TP n°4 : Connexion ssh sur un routeur Cisco et mise en place des protocoles de routage RIP et OSPF (En réel).

Durée : 2h

Objectif principal

Être capable d'activer le service SSH d'un routeur Cisco.

Être capable de configurer en réel, via le port console et avec ssh, en ligne de commande, les interfaces IPv4 de routeurs Cisco.

Être capable de mettre en place en réel en ligne de commande les protocoles de routage dynamique RIP et OSPF sur des routeurs Cisco.

Vous devez noter avec grand soin toutes les commandes de configuration dans votre CR, vous aurez à le refaire en CTP et en SAÉ.

MÉMOS (Cheat Sheets)

RIP | OSPF (source packetlife.net)

En groupes

- Organisez vous avec l'enseignant pour mettre en place en réel cette configuration sur les routeurs et commutateurs en J0-01 (LR1) ou J0-09 (LR2).

Par défaut : Faites 2 groupes disposant chacun de 3 switchs et 3 routeurs

Vous serez donc environ 6 par groupes, 2 par machine/switch/routeur à configurer

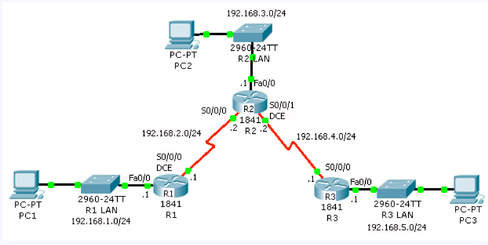
Compte rendu par groupe

Vous devez obligatoirement déposer chacun en fin de séance un compte rendu (CR) illustré de votre groupe au format **TP4.[pdf|odt|docx]** pour ce TP sur Moodle. Vous pouvez compléter ce CR après la séance en déposant un nouveau fichier **TP4v2.[pdf|odt|docx]**.

Vos **CR seront vos uniques documents autorisés en CTP**. Il est donc très important de bien y faire figurer **tous les détails** (commandes précises, notions importantes, manips importantes, ...).

Présentation

- Reprenez le réseau fait dans la partie précédente sur papier en y ajoutant les **noms des ports où sont connectés vos machines**
  - pour chaque machine : le nom de port sur le bandeau blanc où est branchée la deuxième carte réseau pour retrouver ce port dans la baie pour le câblage avec le switch), les **noms des switchs et des routeurs que vous allez utiliser en réel** (valider avec l'enseignant.



Périphérique	Interface	Adresse IP	Passerelle par défaut
R1	Fa0/0	192.168.1.1	
	S0/0/0	192.168.2.1	
R2	Fa0/0	192.168.3.1	
	S0/0/0	192.168.2.2	
	S0/0/1	192.168.4.2	
R3	Fa0/0	192.168.5.1	
	S0/0/0	192.168.4.1	
PC1	carte réseau	192.168.1.10	192.168.1.1
PC2	carte réseau	192.168.3.10	192.168.3.1
PC3	carte réseau	192.168.5.10	192.168.5.1

Connexion ssh pour configurer les routeurs

Vous allez d'abord configurer les routeurs pour qu'ils soient configurables via ssh (plus sécurisé et plus pratique que via le câble bleu sur port série, même si pour la première fois il vous faudra utiliser le câble bleu pour paramétrer la connexion ssh).

Contrairement à packettracer, vous ne pouvez plus configurer graphiquement les équipements. Il faut le faire en mode console avec l'IOS.

- Comme il n'y a pas encore de connexion ssh, utilisez Minicom pour vous connecter sur les équipements sur leurs ports consoles avec le câble bleu Cisco. Faites le depuis votre machine physique, pas besoin d'une machine virtuelle en mode administrateur, après avoir fait les réglages juste faire **sortir** (effectivement vous ne pourrez pas les enregistrer - dans ce cas il faut les droits d'administration et utiliser pour cela une machine virtuelle - mais ils seront pris en compte pour cette session).
  - Lancez minicom avec l'option -s pour faire les réglages du terminal sur port série (ttyS0) suivants : Débits/Parité/Bits : 9600 8N1, contrôle de flux matériel : Non, contrôle de flux logiciel : Non.

```
Port série : /dev/ttyS0
Débits/Parité/Bits : 9600 8N1
Contrôle de flux matériel : Non
Contrôle de flux logiciel : Non
```

  - Répondre "no" à la question "Would you like to enter the initial configuration dialog? (yes/no)".
  - Vous arrivez alors au prompt mode utilisateur:

```
router>
```

- Pour configurer ssh vous pouvez alors effectuer les opérations suivantes
  - Passez en mode configuration :

```
router> en
router# conf t
router(config)#
```

  - La création d'un nom d'hôte et d'un nom de domaine étant nécessaire à la configuration d'une connexion SSH, pour ce TP choisissez un nom en accord avec le plan, par exemple le nom R1 (pour le premier routeur R1) et pour le nom de domaine r201.fr (Ce nom serait bien sûr à mettre en accord avec votre domaine réel).

```
router(config)#hostname R1
R1(config)#ip domain-name r201.fr
```

