

Introduction

Bandwidth is a limited campus resource that must be properly utilized and managed (reference Computing Services Policy 500-001, ASC Network Bandwidth Policy). This procedure focuses on actions that Computing Services will take to ensure campus bandwidth is not intentionally or inadvertently impacted by excessive bandwidth use by an individual user or users.

Section I – Computing Services Response to Apparent Bandwidth Problems

Computing Services actions will be triggered by automatic system notification that campus bandwidth utilization is exceeding 85% of available bandwidth xx times within an xx timeframe. When this occurs, Computing Services staff will take the following actions:

- Analyze current bandwidth utilization using the Netflow, Package Capture and/or NetEqualizer tools
- Identify the top campus “outbound” bandwidth users
- Identify the IP address of the top outbound user
 - ✓ Print out documentation that identifies the top outbound user
- Identify the username and name of the top outbound user
 - ✓ Use Bradford to identify a student username and name
 - ✓ Use SCCM to identify staff or faculty username and name
- Disable the offending network account
 - ✓ In the case of a student, use Bradford to shut down the account and redirect the student to a webpage telling them to contact Computing Services to have their account re-enabled
 - ✓ In the case of staff and faculty, if the bandwidth impact is severe, firewall off the offending account
 - Make every effort to contact the staff or faculty member prior to disabling their account; in the case of faculty, call Mark Manzanares at 587-8203 (his direct line) and Mark will try to locate the faculty member
- For a student, send an email to the Support Services Lead, Resnet Lead (Christine) and Help Desk (Patti) detailing what action has been taken and why; attach a copy of the documentation which supports the action taken
- For a staff or faculty member, send an email to the CIO, AITC Director, Network Lead, Support Services Lead and Help Desk (Patti) detailing what action has been taken and why; attach a copy of the documentation which supports the action taken

Section II – Escalating Computing Services Response for Bandwidth Abuse

As detailed below, Computing Services will use an escalating response in dealing with repetitive bandwidth offenders. Though consistency in dealing with bandwidth abuse is important, our recommended response should be considered a guideline and does not preclude the use of judgment in dealing with individual issues.

Offense	Actions
1st	<p>A. Student: The student must meet with either the Support Services Lead or the Resnet Lead to discuss the incident; the student will sign a form indicating they have received a verbal warning regarding bandwidth abuse</p> <p>B. Staff or Faculty: The staff or faculty member will meet with either the CIO (staff) or Director of Academic Instructional Technology (faculty) to discuss the incident</p>
2nd	<p>A. Student: The student will meet with the Housing Director, Support Services Lead and/or Resnet Lead to discuss the incident; a warning letter will be placed in the student's housing file</p> <p>B. Staff or Faculty: The staff or faculty member will meet with the CIO (staff) or Director of Academic Instructional Technology (faculty) and appropriate Department Manager or Department Chair to discuss the incident</p>
3rd	<p>A. Student: The student's ASC network account could be rate-limited for the remainder of the semester. The student will be able to accomplish "normal" Internet functions such as email and general browsing; the student will not be able to perform bandwidth-intensive applications</p> <p>B. Staff or Faculty: The staff or faculty member's ASC network account will be rate-limited for the remainder of the semester. The staff or faculty member will be able to accomplish "normal" Internet functions such as email and general browsing; the faculty member will not be able to perform bandwidth-intensive applications without first contacting Computing Services</p>