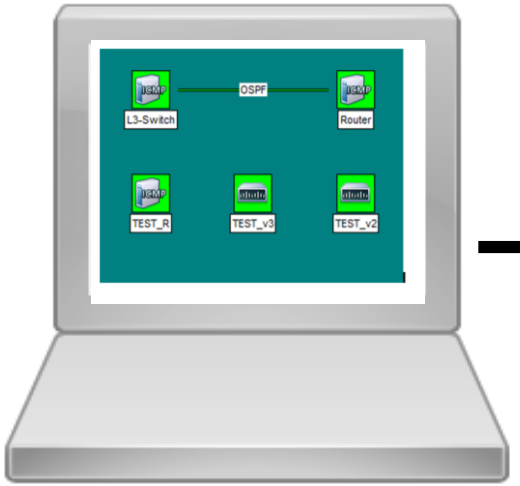
SNMP SUPPLEMENTAL TRAINING

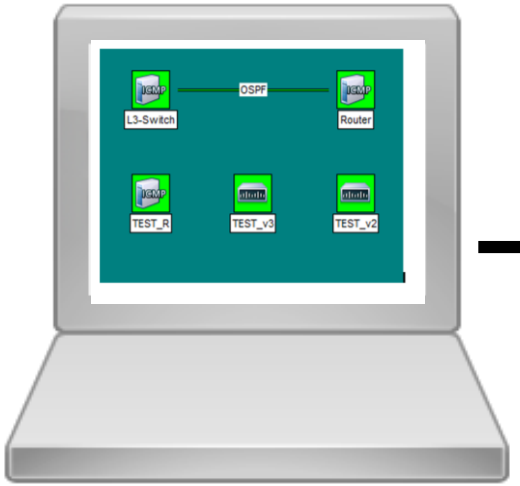
CW2 DELISI



A workstation running SMNPc software is the “manager”. The SNMP icons on the screen provide visual representations of information the manager is getting from the agent.

A router, switch or other network element that has an SNMP cli configuration is the “agent”. The SNMP configuration tells the network element which “managers” it can provide information to and what kind of information.

MANAGER



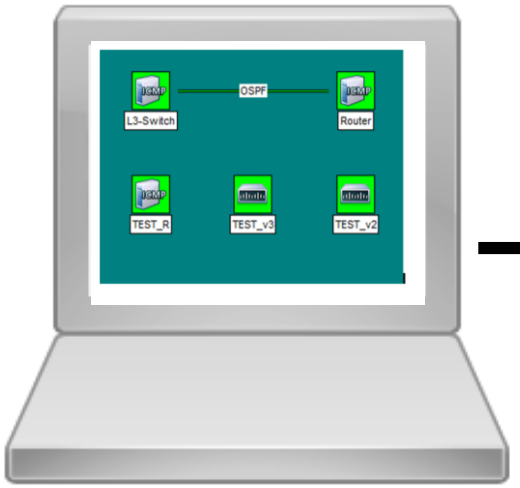
AGENT

If an icon on the SNMP manager is set to poll for ICMP only, it shows a green or “OK” status as long as it can ping the applicable device. The device is identified in the icon by its IP address.

For ICMP reachability to show green on the manager’s SNMP map, the “agent” does not need any SNMP configuration at all. It only has to have a return path for the pings sourced by the manager.

SNMPv2

MANAGER



AGENT

If an icon on the SNMP manager is set to poll for SNMPv2, it needs basic reachability along with credentials listed on the access tab of the icon. The SNMPv2 credentials are called community strings and they are basically just a password that tells the agent whether it should give the manager information (READ ONLY) or information *and* the ability to make configuration changes (READ WRITE) through SNMP.

INFORMATION SPECIFIED ON THE SNMPc ICON ACCESS TAB:

