Colorado State University

Subnet Managers
March 10, 2010

Preliminary Agenda

Agenda Items

- Central Mail Services
- Information Systems
- Middleware
- RamCT
- Licensing

Agenda Items (con't)

- Windows Update
- NOC
- Technology Demonstration
  - Trouble Ticket - Libraries

ACNS Central Mail Services

- Authenticated SMTP Update
- Proof Point
- Eagle mail update

Information Systems

- Update on systems and upcoming maintenance.

ACNS Middleware

- Project Updates
  - Lynda.com
  - Federated Authentication
  - Google Apps
  - Course Wait List Notification
  - Grader

Lynda.com

- On-line software training
  - 705 courses, 42,000 tutorials, 6 new titles every week
  - Includes Microsoft, Adobe, Apple, Macromedia products...and many more

- UTFAB endorsed & funded 1 year pilot
  - Allows access to students, faculty and staff
  - To begin after Spring '10 semester

Federated Authentication

- InCommon Service Provider Update
  - National Institutes of Health
    - Process needs to be put in place to allow LoA 2
  - EBooks Library - An ebook lending service
    - Testing
  - Lynda.com - Online software training
    - Upcoming
  - Colorado Alliance of Research Libraries
    - Testing

Google Apps

- @alumni.colostate.edu - proposal
  - Automatic provisioning of accounts
  - New graduates (Intent to graduate flag in Aries)
  - Provisioned as CSUID@alumni.colostate.edu
  - User can manage account name
  - Email notice to rams account on creation
- Account de-provisioning
- Support for IE6 discontinued March 1

Course Wait List Notification

- RAMweb opt-in for waitlist text alert
- Process
  - Seat opens in course
  - Aries procedure writes record, sends email, calls ACNS web service
  - Web Service validates request, calls Rave API
  - Text message is sent via Rave Alerts
  - Student receives notice, has 24 hours to register

Grader

- Completed Tasks
  - Development complete
  - Archived legacy system with Fall 2009 data built for testing validation
  - Data migration script 90% complete
- Upcoming Milestones
  - 3/10 - Migrate Fall 2009 data from legacy system to new application
  - 3/19 – Complete remaining super user functionality (Invoices, Scan Upload Report)
  - 3/19 – Implement required RAMCT SSO components into production
  - 4/1 – Begin Faculty testing
- Release Date – Start of Summer 2010 Term

RamCT

- Service Pack 3 applied to system over holiday break
  - Mostly behind the scenes fixes.
- Performing a review before we go the our next LMS version. Looking at:
  - Black Board 9.1 (Blends BB with WebCT)
  - Sakai 2.6 – open source
  - Faculty committee, RamCT Coordinators, Server Administrators, students.
-

