

# Documentation 8-link Gigabit copper GTap Model GTap CU 8P



Documentation version: V2

Translated from original manual version 2

Creation date: June, 2024

Last update: July, 2024

@GATEWATCHER - 2024

Disclosure or reproduction of this document, and use or disclosure of the contents hereof, are prohibited except with prior written consent. Any breach shall give right to damages.

All rights reserved, particularly in the case of patent application or other registrations

# Table of contents

<b>Table of contents</b>	<b>i</b>
<b>1 Description</b>	<b>1</b>
1.1 Introduction . . . . .	1
1.2 GTap presentation . . . . .	2
1.2.1 GTap input/output list . . . . .	2
1.2.2 Security seals . . . . .	3
1.2.3 Package contents . . . . .	4
<b>2 Operation</b>	<b>5</b>
2.1 Tap function . . . . .	5
2.2 RJ45 network connectors . . . . .	5
2.3 LED 10 and LED 100 . . . . .	6
2.4 Power supply . . . . .	7
<b>3 Characteristics</b>	<b>8</b>
<b>4 Use cases</b>	<b>9</b>
4.1 Delivery control procedure . . . . .	9
4.1.1 Introduction . . . . .	9
4.1.2 Preliminary procedure . . . . .	9
4.1.3 Procedure . . . . .	10
4.2 Set-up procedure . . . . .	11
4.2.1 Preliminary procedure . . . . .	11
4.2.2 Procedure . . . . .	11
<b>5 Appendices</b>	<b>13</b>
5.1 Safety information . . . . .	13
5.2 Legal information . . . . .	13
5.2.1 Disclaimer . . . . .	13
5.2.2 Copyright . . . . .	13
5.2.3 Trademarks . . . . .	14
5.3 Military Programming Law (MPL) . . . . .	14
5.3.1 Regulatory reminders . . . . .	14
5.3.2 Goal reminders . . . . .	14
5.3.3 Requirements reminders . . . . .	14
5.3.4 MPL applied to the GTap . . . . .	15
<b>6 Glossary</b>	<b>16</b>
<b>Index</b>	<b>17</b>
<b>Index</b>	<b>17</b>

