Interface Masters
TECHNOLOGIES
Innovative Network Solutions

Maintaining Network Visibility While Expanding a Data Center

Introduction

Data Centers are beginning to exponentially grow and as a result, networks have to find faster solutions to keep up with an increase in data being shared. Migration strategy's to fulfill these faster speeds such as server upgrades are becoming very complex and network administrators need to reduce the intricacies of the network. To preserve the quality of service on these networks, more and more tools are being added to ensure that performance is acceptable for the quality of experience (QoE) for the users. While supporting these new appliances, network administrators will still need to maintain and support the older generation of appliances, which create complex network architectures. When designing these new networks, one must be have a strategic approach that will not only be acceptable now, but will prepare the network for further changes down the road. This paper will address the state and issues of networks now and the solutions to mitigate risk for the future.

Problem

Network Monitoring

As networks begin to grow, gaining visibility is becoming increasingly more difficult as there are more amounts of spots to monitor. One of the ways a network engineer is able to collect the data for their tools, is a SPAN port or TAP. Even with many TAPs or SPAN ports, there still may not be enough critical network links that appliances can use. On the other side, some networks though may have more network links than appliances, and thus all the traffic cannot be monitored.

Traffic issues

When the monitoring tools are collecting data, it is common that they are capturing data at either high volume areas on the network or low volume areas. When the traffic that is trying to be monitored is not being sent efficiently, this leads to poor data collecting. As a result of too much network traffic, the links may begin to get oversubscribed. With multiple devices that are trying to take up the port's bandwidth, this can result in poor response time and also you can lose packets if the link burst. When there is too little of traffic on the network, the links may be unsubscribed and thus, not utilizing all the resources that a monitoring tool can use.

CAPEX and OPEX

With the increasing amount of data that needs to be monitored, without a viable solution to efficiently navigate it, the cost of expanding ones network would exponentially grow. While the network is growing, that would thus cause the amount of time needed to monitor and ensure that everything is properly function would increase as well. These put together creates a data center that is financially unsophisticated.

Solution

Ensuring Network Uptime

When an inline tool is introduced into a Data Center network, it is generally placed between the Internet and the Internal LAN connection. This deployment scenario will enable all bi-directional traffic on the network link to be monitored in real time which is crucial to the success of a high functioning network.

A bypass switch is placed in front of the inline appliance and 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 will instantly redirect the network traffic back to the appliance for inline monitoring.

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 (See figure 1). In order to determine whether the Active monitoring device is in good health or not, heartbeats are generated from the Bypass Switch and sent through the Active monitoring device. Should heartbeats not be received, bypass will be initiated, and all the traffic will be re-routed on the bypass switch without losing any packets. Once the heartbeats are received again, indicating the health of the system has returned, the bypass will once again go back to inline mode.

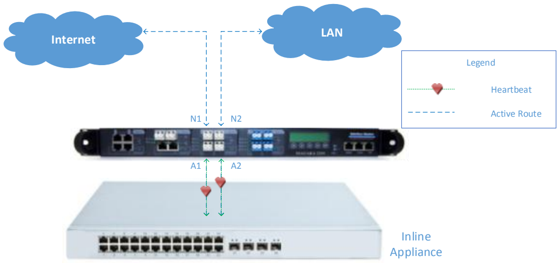

Figure 1: Inline Mode

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 Active monitoring device ensuring network uptime (See figure 2). When the tool is healthy enough to process the heartbeats (pass traffic), the flow of traffic will traverse through the Active monitoring 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.

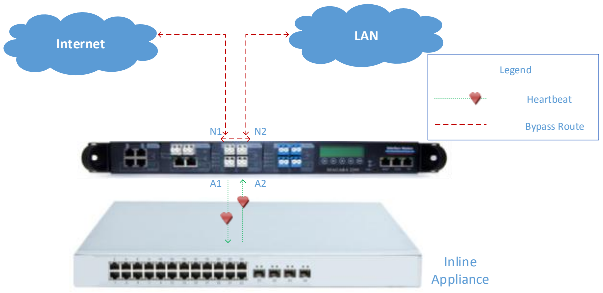

Figure 2: Bypass Mode

Interface Masters provides 1G, 10G and 40G bypass system while Niagara 2822 can support up to 16 network segments in a 2U.

