CSU Subnet Managers
March 22, 2017

What happened to Winter?
Agenda

The usual suspects!

• IS Update – Josh Clark

• Windows Group – Joe Volesky

• Middleware Update – Randy Miotke
Agenda (cont.)

• Canvas – Kevin Nolan
• RAMtech/Licensing – Diane Noren
• Security – Steve Lovaas
• Network/Telecommunications – Greg Redder
Farewell, Rusty Scott

And Thanks!
IS Update

Josh Clark

• HR
  – Stabilizing test environments for smoother upgrades and implementations in the future.

• Kuali
  – Mongo DB
  – Workflow
IS Update

• Banner:
  Banner 9 Upgrade

• Appman:
  Move Appman from AIX to Linux
Windows Group

Joe Volesky, Mike Willard

• SMB signing on servers joined to Colostate
  Questions? windows@colostate.edu

• MS Azure
  Questions? azurehelp@colostate.edu
Middleware Updates

Randy Miotke

• WebAuth end of life
  – December 31, 2017

• Accessibility of Electronic Information and Technologies
  [http://policylibrary.colostate.edu/policy.aspx?id=739](http://policylibrary.colostate.edu/policy.aspx?id=739)

• Checking CSU sites – need to do better with compliance.
• Will offer workshops.
Middleware Updates

Mobile friendly eID template

eID registration and modify email changes
– O365 email – First.Last@colostate.edu

– Google Apps – ename@rams.colostate.edu and First.Last@rams.colostate.edu
Canvas

Kevin Nolan

• Feb 28 “event” with AWS.
  – Canvas unavailable for 5.5 hours.

• “Typo” in input file took down more of their system than expected.

• Communications to campus went well.
Licensing

Diane Noren

Diane will send an email to the group, with updates on software and licensing.
Security Update

Steve Lovaas

• Windows 7 retirement
• Remote access/control from the internet
• Web security headers
• Vulnerability scan responsiveness
• Web site compromises
Windows 7 retirement

• Vista: 4/11/17 final security update (done at CSU)
• Office 2007: 10/10/17 end of the road
• Windows 7 (and Server 2008) “no longer secure”, says MS
  – Need to be moving to Win10
  – End of extended support 1/1/2020
  – BUT with < 3 years to go, MS already warning about unfixable issues
  – Treat this like the XP retirement
Remote access/control from the internet

• Gradual strengthening of our border firewallsing
  – Stage 1 (about 2003): block some things
  – Stage 2: default deny, but allow any requested exceptions (post 2005)

• We’re left with LOTS of holes
  – Stage 3: increase confirming/pruning exceptions (2016)
  – Stage 4: more aggressively block risky protocols (2017)
  – “Risky” = remote control or access that can give root/system access
    – RDP, VNC, SSH, Xwindows, Telnet, etc.

• Rely on Pulse gateway (both web UI and VPN client) to tunnel these
  – This summer: HTML5 support in upgraded Pulse Security Appliance
Web security headers

• SHA1 and SSLv2/3 are gone, TLS1.0 should be on its way out

• Next target: HTML security headers
  – For http, https, html1.0/1.1 – some required, some optional
  – Range from the simple to the complex/problematic

• Let’s implement the 4 easy ones!
  – Required: Expires <date>
  – Required: X-Content-Type-Options nosniff
  – Required: X-FrameOptions DENY
    • Unless the site is intentionally framed, then SAMEORIGIN or allow-from <URL>
  – Optional: X-XSS-Protection 1; mode=block
Web security headers

1) The official document describing coming requirements (the Content Security Policy or CSP) -- we're not doing this part yet, but the CSP will subsume many of the functions of older single security headers
   https://www.w3.org/TR/CSP2/

2) An overview with easy descriptions of the various headers we'll be recommending
   https://www.tunetheweb.com/security/http-security-headers/

3) A checking tool:
   https://securityheaders.io/
   (I'd encourage you to check the "Hide results" box)
Vulnerability scan responsiveness

Doing better, decided to skip a meeting and not shame by name
Web site compromises

Expectations for running a web site

• Maintain current software
• Apply security patches quickly
• Notify ACNS security team
  – If your site gets compromised
  – If you receive a complaint
  – If you find something confusing
  – Don’t wait until it’s fixed
  – soc@colostate.edu

What we actually see

• Lots of old platforms & tools
• Missing patches even for large issues
• We often hear much later
  – I don’t want to hear about it second-hand, after the fact
  – I certainly don’t want to first hear about it when Scott or Pat are sitting in a meeting
Questions?
Going through old papers my dad gave me, I found his map of the internet as of May 1973.

