# Galaxy: A Network Emulation Framework for Cybersecurity

NATURAL COMPUTATION LABORATORY, DEPARTMENT OF COMPUTER SCIENCE, MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY / LOS ALAMOS NATIONAL LABORATORY CYBER SECURITY SCIENCES INSTITUTE

**Kevin Schoonover**, **Eric Michalak**, Sean Harris, Adam Gausmann, Hannah Reinbolt, Joshua Herman, Daniel R. Tauritz, Chris Rawlings, Aaron Scott Pope

MISSOURI S&T

# Outline

- Motivations
- Design
- Application
- Challenges and Lessons Learned
- Future Work

Los Alamos NATIONAL LABORATORY EST. 1943

# Who are we

Kevin Schoonover

- Undergraduate CS student
- Researcher at Missouri S&T

Eric Michalak

- Research Scientist at Los Alamos
- Missouri S&T CS Alumni

Our Team

- CEADS-LIN Project
- Missouri S&T's export-controlled Natural Computation Laboratory
- Los Alamos Advanced Research in Cyber Systems
- Funding: Cyber Security Sciences Institute (Los Alamos and S&T)

MISSOURI S&T

# What is Galaxy?

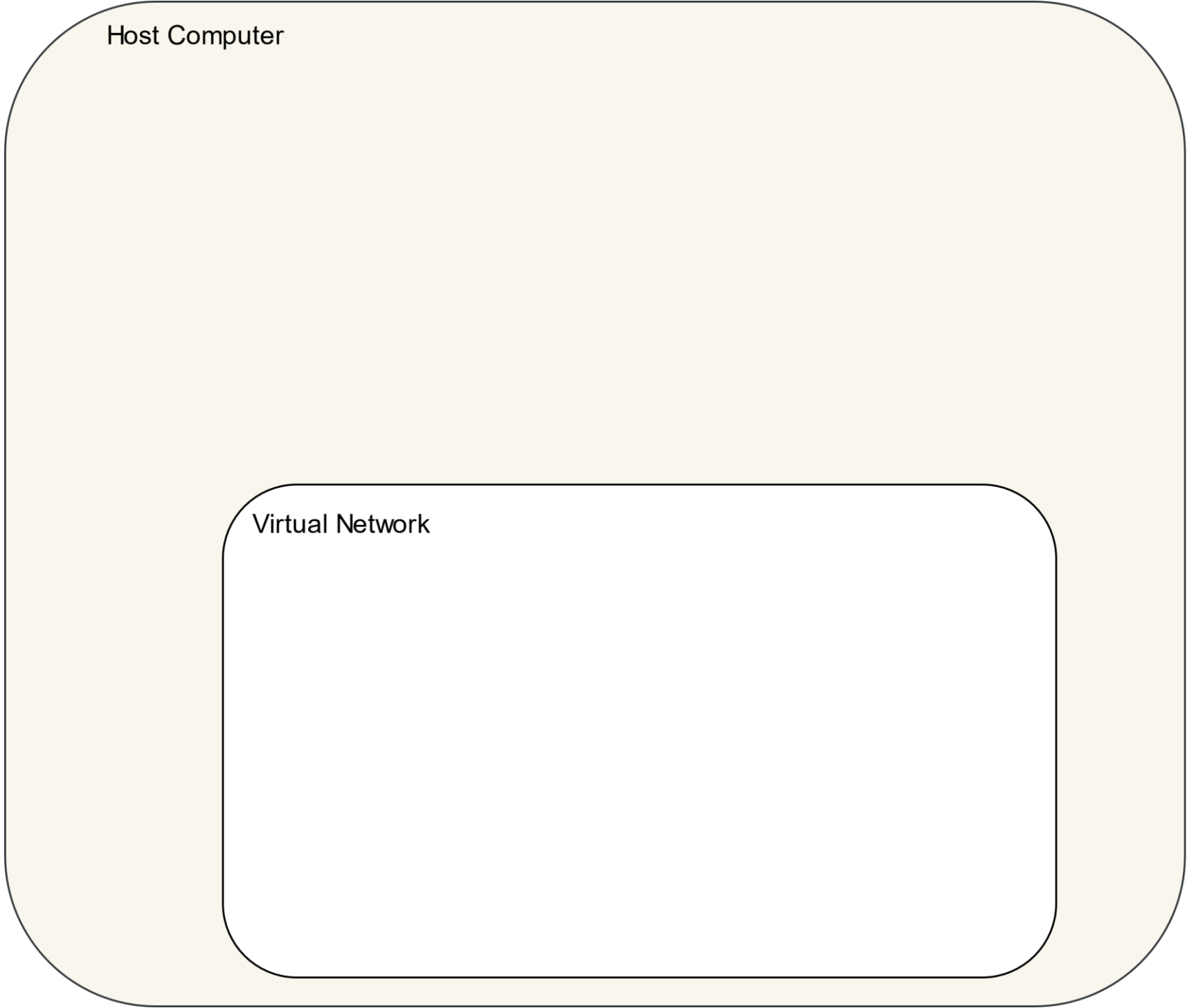
- Network emulation framework
  - Stateless evaluations with low overhead
  - Network fidelity
  - Result storage and collection
- Specialized for agent-based experiments
- Unique from current solutions
  - Rapidly runs successive, stateless evaluations
  - Built-in results reporting
  - Modular components

