

LA GESTION DU RÉSEAU

18.1. Les protocoles CDP et LLDP

Les protocoles CDP « **C**isco **D**iscovery **P**rotocol » et LLDP « **L**ink **L**ayer **D**iscovery **P**rotocol » sont des protocoles de la couche 2 du modèle OSI, qui permettent la découverte des voisins directement connectés pour des diagnostics, de la surveillance, de la gestion ou encore de la configuration.

18.1.1. CDP

CARACTÉRISTIQUES :

Acronyme	Cisco Discovery Protocol
Propriétaire	Cisco
Couche OSI	Liaison de données
Mise à jour	Périodique (toutes les 60 secondes)
Temps de maintien (Hold Time)	180 secondes
État	Activé par défaut

COMMANDES CDP :

Affichage de la configuration CDP :

```
R1#show cdp
Global CDP information:
  Sending CDP packets every 60 seconds
  Sending a holdtime value of 180 seconds
  Sending CDPv2 advertisements is enabled
```

- ➡ Période de mise à jour : 60 secondes
- ➡ Temps de maintien : 180 secondes
- ➡ État : Activé (Enabled)

Désactivation du protocole CDP :

```
R1(config)#no cdp run
R1(config)#interface G0/0
R1(config-if)#no cdp enable
```

Activation du protocole CDP :

```
R1(config)#cdp run
R1(config)#interface G0/0
R1(config-if)#cdp enable
```

Affichage de la liste des voisins CDP :

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID         Local Intrfce  Holdtme  Capability  Platform  Port ID
Switch            Gig 0/1       141      S           2960      Fas 0/1
R2                Gig 0/0       141      R           C2900     Gig 0/0
```

Deux voisins CDP :

- ➡ R2 : Routeur (R)
- ➡ Switch : Commutateur (S)

Affichage de la liste des voisins CDP en détail :

```
R1#show cdp neighbors detail
Device ID: R2
Entry address(es):
Platform: cisco C2900, Capabilities: Router
Interface: GigabitEthernet0/0, Port ID (outgoing port): GigabitEthernet0/0
(Résultats omis)
-----
Device ID: Switch
Entry address(es):
Platform: cisco 2960, Capabilities: Switch
Interface: GigabitEthernet0/1, Port ID (outgoing port): FastEthernet0/1
(Résultats omis)
```

Deux voisins :



Le voisin 1 :

- Nom du voisin : **R2**
- Plateforme : **Cisco C2900**
- Type : **Routeur**
- Interfaces **G0/0** ➡ **G0/0**



Le voisin 2

- Nom du voisin : **Switch**
- Plateforme : **Cisco C2960**
- Type : **Commutateur**
- Interfaces **G0/1** ➡ **F0/1**

18.1.2. LLDP :

CARACTÉRISTIQUES :

Acronyme	Link Layer Discovery Protocol
Propriétaire	Non-propriétaire (Norme IEEE 802.1ab)
Couche OSI	Liaison de données
Mise à jour	Périodique (Toutes les 30 secondes)
Temps de maintien (Hold Time)	120 secondes
État	Désactivé par défaut

COMMANDES LLDP :

Affichage de la configuration LLDP :

```
R1#show lldp
% LLDP is not enabled
```

État : Désactivé (not enabled)

```
R1#show lldp
Global LLDP Information:
Status: ACTIVE
LLDP advertisements are sent every 30 seconds
LLDP hold time advertised is 120 seconds
LLDP interface reinitialisation delay is 2 seconds
```

- ➡ État : Actif (ACTIVE)
- ➡ Période de mise à jour : 30 secondes
- ➡ Temps de maintien : 120 secondes

Activation du protocole LLDP :

```
R1(config)#lldp run
```

Désactivation du protocole LLDP

```
R1(config)#no lldp run
```

Affichage de la liste des voisins LLDP :

```
R1#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID      Local Intf    Hold-time    Capability    Port ID
R2             Gig0/0        120          R             Gig0/0
Switch         Gig0/1        120          B             Fa0/1
```

Deux voisins LLDP :

- ➡ R2 : Routeur (R)
- ➡ Switch : Commutateur (B)

Affichage de la liste des voisins LLDP en détail :