The entire internet.
Network & Telecom Operations

Network Operations

– Wired infrastructure
– Wireless infrastructure

Telecom Operations

– General
– VOIP
Wired Infrastructure
Network infrastructure upgrades completed since Nov.

- MERC (The Factory)
- New routers at South Campus
Wired Infrastructure
Dual 10G upgrades completed since Nov.

- Aggie Labs
- BSB
- VTH
- DMC
- Yates
Wired Infrastructure
Dual 10G upgrades in the queue for this FY

- A/Z
- Clark A-Wing
- Chemistry
- Gibbons
- NESB
- Shepardson
- Student Rec
- USC
Wired Infrastructure
Construction projects

Active

- New Stadium (start of July)
- New Chemistry (End of July)
- New Biology (End of July)
- New Health Center (Mid June)
- Shields Underpass

Coming Soon:

- TMI
- Animal Sci Addition
- WCNR Addition
Wired Infrastructure

Housing Networks

Residence Halls
129.19.32.0/19

Offices
129.82.0.0/16
10.0.0.0/8
Wired Infrastructure

“As-Builts”
Wireless Infrastructure

Since Last Meeting:

• New routers!

• All GA buildings 802.11ac Wave 1, starting Wave 2

• Nearly all GA classrooms upgrade to Wave 2

• Replacing older AP-125's (Non-802.11ac) all over campus.
Wireless Infrastructure

802.11ac upgrades:

- LSC North
- Engineering
- Scott Bioengineering
- McGraw, ATC
- Animal Science
- Laurel Hall
- PreConstruction
- Forestry
- Physiology
- GSB
Wireless Infrastructure
Facebook/Twitter feeds

- Facebook:  www.facebook.com/csuwireless
- Twitter:   @CSUWireless
Network/Telecom operations

• Phone problems!? Plan is to transition these to HelpDesk and out of the toc@colostate.edu and noc@colostate.edu e-mail.

...or call 491-5881 and Darlene, our campus operator, will help you!

Primary/Secondary network managers to retain special “level 1” support.
Network/Telecom operations

Network Operations moved to Zabbix.

Telecom Operations in progress.

Subnet Manager link to “Nagios” to be changed to “Zabbix!”
## Network/Telecom Operations

### System status

<table>
<thead>
<tr>
<th>Host group</th>
<th>Disaster</th>
<th>High</th>
<th>Average</th>
<th>Warning</th>
<th>Information</th>
<th>Not classified</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOC Level1 Routers / Firewalls</td>
<td>0</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NOC Level1 Switches</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>NOC Level2 Switches / RAPs</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NOC Level3 Misc Devices</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NOC Level3 Routers / Firewalls</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NOC Level3 Switches</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>NOC Level3 UPS</td>
<td>0</td>
<td>0</td>
<td>11</td>
<td>0</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>NOC Level3 Wireless</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Updated: 17:21:44
Telecom operations

Missing phone lines...and turning off POE

• Going building by building looking for phones that don’t answer or otherwise don’t exist.

• Turning off POE for ports not using power to help with 911 location service.
POE, 911, conference phones....

- Going building by building to confirm 911 records.
- Conference room phones:
  - We’ll provide an injector for free
Telecom Operations

This meeting’s

“Closet of Shame”
Telecom Operations

After
Telecom Operations

We need network manager’s help....

...keeping these closets clean, neat and the cable managed/labeled properly.

Redoing the closets takes time and money.

**NOTE:** Charges may apply $62/hr – usually 2 hours and a scheduled outage.
Telecom operations

FREE!

Data patching in MDF/IDFs

(Account# required, but if “scared”, you can put in all 0’s!)
VoIP Update/Upcoming

• Main Campus servers upgraded 01/08/2017

• Q1 implementing call encryption
  – PCI compliance on VoIP network
  – You’ll start noticing a lock symbol on the phone icon.

• 7505 Phones
Where’s your phone?
Reminders

• Moving Phones – Don’t!
  – Telecom will move them for FREE

• Move Policy:
  – Phones can only be moved by ACNS/Telecom. To instigate a phone move by ACNS/Telecom, a service order must be placed: Service Order Form.
  – A $56 fee will be assessed for each phone that was moved without a preceding service order.
  – Turning off POE (Power over Ethernet) to non-phone ports.

• No Building Power = No network = No Phone
Thank you.

Network Operations
&
Telecom Operations
Next Subnet Managers Meeting

Wednesday, May 24, 2017
10 am – noon
LSC 372 - 374

Go mow your lawn!