As the web continues to grow exponentially and requires more and more tools to effectively manage increasing network complexity, size and speeds. Your network cannot afford to be down for any time due to introducing and maintaining active monitoring devices. An External Active bypass switch 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.

Intelligent Traffic

With such an overwhelming amount of data now having to be collected as infrastructures are upgrading the appliances, one needs a solution to be able to monitor the high bandwidth network, with a low bandwidth tool. Applications only need specific type of traffic; therefore, by utilizing a Network Packet Broker (PacketMaster) into your network, a solution such as filtering or packet slicing can be performed you can send only the needed packets to the device. Doing modifications to the packets such as just keeping the packet header while stripping down the payload, will save capacity on the network link. This allows for more visibility for the tools to process the packet, which will increase efficiency in the network.

Reduction of tools

In an environment where there are thousands of critical network links that needs to be monitored, it is often a cost restraint to have thousands of monitoring and security appliances. By not scaling appliances with the points on the network, this could leave network “blind spots” and create poor end-user-experience. Using a PacketMaster, you can aggregate multiple network points into one network monitoring or security device (see figure 3). This way you can monitor a larger portion of the network in a more centralized manner. This in turn will also reduce the number of monitoring tools that you have on your network which will save money.

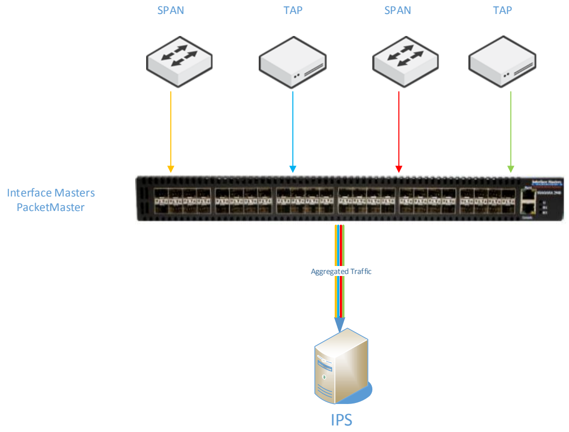

Figure 3: Aggregation

Gathering all critical data

In a Data Center, there are passive monitoring devices such as RMON probes, intrusion detection systems, network recorders and network analyzers. It is common practice to have the passive monitoring devices run out of band on the network as they are not modifying or altering any of the packets or traffic such as inline device (for example WAN optimization) would. A common approach to passing this traffic to these passive devices is the addition of a TAP unit.

A TAP is device that will passively split traffic coming from the network to the passive monitoring device. The TAP will receive both directions of traffic from the network, (Ingress and Egress) in real time to make sure all data is sent to the monitoring device (see figure 4). This traffic is coming on separate channels (RX and TX) so that both directions of traffic will be sent to the passive monitoring device. The TAP will also receive all traffic, as it is passive and will not modify the traffic before being sent to the device. By inserting a TAP into a network environment, administrators are able to ensure that all links will be monitored so the network is able to efficiently and effectively be used by customers, thus improving the QoE and creating full visibility into what is going on. Interface Masters provides a high density TAP, Niagara 3225PT, which can support up to 25 fiber network segments, while copper taps are available in system of up to 4 segments.

