Documentation Multi-mode optical GTap Model GTap O MM

ref.GTAP O850 1P 5050

or

ref.GTAP O850 1P 6040

GATEWATCHER

Documentation version: V1

Translated from original manual version 1

Creation date: July, 2024

Last update: July, 2024

Table of contents

Table of contents i

1 Description 1
- 1.1 Introduction 1
- 1.2 GTap presentation 2
  - 1.2.1 GTap input/output list 2
  - 1.2.2 Security seal 3
  - 1.2.3 Package contents 3

2 Operation 4
- 2.1 Tap function 4
- 2.2 LC network connectors 4
- 2.3 Power supply 4

3 Characteristics 5

4 Use cases 6
- 4.1 Delivery control procedure 6
  - 4.1.1 Introduction 6
  - 4.1.2 Preliminary procedure 6
  - 4.1.3 Procedure 7
- 4.2 Set-up procedure 7
  - 4.2.1 Preliminary procedure 7
  - 4.2.2 Procedure 8

5 Appendices 10
- 5.1 Legal information 10
  - 5.1.1 Disclaimer 10
  - 5.1.2 Copyright 10
  - 5.1.3 Trademarks 10
- 5.2 Military Programming Law (MPL) 11
  - 5.2.1 Regulatory reminders 11
  - 5.2.2 Goal reminders 11
  - 5.2.3 Requirements reminders 11
  - 5.2.4 MPL applied to the GTap 11

6 Glossary 12

Index 13

Index 13

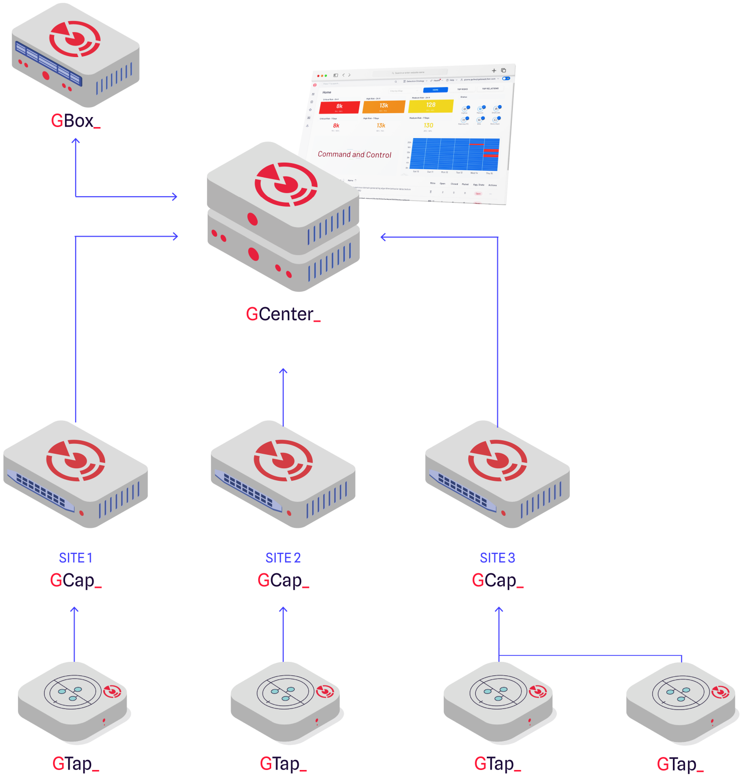
Chapter 1

Description

1.1 Introduction

The AIONIQ® solution is Gatewatcher®'s IDS (Intrusion Detection System) platform.
It includes:

- One or more GTaps
- One or more GCaps
- A GCenter
- A GBox (optional)

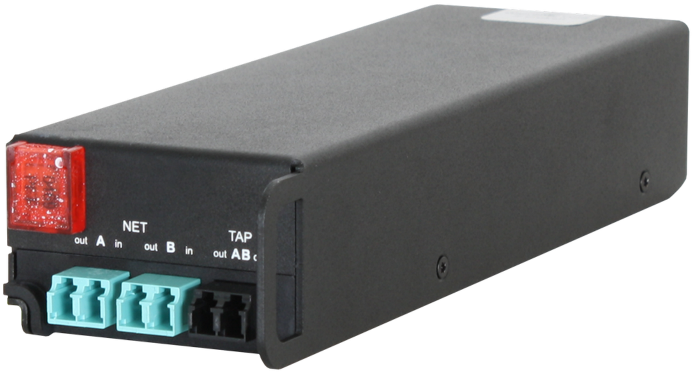


1.2 GTap presentation

The GTap model GTAP_O_MM duplicates the network flow connected to the `NET` ports towards the `TAP` ports.
The GTAP_O_MM is identified by two distinct references:

