# CPS 114/214 Midterm

<div align="center">

Duke University
Department of Computer Science

March 24, 2005

</div>

Answer all questions. Answers are graded on content, not style. Please try to be concise, precise, and complete. Keep it short and dense. Bullet lists of sentence fragments are fine as long as their meaning is clear: use the right key words. The questions are equally weighted.

I promised in a moment of weakness that this would be an open book/open notes exam, so you can look at that material if you want, though it should not be necessary. There shall be no collaboration: the honor system applies.

- Why is it important for a TCP sender to estimate the round-trip time (RTT) of the path to the receiver? Describe and explain the performance impact of overestimating and/or underestimating the RTT for a TCP connection.

- TCP performance suffers when RTTs grow. Quantify the impact and explain it, illustrating with specific examples of as many distinct effects as you can. What factors tend to increase RTTs? What can we do about them, if anything?

- Compare and contrast various approaches to enable an IP-based stream transport sender (e.g., a TCP sender) to discover that there is congestion in the network. We have discussed at least six distinct schemes to signal and/or infer congestion. Name as many as you can, and for each one: characterize it with one sentence, give a one-sentence rationale, and give a bullet list of pros and cons.

- We have discussed a number of proposals to change IP router functions to improve the fairness, efficiency, and/or robustness of the network. The impact of these proposals is frequently questioned because they are so difficult to evaluate and deploy. Could Active Networks help? Why or why not? What new problems does AN introduce with respect to fairness and robustness?

- Sketch a proposal to make BGP more secure, starting from the premise that autonomous systems have private keys and certificates signed by a trusted central authority (e.g., ICAAN). What specific threats does your proposal defend against? How specifically does it use cryptographic or other techniques to defend against those threats? How might an attacker circumvent your defenses?

- When Gigabit Ethernet came out there was a big push to deploy Jumbo Frames to increase the Ethernet packet size from 1500+ to 9000 bytes. Under what conditions could Jumbo Frames improve performance? How much, and why? (Be precise and quantitative.) Could Jumbo Frames ever hurt performance? How much, and why? Some people hate Jumbo Frames, and routers generally do not support them. Why? (We haven't specifically discussed Jumbo Frames, so this is really a general question about the impact of packet size.)