IT Council Meeting

CIO Update

0120 Patuxent Building
January 31, 2007

IT Council Agenda

3:00 pm	**Welcome and Introductions**
3:02 pm	**Agenda Review**
3:04 pm	**Approval of September 20, 2006 minutes**
3:05 pm	**CIO Report - *Huskamp***
3:25 pm	**Anti-cheating Software - *Moore***
3:35 pm	**Building Renovation Priority - *Sinha***
3:55 pm	**Revised Wireless Policy - *Sinha***
4:05 pm	**Removal of Rogue Access Points - *Sinha***
4:10 pm	**IT Security Policy (Action Item) - *Sneeringer***
4:20 pm	**UMD Secure for Wireless - *Sneeringer***
4:30 pm	**Adjourn**

CIO Report

- 10 Year Plan
- Quick Hits
- Major Initiatives - RFP status

10 Year Plan Overview

- Provide a roadmap for what is coming
- Networking is a major part of the plan
- 10 year budget estimate
- Prioritization of projects
- Emphasis is on gaining economies of scale

10 Year Plan Critical Areas

- Administrative Computing Quality Assurance
- Audit Compliance
- Emergency Operations, Disaster Recovery, Business Continuity
- Faculty/Staff Email System
- Identity Management
- ITSM Project for Implementing Best Practices
- Knowledge Management
- Kuali Student Information System Project
- Network Refresh
- Storage Initiative
- Virtualized Resources

