Handling Microbursts

Microbursts

Various data types, flows, and applications often exhibit behavior with rather high amounts of bursts and jitter when transported across IP networks. These can be due to the packetization and packet handling processes within network switches and routers, or can also be an "as designed" function of the application and traffic. Some network switches and routers may also buffer data when sending out mirror or SPAN ports (used for monitoring and analysis purposes), thereby introducing severe jitter and bursty behavior. Since the bursts themselves occur over rather short periods, they are often referred to as microbursts.

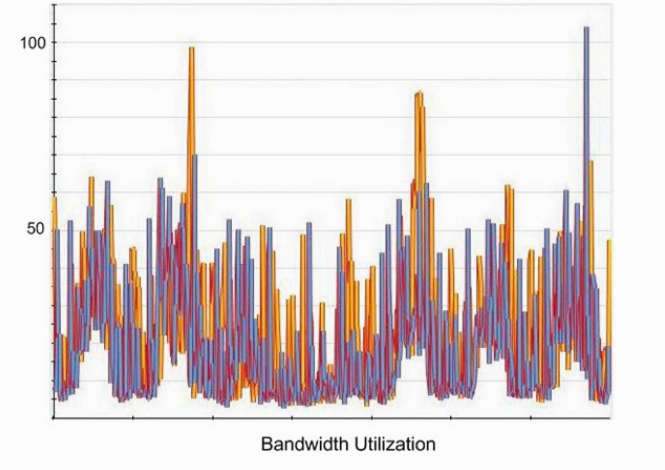

Figure 1: Intermittently Bursty Traffic applied independently or together as needed by the user depending on the monitoring application.

An example of an application with "as designed" microbursts is IPTV, where the video TV channel is being streamed from a central office, and, to enable an "instant channel change" experience for the end user, video streams for all channels are buffered somewhere more locally to the premises. Then, when the user selects a different channel to the one that is being watched, the locally buffered channel is blasted to the user in a rapid dense burst until the centrally located video source is able to catch up and switch the stream over for the new channel. In fact, compressed/encoded video traffic is already bursty by nature, due to the vastly different I, P, and B frame sizes. Another example is the deliberate generation of data bursts to help manage and control congestion through an IP network, known as burst congestion control, where a network controlling device allocates bursts of data for specific intervals over specific routes.

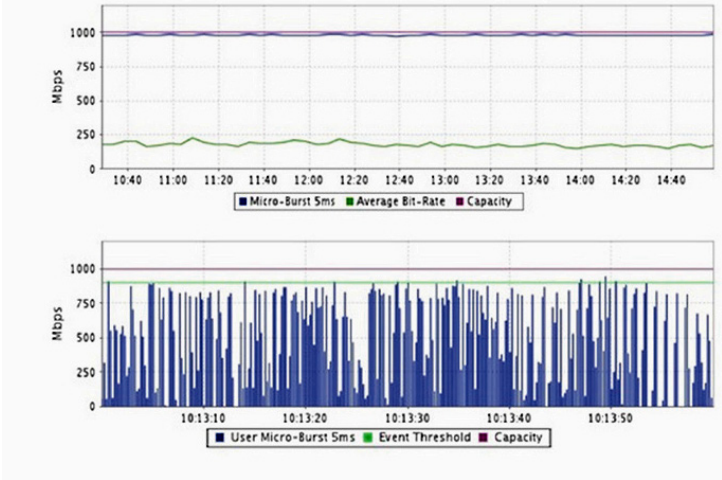

Figure 2: Consistently Bursty Traffic.

Although microbursts may seem counter intuitive, their existence means that, while the apparent utilization of a network or port may appear to be low over a period of 1 second, which is a typical coarse utilization monitor sampling time, there may still be significantly high utilization spikes for short sub-second durations that will not be noticeable when averaged over a 1 second period.

The graph in Figure 3 shows several microbursts of traffic. This was taken from an aggregated output port.

The resolution of the graph is .001 seconds (1 ms). The microburst pattern in the graph illustrates that while most of the traffic is not of a bursty nature, there are periodic microbursts of traffic roughly every tenth of a second.

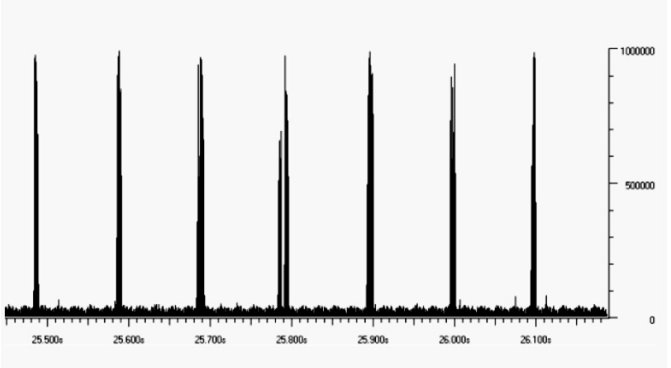

Figure 3: Periodic Microbursts.

