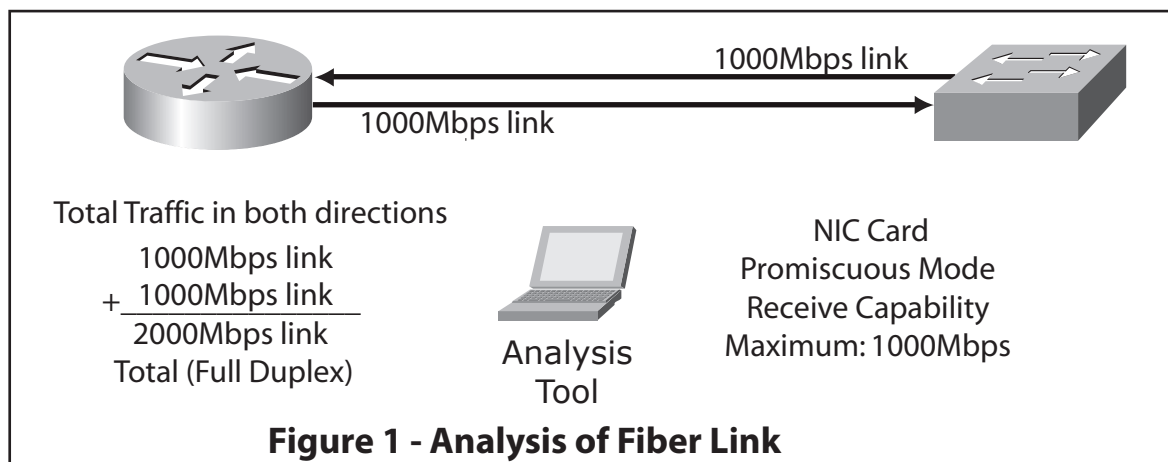


Port and Address Filtering Example

Analysis Example

A common network analysis technique uses a laptop loaded with a packet gathering application. Unfortunately, the network line speed sometimes overwhelms the laptop's hardware and software. This oversubscription results in packets being dropped. Lost packets mean greater difficulty in troubleshooting problems or missed security issues.

This example demonstrates how to use port and Vlan filtering techniques with the Filtered SINGLEstream™ to capture interesting network traffic. A Gigabit fiber connection between network devices is shown in Figure 1, a laptop computer with a standard copper NIC is used to troubleshoot the network link.



The aggregate traffic in each direction is:

$$1000\text{Mbps} + 1000\text{Mbps} = 2000\text{Mbps or } 2\text{Gigabit/s}$$

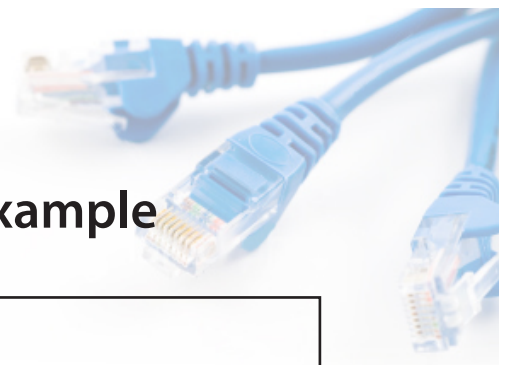
The maximum receive side of the network interface card on the laptop is only:

$$1000\text{Mbps or } 1\text{Gigabit/s}$$

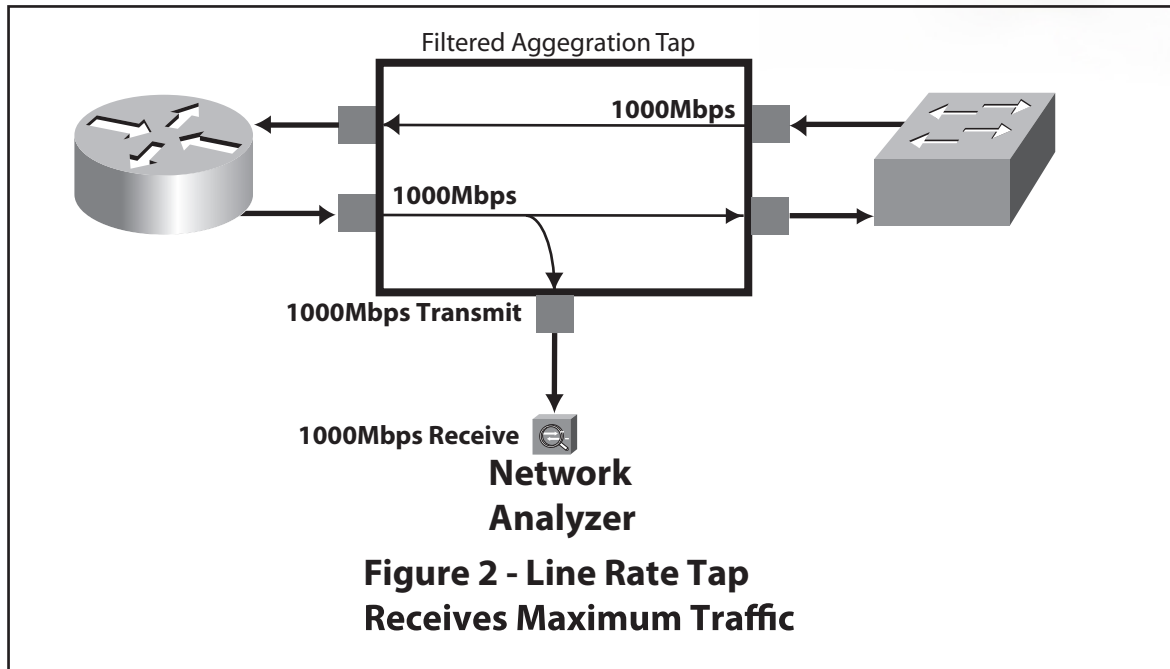
Since the analyzer is oversubscribed the only way to realistically capture interesting traffic is to filter packets before sending them to the analyzer, otherwise traffic is missed.

