IXIA IBYPASS 40-10

Protecting Critical Infrastructure

Ixia iBypass 40-10 is an intelligent bypass switch that provides inline tool protection for inline network link deployments. The iBypass 40-10 augments network-monitoring capability through the use of microsecond resolution heartbeat packets, SNMP traps, field upgradable software, and an easy-to-use Web UI. The iBypass 40-10 allows monitoring of four 10GbE links or daisy-chaining multiple tools on 10GbE links.

Failsafe Inline Tool Deployment

Today's networks are delivering more services and carrying greater amounts of multi-protocol traffic at higher data rates. A single set of wires now carries data, voice and streaming video simultaneously. Increased security threats and tighter regulatory compliance requirements further complicate network operations. Monitoring tools and security tools need to be deployed inline to inspect every packet and block incoming threats before these threats affect the network and potentially disrupt business.

Deployment of any inline tool in the network carries the risk of the tool becoming a point of failure. Should the inline tool become unavailable it can bring the network link down, making a critical segment of the network unavailable and affecting uptime. To avoid this risk, customers need a fail- safe solution that can protect the network from tool failures while allowing inline tools to protect the network from incoming threats.

Highlights

- Bypass up to four 10GbE links

- Protects network availability when deploying inline tools

- Forced Bypass, and Bypass Off (no auto-recovery)

- Supports up to 9 different HA deployment types

- Remote management through SSH V2, Web Interface (HTTPS) and SNMP Browsers

- Bi-directional Heartbeats

- SNMP V2c and SNMP V3 supported

- SNMP traps indicate status changes for system, link, power, and threshold

- Audit Logs collect user and system changes

- Field upgradable software and firmware

- Field-replaceable, hot-swappable fans and power supply

- View size and time of the peak traffic

- View status for power, link, activity, and utilization alarms

- Management and network cables included

- LCD display

KEYSIGHT TECHNOLOGIES

The iBypass 40-10 switch addresses this need by sitting in front of any inline security or monitoring tool and guaranteeing network availability. The iBypass switch essentially serves as a bridge between the network and the inline tool. It lets the inline tool inspect and control network traffic as needed while protecting the network from failures within the tool itself.

Automatic Protection and Recovery

The iBypass switch continuously checks the responsiveness of the inline tool by sending it "heartbeat" packets, expecting to receive those packets back. If the iBypass switch detects that the tool is not responding, it will bypass the inline tool, allowing network traffic to flow without interruption. Should that happen, the iBypass switch will issue an alert to indicate that the tool became unavailable, allowing network or security personnel to take appropriate actions.

The iBypass switch will continue to send heartbeat packets to the inline tool even after the tool stopped responding. As soon as the tool becomes operational again, the iBypass will re-route traffic back through the tool to ensure that the tool is continuing to monitor and/or protect the network.

Flexible Deployments

Having an iBypass switch deployed in front of inline tools provides greater deployment flexibility. When the inline tool needs to be taken out for maintenance the iBypass switch can be configured to bypass the inline tool and let network traffic flow uninterrupted. Once maintenance is complete, the iBypass can route traffic back through the upgraded tool. The 40-10 can be configured as either 4 independent bypass switches or can be configured so that it operates as a more complex multi-segment bypass switch that offers varying degrees of High Availability modes such as ACTIVE-ACTIVE (where two tools are deployed in series) or ACTIVE-STANDBY.

Network Intelligence

The iBypass 40-10 includes Remote Monitoring (RMON) statistics and Ixia ProPush™ statistics. ProPush statistics provide key network statistics every second. The combination of the many RMON and ProPush statistics provides great visibility into the network and allows integration with existing network management tools.

Smart Management

The iBypass 40-10 is a fully managed device and allows the user to view and change settings through a user- friendly Web UI, CLI, and SNMP browsers. Remote management security is provided through Role Based User Access (RBAC), 1024-bit SSL encryption, HTTPS, SNMPV3, SSH V2, and an IP Access List and to prevent unwanted access to management interfaces the iBypass can be configured to disable access to each of the interfaces. In the event there are system, link, power, or threshold changes the iBypass issues SNMP traps that are directed to the desired management devices, set in any of the interfaces.

