

# TP2 : configuration des paramètres de base d'un routeur

## Sommaire

|   |   |
|---|---|
| 1. Partie 1 : Configuration de la topologie et initialisation des périphériques.....  | 2 |
| 2. Partie 2 : Configuration des périphériques et vérification de la connectivité..... | 2 |
| 3. Partie 3 : Affichage des informations du routeur.....                              | 9 |

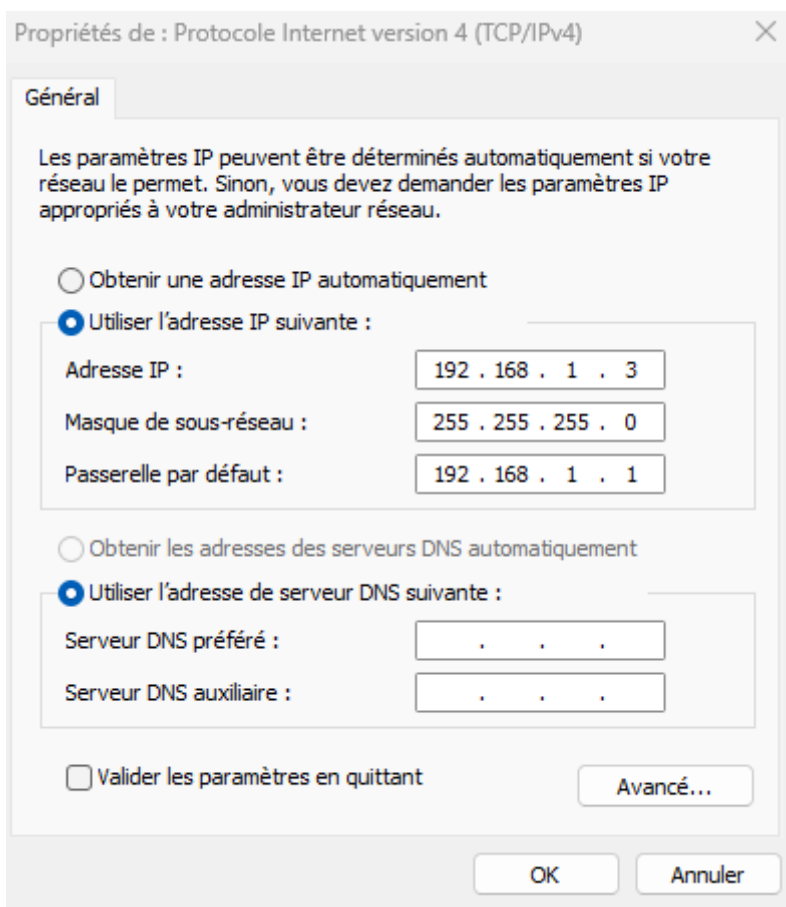
# 1. Partie 1 : Configuration de la topologie et initialisation des périphériques

Câblage du réseau conformément à la topologie et mettez sous tension tous les périphériques de la topologie.

# 2. Partie 2 : Configuration des périphériques et vérification de la connectivité

Étape 1 : Configurez les interfaces des ordinateurs (adresse IP, masque de sous-réseau et passerelle par défaut sur PC-A. ainsi que sur PC-B)

PC-A :



PC-B :

On ne peut pas mettre le screen mais on fait pareil pour le PC-B sauf que l'on met 192.168.0.3 pour l'ip, 255.255.255.0 pour le masque et pour la passerelle par défaut on met 192.168.0.1.

## Étape 2 : Configuration du routeur

On accède au routeur par la console et on active le mode d'exécution privilégié (enable)

```
R1>enable
Password:
R1#
```

Passage en mode de configuration globale (config)

```
R1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
```

On attribue un nom de périphérique au routeur (il s'appeler déjà R1 je l'ai donc renommé Routeur pour après le renommé R1 pour pouvoir tester la commande)

```
R1(config)#hostname Routeur
Routeur(config)#hostname R1
R1(config)#
```

On désactive la recherche DNS pour empêcher le routeur d'essayer de traduire les commandes mal saisies comme s'il s'agissait de noms d'hôtes

```
R1(config)#no ip domain-lookup
R1(config)#
```

10 caractères minimum doivent être utilisés pour les mots de passe

```
R1(config)#security passwords min-length 10
R1(config)#
```

On attribue ciscoenpass comme mot de passe chiffré d'exécution privilégié

```
R1(config)#enable secret ciscoenpass
R1(config)#
```

On attribue ciscoconpass en tant que mot de passe accès console, on définit un délai d'attente, on active la connexion et on ajoute la commande logging synchronous. La commande logging synchronous synchronise le débogage et les résultats du logiciel Cisco IOS, et empêche que ces messages n'interrompent nos entrées au clavier

```
R1(config)#line con 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exec-timeout 5 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
```

