

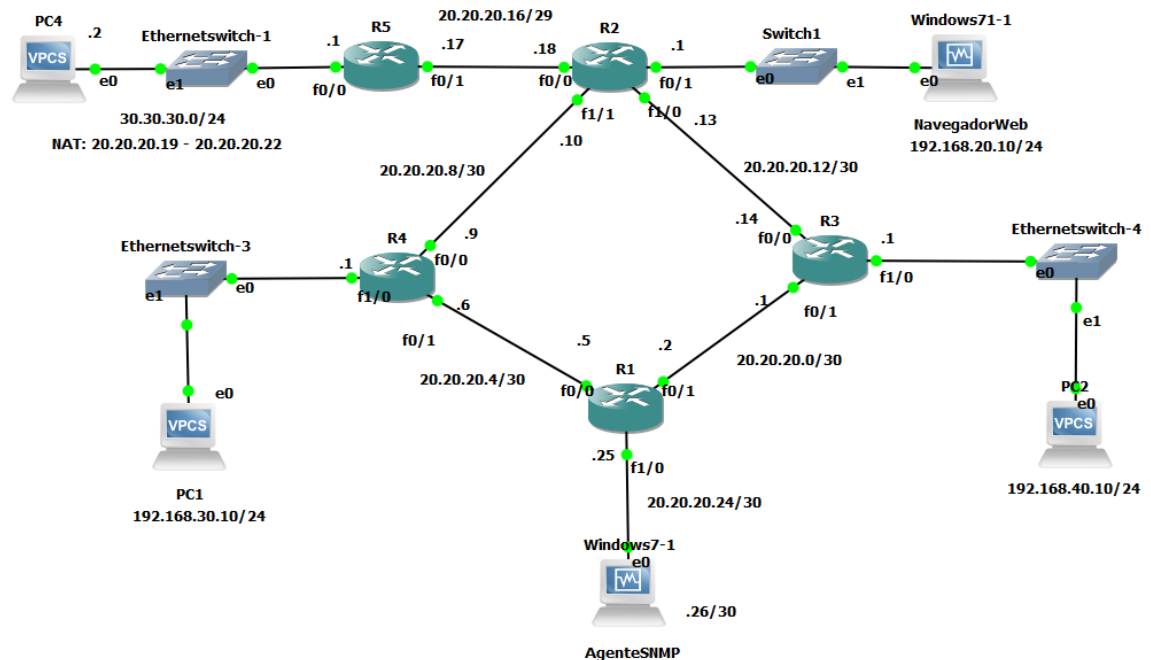
Examen 2° Parcial: Administración de Servicios en Red

Importante

Dentro de este examen, se utilizaron los routers 7200 junto con las máquinas virtuales que tienen Windows 7 la cual contiene el programa de MIB Browser la cual tiene las características necesarias para cumplir los requisitos que nos pide el examen.

Desarrollo

1. Se configuro la topología requerida en el examen con los routers antes mencionados.



2. Se realizo la conexión con OSPF en las diferentes áreas que se encontraron. En esta parte se encontraron que existían 5 áreas sin contar el área 0.

```
router ospf 1
 network 20.20.20.4 0.0.0.3 area 0
 network 20.20.20.8 0.0.0.3 area 0
 network 192.168.30.0 0.0.0.255 area 4
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
```

3. Se configuro DHCP en los routers donde se requerían.

```
ip dhcp excluded-address 192.168.30.1
!
ip dhcp pool red3
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 10.2.9.84
!
```

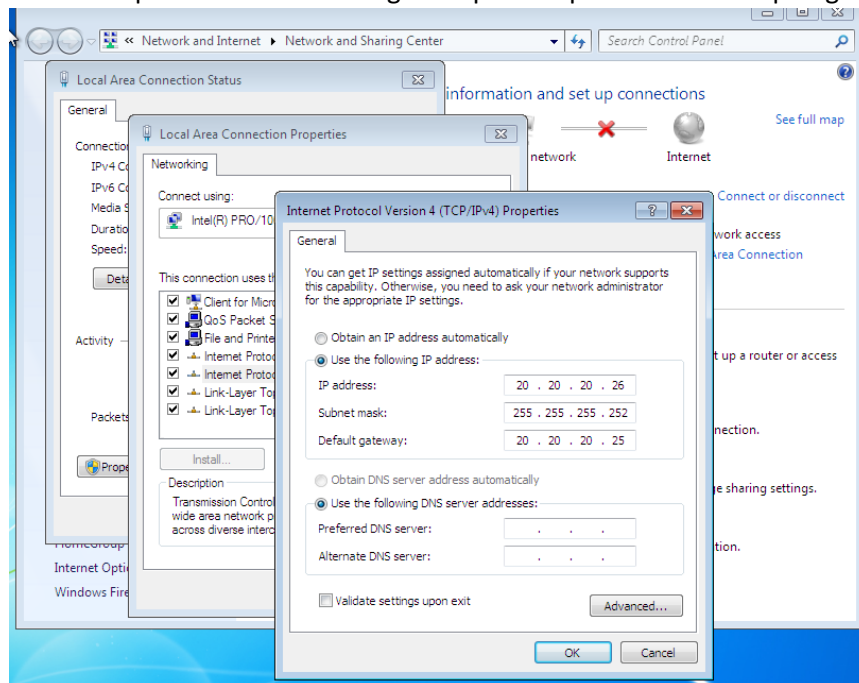
4. En el router 5 se configuro NAT como se pedían en los requerimientos y en los puntos a evaluar.

```
ip nat pool NAT-POOL 20.20.20.19 20.20.20.22 netmask 255.255.255.248
ip nat inside source list 1 pool NAT-POOL
!
access-list 1 permit 30.30.30.0 0.0.0.255
no cdp log mismatch duplex
!
```

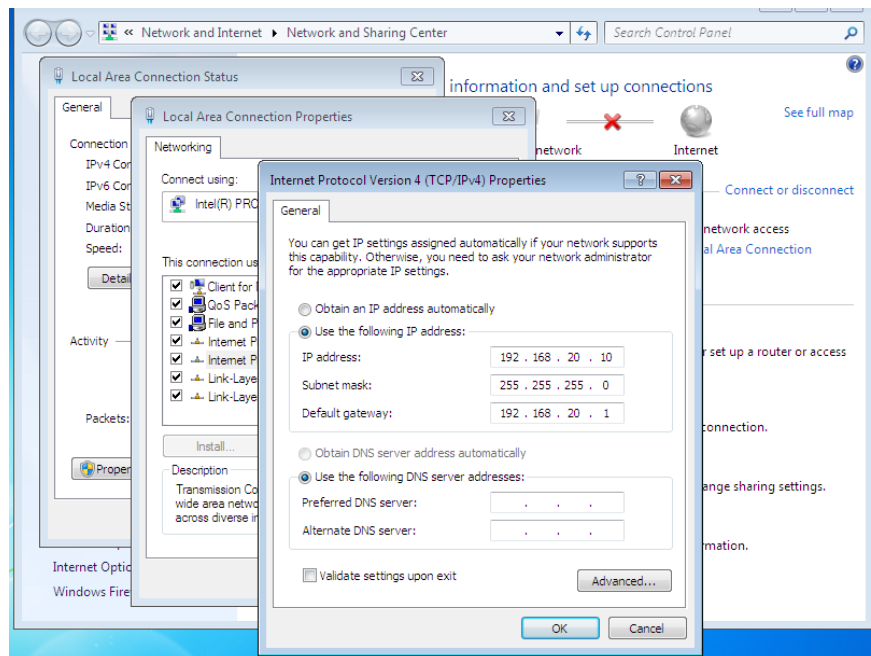
5. Se configuraron los routers del 1 al 4 con SNMP versión 3 con la información proporcionada en el PDF dado por el profesor.

```
snmp-server group 4CM1 v3 priv read V3Read write V3Write
snmp-server view V3Read iso included
snmp-server view V3Write iso included
snmp-server community ro_4CM1 RO SNMP_ACL
snmp-server community rw_4CM1 RW SNMP_ACL
snmp-server location ESCOM_4CM1
snmp-server contact enriquebroly@hotmail.com
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps flowmon
snmp-server enable traps ds1
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps gatekeeper
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps xgcp
snmp-server enable traps entity-sensor threshold
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps flash insertion removal
snmp-server enable traps srp
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
!
```