Software Licensing

- Site License
- Adobe Connect

Licensing

- HP Computer Pricing/Configuration
- Digital Signage

Windows Update

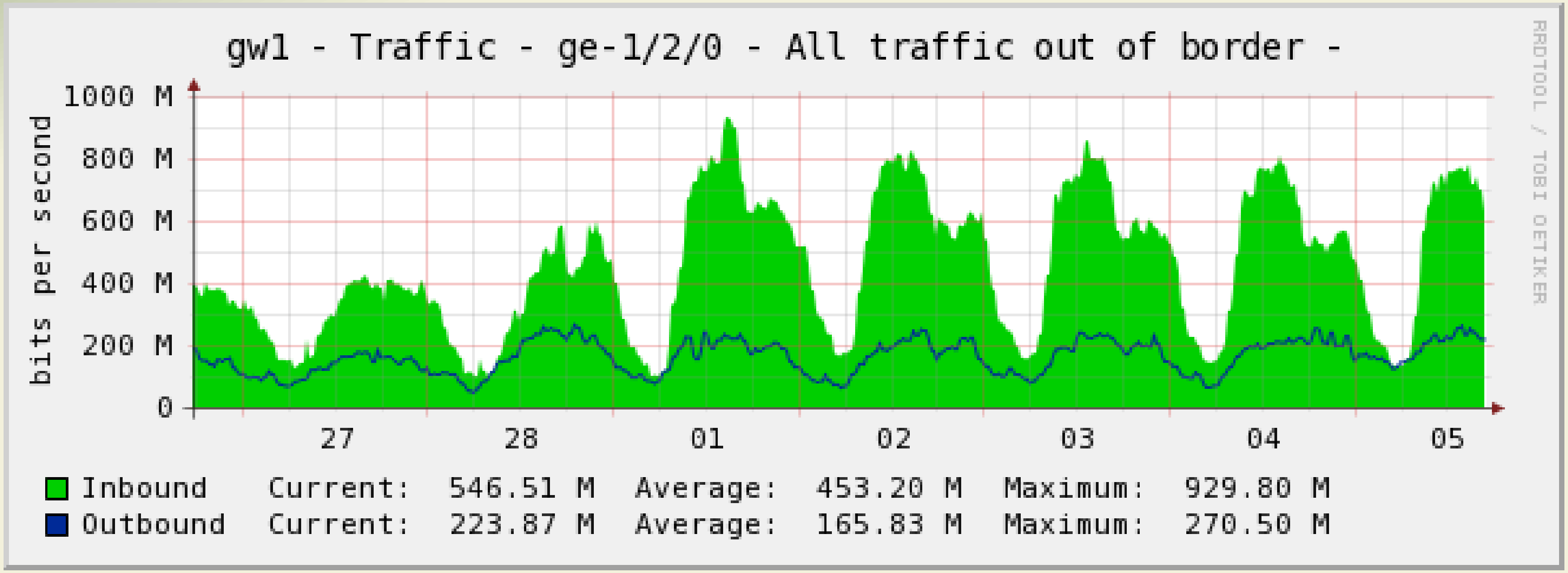
- Exchange 2010 plans.
- Test and production Colostate forest preparations.

Network Operations Center (NOC)

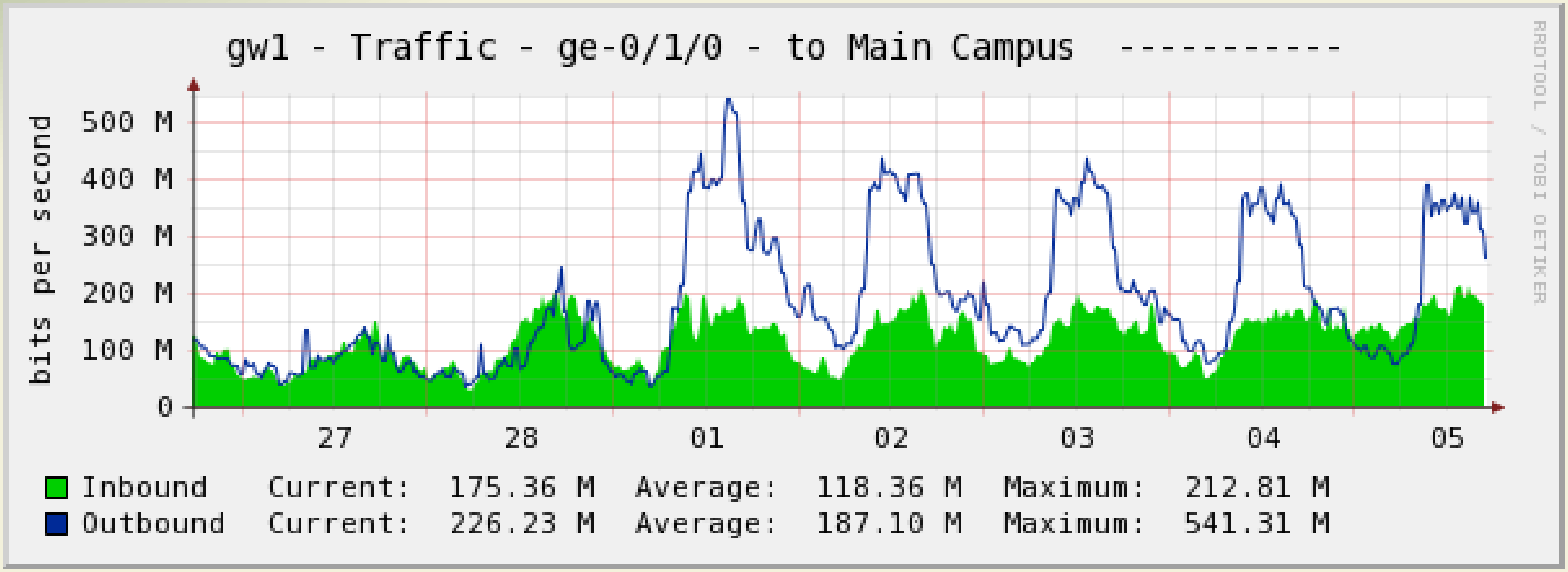
- Traffic update
- Outages
- Wireless update
- Private IP Space Best Practices
- DarkNet/RIAA
- Video Conferencing and Secure Meeting

