

# TP 3 — Supervision de switchs

Mamadou DIARRA

## Exercice 1 — Travail préparatoire

I 1.1 Sur NMS : installez les paquets snmp et wireshark.

Installation des paquets sur les machines avec : « sudo apt install -y snmp wireshark »



I 1.2 Sur M : installez les paquets snmp, wireshark et minicom.

Installation des paquets sur les machines avec : « sudo apt install -y snmp wireshark minicom »



```
elyes@localhost:~$ wireshark
^C
elyes@localhost:~$ sudo apt install snmp wireshark minicom
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
minicom est déjà la version la plus récente (2.8-2).
Les paquets supplémentaires suivants seront installés :
 libwireshark-data libwireshark14 libwiretap11 libwsutil12 wireshark-common wireshark-qt
Paquets suggérés :
 geoipupdate geoip-database geoip-database-extra libjs-leaflet libjs-leaflet.markercluster
 snmp-mibs-downloader wireshark-doc
Les NOUVEAUX paquets suivants seront installés :
 snmp
Les paquets suivants seront mis à jour :
 libwireshark-data libwireshark14 libwiretap11 libwsutil12 wireshark wireshark-common
 wireshark-qt
7 mis à jour, 1 nouvellement installés, 0 à enlever et 325 non mis à jour.
Il est nécessaire de prendre 22,5 Mo dans les archives.
Après cette opération, 962 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n] ■
```

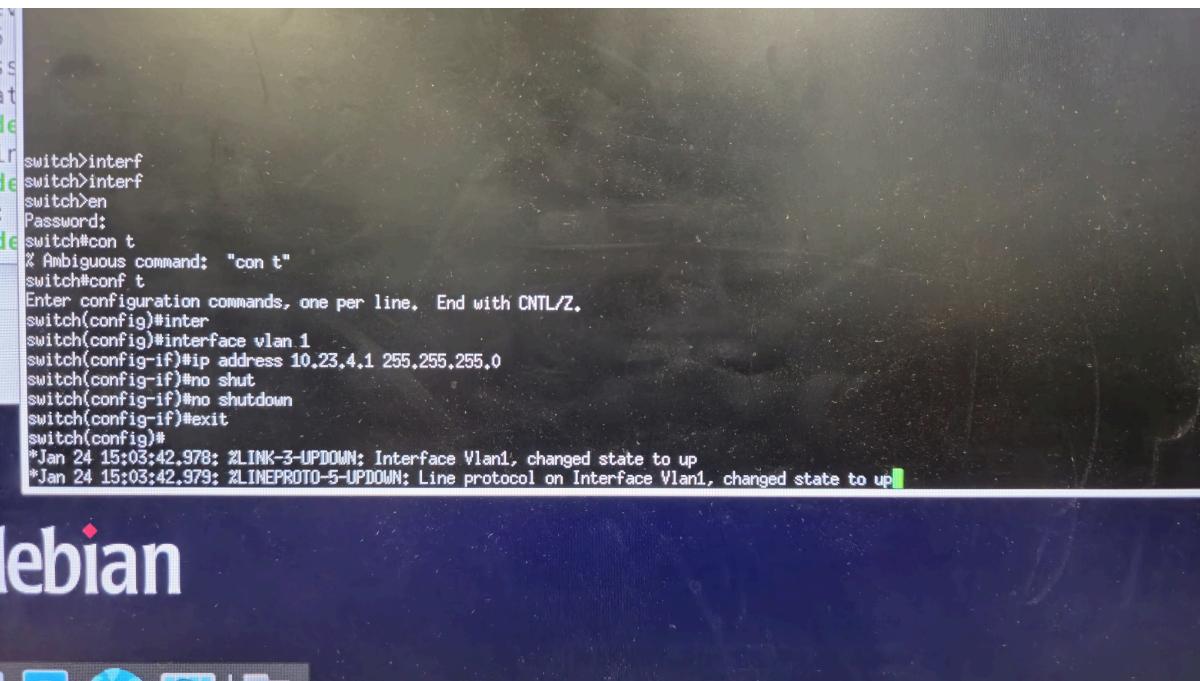
I 1.3 Connectez les interfaces eth0 des deux machines au switch.



