# Network Management and Monitoring

## Basic Configuration

Configure R2 similarly to R1:

- set hostname to R2
- for the interface g0/0/0: the IP address is 172.16.0.2, mask 255.255.0.0, activate interface
- for the interface g0/0/1: the IP address is 10.20.0.1, mask 255.255.0.0, activate interface
- set logging synchronous on the line console 0
- unset domain lookup
- enable OSPF routing:
    - the process is 1, area 0,
    - the router-id 2.2.2.2,
    - propagate the both connected networks,
    - the interface g0/0/1 as passive interface
- copy running-config to startup-config
- examine the startup-config file

Configure S2 similarly to S1:

- set hostname to S2
- for the interface vlan1: the IP address is 10.20.0.2, mask 255.255.0.0, activate interface
- configure the default gateway – 10.20.0.1
- set logging synchronous on the line console 0
- unset domain lookup
- copy running-config to startup-config
- examine the startup-config file

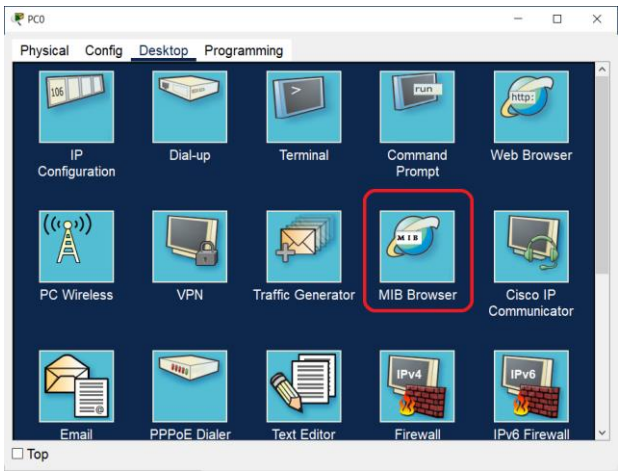
Ping the server from PC0 to test the connection.

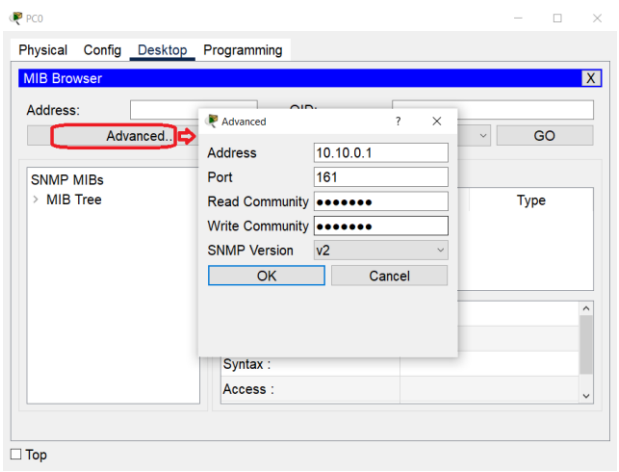
## SNMP (Packet Tracer)

Start a basic SNMP agent on all routers and switches, use the community string ciscoro for reading and ciscorw for writing:

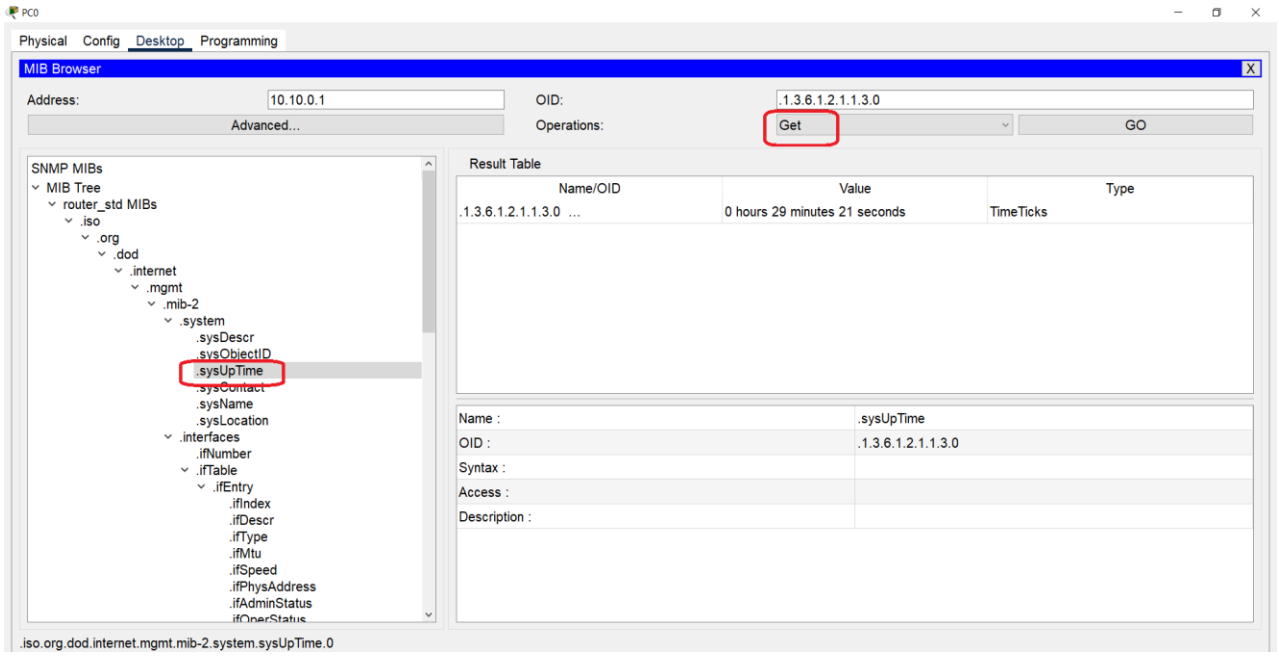
```
configure terminal
       snmp-server community ciscoro ro
       snmp-server community ciscorw rw
```