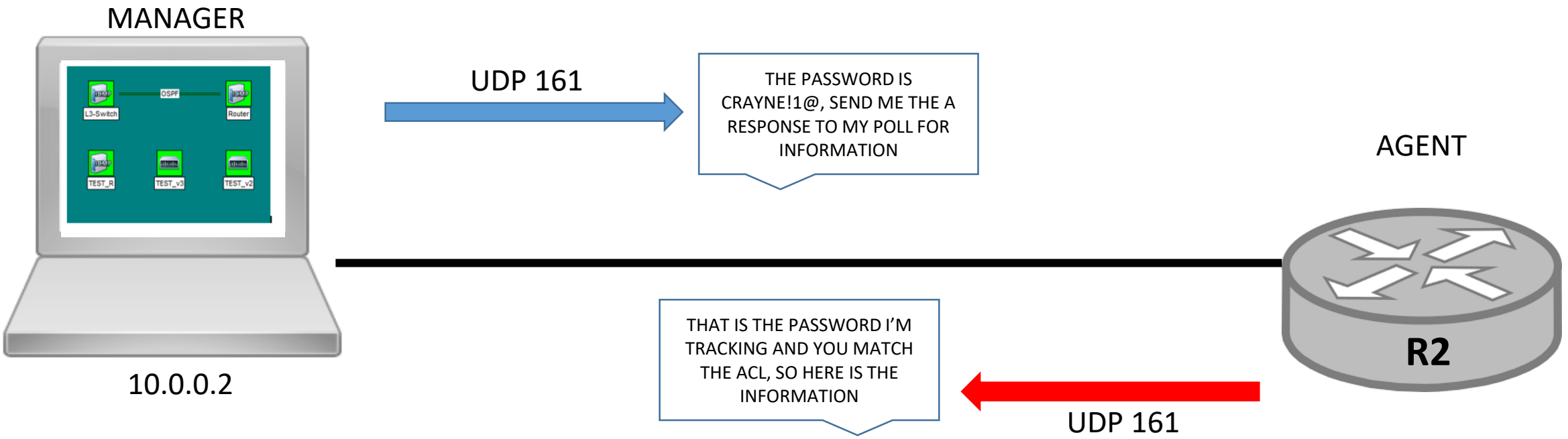
READ ONLY:	SNMPv2
READ/WRITE:	SNMPv2
READ COMMUNITY STRING:	SCHREIER
READ/WRITE COMMUNITY STRING:	REIERHCS

For SNMPv2 to work, the credentials specified in the manager's SNMP icon must match what is in the agent's running config.

If an access-list is added to the SNMPv2 configuration, the credentials must match *and* the manager trying to obtain information or makes changes via SNMP must be permitted by the access-list.

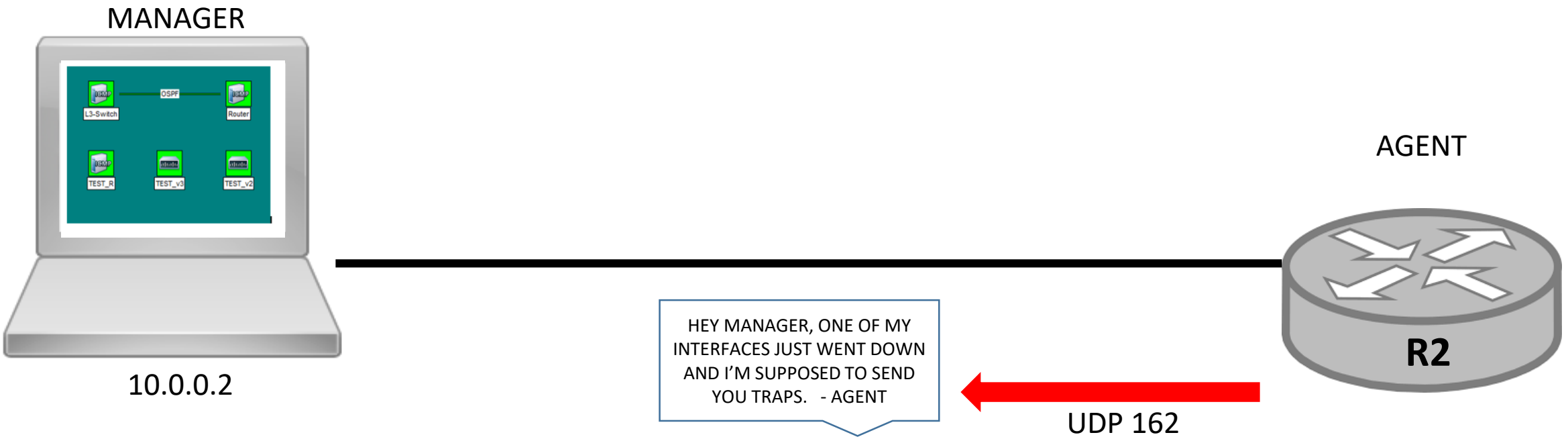
```
SNMPv2 agent running configuration:

snmp-server community SCHREIER RO
snmp-server community REIERHCS RW 11

Ip access-list standard 11
Permit host 10.10.10.11
```

In the configuration above, all managers with the READ ONLY credentials of SCHREIER can extract information from the agent, but only managers with the READ WRITE credentials of REIERHCS that are permitted by access-list 11 are allowed to make configuration changes via SNMP.



