

STUDY GUIDE FOR MODULE NO. LAB 03**NETWORK PERFORMANCE MONITORING IN RPI****MODULE OVERVIEW**

In the contemporary digital landscape, network performance monitoring emerges as a pivotal aspect of system management. Within this context, the Raspberry Pi, an affordable and compact single-board computer, assumes a noteworthy role. This introduction explores the utilization of Cacti, an open-source network monitoring tool, as an instrumental solution for enhancing network performance oversight on the Raspberry Pi platform. Network performance monitoring involves systematically collecting and analyzing data related to network behavior, providing administrators with valuable insights to optimize resource utilization and ensure efficient infrastructure operation. Leveraging Cacti's web-based interface and the Simple Network Management Protocol (SNMP), the Raspberry Pi becomes a formidable ally in pursuing streamlined and effective network monitoring, applicable to diverse settings such as home networks, small businesses, and educational institutions.

**MODULE LEARNING OUTCOMES**

By the end of this module, participants should be able to:

- ✓ Demonstrate the ability to install any network monitoring tool such as Cacti on a Raspberry Pi, understanding dependencies and prerequisites.
- ✓ Configure network monitoring tool settings to align with specific network requirements, adjusting monitoring parameters for optimal performance.
- ✓ Integrate and configure Simple Network Management Protocol (SNMP) settings for effective data collection from network devices.
- ✓ Utilize Cacti's graphical interface to interpret and analyze network performance metrics visually.
- ✓ Develop skills to troubleshoot installation issues, rectify configuration errors, and implement maintenance routines.
- ✓ Implement security measures to safeguard the integrity and confidentiality of monitoring data.
- ✓ Apply network monitoring in practical scenarios such as home networks, small businesses, and educational environments.
- ✓ Create concise documentation detailing key steps and considerations for future reference.

**LEARNING CONTENT (Installing Cacti Network Monitoring Tool in Raspberry Pi)**

Step 1: You must follow several vital steps to install the Cacti Monitoring Tool on a Raspberry Pi. First, ensure you have all the necessary materials, including a compatible Raspberry Pi model, a microSD card (8GB or larger is recommended), a microSD card reader, a computer with an SD card reader, and an internet connection. Considering that you have fulfilled the requirements, you can insert it into your laptop to boot an OS to your SD card, as shown in Figure 3.1



Figure 3.1 – Inserting SD Card into Laptop with RPi Imager



Step 2: Choose the preferred operating system for your Raspberry Pi boot SD Card. In this case, we will use the Raspberry Pi OS Lite (32-bit) since we don't need to use a desktop environment for installing a Cacti Monitoring Tool, and we only need SSH in this case. You can customize your configuration here or even go wireless and enable SSH for easier access. See Figure 3.2 for reference.



Figure 3.2 – Choosing the RPi OS for SD Card

Step 3: After burning your OS in your SD Card, you can access your file explorer to access the freshly installed OS named boot (D:) and create an empty text file named ssh (should be lowercase), as shown in Figure 3.3.

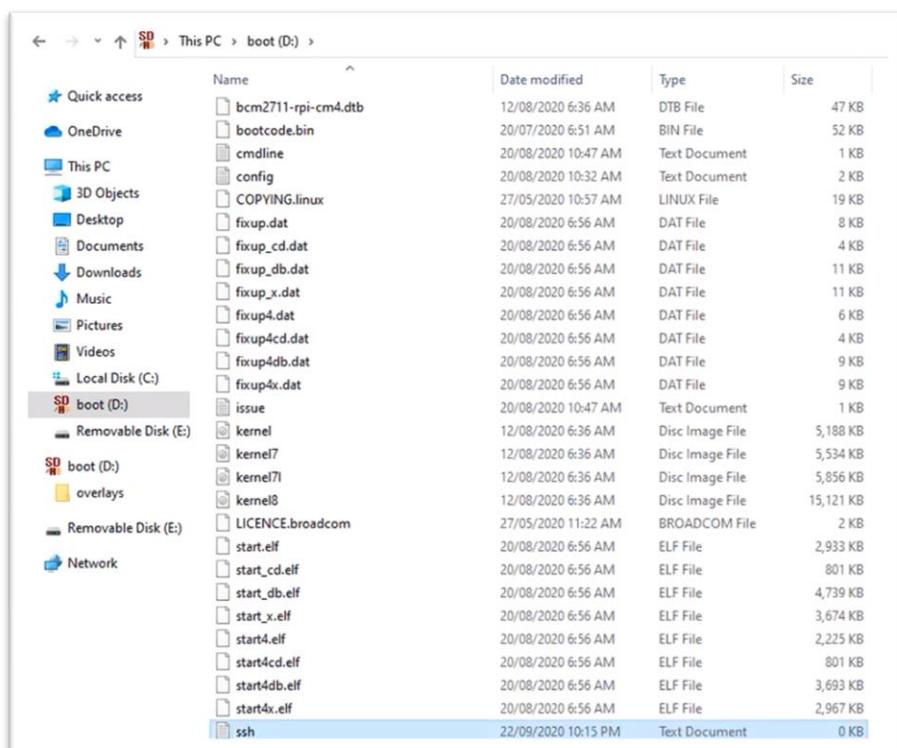


Figure 3.3 – Creating empty SSH text file.

Step 4: Remove your SD Card from your laptop or computer, then insert it into your Raspberry Pi, as shown in Figure 3.4. After that, you can now boot your RPi. You can choose to connect to your AP Router headless or wired, as shown in Figure 3.5.

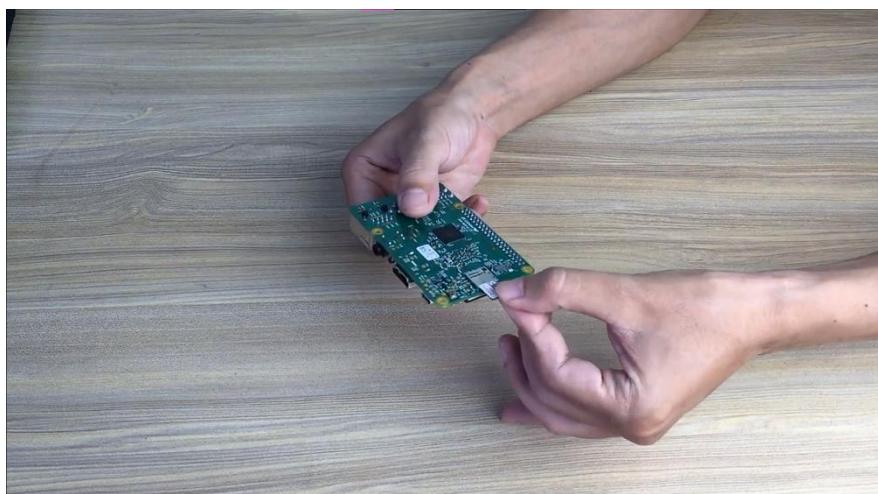


Figure 3.4 – Inserting SD Card on Raspberry Pi

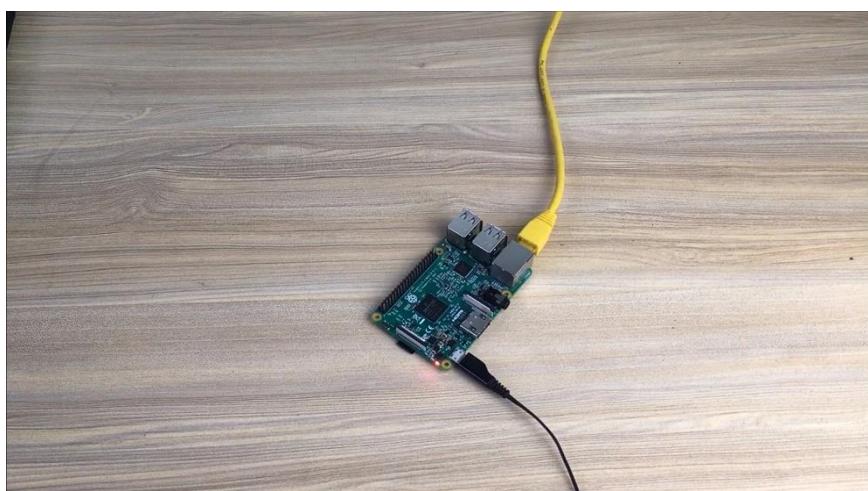


Figure 3.5 – Booting your RPi in Wired Setting

Step 5: Go to your preferred browser, then access the web of your AP router. Next, authenticate your login using the credentials you have. In this case, we will use "username: admin" and "password: admin" for more convenience later, as shown in figure 3.6.

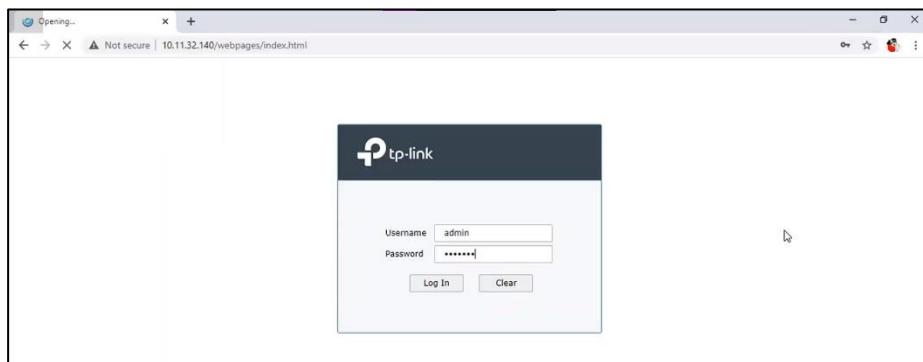


Figure 3.6 – Accessing the AP Router to check IP Address

Step 6: Go to the network drop-down menu and click the LAN option. Since your RPi network relies on DHCP, it is easily found. In this case, it has an IP Address of 10.11.32.130 and is named raspberry pi, as shown in Figure 3.7.

	LAN	DHCP Server	DHCP Client List	Address Reservation	
▶ Status					
▼ Network	9	android-7d97c4bcc7e2e290	C4-6E-7B-05-3F-47	10.11.32.148	1:11:18
• WAN	10	OS-PC	D0-50-99-2D-41-AA	10.11.32.102	1:24:52
• LAN	11	Administrator	90-E6-BA-5A-6F-45	10.11.32.186	1:28:3
• IPTV	12	TL-WR840N	74-DA-88-B0-D1-A7	10.11.32.195	1:33:48
• MAC	13	--	F4-28-53-EF-E6-E0	10.11.32.180	1:52:25
• Switch	14	TL-WR740N	64-66-B3-C5-5E-4D	10.11.32.182	1:53:0
• VLAN	15	21AK22-01092019	B0-6E-BF-2E-87-C0	10.11.32.173	1:29:46
• IPv6	16	Admin-PC	D0-50-99-2D-3E-EB	10.11.32.150	1:46:39
▶ Preferences	17	android-d1354aa560c25167	C4-6E-7B-05-3F-43	10.11.32.118	1:36:25
▶ Transmission	18	raspberrypi	B8-27-EB-70-C9-2D	10.11.32.130	1:58:59
▶ Firewall	19	tt-PC	34-DE-1A-E4-EE-E5	10.11.32.142	0:22:5
▶ Behavior Control	20	android-e9b4bf9b27c2e443	5C-2E-59-1C-E6-6D	10.11.32.103	0:10:41
▶ Authentication	21	android-a563d8a55cee84e1	44-66-FC-B2-CF-FB	10.11.32.125	1:11:13
▶ Services					
▶ System Tools					
Logout					
Copyright © 2017					

Figure 3.7 – Finding the IP Address of Raspberry Pi

Step 7: Now that you know the IP Address, you can go to your Command Prompt and connect to your Raspberry Pi through an SSH connection. To connect with your RPi, type the command:

```
ssh pi@10.11.32.130
```

Where:

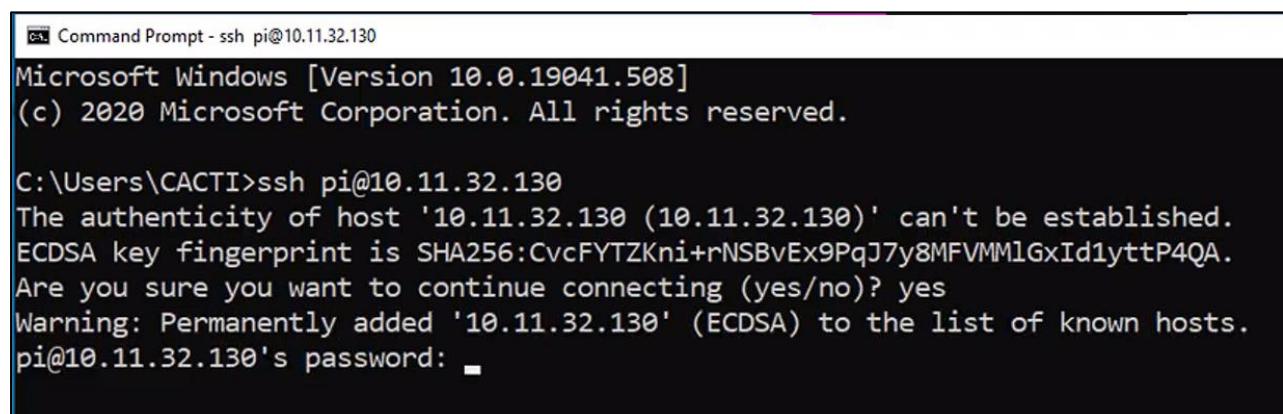
ssh – the command for SSH connection

pi – the username used for authentication

10.11.32.130 – IP Address of the RPi

Note: The command varies depending on the configuration of your Raspberry Pi, so it is important that you configure the credentials in RPi Imager beforehand.

Now, the RPi will ask for your password. It means that you can access the machine through an SSH connection. What is left is the password, and the password here is pi since it is a default password. See Figure 3.8.



```
C:\ Command Prompt - ssh pi@10.11.32.130
Microsoft Windows [Version 10.0.19041.508]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\CACTI>ssh pi@10.11.32.130
The authenticity of host '10.11.32.130 (10.11.32.130)' can't be established.
ECDSA key fingerprint is SHA256:CvcFYTZKni+rNSBvEx9PqJ7y8MFVMMlGxId1yttP4QA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.11.32.130' (ECDSA) to the list of known hosts.
pi@10.11.32.130's password: ■
```

Figure 3.8 – Accessing the RPi with SSH



Step 8: Since your RPi still has the default password, change it to your preference using the command sudo passwd. Then, change your login to root login, as shown in Figure 3.9. Root access will be needed later on for installing the required dependencies.

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

Wi-Fi is currently blocked by rfkill.
Use raspi-config to set the country before use.

pi@raspberrypi:~ $ sudo passwd
New password:
Retype new password:
passwd: password updated successfully
pi@raspberrypi:~ $ su
Password:
root@raspberrypi:/home/pi#
```

Figure 3.9 – RPi Granting Access and changing password.

Step 9: Update your apt package repository using the commands sudo apt update && sudo apt upgrade (this will take time). After the update, install the cacti monitoring tool using the command sudo apt install cacti -y (this will also take time) (see Figure 3.10).

```
pi@raspberrypi: ~
root@raspberrypi:/home/pi# root@raspberrypi:/home/pi#
root@raspberrypi:/home/pi# sudo apt update && sudo apt upgrade
```

Figure 3.10.1 – Updating and upgrading apt packages.