Mainframe Congestion

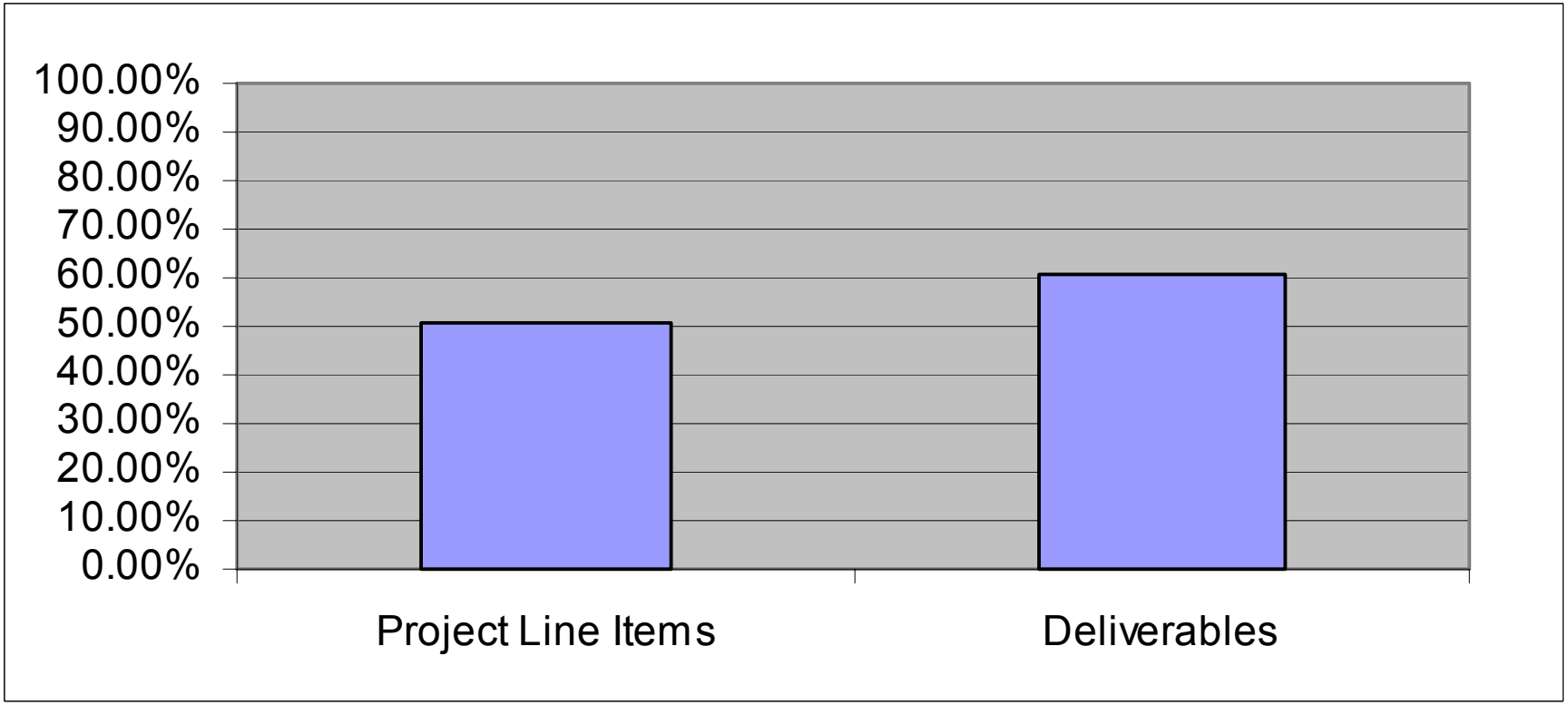
Kuali Student Project

- Carnegie-Mellon, Berkeley and University of British Columbia do not have final approval for this project – possibly by May
- We are slowing down our participation and resource commitment to ensure we are managing this project in the best interest of the university

Security Improvements

- Quarterly audit finding status provided to the Office of Legislative Audit – no response yet
- Password expiration and complexity implemented in October
- Encrypted wireless network launched
- Moved from Kerberos 4 to Kerberos 5

Security Program Metric



CALEA Status

- UM is judged to be exempt from CALEA
- Mid-Atlantic Crossroads is joining most other Gigapops in believing they are exempt from CALEA
- If everyone is exempt, who will be liable for the required monitoring?
- Discussion is continuing

Dial-In Modem Status

Terrapin Technology Store

- Institutional orders that are processed through the Store receive an additional 2% discount
- The Store will receive credit for the sale and will receive 4% of the sale for support of the ACT program
- Please encourage your purchasing departments to utilize this process

ECAR Study of Students and Information Technology 2006

- 240 seniors, 267 freshmen at UM
- 15047 seniors, 9790 freshmen at other four year institutions
- Results at UM did not differ significantly from those of the other four year institutions

How Old Is Your Personal Laptop?

	UM Seniors	UM Freshmen		Other Seniors	Other Freshmen
< 1 yr	14.4%	64.0%		14.8%	55.6%
1 yr	7.6%	8.7%		8.2%	9.9%
2 yr	11.4%	3.8%		11.4%	5.0%
3 yr	11.0%	3.0%		10.7%	2.9%
4 yr	9.3%	1.5%		10.3%	1.3%
>4 yr	5.2%	0.4%		6.0%	1.8%
Not Own	41.1%	18.6%		38.6%	23.5%

Remote Data Center Space

- Physics – 10 racks for Ice Cube Cluster installed
- IPST – one rack being installed this week
- Engineering – installing 1 rack after electrical installation
- Other interested departments – Geology, Physics, Chemical and Life Sciences

Quick Hits

- Dorms are to become wireless by Fall, 2008
- “One Campus” network refresh plan
- Astronomy added 40 nodes to campus HPC cluster – other possibilities include Mechanical Engineering, IPST and Meteorology
- …xxx research machines in secondary data center…
- OIT auditor hired
- OIT disaster recovery tabletop exercise coming up

Quick Hits

- Daylight savings time start/end change may be a problem
- IT Enterprise Applications Subcommittee replaced by Enterprise Administrative Applications Advisory Council
- Innovations in Teaching and Learning Conference – February 23
- Portal soft launch is February 12

Major Initiatives – RFP Status

	Begin	Release	Due	Award
DR Hot Site	3/24/2005	6/19/06	7/17/06	?
Email	1/24/2005	2/1/2007	4/1/2007	7/1/2007
Pay for Print	12/14/2005	6/9/06	7/15/06	?
Voice-over-IP	12/23/2004	2/1/06	5/15/06	?