6. Dentro de cada máquina virtual se les asigno el ip correspondiente a la topología.

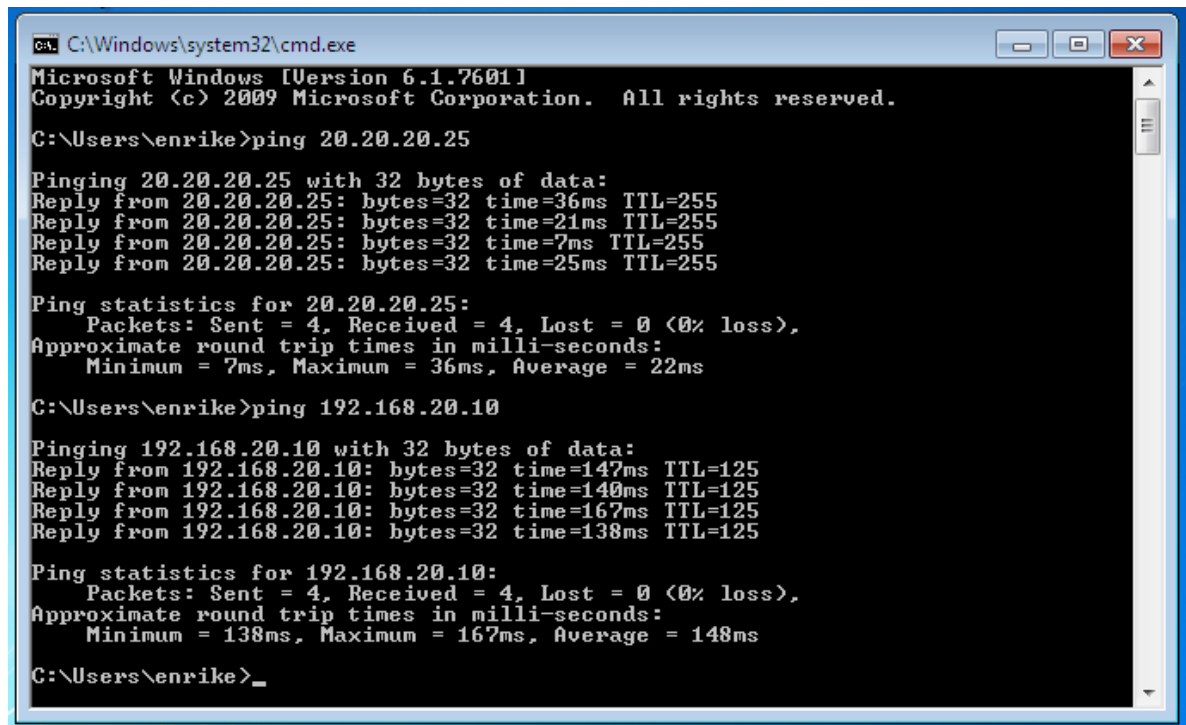


IP Agente SNMP



IP Navegador Web

7. Ambos después de la asignación de sus respectivas IP se prueban con un ping si su conexión en correcta.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\enrike>ping 20.20.20.25

Pinging 20.20.20.25 with 32 bytes of data:
Reply from 20.20.20.25: bytes=32 time=36ms TTL=255
Reply from 20.20.20.25: bytes=32 time=21ms TTL=255
Reply from 20.20.20.25: bytes=32 time=7ms TTL=255
Reply from 20.20.20.25: bytes=32 time=25ms TTL=255

Ping statistics for 20.20.20.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 7ms, Maximum = 36ms, Average = 22ms

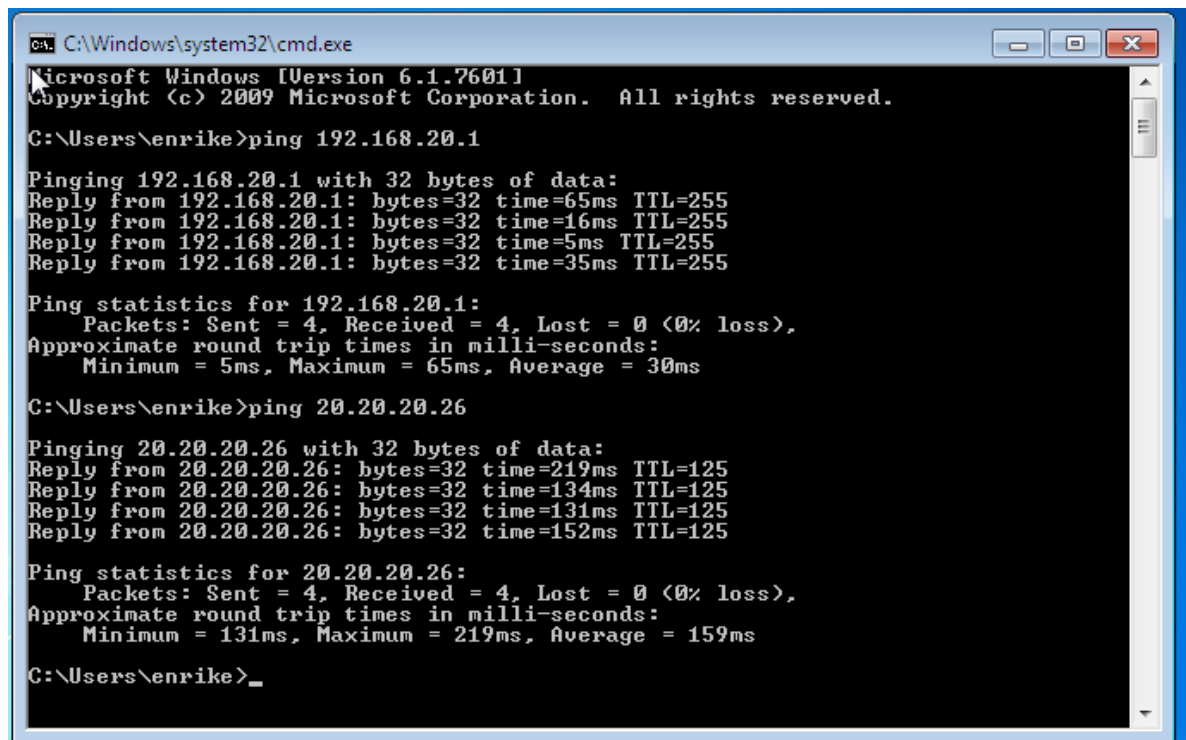
C:\Users\enrike>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time=147ms TTL=125
Reply from 192.168.20.10: bytes=32 time=140ms TTL=125
Reply from 192.168.20.10: bytes=32 time=167ms TTL=125
Reply from 192.168.20.10: bytes=32 time=138ms TTL=125

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 138ms, Maximum = 167ms, Average = 148ms

