# Shadow: Simple HPC for Systems Security Research

*Invited Talk*

*Kansas State University*

*September 25th, 2013*


Rob Jansen
U.S. Naval Research Laboratory
rob.g.jansen@nrl.navy.mil

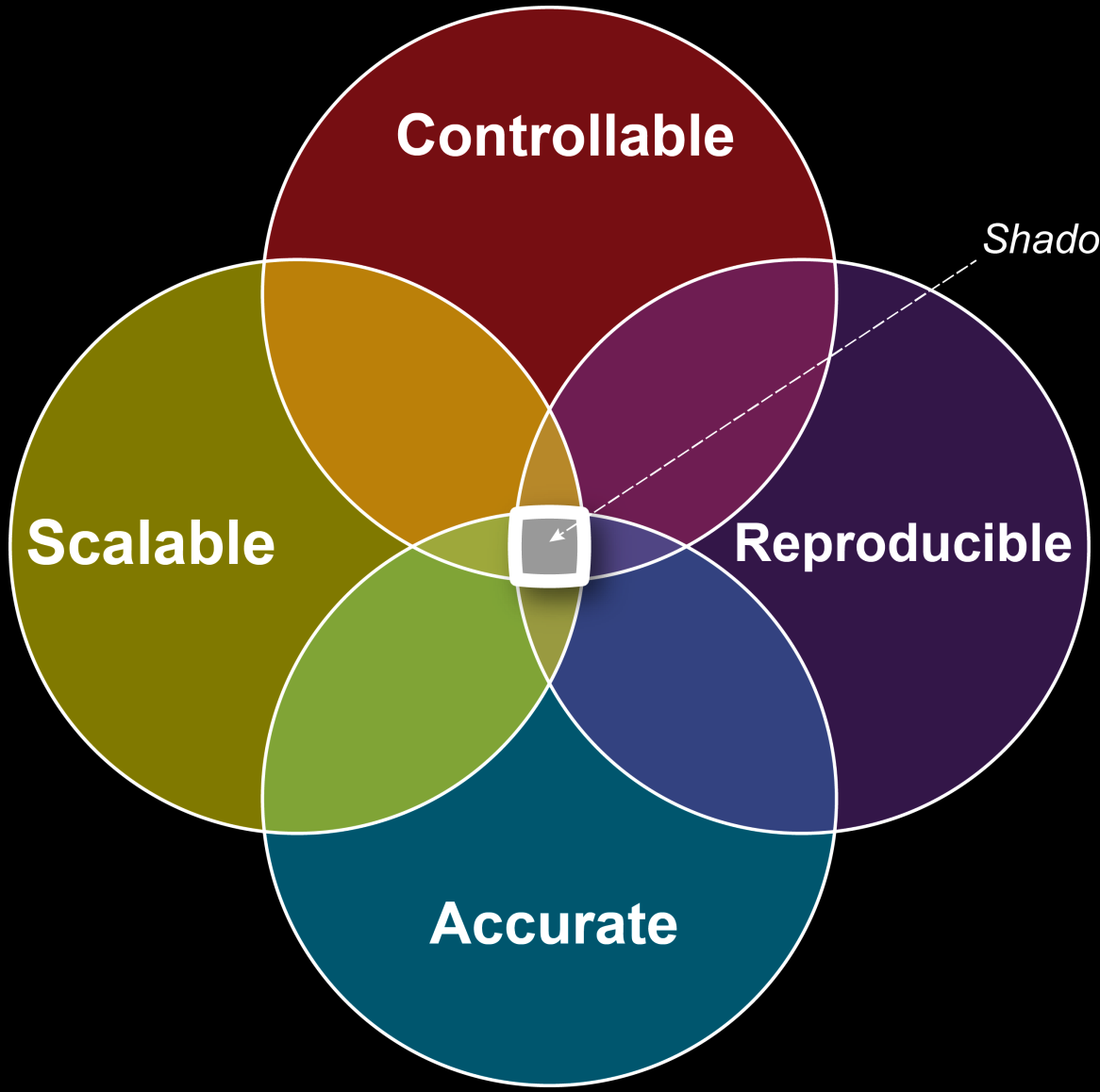
# Outline

- Experimentation Ideology
- Shadow and its Design
- Use case:
  - Overview: the Distributed Tor Network
  - Research: the Sniper Attack Against Tor

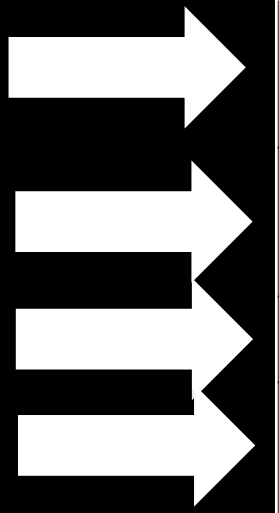
# Outline

- Experimentation Ideology
- Shadow and its Design
- Use case:
  - Overview: the Distributed Tor Network
  - Research: the Sniper Attack Against Tor

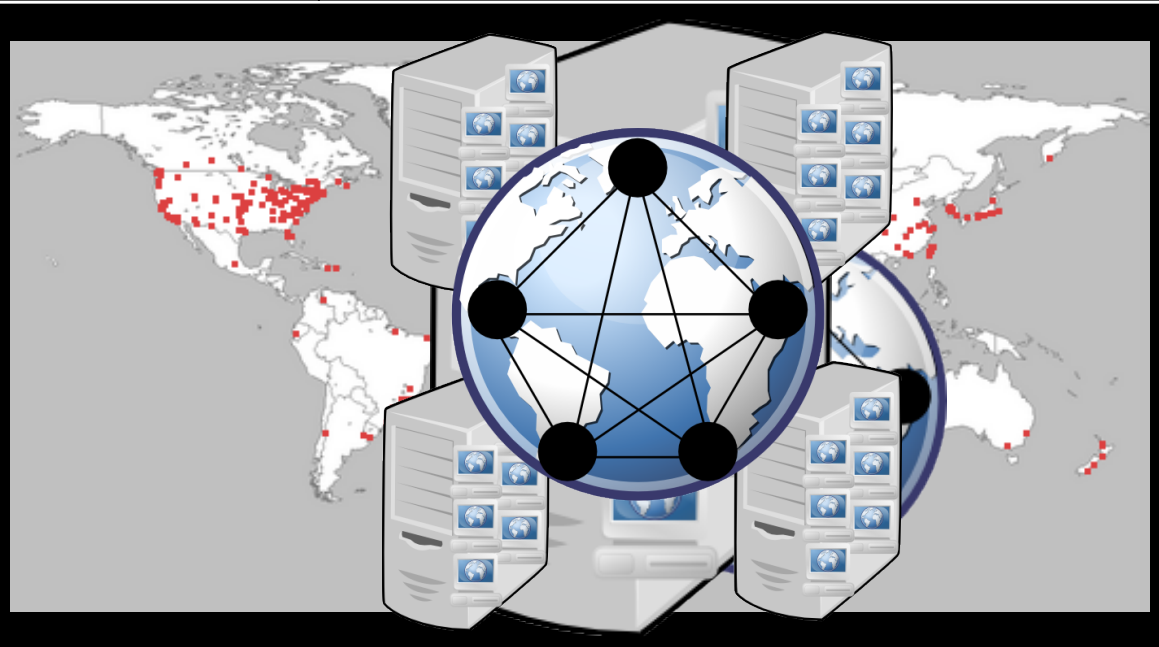
# Properties of Experimentation



# Network Research



| Approaches | Problems |
|---|---|
| Live Network | Hard to manage, lengthy deployment, security risks |
| PlanetLab | Hard to manage, bad at modeling, not scalable |
| Simulation | Not generalizable, inaccurate |
| Emulation | Large overhead, kernel complexities |



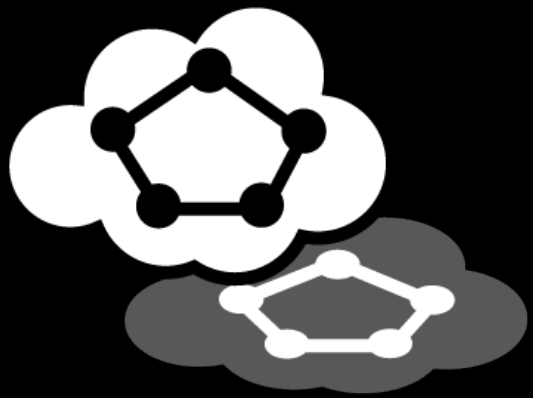
# Testbed Trade-offs

| | Controllable | Reproducible | Scalable | Accuracy | Convenient |
|---|---|---|---|---|---|
| Live Network | | | X | X | |
| PlanetLab | | | | ? | |
| Simulation | X | X | X | | X |
| Emulation | X | | | | X |
| Shadow | X | X | X | ? | X |

# Outline

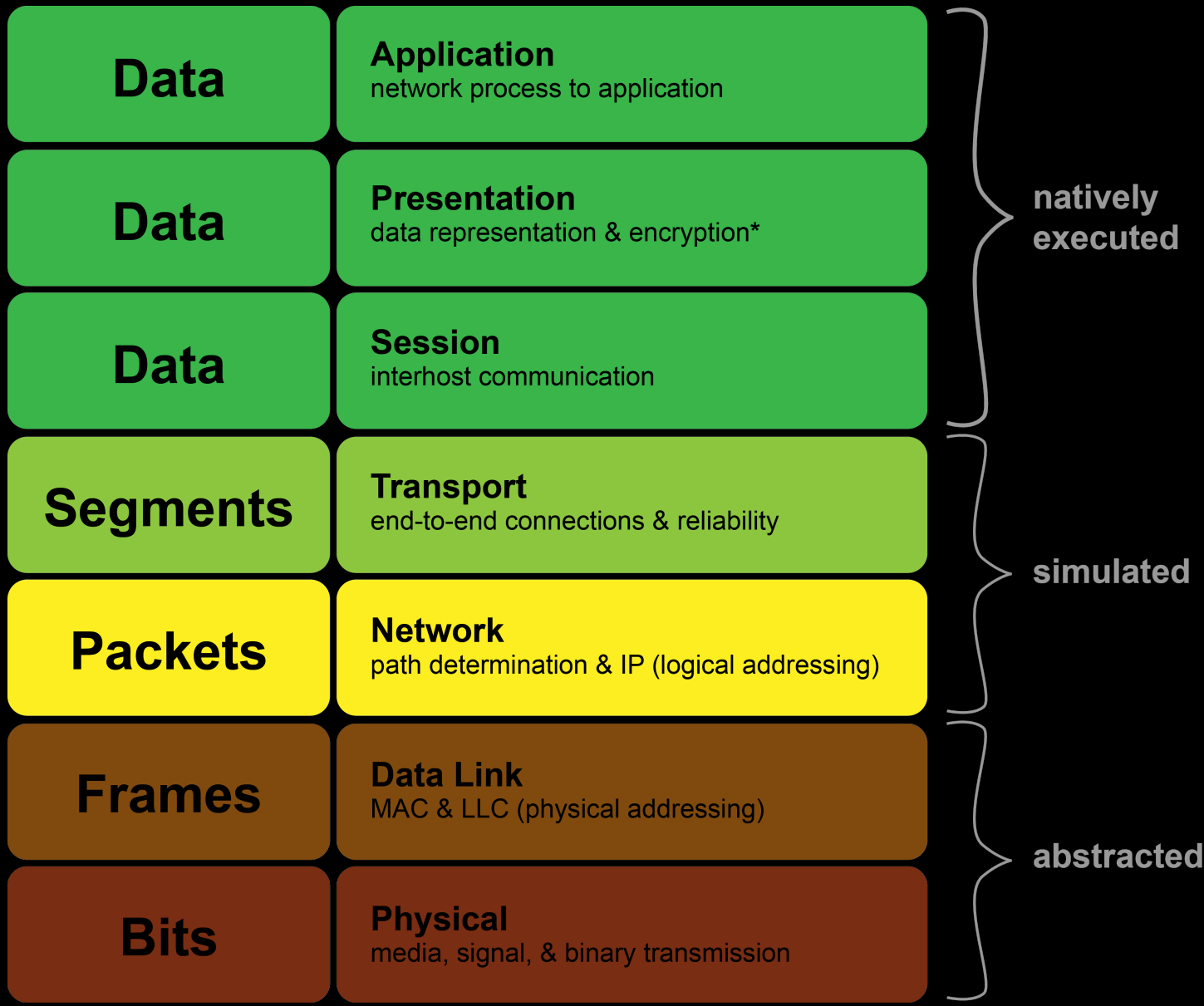
- Experimentation Ideology
- Shadow and its Design
- Use case:
  - Overview: the Distributed Tor Network
  - Research: the Sniper Attack Against Tor

# What is Shadow?

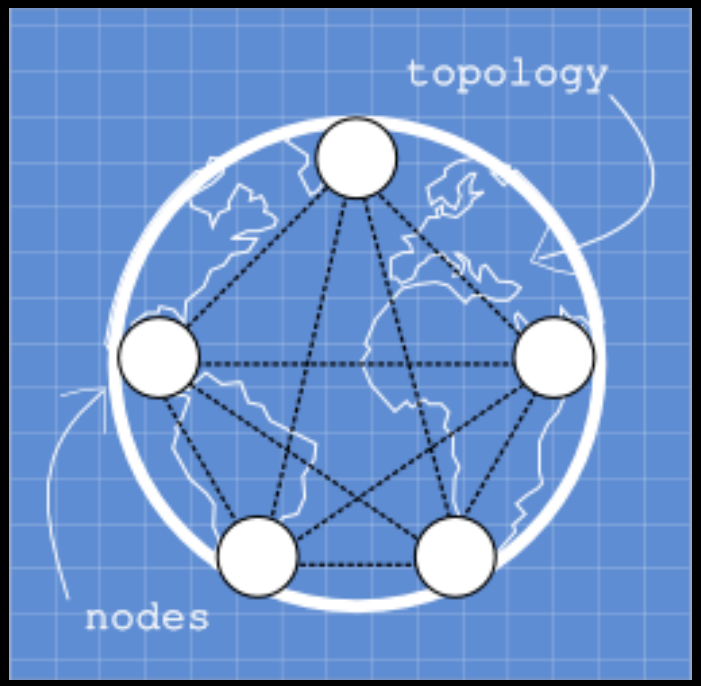


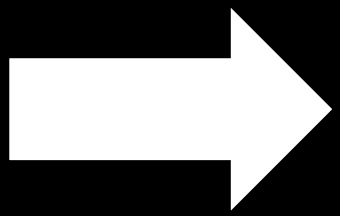
- Discrete event network simulator
- Runs real applications without modification
- Simulates time, network, crypto, CPU
- Models routing, latency, bandwidth
- Single Linux box without root privileges