```
pi@raspberrypi: ~
root@raspberrypi:/home/pi# sudo apt-get install cacti -y
```

Figure 3.10.2 – apt installation of cacti monitoring tool.



Step 10: The package installation asks for your configurations in the database. You should choose the Yes option here, as shown in Figure 3.11.1.

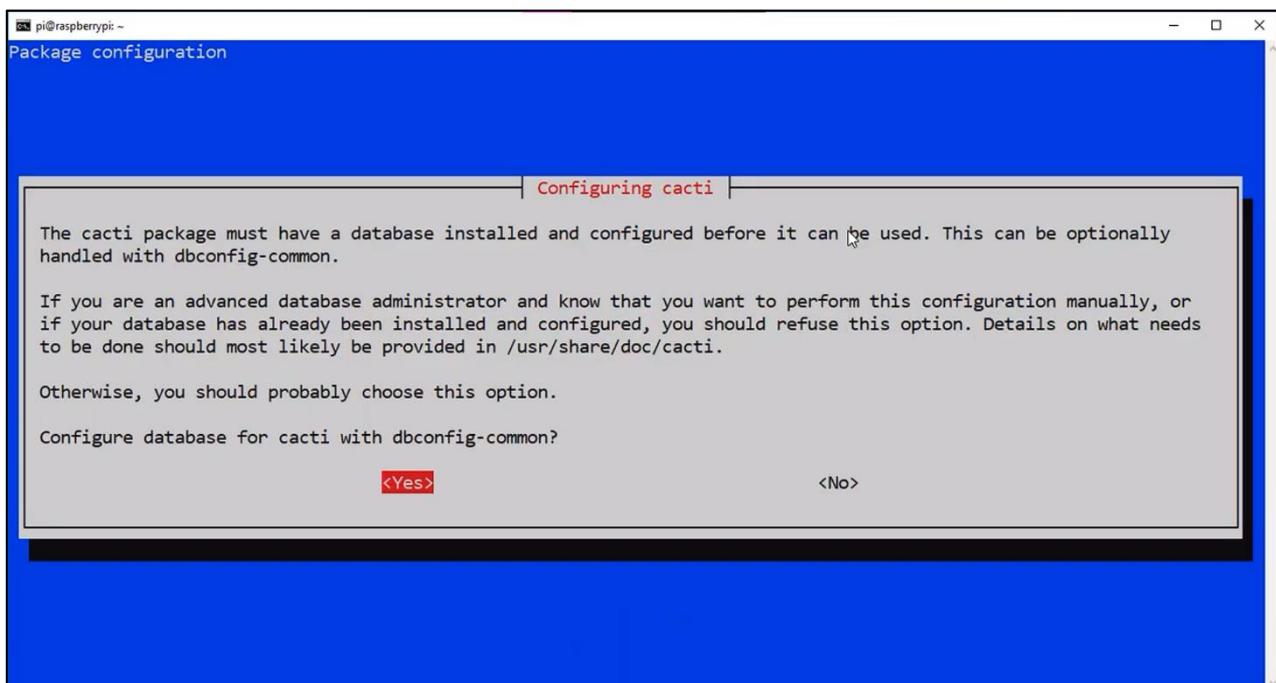


Figure 3.11.1 – configuring cacti database.

Step 11: The package installation will ask you for a password for the MySQL application. Just create a password on your preference, then choose an OK option, as shown in Figure 3.11.2

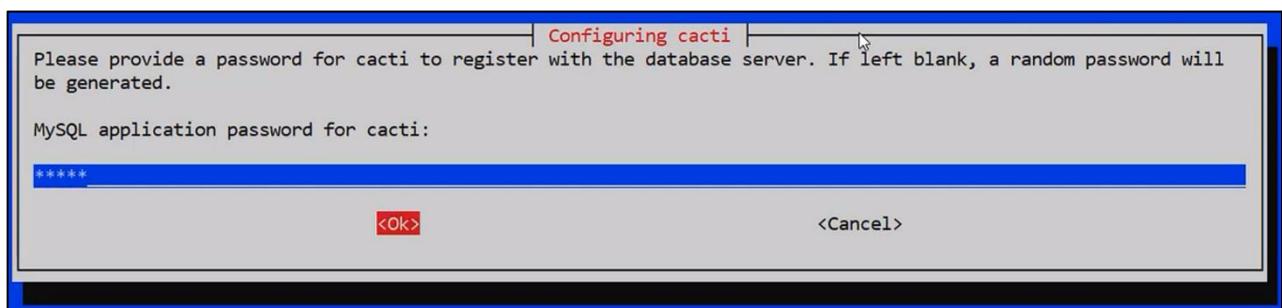


Figure 3.11.2 – configuring MySQL database.

Step 12: Go back to your browser, then type the URL of your webserver. In this case, this will be `http://10.11.32.130/cacti` (This depends on your hostname). After that, the web service will prompt you to authenticate before granting access. You can use the default credential "admin" as your username and password, as shown in Figure 3.12. Then, click log in.

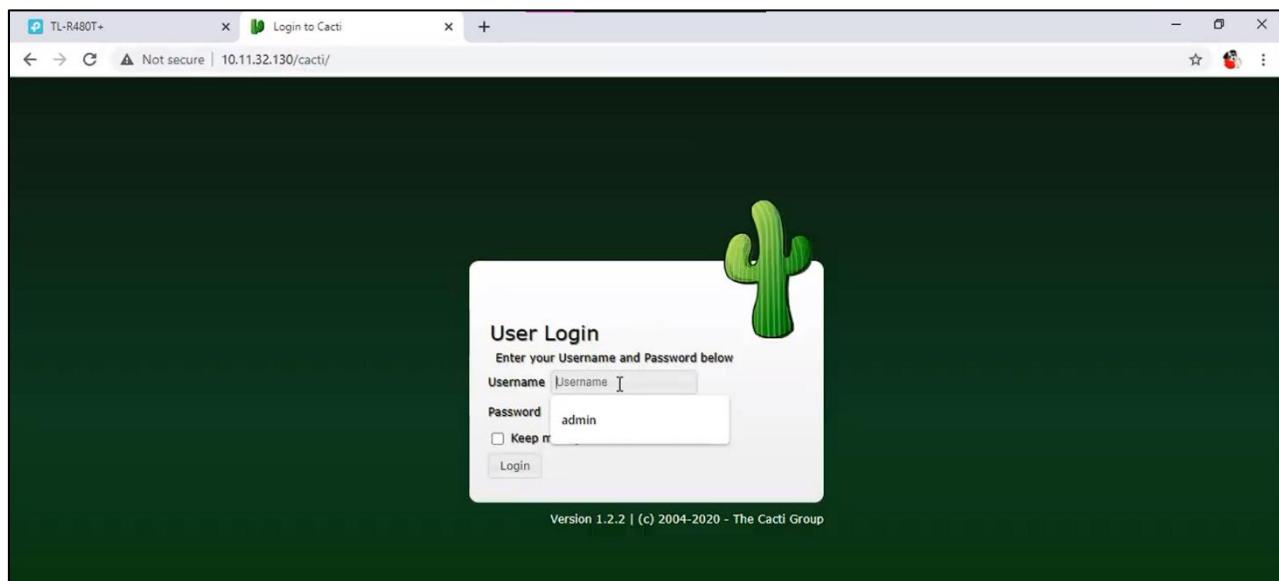


Figure 3.12 – Accessing Cacti Web Server

Step 13: Go back to your Router link, go to the system tools drop-down menu, and choose the SNMP option. Then, click the box of SNMP to enable, then click save, as shown in Figure 3.13.

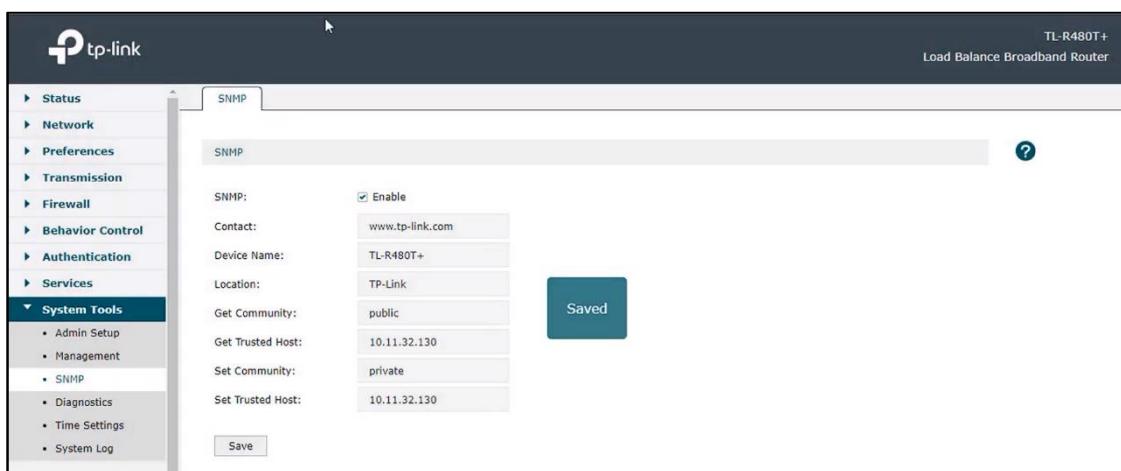


Figure 3.13 – Enabling Router's SNMP

Step 14: Go back to your Cacti, go to devices, and click the add button since no devices have been added yet, as shown in Figure 3.14.



Figure 3.14 – Adding SNMP Devices on Cacti

Step 15: Add a description to your SNMP Device distinct from other devices in the new configuration. Next, click the device templates drop-down menu, then choose the generic SNMP device option, as shown in Figure 2.15. After that, you can leave other configurations as default and proceed to save the configurations.



Figure 3.15 – Configuring Router SNMP.

Step 16: After the configuration, click the create graphs for this device, as shown in 3.16.1. In Data Query, click the box of each option you want to monitor on your SNMP Devices. Choose the option with up status, as shown in Figure 3.16.2, then click Create.



Figure 3.16.1 – Creating graphs for newly-added SNMP Device.

Data Query [SNMP - Interface Statistics]									
All 12 Items									
Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	High Speed	Hardware Address	IP Address
1	Up	lo	lo		24	10000000	10		127.0.0.1
2	Up	eth0	eth0		6	0	0	00 0C 43 28 80 32	<input checked="" type="checkbox"/>
3	Down	ip6tnl0	ip6tnl0		131	0	0		<input type="checkbox"/>
4	Down	sit0	sit0		131	0	0		<input type="checkbox"/>
5	Down	gre0	gre0		131	0	0		<input type="checkbox"/>
6	Down	gretap0	gretap0		6	0	0		<input type="checkbox"/>
7	Down	bond0	bond0		6	0	0	3E 0B 21 09 69 52	<input type="checkbox"/>
8	Up	br-lan	br-lan		6	0	0	70 4F 57 16 A4 B7	10.11.32.140
9	Up	eth0.1	eth0.1		6	0	0	00 0C 43 28 80 32	<input checked="" type="checkbox"/>
10	Up	eth0.10	eth0.10		6	0	0	70 4F 57 16 A4 B8	168.254.165.185
11	Down	eth0.20	eth0.20		6	0	0	70 4F 57 16 A4 B9	<input type="checkbox"/>
13	Up	pppoe-wan1_poe	pppoe-wan1_poe		23	0	0		14.190.237.158

Select a Graph Type to Create Set Default In/Out Bits

Figure 3.16.2 – Choosing interface statistics for SNMP data query.

Step 17: After the Data Query, go to Devices from management options, click the check box of the Router (which is our SNMP Device), then click choose an Action drop-down menu and choose Place on a Tree option, as shown in Figure 3.17. Then click the Go button.

Devices										
All 1 Devices										
Device Description	Hostname	ID	Graphs	Data Sources	Status	In State	Uptime	Poll Time	Current (ms)	Average (ms)
Router	10.11.32.140	1	6	6	Unknown	N/A	N/A	0	0	0

All 1 Devices

Choose an action

Choose an action
Delete
Enable
Disable
Change Device Settings
Clear Statistics
Apply Automation Rules
Sync to Device Template
Place on in Tree (Default Tree)

Figure 3.17 – Placing the SNMP Device on a Tree.



Step 18: Now that you have an SNMP for your Router. The next thing you need to do is to create an SNMP Device for your Windows. Just repeat the step 14 to step 16, as shown in figure 3.18.

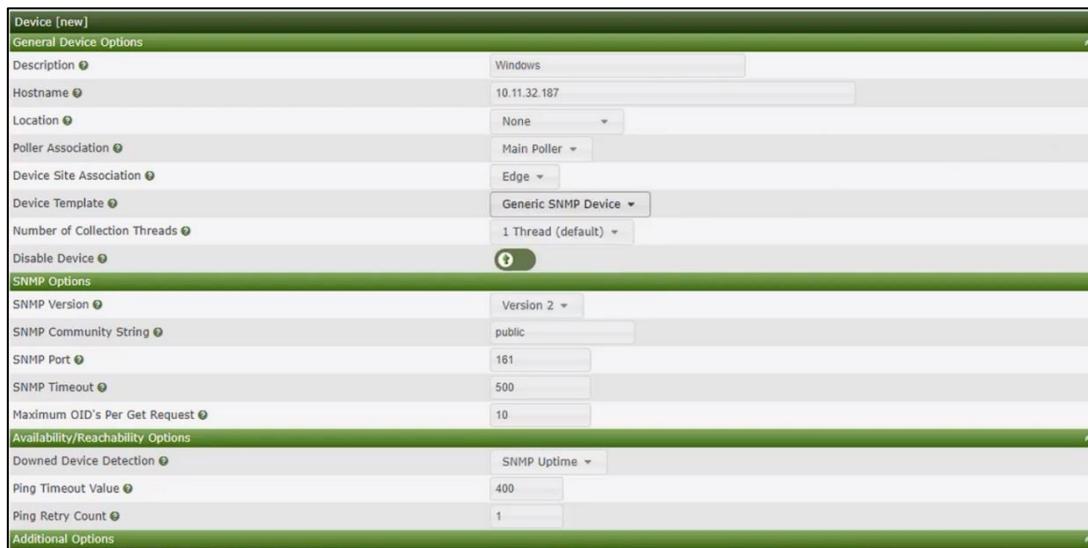


Figure 3.18 – Creating an SNMP Device for Windows

Step 19: Choose your Network Interface Controller, which has an ethernet alias from the option, since we are trying to monitor the network latency from Router to Windows, as shown in figure 3.19. After that, click Create.

Index	Status	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	High Speed	Hardware Address	IP Address	Action
1	Up	Software Loopback Interface 1	loopback_0	Loopback Pseudo-Interface 1	24	1073741824	1073		127.0.0.1	<input type="checkbox"/>
2	notPresent	Microsoft 6to4 Adapter	tunnel_32514	6to4 Adapter	131	0	0			<input type="checkbox"/>
3	Down	WAN Miniport (IKEv2)	tunnel_32769	Local Area Connection™ 2	131	0	0			<input type="checkbox"/>
4	Up	WAN Miniport (Network Monitor)	ethernet_32772	Local Area Connection™ 8	6	0	0			<input type="checkbox"/>
5	notPresent	Microsoft IP-HTTPS Platform A...	tunnel_32513	Microsoft IP-HTTPS Platform In...	131	0	0			<input type="checkbox"/>
6	Up	Realtek PCIe GBE Family Contr...	ethernet_32769	Ethernet	6	100000000	100	34 97 F6 95 F5 EB	10.11.32.187	<input checked="" type="checkbox"/>
7	Up	WAN Miniport (IP)	ethernet_32770	Local Area Connection™ 6	6	0	0			<input type="checkbox"/>
8	Up	Microsoft Teredo Tunneling Ada...	tunnel_32512	Teredo Tunneling Pseudo-Interf...	131	100000	0	00 00 00 00 00 00 E0		<input type="checkbox"/>
9	Down	WAN Miniport (SSTP)	tunnel_32768	Local Area Connection™ 1	131	0	0			<input type="checkbox"/>
10	Up	WAN Miniport (IPv6)	ethernet_32771	Local Area Connection™ 7	6	0	0			<input type="checkbox"/>
11	Down	WAN Miniport (PPTP)	tunnel_32771	Local Area Connection™ 4	131	0	0			<input type="checkbox"/>
12	Down	WAN Miniport (PPPOE)	ppp_32768	Local Area Connection™ 5	23	0	0			<input type="checkbox"/>
13	Up	Famatech RadminVPN Ethernet...	ethernet_32773	Radmin VPN	6	100000000	100	02 50 06 50 CB 8F	26.147.190.58	<input type="checkbox"/>
14	Up	VirtualBox Host-Only Ethernet ...	ethernet_32774	VirtualBox Host-Only Network	6	1000000000	1000	0A 00 27 00 00 0E	192.168.56.1	<input type="checkbox"/>
15	notPresent	Microsoft Kernel Debug Networ...	ethernet_32768	Ethernet (Kernel Debugger)	6	0	0			<input type="checkbox"/>
16	Down	WAN Miniport (L2TP)	tunnel_32770	Local Area Connection™ 3	131	0	0			<input type="checkbox"/>
17	Up	Famatech RadminVPN Ethernet...	ethernet_0	Radmin VPN-WFP Native MAC L...	6	100000000	100	02 50 06 50 CB 8F		<input type="checkbox"/>
18	Up	Famatech RadminVPN Ethernet...	ethernet_1	Radmin VPN-VirtualBox NDIS L...	6	100000000	100	02 50 06 50 CB 8F		<input type="checkbox"/>
19	Up	Famatech RadminVPN Ethernet...	ethernet_2	Radmin VPN-QoS Packet Sched...	6	100000000	100	02 50 06 50 CB 8F		<input type="checkbox"/>
20	Up	Famatech RadminVPN Ethernet...	ethernet_3	Radmin VPN-WFP 802.3 MAC L...	6	100000000	100	02 50 06 50 CB 8F		<input type="checkbox"/>
21	Up	VirtualBox Host-Only Ethernet ...	ethernet_4	VirtualBox Host-Only Network...	6	1000000000	1000	0A 00 27 00 00 0E		<input type="checkbox"/>
22	Up	VirtualBox Host-Only Ethernet ...	ethernet_5	VirtualBox Host-Only Network...	6	1000000000	1000	0A 00 27 00 00 0E		<input type="checkbox"/>

Figure 3.19 – Choosing the SNMP network to monitor.



Step 20: After the Data Query, go to Devices from management options, click the check box of Windows (another SNMP Device), then click Choose an action drop-down menu and choose the Place on a Tree option, as shown in Figure 3.20. Then click the Go button.

Device Description	Hostname	ID	Graphs	Data Sources	Status	In State	Uptime	Poll Time	Current (ms)	Average (ms)	Availability
Router	10.11.32.140	1	6	6	Up	5m	1m	0	4.87	4.87	100 %
Windows	10.11.32.187	2	2	2	Unknown	N/A	N/A	0	0	0	100 %

Figure 3.20 – Placing the Windows SNMP on a Tree.

With all that trouble configuring the SNMP Devices, you can now go to graphs and check all the graphs of the SNMP Devices. See Figures 3.21 and 3.22.^[3]



Figure 3.21 – Windows Network Graph





Figure 3.22 – Route

**LEARNING ACTIVITY 1**Name: Cerujano, Erman Ace M.Due date: February 19, 2024

Step 1: You must follow several vital steps to install the Cacti Monitoring Tool on a Raspberry Pi. First, ensure you have all the necessary materials, including a compatible Raspberry Pi model, a microSD card (8GB or larger is recommended), a microSD card reader, a computer with an SD card reader, and an internet connection. Considering that you have fulfilled the requirements, you can insert it into your laptop to boot an OS to your SD card, as shown in Figure 3.1



Figure 3.1 – Inserting SD Card into Laptop with RPi Imager

Step 2: Choose the preferred operating system for your Raspberry Pi boot SD Card. In this case, we will use the Raspberry Pi OS Lite (32-bit) since we don't need to use a desktop environment for installing a Cacti Monitoring Tool, and we only need SSH in this case. You can customize your configuration here or even go wireless and enable SSH for easier access. See Figure 3.2 for reference.



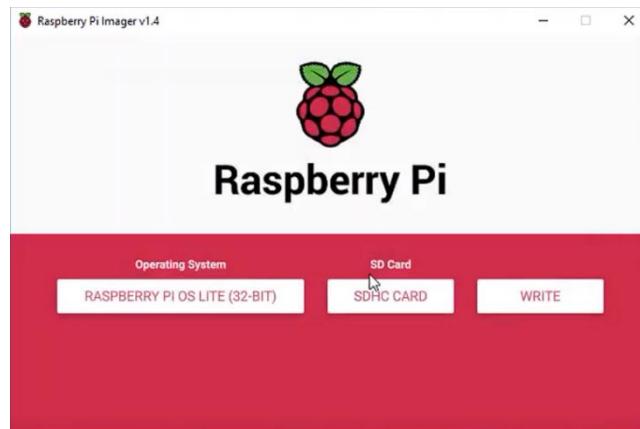


Figure 3.2 – Choosing the RPi OS for SD Card

Step 3: After burning your OS in your SD Card, you can access your file explorer to access the freshly installed OS named boot (D:) and create an empty text file named ssh (should be lowercase), as shown in Figure 3.3.

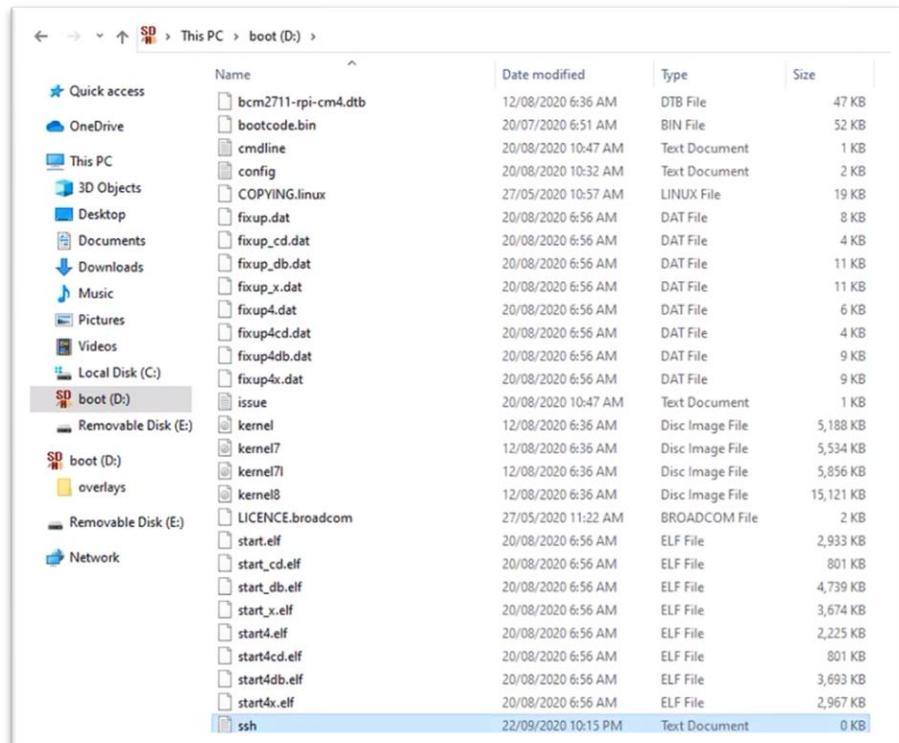


Figure 3.3 – Creating empty SSH text file.

Step 4: Remove your SD Card from your laptop or computer, then insert it into your Raspberry Pi, as shown in Figure 3.4. After that, you can now boot your RPi. You can choose to connect to your AP Router headless or wired, as shown in Figure 3.5.

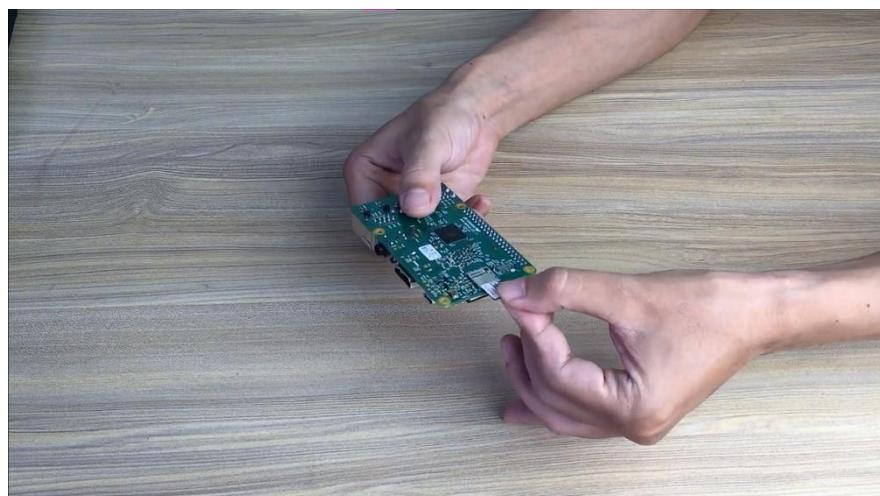


Figure 3.4 – Inserting SD Card on Raspberry Pi

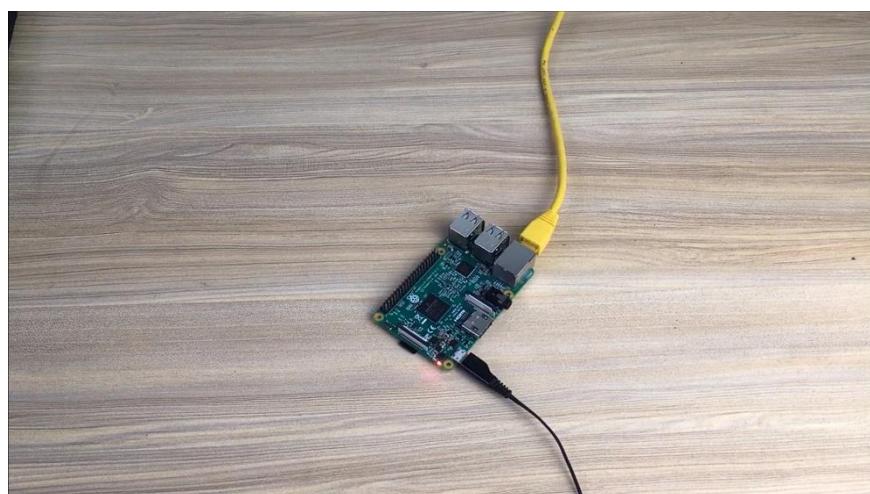


Figure 3.5 – Booting your RPi in Wired Setting

Step 5: Go to your preferred browser, then access the web of your AP router. Next, authenticate your login using the credentials you have. In this case, we will use "username: admin" and "password: admin" for more convenience later, as shown in figure 3.6.

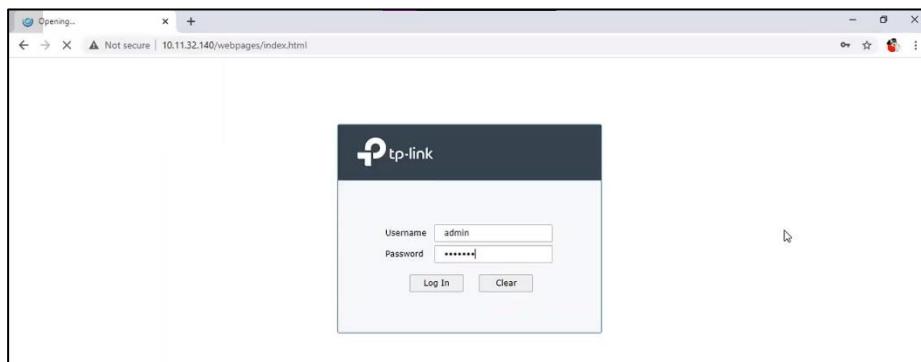


Figure 3.6 – Accessing the AP Router to check IP Address

Step 6: Go to the network drop-down menu and click the LAN option. Since your RPi network relies on DHCP, it is easily found. In this case, it has an IP Address of 10.11.32.130 and is named raspberry pi, as shown in Figure 3.7.

	LAN	DHCP Server	DHCP Client List	Address Reservation	
▶ Status					
▼ Network	9	android-7d97c4bcc7e2e290	C4-6E-7B-05-3F-47	10.11.32.148	1:11:18
• WAN	10	OS-PC	D0-50-99-2D-41-AA	10.11.32.102	1:24:52
• LAN	11	Administrator	90-E6-BA-5A-6F-45	10.11.32.186	1:28:3
• IPTV	12	TL-WR840N	74-DA-88-B0-D1-A7	10.11.32.195	1:33:48
• MAC	13	--	F4-28-53-EF-E6-E0	10.11.32.180	1:52:25
• Switch	14	TL-WR740N	64-66-B3-C5-5E-4D	10.11.32.182	1:53:0
• VLAN	15	21AK22-01092019	B0-6E-BF-2E-87-C0	10.11.32.173	1:29:46
• IPv6	16	Admin-PC	D0-50-99-2D-3E-EB	10.11.32.150	1:46:39
▶ Preferences	17	android-d1354aa560c25167	C4-6E-7B-05-3F-43	10.11.32.118	1:36:25
▶ Transmission	18	raspberrypi	B8-27-EB-70-C9-2D	10.11.32.130	1:58:59
▶ Firewall	19	tt-PC	34-DE-1A-E4-EE-E5	10.11.32.142	0:22:5
▶ Behavior Control	20	android-e9b4bf9b27c2e443	5C-2E-59-1C-E6-6D	10.11.32.103	0:10:41
▶ Authentication	21	android-a563d8a55cee84e1	44-66-FC-B2-CF-FB	10.11.32.125	1:11:13
▶ Services					
▶ System Tools					
Logout					
Copyright © 2017					

Figure 3.7 – Finding the IP Address of Raspberry Pi



Step 7: Now that you know the IP Address, you can go to your Command Prompt and connect to your Raspberry Pi through an SSH connection. To connect with your RPi, type the command:

