Implement SNMP

Introduction

SNMP (Simple Network Monitoring Protocol), is used by technicians to recognize issues on the network before they become problematic. This assignment covers setting up a test network, configuring SNMP, installing a network monitoring tool and analyzing SNMP reports.

Objectives

In this project/lab the student will:

- Setup the Virtual Network
- Enable/Configure Devices for SNMP on the Workstation
- Install and Configure the PRTG Network Monitoring Software

Resources

- VMware Workstation Pro
- Network Monitoring Server Virtual Machine
- Workstation 1 Virtual Machine
- Workstation 2 Virtual Machine
- Prtg.zip downloaded from HERE

Procedure

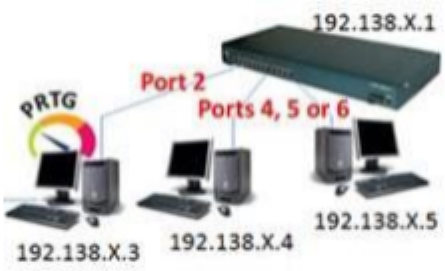
Setup the Virtual Network

1. Set up the following virtual machines in VMware Workstation Pro.
    a. Network Monitoring Server - Windows 10
        i. Default Settings
        ii. Set up for Personal Use
        iii. Offline Account
        iv. Username: PRTG, blank password
        v. IP Address: 192.138.1.3, Subnet Mask: 255.255.255.0, Gateway: 192.138.1.10
    b. Workstation 1 - Windows 10
        i. Default Settings
        ii. Set up for Personal Use
        iii. Offline Account
        iv. Username: Administrator, Password1
        v. IP Address: 192.138.1.4, Subnet Mask: 255.255.255.0, Gateway: 192.138.1.10
    c. Workstation 2 - Windows 10
        i. Default Settings

ii. Set up for Personal Use
iii. Offline Account
iv. Username: Administrator, Password1
v. IP Address: 192.138.1.5, Subnet Mask: 255.255.255.0, Gateway: 192.138.1.10

2. Ensure all virtual machines have their network adapter set to a new LAN segment named SNMP. Disable Windows Firewall (Defender Firewall) on all VMs. Create a second Network Adapter on your Network Monitoring Server set to Bridged mode and ensure Replicate physical network connection state is checked. Ensure you have verified complete connectivity between your VMs before you continue with this lab.

   Your virtual setup should look similar to this:



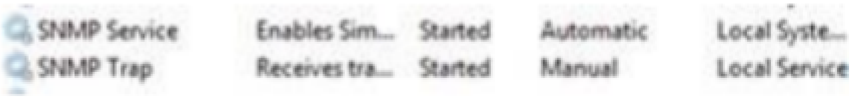
Enable/Configure Devices for SNMP on the Workstation

1. On the WORKSTATIONS 1 & 2 but not the Network Monitoring Server (PRTG SNMP drivers are automatically loaded by the program), in the Windows Search, type Manage Optional Features and open it.

2. Click Add a Feature, and in the Windows Features window, select "Simple Network Management Protocol (SNMP)", click it and then click Install. After Windows completes the requested changes, click Close. In order for SNMP Network Monitor to monitor bandwidth usage (as well as device readings such as memory, CPU load, etc.) on network devices, they must support and be configured for SNMP.

   Note: If the installation of SNMP fails, then it is possible that your Windows 10 installation needs files that are not in your current installation, requiring the Windows 10 machine to have access to the Internet. If this is so, then a). Got to VM/Settings b). In the Hardware tab, click ADD. c). Select Network Adapter. d). Once installed, click on the new adapter and set to NAT. The PC should now have Internet access so Retry the SNMP Optional Feature install again. Once the installation is complete, Remove the 2 nd adapter and continue this lab.

