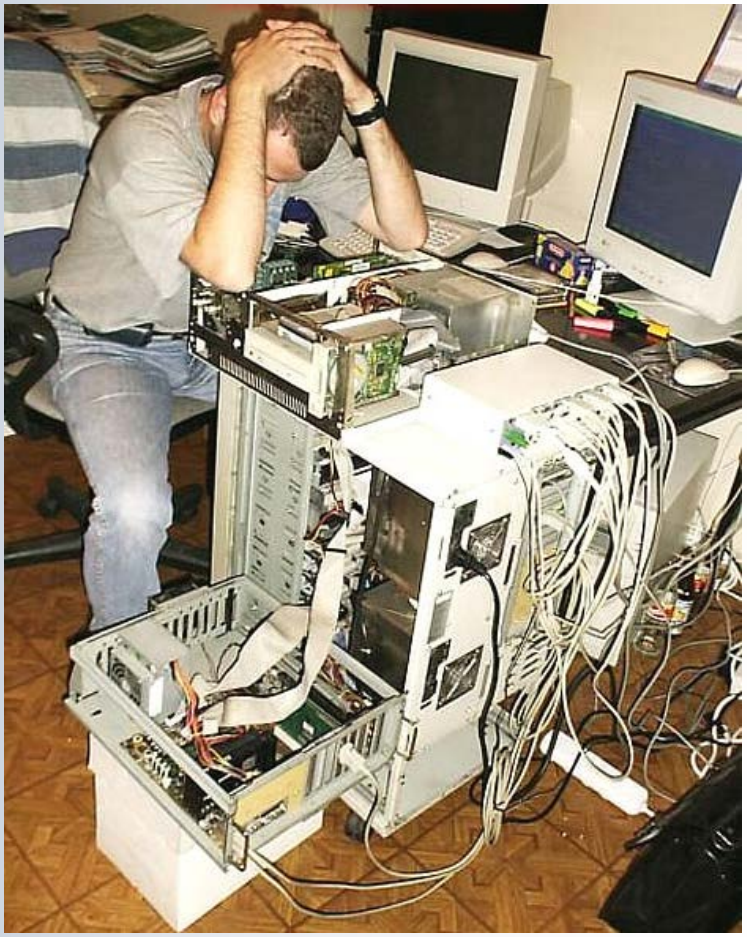
COMP 175

System Administration and Security



"Yesterday I couldn't spell system administrator, and today I are one."

Instructor

.edu

Martin Maxwell – Lecturer (Since 2008)

Office: Baun 210

Office Hours: TU/TR After class (appt)

E-mail: mmaxwell (at) pacific.edu

Currently

COMP 175 - System Administration and Security – Fall
Spring

Previously

ECPE/COMP 177 - Computer Networking
ECPE/COMP 178 - Computer Network Security – Spring
COMP 293 - Security Assessment and Assurance

The dot in .ca.gov

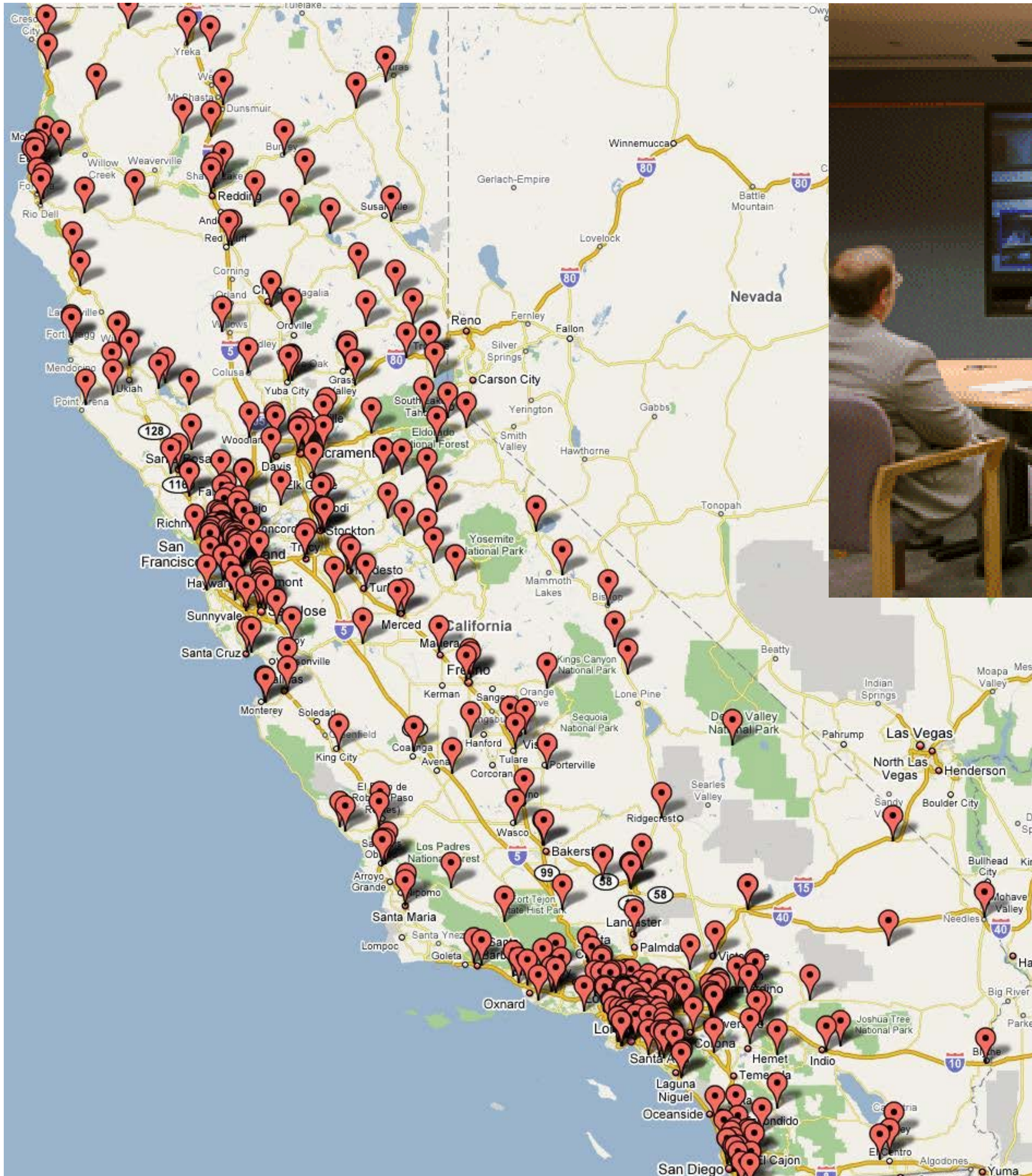
.gov **Retired 8-2012**

Technical Lead, Chief – Enterprise Network Security

California Department of Transportation

- Sun Servers & Workstations
- Six Stratum 1 NTP servers
- Three 1Gb POP's
- 550 sites – MPLS WAN
- Security Appliances
- DNS, DHCP, IPS
- Content filtering
- Logs

