Troubleshoot SNMP Polling and Incorrect Interface Details on SNA

Contents

Introduction

Prerequisites

Requirements

Components Used

Configurations

Background information

Troubleshooting

- Incorrect Interface Names
- Missing Exporters or Interfaces
- Connectivity Problems
  - Validate Manager (SMC) ability to poll exporters
  - Generate a packet capture on the SMC using the IP address of an exporter.
  - Validate SNMP Polling Settings
  - Live troubleshooting of SNMP Polling
- Testing SNMP Polling From Another Device

Related information

Introduction

This document describes how to troubleshoot missing exporter interface information in Secure Network Analytics

Prerequisites

- Cisco recommends that you have basic Simple Network Management Protocol (SNMP) polling knowledge
- Cisco recommends that you have basic Secure Network Analytics (SNA/StealthWatch) knowledge

Requirements

- SNA Manager in version 7.4.1 or newer
- SNA Flow Collector in version 7.4.1 or newer
- Exporter actively sending NetFlow to SNA

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command

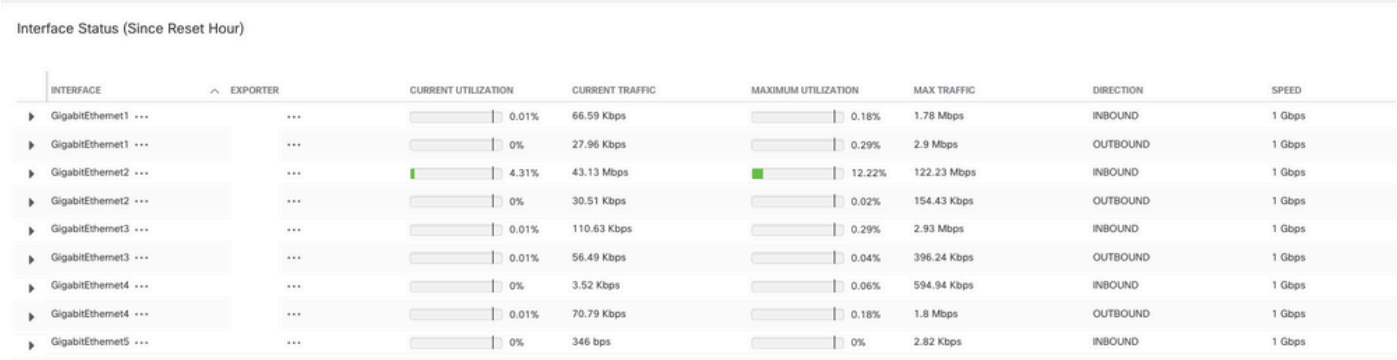
- SNA Manager in version 7.4.1 or newer
- SNA Flow Collector in version 7.4.1 or newer
- SNMPwalk software
- Wireshark software

Configurations

- Device Configuration: The exporters need to be configured to allow SNMP access. This involves configuring SNMP settings on each device, including setting up SNMP community strings, access control lists (ACLs), and defining the SNMP version to be used
- SNMP Polling Configuration on SNA: Upon successful configuration of the exporters, SNMP polling is enabled by default on the SMC using pre-set parameters. It is crucial to supply requisite details pertaining to the exporters, such as SNMP community strings and SNMP versions, to ensure the polling mechanism operates optimally