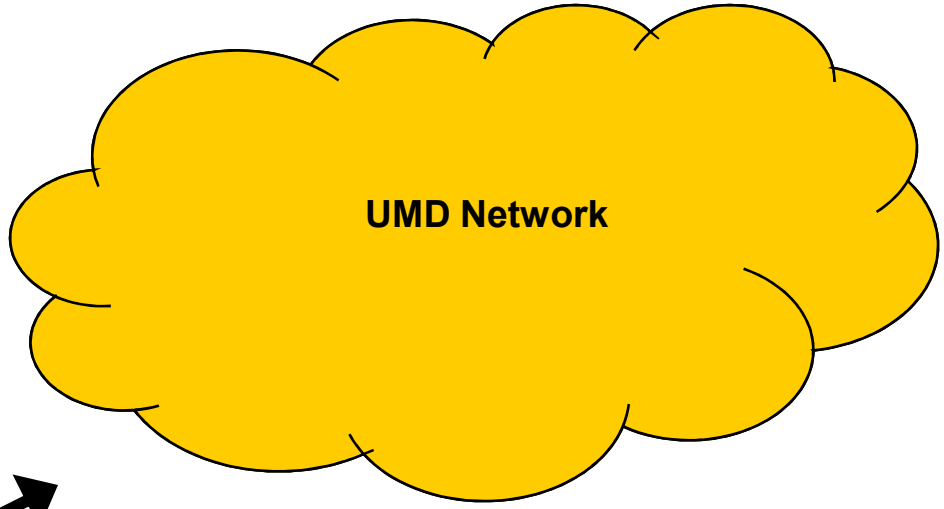
Building Renovation Priority – *Sinha*

Revised Wireless Policy – *Sinha*

Removal of Rogue Access Points - *Sinha*

Scale of UMD Network

245 Buildings on the campus network
57 Academic Buildings
82 Admin/Facilities/Dining/ Halls/Athletics/other
106 Residence Halls
- 46 Dormitories
- 14 Fraternity Row Houses
- 33 Graduate Apartment Buildings
- 13 Public-Private Partnership Buildings



488 NTS Closets with Network Equipment
689 Additional NTS Closets with wiring only

953 NTS Managed switches
39 NTS Managed routers

2166 Number of wireless Access Points (APs) and growing

Approx. 41,000 hosts on the network

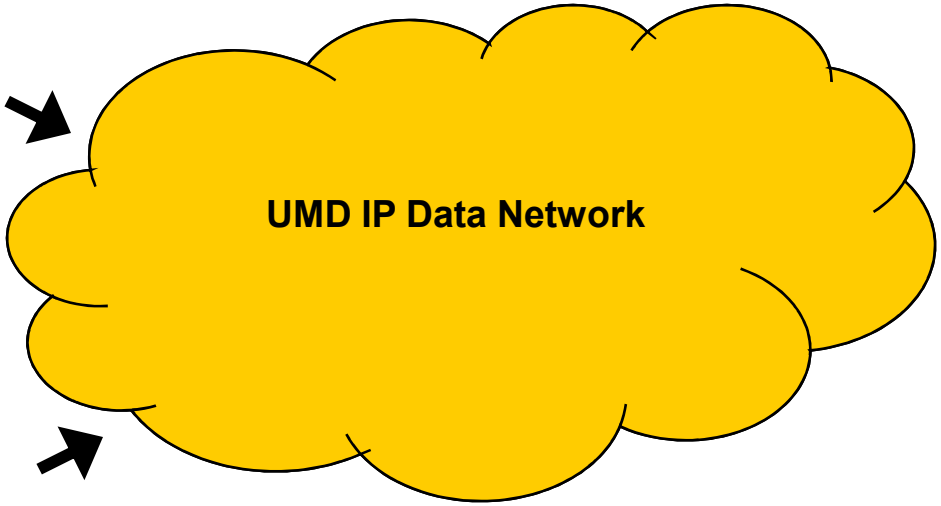
Current State of the Network

75% - 80% of the buildings have Cat3 cabling (1988 standard)

Approx. 78% of the our ports are operating at 10Mbs switched

71% of building network switches are at "end-of-life"

1 Gbs backbone



Desired State

- Upgrade building cabling
- Upgrade port speeds to 100 Mbs switched or better
- Make all network gear current and keep them current
- Upgrade backbone to 10 Gbs

Refreshing the network – NTS Revenue Source

(refer to NTS expense and Revenue handout)

- Rate increases for phone and data services.
- Facilities Council Infrastructure Upgrade Fund
- Student Technology Fee
- Campus base funding

Key guiding principles in allocation of refresh funds

(refer to Funding Allocation and Prioritzation handout)