```
ssh pi@10.11.32.130
```

Where:

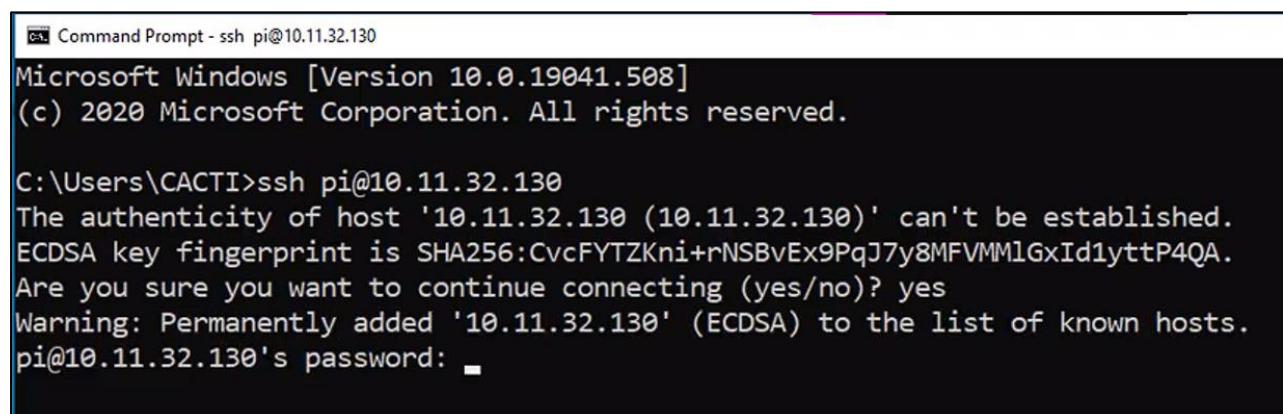
ssh – the command for SSH connection

pi – the username used for authentication

10.11.32.130 – IP Address of the RPi

Note: The command varies depending on the configuration of your Raspberry Pi, so it is important that you configure the credentials in RPi Imager beforehand.

Now, the RPi will ask for your password. It means that you can access the machine through an SSH connection. What is left is the password, and the password here is pi since it is a default password. See Figure 3.8.