Los Alamos NATIONAL LABORATORY EST. 1943

MISSOURI S&T

# Design

Los Alamos NATIONAL LABORATORY EST. 1943

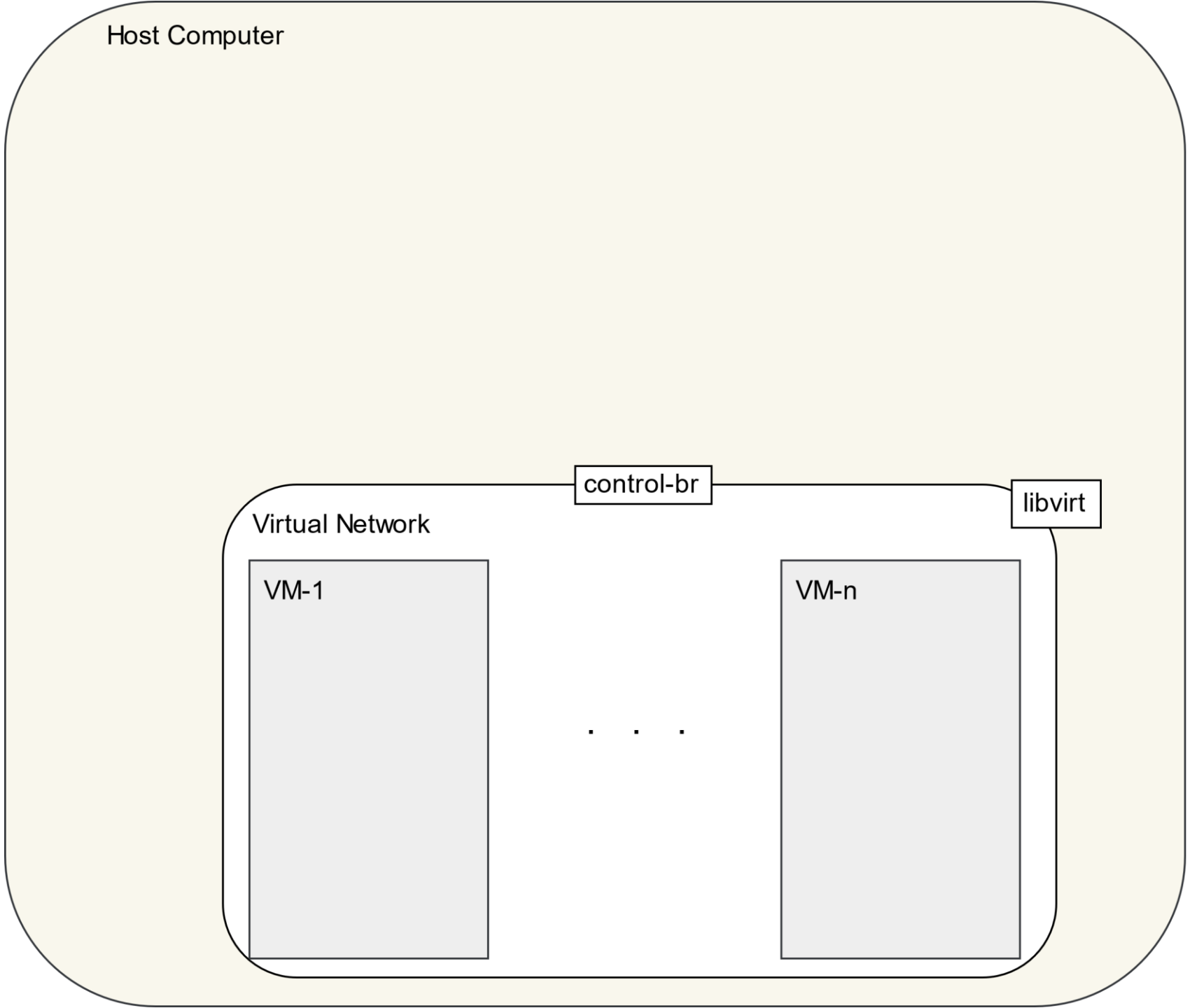

Host Computer
Virtual Network

MISSOURI S&T

# Design - Layers

- Two logical layers
- **Host Layer –** Evaluation orchestration and persistent storage
- **Virtual Layer –** Facilitating and running evaluations

Los Alamos NATIONAL LABORATORY EST. 1943

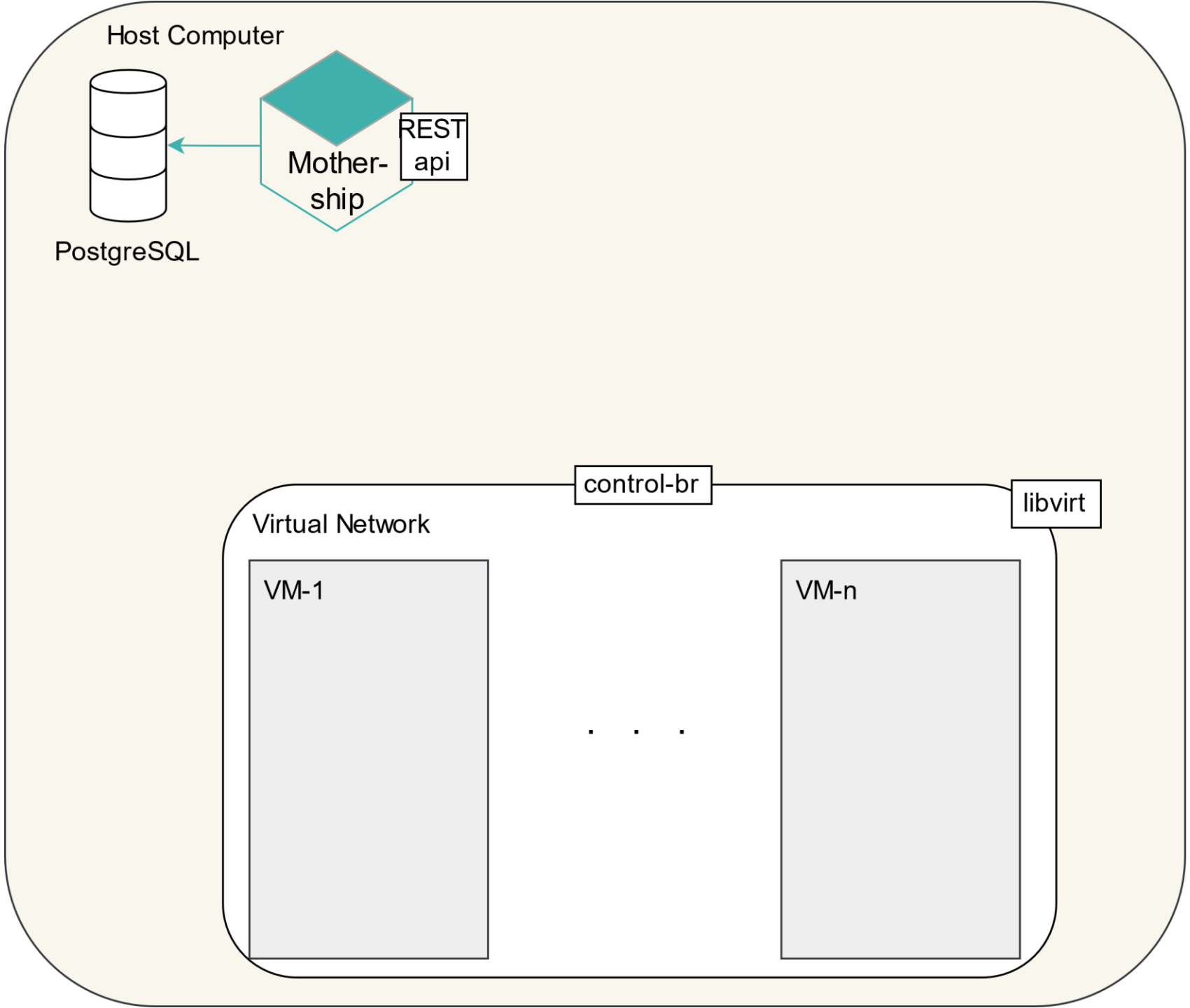

Host Computer
control-br
libvirt
Virtual Network
VM-1
VM-n

MISSOURI S&T

# Design - Infrastructure

- **Libvirt –** Virtualization API utilizing KVM as hypervisor
- **Virtual Machines –** High fidelity emulation of physical hosts
- **Virtual Bridges –** Layer 2 “switches” that network virtual machines together
- **Control Bridge –** Point-to-point command network connected to each virtual machine

