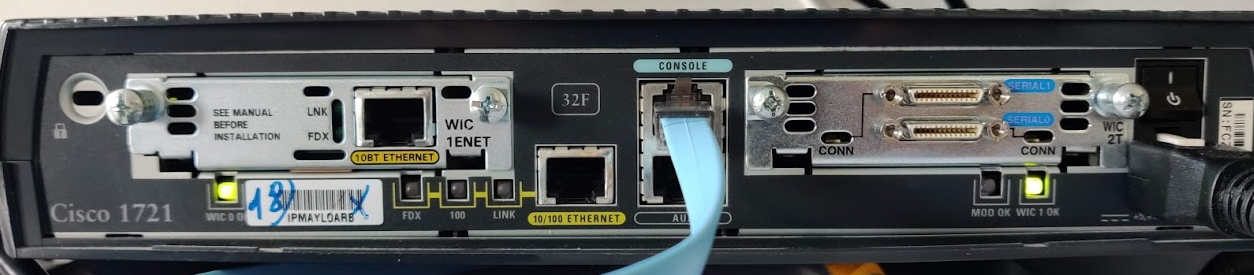
**Mettre** le mot de passe “cisco” à votre routeur.

**Afficher** les interfaces du routeur.

**Compléter** le tableau avec le nom des interfaces.

|  |
| --- |
| Interfaces |
|  |
|  |
|  |
|  |

**Identifier** sur l’image les interfaces trouvées précédemment.



**STOP : Appel Professeur**

**Compléter** le tableau “Table des équipements” avec les informations de l’activité précédente (1/3), en changeant le nom des interfaces par celle de votre routeur.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nom de l’équipement | Interface | Adresse IP | Masque de sous réseau | Adresse réseau |
| Router\_Table |  |  |  |  |
| Router\_Table |  |  |  |  |

**Configurer** les 2 interfaces du routeur “Router\_Table”.

**Configurer** la route nécessaire sur le routeur “Router\_Table”.

**Brasser** l’interface du routeur du réseau 192.168.x.0/24 sur le switch HP vert

**Brasser** l’interface du routeur du réseau 10.0.0.0/8 sur le switch HP rouge

**Relier** le réseau de la salle (switch Netgear bleu) au switch HP rouge

**Brasser** un PC sur le réseau 192.168.x.0/24 (réseau de votre Table)

* **Attribuer** une adresse statique à ce PC.

**Donner** la route que le professeur doit implémenter dans le routeur de la salle RISC.

**Tester** la communication entre ce PC et un autre PC du réseau 10.0.0.0 (réseau de la Salle RISC)

**STOP : Appel Professeur**

**Mise en place d’un serveur DHCP sur le réseau 192.168.1.0**

Paramètre :

* Nom\_du\_LAN = *LAN\_Table#*
* *Addresse\_réseau = 192.168.1.0*
* *Masque = 255.255.255.0*
* Serveur\_DNS = 10.0.6.1
* Passerelle = 192.168.1.1

En Mode Configuration Globale entrer les commandes :

* ip dhcp pool ***Nom\_du\_LAN***
* network ***Addresse\_réseau Masque***
* dns-server *Serveur\_DNS*
* default-router *Passerelle*

**Configurer** le PC du réseau 192.168.1.0, en attribution automatique d’adresse IP.

**Noter** l’adresse obtenue.

# Configuration des routes d’un réseau

## Plan réseau

**Copier** le fichier Config route.pkt sur votre PC.

**Ouvrir** ce fichier.

**Configurer** les routes sur les 2 routeurs.

Sur le routeur Router 0 :

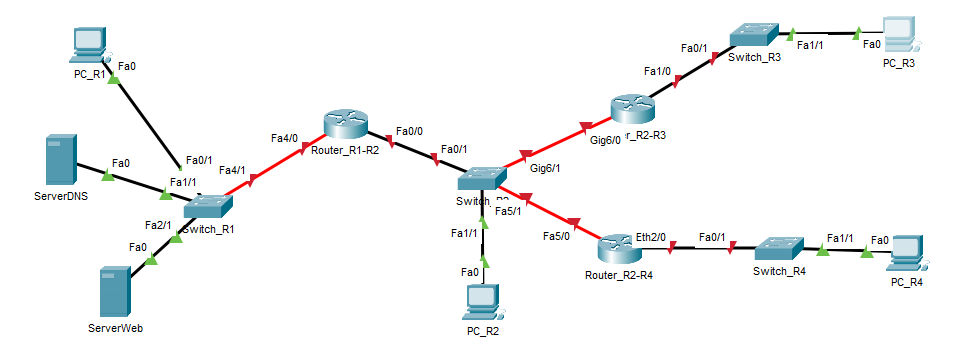
Sur le routeur Router 1 :

# Configuration d'un réseau PT

L’objectif de cette activité est d’être capable de configurer un réseau et ses routeurs.

**Identifier** les 4 réseaux sur le plan réseau :

* Réseau R1
* Réseau R2
* Réseau R3
* Réseau R4

**Le fichier de simulation est :** **activite\_config-router\_2.pka**

**Compléter** le tableau “Table des équipements” au fur et à mesure de l’activité. Ne rien paramétrer dans la simulation PacketTracer.

* **Déterminer** l’adresse réseau et masque de sous réseau des équipements PC\_R1, ServerDNS et ServerWeb
* **Attribuer** les adresses IP selon leurs réseaux pour les équipements PC\_R2, PC\_R3 et PC\_R4
* **Attribuer** une adresse IP, pour chaque interface connectée (**noter** le nom de l’interface) du Router\_R1-R2.
* **Attribuer** une adresse IP, pour chaque interface connectée (**noter** le nom de l’interface) du Router\_R2-R3.
* **Attribuer** une adresse IP, pour chaque interface connectée (**noter** le nom de l’interface) du Router\_R2-R4.
* **Attribuer** les adresses passerellespour les équipements PC\_R2, PC\_R3 et PC\_R4

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nom de l’équipement | Interface | Adresse réseau  / CIDR | Adresse machine IP | Passerelle |
| PC\_R1 | FastEthernet0 | 80.0.0.0 / 8 | 80.0.2.3 | 80.0.2.254 |
| ServerDNS | FastEthernet0 | 80.0.0.0 / 8 | 80.0.2.1 | 80.0.2.254 |
| ServerWeb | FastEthernet0 | 80.0.0.0 / 8 | 80.0.2.2 | 80.0.2.254 |
| Router\_R1-R2 | Fa4/0 | 80.0.0.0 / 8 | 80.0.2.254 |  |
| Router\_R1-R2 | Fa0/0 | 172.20.0.0 / 16 | 172.20.0.251 |  |
| Router\_R2-R3 | Gig6/0 | 172.20.0.0 / 16 | 172.20.0.253 |  |
| Router\_R2-R3 | Fa1/0 | 200.0.30.0 / 24 | 200.0.30.1 |  |
| Router\_R2-R4 | Fa5/0 | 172.20.0.0 / 16 | 172.20.0.254 |  |
| Router\_R2-R4 | Eth2/0 | 200.0.40.0 / 24 | 200.0.40.1 |  |
| PC\_R2 | FastEthernet0 | 172.20.0.0 / 16 | 172.20.0.3 | 172.20.0.251 |
| PC\_R3 | FastEthernet0 | 200.0.30.0 / 24 | 200.0.30.3 | 200.0.30.1 |
| PC\_R4 | FastEthernet0 | 200.0.40.0 / 24 | 200.0.40.3 | 200.0.40.1 |

PC\_R1 ne peut pas communiquer avec le PC\_R3, **créer** les routes nécessaires dans les routeurs Router\_R1-R2 et Router\_R2-R3.

PC\_R1 ne peut pas communiquer avec le PC\_R4, **créer** les routes nécessaires dans les routeurs Router\_R1-R2 et Router\_R2-R4.

PC\_R3 ne peut pas communiquer avec le PC\_R4, **créer** les routes nécessaires dans les routeurs Router\_R2-R3 et Router\_R2-R4.

|  |  |  |  |
| --- | --- | --- | --- |
| Routeur | Network (destination) | Masque | Next Hop |
| Router\_R1-R2 |  |  |  |
| Router\_R1-R2 |  |  |  |
| Router\_R2-R3 |  |  |  |
| Router\_R2-R3 |  |  |  |
| Router\_R2-R4 |  |  |  |
| Router\_R2-R4 |  |  |  |

**Effectuer** un ping entre PC\_R3 et PC\_R4, noter le temps de réponse et le TTL pour un paquet reçu avec succès.

Temps : TTL :

**Effacer** les routes dans les routeurs : Router\_R2-R3 et Router\_R2-R4, remplacer les par une route par défaut :

Exemple : Network 0.0.0.0 Masque 0.0.0.0 Next Hop 172.20.0.151, si le réseau est inconnu et qu’il n’existe pas de route le paquet est transféré à une adresse suivante.

Dans notre activité le Next Hop de la route par défaut sera l’adresse du Router\_R1-R2

**Effectuer** un ping entre PC\_R3 et PC\_R4, noter le temps de réponse et le TTL pour un paquet reçu avec succès.

Temps : TTL :

**Noter** un avantage et un inconvénient de cette méthode.

**Effacer** les routes dans les routeurs : Router\_R2-R3 et Router\_R2-R4, remplacer les par une route par défaut vers une interface :

Exemple :

* Pour le Router\_R2-R3 : Network 0.0.0.0 Masque 0.0.0.0 Next Hop G6/0
* Pour le Router\_R2-R4 : Network 0.0.0.0 Masque 0.0.0.0 Next Hop Fa5/0

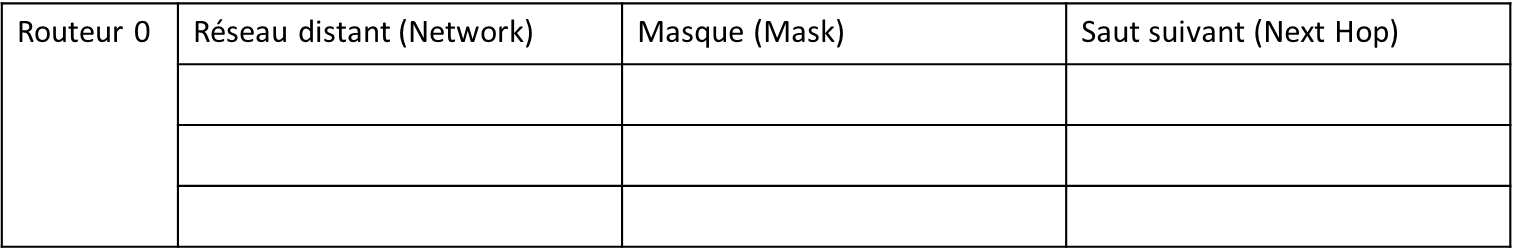
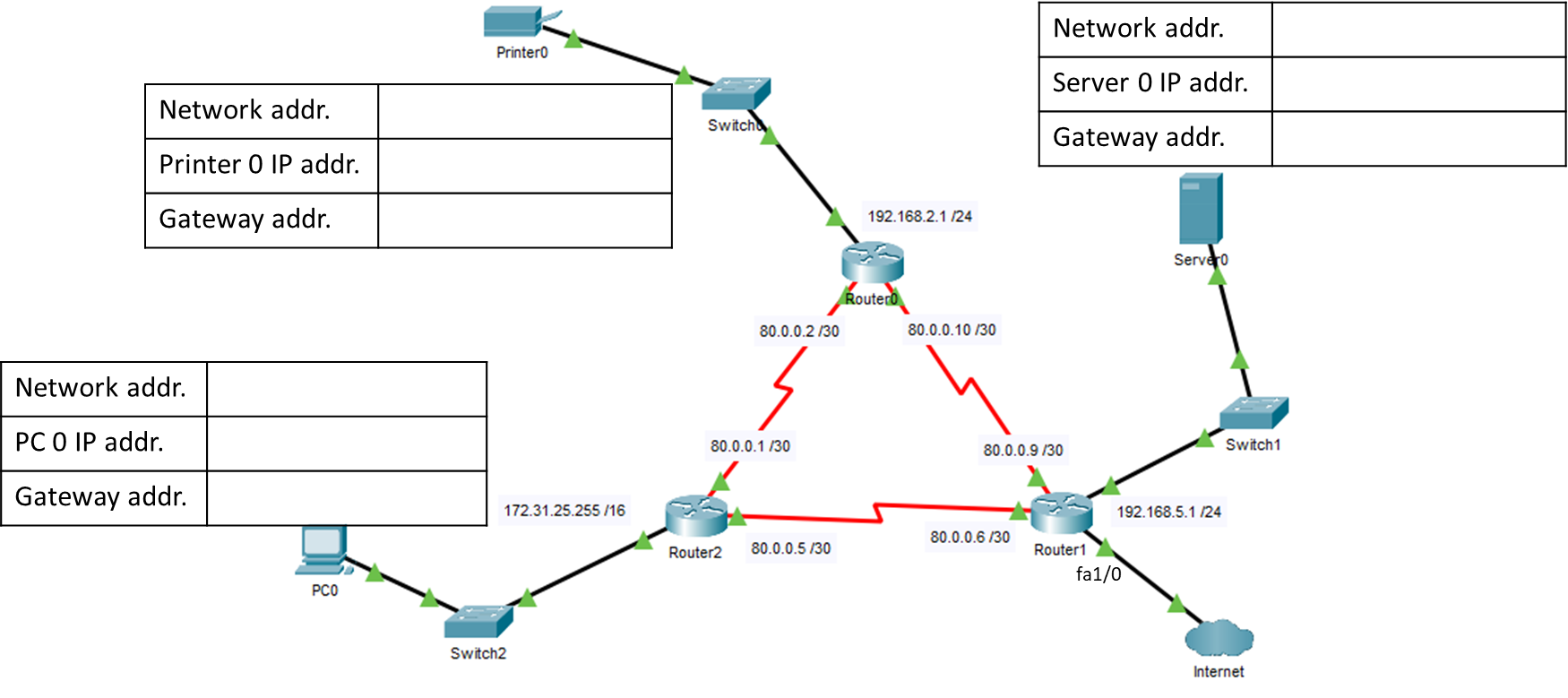
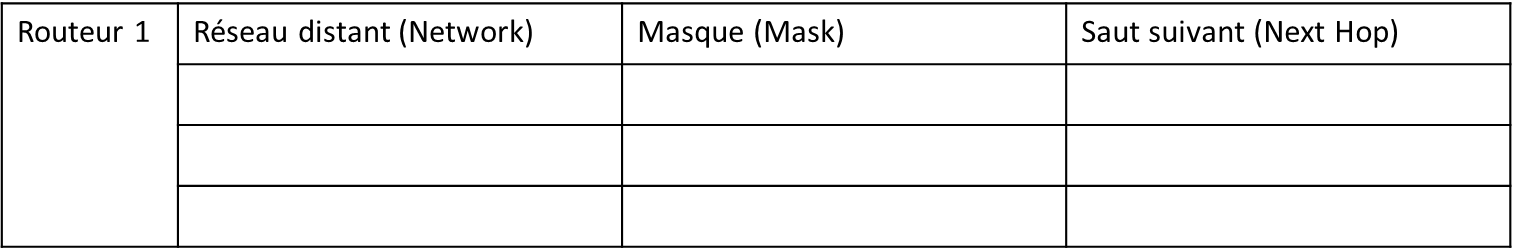
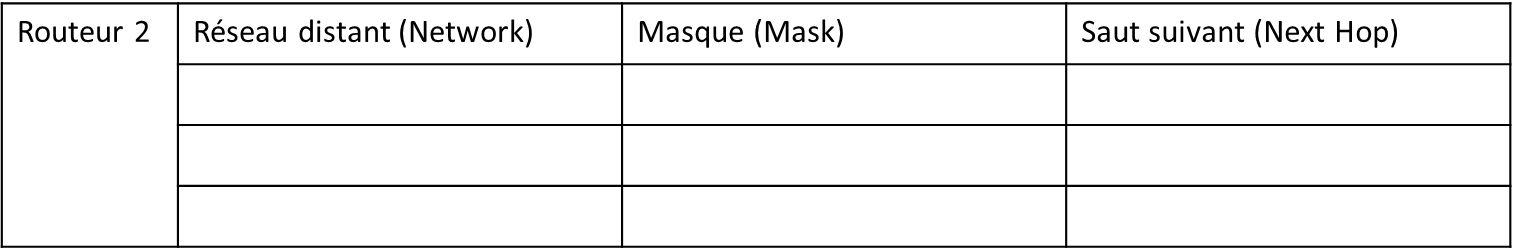
si le réseau est inconnu et qu’il n’existe pas de route le paquet est transféré à une interface. Sous Packet Tracer vous pouvez seulement configurer ce type de route en ligne de commande.