C:\Users\enrike>_
```

Ping Agente SNMP



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\enrike>ping 192.168.20.1

Pinging 192.168.20.1 with 32 bytes of data:
Reply from 192.168.20.1: bytes=32 time=65ms TTL=255
Reply from 192.168.20.1: bytes=32 time=16ms TTL=255
Reply from 192.168.20.1: bytes=32 time=5ms TTL=255
Reply from 192.168.20.1: bytes=32 time=35ms TTL=255

Ping statistics for 192.168.20.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 65ms, Average = 30ms

C:\Users\enrike>ping 20.20.20.26

Pinging 20.20.20.26 with 32 bytes of data:
Reply from 20.20.20.26: bytes=32 time=219ms TTL=125
Reply from 20.20.20.26: bytes=32 time=134ms TTL=125
Reply from 20.20.20.26: bytes=32 time=131ms TTL=125
Reply from 20.20.20.26: bytes=32 time=152ms TTL=125

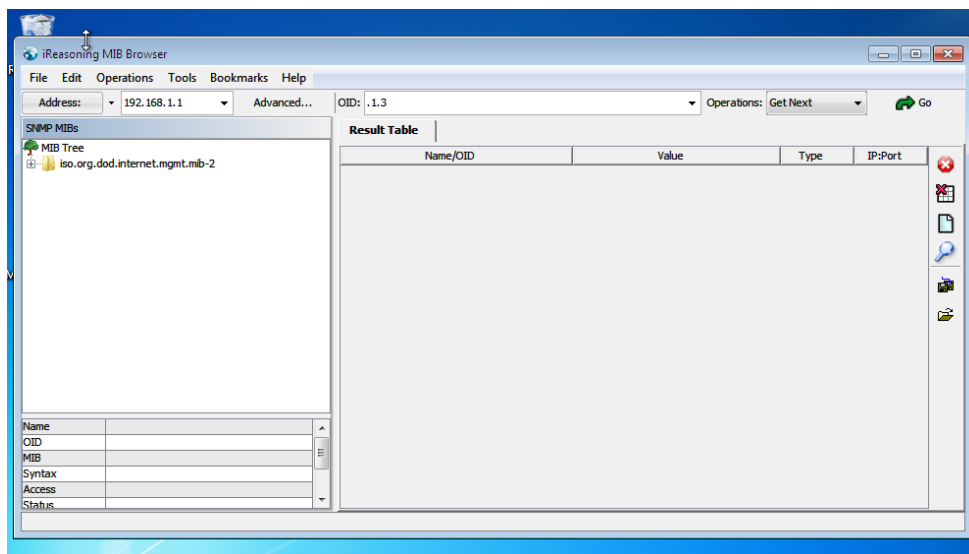
Ping statistics for 20.20.20.26:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 131ms, Maximum = 219ms, Average = 159ms

C:\Users\enrike>_
```

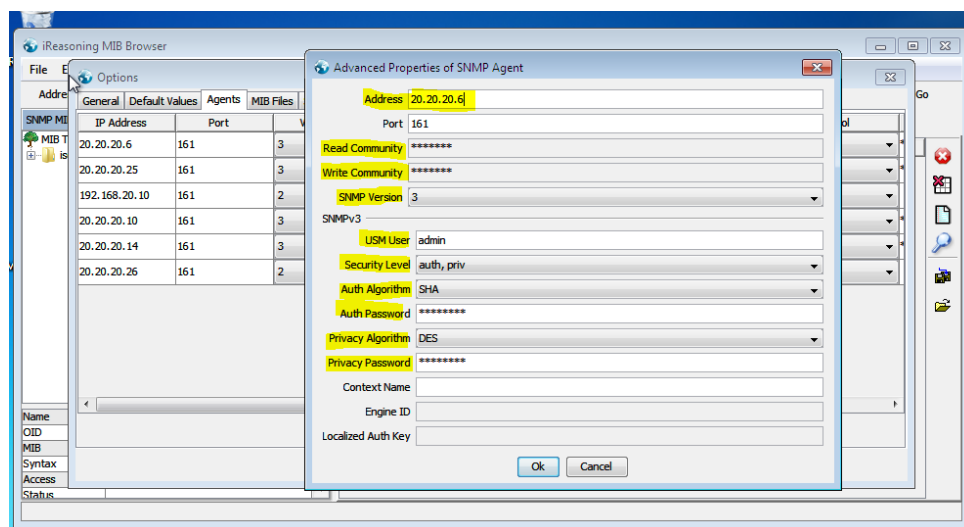
Ping Navegador Web

8. Dentro de cada máquina virtual se tiene instalado MIB Browser para servir como intermediario en la gestión de SNMP. Al iniciar la práctica se pensó en el uso de Power SNMP Manager con lo cual se entregó el primer avance.

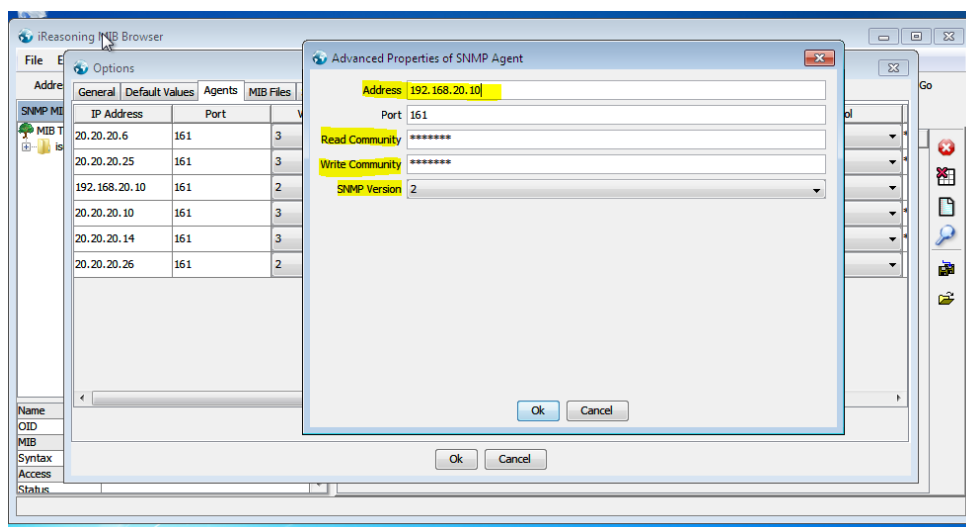
Ya después de eso, se decidió el uso de MIB Browser por tener más facilidad de uso y además por cumplir con los requerimientos que nos pedía el examen.



9. Al completar la instalación de MIB Browser tanto al navegador Web y al Agente SNMP se le configuraron SNMP versión 2 y 3