Los Alamos NATIONAL LABORATORY EST. 1943

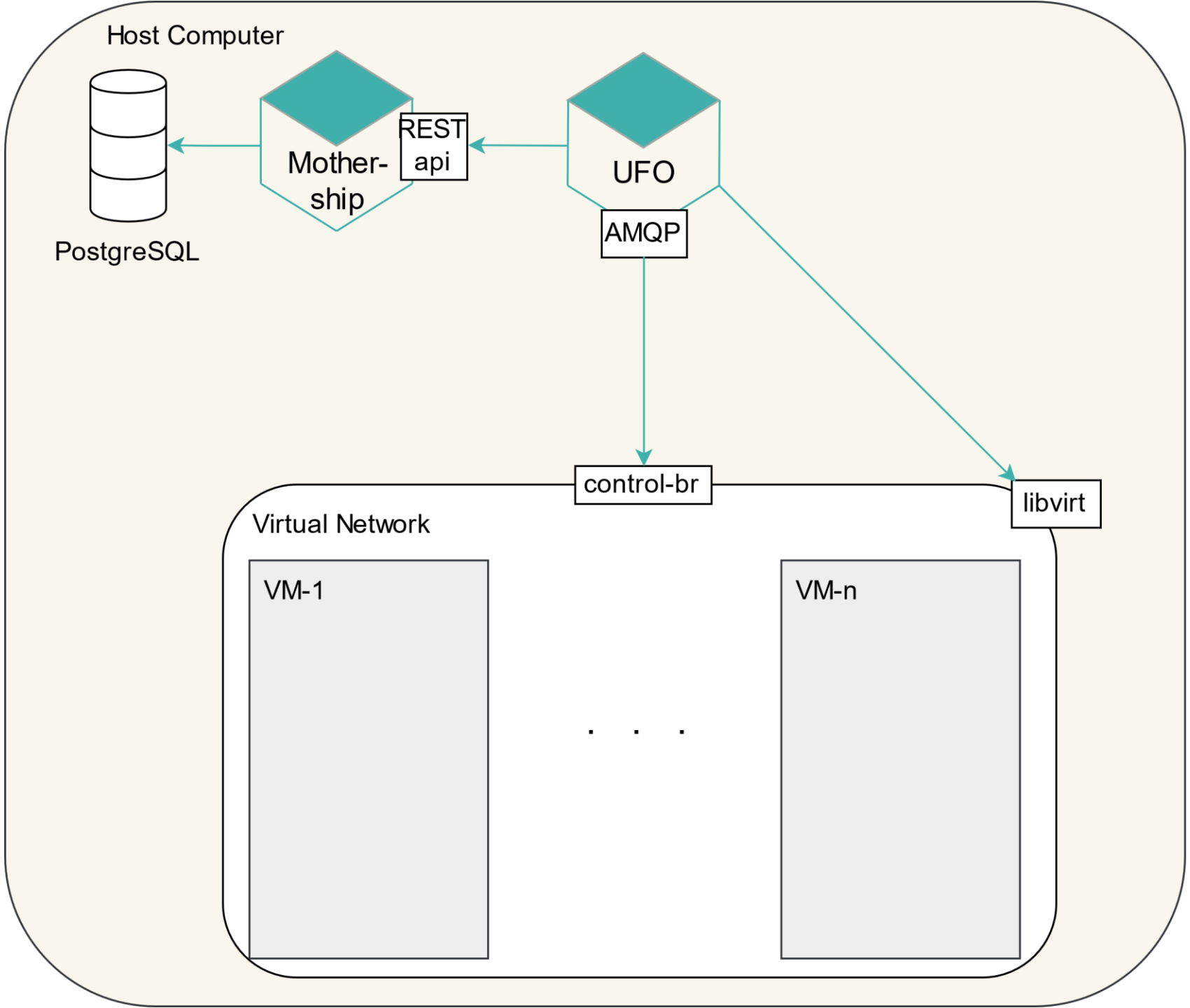

Host Computer
Mother-
ship
REST
api
PostgreSQL
control-br
libvirt
Virtual Network
VM-1
VM-n

MISSOURI S&T

# Mothership

- Primary data storage/retrieval for researchers and agents
- Provides access to persistent evaluation metadata through REST API
  - /queue/
  - /evaluations/
  - /results/
  - /nodes/

Los Alamos NATIONAL LABORATORY EST. 1943

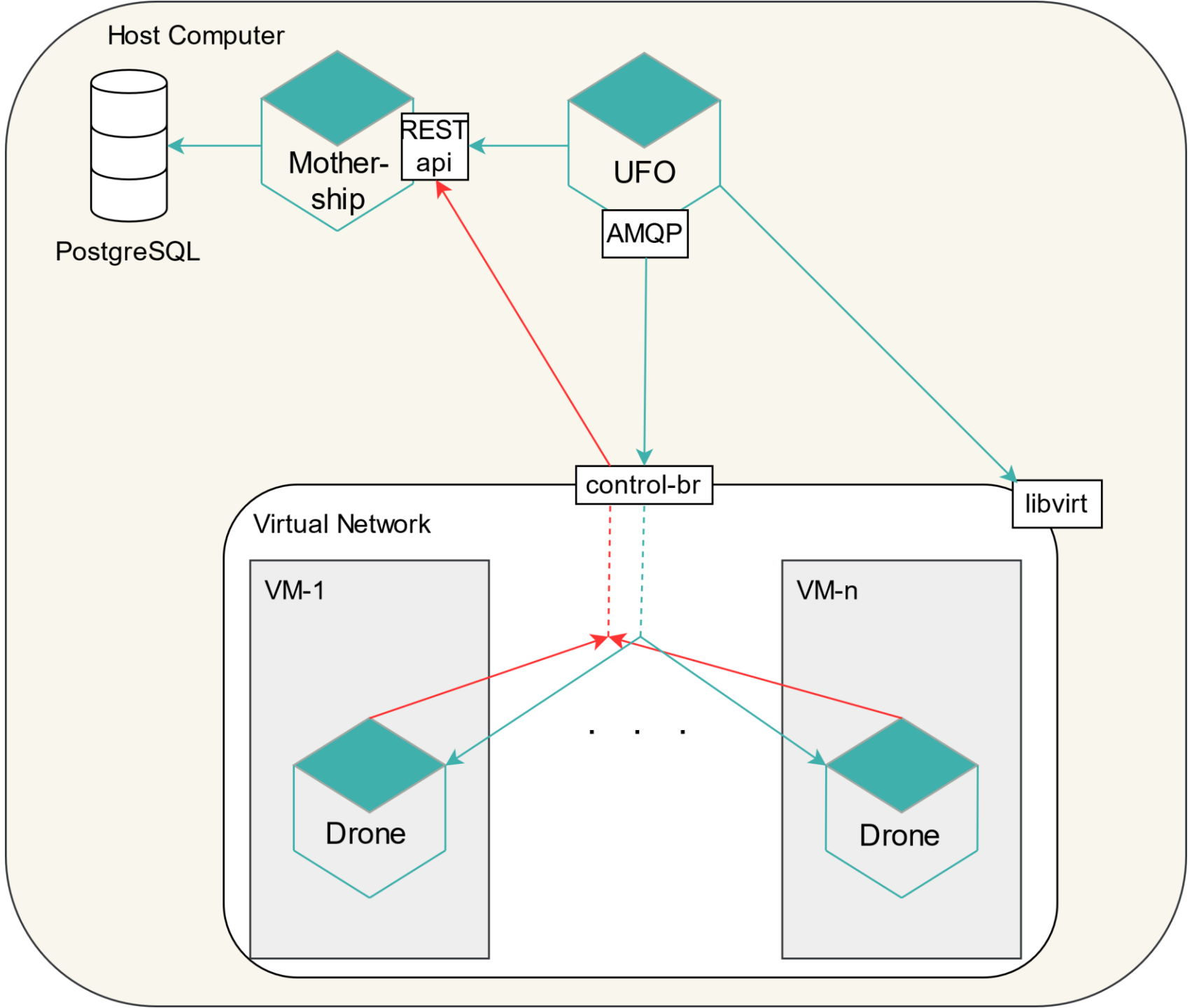

Host Computer
PostgreSQL
Mother-
ship
REST
api
UFO
AMQP
control-br
libvirt
Virtual Network
VM-1
VM-n