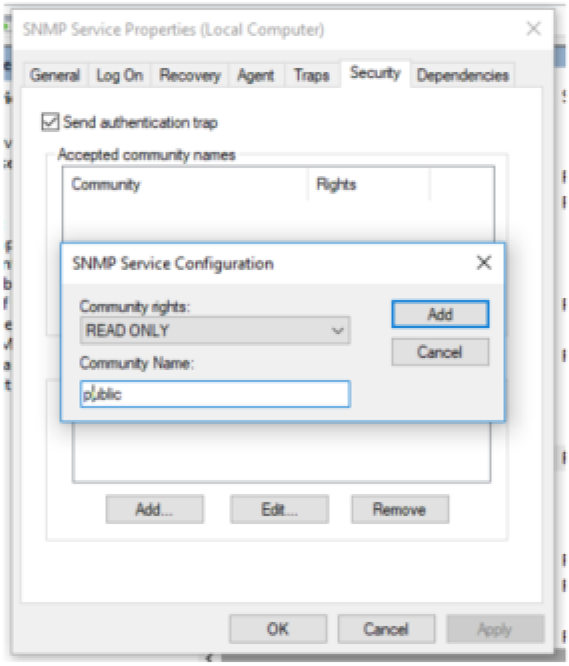
3. Verify that SNMP is now running by clicking Start, then typing "Services.msc" and pressing Enter. Two new services should have been created/running: a. SNMP Service which is the main engine with agents that monitor the activity in the network devices and report the information to the monitoring console workstation. b. SNMP Trap Service which receives trap messages generated by local or remote SNMPagents and forwards the messages to SNMP management programs running on this computer. If not running, hit Start.



SNMP Service	Enables Sim...	Started	Automatic	Local Syste...
SNMP Trap	Receives tra...	Started	Manual	Local Service

4. In the Services window, right click SNMP Service, then select Properties. Click on the Security tab. Under the “Accepted community names” section, click the Add button. Ensure that the accepted community name is “public” and is listed with Read Only community rights. Click Add.

   The SNMP Community String is similar to a user ID or password that allows access to a device's statistics. Note: SNMP community strings are only used by devices that support SNMP V1 and SNMP V2c protocols. SNMP V3 uses safer username/ password authentication, along with an encryption key.



SNMP Service Properties (Local Computer)

☑ Send authentication trap

Accepted community names

Community	Rights

SNMP Service Configuration

Community rights: READ ONLY

Community Name: public

5. In order for the SNMP service to accept and receive SNMP request packets from any host on the network, including external remote hosts regardless of identity, click Accept SNMP packets from any host. Note: This setting is for a lab environment. In the real world, restrict access to local hosts or limited servers only. To limit the acceptance of SNMP packets, click Accept SNMP packets from these hosts, and then click Add, and then type the appropriate host name, IP or IPX address in the “Host name, IP or IPX address” box Finish off by clicking the Add button again.

6. Click OK when done. Reboot the VM for settings to take effect.

7. Repeat this process for Workstation 1 and Workstation 2.

Install and Configure the PRTG Network Monitoring Software

1. Visit the following website to download PRTG on your Network Monitoring Server. https://www.paessler.com/download/prtg-download?download=1 NOTE: When the download completes, click on the download to auto install and apply the license key. Copy/Paste the LICENSE KEY into a text file for safe keeping. You might need this later in the installation.

2. Run the PRTG installation setup program.
   a. Setup Language Selection. Accept the default setup language. Click OK. Setup Wizard Start Screen appears.
   b. Accept the license agreement. Click Next.
   c. Enter an email for the Administrator. (Note: The PRTG server will send important and urgent system alerts to this address - Since we are not live, this will not work in a lab

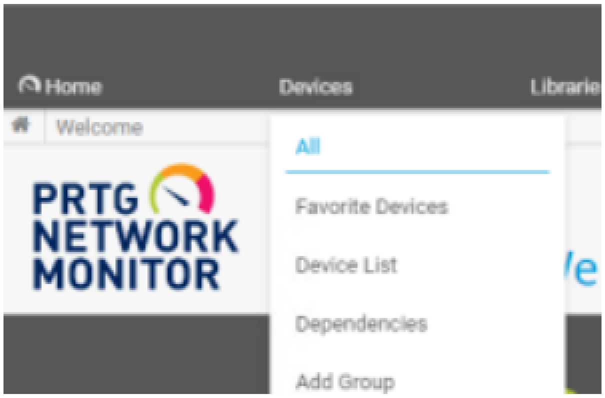
environment). Click Next.