```
R1#show lldp neighbors detail
-----
Chassis id: 0001.962C.1001
Port id: Gig0/0
Port Description: GigabitEthernet0/0
System Name: R2
System Description:
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M),
Version 15.1(4)M4, RELEASE SOFTWARE (fc2)
(Résultats omis)
System Capabilities: R
Enabled Capabilities: R
(Résultats omis)
-----
Chassis id: 0002.1601.CB01
Port id: Fa0/1
Port Description: FastEthernet0/1
System Name: Switch
System Description:
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M),
Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
(Résultats omis)
System Capabilities: B
Enabled Capabilities: B
(Résultats omis)

Total entries displayed: 2
```

Deux voisins LLDP :



Le voisin 1 :

- Nom du voisin : R2
- Logiciel : C2900
- Type : Routeur



Le voisin 2 :

- Nom du voisin : Switch
- Logiciel : Cisco C2960
- Type : Commutateur

Activation de la transmission et de la réception des trames LLDP au niveau d'une interface :

```
R2(config)#interface GigabitEthernet0/0
R2(config-if)#lldp transmit
R2(config-if)#lldp receive
```

Désactivation de la transmission et de la réception des trames LLDP au niveau d'une interface :

```
R2(config)#interface GigabitEthernet0/0
R2(config-if)#no lldp transmit
R2(config-if)#no lldp receive
```

18.2. Le protocole NTP

NTP permet de synchroniser les horloges de plusieurs périphériques sur un réseau.



Configuration de l'adresse du serveur NTP au niveau du client S1 :

```
S1(config)#ntp server 192.168.1.1
```

Configuration du routeur comme serveur NTP :

```
R1(config)#ntp master
```

Configuration de l'heure et la date au niveau du serveur NTP (R1) :

```
R1#clock set 20:34:00 August 15 2022
```

Configuration de l'adresse IP du client NTP :

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.10 255.255.255.0
S1(config-if)#no shutdown
```

Configuration de la passerelle par défaut du client NTP :

```
S1(config)#ip default-gateway 192.168.1.1
```


Vérification de la configuration NTP :

```
S1#show ntp status
Clock is synchronized, stratum 9, reference is 192.168.1.1
(Résultats omis)
```

