Virtual Labs for Training, Teaching, and Research on Networks and Cybersecurity Topics

Jorge Crichigno, Elie Kfoury
University of South Carolina
http://ce.sc.edu/cyberinfra
jcrichigno@cec.sc.edu, ekfoury@email.sc.edu

CI Engineering Lunch and Learn - Online
February 19, 2021

Agenda

- Motivation virtual labs
- Local cloud at UofSC
- Design of virtual labs – POD design
- Virtual lab libraries
- Industry partnership
- Distributed Academic Cloud
- Other topics – research

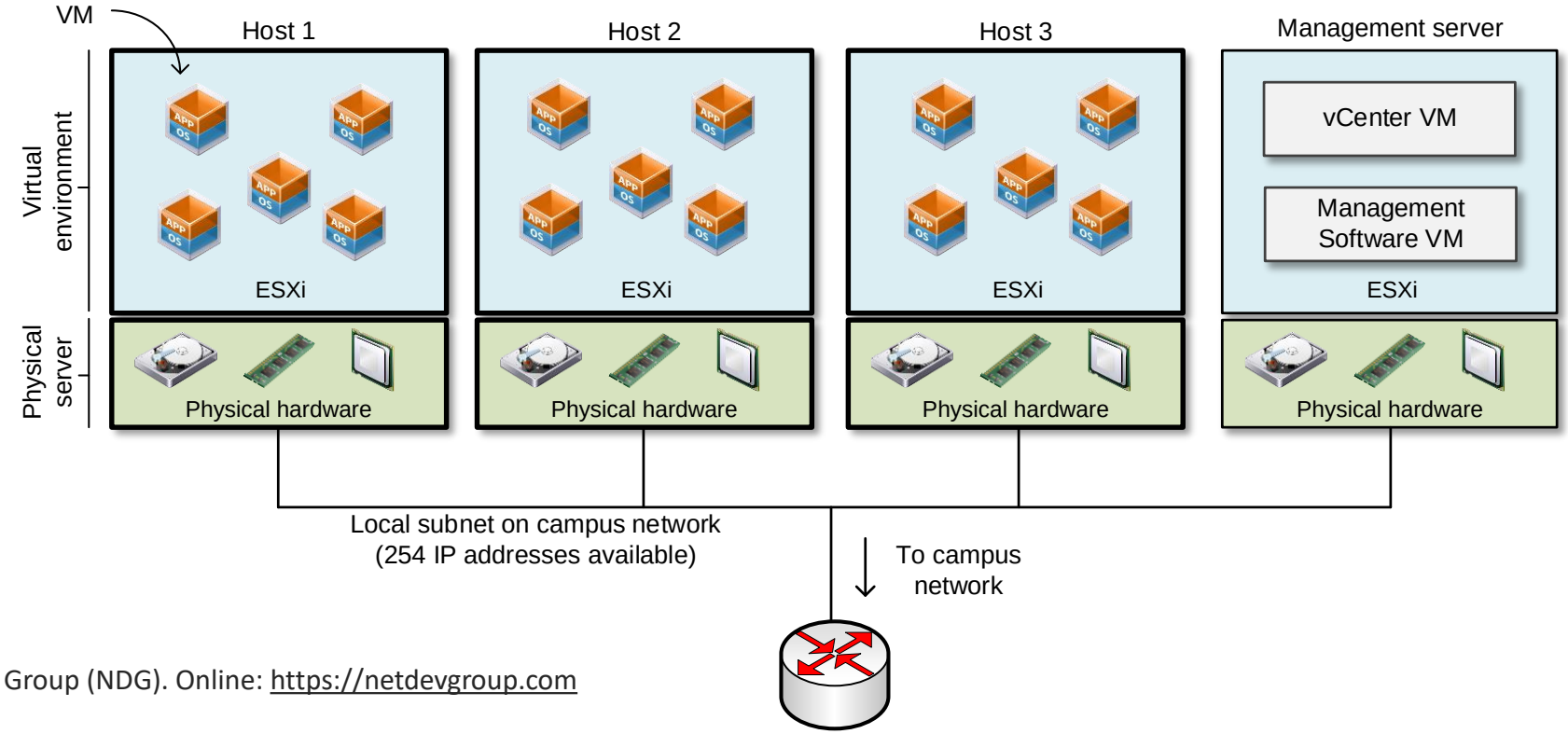
Motivation for Virtual Labs

- Information Technology (IT) programs are more practical than theoretical
- The IT discipline distinguishes from other computing disciplines by being more applied than theoretical and by addressing infrastructure systems and application technologies[1]
- The Department of Integrated Information Technology at UofSC has over 250 undergraduate students and over 50 Master students
- How to include authentic practice, professional tools and platforms, access to computing technology in the work environment in a scalable way?
  - Limited labor, equipment, and space
  - Easy to setup the experimental environment

1. Information Technology Curricula 2017, ACM/IEEE Joint Committee. Online: https://tinyurl.com/4nqqwa5m.

Local Cloud at UofSC

- UofSC cloud; https://netlab.cec.sc.edu
- Hosts 1-3 store virtual machines (VMs) for virtual labs
- Management server runs vCenter, Management Software (NETLAB+)
- Partnership with Network Development Group (NDG)[1]



1. Network Development Group (NDG). Online: https://netdevgroup.com

Local Cloud at UofSC

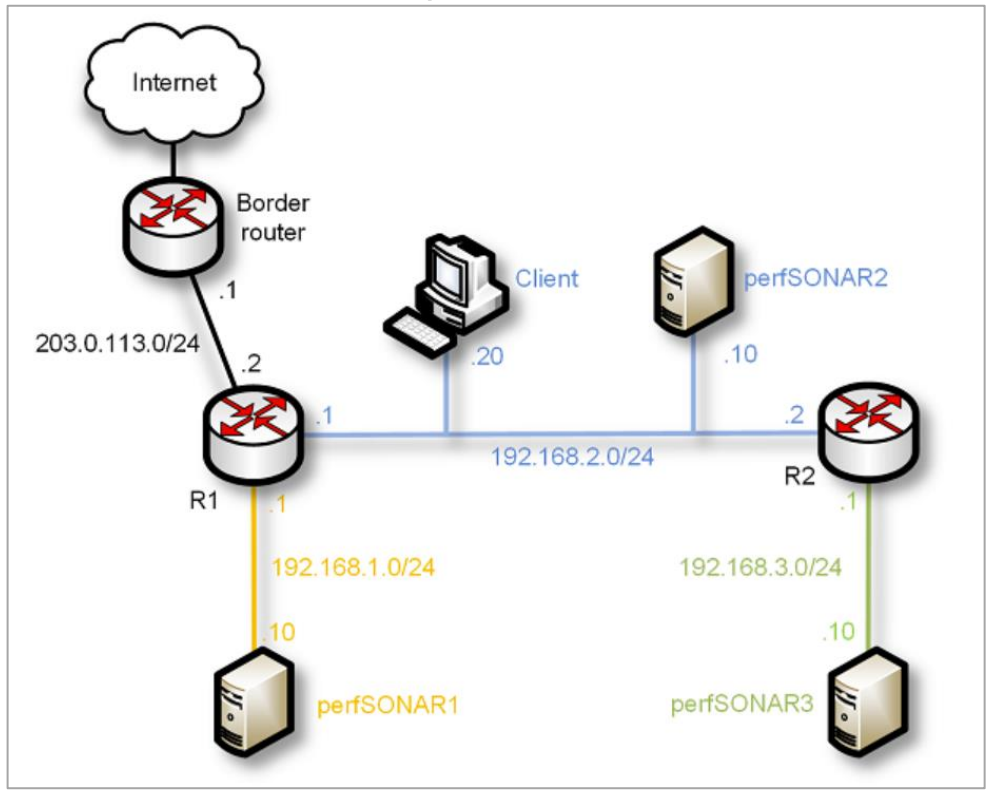
- Servers' specifications

Device	Cores	Storage (TB)	RAM (GB)
Server 1 (management server)	20	4.8	128
Server 2 (VMs for vLabs)	32	4.8	512
Server 3 (VMs for vLabs)	32	1.92	768
Server 4 (VMs for vLabs)	32	1.92	768
Total	**116**	**8.08**	**2,176**

POD Design

- A virtual laboratory experiment requires a **pod** of devices, or simply pod
- Example: perfSONAR library