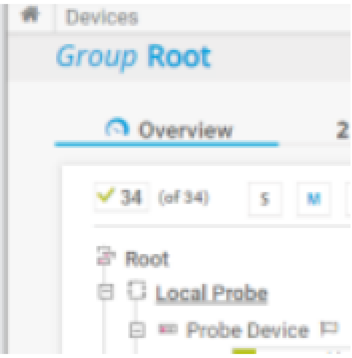
3. After successful installation, your default browser will open and the PRTG Network Monitor Welcome window will appear. If no PRTG browser opens, click the Start menu, then click PRTG Network Monitor (Default Browser). Leave the default login name and password of prtgadmin in each field and click Login.

4. With the most recent method of installation, the downloaded Trial of this software will automatically install the trial-period license key. There should be no other action needed and this installation should work for the next 31 days.

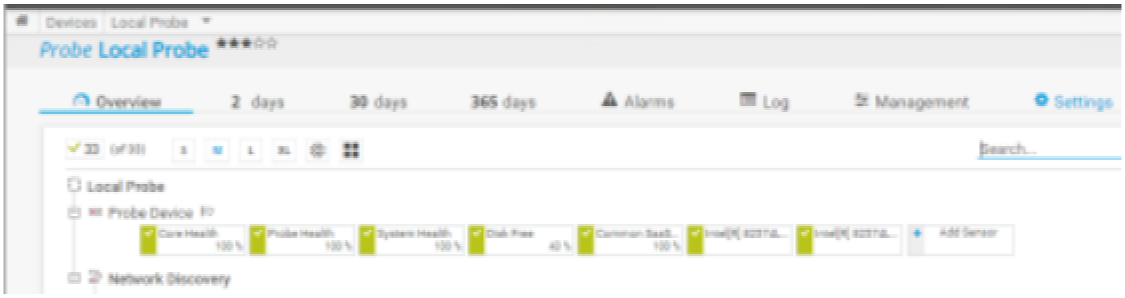
5. Close the warning messages in the top right corner about SSL, password, and email notifications.