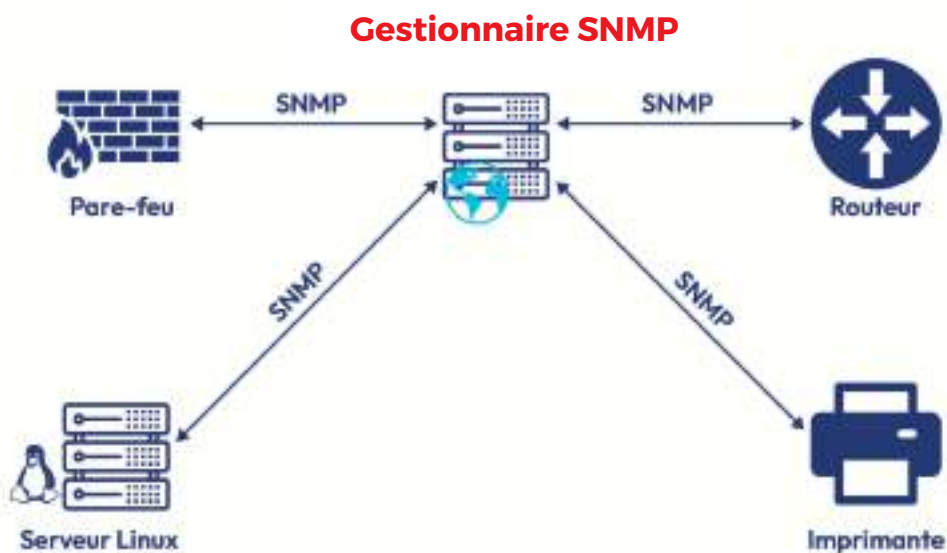
```
S1#show ntp associations
address      ref clock    st when poll reach delay offset disp
*~192.168.1.1 127.127.1.1 8 1 16 37 0.00 0.00 0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

18.3. Le protocole SNMP




18.3.1. Définition :

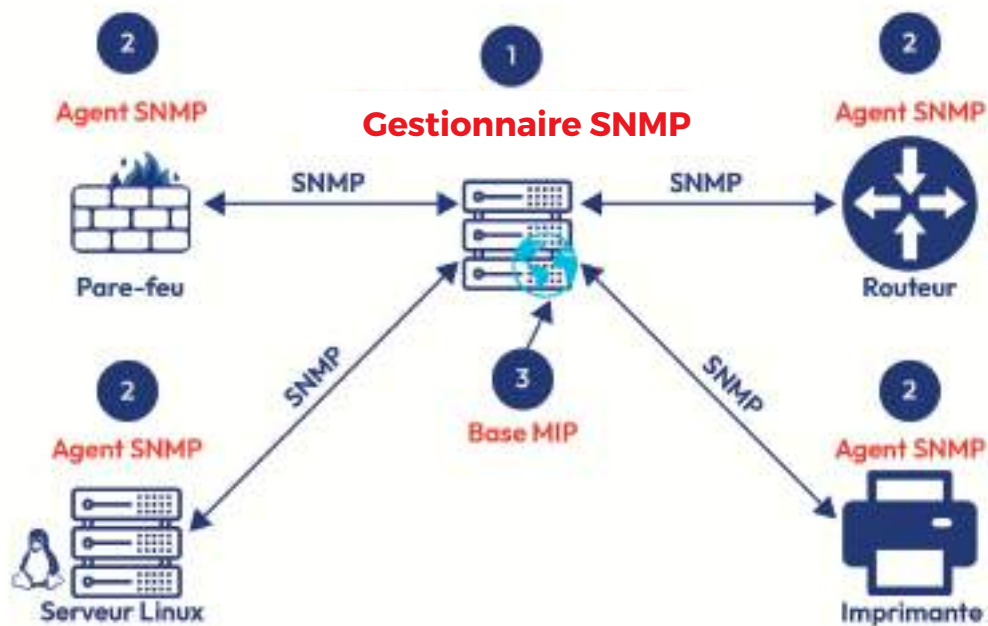
SNMP (Simple Network Management Protocol) est un protocole utilisé pour gérer et surveiller les équipements réseau tels que les routeurs, les commutateurs et les serveurs.

Il permet aux administrateurs réseau de récupérer des informations sur l'état des équipements et de recevoir des alertes en cas d'anomalies.



18.3.2. Les composants SNMP

-  **Gestionnaire SNMP** : (Nagios...)
-  **Agents SNMP** : routeurs, commutateurs, ordinateurs, etc.
-  **La base de données MIB** : elle contient toutes les variables à surveiller (Interfaces, nom des périphériques, protocoles de routage, etc.)



Les agents SNMP sont des programmes installés sur les équipements réseau qui collectent les informations sur l'état de ces derniers et les transmettent aux outils de gestion de réseau.

Les MIB (Management Information Base) sont des bases de données qui décrivent les informations qui peuvent être collectées par les agents SNMP.

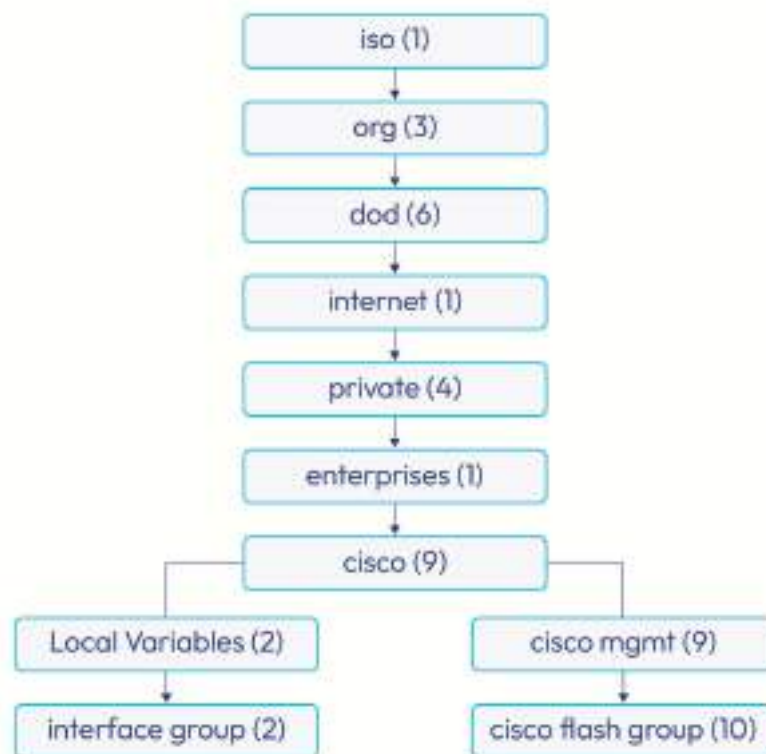
Les MIB définissent les variables SNMP accessibles et les valeurs qu'elles peuvent prendre.

Les OID (Object Identifier) sont des identificateurs uniques qui permettent de spécifier les variables SNMP dans les MIB.

Chaque variable SNMP a un OID associé qui permet de l'identifier de manière unique dans le réseau.

Remarque :

Chaque objet ou variable MIB est identifié par un OID (Object ID)