MISSOURI S&T

# UFO

- Manages evaluations
- Sends commands to agents
  - **START –** Begin an evaluation and perform your actions
  - **UPDATE –** If an agent has an update action, send the update to Mothership.
  - **END –** End the evaluation and gracefully shutdown

Los Alamos NATIONAL LABORATORY EST. 1943


Host Computer
PostgreSQL
Mother-
ship
REST
api
UFO
AMQP
control-br
libvirt
Virtual Network
VM-1
VM-n
Drone
Drone

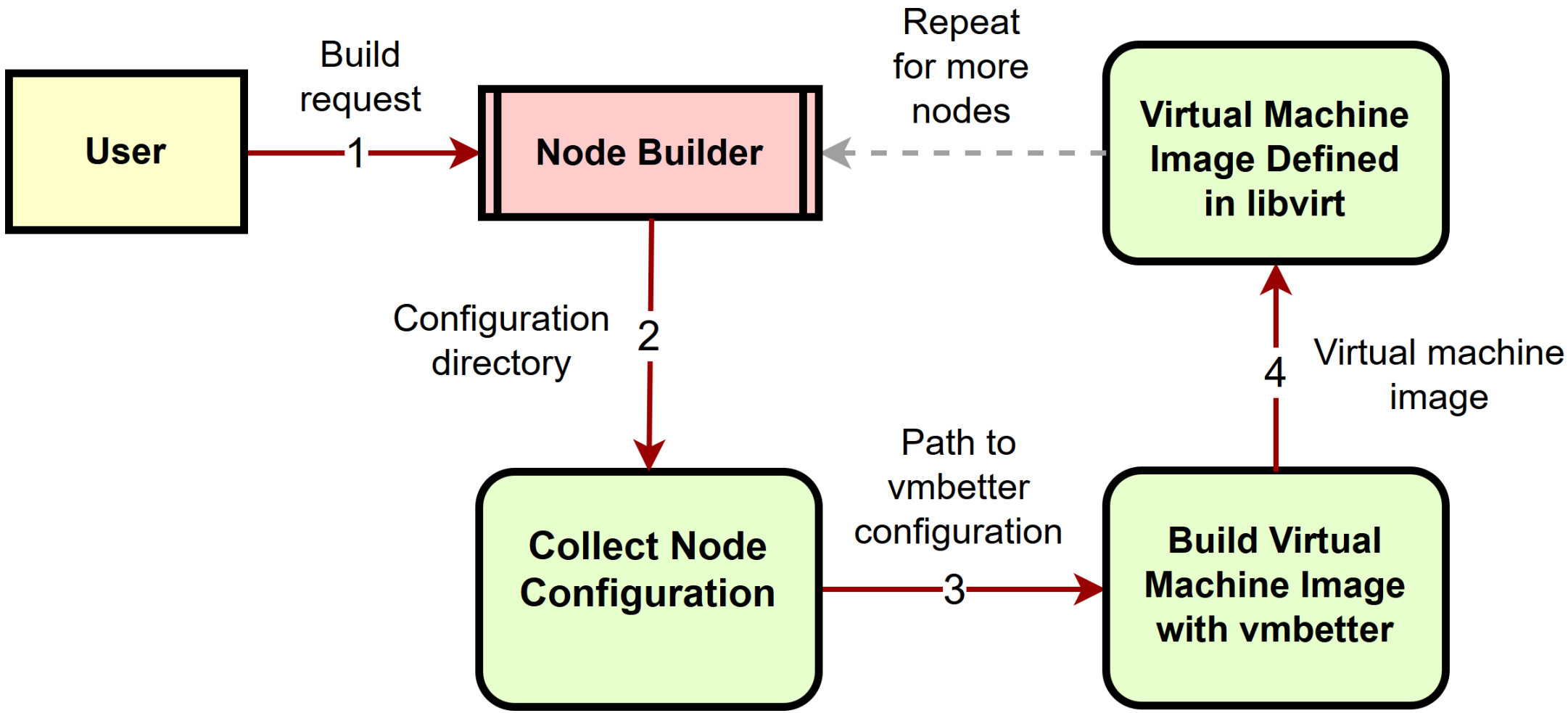
MISSOURI S&T

# Drone

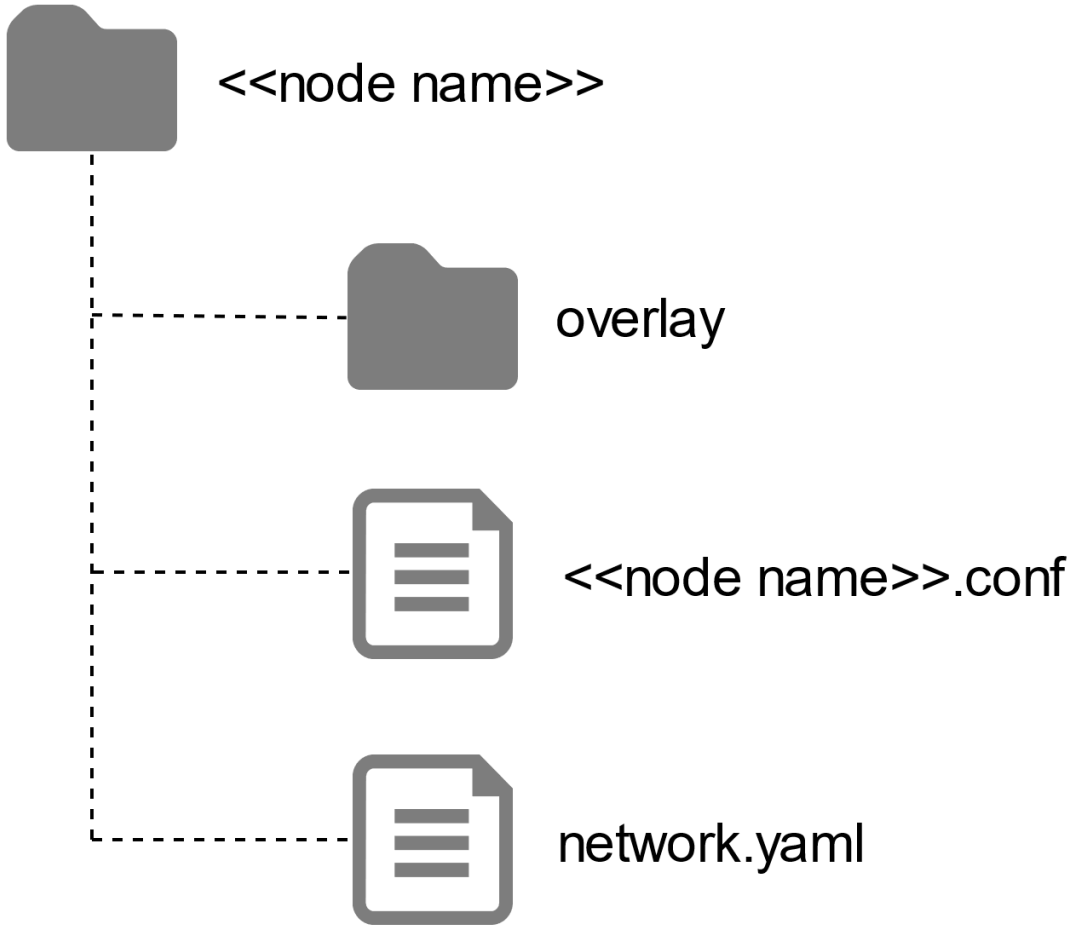
- Metric / data collection agent
- Performs ping tests to ensure network consistency
  - Alerts researcher of infrastructure problems
  - Researcher can then determine to restart or fail an experiment