6. SET CREDENTIALS FOR WINDOWS. Click DEVICES, ALL, Then LOCAL PROBE under ROOT.

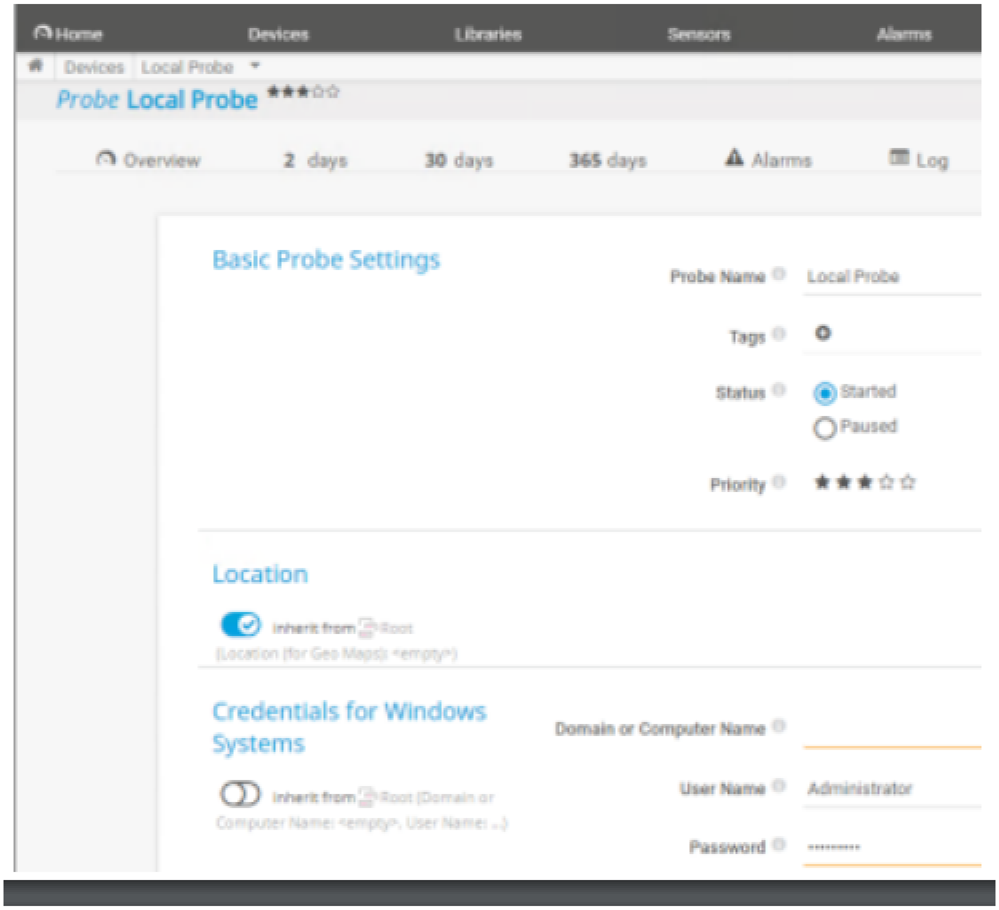




7. Click on SETTINGS for LOCAL PROBE group.



8. Under CREDENTIALS FOR WINDOWS SYSTEMS, Enter in Username: Administrator and Password as “Password1”



Basic Probe Settings

Probe Name: Local Probe

Tags:

Status: ● Started ○ Paused

Priority: ★★★☆☆

Location

Inherit from Root (Location (for Geo Maps): <empty>)

Credentials for Windows Systems

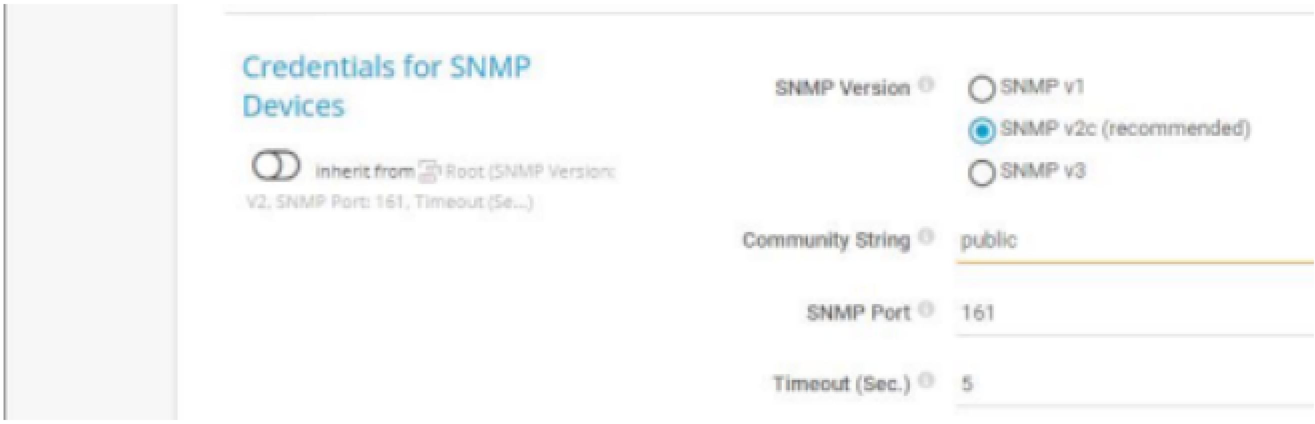
Inherit from Root (Domain or Computer Name: <empty>, User Name: ...)