**Noter** un avantage et un inconvénient de cette méthode.

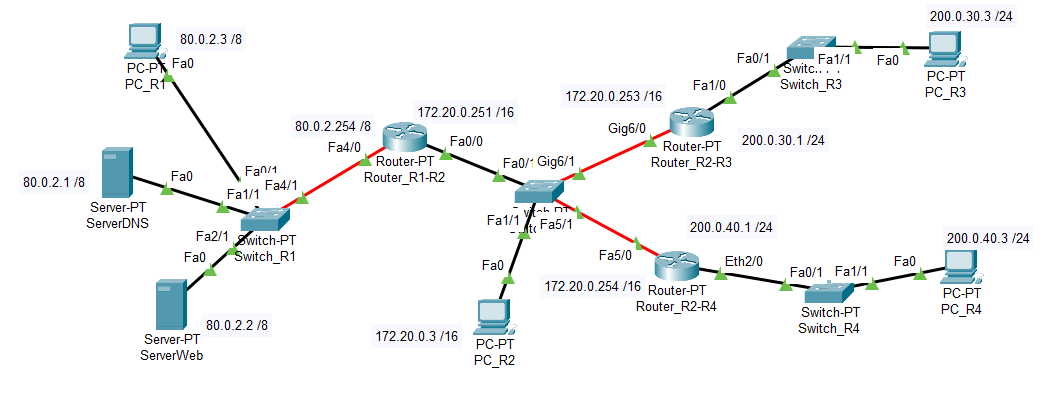
Depuis PC\_R3 ou PC\_R4 **accéder** à la page Web : edison.fr, observer les échanges en mode simulation.

# Bilan configuration d’un routeur

**Le fichier de simulation est :** **Bilan\_config\_routeur.pkt**



# Synthèse de la configuration d'un réseau PT (IP, Passerelles, Routeurs, Routes)

**Le fichier de simulation est :** **Synthese\_config\_routeur.pkt**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nom de l’équipement | Interface | Adresse réseau  / CIDR | Adresse machine IP | Passerelle |
| PC\_R1 | FastEthernet0 | 80.0.0.0 / 8 | 80.0.2.3 | 80.0.2.254 |
| ServerDNS | FastEthernet0 | 80.0.0.0 / 8 | 80.0.2.1 | 80.0.2.254 |
| ServerWeb | FastEthernet0 | 80.0.0.0 / 8 | 80.0.2.2 | 80.0.2.254 |
| Router\_R1-R2 | Fa4/0 | 80.0.0.0 / 8 | 80.0.2.254 |  |
| Router\_R1-R2 | Fa0/0 | 172.20.0.0 / 16 | 172.20.0.251 |  |
| Router\_R2-R3 | Gig6/0 | 172.20.0.0 / 16 | 172.20.0.253 |  |
| Router\_R2-R3 | Fa1/0 | 200.0.30.0 / 24 | 200.0.30.1 |  |
| Router\_R2-R4 | Fa5/0 | 172.20.0.0 / 16 | 172.20.0.254 |  |
| Router\_R2-R4 | Eth2/0 | 200.0.40.0 / 24 | 200.0.40.1 |  |
| PC\_R2 | FastEthernet0 | 172.20.0.0 / 16 | 172.20.0.3 | 172.20.0.251 |
| PC\_R3 | FastEthernet0 | 200.0.30.0 / 24 | 200.0.30.3 | 200.0.30.1 |
| PC\_R4 | FastEthernet0 | 200.0.40.0 / 24 | 200.0.40.3 | 200.0.40.1 |

**Commande pour configurer le routeur R1-R2**

Router\_R1-R2>enable

Router\_R1-R2#configure terminal

Router\_R1-R2(config)#interface fastEthernet 4/0

Router\_R1-R2(config-if)#ip address 80.0.2.254 255.0.0.0

Router\_R1-R2(config-if)#no shutdown

Router\_R1-R2(config-if)#exit

Router\_R1-R2(config)#interface fastEthernet 0/0

Router\_R1-R2(config-if)#ip address 172.20.0.251 255.0.0.0

Router\_R1-R2(config-if)#no shutdown

Router\_R1-R2(config-if)#exit

Router\_R1-R2(config)#exit

Router\_R1-R2#show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 172.20.0.251 YES manual up up

FastEthernet1/0 unassigned YES unset administratively down down

Serial2/0 unassigned YES unset administratively down down

Serial3/0 unassigned YES unset administratively down down

FastEthernet4/0 80.0.2.254 YES manual up up

FastEthernet5/0 unassigned YES unset administratively down down

Router\_R1-R2#configure terminal

Router\_R1-R2(config)#ip route 200.0.30.0 255.255.255.0 172.20.0.253

Router\_R1-R2(config)#ip route 200.0.40.0 255.255.255.0 172.20.0.254

Router\_R1-R2#exit

Router\_R1-R2#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

C 80.0.0.0/8 is directly connected, FastEthernet4/0

C 172.0.0.0/8 is directly connected, FastEthernet0/0

S 200.0.30.0/24 [1/0] via 172.20.0.253

S 200.0.40.0/24 [1/0] via 172.20.0.254

**Commande pour configurer le routeur R2-R3**

Router\_R2-R3>enable

Router\_R2-R3#configure terminal

Router\_R2-R3(config)#interface gigabitEthernet 6/0

Router\_R2-R3(config-if)#ip address 172.20.0.253 255.255.0.0

Router\_R2-R3(config-if)#no shutdown

Router\_R2-R3(config-if)#exit

Router\_R2-R3(config)#interface fastEthernet 1/0

Router\_R2-R3(config-if)#ip address 200.0.30.1 255.255.255.0

Router\_R2-R3(config-if)#no shutdown

Router\_R2-R3(config-if)#exit

Router\_R2-R3(config)#exit

Router\_R2-R3#show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 unassigned YES unset administratively down down

FastEthernet1/0 200.0.30.1 YES manual up up

Serial2/0 unassigned YES unset administratively down down

Serial3/0 unassigned YES unset administratively down down

FastEthernet4/0 unassigned YES unset administratively down down

FastEthernet5/0 unassigned YES unset administratively down down

GigabitEthernet6/0 172.20.0.253 YES manual up up

Router\_R2-R3#configure terminal

Router\_R2-R3(config)#ip route 80.0.0.0 255.0.0.0 172.20.0.251

Router\_R2-R3(config)#ip route 200.0.40.0 255.255.255.0 172.20.0.254

Router\_R2-R3(config)#ip route 0.0.0.0 0.0.0.0 172.20.0.251

Router\_R2-R3(config)#exit

Router\_R2-R3#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C 172.20.0.0/16 is directly connected, GigabitEthernet6/0

C 200.0.30.0/24 is directly connected, FastEthernet1/0

S 80.0.0.0/8 [1/0] via 172.20.0.251

S 200.0.40.0/24 [1/0] via 172.20.0.254

S\* 0.0.0.0/0 is directly connected, GigabitEthernet6/0

[1/0] via 172.20.0.251

**Commande pour configurer le routeur R2-R4**

Router\_R2-R4>enable

Router\_R2-R4#configure terminal

Router\_R2-R4(config)#interface fastEthernet 5/0

Router\_R2-R4(config-if)#ip address 172.20.0.254 255.255.0.0

Router\_R2-R4(config-if)#no shutdown

Router\_R2-R4(config-if)#exit

Router\_R2-R4(config)#interface Ethernet 2/0

Router\_R2-R4(config-if)#ip address 200.0.40.1 255.255.255.0

Router\_R2-R4(config-if)#no shutdown

Router\_R2-R4(config-if)#exit

Router\_R2-R4(config)#exit

Router\_R2-R4#show ip interface brief

Interface IP-Address OK? Method Status Protocol

FastEthernet0/0 unassigned YES unset administratively down down

FastEthernet1/0 unassigned YES unset administratively down down

Ethernet2/0 200.0.40.1 YES manual up up

Serial3/0 unassigned YES unset administratively down down

FastEthernet4/0 unassigned YES unset administratively down down

FastEthernet5/0 172.20.0.254 YES manual up up

Router\_R2-R4#configure terminal

Router\_R2-R4(config)#ip route 80.0.0.0 255.0.0.0 172.20.0.251

Router\_R2-R4(config)#ip route 200.0.30.0 255.255.255.0 172.20.0.253

Router\_R2-R4(config)#ip route 0.0.0.0 0.0.0.0 172.20.0.251

Router\_R2-R4(config)#exit

Router\_R2-R4#show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

\* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C 200.0.40.0/24 is directly connected, Ethernet2/0

C 172.20.0.0/16 is directly connected, FastEthernet5/0

S 200.0.30.0/24 [1/0] via 172.20.0.253

S 80.0.0.0/8 [1/0] via 172.20.0.251

S\* 0.0.0.0/0 is directly connected, FastEthernet5/0

[1/0] via 172.20.0.251

# Configuration d’un réseau avec des VLAN

## Quelques prérequis

Définissez l'acronyme VLAN.

* Virtual LAN

Quels sont les 3 types de VLAN ?

* **VLAN de niveau 1 : VLAN par port**
  + **Ce type de VLAN définit un réseau virtuel en fonction des ports de raccordement sur le commutateur**
* VLAN de niveau 2 : VLAN MAC
  + Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station
* VLAN de niveau 3 :
  + VLAN par sous-réseau : associe des sous-réseaux selon l'adresse IP source
  + VLAN par protocole : créer un réseau virtuel par type de protocole (par exemple TCP/IP, IPX, AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau

Les avantages du VLAN

* Le VLAN permet de définir un nouveau réseau au-dessus du réseau physique et à ce titre offre les avantages suivants :
* Plus de souplesse pour l'administration et les modifications du réseau car toute l'architecture peut être modifiée par simple paramétrage des commutateurs
* Gain en sécurité car les informations sont encapsulées dans un niveau supplémentaire et éventuellement analysées
* Réduction de la diffusion du trafic sur le réseau

Norme VLAN

* IEEE 802.1Q

## Type of VLAN routing

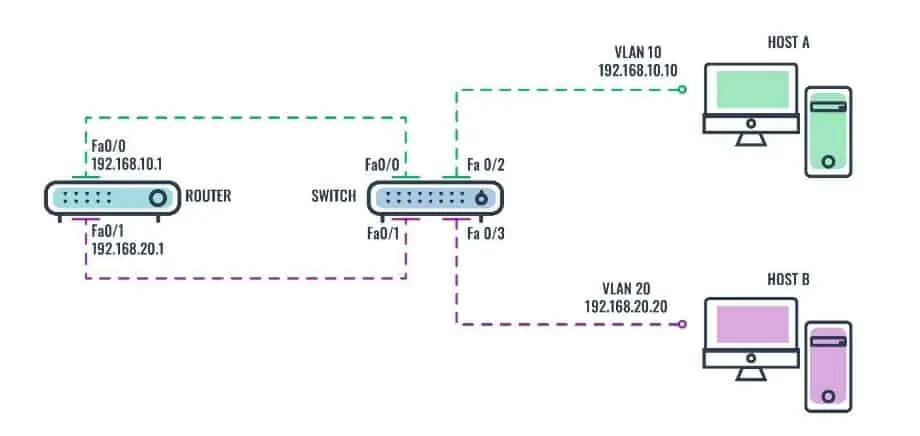
#### Traditional Inter-VLAN Routing

This method of inter-VLAN routing relies on a router with multiple physical interfaces.

Each interface is usually connected to the switch, one for each VLAN.

The switch ports connected to the router are placed in access mode and each router interface can then accept traffic from the VLAN associated with the switch interface that it is connected to, and traffic can be routed to the other VLANs connected to the other interfaces.

This means that each of the routers’ interface IP addresses would then become the default gateway address for each host in each VLAN.



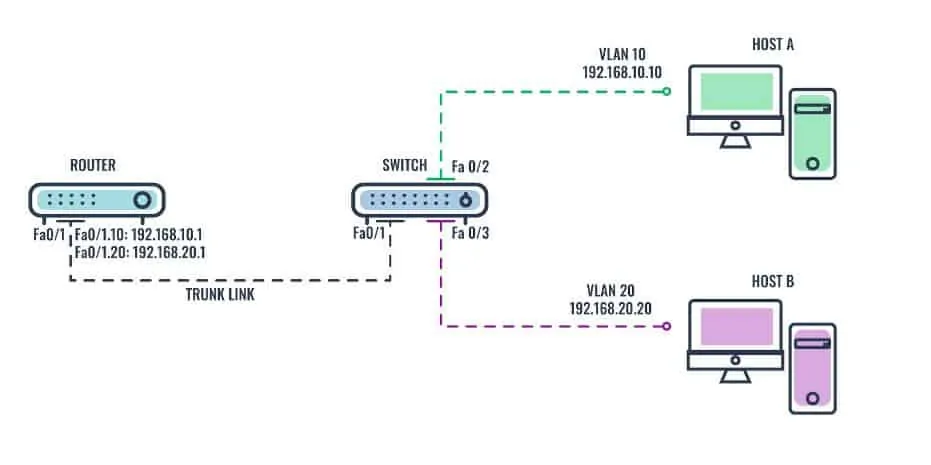
#### Router-on-a-Stick Inter-VLAN Routing

A router-on-a-stick is a method of inter-VLAN routing in which the router is connected to the switch using a single physical interface, hence the name router-on-a-stick.