I 1.4 Suivez les instructions de la section 1 de la documentation cisco.



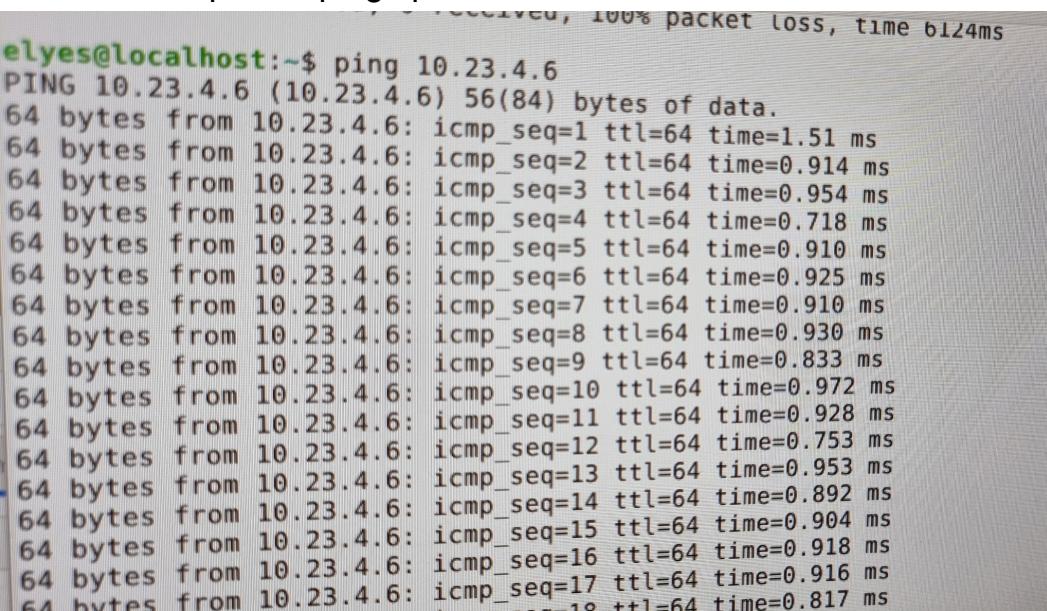
I 1.5 Suivez les instructions de la section 3.8 de la documentation cisco pour donner au switch une IP (sur le VLAN 1) dans le réseau 10.23.G.0/24 (avec G=numéro de groupe). 



```
switch>interf
switch>interf
switch>en
Password:
switch#con t
% Ambiguous command: "con t"
switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#inter
switch(config)#interface vlan 1
switch(config-if)#ip address 10.23.4.1 255.255.255.0
switch(config-if)#no shut
switch(config-if)#no shutdown
switch(config-if)#exit
switch(config)#
*Jan 24 15:03:42.978: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Jan 24 15:03:42.979: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
```

I 1.6 Donnez aux interfaces eth0 des 2 machines des IP dans ce même réseau. 