Los Alamos NATIONAL LABORATORY EST. 1943

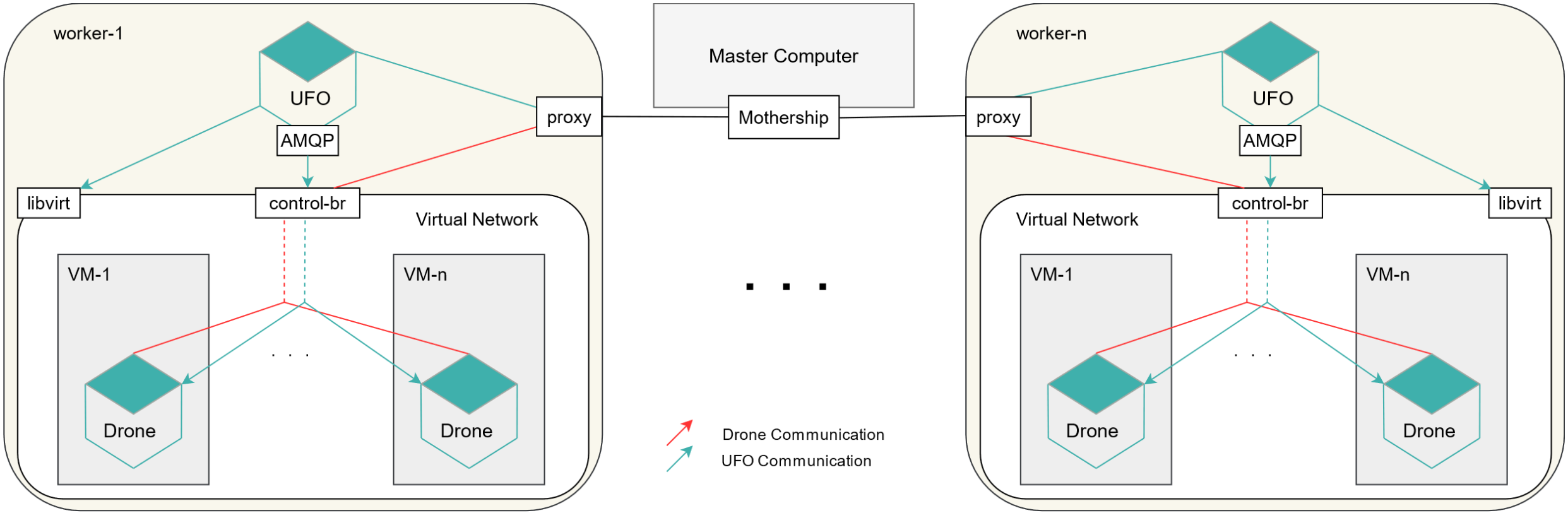
# Building the Network



# Node Configuration



# Scaling Galaxy



MISSOURI S&T

# Experiment Procedure

1. Query Mothership for list of nodes on the topology
2. Revert each VM to initial snapshot, starting VM
3. Send the START command
4. Send the UPDATE command every five seconds
5. Send the STOP command after 60 seconds

Los Alamos NATIONAL LABORATORY EST. 1943

MISSOURI S&T

# Application: CEADS-LIN

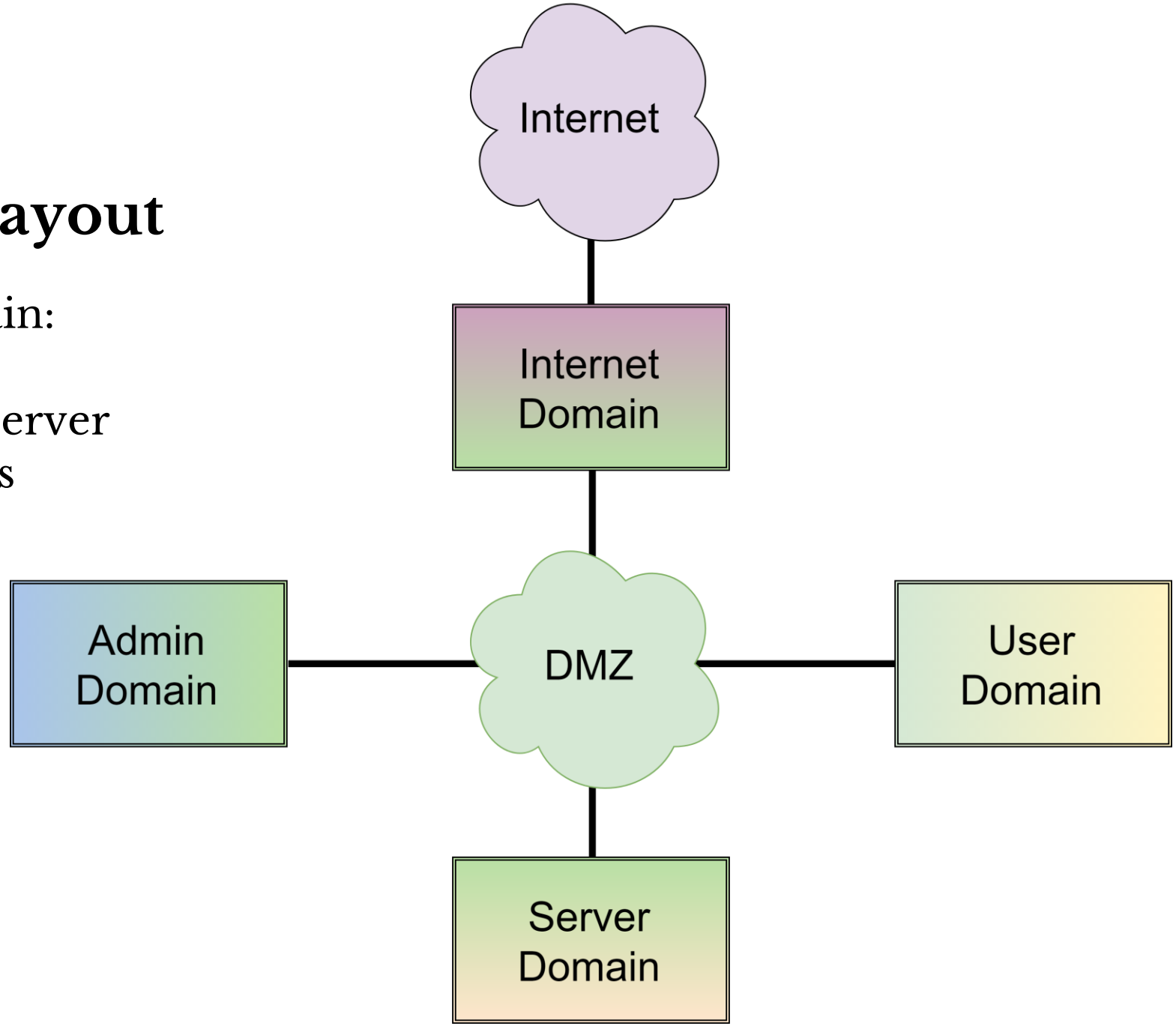
- **C**o**E**volution of **A**ttacker and **D**efender **S**trategies for **L**arge **I**nfrastructure **N**etworks
- Represents Attackers and Defenders as evolutionary agents operating within an emulated network
- Utilizes Galaxy for creating the network, running evaluations, and reporting results

