Interface Masters
TECHNOLOGIES
Innovative Network Solutions

Ensuring Uptime in your Network with Active Monitoring Devices

Overview

A key challenge in today's fast growing inter-networking world is to create cost-effective solutions that provide greater visibility into network traffic while ensuring maximum network uptime. There are numerous tools available in the market that specialize in controlling the flow of traffic, providing functionality ranging from WAN acceleration, prioritizing information, monitoring network links, security or assuring quality for VoIP and video conferencing. These inline tools allow administrators to maintain network traffic for optimal security and visibility, yet those same devices can pose serious threats to network stability and connectivity due to the fact that they impose a single point of failure. With a combined solution of an Active monitoring device and Interface Masters' Active bypass technology, maximum network visibility and network uptime can be achieved in any network environment.

Solution

In networking, a common network topology consists of a router on one side which enables communication from the internal LAN and a switch or router which creates a channel of communication to and from the WAN side. Depending on the network, this is usually a single connection (See figure 1).

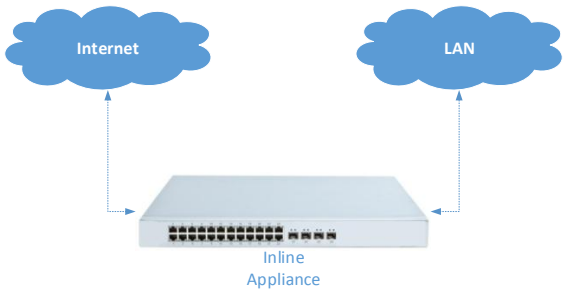

Figure 1: Common Network

When an inline tool is introduced into the network, it is generally placed between the Internal LAN (Intranet) connection and the WAN connection (Internet). This deployment scenario will enable all bi-directional traffic on the network link to be monitored in real time. In order to avoid network down time due to power failure or appliance malfunction and in order to guarantee 100% network uptime a bypass is placed in front of the inline appliance which will direct the flow of traffic to the appliance when it is healthy and bypass the appliance when the appliance fails or goes down. When the appliance comes back up, the bypass is capable of instantly redirect the network traffic back to the appliance for inline monitoring, this depends on the installation and network configuration.

In order to install a Niagara Active bypass unit to protect a network being monitored by an inline device, The Internet and Intranet end points need to be connected directly to the bypass unit on two dedicated ports called Network Port 1 (or N1) and Network Port 2 (or N2) which are the top two ports on any bypass segment. The bottom two ports on the same bypass segment, Appliance Port 1 (or A1) and Appliance Port 2

(or A2) need to connect directly to the active monitoring device (see Figure 2). When the bypass is in an inline state, the traffic will flow through to the Active monitoring device, where the information will be processed according to the rules specified on the system. In order to determine whether the Active monitoring device is in good health or not, heartbeats are generated from A1/A2 and sent through the Active monitoring device to A2/A1. Should heartbeats not be received, bypass will be initiated, and once the heartbeats are received again, indicating the health of the system has returned, the bypass can go back to inline mode.

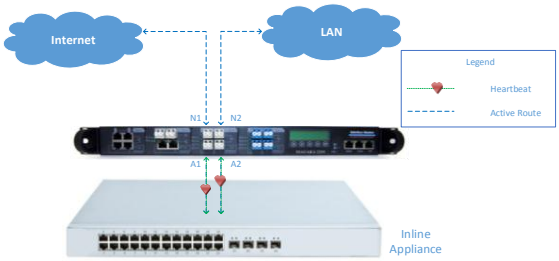

Figure 2: Inline Mode

When the connections are in place, the bypass offers two levels of security. As mentioned previously, when the bypass is operational, the unit will generate heartbeats that are sent on the appliance port and expected to be received back on the adjacent appliance port. This will constantly monitor the Active monitoring device to determine if it is in a healthy state. When the heartbeat is not received in the timeout defined, the traffic will bypass the Inline device ensuring network uptime (See figure 3). When the tool is healthy enough to process the heartbeats (pass traffic), the flow of traffic will traverse through the Inline device again. In the event that the bypass loses power, a second level of protection called Passive bypass will ensure that the traffic will continue to flow even in an unpowered state. Passive bypass is managed by hardware bypass logic that will continuously monitor the bypass and once power is lost will ensure that traffic continues to flow.

