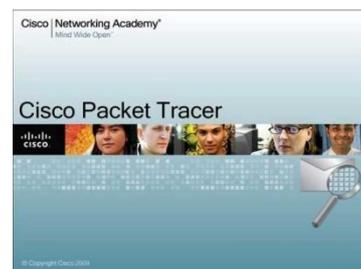


Supervision réseau : SNMP sous PacketTracer

Dans ce document nous allons découvrir les capacités du protocole SNMP, ce qu'il peut apporter, et comment le configurer. Ce document s'adresse à des personnes avancées en informatique et des connaissances du monde TCP/IP.

Le protocole SNMP sous PacketTracer



Sommaire

I.	Introduction.....	3
1.	Opportunity	3
2.	Solution.....	3
II.	La supervision SNMP sous PacketTracer : Routeur	4
3.	Exercice SNMP_Router.pkt.....	4
4.	D'autres fonctionnalités	6
III.	Marquette PacketTracer, etude du MIB browser : Projet GSB	7
5.	Configuration des éléments actifs.....	7
6.	Simulation PacketTracer.....	9
7.	Analyse des PDUs	10

I. Introduction

1. Opportunity

As networking systems continue to evolve in complexity, new curricula and educational tools are emerging to facilitate teaching and learning about networking technology. The Cisco Networking Academy program is designed to keep pace with the evolution of networking systems by providing innovative curricula and educational tools that help students understand the complexities of information and communication technologies (ICTs).

Within this framework, the Cisco Packet Tracer e-learning software was developed to help Networking Academy students gain practical networking technology skills in a rapidly changing environment. Students seeking ICT skills can now benefit from the accessibility of online curricula and new opportunities for social learning, collaboration, and competition.

2. Solution

Cisco Packet Tracer is a powerful network simulation program that allows students to experiment with network behavior and ask “what if” questions. As an integral part of the Networking Academy comprehensive learning experience, Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities to facilitate the teaching and learning of complex technology concepts.

Packet Tracer supplements physical equipment in the classroom by allowing students to create a network with an almost unlimited number of devices, encouraging practice, discovery, and troubleshooting. The simulation-based learning environment helps students develop 21st century skills such as decision making, creative and critical thinking, and problem solving.

Packet Tracer complements the Networking Academy curricula, allowing instructors to easily teach and demonstrate complex technical concepts and networking systems design. Instructors can customize individual or multiuser activities, providing hands-on lessons for students that offer value and relevance in their classrooms. Students can build, configure, and troubleshoot networks using virtual equipment and simulated connections, alone or in collaboration with other students.

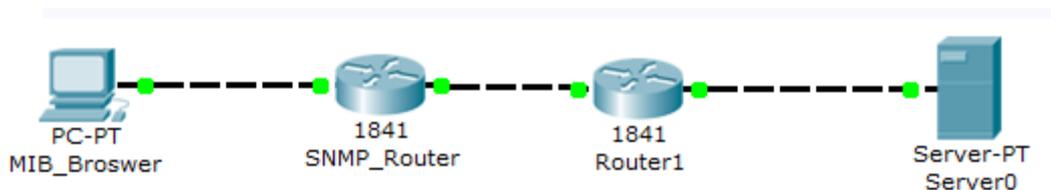
Packet Tracer offers an effective, interactive environment for learning networking concepts and protocols. Most importantly, Packet Tracer helps students and instructors create their own virtual “network worlds” for exploration, experimentation, and explanation of networking concepts and technologies.



