



**RCS Network Injector**

Deployment Manual

Important Notice

HT s.r.l. shall bear no responsibility or liability to a client or to any person or entity with respect to liability, loss or damage caused or alleged to be caused directly or indirectly by any HT s.r.l. product. This includes, but is not limited to, any interruption of service, loss of business or anticipatory profits or consequential damage resulting from the use or operation of any HT products. Information in this document is subject to change without notice and does not represent a commitment on the part of HT s.r.l.   
The systems described in this document are furnished under a license agreement or non-disclosure agreement.

All information included in this document, such as text, graphics, photos, logos and images, is the exclusive property of HT s.r.l. and protected by international copyright laws. Permission is granted to view and photocopy (or print) materials from this document for personal, non-commercial use only. Any other copying, distribution, retransmission or modification of the information in this document, whether in electronic or hard copy form, without the express prior written permission of HT s.r.l., is strictly prohibited. In the event of any permitted copying, redistribution or publication of copyrighted material, no changes in, or deletion of, author attribution, trademark legend or copyright notice shall be made.

All contents of this document are: Copyright © 2014 HT s.r.l. All rights reserved.

Document Approval

| Revision | Author(s) | Release Date |
| --- | --- | --- |
| 1.0 | FAE Team | 13th February 2014 |
|  |  |  |

**Table Of Contents**

1. Overview 5

1.1 Network Injector Appliance Capabilities 5

2. Preliminary Considerations 6

3. Cable Interconnection 8

3.1 Single Path network Integration 8

3.1.1 Installation with SPAN on single linked network 9

3.1.2 Installation with Ethernet TAP on single linked network 10

3.1.3 Installation with Fiber TAP on single linked network 11

3.2 Redundant Path network Integration 12

3.2.1 Installation with SPAN on double linked network 13

# Overview

HackingTeam *Network Injector Appliance* (NIA) is a hardware appliance for monitoring target’s Internet traffic and install RCS Agents over their Internet connection, using an innovative patent technology that allows live streaming injection and executable melting without being inline.

The purpose of this document is to provide instructions about how to properly interconnect the NIA in the ISP Infrastructure.

## Network Injector Appliance Capabilities

The Appliance is engineered to be easily integrated in most common network implementations, safeguarding the network by service interruption and guaranteeing full network flows visibility.

The key features include:

* Installation at Internet Service Provider’s premises;
* Supports Fiber and Copper channels;
* Compatible with redundant network paths;
* Available also for 1GB and 10GB lines;
* Doesn’t need to be installed inline, thanks to a patented technology it provides:
  + noninvasive and surgical attacks, excluding all side effects of inline appliances;
  + no impact on the ISP in case of failures;
* Easy management even when multiple NIA’s are deployed.

# Preliminary Considerations

The deployment of NIA should be realized considering the positioning of appliance into the ISP infrastructure as described in chapter 2 ”ISP deployment and positioning” of the “Network Injector Appliance Whitepaper” document and the specific network implementation of the ISP branch that provides internet connectivity to the target.

By using dedicated wire-speed network interfaces, the NIA is compatible with many physical network links, and is capable of monitoring them even when running at full speed.

In relation to ISP network implementation, the main constraints to check are the following:

* Type of links (Ethernet or Fiber)
* Speed of links (100Mb up to 10Gb)
* Network topology on deployment path

According to this constraints the deployment should be integrated in the ISP in two ways:

|  |  |
| --- | --- |
| Connection | Description |
| SPAN Port | Most enterprise switches copy the activity of one or more ports through a Switch Port Analyzer (SPAN) port, also known as a mirror port. An analysis device can then be attached to the SPAN port to access network traffic. |
| TAP | A TAP (Test Access Point) is a passive splitting mechanism installed between a ‘device of interest’ and the network. TAPs transmit both the send and receive data streams simultaneously on separate dedicated channels, ensuring all data arrives at the monitoring device in real time. |