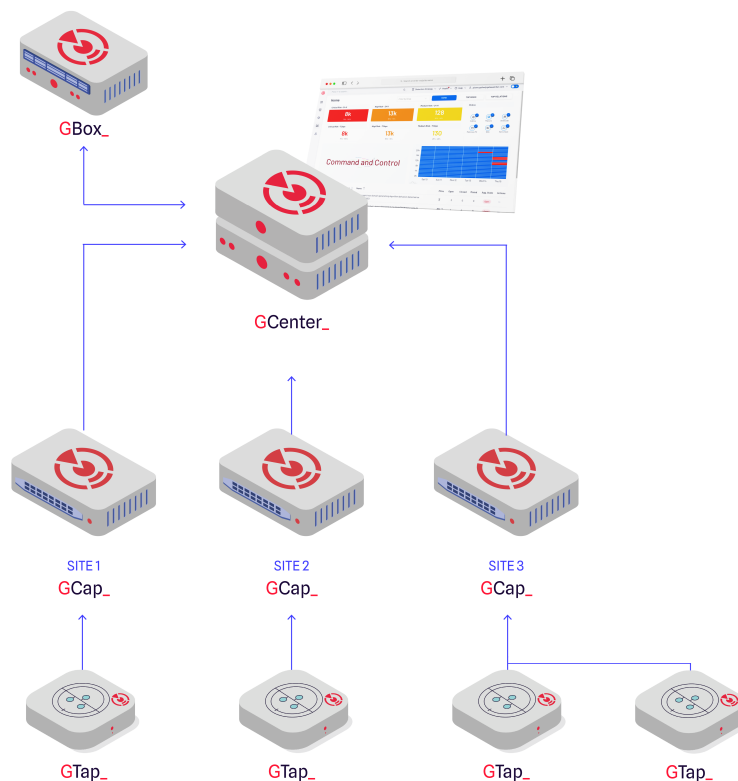
# Chapter 1

## 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

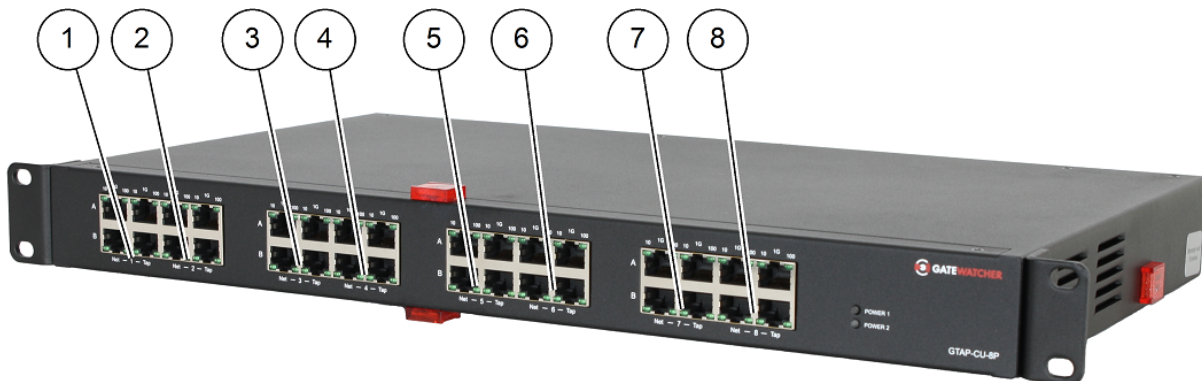
The GTap model GTAP\_CU\_8P consists of:

- Eight independent Tap units, each of which duplicates the network flow connected to the `Net` ports
- One mechanical chassis (1U/19 inches) for rack mounting
- Two redundant power supplies

The GTap takes the following form:



### 1.2.1 GTap input/output list

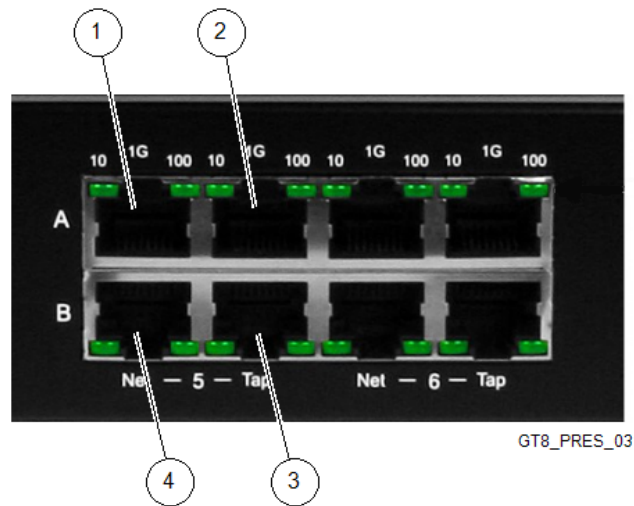


GT8\_PRES\_02

The **GTap** has eight Tap units numbered from 1 to 8, each comprising four ports:

Item	Description
1	Tap unit n°1
2	Tap unit n°2
3	Tap unit n°3
4	Tap unit n°4
5	Tap unit n°5
6	Tap unit n°6
7	Tap unit n°7
8	Tap unit n°8

These Tap units each have four ports:



GT8\_PRES\_03

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

On the rear side, the two C14 power connectors are named <POWER 1> and <POWER 2>.

### 1.2.2 Security seals

The GTap also has six security seals, which are marked as follows:



GT8\_PRES\_04



Item	Description
1	Seal n°1
2	Seal n°2
3	Seal n°3
4	Seal n°4
5	Seal n°5
6	Seal n°6

### 1.2.3 Package contents

The package includes:

- The GTap model GTAP\_CU\_8P
- Two power cords E-type male plug (CEE 7/7) / C13 socket

# Chapter 2

## Operation

### 2.1 Tap function

Each Tap unit faithfully copies all incoming traffic to the RJ45 ports (Net A and Net B) at the same network speed (10/100/1000 BASE-T).

The Tap monitors the seven OSI layers and duplicates:

- Packs of all sizes and types
- Low-level errors and VLAN traffic

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.

The GTap has no IP address and isolates the network to be monitored from the monitoring device.

Once in place, the GTap enables monitoring devices to be connected and disconnected at will, with no impact on the network link to be monitored.

---

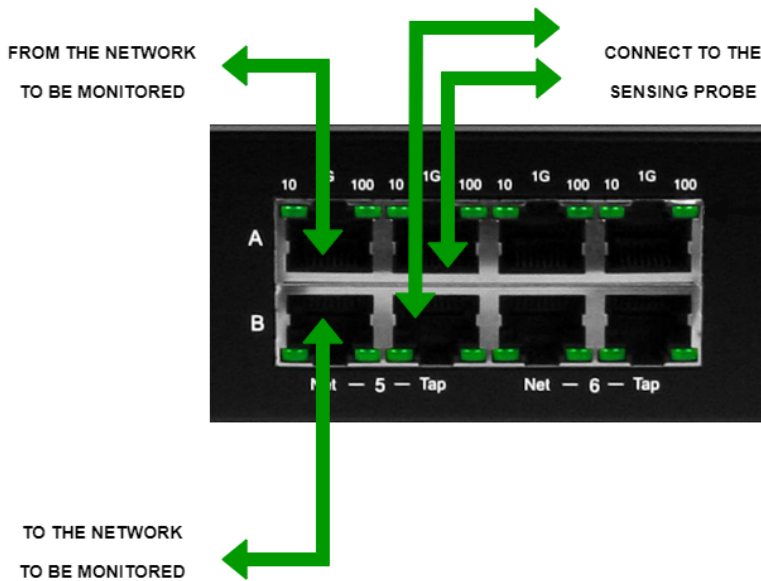
### 2.2 RJ45 network connectors

The GTap\_CU\_8P has a total of 32 RJ45 ports, for eight Tap units (numbered from 1 to 8).

