Office of Information Technology
UNIVERSITY OF COLORADO BOULDER

Incident Report: Level 3 ISP / CU Internet Connectivity Denial-of-Service Attack

November 12, 2012

Issue

On Monday, Nov. 5, 2012, at 10:30 a.m., the Office of Information Technology (OIT) began receiving automatic notifications from our monitoring systems and clients concerning slowness for off-campus commodity Internet access. This did not affect all campus network users. The problem was resolved on Monday Nov. 5, 2012, at 12:30 p.m.

Background

CU Boulder and affiliates share a local 1 Gigabit-per-second (Gbps) connection for commodity Internet access. This normally works well for both parties because affiliates normally generate more traffic than they consume, while CU-Boulder does the opposite, consuming much more traffic than we generate.

Cause

The problem was caused by a denial-of-service (DoS) attack directed at a server at an affiliate from many places around the global Internet. Traffic from the DoS attack saturated the 1 Gbps connection in the same direction as our normal traffic. The most noticeable effect was very slow access to Desire2Learn. This should have had no effect on access to University Information Services (UIS) services, which we reach via our connection to the Front Range GigaPOP (FRGP).

Solution

Once it was determined the Level 3 connection was saturated, OIT redirected CU-Boulder network traffic away from the Level 3 link and routed the traffic via the FRGP. Shortly thereafter, the DoS attack ended and services were returned to normal.

What Can Be Done to Prevent This Again?

Because DoS attacks are unpredictable, OIT will continue to monitor the network for such occurrences. In addition, we are currently working to increase the bandwidth of the shared link to the commodity Internet.

Report prepared by:

Raymond Baum
Associate Director
OIT Network Engineering and Operations
University of Colorado Boulder