EMORY
LIBRARIES &
INFORMATION
TECHNOLOGY

IT Briefing

December 18, 2014

North Decatur Building

4th Floor Auditorium

IT Briefing Agenda

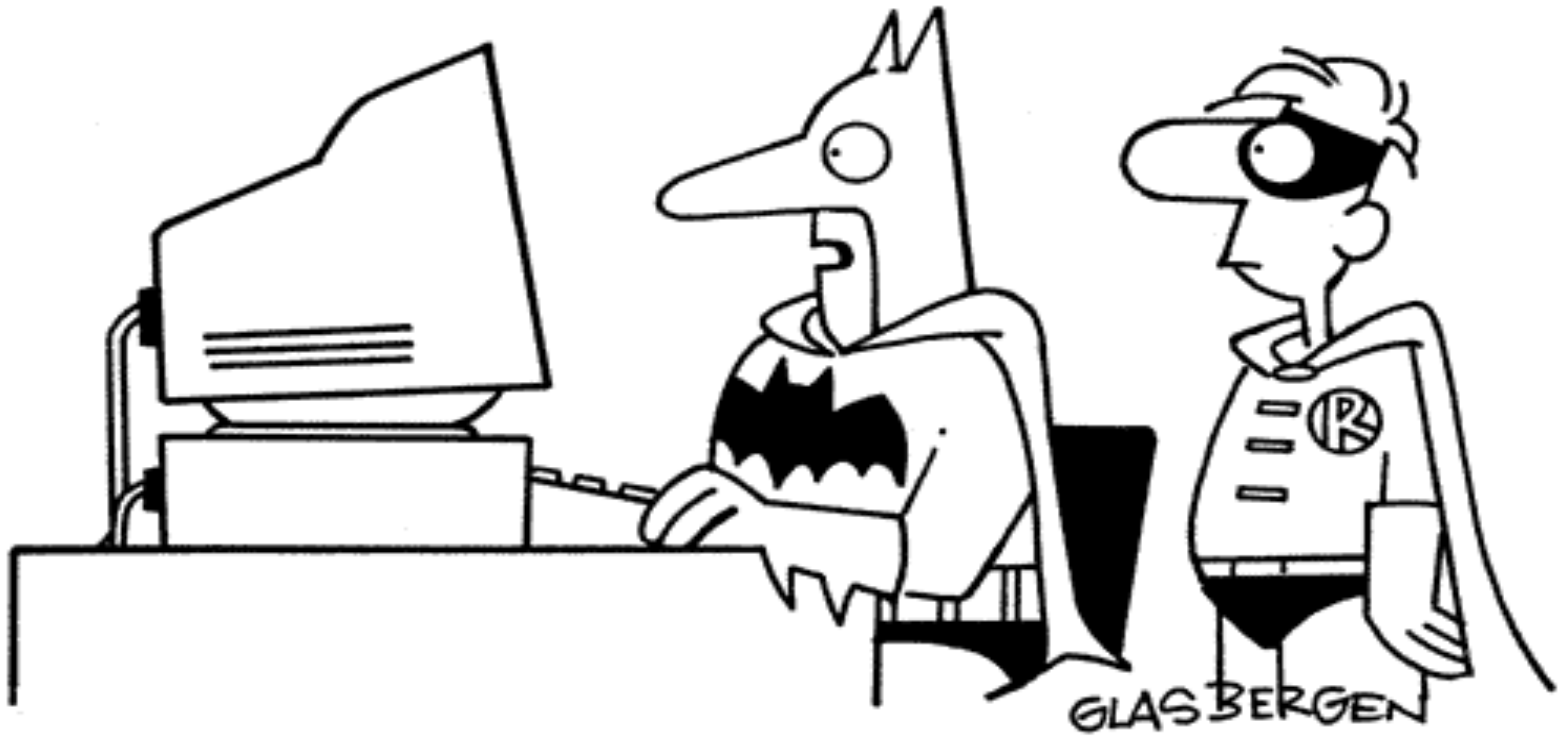
- Postini to EOP Transition
- Border Update
- Security Update
- IT Briefing for 2015

- Jay Flanagan
- Ben Rosenblum
- Derek Spransy
- Wade Moricle

Jay Flanagan

Manager, Messaging Team, Infrastructure

Postini to EOP Transition



"Oh, the usual stuff. Spam from the Joker, another e-mail virus from the Penguin, an illegal chain letter from Cat Woman...."

