

# *F1-10G-BP BYPASS TAP*

*INSTALLATION AND CONFIGURATION MANUAL*



*Congratulations, you have joined the elite.*

For any questions, technical or otherwise, please contact our customer support through our website:

[\*www.profitap.com\*](http://www.profitap.com)

or by email:

[\*info@profitap.com\*](mailto:info@profitap.com)

For the latest documentation and software, visit our Resource Center:

[\*http://www.profitap.com/resource-center/\*](http://www.profitap.com/resource-center/)

# TABLE OF CONTENTS

---

## **Installation** **1**

1. Unpacking & Installation	1
1.1 Unpacking	1
1.2 Installation	1
2. Product Overview	2
2.1 Technical and Electrical Specifications	4
2.2 Front View	5
2.3 Rear View	5
2.4 LED Functionality	6
3. Connecting Power and Start-Up	6
4. Accessing the F1-10G-BP Bypass Tap	7

## **Configuration** **8**

1. Web Administration	8
1.1 Device Status	8
1.2 Port Management	9
1.3 Global Statistics	9
1.4 Bypass	10
1.5 Settings	12
1.6 Logs	13
2. CLI Administration	13

## **Operation Use Cases** **16**

## **Legal** **21**

# INSTALLATION

## 1. UNPACKING & INSTALLATION

### 1.1 Unpacking

Carefully unpack all the items supplied with the F1-10G-BP and retain the packaging for later use:

- 1x F1-10G-BP main unit.
- 1x AC/DC Power supply.
- 1x DB9 to RJ45 Console cable.

► Note: Please contact the supplier if any part is missing or damaged.

### 1.2 Installation

This unit can only be mounted in a standard 19" (1U) rack, using a rackmount kit sold separately.

Up to 3x F1-10G-BP units can be installed on a single 19" rack, using a rackmount chassis kit. When installing the unit(s) in a rack, follow these steps:

- First, install the rackmount chassis kit (sold separately) in the 19" (1U) rack.
- Secure the unit(s) with the thumbscrews in the rackmount chassis kit.
- Make sure the rack is properly grounded.

## *2. PRODUCT OVERVIEW*

Active in-line security appliances are single points of failure in any network.

The F1-10G-BP bypass TAP monitors the health of the connected appliance and removes any point of failure by automatically switching traffic in a bypass mode, to keep critical network link up.

The F1-10G-BP features set include:

- Link Failure Propagation (LFP).
- Bidirectional Heartbeat (ping signal to and from the monitored appliance).
- Predefined and custom Heartbeat signal type.
- Fine Heartbeat control.
- Administration via HTTP/CLI.
- Comprehensive configuration and behavior.
- 1G/10G operation.
- High reliability design, no point of failure.

### *LINK FAILURE PROPAGATION (LFP)*

The in-line network port group (NET A and NET B ports) supports Link Failure Propagation. If a network disconnection occurs on one port of the group, the other port is automatically disabled, propagating the failure on the monitored line and allowing alternative data paths to be used in the networks' routing node.

### *BIDIRECTIONAL HEARTBEAT INJECTION*

When the device operates in Auto Bypass mode, Heartbeat packets A and B are inserted into the network traffic egressing TAP A and TAP B. These Heartbeats packets are used to monitor the inline path of the security appliance.

Heartbeat packets A and B can be configured from a predefined list or can be customized.

Predefined packets include IPX, ICMP request/reply, LCP request/reply and TCP-SYN. The device is factory programmed with two globally unique MAC addresses, used as source MAC addresses for Heartbeat A and B.

### *HEARTBEAT RATE CONTROL*

The Heartbeat injection rate can be set from 50 $\mu$ s to 4s (default value is 1s).

### *HEARTBEAT FAILURE TIMEOUT*

The Heartbeat failure timeout can be set from 50 $\mu$ s to 4s (default value is 3s). When the Heartbeat timeout event occurs on at least one direction, the logical bypass is enabled while the in-line path remains active.