Domain or Computer Name:

User Name: Administrator

Password: ••••••••••

9. Under CREDENTIALS FOR SNMP DEVICES, ensure they are set as below (may be default).



Credentials for SNMP Devices

Inherit from Root (SNMP Version: V2, SNMP Port: 161, Timeout (Se...)

SNMP Version: ○ SNMP v1 ● SNMP v2c (recommended) ○ SNMP v3

Community String: public

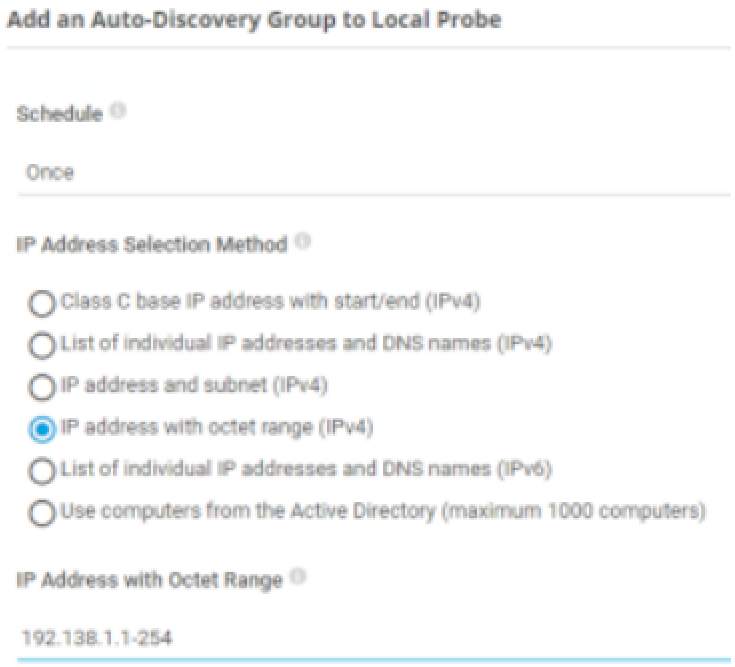
SNMP Port: 161

Timeout (Sec.): 5

10. On the Devices submenu, Add Auto-Discovery Group.

11. In the Add an Auto-Discovery group window, click Local Probe, then click Ok.

12. In the Group Name, type Group1. In the IP Selection Method section, click “IP with octet range (IPv4)” and enter “192.138.1.1-254”. This scans the entire range of IPs in our SNMP LAN segment. Click Ok.