```
C:\ Command Prompt - ssh pi@10.11.32.130
Microsoft Windows [Version 10.0.19041.508]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\CACTI>ssh pi@10.11.32.130
The authenticity of host '10.11.32.130 (10.11.32.130)' can't be established.
ECDSA key fingerprint is SHA256:CvcFYTZKni+rNSBvEx9PqJ7y8MFVMMlGxId1yttP4QA.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.11.32.130' (ECDSA) to the list of known hosts.
pi@10.11.32.130's password: ■
```

Figure 3.8 – Accessing the RPi with SSH



Step 8: Since your RPi still has the default password, change it to your preference using the command sudo passwd. Then, change your login to root login, as shown in Figure 3.9. Root access will be needed later on for installing the required dependencies.

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

Wi-Fi is currently blocked by rfkill.
Use raspi-config to set the country before use.

pi@raspberrypi:~ $ sudo passwd
New password:
Retype new password:
passwd: password updated successfully
pi@raspberrypi:~ $ su
Password:
root@raspberrypi:/home/pi#
```

Figure 3.9 – RPi Granting Access and changing password.

Step 9: Update your apt package repository using the commands sudo apt update && sudo apt upgrade (this will take time). After the update, install the cacti monitoring tool using the command sudo apt install cacti -y (this will also take time) (see Figure 3.10).

```
pi@raspberrypi: ~
root@raspberrypi:/home/pi# root@raspberrypi:/home/pi#
root@raspberrypi:/home/pi# sudo apt update && sudo apt upgrade
```

Figure 3.10.1 – Updating and upgrading apt packages.

```
pi@raspberrypi: ~
root@raspberrypi:/home/pi# sudo apt-get install cacti -y
```

Figure 3.10.2 – apt installation of cacti monitoring tool.



Step 10: The package installation asks for your configurations in the database. You should choose the Yes option here, as shown in Figure 3.11.1.

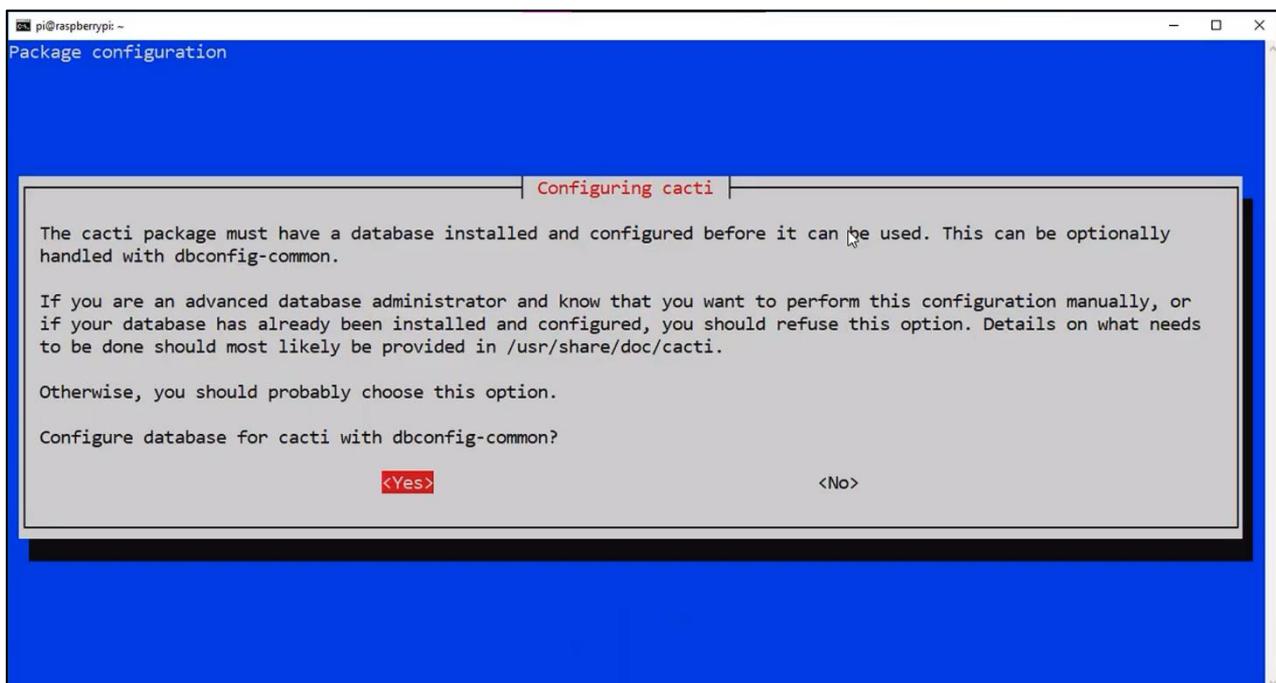


Figure 3.11.1 – configuring cacti database.

Step 11: The package installation will ask you for a password for the MySQL application. Just create a password on your preference, then choose an OK option, as shown in Figure 3.11.2

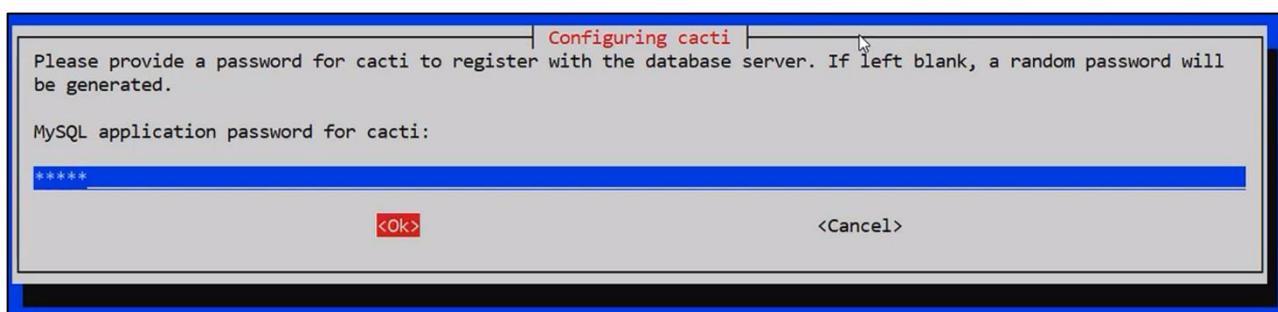


Figure 3.11.2 – configuring MySQL database.

Step 12: Go back to your browser, then type the URL of your webserver. In this case, this will be <http://10.11.32.130/cacti> (This depends on your hostname). After that, the web service will prompt you to authenticate before granting access. You can use the default credential "admin" as your username and password, as shown in Figure 3.12. Then, click log in.

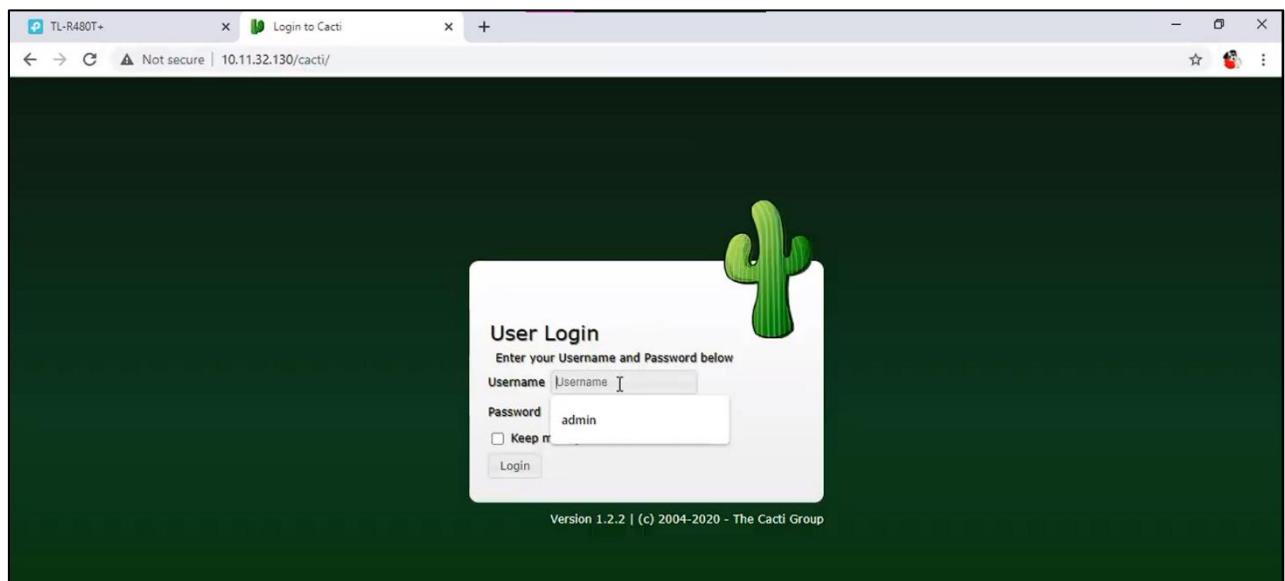


Figure 3.12 – Accessing Cacti Web Server

Step 13: Setting up SNMP on your monitored device involves several steps. Begin by selecting the device you intend to monitor. Then, proceed to configure SNMP by following the instructions provided below. Navigate to the device's settings menu to initiate the process.

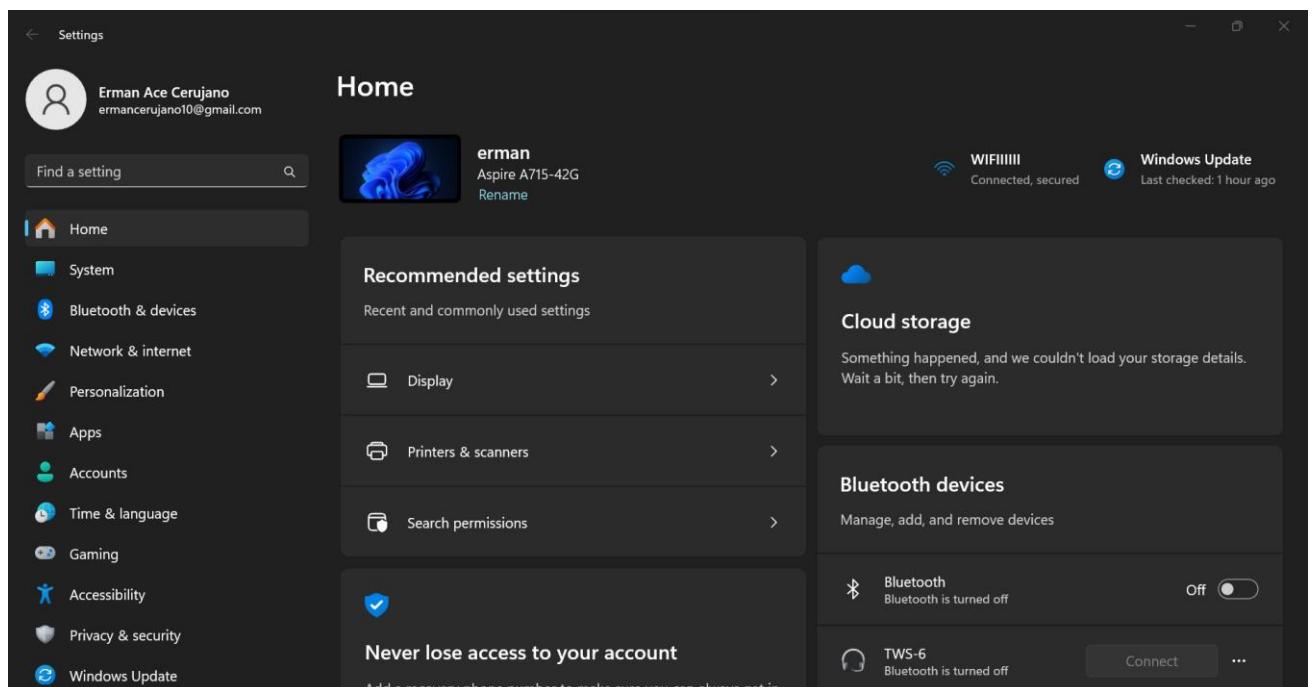


Figure 2-13: Windows Setting

- Search for “Add Optional Feature”

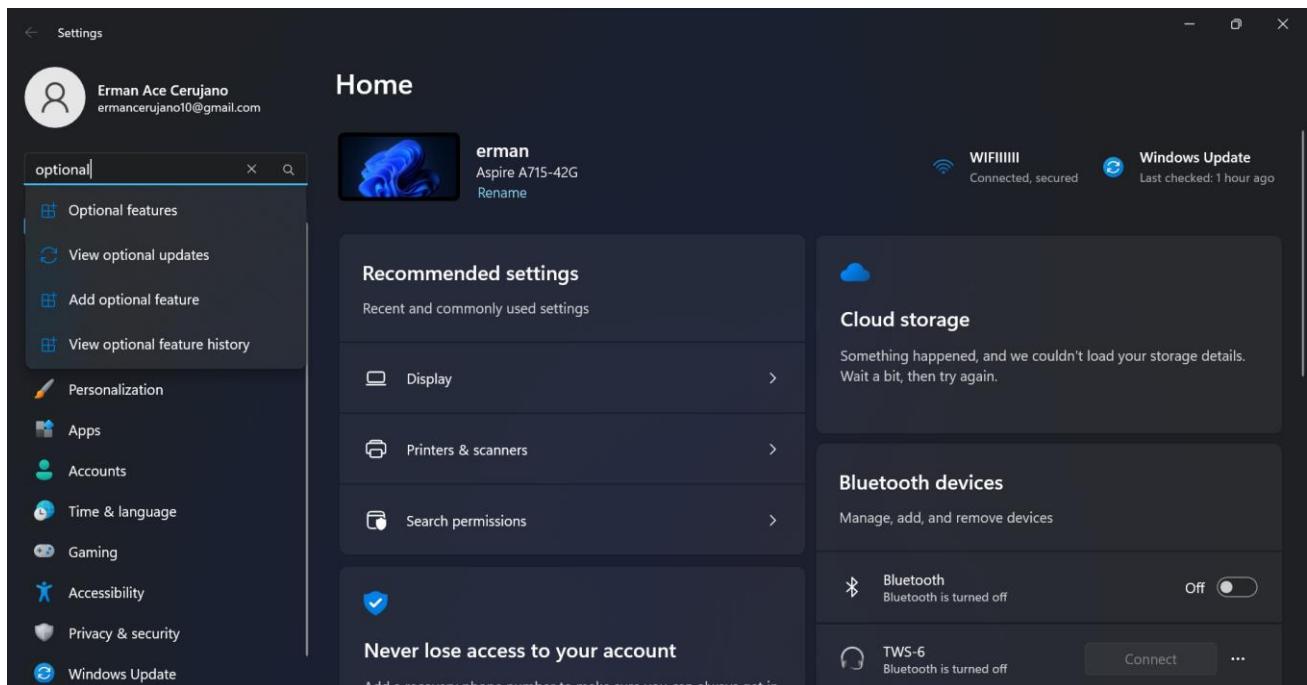


Figure 2-14: Searching for “Add Optional Feature”

- Then click the “Add an optional feature.”