### *HEARTBEAT RECOVERY*

If the logical Bypass is activated due to a Heartbeat failure or TAP link down event, the return to normal operation occurs after N valid Heartbeat packets are received in both directions (default N value is 2).

### *HEARTBEAT PRIORITY*

The injected Heartbeat packets have a higher priority over the network traffic. If the network bandwidth utilization is 100%, some packets might get dropped in order to inject the Heartbeat packets. Dropped packets are reported in "Dropped packets" counters.

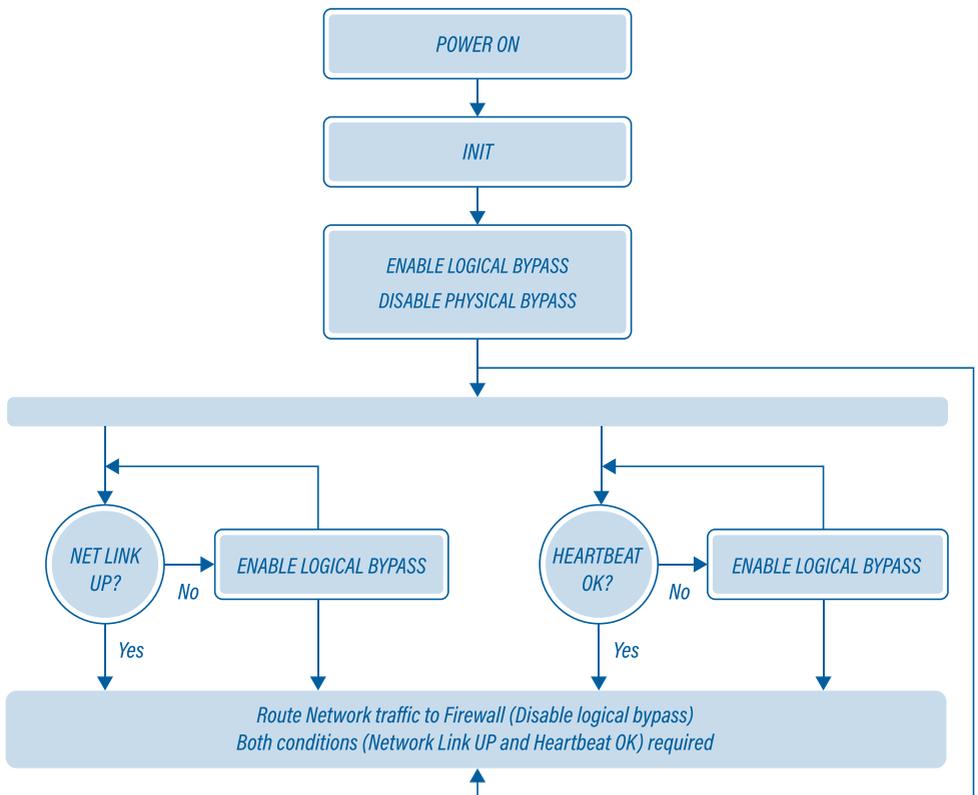
### *BYPASS CIRCUITS*

Covering all failure scenarios, the F1-10G-BP unit is equipped with both a physical bypass (passive) and a logical bypass (activated by the FPGA) used to maintain data flow:

- ◉ In case of power outage, the physical bypass is activated by default (fail open), allowing the network connection on the tapped line to remain functional.
- ◉ In case of Heartbeat failure or TAP link down, the logical bypass is activated

instead, allowing the network connection on the tapped line to remain functional.

The basic functionality is depicted in the following diagram, explaining the logical paths and alternatives FI-10G-BP operates on. For more information regarding operation scenarios, please go to **Operation Use Cases** chapter.