The two possibilities has different peculiarities to be evaluated with the ISP technicians:

|  |  |  |
| --- | --- | --- |
| Connection | Comparsion | |
|  | **Favor** | **Against** |
| SPAN Port | * Faster to implement * Could be used with redundant 10Gb paths (if the effective aggregated load is equal or less than 10Gb) | * If the SPAN port becomes overloaded, frames are dropped * Hardware and media errors are dropped * May alter timing of the frames * May introduce delay * CPU use may significantly increase due to port use * The SPAN port on the switch may not be present or unavailable (if already in use) |
| TAP | * Guarantees complete capture even when the network is 100 percent saturated * Captures everything on the wire, including hardware and media errors * Eliminates the risk of dropped packets | * Slower to implement * May require service downtime for the ISP * Could not be used in redundant 10Gb paths |

The delivery of NIA will provide all components to successfully integrate the solution in the most common network implementations.

In some case, the ISP will not allow the installation of a TAP device in their network so the SPAN configuration is the only one possibility.

1. Due to the importance of the appliance and to the large number of variables that must be analyzed during the installation, Hacking Team always provides a preliminary technical support to understand, together with the client, if the installation can take place at the ISP selected.

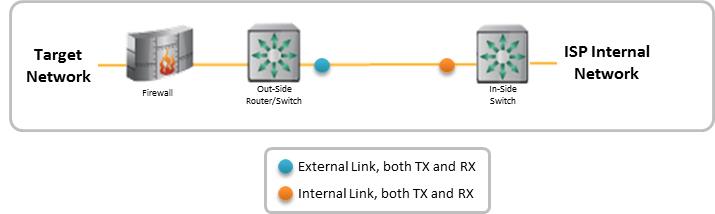
# Cable Interconnection

The present chapter describes how to interconnect the physical cables/links to the NIA monitoring Interface (DAG Card 9.2).

Explanations and diagrams assume the injection will always be performed through a secondary interface

## Single Path network Integration

If the network implementation of the ISP branch that provides internet connectivity to the target is single linked, the NIA interconnection topology will be different due to the type of interconnection (SPAN or TAP) and the type of the link (Ethernet or Fiber).



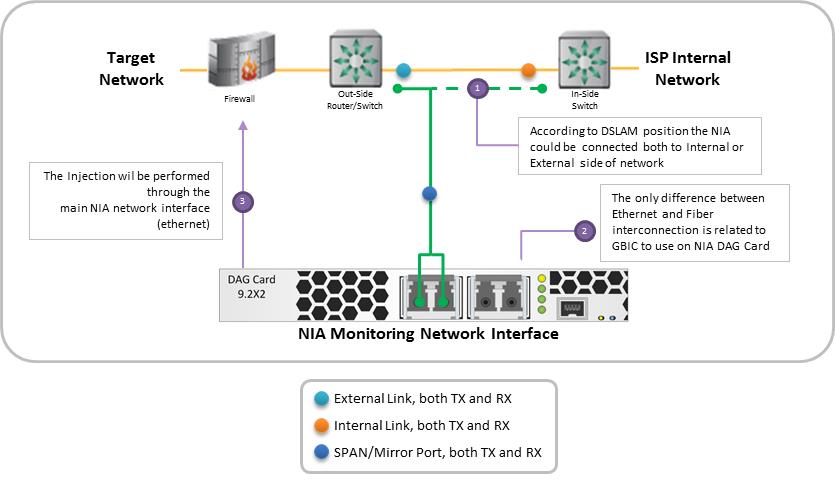
Example of network interconnection before NIA Installation on classical network (single link)

## Installation with SPAN on single linked network

The integration with SPAN port on single link is the simplest way to integrate the NIA within the IPS infrastructure.

According with NIA positioning in relation to DSLAM (See: ”ISP deployment and positioning” of the “Network Injector Appliance Whitepaper” document) the usage of SPAN could be done both on internal or external side of the network and the installation topology will not change in relation to link type.

The main driver which could drive the choice is the availability of a SPAN port in a properly loaded ISP network device.



