TECHNICAL OVERVIEW

Bypass FAQs

Ixia Bypass Switches are inline devices that provide fail-safe protection for inline security and monitoring devices.

Here are some frequently asked questions and answers to help you choose the right iBypass switch for your particular deployment.

General Questions on Bypass Switches

Q: Which iBypass switches can be used for copper (up to 1G speeds) and what are the maximum number of links that can be protected by each model?

A: There are three different models:

I3BP-CU3 - This protects a single copper link (up to 1Gbps)

iBypass HD (IBP-8000) - This is a modular system which can house up to 4 modules. Each copper module (DBM-100) can support up to 2 copper links, so protecting a maximum of 8 copper links.

iBypass VHD - This is a modular system which can house up to 3 modules. Each module (IM-21-BYP) can support up to 4 copper links using SFP transceivers, so protecting up to 12 copper links.

Q: When is an iBypass switch in "ON" state?

A: The bypass switch will be in Bypass State "On" when any of the below events occurs:

- Power loss from the bypass switch
- Monitor Link failure – either one of, or both, the monitor ports 1 and 2 links down
- IPS application failure (can be caused by loss of power to the IPS or not passing Heartbeat packets)
- Bypass On mode is forced administratively

KEYSIGHT TECHNOLOGIES

Q: When is an iBypass switch in “OFF” state?

A: The bypass switch will be in Bypass State “Off” when ALL conditions below are met:

- Bypass switch is in power on
- Monitor Ports 1 and 2 are in link up state
- IPS application is running (passing Heartbeat packets)
- Bypass On mode is not administratively forced

Q: What are the typical bypass modes?

A: There are six (6) bypass switch modes:

1. **Bypass-Fail-Open** is when the bypass switch is in normal bypass operation with fail open functionality. “Fail-Open” allows Network Ports A and B to stay link up and pass traffic between them directly (monitor ports are "bypassed") when bypass switch is in Bypass “On” state
2. **Bypass-Fail-Close** is when the bypass switch is in normal bypass operation with fail close functionality. “Fail-Close” forces Network Ports A and B to be in link down, therefore no traffic between network ports A and B, when bypass switch is in Bypass “On” state.
3. **Force-Bypass-On-Fail Open** is when the bypass switch is forced into Bypass On state with fail open functionality – network ports A and B are still link up, thus allowing network ports A and B traffic flow (Tool maintenance for example)
4. **Force-Bypass-On-Fail Close** is when the bypass switch is forced into Bypass On state with fail close functionality – network ports A and B are forced to link down, no traffic flow at all.
5. **Force-Bypass-Off** is when the bypass switch is forced into Bypass Off state.
6. **Tap** is when the switch becomes a half-duplex breakout Tap, bridging network traffic between network port A and network port B, while mirroring traffic entering network port A to monitor port 1 and traffic entering network port B traffic to monitor port 2.

Q: Does an iBypass drop packets after a power failure?

A: There will always be some packet loss switching from Bypass Off to Bypass On. Any traffic that is on the monitor path will not be returned to the network and any packets caught mid-transition could also be dropped.

Q: What happens if the network link on an iBypass switch is running at line rate and it needs to send heartbeat (HB) packet? Will it drop a packet in order to put a heartbeat packet in or wait until the link is not at 100% utilization to send?

A: In the scenario you describe the iBypass would drop the amount of packets equal to the number of HB packets transmitted on the monitor side (HB packets got priority treatment).

Q: What do the terms ACTIVE-ACTIVE and ACTIVE-STANDBY mean?

A: Unlike many bypass switch vendors many of Ixia's bypass switches support two High Availability modes - ACTIVE-ACTIVE and ACTIVE-STANDBY.

ACTIVE-ACTIVE - indicates that two security devices can be connected in series so that traffic flows through both of them in sequence. Failure of one device means that traffic continues to flow via the bypass switch. The following diagram indicates an ACTIVE-ACTIVE iBypass VHD configuration. Traffic flows through Tool A and Tool B sequentially. Failure of either will still allow traffic to flow through the remaining tool without triggering bypass operation.

