R201 TP 4 :

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

1. 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).

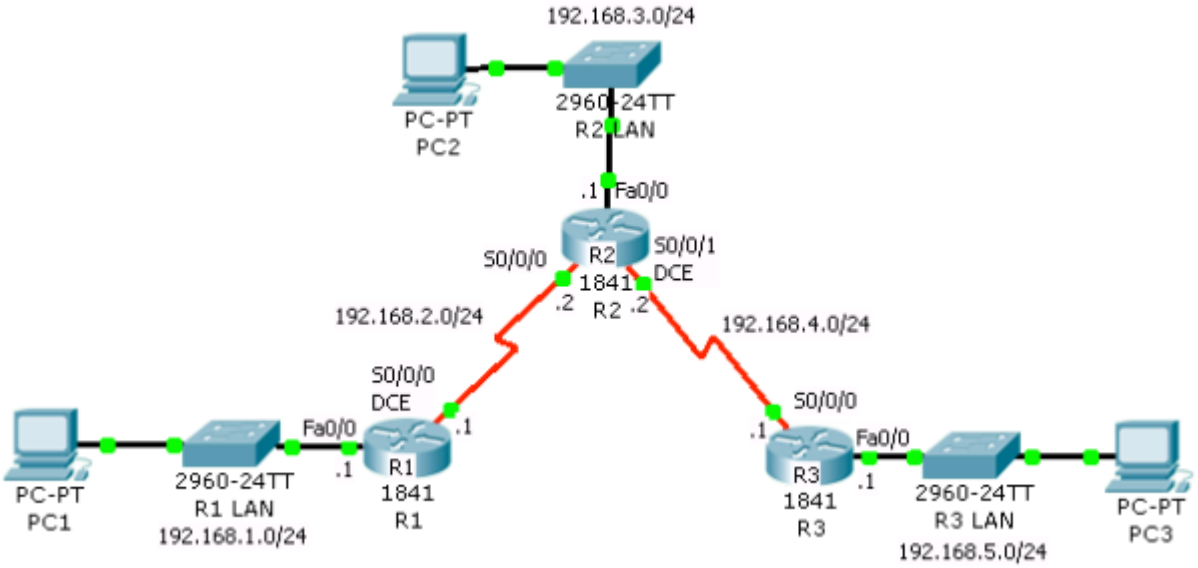
Par défaut : Faites 2 groupes disposant chacun de 3 switchs et 3 routeurs

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

2. 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.



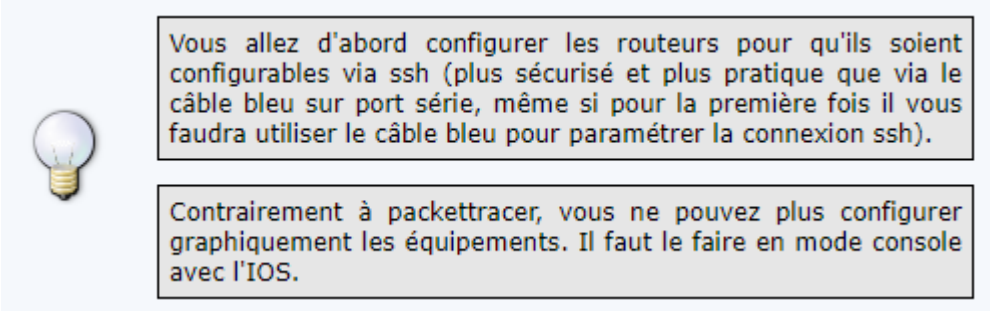
Périphérique	Interface	Adresse IP	Passerelle par défaut
R1	Fa0/0	192.168.1.1	
	S0/0/0	192.168.2.1	
R2	Fa0/0	192.168.3.1	
	S0/0/0	192.168.2.2	
	S0/0/1	192.168.4.2	
R3	Fa0/0	192.168.5.1	
	S0/0/0	192.168.4.1	
PC1	carte réseau	192.168.1.10	192.168.1.1
PC2	carte réseau	192.168.3.10	192.168.3.1
PC3	carte réseau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