"GET" AND "RESPONSE" TRAFFIC IS TYPICALLY SENT BETWEEN DEVICES ON UDP PORT 161

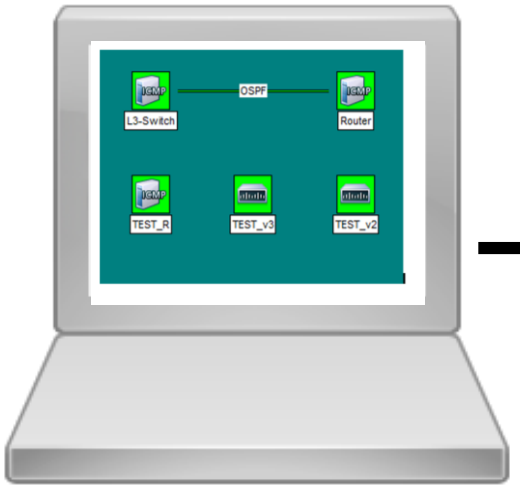
```
SNMPv2 agent running configuration:


R2#
snmp-server community CRAYNE!1@ RO 25
snmp-server community WILSON$$% RW 11

Ip access-list standard 25
Permit 10.0.0.0 0.0.0.3
```



"TRAPS" AND "INFORMS" ARE
TYPICALLY SENT USING UDP PORT 162

SNMPv3

MANAGER



AGENT

If an icon on the SNMP manager is set to poll for SNMPv3, it needs basic reachability along with credentials listed on the access tab of the icon that also specify what (if any) mechanisms are used for authentication and encryption. MD5 and SHA are hash algorithms used for authentication and AES and DES are typically used for encryption.

There are 3 levels of security that can be implemented with SNMPv3:

noAuthnoPriv – username only for authentication, no encryption
authNoPriv - MD5 or SHA for authentication, no encryption
authPriv – MD5 or SHA for authentication and AES/DES for encryption

In SMNPv3 configs authentication is referred to as “auth” and encryption is referred to as “priv”

For SNMPv3 to work, the credentials specified in the manager’s SNMP icon must match along with the types of authentication and encryption in the agent’s running config.

SNMPv3 allows the creation of views which can limit certain SNMPv3 groups of users to certain information and capabilities.

The “iso included” view is the top-level MIB and allows the SNMPv3 users within the associated group to manage all of the device’s information and features.

SNMPv3 agent running configuration:

```
Snmp-server group XYZ v3 priv
Snmp-server user MORALES XYZ v3 auth sha cisco priv aes 128 cisco1
```

In the configuration above, a user defined as “MORALES” is a member of the SNMPv3 group defined as XYZ. The authentication type is sha and they have specified a password of cisco. The encryption type is aes 128 and they have specified a password of cisco1. These credentials would need to be listed on the access tab of the manager’s SNMP icon.

MIBs (management information base) allow the SNMP manager to request very specific types of information from the agent.

A manager might want to know the status of an OSPF neighbor adjacency between two devices. They can create an icon that references the IP address of the agent as the device that will provide the status of the OSPF neighbor state. This is NOT the IP address of the agent's OSPF neighbor. The IP address listed in the first tab of the SNMP icon represents the source of the information that the manager wants.

The manager must have the right SNMP credentials and access to extract information from the agent in order for this to work (SNMPv2 or SNMPv3 rights, as well as permitted traffic).

By right-clicking the agent's icon, you can click on a menu option called tools and then MIB browser.

You then expand the options in the MIB browser until you get to the specific MIB you are looking for. The MIB OID is basically a code that you populate within the icon's attributes tab as a "status variable", along with a value that tells the agent exactly which criteria needs to be met in order to send the manager a "green" status.

MANAGER

AGENT

When you right-click on an SNMPc icon, you can get to the MIB browser by selecting TOOLS > MIB BROWSER.

