Merlin – Integration with Radiflow iSID

Advanced Intrusion Detection System

AN-008-WIE

Hardware Models	Merlin Series
Revision	1.03
Approval status	Approved
Date	06 January 2026
Brief description	Merlin– Radiflow iSID Integration Guide Using Smart Connector Probes

1 Overview

Radiflow iSID is an industrial cybersecurity monitoring platform designed for OT and ICS networks. It passively analyses network traffic, builds an asset inventory, detects anomalies and policy violations, and identifies potential security risks without interfering with operational systems. iSID provides continuous visibility into industrial processes to help operators maintain a secure and compliant OT/IT environment. When applied to large and distributed systems, iSID can integrate with remote collectors, allowing data from remote sites to be forwarded for analysis over smart connections to collector interfaces.

The Merlin device can be used as a remote collector and, as an industrial gateway, is an ideal solution for performing local traffic filtering and monitoring, data collection (tapping) and data distribution.

This application note demonstrates how to integrate a Merlin device (Data Collector) with Radiflow's iSID application (IDS). The example scenario illustrates a basic port mirroring setup, commonly known as encapsulated remote SPAN (ERSPAN), where traffic is duplicated and forwarded to an external IDS for analysis. This document outlines all the steps required to integrate both systems.

1.1 Firmware information

Firmware version: **25.05.31.000** or newer.

1.2 Assumptions

This application note document can be applied to all routers in the Westermo Ireland - Merlin Series and Virtual Access - GW Series, for the purpose of this document all devices will be referred as Merlin Device.

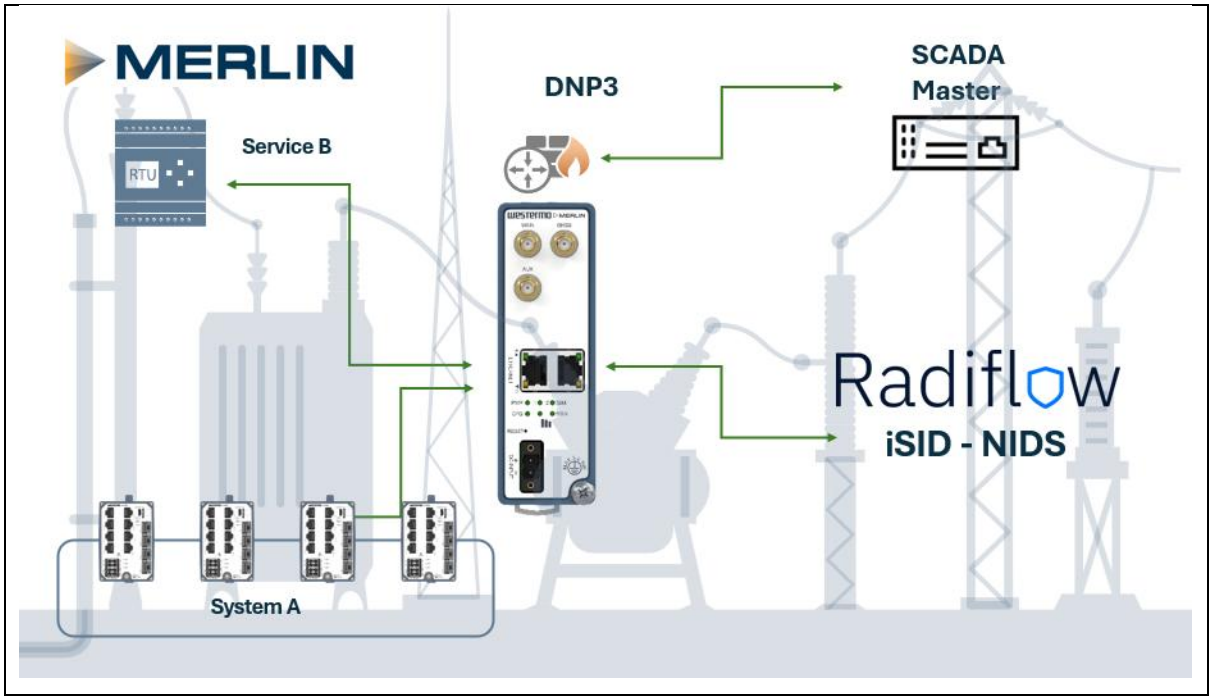
It is assumed that device has been configured and provide communication for intended service and the communication between devices is operational, this document will focus on explaining how to configure traffic mirroring port to duplicate the traffic from one physical port and forward this to IDS.

Application note does not focus on configuring and finetuning Radiflow's iSID application, for all queries of this nature please contact Radiflow directly at support@radiflow.com

1.3 Corrections

Requests for new application notes related to Merlin products, corrections or amendments to this application note are welcome and should be addressed to support.ie@westermo.com

2 Operational environment



2.1 Overview

The Merlin series of versatile cellular routers provides high-speed data connectivity for demanding industrial and smart grid applications. Device offers a complete solution for service delivery, remote access, and security monitoring, and when coupled with the Radiflow iSID application, it can offer an advanced solution for Network Intrusion Detection System (NIDS) of the remote substation.