Enterprise Remote Administration

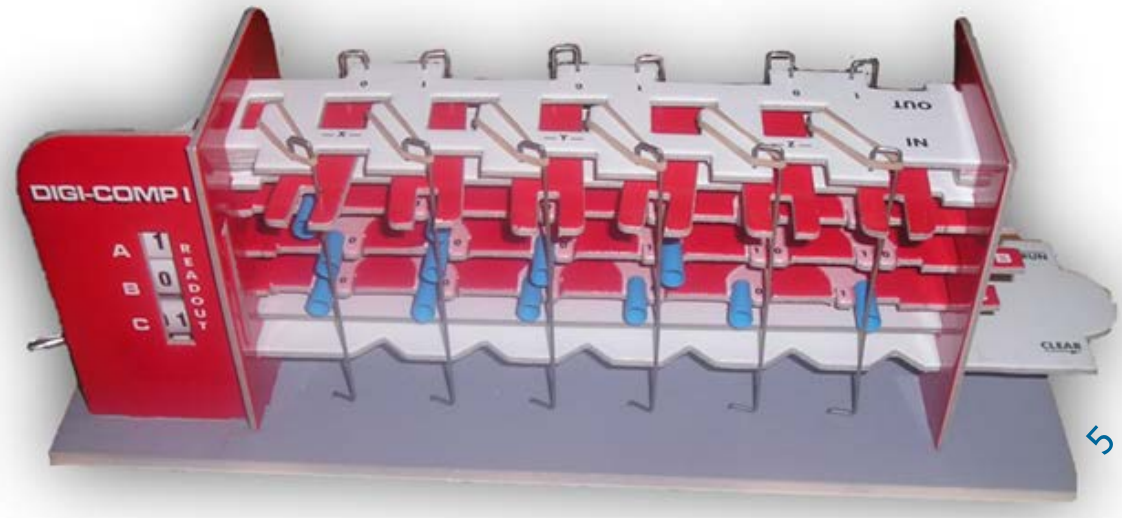


.com

Research & Consulting Services (*aka Startup*)

- Wine filterability software & appliances *(aka an App)*
  - Client production ~>1M cases/year
- Manage a /29 Internet address space
- Linux Internet servers – *since 1995*
- SMTP, DNS, DHCP, NTP, HTTP, etc. services

My first computer
Digi-Comp 1



Institute of Malware Technology

It Begins...

Oslexic - Osnostic - Unices Used

UNIX – AT&T System V

HP-UX

NeXTSTEP

SunOS

Solaris

PC/IX

QNX – *crashed it*

SCO-Xenix

IRIX

NCR UNIX

AIX

BSD

Linux – Slackware, CentOS
Ubuntu, SLAX

OS-X

Plan 9

As well as:

CP/M Wang VS

OS/2 DOS

Windows

Class Website

- Class site: Canvas
- What will be online:
  - Schedule
  - Homework assignments
  - Lecture notes
  - Class reading & reference material
  - Links to various resources

Homework will require access to Lab/Linux

Course Outcome Assessment

- Homework/Labs: 25%
- Quizzes: 25%
- Mid-Term Exam: 25%
- Final Exam: 25%
- GRADING POLICY:
  - A: 90 - 100%
  - B: 80 - 90%
  - C: 70 - 80%
  - D: 60 - 70%
  - F: 0 - 60%
  - Grades within 2% of a border assigned a ± accordingly.

Attendance

- Attendance at all classes is necessary
- Any student missing a class is responsible for studying the material discussed and for being aware of announcements made during the class
- Lecture material will be available online
- Quizzes will normally be announced in the schedule
- Low attendance on any given day may result in a pop quiz

As Described

COMP 175 System Administration and Security(3)

Students are introduced to an operating system from an administrator's standpoint. Topics include installation with the proper allocation of disk resources, maintaining the operating system and various subsystems, security issues that include server hardening, host firewalls and network security issues. Students also study account administration in a networked environment, change management and intrusion detection. Prerequisites: Completion of all fundamental skills and familiarity with console-based operating systems commands. Junior standing. (Fall, every year)

Class Objectives

- Install OS, utilities, applications
- Maintain it – patches, backups
- Manage files, directories, permissions
- Learn how the documentation system works
- Make it secure
- Monitor it

  The above is too easy for this class [Y/N]
- Headless
- Virtualized?
- Cloud?
- Any class objectives?
- Optional projects for those interested

Objectives – the SQL

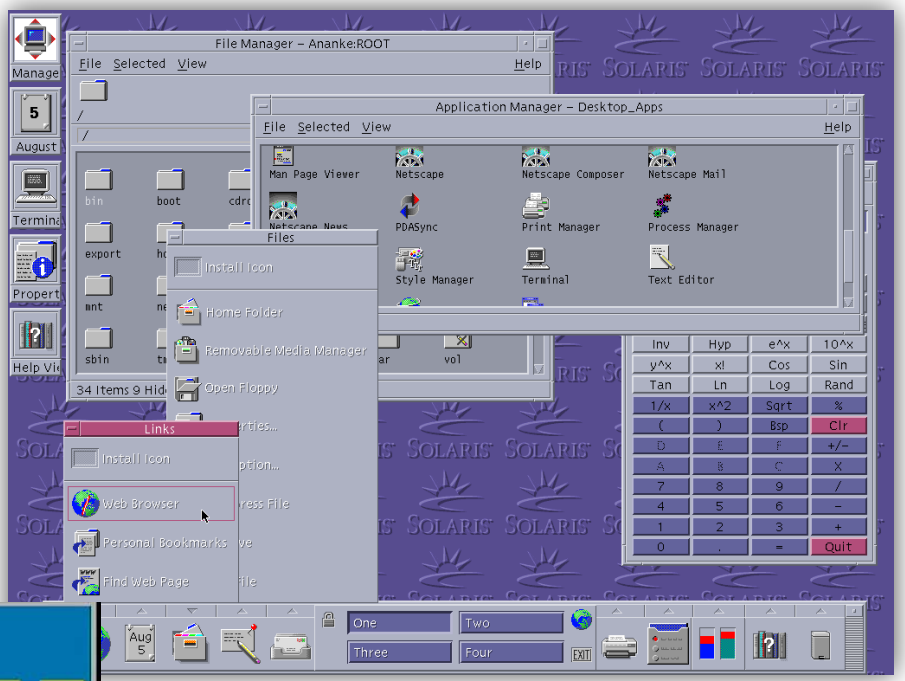
- You will learn how to:
  - Install
  - Configure, and
  - Manage
    - Securely
- A server providing
  - Internal and
  - Internet
- Services without looking like a:
  - n00b or an
  - id10t