Traffic update

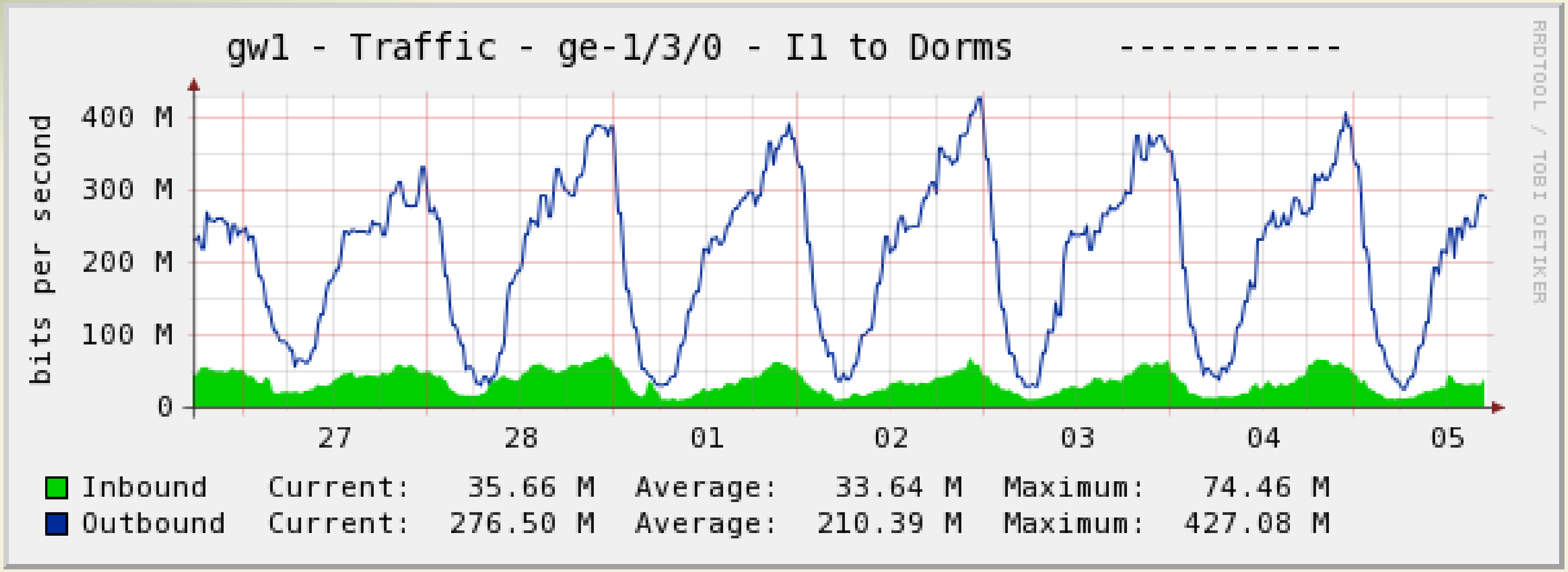
Traffic in/out of campus border



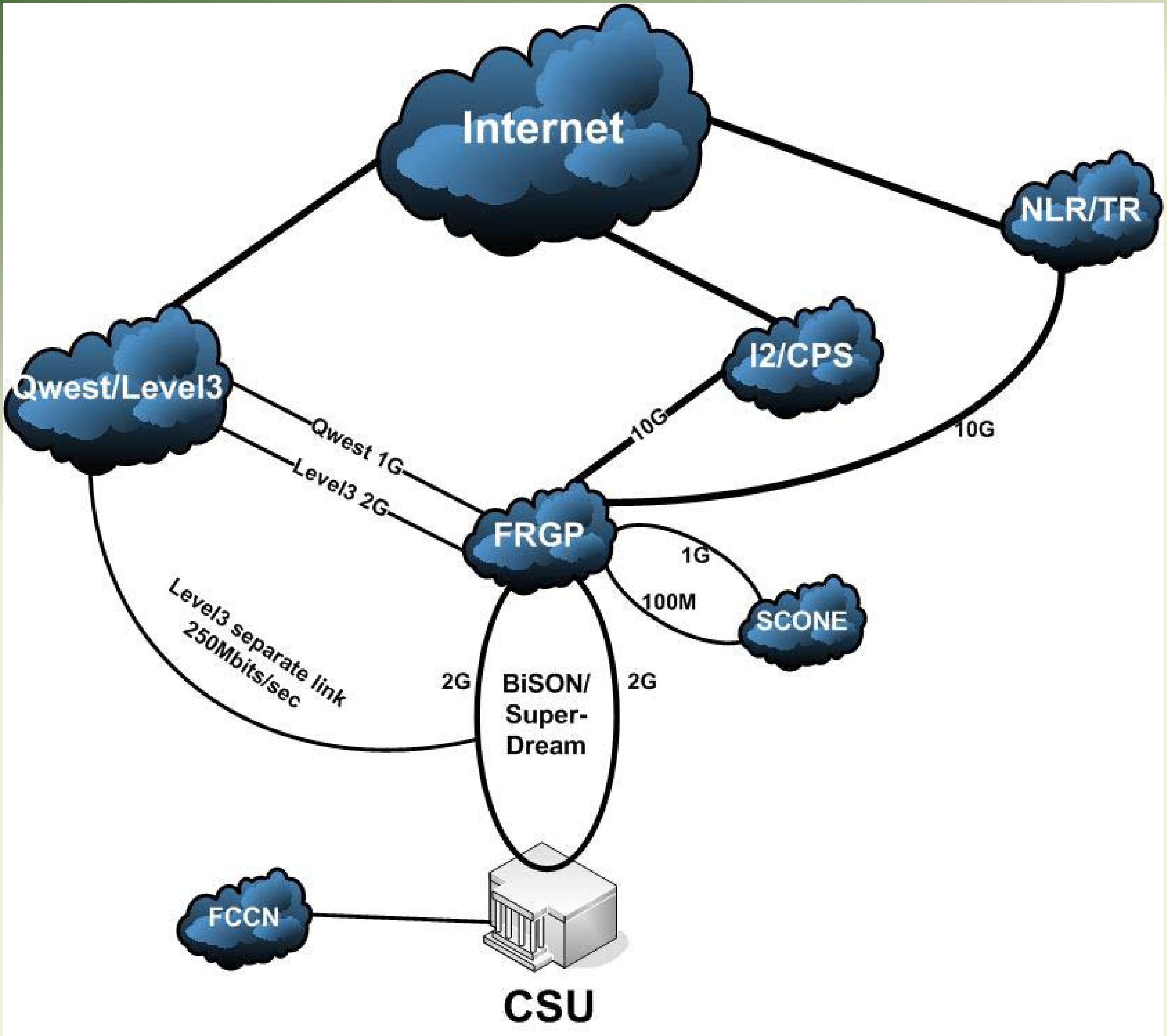
Traffic in/out of main campus



Traffic in/out of residence halls



Outages


Internet
NLR/TR
I2/CPS
Qwest/Level3
Qwest 1G
Level3 2G
10G
10G
FRGP
1G
100M
SCONE
Level3 separate link 250Mbits/sec
2G
BiSON/ Super- Dream
2G
FCCN
CSU

The Great Internet Outage of 2010 February 10, 2010

- Timeline
  - 15:25 power lost at Level3 collocation site
  - 15:25 ACNS Staff and monitoring tools alerted
  - 15:36 Rerouted traffic over Level3's backup link.
  - 15:43 Fixed routing in core to bring up core services.
  - 16:20 Fixed the remainder of campus
  - 16:39 FRGP reports power restored

- Central services offline from Internet for 18 minutes
- IntraCSU traffic not affected
- Some sites not able to get to Internet for 55 minutes

What’d did we learn

- Monitor default route from providers
- Remove single point of failure at Level3 Collocation
- Upgrades by Level3 at collocation site

Core router crash
February 11, 2010

- 7:45pm Router housed in Engineering crashed.