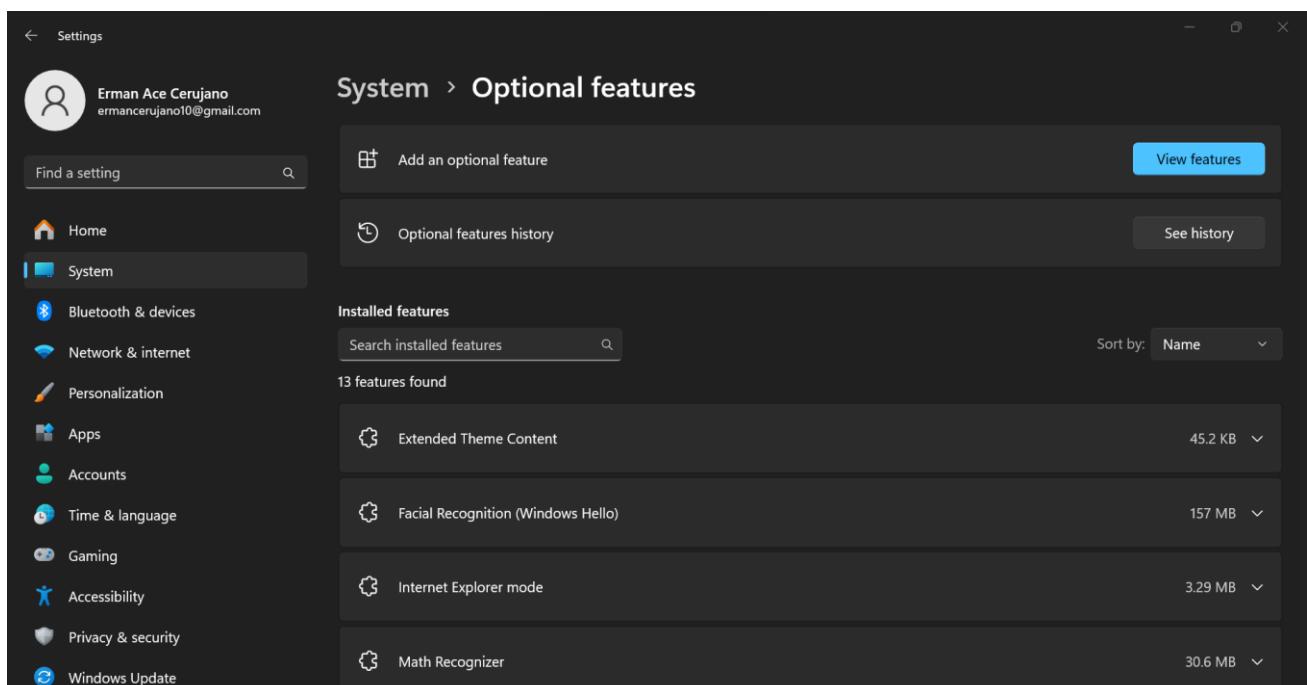


Figure 2-15: Optional Feature Tab



- Search for “SNMP” then click “Next.”

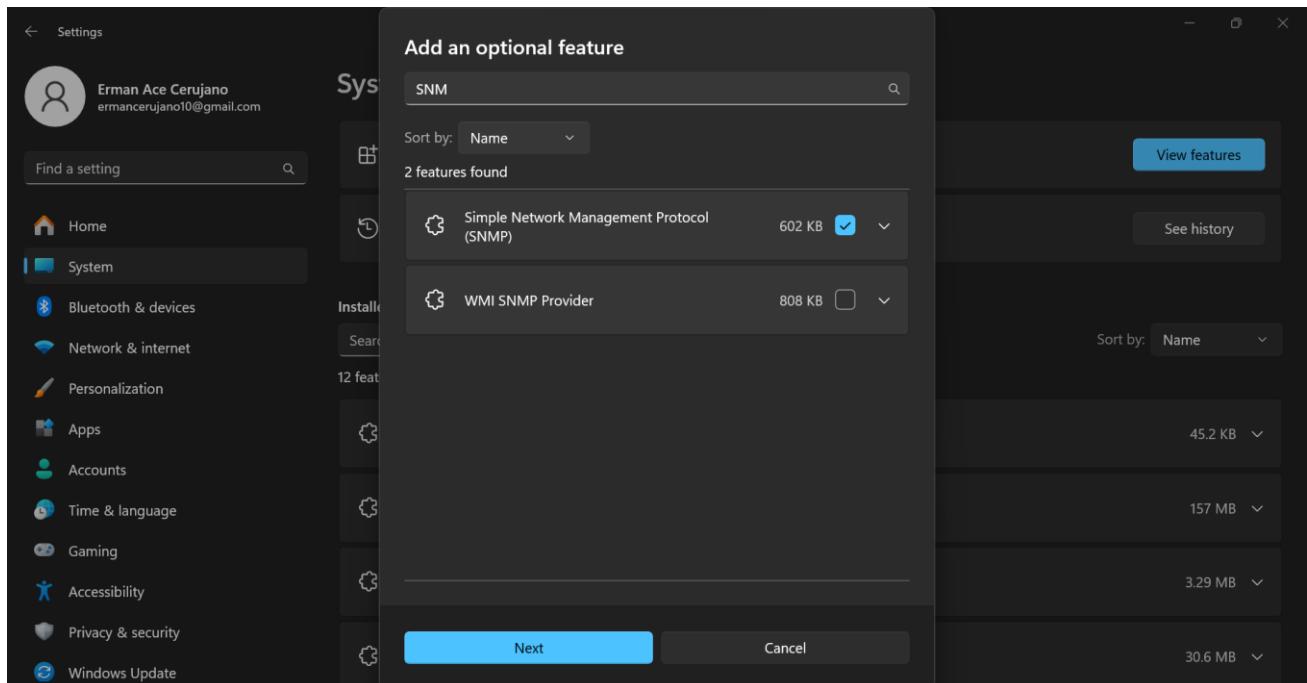


Figure 2-16: Searching for SNMP

- Then click “Install.”

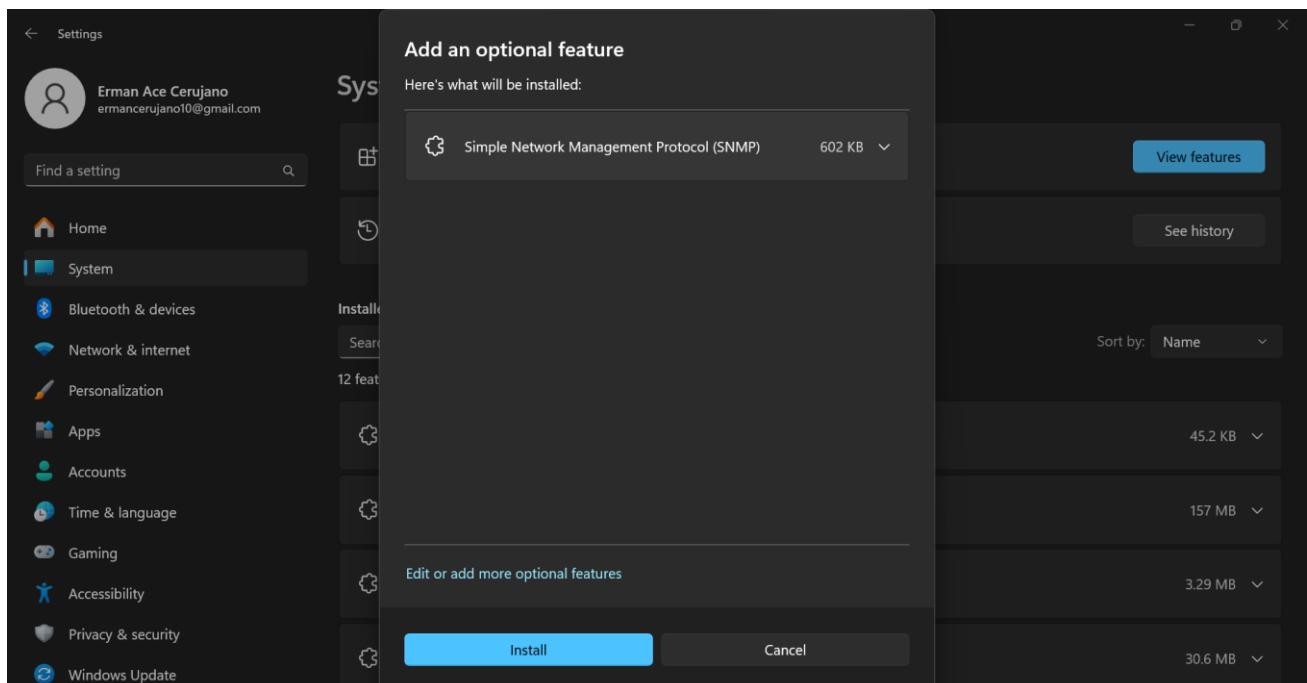


Figure 2-15: Installing SNMP

- Wait for the SNMP to install.



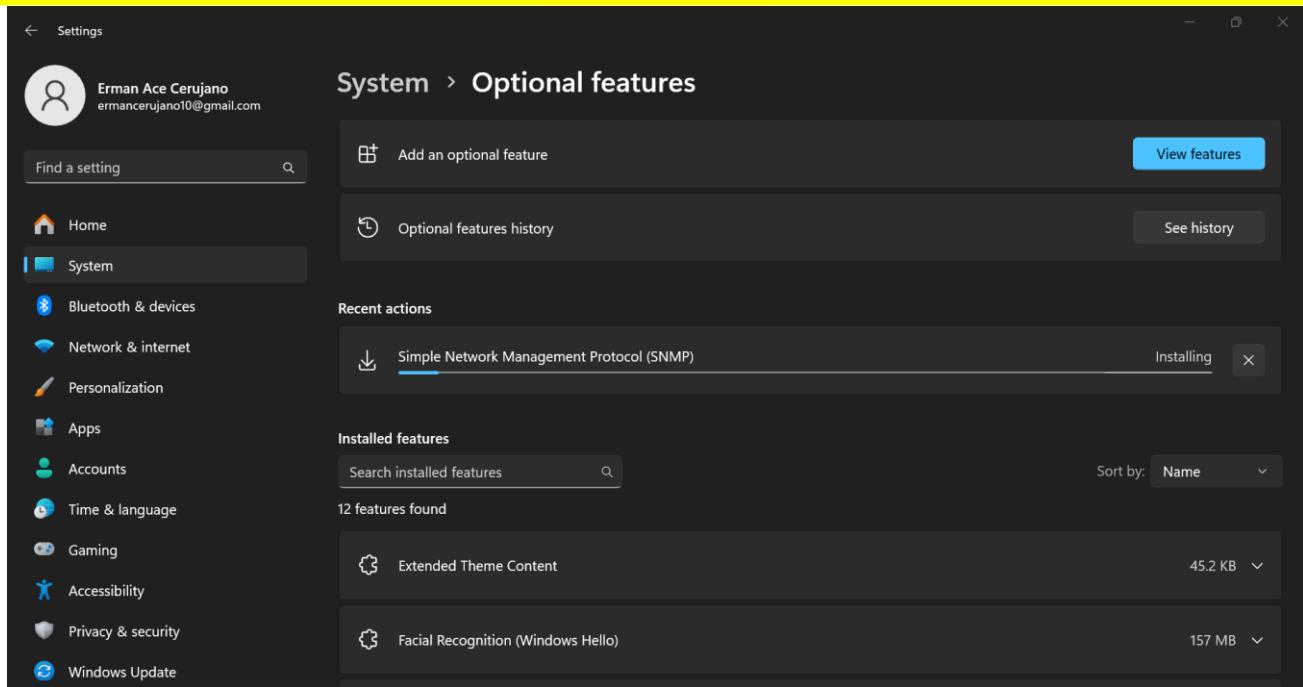


Figure 2-17: Installing SNMP

- You now successfully Install the SNMP into your computer.

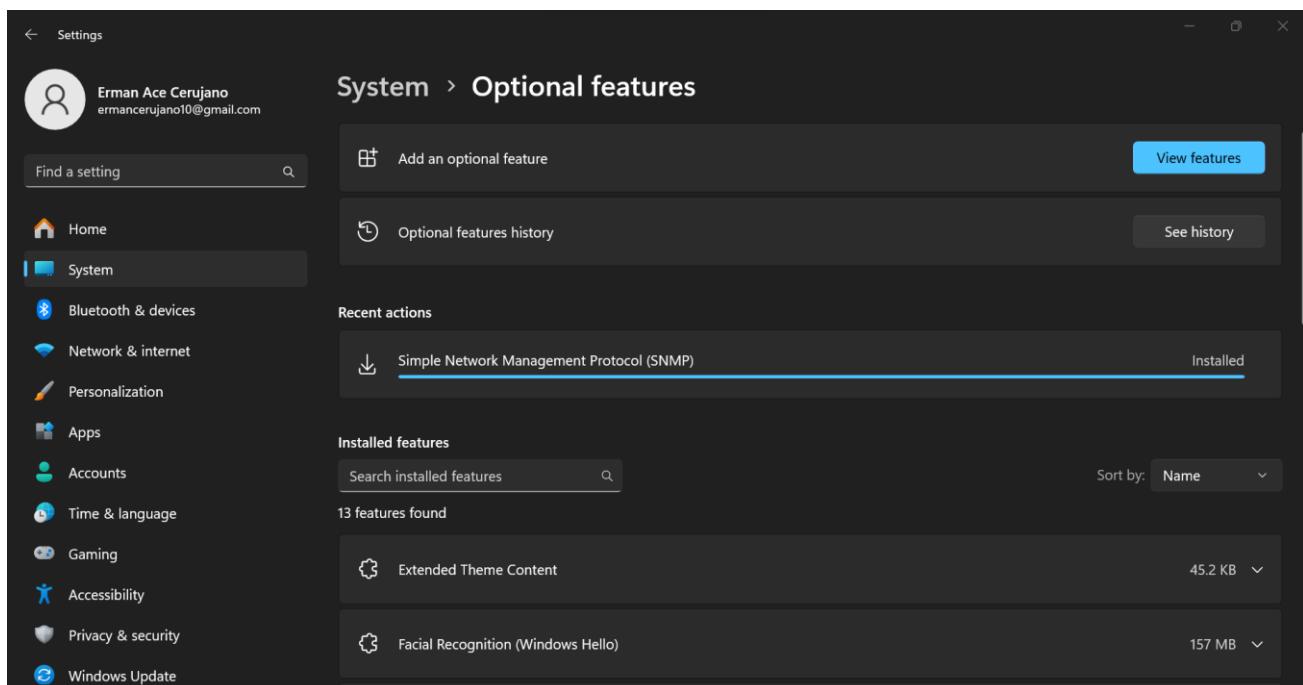


Figure 3-18: Successfully Installed SNMP

Step 14. Before proceeding with monitoring using Cacti, it's essential to configure SNMP on your device. Start by entering the host IP address into the SNMP configuration settings. This step is crucial for ensuring that Cacti can properly recognize and monitor the device.

