TABLE OF CONTENT

TABLE OF FIGURES

1: NETWORK CONGESTION

Network traffic, also referred to as data traffic, is the amount of data moving across a network at a specific point in time. Network data is normally found in network packets and they are what causes load in a network. Network traffic is the main component for measurement and control of network traffic.

On the other hand, congestion is a crucial issue of packet-switched network (transfer of data broken down into several segments across many networks). Network congestion occurs when the number of packets being sent through a network is greater than the number of packets the network can handle.

Congestion can occur in any system that involves waiting. Routers and switches have ‘queues-buffers’ that detain the packets before and after processing hence leading to congestion. Let’s take an example of a router which contains an input queue and an output queue for every interface. When a packet reaches the incoming interface, it goes through three processes before actually leaving, as shown below.

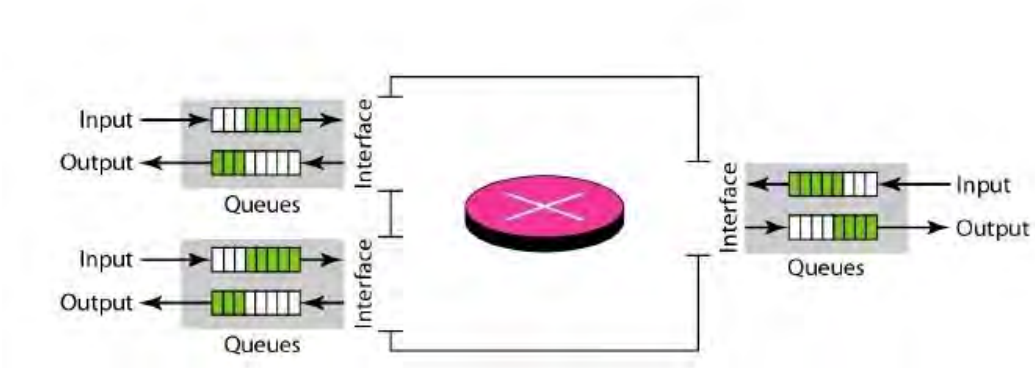

Figure 1 Queues in a router

1. The packet is added to the input queue (at the end) while it waits to go through checking.

2. The packet is taken from the input queue when it reached the front of the line by the processing module. The processing module then utilizes its routing table and the address of the receiver to locate the path.

3. The packet is then placed in the appropriate output queue while it waits to be transmitted. There are 2 points to be noted here. First, if the rate at which the packets arrive is greater than the rate at which the packets are being processed, then the input queues keep on increasing. Secondly, if the rate at which the packet at which the packets are departing is lower than the rate at which the packets are being processed then the output queue once again keeps on increasing.

2: CAUSES OF NETWORK CONGESTION

NON-COMPATIBLE OR OBSOLETE HARDWARE

Hardware can be the reason behind bottleneck in a network. Though network capacity and speed are the primary causes, if the hardware is not kept up to date or compatible, it still creates congestion. Examples of hardware would be switches, routers and servers among others. Hardware also includes wire and cable connections. A typical example would be Ethernet cables which have different categories of data speed. If the network requires higher speed, the Ethernet cable has to be replaced by another one.

LARGE NUMBER OF DEVICES

All networks have a limited capacity and this limited capacity further restraints the amount of bandwidth and traffic that the networks can allow before it begins to influence performance negatively. Hence, if there are too many devices connected to the network, then the network might become overburden with requests for data.

BANDWIDTH HOGS

A bandwidth hog is a device or user that uses more data compared to other devices (by mistake or purposefully). If the usage of the hog is more than the expected level, then it definitely causes the network to be overcrowded with packets, especially there are more than a few hogs.

POOR NETWORK DESIGN AND SUBNETS

Congestion can also be the result of a poorly designed network. A network should be designed in such a way that it covers and connects every part of the network. In the case of subnets (subnet: a network inside a network), it should contain devices permanently connected to the network. If a subnet is recognized as a big data consumer, then it should have an appropriate size.