The illustration above represents a typical remote site where a Merlin device delivers radio communication services for specialised industrial applications and networks. While the Merlin device includes robust, industry-grade security features, it is not designed to perform full traffic flow analysis, advanced malware detection, or deep inspection across a wide variety of protocols. These capabilities fall within the domain of specialised intrusion detection systems such as Radiflow's iSID which would typically be deployed in centralised locations. In such scenarios, Merlin device act as a data collector and forwarder.

3 Configuring Smart Collector

3.1 Introduction

The Smart Collector feature configuration is straightforward, but it does require several steps. It is assumed that the Merlin device is already configured and operational.

Configuration steps summary:

- On Radiflow – Add a new Smart Collector interface
- On Radiflow – Add a Smart Collector probe
- On Merlin Device – Create a new probe interface (e.g., **SCProbe**)
- On Merlin Device – Add parent interface to the probe
- On Merlin Device – Configure the mirroring service

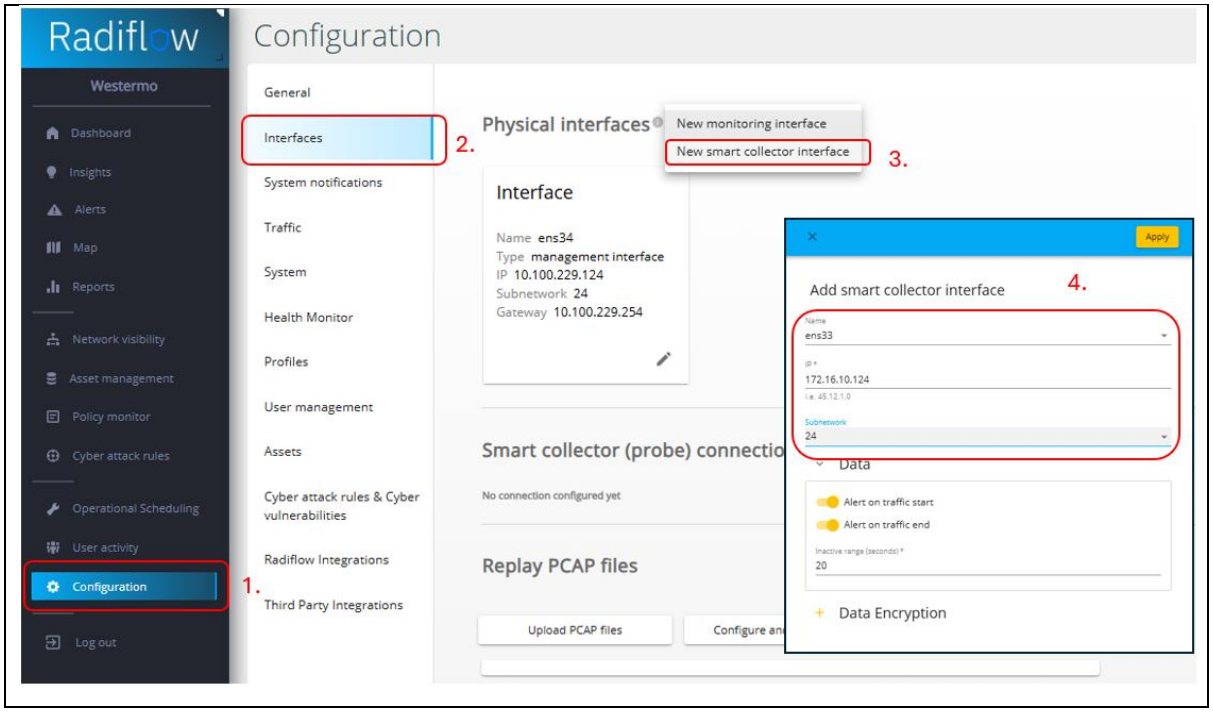
Networking overview:

The Smart Collector interface is configured with a dedicated monitoring subnet. On the Merlin device, this subnet may be assigned to either a physical interface (when the IDS is connected locally) or a virtual interface (when the IDS is deployed remotely), further referred as forwarding interface. For the purpose of this document, configuration on a physical interface is described.

Radiflow's monitoring architecture uses a one-way passive capture interface to ingest mirrored OT/IT traffic without transmitting or interacting with the network. Remote traffic, from Merlin, is delivered through an Ethernet GRE over IPv4 (**GRETAP)** tunnel, where the router mirrors the required traffic and sends GRE-encapsulated frames to the Smart Collector Interface IP.

The iSID system decapsulates the GRE payload and feeds the inner Ethernet frames into the monitoring pipeline as if they arrived directly on the passive interface. This design provides secure, unidirectional traffic ingestion with no risk to operational systems. It is recommended to follow the same principle on the Merlin device by restricting inbound traffic on the probe interface using firewall rules.