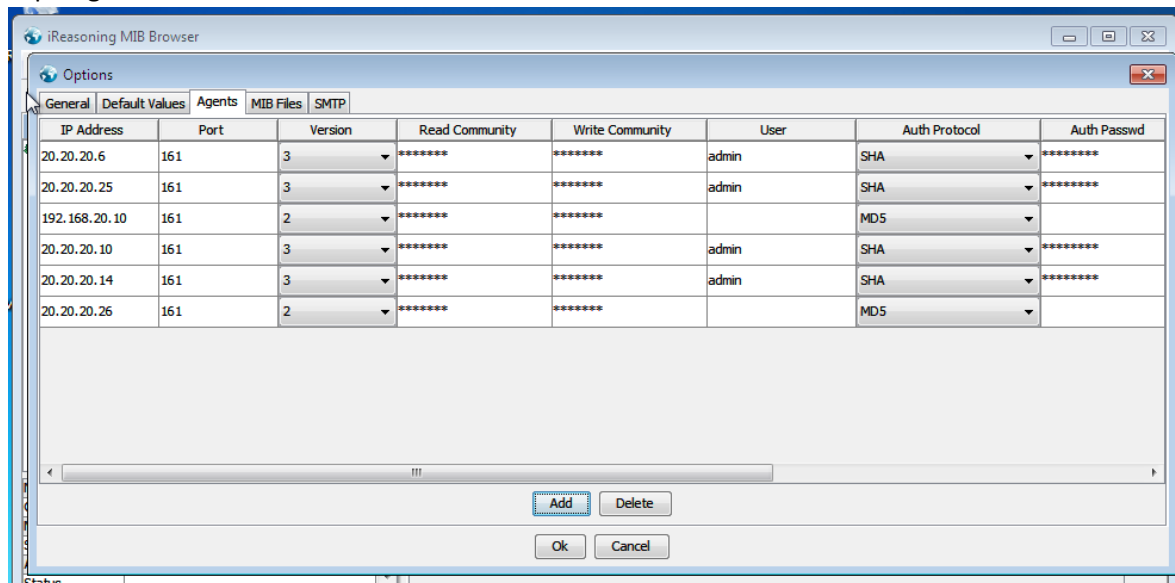


Agente SNMP versión 3



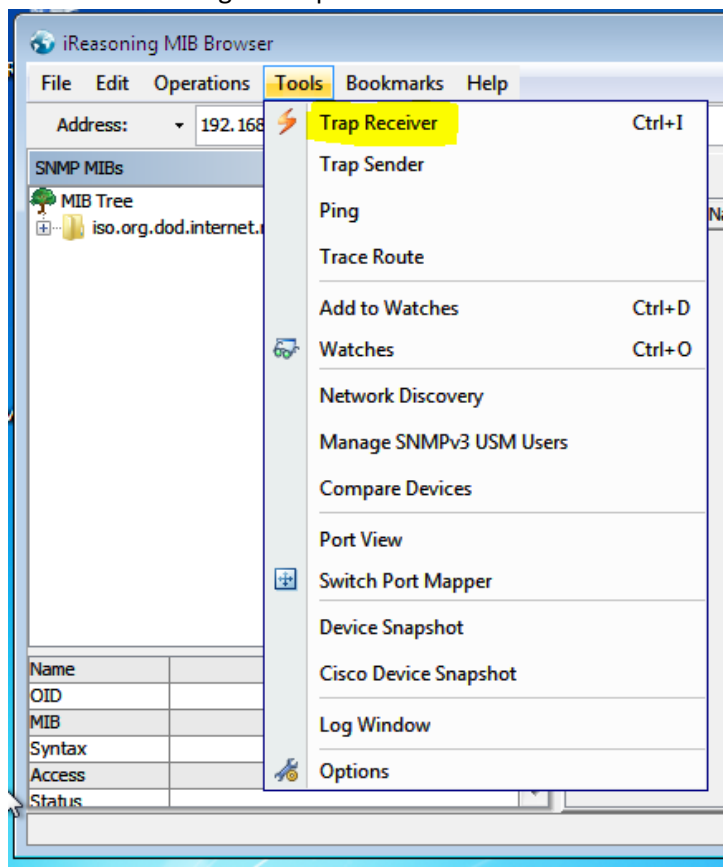
Agente SNMP versión 2

10. Después de realizar los pasos anteriores podemos añadir nuestros agentes dentro de la topología. Esto lo hacemos dentro de la interfaz de MIB Browser.

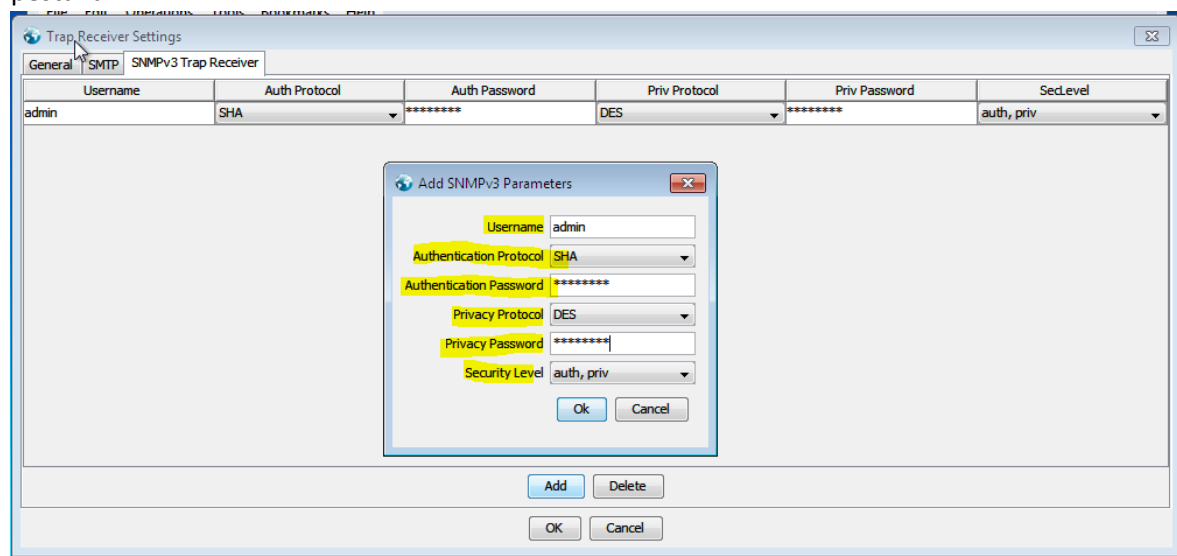


Se puede observar que se muestran todos los routers en la dirección de cada uno y la versión con los que se le configuro.

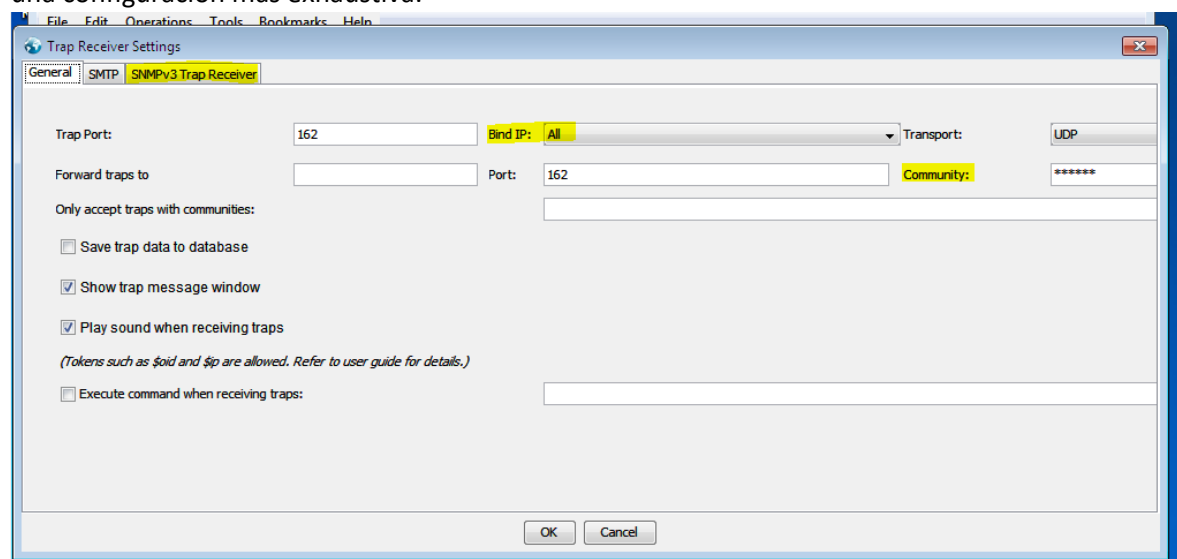
11. Estando dentro de MIB Browser vamos a configurar que tipos de traps vamos a recibir accediendo a la siguiente pantalla.