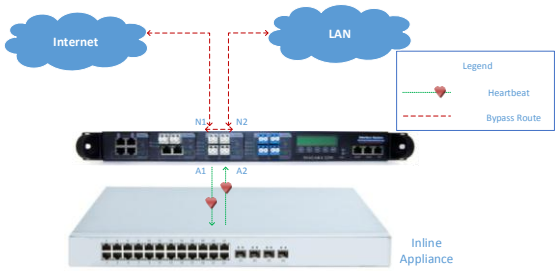

Figure 3: Bypass Mode

One of the advantages of the Active bypass is its plug-and-play capability and highly customizable heartbeat functionality. The programmability of the heartbeat enables administrators to have full control over heartbeat configuration and optimize heartbeat parameters include the timeout/delay to deem a heartbeat packet lost, the type of heartbeat packets required, and the heartbeat packet parameters such as IP, MAC and/or TCP port information.

Conclusion

The web continues to grow exponentially and requires more and more tools to effectively manage increasing network complexity, size and speeds. Companies cannot afford the network to be down for any time due to introducing and maintaining active inline appliances and monitoring devices. The Interface Masters External Active bypass adds critical layers of protection to the network ensuring maximum uptime. Together, The Active monitoring device and the Interface Masters Active Bypass are the ideal solution to effectively manage any network, regardless of complexity, size and speed.

Interface Masters Bypass Switches:

Interface Masters' offers a diverse selection of Active bypass switches to protect critical network links from costly downtime due to power outage, software or hardware failure or link-loss of inline networking or security devices. The Niagara Active bypass solutions can protect one or multiple 10/100, 1G, 10G and/or 40G network links that are being monitored by an inline appliance and supports flexible media configuration options including multi-mode fiber, single-mode fiber, and copper. In addition, these interfaces can be mixed and matched to support datacenter environments where the network requires fiber connection, but the inline tool requires copper connection. In this case, the conversion is done on the bypass saving cost while maximizing space.

Some of the bypass switches can handle Network Packet Broker technology and TAP technology, which are called Premium Bypass Switches. Below is an overview of Interface Masters different Bypass Switch offerings.

1G

The **Niagara 2299** is a 1Gb Bypass Switch. Niagara 2299 supports maximum flexibility and scalability by offering four independent Gigabit Ethernet interface segments with various media combinations including copper, single-mode fiber, multi-mode fiber, Single-mode fiber to Multi-mode fiber conversion and copper to fiber conversion options.

10G

The **Niagara 2818** is a 10G quad-segment Bypass switch. This can provide network protection for up to four fiber 10Gbps appliances. The Niagara 2818 has a high availability mode, where if two appliances are connected, and if the primary appliance fails, all traffic will be re-routed to the secondary appliances. Below is a diagram of High-Availability mode. In figure 4, the traffic is flowing through segment one to the primary system, while the same traffic is being mirrored and copied to the secondary device.

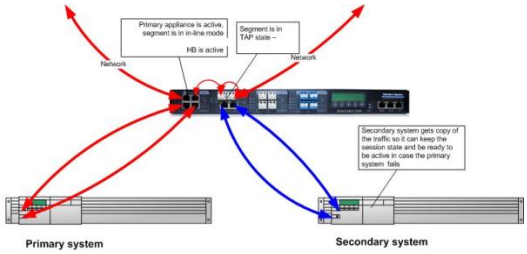

Figure 4: High Availability

If the primary device fails, the traffic is automatically rerouted to secondary device (see figure 5), and because the secondary device has already been receiving the network traffic, it will seamlessly begin monitoring the link without delay.

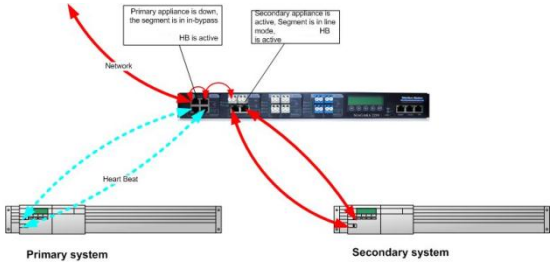

Figure 5: High Availability

40G

Niagara 2831 is a single segment 40G Bypass switch. The Niagara 2831 bypass feature automatically switches the network traffic upon power failure of an attached in-line device, preserving network connectivity. This device has connection availability for single-mode and multi-mode fiber.

Hybrid

As the highest density Bypass switch in the market, the Niagara 2822 is a modular sixteen segment Intelligent Active Bypass that can handle 1 Gb, 10Gb and 40Gb Inline Network Monitoring Devices. The Niagara 2822 can support up to 8 hot pluggable, field replaceable modules that can be either 2 segments of 1G/10G or one segment of 40G. The non-network ports can support 10G/1G SFP+ media or 40G QSFP+ ports depending on what module is selected and can be assigned to any of the network segments. This system allows for great flexibility in deployment of appliances into any network.

Premium Bypass Switches

Along with an already extensive line of Bypass Switches, Interface Masters has integrated their PacktMaster and Bypass technology with the Bypass Switches to create Premium Bypass Switches.