- GTAP_O850_1P_5050
- GTAP_O850_1P_6040

The GTap takes the following form:

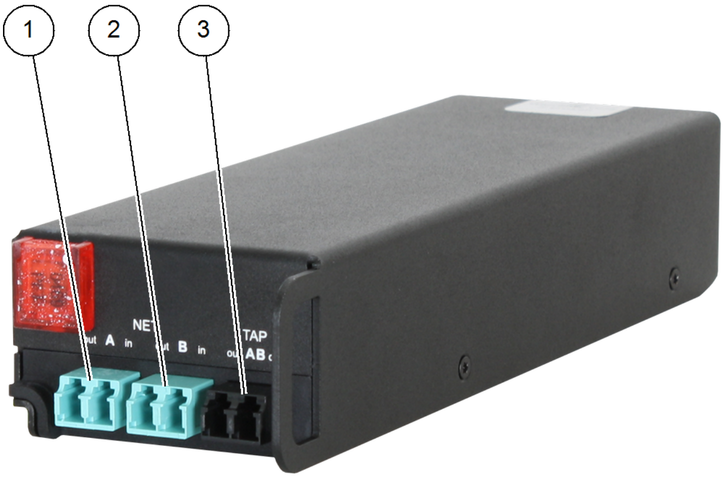


GTM_PRES_01

1.2.1 GTap input/output list

The GTap_O_MM has a total of three duplex LC ports (Lucent Connector):

- The network ports to be monitored: `NET A` and `NET B`
- The port to be connected to the sensing probe: `TAP AB`



GTM_PRES_02

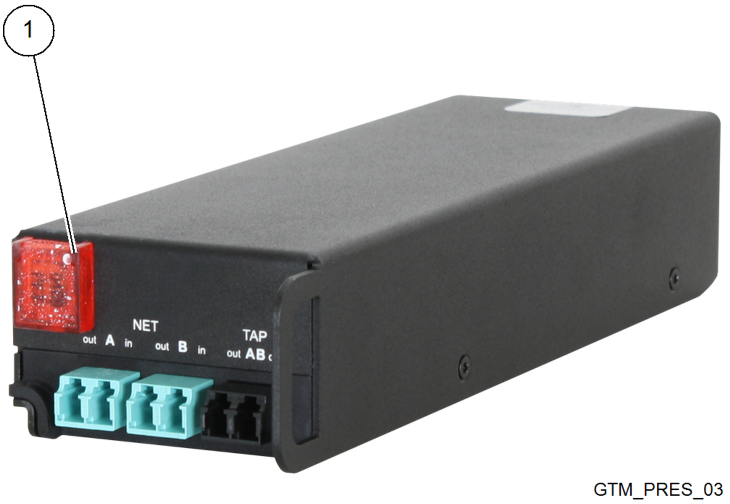
Item	Description
1	NET A: Tap input port connected to the network to be monitored
2	NET B: Tap input port connected to the network to be monitored
3	TAP AB: Tap output port connected to the sensing probe

Note:

Apply the good practices for inserting a Tap on a network.
If necessary, contact the Gatewatcher support or your usual Gatewatcher contact.

1.2.2 Security seal

The GTap also has one security seal, located on the front side:



Item	Description
1	Seal n°1

1.2.3 Package contents

The package includes the GTap model GTAP_O_MM.

Chapter 2

Operation

2.1 Tap function

The GTap prevents potential attacks and disturbances by blocking light from the monitor's ports.
The GTap monitors the seven OSI layers.
The GTap is not configurable and therefore has no management/administration interface.
The GTap does not memorize traffic.
The GTap is non-intrusive and therefore does not disrupt the traffic to be replicated.

Depending on the model, the GTap has a different split ratio:

- GTAP_O850_1P_5050: 50/50 split ratio
- GTAP_O850_1P_6040: 60/40 split ratio

2.2 LC network connectors

The GTap network connectors are specified in the *GTap input/output list*.

2.3 Power supply

The GTap is not equipped with a power supply.