II. La supervision SNMP sous PacketTracer : Routeur

3. Exercice SNMP_Router.pkt

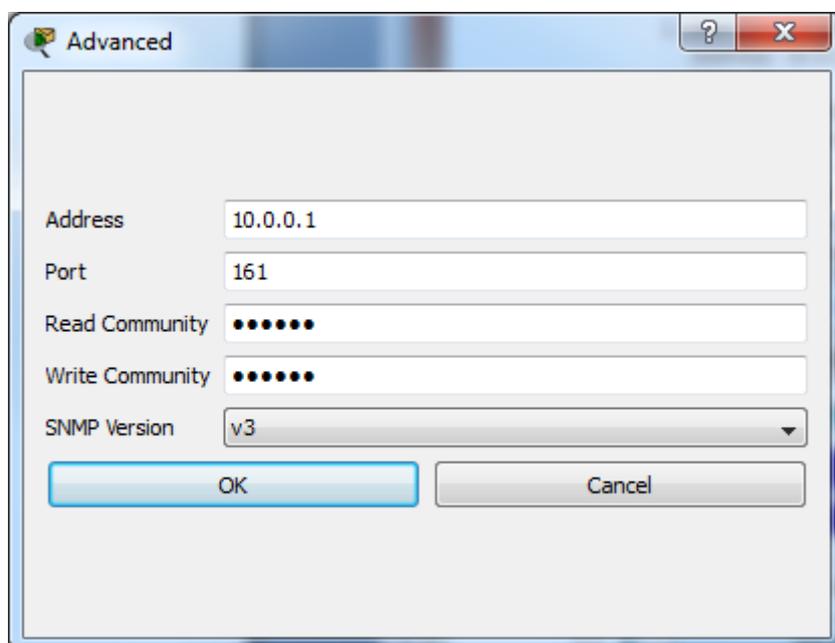
Télécharger PacketTracer dans un premier temps si il n'est pas installé sur votre poste, connectez vous à votre compte cisco netacad pour le récupérer. Lancez ensuite le programme et ouvrez le fichier SNMP_router.pkt dans les fichiers de « **samples** ».



a. Etape 1

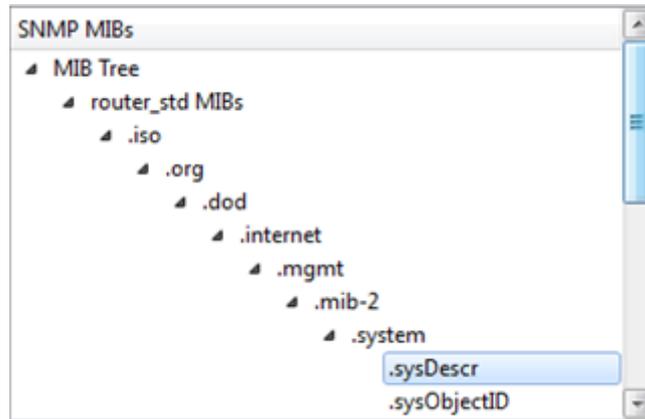
Ouvrez le programme MIB Browser sur le poste MIB_Browser, cliquez sur Advanced et configurer comme_ci-dessous :

- Read Community : Public
- Write Community : Public



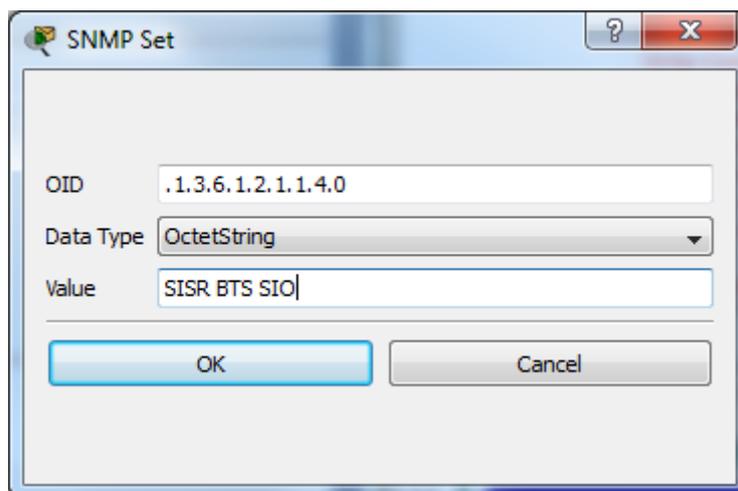
b. Etape 2

Déployez l'arborescence jusqu'à « **.sysDescr** » comme ci-dessous, faites GO, constatez le résultat, on peut voir les informations de description du matériel.



c. Etape 3

Sélectionnez « **.sysContact** » dans l'arborescence et changez les paramètres comme ci-dessous, faites GO.