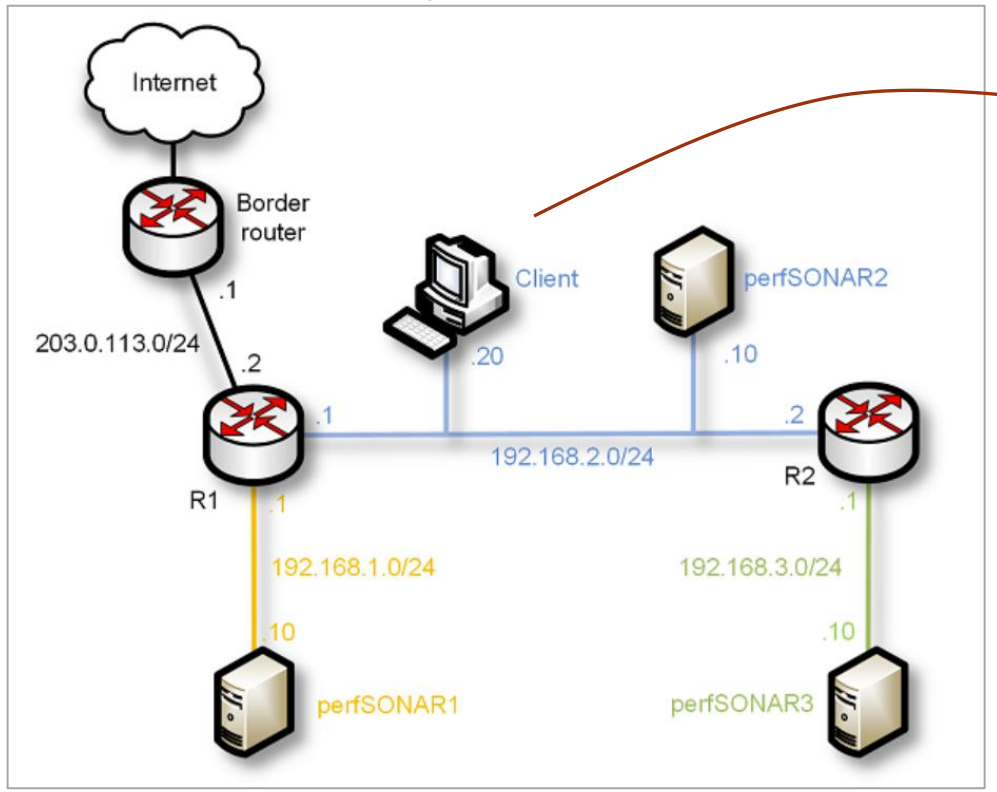
POD for perfSONAR labs

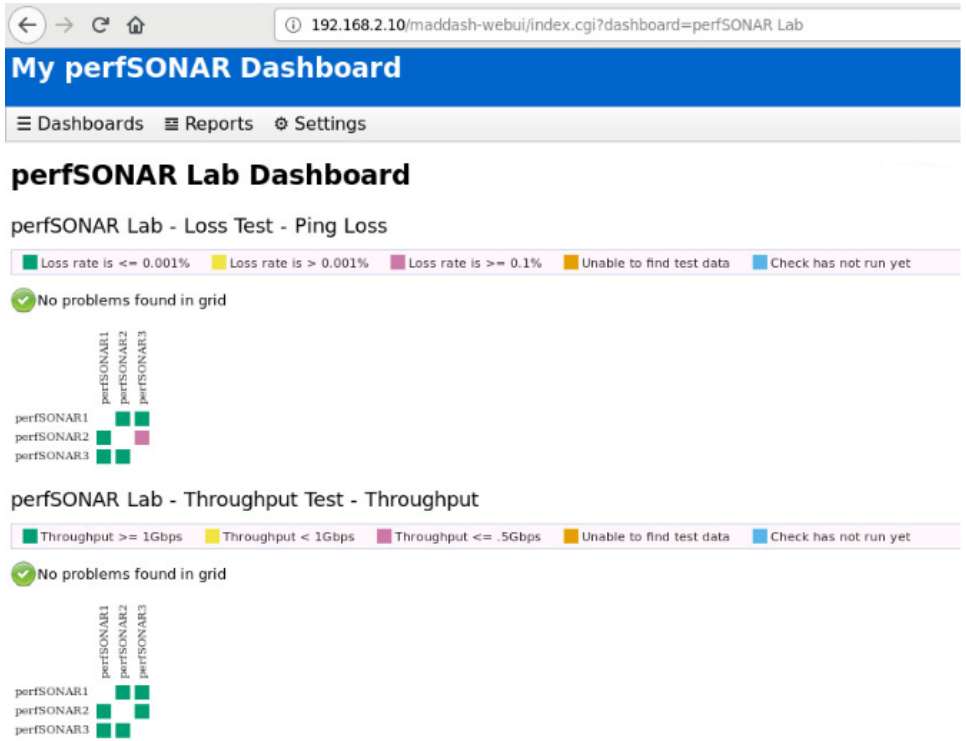


POD Design

- A virtual laboratory experiment requires a **pod** of devices, or simply pod
- Example: perfSONAR library

POD for perfSONAR labs

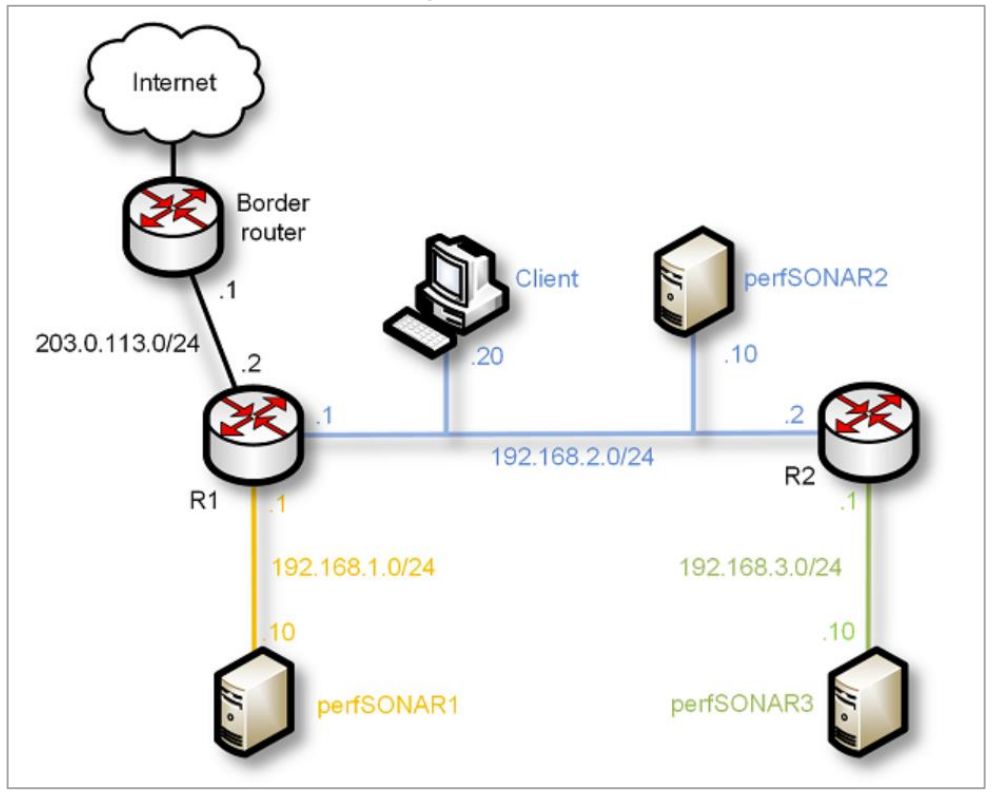




POD Design

- A virtual laboratory experiment requires a **pod** of devices, or simply pod
- Example: perfSONAR library