Add an Auto-Discovery Group to Local Probe

Schedule

Once

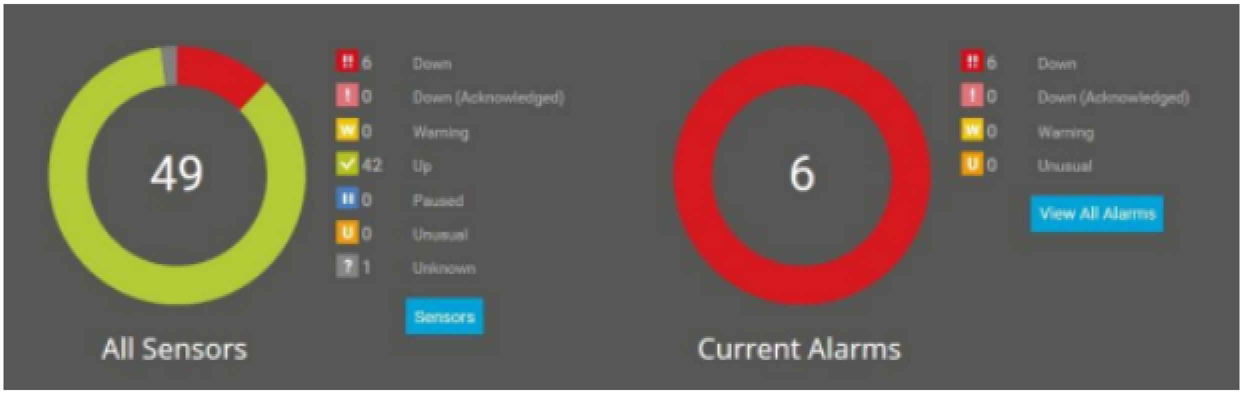
IP Address Selection Method

○ Class C base IP address with start/end (IPv4)
○ List of individual IP addresses and DNS names (IPv4)
○ IP address and subnet (IPv4)
● IP address with octet range (IPv4)
○ List of individual IP addresses and DNS names (IPv6)
○ Use computers from the Active Directory (maximum 1000 computers)

IP Address with Octet Range

192.138.1.1-254

13. If Auto-Discovery was successful, the Overview screen will see an increased number of sensors and log entries.



49

All Sensors

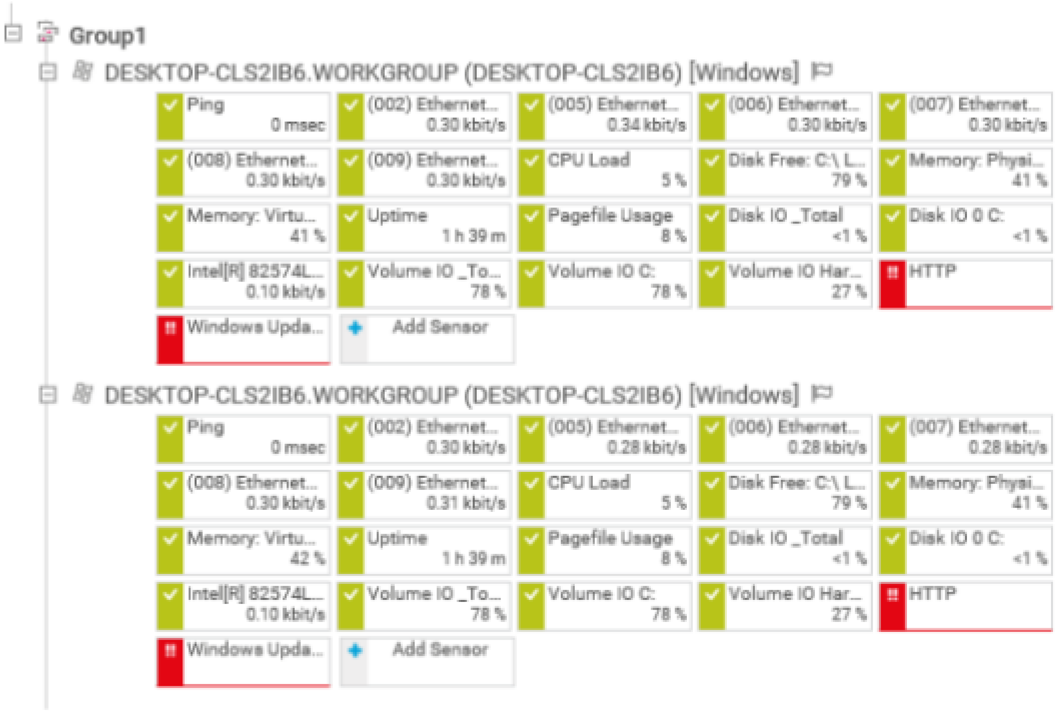
6	Down
0	Down (Acknowledged)
0	Warning
42	Up
0	Paused
0	Unusual
1	Unknown

6

Current Alarms

6	Down
0	Down (Acknowledged)
0	Warning
0	Unusual

14. From the menu, click Devices. In the Overview screen, you should be able to scroll to the bottom and see the results of the Group 1 Auto-Discovery and all of the associated probes that came back with information about the workstation VMs on your network.