The X axis is displayed in 100 ms major increments. Minor increments are in 10 ms. The entire graph is 600 ms.

The Y axis scales to 1,000,000 bits. This is because a Gigabit Ethernet port transmits up to 1,000,000 bits per millisecond.

Effect on Monitoring

This places stress on traffic capture devices when used to aggregate, speed convert, or load balance traffic. In the case of aggregation from more than one network port into fewer monitor ports, any microbursts in the utilized links will become more significant when aggregated to form a higher utilized link – in many cases microbursts on different links may occur, simultaneously, resulting in much higher microbursts on the aggregated monitor port.

Microbursts can be created by the simple process of aggregation itself, where simultaneous arrival of packets on aggregated input links may result in briefly oversubscribed output ports. The oversubscription is essentially when the inter-packet gap is too small for the given output port(s).

In the cases of speed conversion, from one or more higher-bandwidth network ports across several lower-bandwidth monitor ports, microbursts are created as a result of groups of packets arriving at a much higher rate, i.e. inter-packet gaps are smaller, than the output port can handle.

Port Aggregation Requires Buffering

An aggregating tap requires buffering capability to perform the function of merging multiple input streams to one or more output streams. A received packet is only placed in a buffer to allow interleaving of packets and needs to be retained in the buffer until capacity is available on each targeted output port for transmitting.

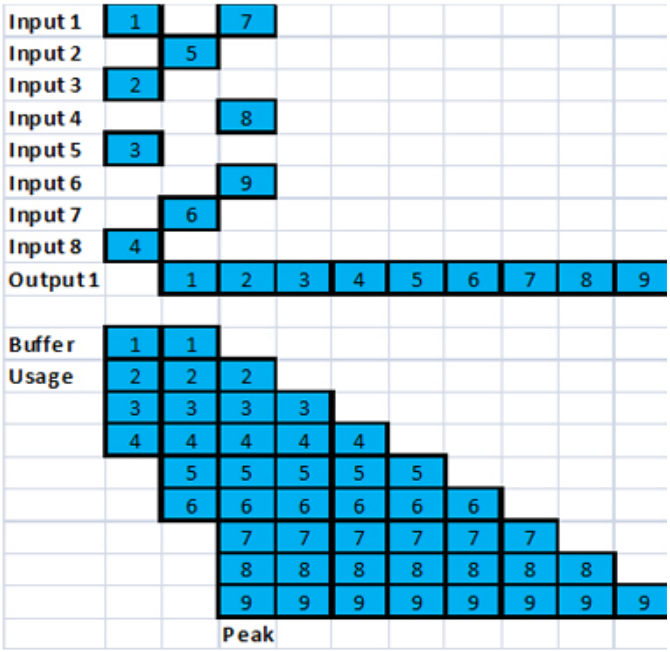

Figure 4: Simplified Aggregation Buffer Usage.

The conceptual illustration in Figure 4 shows eight input ports feeding one output port, where a microburst of up to nine packets is generated by the act of aggregation. The section labeled Buffer Usage shows how the buffers were allocated during the period measured. The column with the Peak label, at the bottom, highlights the largest amount of buffer space that was in use. Each column represents minimum inter-packet delay for the output port.

It is the gaps between the packets that allow the buffered bursty packets to drain to the output port. Typical Ethernet traffic has long gaps between packets, with occasional bursts of back-to-back packets having minimum inter-packet delay.

Normal buffering that exists in traffic capture devices is generally unable to cope with such extremely high (although brief) bursts of oversubscription on the monitor ports, resulting in buffer overflow and loss of monitored packets. The standard buffering was designed for network traffic profiles that have minimal microbursts and/or have relatively low average utilization.

Solution

The only way to prevent packet loss in these circumstances is to have ample buffering to smooth out bursty traffic and regulate it according to the speed (or rate) of the destination link, i.e. monitor port.

To address this problem of microbursts, the NETSCOUT nGenius® Packet Flow Switch high data-burst buffer (HDBB) feature provides a much larger than normal buffer behind network ports, which enhances the ability to handle the forwarding of bursty data that grossly exceeds the maximum bandwidth of output ports, without losing any of the packets. This applies to when aggregating traffic, load balancing traffic, or speed conversion.

