F4-10G-BP BYPASS TAP

INSTALLATION AND CONFIGURATION MANUAL

BRINGING CLARITY INTO NETWORKS.
ANYTIME. ANYWHERE.

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

www.profitap.com

or by email:

info@profitap.com

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

http://www.profitap.com/resource-center/

TABLE OF CONTENTS

INSTALLATION

1. UNPACKING & INSTALLATION

1.1 Unpacking

Carefully unpack all the items supplied with the F4-10G-BP and retain
the packaging for later use:

- 1 x F4-10G-BP main unit
- 2 x 12V 4.5A Power supply
- 1 x DB9 to RJ45 Console cable

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

1.2 Installation

Up to 3 x F4-10G-BP units can be installed in a standard 19″ rack, using the rackmount
chassis kit (ARKB-1U).

To install the unit(s) in the rack, follow these steps:

- Slide the rackmount chassis kit in desired rack location and secure it to the
  rack using appropriate rack screws.
- Slide the unit(s) in the rackmount chassis kit and secure them using the units'
  thumbscrews.
- Make sure the rack is properly grounded.

2. PRODUCT OVERVIEW

Active in-line security appliances are single points of failure in any network. The F4-10G-BP bypass TAP monitors the health of your appliance over copper or fiber connections and removes any point of failure by automatically switching traffic in a bypass mode, to keep the network critical link up.

The F4-10G-BP features set include:

- Link Failure Propagation (LFP)
- Bidirectional Heartbeat (ping signal to and from the monitored appliance)
- Predefined and custom Heartbeat signal type
- Heartbeat control
- Administration via HTTP/SHH/CLI
- Comprehensive configuration and behavior
- 40G 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 50µs to 4s (default value is 1s).

HEARTBEAT FAILURE TIMEOUT

The Heartbeat failure timeout can be set from 50µs 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.

> **Note:** Heartbeat rate and timeout are configurable based on different metrics (nanoseconds, microseconds, milliseconds, seconds, minutes)

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).
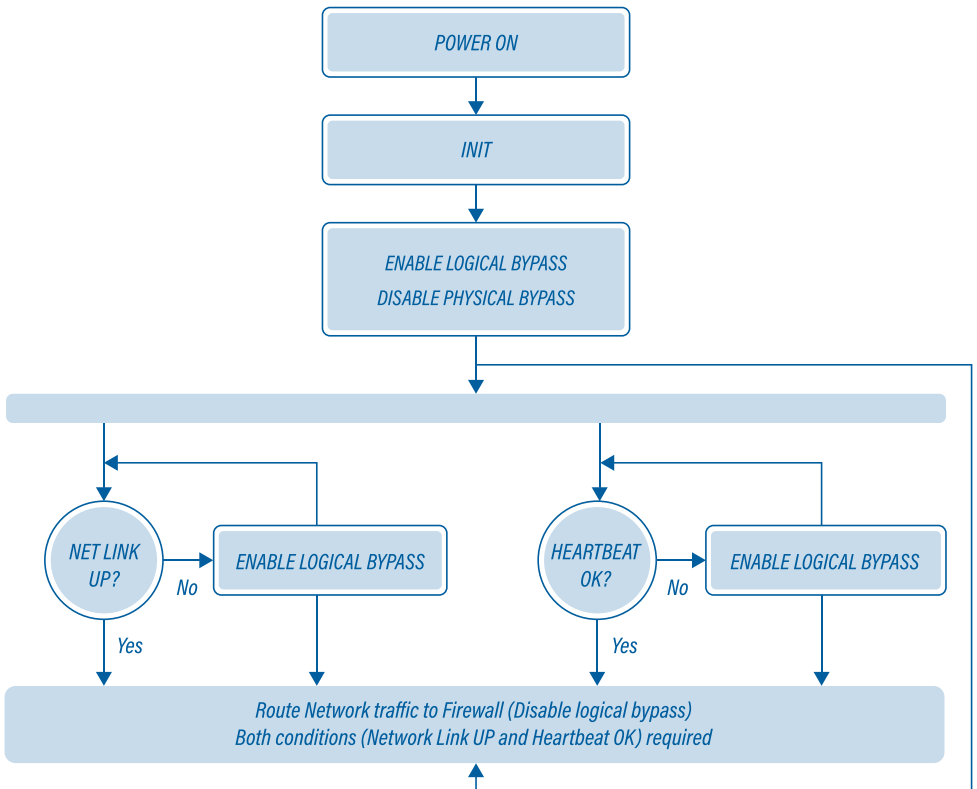
HEARTBEAT PRIORITY