Chapter 3

Characteristics

Reference	Fiber type (µm)	Wavelength (nm)	Split ratio	Maximum insertion loss (dB) NET / TAP	Dimensions (mm)	Weight (g)
GTAP_O850_1P_5050	Multi-Mode 50	850	50/50	3,8 / 5,0	41 x 68 x 217	875
GTAP_O850_1P_6040	Multi-Mode 50	850	60/40	2,8 / 6,0	41 x 68 x 217	875

Chapter 4

Use cases

4.1 Delivery control procedure

4.1.1 Introduction

The GTap comes with one customized security seal that has a unique identification to ensure traceability throughout the supply chain.
This security seal has been photographed before shipment to enhance the level of security it offers.
We ask you to take a photo of the security seal and upload it to the shared drive.
We will compare it and confirm the integrity of your equipment.

During the procedure, the equipment must be stored in a secure facility.
This facility:

- Must have an access strictly limited to authorized personnel and
- Must be subject to an appropriate monitoring process.

Note:

The device is delivered with customized security labels and unique identification to ensure traceability throughout the supply chain.
Please check the integrity of the seal and the correspondence of the identifier.

4.1.2 Preliminary procedure

Note:

Access to the shared drive is provided via an issue opened by our support team on your TAC account.

- Check for a link to the shared drive on your TAC account.
  If this link has not been received, please contact Gatewatcher support to obtain it.
  If necessary, contact the Gatewatcher support or your usual Gatewatcher contact.

4.1.3 Procedure

- Open the box.
- Check that the security seal is present.
- Take a high-definition photo of the security seal.
  - Take the photo as follows:

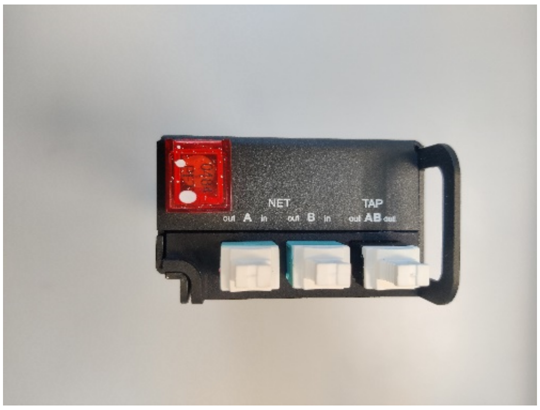


Fig. 1: Example 1

- Click on the link to the shared drive.
- Upload all the photos on the shared drive to the directory defined below.

  The name of the directory is the order reference, and inside it you will find a directory for each GTap (referenced by serial number).

  Please upload the photos in the directory corresponding to each GTap.
- Reply to the TAC issue to confirm the photo upload.

  Once we have completed the inspection, we will let you know the status of your equipment's integrity.
- If the integrity is correct, use the GTap.

  If not, please return it.

4.2 Set-up procedure

4.2.1 Preliminary procedure

Important:

Before installation, check the integrity of the equipment by following the *Delivery control procedure*.

Note:

To capture the flow of the network to be monitored, insert the GTap into the existing network. This can be done either:

- By replacing a multimode LC duplex optical jumper with two jumpers of the same type
- By using the switch's mirroring ports, if so equipped

- Apply the good practices for inserting a Tap on a network.
  If necessary, contact the Gatewatcher support or your usual Gatewatcher contact.
- Procedure for installing the GTaps in a rack :
  - Insert the GTaps into the rack until you hear a click indicating that they are secured in the internal rails.
  - If the GTaps are difficult to insert into the rack, check that the internal rails are at the bottom of the rack and that the GTaps are aligned with the internal rails, with the front panel text vertically aligned.

  Note:

  A 19-inch rack can hold up to six GTap_O_MM.

- If necessary, mount the rack in a bay and secure it.

  Note:

  The height of the GTap rack is 1U.

Important:

Cleanliness of the optical fiber is essential for good signal transmission, as dust and other microscopic particles can disrupt or block the signal.

It is recommended to keep dust caps on unused connectors to reduce the risk of contamination.

In the event of a weak or absent signal, the first step is to clean the cables and connectors.

Before connecting them, it is recommended to clean optical jumpers and connectors using appropriate fiber optic cleaning equipment.