- Go to “Services” and find “SNMP Service.”



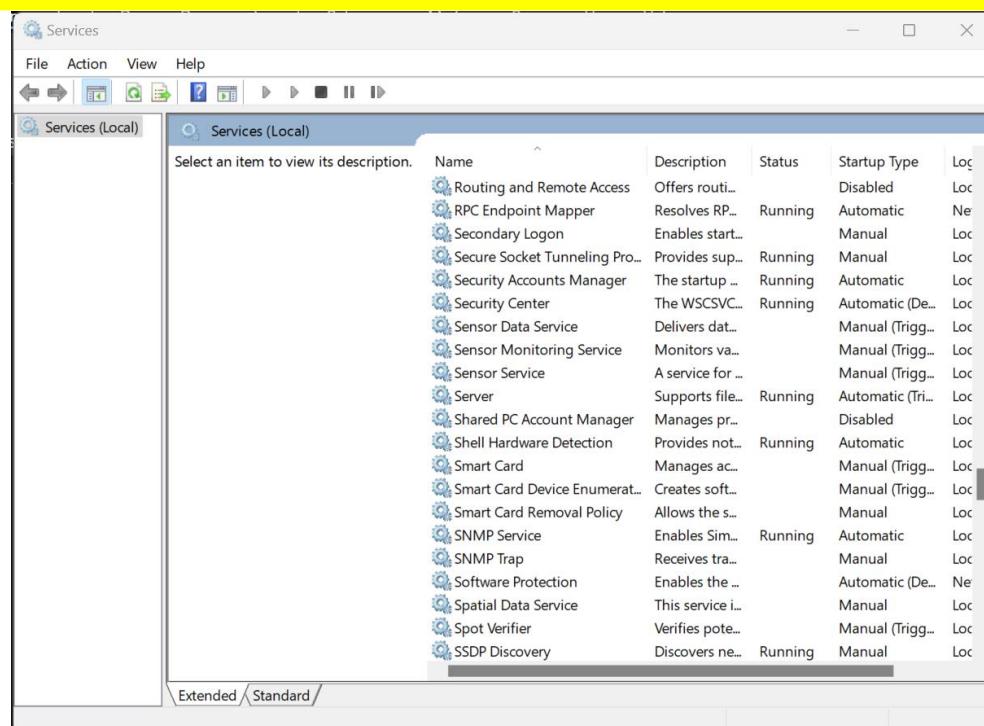


Figure 3-19: Services

- Navigate to the "Agent" section and ensure that all checkboxes are selected. This step ensures that all necessary parameters are enabled for proper functionality.

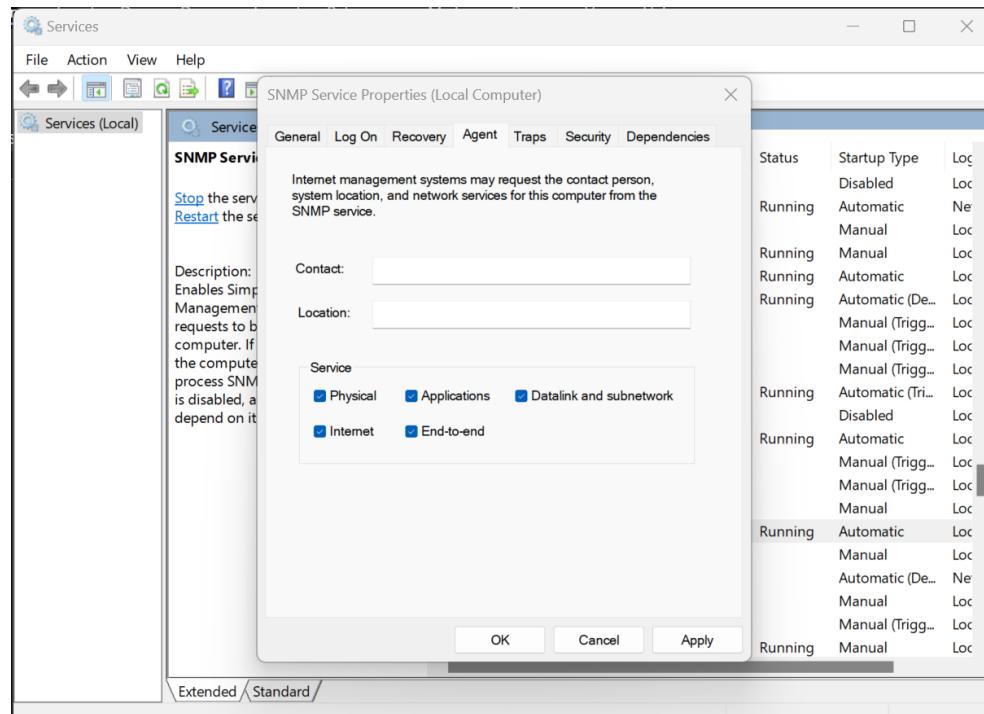


Figure 3-20: Configuring the SNMP Service Properties Agent"

- Go to security then click “Add” in “Accepted Community Names.”



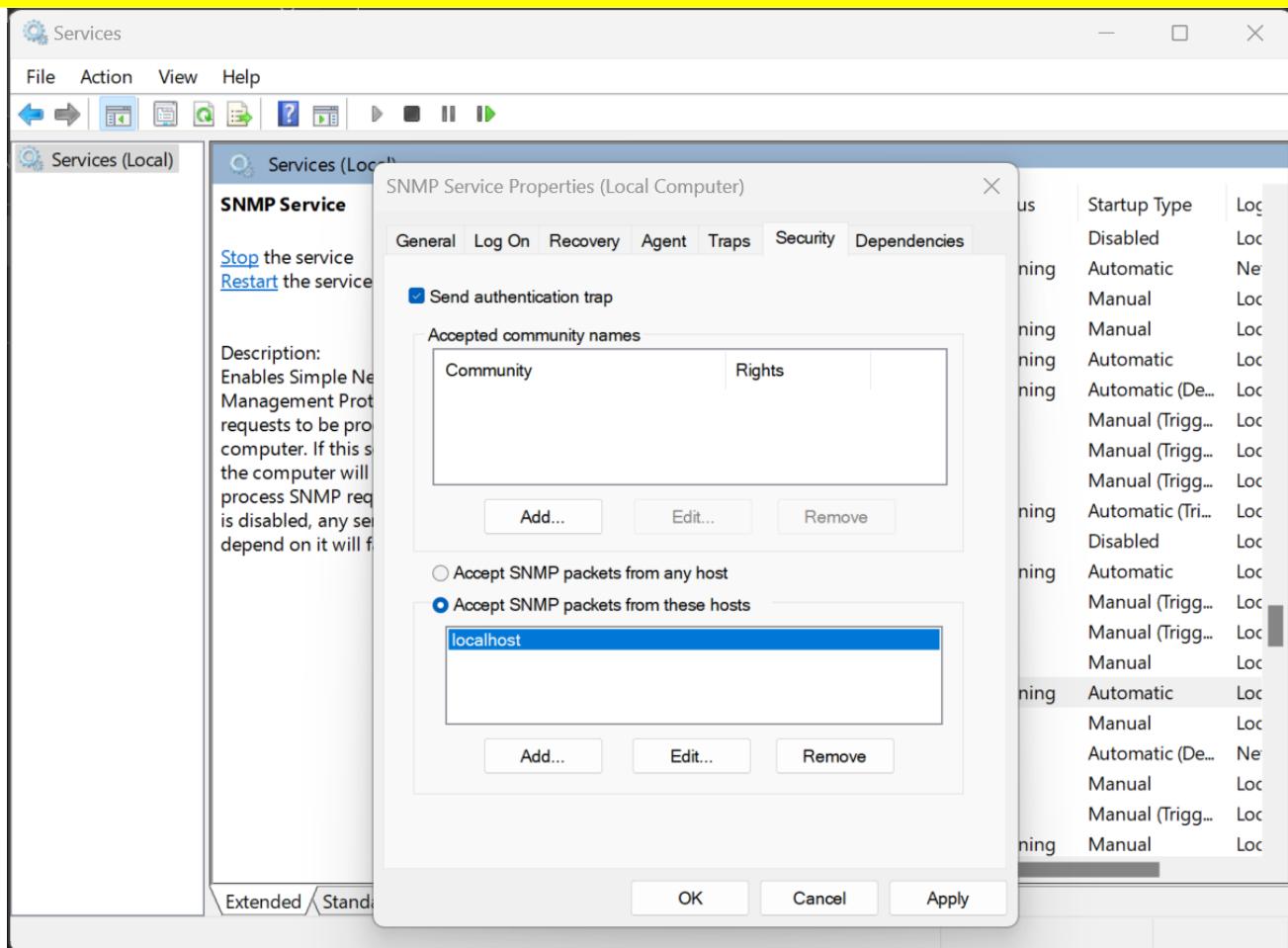


Figure 3-21: Configuring the “SNMP Service Security”

- In “Community Rights” select the “Read Only” and in “Community Name” enter “public” then click the “Add” Button. After that click “Apply” then “OK”



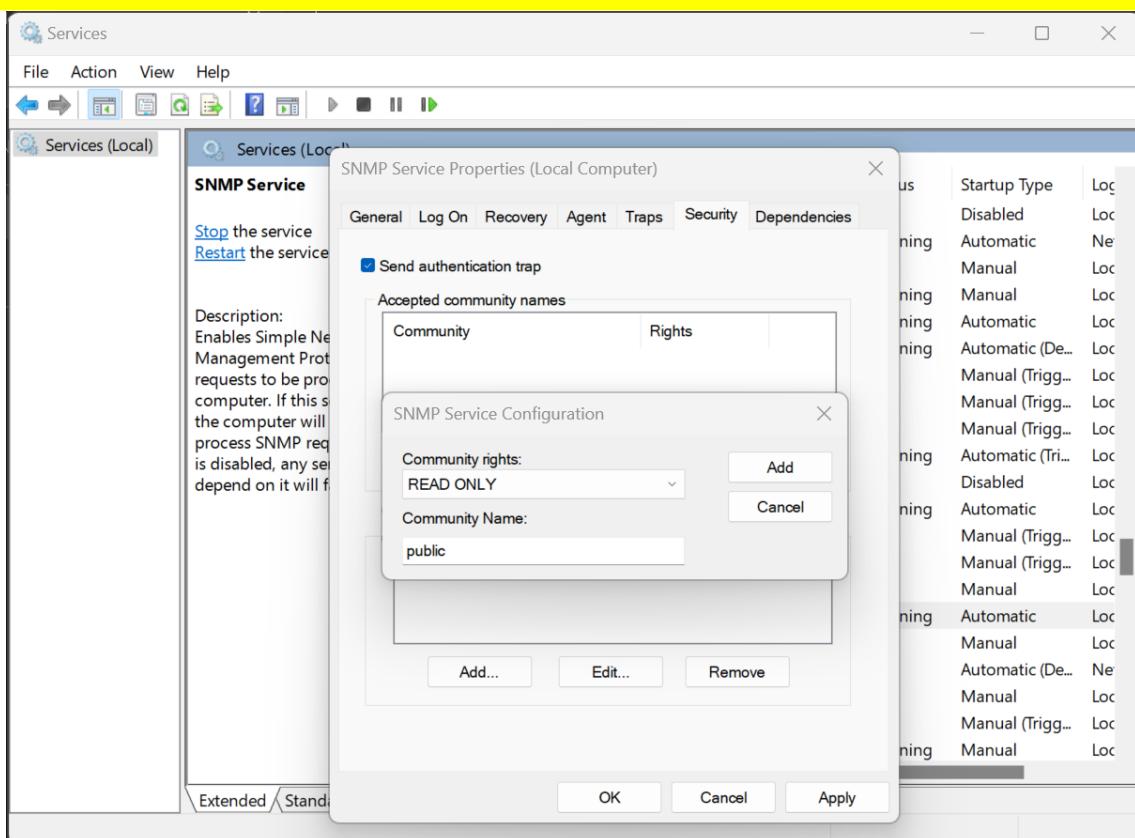


Figure 3-22: Configuring the SNMP Service Security 2

- Next select “Accept SNMP packets from these hosts” then click the “add” button.

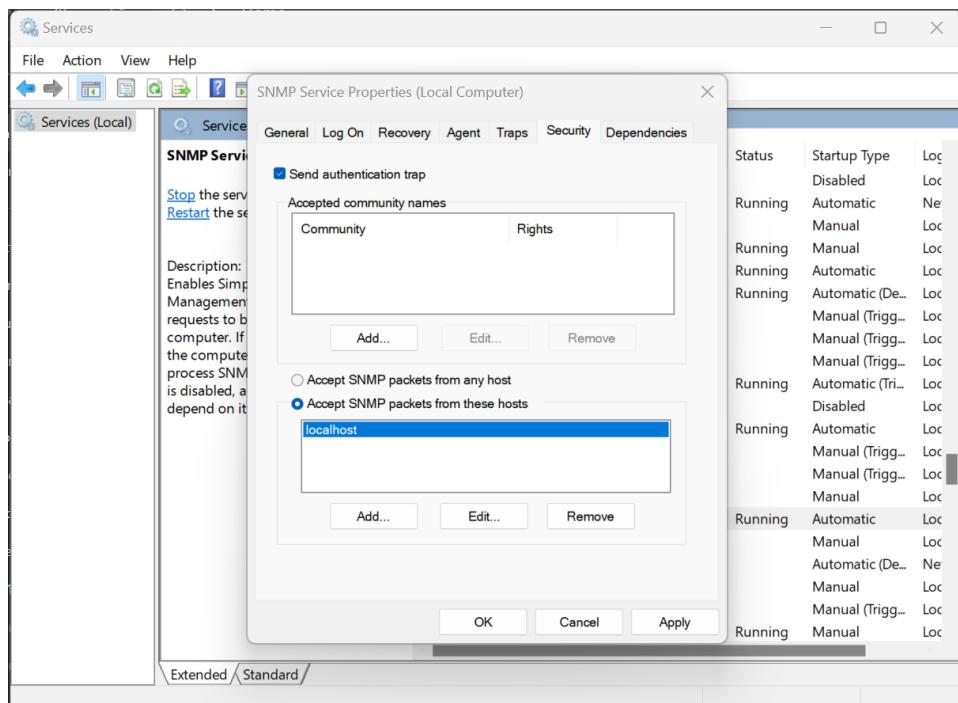


Figure 3-23: Configuring SNMP Service Properties

- Then add the IP address of your RPI then click “Add”



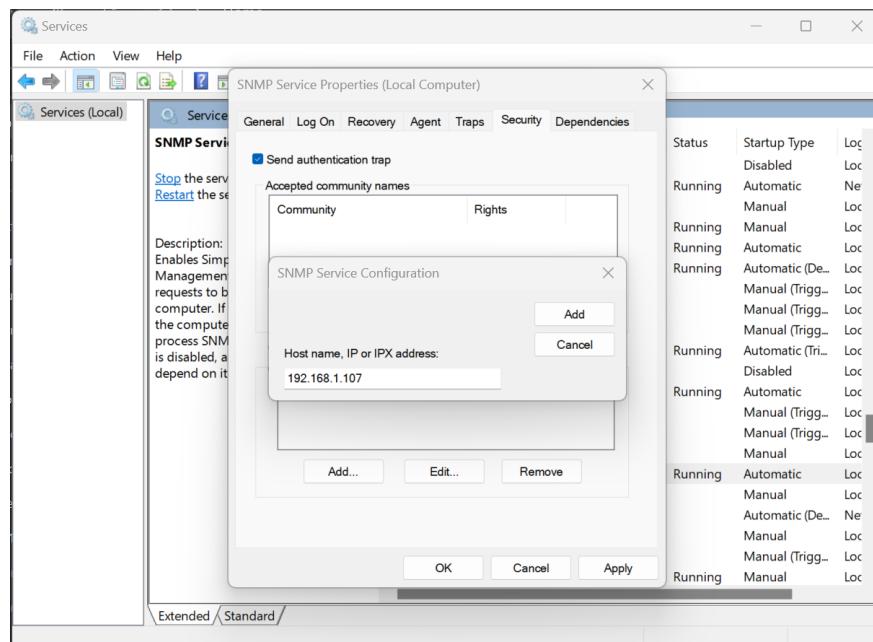


Figure 3-24: Entering the IP of Host.