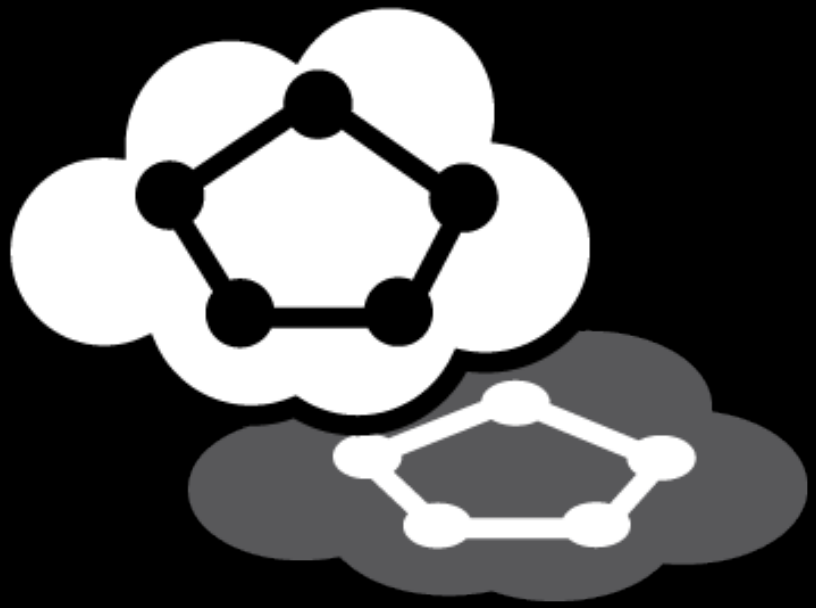
# Shadow's Capabilities



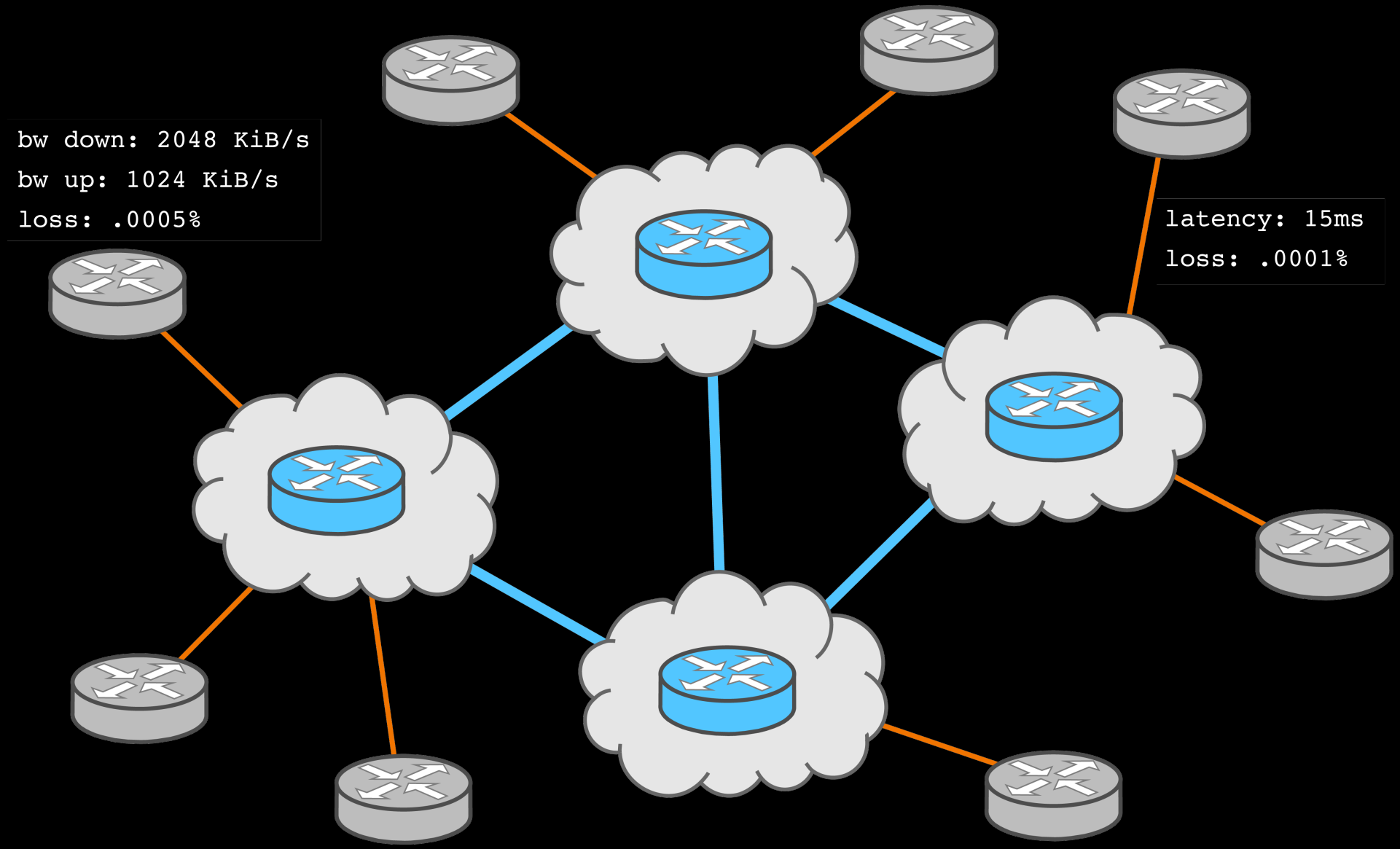
# Bootstrapping Shadow



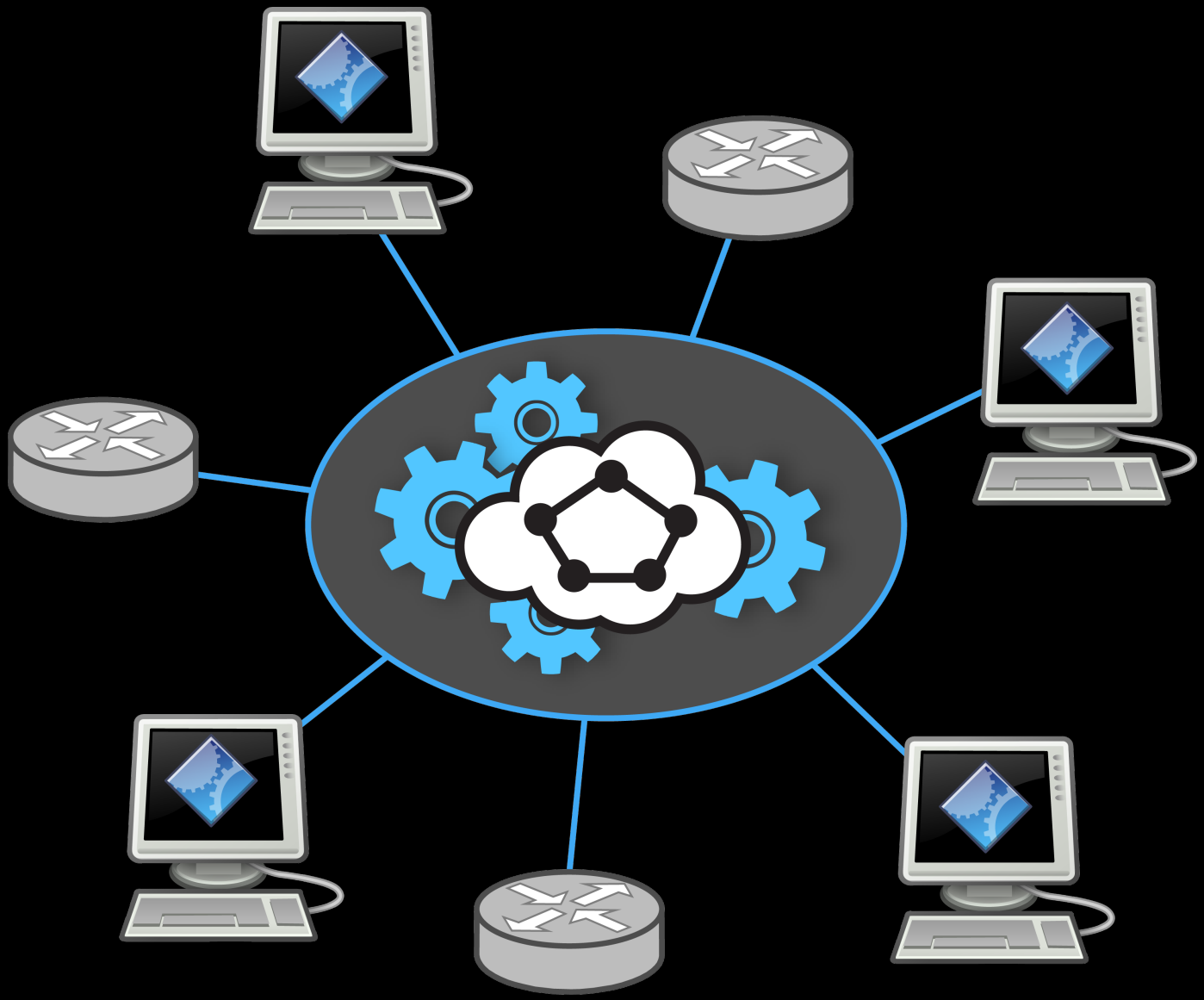


# Virtual Network Configuration

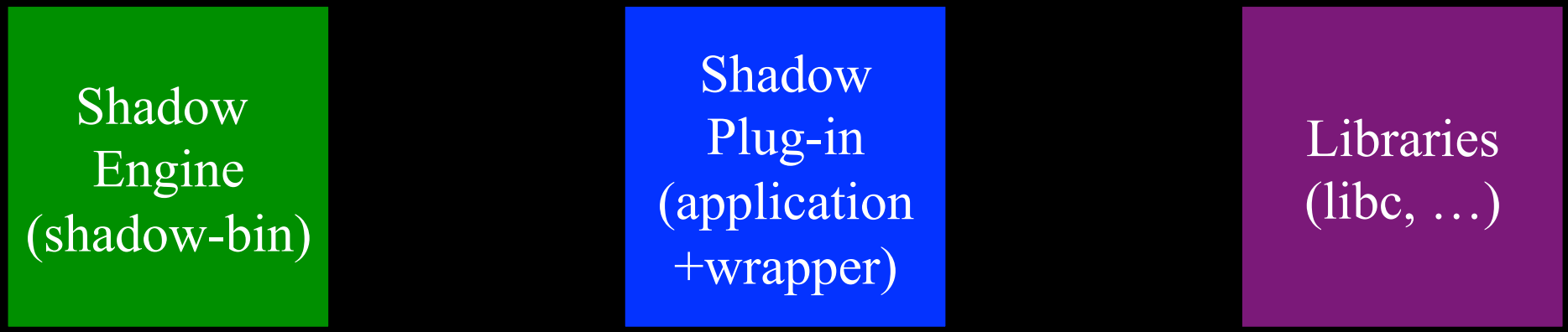


# Virtual Host Configuration

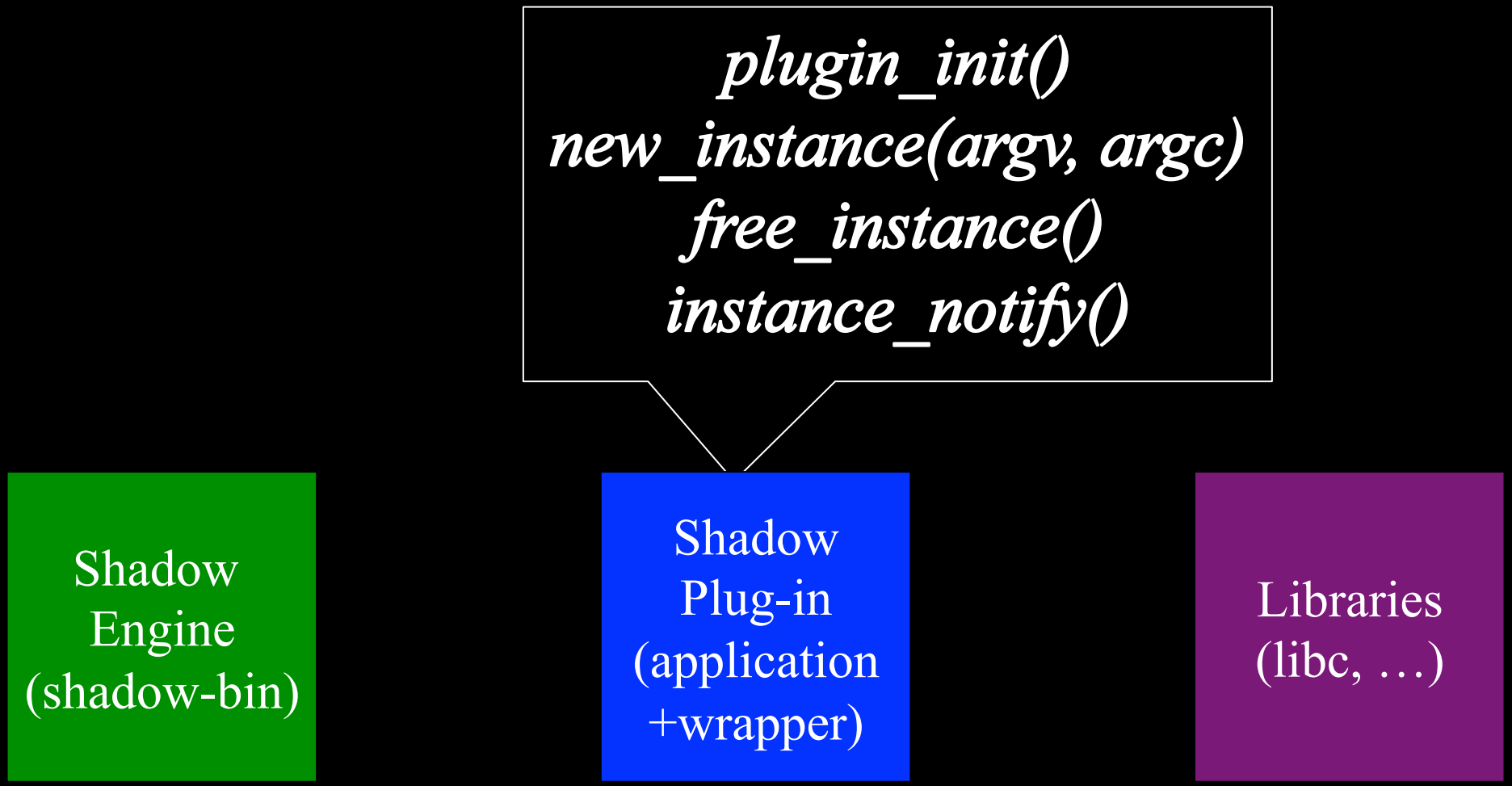