Interesting Traffic

Determining what traffic is appropriate to filter is the next step. First, allow full line rate from one side of the network to pass through the Filtered SINGLEstream™ to the analysis tool. See Figure 2. Since the line speed is 1Gbps and the receive side of the network interface card (NIC) is 1Gbps, this technique permits a full review of traffic in a non-blocking environment, and helps determine interesting (or not interesting) traffic traveling in one direction. Next, permit traffic flowing in the other direction through the Filtered Singlestream™ as unfiltered and non-aggregated traffic. After this step, raw traffic from each direction can be reviewed to determine interesting traffic.

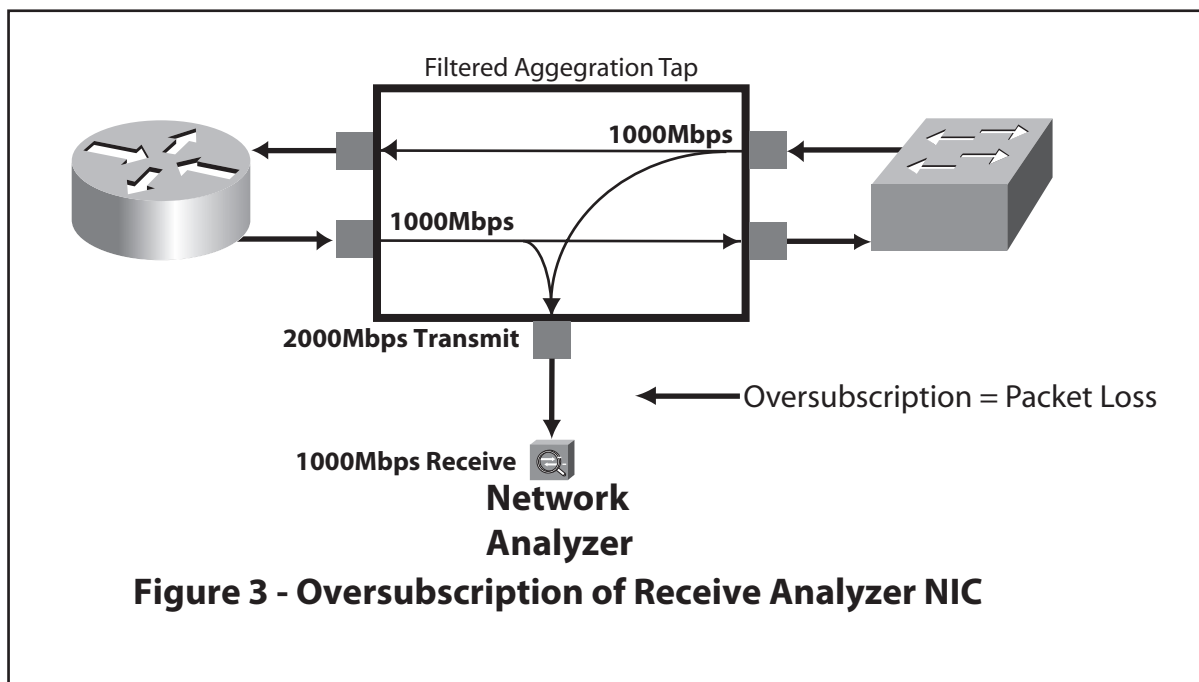


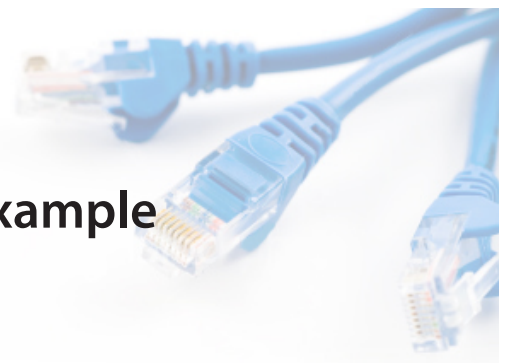
Port and Address Filtering Example



Aggregation

The Filtered SINGLEstream™ Link Aggregation Tap will combine one or more full duplex streams of data from one or more network segments, reassemble the conversation, and send a copy to up to four connected monitoring devices. See Figure 3. Aggregation can reassemble conversations that are routed through alternate paths like primary/secondary firewalls, Gigabit EtherChannel, load balanced servers, and asymmetrically routed traffic. Note that these fully utilized links have oversubscribed the receive side of the Analyzer's NIC. Oversubscription means that packets are dropped before reaching the Analyzer.



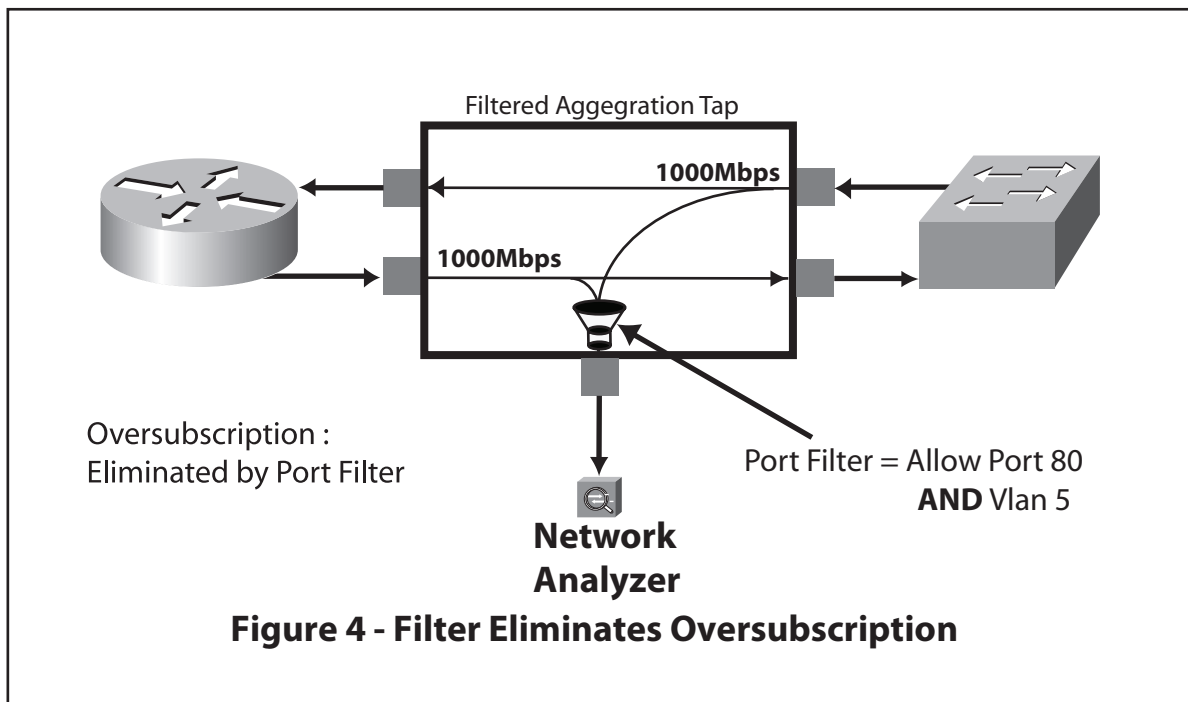


Port and Address Filtering Example

Filtering

Oversubscription is eliminated by hardware based filtering. Advanced filtering technology can filter network traffic sent to any of the monitoring ports based upon IP address, port number, MAC address, VLAN, frame, protocol type, or customizable offsets in the IP header.

Each monitoring port on the Filtered SINGLEstream™ has its own filter. There are four monitoring ports, but this example shows only one. That filter can be a combination of IP address(s), Port number(s), MAC address(s), VLAN(s), Frame, or Protocol types. These filters can be added together to filter a port number from a particular VLAN. Since each monitor port has its own filter, each monitoring tool sees only the traffic that it finds interesting. In this example, only port 80 traffic from Vlan 5 is allowed through to the monitoring tool.



Summary

To apply appropriate filters for network and security monitoring and analysis, allow unidirectional traffic to flow to the packet capture device, as non-aggregated and non-filtered traffic. Traffic captured from this step will show all traffic, which will aid in deciding what type of traffic should be analyzed. Apply filtering at specific monitoring ports based on the type of sensor or probe connected, and the type of traffic it needs to see. Based on the Filtered Aggregation Tap technology, traffic between network devices continues to flow, even after a power interruption to the Filtered Aggregation Tap. Per port filtering, means that each monitoring port, sees the traffic it needs.