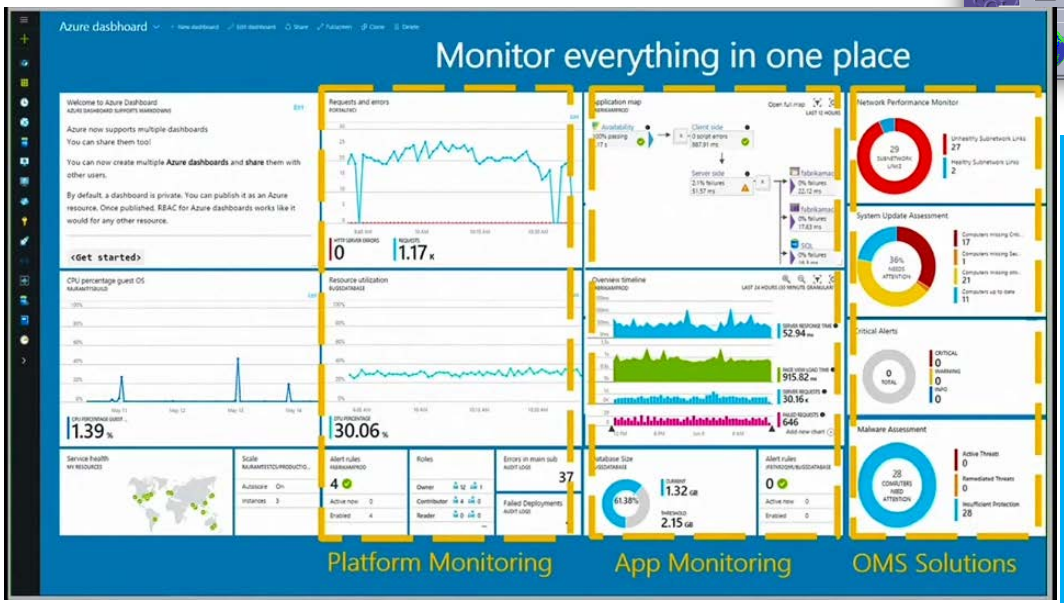
Course Outline

- Introduction
- History
- Operating Systems
- Commands
- File System
- Shells
- Applications
- Daemons
- Processes
- Virtualization
- Installation
- Logging
- Vi
- Backup
- DHCP, DNS, SMTP
- NTP
- Samba
- Firewall
- Applications
- Budgets
- Windows
- Security

What Systems?

- So many OS's
- So little time





It Begins...

UNIX (technically Linux)

Class will presented using:

- Ubuntu (Jammy Jellyfish)
- Possibly others for comparison
  - AWS
  - SLAX
  - CentOS
  - Slackware

But I'm running……

MeeGo Puppy BackTrack Imagineos ChromeOS
OS X Solaris RedHat z/OS AIX GNU Hurd

As long as it's a functional analog …..

or

Use a Virtual Machine

Command Line Interface

Number of UNIX/Linus distros: **TNTC** *

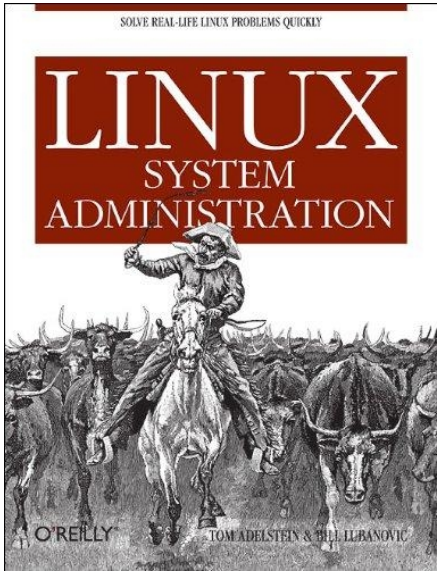
* To numerous to count

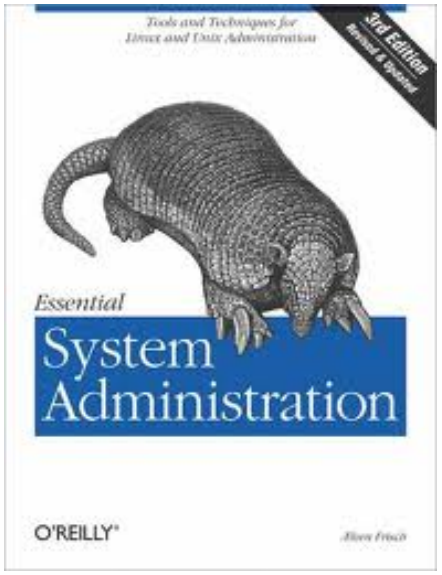
A Top 10 List

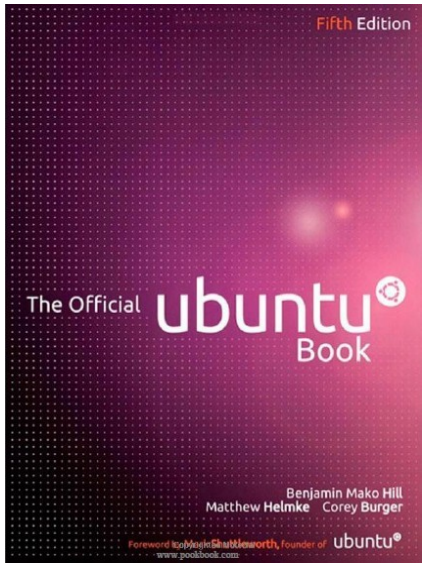
Top 10 Things to Call a Linux Distro from Microsoft

10. IntelliActiveDirectLiveLinuxX Starter Edition16SP2
9. The best thing Microsoft ever came up with
8. Linux BSOD Server Edition 2022
7. All Your Linux are Belong to Us
6. Linux Zune Free Edition
5. Linux BOB Professional
4. Linux ME Ultimate
3. Registry Linux
2. U-reboot-tu
1. Panix

Technical References







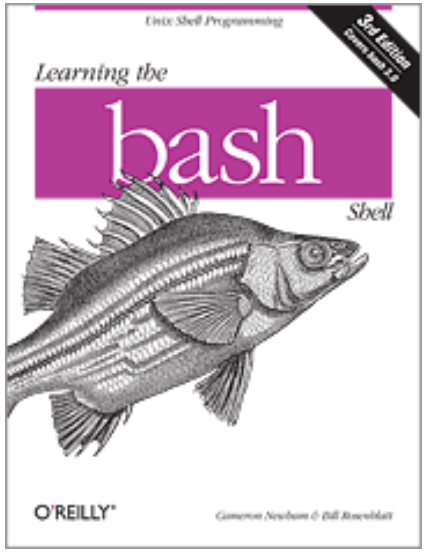
- The DHCP Handbook
- DNS and BIND
  - DNS & Bind Cookbook
- Sendmail (1287 pages)
  - Sendmail Cookbook
  - Sendmail Companion
- Apache Definitive Guide
- Essential SNMP

