“TRAINING COURSES NEEDED TO KEEP TECHNICAL STAFF CURRENT”

J. Crichigno
Department of Integrated Information Technology
University of South Carolina

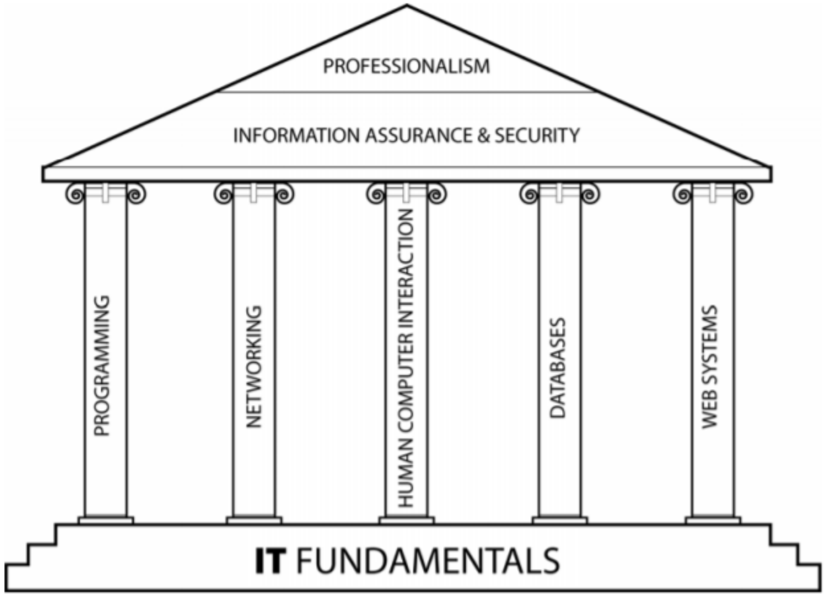
NTU Technical Workshop
Arizona State University
Tempe, AZ, July 31, August 1, 2019

Agenda

- The Information Technology (IT) Discipline
- Traditional and pillars-first IT program
- The Networking pillar
- Promoting lifelong learning
- Current training at University of South Carolina

Background

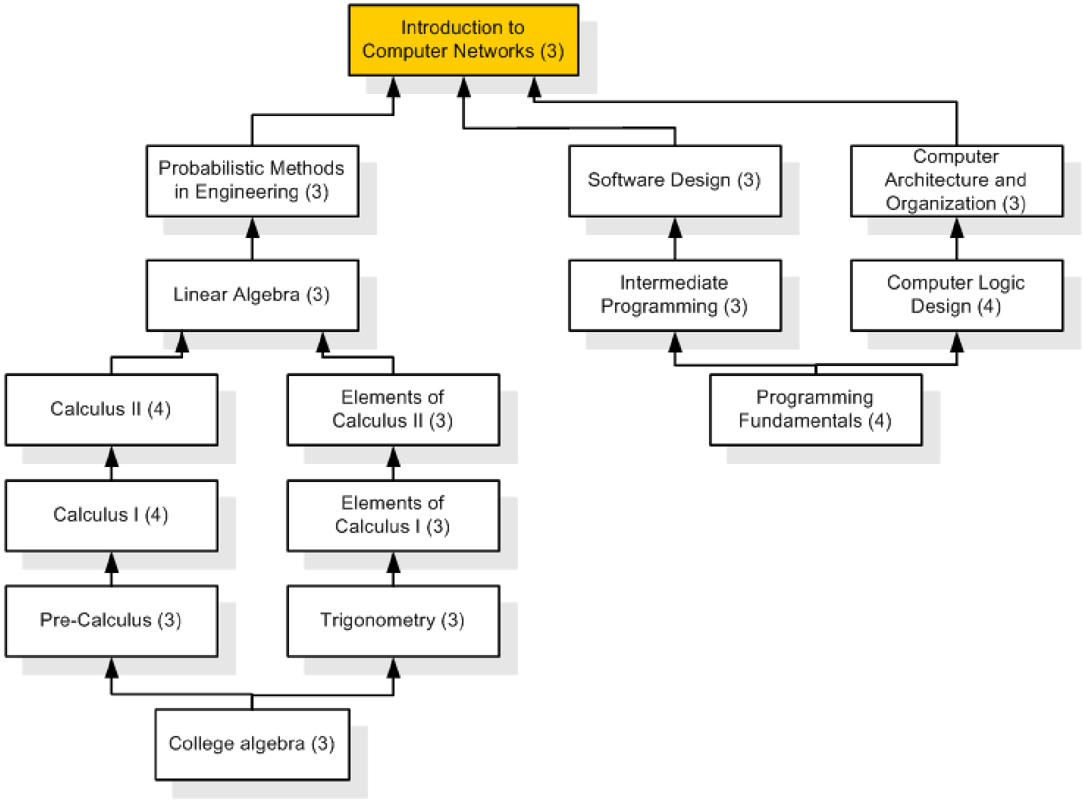
- According to the Guidelines of the ACM and IEEE Computer Society, networking is a **pillar** of **IT**[1, 2]
- Networking identified as a knowledge area with **core** units in the guidelines of programs such as Computer Engineering[3] and Computer Science[4]



[1] Curriculum Guidelines for Undergraduate Degree Programs in Information Technology, ACM and IEEE Computer Society, 2008.
[2] Information Technology Curricula 2017 (IT 2017), ACM and IEEE Computer Society, 2017.
[3] Computer Engineering Curricula 2016 (CE 2016), ACM and IEEE Computer Society, 2016.
[4] Computer Science Curricula 2013 (CS 2013), ACM and IEEE Computer Society, 2013.

IT Programs

- How should programs be built?
- Consider the pre-requisites for an introductory course in computer networks

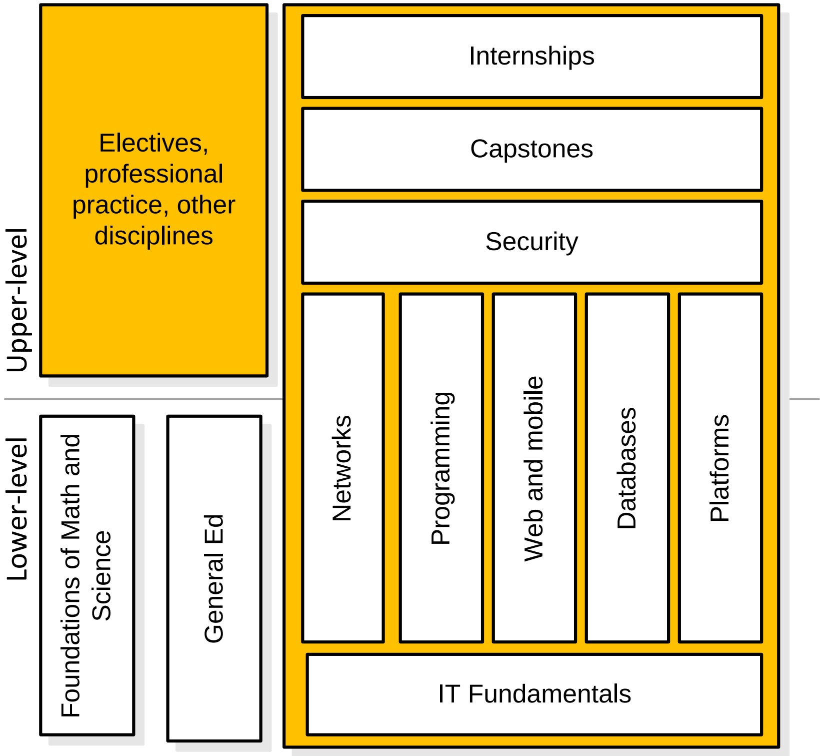

Introduction to Computer Networks (3)
Probabilistic Methods in Engineering (3)
Software Design (3)
Computer Architecture and Organization (3)
Linear Algebra (3)
Intermediate Programming (3)
Computer Logic Design (4)
Calculus II (4)
Elements of Calculus II (3)
Programming Fundamentals (4)
Calculus I (4)
Elements of Calculus I (3)
Pre-Calculus (3)
Trigonometry (3)
College algebra (3)