Most modern inter-VLAN routing implementations are designed using this method. Unlike the traditional inter-VLAN routing method, router-on-stick does not require multiple physical interfaces on both the router and the switch.

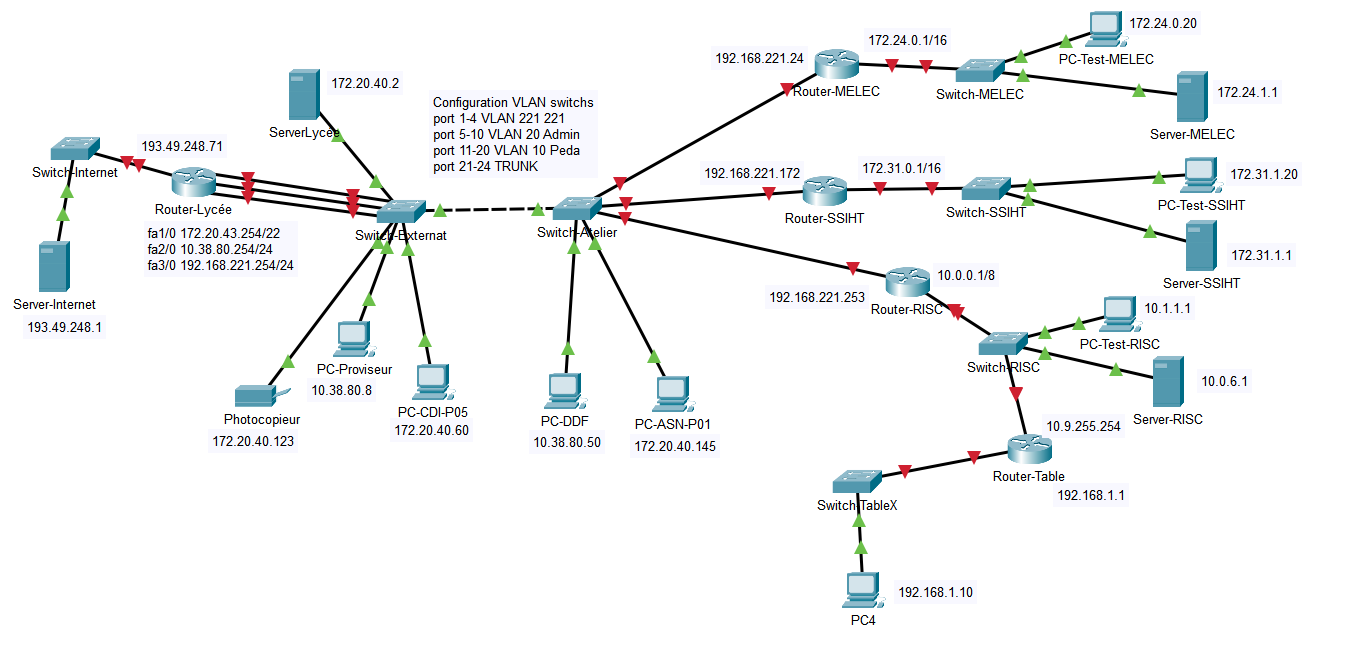
Instead, the router’s operating system makes it possible to configure the router interface to operate as a trunk link, which is then connected to a switch port that is configured in trunk mode.

This implies that only one physical interface is required on the router and the switch to route packets between multiple VLANs. IEEE 802.1Q (Dot1q) protocol—which defines a system of VLAN tagging for Ethernet frames, is used to provide multi-vendor VLAN support.



## Plan réseau

#### Traditional routing



**Ouvrir** le fichier vlan - routeur traditional - todo.pkt

**Compléter** le tableau “Table des équipements” avec les informations dont vous disposez dans la simulation (toutes les informations ne sont pas encore configurées).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nom de l’équipement | Interface | Adresse IP | Masque de sous réseau | Adresse réseau | Passerelle |
| Photocopieur | FastEthernet0 | 172.20.40.123 | 255.255.252.0 | 172.20.40.0 | 172.20.43.254 |
| PC-DDF | FastEthernet0 | 10.38.80.8 | /24 | 10.38.80.0 | 10.38.80.254 |
| Router-MELEC | FastEthernet0/0 | 192.168.221.24 | /24 | 192.168.221.254 |  |
| Router-MELEC | FastEthernet1/0 | 172.24.0.1 | /16 | 172.24.0.0 |  |
| Serveur-MELEC | FastEthernet0 | 172.24.1.1 | /16 | 172.24.0.0 | 172.24.0.1 |
| Serveur-SSIHT | FastEthernet0 | 172.31.1.1 | /16 | 172.31.0.0 | 172.31.0.1 |
| Serveur-RISC | FastEthernet0 | 10.0.6.1 | /8 | 10.0.0.0 | 10.0.0.1 |
| PC4 | FastEthernet0 | 192.168.1.10 | /24 | 192.168.1.0 | 192.168.1.1 |

**Configuration des routes**

**Compléter** le tableau table de routage nécessaire pour ce réseau.

|  |  |  |  |
| --- | --- | --- | --- |
| Routeur : Router-Lycée | Network (destination) | Masque | Next Hop |
|  | 172.24.0.0 | 255.255.0.0 | 192.168.221.24 |
|  | 172.31.0.0 | 255.255.0.0 | 192.168.221.172 |
|  | 10.0.0.0 | 255.0.0.0 | 192.168.221.253 |
| Routeur : Router-RISC | Network (destination) | Masque | Next Hop |
|  | 0.0.0.0 | 0.0.0.0 | 192.168.221.254 |
| Routeur : Router-SSIHT | Network (destination) | Masque | Next Hop |
|  | 0.0.0.0 | 0.0.0.0 | 192.168.221.254 |
| Routeur : Router-MELEC | Network (destination) | Masque | Next Hop |
|  | 0.0.0.0 | 0.0.0.0 | 192.168.221.254 |

## Configuration des routeurs

Paramétrer les équipements réseaux en suivant les commandes IOS Cisco.

### Configuration Routeur-Lycee

enable

configure terminal

hostname Routeur-Lycee

interface FastEthernet0/0

ip address 193.49.248.71 255.255.255.0

no shutdown

exit

interface FastEthernet1/0

ip address 172.20.43.254 255.255.252.0

no shutdown

exit

interface FastEthernet2/0

ip address 10.38.80.254 255.255.255.0

no shutdown

exit

interface FastEthernet3/0

ip address 192.168.221.254 255.255.255.0

no shutdown

exit

ip route 10.0.0.0 255.0.0.0 192.168.221.253

ip route 172.31.0.0 255.255.0.0 192.168.221.172

ip route 172.24.0.0 255.255.0.0 192.168.221.24

exit

### Configuration Routeur-MELEC

enable

configure terminal

hostname Routeur-MELEC

interface FastEthernet0/0

ip address 192.168.221.24 255.255.255.0

no shutdown

exit

interface FastEthernet1/0

ip address 172.24.0.1 255.255.0.0

no shutdown

exit

ip route 0.0.0.0 0.0.0.0 192.168.221.254

exit

### Configuration Routeur-RISC

enable

configure terminal

hostname Routeur-RISC

interface FastEthernet0/0

ip address 192.168.221.253 255.255.255.0

no shutdown

exit

interface FastEthernet1/0

ip address 10.0.0.1 255.0.0.0

no shutdown

exit

ip route 0.0.0.0 0.0.0.0 192.168.221.254

exit

### Configuration Routeur-SSIHT

enable

configure terminal

hostname Routeur-SSIHT

interface FastEthernet0/0

ip address 192.168.221.172 255.255.255.0

no shutdown

exit

interface FastEthernet1/0

ip address 172.31.0.1 255.255.0.0

no shutdown

exit

ip route 0.0.0.0 0.0.0.0 192.168.221.254

exit

## Configuration des switches (configuration des VLAN)

Paramétrer les équipements réseaux en suivant les commandes IOS Cisco.

### Configuration Switch-Externat

enable

configure terminal

hostname Switch-Externat

vlan 10

name Admin

exit

vlan 20

name Peda

exit

vlan 221

name 221

exit

interface range FastEthernet0/1-4

switchport access vlan 221

switchport mode access

exit

interface range FastEthernet0/5-10

switchport access vlan 10

switchport mode access

exit

interface range FastEthernet0/11-20

switchport access vlan 20

switchport mode access

exit

interface range FastEthernet0/21-24

switchport mode trunk

switchport trunk allowed vlan 10

switchport trunk allowed vlan add 20

switchport trunk allowed vlan add 221

exit

### Configuration Switch-Atelier

enable

configure terminal

hostname Switch-Atelier

vlan 10

name Admin

exit

vlan 20

name Peda

exit

vlan 221

name 221

exit

interface range FastEthernet0/1-4

switchport access vlan 221

switchport mode access

exit

interface range FastEthernet0/5-10

switchport access vlan 10

switchport mode access

exit

interface range FastEthernet0/11-20

switchport access vlan 20

switchport mode access

exit

interface range FastEthernet0/21-24

switchport mode trunk

switchport trunk allowed vlan 10

switchport trunk allowed vlan add 20

switchport trunk allowed vlan add 221

exit

**Test du réseau Lycée**

|  |  |
| --- | --- |
| Tester la connexion entre : | OK / NOK |
| PC-DDF et PC-CDI-P05 |  |
| PC-DDF et Server-MELEC |  |
| PC-DDF et Server-RISC |  |
| PC-DDF et Server-SSIHT |  |
| PC-DDF et Server-Lycée |  |

## Configuration du réseau « Table »

**Compléter** la configuration de Router-Table.

|  |  |
| --- | --- |
| Instructions | Commandes IOS Cisco |
| Passer en mode administrateur | enable |
| Passer en mode configuration globale | configure terminal |
| Renommer le routeur « Routeur-Table » | hostname Routeur-Table |
| Configurer l’interface FastEthernet0/0 | interface FastEthernet0/0  ip address 10.9.255.254 255.0.0.0  no shutdown |
| Configurer l’interface FastEthernet1/0 | interface FastEthernet1/0  ip address 192.168.1.1 255.255.255.0  no shutdown |
| Configurer la route par défaut | ip route 0.0.0.0 0.0.0.0 10.0.0.1 |

Ce réseau comportera 3 VLANs :

* VLAN 4 :
  + Nom : CamIP
  + Ports switch « Switch-Table » : 6-10
* VLAN 16 :
  + Nom : TelIP
  + Ports switch « Switch-Table » : 11-15
* VLAN 55 :
  + Nom : PC
  + Ports switch « Switch-Table » : 16-24
* Trunk :
  + Ports switch « Switch-Table » : 1-5
  + VLAN autorisés : 16 et 55

**Compléter** la configuration de Switch-Table.

|  |  |
| --- | --- |
| Instructions | Commandes IOS Cisco |
| Passer en mode administrateur | enable |
| Passer en mode configuration globale | configure terminal |
| Renommer le routeur « Switch-Table » | hostname Switch-Table |
| Créer et nommer le VLAN 4 | vlan 4  name CAMIP  exit |
| Créer et nommer le VLAN 16 | vlan 16  name TELIP  exit |
| Créer et nommer le VLAN 55 | vlan 55  name PC  exit |
| Configurer les interfaces du VLAN 4 | interface range FastEthernet0/6-10  switchport access vlan 4  switchport mode access  exit |
| Configurer les interfaces du VLAN 16 | interface range FastEthernet0/11-15  switchport access vlan 55  switchport mode access  exit |
| Configurer les interfaces du VLAN 55 | interface range FastEthernet0/16-24  switchport access vlan 20  switchport mode access  exit |
| Configurer les interfaces du TRUNK | interface range FastEthernet0/1-5  switchport mode trunk  switchport trunk allowed vlan 16  switchport trunk allowed vlan add 55  exit |

## Plan réseau

#### Routing on a stick

**Ouvrir** le fichier vlan - routeur on a stick - todo.pkt



## Configuration des routeurs

Paramétrer les équipements réseaux en suivant les commandes IOS Cisco.