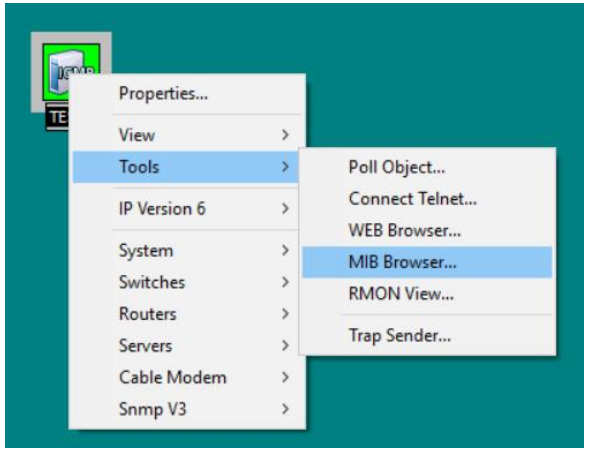
These are the top-level categories of the trees you can expand within the MIB browser. The OSPF neighbor state could be found under:

Mgmt > ospf > ospf neighbor table > ospf neighbor state

some MIBs options are abbreviated

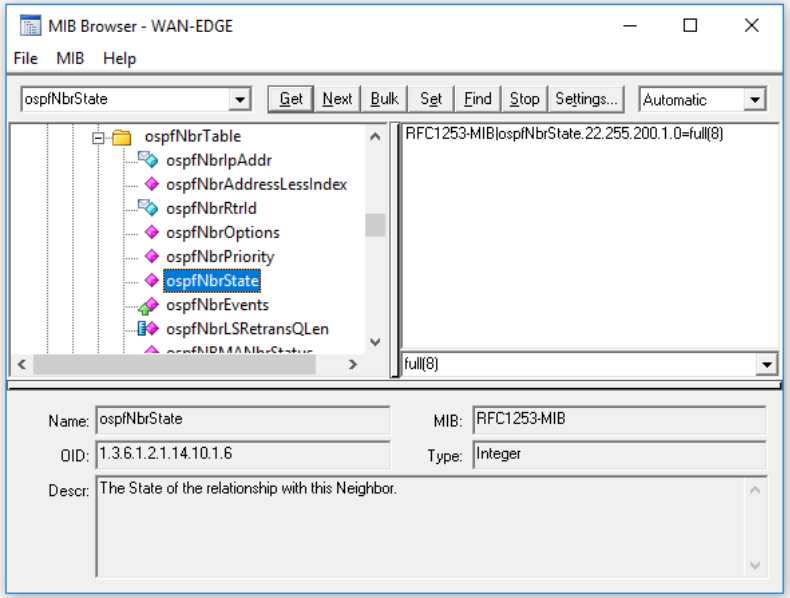
The OID (orange arrow) is the actual code broken down into decimal positions based on its sub-categories. The MIB name (blue arrow) is a representation of that code that is easier for administrators to understand. Sort of like DNS converting 22.18.5.3 to the actual name of Mr. Monette's workstation.

You can put either the OID or the MIB name into the "status variable" section (see next 2 slides for step by step pictures) of your attributes tab. As soon as you do, you will have options in the "status value" drop-down that pertain to that status variable. For example, OSPF states like "init" or "full" would be value options if the status variable was an OSPF neighbor state MIB/OID.