IT Programs

- Traditional emphasis on pre-requisite requirements
- Introduce students to the computer networks area (or other technical areas) at their senior year
- Students exposed at a relative abstract level
- Gap between industry and academia

IT Programs

- Program must prepare students for an undetermined future
- It must be flexible and remain as small as practical, allowing for freedom as needed by stakeholders
- Essential competencies; supplemental competencies for additional depth (e.g., high-performance computing)

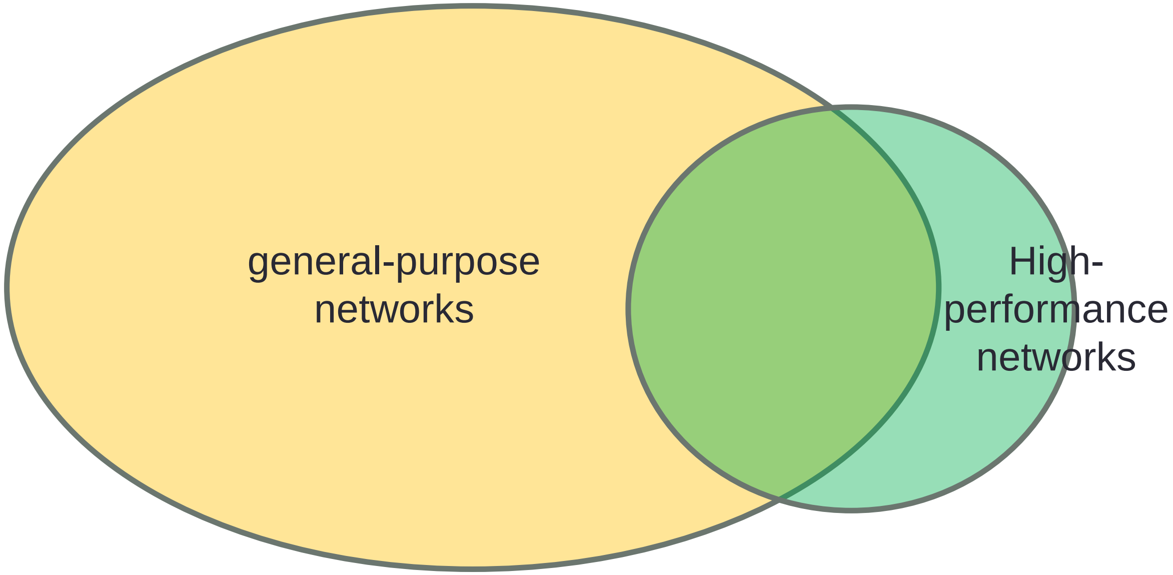


The Networking Pillar

- The IEEE / ACM guideline for IT programs considers networking a pillar of the IT discipline
  - Foundations of networking
  - Networking and interconnectivity
  - Routing, switching, and internetworking
  - Application networking services
  - Network management

The Networking Pillar

- General-purpose (essential topics) vs high-performance networks (supplementation)



The Networking Pillar

- General-purpose vs high-performance networks

	General-purpose	Science DMZ
WANs	➢ Limited bandwidth by commercial ISPs ➢ Routers/switches not optimized for performance ➢ Congestion ➢ Routing achieved independently by ISPs ➢ Typical frame size is 1,500 bytes	➢ Connection to Internet2/NRENs ➢ 10-100 Gbps paths ➢ Routers/switches optimized for performance ➢ Predictable performance ➢ End-to-end routing optimization ➢ Jumbo frames are supported
Switches / routers	➢ Rates lower than 10 Gbps ➢ Recommended buffer size equals BDP/√N ➢ Cut-through is used as forwarding method ➢ Many switches use shared memory for buffering ➢ Switching methods include shared-memory, bus fabrics	➢ Rate higher than 10 Gbps ➢ Recommended buffer size equals BDP ➢ Store-and-forward should be used for forwarding ➢ Buffer allocation should be port-based ➢ Recommended fabric is crossbar
Transport	➢ Stop-and-wait protocol behavior acceptable ➢ TCP buffer size has small impact on performance ➢ Mostly window-based congestion control used ➢ No pacing, no parallel streams	➢ pipelined behavior essential for performance TCP buffer size must be greater than BDP ➢ Rate-based congestion control has positive impact ➢ Pacing, parallel streams improve throughput

The Networking Pillar

- General-purpose vs high-performance networks

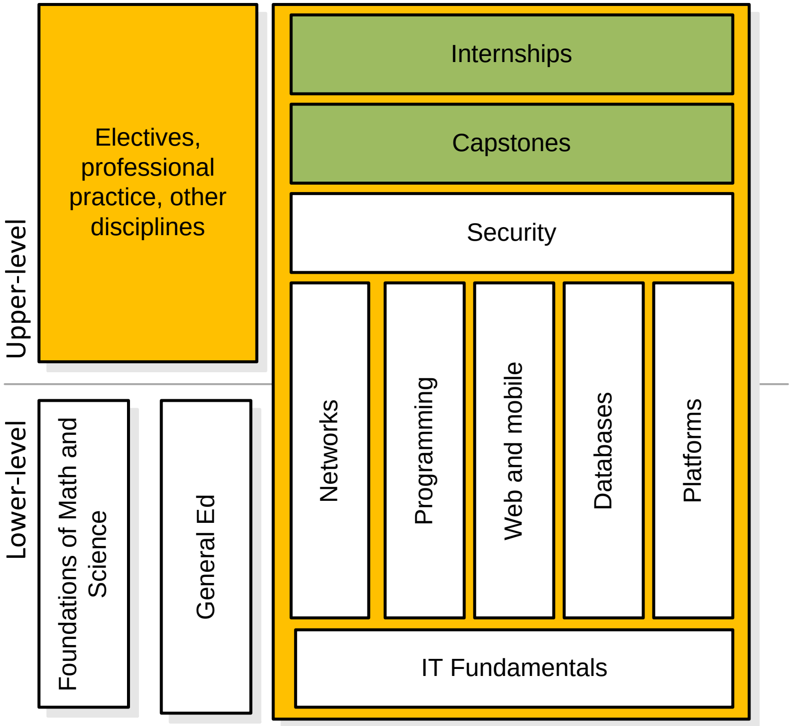
	General-purpose	Science DMZ
Applications	➢ Variety of applications ➢ General-purpose data transfer tools (SCP, FTP) ➢ Single-domain monitoring application (SNMP, Syslog)	➢ Small set of applications ➢ Specialized data-transfer tools (Globus) ➢ Multi-domain performance monitoring (perfSONAR)
Security	➢ Online devices (IPSs, firewalls) are typical ➢ IDS and ACLs used as complement to IPS and firewalls ➢ Frequent application changes and updates ➢ Multimedia, image, data processing, conde execution (HTML, XML, SQL, etc.)	➢ Online devices are not used ➢ ACL used as primary defense ➢ Flow-based IDS is attractive ➢ Changes are not frequent ➢ Limited operations over data (file operations mostly)

