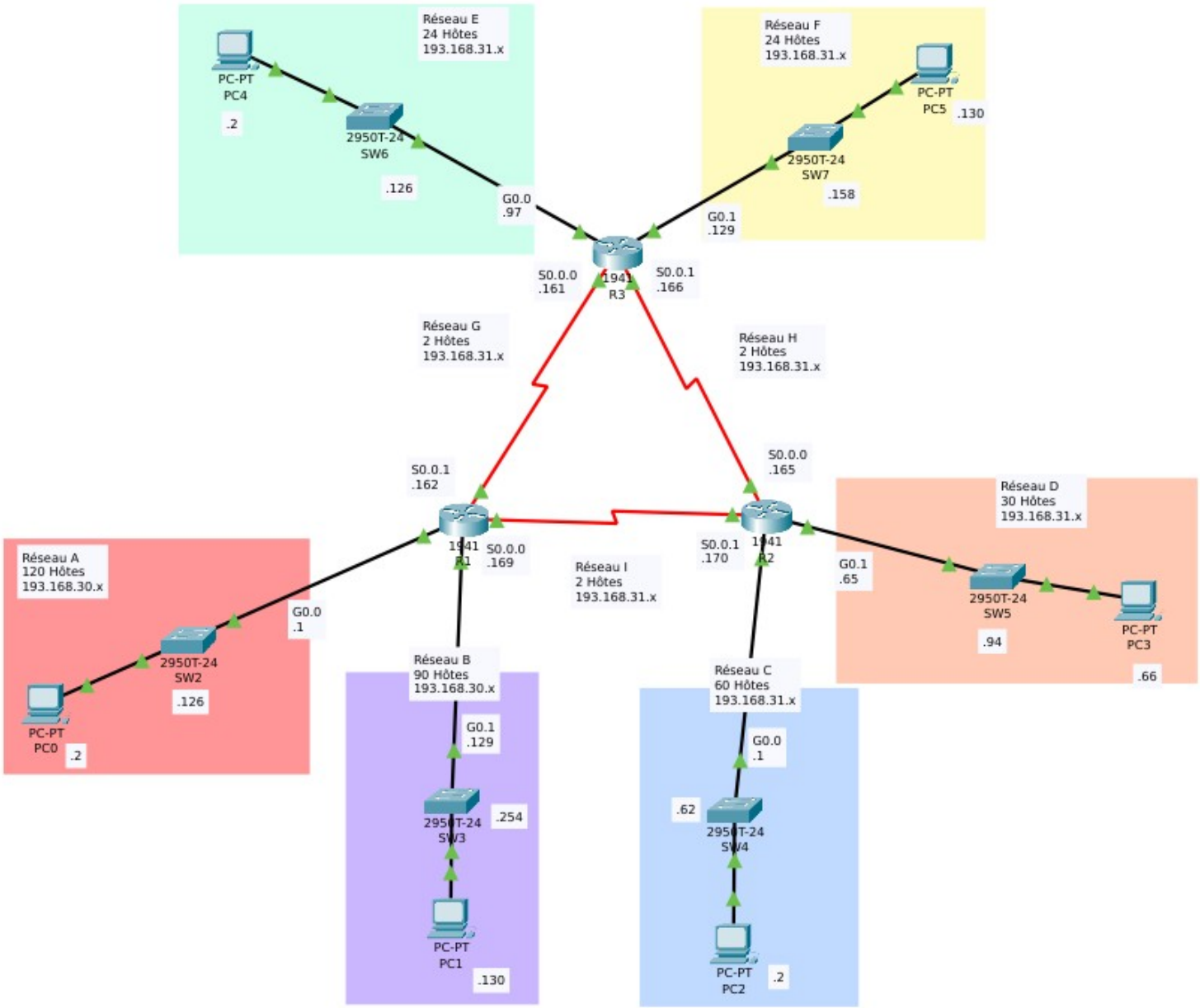
Compte-Rendu Examen du 05/04

Mise en place d'un réseau sécurisé avec prise en compte du protocole SSH.