### Configuration Routeur-Lycee

enable

configure terminal

hostname Routeur-Lycee

interface FastEthernet0/0

ip address 193.49.248.71 255.255.255.0

no shutdown

exit

interface FastEthernet1/0

no shutdown

interface FastEthernet1/0.20

ip address 172.20.43.254 255.255.252.0

encapsulation dot1Q 20

exit

interface FastEthernet1/0.10

ip address 10.38.80.254 255.255.255.0

encapsulation dot1Q 10

exit

interface FastEthernet1/0.221

ip address 192.168.221.254 255.255.255.0

encapsulation dot1Q 221

exit

ip route 10.0.0.0 255.0.0.0 192.168.221.253

ip route 172.31.0.0 255.255.0.0 192.168.221.172

ip route 172.24.0.0 255.255.0.0 192.168.221.24

exit

### Configuration Routeur-MELEC

Même configuration que précédemment

### Configuration Routeur-RISC

Même configuration que précédemment

### Configuration Routeur-SSIHT

Même configuration que précédemment

## Configuration des switches (configuration des VLAN)

### Configuration Switch-Externat

Même configuration que précédemment

### Configuration Switch-Atelier

Même configuration que précédemment

## Configuration du routeur et switch : Table

### Configuration Routeur Table

**Compléter** la configuration de Routeur-Table.

|  |  |
| --- | --- |
| Instructions | Commandes IOS Cisco |
| Passer en mode administrateur | enable |
| Passer en mode configuration globale | configure terminal |
| Renommer le routeur « Routeur-Table » | hostname Routeur-Table |
| Configurer l’interface FastEthernet0/0 | interface FastEthernet0/0  ip address 10.9.255.254 255.0.0.0  no shutdown |
| Configurer la sous interface FastEthernet1/0.4 du VLAN 4  172.9.4.254 | interface FastEthernet1/0  no shutdown  interface FastEthernet1/0.4  ip address 172.9.4.254 255.255.255.0  encapsulation dot1Q 4  exit |
| Configurer la sous interface FastEthernet1/0.16 du VLAN 16  172.9.16.254 | interface FastEthernet1/0.16  ip address 172.9.16.254 255.255.255.0  encapsulation dot1Q 16  exit |
| Configurer la sous interface FastEthernet1/0.55 du VLAN 55  172.9.55.254 | interface FastEthernet1/0.55  ip address 172.9.55.254 255.255.255.0  encapsulation dot1Q 55  exit |
| Configurer la route par défaut sortante | ip route 0.0.0.0 0.0.0.0 10.0.0.1  exit |

### Configuration Switch-Table

Même configuration que précédemment

Quelle route doit-on paramétrer dans le routeur RISC, pour que votre réseau communique avec l’extérieur ?

|  |
| --- |
| ip route 172.9.0.0 255.255.0.0 10.9.255.254 |

Observer la configuration des VLAN dans le switch NETGEAR, en accédant à sa page web : 10.0.9.x (# numéro de table)

* login : admin // mdp : Edison38130

# Révision d’un réseau avec des VLAN

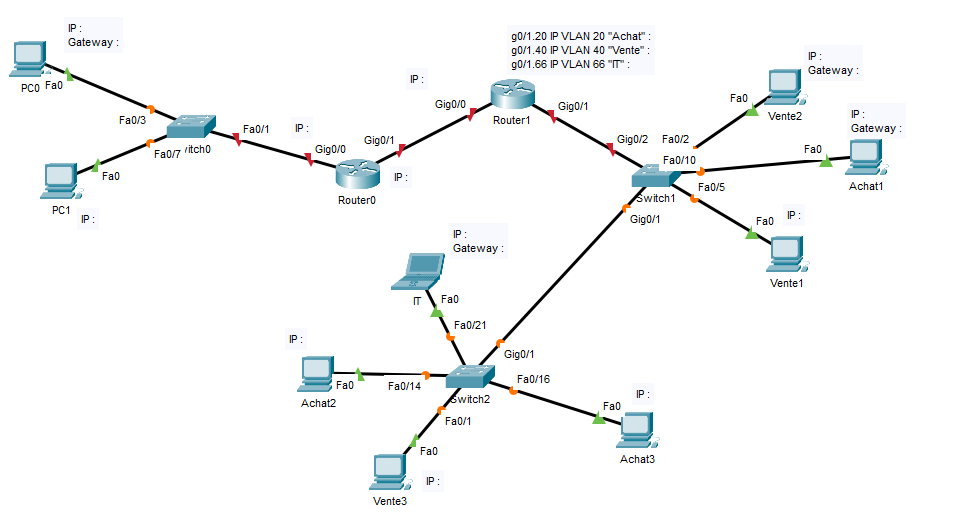
## Plan réseau

**Adressage réseau**

Réseau noir (PC0/PC1) : 192.168.1.0 / 24

Réseau inter-routeur : 192.168.221.0 /30

Réseau VLAN 20 « Achat » : 172.20.20.0 /21

Réseau VLAN 40 « Vente » : 172.40.40.0 /21

Réseau VLAN 66 « IT » : 192.168.66.0 /28

**Ouvrir** le fichier vlan - revision - todo.pka

**Pour les 5 réseaux trouver :**

* **1ère adresse attribuable**
* **Dernière adresse attribuable**
* **Adresse de broadcast**
* **Nombre de machines possible sur le réseau**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

**Attribuer des adresses IP aux éléments du réseau**

**Configurer les routes sur le routeur 0 et routeur 1**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nom** | **Routeur** | **Network (destination)** | **Mask** | **Passerelle – Next Hop** |
| Réseau noir vers Achat | 0 |  |  |  |
| Réseau noir vers Vente | 0 |  |  |  |
| Réseau noir vers IT | 0 |  |  |  |
| Réseau any vers noir | 1 |  |  |  |

**Ou avec route par default**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nom** | **Routeur** | **Network** | **Mask** | **Passerelle** |
| Réseau noir vers any | 0 |  |  |  |
| Réseau any vers any | 1 |  |  |  |

**Any = « n’importe lequel »**

**Configuration VLAN**

VLAN 20 « Achat » :

* Ports des switches : fa0/10 à fa0/19

VLAN 40 « Vente » :

* Ports des switches : fa0/0 à fa0/9

VLAN 66 « IT » : 192.168.66.0 /28

* Ports des switches : fa0/21 à fa0/24

Trunk :

* Ports des switches : g0/1
* Autoriser les VLANs 20 et 66 mais pas 40

**Paramétrer les équipements réseaux en suivant les commandes IOS Cisco.**

# VLSM

## FLSM

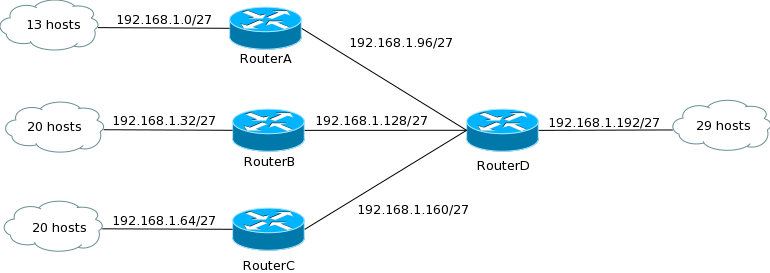
En FLSM (Fixed Length Subnet Mask), le découpage du réseau a été fait de manière fixe, c’est-à-dire que tous les sous-réseaux peuvent contenir le même nombre d’hôtes.

Or deux réseaux peuvent parfaitement avoir deux besoins radicalement différents à ce niveau. Un premier réseau peut avoir besoin d’héberger 120 hôtes tandis qu’un deuxième seulement… 2 (dans le cas d’un réseau point à point par exemple).

Un réseau trop grand par rapport au nombre d’hôtes qu’il doit héberger provoque une perte d’adresses car ces adresses ne peuvent pas être réattribuées en dehors de leurs subnets respectifs.

Bien sûr cela n’est pas critique lorsqu’il est question d’adressage privé car ces adresses sont gratuites et, au pire, l’organisation du réseau sera moins pratique. En revanche lorsqu’il s’agit d’adresses publiques, l’heure n’est plus au gaspillage d’une part car l’entreprise (ou le fournisseur d’accès Internet) paie ces adresses et d’autre part car il devient très difficile aujourd’hui d’en obtenir à cause de la pénurie d’adresses.

#### Exemple :



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sous-réseau | Adresse IP sous-réseau | Première IP utilisable | Dernière IP utilisable | Adresse de diffusion |
| 1 | 192.168.1.0 | 192.168.1.1 | 192.168.1.30 | 192.168.1.31 |
| 2 | 192.168.1.32 | 192.168.1. | 192.168.1. | 192.168.1.63 |
| 3 | 192.168.1.64 | 192.168.1. | 192.168.1. | 192.168.1.95 |
| 4 | 192.168.1.96 | 192.168.1. | 192.168.1. | 192.168.1.127 |
| 5 | 192.168.1.128 | 192.168.1. | 192.168.1. | 192.168.1.159 |
| 6 | 192.168.1.160 | 192.168.1. | 192.168.1. | 192.168.1.191 |
| 7 | 192.168.1.192 | 192.168.1.193 | 192.168.1.222 | 192.168.1.223 |

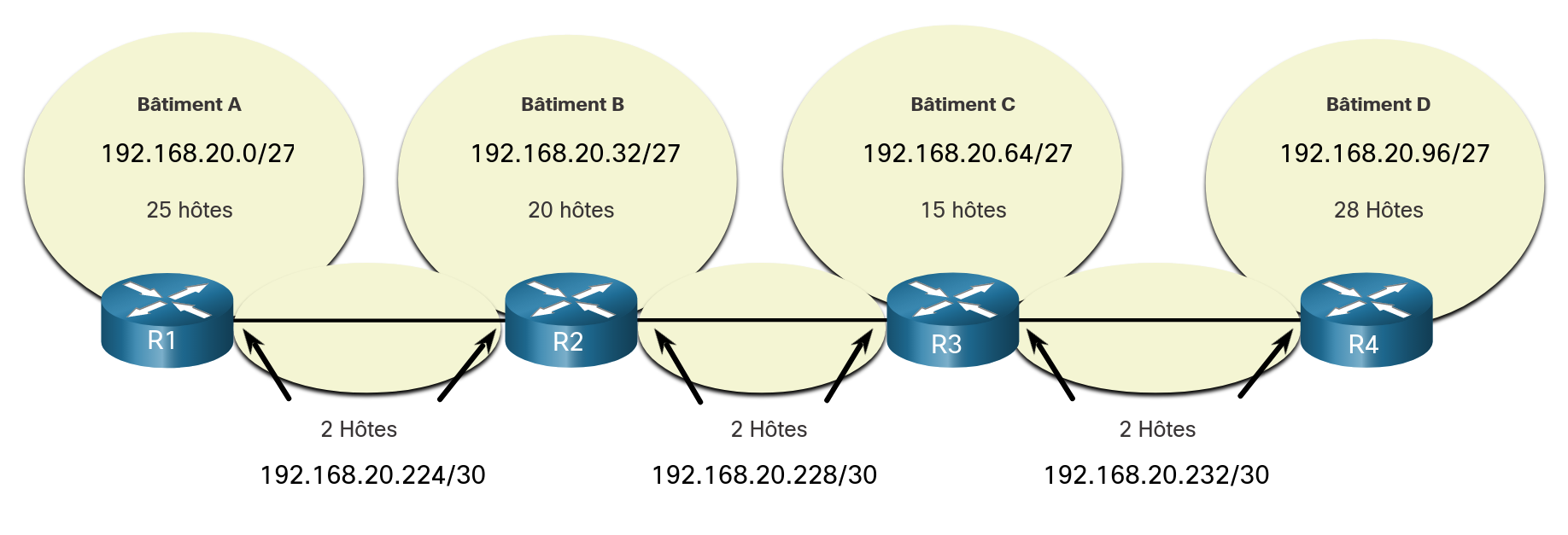
## VLSM

VLSM (Variable Length Subnet Mask) est un masque de sous-réseau à longueur variable.

La technique VLSM est une simple extension du découpage en sous-réseaux de base, où une même adresse de classe A, B ou C est découpée en sous-réseaux à l'aide de masques de longueurs différentes. La VLSM permet d'optimiser l'attribution des adresses IP et offre davantage de souplesse dans l'affectation du nombre adéquat d'hôtes et de sous-réseaux, à partir d'un nombre limité d'adresses IP.

La technique VLSM permet à une entreprise d’utiliser plusieurs sous-masques dans le même espace d'adressage réseau. La mise en œuvre de VLSM est souvent appelée « subdivision d’un sous-réseau en sous-réseaux » et peut être utilisée pour améliorer l’efficacité de l’adressage.

#### Exemple : Réseau donné en 192.168.20.0/24



|  |  |  |  |
| --- | --- | --- | --- |
| Sous-réseau | Adresse IP sous-réseau | Adresse de diffusion | Nombre d’hôtes max |
| 1 | 192.168.20.0 /27 | 192.168.20.31 | 30 |
| 2 | 192.168.20.32 /27 | 192.168.20.63 | 30 |
| 3 | 192.168.20.64 /27 | 192.168.20.95 | 30 |
| 4 | 192.168.20.96 /28 | 192.168.20.111 | 16 |
| 5 | 192.168.20.112 /30 | 192.168.20.115 | 2 |
| 6 | 192.168.20.116 /30 | 192.168.20.119 | 2 |
| 7 | 192.168.20.120 /30 | 192.168.20.123 | 2 |

#### Application 1

|  |  |  |  |
| --- | --- | --- | --- |
| Sous-réseau | Adresse IP sous-réseau | Adresse de diffusion | Nombre d’hôtes max |
| 1 | 172.16.32.0 /26 | 172.16.32.63 | 62 |
| 2 | 172.16.32.64 /26 | 172.16.32.127 | 62 |
| 3 | 172.16.32.128 /26 | 172.16.32.191 | 62 |
| 4 | 172.16.32.192 /30 | 172.16.32.195 | 2 |
| 5 | 172.16.32.196 /30 | 172.16.32.199 | 2 |
| 6 | 172.16.32.200 /30 | 172.16.32.203 | 2 |

#### 

#### Application 2 : Réseau donné en 192.168.1.0/24

|  |  |  |  |
| --- | --- | --- | --- |
| Sous-réseau | Adresse IP sous-réseau | Adresse de diffusion | Nombre d’hôtes max |
|  | 192.168.1.0 /26 | 192.168.1.63 | 62 |
|  | 192.168.1.64 /27 | 192.168.1.95 | 30 |
|  | 192.168.1.96 /28 | 192.168.1.111 | 14 |
|  | 192.168.1.112 /28 | 192.168.1.127 | 14 |
|  | 192.168.1.128 /30 | 192.168.1.131 | 2 |
|  | 192.168.1.132 /30 | 192.168.1.135 | 2 |
|  | 192.168.1.136 /30 | 192.168.1.139 | 2 |
|  | 192.168.1.140 /30 | 192.168.1.143 | 2 |

1. Quelle est la notation de longueur du préfixe pour le masque de sous-réseau 255.255.255.224 ?

/27

1. Combien d'adresses d'hôte valides sont disponibles sur un sous-réseau IPv4 configuré avec un masque /26 ?

62

1. Quel masque de sous-réseau serait utilisé si 5 bits d'hôte étaient disponibles ?

255.255.255.224 = /27

1. Un administrateur réseau segmente le réseau 192.168.10.0/24 en sous-réseaux avec des masques /26. Combien de sous-réseaux de taille égale seront créés ?