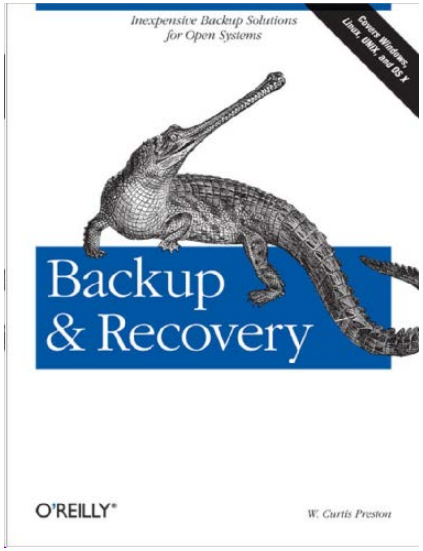
- meh

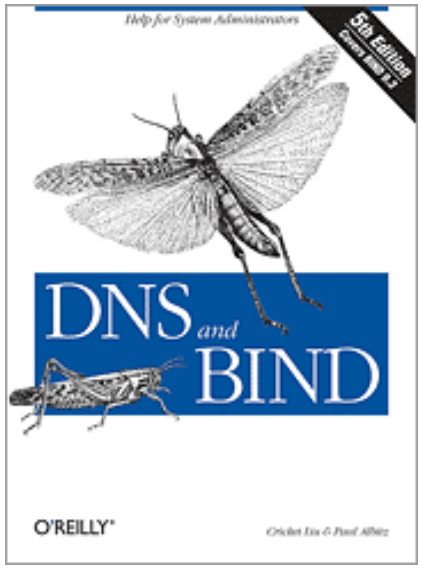
Technical References

As well as....

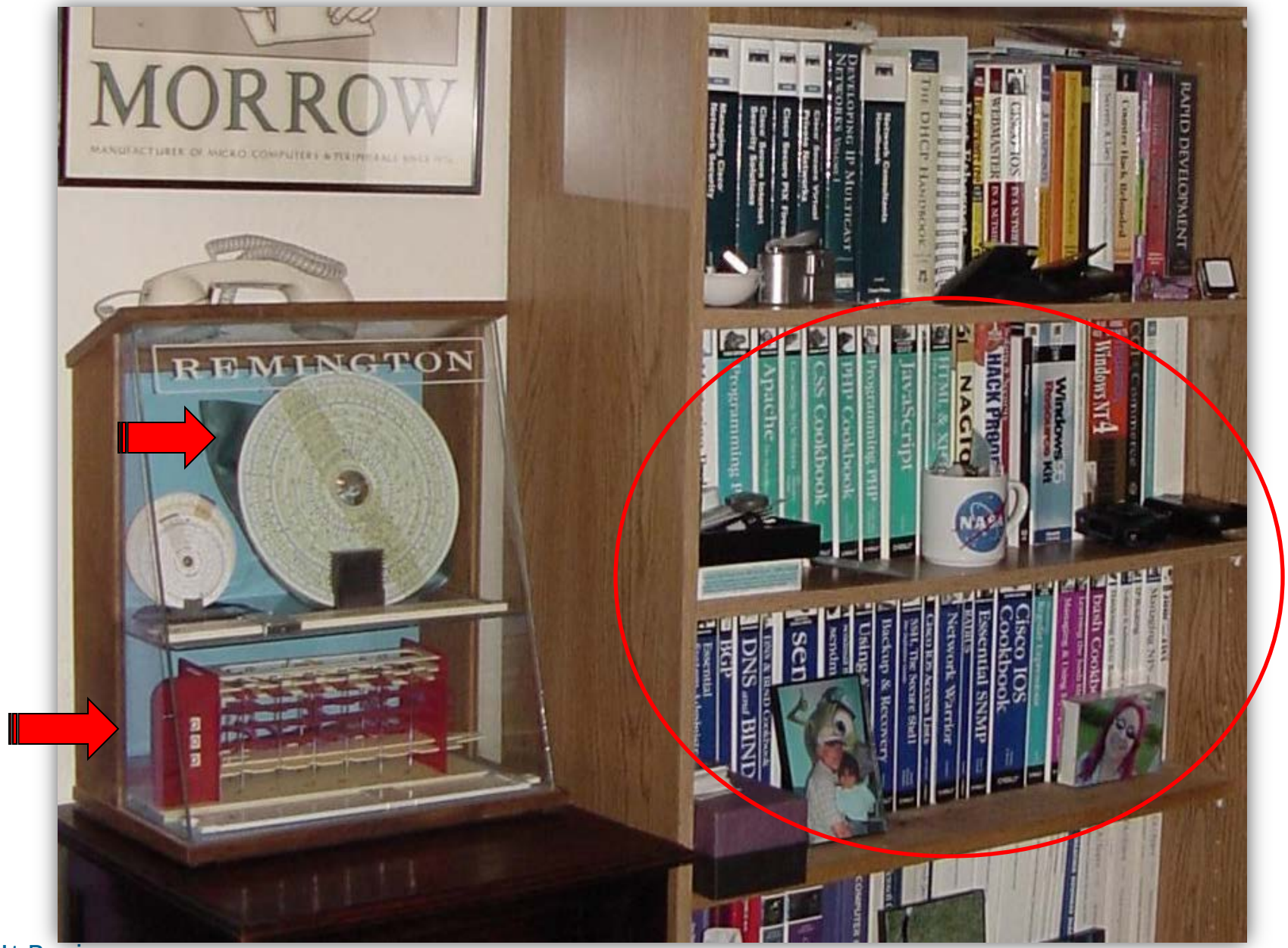
- TCP/IP Network Administration
- Managing NFS
- Using Samba
- Radius
- BGP







Reference Library



Internet Resources

"On 6 August 1991, Sir Tim Berners-Lee, then a humble scientist at CERN, made the first page on the World Wide Web publicly available in a move that, unbeknown to him at the time, would change the world more quickly and profoundly than anything before or since." *web is 31 years old*

You grew up with the Internet, the web

Next gen growing up with iPhone

Textbook

- No required textbook
- Reading material will be available

- In lieu of a required textbook – you may want a USB flash drive to install & configure a persistent live image ~8GB+

Rules

- No malware, rootkits, trojans, exploits, etc.
  - Save that for ECPE/COMP 178 in the Spring
- No whining
- Coopetition & leverage
- Don’t generate noise on the network
  - Monitor configuration
  - Log

Assignment 1: Class Experience

Name:

Operating System Poll

- Windows (version)
- Apple OS-X (Lion?)
- Linux Distro (which)

Why?