I 1.7 Vérifiez que les pings passent bien entre les machines et le switch. 



```
elyes@localhost:~$ ping 10.23.4.6
PING 10.23.4.6 (10.23.4.6) 56(84) bytes of data.
64 bytes from 10.23.4.6: icmp_seq=1 ttl=64 time=1.51 ms
64 bytes from 10.23.4.6: icmp_seq=2 ttl=64 time=0.914 ms
64 bytes from 10.23.4.6: icmp_seq=3 ttl=64 time=0.954 ms
64 bytes from 10.23.4.6: icmp_seq=4 ttl=64 time=0.718 ms
64 bytes from 10.23.4.6: icmp_seq=5 ttl=64 time=0.910 ms
64 bytes from 10.23.4.6: icmp_seq=6 ttl=64 time=0.925 ms
64 bytes from 10.23.4.6: icmp_seq=7 ttl=64 time=0.910 ms
64 bytes from 10.23.4.6: icmp_seq=8 ttl=64 time=0.930 ms
64 bytes from 10.23.4.6: icmp_seq=9 ttl=64 time=0.833 ms
64 bytes from 10.23.4.6: icmp_seq=10 ttl=64 time=0.972 ms
64 bytes from 10.23.4.6: icmp_seq=11 ttl=64 time=0.928 ms
64 bytes from 10.23.4.6: icmp_seq=12 ttl=64 time=0.753 ms
64 bytes from 10.23.4.6: icmp_seq=13 ttl=64 time=0.953 ms
64 bytes from 10.23.4.6: icmp_seq=14 ttl=64 time=0.892 ms
64 bytes from 10.23.4.6: icmp_seq=15 ttl=64 time=0.904 ms
64 bytes from 10.23.4.6: icmp_seq=16 ttl=64 time=0.918 ms
64 bytes from 10.23.4.6: icmp_seq=17 ttl=64 time=0.916 ms
64 bytes from 10.23.4.6: icmp_seq=18 ttl=64 time=0.817 ms
```

```
--- 10.23.4.7 ping statistics ---  
4 packets transmitted, 0 received, 100% packet loss, time 300ms  
  
sherazade@localhost:~$ sudo ping 10.23.4.1  
PING 10.23.4.1 (10.23.4.1) 56(84) bytes of data.  
64 bytes from 10.23.4.1: icmp_seq=2 ttl=255 time=2.89 ms  
64 bytes from 10.23.4.1: icmp_seq=3 ttl=255 time=2.21 ms  
64 bytes from 10.23.4.1: icmp_seq=4 ttl=255 time=1.11 ms  
64 bytes from 10.23.4.1: icmp_seq=5 ttl=255 time=0.807 ms  
^C  
--- 10.23.4.1 ping statistics ---  
5 packets transmitted, 4 received, 20% packet loss, time 4008ms  
rtt min/avg/max/mdev = 0.807/1.755/2.888/0.837 ms  
sherazade@localhost:~$ sudo ip link set eth1 up
```

## **Exercice 2—Activation de l'agent SNMP**

I 2.1 Suivez les instructions de la section 3.9 de la documentation cisco pour créer deux ACL répondant aux contraintes énoncées, une pour chaque communauté. ✓

```
/dev/ttyUSB0 - PuTTY
switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#acc
switch(config)#access-list 11
switch(config)#access-list 10 permit ho
switch(config)#access-list 10 permit host 10.23.4.2
switch(config)#access-list 20 permit host 10.23.4.0 0.0.0.255
Translating "host ...domain server (255.255.255.255)
% Invalid input detected at '^' marker.

switch(config)#
switch(config)#access-list 10 permit host 10.23.4.2
% Duplicate permit statement ignored.

switch(config)#access-list 20 permit 10.23.4.0 0.0.0.255
switch(config)#access-list 20 deny hos
switch(config)#access-list 20 deny host 10.23.4.2
Access rule can't be configured at higher sequence num as it is part of the existing rule at sequence num 10
switch(config)no acc
switch(config)no access-l1
switch(config)no access-list 20
switch(config)ac
switch(config)access-l1
switch(config)access-list 20 den
switch(config)access-list 20 deny ho
switch(config)access-list 20 deny host 10.23.4.2
switch(config)ac
switch(config)access-l1
switch(config)access-list 20 per
switch(config)access-list 20 permit 10.
%Error opening tftp://255.255.255.255/network-config (Timed out)
%Error opening tftp://255.255.255.255/switch-config (Timed out)23
*Jan 24 15:26:35.487: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/network-config) failed
*Jan 24 15:26:35.489: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/switch-config) failed
% Invalid input detected at '^' marker.
```

```

switch(config)#access-list 10 permit host 10.23.4.2
switch(config)#access-list 20 permit host 10.23.4.0 0.0.0.255
Translating "host"...domain server (255.255.255.255)
      % Invalid input detected at '^' marker.

switch(config)#
switch(config)#access-list 10 permit host 10.23.4.2
      % Duplicate permit statement ignored.

switch(config)#access-list 20 permit 10.23.4.0 0.0.0.255
switch(config)#access-list 20 deny host
switch(config)#access-list 20 deny host 10.23.4.2
Access rule can't be configured at higher sequence num as it is part of the existing rule at sequence num 10.
switch(config)#no acc
switch(config)#no access-li
switch(config)#no access-list 20
switch(config)#ac
switch(config)#access-li
switch(config)#access-list 20 den
switch(config)#access-list 20 deny ho
switch(config)#access-list 20 deny host 10.23.4.2
switch(config)#ac
switch(config)#access-li
switch(config)#access-list 20 per
switch(config)#access-list 20 permit 10,
%Error opening tftp://255.255.255/network-confg (Timed out)
%Error opening tftp://255.255.255/switch-confg (Timed out)23
*Jan 24 15:26:35.487: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255/network-confg) failed
*Jan 24 15:26:35.489: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255/switch-confg) failed
23
      % Invalid input detected at '^' marker.

switch(config)#
switch(config)#
      %Error opening tftp://255.255.255/cisconet.cfg (Timed out)
      %Error opening tftp://255.255.255/switch.efc (Timed out)

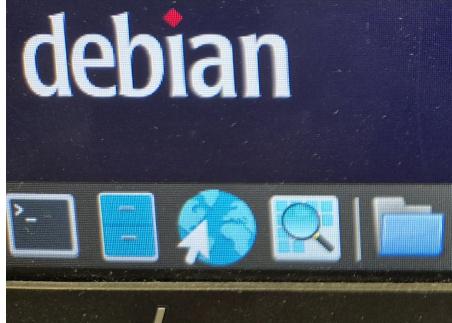
```