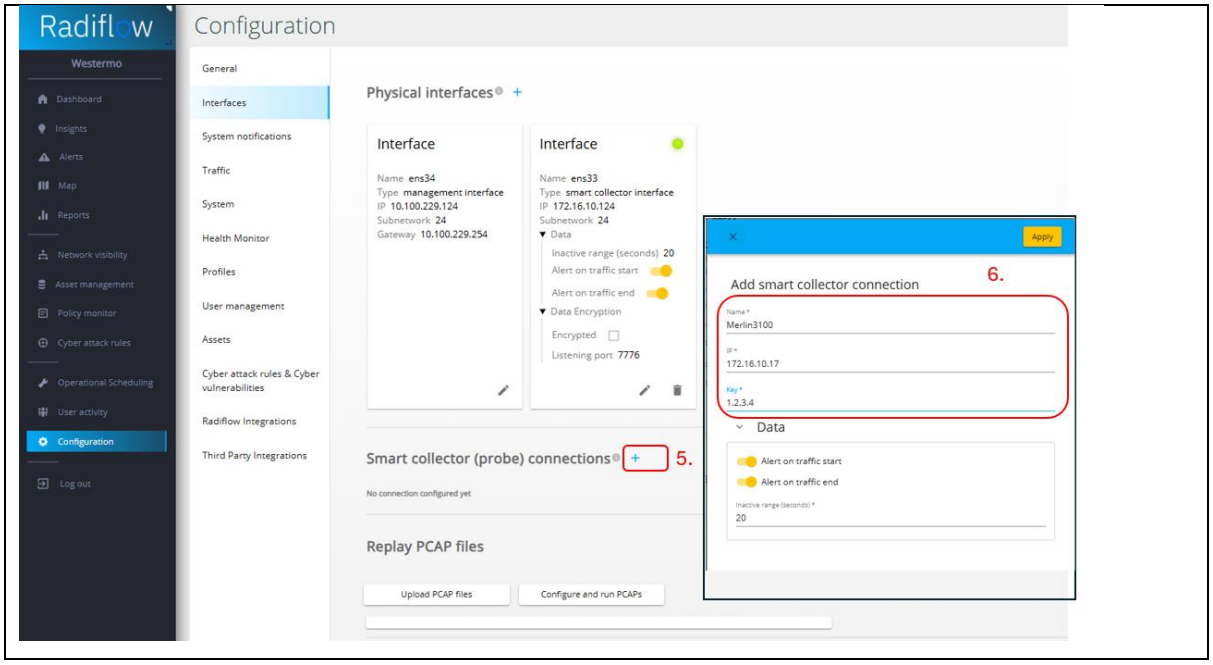
3.2 Configuring Smart Collector Interface on iSID



1. Access **Configuration** from side menu
2. Go to **Interfaces**
3. Click + next to Physical interfaces and select **New smart collector interface**
4. Select your interfaces and configure **Smart Collector Network**

Once configured, new network interface tile will appear. Green light indicates correct operations, whereas a warning triangle denotes that no traffic is being received.

3.3 Configuring Smart Probe Connection on iSID

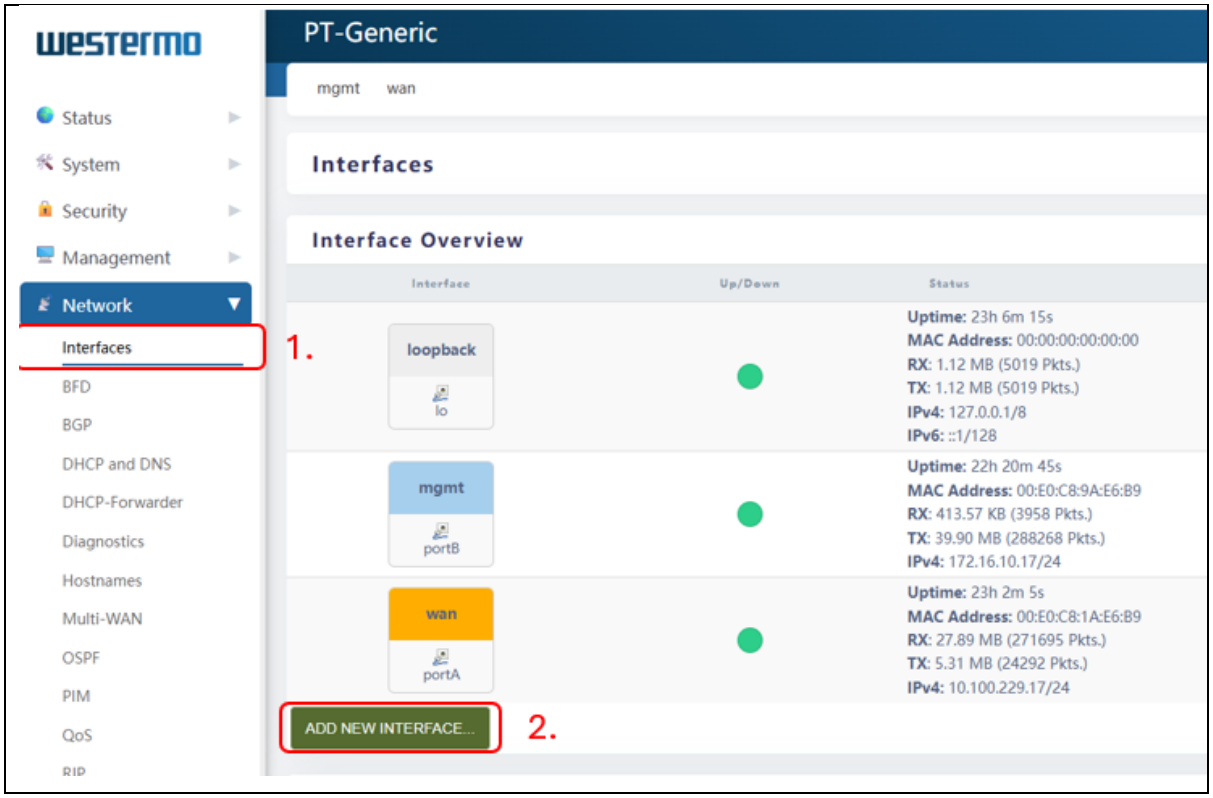


5. Click + to create new **Smart collector probe connection**
6. In popup window:
    a. Add custom name
    b. Add IP address of forwarding interface from Merlin Device
    c. Add 32bit unique key in form of IP address.