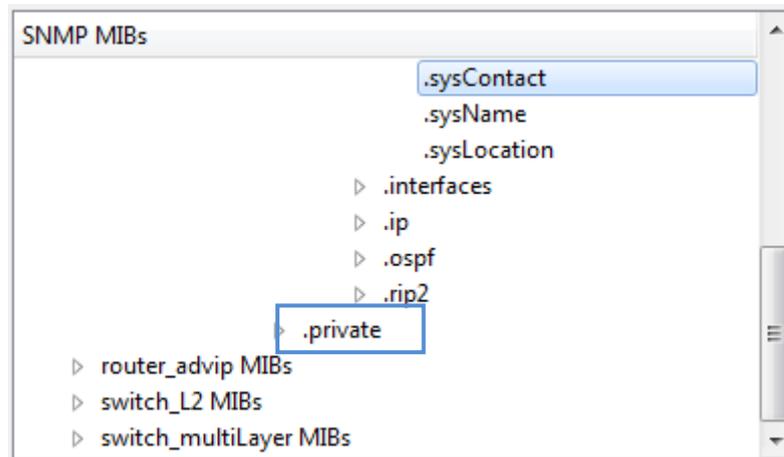


Dans votre résultat vous devriez avoir la valeur que vous avez entrée. Validez ce résultat.

Name/OID	Value	Type
.1.3.6.1.2.1.1.4.0	SISR BT...	OctetStr...

4. D'autres fonctionnalités

Sur l'image ci-dessous on peut voir que notre MIB gère la partie privé



Ceci dit packet tracer ne gère pas une partie RMON.

III. Marquette PacketTracer, etude du MIB browser : Projet GSB

5. Configuration des éléments actifs

Premièrement sur le fichier PacketTracer on peut remarquer l'absence de la configuration du protocole SNMP nous allons donc configurer les différents éléments actifs (switchs, routeurs), ci-dessous un exemple de configuration d'une des éléments actif pour le protocole SNMP :

```
MUT-DATAS(config)# snmp-server community public rw
```

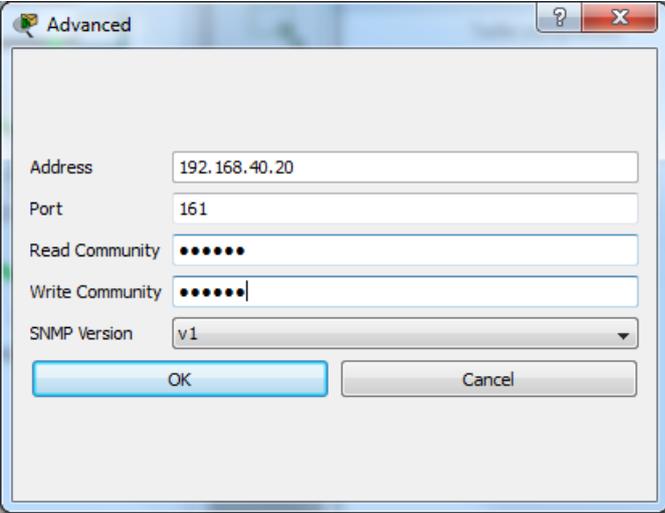
Deuxièmement, afin de pouvoir récupérer des informations sur les éléments actifs il faut également configurer une adresse IP, sur les routeurs elles sont déjà présentes car elles servent de passerelle au postes voici si dessous un exemple de configuration d'adresse IP sur le VLAN 40 :

```
se1_1(config)#interface vlan 40
se1_1(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan40, changed state to up

se1_1(config-if)#no shutdown
se1_1(config-if)#ip address 192.168.40.20 255.255.255.0
```