- I 2.2 Suivez les instructions de la section 3.10.1 de la documentation cisco pour créer deux communautés avec des noms de votre choix en les associant aux ACL créées. 

```

%Error opening tftp://255.255.255.255/cisconet.cfg (Timed out)
%Error opening tftp://255.255.255.255/switch.cfg (Timed out)
*Jan 24 15:27:13.500: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.
*Jan 24 15:27:13.500: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.
switch(config)#snmp
switch(config)#snmp
switch(config)#snmp-s
switch(config)#snmp-server comm
switch(config)#snmp-server community RO
switch(config)#snmp-server community RO_COMMUNITY ro 20
switch(config)#snmp-server community RW_COMMUNITY rw 10
switch(config)#

```



- I 2.3 Effectuez, depuis M et le NMS, plusieurs requêtes SNMP pour tester votre configuration. Vous choisirez des tests permettant de montrer que les contraintes énoncées sont bien respectées. 

```

Fichier Édition Affichage Terminal Onglets Aide
iso.3.6.1.2.1.10.7.2.1.17.10121 = OID: ccitt.0
iso.3.6.1.2.1.10.7.2.1.17.10122 = OID: ccitt.0
iso.3.6.1.2.1.10.7.2.1.17.10123 = OID: ccitt.0
^C
sherazade@localhost:~$ snmpwalk -v2c -c RO_COMMUNITY 10.23.4.1
snmpwalk: Failure in sendto (Network is unreachable)
sherazade@localhost:~$ sudo ip addr add 10.23.4.6/24 dev eth1
sherazade@localhost:~$ sudo ping 10.23.4.1
PING 10.23.4.1 (10.23.4.1) 56(84) bytes of data.
64 bytes from 10.23.4.1: icmp_seq=1 ttl=255 time=5.70 ms
64 bytes from 10.23.4.1: icmp_seq=2 ttl=255 time=2.33 ms
64 bytes from 10.23.4.1: icmp_seq=3 ttl=255 time=3.09 ms
^C
--- 10.23.4.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.331/3.704/5.695/1.441 ms
sherazade@localhost:~$ snmpwalk -v2c -c RO_COMMUNITY 10.23.4.1
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, C1000 Software (C1000-UNIVERS
ALK9-M), Version 15.2(7)E6, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2022 by Cisco Systems, Inc.
Compiled Tue 22-Mar-22 10:25 by mpree"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.2959
iso.3.6.1.2.1.1.3.0 = Timeticks: (397547) 1:06:15.47

elyes@localhost:~$ 
elyes@localhost:~$ 
elyes@localhost:~$ 
elyes@localhost:~$ 
elyes@localhost:~$ snmpget -v2c -c RO_COMMUNITY 10.23.4.1 1.3.6.1.2.1.1.5.0
iso.3.6.1.2.1.1.5.0 = STRING: "switch"
elyes@localhost:~$ 

```

Q 2.1 Justifiez le choix des tests effectués.