On attribue ciscovtpass en tant que mot de passe vty, on définit un délai d'attente, on active la connexion et on ajoute la commande logging synchronous

```
R1(config)#line vty 0 4
R1(config-line)#password ciscovtpass
R1(config-line)#login
R1(config-line)#exec-timeout 5 0
R1(config-line)#logging synchronous
R1(config-line)#exit
R1(config)#
```

On chiffre tous les mots de passe en clair

```
R1(config)#service password-encryption
R1(config)#
```

On créer une bannière qui avertit que la configuration du routeur a été modifiée

```
R1(config)#banner motd #Configuration modifiée#  
R1(config)#
```

On configure une adresse IP et une description d'interface. On active les deux interfaces sur le routeur

```
R1(config)#int g0/0  
R1(config-if)#description Connexion a PC-B  
R1(config-if)#ip address 192.168.0.1 255.255.255.0  
R1(config-if)#no shutdown  
R1(config-if)#int g0/1  
R1(config-if)#description Connexion a S1  
R1(config-if)#ip address 192.168.1.1 255.255.255.0  
R1(config-if)#no shutdown  
R1(config-if)#^Z  
R1#
```

On enregistre la configuration en cours dans le fichier de configuration initiale

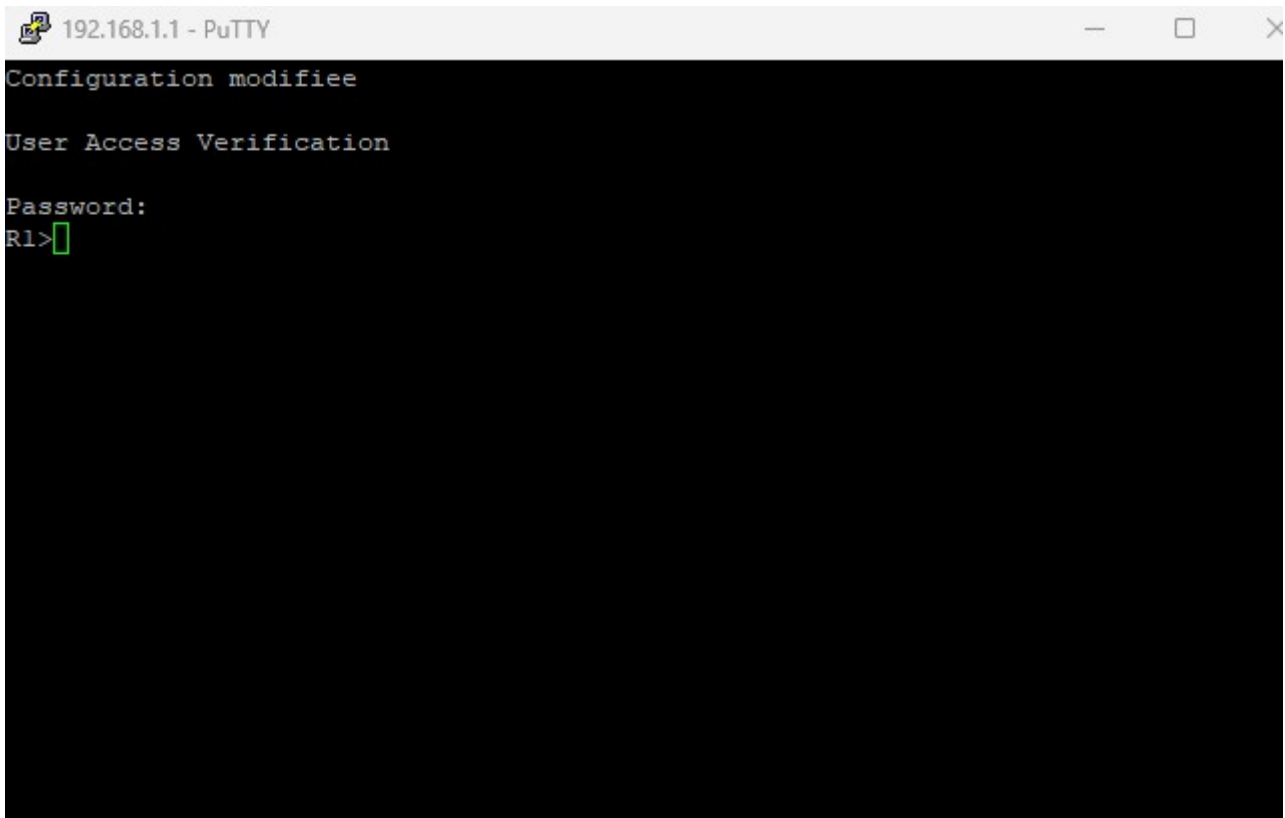
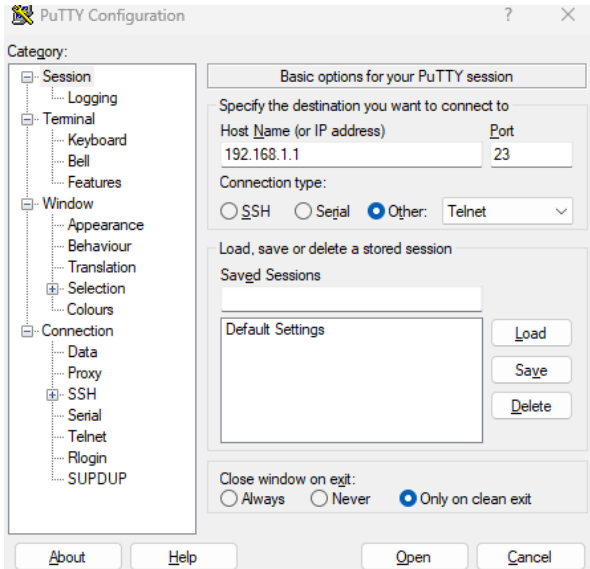
```
R1#copy running-config startup-config  
Destination filename [startup-config]?  
Building configuration...  
[OK]  
R1#
```