Par exemple : .1.3.6.1.2.1.1.5.0 = Le nom de l'agent SNMP

18.3.3. Les messages SNMP :

TYPE	DESCRIPTION
Get	Les messages « Get » sont utilisés pour obtenir la valeur d'une ou plusieurs variables MIB
Set	Les messages « Set » sont utilisés pour modifier la valeur d'une ou plusieurs variables MIB
Trap	Les messages « Trap » sont envoyés de l'agent SNMP vers le gestionnaire SNMP sans qu'il lui demande afin de lui indiquer une modification d'une variable MIB (État d'une interface par exemple)

Plus de détails :

TYPE	DESCRIPTION
Get-request	Envoyé par le gestionnaire SNMP pour obtenir la valeur d'une seule variable MIB
Get-Next-Request	Envoyé par le gestionnaire SNMP pour obtenir les valeurs d'une liste de variables MIB
Get-Bulk-Request	Envoyé par le gestionnaire SNMP pour obtenir les valeurs de plusieurs variables MIB
Get-Response	Réponse de l'agent SNMP suite à une requête « Get »
Set-Request	Envoyé par le gestionnaire SNMP pour modifier la valeur d'une variable MIB
Trap	Envoyé par l'agent SNMP pour indiquer au gestionnaire SNMP une modification d'une variable MIB

18.3.4. Les versions SNMP :

SNMPv1 :



Pas de sécurité : pas d'authentification et pas de confidentialité (chaîne de communauté envoyée en clair).

SNMPv2c :



Pas de sécurité : Pas d'authentification et pas de confidentialité



Utilisation de Get-Bulk-Request



Code d'erreur détaillé

SNMPv3 :



Trois niveaux de sécurité :

- **NoAuthNoPriv** : Pas d'authentification et pas de confidentialité
- **AuthNoPriv** : Authentification (HMAC-MD5, HMAC-SHA) et pas de confidentialité
- **AuthPriv** : Authentification et confidentialité (AES, DES)

18.3.5. Configuration d'un routeur comme agent SNMP :

