



**Instituto Politécnico Nacional
Escuela Superior de Cómputo
Academia de Ingeniería de Software**



Práctica 1

Integrantes del equipo:

**Castro Flores Marcela
Sánchez Cruz Rosa María
Santiago Mancera Arturo Samuel**

M. en C. Tanibet Pérez de los Santos Mondragón

México, Ciudad de México a 5 de de septiembre de 2018

Índice general

1. Introducción	5
2. Gestor y agentes	6
2.1. Observium	6
2.2. Configuración de agente en Linux	6
2.3. Configuración de agente en Windows	12
3. Cuestionario	16
3.1. Cuestionario	16
4. Marco teórico	19
4.1. Seccion	19
4.1.0.1. Subseccion	19

Índice de figuras

2.1. Configuración de snmp (1).	7
2.2. Configuración de snmp (2).	8
2.3. Archivo de configuración finalizado.	9
2.4. Archivo de hosts Observium.	10
2.5. Ping a Linux.	10
2.6. Agente añadido.	11
2.7. Información del agente.	11
2.8. Características de Windows.	12
2.9. Protocolo SNMP.	12
2.10. Captura SNMP.	13
2.11. Comunidad SNMP.	13
2.12. Permisos de la comunidad.	14
2.13. Servicio SNMP.	14
2.14. Firewall de Windows.	15
3.1. Último reinicio del agente en Linux.	16
3.2. Último reinicio del agente en Windows.	16
3.3. Número de interfaces Ethernet en Linux.	17
3.4. Número de interfaces Ethernet en Windows.	17
3.5. Velocidad de las interfaces en Linux.	17
3.6. Velocidad de las interfaces en Windows.	18

Índice de cuadros

CAPÍTULO 1

Introducción

Aquí va la introducción

BLABLABLABALABA [1].

2.1. Observium

2.2. Configuración de agente en Linux

Una vez que se realizó la instalación de Observium, continuamos con la instalación de la máquina virtual en Linux, en este caso, se utilizó Linux de forma nativa por lo cual pasamos directamente a la instalación de los paquetes “SNMP” y “SNMPD” por medio de la instrucción en consola:

- **sudo apt-get install snmp snmpd**

Posteriormente, se realizó la configuración del protocolo SNMP por medio del comando:

- **snmpconf – r none – g basic _ setup**

Se puede observar en la figura 2.1 el procedimiento que nos apareció al ejecutar el comando anterior. A continuación se enlistarán las opciones que fueron seleccionadas en el transcurso de dicha configuración:

- Configurar la información devuelta en el sistema del grupo de la MIB.
- Ingresamos un nombre para el almacenamiento del sistema.
- Agregamos un correo electrónico.
- Seleccionamos que no deseabamos configurar el valor de sysService.
- Sí configuramos el agente de control de acceso.
- No permitimos el acceso basado en usuario SNMPv3 de solo escritura.
- No permitimos el acceso basado en usuario SNMPv3 de solo lectura.
- Sí permitimos el acceso de la comunidad SNMPv1/v2c de lectura–escritura.
- Añadimos un nombre a la comunidad de acceso de lectura–escritura.
- Seleccionamos que no deseabamos agregar otra línea a rwcommunity.
- Por último, no permitimos que la comunidad SNMPv1/v2c tuviera acceso de solo lectura.

```

~ snmpconf -r none -g basic setup
*****
*** Beginning basic system information setup ***
*****
Do you want to configure the information returned in the system MIB group (contact info, etc)? (default = y): y

Configuring: syslocation
Description:
  The [typically physical] location of the system.
  Note that setting this value here means that when trying to
  perform an snmp SET operation to the sysLocation.0 variable will make
  the agent return the "notWritable" error code. IE, including
  this token in the snmpd.conf file will disable write access to
  the variable.
  arguments: location_string

The location of the system: Laboratorio progra 1

Finished Output: syslocation "Laboratorio progra 1"

Configuring: syscontact
Description:
  The contact information for the administrator
  Note that setting this value here means that when trying to
  perform an snmp SET operation to the sysContact.0 variable will make
  the agent return the "notWritable" error code. IE, including
  this token in the snmpd.conf file will disable write access to
  the variable.
  arguments: contact_string

The contact information: march.castrof@gmail.com

Finished Output: syscontact march.castrof@gmail.com
Do you want to properly set the value of the sysServices.0 OID (if you don't know, just say no)? (default = y): n
*****
*** BEGINNING ACCESS CONTROL SETUP ***
*****
Do you want to configure the agent's access control? (default = y): y
Do you want to allow SNMPv3 read-write user based access (default = y): n
Do you want to allow SNMPv3 read-only user based access (default = y): n
Do you want to allow SNMPv1/v2c read-write community access (default = y): y

Configuring: rwcommunity
Description:
  a SNMPv1/SNMPv2c read-write access community name
  arguments: community [default|hostname|network/bits] [oid]

Enter the community name to add read-write access for: comunidadMarcela
The hostname or network address to accept this community name from [RETURN for all]:
The OID that this community should be restricted to [RETURN for no-restriction]:

Finished Output: rwcommunity comunidadMarcela
Do another rwcommunity line? (default = y): n
Do you want to allow SNMPv1/v2c read-only community access (default = y): n
*****