Example of NIA installation with SPAN Port in a classical network (single link)

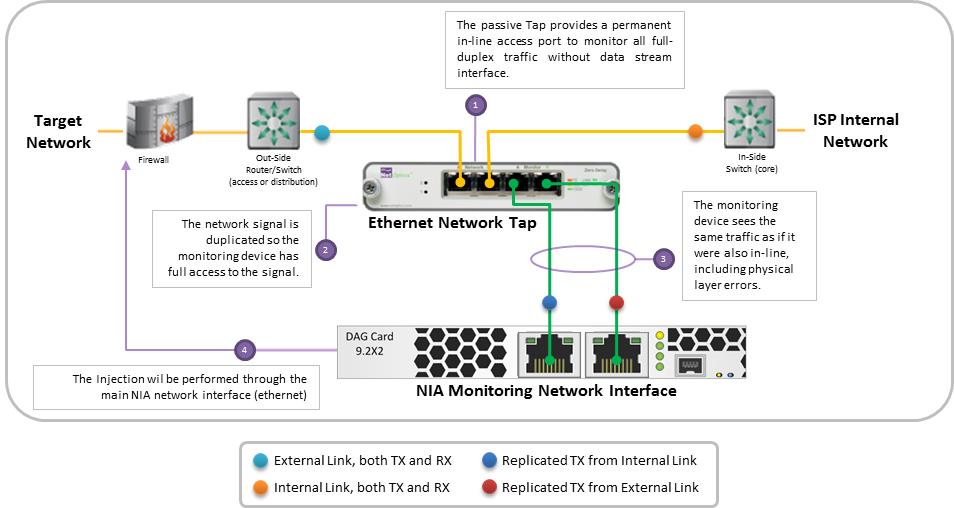
## Installation with Ethernet TAP on single linked network

The use of TAP on single linked network will introduce some difference in installation topology in relation to the type of link and as consequence with the type of TAP needed.

Basing on specific low level port configuration capabilities of network devices of ISP (switch or router) crossover cables may be needed for interconnection between ISP network devices and TAP.

Generally if both of the devices connected to the TAP are 10/100base T devices that do not support Automatic MDI/MDI-X configuration, then specific cabling must be used in order to maintain a successful link.

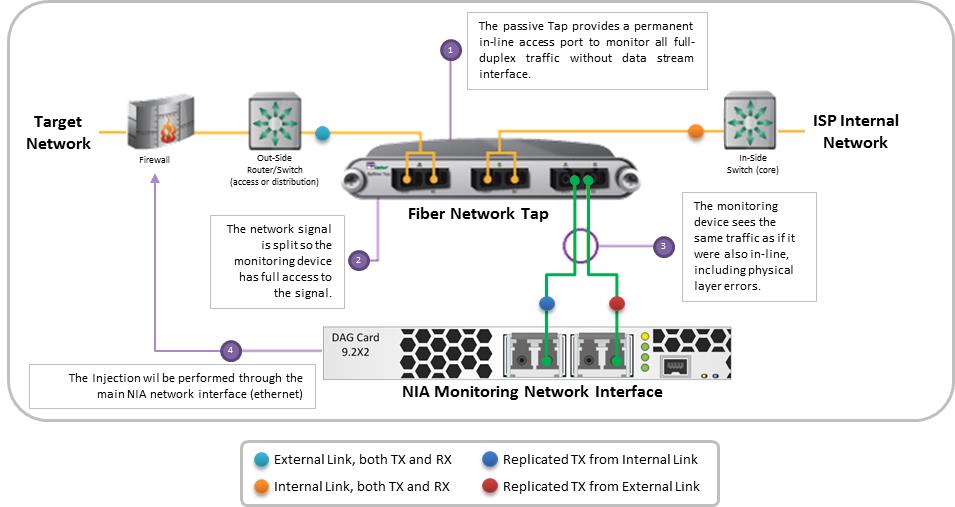
* If connecting to switches of Hubs, use CAT5 RJ45 may be needed cross-over cables;
* If connecting to routers or NICs, use CAT5 RJ45 usually will be used straight-over cables.



Example of NIA installation with Ethernet TAP usage in a classical network (Ethernet single link)

## Installation with Fiber TAP on single linked network

The Fiber TAP splits and provides to the monitoring interface only the TX side of both links. For this reason the DAG Card of NIA must be properly configured (disabling the laser) to receive the signal also if the GBIC interfaces are not able to negotiate a link.