Background information

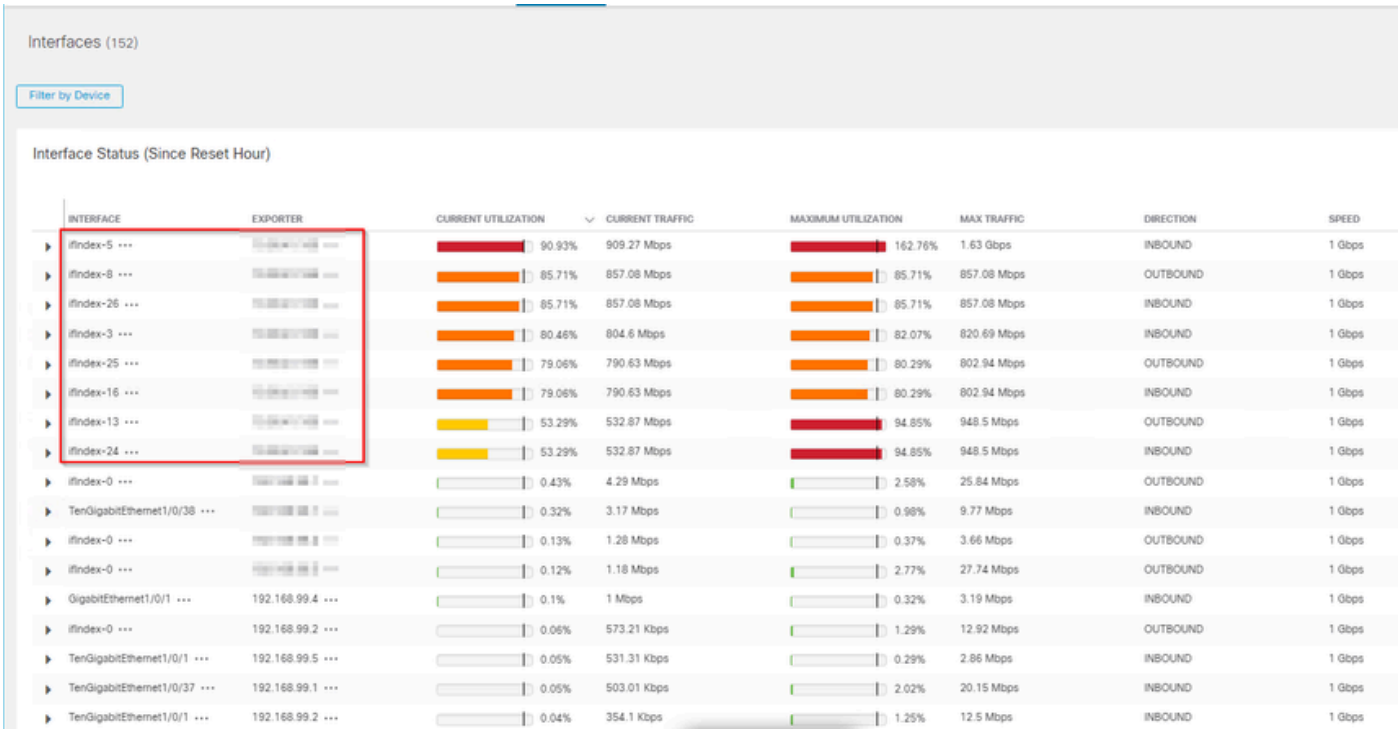
SNA possesses the capability to provide comprehensive interface status reporting, along with the ability to display interface names for exporters that are actively transmitting NetFlow data to a Flow Collector. This interface detail can be seen by navigating to the Investigate -> Interfaces menu from the Manager Web UI.



Troubleshooting

Incorrect Interface Names

In the event that the generated report displays an "ifindex-#" which does not correspond to your exporter interfaces, it suggests a potential configuration issue with SNMP polling either on the SMC or on the exporter ifself. In this example, I have highlighted an apparent problem with SNMP polling of a given exporter.