Experience Levels

Laptops? Desktop?

CPU? Memory?

Expectation from class

Homework

System Administrator

aka SysAdmin

Defined

- System administrator - responsible for installing, supporting, and maintaining servers or other computer systems, planning for and responding to service outages, and other problems.
- Most important skill is problem solving, frequently under various sorts of constraints and stress.
- Typically on call when a computer system goes down or malfunctions, and must be able to quickly and correctly diagnose what is wrong and how best to fix it. 24x7x365

Challenges

- Difficulty with teaching system administration is that the industry and technology changes much faster than the typical textbook and coursework
- Difficulty with being a system administrator is that the industry and technology changes fast. The scope of knowledge required is also increasing.
  - Components
  - Operating system
  - Application software
  - Networks & Network services
  - Storage
  - Virtualization
  - Security

SysAdmin Duties

- Analyzing system logs and identifying potential issues
- Introducing and integrating new technologies
- Performing routine audits of systems and software
- Performing regular backups (and testing the backups)
- Applying OS updates, patches, and configuration changes
- Installing and configuring new hardware and software
- Adding, removing, or updating user account information
- Resetting passwords
- Answering technical queries, dealing with frustrated users
- Responsibility for security
- Documenting the system configuration
- Troubleshooting any reported problems.
- System performance tuning.
- Ensuring network infrastructure is up (monitoring)

A Few Examples

Posted at: 8:40 PM, August 4, 2013

We are still working in full force on the configurations to the core network servers and are continuing to work through the defined strategy to bring up services.

Posted at: 7:05 AM, August 5, 2013

University of the Pacific network systems are still down this morning, including the website, IP phones, email, insidePacific, and Sakai. The Office of Information Technology has been working through the weekend, 24/7, to restore systems.

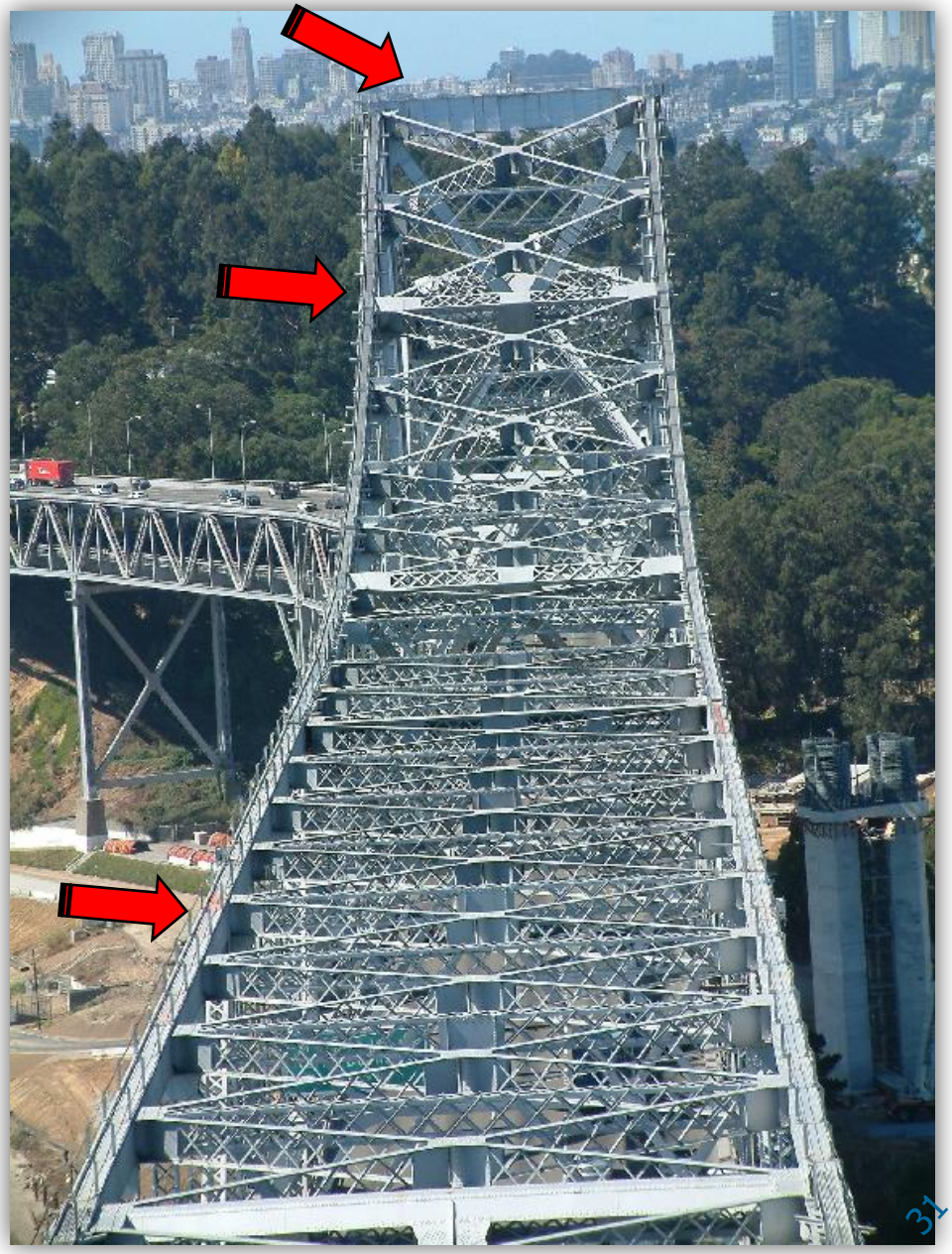
Posted at: 11:39 AM, August 5, 2013

Attention students and parents: The Stockton-campus Student Accounts Office has extended the August 1 payment deadline to Friday, August 9, due to the current system outage.