The Networking Pillar

- The subject of networking is complex and evolving
- Many topics covered in supplemental units (e.g., Science DMZ) evolve from general-purpose networks
- The curriculum must promote critical thinking, lifelong learning, self-directed professional development

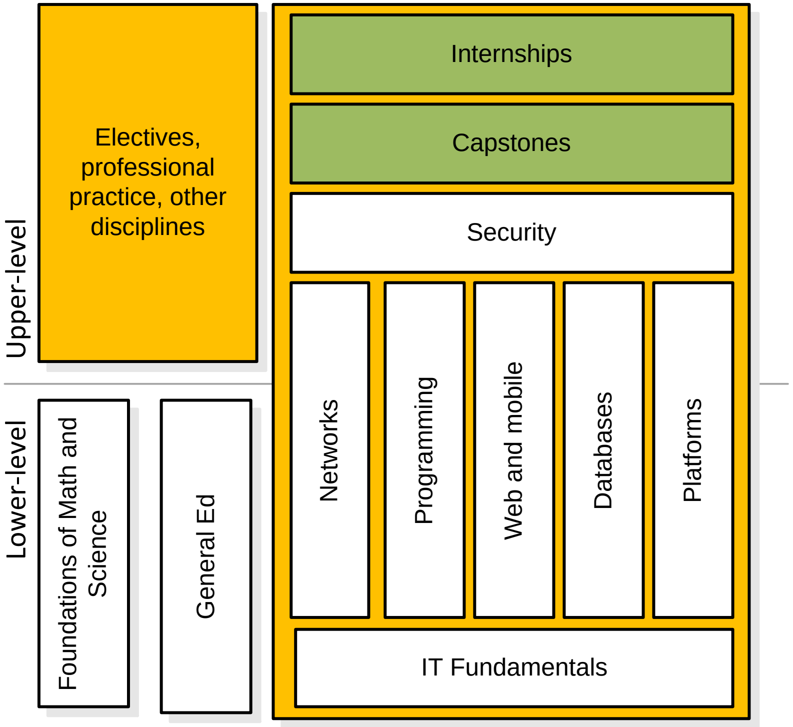
Promoting Lifelong Learning

- The subject of networking is complex and evolving
- Many topics covered in supplemental units (e.g., Science DMZ) evolve from general-purpose networks
- The curriculum must promote critical thinking, lifelong learning, self-directed professional development



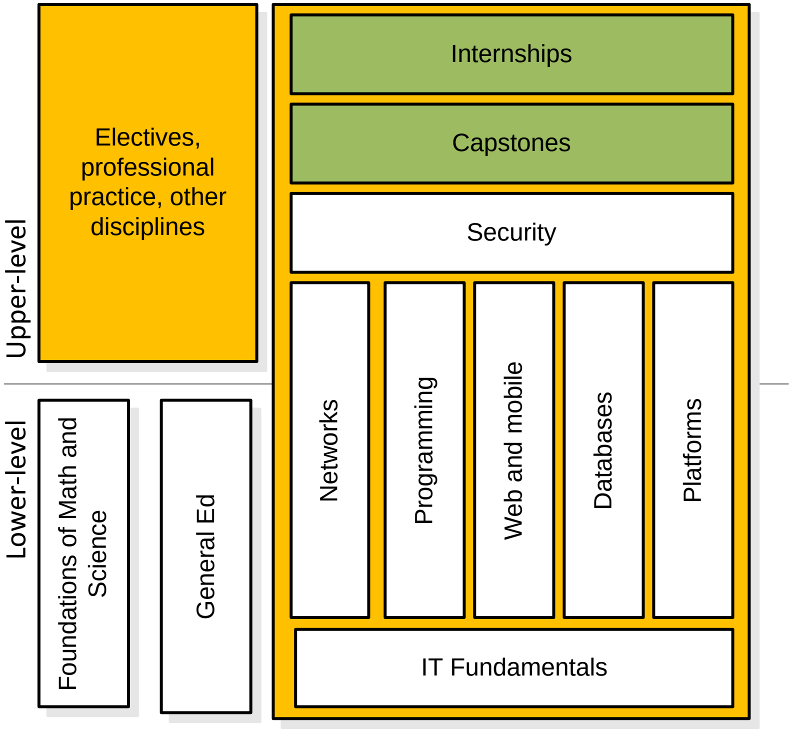
Promoting Lifelong Learning

- As students learn more about the underlying real-world IT issues, they become more interested in their studies
  - Real-world capstone projects for external clients, external judges
  - Laboratory experiences with workplace relevance
  - Internship experiences
  - Research agenda emerges from the practice

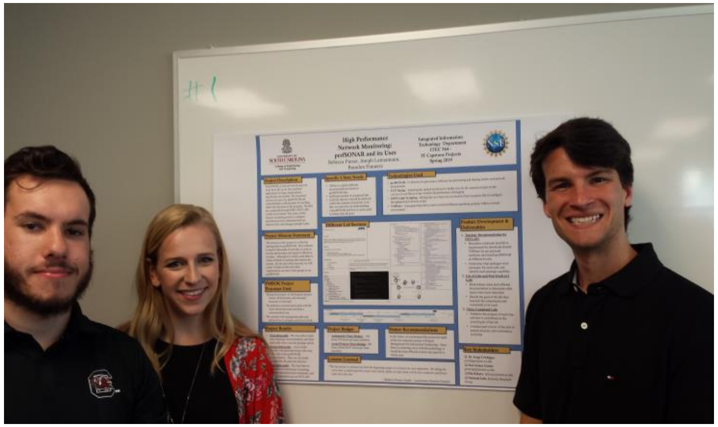


Promoting Lifelong Learning

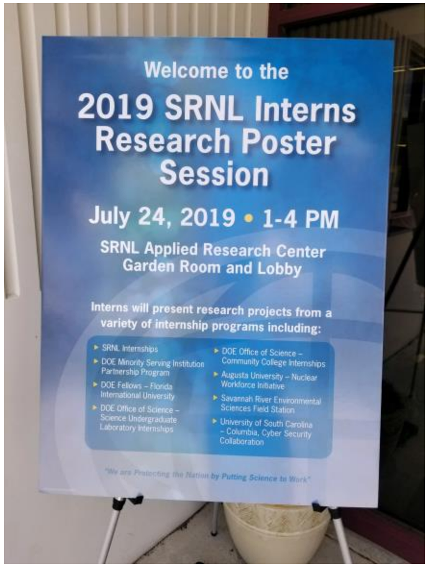
- Incorporating professional practice into the curriculum serves as a catalyst to stimulate student’s interest in the IT profession
- Experiential learning promotes leadership and help develop interpersonal skills