Each Tap unit consists of four ports:

- The network ports to be monitored: `Net A` and `Net B`
- The ports to be connected to the sensing probe: `Tap A` and `Tap B`

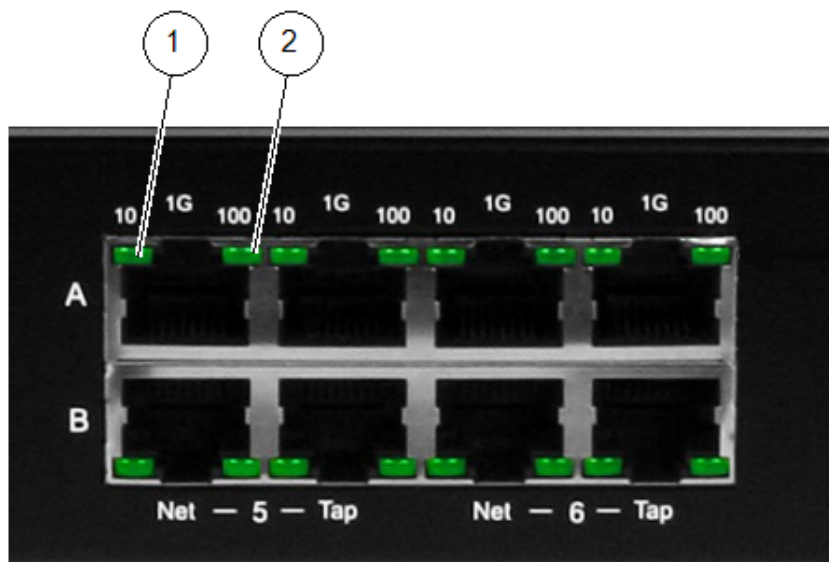




**Note:**

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

### 2.3 LED 10 and LED 100



GT8\_LED\_01

Marker	Description
1	LED 10 Mb/s
2	LED 100 Mb/s

After negotiation on active and connected network ports, the LEDs light up steadily to indicate network speed:

- LED 10 (1) is lit steady for a 10 Mb/s connection
- LED 100 (2) is lit steady for a 100 Mb/s connection
- Both LEDs are lit steady for a 1 Gb/s connection

The flashing means that a signal is detected and only one network cable is connected.

---

## 2.4 Power supply

The GTap is equipped with two redundant power supplies.

The presence of power is indicated by the <POWER 1> and <POWER 2> LEDs.

In the event of a power supply failure (one of the two LEDs is off), contact the Gatewatcher support.

In the event of a total power failure, the GTap instantly switches to totally passive mode, so that the monitored network link remains operational.

---

## Chapter 3

# Characteristics

	CHARACTERISTICS
Connectors	8 Tap units (4 RJ45 ports per Tap), gold plated
LEDs	2 LEDs 10/100 per RJ45 port (Speed, Link, Activity) 1 LED POWER per supply (voltage presence)
Power supply	2 x 100-240VAC stabilized, 50-60Hz, 50W
Power consumption	50W
MTBF (mean time between failures)	150 000 hours
Enclosure	Steel and aluminium, black painted
Dimensions (W x D x H)	44 x 440 x 260 mm (1U/19 inches) 17.3 x 10.2 x 1.7 in
Weight	3,6 kg 7.94 lb
Operating temperature	0 °C to 50 °C 32 °F to 122 °F
Storage temperature	-20 °C to 70 °C -4 °F to 158 °F
Humidity	10 to 90 %, non-condensing
Certifications	RoHS — CE — FCC class A IEEE 802.3 — UL 62368-1

# Chapter 4

## Use cases

### 4.1 Delivery control procedure

#### 4.1.1 Introduction

The GTap comes with six customized security seals, each with a unique identification to ensure traceability throughout the supply chain.