```

Figura 2.1: Configuración de snmp (1).

Una vez finalizada toda la configuración básica, continuamos con la siguiente parte de la configuración mostrada en la figura 2.2, en la cual se indicaron únicamente dos partes:

- No se configuró si el agente enviaría traps (trampas).
- No se configuró la habilidad al agente para monitorear el sistema.

Es importante recalcar que una vez finalizadas estas dos acciones, se muestra que el archivo nombrado como **snmpd.conf** fue creado pues fue el utilizado posteriormente.

```
*****
*** Beginning trap destination setup ***
*****
Do you want to configure where and if the agent will send traps? (default = y):
n
*****
*** Beginning monitoring setup ***
*****
Do you want to configure the agent's ability to monitor various aspects of your
system? (default = y): n

The following files were created:

  snmpd.conf

These files should be moved to /usr/share/snmp if you
want them used by everyone on the system.  In the future, if you add
the -i option to the command line I'll copy them there automatically for you.

Or, if you want them for your personal use only, copy them to
/home/marce/.snmp .  In the future, if you add the -p option to the
command line I'll copy them there automatically for you.
```

Figura 2.2: Configuración de snmp (2).

Como se mencionó anteriormente, ya que se generó nuestro archivo de la configuración, se cambió el lugar de almacenamiento a la carpeta correcta por medio del comando:

- **sudo mv snmpd.conf /etc/snmp/snmpd.conf**

Y una vez que este fue almacenado debidamente, se reinició el servicio snmpd mediante la instrucción:

- **sudo service snmpd restart**

Y finalmente, por medio del comando:

- **nano /etc/snmp/snmpd.conf**

pudimos acceder al archivo mostrado en la figura 2.3 en el cual podemos observar todo lo que se fue configurando y el cual es de mucha utilidad en caso de que hayamos olvidado el nombre de nuestra comunidad por ejemplo.


```

GNU nano 2.5.3      File: /etc/snmp/snmpd.conf
#####
#                               Arduino IDE
# snmpd.conf
# - created by the snmpconf configuration program
#
#####
# SECTION: Access Control Setup
#
#   This section defines who is allowed to talk to your running
#   snmp agent.
#
#   rwcommunity: a SNMPv1/SNMPv2c read-write access community name
#   arguments:  community [default|hostname|network/bits] [oid]
#
rwcommunity  comunidadMarcela
#
#####
# SECTION: System Information Setup
#
#   This section defines some of the information reported in
#   the "system" mib group in the mibII tree.
#
#   syslocation: The [typically physical] location of the system.
#   Note that setting this value here means that when trying to
#   perform an snmp SET operation to the sysLocation.0 variable will make
#   the agent return the "notWritable" error code.  IE, including
#   this token in the snmpd.conf file will disable write access to
#   the variable.
#   arguments:  location_string
#
syslocation  "Laboratorio progra 1"
#
#   syscontact: The contact information for the administrator
#   Note that setting this value here means that when trying to
#   perform an snmp SET operation to the sysContact.0 variable will make
#   the agent return the "notWritable" error code.  IE, including
#   this token in the snmpd.conf file will disable write access to
#   the variable.
#   arguments:  contact_string
#
syscontact  march.castrof@gmail.com


```

Figura 2.3: Archivo de configuración finalizado.

