NetOptics®
an ixia company

External Bypass Switch Enhances IPS Solution

Abstract

Bypass functionality ensures network uptime by bypassing an in-line device such as an IPS when the device becomes unavailable for any reason. An independent, external Bypass Switch device used in conjuntion with an IPS improves overall solution reliability and increases application availibility. In addition, it can provide traffic instrumentation and add the convenience and cost savings of remote monitoring and control. These benefits justify the cost of an external Bypass Switch even if the IPS integrates bypass functionality internally.

White Paper

External Bypass Switch Enhances IPS Solution

White Paper

Introduction

This paper shows how an external Bypass Switch adds value to an IPS deployment, even if the IPS is available with internal bypass circuitry. An external Bypass Switch device increases the reliability of the overall solution and improves uptime of critical business applications. It can also improve the system instrumentation and provide the convenience and cost savings of remote management.

But first, let's review why bypass switches are needed at all.

The Need for Bypass Functionality

When a network monitoring device such as an Intrusion Prevention System (IPS) is deployed in-line in a network link, it is vital to ensure that link traffic continues to flow in all circumstances, even if the IPS loses power, so that mission-critical business applications remain available. If the IPS function is crucial to application security, traffic must be switched to a backup IPS device. However, in some cases, it may be acceptable to operate the link for a period without the IPS active; for example, if the IPS is a secondary security precaution and the primary security system is a firewall on the same link. In this case, application availability can be ensured by bypass switch circuitry.

A bypass switch is passive circuitry that opens the link to traffic flow when the IPS is not available. In simple terms, it can be a relay for copper links or an optical switch for fiber links, as long as the relay or switch defaults to a state that passes traffic in the absence of power. The bypass switch must also ensure that the signal integrity of the link is preserved, by physically decoupling the attached IPS or by other techniques.

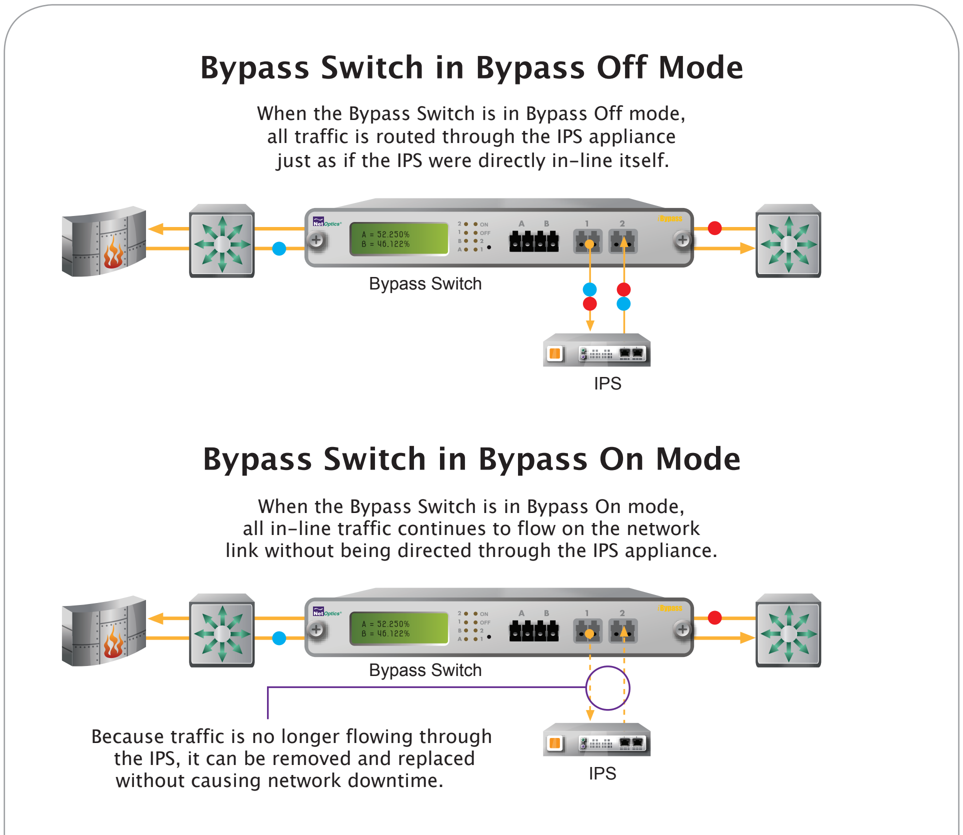
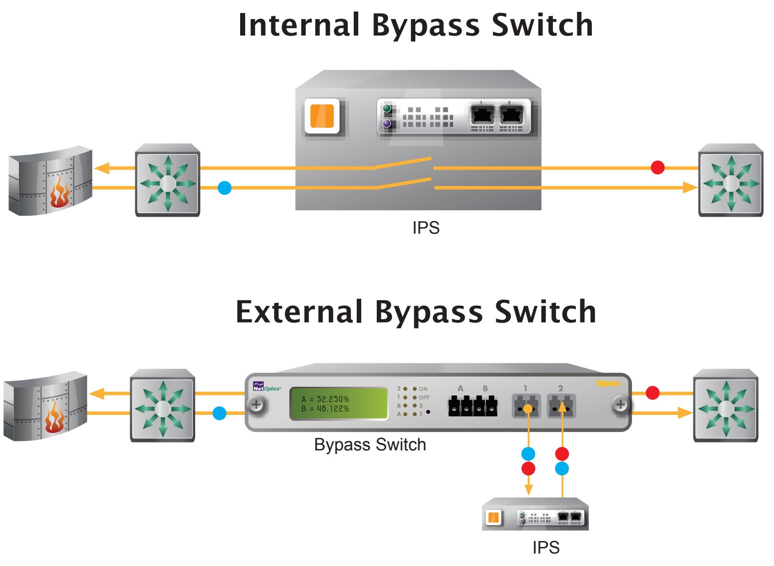