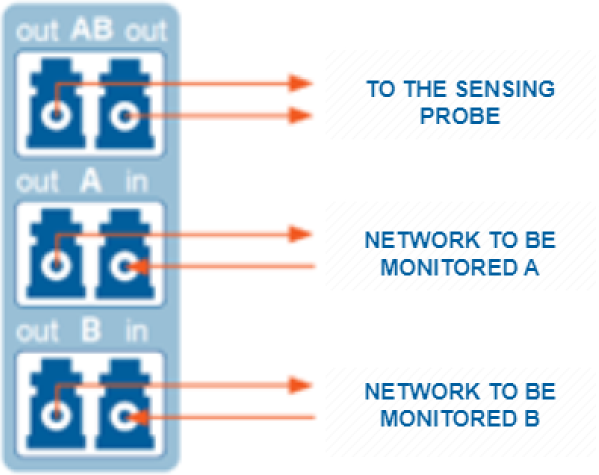
4.2.2 Procedure

- Connection to the network to be monitored:
  - Connect the multimode LC duplex optical jumper of the network to be monitored to the `` `NET A` `` port.
  - Connect the multimode LC duplex optical jumper of the network to be monitored to the `` `NET B` `` port.

  Note:

  For each jumper, remove the covers protecting the fibers and connect the jumper.

- Connection to the sensing probe:
  - Connect the `` `TAP AB` `` port to the sensing probe using a split duplex jumper.
  - Connect the jumpers as shown in the diagram below:


out AB out
out A in
out B in
TO THE SENSING PROBE
NETWORK TO BE MONITORED A
NETWORK TO BE MONITORED B

Chapter 5

Appendices

5.1 Legal information

5.1.1 Disclaimer

The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.
The manufacturer reserves the right to revise this publication and to make changes in the content thereof without obligation of the manufacturer to notify any person of such revision or changes.

5.1.2 Copyright

The communication or reproduction of this document, or the exploitation or communication of its contents, is forbidden without prior written consent.
Any infringement will give rise to damages.
All rights reserved, particularly in the case of patent applications or other registrations.

5.1.3 Trademarks

The trademarks mentioned in this manual are the exclusive property of Gatewatcher:

- TRACKWATCH®/AIONIQ®
- Gatewatcher®

5.2 Military Programming Law (MPL)

5.2.1 Regulatory reminders

Some reminders of the main principles of the French Military Programming Law (MPL):

- French Military Programming Law (Act no. 2013-1168 of 18 December 2013)
- Article 22: implementation supervised by the ANSSI for the OIVs
  - Impose security measures
  - Impose controls on the most critical information systems
  - Make it compulsory to report incidents observed by the OIVs on their information systems
- Article L.1332-6-1 of the Defense Code amended by Act no. 2015-917 of 28 July 2015 - Art. 27
  - Establish organizational and technical measures
  - Define procedures for identifying and reporting security incidents affecting vital information systems (IVIS)

5.2.2 Goal reminders

The goals are:

- To protect national critical infrastructures against cyber attacks,
- Reduce the exposure to risks and
- Optimize the quality of services provided by organizations.

5.2.3 Requirements reminders

Requirements for OIVs and security incident detection service provider (PDIS) actors are to be taken into account on equipment:

- Implement an information systems security policy
- Carry out a security certification
- Communicate the elements on the IVIS set up by the operator to the ANSSI
- Observe and react to security alerts
- Limit access
- Partition the networks
- Select the qualified technologies

5.2.4 MPL applied to the GTap

The GTap model GTAP_O_MM complies with the French Military Programming Law and has been qualified by the ANSSI.

Chapter 6

Glossary

GBox

The GBox can operate as a stand-alone unit or in conjunction with the GCenter. It features four complementary analysis engines, plus an engine to detect domain names generated by DGAs.

GCap

The GCap is the detection probe of the Aioniq solution. It retrieves the network stream from the GTap and reconstitutes the files it sends to the GCenter.

GCenter

The GCenter is the component that administers the GCap and analyzes the files sent by the GCap.

GTap

The GTap is a passive device that duplicates the flow of a network and copies it in its entirety, without memorizing or impacting it.

IDS

Intrusion detection systems are software or hardware systems designed to automate the monitoring of events occurring in a network or on a particular machine, and to be able to report to the system administrator any trace of abnormal activity on the latter or on the monitored machine.

OSI

The OSI (Open Systems Interconnection) model is a conceptual framework that defines how network systems communicate and send data from a sender to a receiver. It contains seven layers, stacked conceptually from bottom to top.

TAC

The TAC (Technical Assistance Center) is Gatewatcher's support platform

`PDF Documentation GTap O MM`

Index

G

GBox, **12**
GCap, **12**
GCenter, **12**
GTap, **12**

I

IDS, **12**

O

OSI, **12**

T

TAC, **12**