Después regresamos a nuestro gestor de Observium en el cual abrimos nuestro archivo de hosts haciendo uso de la instrucción:

- `nano /etc/hosts`

mismo que nos abrirá el archivo mostrado en la figura 2.4 en el cual agregamos la ip de nuestro sistema operativo Linux y un nombre identificador.



```

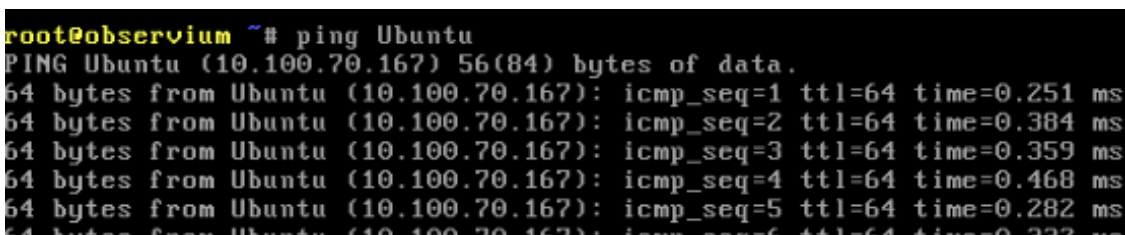
GNU nano 2.7.4      File: /etc/hosts      Modified
127.0.0.1 localhost
127.0.1.1 observium
10.100.77.167 Ubuntu
10.100.77.195 Windows

#Required for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts

^G Get Help  ^O Write Out ^W Where Is  ^R Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^_ Replace   ^U Uncut Text ^T To Spell  ^_ Go To Line
  
```

Figura 2.4: Archivo de hosts Observium.

Guardamos y salimos para finalmente probar el funcionamiento de nuestra conexión mediante un ping más el nombre identificador escrito que en este caso fue Ubuntu para obtener una la respuesta mostrada en la figura 2.5



```

root@observium ~# ping Ubuntu
PING Ubuntu (10.100.70.167) 56(84) bytes of data:
64 bytes from Ubuntu (10.100.70.167): icmp_seq=1 ttl=64 time=0.251 ms
64 bytes from Ubuntu (10.100.70.167): icmp_seq=2 ttl=64 time=0.384 ms
64 bytes from Ubuntu (10.100.70.167): icmp_seq=3 ttl=64 time=0.359 ms
64 bytes from Ubuntu (10.100.70.167): icmp_seq=4 ttl=64 time=0.468 ms
64 bytes from Ubuntu (10.100.70.167): icmp_seq=5 ttl=64 time=0.282 ms
64 bytes from Ubuntu (10.100.70.167): icmp_seq=6 ttl=64 time=0.337 ms
  
```

Figura 2.5: Ping a Linux.

Por último, entramos a nuestra dirección de Observium en el navegador para añadir un dispositivo para monitorearlo como se observa en la figura 2.6, esto añadiendo un hostname que en este caso fue **Ubuntu** y una comunidad SNMP, misma que debe ser el nombre de la comunidad que elegimos poner en nuestro archivo de configuración que fue **comunidadMarcela**.

The image shows the OBSERVUM web interface. The 'Basic Configuration' panel on the left includes fields for Hostname (Ubuntu), Skip PING (checked), Protocol Version (v2c), Transport (UDP), Port (161), Timeout (1), Retries (5), and Ignore existing RRDs (checked). The 'Authentication Configuration' panel on the right shows the SNMP Community (comunidadMarcela). A search bar and navigation icons are at the top. A 'Add device' button is at the bottom of the Basic Configuration panel.

Figura 2.6: Agente añadido.

Posteriormente, volvimos a la pestaña de Devices, seleccionamos All devices y aquí encontramos nuestro agente de Ubuntu como vemos en la figura 2.7, mismo que al seleccionar nos muestra las diferentes gráficas e información de este.