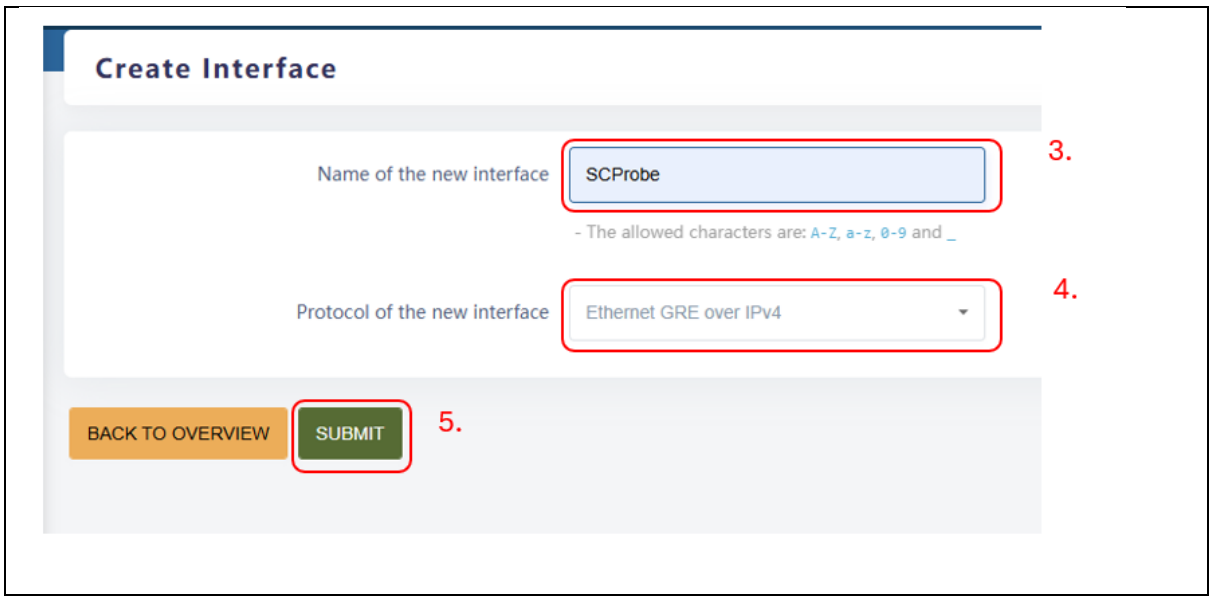
Note: Each device requires its own dedicated interface for connecting the Smart Collector probe.

After configuration is complete, a new Connection interface tile will be displayed. A green indicator signifies proper operation, whereas a warning triangle denotes that no traffic is being received.

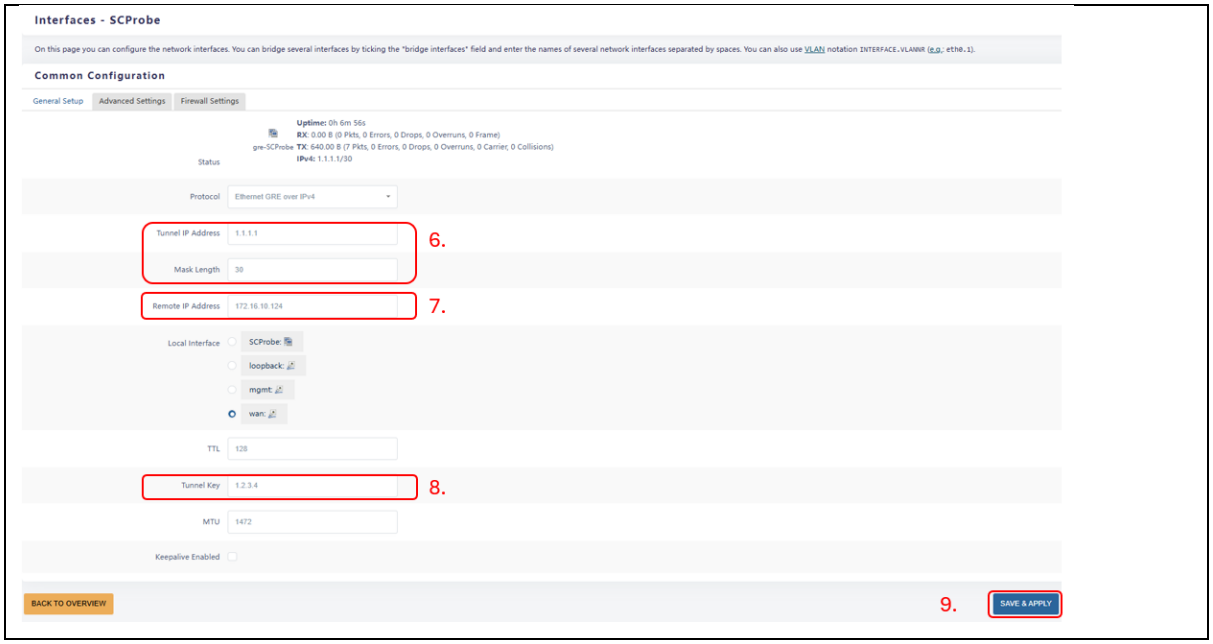
3.4 Configuring SCProbe Interface on Merlin