Bypass Switch in Bypass Off Mode
When the Bypass Switch is in Bypass Off mode, all traffic is routed through the IPS appliance just as if the IPS were directly in-line itself.
Bypass Switch
IPS
Bypass Switch in Bypass On Mode
When the Bypass Switch is in Bypass On mode, all in-line traffic continues to flow on the network link without being directed through the IPS appliance.
Bypass Switch
Because traffic is no longer flowing through the IPS, it can be removed and replaced without causing network downtime.
IPS

Figure 1: Bypass switch circuitry keeps traffic flowing

Bypass switch circuitry is built into many IPS models from various vendors. It may be called a bypass switch, a bypass, a zero-power high availability feature, a fail-open device or mechanism, or another term, but it means that link traffic continues to flow when the IPS is powered off. We will refer to it as an internal bypass switch, because the circuitry is integrated in the IPS.

The bypass function can also be performed outside the IPS itself, using an external Bypass Switch device. For example, Net Optics provides a line of Bypass Switch devices that support any link media type and provide a variety of features that are discussed in subsequent sections. This paper examines the value an external Bypass Switch can provide, over and above that of an internal bypass switch. We will show that an external Bypass Switch can improve the overall solution reliability, increase application availability, provide better instrumentation, and add the convenience and cost savings of remote monitoring and control.


Internal Bypass Switch

External Bypass Switch

Figure 2: Bypass circuitry can be internal or external

Improved Overall Reliability

Anything can fail. The question is never “Will it fail?” but rather “When will it fail?” An external Bypass Switch increases the reliability of an IPS deployment because it keeps traffic flowing whenever the IPS fails, for any reason. This is not to imply that IPSs are failure-prone devices. To the contrary, IPSs from the leading vendors are designed and manufactured to the highest reliability and quality standards, and may well be reliable enough that you don’t need the extra insurance of an external Bypass Switch. But don’t confine your analysis to the MTBF of the hardware components. Failures of an IPS in a network can also come about from other causes, such as:

- **A cable is unplugged from the IPS**
- **Someone misconfigures the IPS**
- **A software bug hangs or slows down the IPS**
- **Excessive traffic overwhelms the IPS**

In some of these cases, for instance if a cable is unplugged, an internal bypass switch cannot possibly help. In other cases, an internal bypass switch may provide protection. However, IPS designers are not necessarily experts in bypass design, as Bypass Switch engineers are. Internal bypass switches may not have all the technology advantages of an external solution, and therefore simply do not protect your network as well.