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 F4-10G-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 F4-10G-BP operates on. For more information regarding operation scenarios, please go to Operation Use Cases chapter.

```
                        POWER ON

                          INIT

              ENABLE LOGICAL BYPASS
              DISABLE PHYSICAL BYPASS


   NET LINK          ENABLE LOGICAL BYPASS        HEARTBEAT        ENABLE LOGICAL BYPASS
    UP?        No                                  OK?        No

         Yes                                          Yes

            Route Network traffic to Firewall (Disable logical bypass)
            Both conditions (Network Link UP and Heartbeat OK) required
```
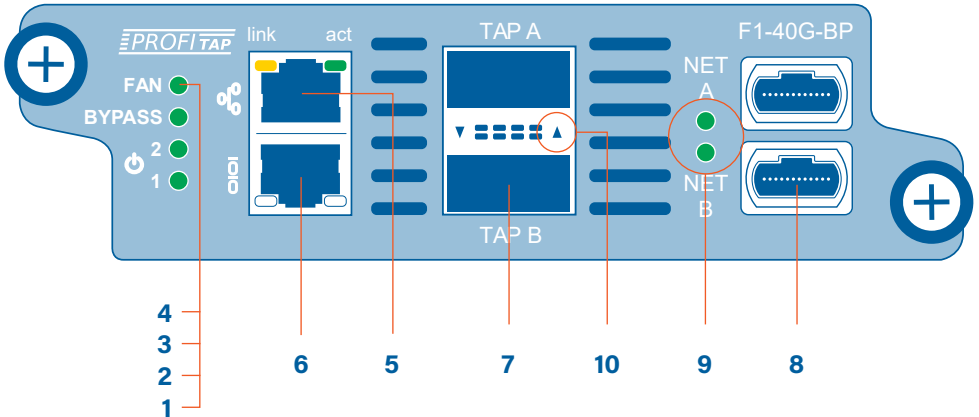
2.1 Technical and Electrical Specifications

Dimensions (WxDxH): 120 x 315 x 40 mm — 4.7 x 12.4 x 1.6 in

Weight: 1360 g — 2.99 lb

Power requirement: 12V 4.5A

2.2 Front View

1, 2	PSU1, PSU2 Status LEDs	**7**	QSFP+ interfaces, accepting copper/fiber modules, used for connecting to monitored security appliances. (40Gbps)
3	Bypass Status Led		
4	Fan Status LED	**8**	In-Line network ports, accepting MTP optical fiber connections. (40Gbps)
5	Ethernet management interface 10 / 100 Mbps		
6	Serial Management interface 115200 / 8 / 1 / n	**9**	Rx / Tx activity LEDs for NET A & NET B
		10	Rx / Tx activity LEDs for TAP A & TAP B

2.2 Rear View
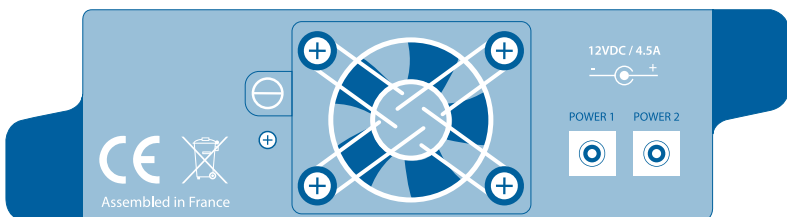
2.4 LED Functionality

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	Green	PSU2 connected
	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 powers on when one of the power supplies is connected to the main power.

► **Note:** The use of both power supplies is recommended to ensure fail-safe operation.

The F4-10G-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 F4-10G-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 any terminal software (xterm, PuTTY, etc.), use the following connection settings: 115200 baud rate, 8 bit, no parity, 1 bit stop. Login, using the following credentials:

   - ◉ 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 F4-10G-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 F4-10G-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
- Administration
- 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.