Missing Exporters or Interfaces

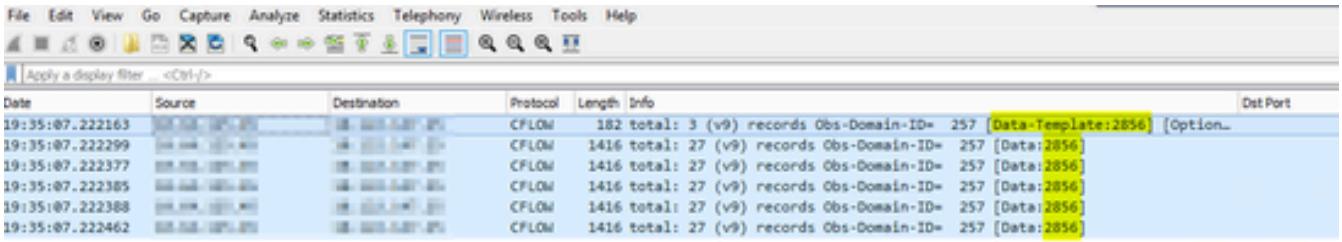
Template verification holds significant importance in the context of NetFlow data processing. Specifically, it ensures that the NetFlow template received from the exporter contains all the requisite fields required for successful decoding and processing by the Flow Collector. Failure to encounter a valid template leads to the exclusion of the associated set of flows from decoding, therefore resulting in their absence from the list of interfaces.

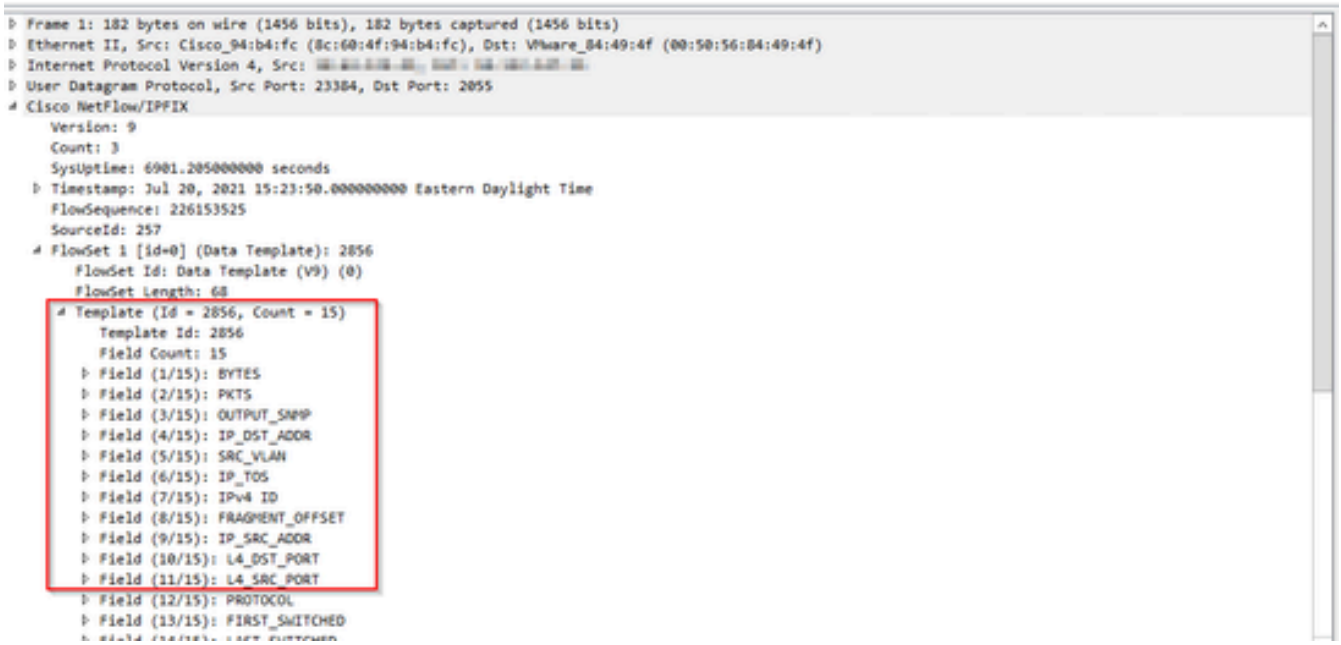
If you do not see the expected exporter/interfaces in the interfaces list, you should verify the incoming netflow data dn template. In order to verify the NetFlow template a packet capture can be created on the Flow Collector side, specifying the IP from the exporter we are getting NetFlow from by changing "x.x.x.x":