Group1

DESKTOP-CLS2IB6.WORKGROUP (DESKTOP-CLS2IB6) [Windows]

✓ Ping 0 msec	✓ (002) Ethernet... 0.30 kbit/s	✓ (005) Ethernet... 0.34 kbit/s	✓ (006) Ethernet... 0.30 kbit/s	✓ (007) Ethernet... 0.30 kbit/s
✓ (008) Ethernet... 0.30 kbit/s	✓ (009) Ethernet... 0.30 kbit/s	✓ CPU Load 5 %	✓ Disk Free: C:\ L... 79 %	✓ Memory: Physi... 41 %
✓ Memory: Virtu... 41 %	✓ Uptime 1 h 39 m	✓ Pagefile Usage 8 %	✓ Disk IO _Total <1 %	✓ Disk IO 0 C: <1 %
✓ Intel[R] 82574L... 0.10 kbit/s	✓ Volume IO _To... 78 %	✓ Volume IO C: 78 %	✓ Volume IO Har... 27 %	!! HTTP
!! Windows Upda...	+ Add Sensor			

DESKTOP-CLS2IB6.WORKGROUP (DESKTOP-CLS2IB6) [Windows]

✓ Ping 0 msec	✓ (002) Ethernet... 0.30 kbit/s	✓ (005) Ethernet... 0.28 kbit/s	✓ (006) Ethernet... 0.28 kbit/s	✓ (007) Ethernet... 0.28 kbit/s
✓ (008) Ethernet... 0.30 kbit/s	✓ (009) Ethernet... 0.31 kbit/s	✓ CPU Load 5 %	✓ Disk Free: C:\ L... 79 %	✓ Memory: Physi... 41 %
✓ Memory: Virtu... 42 %	✓ Uptime 1 h 39 m	✓ Pagefile Usage 8 %	✓ Disk IO _Total <1 %	✓ Disk IO 0 C: <1 %
✓ Intel[R] 82574L... 0.10 kbit/s	✓ Volume IO _To... 78 %	✓ Volume IO C: 78 %	✓ Volume IO Har... 27 %	!! HTTP
!! Windows Upda...	+ Add Sensor			

15. Attach a screenshot of your Group 1 Network Discovery to this assignment.

16. Use the PRTG Network Monitor to answer the Reflection questions.

Reflection

1. Click the menu and select Sensors. List all of the sensors active on your devices along with their status. For example, one sensor is “Core Health” and Status is Up. Take a screenshot.

2. Click the menu and select Alarms. Are there any alarms present? What are they? Take a screenshot.

3. Click the menu and select Reports. List 5 of the available reports. How can these reports be used by a Network Administrator in his/her job?

4. Select the Top 100 Busy/Idle Processor Sensors report. In the Period section, click Current Period and click Run Report. Take a screenshot of your report. What is the maximum CPU load of one of your desktops?

5. Return to the Reports and select the Top 100 Free/Full Disk Space Sensors report.In the Period section, click Current Period and click Run Report. Take a screenshot of your report. What is the average disk space of one of your desktops?

6. Return to the Reports and select Top 100 Most/Least Used Memory Sensors report. In the Period section, click Current Period and click Run Report. Take a screenshot of your report. What is the minimum physical memory used of one of your desktops?

Rubric

Standards for This Competency	Point Value
Submitted screenshot of Group 1 Network Discovery	10 points
Correct answer to Question 1	15 points
Correct answer to Question 2	15 points
Correct answer to Question 3	15 points
Correct answer to Question 4	15 points
Correct answer to Question 5	15 points
Correct answer to Question 6	15 points