One such important technology included in many Net Optics Bypass Switches is the Heartbeat$^{\text{TM}}$ packet. This is a small packet that the Bypass Switch passes through the IPS on a regular basis. If the Heartbeat packet is not returned to the Bypass Switch within a programmed timeout period (and number of retries), the Bypass Switch knows the IPS is unresponsive – regardless of the reason – and it immediately opens the link allowing network traffic to flow directly, bypassing the IPS. The Heartbeat packet is a foolproof technique for determining the health of the attached IPS. The reliability of the IPS solution is increased by this on-going, independent evaluation of the IPS's status.

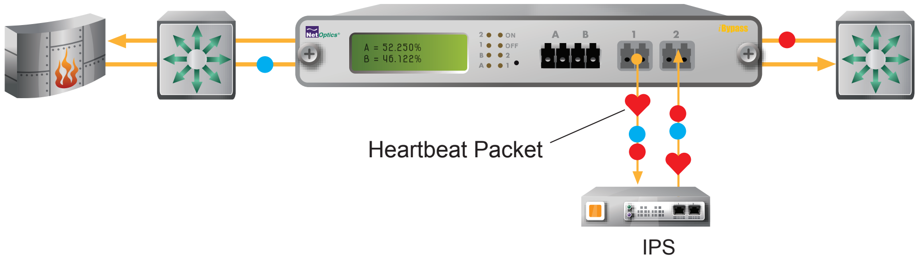


Figure 3: An external Bypass Switch continuously monitors IPS health by passing a Heartbeat packet through the IPS

Increased Application Availability

While an external Bypass Switch improves the solution reliability by adding an independent check on the IPS, it also contributes to application availability in another way. When an IPS is deployed with an external Bypass Switch, the IPS can be taken off-line or removed from the link at any time without impacting link traffic.

For example, if a new set of intrusion signatures is activated and the impact on the network is not what was expected – if too many false positives show up, blocking critical traffic – the IPS can simply be stopped, or the Bypass Switch can be forced into Bypass On mode; in either case, the external Bypass Switch keeps link traffic flowing. This capability may or may not be provided by an internal bypass switch.

However, consider another example that cannot possibly be handled by internal bypass circuitry. Sometimes it is necessary to physically remove the IPS from the link, perhaps for maintenance, upgrade, or reconfiguring the network. If the IPS was deployed with an external Bypass Switch, the IPS can be physically removed from the link without impacting link traffic or application availability. With an internal bypass switch, or no bypass switch at all, you would have to wait for a scheduled maintenance window, perhaps get a network change authorization signed, and alert users of all applications dependent on the link that their service will be interrupted for a period. Clearly the external Bypass Switch saves a lot of time and trouble in this case.

But the scenario can be worse than that. So far, the examples assumed a planned event. It may also happen that the IPS is, or must be, taken offline or physically removed because of an unplanned situation. For example, a cable could be accidentally unplugged from the IPS during some maintenance activity, and the technician may not even realize it happened. Or the IPS could experience a physical failure such as an electrical component going bad (which is much more likely to happen in the IPS than in the external Bypass Switch, because it is a much more complex device). The external Bypass Switch ensures that the application is not taken down by one of these unplanned events, should they occur.

Better Instrumentation

We have seen that a basic external Bypass Switch improves the overall solution reliability and application availability compared to a bypass switch internal to the IPS. However, Net Optics offers Bypass Switches with additional features that add even more value to the solution. In particular, the iBypass family of Bypass Switches integrates more intelligence in the bypass device. These products include a remote management interface that enables network professionals to monitor the status of the iBypass Switch itself, the attached IPS device, and the links into and out of the iBypass Switch.

The ability to obtain traffic statistics from the iBypass Switch is particularly valuable. Information such as bandwidth utilization, peak traffic, packet and byte counts, and error counts enable security personnel to measure the impact of new IPS signature sets and configurations, without the need for additional monitoring tools and network taps, and without reconfiguring Span ports on switches.

The iBypass Switch can also generate alarms (SNMP traps) when traffic on a given port exceeds a programmed utilization level. These traps can be used by a network management system such as IBM Tivoli or HP OpenView to alert an operator that an unusual condition exists – perhaps one in which the traffic volume could exceed the capability of the IPS. For environments without comprehensive SNMP management systems, alarm conditions are also displayed by the System Manager (platform based) and Web Manager (Web browser based) tools provided in the Net Optics Indigo™ device management software suite included with every iBypass Switch. In addition, LED indicators on the iBypass Switch front panel display alarm conditions, and an alpha-numeric LCD display shows live traffic statistics, for at-a-glance system status checking.