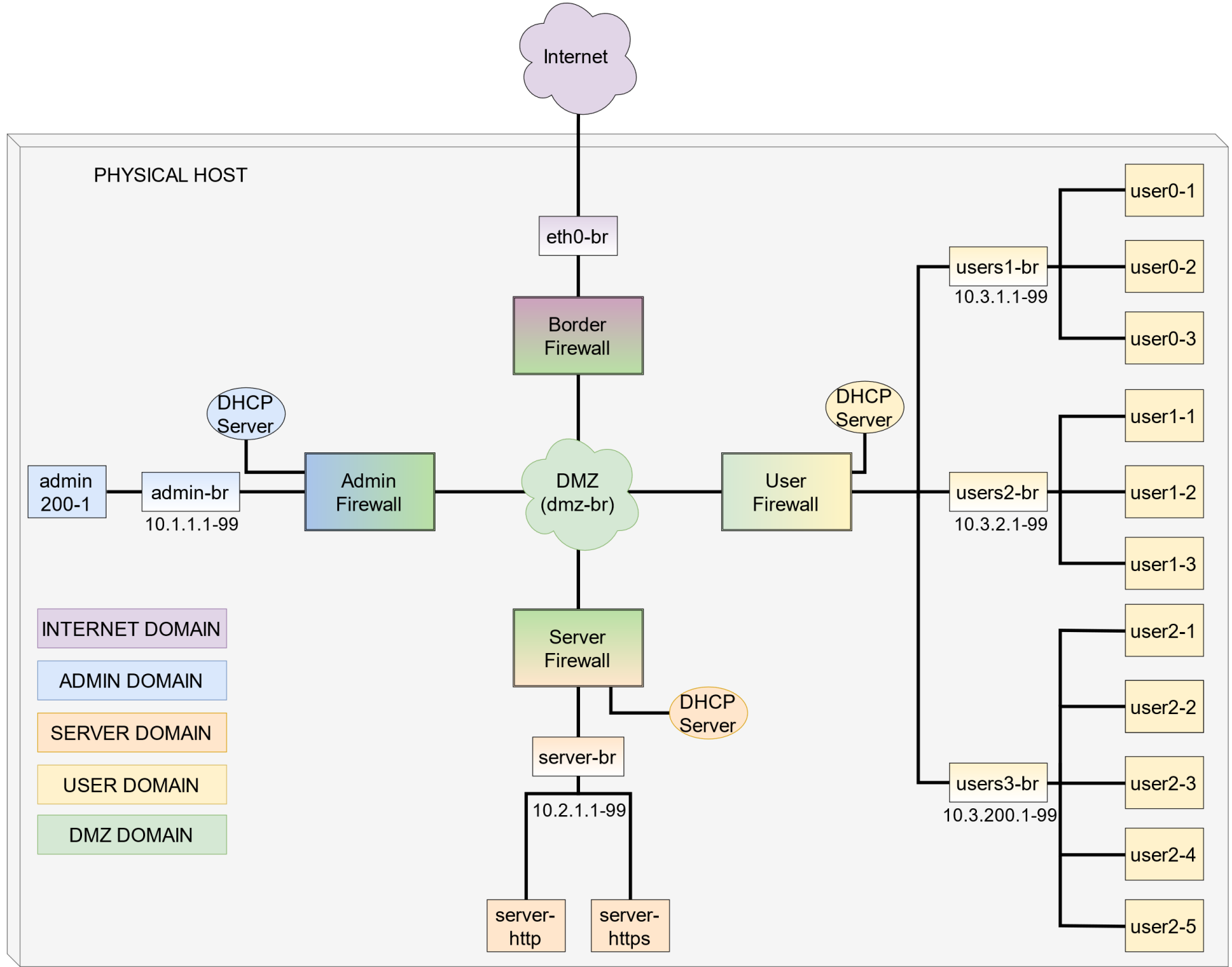
Los Alamos NATIONAL LABORATORY EST. 1943