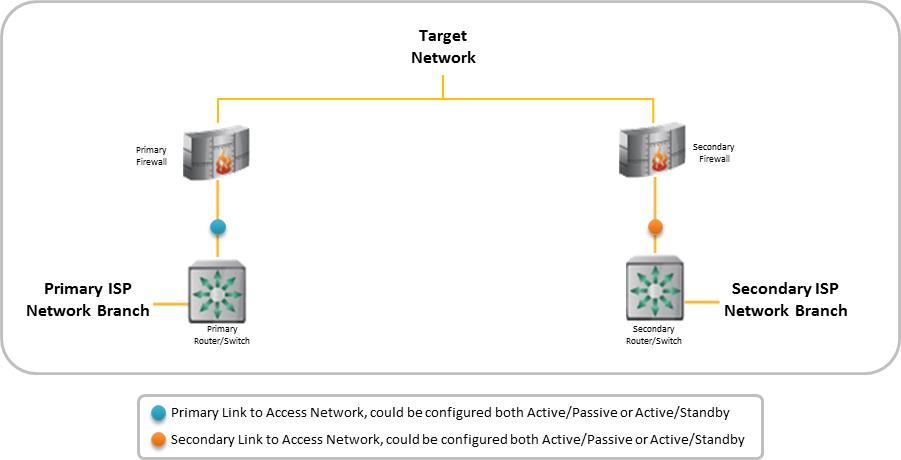


Example of NIA installation with Fiber TAP usage in a classical network (single link)

## Redundant Path network Integration

If the network implementation of the ISP branch that provides internet connectivity to the target is redundant (double linked), the NIA interconnection topology will be the same both with Ethernet or Fiber links.

With redundant paths, the SPAN is the only integration supported.

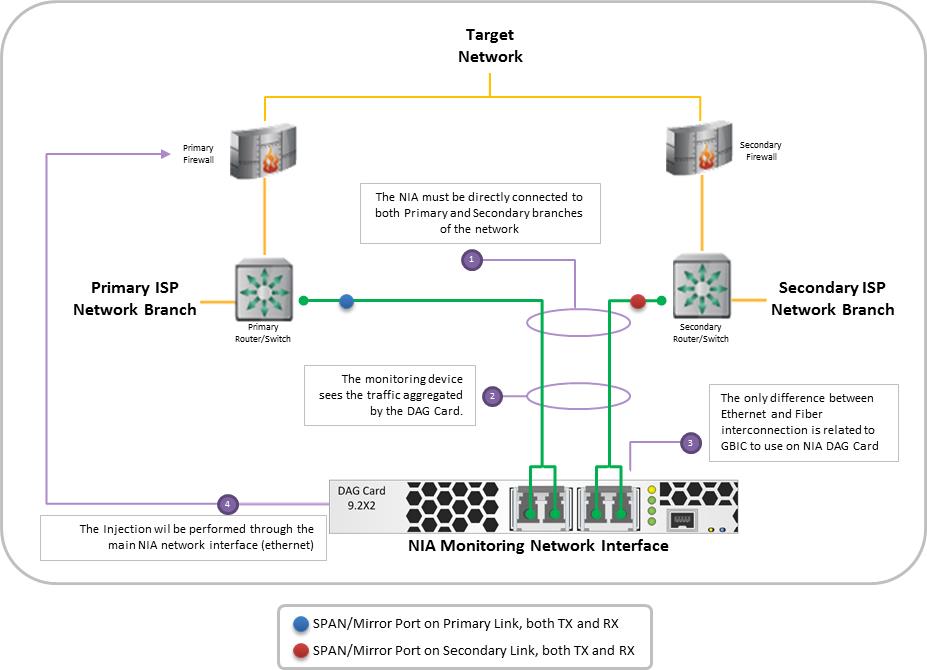


Example of network interconnection before NIA Installation in a redundant network (double link)

## Installation with SPAN on double linked network

According with NIA positioning in relation to DSLAM (See: ”ISP deployment and positioning” of the “Network Injector Appliance Whitepaper” document) the usage of SPAN could be done both on internal or external side of the network and the installation topology will not change in relation to link type.

In case of Ethernet links refer to “3.1.2 Installation with Ethernet TAP on single linked network” for tips about cables needed.



Example of NIA installation with SPAN in a redundant network (double link)