POD for perfSONAR labs

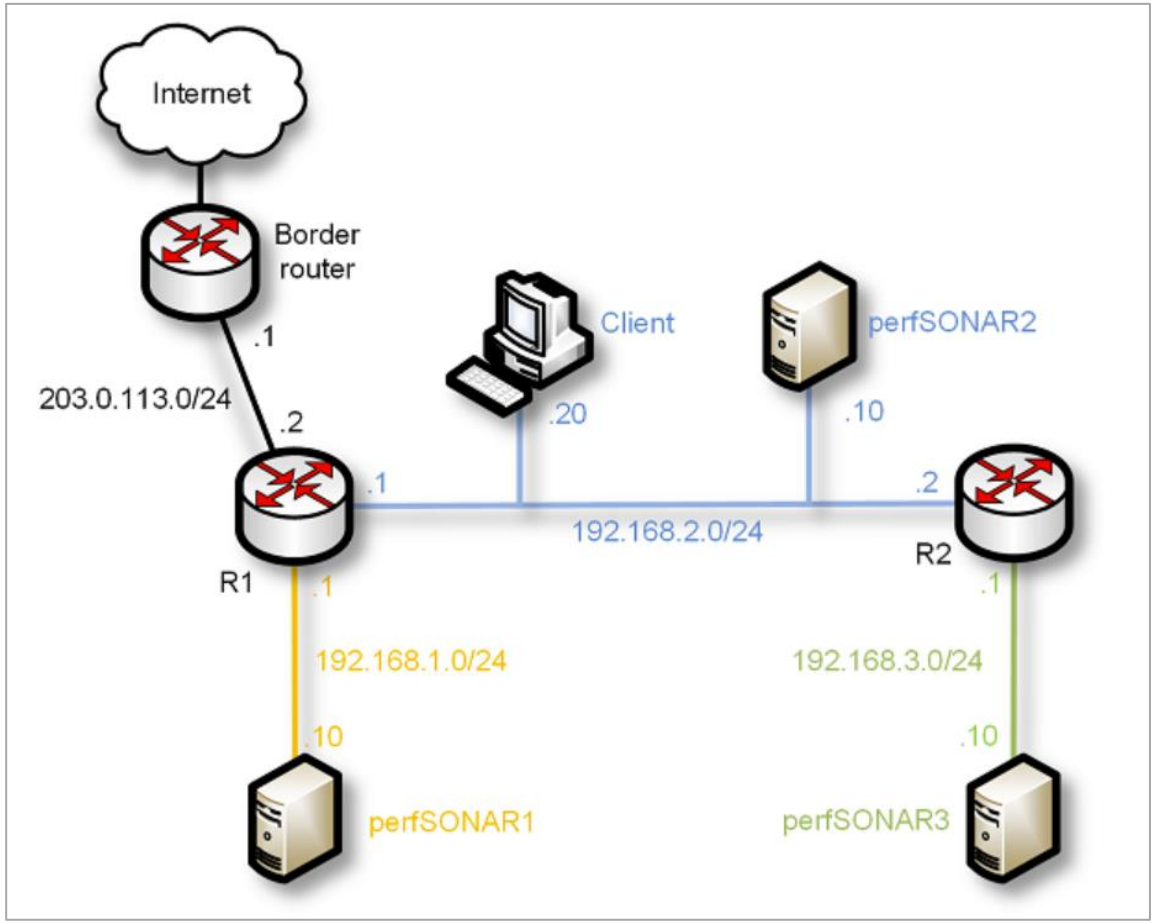


perfSONAR labs

Lab 1	Configuring Administrative 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

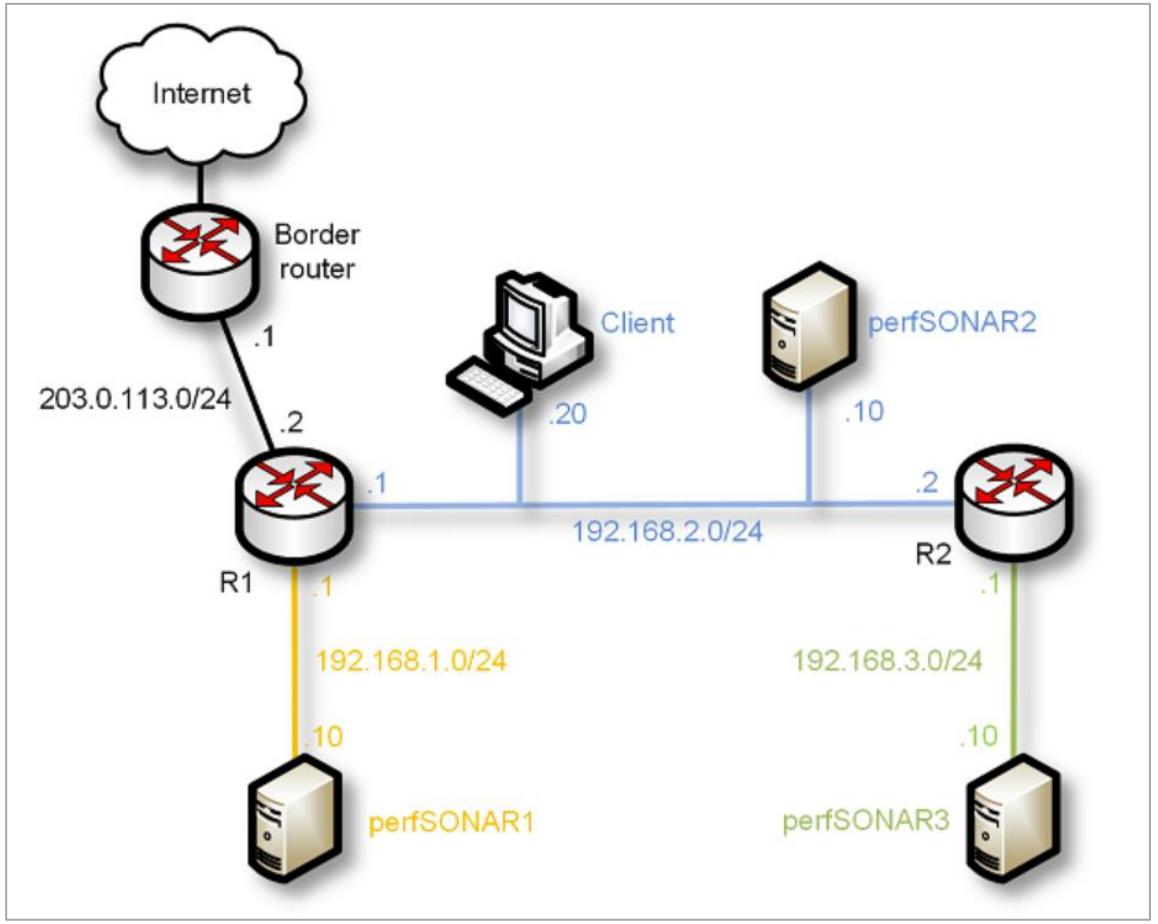
POD Design

- Details of perfSONAR pod
  - Four networks
  - Three servers
  - One client
  - Three routers
  - Connectivity to the Internet
  - Total of 7 heterogeneous VMs



POD Design

- Details of perfSONAR pod
  - PODs running simultaneously use the same block of IP addresses
  - Lab manuals are uniform
  - “Local NAT” is performed by the device connected to the campus network
  - There is a master pod in the system
  - Linked clone VMs are created from the master pod VMs



Lab Libraries

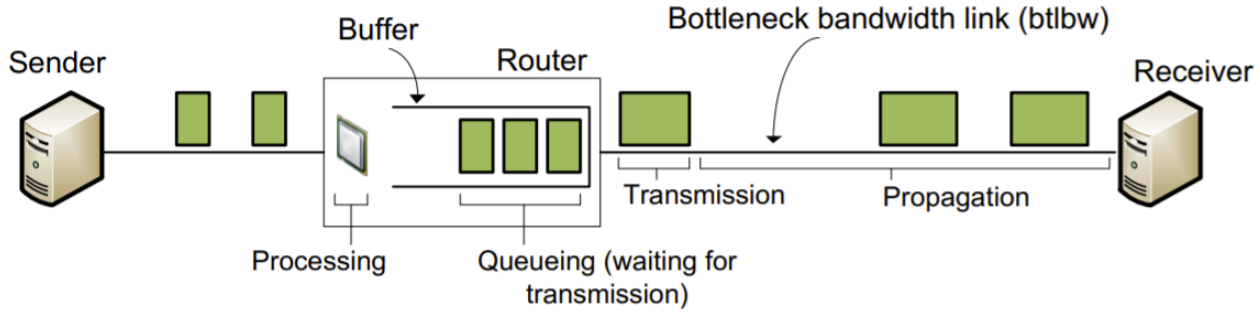
- Network Tools and Protocols

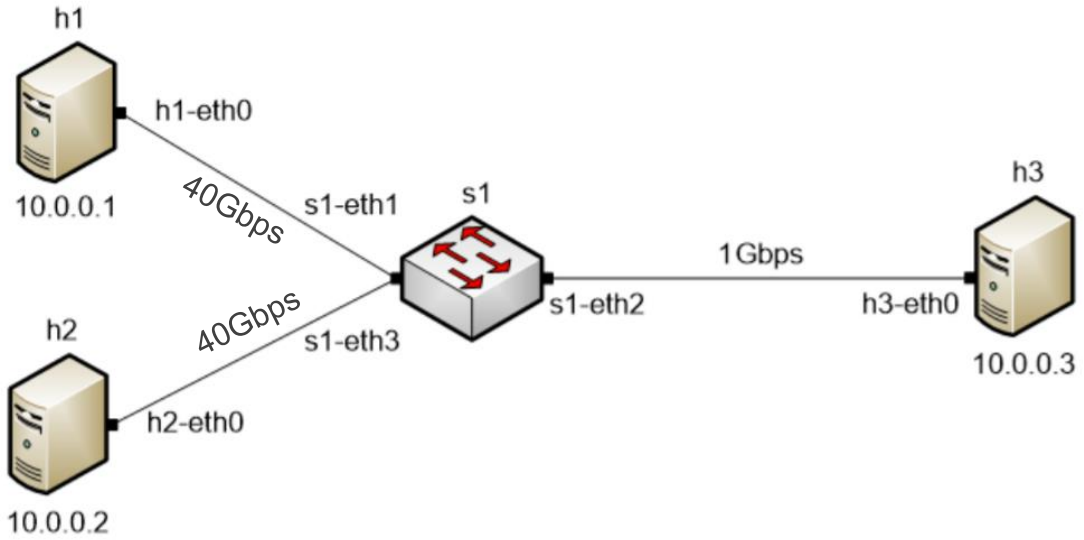
Lab 1	Introduction to Mininet
Lab 2	Introduction to Iperf3
Lab 3	Emulating WAN with NETEM I: Latency, Jitter
Lab 4	Emulating WAN with NETEM II: Packet Loss, Duplication, Reordering, and Corruption
Lab 5	Setting WAN Bandwidth with Token Bucket Filter (TBF)
Lab 6	Understanding Traditional TCP Congestion 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 MSS on Throughput
Lab 14	Router's Bufferbloat
Lab 15	Analyzing the Impact of Hardware Offloading on TCP Performance
Lab 16	Random Early Detection
Lab 17	Stochastic Fair Queueing
Lab 18	Controlled Delay (CoDel) Active Queue Management
Lab 19	Proportional Integral Controller-Enhanced (PIE)
Lab 20	Classifying TCP traffic using Hierarchical Token Bucket (HTB)

