



---

# *HANDLING MICROBURSTS*

## White Paper

## 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.

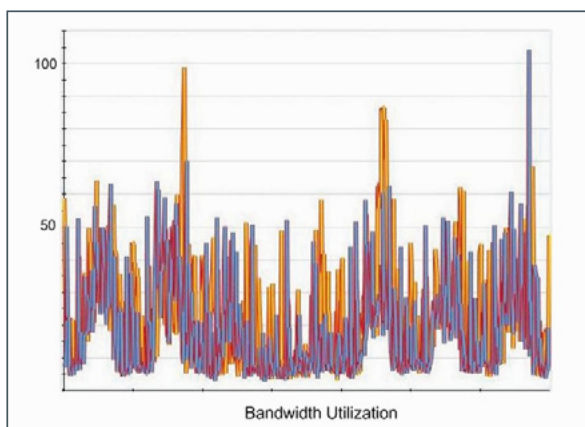


Figure 1. Intermittently Bursty Traffic applied independently or together as needed by the user depending on the monitoring application.

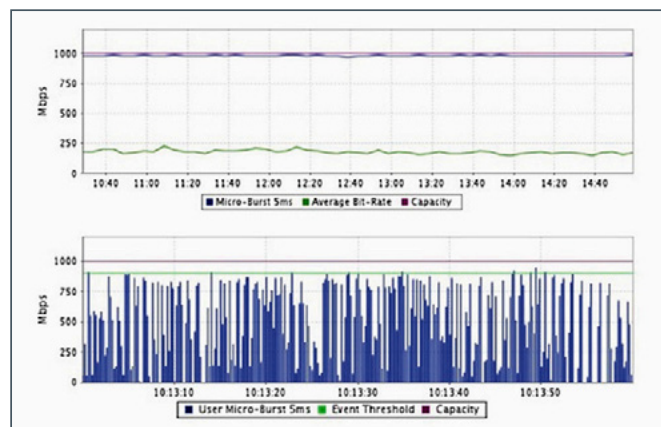


Figure 2. Consistently Bursty Traffic

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.

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.

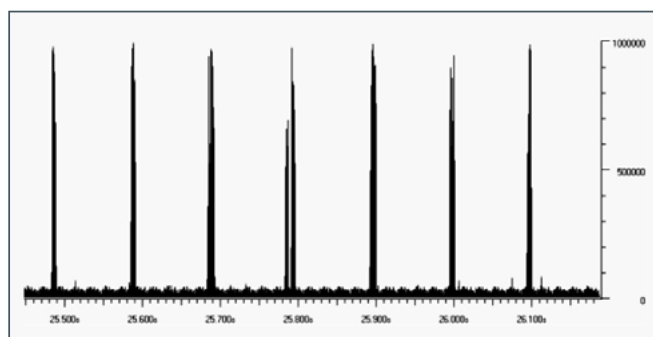


Figure 3. Periodic Microbursts



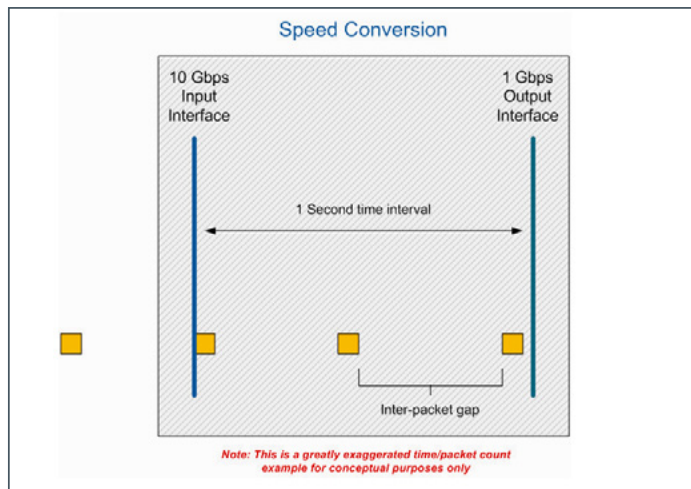


Figure 5. Speed Conversion; Long Inter-Frame/Package Gap

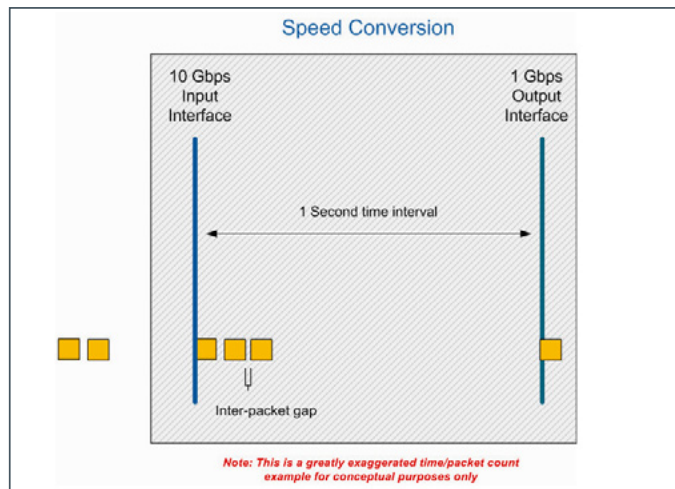


Figure 6. Speed Conversion; Short Inter-Frame/Package Gap Bursts

The High Data Burst Buffer feature is available on the Expert editions of VSS’ Distributed Traffic Capture Systems™ (DTCS) range of products.

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.

VSS Monitoring’s 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 can be used on a continual basis to monitor the ongoing microburst activity within your network.

The vCapacity feature is available on the Expert editions of VSS’ DTCS range of products.



Network Visibility. Optimized.

USA  
 (Corporate HQ)  
 + 1 650 697 8770 phone  
 + 1 650 697 8779 fax  
 1850 Gateway Drive - Suite 500  
 San Mateo, CA 94404  
 USA  
 www.vssmonitoring.com

Japan  
 + 81 422 26-8831 phone  
 + 81 422 26-8832 fax  
 T’s Loft 3F, 1-1-9,  
 Nishikubo, Musashino,  
 Tokyo, 180-0013  
 Japan  
 www.vssmonitoring.co.jp

China  
 + 86 10 6563-7771 phone  
 + 86 10 6563-7775 fax  
 C519, 5 Floor,  
 CBD International Tower  
 16 Yong’An Dong Li,  
 Beijing, China 100022  
 www.vssmonitoring.com.cn

VSS Monitoring, Inc. is the world’s leading innovator of Distributed Traffic Capture Systems and network taps, focused on meeting the rapidly evolving requirements of security and performance conscious network professionals. Distributed Traffic Capture Systems herald a new architecture of network monitoring, one which fundamentally improves its capability and price-performance.

VSS, Distributed Traffic Capture System, DTCS, vCapacity, vAssure, vStack+, and LinkSafe are trademarks or registered trademarks of VSS Monitoring, Inc. in the United States and other countries. Any other trademarks contained herein are the property of their respective owners.