# Simulation Engine



# Program Layout

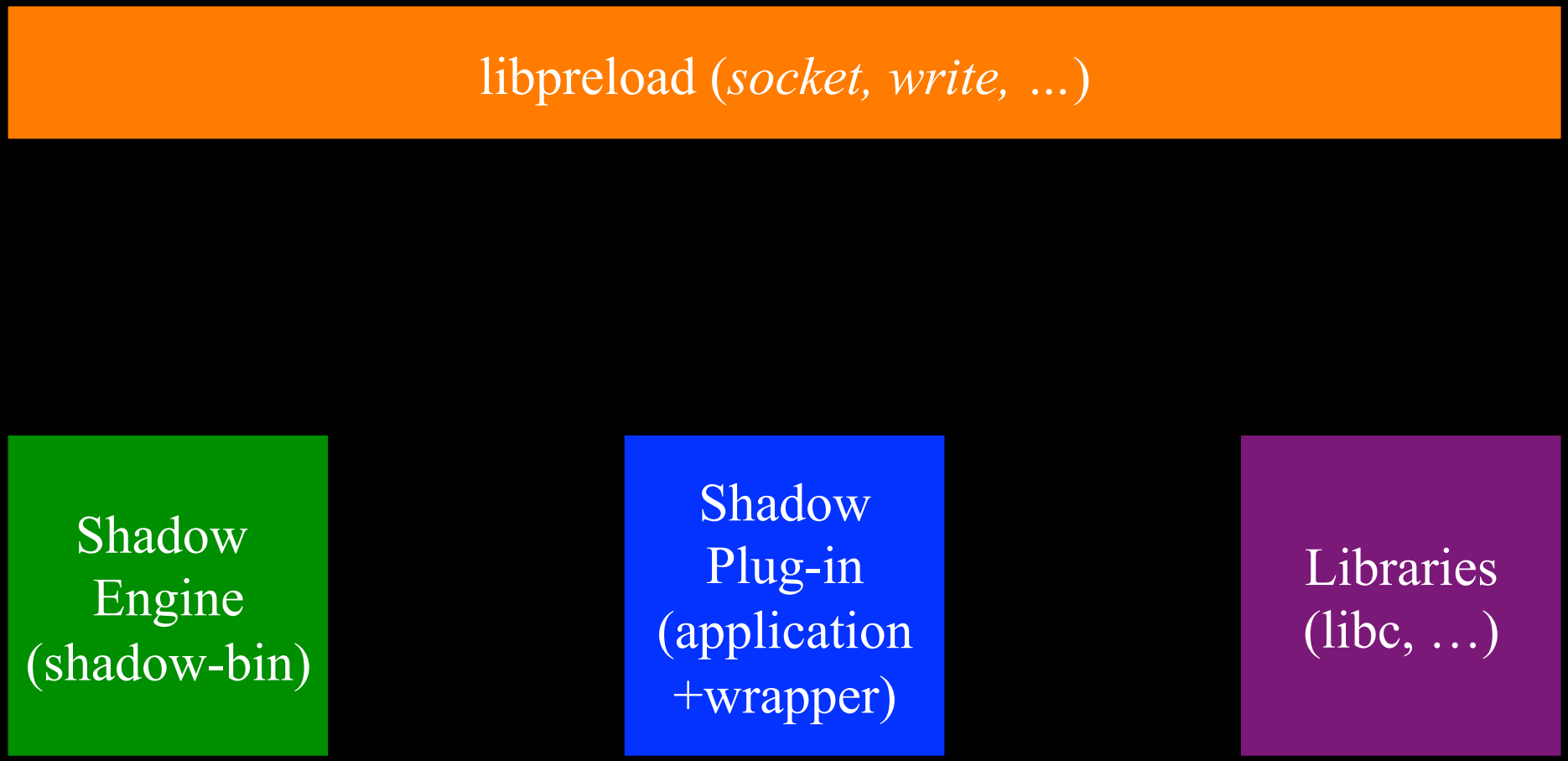


# Plug-in Wrapper Hooks



# Function Interposition

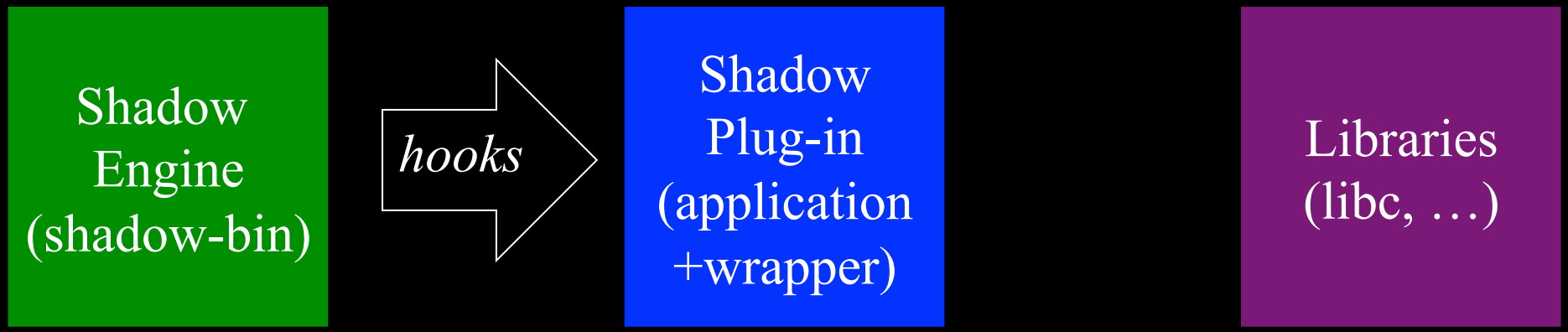
LD_PRELOAD=/home/rob/libpreload.so



# Function Interposition

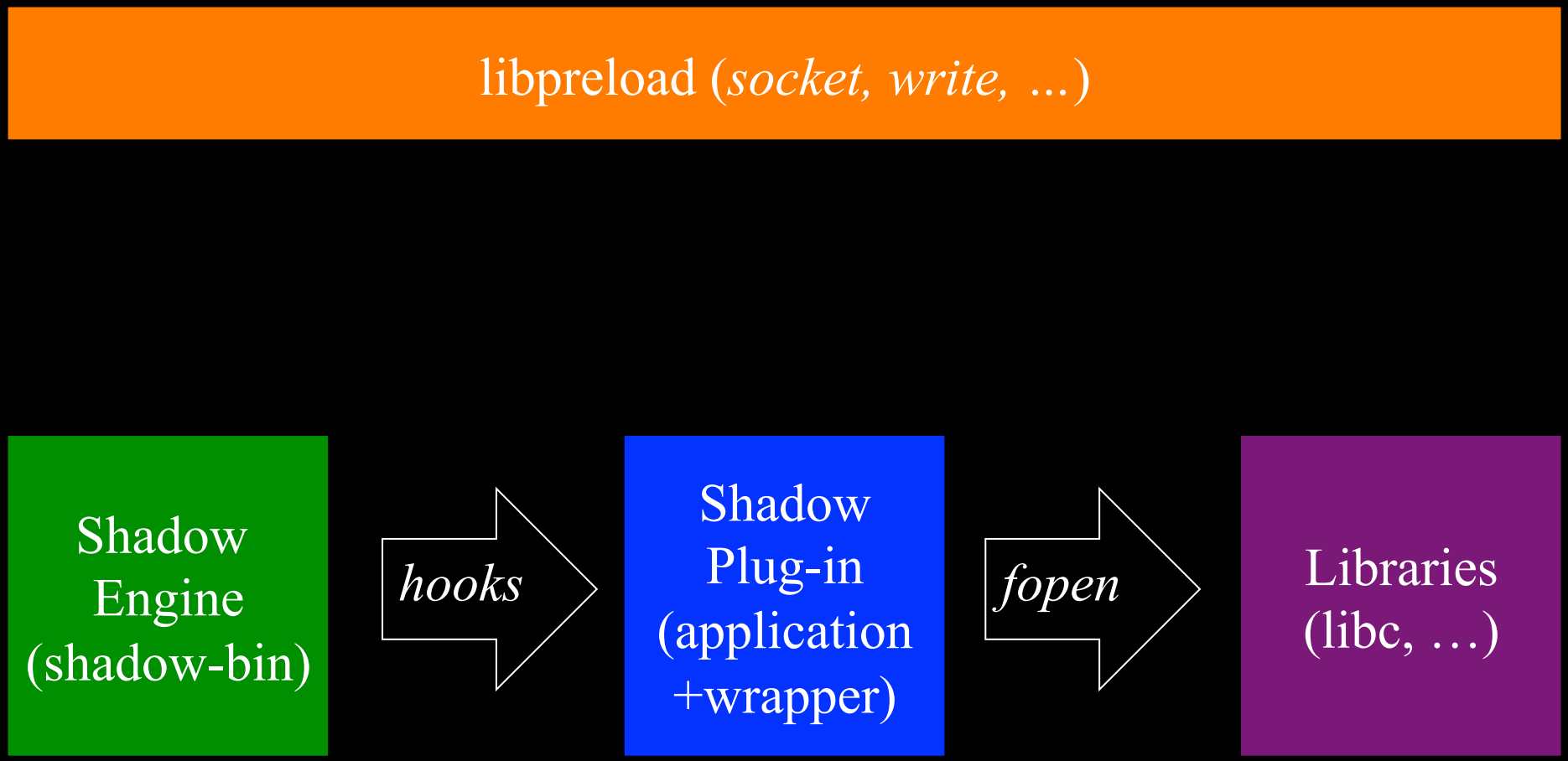
LD_PRELOAD=/home/rob/libpreload.so

libpreload (*socket, write, …*)



