



SNMP



Objectif: Découvrir le rôle du protocole SNMP dans l'administration d'un réseau.

Condition : Le Tp est réalisé seul ou en binôme.

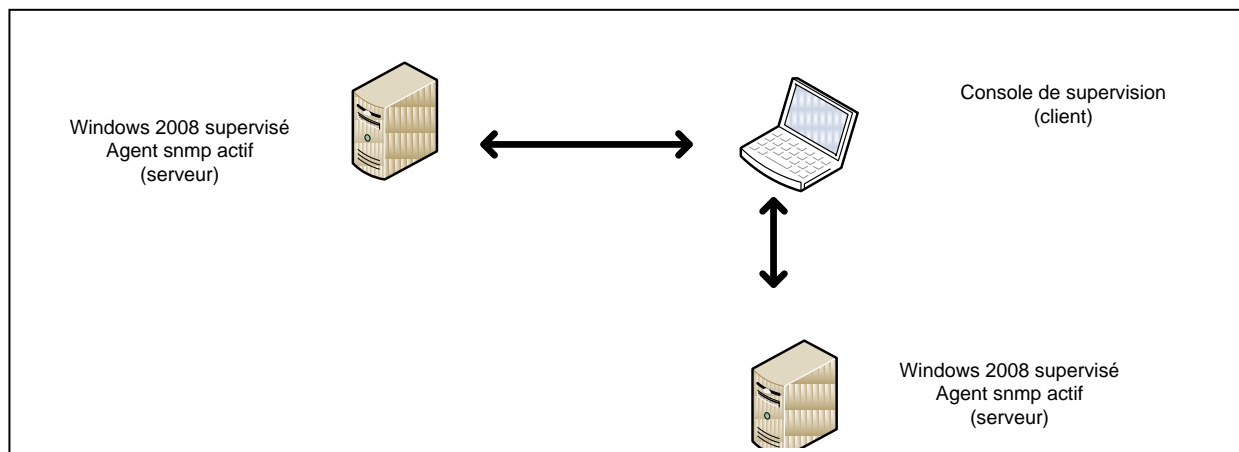
(Il faut 2 postes : windows 2008 + w7 (console) (ou 2 postes 2008)

La console d'administration supervisera le serveur 2008

Partie1: Introduction au protocole SNMP

SNMP utilise le modèle client-serveur où le client est représenté par la station d'administration qui interroge des serveurs représentés par les agents SNMP implantés sur les nœuds administrables.

Depuis une station d'administration, on peut alors interroger chaque nœud manageable du réseau, prendre connaissance de son état, consulter les informations (nombre d'octets reçus ou émis...), configurer certaines caractéristiques (interdire l'emploi de tel ou tel port...), etc.



Le protocole SNMP (Simple Network Management Protocol) permet de contrôler à distance l'état des principaux constituants du réseau.

Sur chaque composant du réseau qui peut être administré - MN (Managed Node) ou nœud manageable - (station, serveur, imprimante réseau, concentrateur, commutateur, routeur, onduleur, ...), on installe un **agent SNMP**. Cet agent est un programme qui enregistre en permanence certaines informations relatives au composant et les stocke dans une base de données : **la MIB (Management Information Base)**.

Partie 2 : Installation et configuration du service SNMP

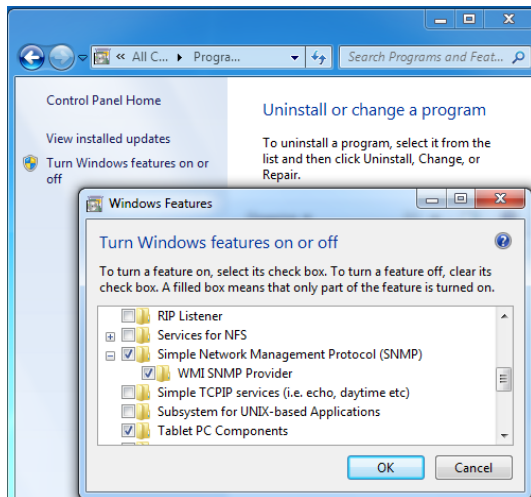
Préparation sur le serveur 2008 supervisé

- Vérifier la connexion entre les deux postes (attention aux adresses IP)
- Configurer le service DHCP avec une étendue de 10 adresses, attention aux conflits.
- Activer si nécessaire cette nouvelle étendue (pour la question 10).

sur la console de supervision

Installer iReasoning MIB browser pour collecter les informations d'un agent SNMP.