## 2.1 Technical and Electrical Specifications

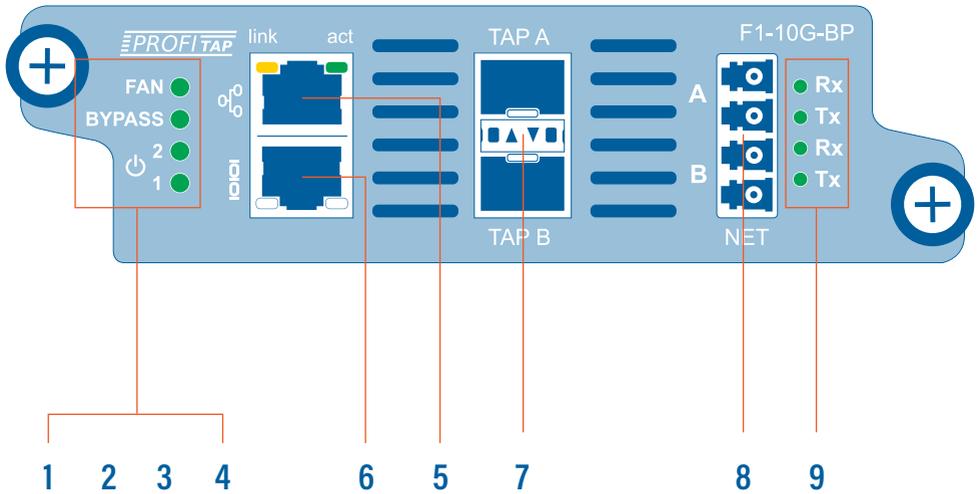
Dimensions: 40.5 x 149 x 220mm (height x width x depth)

Weight: 950g

Power requirement: 12V 1.5A

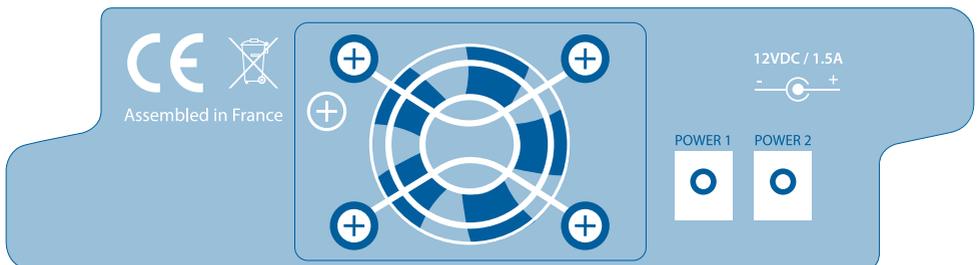
BTU/hr: 62

## 2.2 Front View



- |  |   |
|--|---|
| <b>1, 2</b> PSU1, PSU2 Status LEDs                   | <b>6</b> Serial Administration interface 115200 / 8 / 1 / n |
| <b>3</b> Bypass Status Led                           | <b>7</b> TAP / Appliance A,B. 1Gbps/10Gbps                  |
| <b>4</b> Fan Status LED                              | <b>8</b> In-line network segment port A,B. 1Gbps/10Gbps     |
| <b>5</b> Ethernet management interface 10 / 100 Mbps | <b>9</b> Rx / Tx activity LEDs for NET A & NET B            |

## 2.2 Rear View



## 2.4 LED Functionality

LED FUNCTION / STATE	MEANING / CONTROL	
Fan LED	Green	PSU is operating normally
	Orange	OVP: Over Voltage Protection UVP: Under Voltage Protection
Bypass LED	Green	PSU is operating normally
	Orange	Monitored appliance is down, bypass is activated.
1 LED	Green	PSU1 is connected
	Orange	PSU1 not connected or not working
2 LED		
	Orange	PSU2 not connected or not working
	link Amber	Link up @ 10 / 100 Mbps
	act Blinking Green	Link up with activity.
FAN, Bypass, 1, 2	Orange	Unit is rebooting

## 3. CONNECTING POWER AND START-UP

The system does not have a main switch, it powers up as soon as one of the redundant power supplies is connected to the unit.

- ▶ **Note:** The use of both power supplies is recommended to achieve a maximum failsafe operation at any time.

The F1-10G-BP is equipped with status and activity leds. For more details on status leds color and coding, please see **2.4 Led Functionality** chapter.