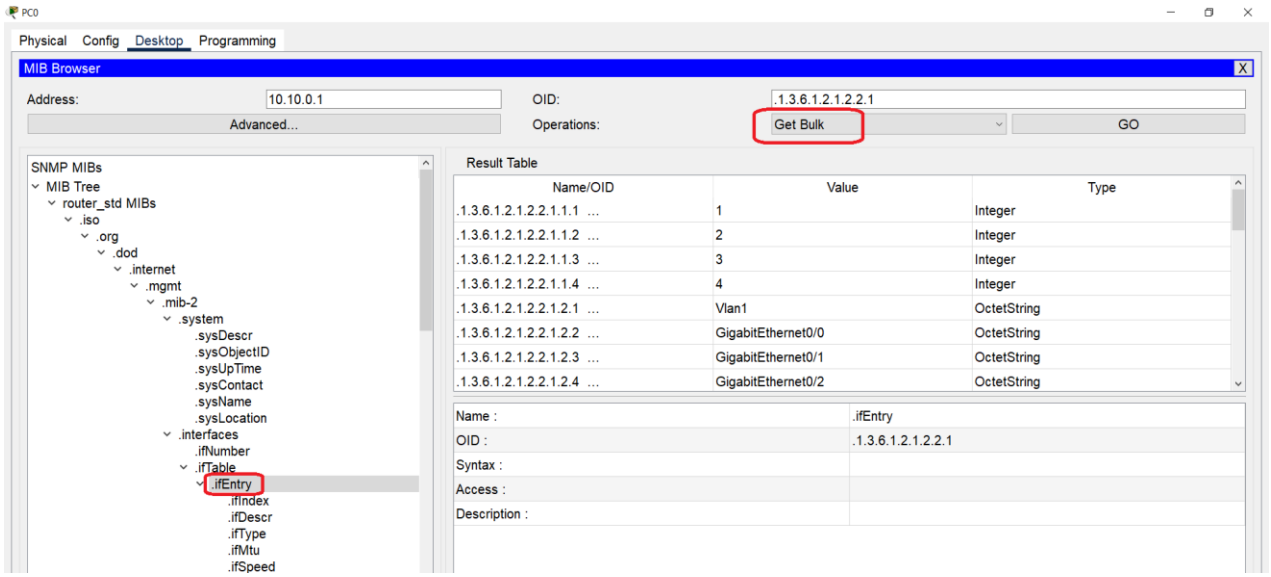
Start a basic SNMP manager (MIB browser) on PC0:

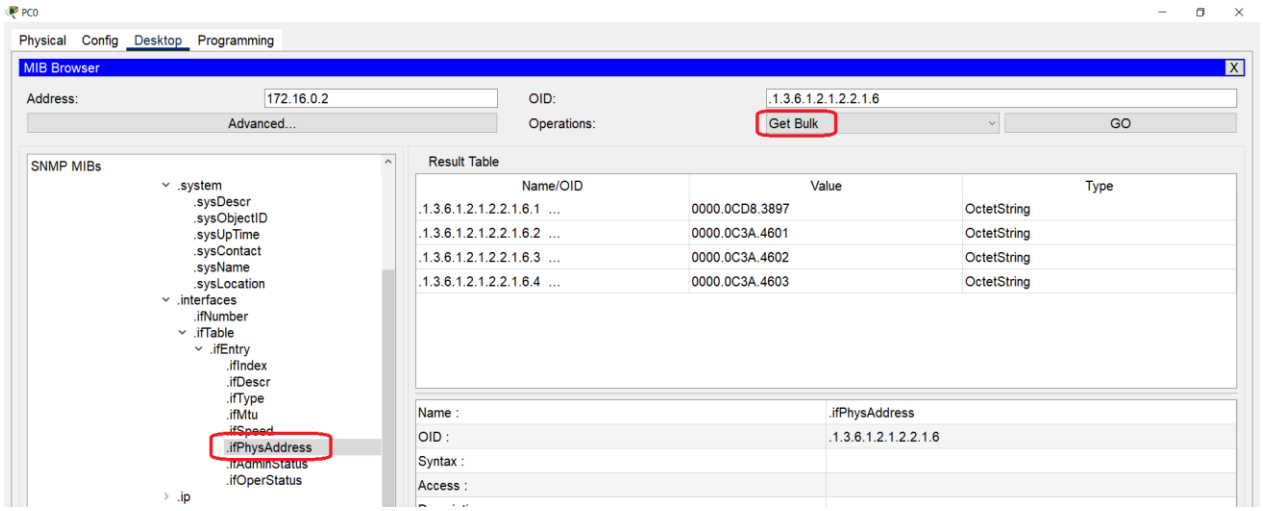


Request some of the device parameters (for simple variables, use the GET method, for table variables, use the GET BULK method):



# SNMPv2 (real device)

With a real device, we have many more options:

```
configure terminal
       snmp-server community ciscoro ro SNMP_ACL
       snmp-server community ciscorw rw SNMP_ACL
       snmp-server contact admin@some.company.com
       snmp-server enable traps
       ip access-list standard SNMP_ACL
              permit 10.10.0.31
              end
show snmp
```

SNMP management tools – free possibilities:

- ManageEngine MibBrowser Free Tool
- Paessler PRTG Monitoring Tool
- iReasoning
- …

# SNMP message format

Go to the webpage: packetlife.net, Captures, find the SNMP protocol using filters; or go to

https://packetlife.net/captures/protocol/snmp/

Open the last example capture and browse the packets format.

# Port Mirroring

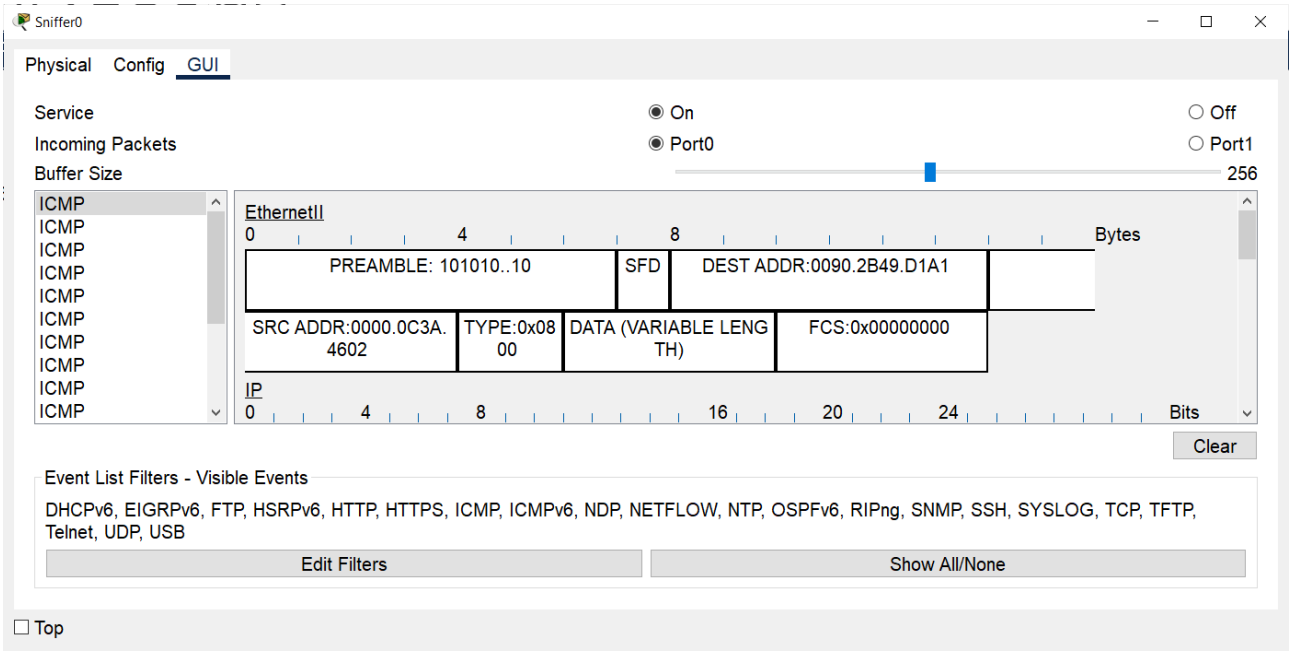
Connect a sniffer (end devices) to switch S2 (port f0/24). Configure the switch for port mirroring:

```
configure terminal
       monitor session 10 source int f0/1         ; leading to the server
       monitor session 10 destination int f0/24   ; leadint to the sniffer
```