The iBypass comes with different LED indicators for power, link, bypass status, and utilization threshold alarms. The LCD provides peak and real-time network utilization information for both of the network ports enhancing local, on-site, device monitoring options.
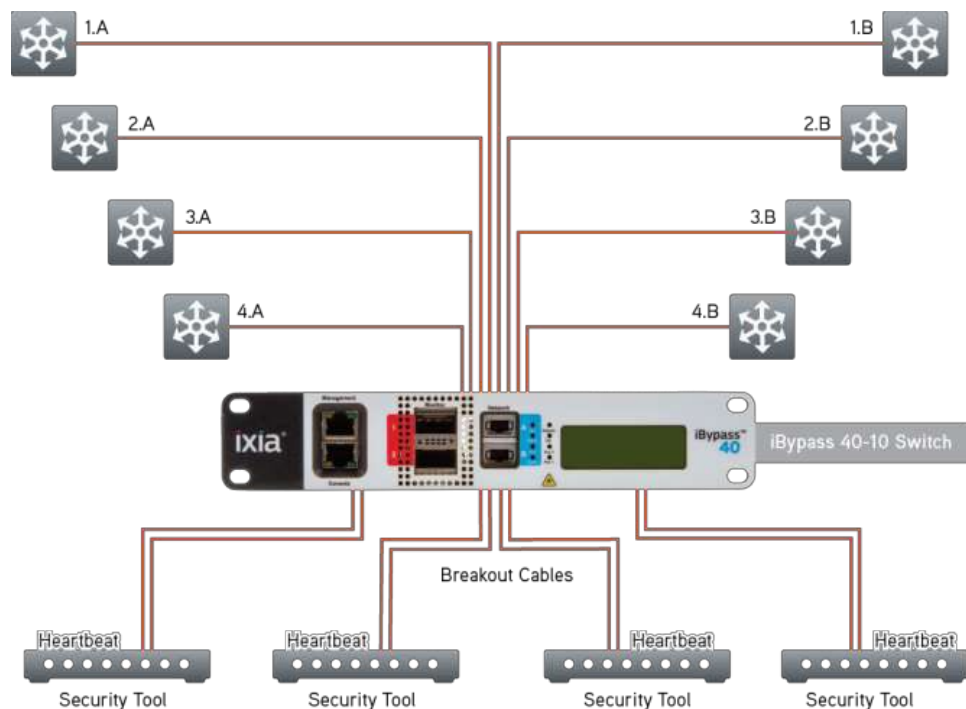
Centralized Management

The iBypass is integrated into the Ixia Indigo Pro Management Platform which is a highly versatile tool for managing and monitoring the multitude of Net Optics devices from a single screen. The easy-to-use graphical user interface makes configuring multiple iBypass switches simple.
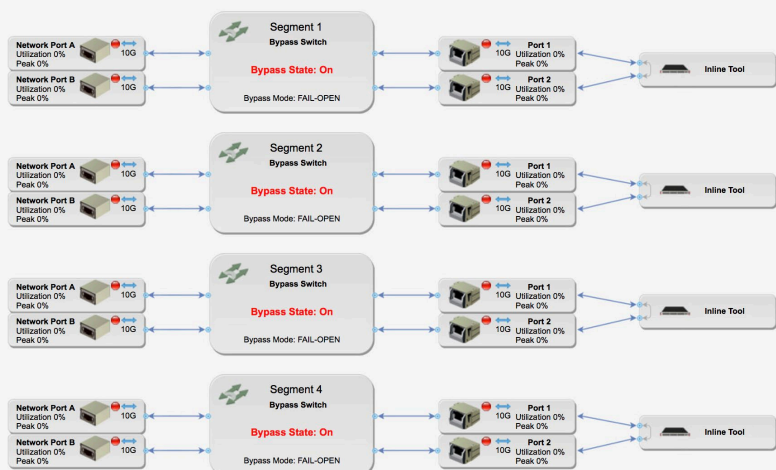
Operating Modes

iBypass 40-10 supports the following modes:

- **Tap** – In this mode the iBypass 40-10 operates as a duplex breakout Tap, copying the traffic received at Network Port A to Monitor Port 1, and traffic received at Network Port B to Monitor Port 2.