Dentro de ella accedemos a la opción marcada, donde nos desplegara la siguiente pestaña.

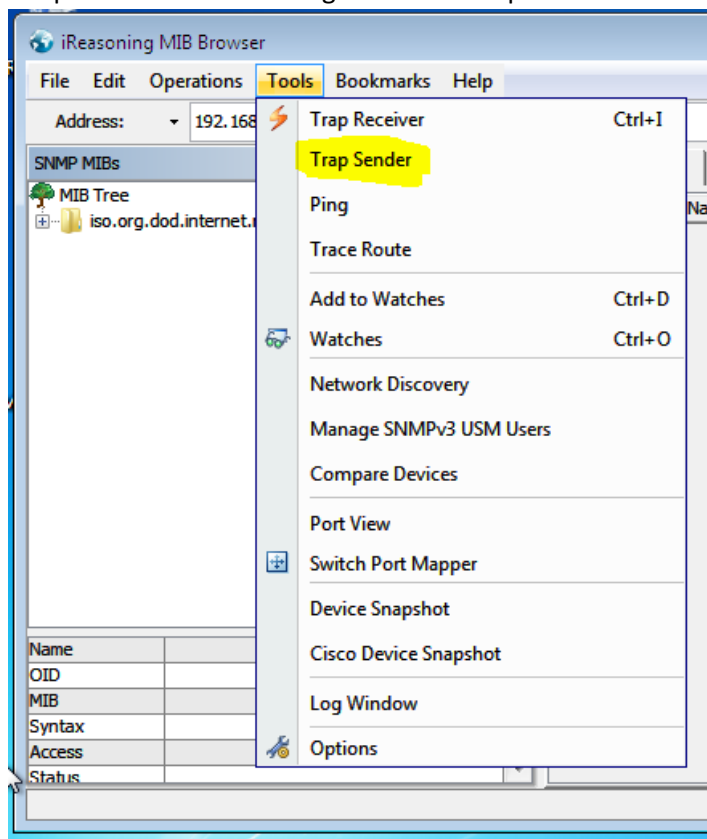


En ella vamos a acceder los parámetros para recibir las traps de v3. Y podemos realizar una configuración más exhaustiva.

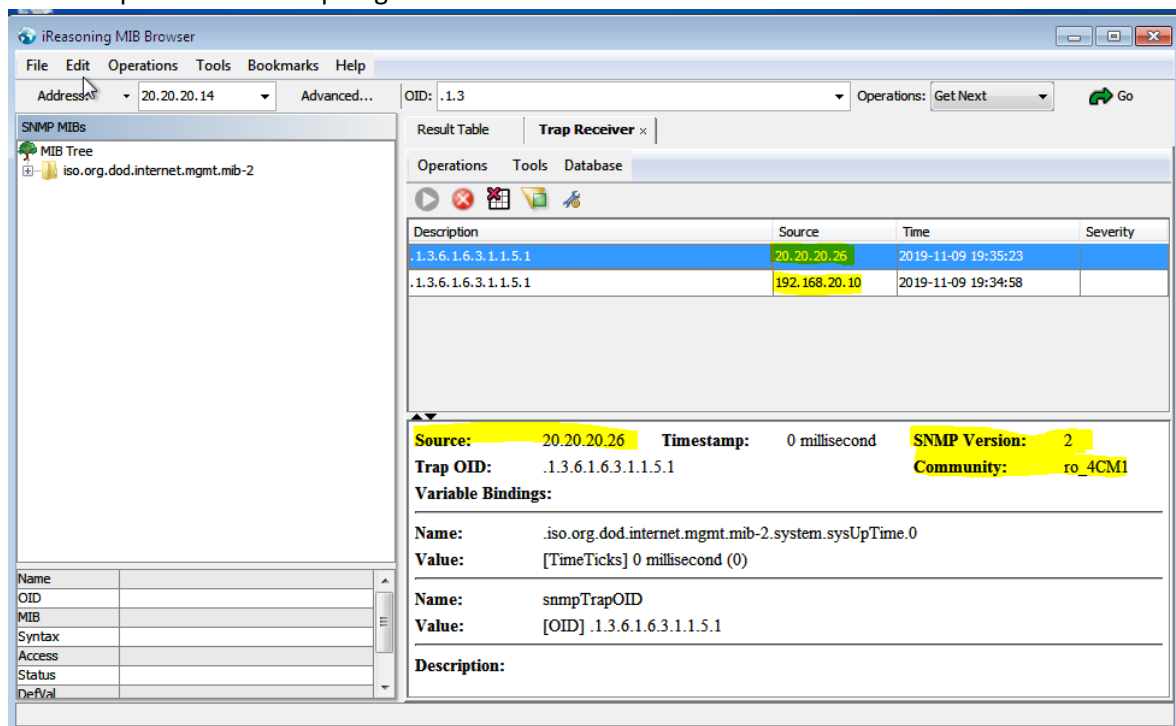


Donde se definirán que IP podemos recibir y de que comunidad.

12. Después se realizó la configuración de Traps Sender.



En la pantalla se verán las traps que estamos recibiendo de las modificaciones que se realizan en los dispositivos de la topología.



Podemos visualizar en la pantalla de que dispositivo se envió la trap, con que versión se implementó y la comunidad donde se encuentra.

The screenshot shows the iReasoning MIB Browser interface. The 'Trap Receiver' window is active, displaying a table of traps. The table has columns: Description, Source, Time, and Severity. The first row is highlighted in blue.

Description	Source	Time	Severity
.1.3.6.1.6.3.1.1.5.3	20.20.20.6	2019-11-09 19:36:45	
.1.3.6.1.4.1.9.9.138.2.0.1	20.20.20.6	2019-11-09 19:36:44	
.1.3.6.1.2.1.14.16.2.13	20.20.20.6	2019-11-09 19:36:44	
.1.3.6.1.2.1.14.16.2.13	20.20.20.6	2019-11-09 19:36:43	
.1.3.6.1.2.1.14.16.2.13	20.20.20.6	2019-11-09 19:36:43	
.1.3.6.1.2.1.14.16.2.13	20.20.20.6	2019-11-09 19:36:43	
.1.3.6.1.2.1.14.16.2.13	20.20.20.6	2019-11-09 19:36:43	
.1.3.6.1.2.1.14.16.2.13	20.20.20.6	2019-11-09 19:36:43	
.1.3.6.1.2.1.14.16.2.16	20.20.20.6	2019-11-09 19:36:42	
.1.3.6.1.2.1.14.16.2.13	20.20.20.6	2019-11-09 19:36:42	
.1.3.6.1.2.1.14.16.2.13	20.20.20.6	2019-11-09 19:36:42	
.1.3.6.1.2.1.14.16.2.13	20.20.20.6	2019-11-09 19:36:42	
.1.3.6.1.2.1.14.16.2.16	20.20.20.6	2019-11-09 19:36:42	
.1.3.6.1.4.1.9.9.43.2.0.1	20.20.20.6	2019-11-09 19:36:34	

Below the table, the details for the selected trap are shown:

Source: 20.20.20.6 **Timestamp:** 21 minutes 2 seconds **SNMP Version:** 3 (EngineID: 0x800000090300CA0408CC0008)

Trap OID: .1.3.6.1.6.3.1.1.5.3 **User:** admin

Variable Bindings:

