Network Topology NS2 Simulation

TV.ABIRAAMI
RESEARCH SCHOLAR

Nodes:

n0: The sender node with a TCP agent.

n1: A node with a UDP agent.

n2: An intermediary node connecting n0, n1, and n3.

n3: The receiving node with a TCP sink and a null agent.

Duplex Links

n0 to n2:

Bandwidth: 2 Mbps

Delay: 10 ms

Duplex Links

Queue Type: DropTail (max size 10 packets)

n1 to n2:

Bandwidth: 2 Mbps

Delay: 10 ms

Queue Type: DropTail (max size 10 packets)

n2 to n3:

Bandwidth: 1.7 Mbps

Delay: 20 ms

Queue Type: DropTail (max size 10 packets)

Agents and Applications

TCP Agent (n0):

Responsible for sending data to the TCP sink attached to n3.

Uses a default maximum packet size of 1 KB.

TCP Sink Agent (n3):

Receives packets from the TCP agent.

Generates acknowledgment (ACK) packets for received data and frees the received packets.

UDP Agent (n1):

Connected to a null agent on n3.

The null agent discards any packets it receives, effectively acting as a sink that doesn't process the data.

FTP Traffic Generator:

Attached to the TCP agent (n0).

Generates data traffic, starting at 1.0 seconds and stopping at 4.0 seconds.

CBR (Constant Bit Rate) Traffic Generator:

Attached to the UDP agent (n1).

Configured to send 1 KB packets at a rate of 1 Mbps, starting at 0.1 seconds and stopping at 4.5 seconds.

Traffic Behavior

The CBR generator will continuously send packets to n3 through n1 and n2, while the UDP agent will send packets without expecting any acknowledgment since it connects to a null agent.

The FTP application will start sending data at 1.0 seconds, which will be managed by the TCP agent at n0. The TCP sink at n3 will receive this data and send ACKs back to n0.

The maximum queue size of 10 packets means that if the queues become full, any incoming packets will be dropped, which can lead to congestion and loss of data packets, especially under high traffic conditions.

Considerations

Packet Loss: The DropTail queue mechanism can lead to packet loss if both TCP and UDP traffic are high. Since TCP will slow down in response to lost packets (through the use of timeouts and retransmissions), this can create interesting dynamics in your simulation.

Traffic Interaction: The interaction between TCP and UDP traffic could impact the performance of the TCP flow. TCP's congestion control mechanisms could be affected by the behavior of the CBR traffic, especially if packets are being dropped.

Performance Analysis: Monitoring throughput, packet loss, and delay in the trace file will give insights into how well the network performs under this mixed traffic scenario.