Lab Libraries

- Network Tools and Protocols, Lab 14: “Router’s Bufferbloat”

Description of the problem





Topology

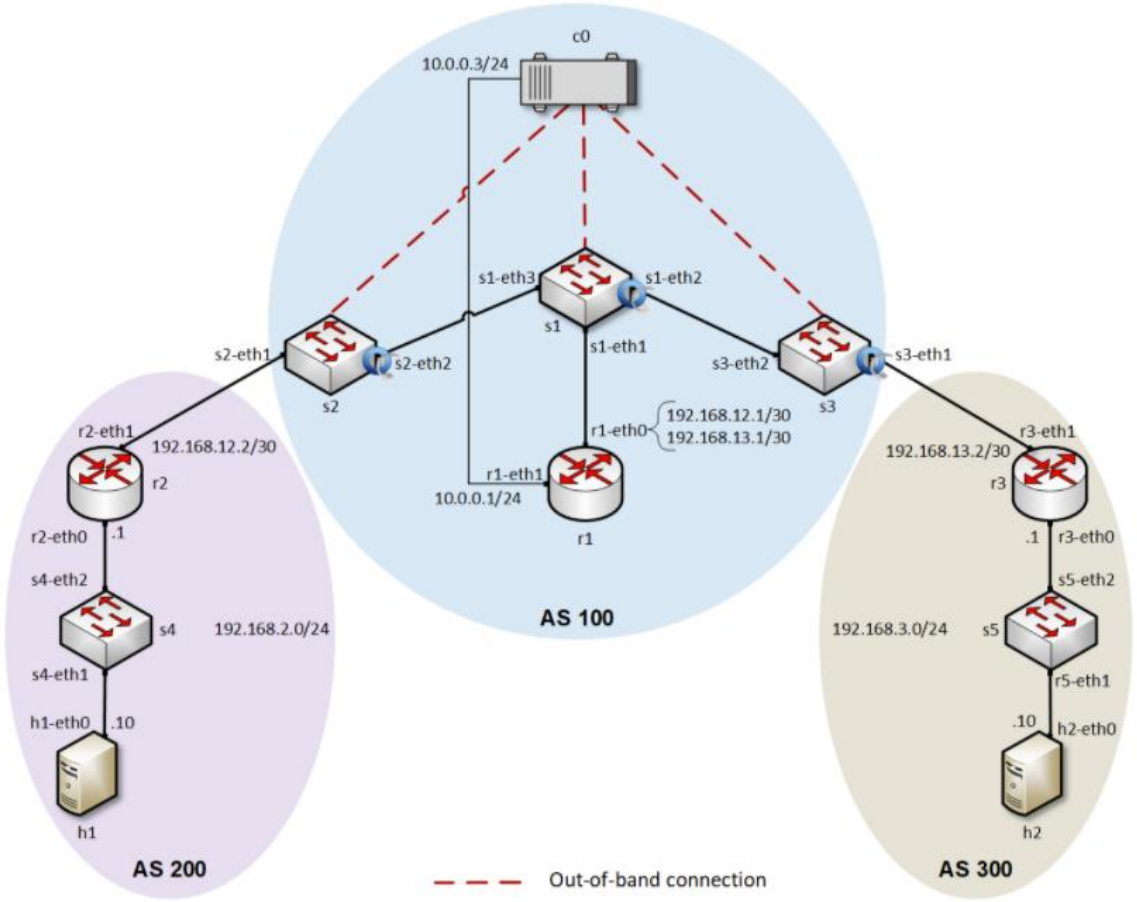
Lab Libraries

- Introduction to SDN

Lab 1	Introduction to Mininet
Lab 2	Legacy Networks: BGP Example as a Distributed System and Autonomous Forwarding Decisions
Lab 3	Early efforts of SDN: MPLS Example of a Control Plane that Establishes Semi-static Forwarding Paths
Lab 4	Introduction to SDN
Lab 5	Configuring VXLAN to Provide Network Traffic Isolation
Lab 6	Introduction to OpenFlow
Lab 7	Routing within an SDN network
Lab 8	Interconnection between Legacy Networks and SDN Networks
Lab 9	Configuring Virtual Private LAN Service (VPLS)
Lab 10	Applying Equal-cost Multi-path Protocol (ECMP) within SDN networks

Lab Libraries

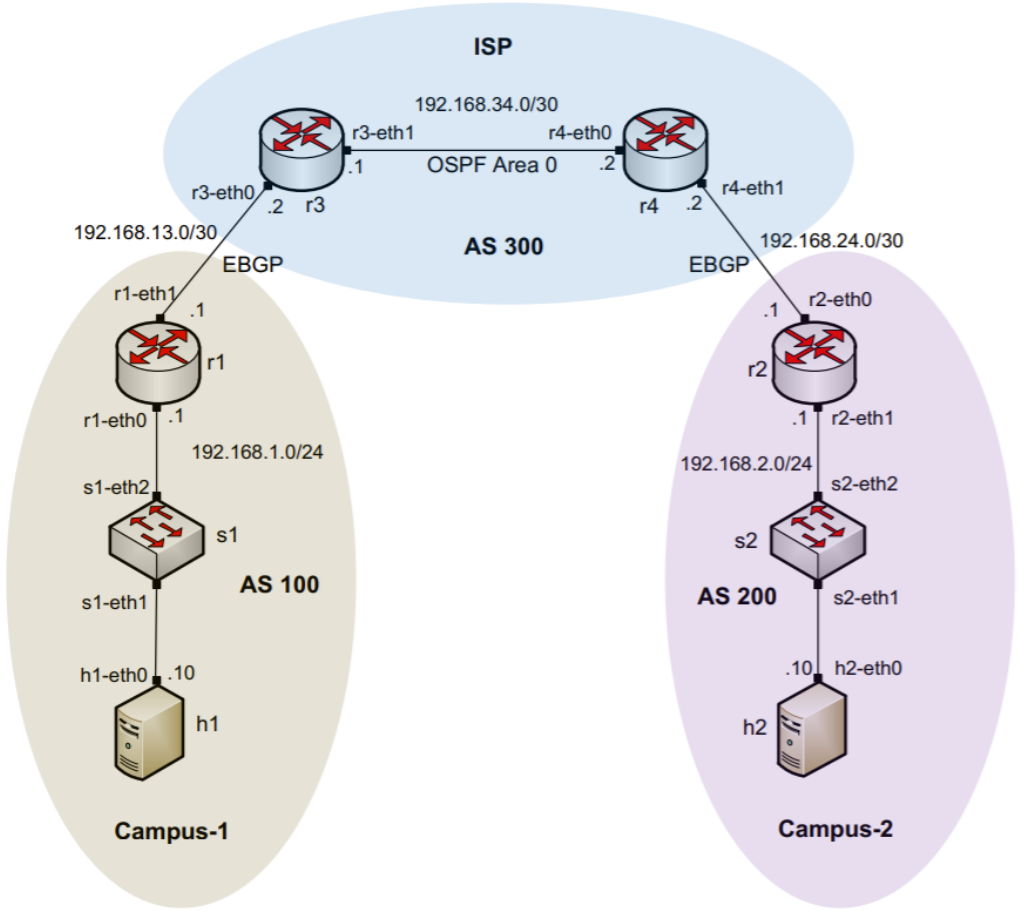
- Introduction to SDN, Lab 8: “Interconnection between Legacy Networks and SDN Networks”