3: EFFECT OF CONGESTION ON NETWORK TRAFFIC

LATENCY

Also known as Delay, latency is the time taken for a packet to reach its destination from its sender. A very common example would be time taken for a webpage to load. The time taken is the result of how long the packets took to travel from the web server to the client. Another example is online video streaming.

PACKET LOSS

Packet loss is a more serious issue than latency. While in the latter, the packet will take time to reach (but will reach), in this case, the packet is loss or discarded. If packets arrive too fast for the node to process them (make routing decisions) or faster than packets can be cleared from the outgoing buffers, then eventually packets will arrive for which no memory is available., hence they are discarded.

Here, the consequence of congestion is very grave since the packet forms part of a bigger data, without which the data will make no sense or cause errors. This is not good for applications like Voice over IP (VoIP) that may result in dropped calls or other effects.

TIMEOUTS

One more repercussion of network congestion can lead to timeouts in various applications. Many connections will not keep on waiting indefinitely for packets to arrive. Therefore, this can result in lost connections.

4: NETWORK PERFORMANCE

Congestion control utilizes two factors that measure the performance of a network: delay and throughput. The following diagrams show these two performance measures as function of load in a network.

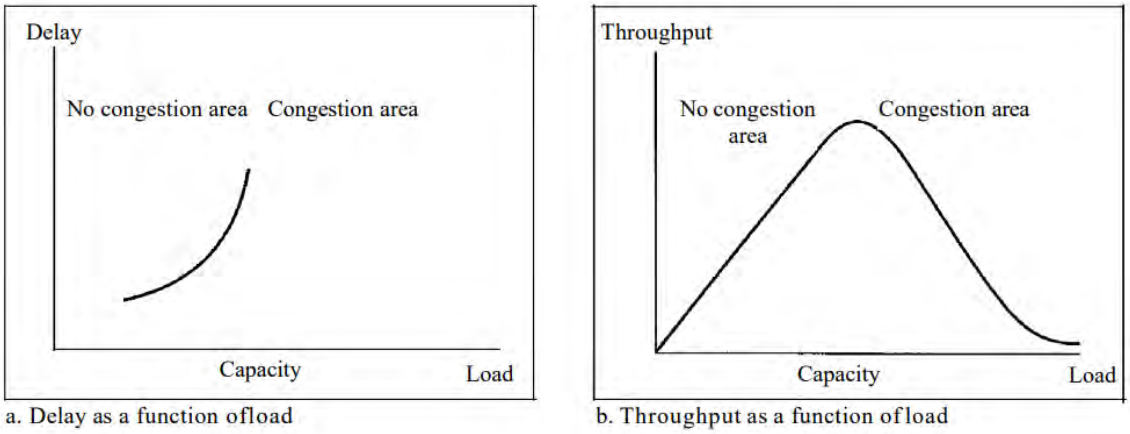

Figure 2 Packet delay and throughput as a function of load

DELAY VERSUS LOAD

When load is lower than the capacity of the network, there is minimum delay. This minimum delay consists of accumulated delay and processing delay, which is acceptable. But when the load becomes equal to the network capacity, there is an acute increase in the delay. This is because the waiting time spent in queues-for all router- needs to be added to the total delay. The delay becomes unlimited when the load becomes higher than the network capacity.

For example, if no packet is able to arrive at its destination or arrives with infinite delay, the queues keep on increasing. Delay influences the load negatively and as a consequence, the congestion also worsens. When a packet gets delayed, the source which is awaiting acknowledgement and does not get it, retransmits the packet, which worsens the delay and the congestion further.

THROUGHPUT VERSUS LOAD

Throughput in a network can be defined as the number of packets passing through the network in a unit of time. When the load is less than the capacity of the network, the throughput increments in proportion to the load. After reaching the network capacity, there is a severe reduction in the throughput.

This is because routers have started to discard packets. When the load is in excess of capacity, the queues fill up and some packets have to be dropped. Dropping the packets however does not reduce the quantity of packet in circulation because the sources retransmit the packets when their timer times out when the packets do not reach the final receiver.