## 4. ACCESSING THE F1-10G-BP BYPASS TAP

System access can be achieved through serial or Ethernet connection. By default, the unit network interface has DHCP enabled.

For accessing the unit through the serial connection, follow these steps:

1. Power up the unit.
2. Wait for the unit to boot.
3. Connect your computer to the serial administration interface.
4. Using the favorite terminal software (xterm, putty, etc), the following connection settings must be used: 115200 baud rate, 8 bit, no parity, 1 bit stop. The following credentials are accepted:
  - Username: master
  - Password: master

For accessing the unit through its IP address, either in CLI mode (ssh) or via web interface (BP Manager), follow these steps:

1. Power up the unit.
2. Wait for the unit to boot.
3. Connect the Ethernet management port to the local network. By default, the DHCP is enabled.

- **Note:** The IP must first be discovered in the network, in case it is not allocated by the gateway, using a mac allocation table. As an alternative, the IP can be obtained by connecting to the unit through its serial interface and running the `network.status` command.

4. Type the device IP in a browser. Alternatively, connect via SSH, using the unit's IP address.
5. Login with the default credentials. (master:master). Modify the default admin account, if desired.
6. Login again, using the modified username;password combination.

# CONFIGURATION

## 1. WEB ADMINISTRATION

The F1-10G-BP can be administered either in CLI mode or in a graphical OS and platform independent web-based interface, called **BP Manager**.



► **Note:** BP Manager can only administer and monitor a single F1-10G-BP unit.

Grouped by functionality, there are six menu tabs displayed in the left side of the screen:

- ◉ Device Status
- ◉ Port Management
- ◉ Global Statistics
- ◉ Bypass
- ◉ Settings
- ◉ Logs



### 1.1 Device Status

The Device Status page displays the device status and sensors information. Without logging in, this menu is the only one available. The following information is displayed:

- ◉ Revision information (model number, sw/hw revision)
- ◉ Administrator information (user name, phone number, email address)
- ◉ Date and time information

- Network details
- Sensors (the air temperature is measured in proximity of the fans block, the system temperature is measured within the forwarding plane chip).
- Temperature readings for CPU, system and external air.



## 1.2 Ports Management

The Port Management page displays the name, link status and speed of all interfaces.

Name	Link	Speed
NET A	Down	10G
TAP B	Up	10G

Changing the speed at which interfaces operate (between 1G and 10G) is only available via CLI, using the **mode** command.

▶ **Note:** Interface speed changes apply for all interfaces: NET A, NET B, TAP A and TAP B.



## 1.3 Statistics

The Global Statistics page displays the counters for each interface, offering an overview on all data flow:

- Rx good packets: all packets received in good shape are counted here.
- Rx CRC error packets: all packets received, failing the CRC error checking (the Heartbeat packets or the network traffic which are sent to the monitored appliance come back corrupted - having the wrong Ethernet FCS) are counted here.
- Dropped packets: all packets dropped so that Heartbeat packets could be injected

in case of a 100% network bandwidth utilization, are counted here.

- ◉ Rx Heartbeat packets: all Heartbeat packets (replied from an ALIVE monitored appliance) received in good shape are counted here.



## 1.4 Bypass

The Bypass page represents the heart of FI-10G-BP functionality configuration, allowing the user to custom tailor the unit's behavior, given various environment scenarios.

For more information regarding operation scenarios, please goto ***Operation Use Cases*** chapter.

***MANUAL BYPASS:*** This checkbox allows the user to force the unit to bypass the traffic regardless of other bypass related rules.

***IN CASE MANUAL BYPASS IS ON:*** This option is only relevant when Manual Bypass options is ON, allowing the user to configure whether the TAP mode is ON and the data is being replicated or the TAP mode is off.

***IN CASE OF POWER FAILURE:*** This selection allows the user to program the physical (passive) bypass to be activated or deactivated in case of a power loss in the unit.

***IN CASE OF HEARTBEAT FAILURE:*** This selection allows the user to program the bypass behavior in case of a Heartbeat timeout. The timeout is also user customizable in the Heartbeat failure timeout field.