- Then click “Apply” and “OK”

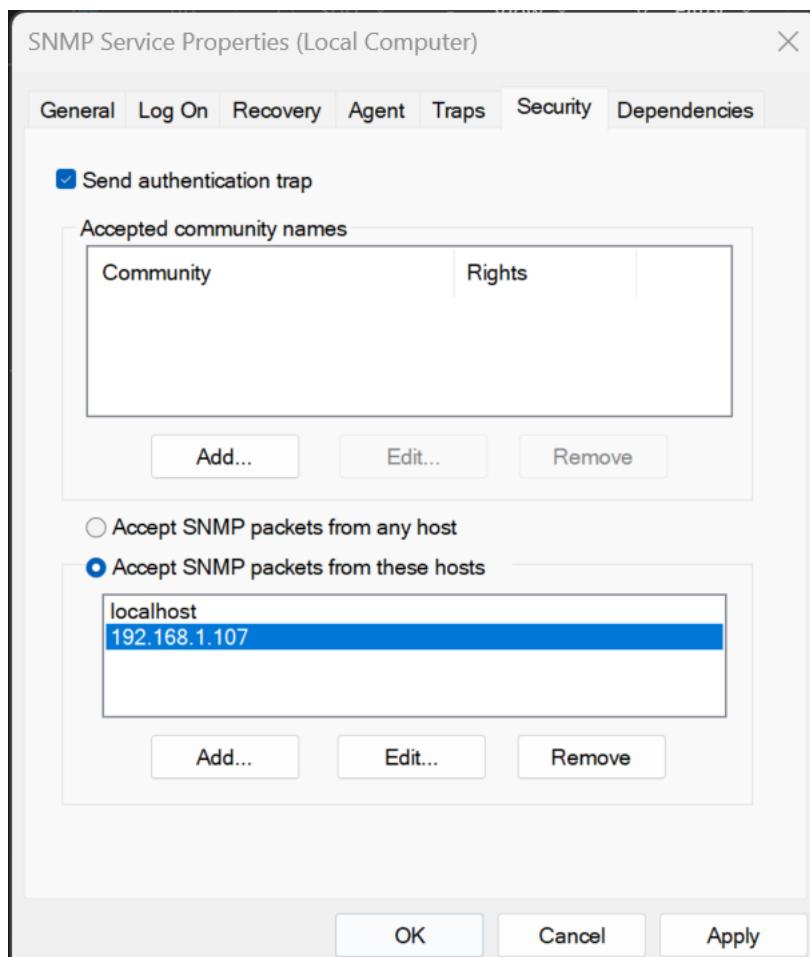


Figure 3-24: Done Configuring the SNMP Service



You have now successfully completed the configuration of SNMP on your computer.

Step 15. Adding your device into the Cacti. Go back to your cacti then go to “Management” then click “Devices” then click the “Add” button.

All 16 Devices											
Device Description	Hostname	ID	Graphs	Data Sources	Status	In State	Uptime	Poll Time	Current (ms)	Average (ms)	Availability
Ace Device	192.168.1.100	12	7	5	Up	25m	11h:40m	0.08	6.93	9.21	100 %
Ace Device Laptop	192.168.1.100	13	29	27	Up	25m	11h:40m	0.38	6.93	9.21	100 %
Device	192.168.1.107	6	7	5	Down	11h:25m	N/A	1.01	0	0	0 %
Device 1	192.168.1.100	16	20	20	Up	25m	11h:40m	0.44	6.93	9.21	100 %
Device1	192.168.1.107	5	19	27	Down	11h:25m	N/A	1.01	0	0	0 %
Device2	192.168.1.107	7	7	5	Down	11h:25m	N/A	1.01	0	0	0 %
Device2	192.168.1.107	8	7	5	Down	11h:25m	N/A	1.01	0	0	0 %
Device2	192.168.1.107	9	7	5	Down	11h:25m	N/A	1.01	0	0	0 %
Device2	192.168.1.100	10	29	27	Up	25m	11h:40m	0.43	6.93	9.21	100 %
floyd	192.168.1.103	15	16	16	Down	20m	N/A	1.01	44.66	50.87	50 %
Floyd Device	192.168.1.103	14	4	4	Down	20m	N/A	1.01	44.66	50.87	50 %
Laptop	192.168.1.107	3	3	3	Down	11h:25m	N/A	1.01	0	0	0 %
Laptop	192.168.1.107	4	5	5	Down	11h:25m	N/A	1.01	0	0	0 %
Laptop-1	192.168.1.100	11	7	5	Up	25m	11h:40m	0.07	6.93	9.21	100 %
PC 1	192.168.1.1	1	5	5	Down	6h:5m	N/A	1.01	0	0	0 %
	11.22.2.1	2	3	3	Down	5h:20m	N/A	1.01	0	0	0 %

Figure 3-25: Cacti Devices

Step 16. Now, input the necessary details as outlined below:

- For the Description, choose any name that you prefer for the device you intend to monitor.
- Input the IP address of the device you wish to monitor into the Hostname field.
- Select the "Generic SNMP Device" option from the device template.
- Finally, press Enter to proceed.

Figure 3-26: Adding Device into your Cacti Devices



Step 17. Creating Graphs. If the SNMP information of your device is working can now be able to create a graph to your device. Click the “Create Graphs for this Device” button.

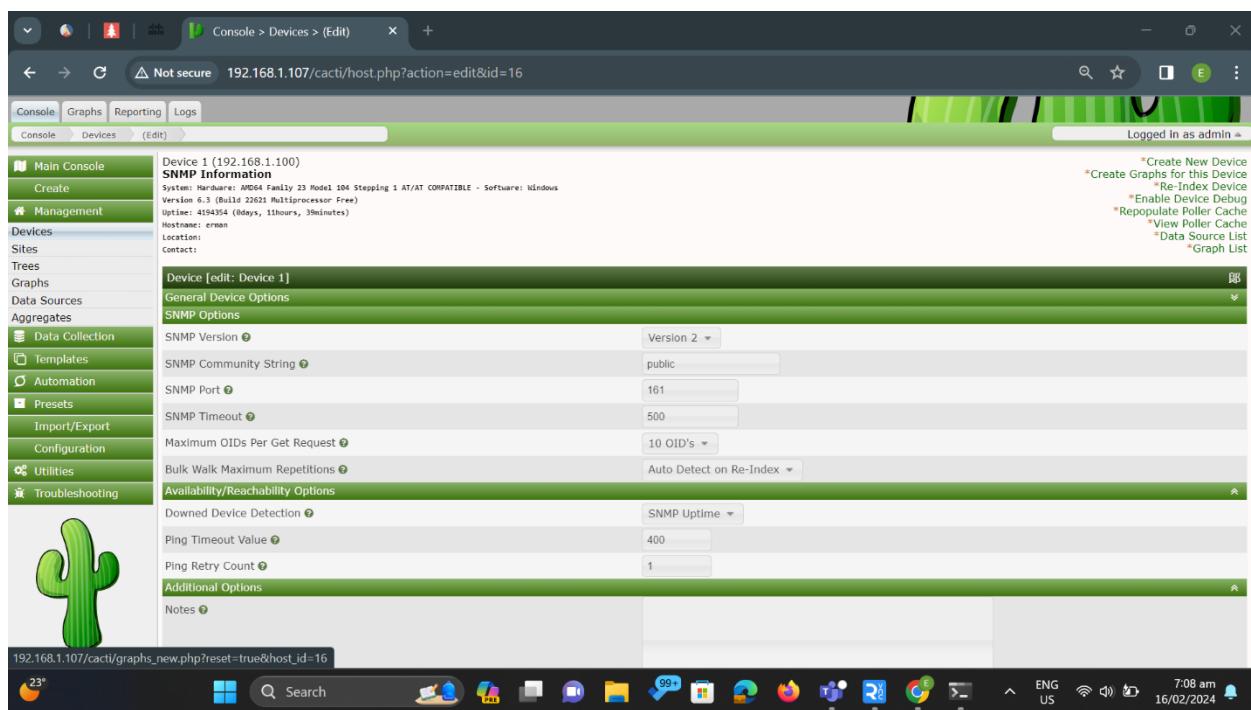


Figure 3-26: Successfully add a device in Cacti Devices

Step 18. Go to the “Data Query [SNMP – Interface Statistics]” and select all that has a “UP” status. After that click “create”

Index	Status	AdminStatus	Description	Name (IF-MIB)	Alias (IF-MIB)	Type	Speed	High Speed	Hardware Address	IP Address
1	Up	Up	Software Loopback Interface 1	loopback_0	Loopback Pseudo-Interface 1	24	1073741824	1073		127.0.0.1
2	Up	Up	WAN Miniport (IP)	ethernet_32771	Local Area Connection* 8	6	0	0		
3	notPresent	Down	Microsoft 6to4 Adapter	tunnel_32514	6to4 Adapter	131	0	0		
4	notPresent	Down	Microsoft Kernel Debug Netw...	ethernet_32770	Ethernet (Kernel Debugger)	6	0	0		
5	Down	Up	WAN Miniport (PPPOE)	ppp_32768	Local Area Connection* 7	23	0	0		
6	notPresent	Down	Microsoft IP-HTTPS Platform Ad...	tunnel_32513	Microsoft IP-HTTPS Platform In...	131	0	0		
7	Down	Up	WAN Miniport (L2TP)	tunnel_32770	Local Area Connection* 5	131	0	0		
	notPresent	Down	Bluetooth Device (Personal Are...	ethernet_32769	Bluetooth Network Connection	6	0	0	14 5A FC 69 21 B2	



Study Guide in (Elective 1 – Systems and Network Administration 1)

Module No. Lab 03

Figure 3-26: Cacti Data Query

ID	Status	Name	MAC Address	Driver	Connection Type	Speed	Duplex	MTU	MAC Address
11	Up	VMware Virtual Ethernet Adapter	ethernet_32775	VMware Network Adapter VMnet8	6	100000000	100	00 50 56 C0 00 01	192.168.64.1
12	Down	Microsoft Wi-Fi Direct Virtual Adapter	wireless_32769	Local Area Connection* 1	71	0	0	16 5A FC 69 21 A1	
13	Down	WAN Miniport (PPTP)	tunnel_32771	Local Area Connection* 6	131	0	0		
14	Up	VMware Virtual Ethernet Adapter	ethernet_32776	VMware Network Adapter VMnet8	6	100000000	100	00 50 56 C0 00 08	192.168.179.1
15	Down	Microsoft Wi-Fi Direct Virtual Adapter	wireless_32770	Local Area Connection* 2	71	0	0	16 5A FC 69 21 B1	
16	Up	VirtualBox Host-Only Ethernet Adapter	ethernet_32777	Ethernet 3	6	1000000000	1000	0A 00 27 00 00 10	192.168.56.1
17	Down	WAN Miniport (IKEV2)	tunnel_32769	Local Area Connection* 4	131	0	0		
18	notPresent	Down	Microsoft Teredo Tunneling Adapter	tunnel_32512	Teredo Tunneling Pseudo-Interface	131	0	0	
19	Up	MediaTek Wi-Fi 6 MT7921 Wireless Adapter	wireless_32768	Wi-Fi	71	144400000	144	14 5A FC 69 21 B1	192.168.1.100
20	Up	Realtek PCIe Gbe Family Controller	ethernet_32768	Ethernet	6	1000000000	1000	08 8F C3 34 D0 92	10.0.0.10
21	Down	WAN Miniport (SSTP)	tunnel_32768	Local Area Connection* 3	131	0	0		
22	notPresent	Down	Remote NDIS based Internet Sharing	ethernet_32774	Ethernet 2	6	0	0	FC DE 56 FF 01 06
23	Up	VirtualBox Host-Only Ethernet Adapter	ethernet_0	Ethernet 3-WFP Native MAC Layer	6	1000000000	1000	0A 00 27 00 00 10	
24	Up	VirtualBox Host-Only Ethernet Adapter	ethernet_1	Ethernet 3-Npcap Packet Drive	6	1000000000	1000	0A 00 27 00 00 10	
25	Up	VMware Virtual Ethernet Adapter	ethernet_3	VMware Network Adapter VMnet8	6	100000000	100	00 50 56 C0 00 08	
26	Up	VirtualBox Host-Only Ethernet Adapter	ethernet_2	Ethernet 3-QoS Packet Scheduler	6	1000000000	1000	0A 00 27 00 00 10	
27	Up	VirtualBox Host-Only Ethernet Adapter	ethernet_4	Ethernet 3-WFP 802.3 MAC Layer	6	1000000000	1000	0A 00 27 00 00 10	
28	Up	VMware Virtual Ethernet Adapter	ethernet_5	VMware Network Adapter VMnet8	6	100000000	100	00 50 56 C0 00 01	
29	Up	Realtek PCIe Gbe Family Controller	ethernet_6	Ethernet-WFP Native MAC Layer	6	1000000000	1000	08 8F C3 34 D0 92	
30	Up	Realtek PCIe Gbe Family Controller	ethernet_7	Ethernet-Npcap Packet Driver (...	6	1000000000	1000	08 8F C3 34 D0 92	

Figure 3-27: Creating Cacti Graph into your Device

Step 19. Go back to your devices. Then select your device, then select the “Place on a Tree (Default Tree) in the “Choose an Action” menu then click “Go.”