- Log in to the Flow Collector via SSH or console with **root** credentials.
- Run a packet capture from the exporter IP and netflow port in question:

```
tcpdump -s0 -v -nnn -i eth0 host x.x.x.x and port 2055 -w /lancope/var/admin/tmp/<name>.pcap
```

- Copy the packet capture from the appliance, to a workstation with the Wireshark application installed, use your preferred method (For example: SCP, SFTP).
- Open the packet capture with Wireshark and verify the template and data that the exporter is sending to the flow collector





Verify that the NetFlow template is using the 9 required fields, the exact name of these template fields can vary depending on the exporter type so be sure to consult the documentation for the specific exporter type you are configuring:

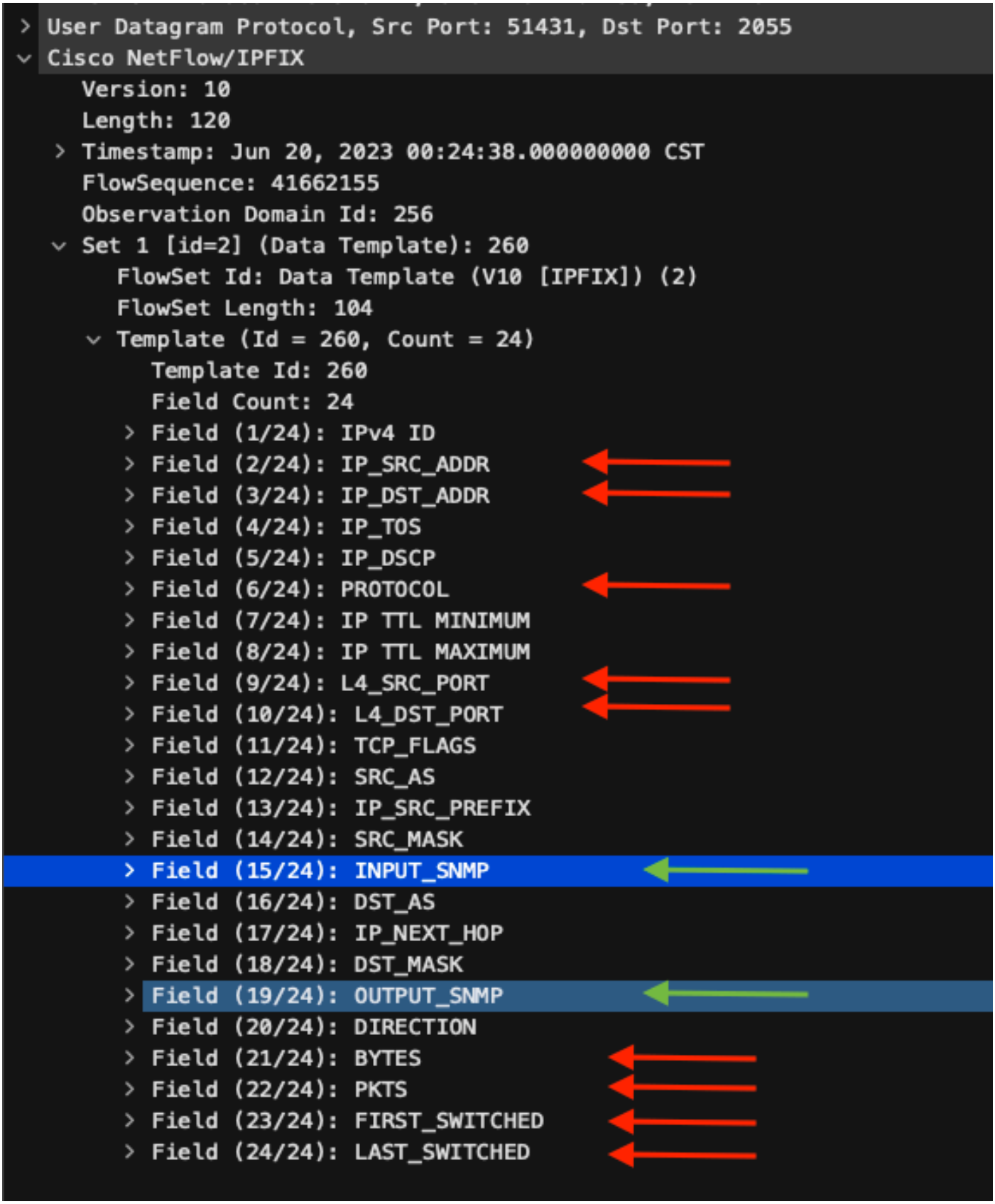
- Source IP Address
- Destination IP Address
- Source port
- Destination port
- Layer 4 Protocol
- Bytes count
- Packet count
- Flow Start Time
- Flow End Time