***IN CASE THE TAP LINK IS DOWN:*** This selection allows the user to program the bypass behavior in case the TAP link is down.

***HEARTBEAT A, B:*** There are two sections, one corresponding to the Heartbeat packet sent

from NET A port to NET B port and one corresponding to the Heartbeat packet sent from NET B port to NET A port, allowing the user to customize these packets and save/load them to/from a local location.

- The drop down menu, allows “shaping” the Heartbeat packet after various pre-defined ping like signatures or completely customize it by choosing Custom packet from this menu.
- **+** **-** These buttons allow the user to tailor the size of the Heartbeat custom packet. There is a minimum and a maximum size allowed. Added blocks (**+**) of information to the custom packet are initially filled with “00”, which can be changed as desired.
- The packet snapshot can be edited in the left side (HEX) while the ASCII form is displayed in the right side.

```
00000000 08 00 45 00 00 34 32 2D 40 00 80 06 4A D0 C0 A8 LE 42-@ [LJBA
00000010 00 C3 97 65 24 F6 55 62 00 50 07 F6 50 C3 00 00 ACes8Ub pCpA
00000020 00 00 80 02 FA F0 47 ED 00 00 02 04 05 B4 01 03 [G6G1 [C[C
00000030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
```

**HEARTBEAT RATE:** Allows the user to change the rate of sending Heartbeat packets to the monitored appliance, measured in microseconds. For example, setting this value to 1,000,000, will generate a rate of 1 Heartbeat package per second. Setting this value to 500,000, will generate a rate of 2 Heartbeat packages per second.

**HEARTBEAT FAILURE TIMEOUT:** Allows the user to set a specified time interval that will be allowed to elapse between sending and receiving a Heartbeat packet. If this interval is exceeded, the behavior is interpreted as failure and the Bypass is set to ON or OFF, depending on the selection user made on the “IN CASE OF HEARTBEAT FAILURE (timeout)” option.

**HEARTBEAT RECOVERY AFTER:** After a Heartbeat timeout occurs, it is important not to

consider the appliance alive again (or the network being up again) after only receiving a single Heartbeat packet. It is safer to receive at least 2 or more Heartbeat packets to be sure the service is alive again. This option allows the user to configure the number of these consecutive received Heartbeats, after a Heartbeat failure, after which the system enables or disables the Bypass behavior contrary to the selection user made on the “In case of Heartbeat failure (timeout)” option.



## 1.5 User Settings

The Settings page allows changing system related settings.

The Setup tab allows editing the administration contact details, the system date and time and the network address.

- ▶ **Note:** In case the IP is changed from static to dynamically allocated (DHCP), the new IP must first be discovered or allocated by the gateway (using a MAC address allocation table). Also, disabling the network interface will make the web interface unavailable, in which case a serial connection to the unit must be established to reactivate the network interface (see *CLI Administration* for additional details).

The **Update** tab allows the system to be updated to a new version, from a locally stored update file.

- ▶ **Note:** Please do not unplug the power cable during the update process. The device will reboot once the installation is complete and the webpage will be reloaded.



## 1.6 Logs

The Logs page allows downloading both the bypass log and the system log.

Download bypass log

Download system log

## 2. CLI ADMINISTRATION

After logging into the system, the user has access to all available commands. Useful commands to navigate the console:

- 'ls' or 'help' for available branches.
- TAB autocompletes commands and also shows the available branches.
- Ctrl+D cancels a command.
- " returns to initial branch.
- '..' returns to previous branch.
- PgUp and PgDown scrolls the console.
- CTRL+C closes the terminal.