Capstones and Professional Presentations



Internships



Welcome to the

2019 SRNL Interns Research Poster Session

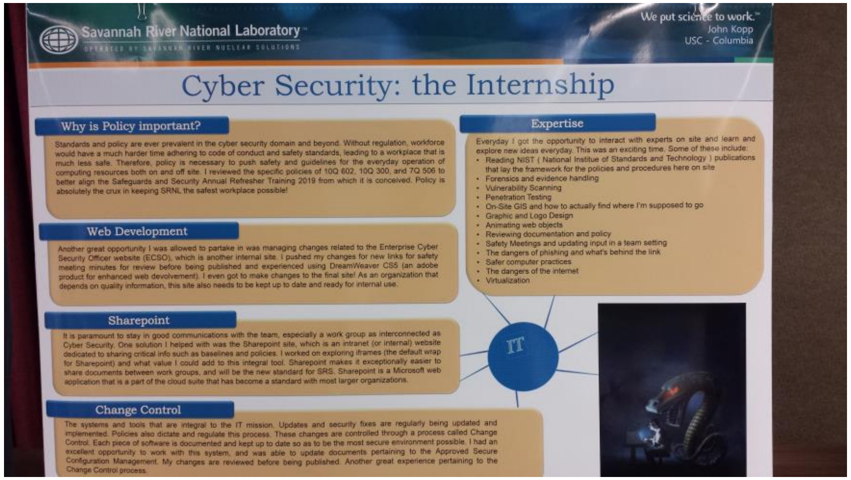
July 24, 2019 • 1-4 PM

SRNL Applied Research Center
Garden Room and Lobby

Interns will present research projects from a variety of internship programs including:

- SRNL Internships
- DOE Minority Serving Institution Partnership Program
- DOE Fellows – Florida International University
- DOE Office of Science – Science Undergraduate Laboratory Internships
- DOE Office of Science – Community College Internships
- Augusta University – Nuclear Workforce Initiative
- Savannah River Environmental Sciences Field Station
- University of South Carolina – Columbia, Cyber Security Collaboration

"We are Protecting the Nation by Putting Science to Work"



Savannah River National Laboratory
OPERATED BY SAVANNAH RIVER NUCLEAR SOLUTIONS

We put science to work.

John Kopp
USC - Columbia

Cyber Security: the Internship

Why is Policy important?

Standards and policy are ever prevalent in the cyber security domain and beyond. Without regulation, workforce would have a much harder time adhering to code of conduct and safety standards, leading to a workplace that is much less safe. Therefore, policy is necessary to push safety and guidelines for the everyday operation of computing resources both on and off site. I reviewed the specific policies of 10Q 602, 10Q 300, and 7Q 506 to better align the Safeguards and Security Annual Refresher Training 2019 from which it is conceived. Policy is absolutely the crux in keeping SRNL the safest workplace possible!

Web Development

Another great opportunity I was allowed to partake in was managing changes related to the Enterprise Cyber Security Officer website (ECSO), which is another internal site. I pushed my changes for new links for safety meeting minutes for review before being published and experienced using DreamWeaver CS5 (an adobe product for enhanced web devolvement). I even got to make changes to the final site! As an organization that depends on quality information, this site also needs to be kept up to date and ready for internal use.

Sharepoint

It is paramount to stay in good communications with the team, especially a work group as interconnected as Cyber Security. One solution I helped with was the Sharepoint site, which is an intranet (or internal) website dedicated to sharing critical info such as baselines and policies. I worked on exploring iframes (the default wrap for Sharepoint) and what value I could add to this integral tool. Sharepoint makes it exceptionally easier to share documents between work groups, and will be the new standard for SRS. Sharepoint is a Microsoft web application that is a part of the cloud suite that has become a standard with most larger organizations.

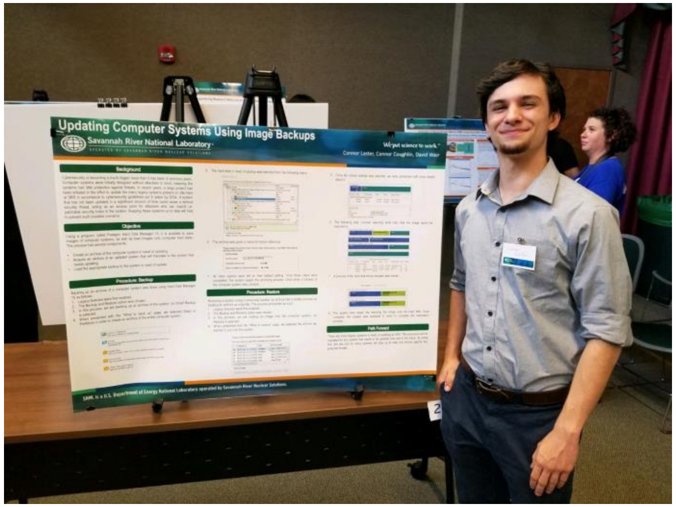
Change Control

The systems and tools that are integral to the IT mission. Updates and security fixes are regularly being updated and implemented. Policies also dictate and regulate this process. These changes are controlled through a process called Change Control. Each piece of software is documented and kept up to date so as to be the most secure environment possible. I had an excellent opportunity to work with this system, and was able to update documents pertaining to the Approved Secure Configuration Management. My changes are reviewed before being published. Another great experience pertaining to the Change Control process.

Expertise

Everyday I got the opportunity to interact with experts on site and learn and explore new ideas everyday. This was an exciting time. Some of these include:

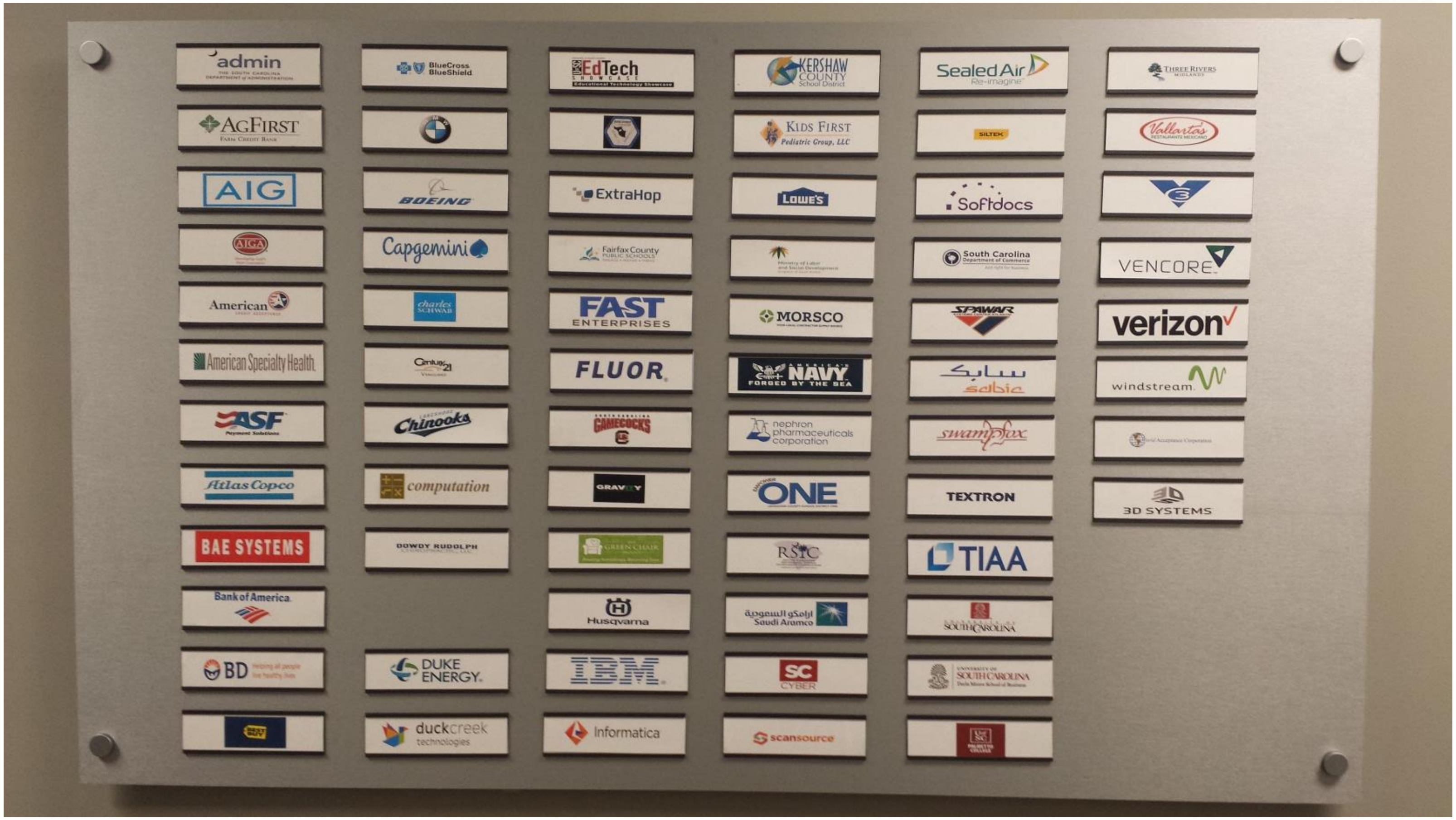
- Reading NIST (National Institue of Standards and Technology) publications that lay the framework for the policies and procedures here on site
- Forensics and evidence handling
- Vulnerability Scanning
- Penetration Testing
- On-Site GIS and how to actually find where I'm supposed to go
- Graphic and Logo Design
- Animating web objects
- Reviewing documentation and policy
- Safety Meetings and updating input in a team setting
- The dangers of phishing and what's behind the link
- Safer computer practices
- The dangers of the internet
- Virtualization



Updating Computer Systems Using Image Backups
Savannah River National Laboratory
We put science to work.

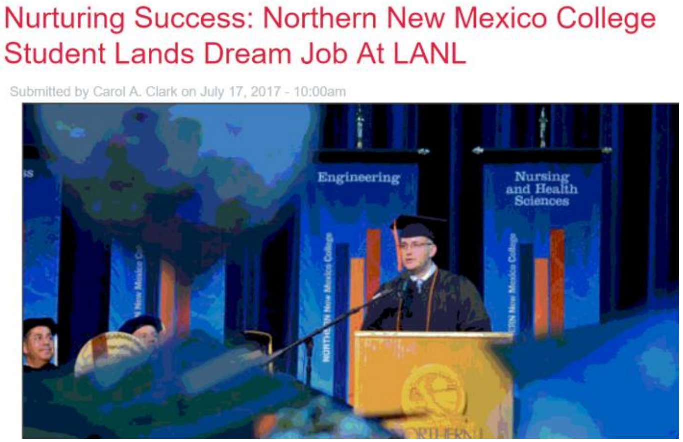
Current Training at USC

- Employers, alumni, partners



Internship providers

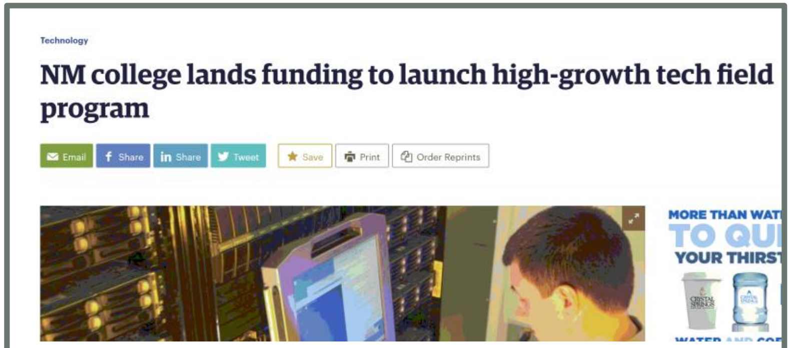
Internships Northern New Mexico College



Nurturing Success: Northern New Mexico College Student Lands Dream Job At LANL

Submitted by Carol A. Clark on July 17, 2017 - 10:00am

Los Alamos Daily, July 17, 2017



Technology

NM college lands funding to launch high-growth tech field program

Albuquerque Business First, Aug. 24, 2017

LANL – NNMC: Internship program, Biology and Information Engineering Technology, Spring 2018

Science DMZ team, from left to right Chase: Comp. Sys. Professional 2, LANL; Joseph: Scientist 1 at LANL, GA Tech Master program; Sergio: graduate in Fall 2017, intern at LANL, Analysis, Intelligence, and Technology, GA Tech Master program

Co-PI Biology team, NM IMBRE ‘16 Conf.

1st place award, Bioinformatics; 2016 NM IMBRE conference

Top: Maria, Colo. State Research Symp. ’16, 2nd place award
Bottom: Britney, NM Biomedical Symp. ‘16

Current Training at USC

- Initially targeted for students, IIT’s material helps to train IT staff and self-pace learners from other departments
- Provide foundations, including state-of-the art technology
  - E.g., when covering the network layer, include Software-defined Networking (SDN)
  - P4 programmable data plane switches (master, PhD level)
- Facilitate the use of hands-on tools
  - Agreements with Cisco, Palo Alto, Juniper, VMware, Amazon, Barefoot Networks
  - Theoretical concepts reinforced with material developed by vendors
  - Develop material for training not provided by vendors (traffic analysis tools, Bro, high-speed networks, programmable data plane switches)

Current Training at USC

- Train students to be a problem solver, skilled practitioner
- Promote applied research using professional tools and platforms
  - Ease the transition from academia to the workplace
  - Some vendors offer excellent tools that complement theory, at no cost
  - Vendor-specific certifications are practice-oriented, highly technical in nature; used as a complement for core concepts
  - Many open source applications are highly recognized

2017 NSF CC* Meeting

Comments by attendees of 2017 NSF CC meeting[1]
“Working with researchers… HPC, Science DMZ, DTN, Big Data and/or GPU platforms”
“Very difficult to find, or nonexistent - difficult to retain (CI engineers)”
“time to hire (CI engineers)... ended up taking 10 months”
“Combination of education and experience”
“At least one tour of duty as an intern or apprentice”
“System and network engineering, user support experience, good communication…”
“Routing and switching (e.g., Juniper, Cisco), …training in security (e.g., Palo Alto or similar), cabling”
“Working knowledge of theory and practice underlying VLAN/LAN/WAN… Windows and Unix/Linux”
“We get great mileage out of community college student interns for tasks at the system / network admin”