To display interfaces correctly please also add:

  - interface output
  - interface input

Here is an example template packet capture from an given exporter device

- Red arrows: required NetFlow fields
- Green arrows: SNMP fields



Note: Port listed in the example command can vary depending on your exporter configuration, default is 2055

Note: Keep the packet capture running from 5-10 minutes, depending on the exporter the template can be send every N minutes and you need to catch that template so the NetFlow gets decoded correctly, if template does not show, repeat the packet capture for a longer period of time

Connectivity Problems

Check Connectivity: Ensure that there is connectivity between SNA Manager appliance and the exporters. Verify that the exporters are reachable from the Stealthwatch management console by pinging their IP addresses. If there are any network connectivity issues, troubleshoot and resolve them accordingly.

Validate Manager (SMC) ability to poll exporters

- Connect to SNA manager vis SSH and log in with **root** credentials
- Analyze the **/lancope/var/smc/log/smc-configuration.log** file and search for the logs of type **ExporterSnmpSession:**

```
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
INFO [ExporterSnmpSession] SNMP polling for 10.1.0.253 took 0s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
WARN [ExporterSnmpSession] SNMP polling for 10.10.0.254 failed: java.lang.Exception: timeout
INFO [ExporterSnmpSession] SNMP polling for 10.10.0.254 took 20s
```

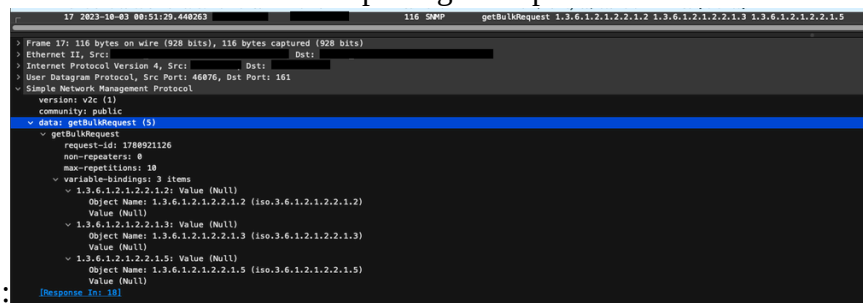
- In this polling example, there were no errors detected for exporter 10.1.0.253. However,exporter 10.1.0.254 experienced a timeout. The default timeout interval is 5000 ms with a retry count of 3. So from the time an exporter is polled to the moment it's timed out should be 20 seconds in an environment where you haven't changed the settings.

Generate a packet capture on the SMC using the IP address of an exporter.