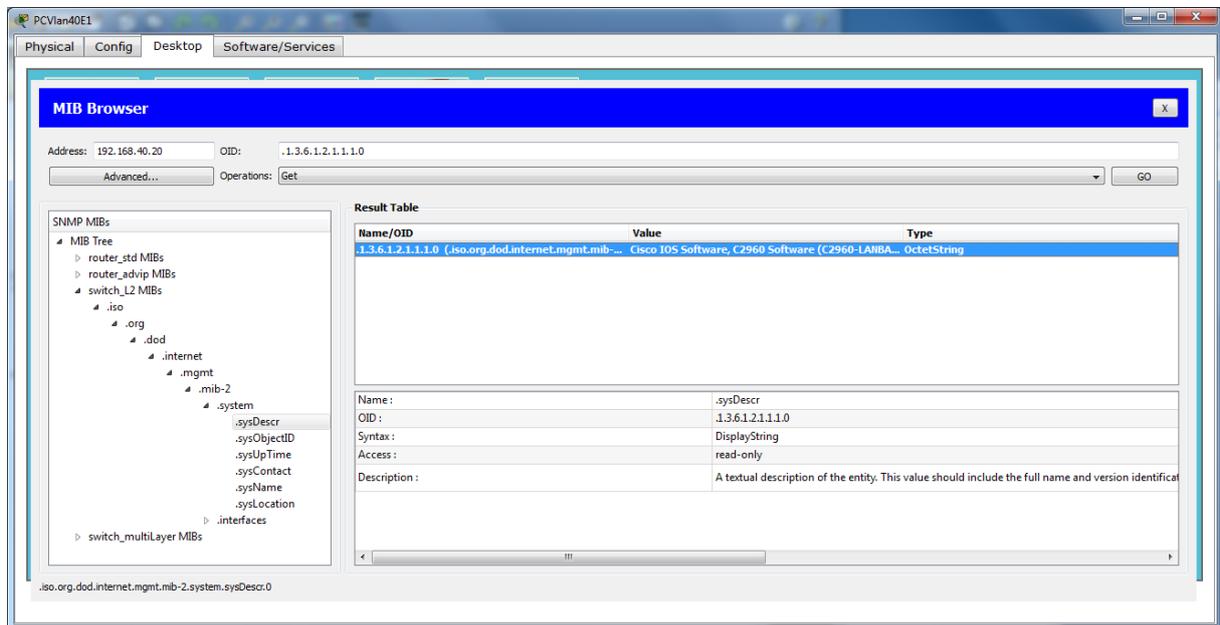
Maintenant configurons le poste MIB , cliquez sur « **Advanced** », et configurer comme ci-dessous.