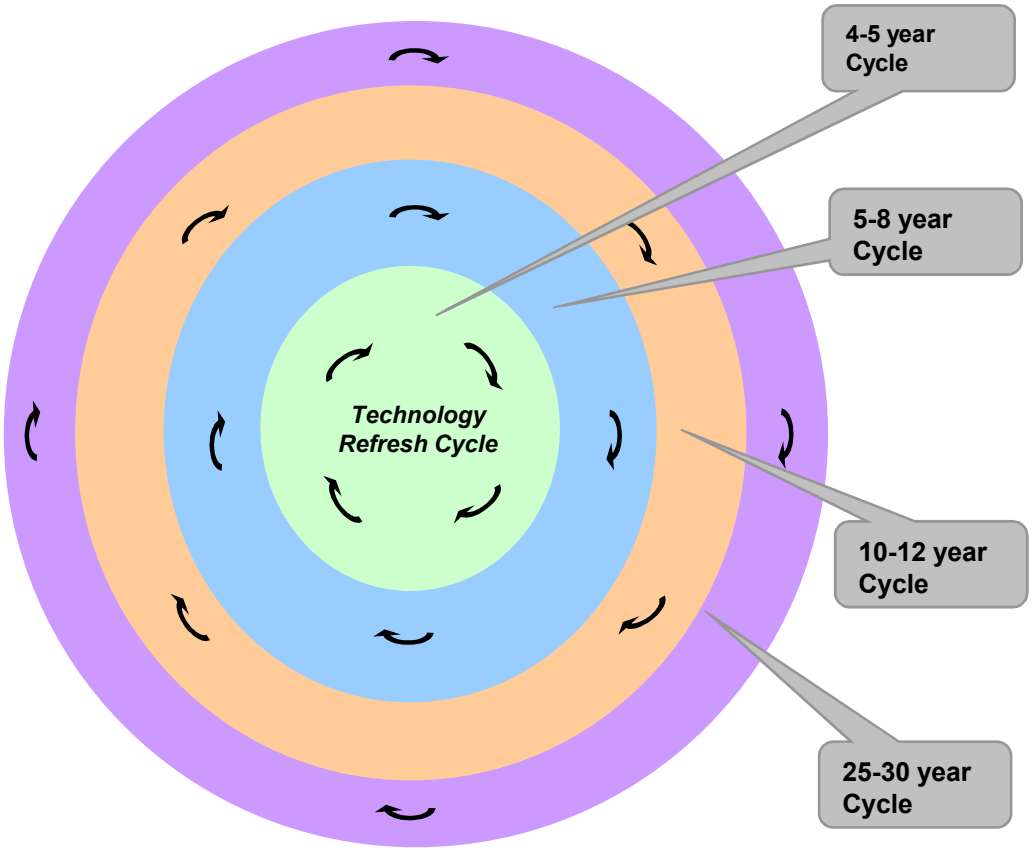
- A portion of this revenue is applied to upgrade the dormitories per year.
- The Student Technology Fee is applied to those parts of the network that are available for use by all students.
- Remaining funds are applied to refreshing the remainder of the academic and administrative portions of the campus network.

Annual prioritization of network refresh

(refer to Funding Allocation and Prioritzation handout)