Commands residing in one branch can also be executed from different branches, using the [.] prefix, provided the path and the command name is known, for example:

```
.date_time.> .users.list
Users: master
.date_time.>
```

The following commands are available in the CLI:

<i>date_time</i>	show: Displays the date. set: Allows the user to set the date and time.
<i>factory_reset</i>	Should the system become corrupted or the main parameters need to be restored to their default values, this option resets the device to the factory state and reboots the system.
<i>import</i>	Allows the user to update the system's firmware from an URL address.
<i>show_legal_info</i>	Displays the Product Legal Information.
<i>mode</i>	show: Displays the fiber link speed. It can be either 1G or 10G. set: Allows the user to change the fiber link speed between 1G and 10G. <i>WARNING:</i> changing the fiber link speed will restart the unit.
<i>network</i>	configure: Allows the user to set the IP acquisition mode of the unit to either DHCP or STATIC. In case STATIC is selected, the user has to input the IPv4, network mask, gateway and DNS address. disable: Disables the Ethernet interface. The serial management port will still be operating.

► **Note:** if connected through ssh via Ethernet port, after disabling the network interface, the session will be lost.

enable: Allows the user to re-enable the Ethernet interface. The network configuration before disabling the Ethernet interface will be restored.

reset: Allows the user to reset the Ethernet interface to its default configuration: interface:enabled, DHCP: active.

status: Displays the network parameters of the unit: IP, Mask, Gateway, DNS and MAC address.

### *reboot*

Immediately reboots the system, keeping all configurations intact.

### *ssl\_cert\_reset*

It creates a new SSL certificate for the BP Manager web interface. After issuing the command, the unit restarts and the new certificate must be accepted again when accessing the web interface. Manually renewing licenses is especially helpful in preventing man in the middle type attacks.

### *system\_log*

Displays all system related logs and their timestamps.

### *bypass\_log*

Displays all bypass events related logs and their timestamps.

### *users*

list: Displays the list of users.

reset: Resets the password for the master admin user, and erases the rest of the users.

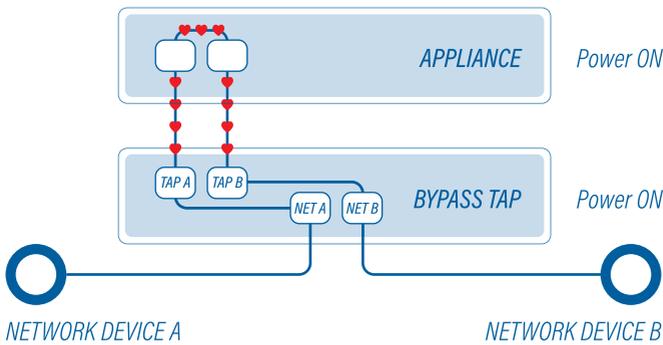
► **Note:** At this time, the firmware does not allow adding new users into the system.

# OPERATION USE CASES

The following cases depict all possible functional states in which FI can operate, depending on the environment changes and its configuration.

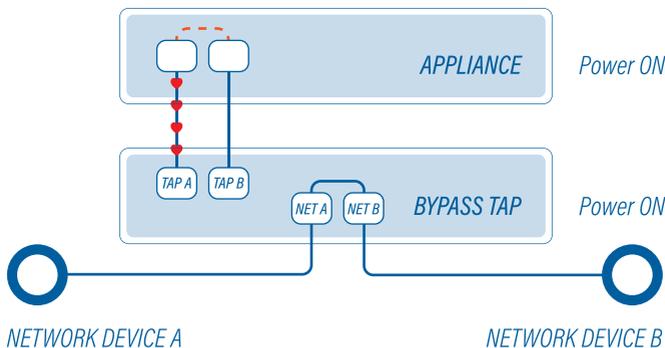
## Case 1 - Normal Operation

The traffic is forwarded to the appliance and heartbeat packets are injected in the network traffic in both directions.