...other duties as required

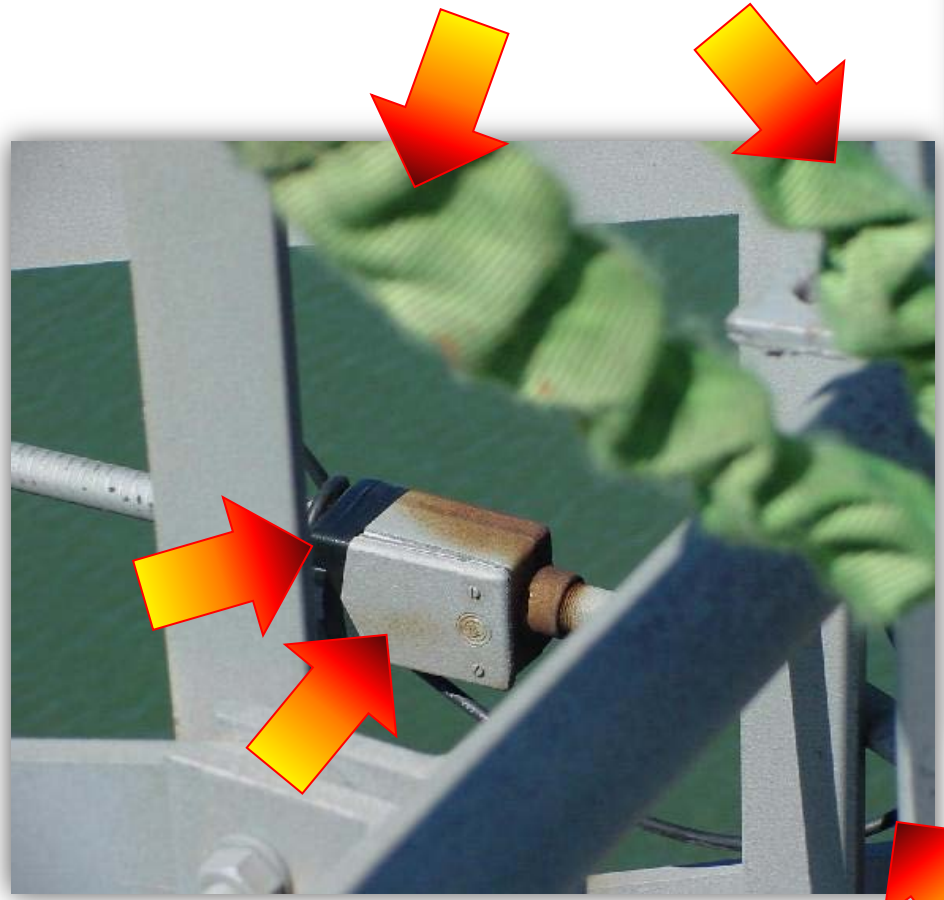
Previous duties same as:

- Database Admin
- Network Admin
  - Interesting worksites



A Wireless Bridge

Identify the arrows

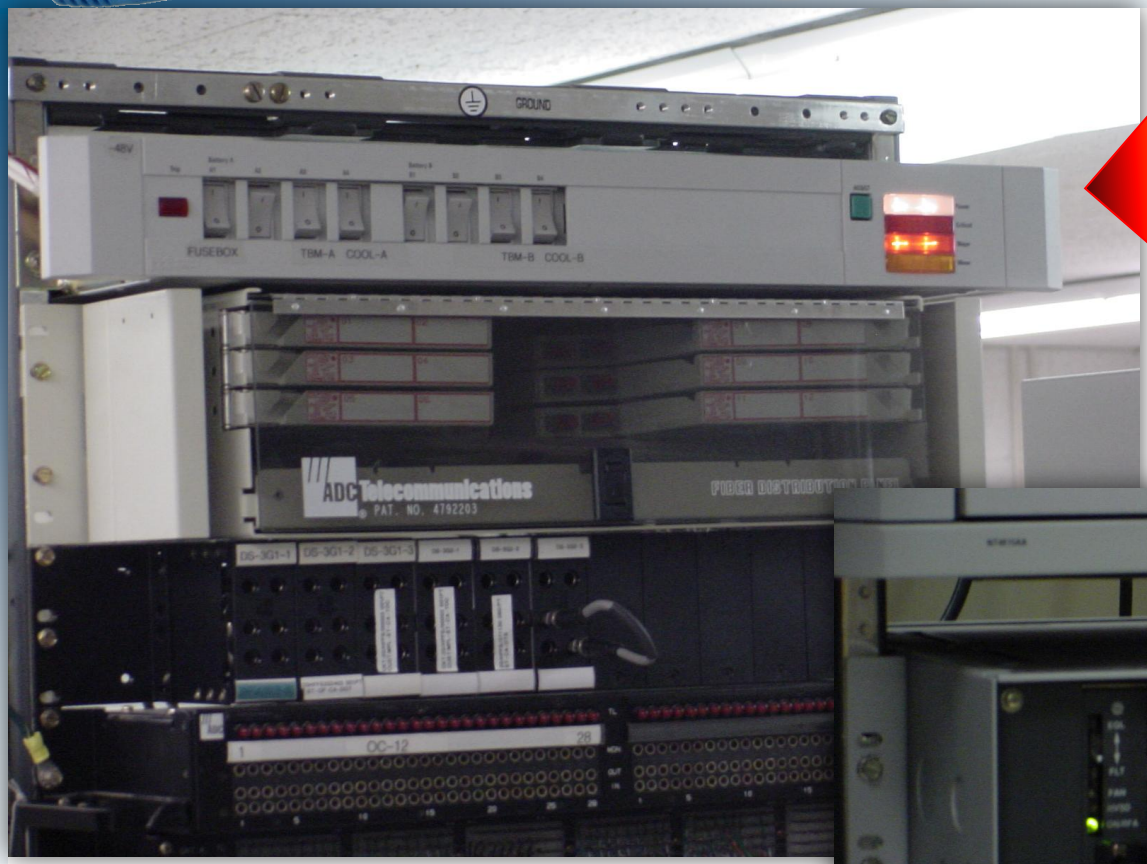


No bird poop!

Wireless is largely line of sight.....