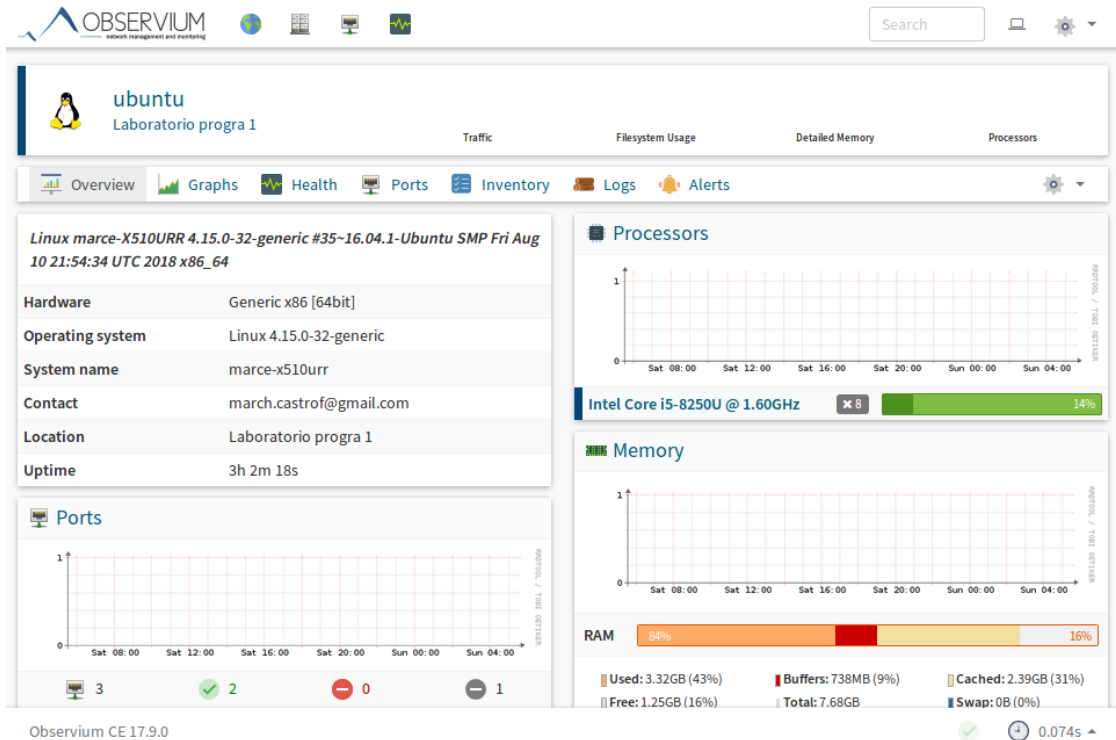


Figura 2.7: Información del agente.

2.3. Configuración de agente en Windows

Para la configuración de un agente en el sistema operativo Windows, se debe agregar una característica del sistema operativo. Esto con la finalidad de habilitar el servicio de "SNMP". Para habilitar la característica nos dirigimos al **Panel de control** de Windows y después a la sección de **Programas y características** como se muestra en la figura 2.8.

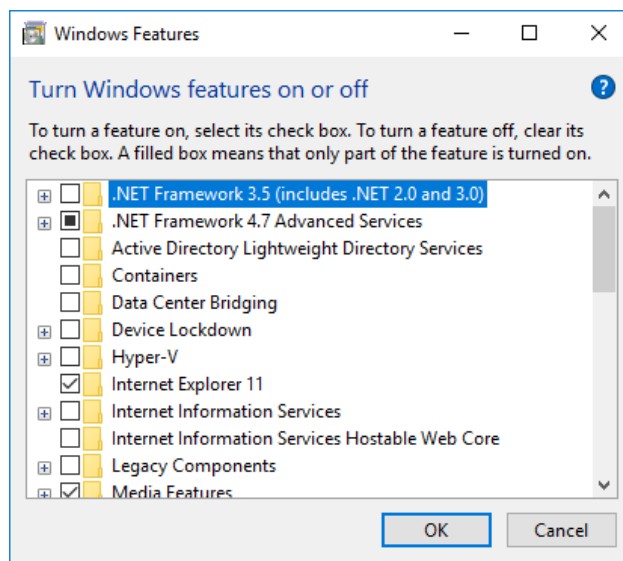


Figura 2.8: Características de Windows.

Una vez aquí debemos buscar el Protocolo Simple de Administración de Redes (SNMP) o *Simple Network Management Protocol (SNMP)* y activar su casilla correspondiente así como la de del nodo que se origina a partir de él tal y como se indica en la 2.9.

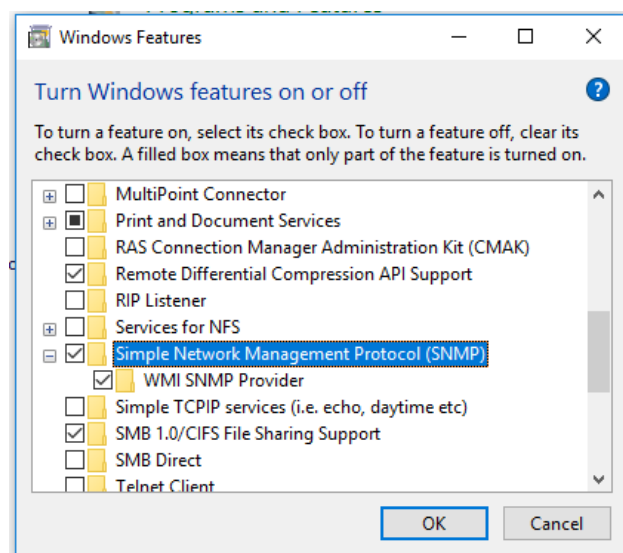


Figura 2.9: Protocolo SNMP.