*Nous avons effectué des tests de communauté en read et read write pour vérifier que la configuration respecte les contraintes de sécurité et de fonctionnement demandées.*

## Exercice 3—Activation de syslog

I 3.1 Sur le switch : suivez les instructions de la section 3.11 de la documentation cisco pour activer l'envoi des logs vers le NMS avec un niveau maximal de notification fixé à 5.

```

error opening tftp://255.255.255.255/switch-confg (timed out)
*Jan 24 15:51:23.506: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/network-confg) failed
*Jan 24 15:51:23.506: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/switch-confg) failed
switch>
switch>enable
Password:
switch>log
switch>log
switch>conf t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#log
switch(config)#log
switch(config)#logging host
switch(config)#Logging host 10.23.4.2
switch(config)#Logging host 10.23.4.2
*Jan 24 15:52:01.506: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/cisconet.cfg) failed
*Jan 24 15:52:01.508: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/switch.cfg) failed
% Incomplete command.

switch(config)#log
switch(config)#log
switch(config)#Logging has
switch(config)#Logging host 10.23.4.2
switch(config)#Logging host 10.23.4.2
*Jan 24 15:52:24.857: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.23.4.2 port 514 started - CLI initiat
^
% Invalid input detected at '^' marker.

switch(config)#logging tra
switch(config)#logging trap noti
switch(config)#logging trap notifications
switch(config)#

```

I 3.2 Sur le NMS : trouvez, puis décommenter, dans le fichier de configuration de rsyslog (/etc/rsyslog.conf), les deux lignes qui activent la réception de messages syslog sur le port UDP 514.

```

GNU nano 5.4                               /etc/rsyslog.conf *
# /usr/share/doc/rsyslog-doc/html/configuration/index.html

#####
#### MODULES #####
#####

# provides support for local system logging
module(load="imuxsock")
# provides kernel logging support
module(load="imklog")
# provides --MARK-- message capability
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

Nom du fichier à écrire: /etc/rsyslog.conf
^G Aide          M-D Format DOS    M-A Ajout (à la fin)M-B Copie de sécu.
^C Annuler      M-M Format Mac   M-P Ajout (au début)^T Parcourir

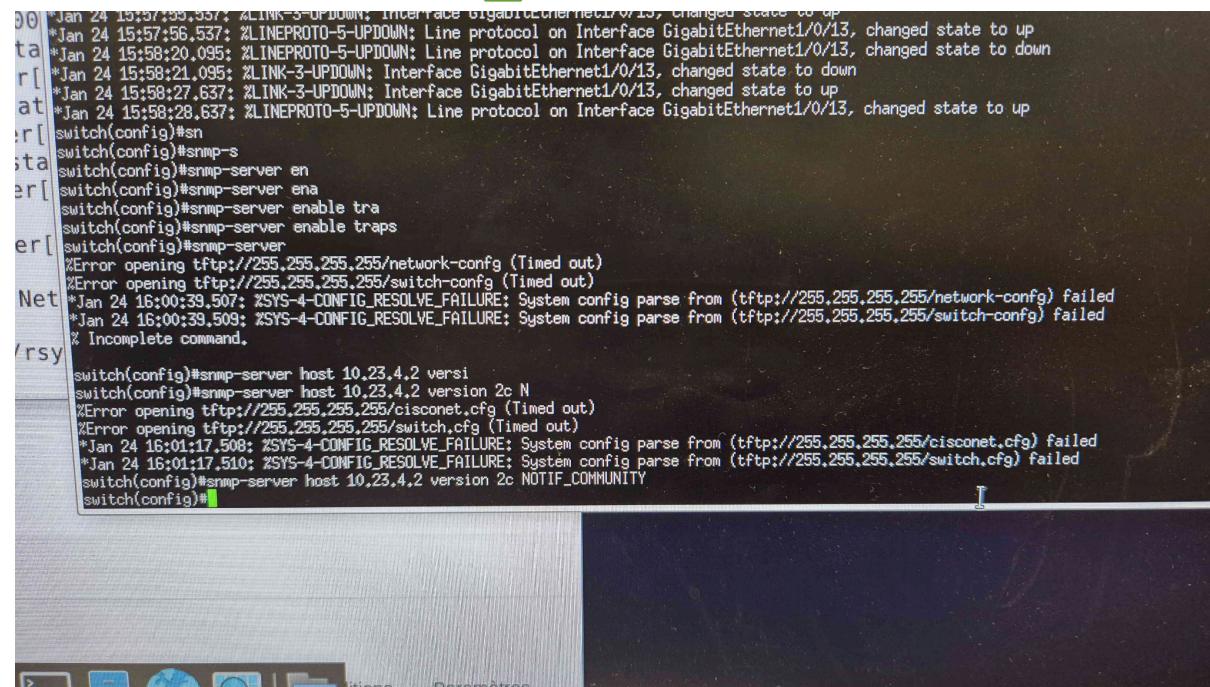
```