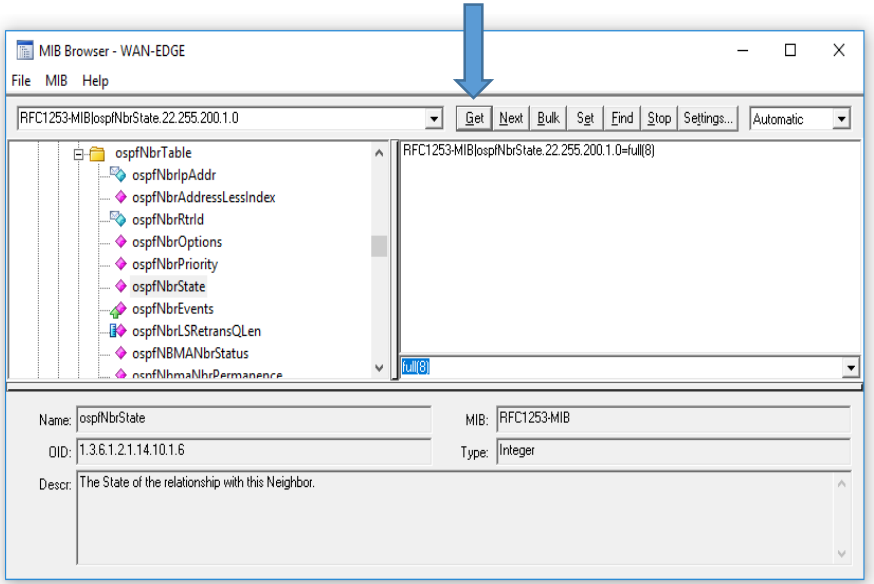


Step 1: Right click an SNMPc icon, Click tools, then MIB Browser

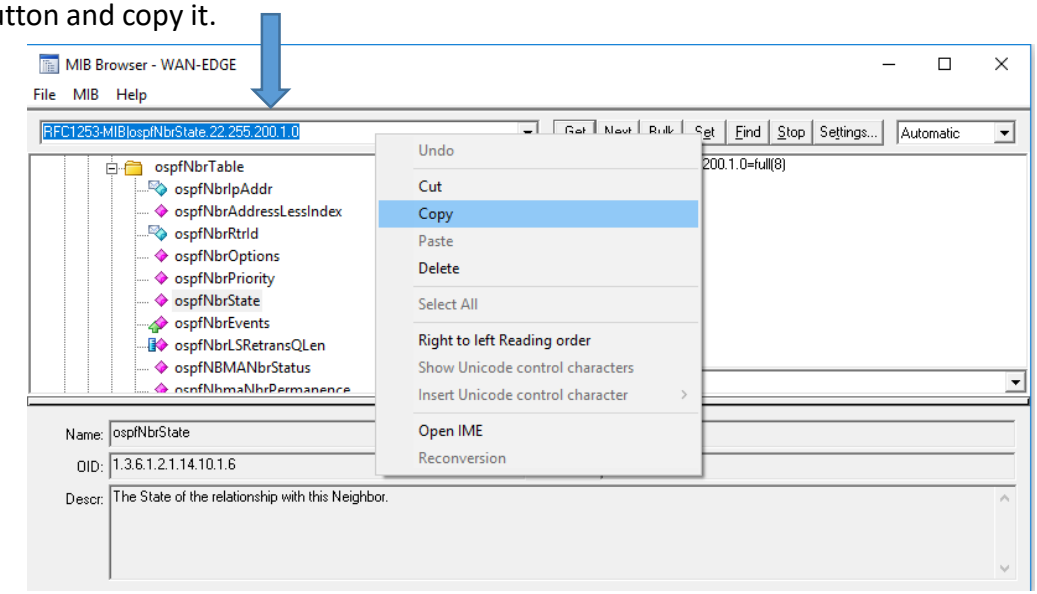
Step 2: Use the menu-tree to find the MIB you want. In this case we want an to check for an OSPF neighbor, so go to Mgmt > ospf > ospfNbrTable > ospfNbrState



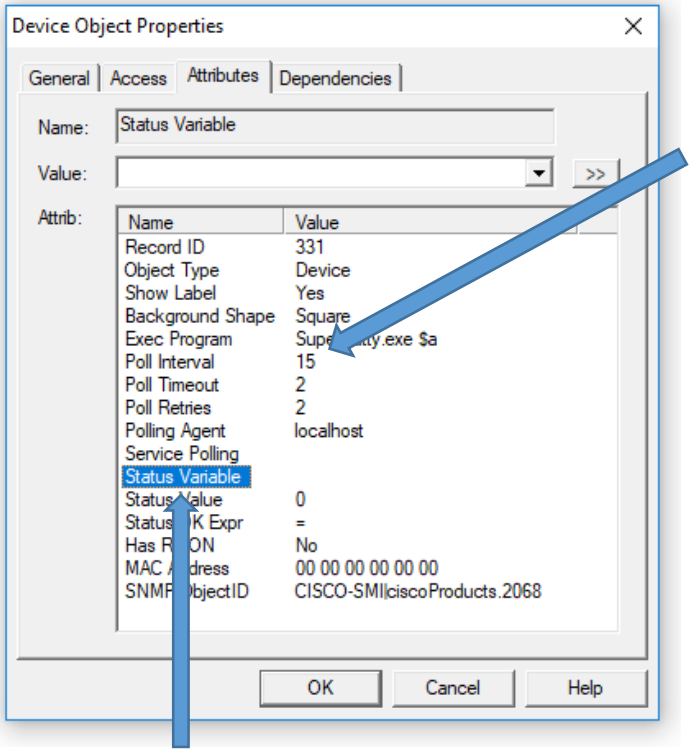
Step 3: Once you have highlighted the MIB you want (ospfNbrState) click on “get”.
NOTE: You must have SNMP credentials established to extract information this way. It will not work with just ICMP.