El siguiente paso será iniciar el servicio de SNMP y de captura SNMP. Para ello entramos a los **Servicios**

de Windows y buscamos **Captura SNMP** o *SNMP Trap* como se indica en la figura 2.10. Hacemos clic derecho sobre él y lo iniciamos:

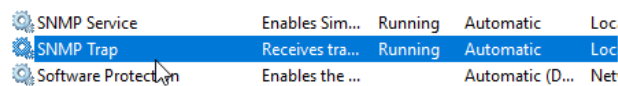


Figura 2.10: Captura SNMP.

Después, buscamos el servicio **SNMP** o *SNMP Service*, hacemos clic derecho sobre él y en la pestaña de **Capturas** o **Traps** ingresamos el nombre de la comunidad a la que pertenecerá el agente como se observa en la figura 2.11.

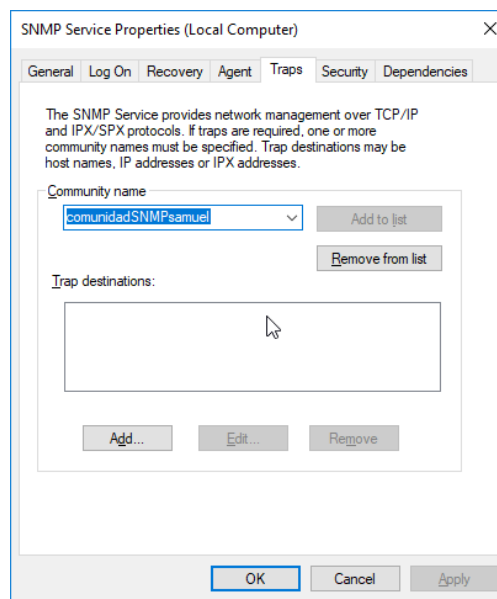


Figura 2.11: Comunidad SNMP.

Posteriormente, como observamos en la figura 2.12, debemos establecer los permisos que tendrá la comunidad anterior sobre el agente. Para ello, nos dirigimos a la pestaña de **Seguridad** o **Security**, hacemos clic en **Agregar** o **Add** y establecemos los permisos de **Lectura y Escritura** o **Read and Write**.

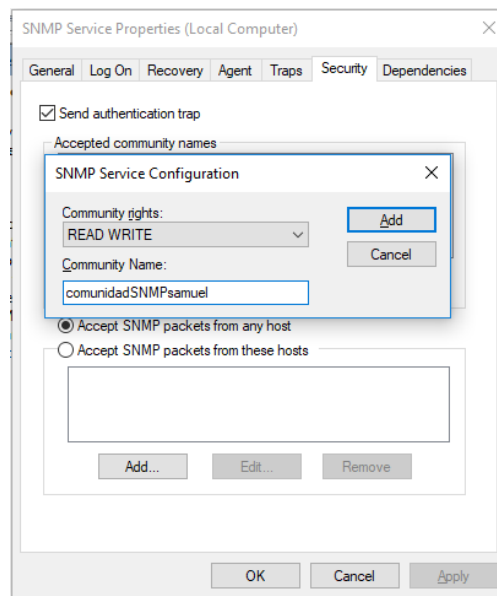


Figura 2.12: Permisos de la comunidad.

Finalmente, escribimos el nombre de la comunidad, tal y como se observa en la figura 2.13; y habilitamos la opción de **Aceptar paquetes de cualquier host**. Hacemos clic en **Aplicar**, **Aceptar** y reiniciamos el servicio de SNMP.

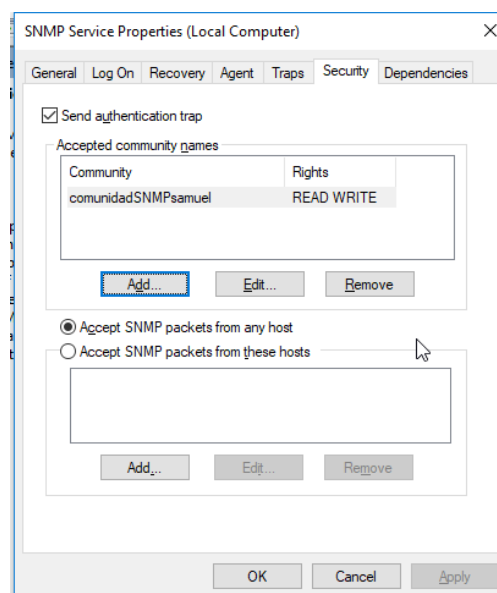


Figura 2.13: Servicio SNMP.

