PacketLoss

Packet Loss

Packet loss is the probability of a packet to be lost in transit from a source to a destination.

A One-way Packet Loss Metric for IPPM is defined in RFC 2680. RFC 3357 contains *One-way Loss Pattern Sample Metrics*.

Decomposition

There are two main reasons for packet loss:

Congestion

When the offered load exceeds the capacity of a part of the network, packets are buffered in queues. Since these buffers are also of limited capacity, severe congestion can lead to queue overflows, which lead to packet drops. In this context, severe congestion could mean that a moderate overload condition holds for an extended amount of time, but could also consist of the sudden arrival of a very large amount of traffic (burst).

Errors

Another reason for loss of packets is corruption, where parts of the packet are modified in-transit. When such corruptions happen on a link (due to noisy lines etc.), this is usually detected by a link-layer checksum at the receiving end, which then discards the packet.

Impact on end-to-end performance

Bulk data transfers usually require reliable transmission, so lost packets must be retransmitted. In addition, congestion-sensitive protocols such as TCP must assume that packet loss is due to congestion, and reduce their transmission rate accordingly (although recently there have been some proposals to allow TCP to identify non-congestion related losses and treat those differently).

For real-time applications such as conversational audio/video, it usually doesn't make much sense to retransmit lost packets, because the retransmitted copy would arrive too late (see delay variation). The result of packet loss is usually a degradation in sound or image quality. Some modern audio/video codecs provide a level of robustness to loss, so that the effect of occasional lost packets are benign. On the other hand, some of the most effective image compression methods are very sensitive to loss, in particular those that use relatively rare "anchor frames", and that represent the intermediate frames by compressed differences to these anchor frames - when such an anchor frame is lost, many other frames won't be able to be reconstructed.

Measurement

Packet loss can be actively measured by sending a set of packets from a source to a destination and comparing the number of received packets against the number of packets sent.

Network elements such as routers also contain counters for events such as checksum errors or queue drops, which can be retrieved through protocols such as SNMP. When this kind of access is available, this can point to the location and cause of packet losses.

Reducing packet loss

Congestion-induced packet loss can be avoided by proper provisioning of link capacities. Depending on the probability of bursts (which is somewhat difficult to estimate, taking into account both link capacities in the network, and the traffic rates and patterns of a possibly large number of hosts at the edge of the network), buffers in network elements such as routers must also be sufficient. Note that large buffers can be detrimental to other aspects of network performance, in particular one-way delay (and thus round-trip time) and delay variation.

Quality-of-Service mechanisms such as DiffServ or IntServ can be used to protect some subset of traffic against loss, but this necessarily increases packet loss for the remaining traffic.

Lastly, Active Queue Management (AQM) and Excplicit Congestion Notification (ECN) can be used to mitigate both packet loss and queueing delay (and thus one-way delay,round-triptime and delay variation).

References

- *A One-way Packet Loss Metric for IPPM,* G. Almes, S. Kalidindi, M. Zekauskas, September 1999, RFC 2680
- *Improving Accuracy in Endtoend Packet Loss Measurement,* J. Sommers, P. Barford, N. Duffield, A. Ron, August 2005, SIGCOMM'05 (PDF)
    - Main.SimonLeinen - 01 Nov 2004