```
R1(config)# ! ACL des gestionnaires SNMP autorisés
R1(config)# ip access-list standard SNMP-ACL
R1(config-std-nacl)# permit host 192.168.1.100
R1(config-std-nacl)# exit
R1(config)# ! Identifiant de communauté et du niveau d'accès
R1(config)# snmp-server community Formip rw SNMP-ACL
R1(config)# ! Emplacement de l'agent SNMP
R1(config)# snmp-server location Salle des TP
R1(config)# ! Contact SNMP
R1(config)# snmp-server contact Administrateur Formip
R1(config)# ! Le gestionnaire SNMP gérant les déroutements (traps) avec SNMP V2c
R1(config)# snmp-server host 192.168.1.100 version 2c Formip
R1(config)# ! Le gestionnaire SNMP gérant les déroutements (traps) avec SNMP V3
R1(config)# snmp-server host 192.168.1.100 version 3 priv Formip
R1(config)# ! Activation des traps (Déroutements)
R1(config)# snmp-server enable traps
```

18.4. SYSLOG :

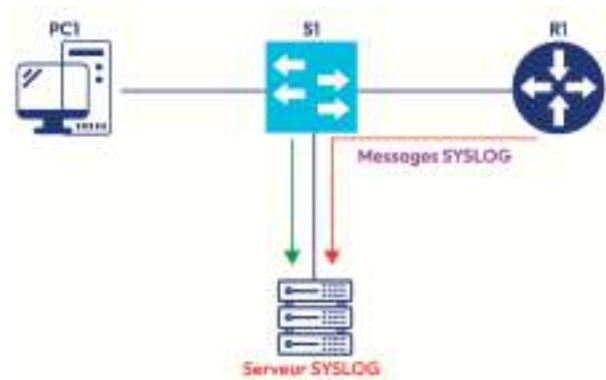
18.4.1. Fonctionnement SYSLOG :

INTRODUCTION :

SYSLOG permet aux administrateurs réseau de récupérer des messages système détaillés envoyés par les périphériques réseau.

Ces messages SYSLOG peuvent être stockés dans :

- ➡ Le tampon de journalisation (RAM)
- ➡ La ligne console
- ➡ La ligne de terminal
- ➡ Un serveur SYSLOG externe



MESSAGES SYSLOG :

Niveaux de gravité :

NIVEAU	NOM DE GRAVITÉ EN FRANÇAIS	NOM DE GRAVITÉ EN ANGLAIS	DESCRIPTION
0	Urgence	Emergencies	Système inutilisable
1	Alerte	Alerts	Action immédiate requise
2	Critique	Critical	Condition critique
3	Erreur	Errors	Condition d'erreur
4	Avertissement	Warnings	Condition d'avertissement
5	Notification	Notifications	Événement normal, mais important
6	Information	Informational	Message informatif
7	Débogage	Debugging	Message de débogage

Les capacités classiques :

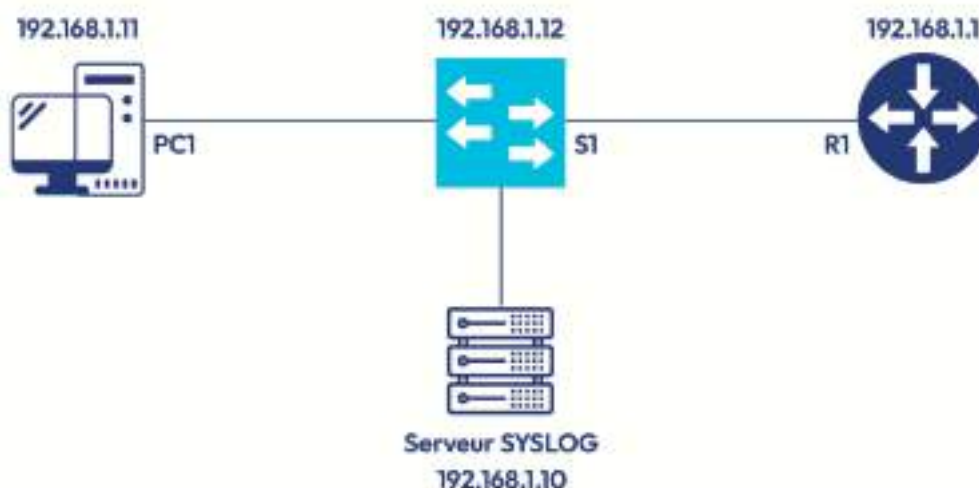
NOM DE LA CAPACITÉ	DESCRIPTION
IP	Protocole IP
OSPF	Protocole OSPF
SYS	Système d'exploitation
IPSEC	Protocole IPSEC
IF	Adresse IP d'interface

Format d'un message SYSLOG :