Raised Floor – Find A Cable

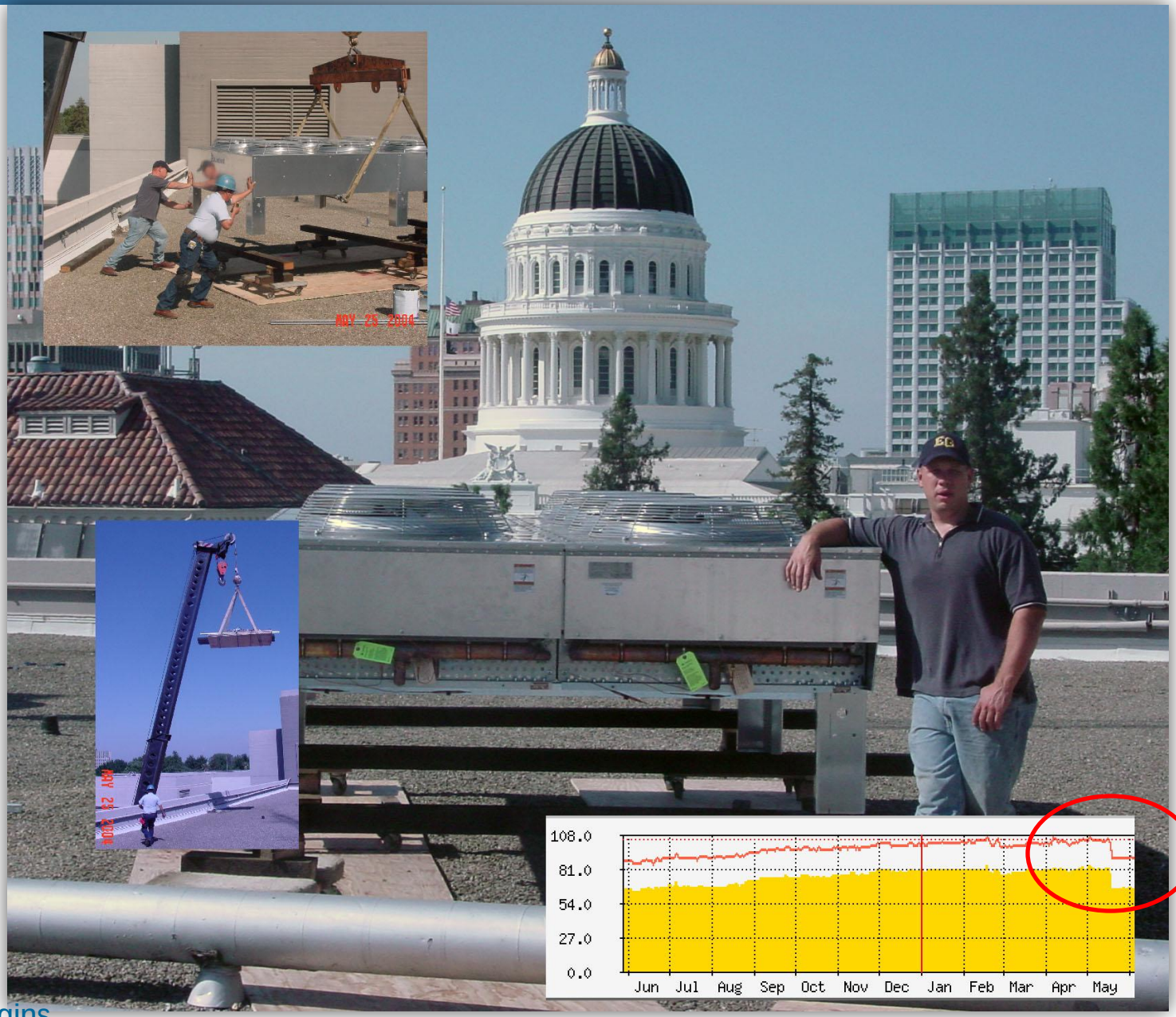
Warning Lights....warn...



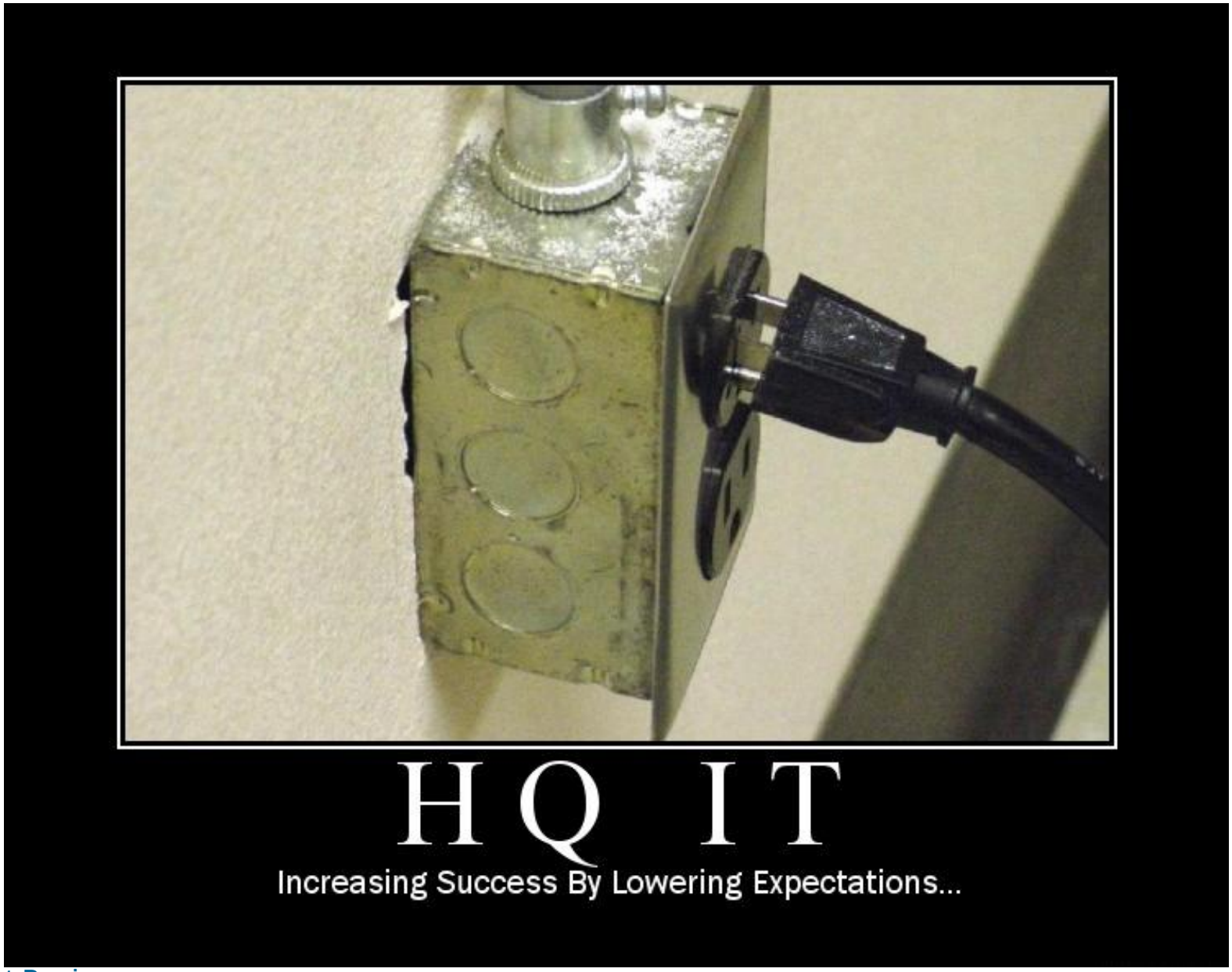
Major Fault

Who's Fault?
Redundancy only goes so far

Chillin.....


