eSubnet Fragment Article

Network Slowdown

Corporate computer users often claim that their network is slow. The challenge is determining the source, from the potentially numerous causes for these slowdowns. I am going to identify a few of these sources which, individually or in concert, can cause the noticeable reductions in performance that everyone complains about.

Transmission Control Protocol (TCP) is the primary underpinning technology for IP traffic today. TCP is a stateful protocol, which is to say, there are mechanisms in place to ensure that traffic is delivered. With TCP, data is sent out in groups of packets, these streams of data are known as the TCP window. When there is packet loss or corruption, two events occur; the data is retransmitted, and the TCP window size is reduced, resulting in perceived slower network connectivity.

Network Tubes
Bandwidth is the capacity of a network link to move or transmit data, which is measured in bits per second. When diagnosing slow network performance this is where we look first. Is there enough bandwidth for the desired level of traffic passing over the network?

Typically, LAN deployments are designed with normal usage in mind. However, the regular bandwidth may be overloaded during the transfer of large amounts of data during backups. This is a relatively easy fix as backups and other high bandwidth activities can be scheduled to run after normal business hours thus avoiding this cause of “traffic jams” by proper planning.

WAN and Internet accesses are easily subject to network slowdown, their higher costs leads to the purchase of “thinner tubes” or less bandwidth than internally. Internet access requires ever more bandwidth as online content is increasingly media rich. Sites such as YouTube, Digg, and VideoShift use Flash delivered over HTTP; for example, 5 people at an organization looking at the same video will generate 5 traffic streams. The fix for this is a web-cache proxy, which will help reduce the traffic over the Internet connection, by caching such content locally, and reducing the draw on bandwidth.

Latency
In networking, latency (measured in milliseconds) is the time it takes for a packet to go from source to destination. There are many elements within a network path which can increase latency, such as media transformation (Ethernet to serial), insufficient buffer space in routers, badly configured links, and packet size.

Wherever there is a change at the Layer-1 or Layer-2 network technology, the router rewrites the packet. Packet rewrites take time and will increase the packet’s latency, by definition the time it takes to move from source to destination. Classic examples of this are serial connections such as a T1. A T1 imparts a latency of 2-5ms vs. Ethernet’s 0.3ms. Broadband modems for cable or DSL impart 10-20ms of delay. When a server is connected to the Internet by a T1, providing 1.54 Mbps, it may provide poorer performance than an Ethernet over fiber connection capped at 1.0 Mbps.

An additional side effect of changing the Layer-1 or Layer-2 medium is the change in MTU. Changing from a larger MTU to a smaller MTU results in fragmentation, which are more work for the router and another cause for perceived slowness. Below is a list of network technologies and their associated MTU:

MTU	Technology
17914	6 Mbps Token Ring
4464	4 Mbps Token Ring
4352	FDDI
1500	Ethernet
1480	PPPoE (WAN Miniport)

Packet buffers are used in routers to hold the data until the line is clear for another transmission. If the amount, size of packet, or number of packets exceed the space available in buffer memory something has to give and packets are dropped. Once again, retransmission and reduction of the TCP window occurs.

Jitter
Jitter refers to the unequal timing variation in the transmission of data packets. Jitter is of concern in situations where the quality of a streaming signal is critical to an application’s success. The main sources of Jitter are buffer capacity, packet size, and the synchronous nature of the line itself.

Certain network technologies are susceptible to jitter. IP over ADSL is prone to jitter, especially with large file transfers or where a residential grade router is installed in place of business grade device. Contrast IP over ADSL with ATM which has a consistent frame size and clock-based transmission mechanism, it is practically free of jitter. If jitter is a concern, we can work to select a more constant network technology.

Conclusion
Oddly enough the errors that you do see indicate that your local area network and the Internet are both working as they should. It is the detail

you do not see, which may cause slowdowns in the delivery of applications and content. A case in point is the “HTTP 404, file not found” notice; it only indicates that the web server could not find the file, the packets themselves, more often than not, have made the trip to the server just fine.

It is the errors you don’t see such as packet loss, jitter and congestion which are evident when a web page is found but takes a long time to load. To see these errors you need to deploy a packet-sniffer such as Wire Shark or TCPDump.

Mission critical applications and time sensitive connectivity require a clean network. The number of media conversions, the packet buffer overruns, the number of hops (accumulating latency and prospect of errors) and the network segments susceptible to congestion all add up to increasing the opportunity to slow down network traffic and thereby reducing the efficiency of staff.

Originally published OCT, 2009

About the Author

Richard Danielli is the founder and President of eSubnet Enterprises. He has broad expertise in the fields of networking and data security. Based in Toronto, eSubnet provides superior customized solutions for networking and data security. Additional articles are available at http://www.esubnet.com/fragment.html.

Reprints