Sommaire

Préambule

Dans le cadre de ce compte-rendu la plupart des commandes routeurs/commutateurs seront écrient au complet cependant les appareils cisco autorise aux utilisateurs à les raccourcir pour gagner du temps. Nous allons donc configurer un réseau en triangle composé de 3 routeurs, 6 commutateurs et 6 PCs. Au préalable nous avons effectué le mappage du réseau (définir les adresses des hôtes, des réseaux, et les masques). En plus de la configuration nous allons aussi effectuer la configuration du SSH, un système qui permet de sécurisé en partie le réseau. En première partie nous allons configurer les PCs et voir les commandes disponibles pour pouvoir ensuite tester le réseau. Ensuite nous allons configurer les commutateurs car ils sont plus faciles à tester indépendamment que les routeurs. Et enfin nous allons configurer les routeurs. Pour un soucis de simplicité nous conseillons de réaliser la partie sécurisation en dernier car celle-ci n’influe pas sur la partie communication et en cas de problème il sera plus facile de détecter les erreurs.

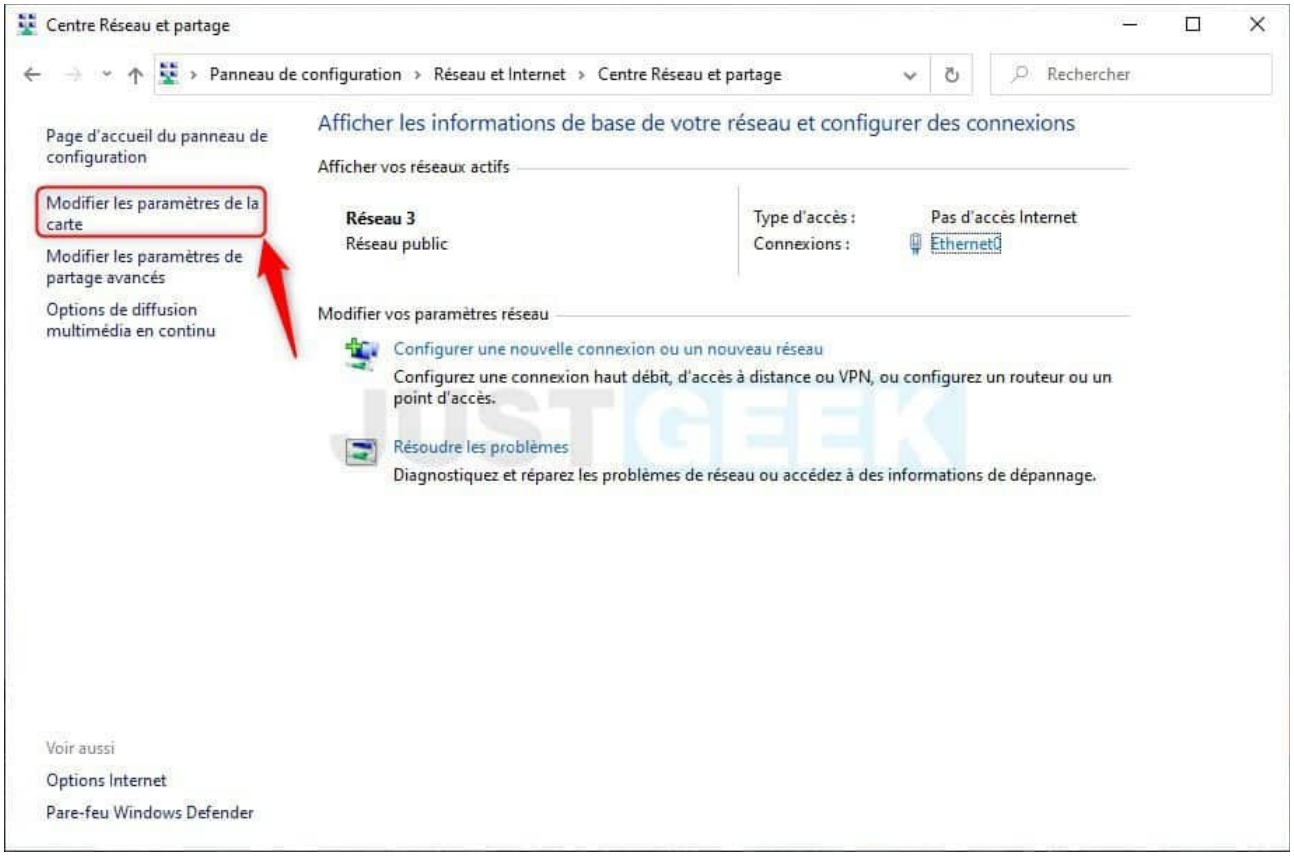
Configuration des ordinateurs :