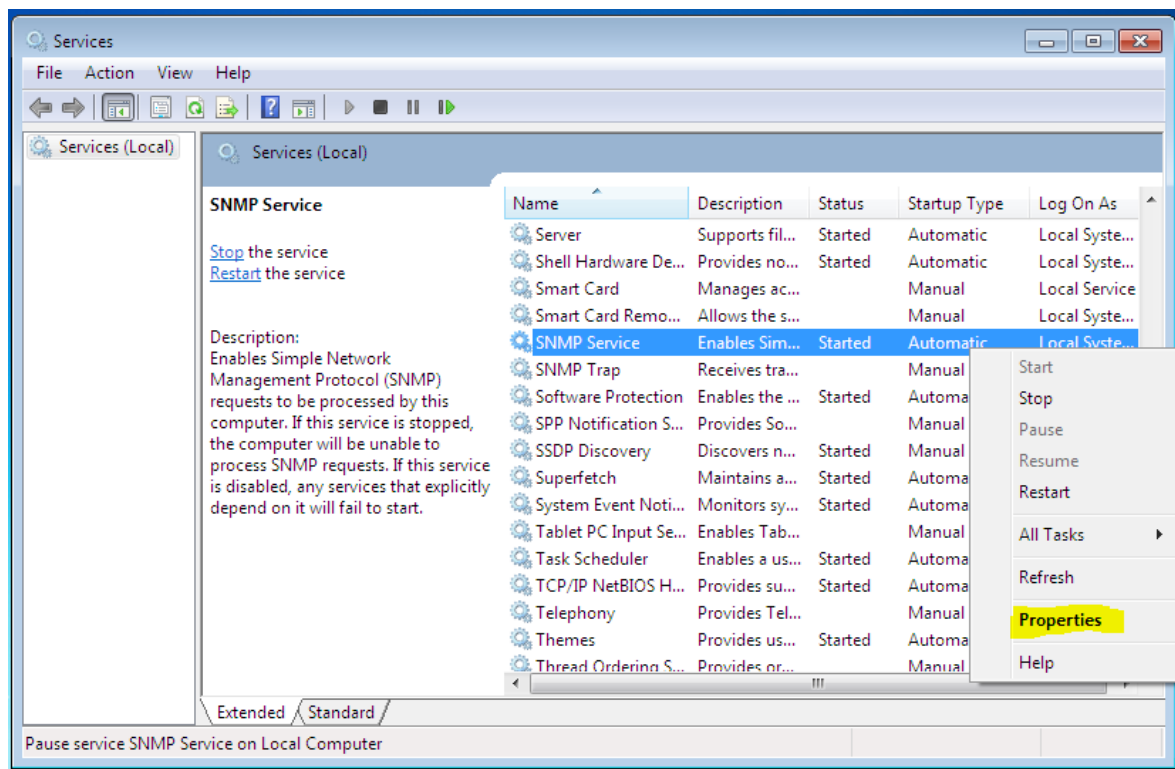
Name: .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0

También si recorremos dentro de la barra de información podemos encontrar en que interfaz Ethernet se realizó el cambio o el lugar donde se realizó, también se puede ver que acción se realizó.

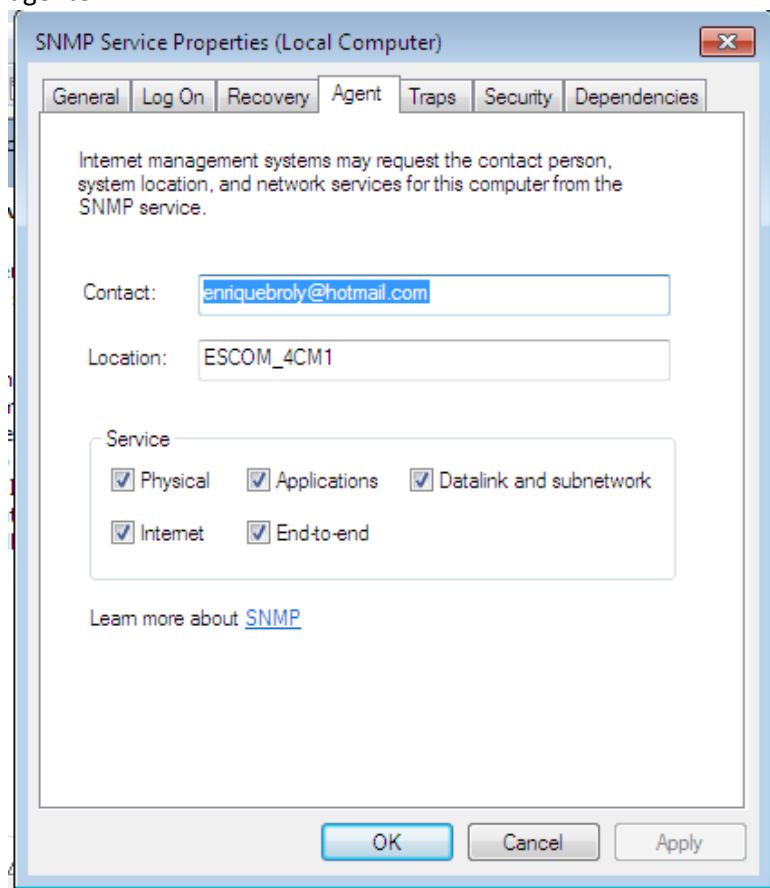
Por ejemplo, en la siguiente imagen se puede ver que el cambio se realizó en la Fast Ethernet 1/0 y la acción realizada fue que se apagó esa conexión.

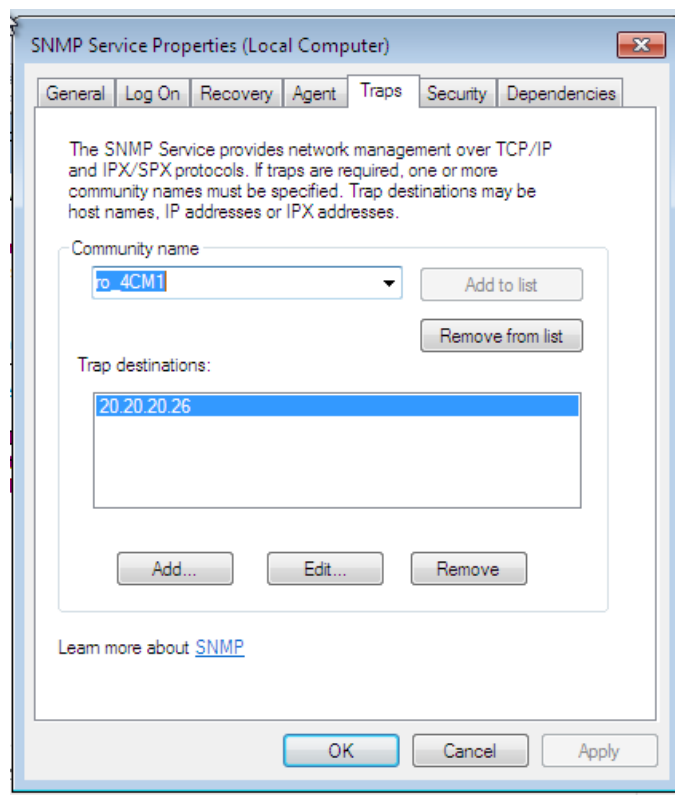
This screenshot is identical to the one above, showing the iReasoning MIB Browser interface with the 'Trap Receiver' window. It displays a table of traps and details for a specific trap, including the source IP, timestamp, SNMP version, trap OID, user, and variable bindings.