[1] http://www.thequilt.net/wp-content/uploads/NSF-2017-PI-Workshop-CI-Engineer-Survey_v4.pdf

Current Training at USC

Introduction to Networks

Routing and Switching

High-speed Networks

perfSONAR

SOC cyber-operations

Next-generation Firewalls

Traffic Analysis with Bro

Introduction to Cryptography

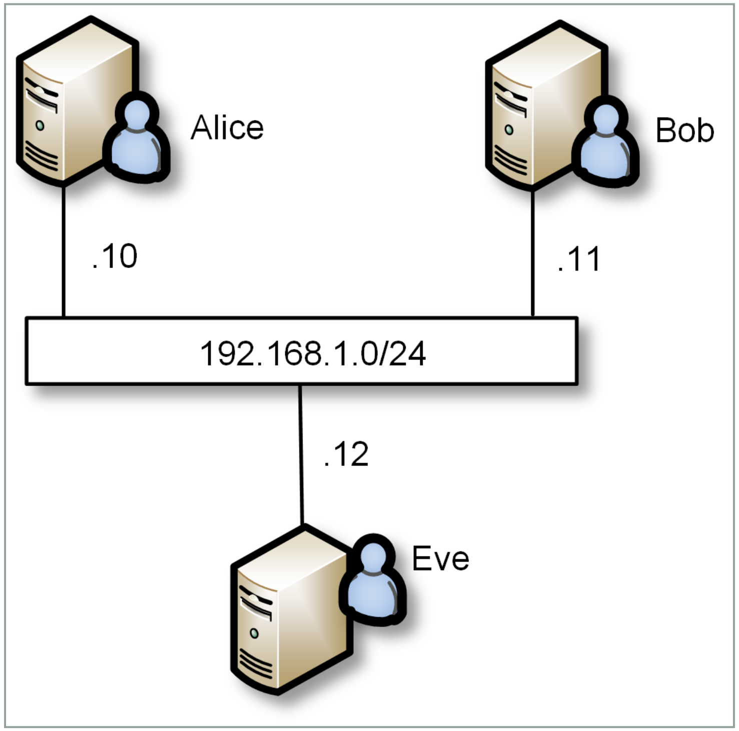
Linux Essentials

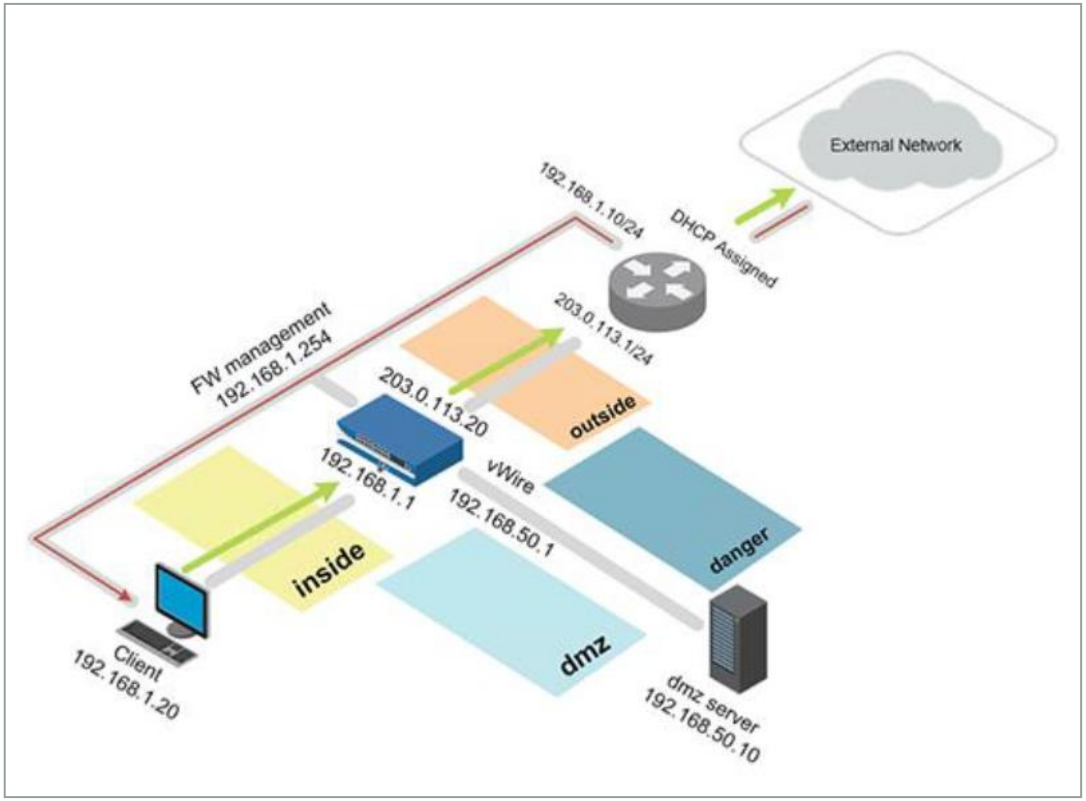
Introduction to Virtualization

Virtualized Datacenter

…

Hands-on Training

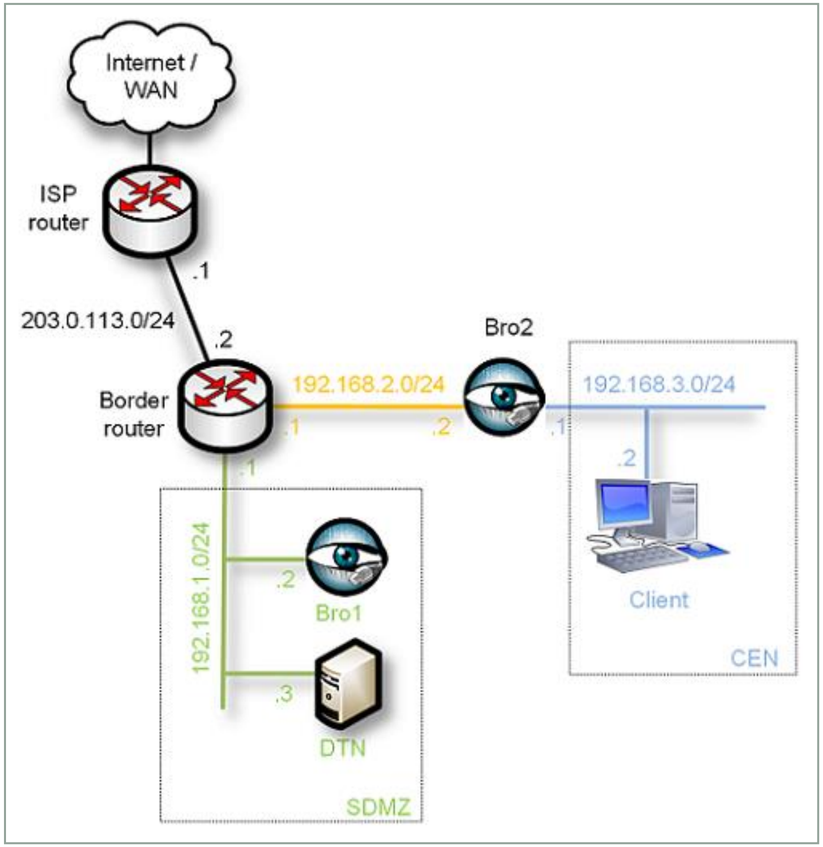




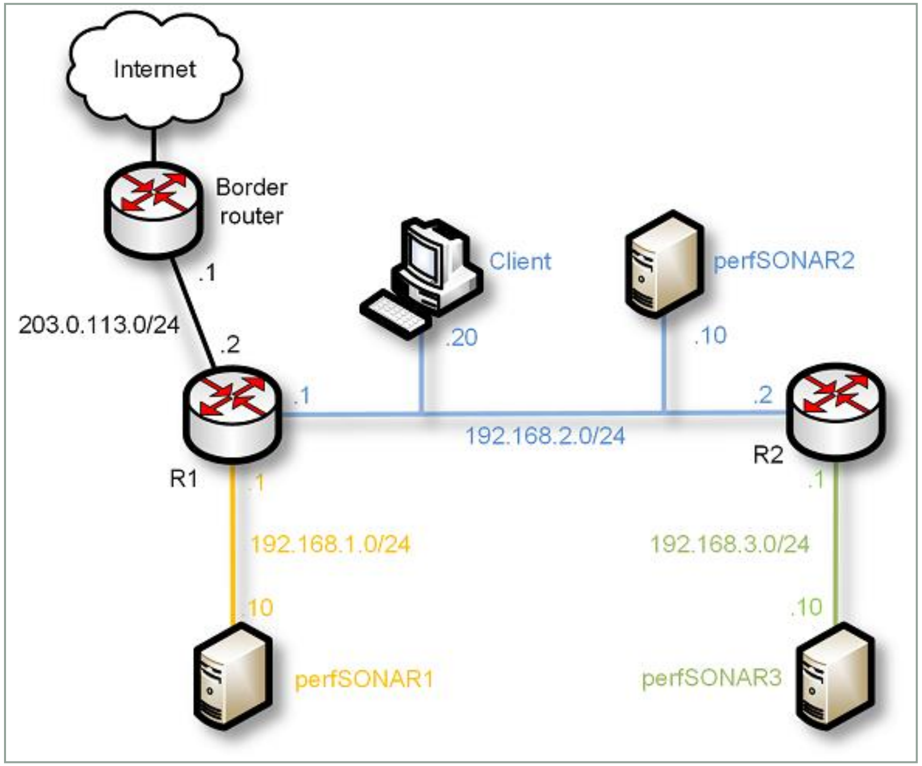
Introduction to Cryptography

PAN / Next-generation Firewalls

Hands-on Training

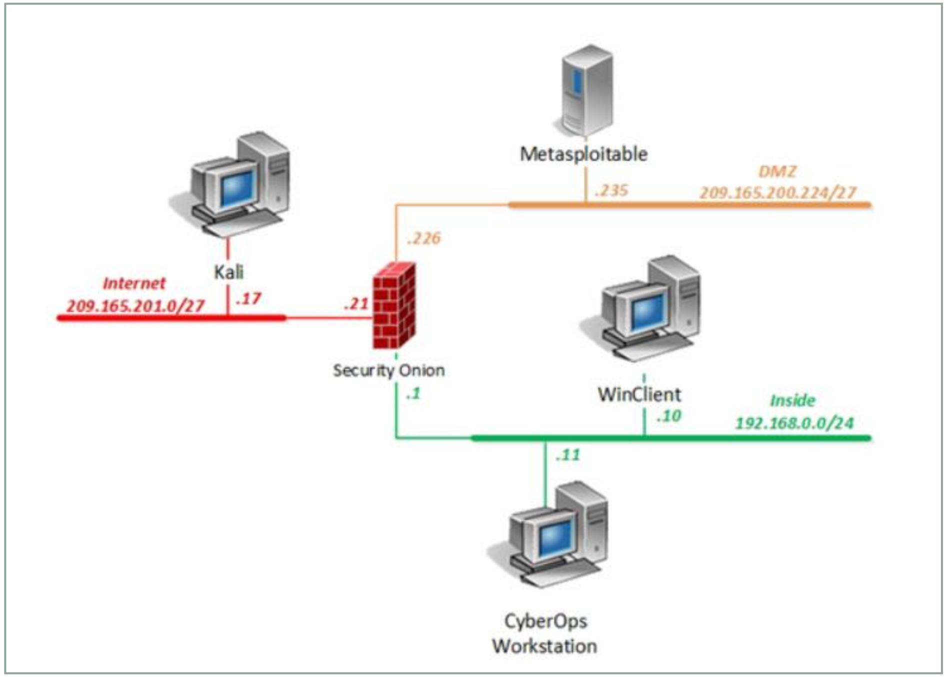


Introduction to Zeek / Bro

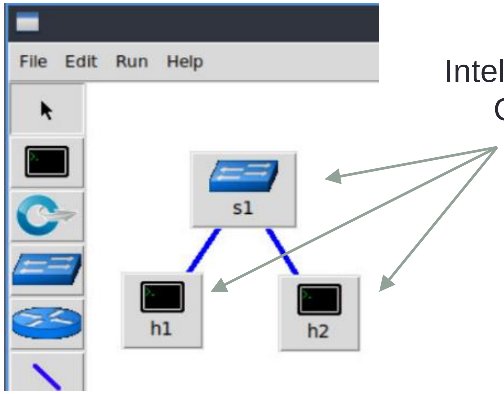


perfSONAR

Hands-on Training



Cyber-operations



Intel Xeon Gold 6130 CPU, 2.1 GHz

Network Tools and Protocols
(High-speed Networks)

Labs Series: Networks Tools and Protocols

- Lab 1: Introduction to Mininet
- Lab 2: Introduction to iPerf
- Lab 3: Emulating WAN with NETEM I Latency, Jitter
- Lab 4: Emulating WAN with NETEM II Packet Loss, Duplication, Reordering, and Corruption
- Lab 5: Setting WAN Bandwidth with Token Bucket Filter (TBF)
- Lab 6: Understanding Traditional TCP Congestion Control (HTCP, Cubic, Reno)
- Lab 7: Understanding Rate-based TCP Congestion Control (BBR)
- Lab 8: Bandwidth-delay Product and TCP Buffer Size
- Lab 9: Enhancing TCP Throughput with Parallel Streams
- Lab 10: Measuring TCP Fairness
- Lab 11: Router's Buffer Size
- Lab 12: TCP Rate Control with Pacing
- Lab 13: Impact of Maximum Segment Size on Throughput
- Lab 14: Router's Bufferbloat