1. Go to **Network** Tab and click **Interfaces**
2. Click **Add New Interface**



3. Create new name for the interface e.g. "SCProbe"
4. Select **Ethernet GRE over IPv4** (GRETAP) as protocol interface
5. Click **Submit**

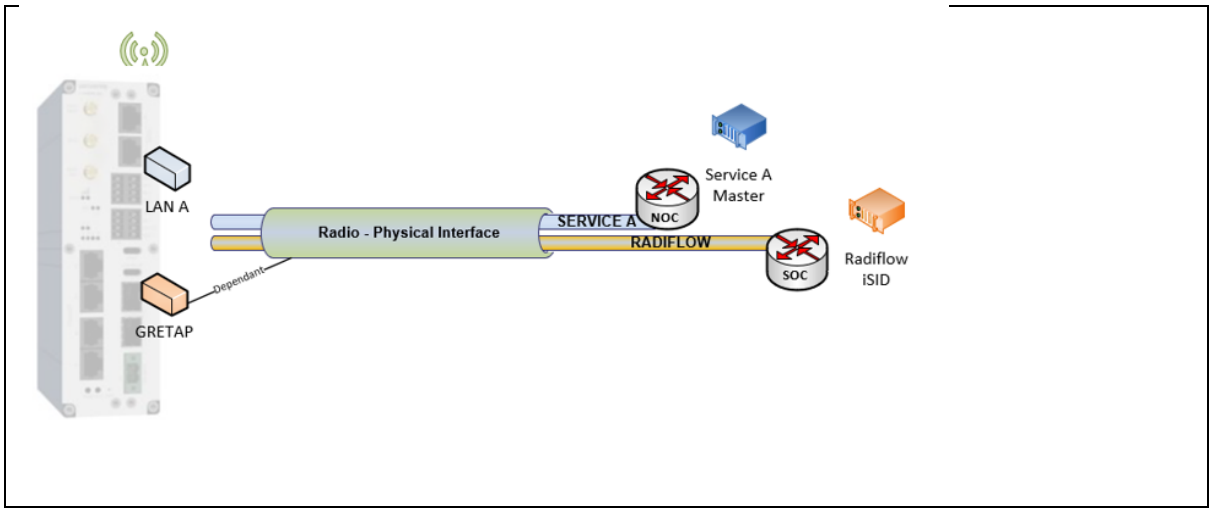


6. Configure with a dummy IP and Mask (e.g. 1.1.1.1/30)
7. Configure with IP address of **Smart Collector Interface on Radiflow**
8. Configure the 32bit key as in Radiflow configurations
9. Click **Save & Apply**

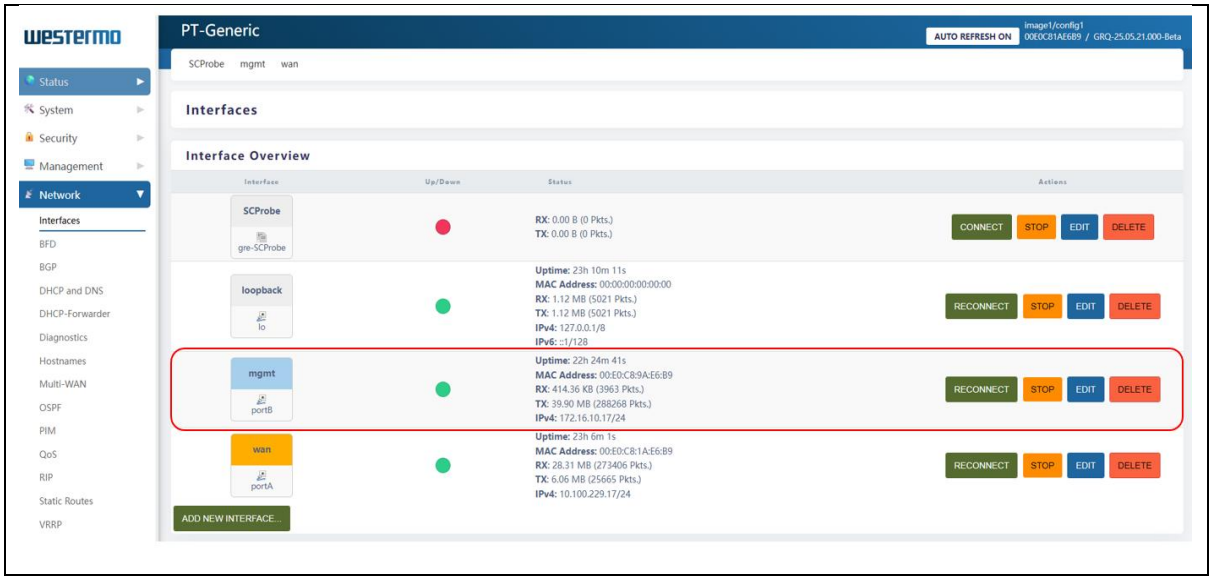
3.5 Configuring SCProbe Parent Interface on Merlin