Pour pouvoir tester nos futures configurations nous allons configurer les PC. Comme indiqué sur le schéma du réseau il va y avoir 1 PC par réseau pour pouvoir tester chaque commutateur. Dans un soucis de simplicité l'adresse de nos PC sera la deuxième adresse disponible dans le réseau.

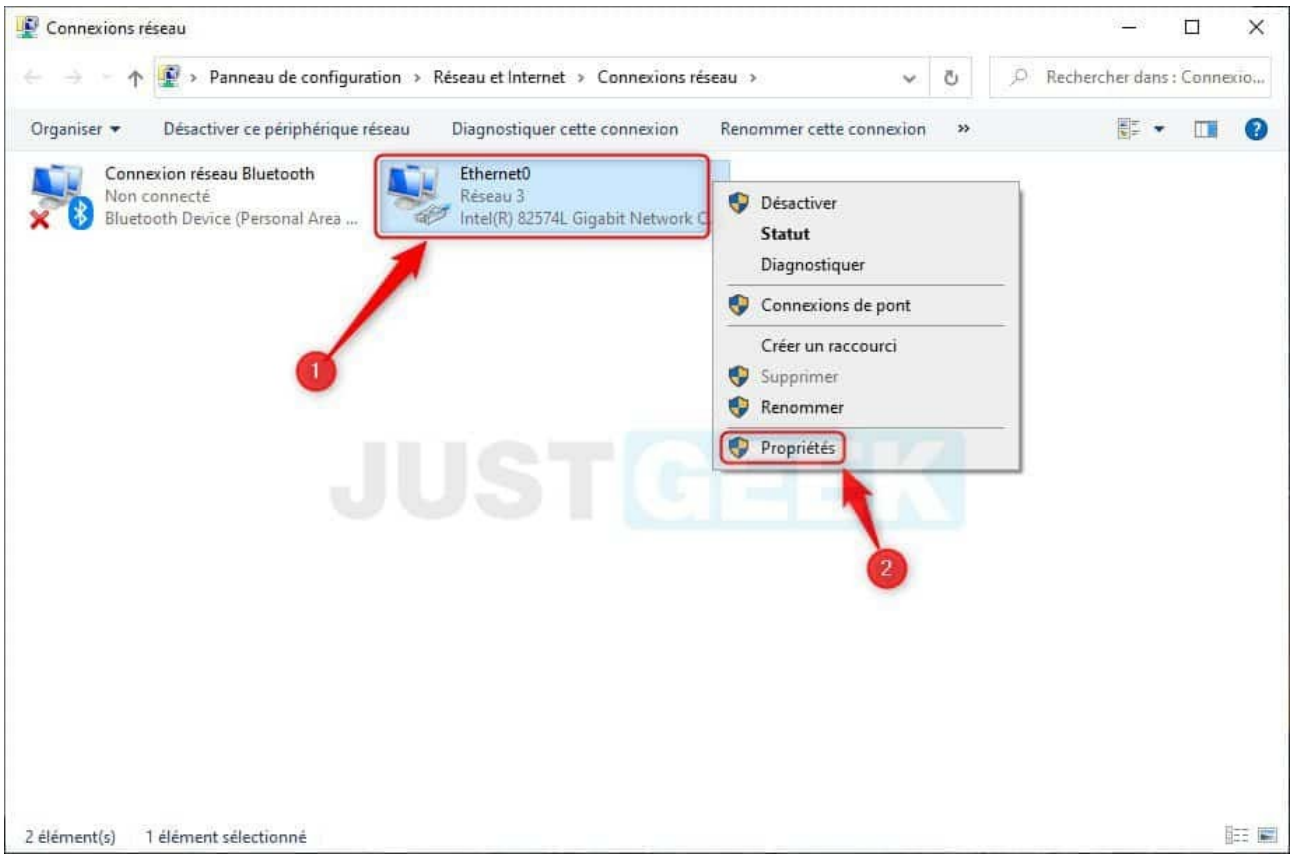
Configuration de l'adresse IP et de la passerelle par défaut :

En premier lieu il va falloir configurer l'adresse ip, le masque et la passerelle par défaut de chaque ordinateur.