13. Para establecer la máquina virtual como Agente SNMP, debemos activar el servicio SNMP de Windows 7:



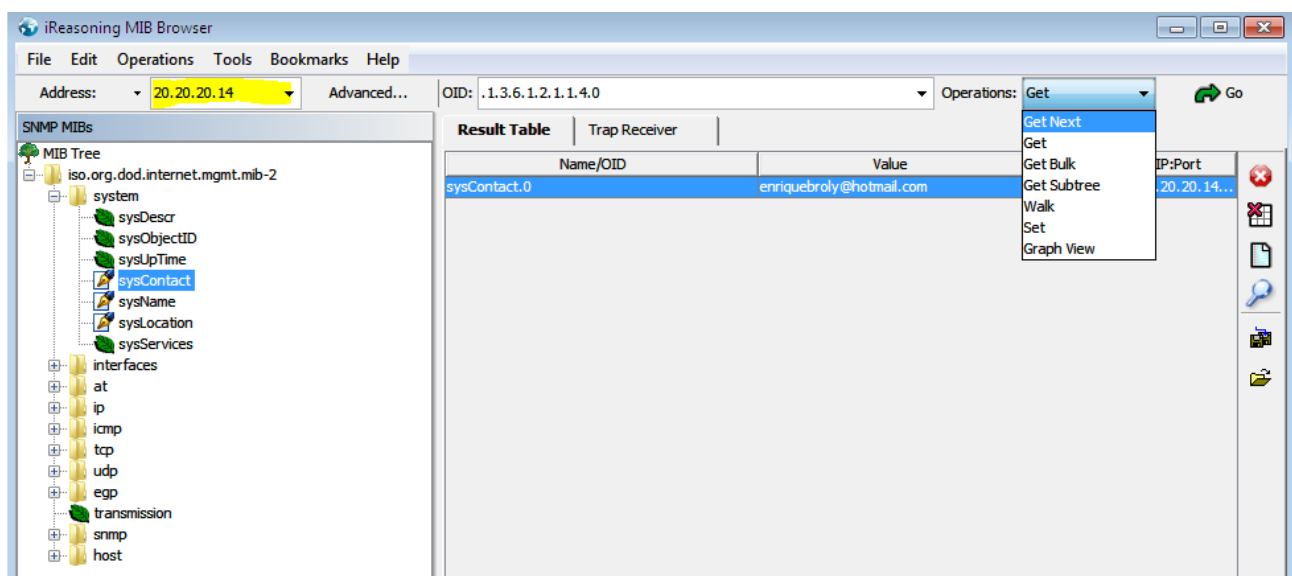
Abrimos la opción de Properties, vamos a encontrar los datos con los que cuenta el agente.



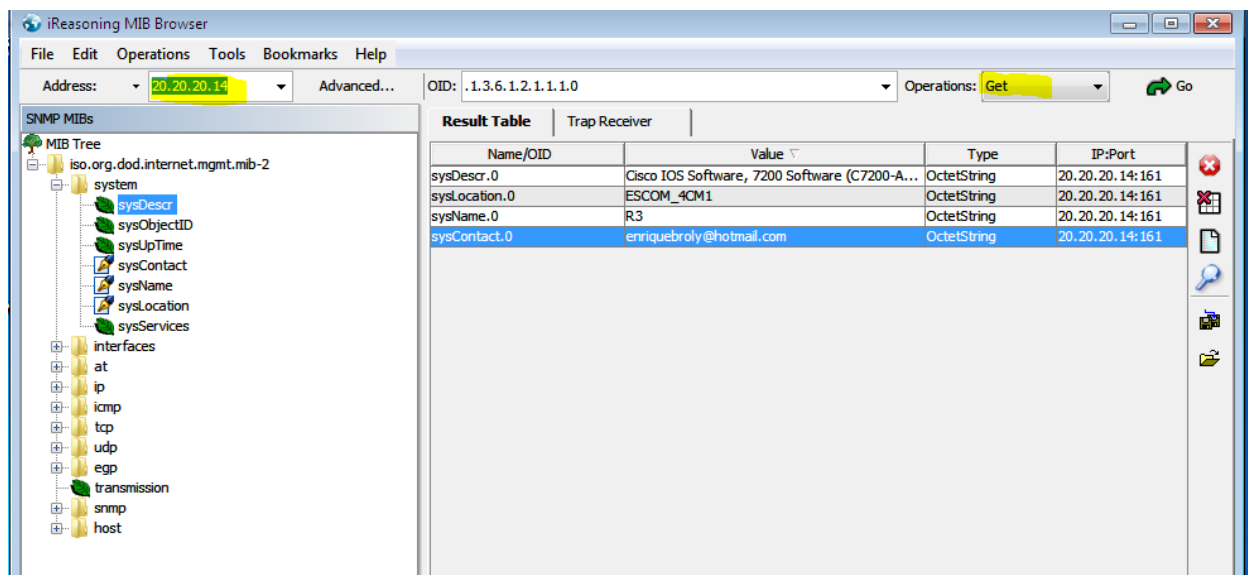


Hasta se pueden añadir traps desde este punto.

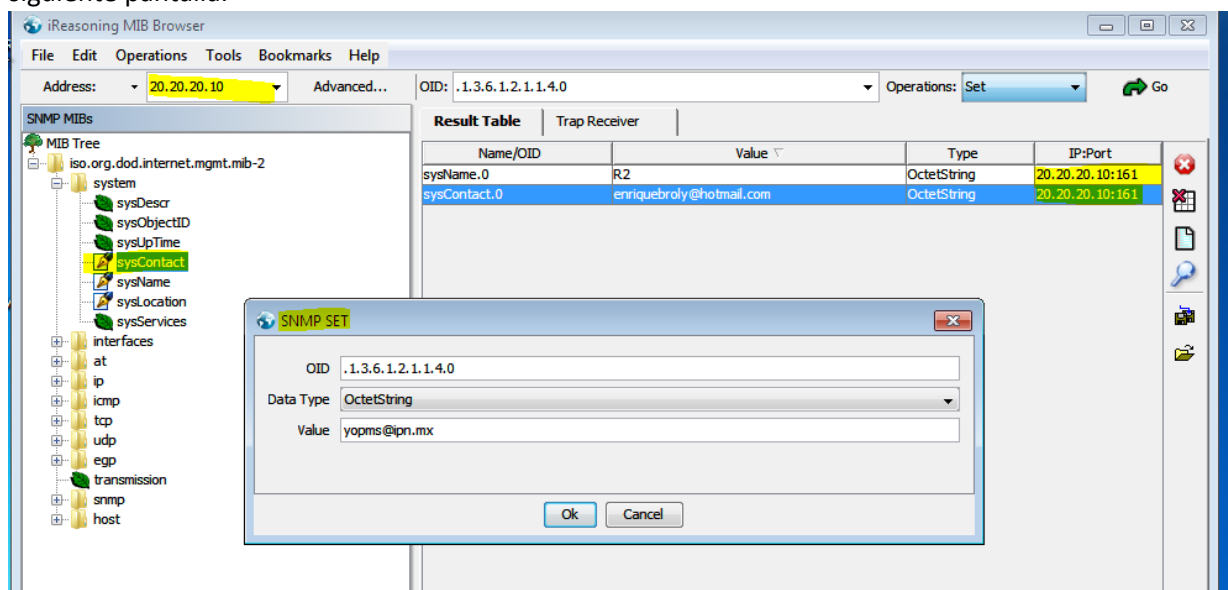
14. Pasando a la parte donde podemos realizar get's y set's, estos se pueden realizar desde la interfaz.
15. Pedimos un get desde la dirección 20.20.20.14 en donde nos tiene que aparecer el Contact de esta dirección.