What's Happening Now?

- Engagement with MS
  - Wes Blalock
  - Handling the technical side
  - Global rules being moved
  - Global approved and blocked senders lists

What's Happening Now?

- Engagement with Intellisoft
  - Holly French
  - User docs
  - Email correspondence

What's Happening Now?

- Communication Plan
  - Emails
    - Weekly through January
    - Quick Reference Guides
  - IT Briefings
  - Articles via Wheel / Emory Report
  - FAQ's
  - Web Site
  - Other

How Will it Affect Me?

- Will get more spam initially as we tweak the service
- No more quarantine email
- Managed via the junk folder
- Will need to recreate new personal approved and blocked senders lists
- Will have a bigger role in managing own spam
- Right click and then click on junk and choose option

Time-Frame

- Complete Technical Work – December
- Finalize Communication Plan – December and early January
- Begin sending out communication about the change – Early January
- Continue to send out communication – Throughout January and early February
- Cut over tentatively scheduled for February 9th

Questions?

Ben Rosenblum

Communications Architect, Architecture and Security Team, Infrastructure

Border Update

Sense of Urgency

- Internet usage has increased ~33% since the beginning of the current school year. It has more than doubled since the beginning of the last school year.
- This increase has pushed the limits of the current 7600/ FWSM/IPS border beyond it's original designed capacity.
- Original design limit was 512K routes on the 7600. We are currently at 514K.
- Original design limit was 256K simultaneous NAT translations. We are currently peaking at 350K.
- Original design limit was 5G aggregate bandwidth usage through the IPS. We are now at over 4G daily.
- All pieces of the border have exceeded their design limits. Most have been temporarily patched to provide additional capacity while a new border is installed.

Problem 1 – Routing Table Size

- In July we identified that the CEF memory on the 7600s were above 95% utilization.
- Default CEF memory allocation on the 7600 provided space for 512K total routes.
- CHG122495 (Normal – Level 3) executed proactively on August 1st.
- Manual reallocation of memory increased capacity to 768K by harvesting memory from other processes and limiting our future growth.
- Had we not executed the change, if/when the internet topped over 512K routes, we would have gone into an unstable state where routes would be dropped at random causing traffic to randomly not reach it's destination.
- The internet reached 512K routes on August 12th for the first time. Large scale outages happened while ISPs scrambled to fix this. It is still over 512K as of today.

Problem 2 – IPS Throughput Capacity

- When students came back to school we started noticing that the internet was acting “weird” during peak usage. We had a gremlin.
- Users were reporting failure to reach some pages while others loaded perfectly and quickly.
- The original IPS design could only handle a total of 3G through each segment. This is a sum of both our inbound and outbound traffic.
- The IPS had 3x 1G paths wired for each 10G segment.
- Analysis of the IPS was showing multiple 1G paths were reaching full capacity and causing traffic to be dropped. Since flows were limited to a single path, this was believed to be the cause of the issue.
- CHG123533 (Emergency – Level 3) was executed on September 18th. This change removed two of our four redundant paths and reallocated those resources to the two remaining paths.
- Both IPS devices have sent alarms since that individual 1G links were above 90% indicating that we are still approaching maximum capacity.
- While this fixed one issue, it did not resolve the original problem.