Lab Series: perfSONAR

- Lab 1: Configuring Admin. Information Using perfSONAR Toolkit GUI
- Lab 2: PerfSONAR Metrics and Tools
- Lab 3: Configuring Regular Tests Using perfSONAR GUI
- Lab 4: Configuring Regular Tests Using pScheduler CLI Part I
- Lab 5: Configuring Regular Tests Using pScheduler CLI Part II
- Lab 6: Bandwidth-delay Product and TCP Buffer Size
- Lab 7: Configuring Regular Tests Using a pSConfig Template
- Lab 8: perfSONAR Monitoring and Debugging Dashboard
- Lab 9: pSConfig Web Administrator
- Lab 10: Configuring pScheduler Limits

Labs Series: Introduction to Zeek

- Lab 1: Introduction to the Capabilities of Zeek
- Lab 2: An Overview of Zeek Logs
- Lab 3: Parsing, Reading and Organizing Zeek Files
- Lab 4: Generating, Capturing and Analyzing Network Scanner Traffic
- Lab 5: Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic
- Lab 6: Introduction to Zeek Scripting
- Lab 7: Advanced Zeek Scripting for Anomaly and Malicious Event Detection
- Lab 8: Preprocessing of Zeek Output Logs for Machine Learning
- Lab 9: Developing Machine Learning Classifiers for Anomaly Inference and Classification
- Lab 10: Profiling and Performance Metrics of Zeek

Labs Series: NGFW - PAN

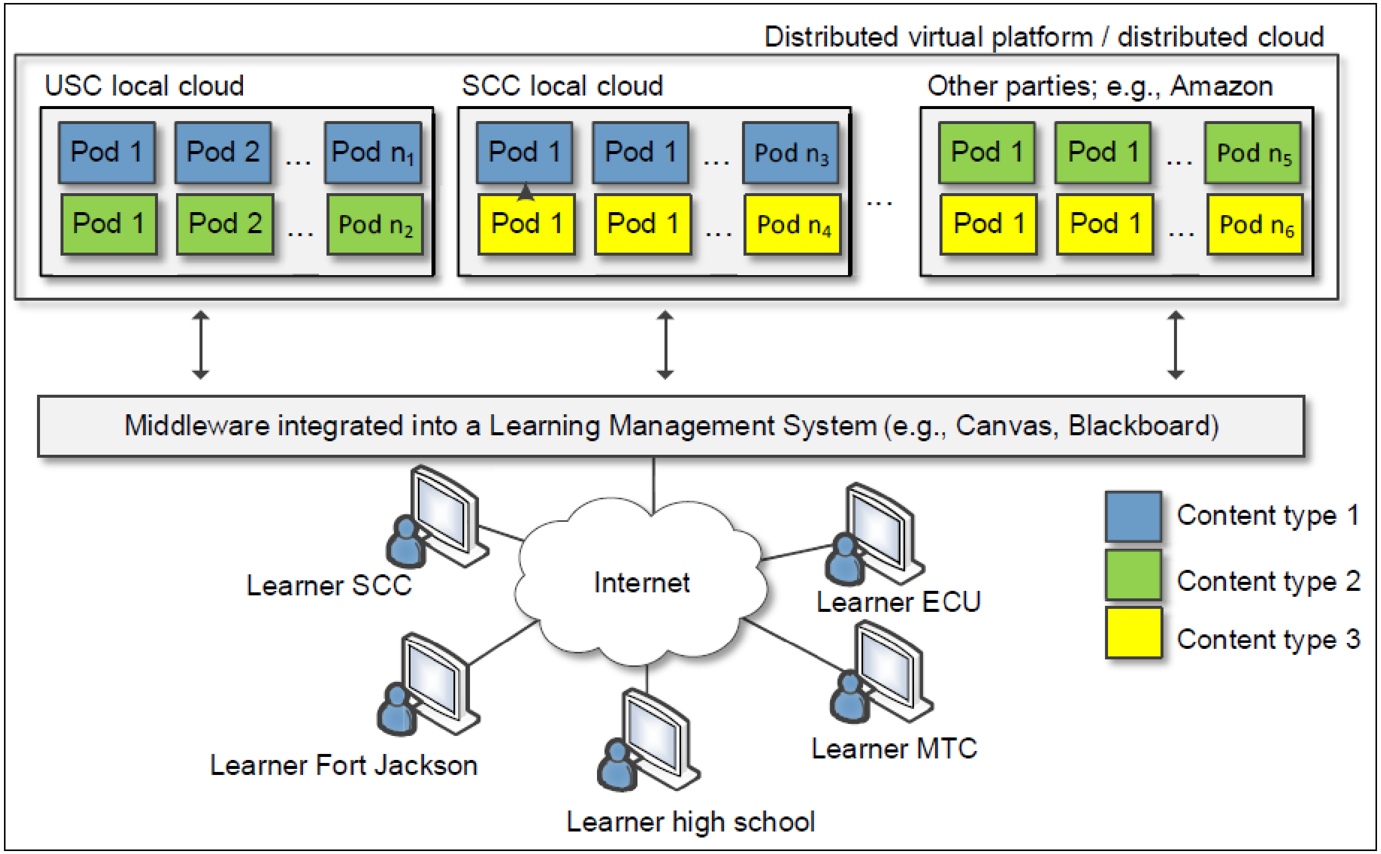
- Lab 1: Initial configuration
- Lab 2: Interface configuration
- Lab 3: Security and NAT policies
- Lab 4: Protecting networks using Application ID
- Lab 5: Protecting networks using Content ID
- Lab 6: URL filtering
- Lab 7: Decryption
- Lab 8: Sandbox malware execution
- Lab 9: User identification
- Lab 10: Global protection
- Lab 11: Site-to-site VPN
- Lab 12: Monitoring and reporting
- Lab 13: Active/Passive High-availability

Labs Series: SOC Cyber-operations

- Lab 1: Identify Running Processes
- Lab 2: Exploring Processes, Threads, Handles, and Windows Registry
- Lab 3: Windows Tools
- Lab 4: Linux Shell
- Lab 5: Linux Servers
- Lab 6: Log Files
- Lab 7: Navigating the Linux File System and Permission Settings
- Lab 8: Tracing a Route
- Lab 9: Wireshark: Ethernet frames, TCP 3-way handshake
- Lab 10: Exploring NMAP
- Lab 11: UDP DNS Captures
- Lab 12: HTTP and HTTPS (Sguil Network Security Analysis)
- Lab 13: Attacking a mySQL Server
- Lab 14: Snort and Firewall Rules
- Lab 15: Regular Expressions
- Lab 16: Isolate Compromise Host using Flow’s 5-tuple

Building a Cloud / Portal for Training

- Distributed cloud integrated into a Learning Management System
  - Learn: learner selects a self-pace training module
  - Teach: instructor selects a module to incorporate into course



Distributed virtual platform / distributed cloud

USC local cloud

Pod 1 Pod 2 … Pod n_1

Pod 1 Pod 2 … Pod n_2

SCC local cloud

Pod 1 Pod 1 … Pod n_3

Pod 1 Pod 1 … Pod n_4

…

Other parties; e.g., Amazon

Pod 1 Pod 1 … Pod n_5

Pod 1 Pod 1 … Pod n_6

Middleware integrated into a Learning Management System (e.g., Canvas, Blackboard)

Internet

Learner SCC

Learner Fort Jackson

Learner high school

Learner ECU

Learner MTC

🟦 Content type 1

🟩 Content type 2

🟨 Content type 3