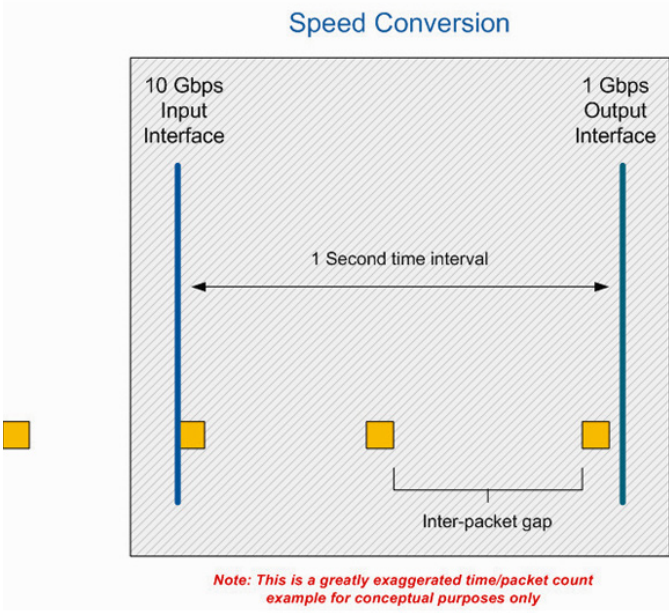

Figure 5: Speed Conversion; Long Inter-Frame/Packet Gap.

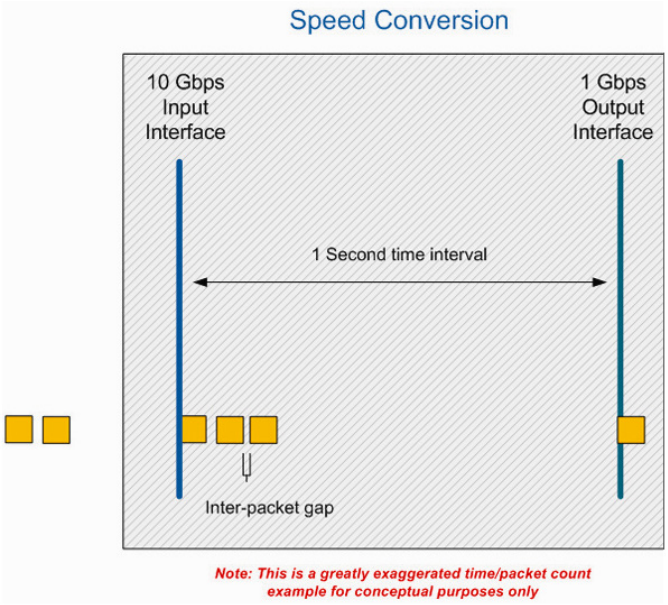

Figure 6: Speed Conversion; Short Inter-Frame/Packet Gap Bursts.

This is achieved by providing between 1,000 to 4,000 times more buffering behind each port than is available, in total, on a normal tap. Although, when smoothing out the bursts and fitting the packets into each aggregated or load balanced monitor port, the buffering may introduce some unavoidable additional latency, it will not introduce any latency during normal traffic patterns without microbursts.

Besides additional buffering, other methods of addressing bursty traffic in the monitoring network include:

- Filtering the traffic to reduce the traffic towards the monitor ports that are being oversubscribed; this can be effective in situations where filtering is able to be applied
- Balancing the traffic across more monitor ports/tools; this has limited success because maintaining flow-awareness means that a single flow to a single port can quite easily oversubscribe that port

Measurement

If there is uncertainty or doubt at all about the existence of microbursts in a network, then measurements may need to be conducted to confirm this.

Solution

The NETSCOUT nGenius vCapacity feature provides the ability to measure at a sub-millisecond level and record the network utilization with a millisecond granularity. This capability will provide evidence of the occurrence of microbursts, and this data can be used on a continual basis to monitor the ongoing microburst activity within your network.

The nGenius 2200 and 4200 Series Packet Flow Switch families support both HDBB and vCapacity as selectable options.

NETSCOUT

Americas East
310 Littleton Road
Westford, MA 01886-4105
Phone: 978-614-4000
Toll Free: 800-357-7666

Americas West
178 E. Tasman Drive
San Jose, CA 95134
Phone: 408-571-5000

Asia Pacific
17F/B
No. 167 Tun Hwa N. Road
Taipei 105, Taiwan
Phone: +886 2 2717 1999

Europe
One Canada Square
29th floor, Canary Wharf
London E14 5DY, United Kingdom
Phone: +44 207 712 1672

NETSCOUT offers sales, support, and services in over 32 countries.

For more information, please visit www.netscout.com or contact NETSCOUT at 800-309-4804 or +1 978-614-4000