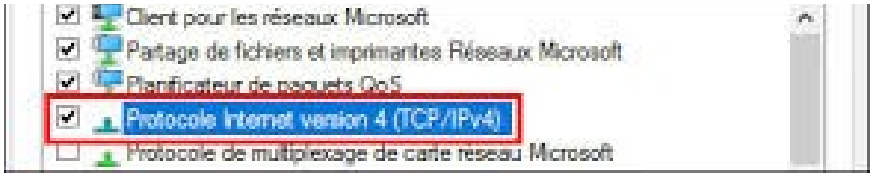
Tous d'abord tapez dans la barre de recherche windows «Panneau de configuration», puis dans ce panneau appuyez sur « Réseau et Internet », puis « Centre Réseau et partage ».



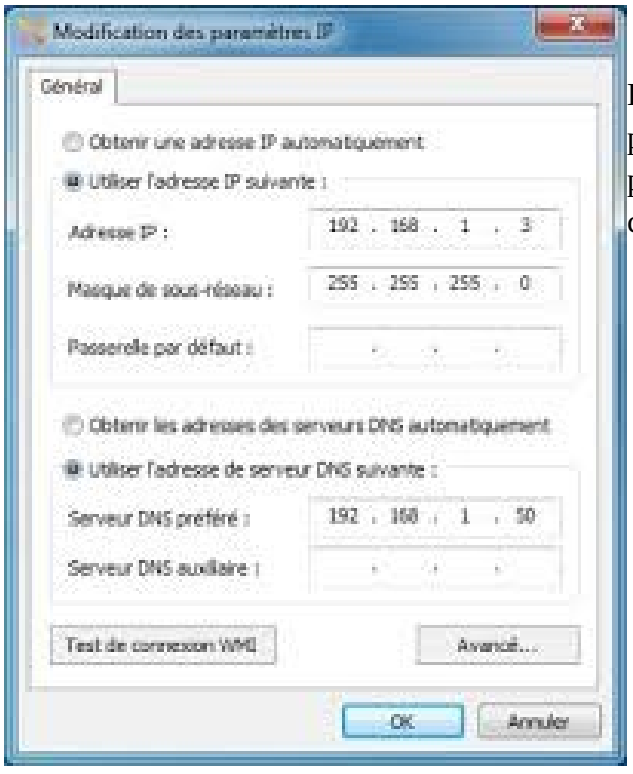
Après être arrivé à cette page cliquez sur « Modifier les paramètres de la carte », comme indiquer ci-dessus.



Ensuite double cliquez sur «Ethernet» (c'est le port Ethernet de votre PC) et appuyez sur «Propriétés».



Et enfin il ne reste plus qu'à double-cliquer sur «Protocole Internet version 4(TCP/IPv4)»