On the sniffer, deny some protocols by filter – STP, DTP, CDP,...

Ping 10.20.0.99 from PC0.

Check the sniffer.

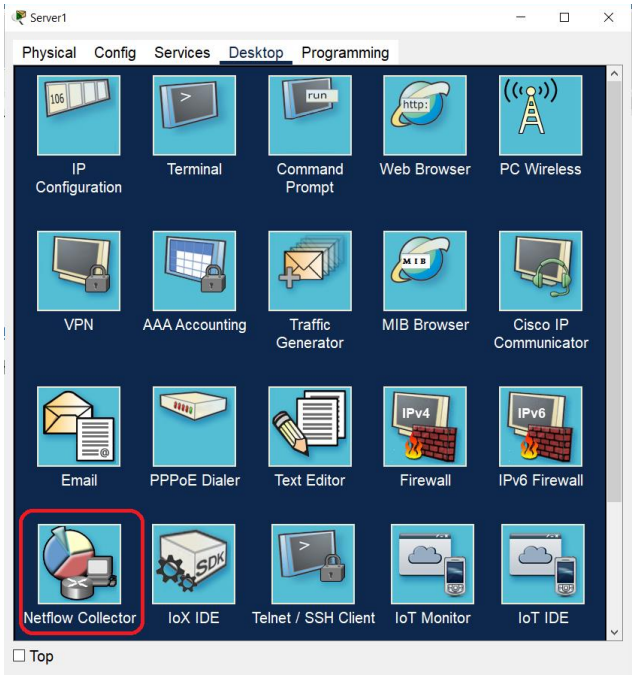


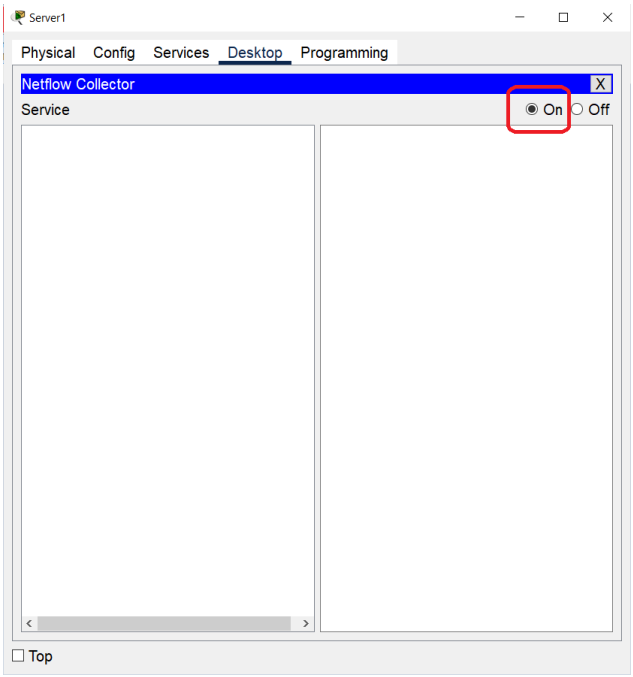
Check if the http server is running on Server0 (Services tab), or what websites are available there.

On PC0, enter the IP address of this server into the web browser with one of the available web addresses. Check if the sniffer has captured the communication.

# NetFlow

Run NetFlow Collector on Server1.




Then configure NetFlow collection on R1:

We will export all captured flows to 10.30.0.2, UDP port 2055, and it is good to set the version of NetFlow.

```
configure terminal
       ip flow-export destination 10.30.0.2 2055
       ip flow-export version 9
```

Now we set the ingress and egress ports:

```
int g0/0
       ip flow ingress
int g0/1
       ip flow egress
```

Ping the gateway from the FlowCollector Server to complete ARP process.

Test the capture – ping 10.20.0.99 from PC0.

Then look into the router NetFlow cache:

```
show ip cache flow
```