With TAP

Often times network architects will find they have the same inline (Ex: Wan Optimization) and out of band (Ex: Intrusion Detection System) monitoring devices that can use the same network data. The amount of critical links that need to be monitored is often expensive and not efficient to be individually TAP'd into. With a TAP integrated with a Bypass Switch, the network links are able to share information to both Active and Passive Monitoring devices. There are two different types of TAPS, an active TAP which can aggregate two network feeds together and a passive TAP that takes a pure copy of the traffic from each network link and mirrors it to an appliance.

Niagara 2818PT (See figure 6) is a 10Gb Bypass switch that supports 8 ports of passive TAP functionality. Off of these 8 ports you can passively monitor eight different devices such as an IDS.

Figure 6: Niagara 2818PT

The **Niagara 2818T** is also a 10Gb Bypass switch that supports 7 ports of Active TAP. These 7 ports can support three different passive monitoring devices.

Niagara 2831T is a single segment 40Gb Bypass switch that will support four different passive monitoring devices.

Niagara 2842 is a modular 1G, 10G and 40G Intelligent Active Bypass Switch with up to 32 multi-purpose SFP+ Ports that can be a combination of either Bypass Switch ports, Passive TAP ports or Active TAP ports.

With PacketMaster

Integrating PacketMaster technology, , which is Network Packet Broker (NPB) functionality, with a Bypass Switch allows for extensive packet filtering, distribution, aggregation and mirroring functionality.

Having these two technology's in one system allows for much greater integration into network architectures and creates greater visibility into the network. Interface Masters

currently supports three different Bypass Switches with PacketMaster.

The **Niagara 2804** supports all of Niagara 2818's functionality's and additionally integrates with 16 multi-purpose SFP+ Ports that can support 1G SFP or 10G SFP+ media and can be assigned to any of the network segments. These 16 ports are loaded with PacketMaster capabilities (See figure7).

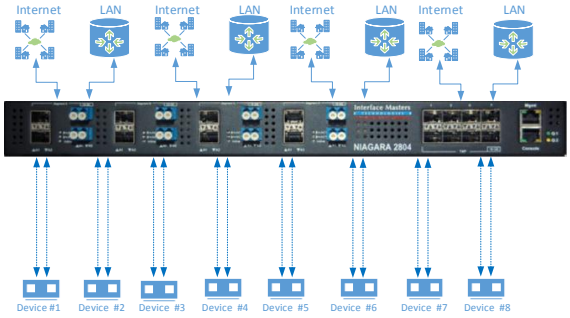

Figure 7: Niagara 2804 Implementation

Niagara 2841 consists of a single segment of 40Gb bypass (Niagara 2831) which possesses active and passive bypass switching capabilities and 8 additional 10G SFP+ PacketMaster ports for flexible 10G or 1G monitoring of network traffic. One use case of this system (See figure 8) is LoadBalacing the 40G of bandwidth from the network to four different active monitoring devices that can handle 10G of bandwidth each. Once these systems process the packets, they will send it back to the Niagara 2841 to be re-aggregated back to a 40G network.

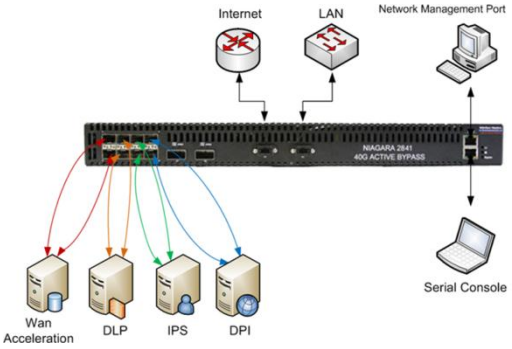

Figure 8: Niagara 2841

Niagara 2842 is a modular 1G, 10 Gigabit and 40 Gigabit Intelligent Active Bypass Switch with up to 32 multi-purpose Ports for extensive packet filtering, distribution, aggregation and mirroring functionality.

Interface Masters Technologies

Interface Masters Technologies is a leading vendor in the network monitoring and visibility market including Bypass, TAP, switches and smart NICs products, based in the heart of the Silicon Valley. Interface Masters' expertise lies in Gigabit, 10GbE and 40GbE networking solutions that integrate with monitoring, inline networking, IPS, UTM, Load Balancing, WAN acceleration, and other mission-critical IT and security appliances. Flagship product lines include PacketMaster® Network Packet Broker, specialized 10GE internal server adapter cards, switches, 10Gb and 40Gb external intelligent Network TAP and Bypass and failover systems. Company Headquarters are located in San Jose, CA with satellite offices in Hong Kong and Europe.

150 East Brokaw ● San Jose, CA 95112
Sales: 408.441.9341 ext. 100
Support: 408.441.9341 ext. 2
www.interfacemasters.com