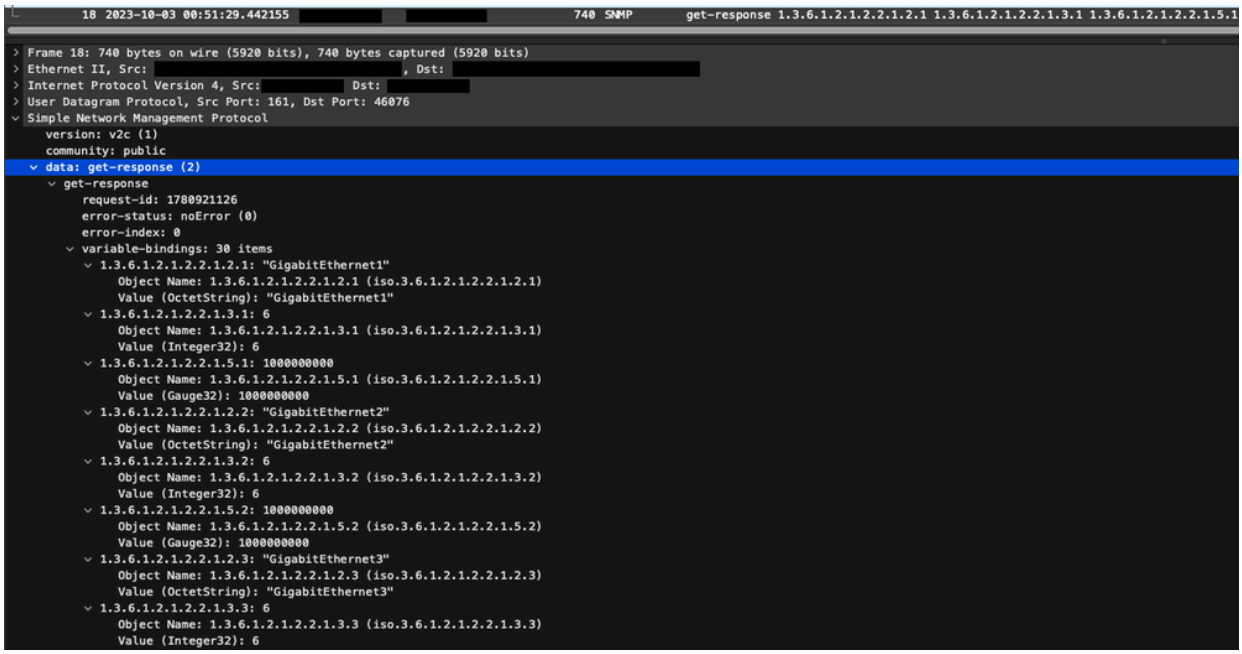
- Log in to the Manager node via SSH or console with **root** credentials
- Run:

```
tcpdump -s0 -v -nnn -i [Interface] host [Exporter_IP_address] -w /lancope/var/admin/tmp/[file_name
```

- Export the packet capture from the appliance with your preferred method (Example: SCP, SFTP)
- Open the packet capture with Wireshark to view the successful polling attempts
  - Request made from the SMC:



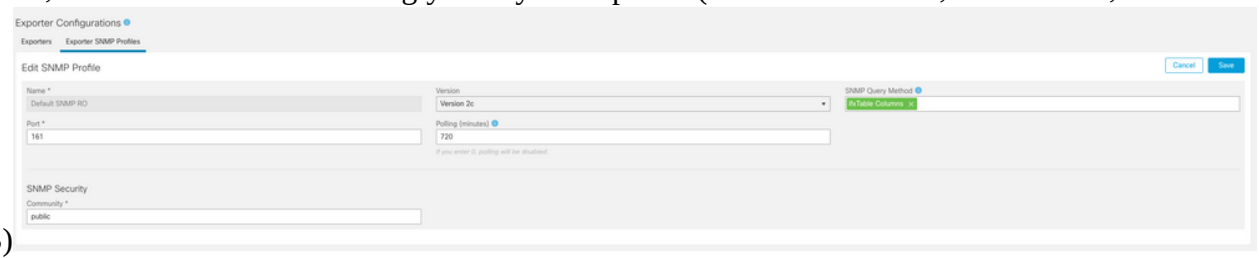
  - SNMP Response from the exporter with interface information:



Validate SNMP Polling Settings

Make sure the polling intervals are appropriate and that the desired metrics are included in the SNMP queries

- On the web UI navigate to: **Configure -> Exporters -> Exporter SNMP Profiles**:
- Validate that the correct SNMP port (typically UDP port 161) and the correct SNMP Query Method selected, these must match accordingly with your exporter (ifxTable Columns, CatOS MIB, PanOS MIB)



Note: If you have 10 Gbps interfaces, we recommend that you choose the ifxTable columns option for the SNMP query method.

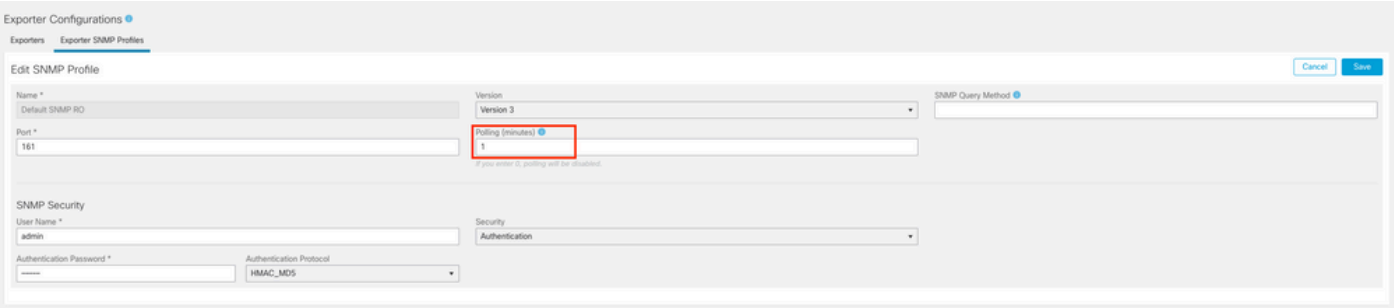
Note: For optimal system performance, set SNMP polling to a 12-hour interval. Polling more frequently does not make your utilization metrics more up to date and can cause your system to run slower.

- Validate that the SNMP versions configured on both SNA and the exporters are compatible. SNA supports SNMPv1, SNMPv2c, and SNMPv3. Check if the exporters are configured to use the same SNMP version as configured in SNA.
    - In case of using SNMPv3, verify the SNMP configuration is correct (Username, Authentication Password, Authentication Protocol, Privacy Password, Privacy Protocol)

Live troubleshooting of SNMP Polling

On the web UI navigate to **Configure -> Exporters -> Exporter SNMP Profiles**

- Set Polling (minutes) to 1 (minute) temporarily.



- Log in to the SMC via SSH or console with **root** credentials.
- Navigate to this folder:

```
cd /lancope/var/smc/log
```

- Run:

```
tail -f smc-configuration.log
```

- For SNMPv3, a common error message would be:

```
failed: java.lang.IllegalArgumentException: USM passphrases must be at least 8 bytes long (RFC3414
```

- Verify the authentication password in the SNMP Profile is set to 8 characters or more.
- Once live troubleshooting is finished, return Polling (minutes) configuration for the exporter or its configuration template to its previous value.