Étape 3 : Vérifiez la connectivité du réseau

On envoie une requête ping à PC-B à partir d'une invite de commande sur PC-A

```
C:\Users\mballester>ping 192.168.0.1  
  
Envoi d'une requête 'Ping' 192.168.0.1 avec 32 octets de données :  
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=255  
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=255  
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=255  
Réponse de 192.168.0.1 : octets=32 temps<1ms TTL=255  
  
Statistiques Ping pour 192.168.0.1:  
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),  
Durée approximative des boucles en millisecondes :  
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

On accède à distance à R1 à partir de PC-A à l'aide du client Telnet de Putty. On saisie l'adresse IP 192.168.1.1 de l'interface G0/1 et on s'assure que Telnet soit sélectionné



## Étape 4 : Configurez le routeur pour l'accès SSH

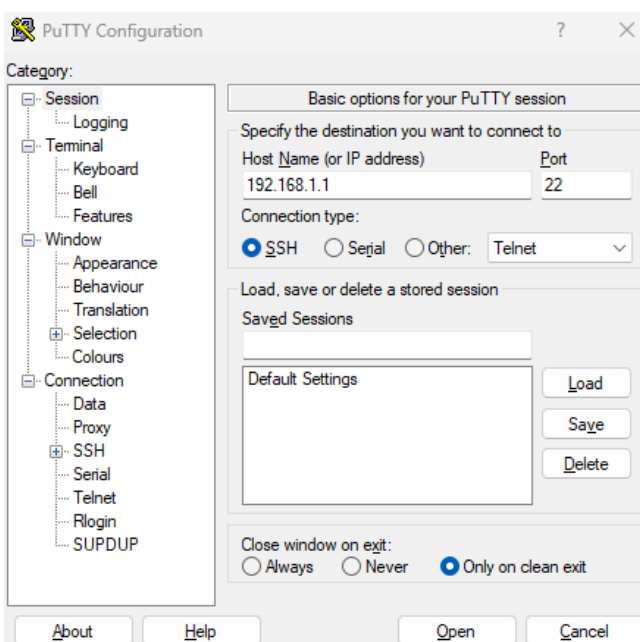
On active les connexions SSH et on crée un utilisateur dans la base de données locale du routeur

```
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip domain-name exupery.local
R1(config)#crypto key generate rsa modulus 1024
The name for the keys will be: R1.exupery.local

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 3 seconds)

R1(config)#
Jan 21 06:29:48.267: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#username admin privilege 15 secret adminvtypass
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#^Z
R1#
```

On accède à distance à R1 à partir de PC-A à l'aide du client SSH de Putty. On saisit l'adresse IP de l'interface G0/1 de R1 (192.168.1.1) et on s'assure que SSH soit sélectionné. Puis enfin on se connecte avec le nom d'utilisateur admin et le mot de passe adminvtypass