(site : <http://ireasoning.com>)



Installation du service SNMP sur les deux postes

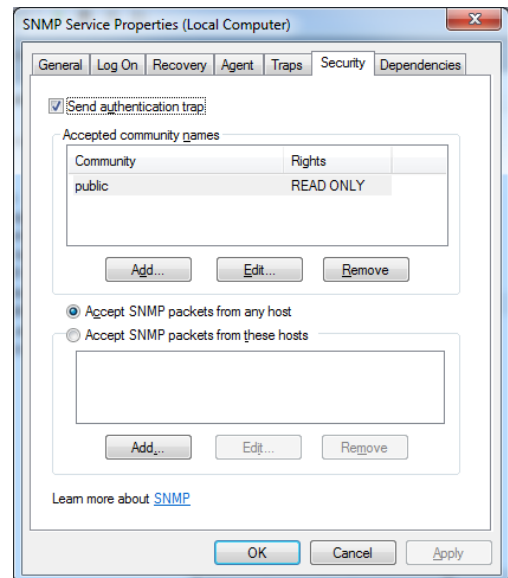
Sous windows 7

Ouvrir "Panneau de Configuration/Programmes et Fonctionnalités", cliquer "Activer/désactiver les fonctionnalités de Windows", et cochez SNMP:

Configurer le service SNMP

Ouvrir "Service/SNMP", sélectionner l'onglet "Sécurité", Assurez

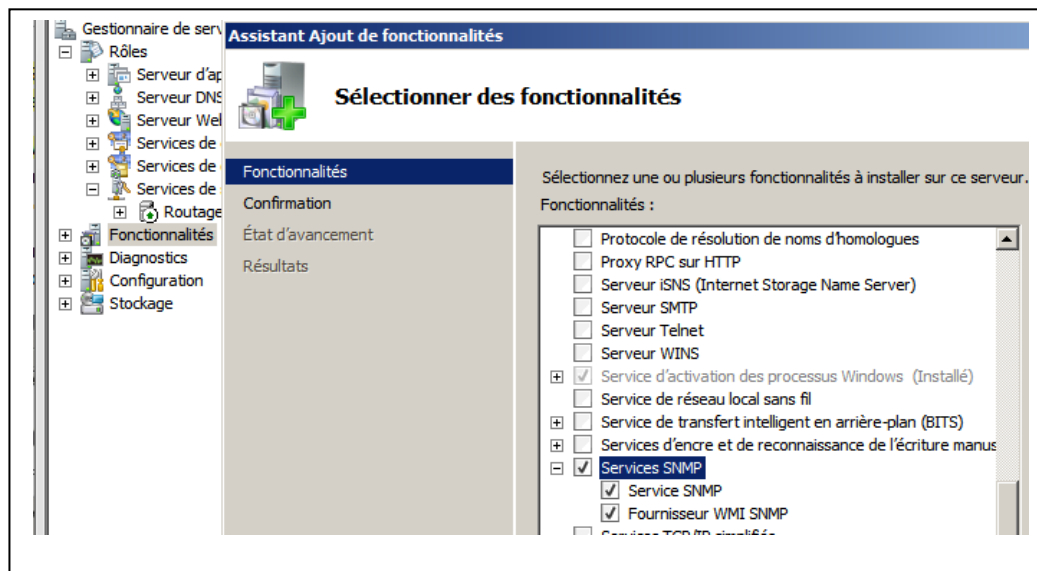
vous qu'il y a au moins une communauté (généralement : **public**). Si d'autre hôtes ont besoin d'avoir accès à ce service SNMP, validez l'option "Accepter les paquets SNMP provenant de n'importe quel hôte".



