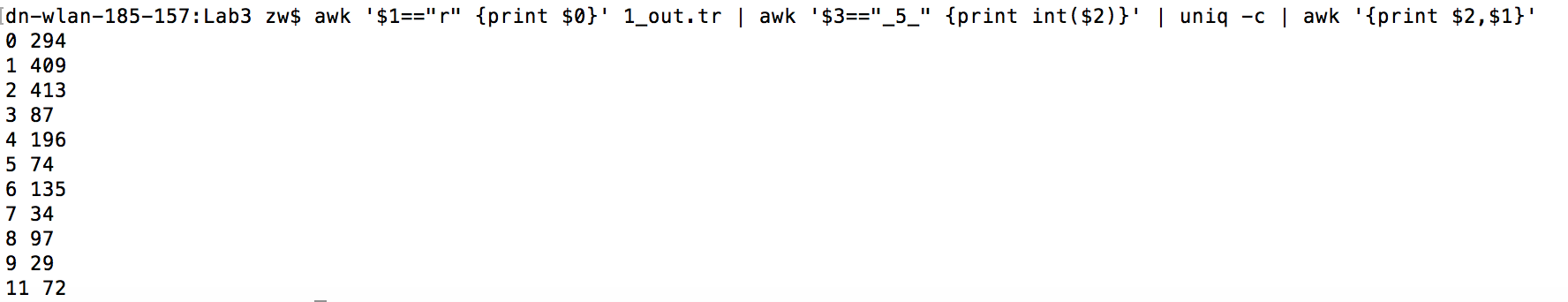
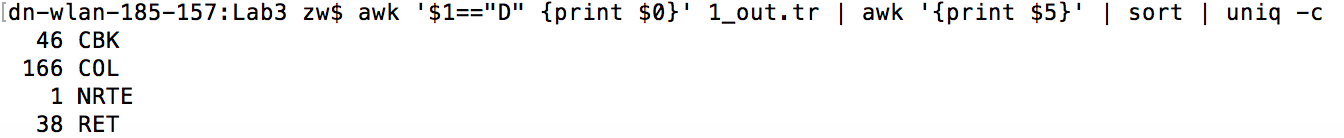
1. From the simulation trace, work out the TCP throughput (how many TCP packages are received at Node 5) over time (per second)



1. Similarly, work out how many TCP packets are dropped over time. [1]



1. Analyze the causes for packet droppings as indicated by the trace. [1]



The bar chart illustrates the packets that dropped in the whole process. It is obvious that the main packets dropping is due to three categories: CBK, COL and RET.

From the NS2 web site:

"COL" is for: DROP\_MAC\_COLLISION

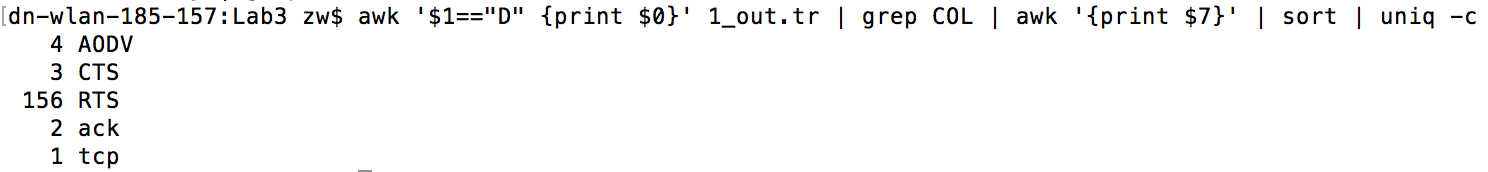
"RET" is for: DROP\_MAC\_RETRY\_COUNT\_EXCEEDED

"CBK" is for: DROP\_RTR\_MAC\_CALLBACK

There are two reasons for causing such packets dropping:

The first reason connecting with “CBK” and “RET”, the direct explanation is that the during TCP connection, there is a link failure, after 7 times RTS packets are transmitted and there is no CTS, the node will drop the packet at MAC layer with flag “MAC\_RETRY\_COUNT\_EXCEEDED” which shows up as RET flag; meanwhile, it will drop the tcp packets in the buffer stored in the queue which cause so many associated dropping tcp packets in RTR.

The second reason which is also the biggest packets dropping is caused by DROP\_MAC\_COLLISION.



If we do another filter to check the category of collision, we can easies see that the main source of collision is from RTS (request to send).

1. Analyze how the motions of the nodes affect the TCP performance. Conduct extra simulations if necessary.