	Bypass 1		Bypass 2		Bypass 3		Bypass 4	
	Link	Speed	Link	Speed	Link	Speed	Link	Speed
NET A	Down	10G	Down	10G	Up	10G	Down	10G
NET B	Down	10G	Down	10G	Up	10G	Down	10G
TAP A	Up	10G	Up	10G	Up	10G	Up	10G
TAP B	Up	10G	Up	10G	Up	10G	Up	10G

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 Settings

The Bypass page represents the heart of F4-10G-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.
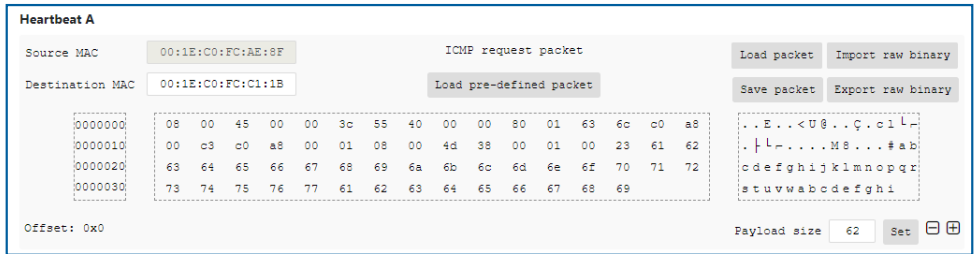
IN CASE OF HEARTBEAT FAILURE: This selection allows the user to program the bypass behavior in case of a Heartbeat timeout. The timeout is also user customizable in the Heartbeat failure timeout field.

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 Heartbeat packets (A,B) can be either edited in the HEX editor or selected from a list of pre-defined signatures. Load pre-defined packet

⊙ **[+] [-]** 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.

Heartbeat A

Source MAC	00:1E:C0:FC:AE:8F							ICMP request packet								
Destination MAC	00:1E:C0:FC:C1:1B							Load pre-defined packet								

Load packet   Import raw binary
Save packet   Export raw binary

```
0000000   08  00  45  00  00  3c  55  40  00  00  80  01  63  6c  c0  a8    ..E..<U@..ç.cl └─
0000010   00  c3  c0  a8  00  01  08  00  4d  38  00  01  00  23  61  62    .├└─....M8...#ab
0000020   63  64  65  66  67  68  69  6a  6b  6c  6d  6e  6f  70  71  72    cdefghijklmnopqr
0000030   73  74  75  76  77  61  62  63  64  65  66  67  68  69            stuvwabcdefghi
```

Offset: 0x0

Payload size 62 Set ⊟ ⊞

HEARTBEAT RATE: Allows the user to change the rate at which Heartbeat packets are sent to the monitored appliance. The rate can be set in nanoseconds, microseconds, milliseconds, seconds, or minutes.

HEARTBEAT FAILURE TIMEOUT: Allows the user to set a specific time interval that will be allowed to elapse between sending and receiving a Heartbeat packet. The interval can be set in nanoseconds, microseconds, milliseconds, seconds, or minutes. If this interval is exceeded, the behavior is interpreted as failure and the Bypass is set to ON or OFF, depending on how the "IN CASE OF HEARTBEAT FAILURE (timeout)" option is configured.

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.

> ► **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.

⚙ *1.5 Administration*

The Administration 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 Firmware 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.

The SNMP tab allows the users to enable and configure the Simple Network Management Protocol (SNMP).

SNMP v1 and v2c use a community string for authentication, sent as clear text, an approach less than ideal, security wise. This is why SNMPv3 has been developed, improving on v1 and v2c by introducing the following security features:

- Message integrity: prevents packets to be intercepted or tampered with during transit.
- Authentication: ensures the message comes from a valid source.
- Encryption: scrambles the contents of the packets to avoid deciphering in case of interception by third parties.

The SNMP service allows users to configure the following security options:

- SNMP communities: (for SNMP v1 and v2c) Allows adding, deleting or editing SNMP communities, used for establishing trust without standard credentials.
- SNMP users: (for SNMP v3 only) Allows adding, deleting and editing SNMP users, including their security level and authentication/privacy type and hash.
- SNMP trap_sinks: Allows adding, deleting and configuring hosts which SNMP notifications (traps) will be sent to.