```
000037: *Aug 21 20:46:07.947: %LINK-3-UPDOWN:
Interface FastEthernet0/0, changed state to down
```

000037	Numéro de séquence
*Aug 21 20:46:07.947	Date de l'événement
LINK	Capacité
3	Niveau de gravité
UPDOWN	Valeur mnémonique
Interface FastEthernet0/0, changed state to down	Description détaillée de l'événement

18.4.2. Configuration SYSLOG :



CONFIGURATION DE BASE SYSLOG :

Configuration de l'adresse IP du serveur SYSLOG :

```
R1(config)#logging 192.168.1.10
```

Contrôle des messages SYSLOG à envoyer au serveur :

```
R1(config)# logging trap 4
```

On peut utiliser le nom du niveau de gravité

```
R1(config)# logging trap warning
```

AUTRES COMMANDES SYSLOG :

Définition de l'interface source des messages SYSLOG :

```
R1(config)# logging source-interface g0/0
```

Activation du service d'horodatage pour les messages SYSLOG

```
R1(config)#service timestamps log datetime msec
```

Activation de l'affichage des numéros de séquence des messages SYSLOG :

```
R1(config)#service sequence-numbers
```

Activation de l'affichage des messages SYSLOG dans la ligne console :

```
R1(config)#logging console
```

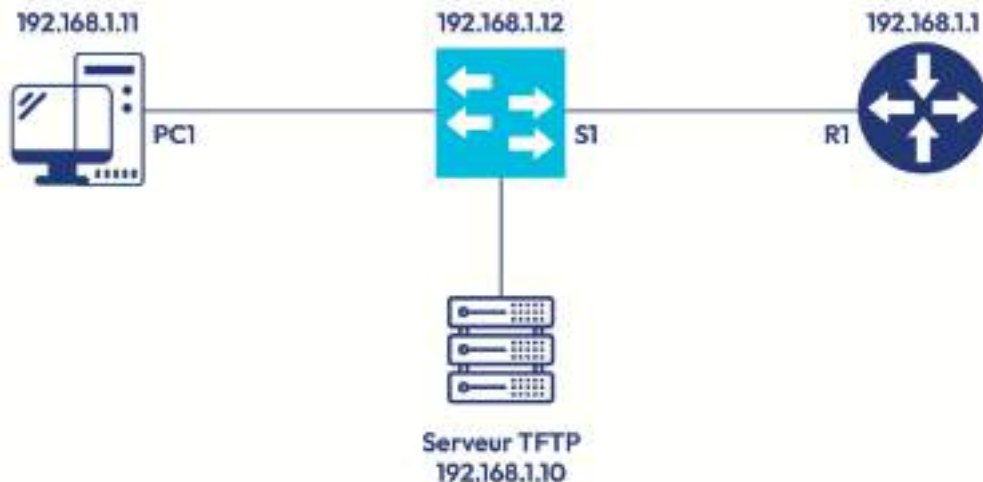
Désactivation de l'affichage des messages SYSLOG dans la ligne console :

```
R1(config)#no logging console
```

Vérification de SYSLOG :

```
R1# show logging
```


18.5. Gestion des fichiers d'un équipement réseau :



18.5.1. Affichage et sauvegarde du fichier de configuration dans la NVRAM :

AFFICHAGE DE LA CONFIGURATION EN COURS (RAM) :

```
R1#show running-config  
(Résultats omis)  
hostname R1  
!  
(Résultats omis)
```

SAUVEGARDE DE LA CONFIGURATION DANS LA NVRAM :

On peut utiliser la commande « Write » :

```
R1#write  
Building configuration...  
[OK]
```

Ou la commande « copy » :

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

AFFICHAGE DE LA CONFIGURATION DE DÉMARRAGE "INITIALE" (NVRAM) :

```
R1#show startup-config
(Résultats omis)
hostname R1
!
(Résultats omis)
```

18.5.2. Sauvegarde de la configuration dans un serveur TFTP :

CONFIGURATION DE L'ADRESSE IP :