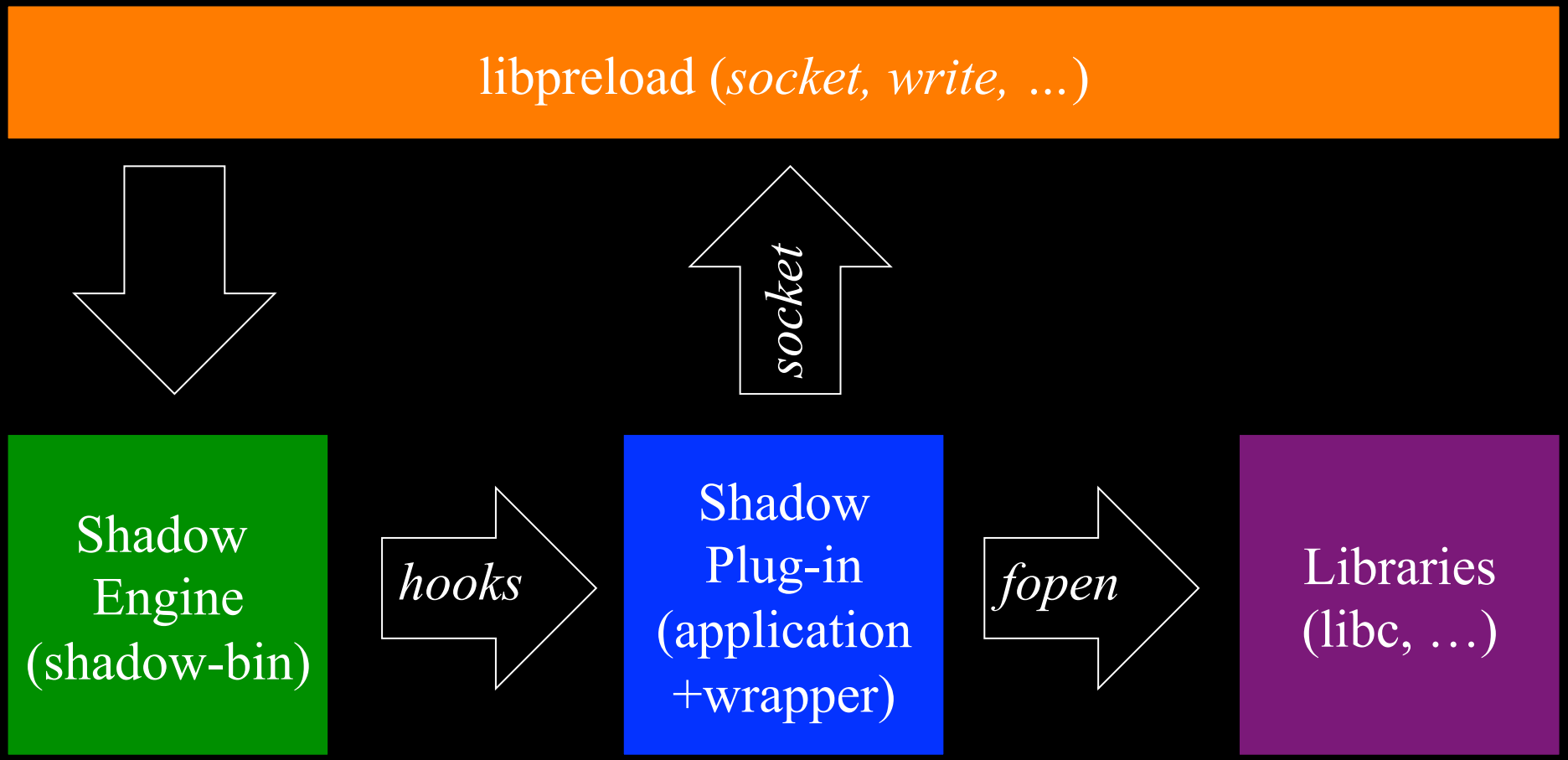
# Function Interposition

LD_PRELOAD=/home/rob/libpreload.so



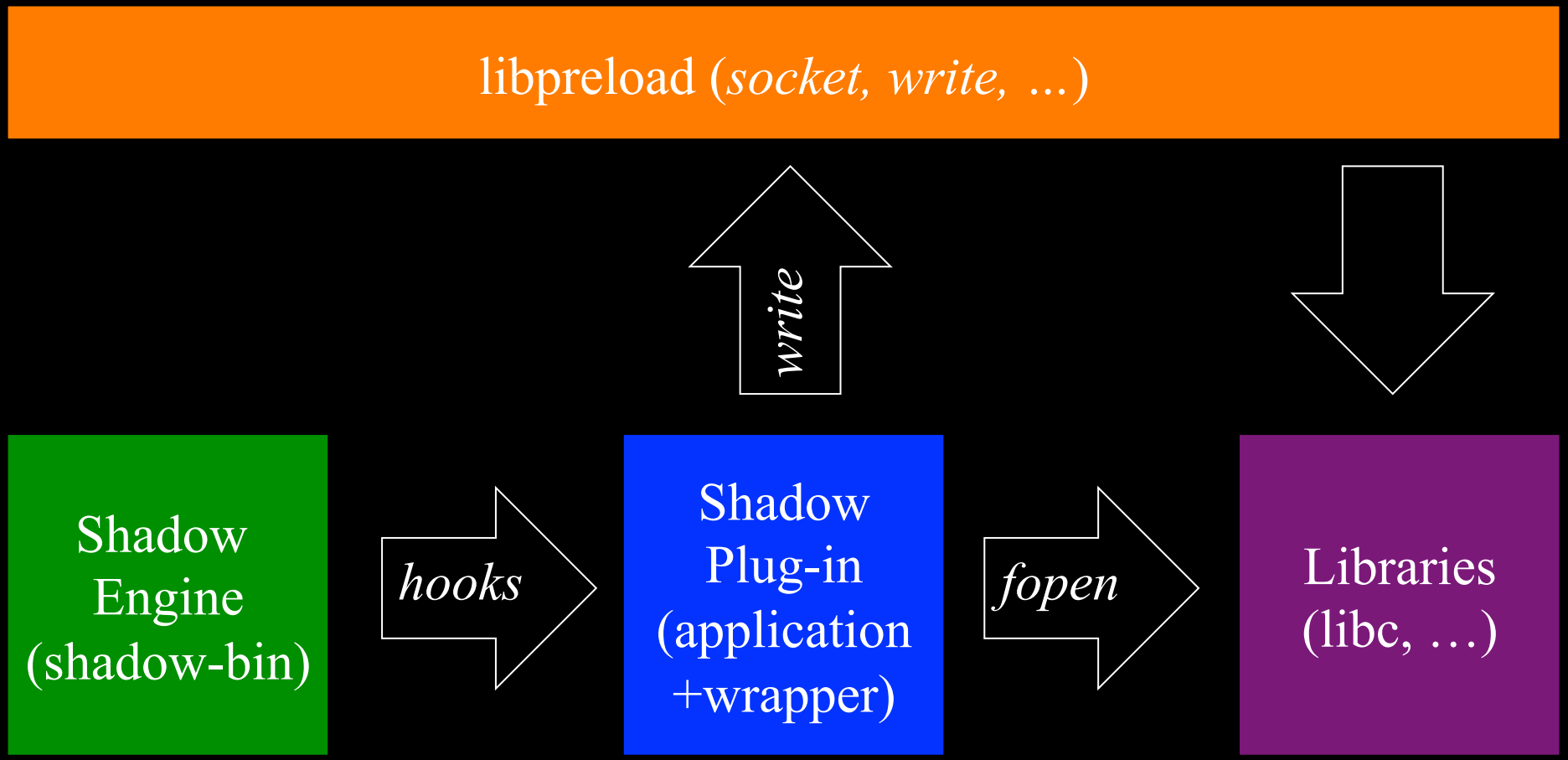
# Function Interposition

LD_PRELOAD=/home/rob/libpreload.so



# Function Interposition

LD_PRELOAD=/home/rob/libpreload.so

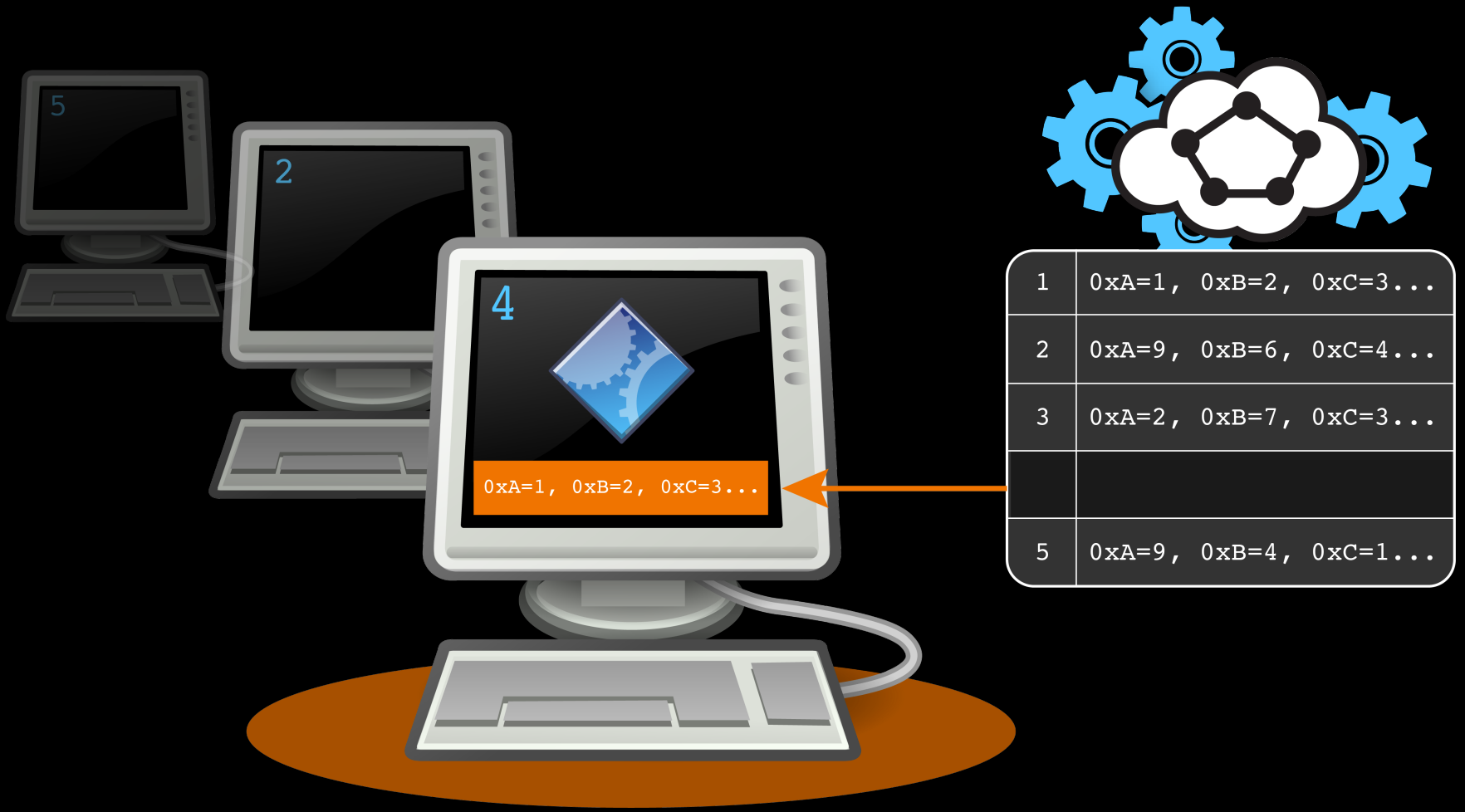


# Virtual Context Switching

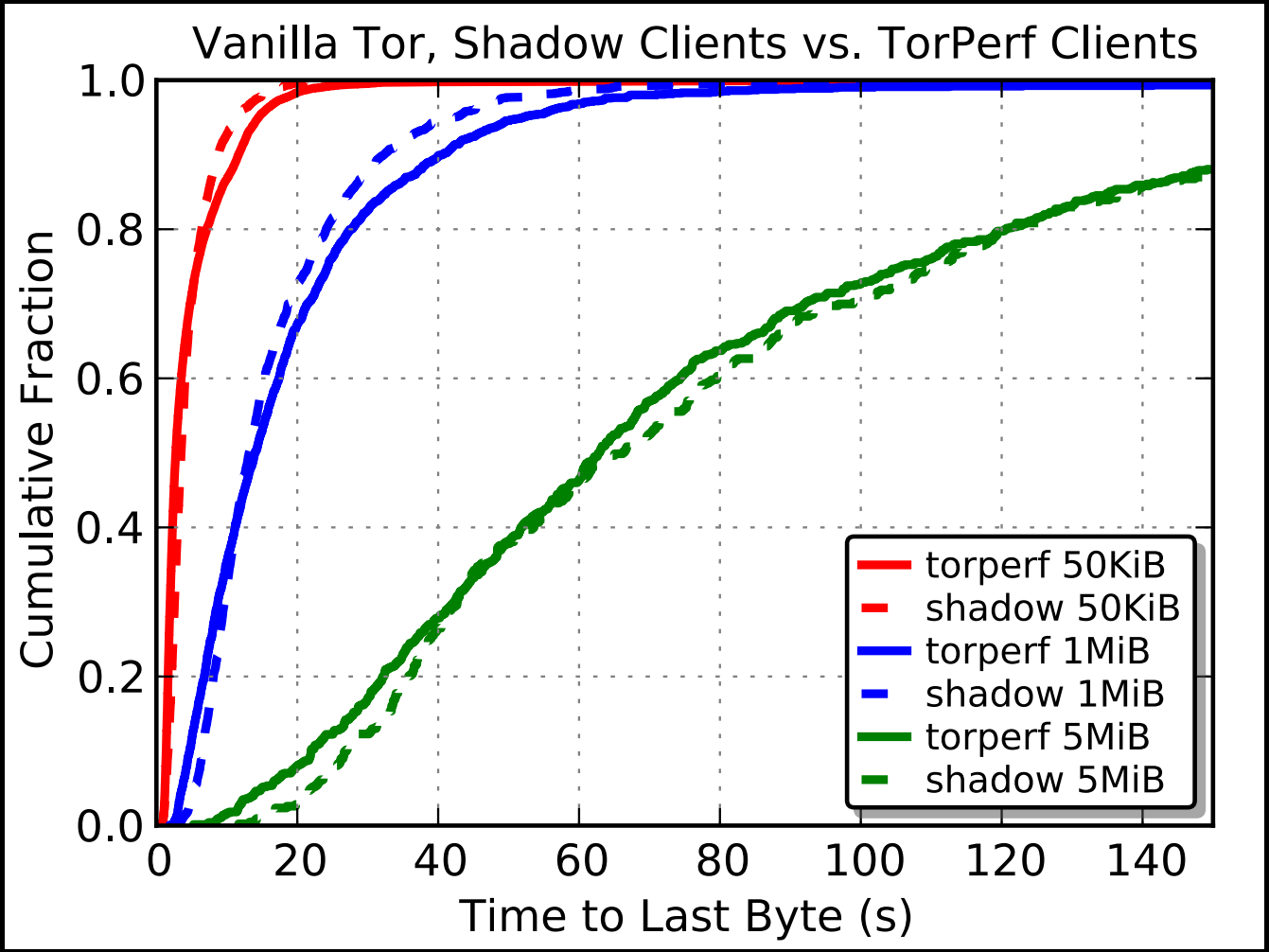

| | |
|---|---|
| 1 | 0xA=1, 0xB=2, 0xC=3... |
| 2 | 0xA=1, 0xB=2, 0xC=3... |
| 3 | 0xA=1, 0xB=2, 0xC=3... |
| 4 | 0xA=1, 0xB=2, 0xC=3... |
| 5 | 0xA=1, 0xB=2, 0xC=3... |

Clang/LLVM
(custom pass)