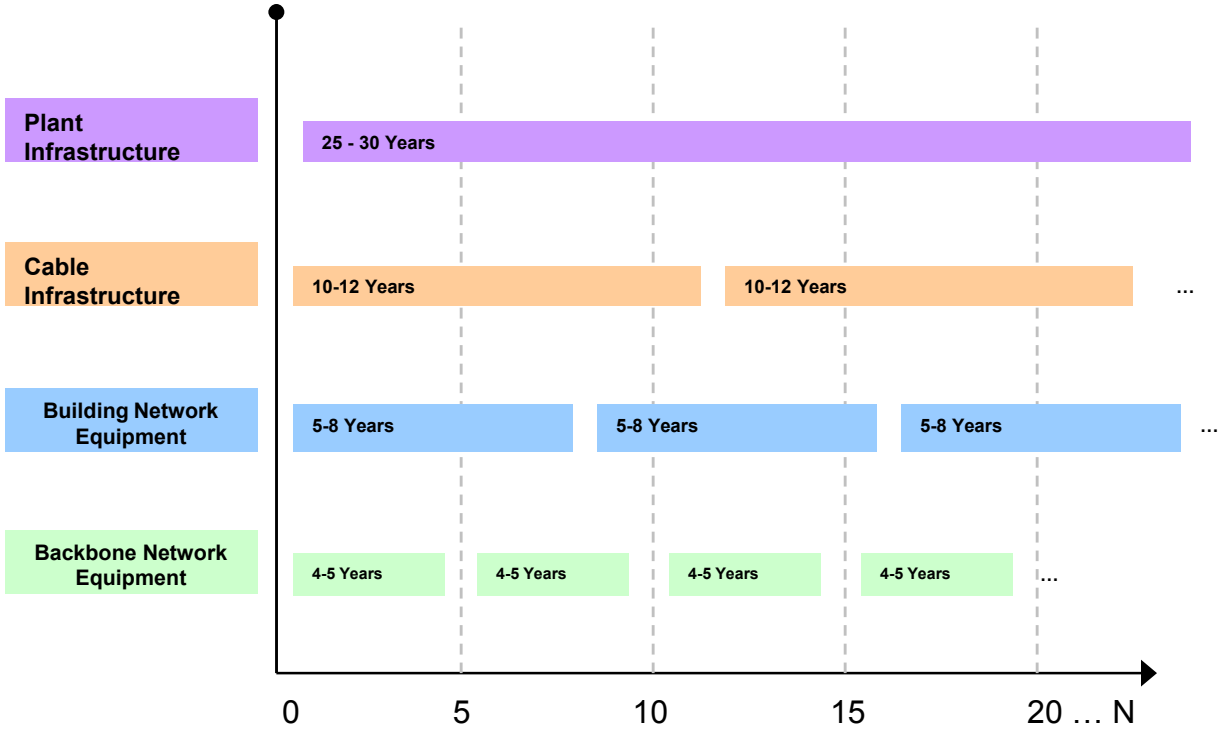
- Step 1: If the building is in danger of delivering service at the current minimum campus standard (CAT-3, 10MB/100MB switched) then deem it as high priority. This might be if the electronics are in danger of failing.
- Step 2: If the building is performing at the current minimum campus standard but there are building residents that require higher performance to succeed, then deem the building as middle priority.
- Step 3: If the building does not have strategic occupants (e.g. an administrative building), deem the building as low priority.

The Refresh Cycle



The Refresh Timeline

(refer to the "big" spreadsheet)



Time in years where Year 0 = 2007

Wireless Policy (draft)

(refer to the draft wireless policy handout)

- **Key Elements**
  - Provide a reliable wireless networking service
  - Maintain the integrity of the UM network
  - Maintain the security of the UM network
  - Comply with state audit requirements

Wireless Policy (draft)

- **Achieving these elements**
  - Unlicensed radio frequency (RF) bands of 2.4 GHz and 5 GHz will need to be managed appropriately to offer reliable service.
  - OIT will be responsible for managing and coordinating wireless access to the UM network and radio frequencies used for communications.
  - Exceptions will be granted for research, academic and administrative uses. OIT will work with users so that access will preserve the integrity and security of the UM network.

Wireless Policy Corollary – Removing Rogue Access Points (draft)

- **Key Elements**
  - Access provided to the UMD network via rogue access points:
    - non-OIT supported access points AND
    - access points that have not received an exception
  - Such access will be identified routinely.
  - The access will be disabled.
  - A process is defined for disablement.

Process for Rogue Disablement (draft)

- **Our ability**
  - Our Access Points (APs) can identify legitimate “components of the wireless network gear infrastructure”
  - Our APs can identify components that are not authorized
  - Our APs can identify those components that have been given an exception to operate securely within our infrastructure
  - Our APs can identify components attempting to impersonate official services

Process for Rogue Disablement (draft)

- **Possible ways to use our ability to enforce our policy**
  - APs identify rogue access points and render them inoperable
  - APs identify rogue access points that have stolen our identity and render them inoperable
  - APs identify access points that have been granted exceptions and will allow them to co-exist

Process for Rogue Disablement (draft)

- **Scope of Enforcement**
  - Dorm footprint – as UMD wireless services are offered, identify rogues and then disable
  - Buildings that have wireless service - identify rogues and then disable
  - Buildings that do not have wireless service - identify rogues and work with departments on bringing UMD wireless services to the buildings