I 3.3 Débranchez puis rebranchez le câble ethernet entre M et le switch.

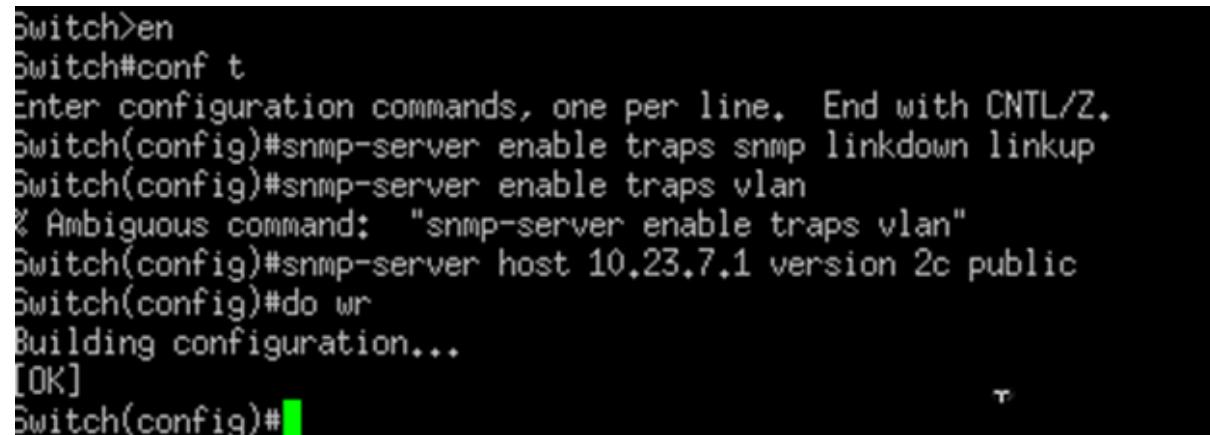
I 3.4 Vérifiez que le journal (/var/log/syslog) du NMS contient bien deux nouvelles lignes.