Problem 3 – NAT Session Limits

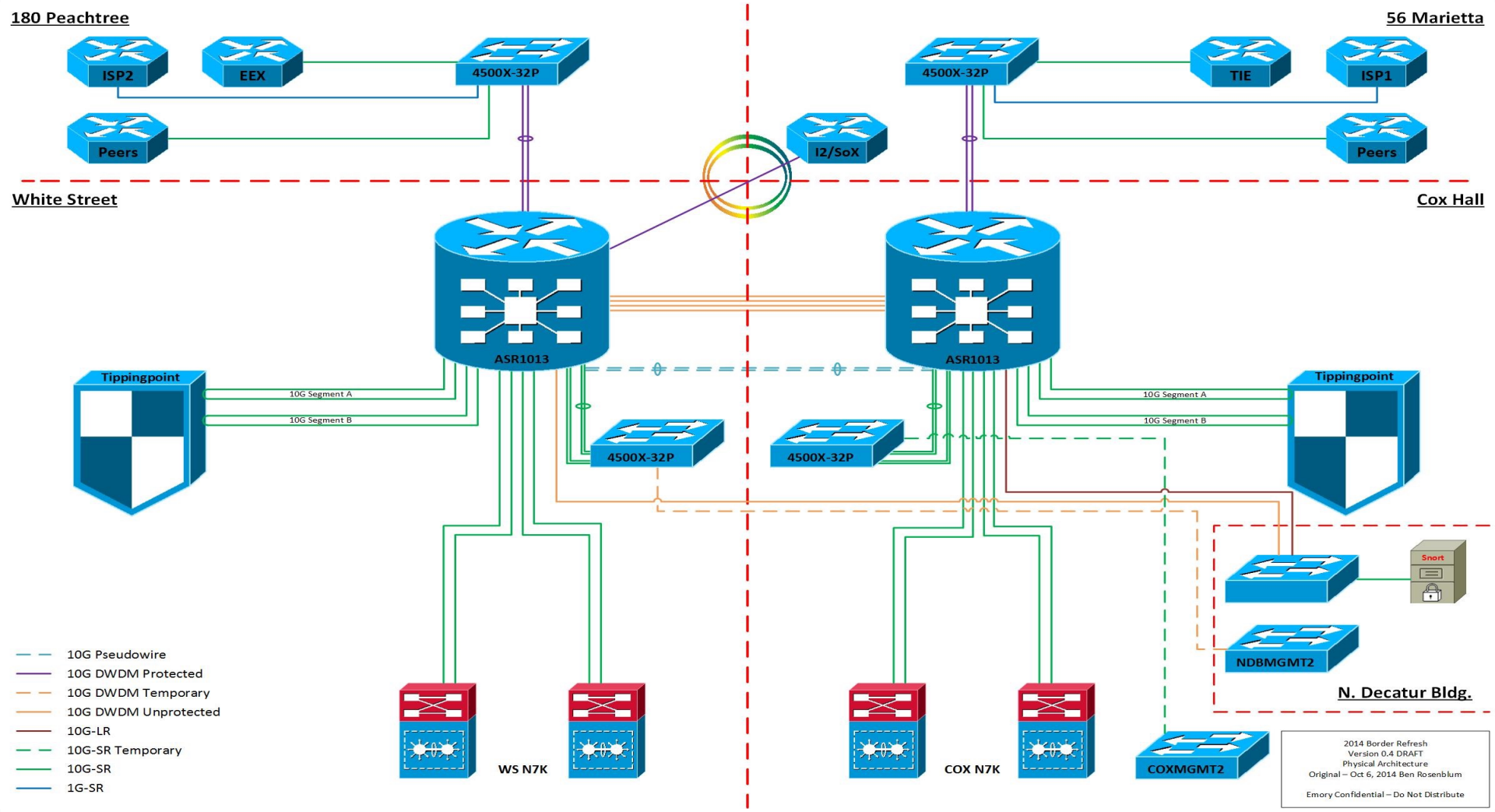
- Initially we believed that the IPS capacity limit was the cause of the degraded service.
- After the IPS was patched, we still noticed issues.
- After additional troubleshooting we identified that the FWSM cluster in the 7600s which handled our NAT would reach their 256K limit at around 11AM every day and stay at maximum until about 4PM.
- When the system runs out of NAT session resources, users trying reach the internet would be unable to get to their destination.
- As sessions would timeout, some user traffic would randomly be given those now free sessions and it would reach it's destination. Once a session was allocated, that traffic would flow unobstructed until it timed out or was closed.
- CHG123669 (Emergency – Level 3) was executed on September 24th to add an additional FWSM cluster. Some academic load was moved to this cluster to reduce the pressure and restore services.
- Internet service was finally restored to a non-degraded state.