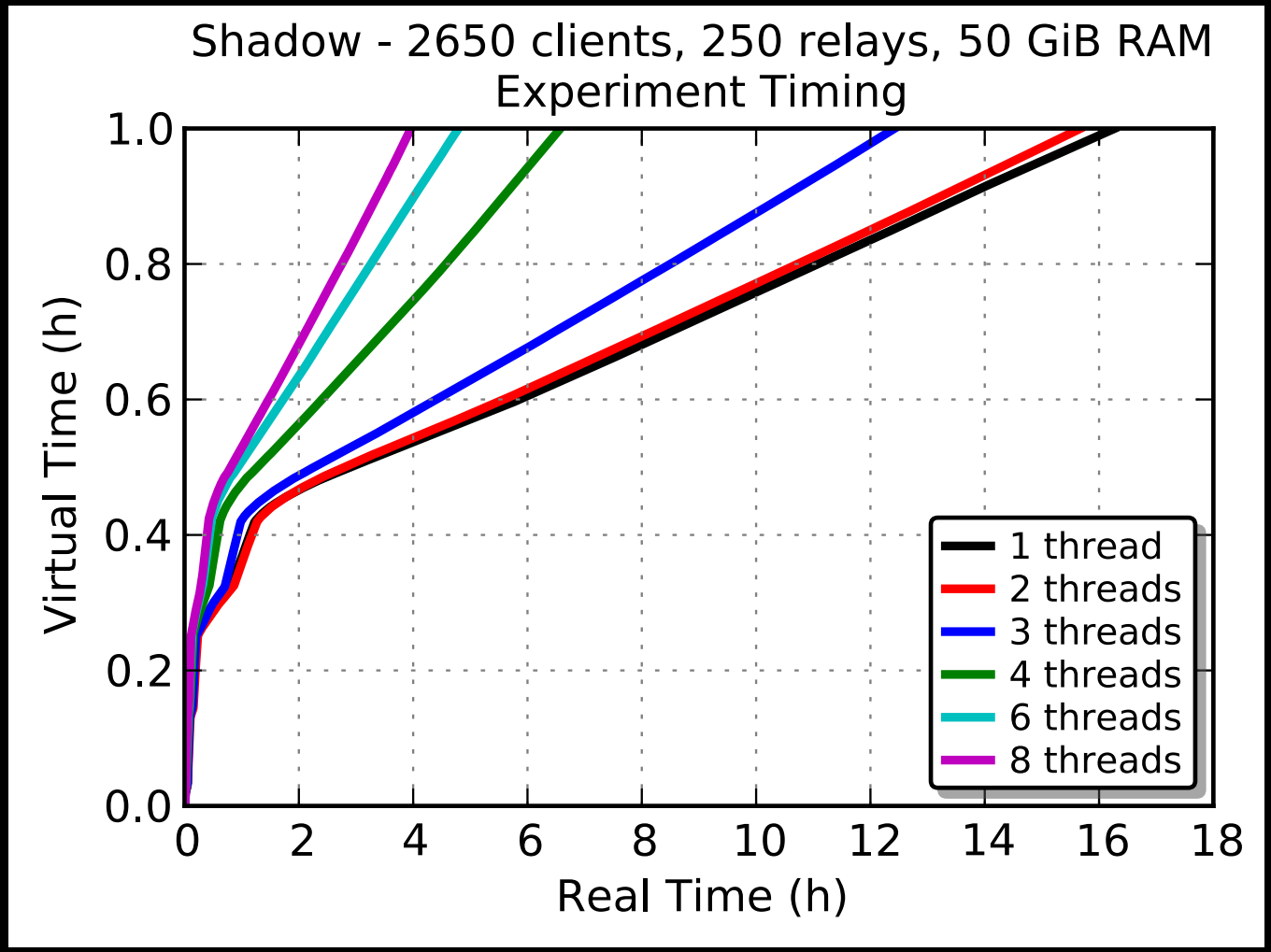
# Virtual Context Switching



# Shadow-Tor's Accuracy



# Shadow-Tor's Scalability

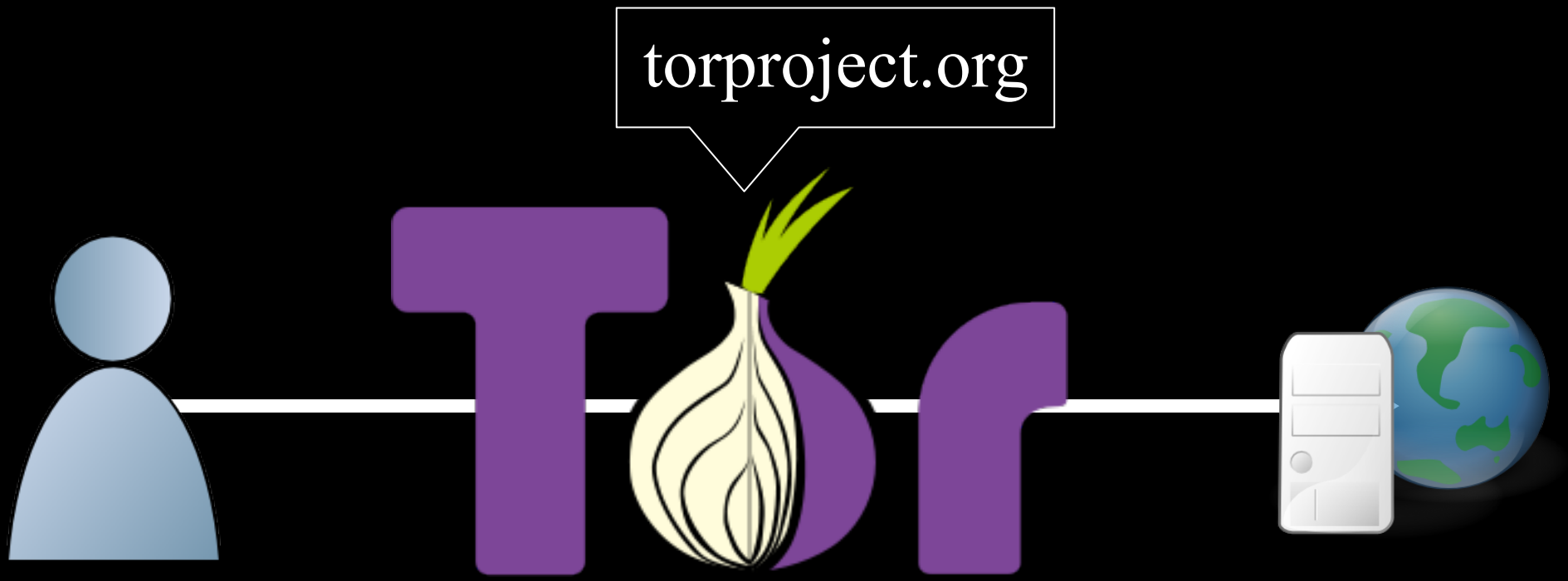



Memory:
20-30 MiB
per virtual
Tor host

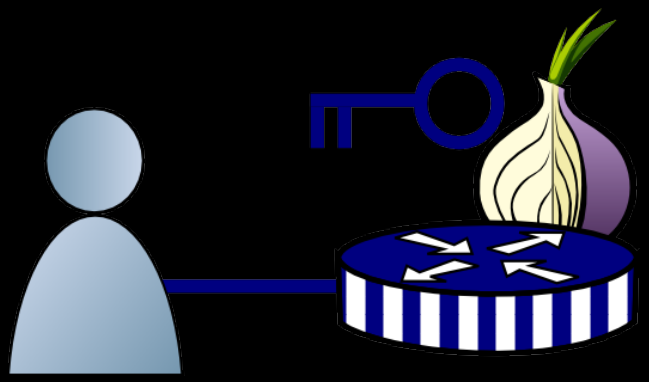
# Outline

- Experimentation Ideology
- Shadow and its Design
- Use case:
  - Overview: the Distributed Tor Network
  - Research: the Sniper Attack Against Tor