Device Description	Hostname	ID	Graphs	Data Sources	Status	In State	Uptime	Poll Time	Current (ms)	Average (ms)	Availability
Ace Device	192.168.1.100	12	7	5	Down	10m	N/A	1.01	7.31	9.09	87.5 %
Ace Device Laptop	192.168.1.100	13	29	27	Down	10m	N/A	1.01	7.31	9.09	87.5 %
Device	192.168.1.107	6	7	5	Down	10h:50m	N/A	1.05	0	0	0 %
Device 1	192.168.1.100	16	20	20	Unknown	N/A	N/A	0	0	0	100 %
Device1	192.168.1.107	5	19	27	Down	10h:50m	N/A	1.1	0	0	0 %
Device2	192.168.1.107	7	7	5	Down	10h:50m	N/A	1.01	0	0	0 %
Device2	192.168.1.107	8	7	5	Down	10h:50m	N/A	1.02	0	0	0 %
Device2	192.168.1.107	9	7	5	Down	10h:50m	N/A	1.02	0	0	0 %
Device2	192.168.1.100	10	29	27	Down	10m	N/A	1.01	7.31	9.09	87.5 %
Floyd	192.168.1.103	15	16	16	Down	10m	N/A	1.01	44.66	50.87	60 %
Floyd Device	192.168.1.103	14	4	4	Down	10m	N/A	1.01	44.66		
Laptop	192.168.1.107	3	3	3	Down	10h:50m	N/A	1.01	0		
Laptop	192.168.1.107	4	5	5	Down	10h:50m	N/A	1.01	0		
Laptop-1	192.168.1.100	11	7	5	Down	10m	N/A	1.01	7.31		
PC 1	192.168.1.1	1	5	5	Down	6h:0m	N/A	1.01	0		
Router	11.22.2.1	2	3	3	Down	5h:15m	N/A	1.01	0		

Figure 3-28: Adding the device into tree



Then click “Continue” to place the following Device(s) under the branch selected below.

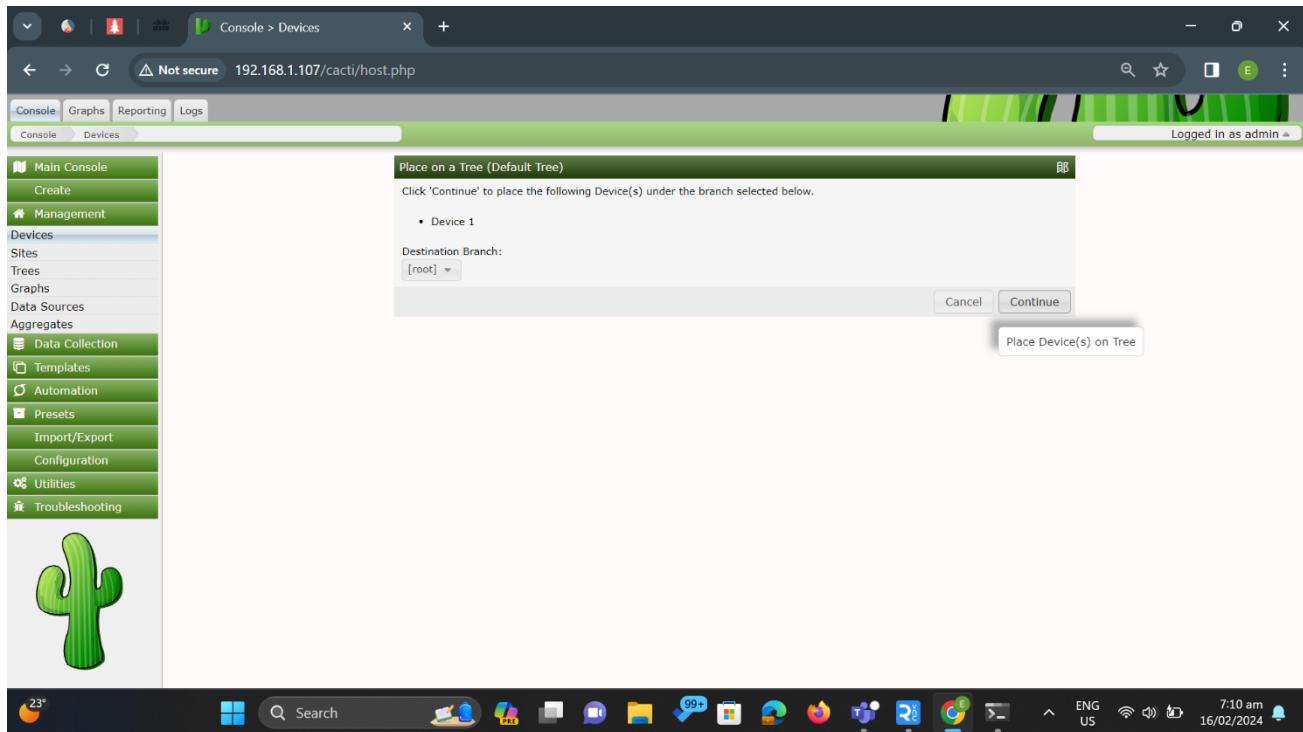


Figure 3-29: Placing your device into tree

Step 20. Creating Graphs. Now that we have successfully added the device to our tree, it's time to create a graph to monitor its performance. To begin, click on the "Graphs" tab.

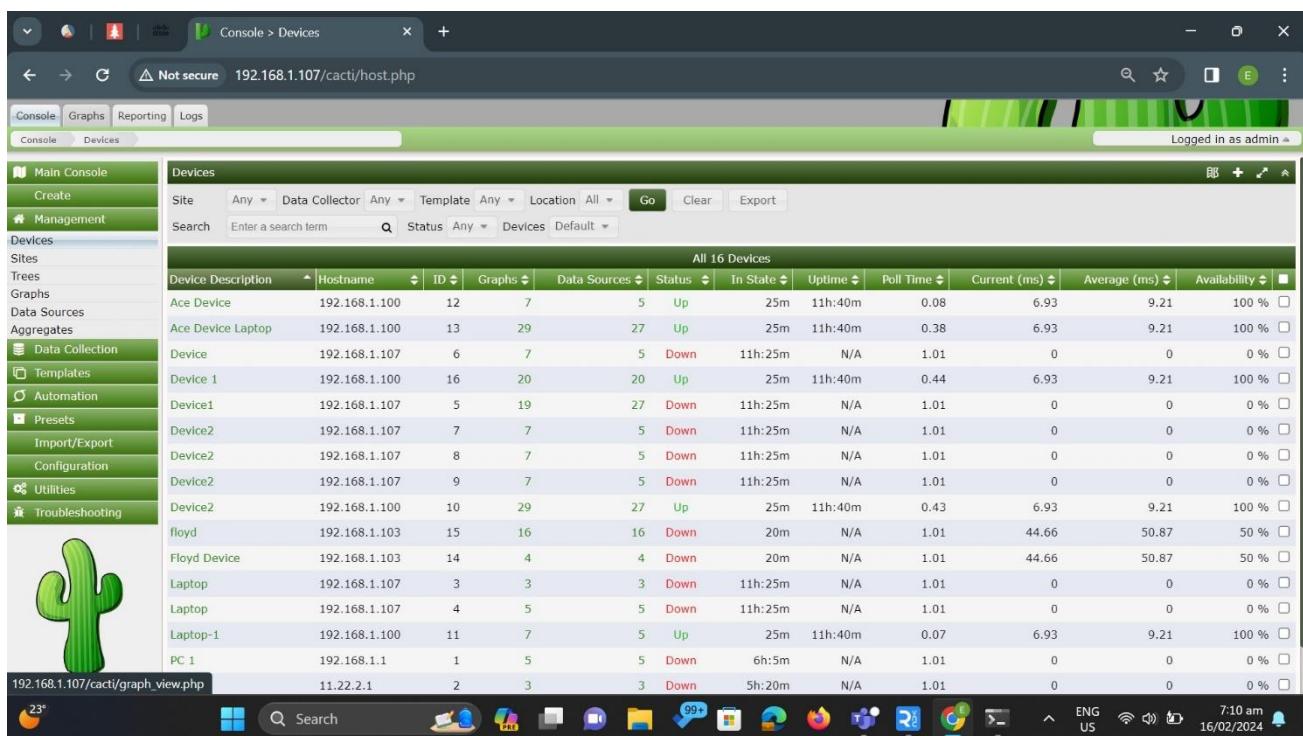


Figure 3-30: Cacti Devices Tab



Then select the device.

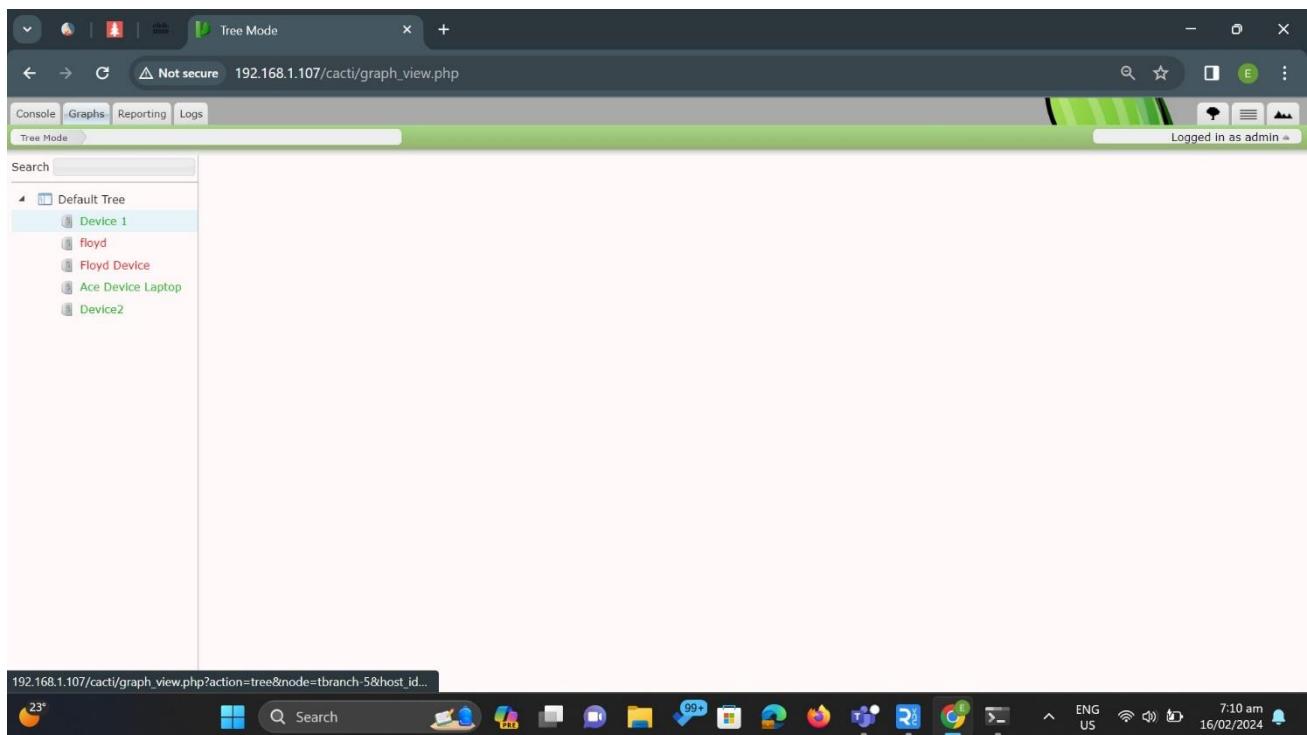


Figure 3-31: Cacti Graphs Tab

You can now monitor the network of the device in a graph form.

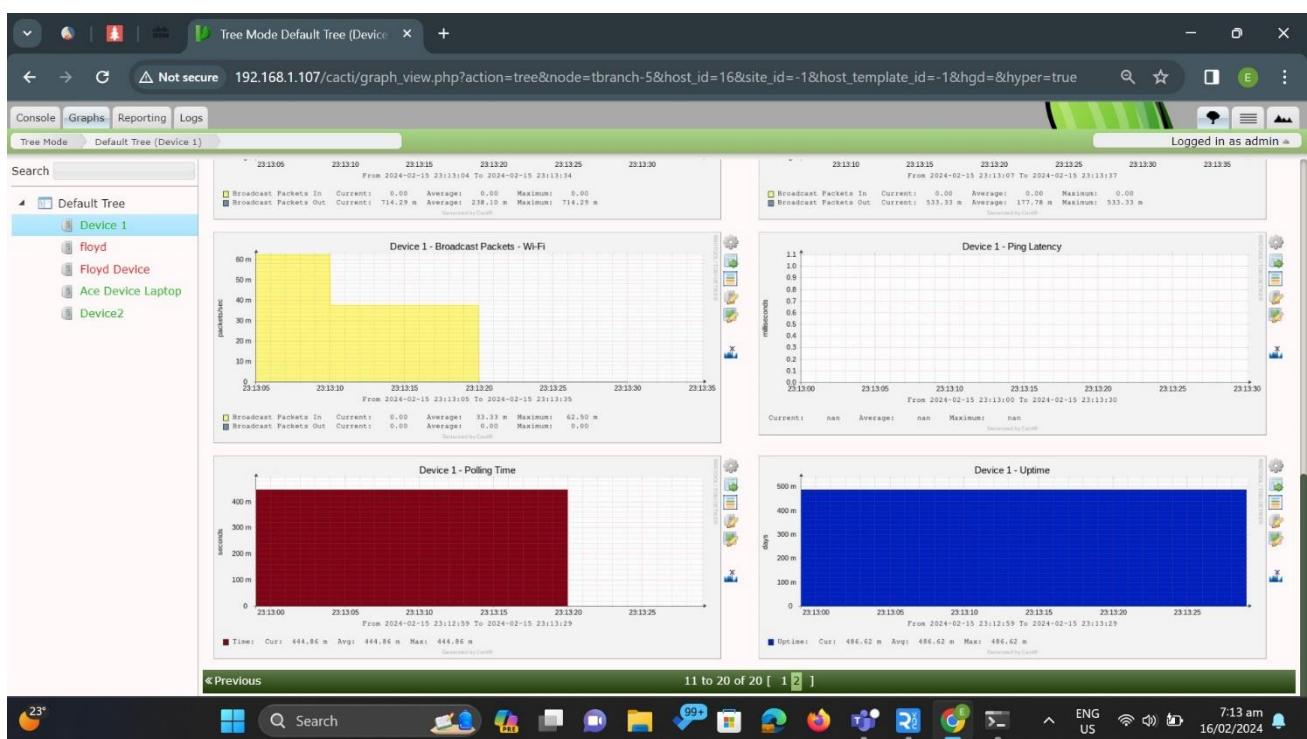


Figure 3-32: Network Monitoring of Device1





SUMMARY / CONCLUSION

In conclusion, leveraging Raspberry Pi for network monitoring offers a cost-effective and versatile solution. By utilizing the compact size and low power consumption of the Raspberry Pi, organizations can deploy monitoring nodes throughout their network infrastructure with ease. This enables real-time monitoring of network performance, traffic analysis, and security surveillance without the need for expensive dedicated hardware.

Furthermore, the flexibility of Raspberry Pi allows for customization and scalability to meet specific monitoring requirements. Whether it's monitoring small-scale local networks or larger enterprise environments, Raspberry Pi-based solutions can be tailored to suit the needs of various organizations. With the abundance of open-source monitoring software available for the Raspberry Pi platform, users have the freedom to choose and configure tools according to their preferences, ensuring efficient network management and optimization.

REFERENCES

NetVN82. (2020, September). How to network monitor using Raspberry PI | Cacti | NETVN. Retrieved November 21, 2023, from https://www.youtube.com/watch?v=zGS38_VTppg

For your additional References that has been used please use the citation tools on the website <https://www.scribbr.com/> using APA 7th Edition English, and paste it below.