4

1. Quel masque de sous-réseau est représenté par la notation /20 ?

255.255.240.0

1. Combien d'adresses IP utilisables sont disponibles sur le réseau 192.168.1.0/27 ?

30

1. Quel masque de sous-réseau serait utilisé si 4 bits d'hôte étaient disponibles ?

255.255.255.240 = /28

1. Quelles sont les deux parties des composants d'une adresse IPv4 ?

Réseau / Hôte

1. Si un périphérique réseau a le masque /26, combien d'adresses IP sont disponibles pour les hôtes de ce réseau ?

62

1. Que représente l'adresse IP 172.17.4.250/24 ?

Une adresse unicast

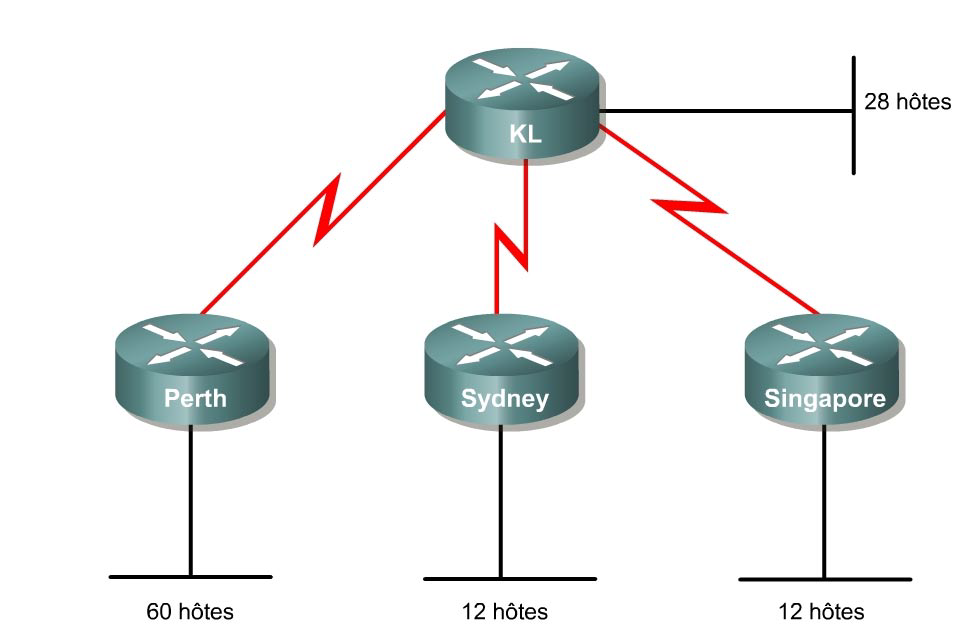
1. Si un périphérique réseau a le masque /28, combien d'adresses IP sont disponibles pour les hôtes de ce réseau ?

14

1. Un administrateur réseau crée des sous-réseaux de façon variable sur un réseau. Le plus petit sous-réseau dispose d'un masque de 255.255.255.248. Combien d'adresses d'hôte utilisables ce sous-réseau prendra-t-il en charge ?

6

## Exercice 1



**Objectif**

Utiliser la technique VLSM (Variable-Length Subnet Mask) pour gérer plus efficacement l’attribution des adresses IP et réduire la quantité d’informations de routage au niveau supérieur.

L’adresse de classe C 192.168.10.0/24 a été attribuée.

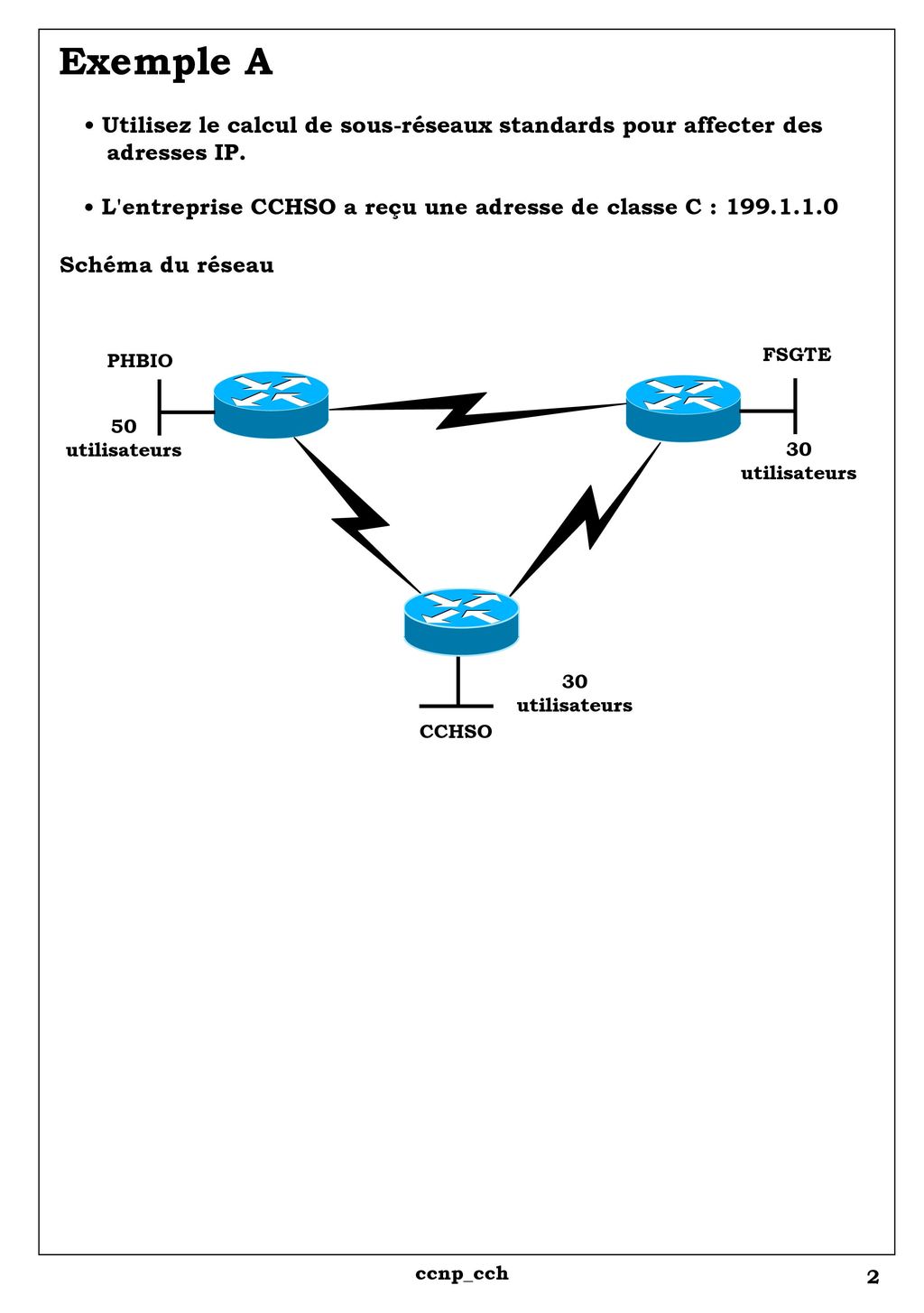
Perth, Sydney et Singapore sont reliés par une connexion WAN à Kuala Lumpur.

• Perth a besoin d’une capacité de 60 hôtes.

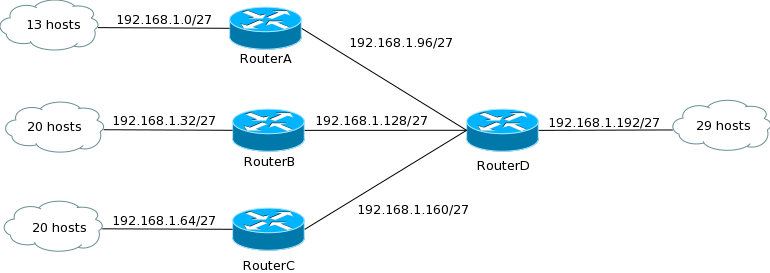
• Kuala Lumpur a besoin d’une capacité de 28 hôtes.

• Sydney et Singapore ont chacun besoin d’une capacité de 12 hôtes.

## Exercice 2

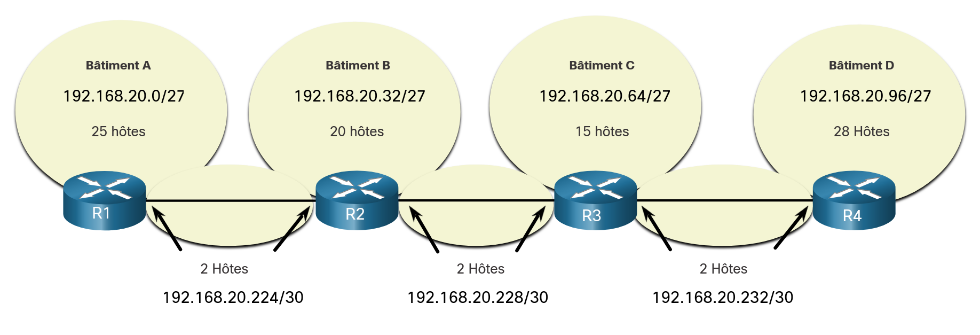


# Synthèse VLSM

**FLSM** (Fixed Length Subnet Mask), le découpage du réseau a été fait de manière fixe, c’est-à-dire que tous les sous-réseaux peuvent contenir le même nombre d’hôtes.

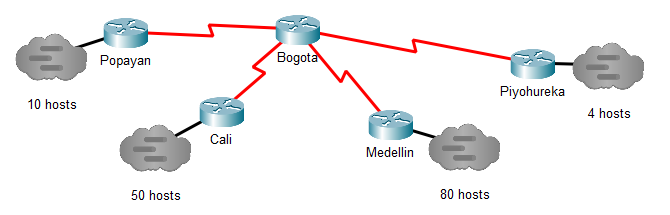
#### Exemple :

|  |  |  |  |
| --- | --- | --- | --- |
| Sous-réseau | Adresse IP sous-réseau | Adresse de diffusion | Nombre d’hôtes max |
| 1 | 192.168.1.0 | 192.168.1.31 | 30 |
| 2 | 192.168.1.32 | 192.168.1.63 | 30 |
| 3 | 192.168.1.64 | 192.168.1.95 | 30 |
| 4 | 192.168.1.96 | 192.168.1.127 | 30 |
| 5 | 192.168.1.128 | 192.168.1.159 | 30 |
| 6 | 192.168.1.160 | 192.168.1.191 | 30 |
| 7 | 192.168.1.192 | 192.168.1.223 | 30 |

**VLSM** (Variable Length Subnet Mask) est un masque de sous-réseau à longueur variable. La mise en œuvre de VLSM est souvent appelée « subdivision d’un sous-réseau en sous-réseaux » et peut être utilisée pour améliorer l’efficacité de l’adressage.

#### Exemple : Réseau donné en 192.168.20.0/24

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Sous-réseau | Adresse IP sous-réseau | | Adresse de diffusion | | | Nombre d’hôtes max | |
| 1 | 192.168.20.0 /27 | | 192.168.20.31 | | | 30 | |
| 2 | 192.168.20.32 /27 | | 192.168.20.63 | | | 30 | |
| 3 | 192.168.20.64 /27 | | 192.168.20.95 | | | 30 | |
| 4 | 192.168.20.96 /28 | | 192.168.20.111 | | | 16 | |
| 5 | 192.168.20.112 /30 | | 192.168.20.115 | | | 2 | |
| 6 | 192.168.20.116 /30 | | 192.168.20.119 | | | 2 | |
| 7 | 192.168.20.120 /30 | | 192.168.20.123 | | | 2 | |
| Longueur du préfixe  CIDR  Nbr de bit réseau | | Nombre d’hôtes max | | Masque de sous réseau | Masque inversé de sous réseau | | Préfixe | |
| /16 | | 65534 | | 255.255.0.0 | 0.0.255.255 | | /16 | |
| /17 | | 32766 | | 255.255.128.0 | 0.0.127.255 | | /17 | |
| /18 | | 16382 | | 255.255.192.0 | 0.0.0.63.255 | | /18 | |
| /19 | | 8190 | | 255.255.224.0 | 0.0.31.255 | | /19 | |
| /20 | | 4094 | | 255.255.240.0 | 0.0.15.255 | | /20 | |
| /21 | | 2046 | | 255.255.248.0 | 0.0.7.255 | | /21 | |
| /22 | | 1022 | | 255.255.252.0 | 0.0.3.255 | | /22 | |
| /23 | | 510 | | 255.255.254.0 | 0.0.1.255 | | /23 | |
| /24 | | 254 | | 255.255.255.0 | 0.0.0.255 | | /24 | |
| /25 | | 126 | | 255.255.255.128 | 0.0.0.127 | | /25 | |
| /26 | | 62 | | 255.255.255.192 | 0.0.0.63 | | /26 | |
| /27 | | 30 | | 255.255.255.224 | 0.0.0.31 | | /27 | |
| /28 | | 14 | | 255.255.255.240 | 0.0.0.15 | | /28 | |
| /29 | | 6 | | 255.255.255.248 | 0.0.0.7 | | /29 | |
| /30 | | 2 | | 255.255.255.252 | 0.0.0.3 | | /30 | |



Nous avons un réseau : 89.5.2.0/24

bogota.pkt

|  |  |  |  |
| --- | --- | --- | --- |
| Sous-réseau | Nom du réseau | Adresse IP sous-réseau | Adresse de diffusion |
| 1 | Medelin | 89.5.2.0 /25 | 89.5.2.127 |
| 2 | Cali | 89.5.2.128 /26 | 89.5.2.191 |
| 3 | Popayan | 89.5.2.192 /28 | 89.5.2.207 |
| 4 | Piyohureka | 89.5.2.208 /29 | 89.5.2.215 |
| 5 | Bogota-Popayan | 89.5.2.216 /30 | 89.5.2.219 |
| 6 | Bogota-Cali | 89.5.2.220 /30 | 89.5.2.223 |
| 7 | Bogota-Medelin | 89.5.2.224 /30 | 89.5.2.227 |
| 8 | Bogota-Piyohureka | 89.5.2.228 /30 | 89.5.2.231 |

# ACL : Access Control List

Access Control List (ACL) ou liste de contrôle d'accès désigne deux choses en sécurité informatique :

* un système permettant de faire une gestion fine des droits d'accès aux fichiers.
* en réseau, une liste des adresses et ports autorisés ou interdits par un pare-feu.

|  |
| --- |
| ACL |
| ACE 1 |
| ACE 2 |
| … |

La notion d'ACL est cela dit assez généraliste, et on peut parler d'ACL pour gérer les accès à n'importe quel type de ressource.

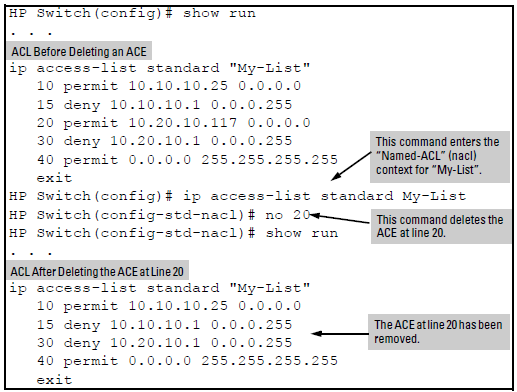
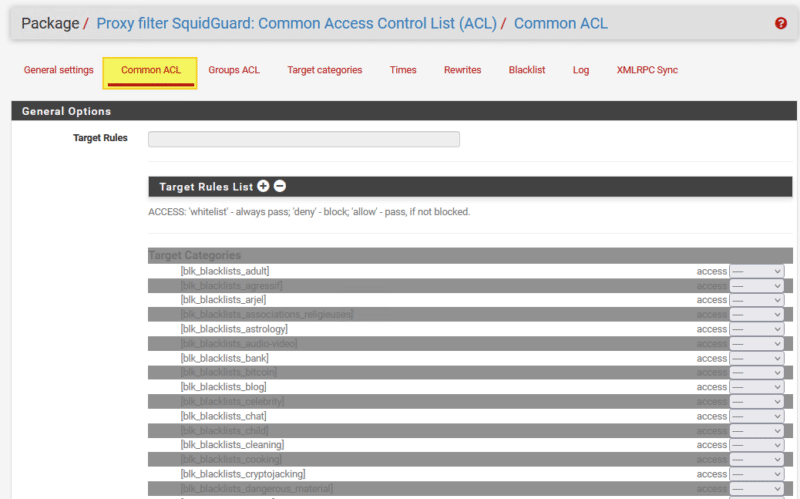
Une ACL est une liste d’Access Control Entry (ACE) ou entrée de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe.