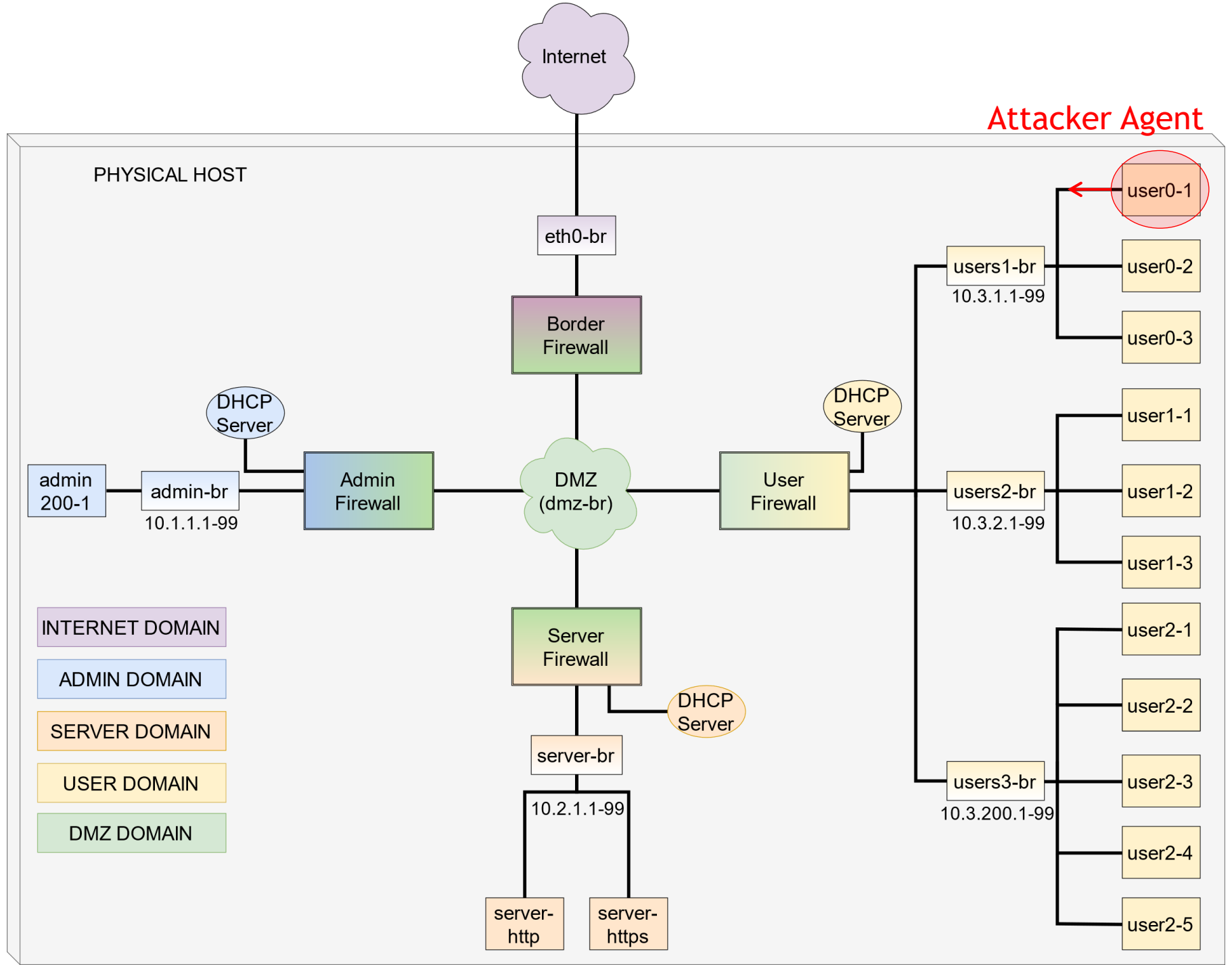
# CEADS
# Network Layout

Domains Contain:

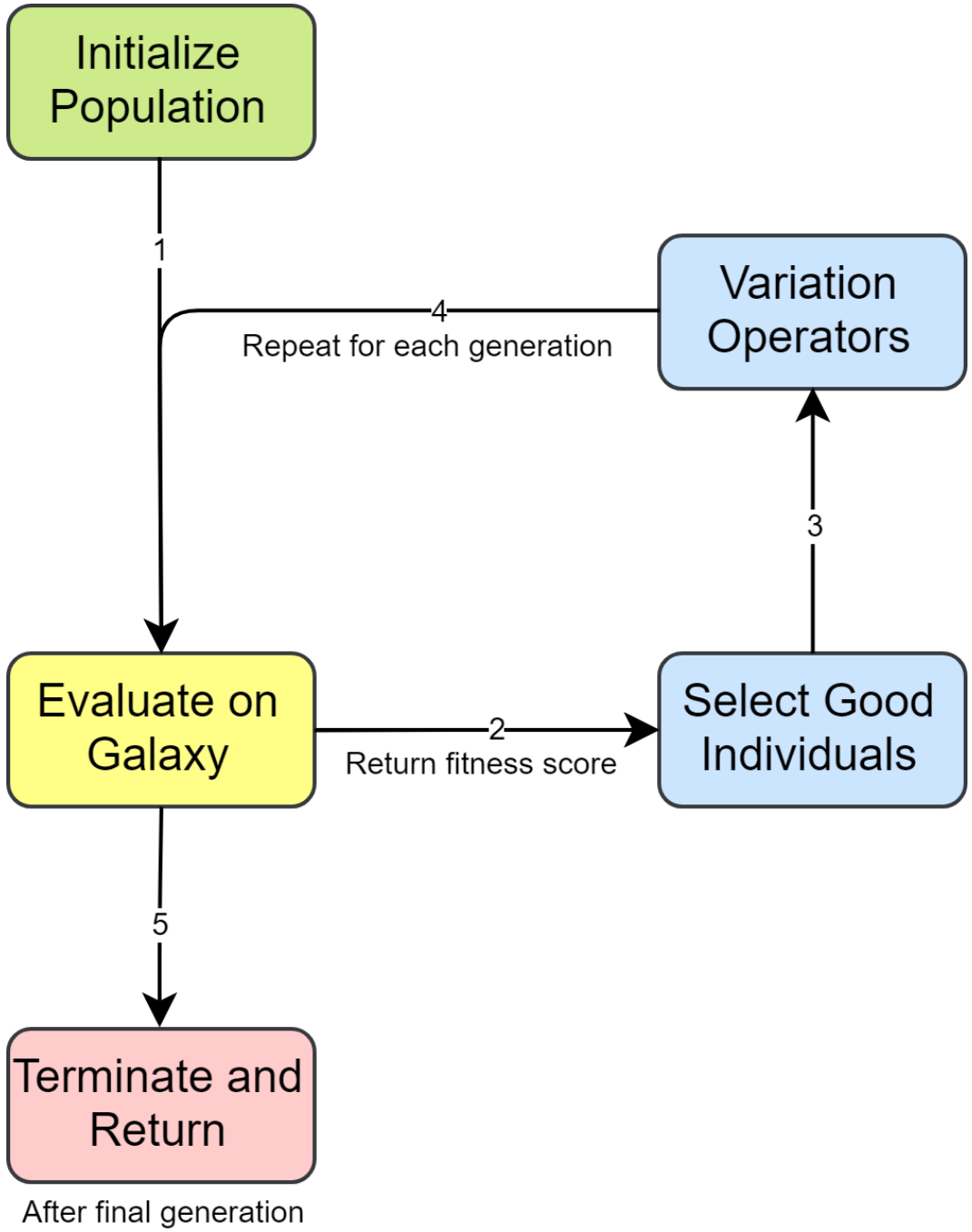
- A Firewall
- A DHCP Server
- End Nodes




Internet
PHYSICAL HOST
eth0-br
Border Firewall
DHCP Server
admin 200-1
admin-br
10.1.1.1-99
Admin Firewall
DMZ (dmz-br)
User Firewall
DHCP Server
users1-br
10.3.1.1-99
user0-1
user0-2
user0-3
users2-br
10.3.2.1-99
user1-1
user1-2
user1-3
users3-br
10.3.200.1-99
user2-1
user2-2
user2-3
user2-4
user2-5
INTERNET DOMAIN
ADMIN DOMAIN
SERVER DOMAIN
USER DOMAIN
DMZ DOMAIN
Server Firewall
DHCP Server
server-br
10.2.1.1-99
server-http
server-https