```
R1(config)#interface G0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
```

Pour le commutateur, on utilise l'interface de gestion vlan 1 :

```
S1(config)#interface Vlan 1
S1(config-if)#ip address 192.168.1.12 255.255.255.0
S1(config-if)#no shutdown
```

SAUVEGARDE DE LA CONFIGURATION DANS LE SERVEUR TFTP :

```
R1#copy startup-config tftp:
Address or name of remote host []? 192.168.1.10
Destination filename [R1-config]?
Writing startup-config....!!
[OK - 700 bytes]
700 bytes copied in 3.019 secs (231 bytes/sec)
```

18.5.3. Récupération de la configuration à partir d'un serveur TFTP :

SUPPRESSION DE LA CONFIGURATION INITIALE :

```
R1#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
```

RÉCUPÉRATION DE LA CONFIGURATION D'UN ROUTEUR :

Configuration de l'adresse IP du routeur :

```
Router(config)#interface G0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#end
```

Pour le commutateur, on utilise l'interface de gestion vlan 1 :

```
S1(config)#interface Vlan 1
S1(config-if)#ip address 192.168.1.12 255.255.255.0
S1(config-if)#no shutdown
```

Récupération de la configuration à partir du serveur TFTP :

```
Router#copy tftp: running-config
Address or name of remote host []? 192.168.1.10
Source filename []? R1-config
Destination filename [running-config]?
Accessing tftp://192.168.1.10/R1-config....
Loading R1-config from 192.168.1.10: !
[OK - 700 bytes]
700 bytes copied in 3.011 secs (232 bytes/sec)
```

Sauvegarde de la configuration dans la NVRAM :

```
R1#copy running-config startup-config
```

18.5.4. Procédure de récupération des mots de passe :

ACCÈS AU MODE ROMMON :

CTRL + PAUSE :

```
Self decompressing the image :  
#####  
monitor: command "boot" aborted due to user interrupt  
rommon 1 >
```

CONFIGURATION DU REGISTRE 0X2142 :

```
rommon 1 > confreg 0x2142
```

DÉMARRAGE DU ROUTEUR :

```
rommon 1 > reset
```

COPIE DE LA CONFIGURATION DE LA NVRAM DANS LA RAM :

```
Router>enable  
Router#copy startup-config running-config  
Destination filename [running-config]?  
879 bytes copied in 0.416 secs (2112 bytes/sec)
```

MODIFICATION DES MOTS DE PASSE :

```
R1(config)#enable secret Formip123  
R1(config)#enable password Formip321  
R1(config)#line console 0  
R1(config-line)#password Formip123456  
R1(config-line)#login
```

RÉTABLISSEMENT DE LA VALEUR PAR DÉFAUT DE LA CLÉ DE REGISTRE 0X2102 :

```
R1(config)#config-register 0x2102
```

COPIE DE LA CONFIGURATION DE LA RAM DANS LA NVRAM :

```
R1#copy running-config startup-config
```

REDÉMARRAGE DU ROUTEUR :