Sous windows 2008

Afin de faire fonctionner la remonté d'informations SNMP, il faut que le service SNMP soit démarré. S'il n'est pas présent, il faut l'installer. Il est déjà préconfiguré sur les templates VMware Windows 2003 et 2008.

Sous Windows 2008, c'est une fonctionnalité à ajouter et qui ne nécessite pas le CD de windows pour être installé. Néanmoins, on est obligé de **redémarrer le service** pour avoir accès aux informations de configuration.



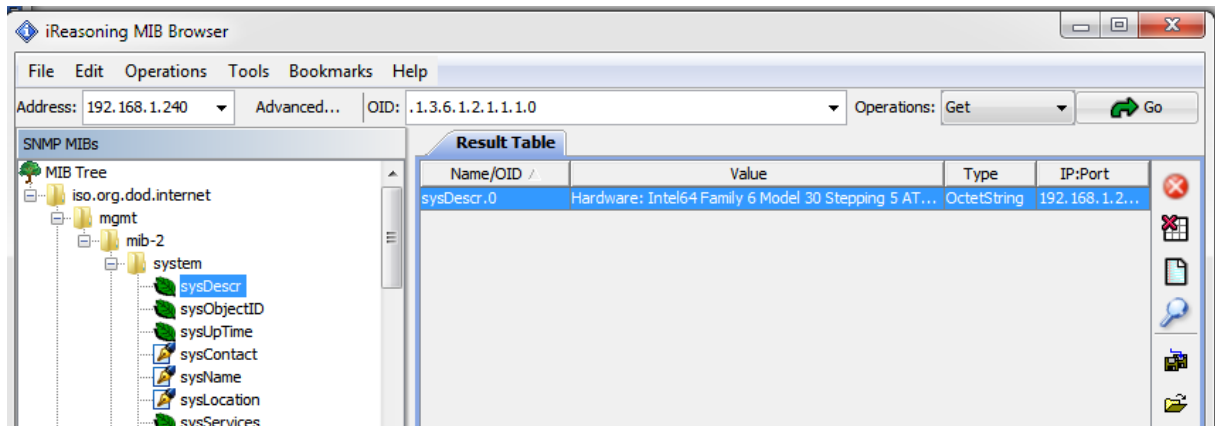
- Puis clic droit sur service SNMP, Propriétés, Onglet Sécurité,
- Pour les noms des communautés acceptées, bouton Ajouter, **nom : public**
- Accepter les paquets SNMP provenant de n'importe quel hôte.**
- Bouton Appliquer et fermer la console Service.
- redémarrer le service**

Afficher les données via SNMP et Mib Browser

Dans cette phase, vous allez employer **MibBrowser** pour vérifier que l'agent SNMP est bien configuré pour communiquer avec un gestionnaire SNMP.

Configurer MibBrowser pour obtenir des infos sur le serveur 2008

- **Ip** de la machine supervisée :
- **Communauté** : public
- **SNMP** version 2
- **OID** .1.3.6.1.2.1.1.1.0 → GET + GO



Qu'obtient-on ?

VariableValue L'OID peut-être remplacé par le nom de la variable, donner la commande du a) en remplaçant l'OID par le nom de la variable : (**attention à la casse**)

Nom correspondant :

Afficher le contenu de l'OID .1.3.6.1.2.1.1.5.0

Qu'obtient-on ?

Name/OID:

Value (Integer):

on peut aussi utiliser la MIB pour stocker ses propres informations.

