Comparing Simulated Packet Loss and Real-World Network Congestion

November 2010
COMPARING SIMULATED PACKET LOSS AND REAL-WORLD NETWORK CONGESTION

Executive Summary

WAN simulators are useful for testing the impact of latency and bandwidth constraints; however, caution should be used when using WAN simulation devices to generate packet loss. Many WAN simulators are incapable of accurately simulating the most common type of packet loss found in real-life networks—congestive packet loss, which is characterized by bursty loss patterns. Rather, the more simplistic WAN simulators assign a fixed probability of loss to each individual packet, leading to loss patterns that are more characteristically caused by bit errors in the transmission media.

While Forward Error Correction (FEC) and other parity checking techniques can be effective when applied to single-drop patterns resulting from transmission bit errors and simplistic WAN simulators, these error correction techniques are much less effective when applied to bursty consecutive-loss patterns that are far more prevalent in IP networks.

To avoid misleading and skewed test results, Riverbed recommends avoiding use of low-end WAN simulators that are incapable of accurately simulating the bursty packet loss patterns resulting from network congestion. Using such devices to simulate packet loss will not lead to an accurate assessment of the performance and behavior of the devices in a real-life network environment.

Types of Packet Loss

Packet loss results whenever the network fails to deliver a packet to its intended destination. The causes and types of packet loss—their impacts on network performance—have been extensively analyzed and modeled in a number of different studies. These studies generally characterize the two primary causes of packet loss in IP-based networks, which are:

- **Congestive loss**: Results when the network is unable to support the amount of traffic that it receives. Router buffers become full, forcing it to drop packets. Rarely is just a single packet dropped—usually congestion-related packet loss is characterized by patterns consisting of sequences of consecutive dropped packets. Furthermore, loss levels (as measured in loss percentage) tend to increase when network utilization increases and decrease when network utilization decreases.

- **Loss due to transmission bit errors**: Bit errors result from transmission channel noise, distortion, signal weakness, bit synchronization, or attenuation. Packet loss resulting from bit errors is characterized by low-density individual packet drops at random intervals. Unlike the case with congestive loss, packet loss resulting from transmission bit errors (as measured in loss percentage) usually remains constant and does not change with the level of network utilization.

The above two types of packet loss result in very different network behaviors. To illustrate the difference between them, let’s suppose we have two WAN links—one is afflicted with misconfigured telecom equipment resulting in a steady bit error rate, while another is simply an over-subscribed and over-utilized WAN link for a short instant in time. While both WAN links might be afflicted with so-called 1% packet loss, nevertheless their behavioral characteristics are very different. To transmit a given file carried in 10,000 packets, both WAN links will drop 100 packets. But the WAN link with the bit error will drop a single packet at an average interval of roughly every 100 packets, while the congested WAN link may drop 5-10 consecutive packets each on roughly a dozen instances for the duration of the file transfer. Although both WAN links drop the same number of packets and exhibit the same level of reliability as far as their ability to deliver packets, nevertheless a technique designed to address the type of packet loss behavior in the first link won’t necessarily work in addressing the packet loss behavior for the other WAN link.

It’s important to realize that loss due to bit errors is very rare among terrestrial WAN links commercially provided by telecommunications vendors. Fiber-optic technology now affords the ability to achieve extremely low bit error rates of $10^{-12}$ to $10^{-15}$.

---

for virtually error-free data transmission. Furthermore, most telecom transmission equipment overlay additional parity checking capabilities at the physical layer through Forward Error Correction (FEC) techniques (more on this later), which further reduce or eliminate packet loss resulting from these already-low bit error rates.

Due to the rarity of bit-error related packet loss, almost all packet loss encountered in terrestrial IP networks will most likely be a result of network congestion. And as described earlier, congestive packet loss patterns are characterized by consecutive losses in sequence. This is vividly illustrated in a study by Raghavendra, who measured (a) packet loss and (b) loss lengths in a typical residential broadband network. Loss length refers to the number of consecutive packets that are dropped by the network in each packet loss incident. The cumulative distribution function (CDF) measured by Raghavendra shows that although the packet loss rate (graph a) was below 1% for about 90% of the time, the median loss length (CDF = 0.5) was about 5 consecutive lost packets for wired broadband, and about 15 consecutive lost packets for wireless broadband (graph b). More importantly, graph (b) indicates that in the observed residential broadband network, single isolated packet drops are very rare, occurring with a probability of far less than 0.1.

![Graphs showing loss rates and loss lengths](image)

Raghavendra, 2009

Use caution when using WAN simulators to simulate packet loss

Use of WAN simulators is an understandable approach for customers evaluating various WAN optimization solutions. They allow for convenient and accurate measurement on the impact of bandwidth constraints and WAN latency, without having to deploy a live proof-of-concept (POC) trial.

Most WAN simulators also have the capability of generating packet loss. But before using a WAN simulator to test packet loss, it is important to understand what types of packet loss the WAN simulator is capable of generating. Just about every WAN simulator—including a simple Network Nightmare—is capable of generating packet loss behavior that assigns a fixed probability of loss to each individual packet in the test stream. The result is a low-density packet loss pattern is representative of loss caused by a bit error, as described in the previous section. On the other hand, only the more sophisticated WAN simulators are capable of generating “bursty” loss patterns that more accurately simulate the effects of network congestion. Such devices are available from vendors such as Shunra and Packet Storm.