Como paso adicional, se deben agregar las reglas de firewall de Windows que permitan la transmisión y recepción de paquetes SNMP. Sin embargo, para este caso de prueba procederemos a desactivar completamente el firewall de Windows. En este caso, al ser una versión de Windows 10 nos dirigimos a **Windows Defender** y lo deshabilitamos:

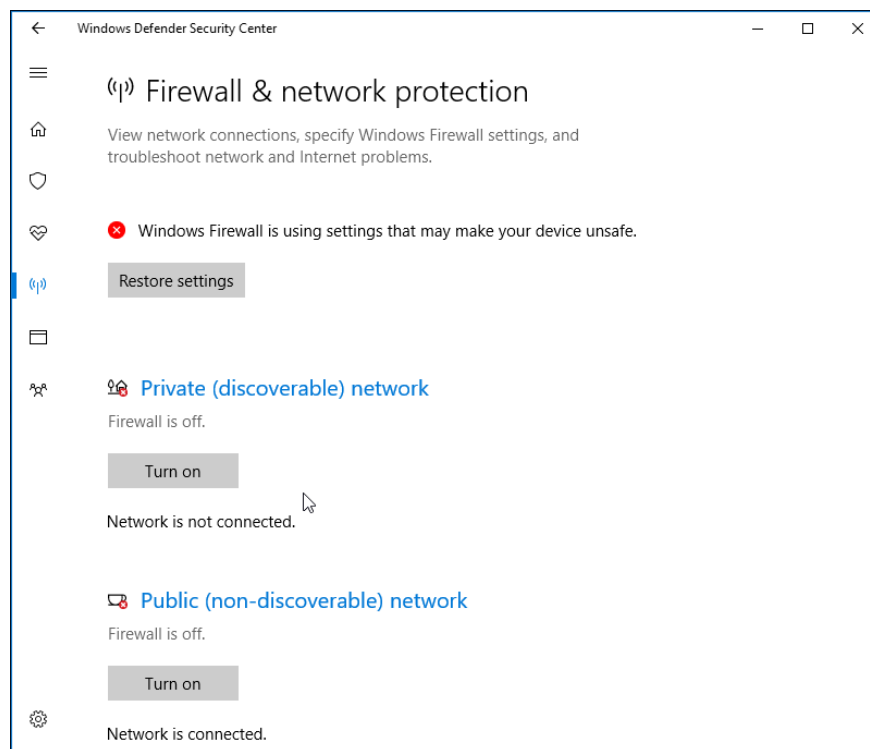


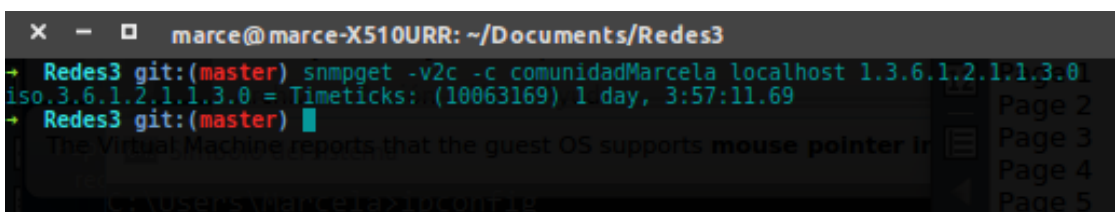
Figura 2.14: Firewall de Windows.

En este capítulo se observan las diferentes pantallas que responden a las consultas realizadas a la MIB desde Linux y desde Windows.

3.1. Cuestionario

1. ¿Cuándo fue el último reinicio (Día, hora y minuto) de los agentes?