Step 4: Right click the MIB code displayed to the left of the “Get” button and copy it.

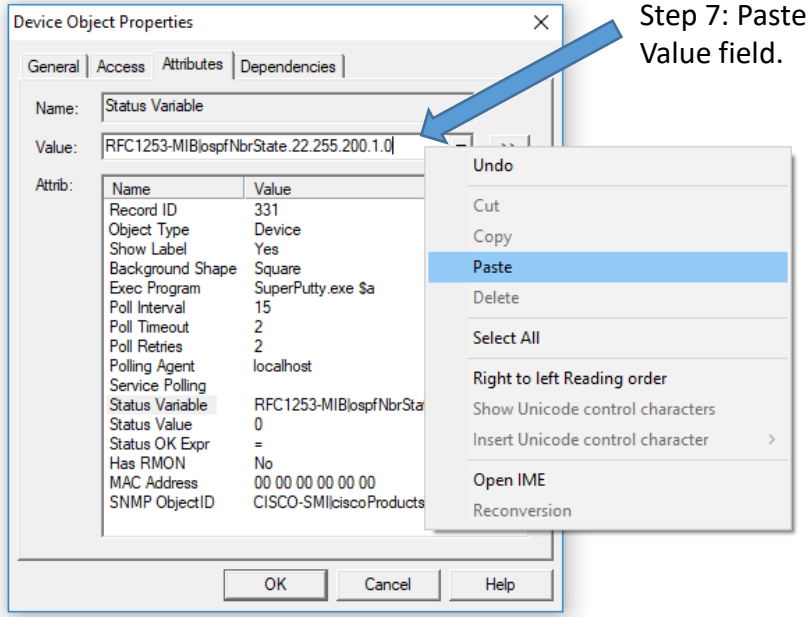


Step 5: Exit the MIB Brower on go back to your SNMPc ICON
Next Slide

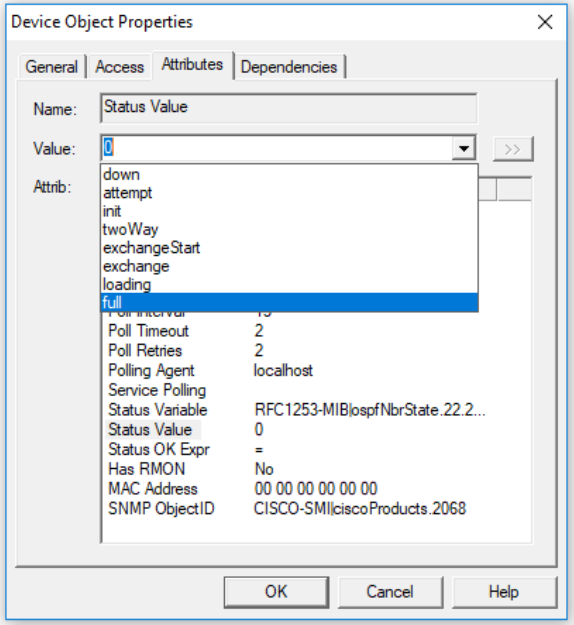


Step 6: Go to the attributes tab of the SNMPc icon you want to use and highlight the "Status Variable" field.

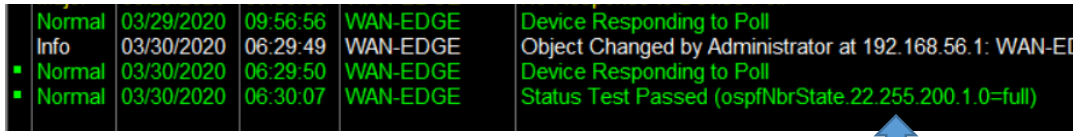
NOTE: Make sure the poll interval is not set for 0. For quick feedback on the status check, set the poll interval for 10 sec.



Step 7: Paste MIB code (from step 4) into the Value field.



Step 8: Once a "Status Variable" Has been populated you will Have options in your "Status Value" Field. Click of the Status Value field And select an option from the drop-down Menu. In this case we see OSPF neighbor state Options, select "full"



Step 9: Check your active events statuses. You should see an indicator that an OSPF neighbor state test was passed.