Internet
Attacker Agent
PHYSICAL HOST
eth0-br
Border Firewall
DHCP Server
admin 200-1
admin-br
10.1.1.1-99
Admin Firewall
DMZ (dmz-br)
DHCP Server
User Firewall
user0-1
users1-br
10.3.1.1-99
user0-2
user0-3
user1-1
users2-br
10.3.2.1-99
user1-2
user1-3
INTERNET DOMAIN
ADMIN DOMAIN
SERVER DOMAIN
USER DOMAIN
DMZ DOMAIN
Server Firewall
DHCP Server
server-br
10.2.1.1-99
server-http
server-https
user2-1
user2-2
users3-br
10.3.200.1-99
user2-3
user2-4
user2-5

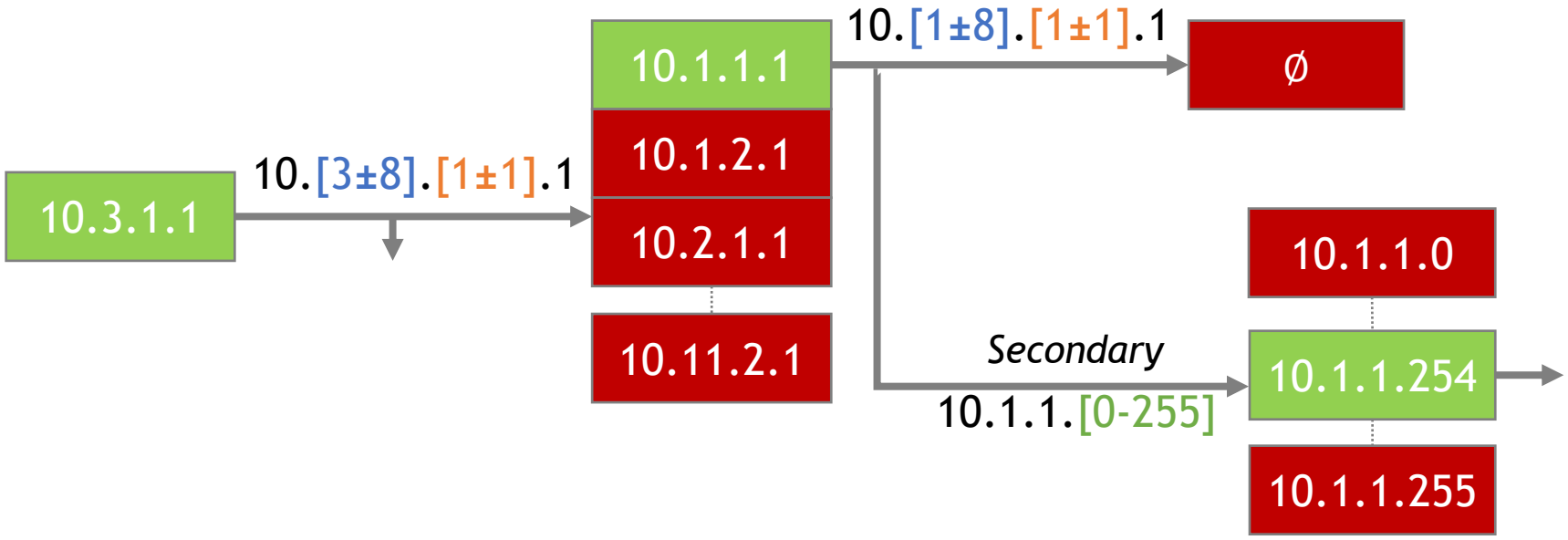
# Evolutionary Algorithms



# Results

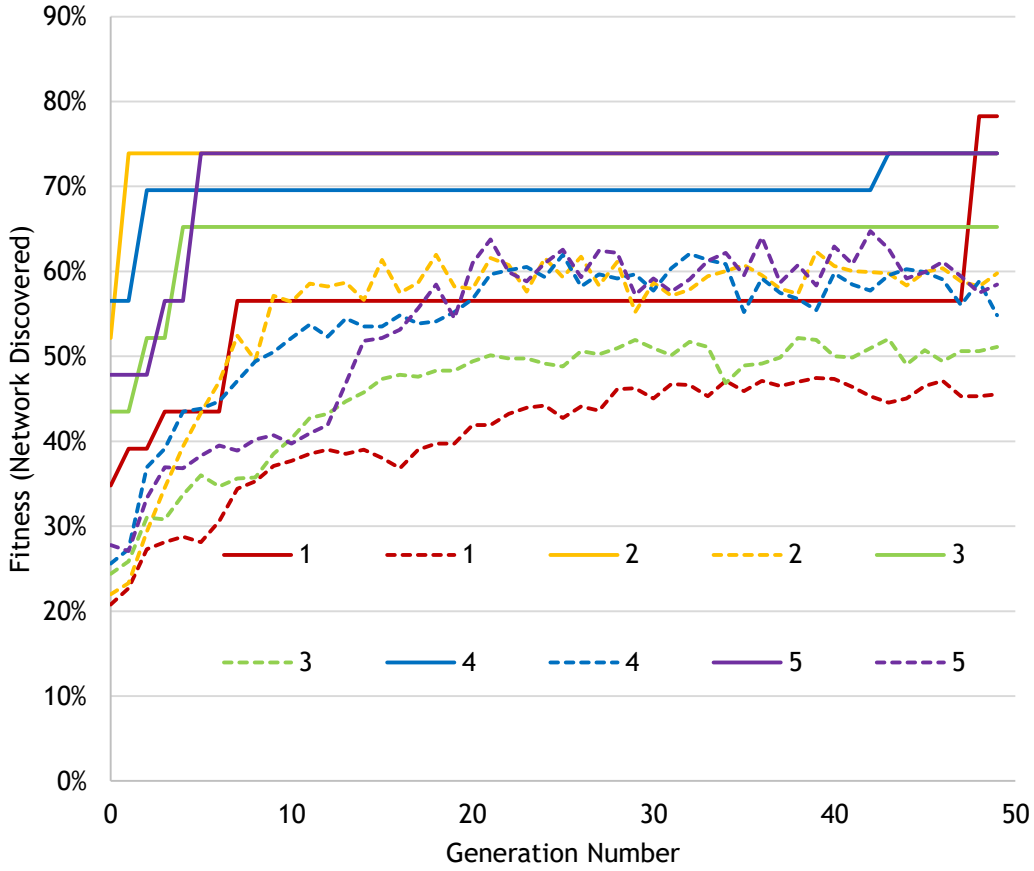
Example Enumeration Strategy

- Primary Search: **A.B±8.C±1.D**
- Secondary Search: **A.B.C.[0-255]**
- Root Node: own IP address



# Results

- Moderate success – 75% of network discovered



MISSOURI S&T

# Challenges and Lessons Learned

- Overhead time
- Dynamically building networks
- Complex attack strategies
- Simulation vs Emulation

Los Alamos NATIONAL LABORATORY EST. 1943

MISSOURI S&T

# Future Work

- Containerization
- Web application to interact with components
- Additional infrastructure support: AWS, Baremetal, etc

Los Alamos NATIONAL LABORATORY EST. 1943