```
192.168.1.1 - PuTTY
login as: admin
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Configuration modifiée
R1#
```

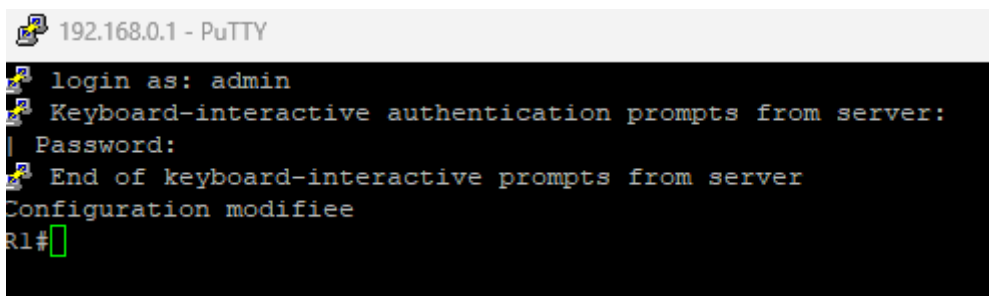
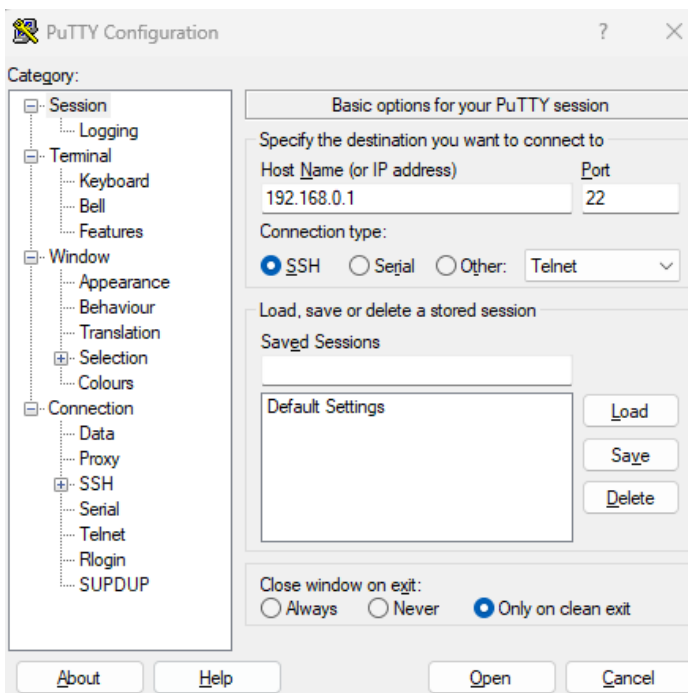
On consulte la configuration du routeur à l'aide de la commande show run

```
R1#show run
Building configuration...

Current configuration : 1868 bytes
!
! Last configuration change at 06:30:48 UTC Wed Jan 21 2026
! NVRAM config last updated at 05:55:36 UTC Wed Jan 21 2026
! NVRAM config last updated at 05:55:36 UTC Wed Jan 21 2026
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
security passwords min-length 10
enable secret 4 pz9A9n/f8wxdG3elkEn8T6zR/eMGkCmgWdoDscKwgGA
enable password 7 082C485E
!
no aaa new-model
memory-size iomem 15
!
no ipv6 cef
ip source-route
ip cef
!
!
!
!
!
no ip domain lookup
ip domain name exupery.local
multilink bundle-name authenticated
!
!
crypto pki token default removal timeout 0
!
!
!
license udi pid CISCO2901/K9 sn FCZ1648C1EN
!
!
username admin privilege 15 secret 4 N8MFSN4ih5aPHwGKWri82fJTo5xdZQ/0.3PlqOUqRFk
!
```

### 3. Partie 3 : Affichage des informations du routeur

À l'aide de Putty sur PC-B, on ouvre une session SSH avec R1 à l'adresse IP 192.168.0.1



On utilise la commande show version pour répondre aux questions sur le routeur

```
R1#show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M4, REL
EASE SOFTWARE (fcl)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Tue 20-Mar-12 18:57 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fcl)

R1 uptime is 2 hours, 45 minutes
System returned to ROM by power-on
System restarted at 04:53:50 UTC Wed Jan 21 2026
System image file is "flash0:c2900-universalk9-mz.SPA.151-4.M4.bin"
Last reload type: Normal Reload

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wvl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco CISCO2901/K9 (revision 1.0) with 450560K/73728K bytes of memory.
Processor board ID FCZ1648C1EN
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)
```

**Quel est le nom de l'image IOS exécutée par le routeur ?**

c2900-universalk9-mz.SPA.151-4.M4.bin

**Quelle quantité de mémoire vive non volatile (NVRAM) le routeur possède-t-il ?**

Il possède 255K de mémoire vive non volatile

**Quelle quantité de mémoire Flash le routeur possède-t-il ?**

Il possède 250880K de mémoire flash

**Quel est le processus de démarrage du routeur lors du prochain redémarrage ?**

Le processus de redémarrage du routeur lors du prochain redémarrage est 0x2102

**Étape 3 : Affichez la configuration initiale.**

**Comment les mots de passe sont-ils présentés dans les résultats ?**

Les mots de passe sont chiffrés

**Quel est le résultat de l'exécution de cette commande ?**

Le résultat de cette commande est :

```
line vty 0 4
  exec-timeout 5 0
  password 7 094F471A1A0A0106121C053939
  logging synchronous login local
  transport input ssh
!
scheduler allocate 20000 1000
end
```