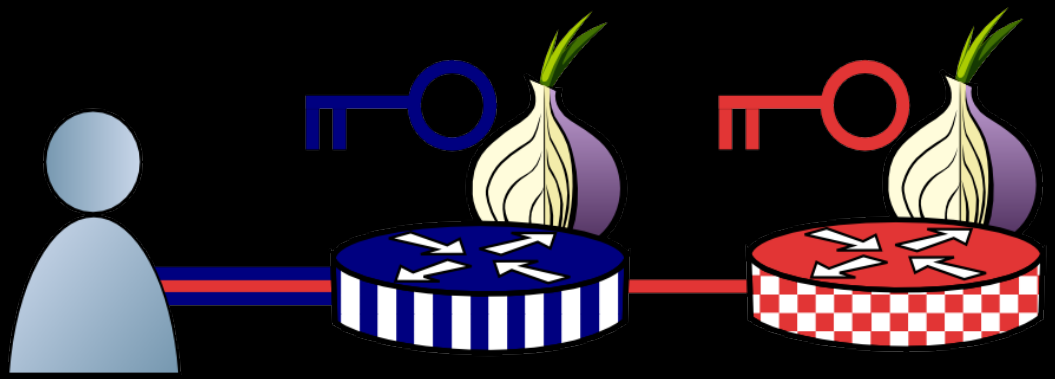
# The Tor Anonymity Network



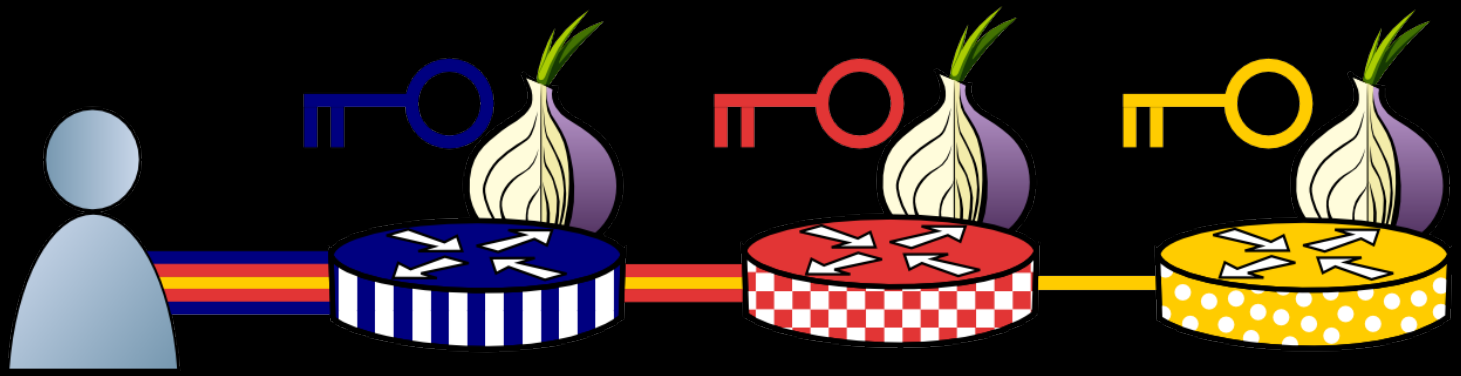
# How Tor Works



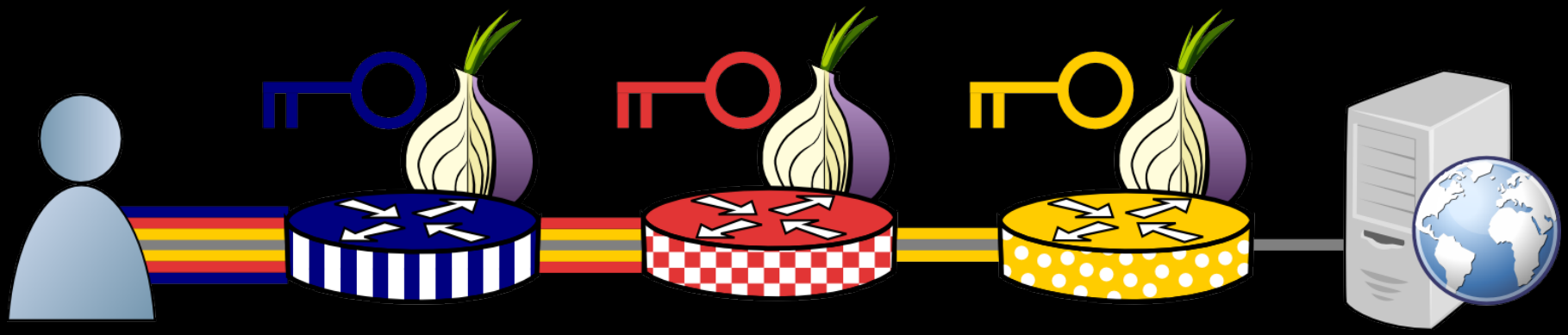
# How Tor Works



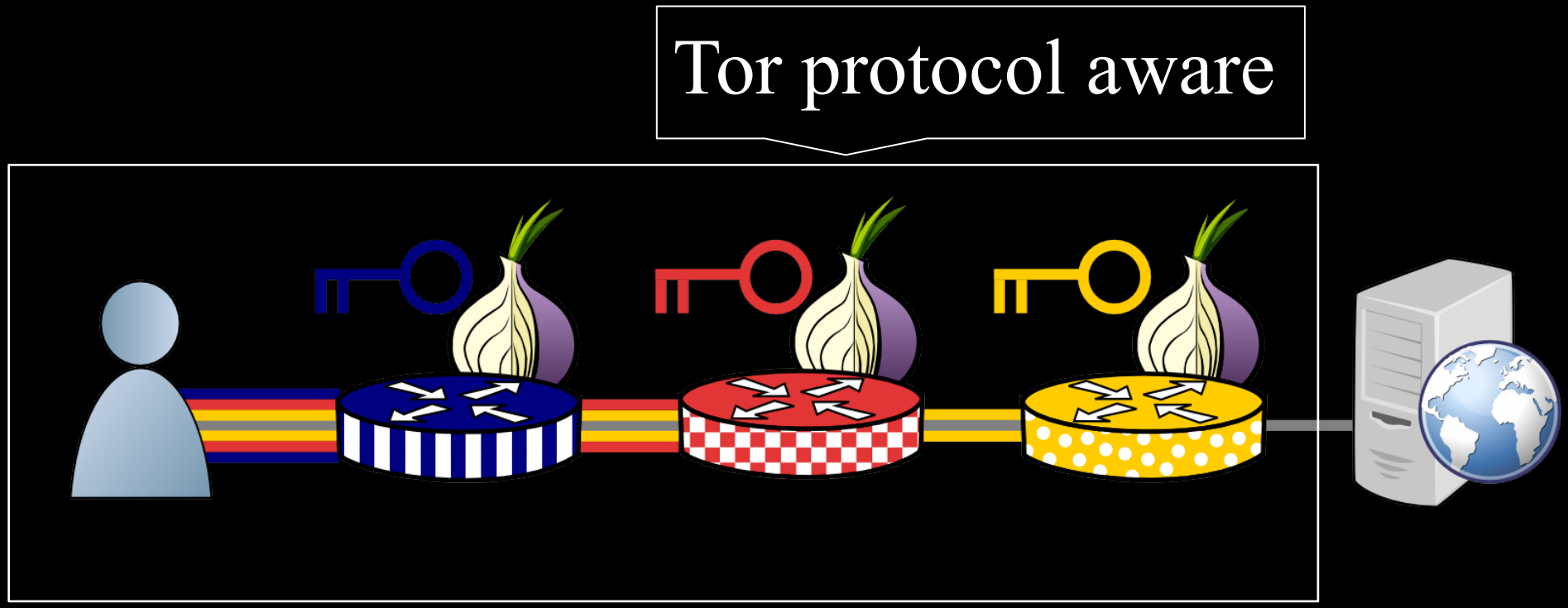
# How Tor Works



# How Tor Works



# How Tor Works

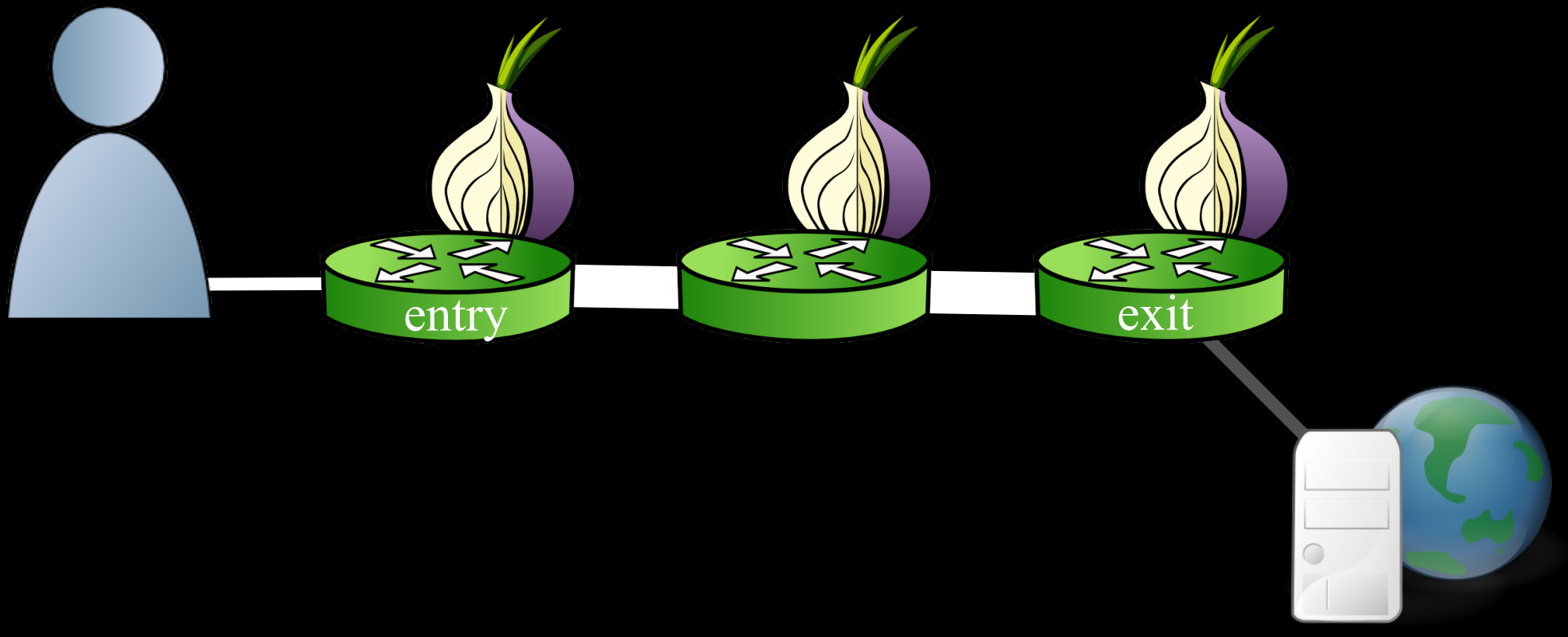


# Outline

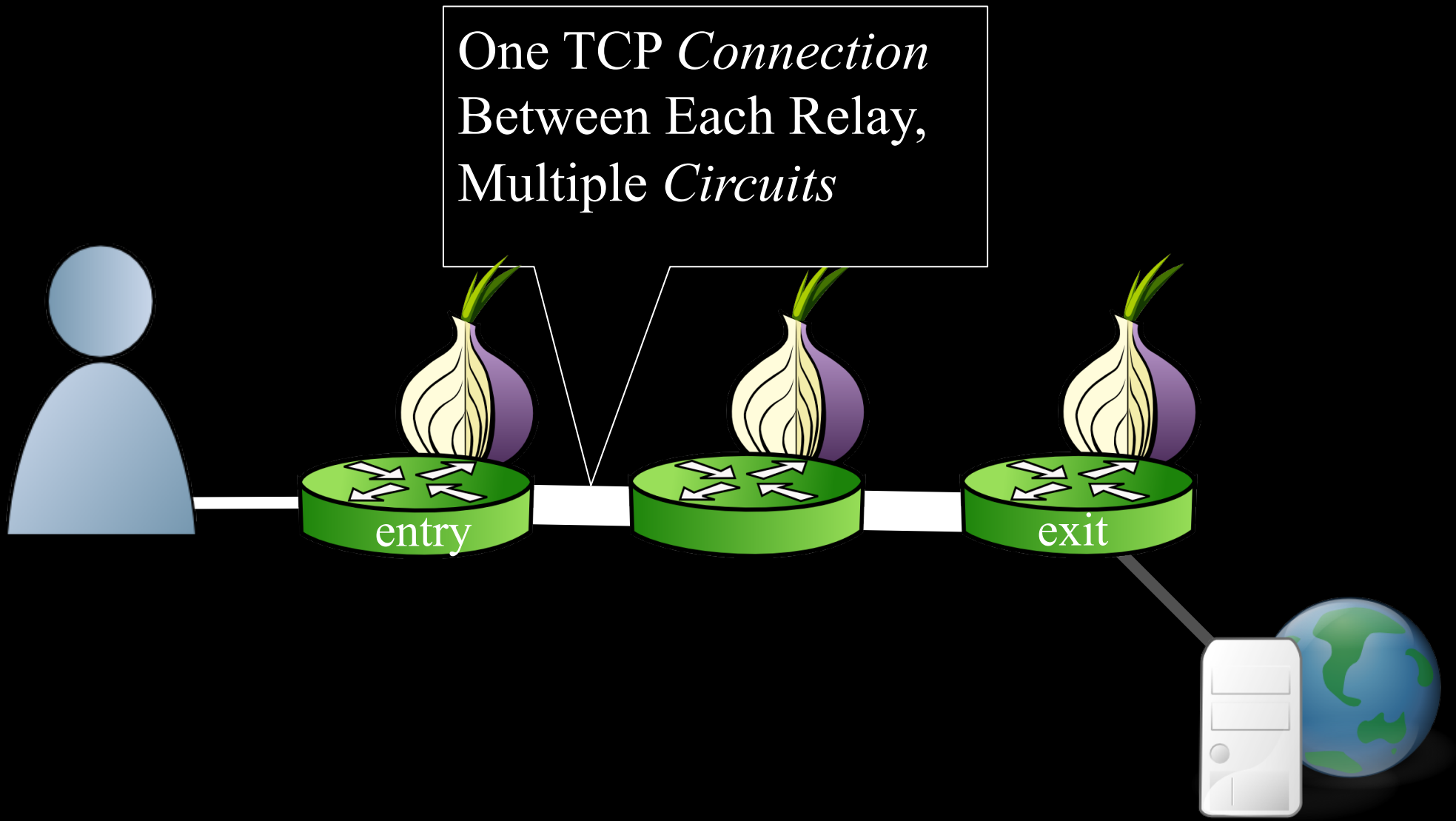
- Experimentation Ideology
- Shadow and its Design
- Use case:
  - Overview: the Distributed Tor Network
  - *Research: the Sniper Attack Against Tor