3. Configuration ssh pour configurer les routeurs :

Configuration des routeurs :

```
+-----------------------------------------------------------------------+
| A -                Port série : /dev/ttyS0                            |
| B - Emplacement fichier verr. : /var/lock                             |
| C -     Prog. d'appel entrant :                                       |
| D -     Prog. d'appel sortant :                                       |
| E -         Débit/Parité/Bits : 9600 8N1                              |
| F - Contrôle de flux matériel : Oui                                   |
| G - Contrôle de flux logiciel : Oui                                   |
| H -     RS485 Enable      : No                                        |
| I -   RS485 Rts On Send   : No                                        |
| J -  RS485 Rts After Send : No                                        |
| K -  RS485 Rx During Tx   : No                                        |
| L -  RS485 Terminate Bus  : No                                        |
| M - RS485 Delay Rts Before: 0                                         |
| N - RS485 Delay Rts After : 0                                         |
|                                                                       |
|    Changer quel réglage ?                                             |
+-----------------------------------------------------------------------+
```

Question 1 :



- 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 : Oui, contrôle de flux logiciel : Oui.

- **Port série : /dev/ttyS0**
  Débits/Parité/Bits : 9600 8N1
  Contrôle de flux matériel : Oui
  Contrôle de flux logiciel : Oui

- 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

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

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

```
R1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R1.r201.fr

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Feb 19 11:07:22.131: %SSH-5-ENABLED: SSH 1.99 has been enabled
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)#ip ssh version 2
R1(config)#line vty 0 4
R1(config-line)#trans
R1(config-line)#transport input ssh
R1(config-line)#transport output ssh
R1(config-line)#login local
R1(config-line)#exit
```

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

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

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)#

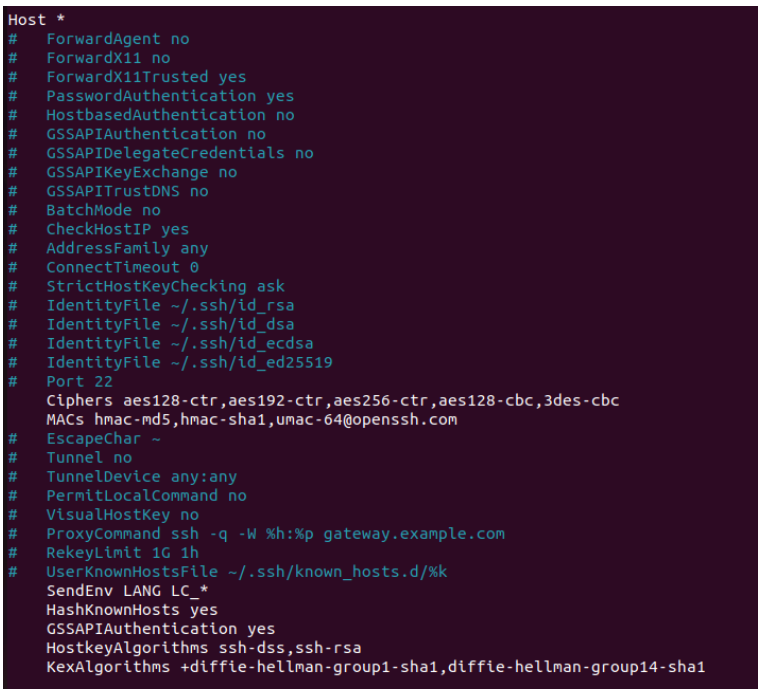
  Pour vérifier la bonne configuration :

- **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)

Il faut d'abord pour que le ssh fonctionne configurer le dossier de config du ssh pour autoriser des méthodes d'échange ssh avec la commande :

sudo nano /etc/ssh/ssh_config



Comme on peut le voir ci-dessus nous avons activer les lignes :

Ciphersaes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc

MACs hmac-md5,hmac-sha1,umac-64@openssh.com

Ainsi que rajouter les lignes suivantes pour autoriser certains échangent qui n'était pas autorisé :