## ACL sur les fichiers :

* OS UNIX : Les ACL donnent à n'importe quel utilisateur, ou groupe, un des trois droits (lecture, écriture et exécution) et cela sans limitation du nombre d'utilisateurs à ajouter.
* OS Windows : les ACL peuvent être définis sur des fichiers ou des répertoires et acceptent les types de droits suivants :
  + parcours d'un dossier ;
  + liste d'un dossier ;
  + lecture des méta-données ;
  + ajout de fichier ;
  + ajout de répertoire ;
  + ajout de données à un fichier existant ;
  + modification des droits ;
  + suppression ;
  + lecture ;
  + appropriation ;
  + exécution.

## ACL en réseau

Une ACL sur un pare-feu (Activité Configuration pare-feu pfsense) ou un routeur filtrant (Activité Configuration ACL sur routeur Cisco) est une liste d'adresses ou de ports autorisés ou interdits par le dispositif de filtrage.

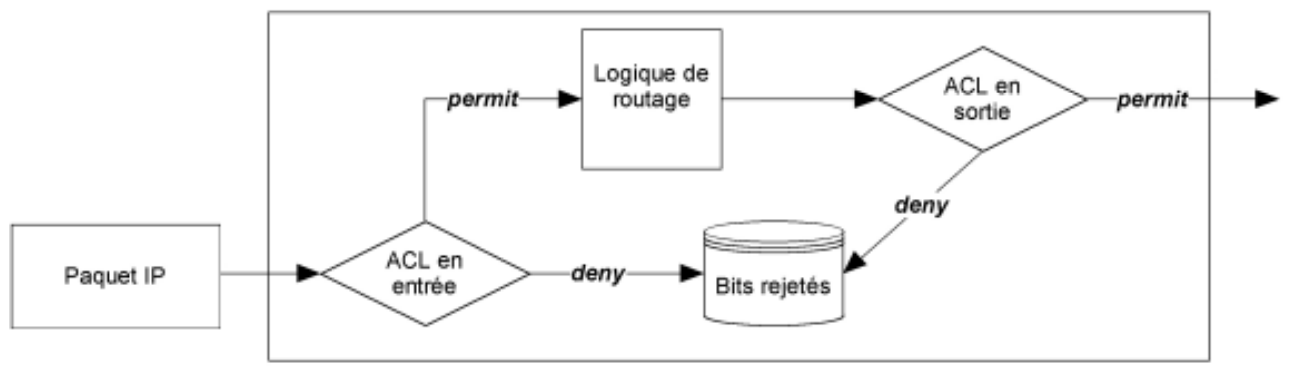


## Les ACL sous IOS Cisco

*Sources : CCNA Cisco*

Une ACL est une liste de règles permettant de filtrer ou d’autoriser du trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole, …).

* Une ACL permet d’autoriser du trafic (permit) ou de le bloquer (deny).
* Maximum d’une ACL par interface et par sens (input/output).
* Analyse séquentielle des ACE.
* Dès qu’une règle correspond au trafic, l’action définie est appliquée, le reste de l’ACL n’est pas analysé.
* Toute ACL par défaut bloque tout trafic. Donc tout trafic ne correspondant à aucune règle d’une ACL est rejeté.



|  |  |
| --- | --- |
| **ACL Standard** | **ACL Etendues** |
| Permet d’analyser du trafic en fonction de :   * Adresse IP source | Permet d’analyser du trafic en fonction de :   * Adresse IP source * Adresse IP destination * Protocole (tcp, udp, icmp, …) * Port source * Port destination * ... |
| *Les ACLs standard sont à appliquer le plus proche possible de la destination en raison de leur faible précision.* | *Les ACLs étendues sont à appliquer le plus proche possible de la source.* |

**Concevoir une ACL** : Lorsqu’une ACL contient plusieurs règles il faut placer les règles les plus précises en début de liste et donc les plus génériques en fin de liste.

**Conseils :**

* Concevoir une ACL dans un éditeur de texte et la configurer par copier/coller.
* Désactiver une ACL sur une interface avant de la modifier.

**Le masque générique ou Wildcard Mask**

Un masque générique est un masque de filtrage. Quand un bit aura une valeur de 0 dans le masque, il y aura vérification de ce bit sur l'adresse IP de référence. Lorsque le bit aura une valeur de 1, il n'en y aura pas.

Le masque générique à utiliser est généralement le masque inversé de réseau pour un réseau à filtrer.

Par exemple :

* Pour filtrer toutes les adresses du réseau 192.168.1.0/24 (255.255.255.0), on prendra un masque générique 0.0.0.255.
* Pour filtrer toutes les adresses du réseau 192.168.1.0/27 (255.255.255.224), on prendra un masque générique 0.0.0.31.

Donner le Wildcard Mask pour filtrer toutes les adresses du réseau 10.0.0.0/8

|  |
| --- |
| Masque réseau = 255.0.0.0  donc Wildcard = 0.255.255.255 |

Donner le Wildcard Mask pour filtrer toutes les adresses du réseau 172.20.40.0/26

|  |
| --- |
| Masque réseau = 255.255.255.192  donc Wildcard = 0.0.0.63 |

Le mot "any" remplace le 0.0.0.0 255.255.255.255, autrement dit toute adresse IP

Le mot "host" remplace le masque 0.0.0.0, par exemple, 10.1.1.1 0.0.0.0 peut être remplacé par "host 10.1.1.1"

## ACL standard

#### Configuration d’une ACL numérique standard (1 à 99 ou 1300 à 1999)

Wildcard Mask

Adresse IP source

Action

Numéro de l’ACL

R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255

R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255

R1(config)#access-list 1 deny 192.168.0.0 0.0.3.255

R1(config)#access-list 1 permit any

|  |  |  |
| --- | --- | --- |
| ACE 10 | permit 192.168.0.0 0.0.0.255 | Autorise le trafic source du réseau  Adresse IP 192.168.0.0 / 24  De l’adresse 192.168.0.0 à 192.168.0.255 |
| ACE 20 | permit 192.168.1.0 0.0.0.255 | Autorise le trafic source du réseau  Adresse IP 192.168.1.0 / 24  De l’adresse 192.168.1.0 à 192.168.1.255 |
| ACE 30 | deny 192.168.0.0 0.0.3.255 | Refuse le trafic source du réseau  Adresse IP 192.168.0.0 / 22  De l’adresse 192.168.0.0 à 192.168.3.255 |
| ACE 40 | permit any | Autorise le trafic de n’importe quelle source |

#### Configuration d’une ACL nommée standard

R1(config)#ip access-list standard monACL

R1config-std-nacl)#permit 192.168.0.0 0.0.0.255

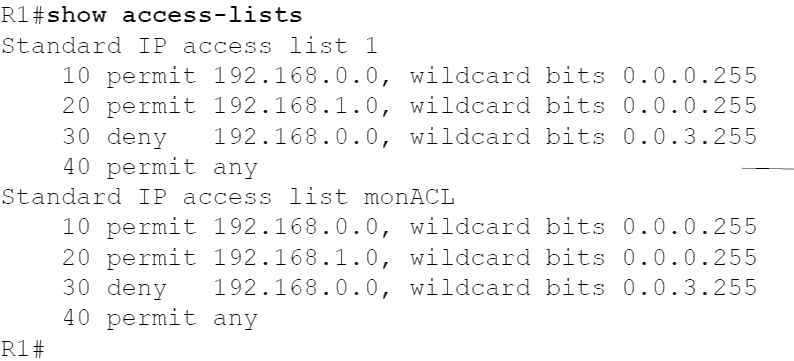
R1(config-std-nacl)#permit 192.168.1.0 0.0.0.255

R1(config-std-nacl)#deny 192.168.0.0 0.0.3.255

R1(config-std-nacl)#permit any

R1(config-std-nacl)#exit

#### Voir les ACL configurées



#### Exemple : Configuration d’une ACL standard

R1(config)#access-list 1 deny host 172.16.3.10

R1(config)#access-list 1 permit 172.16.0.0 0.0.255.255

R1(config)#access-list 1 deny any

|  |  |  |
| --- | --- | --- |
| ACE 10 | deny host 172.16.3.10 |  |
| ACE 20 | permit 172.16.3.0 0.0.0.255 |  |
| ACE 30 | deny any |  |

## ACL étendue

#### Configuration d’une ACL numérique étendue (100 à 199 ou 2000 à 2699)

Port destination

Adresse IP destination

Adresse IP source

Protocole

Action

Numéro de l’ACL

R1(config)#access-list 100 permit tcp any host 192.168.1.100 eq 80

R1(config)#access-list 100 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100

|  |  |  |
| --- | --- | --- |
| ACE 10 | permit tcp any host 192.168.1.100 eq 80 | Autorise le trafic TCP sur le port 80, de toutes les sources vers l’hôte 192.168.1.100 |
| ACE 20 | permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100 | Autorise le réseau qui va de 192.168.0.0 à .255, à envoyer des requêtes ICMP vers l’hôte 192.168.1.100 |

#### Configuration d’une ACL nommée étendue

R1(config)#ip access-list extended monACLextended

R1(config-ext-nacl)#permit tcp any host 192.168.1.100 eq 80

R1(config-ext-nacl)#permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100R1(config-ext-nacl)#exit

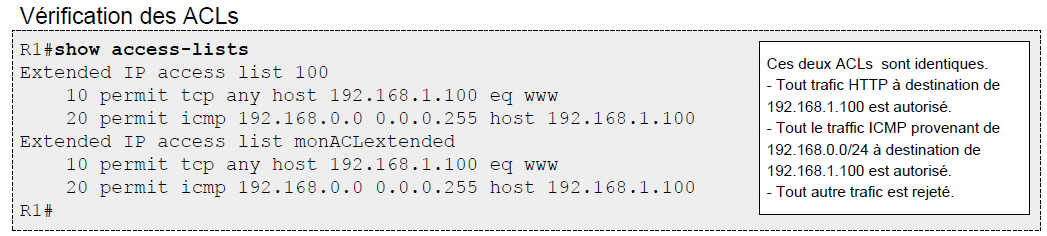
#### Exemple : Configuration d’une ACL numérotée étendue

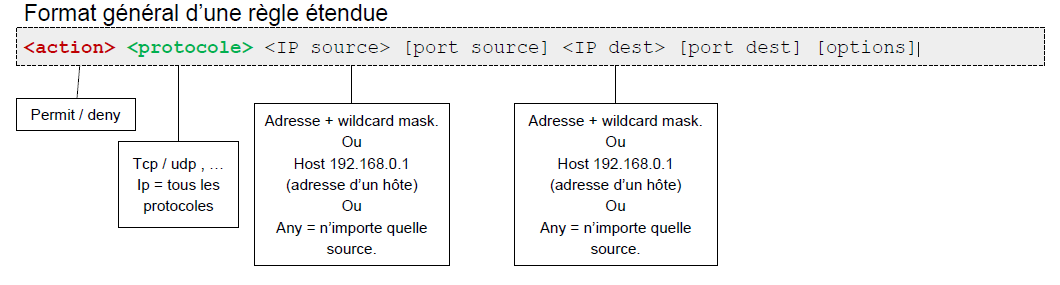
R1(config)#access-list 100 deny tcp host 180.10.10.1 host 220.10.10.1 eq www

R1(config)#access-list 100 deny tcp host 180.10.10.1 host 220.10.10.1 eq 443

R1(config)#access-list 100 permit ip any any

|  |  |  |
| --- | --- | --- |
| ACE 10 | deny tcp host 180.10.10.1 host 220.10.10.1 eq www | interdit protocole tcp port 80 de la source 180.10.10.1 vers l’adresse de destination 220.10.10.1 |
| ACE 20 | deny tcp host 180.10.10.1 host 220.10.10.1 eq 443 | interdit protocole tcp port 443 de la source 180.10.10.1 vers l’adresse de destination 220.10.10.1 |
| ACE 30 | permit ip any any | Autorise tous les protocoles |





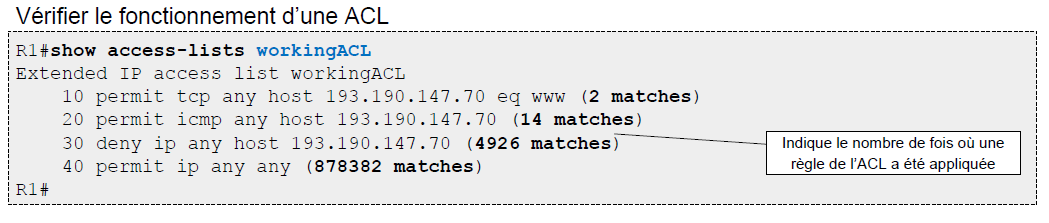
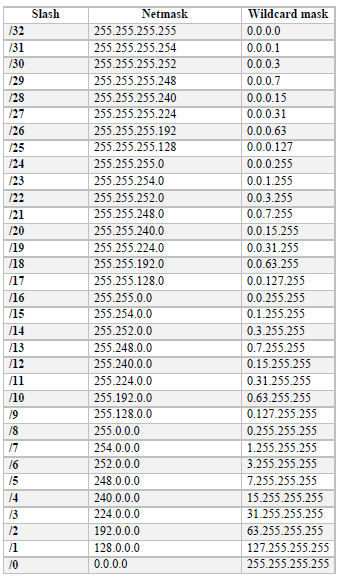
## Appliquer une ACL sur une interface

R1(config)#interface fastethernet 0/0

R1(config-if)#ip access-group 1 in

R1(config-if)#ip access-group 2 out

Applique l’ACL 1 pour le trafic entrant sur l’interface et l’ACL 2 pour le trafic sortant de l’interface