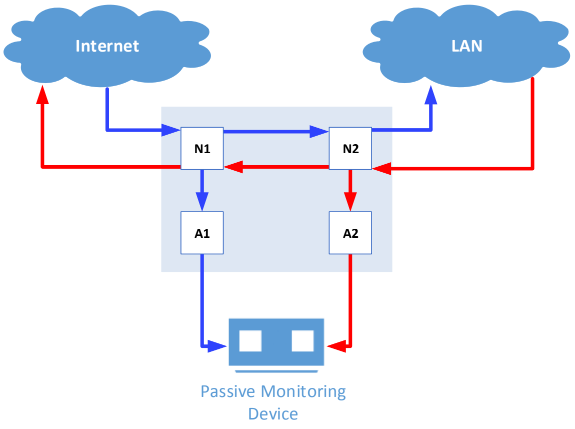

Figure 4: Single TAP Segment

Ability to Grow the Network

New threats and new information relating to how networks can be monitored is changing daily. Companies will create new devices to mitigate these subsequently. A pain point for many network architects though is finding new places on the network to add these devices. One solution is mirroring traffic that is already being processed by a PacketMaster. This will enable engineers to introduce new appliances without having to TAP more parts of a network link. The addition or changes of these tools will not affect any physical change to the existing network architecture by only having to direct in the graphical user interface (GUI) or CLI where you would want the pre-existing network link to mirror to allowing appliances to be added on the fly.

Increasing Bandwidth

As demand grows for faster networks, data centers will find they will need to grow their internal bandwidth as well. A roadblock to increasing the speed of traffic on the network is the lower speed tools or security devices on the network. Buying new tools for a network is extremely costly, especially when you are moving up in speeds (ex: 10Gb to 40Gb), but with the PacketMaster, LoadBalancing feature, you can still use your existing lower speed tools. With the LoadBalancing feature, if you have a 40Gb stream for instance, you can load balance the traffic to four existing 10Gb tools (see figure 5).

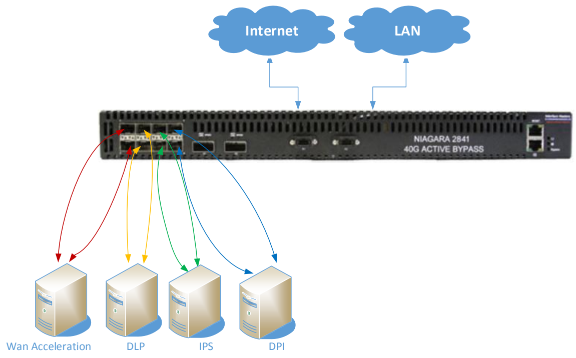

Figure 5: LoadBalancing

Once you do upgrade the tools to 10Gb, you can replace the SFP modules (1Gb) with SFP+ modules (10Gb) and mirror the traffic to the new 10Gb devices (see figure 6).

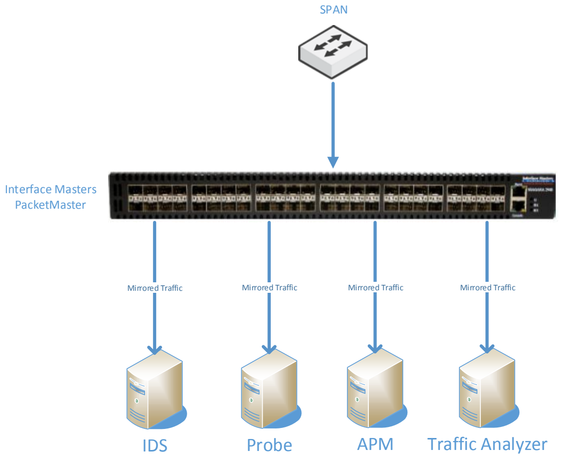

Figure 6: Mirroring

Conclusion

Looking towards the future of how data will be received is drastically changing. The end quality for the users has to not only stay the same but increase in speed, to be competitive with other companies. Networks are expanding and the amount of links needed for monitoring appliances needs to be maintained. Inefficiency's in the network are creating financially unstable environments that may not be viable for the future, so it is important to keep a datacenter updated and efficient. Some of the solutions we provided are:

- Utilize filtering and packet slicing to reduce the amount of traffic being sent to monitoring appliances, will allow for more efficient traffic monitoring
- Having no downtime on a network if a inline appliance goes down or needs to be replaced

- Not needing to increase the amount of tools on your network by aggregating multiple network feeds to one appliance
- Making sure you can monitor every critical link possible with a TAP
- Bring on new tools to the network seamlessly without any delay
- Increase bandwidth for the future while not having to upgrade your existing tools which could be expensive
- Maintain visibility of network while keeping all points needed monitored

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