Lab Libraries

- Introduction to BGP

Lab 1	Introduction to Mininet
Lab 2	Introduction to Free Range Routing (FRR)
Lab 3	Introduction to BGP
Lab 4	Configure and Verify EBGP
Lab 5	BGP Authentication
Lab 6	Configure BGP with Default Route
Lab 7	Using AS_PATH BGP Attribute
Lab 8	Configuring IBGP and EBGP Sessions, Local Preference, and MED
Lab 9	IBGP, Next Hop and Full Mesh Topology
Lab 10	BGP Route Reflection

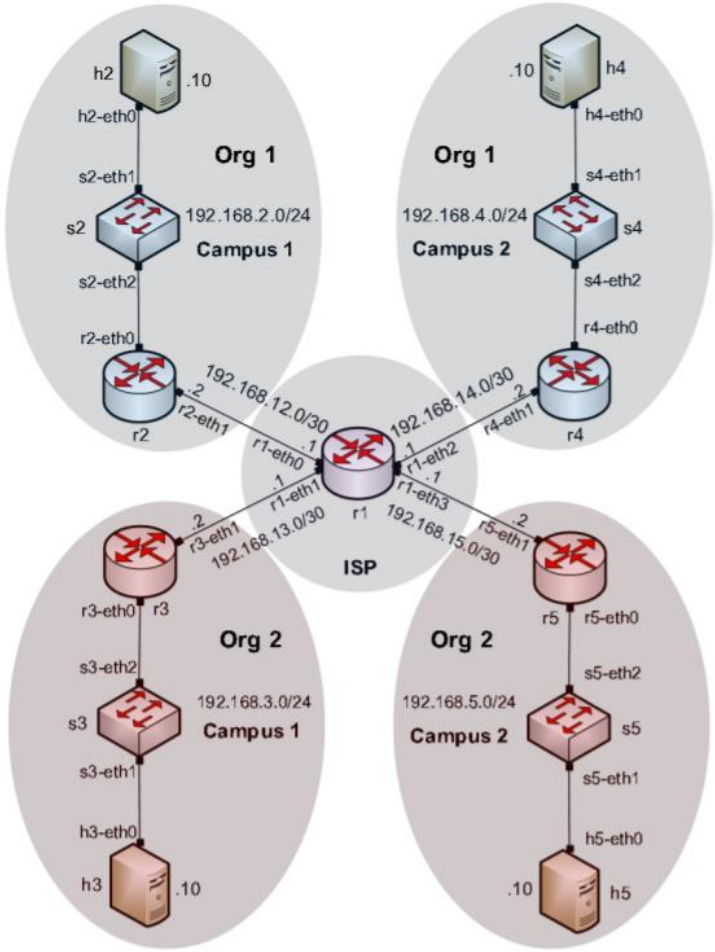


Topology for Lab 4

Lab Libraries

- MPLS and Advanced BGP Topics

Lab 1	Configuring Multiprotocol BGP
Lab 2	IP Spoofing and Mitigation Techniques
Lab 3	BGP Hijacking
Lab 4	Introduction to MPLS
Lab 5	Label Distribution Protocol (LDP)
Lab 6	Virtual Routing and Forwarding (VRF)
Lab 7	MPLS Layer 3 VPN using MP-BGP
Lab 8	Ethernet VPN (EVPN) using MP-BGP
Lab 9	Introduction to Segment Routing over IPv6 (SRv6)



Topology for Lab 6

Lab Libraries

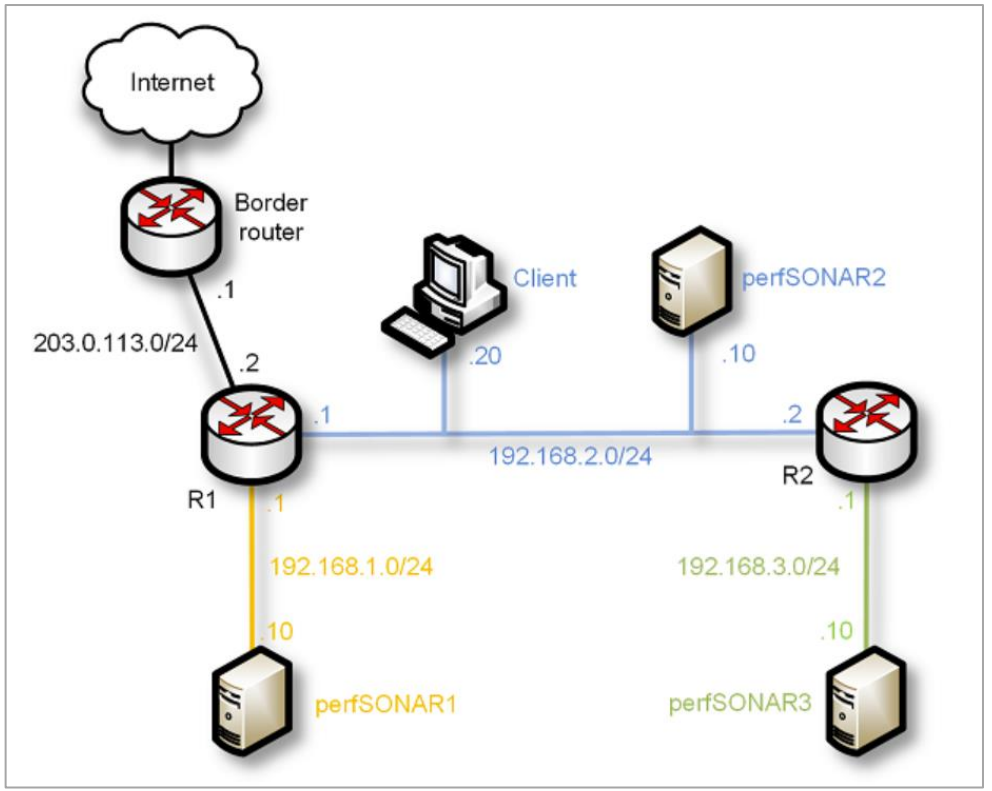
- Open Virtual Switch

Lab 1	Introduction to Linux Namespaces and Open vSwitch
Lab 2	Introduction to Mininet
Lab 3	Open vSwitch Flow table
Lab 4	Introduction to Open vSwitch
Lab 5	Implementing VLANs in Open vSwitch
Lab 6	VLAN trunking in Open vSwitch
Lab 7	Implementing Routing in Open vSwitch
Lab 8	Open Vswitch Database Management Protocol (OVSDB)
Lab 9	Open Vswitch Kernel Datapath
Lab 10	Configuring Stateless Firewall using ACLs
Lab 11	Configuring Stateful Firewall using Connection Tracking
Lab 12	Configuring GRE Tunnel
Lab 13	Configuring IPsec GRE Tunnel
Lab Manuals	

Lab Libraries

- perfSONAR

Lab 1	Configuring Administrative 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

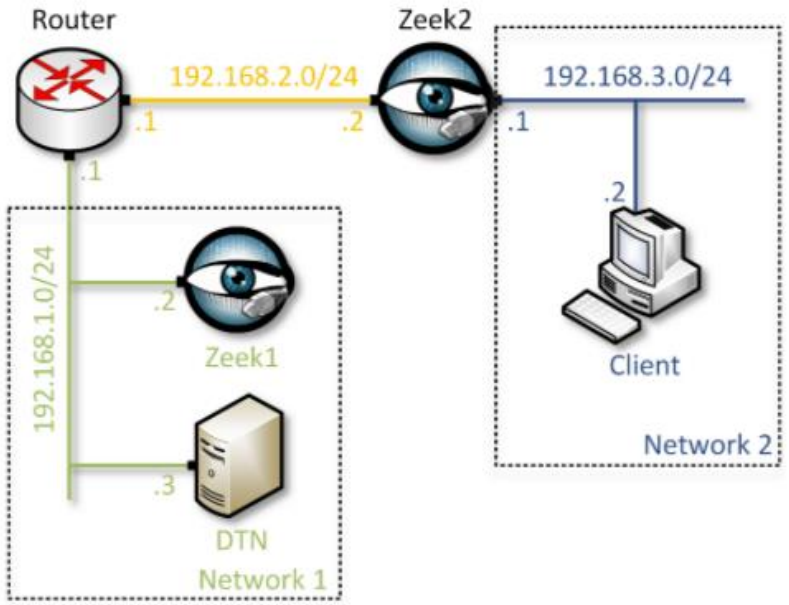


Topology for perfSONAR labs

Lab Libraries

- Zeek Intrusion Detection

Lab 1	Introduction to the Capabilities of Zeek
Lab 2	An Overview of Zeek Logs
Lab 3	Parsing, Reading and Organizing Zeek Log 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	Introduction to Zeek Signatures
Lab 8	Advanced Zeek Scripting for Anomaly and Malicious Event Detection
Lab 9	Profiling and Performance Metrics of Zeek
Lab 10	Application of the Zeek IDS for Real-Time Network Protection
Lab 11	Preprocessing of Zeek Output Logs for Machine Learning
Lab 12	Developing Machine Learning Classifiers for Anomaly Inference and Classificati