16. Si realizamos la misma petición de get pero ahora sobre sysDescr obtendremos toda la información que se ingresó en los routers o en la dirección donde se esté realizando la consulta.

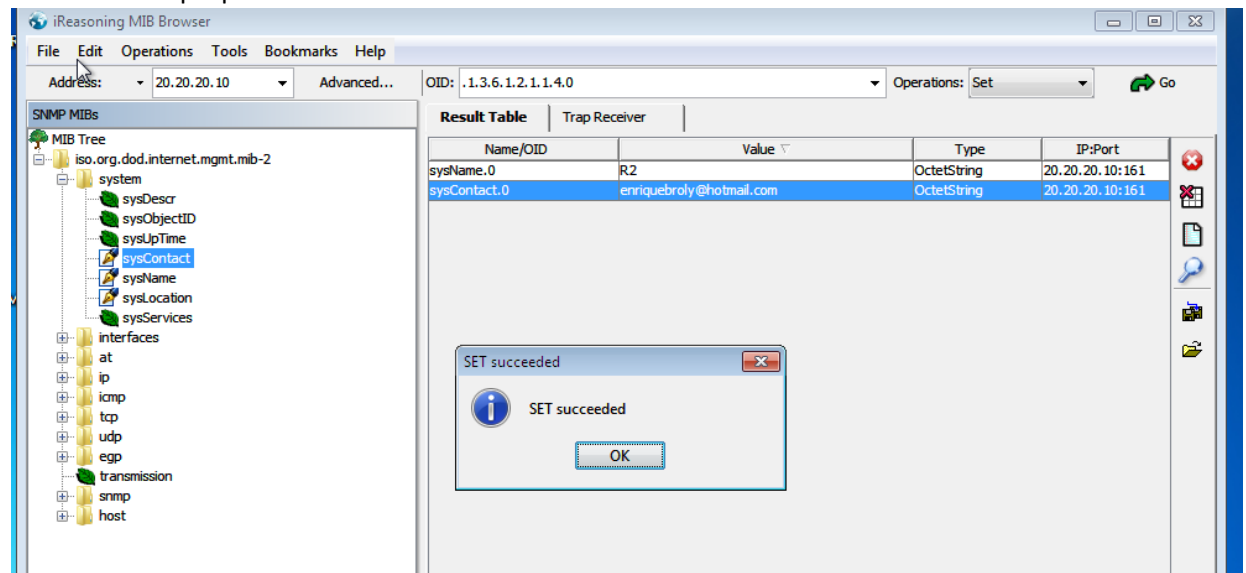


17. Ahora si cambiamos de método e implementamos un set en sysContact nos muestra la siguiente pantalla.

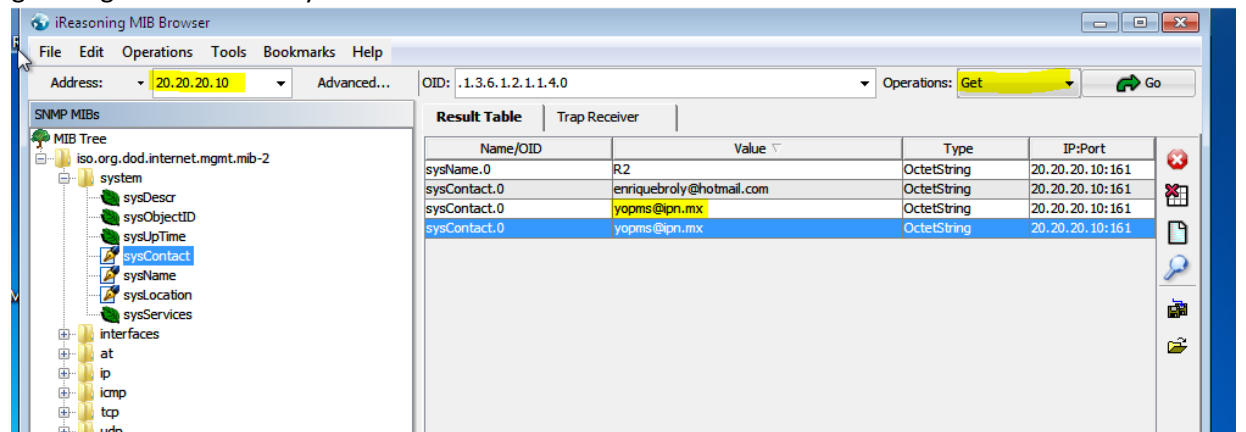


En ella se puede modificar el valor para sysContact y en la sección de value se ingresa el

nuevo valor a proporcionar.

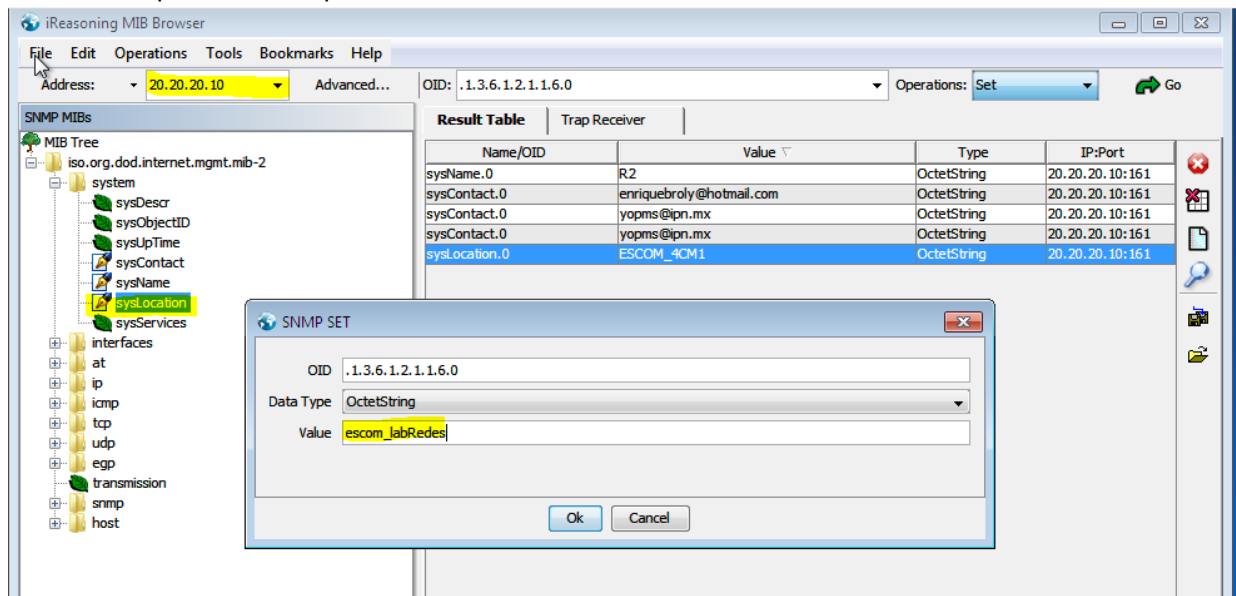


Al confirmar nos muestra la pantalla anterior, para confirmar el cambio seleccionamos un get de igual manera de sysContact.



En la pantalla podemos visualizar un get realizado antes del set, el cual muestra el anterior contact y la marca amarilla se muestra el nuevo valor para sysContact

18. De igual forma si realizamos un set en sysLocation saldrá una pantalla para escribir el nuevo valor para este campo.



19. Comprobando con el mismo procedimiento de sysContact con un get lo podemos visualizar.

