OFFICE OF
Information Technology

910 Yukon Drive, Suite 103 | Fairbanks, AK 99775-5320 | Phone: 907-450-8380 | Fax: 907-450-8381

Root Cause Analysis

Event: E-mail slowdown, March 9, 2010

Summary: On Tuesday March 10, 2010, at approximately 10:00 AM, e-mail delivery was taking almost an hour to complete. The e-mail router and associated servers had a high volume of messages queued for address lookup. The proximate cause of the queue backup and delivery slowdown was a demand for service (number of messages to route) beyond the capacity of the e-mail routing infrastructure. A configuration change in the Proofpoint spam-filter server, prior to the event, appears to have been the root cause of increased demand.

Detail: Increased load appears to have been generated due to spam messages not being filtered by Proofpoint. A configuration change was made on the proofpoint server sometime the previous evening that dropped 22,000 email addresses from consideration during filtration of email messages. That is, all these messages were sent to the mail server for address resolution via EDIR. Prior to this event, these messages were filtered by the Proofpoint server with spam being removed from the queue.

Without detailed examination of logs during this event and comparing with logs at other times, we cannot say with absolute certainty that the increased load was because of bypassing the Proofpoint server; but the coincidence of the delays and backlogged events with the modified Proofpoint configuration is strong circumstantial evidence.

Immediate temporary remediation: The Proofpoint server was re-configured to again filter email messages for the 22,000 email addresses that were previously opted out. Once this change was made, load decreased within minutes and normal e-mail delivery resumed.

Action Items and Future Prevention: The shortest path to remediation is to increase the system and server resources available to the email address resolution infrastructure. Using the currently configured servers as a model, we can estimate that 300 connections per server is the high water mark at which service begins to degrade. To handle the peak load seen during this event, we will need to devote 10 servers total to the email lookup infrastructure.

Another potential remedy may be to migrate the service to a server configuration which would provide higher throughput. IAM recommends that each major component of the infrastructure be benchmarked to ensure it will perform at the level required and to better understand its capabilities for better emergency resource allocation and load distribution.