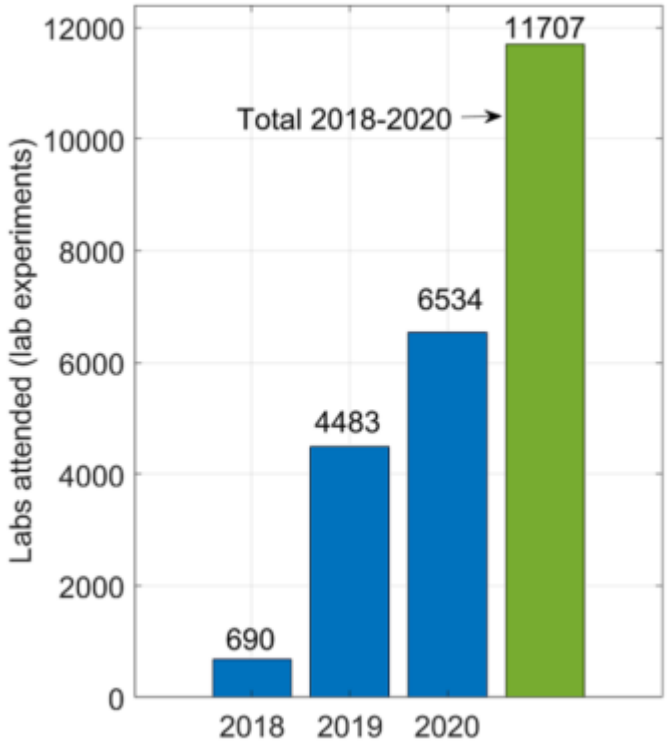
Topology for Zeek labs

Cloud Features

Feature	Comments
Allocation of resources	Granular allocation of physical resources
Custom pods	Easy to create custom pods
Cost	Cost-effective when used extensively
Presentation layer for pedagogy	Topology is graphically presented to the learner using a regular browser
Time sharing	The owner controls who can access resources; easy to implement time-sharing policies
IP addresses	Pods (and learners) can have the same topology and IP addresses (overlapping addresses w/o conflict)
Functional realism	Virtual labs have the same functionality as real IT hardware in a real deployment, and execute the same code
Traffic realism	Devices generate/receive real, interactive network traffic to/from the Internet, or to/from other devices within the lab environment

Cloud Usage at UofSC – IIT Department

- Total labs experiments in 2020: **6,534**
- Total hours: **25,158.03**
- Hours per lab: **3.85**



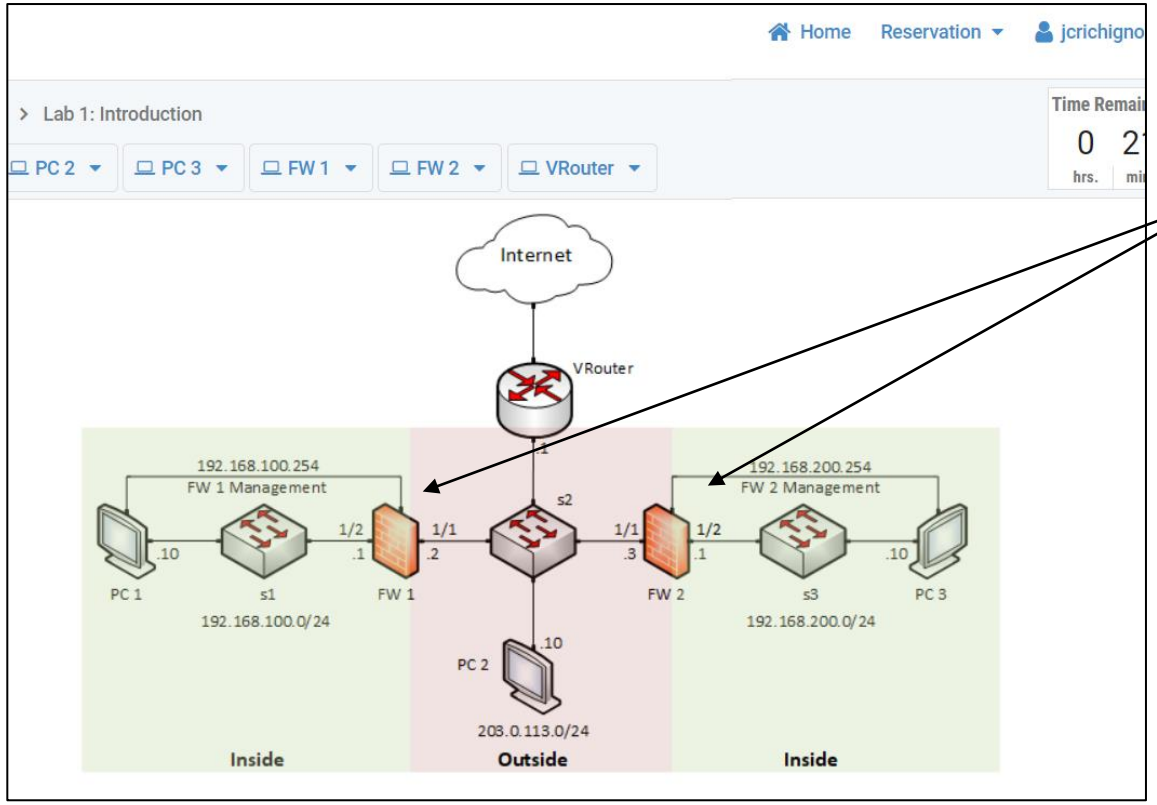
Partnership with Industry

- The IEEE and ACM are the main societies which guide IT education
  - IT curriculum should emphasize “learning IT core concepts combined with authentic practice” and “use of professional tools and platforms”[1]
- UofSC works with the Network Development Group (NDG)[2], VMware, Palo Alto Cybersecurity Academy, Cisco, Juniper, and others to virtualize labs

1. “Information Technology Curricula Guideline 2017 (IT2017),” report by the ACM / IEEE Task Force on Information Technology Curricula, Dec. 2017. Online: https://tinyurl.com/yxauot8w
2. Network Development Group (NDG). Online: https://netdevgroup.com

Partnership with Industry

- These labs enhance the student's understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)

