CBN Abuse Policy

Response to Backbone Network Abuse, Attacks, and Denial of Service Conditions

Communications Technology Services (CTS) is responsible for the operation and maintenance of the UCLA Campus Backbone Network (CBN). When CTS becomes aware of activity that disrupts, or that intends to disrupt, network connectivity or the operation of networked computer systems, CTS Network Operations will immediately block the offending traffic. The block will be placed so as to minimally impact the flow of other, non-disruptive traffic. When such an action is taken, CTS Network Operations will notify, as soon as possible, the IT Security Coordinator and the Network Coordinator(s) (NC) responsible for, or affected by, the traffic being blocked. This notification will be accomplished using the contact data provided by the NC to the Network Operations Center (NOC). It is the responsibility of the NC to notify, update, and work with the users and Computer Support Coordinator(s) (CSC) in his or her department in response to actions taken under this policy. The NC will have overall responsibility for managing the resolution of the problem. When notified by the NC that the problem has been resolved, CTS Network Operations will remove any blocks put in place.

Example Scenarios

CTS regularly tests the UCLA IP address space for networks that propagate directed broadcasts and are thus susceptible to exploitation as a relay network for “smurf” attacks. If such a network is found:

- CTS will configure the appropriate backbone access router(s) to refuse any ICMP echo response traffic from the susceptible network.
- CTS will notify the affected NC and the UCLA IT Security Coordinator as soon as possible after such an action is taken.
- The NC will be responsible for correcting the problem and notifying the NOC of the rectification.
- Upon such notification, CTS will verify the correction and restore the normal handling of ICMP traffic.

CTS discovers a host on a departmental network conducting scans of other hosts. As such scans are often the precursor to network attacks, and it is rare for such scanning to have a legitimate basis, in response to such a discovery:

- CTS will configure the appropriate backbone access router(s) to refuse any IP traffic from the host in question.
- CTS will notify the affected NC and the UCLA IT Security Coordinator as soon as possible after such an action is taken.
- The NC will be responsible for correcting the problem and notifying the NOC of the rectification.
- Upon such notification, CTS will verify the correction and restore the normal handling of traffic.

An attack is launched against a UCLA host or network resulting in a degradation of network connectivity for the entire campus. In response:

- CTS will request that the ISP serving UCLA block all traffic destined for the target host or network.
- CTS will notify the affected NC and the UCLA IT Security Coordinator as soon as possible after such an action is taken.
- CTS will notify all NCs of the incident and actions taken to resolve it.
- CTS will ask the ISP
  - to monitor and track the traffic to quench the traffic at its source;
  - to remove the block when the traffic has stopped;
  - to provide regular reports to the NOC.
- CTS will provide regular reports to the affected NC.