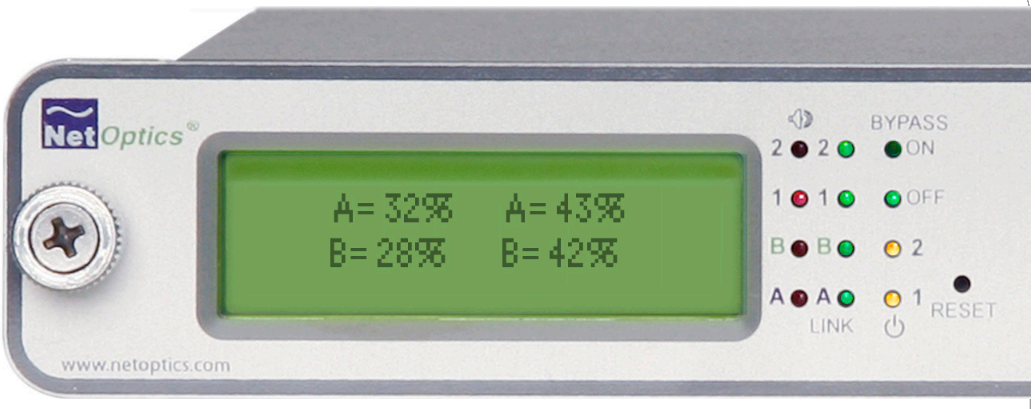


Figure 4: iBypass front panel with monitoring information – LEDs show alarms (first column), link status (second column), bypass state (top of third column), and power supply status (bottom of third column); the RESET button clears alarm conditions

Remote Monitoring and Control

The management interfaces in the iBypass Switch family of devices also provide the convenience and cost savings of remote operation. Any Web browser on any computer can connect to the iBypass Switch Web Manager software, which is embedded in the device itself. Alternately, System Manager, creates a central server for managing any number of iBypass Switches and other Net Optics iTap technology enabled devices. To maintain a secure monitoring environment, Web Manager and System Manager are password-protected and only accessible over the device's dedicated management port, which can be isolated on a secure management VLAN if desired.

By logging into the device from anywhere on the network, operators can monitor traffic and device status, and configure and control the device. One aspect of device control is the ability to force the iBypass Switch into Bypass On mode, taking the IPS offline. This capability can be handy for easily removing the IPS from service without requiring a technician to be physically on site with the IPS, saving time and travel costs.

Another valuable feature of the iBypass Switch is that when it is in Bypass On mode, taking the IPS offline, the iBypass Switch assumes the function of a full-duplex network tap, mirroring all the traffic received at network link Port A to monitor Port 1, and all the traffic received at network link Port B to monitor Port 2. This enables the IPS to continue to monitor the network traffic, acting as an out-of-band Intrusion Detection System (IDS), a useful way to test signature sets before actually applying them to network traffic. When switched to Bypass On mode, the device can also be used as a conventional network Tap, eliminating the need to break the link to install a Tap when other types of monitoring tools are required to investigate a network issue.

Conclusion

It has been shown that an external Bypass Switch makes an IPS deployment more reliable and flexible as compared to depending on bypass circuitry integrated within the IPS. Moreover, the cost of the external Bypass Switch is further justified by the value-add of improved instrumentation and the cost savings of remote management capabilities. The cost may also be partially offset by purchasing a lower cost IPS model without an internal bypass, if the manufacturer offers such a model. Therefore, even if an internal bypass switch provides all the reliability and functionality required in your environment, it is worth considering whether the added benefits of an external Bypass Switch may prove to be the wiser choice.

About Net Optics

Net Optics is the leader in innovative passive in-line devices for network security, traffic analysis, and IT monitoring solutions. Our products are used to access and monitor networks by enterprises, service providers, and government organizations around the world. Leading vendors of protocol analyzers, RMON probes, and IPS appliances have chosen Net Optics products for their customers' networks—from T1 to 10 Gigabit links.

For further information about Bypass Switch technology:

http://www.netoptics.com/support/whitepapers
Net Optics, Inc.
5303 Betsy Ross Drive
Santa Clara, CA 95054
(408) 737-7777
ts-support@netoptics.com
www.netoptics.com

Customer First!