*Joint with Aaron Johnson, Florian Tschorsch, Björn Scheuermann

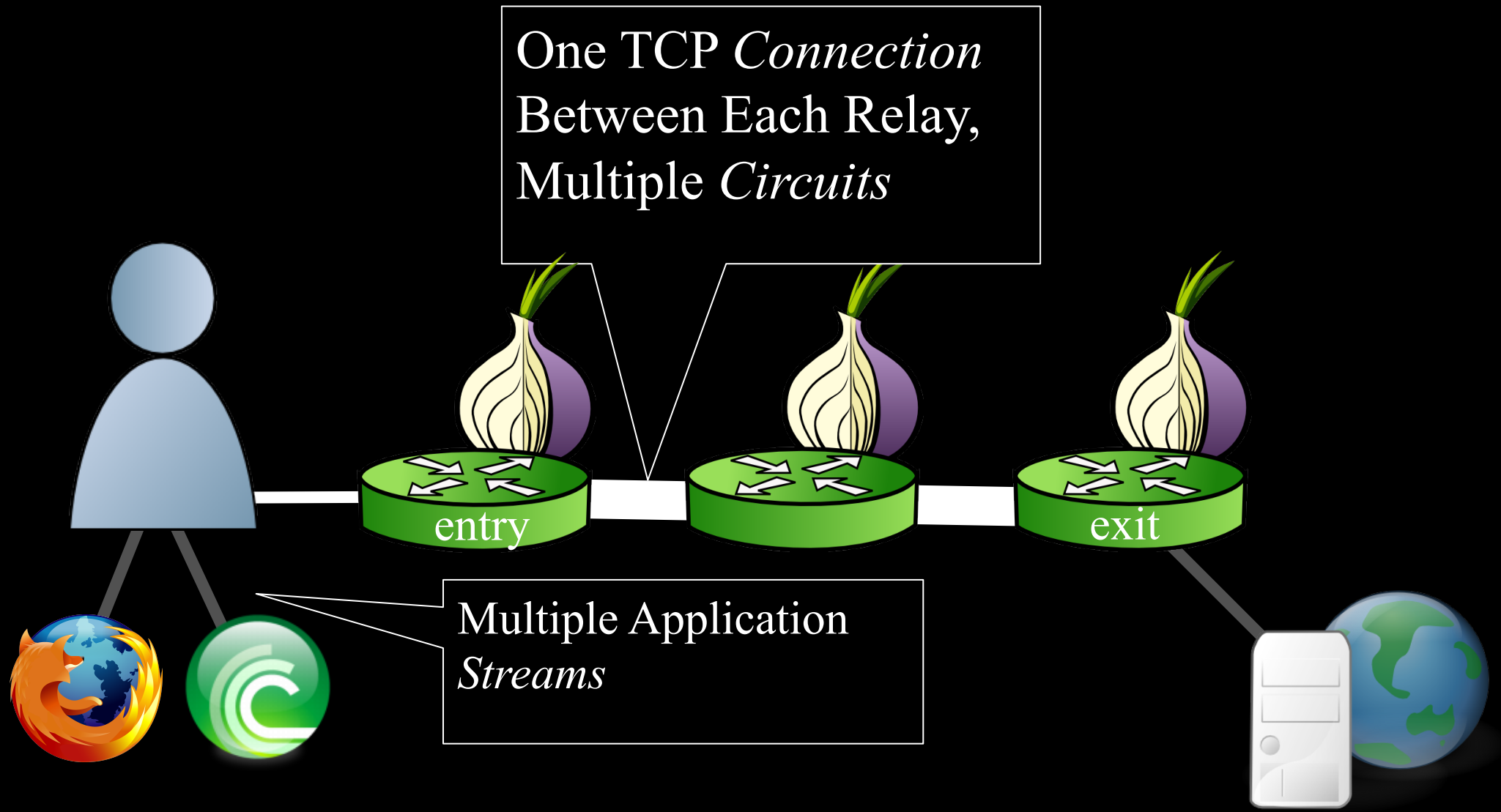
# Tor Flow Control



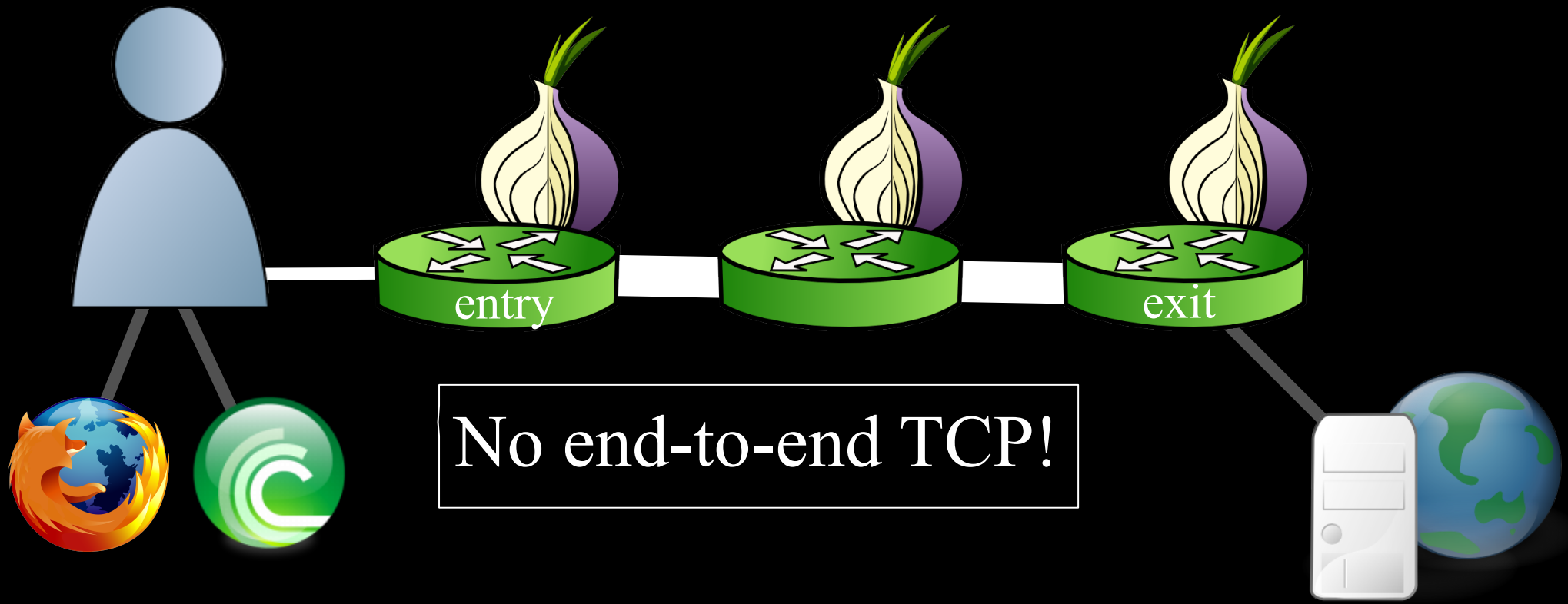
# Tor Flow Control



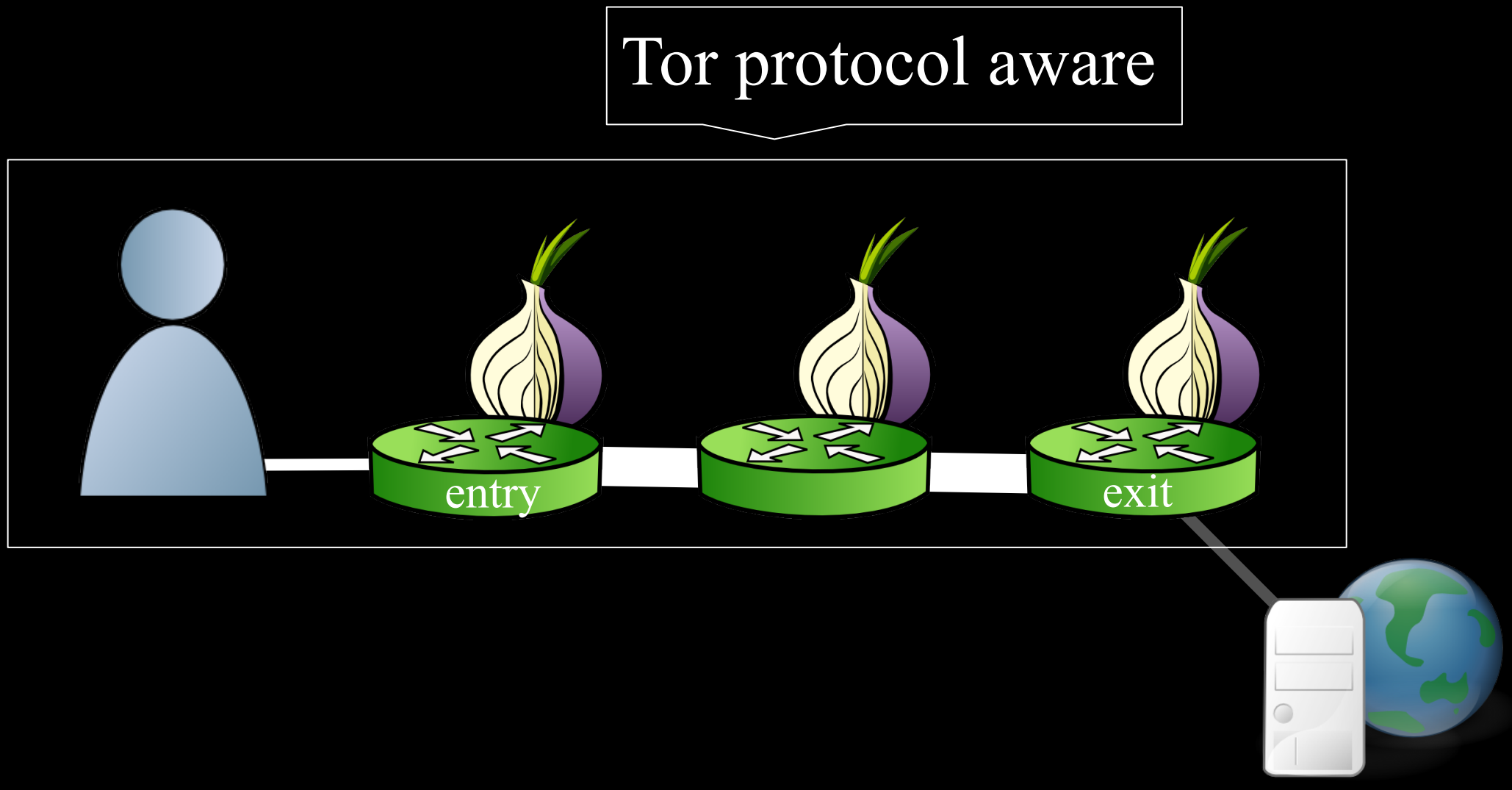
# Tor Flow Control



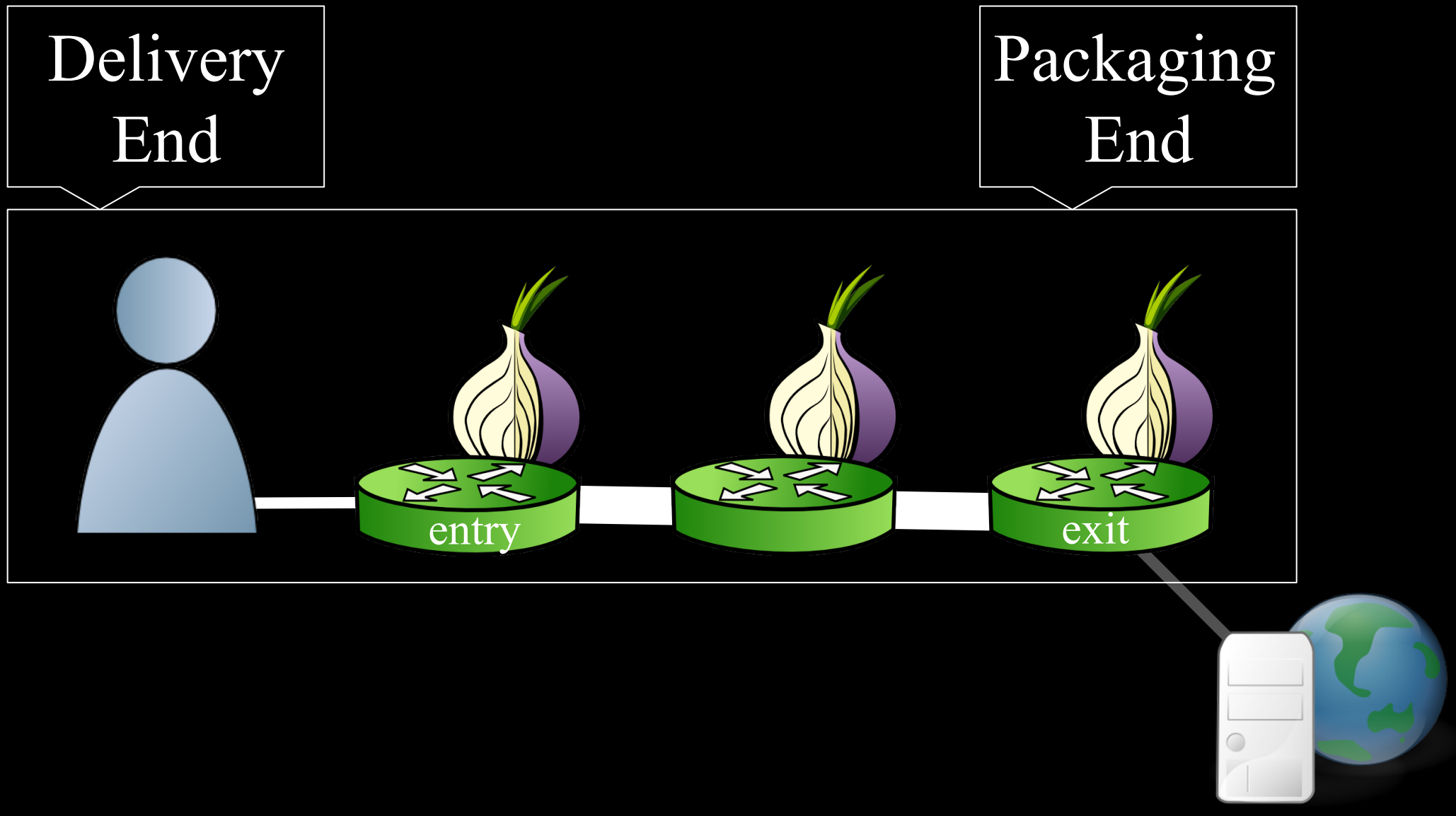
# Tor Flow Control



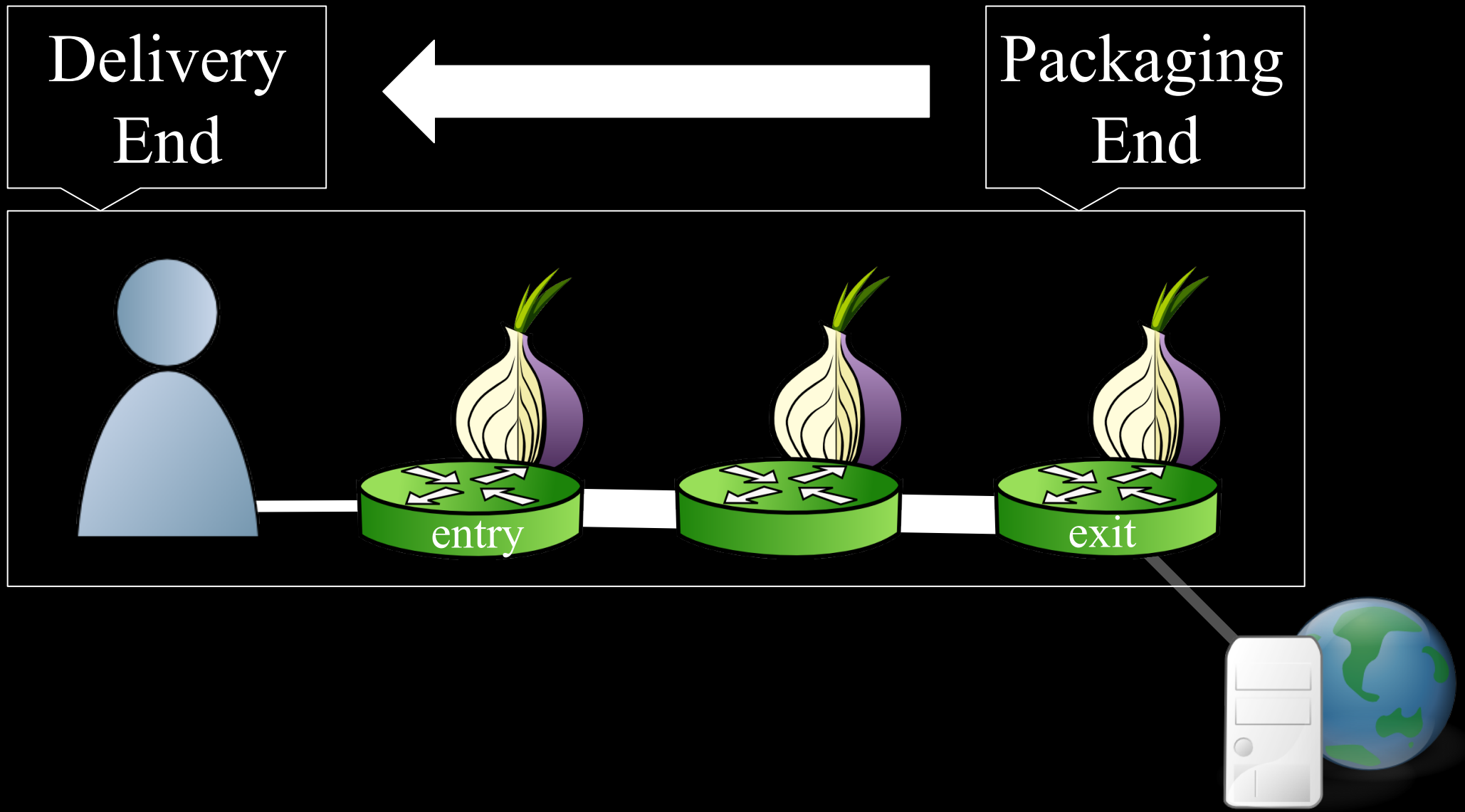
# Tor Flow Control



# Tor Flow Control



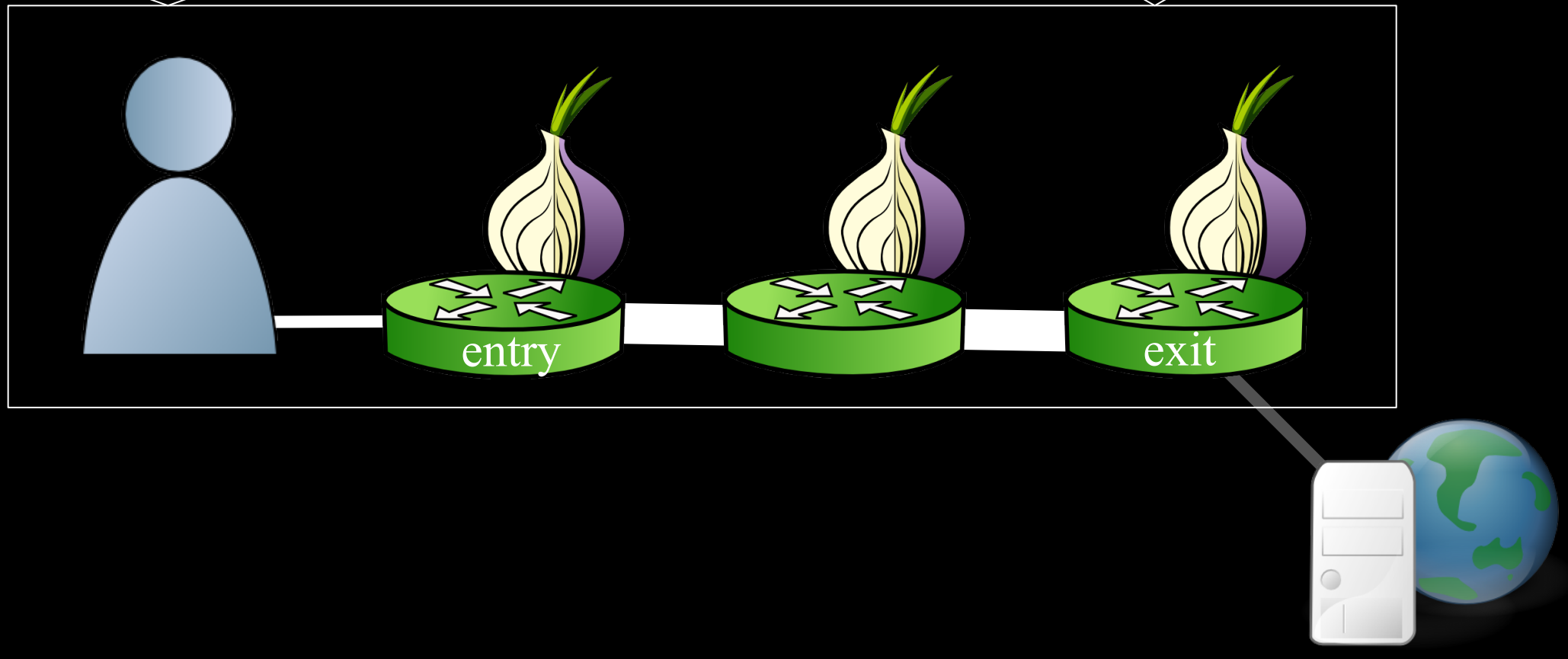