These security seals have been photographed before shipment to enhance the level of security they offer. We ask you to take a photo of each security seal and upload them to the shared drive. We will compare them 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 seals 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 all security seals are present.
- Take high-definition photos of each security seal (GTap CU\_8P has six, i.e. six photos in total).
  - Take photos as follows:



Fig. 1: Example1

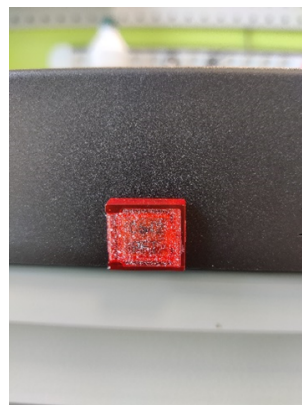


Fig. 2: Example2

- 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 an existing network cable with two tap-off cables to the Tap
  - 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.
  - Do not turn on the GTap.
  - If necessary, mount and secure the GTap in a rack (19 inches).

**Note:**

The height of the GTap is 1U without the security seals.

---

### 4.2.2 Procedure

- Connecting the GTap power cables:

**Note:**

Recommendation: connect the GTap power supplies to two different feeders, themselves connected to separate power lines with different circuit breakers.

- Connect the first C13 power cord supplied:
  - \* On one side to the <POWER 1> connector (type C14) on the GTap
  - \* On the other side to the first feeder in the rack

**Important:**

Use only properly grounded power cords and feeders.  
The feeders must remain easily accessible after the installation.

- Connect the second C13 power cord supplied:
  - \* On one side to the <POWER 2> connector (type C14) on the GTap
  - \* On the other side to the second feeder in the rack

- Checking the GTap power supply:
  - Check that the <POWER 1> and <POWER 2> LEDs are lit.  
If this is not the case, check that the cables are correctly plugged into the sockets and that the rack's feeders are properly powered.
- Connection to the network to be monitored:
  - Connect the cables of the network to be monitored to the `Net A` and `Net B` connectors.
    - \* Use category 5e or higher RJ45 UTP cables.

In the case of 10/100 MB network equipment that does not support auto-crossover:

    - Use two straight cables if network devices are of different types (one DTE and one DCE)
    - Use a straight cable and a crossover cable if the two network devices are of the same type (both DTE or both DCE).
- Checking the network flow to be monitored with the LEDs:
 

After negotiation on active and connected network ports, the LEDs light up steadily to indicate network speed:

  - LED 10 (1) is lit steady for a 10 Mb/s connection
  - LED 100 (2) is lit steady for a 100 Mb/s connection
  - Both LEDs are lit steady for a 1 Gb/s connection

The flashing means that a signal is detected and only one network cable is connected.

  - Check that the `Net A` and `Net B` LEDs of the Tap units used are permanently lit.  
If a Tap unit's LEDs are flashing, check its cables and connections.
  - Check the activity of the network to be monitored.  
To do this, check that the LEDs on the Tap unit's `Net A` and `Net B` are flashing rapidly.
- Connection to the sensing probe:
  - Connect the Tap's `Tap A` and `Tap B` ports to the sensing probe, using straight or crossover RJ45 UTP cables of category 5e or higher.

**Note:**

A powered Tap will always correct a bad cable configuration.  
The network traffic received on the port `Net A` is duplicated on the port `Tap A` and network traffic received on the port `Net B` is duplicated on the port `Tap B`.  
The maximum distance between connected devices is 100 meters.

- Checking the flow of the network to be monitored with the LEDs:

**Note:**

The monitored `Tap` ports operate at the same speed as the `Net` input ports.

- Checking the speed of `Tap` links:
  - \* Check that the LEDs (10 and 100) of each `Tap` and `Net` port are lit identically.
- Checking the activity of the network to be monitored:
  - \* Check that the LEDs of the `Tap A` and `Tap B` in use are flashing rapidly.

# Chapter 5

## Appendices

### 5.1 Safety information

This equipment is not suitable for use in areas where children are likely to be present.

This equipment has several power supplies.

- Unplug ALL power cords during removal/reinstallation.
  - Do not push or force objects through any opening in the chassis frame, as this may result in electric shock or fire.
  - Avoid spilling liquid on the equipment, as this may cause electric shock or damage the equipment.
- 

### 5.2 Legal information

#### 5.2.1 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.

---

#### 5.2.2 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.

---



### 5.2.3 Trademarks

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

- TRACKWATCH®/AIONIQ®
  - Gatewatcher®
- 

## 5.3 Military Programming Law (MPL)

### 5.3.1 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)
- 

### 5.3.2 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.
- 

### 5.3.3 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
-

### 5.3.4 MPL applied to the GTap

The GTap model GTAP\_CU\_8P complies with the French Military Planning 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 TAP 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.

**PSU**

The PSU is the power supply unit.

**TAC**

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

PDF Documentation GTap CU\_8P

# Index

## G

GBox, 16

GCap, 16

GCenter, 16

GTap, 16

## I

IDS, 16

## O

OSI, 16

## P

PSU, 16

## T

TAC, 16