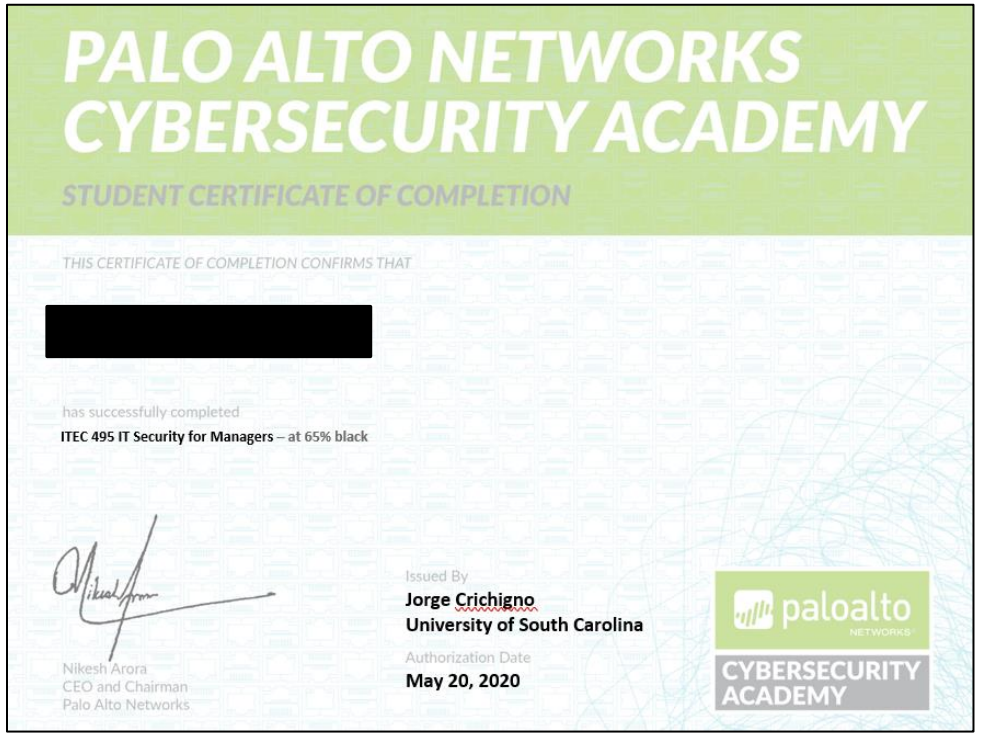


Pod deployed in private cloud

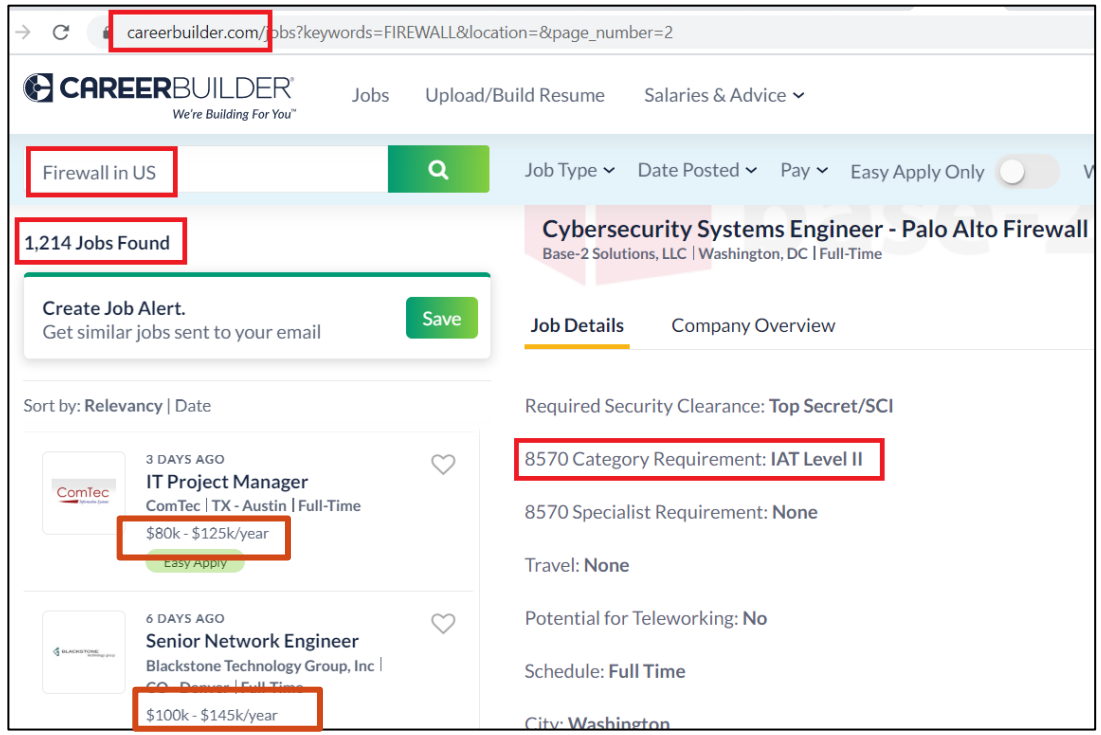
Next-generation Firewall Virtual Machine + licenses

Partnership with Industry

- These labs enhance the student's understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)



Additional credentials



Job search

Partnership with Industry

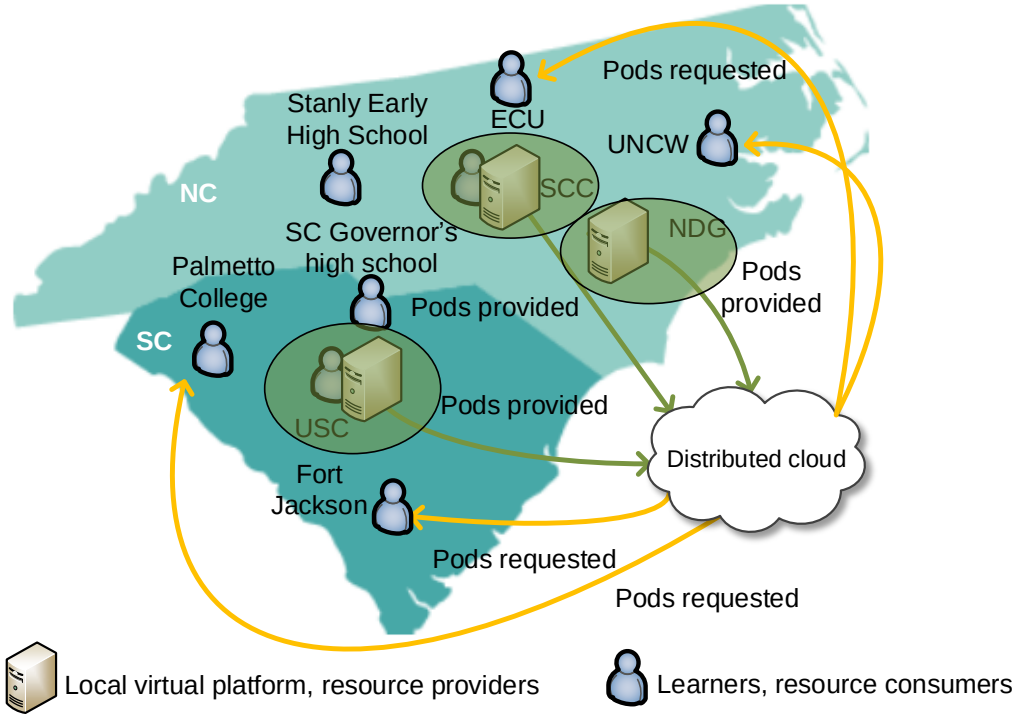
- DoD's Information Assurance (IA) workforce is classified in IA technical (IAT):
  - Level 1 (IAT 1): Computing environment information assurance
  - Level 2 (IAT 2): Network environment information assurance

Covered in	IAT 1	IAT 2	NICE framework	Networks cert.
ITEC 233 Hw/Sw	✓			
ITEC 293 Cybersec Ops	✓			
ITEC 293 Cybersec Ops	✓	✓		
ITEC 493 IT Security	✓	✓		
ITEC 245, ITEC 445				✓
ITEC 493 IT Security			✓	
ITEC 493 IT Security			✓	

NICE: National Initiative for Cybersecurity Education

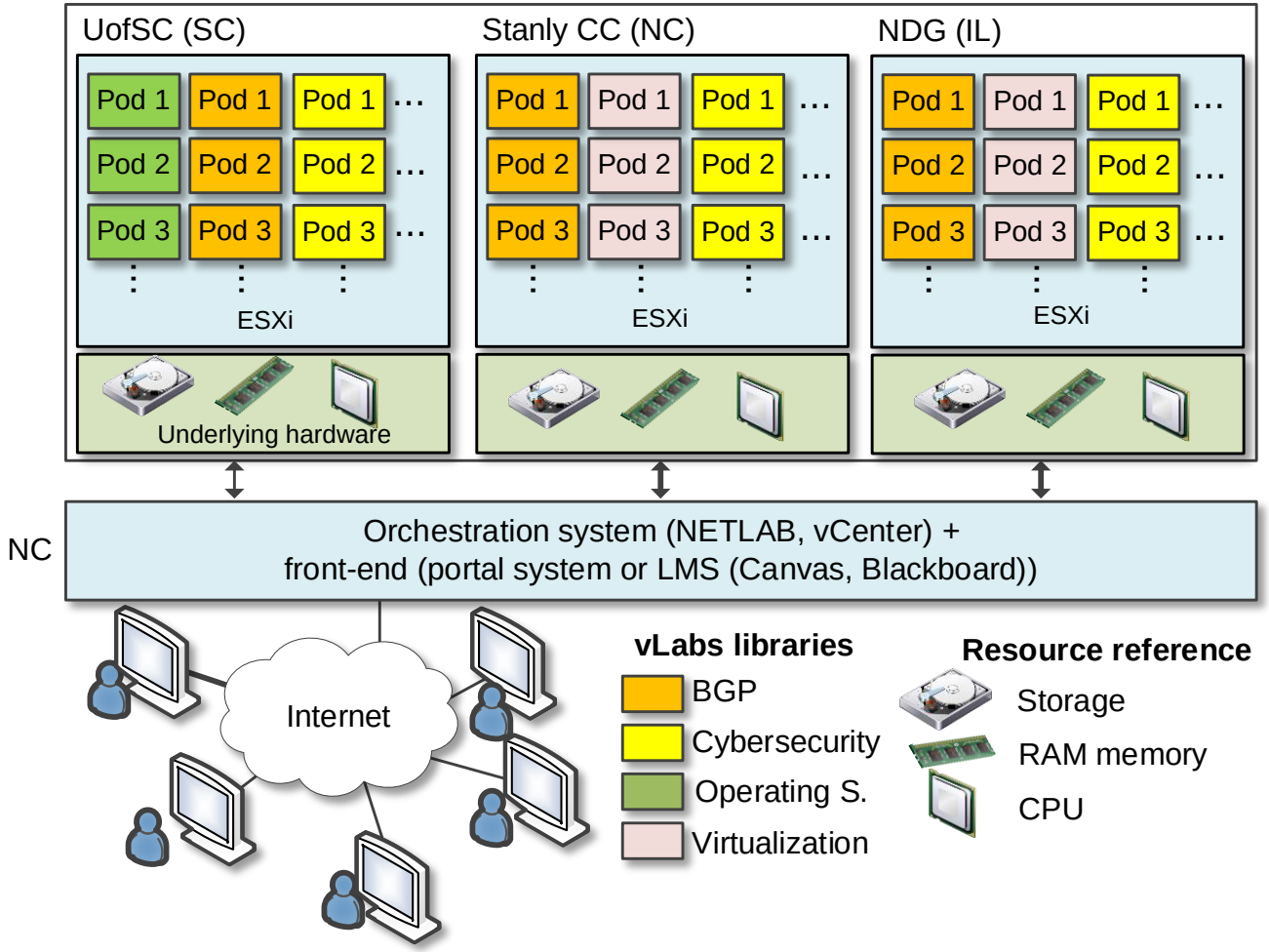
Distributed Academic Cloud

- University of South Carolina (SC), Stanly Community College (NC), and the Network Development Group are building a Distributed Academic Cloud
  - NSF Advanced Technology Education: “Multi-state Community College, University and Industry Collaboration to Prepare Learners for 21st Century Information Technology Jobs”
- The goal is scalability, using the resources available on campus networks
- Industry partnership
- Platform use
  - Community Colleges
  - Universities
  - High Schools
  - SANS institute (“girlsgocyber”)
  - Fort Gordon (U.S. Army Signal School)