- Affect to campus
  - Internet: Not Accessible
  - Central Services: Accessible (for those campus users not directly connected to Engr6500)
  - NonCentral Services: Accessible (Those not directly connected to Engr6500)

- 8:30pm Router restored to production

What’d did we learn

- Internal redundancy for central services stayed up!
- Continue to move toward redundancy of core routers.

Wireless update

New Buildings & Upcoming Buildings

- New
  - Engineering
  - Chemistry
- Upcoming
  - Phase 2: Eddy, Education, Engineering, Chemistry
  - Phase 1: Plant Sciences, Wagar, Natural Resources

Private IP Space Best Practices

- Non (Never) routed private IP space
- Routed private IP space

Non (Never) Routed IP Space

- 192.168.X.0 /Y where X matches subnet and Y matches network mask.
- VLAN should be current VLAN number plus 1000

Example:

Morgan Library has the 129.82.28.0/22 network which maps to VLAN 28. Thus their non-routed private network/VLAN would be:

  - 192.168.28.0/22
  - Vlan 1028

Routed Private IP Space

- 10.1.X.0 /Y where X matches subnet and Y matches network mask.
- 10.X.0.0 /16 where X matches their subnet range for /16 networks

Example:

Morgan Library has the 129.82.28.0/22, VLAN 28
Their private LAN would be:
10.1.28.0/22 and VLAN ACNS Assigned

Or if a larger, routed private net is needed.

Morgan Library has the 129.82.28.0/22 VLAN 28
Their private LAN would be:
10.28.0.0/16 and VLAN ACNS Assigned

DarkNet/RIAA

- DarkNet: 129.82.155.0/24
  - Machines likely infected if they “touch” DarkNet
- RIAA: Recording Industry Association of America
  - Mitigate
  - Consult user on AUP
  - Respond back as to what was done
  - ACNS will respond back to RIAA

Videoconferencing & Secure Meeting

- Don’t forget about these easy to use tools to save time and money!
- 13 Video Conference Sites scattered around campus.
- Secure meeting – use for meetings and tech. support.

Security: Targeting old apps

- Old Cisco VPN clients
  - Before 5.0.03 have known vulnerabilities
  - Notifying via pop-up, mail directly, mail to subnet mgrs
  - Old clients will be disabled soon!
- SAV 10
  - On its way to End-of-Life, but already dead to me!
  - Contact Scott Dawson if you need to upgrade
- Old Adobe products
  - Reader
  - Flash player
  - 80% of all exploits in 2009!

SSL gateway outage (3/1 – 3/2)

- What happened
  - Crash dump file space filled up, couldn’t boot
  - Had to factory-default and install old config
  - Investigating the cause with Juniper
- Status
  - Back up and running, configuration restored
  - Anyone with problems please contact me
- Moving forward
  - More frequent configuration backup
  - Spring break: trying again to implement redundancy

Risk Assessment

- Completion status
  - WCNR
  - CAHS
  - Next?
- Old IT Security Policy Questionnaire
  - Old app, no longer supported
  - BUT – server scan registrations still valid (please review)
  - http://www.acns.colostate.edu/index.aspx?page=security_compliance_index

Symantec Endpoint Protection Enhancements

- Not just Anti-Virus any more
  - Anti-virus/anti-spyware (scan the HD for signatures)
  - Proactive Threat Protection (scans the process table)
  - Network Threat Protection (IPS and firewall)
  - Application & Device Control
- Protection versus convenience/performance?
  - False positives vs. misses
    - Make sure the client is actually doing HD scans
    - Can increase sensitivity of signature matching
  - Enable IPS
  - Symantec firewall rather than Windows firewall? (we'll talk)
  - Application & Device Control – can block known filenames

Technology Demo

- Help Desk Trouble Ticket Demonstration
  - Morgan Library IT Staff