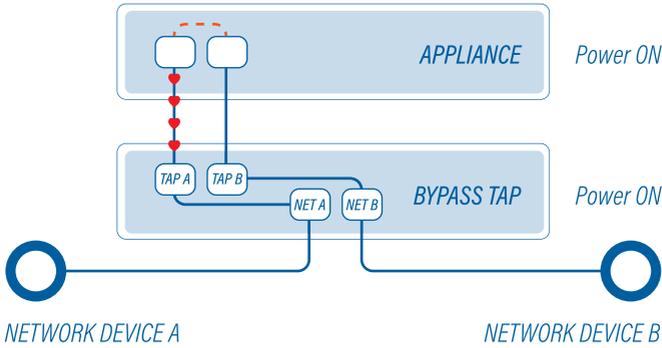
## Case 2 - Heartbeat failure, Bypass ON

If the heartbeats packets are sent to the appliance but are not forwarded back, and the Bypass in case of heartbeat failure is set to ON, the logical bypass is activated by the FPGA. The network path between Network Device A and Network Device B remains **functional**.



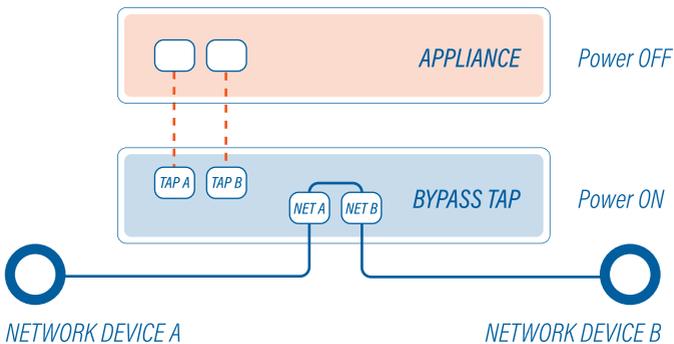
### Case 3 - Heartbeat failure, Bypass OFF

If the heartbeat packets are sent to the appliance but are not forwarded back, and the Bypass in case of heartbeat **failure** is set to OFF, the FPGA will not activate the bypass feature, resulting in a link failure between Network Device A and Network Device B.



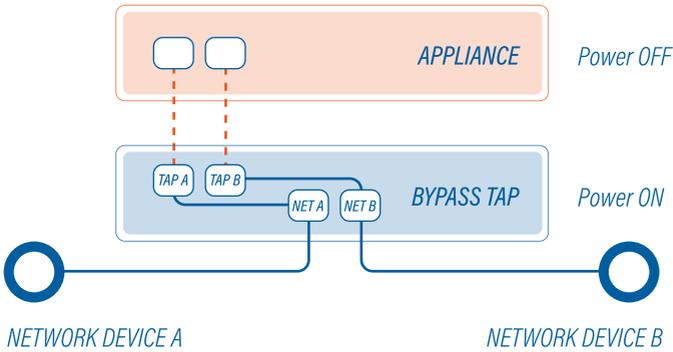
### Case 4 - Appliance Link Down, Bypass ON

If the Appliance is unpowered or the ports are disconnected, and the In case the TAP link is **DOWN** is set to ON, the logical bypass is activated by the FPGA. The network path between Network Device A and Network Device B remains **functional**.



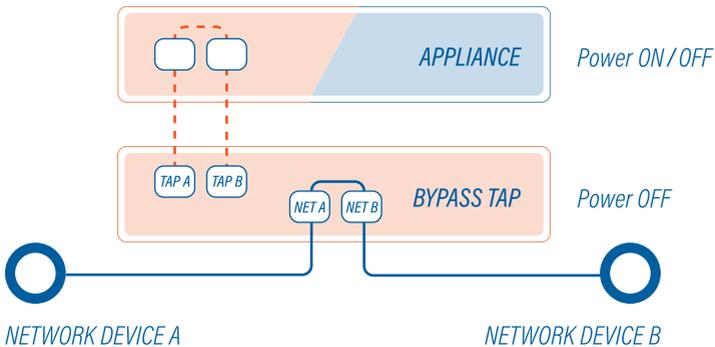
### Case 5 - Appliance Link Down, Bypass OFF

If the Appliance is unpowered or the ports are disconnected, and the In case the TAP link is DOWN is set to OFF, the FPGA will not activate the bypass feature, resulting in a link **failure** between Network Device A and Network Device B.