ACTIVE-STANDBY - indicates that two security are connected to the iBypass switch, but only one of them is live at the same time. If the primary tool fails then traffic is diverted via the remaining tool. The following diagram indicates an ACTIVE-STANDBY iBypass VHD configuration. Traffic usually flows through Tool A Primary. Failure of this will cause traffic to flow through Tool A Secondary without triggering bypass operation.

Q: What does the term Link Fault Detect (LFD) mean?

A: LFD is an optional feature on some iBypass Switches that causes the link status on both sides of the network links to remain "in sync". Failure of one side of the network link passing into the iBypass switch causes the switch to force the other side of the link to go down. This is useful in readily indicating failure of the network link to communications equipment on either side of the Bypass Switch. Without LFD the communications devices may continue to transmit traffic not 'knowing' that the remote side of the link was down.

Q: What does the term Link Fault Detect - Cascade (LFDC) mean?

A: The LFD capability addresses the issue of indicating to a remote communications device that the distant network link has failed. However, in some cases it is necessary to indicate that the links have failed to the security device connected to the monitor ports. This optional capability is known as LFDC and is available on some of the Ixia iBypass switches. Essentially it mirrors the network link status to any connected monitor port - as long as LFD is also enabled.

iBypass VHD

Q: With the VHD can I display some text on each GUI screen to show which box I am logged on to? With many windows open its possible to get 'lost'!

A: By default the IP address of each VHD is shown in the top left hand corner of each screen. However, it is also possible to have a name assigned to each VHD and have this displayed as well. See the attached screen shot of a VHD which has had the name “BYPASS-RACK2" assigned. This name will appear on every screen. To set this name go to SETTINGS/SYSTEM RESTART/SYSTEM NAME and set up the “System Host” name.

Q: Can I set up a "banner message" to display whenever someone logs onto the VHD Bypass Switch?

A: Yes - This capability is supported on the device - SETTINGS-SYSTEM_RESTART/MESSAGE OF THE DAY.

Q: What is the fastest way of setting up a VHD Bypass switch?

A: Go to the CONFIGURATION/PRESETS on the main menu. You will find a variety of common configurations that make a good basis for initial configurations.

Q: I want to "time stamp" all events accurately. Does the iBypass VHD support an NTP clock time source?

A: Yes. Up to 3 NTP time sources can be configured. See screen shot below. These can be set up via SETTINGS/DEVICE and then click on the NTP folder.

Q: In an complex ACTIVE-ACTIVE or ACTIVE-STANDBY configuration can you 'mandate' that a given tool must be live and if it fails the iBypass VHD would switch ON?

A: Yes.

Look at the following diagram of a iBypass VHD deployment (BTW imagine trying to visualize this without a GUI – good luck!). This is set up so that traffic from port A.01 flows via the bypass switch via port A.11 to Tool A – Primary, then via port A.12 back through the switch and on via A.13 to Tool B, then back via A. 14 and the switch to the network A.02 connection. In the event of a failure of Tool A Primary (detected via heart beat failures) the traffic will be diverted via ports A.09 and A.10 to Tool A Secondary. In addition a Tap has been set up to feed inbound traffic to ports A.16 and A.15. Also the bypass switch has been set up with both a primary and secondary network connection on the network side. All good.

But suppose Tool B is mandatory - no matter what it must be live in the network path. To set that the bypass switch must always go through Tool B, go to the Bypass Swith settings and the Inline Tool menu and select “Required” against Tool B. Once this is set the word "Required" appears under the "Tool 2" text and indicates that if this Tool ever fails then the Bypass will switch into ON mode. If in this scenario Tool B had not been set to "Required", then the failure of this tool would have simply resulted in Tool B being switched out of the traffic path and traffic would have continued to flow just through Tool A.

Q: Can you set up VHD to send syslog messages to remote syslog servers?

A: Yes. Go to UTILITIES and click on "Remote Syslog is ON/OFF" button and you will be able to set up unto 10 remote syslog servers.

iBypass 10G (IBPO-HBXXYY-XFP Models)

Q: Does iBypass 10G have SNMP OID for current bypass status – Bypass ON or OFF?