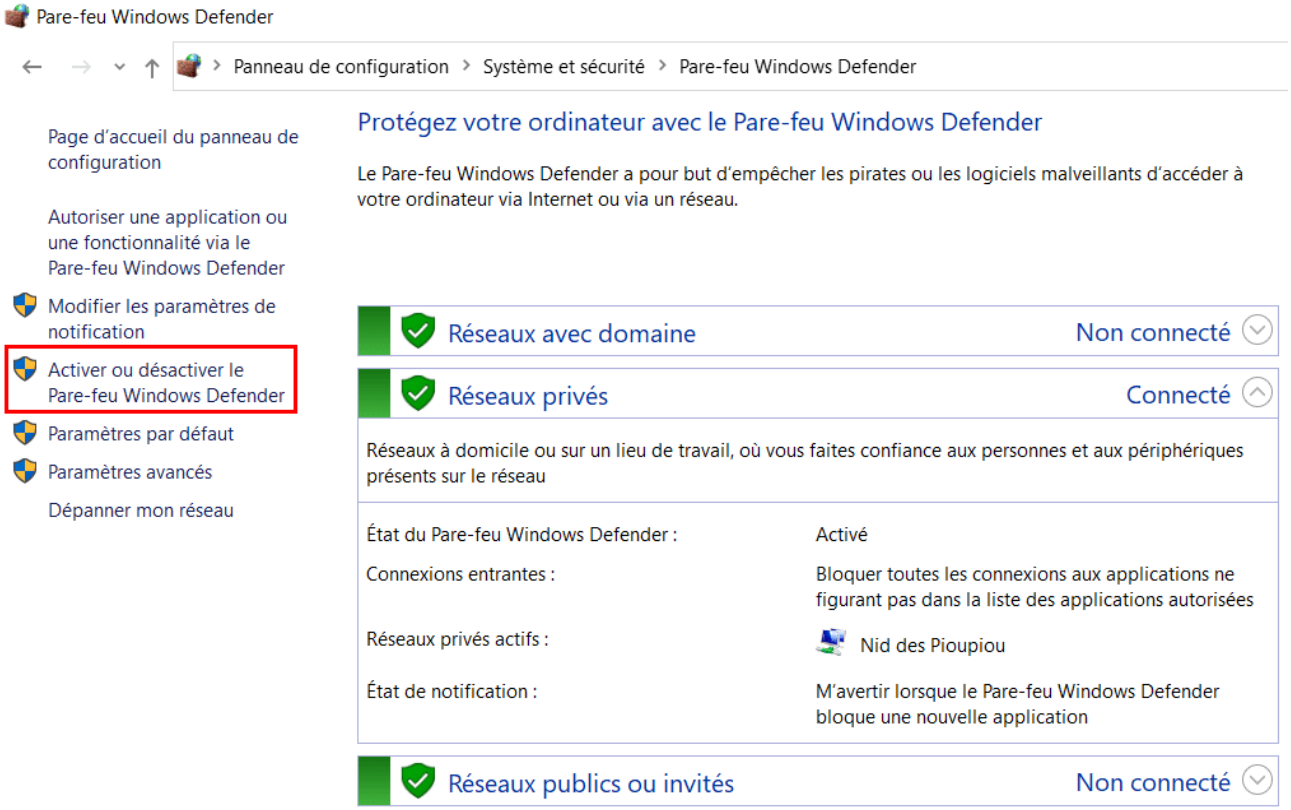


Ensuite cette page apparaîtra et il ne vous restera plus qu'a inscrire vos adresses. Pour la passerelle par défaut celle-ci sera l'adresse du routeur en charge du réseau du PC.