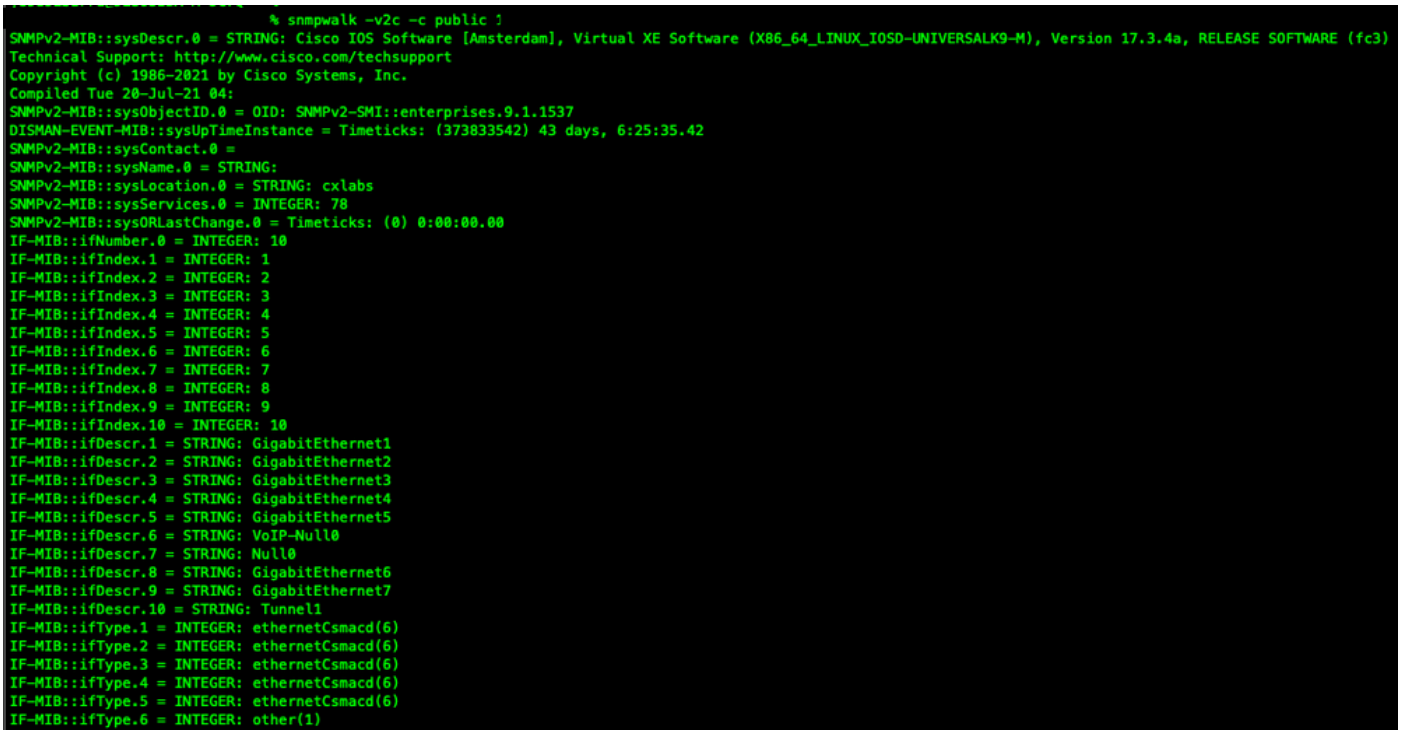
Testing SNMP Polling From Another Device

Test SNMP Polling: Manually initiate an SNMP poll from a local machine to a specific network device and check if it receives a response. This can be done by using SNMP polling tools or utilities like SNMPwalk. Verify that the network device responds with the requested SNMP data. If there is no response, it indicates a problem with the SNMP configuration or connectivity.

- On your local machine with SNMPwalk software, replace "x.x.x.x" for the exporter IP and run on CLI:

```
snmpwalk -v2c -c public x.x.x.x
```

    - -v2c: specifies SNMP version to use
    - -c: sets the community string



- Verify the exporter responds with SNMP data

Related information

- For additional assistance, please contact Technical Assistance Center (TAC). A valid support contract is required: Cisco Worldwide Support Contacts.
- You can also visit the Cisco Security Analytics Communityhere.
- Technical Support & Documentation - Cisco Systems