> ► **Note:** Every time an entry is added, the change must be applied by clicking ✔ . Navigating away from the SNMP tab without applying changes will result in losing the latest changes.

The SNMP management information base (MIB) used for managing the entities in the secured accessed network can also be downloaded from this tab, by clicking on

⬇ Download the MIB files

1.6 Logs

The Logs page displays Bypass and System logs for the specified period. To change the period, select the desired *From* and *Until* dates, and click the *View* button. The displayed log files can be downloaded either individually, by clicking the *Download* button next to the desired file's name, or as a single file, by clicking the *Download range* button.

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:

date_time	**show:** Displays the date.
	set: Allows the user to set the date and time.

factory_reset   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.

> ► **Note:** Another way of resetting the device to factory defaults is to interrupt the boot sequence and press a key when prompted:"F4-10G-BP failed to boot on last attempt and has now successfully booted in recovery mode. Press any key within 10 seconds to install the base firmware or wait for the unit to attempt a new boot sequence."

hostname   Uniquely identifies each unit with a label, a useful feature in case multiple devices are connected within the same network or to the same host machine, having the remote_logging feature enabled.

firmware_update   Allows the user to update the system's firmware from an URL address.

port_speed   **show:** Displays the fiber link speed. It can be 1G, 10G and 40G.
set: Allows the user to change the fiber link speed between 1G, 10G and 40G.

network settings

edit: 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.

interface.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.

interface.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.

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

reboot

Immediately reboots the system, keeping all configurations intact.

remote_logging

In case a rsyslog service is set up on the connected network, enabling this option will result in sending the bypass log or the system log to the remote rsyslog service.

disable/enable: Disables or enables the feature.

show: Displays whether the feature is enabled or disabled.

targets: Allows the user to configure the remote machine running the rsyslog service which the bypass log or the system log will be sent to.

bypass_log.show	Displays all bypass events related logs and their timestamps.
show_legal_info	Displays the Product Legal Information.
system_log	**monitor:** Displays all system related logs and their timestamps in real time. **show:** Displays all system related logs and their timestamps.
snmp	Allows the user to configure the Simple Network Management Protocol. SNMP v1 and v2c use a community string for authentication, sent as clear text, an approach less than ideal, security wise. This is why SNMPv3 has been developed, improving on v1 and v2c by introducing the following security features:

- Message integrity: prevents packets to be intercepted or tampered with during transit.
- Authentication: ensures the message comes from a valid source.
- Encryption: used for scrambling the contents of the packets to avoid deciphering in case of interception by third parties.

communities: (for SNMP v1 and v2c) Allows users to add, delete or edit SNMP communities, used for establishing trust without standard credentials.
users: (for SNMP v3 only) Allows adding, deleting and editing SNMP users, including their security level and authentication/privacy type and hash.

LEVEL	ENCRYPTION METHOD	AUTHENTICATION KEY	BEHAVIOR
no auth	*NO*	*USERNAME ONLY*	*Authentication is done using a username only.*
auth	*NO*	*PASSPHRASE IN MD5 OR SHA*	*The authentication is done using the MD5 or SHA hash of the passphrase.*
priv	*DES or AES*	*MD5 or SHA*	*The authentication is done using the MD5 or SHA hash of the passphrase. The channel is encrypted using DES or AES algorithms.*

disable/enable: Disables or enables the SNMP support.

> ► **Note:** At least one user/community/trap sink must be present before SNMP support can be enabled.

show: Displays whether the feature is enabled or disabled.

trap_sinks: Allows adding, deleting and configuring hosts which SNMP notifications (traps) will be sent to.

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.

users

show: 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 F4-10G-BP 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.
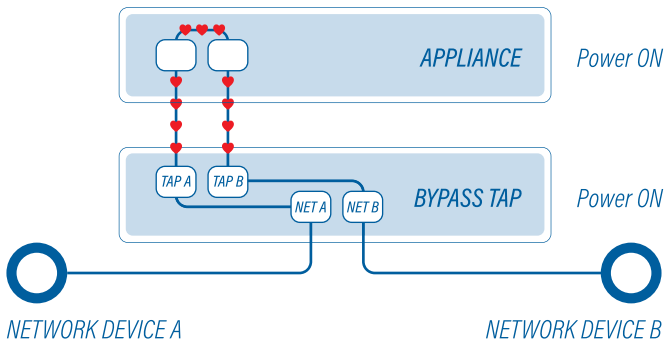