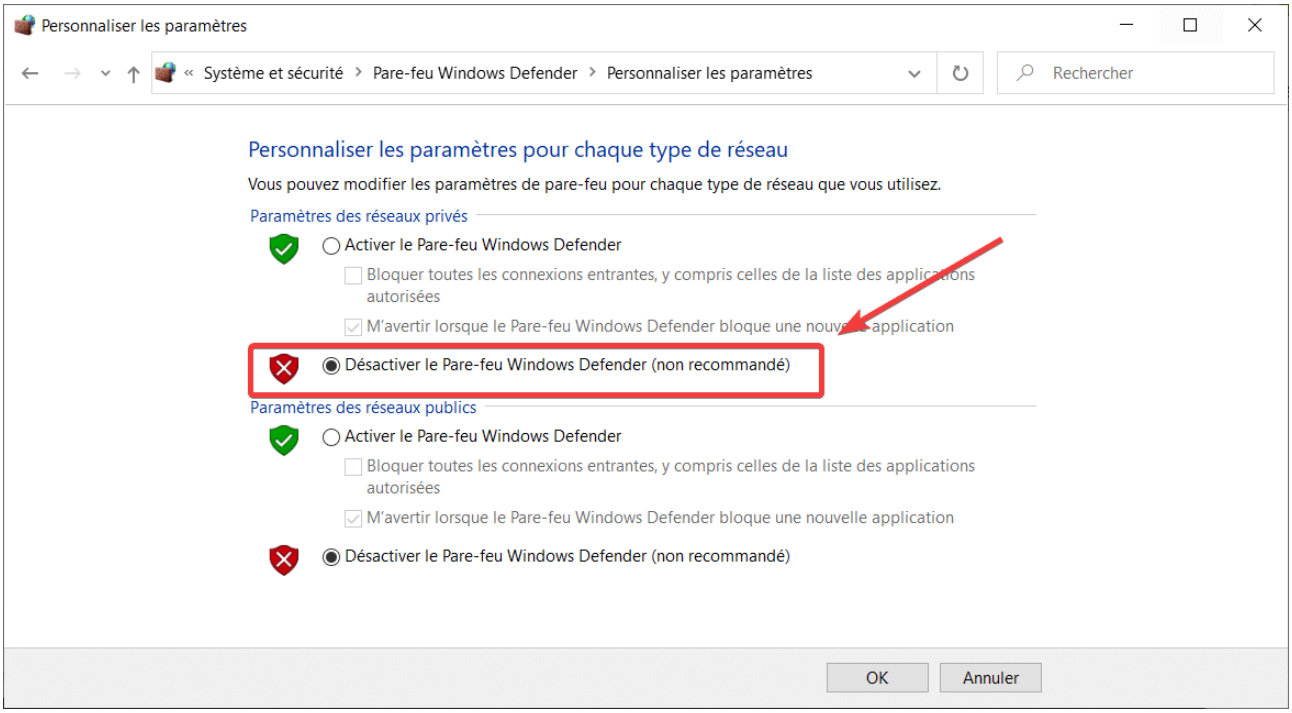
Enlever le pare-feu

Le pare-feu est un moyen de sécuriser les données entrante dans votre PC, cependant celui-ci peut poser problème lors de la mise en place d'un réseau comme par exemple couper les communications.

Tous d'abord chercher «Pare-feu Windows Defender» dans la barre de recherche Windows. Ensuite le menu pare-feu s'ouvrira.



Après l'ouverture du menu appuyer «Activer ou désactiver le Pare-feu Windows Defender».



Il ne restera plus qu'à désactiver les pares-feu comme monter ci-dessus.

Tester la connexion

Enfin quand votre réseau sera près il faudra tester les connexions pour cela rien de plus simple, voici quelques commandes permettant de tester les connexions.

Ping

La commande ping permet de simplement tester les communications en envoyant des paquets et en attendant une réponse. Il est possible de communiquer avec tous les hôtes du réseau tel que les Pcs, les routeurs, les commutateurs, etc.

```
C:\Users\Eleves>ping {adresse à contacter}
```

Tracert

La commande tracert est de même fonction que la commande ping, cependant celle-ci indique le chemin que les données empreintes.

```
C:\Users\Eleves>tracert {adresse à contacter}
```

SSH

La commande ssh qui va suivre permet d'activer une connexion ssh sur un hôte. C'est à dire que l'on va pouvoir prendre accès à un routeur, par exemple, simplement en entrant cette commande ,le nom et le mot de passe que l'on aura configuré dans les futures étapes.

```
C:\Users\Eleves>C:\>ssh -l {nom de l'utilisateur} {adresse à contacter}
```

Base de la configuration d’un appareil cisco:

Changer de mode d’utilisateur:

Dans un appareils cisco il y a différents mode d’utilisateur. Au démarrage nous sommes en mode «Utilisateur». Ensuite on doit passer en mode de configuration globale ou mode «Privilège». Il permet d’utiliser plus de commandes que le mode précédent:

```
Switch>enable
```

Résultat:

```
Switch#
```

Enfin il y a le mode de «Configuration Globale». Celui-ci nous permettra la gestion des machines, cependant si vous souhaitez utiliser les commandes des modes précédents il vous faudra retourner dans ces modes ou alors ajouter le mot clé «do» au début de votre commande.

```
Switch#configure terminal
```

Résultat:

```
Switch(config)#
```

Changer nom de la machine:

Pour un soucis d’organisation on modifie le nom que la machine va afficher pour pouvoir plus facilement l’identifier.

```
Switch(config)#hostname {nom de la machine}
```