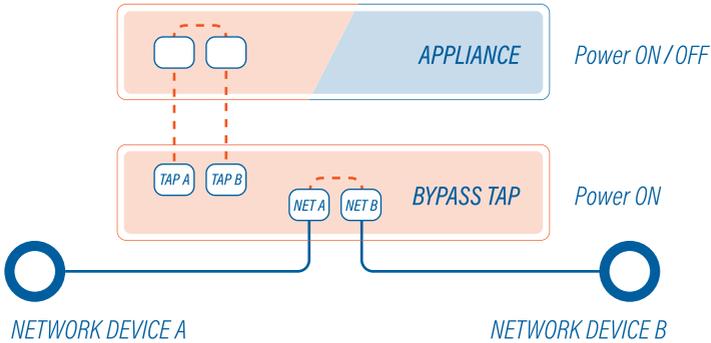
### Case 6 - Power Failure, Bypass ON

If power failure occurs and In case of power failure is set to ON (fail open), the physical bypass circuit (optical relay) inside the F1-10G-BP unit is activated. The network path between Network Device A and Network Device B remains **functional**.



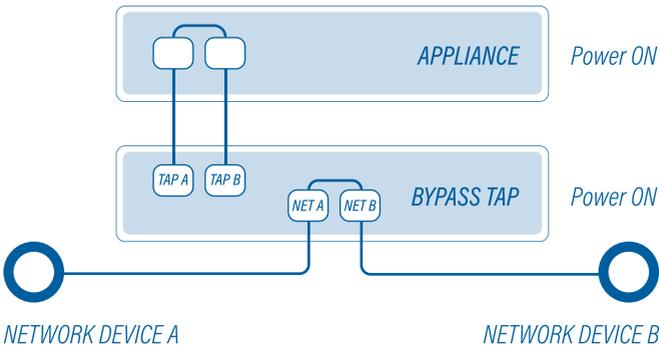
### Case 7 - Power Failure, Bypass OFF

If power failure occurs and In case of power failure is set to OFF (fail close), the physical bypass circuit (optical relay) inside the F1-10G-BP will not be activated resulting in a link **failure** between Network Device A and Network Device B.



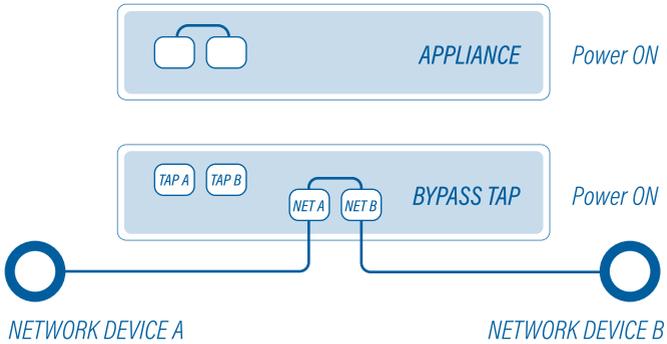
### Case 8 - Manual Bypass, TAP ON

If both Manual Bypass and TAP Mode are set to ON, the physical bypass circuit (optical relay) inside the F1-10G-BP is activated. The network path between Network Device A and Network Device B remains **functional**, while the traffic is still being forwarded to the appliance through Tap A and Tap B ports.



### Case 9 - Manual Bypass, TAP OFF

If Manual Bypass is set to ON but TAP Mode is set to OFF, the physical bypass circuit (optical relay) inside the F1-10G-BP is activated. The network path between Network Device A and Network Device B remains **functional**, but there is no traffic forwarded to the appliance.



## *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.

## *COPYRIGHT*

This publication, including all photographs and illustrations, is protected under international copyright laws, with all rights reserved. Neither this manual, nor any of the material contained herein, may be reproduced without written consent of the author.

## *TRADEMARKS*

The trademarks mentioned in this manual are the sole property of their owners.

PROFITAP HQ B.V. - High Tech Campus 9  
5656 AE Eindhoven - The Netherlands

[sales@profitap.com](mailto:sales@profitap.com)  
[www.profitap.com](http://www.profitap.com)

© 2018 Profitap — v1.1-06