New Border Design

Requirements:

- 20G of aggregate bandwidth expandable to 60G.
  - 100G was the original target however it proved to be cost prohibitive and was removed from the requirement list.
- NAT space to grow up through 4M translations
- Routing space to grow up through 1M routes
- Capability to add border firewall in the future
- Resolve single point of failure of the TelX Internet Exchange and 56 Marietta
- Site level redundancy using White Street as alternate site instead of NDB
- Estimated lifetime – 5-8 Years (8 would require a mid-cycle upgrade of some components)

New Border Design



New Border Status

- Final BoM was triple bid to WWT, CDW, and Presidio.
- Equipment ordered from CDW (lowest bidder) on December 3rd. Total cost ~$2.04M.
- Estimated arrival time is between now and January 28th.
- New racks and power to be installed in Cox Hall and White Street prior to January 28th.
- 180 Peachtree under evaluation as second PoP.
- Phase 1 Rollout – Migration from 7600 to ASR1013 (January thru March)
- Phase 2 Rollout – Migration of border services to new infrastructure (April until completed)

New Border Design Caveats

- Current border throughput is limited to 20G because of the IPS. This is expandable by adding an additional IPS to each facility.
- If expanded to 40G worth of IPS, this approaches the current throughput limit of the ASR1013. While they have 100G switch processors, each packet is passed through the device twice which decreases it's available capacity to 50G. One more additional IPS can be added if needed to increase IPS capacity to 60G. The addition of a second or third IPS does not increase the passes above 2 as they run in parallel.
- If a border firewall is added in the future, this increases the passes from 2 to 3 which decreases available bandwidth from 50G to 33G. This can be mitigated by replacing the switch processor with 200G capable cards which would make the available throughput now 66G.
- Assuming that three IPS devices are installed at each site, and that the switch processor is increased to 200G, the total theoretical maximum that this border can support is 60G. To note, this will potentially require reconfiguration of the ports to support this connectivity.
- No single flow can ever exceed 10G.

Border Update

Derek Spransy

Sr Information Security Specialist, Information Security

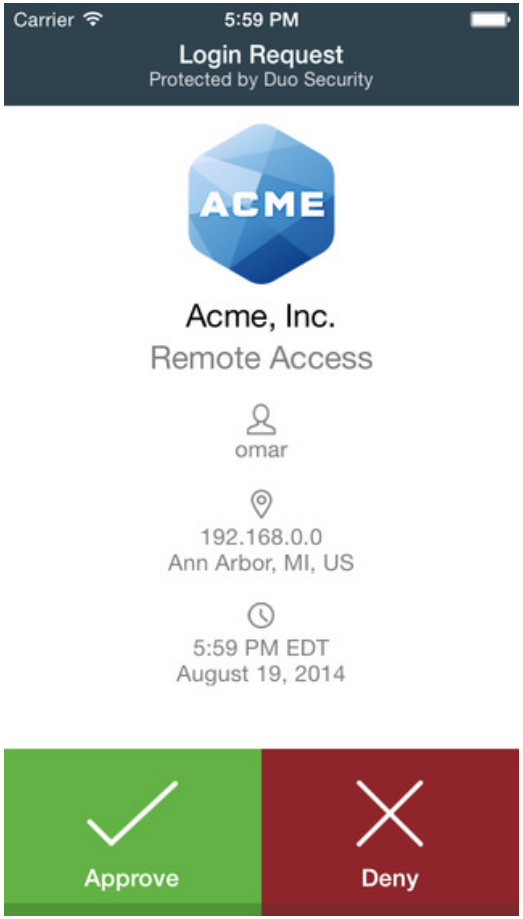
IT Security Update

Poodle/ShellShock /Old OS'

- Continue patching systems for these vulnerabilities
- Over 100 systems still using SSLv3 that are Internet facing. See KB04501 for additional information
- Continue to remediate instances of old unsupported Operating Systems: XP, 2003, MacOS 10.7 and below

Two-Factor Authentication Update

- Duo Mobile Security has been chosen to go to the Proof of Concept phase
- In the coming months we will test integration with the eight identified high value systems
- If successful Duo will be chosen to move into production



Security Update

Wade Moricle

Marketing and Communication Specialist,
Campus and Community Relations

IT Briefing 2015

How We Did in 2014

- 10 Security Updates
- 9 Office 365 Updates
- 5 IdM, Single NetID, LDA Migration updates
- 4 PS Financials Updates
- 3 Core Router Updates
- 2 Monitoring, NAC Updates
- Kronos, E-Notify, Apple McAfee, ART Review, Emory Commons, SPOK Mobile, Back to School, Trusted Storage, Service Desk, B&N, SimplyMap, REDCap, Eduroam, Bell Techlogix, Box.net, Virtual Desktop, Blackboard CSI,
- ….and a partridge in a pear tree!

What Do We Want For 2015?

- ?
- ?
- ?
- ?
- ?
- ?
- ?

Thank you for coming!