Exemple:

```
Switch(config)#hostname SW2
```

Résultat:

```
SW2(config)#
```

Dorénavant dans les exemples notre commutateur portera le nom SW2

Configuration des interfaces physiques :

Après s’être mis en mode Configuration Globale on va pouvoir commencer

Ensuite, examinez les interfaces à configurer et entrez dans le mode de configuration spécifique à chaque interface avec la commande suivante :

```
Switch(config)#interface {nom de l'interface} //rentrer dans la configuration d'une interface
Switch(config)#interface  range {nom des interfaces} //rentrer dans la configuration de plusieurs interfaces
```

Exemple:

Voici des exemples pour la mise en œuvre de ces commandes, pour cette exemple on va prendre en compte des prises FastEthernet que l'on va réduire en f0/x:

```
SW2(config)#interface f0/1 //rentrer dans la configuration de l'interface 1
SW2(config)#interface  range f0/1-24 //rentrer dans la configuration des interfaces 1 à 24
```

PS:

Il existe aussi une autre commande qui peut offrir un gain de temps. Lorsque vous tapez une commande non-valide, de base, l'appareil va penser que c'est un nom de domaine, et il va donc effectuer une recherche, qui peut prendre plusieurs dizaines de secondes. Cette commande permet d'annuler ces recherches et donc de gagné du temps.

```
SW1(config)#no ip domain-lookup
```

Configuration d'un commutateur:

En premier lieu nous allons configurer les commutateurs. Un commutateur permet de relier les différents hôtes d'un réseau et va se charger d'envoyer les données au routeur. Pour les exemples qui vont suivre nous allons configurer le commutateur «SW2», dans le réseau A.

Il y aura 2 parties principales dans cette partie:

-la configuration de tous ce qui concerne le transport des données

-la configuration de la sécurité

Configuration d'une interface virtuel :

Les interfaces virtuel permettent de configurer l'adresse du commutateur. Elles sont nommées vlan dans la console.

```
Switch(config)#interface vlan{numéro du vlan} //rentrer dans la configuration d'un vlan
Switch(config-if)#ip address {Adresse à attribuer} {Masque à attribuer} //configurer l'adresse et le masque du vlan1
Switch(config-if)#no shutdown //allumer le vlan1
```

Exemple:

```
SW2(config)#interface vlan1 //rentrer dans la configuration du vlan1
SW2(config-if)#ip address 193.168.30.126 255.255.255.128 //configurer l'adresse et le masque du vlan1
SW2(config-if)#no shutdown //allumer le vlan1
```

Configuration de la passerelle par défaut:

La passerelle par défaut est l'adresse du routeur auquel le commutateur est connecté. Elle indique au commutateur où l'envoie de données s'effectue.

```
Switch(config)#ip default-gateway {adresse de la passerelle}
```

Exemple:

```
SW2(config)#ip default-gateway 193.168.30.1
```

Configuration de la sécurité:

Maintenant que toutes les connections sont effectuées dans notre commutateur il faut les tester, pour cela il faut vous rendre à la fin de ce document pour voir comment tester les connections. Actuellement nous configurer toutes la sécurité du commutateur.

Mot de passe du mode Privilège:

En premier lieu nous allons configurer le mot de passe qui sera demandé quand vous essaierais de passer en mode Privilège.

```
Switch(config)#enable secret {mot de passe}
```

Pour cette commande il y a deux options différentes, vous pouvez mettre secret ou password, la différence est que secret permet de l'encrypter de base qu'avec password il n'y aura pas cette encryptage automatique.

```
SW2(config)#enable secret cisco
```

Cryptage des mots de passe:

Cette option permet de crypté tous les mots de passe automatiquement

```
Switch(config)#service password-encryption
```

Configuration SSH:

Le SSH est un système de sécurité du commutateur. Il nécessite plusieurs commande présenté ci-dessous.

```
 SW1(config)#ip domain-name {nom de domaine} //configuration du nom de domaine
 SW1(config)#crypto key generate rsa //génération d'une clé de cryptage, ensuite l'appareil vous demandera la taille de la clef. Nous mettrons 1024 pour une meilleur sécurité
 SW1(config)#username {nom d'utilisateur} password {mot de passe} //création d'un utilisateur
 SW1(config)#line vty 0 4 //ligne virtuel à utiliser
 SW1(config-line)#transport input ssh //définit le protocole à utiliser
 SW1(config-line)#login local //demandera obligatoirement un utilisateur lors d'une connexion SSH
 SW1(config-line)#exec-timeout {temps en minutes} //temps où le commutateur peu rester connecté sans être  utiliser avant la mise en veille
```

Configuration d'un routeur :

Le routeur permet de communiquer entre les différents réseaux. Dans les exemples qui vont suivre nous allons configurer le routeur «R1». Il fait la passerelle entre 4 réseaux:

- Réseau A
- Réseau B
- Réseau G
- Réseau I

Pour configurer les interfaces il suffit de se référer aux commandes disponibles au début du document, en adaptant bien les interfaces et les adresses.

Configuration des routes statiques :

Les routes statiques permettent au routeur d'envoyer les informations vers un certain réseau en fonctions des données dans le message à envoyer. Nous allons créer une table de routage manuellement pour être sûre de la destinations de nos paquets.

```
Router(config)#ip route {Adresse du réseau à atteindre} {Masque du réseau à atteindre} {Adresse du routeur à joindre}
```

Exemple:

Comme exemple nous allons configurer la route pour accéder au réseau E

```
R1(config)#ip route 193.168.31.96 255.255.255.224 193.168.31.161
```

Il est aussi nécessaire de configurer des routes par défauts. Celle-ci permettent en cas de panne sur une ligne, de communiquer tous de même par le réseau en prenant un chemin plus long. Par exemple si on veux communiquer au R2 alors que la ligne R1-R2 est coupé il faut configurer une route par défaut sur la ligne R1-R3.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 {Adresse du router par lequel passer}
```

Exemple :

```
R1(config)#ip route 0.0.0.0 0.0.0.0 193.168.31.161
```

Configuration de la sécurité :

Pour la sécurité du routeur il y aura plus de commandes car celui-ci est connecté à des réseaux externes.

Port console:

Pour éviter que n'importe qui puisse se connecter sur le port console de notre routeur on va y mettre un mot de passe.

```
Router(config)#line console 0 //se connecter au port console
Router(config-line)#password {mot de passe} //définir un mot de passe
Router(config-line)#login //demandera le mot de passe
```

Interfaces virtuels:

Il est aussi utile de configurer des mots de passes pour la connections aux interfaces virtuels.

```
Router(config)#line vty 0 4 //se connecter au port console
Router(config-line)#password {mot de passe} //définir un mot de passe
Router(config-line)#login //demandera le mot de passe
```

Taille des mots de passe

On peut aussi définir une taille de mot de passe minimum que les utilisateurs utiliseront.

```
Router(config)#security password min-length {taille du mot de passe en caratère}
```

Configurer le SSH :

```
Router(config)#username {nom d'utilisateur} password {mot de passe}
Router(config)#ip domain-name {nom de domaine}
Router(config)#crypto key generate RSA
Router(config)#login block-for {temps en s}
Router(config)#line vty 0 4
Router(config)#transport input ssh
Router(config)#login local
Router(config)#exec-timeout {temps en minutes}
Router(config-line)#ip ssh version 2
```

Exemples:

```
R1(config)#username toto password toto //définir un utilisateur et son mot de passe
R1(config)#ip domain-name ciel.com //définir un nom de domaine
R1(config)#crypto key generate RSA //générer une clé de cryptage ensuite l'appareil vous demandera la taille de la clef. Nous mettrons 1024 pour une meilleur sécurité
SW1(config)#line vty 0 4 //ligne virtuel à utiliser
 SW1(config-line)#transport input ssh //définit le protocole à utiliser
 SW1(config-line)#login local //demandera obligatoirement un utilisateur lors d'une connexion SSH
 SW1(config-line)#exec-timeout 5 //temps où le commutateur peu rester connecté sans être utiliser avant la mise en veille
SW1(config-line)#ip ssh version 2 //Passer la version du ssh en version2
```