Distributed Academic Cloud

- Academic Cloud as of January 2021



Distributed Academic Cloud

- News

South Carolina

INDUSTRY
UNIVERSITY OF SOUTH CAROLINA
COLLEGE OF ENGINEERING
AND COMPUTING

LOCATION
COLUMBIA, SOUTH CAROLINA

KEY CHALLENGES
- Needed to educate students who were located in multiple academic and military institutions for high-demand technology jobs.
- Needed remote access to hands-on labs and exercises that could scale.

The University of South Carolina partners with VMware IT Academy to help students learn digital technology skills to fill high-demand jobs

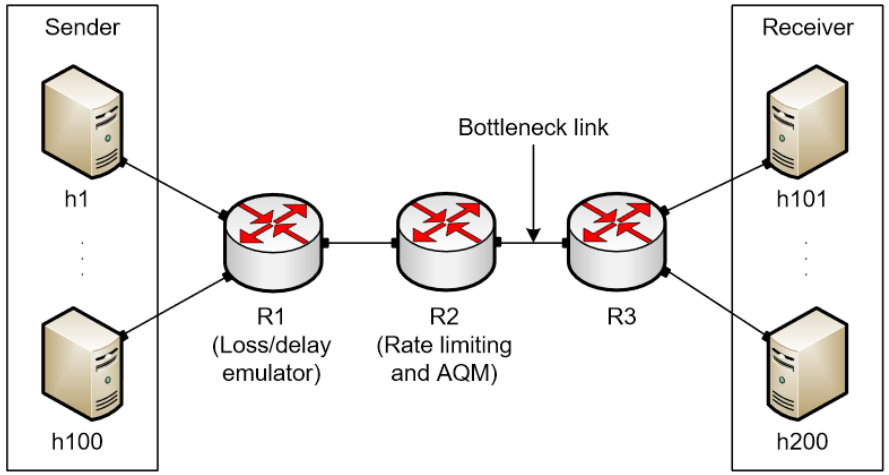
Who we are
Located in Columbia, South Carolina, the **University of South Carolina (USC)** is a

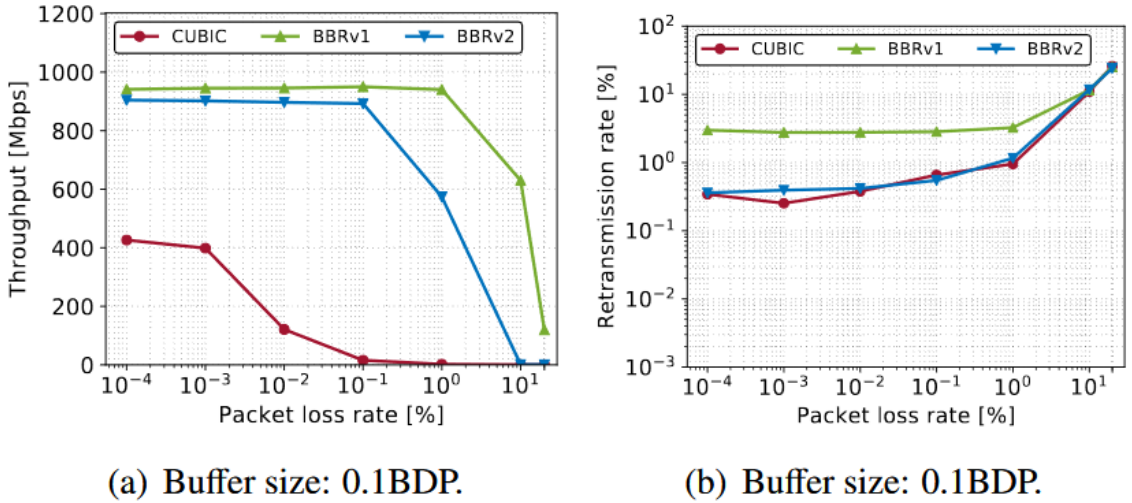
Stanly Community College Awarded $300,000 National Science Foundation Grant

Stanly Community College Awarded $300,000 National Science Foundation Grant

Using Pods for Research

- Pods in the virtual platform can be used to conduct experiments
- Useful for parallelizing tests
- For example, comparing the performance of CUBIC, BBRv1, and BBRv2[1]
  - Experiments were executed 10 times and the results were averaged
  - Each pod is used to execute a single experiment



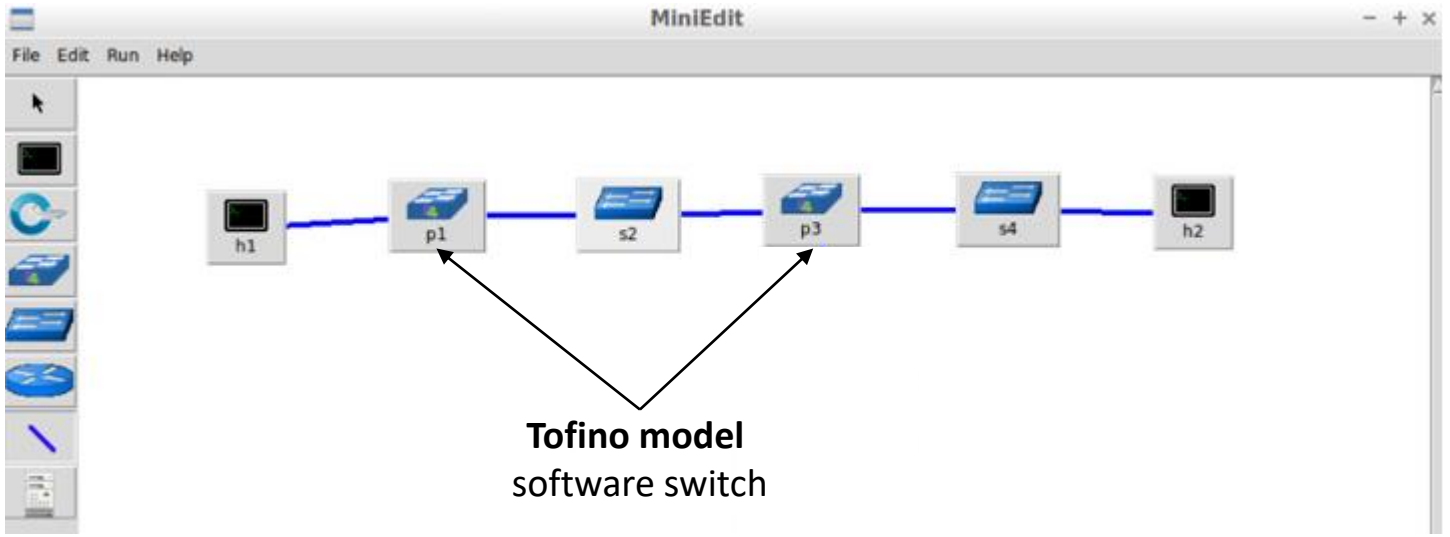


(a) Buffer size: 0.1BDP. (b) Buffer size: 0.1BDP.

1. E. Kfoury, J. Gomez, J. Crichigno, E. Bou-Harb, "An Emulation-based Evaluation of TCP BBRv2 Alpha for Wired Broadband", Computer Communications, July 2020.

Using Pods for Research

- Pods can also be used to enhance the collaboration on a research project
- Multiple researchers working in the same environment
- Example projects:
  - Prototyping an in-network defense scheme using P4 programmable switches
  - Offloading conversational media traffic to P4 switches
  - Using P4 switches as passive instruments to analyze traffic in a legacy network



UNIVERSITY OF
SOUTH CAROLINA