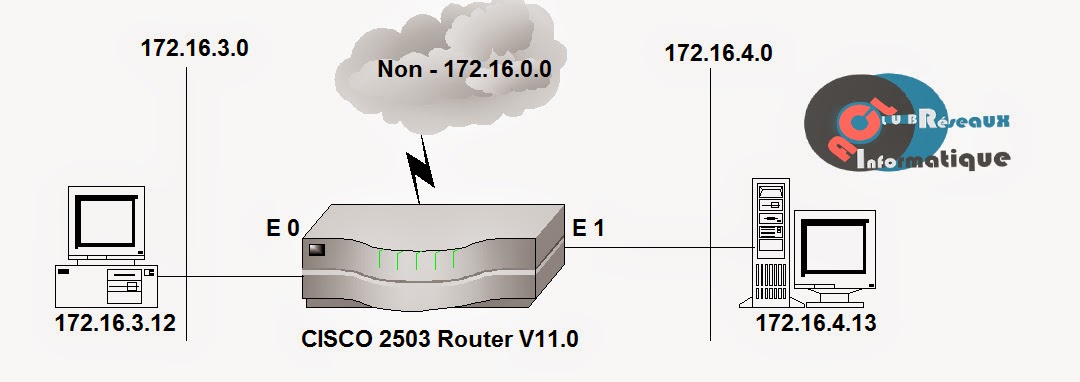
# Exercices ACL : Access Control List

## Exercice 1 : Calcul du filtre avec le Wildcard

Donnez l’ensemble des adresses IP concernées par les notations suivantes :

|  |  |  |
| --- | --- | --- |
| Adresse IP | Wildcard |  |
| 192.168.10.0 | 0.0.0.255 | 192.168.10.0 à 192.168.10.255 |
| 172.16.0.0 | 0.0.255.255 | 172.16.0.0 à 172.16.255.255 |
| 10.0.0.0 | 0.255.255.255 | 10.0.0.0 à 10.255.255.255 |
| 192.168.50.1 | 0.0.0.254 | 0.0.0.254 => 0.0.0.1111 1110  Toutes les adresses impaires de 192.168.50.1 à 192.168.50.255 |
| 192.168.10.128 | 0.0.0.95 | 192.168.10.32 à 192.168.10.63  et 192.168.10.96 à 192.168.10.127 |

## Exercice 2 : ACL standard et étendue



Router(config)#access-list 1 permit 172.16.0.0 0.0.255.255

Router(config)#interface Ethernet 0

Router(config-if)#ip access-group 1 out

Router(config)#interface ethernet 1

Router(config-if)#ip access group 1 out

Comment peut-on reconnaître qu’il s’agit d’une ACL standard ?

|  |
| --- |
|  |

Que fait cette règle ACL ?

|  |
| --- |
|  |

Ecrire la même règle en ACL étendu ?

|  |
| --- |
|  |

## Exercice 3 : ACL standard

Router(config)# access-list 1 deny 172.16.4.13 0.0.0.0

Router(config)# interface ethernet 0

Router(config)# ip access-group 1 out

Que fait cette règle ACL ?

|  |
| --- |
|  |

Quelle règle ajouter pour avoir un réseau fonctionnel ?

|  |
| --- |
| access-list 1 permit ip any any |

## Exercice 4 : ACL étendue

Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20

Router(config)#access-list 101 permit ip any any

Router(config)#interface ethernet 0

Router(config-if)#access-group 101 out

Que fait cette règle ACL ?

|  |
| --- |
|  |

## Etude réseau 1 :

Le réseau de l'entreprise doit être parfaitement hermétique à toute intrusion de l'extérieur. Cependant, les postes de ce réseau doivent toujours pouvoir accéder à internet.

On affectera donc à l'interface côté réseau d'entreprise, une liste de contrôle d'accès en entrée et en sortie :

En entrée :

* Autoriser tous les protocoles IP venant du réseau 172.16.0.0 vers tous les hôtes

En sortie :

* Autoriser le protocole TCP en provenance du port 80 de tous les hôtes à destination du réseau 172.16.0.0
* Autoriser le protocole ICMP en provenance du réseau de la DMZ à destination du réseau d'entreprise
* Autoriser le protocole ICMP en provenance de tous les hôtes et à destination du réseau d'entreprise

Ecrivez les listes de contrôle d'accès correspondantes :

|  |  |
| --- | --- |
| En entrée ACL 100 | access-list 100 permit ip 172.16.0.0 0.0.255.255 any |
| En sortie ACL 101 | access-list 101 permit tcp any 172.16.0.0 0.0.255.255 eq 80  access-list 101 permit icmp 10.0.0.0 0.0.0.7 172.16.0.0 0.0.255.255  access-list 101 permit icmp any 172.16.0.0 0.0.255.255 |

## Deny a Select Host to Access the NetworkEtude réseaux 2a :

Refuser l'accès au réseau NetA pour un hôte B

|  |
| --- |
| access-list 1 deny host 192.168.10.1  access-list 1 permit any  interface ethernet0  ip access-group 1 in |

## Etude réseaux 2b :

Autoriser l'accès du réseau NetB au réseau NetA

|  |
| --- |
| access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.200.0 0.0.0.255  interface ethernet0  ip access-group 101 in |

## Etude réseaux 2c :

Refuser le trafic Telnet (TCP, port 23) depuis NetB vers NetA

|  |
| --- |
| access-list 102 deny tcp any any eq 23  access-list 102 permit ip any any  interface ethernet0  ip access-group 102 in |

## Etude réseaux 2d :

Refuser le trafic FTP (TCP, port 21) depuis NetB vers NetA

|  |
| --- |
| access-list 102 deny tcp any any eq ftp  access-list 102 deny tcp any any eq ftp-data  access-list 102 permit ip any any  interface ethernet0  ip access-group 102 in |

## QUIZ

1-Quel ensemble d’entrées de contrôle d’accès permettrait à tous les utilisateurs du réseau 192.168.10.0/24 d’accéder à un serveur Web situé à l’adresse 172.17.80.1, sans toutefois les autoriser à utiliser le protocole Telnet ?

access-list 103 permit 192.168.10.0 0.0.0.255 host 172.17.80.1

access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq telnet​​

access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80

access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23

access-list 103 permit tcp 192.168.10.0 0.0.0.255 host 172.17.80.1 eq 80

access-list 103 deny tcp 192.168.10.0 0.0.0.255 any eq 23 VRAI

access-list 103 deny tcp host 192.168.10.0 any eq 23

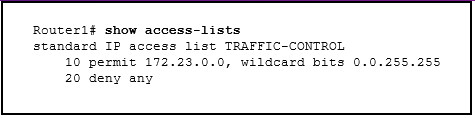
access-list 103 permit tcp host 192.168.10.1 eq 80

2-Une ACL est appliquée en entrée sur une interface de routeur. L’ACL se compose d’une entrée unique :

access-list 101 permit udp 192.168.100.0 0.0.2.255 64.100.40.0 0.0.15 eq telnet

Si un paquet avec une adresse source 192.168.101.45, une adresse de destination 64.100.40.4 et un protocole 23 est reçu sur l’interface, le paquet est-il autorisé ou refusé ? refusé

3-Un administrateur réseau souhaite ajouter une entrée ACE à la liste de contrôle d’accès TRAFFIC-CONTROL pour refuser le trafic IP du sous-réseau 172.23.16.0/20. Quelle entrée ACE répond à cette exigence ?

30 deny 172.23.16.0 0.0.15.255

5 deny 172.23.16.0 0.0.255.255

15 deny 172.23.16.0 0.0.15.255

5 deny 172.23.16.0 0.0.15.255 vrai

4-Un administrateur réseau établit une liste de contrôle d’accès standard qui interdira tout trafic venant du réseau 172.16.0.0/16 mais autorisera tous les autres trafics. Quelles sont les deux commandes à utiliser ? (Choisissez deux réponses.)

Router(config)# access-list 95 172.16.0.0 255.255.255.255

Router(config)# access-list 95 host 172.16.0.0

Router(config)# access-list 95 deny any

Router(config)# access-list 95 deny 172.16.0.0 255.255.0.0

Router(config)# access-list 95 permit any vrai

Router(config)# access-list 95 deny 172.16.0.0 0.0.255.255 vrai

5-Une ACL est appliquée en entrée sur une interface de routeur. L’ACL se compose d’une seule entrée :

access-list 101 permit tcp 10.1.1.0 0.0.0.255 host 192.31.7.45 eq dns

Si un paquet avec une adresse source de 10.1.1.201, une adresse de destination de 192.31.7.45 et un protocole de 23 est reçu sur l’interface, le paquet est-il autorisé ou refusé ? refusé

6-Une ACL est appliquée en entrée sur une interface de routeur. L’ACL se compose d’une seule entrée :

access-list 100 permit tcp 192.168.10.0 0.0.0.255 172.17.200.0 0.0.0.255 eq www

Si un paquet avec une adresse source de 192.168.10.244, une adresse de destination de 172.17.200.56 et un protocole de 80 est reçu sur l’interface, le paquet est-il autorisé ou refusé ?

Refusé

## Pratique Packet Tracer

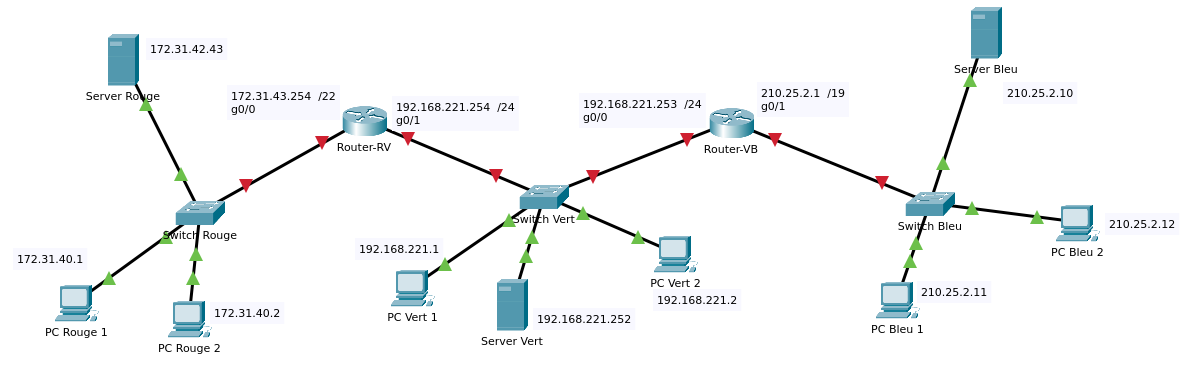
5.1.8 – Packet Tracer – Configurer Des Listes ACL IPv4 Standard Numérotées

5.1.9 – Packet Tracer – Configurer Les ACLs IPv4 Standard Nommées

5.4.13 – Packet Tracer – Configurer Les Listes De Contrôle D’accès IPv4 Étendues – Scénario 2

# ACL Réseau à configurer

Fichier dans ressources Cisco -> ACL PT.pka



## Configurer les adresses IP, passerelles et routes de ce réseau

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nom | Interface | Adresse IP | Masque de sous réseau | Adresse Réseau | Passerelle |
| Server Rouge |  |  |  |  |
| PC Rouge 1 |  |  |  |  |
| PC Rouge 2 |  |  |  |  |
| Router-RV | g0/0 |  |  |  |  |
| Router-RV | g0/1 |  |  |  |  |
| Server Vert |  |  |  | 192.168.221.254 |
| PC Vert 1 |  |  |  | 192.168.221.254 |
| PC Vert 2 |  |  |  | 192.168.221.254 |
| Router-VB | g0/0 |  |  |  |  |
| Router-VB | g0/1 |  |  |  |  |
| Server Bleu |  |  |  |  |
| PC Bleu 1 |  |  |  |  |
| PC Bleu 2 |  |  |  |  |

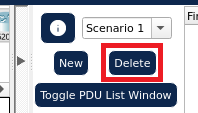
Route sur Router-RV pour aller sur le réseau Bleu

|  |  |  |
| --- | --- | --- |
| Réseau de destination | Masque de réseau | Next-Hop (Passerelle) |
|  |  |  |

Route sur Router-VB pour aller sur le réseau Rouge

|  |  |  |
| --- | --- | --- |
| Réseau de destination | Masque de réseau | Next-Hop (Passerelle) |
|  |  |  |

## Configurer les adresses IP, passerelles et routes de ce réseau

* Configurer les adresses IP de tous les éléments (PC, Server et Routeur)
* Configurer les passerelles sur les PC et Serveurs
* Configurer les routes sur les 2 routeurs
* Tester les connexions entre les réseaux :
  + Conseil utiliser les « simple PDU » (raccourci P) pour tester la connectivité
  + Effacer la liste de PDU après 2-3 PDU pour plus de clarté

Rappel du cours :

* Les ACLs standard sont à appliquer le plus proche possible de la destination en raison de leur faible précision.
* Les ACLs étendues sont à appliquer le plus proche possible de la source.

## Configurer des règles ACL standards

#### Règle 1

* Ecrire une règle ACL standard.

Objectif :

* bloquer les connexions venant du réseau Vert vers le réseau Bleu
* autoriser les connexions venant du réseau Rouge vers le réseau Bleu

Où l’appliquer :

* Router-VB ; Interface g0/0 ; En entrée

|  |
| --- |
| access-list 1 deny 192.168.221.0 0.0.0.255  access-list 1 permit 172.31.40.0 0.0.3.255  interface g0/0  ip access-group 1 in |

* Tester et valider la règle.

#### Règle 2

Objectif :

* bloquer les connexions venant du réseau Vert vers le réseau Rouge
* autoriser les connexions venant du réseau Bleu vers le réseau Vert

Où l’appliquer :

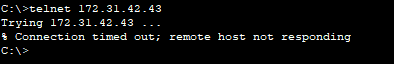
* ………………………. ; ………………………………… ; …………………………..

|  |
| --- |
| access-list 1 deny 192.168.221.0 0.0.0.255  access-list 1 permit 210.25.0.0 0.0.31.255  interface g0/1  ip access-group 1 in |

* Tester et valider la règle.
* Supprimer les ACLs mises sur les 2 routeurs

## Configurer des règles ACL étendues

Conseils :

* Utiliser le navigateur pour tester la connexion www ou port 80
* Utiliser le terminal (cmd) pour tester les connexions telnet ou ssh :
  + Exemple : telnet 192.168.1.1



Echec de la connexion avec l’hôte Connexion réussie avec l’hôte

#### Règle 1

Objectif :

* bloquer les connexions telnet venant de la machine PC-Vert 1 vers le réseau Rouge
* autoriser les connexions www venant du réseau Bleu vers le réseau Rouge
* autoriser les connexions 443 venant du réseau Bleu vers le réseau Rouge
* autoriser les connexions ssh venant du réseau Vert vers le réseau Rouge

Où l’appliquer :

* ………………………. ; ………………………………… ; …………………………..

|  |
| --- |
|  |

* Tester et valider la règle.