Only in the most extreme cases is it appropriate to test with a simplistic WAN simulator that generates packet loss by assigning fixed drop probabilities to individual packets. As discussed previously, packet loss resulting from bit errors is very

---

Simulated Packet Loss and Real-World Network Congestion

rare in commercial-grade WAN links. Unless this is a known problem in the WAN environment, use of such a WAN simulation device may lead to skewed test results that do not accurately reflect the performance for WAN optimization devices deployed in the real-life network environment. Rather, if it is necessary to test the effects of congestive packet loss, it's important that bursty packet loss patterns (including consecutive packet drops) be generated as part of the test. This can be done through use of a load generator such as IP Perf or LoadSim to source additional traffic flows that congest a bandwidth-constrained simulated WAN link. Alternatively, use of more sophisticated WAN simulation devices may be considered as long as they are specifically configured to generate bursty packet loss patterns that drop multiple consecutive packets.

**Why Forward Error Correction (FEC) is inappropriate for congestive packet loss**

As with any significant technical challenge, it's important that the chosen solution is appropriate for the problem. Earlier in this document we discussed how FEC can be effective for packet loss resulting from bit errors in the transmission media. However, some vendors have naively attempted to extend the application of FEC beyond its original intended purpose, claiming that FEC can be useful for any and all types of packet loss, including loss resulting from network congestion. But there are serious problematic issues with these dubious claims.

![Diagram of FEC process](image)

**FEC is a technique where additional traffic for parity information is injected into the traffic stream. As long as no more than one packet is lost within each protected interval, the lost packet can be regenerated through a calculation using the parity data.**

Forward Error Correction (FEC) is a technique that injects parity information into the original traffic stream. As long as no more than one packet is lost within the protection interval, the surviving packets can be compared to the added parity data in order to re-generate the lost packet. The scheme is analogous to a RAID-protected computer system, where multiple disks are used to provide high availability of the disk-resident data.

However, if more than one packet is lost within the FEC protection interval, then the FEC mechanism fails to achieve its objective. In this case, the lost packets cannot be regenerated, and the additional parity overhead information simply adds to the network utilization, worsening the congestion problem. Such a failure is analogous to a failure of more than one disk in a RAID-5 protected computer system.

**Applying FEC to simplistic loss patterns generated by a WAN simulator leads to deceptively superior results compared to actual results that would be achieved with the same levels of congestive packet loss in a real-life network.** It is important that the correct type of packet loss be simulated. Because almost all packet loss in real-life networks is congestion-related loss, then it is important that bursty packet loss patterns be generated when testing the effects of a product's FEC capabilities.
Congestive packet loss is characterized by bursty loss patterns where multiple consecutive packets are lost. FEC is ineffective when applied to bursty packet loss patterns.

Finally, it’s important to realize that use of FEC is not without cost; using FEC involves adding overhead traffic through the parity information injected into the original traffic stream, which consumes bandwidth that otherwise would have been available to deliver additional data. The amount of parity data injected depends on the level of packet loss anticipated in the network. For example, protecting against an anticipated 5% packet loss requires an additional ~5.26% overhead in additional parity data, while protecting against an anticipated 20% packet loss requires 25% overhead.

What about “adaptive” FEC?

But the vendor advocating FEC may claim that the additional traffic overhead is not a problem, because their implementation of FEC “adapts” to the appropriate level of packet loss. When there is little or no packet loss in the network, their FEC ratchets down the protection level, thereby reducing the amount of traffic overhead. When packet loss increases, their implementation of FEC increases the protection level, which of course increases the amount of traffic overhead.

The main problem with “adaptive” FEC is that its behavior is exactly the opposite of what is necessary to deal with congestion-related packet loss. As discussed earlier, congestive packet loss tends to increase with higher network utilization levels. But if a vendor’s “adaptive” FEC reacts to congestive packet loss by increasing the amount of overhead traffic, then the congestive packet loss problem can become worse. In severe instances, such behavior can potentially contribute to a congestion collapse scenario such as those that were common in the early days of the Internet, before the widespread adoption of Van Jacobson’s TCP congestion control mechanisms. In fact, section 5 of RFC 2914 specifically warns that an adaptive FEC mechanism that dynamically adjusts its protection level to the amount of measured packet loss is especially destructive to the integrity of the IP network.

Other tools for addressing packet loss

There are a number of other tools available to address congestive packet loss; unlike the FEC approach, these other tools do not generate additional traffic overhead, and they generally do not worsen the network congestion that may be causing the packet loss in the first place. In the Riverbed Steelhead product, these tools include MX-TCP, LTTS, TCP-Westwood, and TCP-Vegas, each of which engage various approaches to avoid performance drop-off due to TCP congestion avoidance and slow start processes. Of these, MX-TCP is the most aggressive in its behavior to sustain transmission throughputs despite the occurrence of packet loss.

---

Summary

Network congestion is by far, the most common cause of packet loss in real-life IP networks. Congestive packet loss is characterized by loss of multiple consecutive packets. But many WAN simulators are not equipped to simulate this type of packet loss; rather, when configured to inject loss, most simulators will simply assign a fixed probability of loss to each individual packet in the test stream. Because such a packet loss pattern rarely occurs in real-life, the test results will not reflect real-life performance and behavior when the packet loss is applied to WAN optimization devices.

Forward Error Correction (FEC) techniques can be effectively applied to recover bit-error related packet loss. However, FEC is ineffective—and potentially harmful—when applied to packet loss that results from network congestion. Properly testing a product’s FEC capabilities requires that bursty packet loss patterns—the type of packet loss prevalent in real-life IP networks—be used in the simulation test.

About Riverbed

Riverbed Technology is the IT infrastructure performance company. The Riverbed family of wide area network (WAN) optimization solutions liberates businesses from common IT constraints by increasing application performance, enabling consolidation, and providing enterprise-wide network and application visibility—all while eliminating the need to increase bandwidth, storage or servers. Thousands of companies with distributed operations use Riverbed to make their IT infrastructure faster, less expensive and more responsive. Additional information about Riverbed (NASDAQ: RVBD) is available at www.riverbed.com.