CASE 2 - HEARTBEAT FAILURE, BYPASS ON

If the heartbeats packets are sent to the appliance but are not forwarded back, and the **Bypass in case of heartbeat failure** option 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.
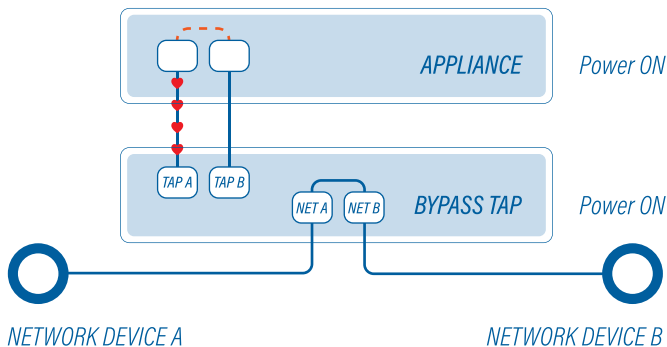
CASE 3 - HEARTBEAT FAILURE, BYPASS OFF

If the heartbeat packets are sent to the appliance but are not forwarded back, and the **Bypass in case of heartbeat failure** option 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.

APPLIANCE — Power ON

TAP A TAP B NET A NET B BYPASS TAP — Power ON

NETWORK DEVICE A
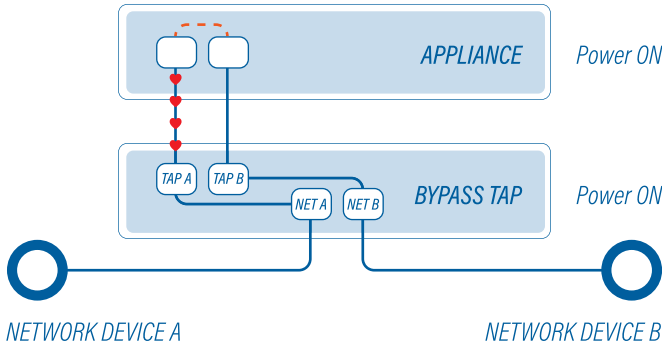
NETWORK DEVICE B

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** option 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.

APPLIANCE — Power OFF

TAP A TAP B NET A NET B BYPASS TAP — Power ON

NETWORK DEVICE A

NETWORK DEVICE B
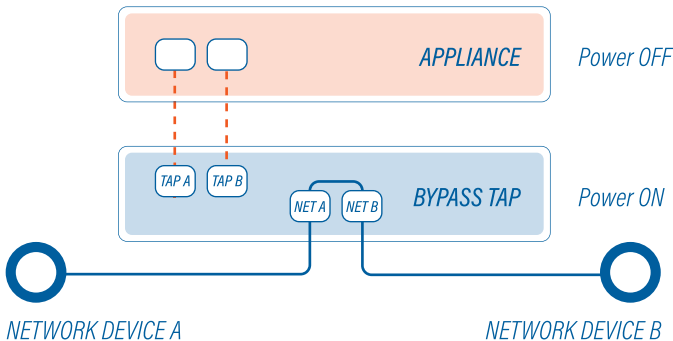
CASE 5 - APPLIANCE LINK DOWN, BYPASS OFF

If the Appliance is unpowered or the ports are disconnected, and the **In case the TAP link is DOWN** option 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.
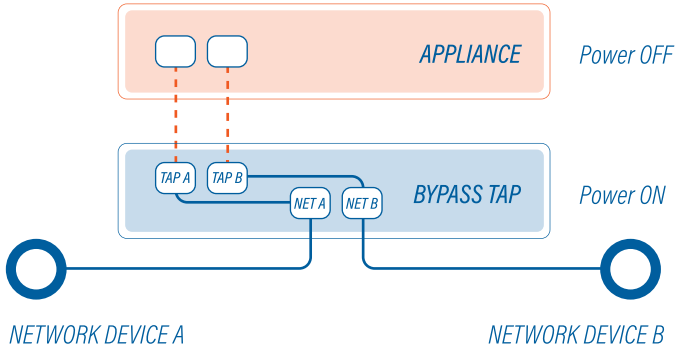