- **Fail Open** - When the number of Heartbeat retries is exceeded, monitor link is brought down, and traffic is routed through the network ports.

- **Fail Close** - With this mode, when the heartbeat packet is not detected on either monitor ports, network ports are disabled. Network ports are enabled after the in-line device has responded to the heartbeat.

- **Force Bypass Off** - This mode ensures that network traffic flows uninterruptedly to monitor ports back and forth regardless of Heartbeat status.

- **Force Bypass On-Open** - In this mode the device is forced into bypass mode regardless of the heartbeat status. This mode allows users to intentionally bypass the connected tool, for example to upgrade the tool's software without interruption to network traffic.

- **Force Bypass On-Closed** - This mode instructs the system to not let traffic ingress port A nor ingress port B. This mode allows users to intentionally stop network traffic while traffic cannot be inspected by the connected tool, for example to upgrade or otherwise maintain the tool's software.

Diagram showing use of breakout cables with iBypass 40-10.

Dashboard view

Configuration view

Specifications	
Operating	• Operating Temperature: 0˚C to 40˚C • Relative Humidity: 10% min, 95% max, non-condensing
Non-Operating	• Storage Temperature: -10ºC to 70ºC • Relative Humidity: 10% min, 95% max, non-condensing
Mechanical	• Dimensions: 1.724" high x 24" deep x 9.5" wide • Weight: 2.25 lbs.
Cable Interface	• Multimode SR Model: Fiber Core: 50µm; Wavelength: 850nm • Single Mode LR Model: Fiber Core: 8.5µm; Wavelength: 1310nm
Electrical	• AC Power Supply • Input: 100-240VAC, 1A, 47-63Hz • Output: 12V, 9A • Power Dissipation 368 BTU/Hr 108W
Indicators	• (2) Link / Activity LEDs • (2) Threshold Alarm LEDs • (2) Bypass State • (2) Power LEDs • (1) LCD
Management	• Interfaces: • Serial Console: RJ45 • Management: RJ45 • Device Management: • Web UI (HTTPS), Serial Console, SSHv2, SNMPv2c, SNMPv3, Remote Software Upgrades
Network/Monitor Interface	• Network Interface: 2 x MTP 12 Fiber Adapters • Monitor Interface: 2 x QSFP+ Cages

Specifications	
Certifications	• Fully RoHS compliant • Regulatory Certifications: UL, CB, CE, FCC, VCCI

Ordering Information

I2BP-4X10-SR-50-QSFP

iBypass, 4x10GbE, SR, 50µm, QSFP+ Cages

12BP-4X10-LR-85-QSFP

iBypass, 4x10GbE, LR, 8.5µm, QSFP+ Cages

These bypass switches come complete with two 3m MTP to LC breakout cables for use on the network side of the bypass switch. These are either Single Mode or Multi Mode depending on which of the two bypass switches are ordered.

Customers must order their own breakout cables on the security tool side of the device depending on whether they are using multi-mode or single mode transceivers. Ixia can supply such cables and the part numbers are:

Part Number	Description
CKT-MTP-4LC-50-OM4	Cable Breakout Kit, MTP to 4 LCs, MM, 50um, OM4 (955-8115) (CKT-MTP-4LC-50-OM4)
CKT-MTP-4LC-85-LR	Cable Breakout Kit, MTP to 4 LCs, SM, 8.5um, (955-8162) (CKT-MTP-4LC-85-LR)

Compatible Transceivers

Part Number	Description
QSFP-PLUS-KT-50SR4	40G QSFP+ Transceiver Kit 850nm, 50um (955-8035) (QSFP+KT-50SR4)
IXQSFP-PLUS-PLR4	Ixia Transceiver kit - QSFP+ - Fiber – 40G – PLR4 – 1310m with 8.5 micron break out cable (955-8061) (IxQSFP+-PLR4)

Note that the PLR4 Single Mode transceiver kit already includes the required MTP to 4 LCS break out cable.

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT
TECHNOLOGIES