Plus précisément, il existe deux champs de type string qui peuvent être utilisés et interrogés via SNMP : **SysLocation** et **SysContact**

Ces deux champs sont en fait deux clés de registres. Si ces deux clefs sont renseignées on peut alors obtenir leurs valeurs par une simple requête SNMP

Ouvrez la base de registre avec **Regedit**, Allez à la clef :

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\SNMP\Parameters\RFC1156Agent

Donnez à la clef **sysLocation** la valeur CACHAN

Donnez à la clef **sysContact** le valeur LMSAdmin@sio.lms

Appuyez sur F5 pour mettre à jour la base de registre.

Tester avec **Mib Browser** sur la machine supervisée les variables, donner l'oid et la valeur de :
sysLocation
sysContact

Capture des trames SNMP

- lancer une capture de trames sur la carte réseau concernée,
- A partir du poste client, lancer une commande **Mib Browser**
- Dans la console du moniteur réseau, Arrêter et afficher la capture.

-Combien de trames SNMP ?
-Quelle est la version du protocole SNMP :.
-Quel est le protocole de niveau transport utilisé :
-Quel est le port utilisé par le protocole SNMP:

Partie 3 : Parcourir la MIB . Utilisation de getnext et walk

La **commande get** permet d'obtenir la valeur d'une variable désignée et la **commande getnext** permet d'obtenir la valeur de la prochaine variable. Faire les tests avec les commandes suivantes :

- **commande Get avec OID .1.3.6.1.2.1.1.1**
Résultat :

-- **commande GetNext avec OID.1.3.6.1.2.1.1.1**
Résultat:

-- -- **commande GetNext avec OID.1.3**
Résultat:

-- **commande Walk avec OID.1.3**
Résultat : combien d'entrées environ ? Quel type d'infos peut-on récupérer ?

-Dans l'arborescence, sélectionner **la branche IP** sélectionner Get SubTree bouton GO
Retrouver l'adresse physique de la carte réseau :

-Dans l'arborescence, sélectionner **la branche IP** sélectionner Get SubTree bouton GO
Retrouver le nombre de datagrammes reçus par l'hôte :
Variable

-Dans l'arborescence, sélectionner **la branche ICMP** sélectionner Get SubTree bouton GO
Retrouver le nombre de messages ICMP reçus par l'hôte :
Variable

Retester après un ping sur l'hôte

*La nature nous a donné deux oreilles et seulement une langue afin de
pouvoir écouter davantage et parler moins.
-- Zénon D'Elée --*

Ecrire grâce à la MIB

- Ajouter sur l'hôte supervisé, une **communauté SNMPv2 en lecture/écriture appelée private**
- Modifier les paramètres (Advanced) de MibBrowser pour prendre en compte les possibilités d'écriture

Modifier avec **Mib Browser (set)** sur la machine supervisée les variables avec les valeurs suivantes :

sysLocation : STS SIO

sysContact : SISRAAdmin@sio.lms

commentaire :

Partie 4 Configuration de la MIB privée

Rechercher sur le serveur l'OID .1.3.6.1.4.1.311.1.3.1.1.0

Afin d'exploiter au maximum les possibilités des divers composants des réseaux, les constructeurs ajoutent souvent des informations spécifiques à tel ou tel agent. Ces informations constituent la **MIB privée** et tous les clients ne sont pas capables de lire les MIB privées.