CASE 6 - POWER FAILURE, BYPASS ON

If power failure occurs and **In case of power failure** option is set to ON (fail open), the physical bypass circuit (optical relay) inside the F4-10G-BP unit is activated. The network path between Network Device A and Network Device B remains functional.
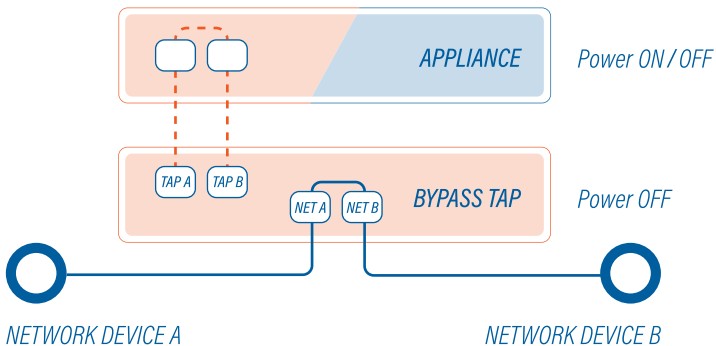
CASE 7 - POWER FAILURE, BYPASS OFF

If power failure occurs and **In case of power failure** option is set to OFF (fail close), the physical bypass circuit (optical relay) inside the F4-10G-BP will not be activated resulting in a link failure between Network Device A and Network Device B.
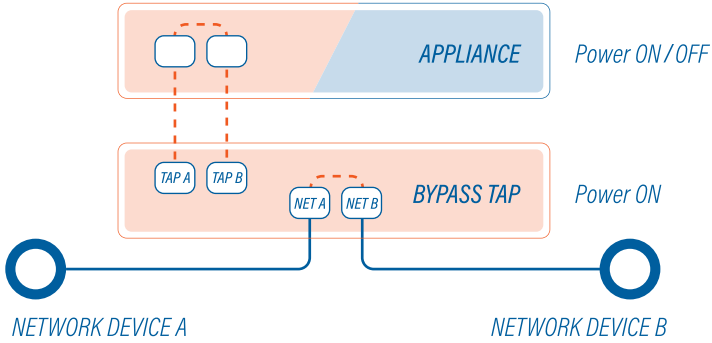

CASE 8 - MANUAL BYPASS, TAP ON

If both **Manual Bypass** and **TAP Mode** options are set to ON, the physical bypass circuit (optical relay) inside the F4-10G-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.
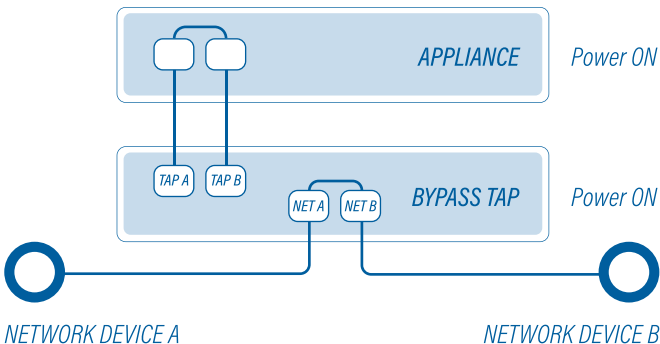
CASE 9 - MANUAL BYPASS, TAP OFF

If the **Manual Bypass** option is set to ON but **TAP Mode** option is set to OFF, the physical bypass circuit (optical relay) inside the F4-10G-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.
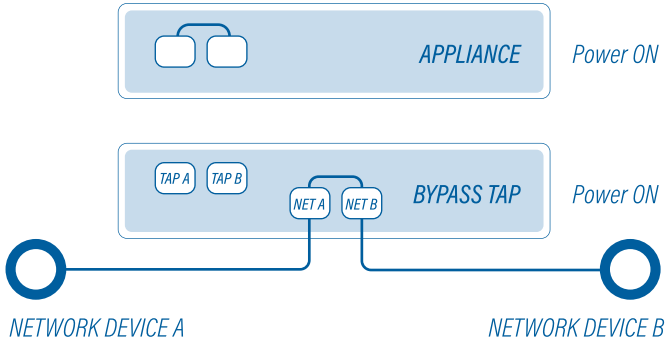
Legal

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.