  - Générez ensuite une paire de clés RSA de 1024 bits (un exemple de chiffrement asymétrique, plus de détails dans la suite de la formation R&T, pour l'instant retenez que la clé publique - tout le monde peut la connaître - sert à chiffrer des informations et la clé privée - tenue bien secrète quant à elle - sert à déchiffrer les informations chiffrées avec la clé publique). Cette paire de clés sera utilisée pour chiffrer les connexions ssh du routeur.

```
R1(config)#crypto key generate rsa modulus 1024
```

  - Activez ensuite la version 2 du protocole SSH (plus sécurisée que la version 1).

```
R1(config)#ip ssh version 2
```

  - Configurez ensuite les lignes virtuelles (VTY) du routeur pour n'accepter et ne lancer que des connexions SSH, et utiliser des logins locaux au routeur (comptes locaux).

```
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#transport output ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#
```

  - Ajoutez enfin un compte local qui va pouvoir se connecter en ssh sur le routeur avec un niveau de privilège haut pour pouvoir entrer en mode configuration, par exemple le login toto avec le mot de passe progtr00.

```
R1(config)#username toto privilege 15 secret progtr00
```

Rappel, **ne surtout pas sauvegarder cette config** (**pas de write ni de copy running-config startup-config**) pour permettre aux groupes suivants de démarrer sereinement leurs TP avec des routeurs prêts sans configuration à enlever.

  - Pour tester la connexion ssh depuis PC1, il vous faut configurer l'interface GigaEthernet vers PC1 avec la bonne adresse (192.168.1.1), rappel :

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

  - Pour vérifier la bonne configuration :

```
R1(config)#exit
R1#show ip int brief
```

  - Configurez ensuite une machine "PC1" (@IP 192.168.1.10) c'est-à-dire pour vous en réel une machine virtuelle mode bridge sur la deuxième carte réseau de votre machine physique (généralement eth1 mais vérifiez) et testez depuis cette machine une connexion ssh sur le routeur (login toto, mot de passe progtr00)

Vérifiez d'abord qu'un ping fonctionne entre la machine et le routeur, puis sur la machine testez cette connexion ssh

```
ssh toto@192.168.1.1
```

Voici comment vous devez configurer votre client ssh sur un PC, notamment les chiffrements ou "cyphers" en anglais, et échanges de clés possibles (cette partie sera vue en 2e année), pour pouvoir vous connecter en ssh sur un équipement Cisco du département.

Éditez le fichier de configuration ssh de votre machine

```
sudo nano /etc/ssh/ssh_config
```

pour décommenter les deux lignes suivantes

```
# MACs hmac-md5,hmac-sha1,hmac-sha2-256,umac-64@openssh.com,hmac-ripemd160
# Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
```

et ajouter à la fin les deux lignes suivantes

```
HostKeyAlgorithms ssh-dss,ssh-rsa
KexAlgorithms +diffie-hellman-group1-sha1,diffie-hellman-group14-sha1
```

(source)

- Configurez ensuite l'autre interface série (Serial) du routeur R1 192.168.2.1 puis les autres routeurs R2 et R3 et les PCC 2 et 3.
- À vous de configurer vos machines et vos routeurs avec RIP puis OSPF (rien à faire sur les switchs) pour faire fonctionner ce réseau.
- Insérez dans votre compte rendu les captures des pings réussis entre toutes vos machines.
- Insérez également une capture de toutes les tables de routage.

"exit" ou "end" vous permettent de remonter les différents modes

- Mode utilisateur (prompt >)

```
R1>
```

- Mode utilisateur privilégié (prompt #)

```
R1#
```

- Mode de configuration globale (prompt (config)#)

```
R1 (config)#
```

- Mode de configuration d'une interface (prompt (config-if)#)

```
R1 (config-if)#
```

- ...

Par rapport à la documentation additionnelle que vous pourriez lire, **NE SURTOUT PAS SAUVEGARDER VOTRE CONFIG** avec des commandes comme write ou copy running-config startup-config pour permettre aux groupes suivants de démarrer sereinement leurs TP avec des routeurs prêts sans configuration à enlever.

N'oubliez pas de déposer votre compte rendu.

SYNTHÈSE

À l'issue de ce TP :

- Vous êtes capable de configurer en réel via le port console et en ssh des routeurs Cisco avec notamment des protocoles de routage dynamique comme RIP ou OSPF.
- Rappel : vous savez également configurer des switchs et vlan via la ressource R103.
- Vous avez fait un mémento de toutes les commandes importantes dans votre CR pour pouvoir refaire cette manip en CTP.

(Les commandes font également l'objet de questions aux DS et évaluations écrites)) (Un mémento vlan)