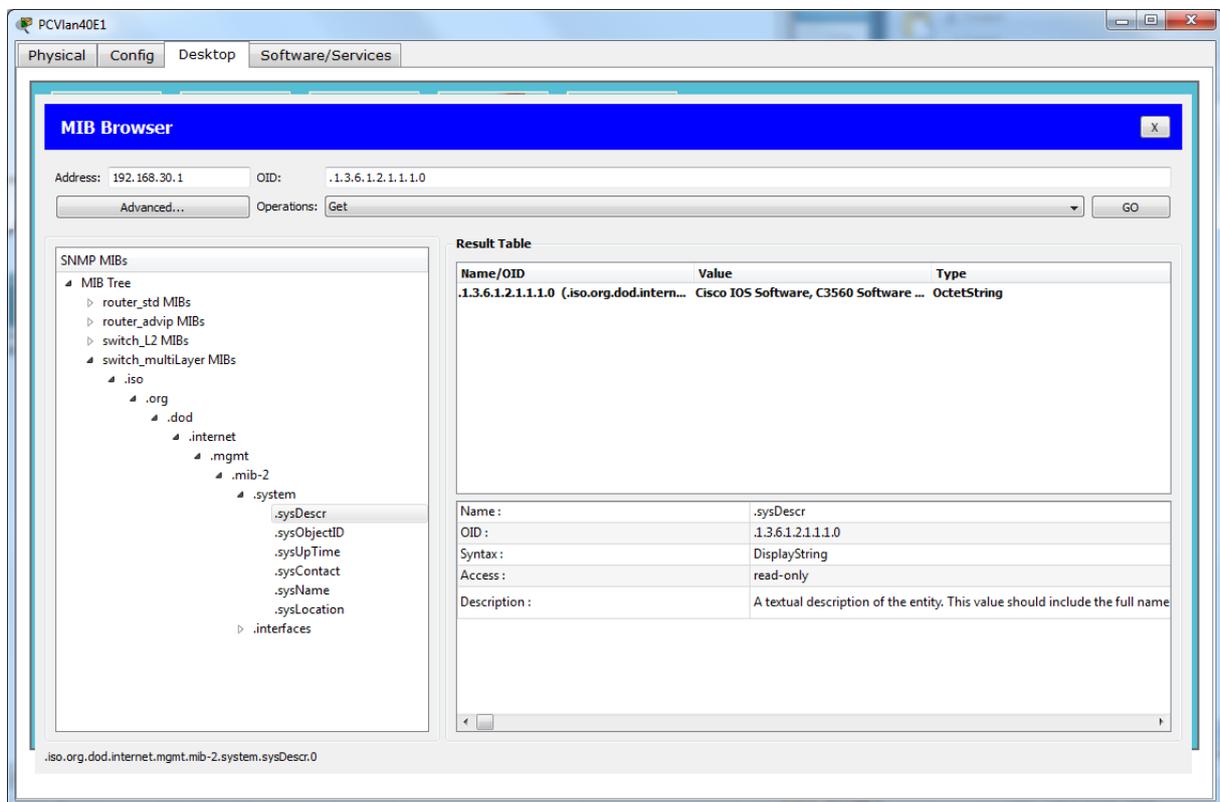
Read Community : **Public**

Write Community : **Public**

Lancez maintenant une requête SNMP ver le switch 192.168.40.20 et constatez le résultat, on peut voir dans value une description détail des caractéristique du switch.



Essayons maintenant sur le routeur, de même les value correspond au descriptif technique du routeur



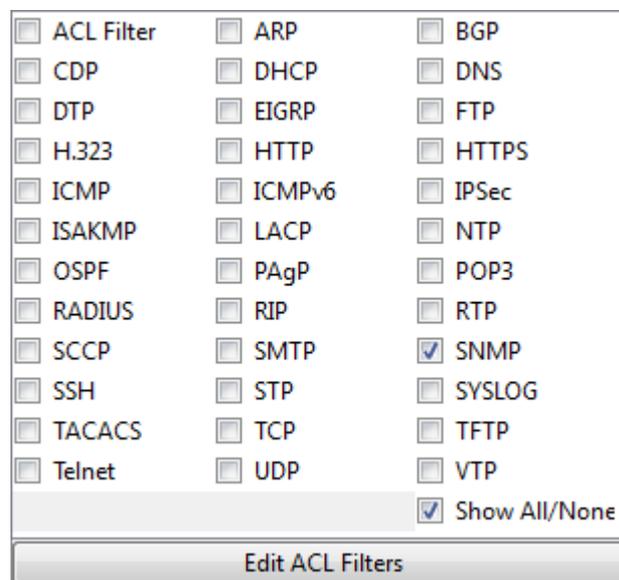
6. Simulation PacketTracer

Sous PacketTracer il est possible d'exécuter une simulation de trafic avec une capture de trames, de type Wireshark, divers options sont disponibles. Cliquez en bas à droite sur l'icône en forme

d'horloge pour passer en mode « **Simulation** » , lancez une capture de trame en cliquant sur , puis lancez une requête SNMP vers votre agent.