Important notes:

- The main parent interface must be a physical interface.
- The parent interface's traffic cannot be mirrored back to the SCProbe (GRETAP) to avoid loops.
- When using a radio interface for traffic delivery, as illustrated below, it is essential to consider both its throughput and bandwidth.

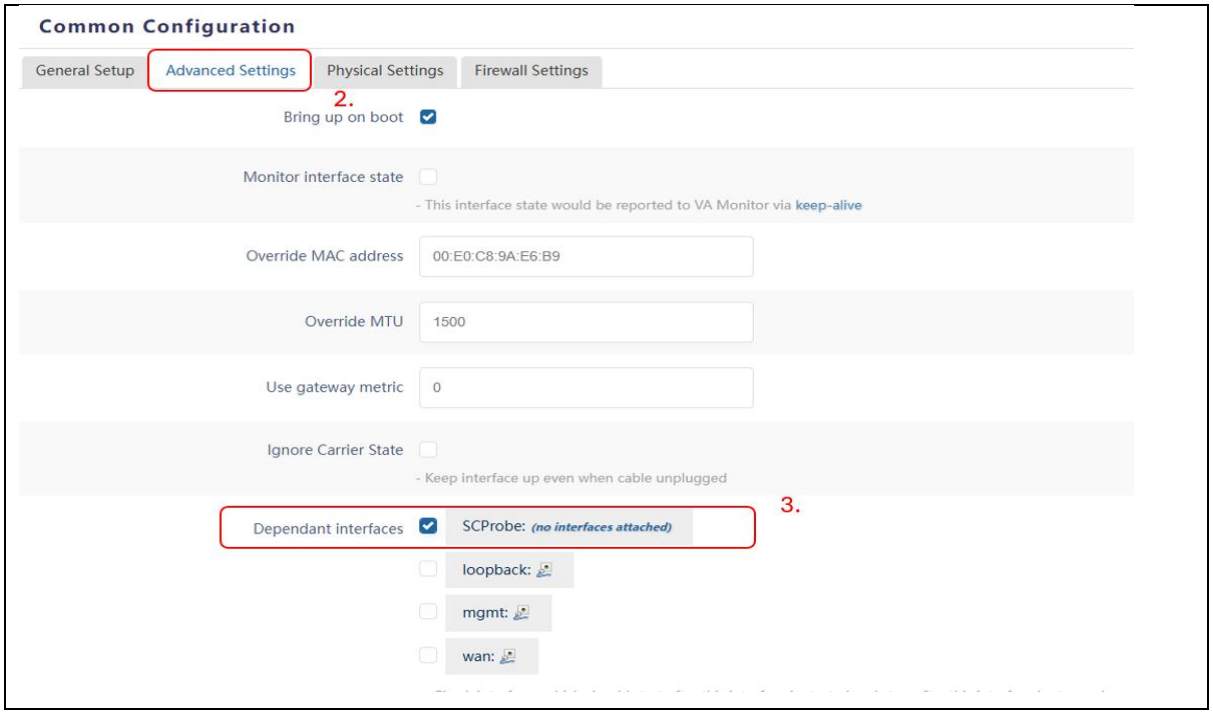


To configure SCProbe Parent interface, go to **Network** > **Interface** settings on Merlin Device.