108.0
81.0
54.0
27.0
0.0
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Mar
Apr
May

Room Access & Halon Panels



Infrastructure

What is not pictured…

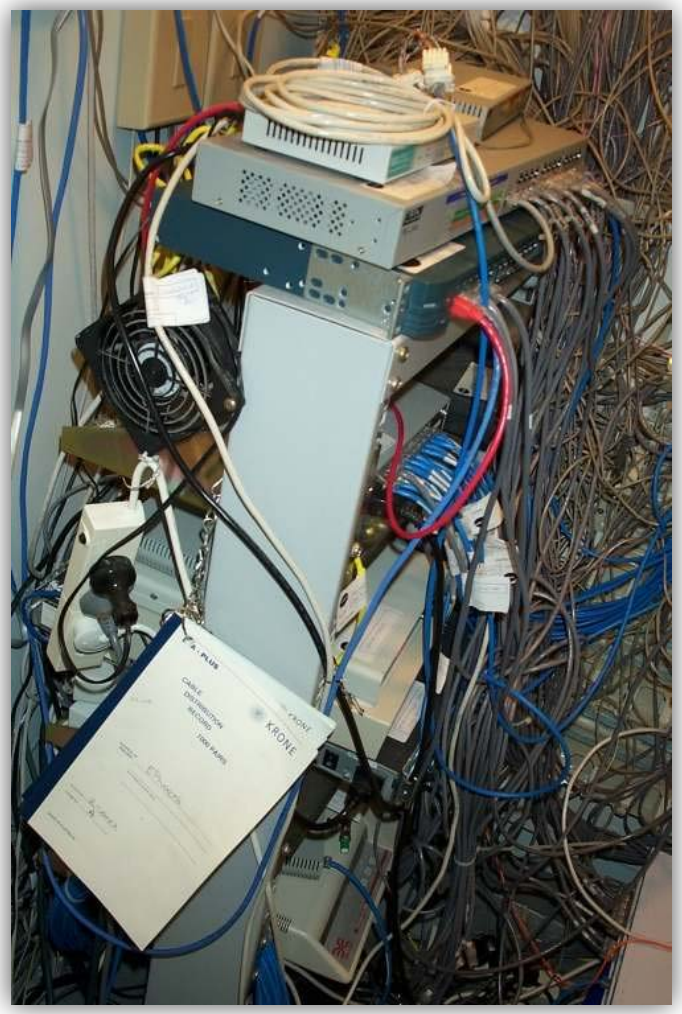
- Weekend
- Break in chilled pipe
- No chilled water
- 5K sq ft data center
- Humid – very humid
- Hot
- Big UPS’s
- Big PDU’s

Ownership

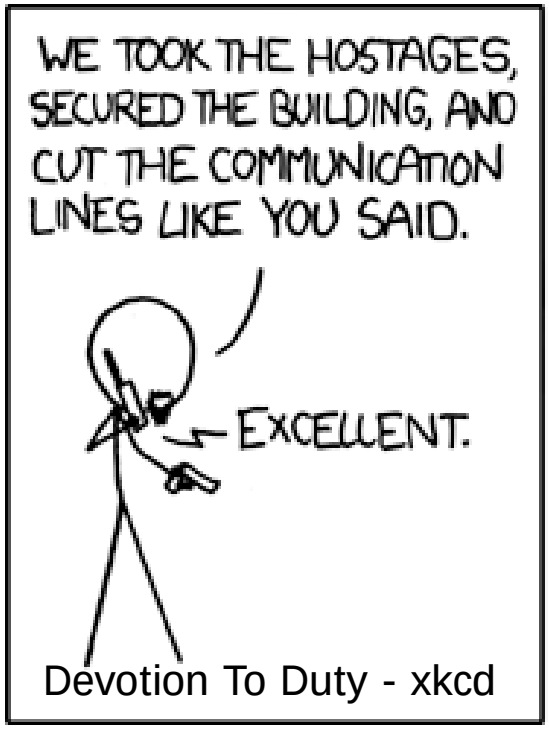
- If you don’t own it – you can’t count on it
- What is not measured, cannot be managed
- Evil has to sleep at night, stupidity is 24/7
- Bad documentation is worse than none at all
- Things rarely happen during 8-5
- Redundancy doesn't just happen
- Manage management
- Insufficient paranoia
- Benthic technology
- Inspect everything
- Maintenance

High Availability

- Availability vs downtime (scheduled maintenance)
- Availability != uptime (WHY IS THAT?)
- Redundant
  - power sources
  - power distribution units
  - UPS
  - power supplies
  - NICs
  - switch ports
  - network circuits

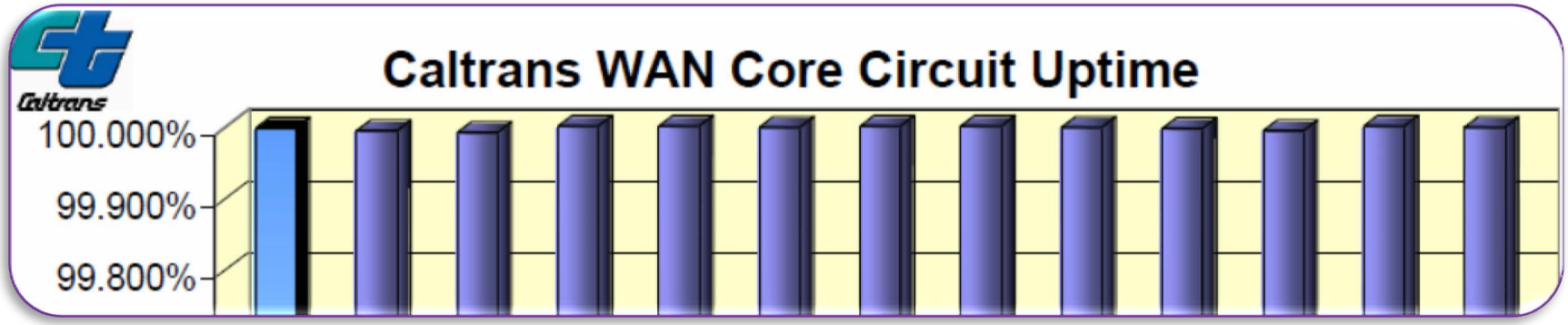


Sysadmin



Devotion To Duty - xkcd

Availability is usually expressed as a percentage of uptime in a given year. It's typically expressed as nine's. 90%=1 nine 99%=2 nines 99.9% =3 nines 99.99%=4 nines=53 minutes of downtime per year.



System Administration Work

- Median is $85.4K USD
- City of New York
  - Degree +3 yrs Sun experience
  - $90-$115K
- State of California $70K - $100K
- Private sector - $$ contract work

- thedailywtf.com/
- alt.sysadmin.recovery
- BOFH - Bastard (System) Operator From Hell
  - See Wikipedia entry

Assignment 1: Class Experience

Name:

Operating System Poll

- Windows (version)
- Apple OS-X (Lion?)
- Linux Distro (which)

Why?

Experience Levels

Laptops? Desktop?

CPU? Memory?

Expectation from class

Homework