Le panneau latérale droit affiche les événements de trafic, repérer avec des protocoles les différents trames sont facilement repérable ceci dit nous allons filtrer les trames, nous allons afficher seulement les trames de type SNMP, pour cela cliquez sur ,

le panneau ci-dessous s'affiche cocher la case Show All/None, puis sélectionnez seulement le protocole SNMP.



Vous devriez normalement avoir dans votre « **Event List** », un affichage de ce type.

Event List					
Vis.	Time (sec)	Last Device	At Device	Type	Info
	0.004	--	PCVlan40E1	SNMP	
	0.005	PCVlan40E1	Switch1Etag1	SNMP	
	0.005	--	Switch1Etag1	SNMP	
	0.006	Switch1Etag1	PCVlan40E1	SNMP	

7. Analyse des PDUs

Double cliquez sur chaque des trames afin de voir pas à pas le chemin de votre requête de sa réponse, regarder votre schéma des enveloppe apparaissent sur l'agent et le MIB, cliquez dessus pour afficher le PDU, regardons le premier.



On constate dans la trame IP les adresse correspondante :

IP					
0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 58		
ID: 0x9		0x0	0x0		
TTL: 128		PRO: 0x11	CHKSUM		
SRC IP: 192.168.40.2					
DST IP: 192.168.40.20					
OPT: 0x0			0x0		
DATA (VARIABLE LENGTH)					

Dans la description OSI Model, on peut voir qu'il s'agit effectivement d'une requête.

PDU Information at Device: PCVlan40E1

OSI Model | **Outbound PDU Details**

At Device: PCVlan40E1
Source: PCVlan40E1
Destination: 192.168.40.20

In Layers	Out Layers
Layer7	Layer 7: SNMP
Layer6	Layer6
Layer5	Layer5
Layer4	Layer 4: UDP Src Port: 161, Dst Port: 161
Layer3	Layer 3: IP Header Src. IP: 192.168.40.2, Dest. IP: 192.168.40.20
Layer2	Layer 2: Ethernet II Header 0060.47B8.42DA >> 0001.635B.BA28
Layer1	Layer 1: Port(s): FastEthernet

1. SNMP Manager sends a GET Request for OID .1.3.6.1.2.1.1.1.0 to 192.168.40.20.

Dans SNMP, la version et la communauté correspondante.

SNMP			
0	8	16	31 Bits
VERSION: 1			
COMMUNITY: public			

La trame est maintenant envoyée :

0.005 PCVlan40E1 Switch1Etag1 SNMP

Et maintenant la réponse de notre agent :

0.006 Switch1Etag1 PCVlan40E1 SNMP

On peut voir les adresses IP qui ont changées.

IP

0	4	8	16	19	31 Bits
4	IHL	DSCP: 0x0	TL: 241		
ID: 0x4			0x0	0x0	
TTL: 255		PRO: 0x11	CHKSUM		
SRC IP: 192.168.40.20					
DST IP: 192.168.40.2					
OPT: 0x0				0x0	
DATA (VARIABLE LENGTH)					

Ainsi que dans la partie OSI Model, la couche 7 : SNMP indique effectivement qu'il s'agit d'une réponse de la part de l'agent :

PDU Information at Device: PCVlan40E1

OSI Model Inbound PDU Details

At Device: PCVlan40E1
Source: Switch1Etag1
Destination: 192.168.40.2

In Layers	Out Layers
Layer 7: SNMP	Layer7
Layer6	Layer6
Layer5	Layer5
Layer 4: UDP Src Port: 161, Dst Port: 161	Layer4
Layer 3: IP Header Src. IP: 192.168.40.20, Dest. IP: 192.168.40.2	Layer3
Layer 2: Ethernet II Header 0001.635B.BA28 >> 0060.47B8.42DA	Layer2
Layer 1: Port FastEthernet	Layer1

1. SNMP Manager receives and processes an SNMP GET Response.