1. Click **EDIT** in the action section of the selected parent interface.

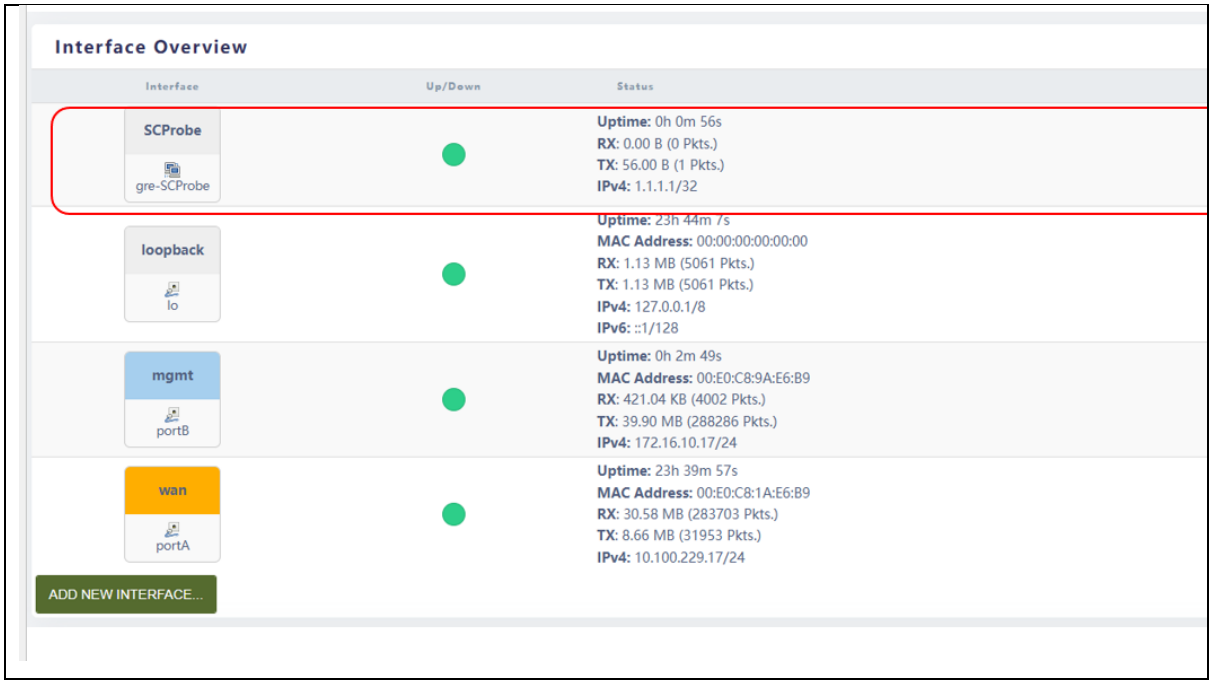
Note: the Smart Collector Probe Connection on Radiflow was configured with IP address of this physical interface.



2. Go to **Advanced Settings**
3. Add **SCProbe** as **Dependant Interface**

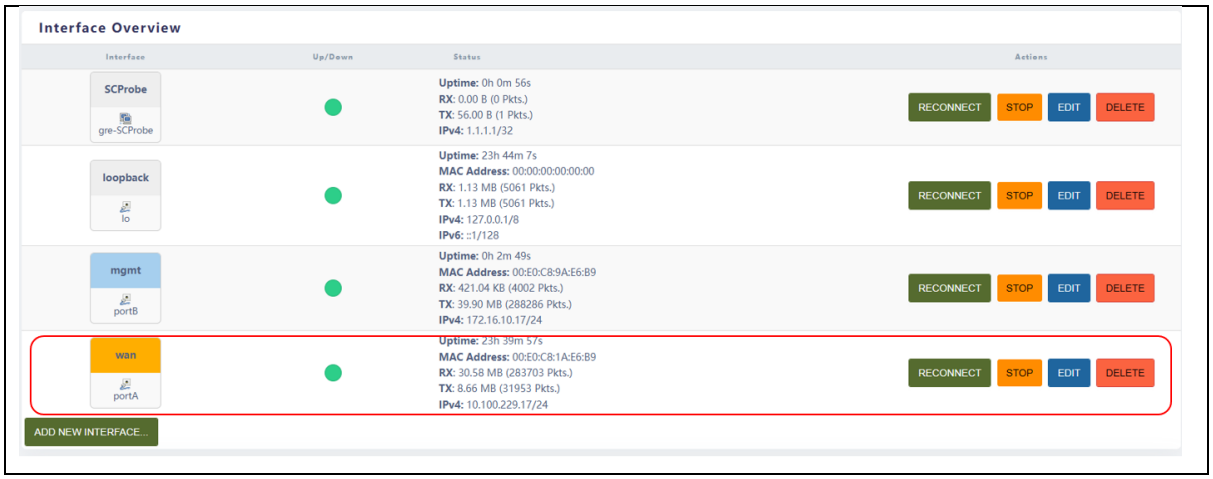
Click **Save& Apply** at the bottom of the page

After configuration, the SCProbe interface appears in the list with a green light to show it's operational.