## Exercice 4 —Activation des notifications

I 4.1 Sur le switch, suivez les instructions de la section 3.10.2 de la documentation cisco pour programmer l'envoi de notifications SNMP au NMS dans les situations suivantes : 



```
00 *Jan 24 15:57:55.557: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up
*Jan 24 15:57:56.537: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to up
*Jan 24 15:58:20.095: %LINK-3-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to down
*Jan 24 15:58:21.095: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to down
*Jan 24 15:58:27.637: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up
*Jan 24 15:58:28.637: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/13, changed state to up
switch(config)#snmp-s
switch(config)#snmp-server en
switch(config)#snmp-server enable tra
switch(config)#snmp-server enable traps
switch(config)#snmp-server
%Error opening tftp://255.255.255.255/network-confg (Timed out)
%Error opening tftp://255.255.255.255/switch-confg (Timed out)
*Jan 24 16:00:39.507: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/network-confg) failed
*Jan 24 16:00:39.509: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/switch-confg) failed
% Incomplete command.
/rsy
switch(config)#snmp-server host 10.23.4.2 versi
switch(config)#snmp-server host 10.23.4.2 version 2c N
%Error opening tftp://255.255.255.255/cisconet.cfg (Timed out)
%Error opening tftp://255.255.255.255/switch.cfg (Timed out)
*Jan 24 16:01:17.508: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/cisconet.cfg) failed
*Jan 24 16:01:17.510: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/switch.cfg) failed
switch(config)#snmp-server host 10.23.4.2 version 2c NOTIF_COMMUNITY
switch(config)#
I
```



```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#snmp-server enable traps snmp linkdown linkup
Switch(config)#snmp-server enable traps vlan
% Ambiguous command: "snmp-server enable traps vlan"
Switch(config)#snmp-server host 10.23.7.1 version 2c public
Switch(config)#do wr
Building configuration...
[OK]
Switch(config)#
T
```

Les notifications seront envoyées au format SNMPv2c avec une communauté de votre choix.

I 4.2 Testez avec wireshark que des notifications sont bien reçues dans les trois cas. 

No.	Time	Source	Destination	Protocol	Length	Info
79	98.529236869	10.23.7.3	10.23.7.1	SNMP	211	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0
80	98.529278904	10.23.7.1	10.23.7.3	ICMP	239	Destination unreachable (Port unreachable)
81	98.779237781	10.23.7.3	10.23.7.1	SNMP	209	snmpV2-trap 1.3.6.1.2.1.1.3.0 1.3.6.1.6.3.1.1.4.1.0
82	98.779273300	10.23.7.1	10.23.7.3	ICMP	237	Destination unreachable (Port unreachable)

Q 4.1 Pour chaque notification capturée, dites si c'est une notification SNMPv2c standard ou si c'est une notification propre aux équipements CISCO. Justifiez.

**Les alertes sont propres car elles comportent le OID cisco.**

## Exercice 5 — Droits d'accès à la MIB

I 5.1 Créez une nouvelle ACL contenant uniquement M ainsi que les vues et communautés répondant aux contraintes énoncées. Une communauté ne pouvant être associée qu'à une seule vue, il est nécessaire de définir deux communautés pour M. La première sera utilisée pour accéder à la branche MIB-2 en lecture seule ; la deuxième pour accéder à la branche système en lecture/écriture. Les instructions pour créer les vues sont décrites dans la section 3.10.3 de la documentation cisco.

```
Switch(config)#snmp-server view mib2view 1.3.6.1.2.1 included
Switch(config)#snmp-server view system2view 1.3.6.1.2.1 included
Switch(config)#snmp-server vcomm
Switch(config)#snmp-server vcommu
Switch(config)#snmp-server vcommuni
Switch(config)#snmp-server vcommunity mib2community ro view mib2view
```

```
Switch(config)#snmp-server community comm view ro mib2view
Switch(config)#snmp-server community comm view rw systemview
Switch(config)#[img]
```

I 5.2 Proposez et lancez une série de tests (sous forme de requêtes SNMP) sur M permettant de tester que votre configuration répond aux contraintes énoncées. Dans vos tests, vous pourrez utiliser l'objet 1.3.6.1.2.1.11.30 qui est modifiable, dans la branche MIB-2 mais pas dans la branche system.



Test 1 : Accès à la branche MIB-2 en lecture seule

Test 2 : Accès à la branche system en lecture/écriture

Test 3 : Vérification des restrictions sur le reste de la MIB

Q 5.1 Justifiez les choix des tests effectués. 

Le test de lecture avec **COMM\_MIB2\_RO** valide que la vue **VIEW\_MIB2** est correctement configurée.

Le test de lecture avec **COMM\_SYSTEM\_RW** vérifie que l'accès à la branche **system** est autorisé.

Les tests sur des branches non autorisées (par exemple, Cisco MIB propriétaire) confirment que les vues et ACL interdisent l'accès à ces parties de la MIB.