A: No, there is not an indicator in the v4.2 iBypass 10G for Bypass status.

iBypass 40-10 Models (I2BP-4X10-XX-YY-QSFP Models)

Q: When I buy a iBypass 40-10, what else do I need?

A: The only thing you need to buy with the iBypass 40-10, are 2 x QSFP+ SR4 transceivers and the tool side cables. All other cables, power supplies, and rack mounts are included in each unit. Tool side cables are not supplied as customers can use either Single Mode or Multi Mode fiber on the tool side, regardless of the media on the network side.

Q: Does the iBypass 40-10 support 40G native links?

A: No.

Q: What are the advanced High Availability (HA) modes supported by iBypass 40-10 today?

A: **A Part 1: HA Active-Standby**

Mode 1: segment 1 (both network/monitor port pair) is Active, and segment 2 to 4 are sequentially failover segments.

Failover - If Active segment (S1) network or monitor port pair fails, the traffic goes to next available segment network or monitor port pair.

Recover - a. When Active segment (S1) port pair is recovered, the traffic goes to Active segment port pair automatically.

b. The traffic path will change to the higher priority failover segment when it is available.

Mode 2: Segment 1 and 2 are one set of Active-Standby segments, segment 3 and 4 are another set.

Mode 3: segment 1 and 2 are regular Active bypass without standby segment. Segment 3 and 4 are Active-Standby segments.

A Part 1: HA Active-Active

Mode 11: segment 1 (both network/monitor port pair) is Active, and segment 2 to 4 monitor port pairs are active. The traffic that goes in from segment 1 network port pair will sequentially flow monitor port pair of segment 2 to 4 and then come back from network port pair of segment 1. Any monitor port pair fail will cause bypass on.

: If any of the segment 1, 2, 3 and 4's monitor ports fail, traffic only flows between segment 1 Network ports A and B.

Mode 12: This is extension to mode 11. This mode adds segment 2 network port pair as failover for segment 1. The data flows between monitor port pairs are same as mode 11. The failover is only between the network port pair of segment 1 and 2.

Failover - If Active segment (S1) network port pair fails, the traffic will goes to segment 2 network port pair.

Recover - When Active segment (S1) network port pair is recovered, the traffic will flow to Active segment network port pair automatically.

Mode 13: segment 3 and 4 are regular Active bypass without standby segment. Segment 1 and 2 monitor port pairs are Active-Active segments, and segment 2 network port pair is failover of segment 1 network port pair.

Q: For iBypass 40-10, when Seg 1 and Seg 2 are configured in HA mode (ActiveStandby2 for example), how does the iBypass determine Seg 1 Network is down and switch to Seg 2 Network (failover)?

A: Unlike the tool ports that use HeartBeat to detect both physical failure (link DOWN) as well as logical failure (Tool stuck), the Network port failure is only based on physical status - ie, when the link is DOWN. Currently, there is no mechanism to detect logical failure of an active network link.

Q: Can I use a standard QSFP+ Single Mode transceiver on the tool side of a iBypass 40-10?

A: No. The iBypass 40-10 uses a break out cable to to connect upto 4 security devices to the tool ports. "Standard" Single Mode QSFP+ transceivers support 4 x 10G lanes that are wavelength multiplexed onto a single pair of fiber optic cables. What we need is a total of 4 x 10G lanes that are spatially separated onto 4 separate pairs of fiber optic cables. To do this we need a special kind of 40G transceiver called a "PLR4" - "Parallel" LR4 QSFP+ transceiver. Ixia sell these using the part number "IxQSFP+-PLR4". For Multi Mode applications standard QSFP+ transceivers can be used.

iBypass HD (IBP-8000 Model Plus Associated Bypass Modules)

Q: Does iBypass HD have the capability to have mode fail close when it loses power?

A: The iBypass will fail open ALWAYS in power loss condition regardless of how it’s configured to operate under power. It has relays/optical switches that are held open by power. With no power the relay drops and passes traffic (Bypass is ON/Closed).