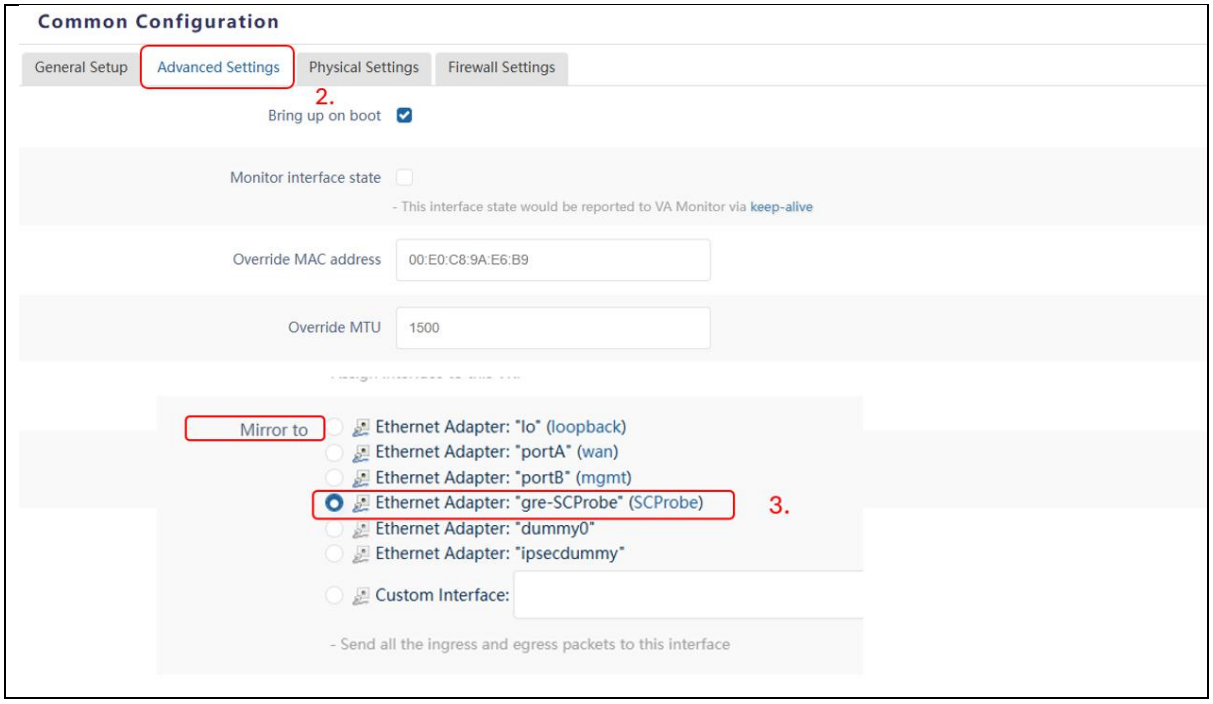


3.6 Configuring port mirroring feature on Merlin

In this simple example scenario, all traffic from the interface used for Service A will be mirrored to the SCProbe interface.



1. Click EDIT in the action section of the Service A interface.

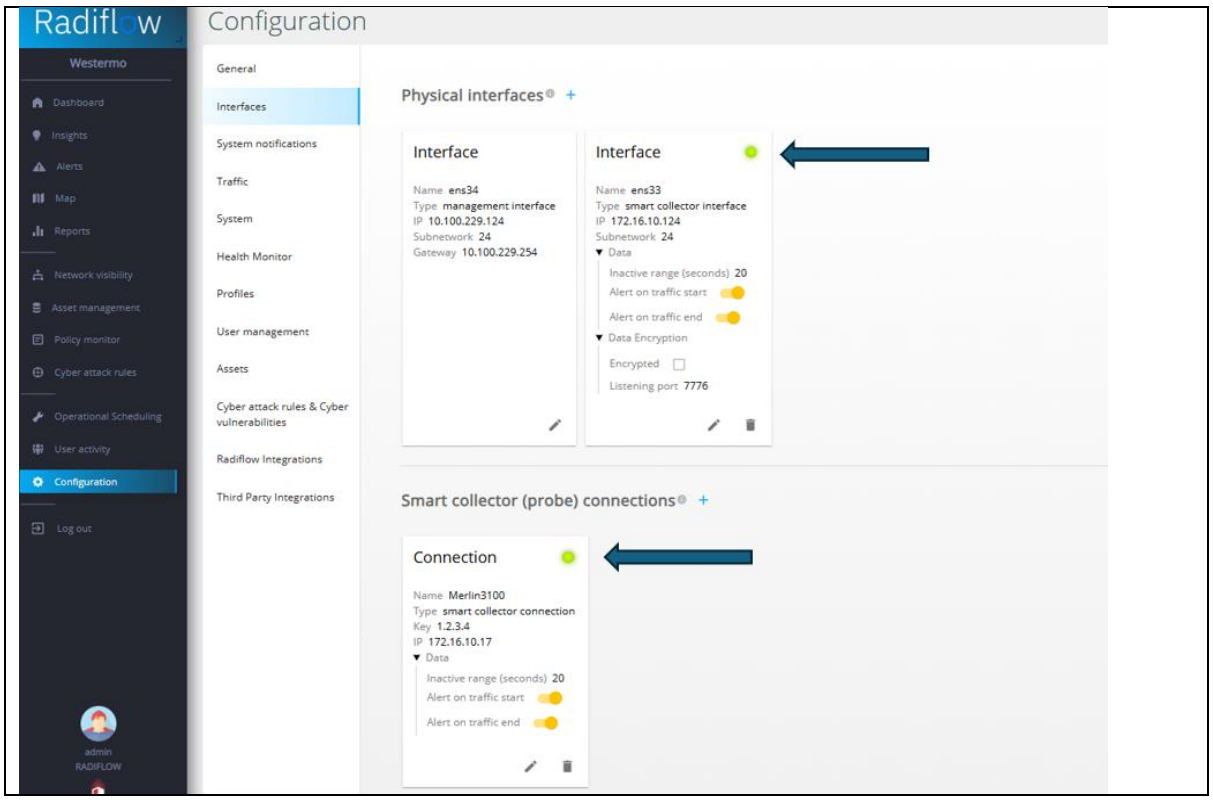


2. Go to **Advanced Settings**
3. Add **SCProbe** interface in **Mirror to** section (Mirror section is at the bottom)

Click **Save& Apply** at the bottom of the page

4 Summary and system verification

Under iSID **Configurations** > **Interfaces**, both Smart Collector and Smart Collector (probe) interfaces should stay green. The warning triangle should no longer be visible, which shows that traffic is now being received.



Once fully configured, the iSID's dashboard should start to produce indicators and metrics.