HostkeyAlgorithms ssh-dss,ssh-rsa

KexAlgorithms +diffie-hellman-group1-sha1,diffie-hellman-group14-sha1

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**

Pour la connexion ssh, le chiffrement (ou "cypher" en anglais) utilisé par défaut par le client ssh n'est pas toujours accepté par le routeur, il faut dans ce cas forcer l'utilisation d'un chiffrement autorisé, **par exemple :**

ssh -c aes128-cbc login@ip

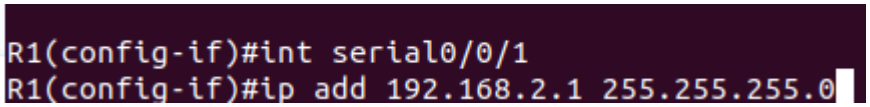
```
administrateur@rt-mv:~$ ssh toto@192.168.1.1
(toto@192.168.1.1) Password:
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#do sh run
Building configuration...

Current configuration : 1241 bytes
!
! Last configuration change at 11:34:19 UTC Mon Feb 19 2024
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
!
ip domain name r201.fr
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
```

Comme on peut le voir la connexion ssh fonctionne correctement avec le routeur R1

Le fonctionnement de ssh sera approfondi dans la suite de votre formation R&T.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



RIP :

- Mode utilisateur (prompt >)
- **R1>**
  Mode utilisateur privilégié (prompt #)
- **R1#**
  Mode de configuration globale (prompt (config)#)
- **R1 (config)#**
- **R1(config)#** router rip
- **R1(config-router)#**network 192.168.1.0
- **R1(config-router)#**network 192.168.2.0
- **R1#**show ip route
- **R1#**exit

```
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
R1(config-router)#do ip route
                     ^
% Invalid input detected at '^' marker.

R1(config-router)#do sh ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
```

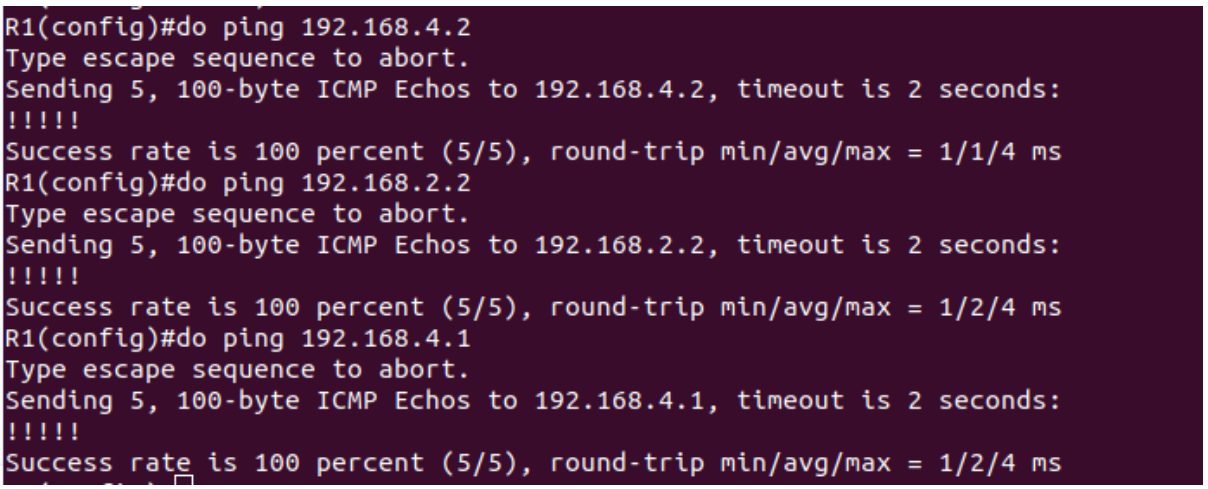
```
R1(config-if)#do ping 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1(config-if)#do ping 192.168.4.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1(config-if)#do ping 192.168.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
R1(config-if)#do ping 192.168.4.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Ça marche super bien 👍

OSPF :

- **R1(config)#**no router rip
- **R1(config)#**router ospf 1
- **R1(config-router)#**network 192.168.1.0 0.0.0.255 area 0
- **R1(config-router)#**network 192.168.2.0 0.0.0.255 area 0
- **R1#**show ip route
- **R1#**exit

```
R1(config-if)#no router rip
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 192.168.2.0 0.0.0.255 area 0
R1(config-router)#do sh ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Serial0/0/1
L        192.168.2.1/32 is directly connected, Serial0/0/1
```



Sa marche super bien aussi 👍 👋

apt-get install -y ipcalc