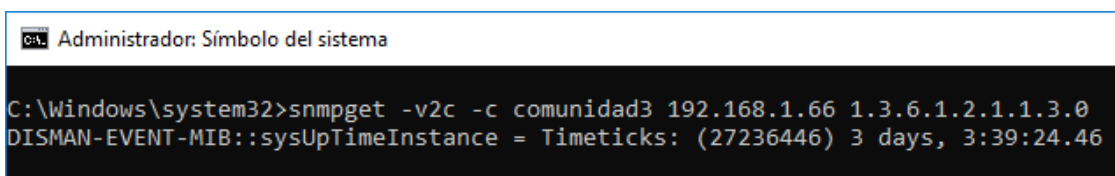
El resultado del último reinicio en Linux como se observa en la figura 3.1 fue:



```
marce@marce-X510URR: ~/Documents/Redes3
→ Redes3 git:(master) snmpget -v2c -c comunidadMarcela localhost 1.3.6.1.2.1.1.3.0
iso.3.6.1.2.1.1.3.0 = Timeticks: (10063169) 1 day, 3:57:11.69
→ Redes3 git:(master) █
```

Figura 3.1: Último reinicio del agente en Linux.

Por otro lado, el resultado del último reinicio en Windows como se observa en la figura 3.2 fue:



```
Administrador: Símbolo del sistema
C:\Windows\system32>snmpget -v2c -c comunidad3 192.168.1.66 1.3.6.1.2.1.1.3.0
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (27236446) 3 days, 3:39:24.46
```

Figura 3.2: Último reinicio del agente en Windows.

2. ¿Cuántas interfaces Ethernet tienen?

Se puede observar en la figura 3.3 resultado en Linux fue de una interfaz Ethernet.


```

+ Redes3 git:(master) * snmpwalk -v2c -c comunidadMarcela localhost 1.3.6.1.2.1.2.2.1.2
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "lo"
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "Intel Corporation Device 24fd"
iso.3.6.1.2.1.2.2.1.2.3 = STRING: "vboxnet0"
+ Redes3 git:(master) *

```

Figura 3.3: Número de interfaces Ethernet en Linux.

De igual manera, se puede observar en la figura 3.4 que el resultado en Windows fue de 4 interfaces Ethernet.

```

C:\Windows\system32>snmpwalk -v2c -c comunidad3 192.168.1.66 1.3.6.1.2.1.2.2.1.2
IF-MIB::ifDescr.1 = STRING: Software Loopback Interface 1
IF-MIB::ifDescr.2 = STRING: Microsoft 6to4 Adapter
IF-MIB::ifDescr.3 = STRING: Microsoft IP-HTTPS Platform Adapter
IF-MIB::ifDescr.4 = STRING: Microsoft Kernel Debug Network Adapter
IF-MIB::ifDescr.5 = STRING: Microsoft Teredo Tunneling Adapter
IF-MIB::ifDescr.6 = STRING: Intel(R) PRO/1000 MT Desktop Adapter
IF-MIB::ifDescr.7 = STRING: Intel(R) PRO/1000 MT Desktop Adapter-WFP Native MAC Layer LightWeight Filter-0000
IF-MIB::ifDescr.8 = STRING: Intel(R) PRO/1000 MT Desktop Adapter-QoS Packet Scheduler-0000
IF-MIB::ifDescr.9 = STRING: Intel(R) PRO/1000 MT Desktop Adapter-WFP 802.3 MAC Layer LightWeight Filter-0000

```

Figura 3.4: Número de interfaces Ethernet en Windows.

3. ¿Cuál es la velocidad (en MBPS) de esas interfaces?

El resultado en Linux mostrado en la figura 3.5 fue:

- lo = 100000000
- Intel Corporation Device 24fd = 0
- vboxnet0 = 100000000

Sin embargo, es importante recalcar que en este caso, aunque la interfaz Ethernet corresponder a la llamada "Intel Corporation Device 24fd", su velocidad aparece ser de 0 mbps debido a que esta está obteniendo el ancho de banda vía wi-fi y no de forma alámbrica.

```

+ Redes3 git:(master) * snmpwalk -v2c -c comunidadMarcela localhost 1.3.6.1.2.1.2.2.1.2
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "lo"
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "Intel Corporation Device 24fd"
iso.3.6.1.2.1.2.2.1.2.3 = STRING: "vboxnet0"
+ Redes3 git:(master) * snmpwalk -v2c -c comunidadMarcela localhost 1.3.6.1.2.1.2.2.1.5
iso.3.6.1.2.1.2.2.1.5.1 = Gauge32: 10000000
iso.3.6.1.2.1.2.2.1.5.2 = Gauge32: 0
iso.3.6.1.2.1.2.2.1.5.3 = Gauge32: 10000000

```

Figura 3.5: Velocidad de las interfaces en Linux.

