Quota Management

Considerations for a University Environment

Kevin Littlejohn
Obsidian Consulting Group Pty Ltd

Why?
Perspective/background

- Cost allocation per department
- Departmental allocation to staff/students
- Student purchase of extra quota
- Integration of other billable resources

Three broad areas:

- **Authentication/Authorisation**
- **Accounting**
- **Quota Definitions**

These three areas are where we spend the most time with any university roll-out.

Each affects the other, and they together affect network layout.

Quotas

- **Every University manages quota and charging differently**

- from the simple to the complex...

Starting Simple: IP-Based

Assign IP numbers based on department and track usage per IP.

- **Advantages**
  - Simple approach
  - Starting point for most universities.
- **Disadvantages**
  - Doesn't deal well with labs, libraries, or mobile computing.

Next Step: User-Based

Track usage per User

- **Require users to login to the network before use**
- **Assign users to departments**
- **Automate as much of this as possible**
- **Advantages**
  - More accurate tracking of departmental use
  - Can integrate other devices such as dialup, wireless
- **Disadvantages**
  - More intrusive, may require re-working authentication

User-Differentiation

- **A user-based approach enables user-differentiation**
- **Segment out different 'types' of users, for example:**
  - Set staff to 'postpaid' accounts, and
  - Set students to 'prepaid' accounts.

User Differentiation continued...

- **Ability to differentiate between *bought* quota and *assigned* quota, with**
  - differential handling of paid vs assigned quota
  - management tools
- **Implement rules for purchasing extra quota using a credit card, etc.? - this is a political area**

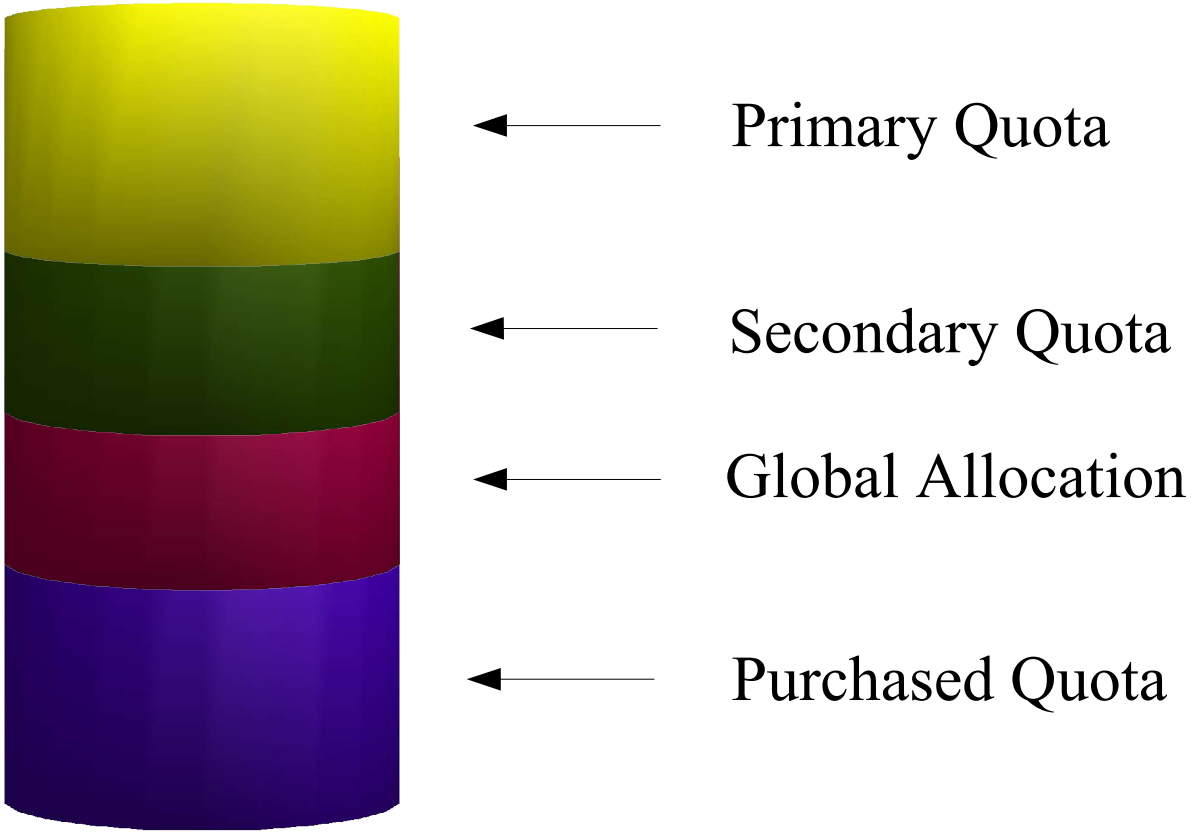
An example quota system

VicUni's quota system:

The University of Victoria's quota system involves *cascading buckets of quota*.

- Users are allocated a number of 'pools' of credit – primary course, secondary course, global, and purchased quota.
- These quota pools are grouped together as a functional group in a cascading relationship, such that credit is used in the order described above – first primary course assigned quota, then secondary, then global, and finally any student-purchased quota.
- The order of use is important because, in the case of primary, secondary, and global, quota will be assigned periodically from a departmental quota reservoirs according to departmental rules.
- At the end of each month, the quota that has been used by the user will be billed back to the appropriate department by the IT department.

VicUni Quota System



VicUni Complexities

- Reporting to users has to breakdown quota
- Building/automating reports for admin and flows of quota between depts/users
- Managing student changes of course
- Managing staff department changes
- Rules for expiring quota without causing student complaints (I purchased quota, now it's gone)
- Implementing rules for actually using quotas in the right order

External Differentiation

- **Charging differently for different types of traffic.**
- **The usual starting point (and often ending point) is:**
  - Internal traffic – free
  - External traffic – charged

Accounting

Limitations based on network layout (or, network layout based on requirements)

Combining multiple collection points sometimes the answer, but also poses some problems

Traffic counting and collection

- **RADIUS/802.1x**
  - great, but bulk data only
  - Some indications new equipment may not properly support this yet
- **Netflow**
  - better
  - no "*end of flow*"/logout for shared computer (i.e. lab/library computers)
- **SSG**
  - excellent
  - allows differentiation and logout
  - requires Cisco
  - only applies at external edges
  - fairly intrusive design-wise

Traffic counting and collection (continued)

- **Proxy logs and similar**
  - Different type of counting
  - limited services
- **Vendor Devices**
  - Varying capabilities
  - Require custom work to integrate

Authentication/Access

- Where do you force authentication?
- How?
- What do you authenticate?

- Forced logins
  - at outside edge of portal system, or
  - at inside edge by Novell/MS login hooks

Choke point for logins

- Novell
  - issue with notifying devices that a user is authenticated (NSure for SNMP traps)
- Microsoft Domain logins
- Proxy servers/socks clients
- 802.1x
- SSG
- Other devices as gateways

Authentication Source

- **LDAP**
  - Most common way to authenticate
  - Ties in with Novell or MS logins nicely
- **Others?**

Summary

Three Broad Areas:

- **Quotas**

  Define rules for quotas in terms of:

  - External Differentiation (differentiation based on traffic types),
  - Internal Differentiation (IP-based, user-based, etc), and
  - Ability to control quota (department or individual)

- **Accounting**

  Decide based on:

  - Differentiation requirements
  - Where and what you need to count

Summary (continued)

- **Authentication/Access**
  - Decide where to enforce choke points
  - What devices need to be involved in forcing authentication?
  - Authentication source – pick a single, central source for user passwords.