#### Règle 2

Objectif :

* bloquer toutes les connexions venant de la machine PC-Vert 1 vers le réseau Bleu
* autoriser les connexions www venant du réseau Vert vers le réseau Bleu
* bloquer les connexions du port 555 venant du réseau Vert vers le réseau Bleu
* bloquer les connexions ftp venant du réseau Vert vers le réseau Bleu
* autoriser les restes

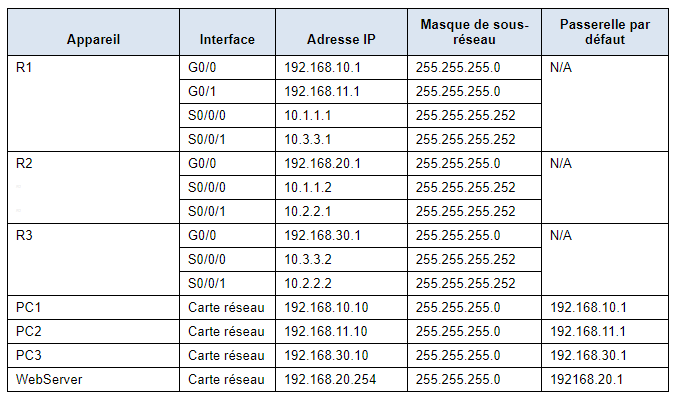
Où l’appliquer :

* ………………………. ; ………………………………… ; …………………………..

|  |
| --- |
|  |

* Tester et valider la règle.

# Exercices simulation PT : Configurer les ACLs IPv4 standard numérotées

fichier : 5.1.8-packet-tracer---configure-numbered-standard-ipv4-acls\_fr-FR.pkt

**Table d'adressage**

Instructions

Avant d'appliquer une liste de contrôle d'accès à un réseau, il convient de vérifier que vous disposez d'une connectivité complète. Vérifiez la connectivité complète du réseau en choisissant un PC et en envoyant une requête ping à d'autres périphériques sur le réseau. Vous devriez être en mesure d'effectuer un ping avec succès pour chaque appareil.

Les politiques de réseau suivantes sont mises en œuvre sur la **R2**:

·         Le réseau 192.168.11.0/24 n'est pas autorisé à accéder au **ServeurWeb** sur le réseau 192.168.20.0/24.

·         Tout autre accès est autorisé.

Pour limiter l'accès du réseau 192.168.11.0/24 vers **ServeurWeb** sur 192.168.20.254 sans perturber le reste du trafic, il faut créer une liste de contrôle d'accès sur **R2**. La liste d'accès doit être placée sur l'interface de sortie vers le **serveur web**. Une deuxième règle doit être créée sur **R2** pour permettre tout autre trafic.

Les politiques de réseau suivantes sont mises en œuvre sur la **R3**:

·         Le réseau 192.168.10.0/24 n'est pas autorisé à communiquer avec le réseau 192.168.30.0/24.

·         Tout autre accès est autorisé.

Pour limiter l'accès du réseau 192.168.10.0/24 au réseau 192.168.30/24 sans interférer avec les autres trafics, une liste d'accès devra être créée sur **R3**. Il faut placer la liste ACL sur l’interface sortante vers **PC3**. Une deuxième règle doit être créée sur **R3** pour autoriser tous les autres types de trafic.

### Étape 1 : Configurer et appliquer une ACL standard numérotée sur R2.

Créez une liste de contrôle d'accès en utilisant le numéro **1** sur **R2**

|  |
| --- |
| R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255  R2(config)# access-list 1 permit any |

Avant d'appliquer une liste d'accès à une interface pour filtrer le trafic, il est recommandé d'examiner le contenu de la liste d'accès afin de vérifier qu'elle filtrera le trafic comme prévu.

R2# **show access-lists**

Pour que l'ACL puisse réellement filtrer le trafic, il doit être appliqué à une opération de routeur. Appliquez la liste de contrôle d'accès en la plaçant pour le trafic sortant sur l'interface Gigabit Ethernet 0/0.

Remarque : Dans un réseau opérationnel réel, il n'est pas recommandé d'appliquer une liste d'accès non testée à une interface active.

|  |
| --- |
| R2(config)# interface GigabitEthernet0/0  R2(config-if)# ip access-group 1 out |

### Étape 2 : Configurez et appliquez une liste ACL standard numérotée sur le routeur R3.

Créez une liste de contrôle d'accès en utilisant le numéro **1** sur **R3**

|  |
| --- |
| R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255  R3(config)# access-list 1 permit any |

Vérifiez que la liste d'accès est correctement configurée.

R3# **show access-lists**

Appliquez la liste de contrôle d'accès en la plaçant pour le trafic sortant sur l'interface Gigabit Ethernet 0/0.

|  |
| --- |
| R3(config)# interface GigabitEthernet0/0  R3(config-if)# ip access-group 1 out |

### Vérifiez la configuration et le fonctionnement des listes de contrôle d'accès.

Avec les deux listes de contrôle d'accès en place, le trafic réseau est limité en fonction des stratégies détaillées dans la Partie 1. Utilisez les tests suivants pour vérifier les implémentations du ACL :

|  |  |
| --- | --- |
| ·         Une requête ping de 192.168.10.10 vers 192.168.11.10 aboutit.  ·         Une requête ping de 192.168.10.10 vers 192.168.20.254 aboutit.  ·         Une requête ping de 192.168.11.10 vers 192.168.20.254 échoue. | ·         Une requête ping de 192.168.10.10 vers 192.168.30.10 échoue.  ·         Une requête ping de 192.168.11.10 vers 192.168.30.10 aboutit.  ·         Une requête ping de 192.168.30.10 vers 192.168.20.254 aboutit |

Exécutez à nouveau la commande **show access-lists** sur les routeurs **R2** et **R3**. Vous devriez voir une sortie qui indique le nombre de paquets qui ont correspondu à chaque ligne de la liste d'accès. Remarque : Le nombre de correspondances affichées pour vos routeurs peut être différent, en raison du nombre de pings envoyés et reçus.

|  |  |
| --- | --- |
| R2# **show access-lists**  Standard IP access list 1  10 deny 192.168.11.0 0.0.0.255 (4 match(es))  20 permit any (8 match(es)) | R3# **show access-lists**  Standard IP access list 1  10 deny 192.168.10.0 0.0.0.255 (4 match(es))  20 permit any (8 match(es) |

# Exercices simulation PT : Configurer les ACLs IPv4 standard nommées

fichier : 5.1.9-packet-tracer---configure-named-standard-ipv4-acls\_fr-FR.pkt

**Table d'adressage**

# 

## Configurer et appliquer une liste ACL standard nommée *fenêtre de configuration.*

a.     Configurez l'ACL nommé suivant sur **R1**.

R1(config)# **ip access-list standard File\_Server\_Restrictions**

R1(config-std-nacl)# **permit host 192.168.20.4**

R1(config-std-nacl)# **permit host 192.168.100.100**

R1(config-std-nacl)# **deny any**

b.     Utilisez la commande **show access-lists** pour vérifier le contenu de la liste d'accès.

R1# **show access-lists**

Standard IP access list File\_Server\_Restrictions

10 permit host 192.168.20.4

20 permit host 192.168.100.100

30 deny any

### Appliquer la ACL nommé.

a.     Appliquez l'ACL en sortie sur l'interface Fast Ethernet 0/1.

R1(config-if)# **ip access-group File\_Server\_Restrictions out***.*

### Vérification de la configuration de la ACL et de l'application à l'interface.

*Ouvrez la fenêtre de configuration.*

Utilisez la commande **show access-lists**pour vérifier la configuration de l'ACL. Utilisez la commande **show run**ou **show ip interface fastethernet 0/1**pour vérifier que l'ACL est correctement appliquée à l'interface.

### Vérifiez que la ACL fonctionne correctement.

Les trois postes de travail devraient être en mesure d'envoyer un ping au serveur **Web , mais seuls le PC1 et le serveur Web devraient pouvoir envoyer un ping au serveur de fichiers. Répétez la commande show access-lists pour voir le nombre de paquets correspondant à chaque instruction.**

# Exercices simulation PT : Configurer les ACLs IPv4 étendues

fichier : 5.4.13-packet-tracer---configure-extended-ipv4-acls---scenario-2\_fr-FR.pkt

**Table d'adressage**

# 

Contexte / Scénario

Dans ce scénario, certains appareils du LAN sont autorisés à accéder à différents services sur des serveurs sur l'internet.

Configurer une liste de contrôle d'accès étendue nommée

* Configurez une liste de contrôle d'accès nommée pour implémenter la stratégie suivante :

·         Bloquer les accès HTTP et HTTPS de **PC1**au **Serveur 1**et **Serveur 2.**Les serveurs sont dans le cloud et vous êtes la seule personne qui connaît leur adresse IP.

·         Bloquer l'accès FTP de **PC2**au **Serveur1**et **Serveur2**.

·         Bloquez l'accès ICMP de **PC3**au **Serveur1**et **Serveur2**.

### Refusez à PC1 l'accès aux services HTTP et HTTPS sur Serveur1 et Serveur2.

|  |
| --- |
| RT1(config)# ip access-list extended ACL1  RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254 eq 80  RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.101.255.254 eq 443  RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254 eq 80  RT1(config-ext-nacl)# deny tcp host 172.31.1.101 host 64.103.255.254 eq 443 |

### Refusez à PC2 l'accès aux services FTP sur Serveur 1 et Serveur 2.

|  |
| --- |
| RT1(config-ext-nacl)# deny tcp host 172.31.1.102 host 64.101.255.254 eq 21  RT1(config-ext-nacl)# deny tcp host 172.31.1.102 host 64.103.255.254 eq 21 |

### Empêchez PC3 d'envoyer une requête ping à Serveur1 et Serveur2.

|  |
| --- |
| RT1(config-ext-nacl)# deny icmp host 172.31.1.103 host 64.101.255.254  RT1(config-ext-nacl)# deny icmp host 172.31.1.103 host 64.103.255.254 |

### Autorisez tout autre trafic PC.

|  |
| --- |
| RT1(config-ext-nacl)# permit ip any any |

### Vérifiez la configuration de la liste d'accès avant de l'appliquer à une interface.*e de configuration.*

## Appliquer et vérifier la liste de contrôle d'accès étendue

Le trafic à filtrer vient du réseau 172.31.1.96/27 et est destiné à des réseaux distants. L'emplacement approprié de la liste de contrôle d'accès dépend également de la relation du trafic par rapport à **RT1**. En général, les listes d'accès étendues doivent être placées sur l'interface la plus proche de la source du trafic.

### Appliquez la liste de contrôle d'accès à l’interface appropriée dans la bonne direction.

Sur quelle interface l'ACL nommée doit-elle être appliquée et dans quelle direction ?

|  |
| --- |
| G0/0 in |

*Ouvrez la fenêtre de configuration.*

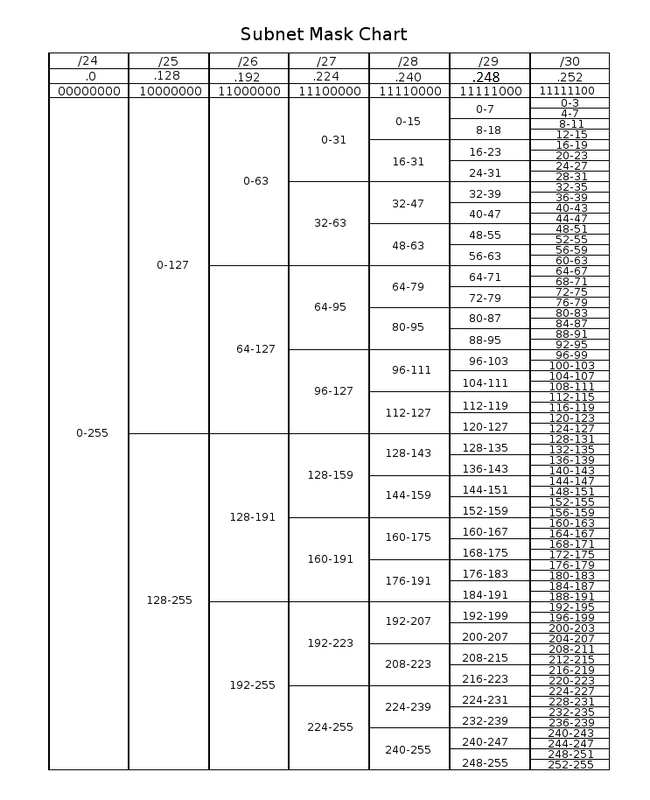
Saisissiez la commande de configuration pour appliquer la liste de contrôle d'accès à l'interface.*z la fenêtre de configuration.*

|  |
| --- |
| RT1(config)# interface g0/0  RT1(config-if)# ip access-group ACL1 in |

Accédez au FTP de **Serveur1** et **Serveur2** à l'aide de **PC1**. Le nom d'utilisateur et le mot de passe sont **cisco**.

Ping **Serveur1** et **Serveur2** à partir de **PC1**.

Répétez les étapes avec **PC2** et **PC3** pour vérifier le bon fonctionnement de la liste d'accès.



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Longueur du préfixe  CIDR  Nbr de bit réseau | Nombre d’hôtes max | Masque de sous réseau | Masque inversé de sous réseau | Préfixe |
| /16 | 65534 | 255.255.0.0 | 0.0.255.255 | /16 |
| /17 | 32766 | 255.255.128.0 | 0.0.127.255 | /17 |
| /18 | 16382 | 255.255.192.0 | 0.0.0.63.255 | /18 |
| /19 | 8190 | 255.255.224.0 | 0.0.31.255 | /19 |
| /20 | 4094 | 255.255.240.0 | 0.0.15.255 | /20 |
| /21 | 2046 | 255.255.248.0 | 0.0.7.255 | /21 |
| /22 | 1022 | 255.255.252.0 | 0.0.3.255 | /22 |
| /23 | 510 | 255.255.254.0 | 0.0.1.255 | /23 |
| /24 | 254 | 255.255.255.0 | 0.0.0.255 | /24 |
| /25 | 126 | 255.255.255.128 | 0.0.0.127 | /25 |
| /26 | 62 | 255.255.255.192 | 0.0.0.63 | /26 |
| /27 | 30 | 255.255.255.224 | 0.0.0.31 | /27 |
| /28 | 14 | 255.255.255.240 | 0.0.0.15 | /28 |
| /29 | 6 | 255.255.255.248 | 0.0.0.7 | /29 |
| /30 | 2 | 255.255.255.252 | 0.0.0.3 | /30 |