```
R1#reload  
Proceed with reload? [confirm]
```

La récupération de mots de passe sur un équipement réseau peut être **cruciale** pour assurer la sécurité de votre réseau.

En cas de perte ou d'oubli de mot de passe d'administrateur, la **récupération de mot de passe** permet de rétablir l'accès à l'équipement sans avoir à le remplacer.

Cela peut également être utile en cas de besoin d'accéder à un équipement qui a été configuré par une personne qui n'est plus disponible pour fournir les informations de connexion.

Enfin, il est important de respecter les politiques de sécurité de l'entreprise en utilisant ces méthodes.

18.5.5. Autres commandes :

Affichage des systèmes de fichiers :

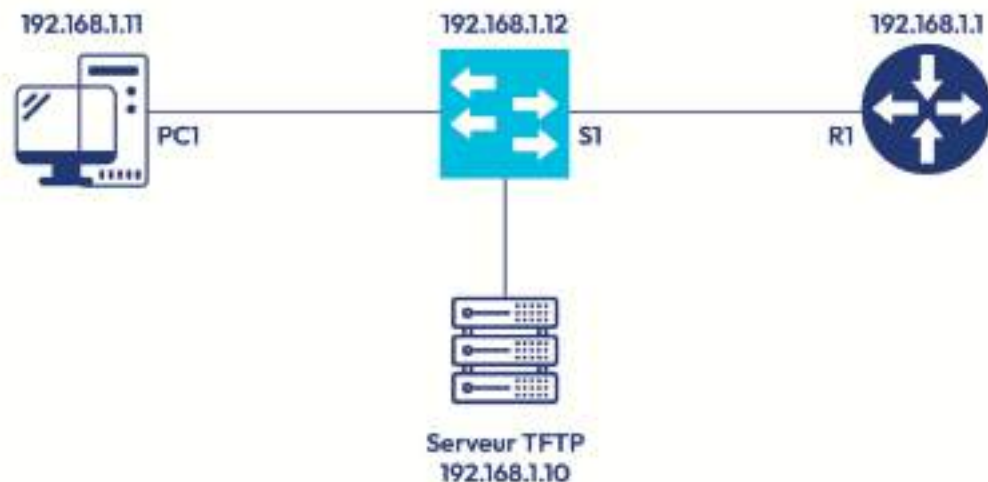
```
R1#show file systems  
File Systems:  
  
      Size(b)      Free(b)  Type  Flags  Prefixes  
*  255744000      221896413  disk   rw    flash0: flash:#  
    262136        255005  nvram   rw    nvram:
```

Affichage du contenu de la NVRAM :

```
R1#dir nvram:  
Directory of nvram:/  
  
 238 -rw-    743    <no date> startup-config  
  
743 bytes total (237588 bytes free)
```

18.6. Gestion des images IOS :

18.6.1. Sauvegarde d'une image IOS dans un serveur TFTP :



AFFICHAGE DU CONTENU DE LA MÉMOIRE FLASH :

```
R1#show flash:

System flash directory:
File Length Name/status
 3 33591768 c2900-universalk9-mz.SPA.151-4.M4.bin
 2 28282    sigdef-category.xml
 1 227537    sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
```

“c2900-universalk9-mz.SPA.151-4.M4.bin” est le nom de l'image IOS.

RÉCUPÉRATION DE L'IMAGE IOS D'UN SERVEUR TFTP :

```
R1# copy tftp: flash:
Address or name of remote host []? 192.168.1.10
Source filename []? ios_c2900_saved.bin
Destination filename [ios_c2900_saved.bin]?

Accessing tftp://192.168.1.10/ios_c2900_saved.bin....
Loading ios_c2900_saved.bin from 192.168.1.10:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 33591768 bytes]

33591768 bytes copied in 4.368 secs (807462 bytes/sec)
```

Fichier source contenu dans le serveur **TFTP** : `ios_c2900_saved.bin`

Adresse du serveur **TFTP**: `192.168.1.10`

Nom de l'image IOS dans la destination (Mémoire FLASH): `ios_c2900_saved.bin`

18.6.3. La commande boot system :

```
R1(config)# boot system tftp ios_c2900_saved.bin 192.168.1.10
```

La commande "**boot system**" est utilisée pour spécifier le chemin d'accès vers le fichier d'image de démarrage (par exemple, IOS ou firmware) sur un équipement réseau, comme un routeur ou un commutateur.

En effet, cette commande est généralement utilisée pour choisir quel fichier d'image de démarrage utiliser lorsque l'équipement démarre, ou pour changer de fichier d'image de démarrage dans le but d'effectuer une mise à niveau ou une récupération.

Elle doit être saisie dans la configuration globale de l'équipement pour être prise en compte lors du démarrage.

Elle peut être utilisée pour spécifier plusieurs fichiers d'image de démarrage en les ordonnant par ordre de priorité.

Ainsi, si le premier fichier d'image spécifié ne peut pas être trouvé ou utilisé, l'équipement passera au fichier d'image suivant dans la liste.