- récupérer les mibs complémentaires

<http://www.oidview.com/mibs/311/DHCP-MIB.html>

-ajouter **DHCP-MIB** Ceci ajoute 19 entrées

Statistics for **MIB DHCP-MIB:**

Objects: 19

OIDS: 17

Object Groups: 0

Traps: 0


















Notifications: 0

Notification Groups: 0

Tables: 1

Tabulars: 4

Scalars/Other: 12

Object Name	Object Identifier
 dhcp	1.3.6.1.4.1.311.1.3
 dhcpPar	1.3.6.1.4.1.311.1.3.1
 parDhcpStartTime	1.3.6.1.4.1.311.1.3.1.1
 parDhcpTotalNoOfDiscovers	1.3.6.1.4.1.311.1.3.1.2
 parDhcpTotalNoOfRequests	1.3.6.1.4.1.311.1.3.1.3
 parDhcpTotalNoOfReleases	1.3.6.1.4.1.311.1.3.1.4
 parDhcpTotalNoOfOffers	1.3.6.1.4.1.311.1.3.1.5
 parDhcpTotalNoOfAcks	1.3.6.1.4.1.311.1.3.1.6
 parDhcpTotalNoOfNacks	1.3.6.1.4.1.311.1.3.1.7
 parDhcpTotalNoOfDeclines	1.3.6.1.4.1.311.1.3.1.8
 dhcpScope	1.3.6.1.4.1.311.1.3.2
 scopeTable	1.3.6.1.4.1.311.1.3.2.1
 scopeTableEntry	1.3.6.1.4.1.311.1.3.2.1.1
 subnetAdd	1.3.6.1.4.1.311.1.3.2.1.1.1
 noAddInUse	1.3.6.1.4.1.311.1.3.2.1.1.2
 noAddFree	1.3.6.1.4.1.311.1.3.2.1.1.3
 noPendingOffers	1.3.6.1.4.1.311.1.3.2.1.1.4

Rechercher à nouveau sur le serveur l'OID .1.3.6.1.4.1.311.1.3.1.1.0

Rechercher sur la console de supervision l'OID .1.3.6.1.4.1.311.1.3.1.1.0

-Pour le serveur DHCP, retrouver le nombre d'adresses **IP non attribuées**
OID variable

-Configurer le poste console en client DHCP, lancer ipconfig/renew

-Vérifier le **nombre d'IP libres sur le serveur DHCP**
résultat :

-Remettre le poste client en adresse IP fixe (toujours compatible avec le serveur)

Arrêter le service DHCP

Partie 5 : Messages d'alerte de l'agent SNMP : TRAP

On vient de voir que l'agent SNMP peut être sollicité au travers de commandes ou de requêtes SNMP (get, getnext, walk, set) afin d'obtenir différentes informations de la base de données MIB. Mais il peut aussi envoyer des messages d'alerte (traps) au Manager sans forcément être sollicité (vu de la console de supervision, il s'agit du **mode passif**).

Alerte sur les tentatives d'accès non autorisées à l'agent SNMP

Configuration du **service SNMP sur 2008**

service SNMP, Propriétés, **Onglet Interruptions**,

- Saisir le nom de la **communauté** : « **public** » dans la liste déroulante et Ajouter à la liste,
- Pour la destination des interruptions, bouton Ajouter, saisir l'adresse IP de la console
- Bouton Appliquer et fermer la console Service.

Configurer Windows pour envoyer des alertes SNMP

Il est possible de configurer Windows pour rediriger des messages d'erreurs de l'observateur d'événements, sous forme d'alerte SNMP(trap). L'outil utilisé est **evntwin.exe**, il permet donc de **convertir un événement en interruption SNMP**.

Dans cette dernière étape, vous allez configurer le poste supervisé pour envoyer une alerte SNMP à la console, lorsqu'il détecte un conflit d'adresse IP.- lancer l'outil **evntwin.exe** en ligne de commande

- Sélectionner **personnalisée** dans type de configuration et **bouton Modifier**,
- Dans la fenêtre sources de l'événement, développer **DNS Server /DNS**
- Dans la fenêtre de droite, Événements, faire un double clic sur **l'événement N°3**,
- Dans la description, à quel problème correspond cet événement ?

-Bouton Ok pour valider, bouton Appliquer et OK pour fermer le convertisseur d'événement.

Test à partir de la console

- Tools / Trap Receiver (cette fenêtre est en attente d'alerte SNMP)
- Lancer l'analyse de trames

Sur le serveur2008 - arrêter le service DNS

- Sur quel **port a été transmise l'alerte** ?
- Quelles autres infos peut-on récupérer ? :

Tester d'autres événements :

System\ntfs, événement 3 7, Un utilisateur a atteint son quota sur le volume
Conflit d'adresses IP ...