En el caso de Windows, el resultado mostrado en la figura 3.6 fue:

- Software Loopback Interface 1 = 1073741824
- Microsoft 6to4 Adapter = 0
- Microsoft IP-HTTPS Platform Adapter = 0
- Microsoft Kernel Debug Network Adapter = 0
- Microsoft Teredo Tunneling Adapter = 0
- Intel(R) PRO/1000 MT Desktop Adapter = 1000000000
- Intel(R) PRO/1000 MT Desktop Adapter-WFP Native MAC Layer LightWeight Filter-0000 = 1000000000
- Intel(R) PRO/1000 MT Desktop Adapter-QoS Packet Scheduler-0000 = 1000000000

- Intel(R) PRO/1000 MT Desktop Adapter-WFP 802.3 MAC Layer LightWeight Filter-0000 = 1000000000

```
C:\Windows\system32>snmpwalk -v2c -c comunidad3 192.168.1.66 1.3.6.1.2.1.2.2.1.2
IF-MIB::ifDescr.1 = STRING: Software Loopback Interface 1
IF-MIB::ifDescr.2 = STRING: Microsoft 6to4 Adapter
IF-MIB::ifDescr.3 = STRING: Microsoft IP-HTTPS Platform Adapter
IF-MIB::ifDescr.4 = STRING: Microsoft Kernel Debug Network Adapter
IF-MIB::ifDescr.5 = STRING: Microsoft Teredo Tunneling Adapter
IF-MIB::ifDescr.6 = STRING: Intel(R) PRO/1000 MT Desktop Adapter
IF-MIB::ifDescr.7 = STRING: Intel(R) PRO/1000 MT Desktop Adapter-WFP Native MAC Layer LightWeight Filter-0000
IF-MIB::ifDescr.8 = STRING: Intel(R) PRO/1000 MT Desktop Adapter-QoS Packet Scheduler-0000
IF-MIB::ifDescr.9 = STRING: Intel(R) PRO/1000 MT Desktop Adapter-WFP 802.3 MAC Layer LightWeight Filter-0000

C:\Windows\system32>snmpwalk -v2c -c comunidad3 192.168.1.66 1.3.6.1.2.1.2.2.1.5
IF-MIB::ifSpeed.1 = Gauge32: 1073741824
IF-MIB::ifSpeed.2 = Gauge32: 0
IF-MIB::ifSpeed.3 = Gauge32: 0
IF-MIB::ifSpeed.4 = Gauge32: 0
IF-MIB::ifSpeed.5 = Gauge32: 0
IF-MIB::ifSpeed.6 = Gauge32: 1000000000
IF-MIB::ifSpeed.7 = Gauge32: 1000000000
IF-MIB::ifSpeed.8 = Gauge32: 1000000000
IF-MIB::ifSpeed.9 = Gauge32: 1000000000
```

Figura 3.6: Velocidad de las interfaces en Windows.

- ¿Cuál es la interfaz que ha recibido el mayor número de octetos?
- Indica el número de octetos de la interfaz que ha recibido el mayor número de octetos
- ¿Cuál es la MAC de esa interfaz?
- ¿Cuál es la ip de la Interfaz que ha recibido el mayor número de octetos?
- ¿Cuántos mensajes ICMP ha recibido el agente?
- ¿Cuántas entradas tiene la tabla de enrutamiento IP?
- ¿Cuál es la interfaz que ha recibido el mayor número de octetos?
- Indica el número de octetos de la interfaz que ha recibido el mayor número de octetos
- ¿Cuál es la MAC de esa interfaz?
- ¿Cuál es la ip de la Interfaz que ha recibido el mayor número de octetos?
- ¿Cuántos mensajes ICMP ha recibido el agente?
- ¿Cuántas entradas tiene la tabla de enrutamiento IP?
- ¿Cuántos datagramas UDP ha recibido el agente?
- ¿El agente ha recibido mensajes TCP? ¿Cuántos?
- ¿Cuántos mensajes EGP ha recibido el agente?
- Indica el Sistema Operativo que maneja el agente.
- Modifica el estatus administrativo (a down) de la interfaz que ha recibido más octetos.
- Genera una alerta para avisar cuando se reinicie el agente.
- Dibuja la MIB del agente.

BLABLA

4.1. Seccion

UN PARRAFO

OTRO PARRAFO [1].

4.1.0.1. Subseccion

JAJAJAJAJ.

BLABLABLABLABALBALBAA

Referencias y bibliografías

- [1] MITCHELL, T. (1997), *Machine Learning*. 1st ed. McGraw-Hill Science/Engineering/Math.