# Tor Flow Control



# Tor Flow Control

SENDME Signal
Every 100 Cells

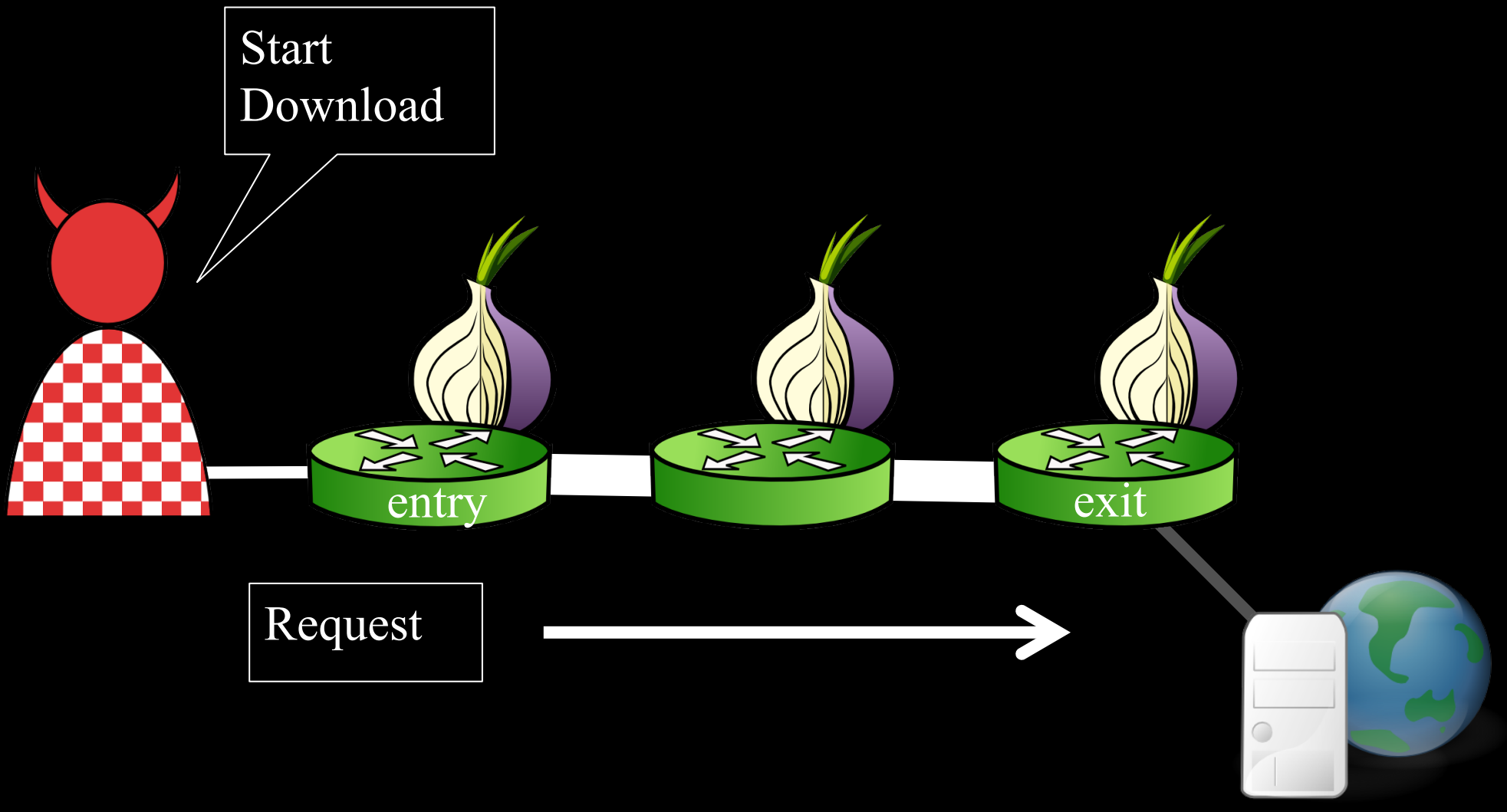
1000 Cell
Limit



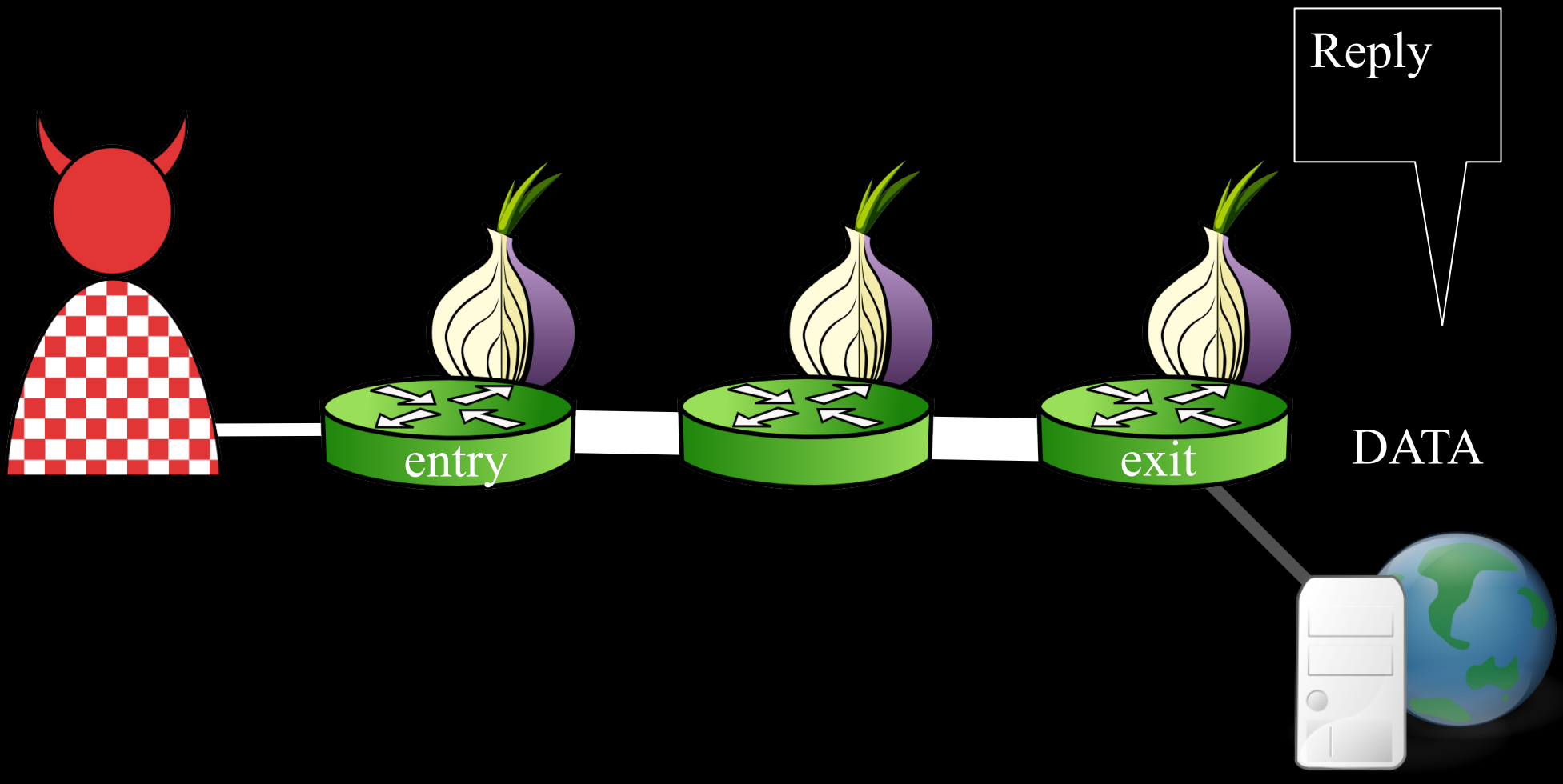
# The Sniper Attack

- Low-cost memory consumption attack
- Disables arbitrary Tor relays
- Anonymous if launched through Tor

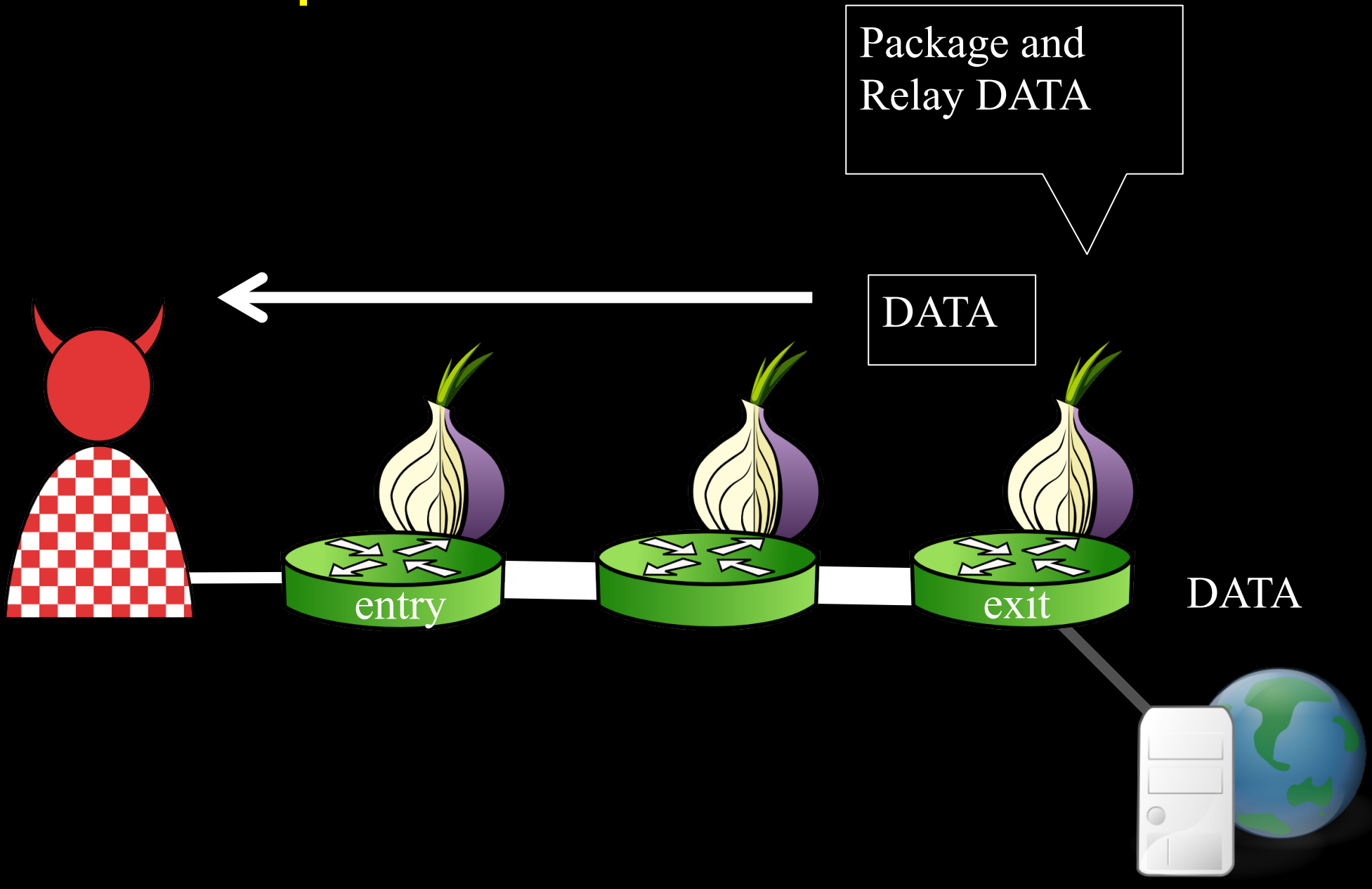
# The Sniper Attack



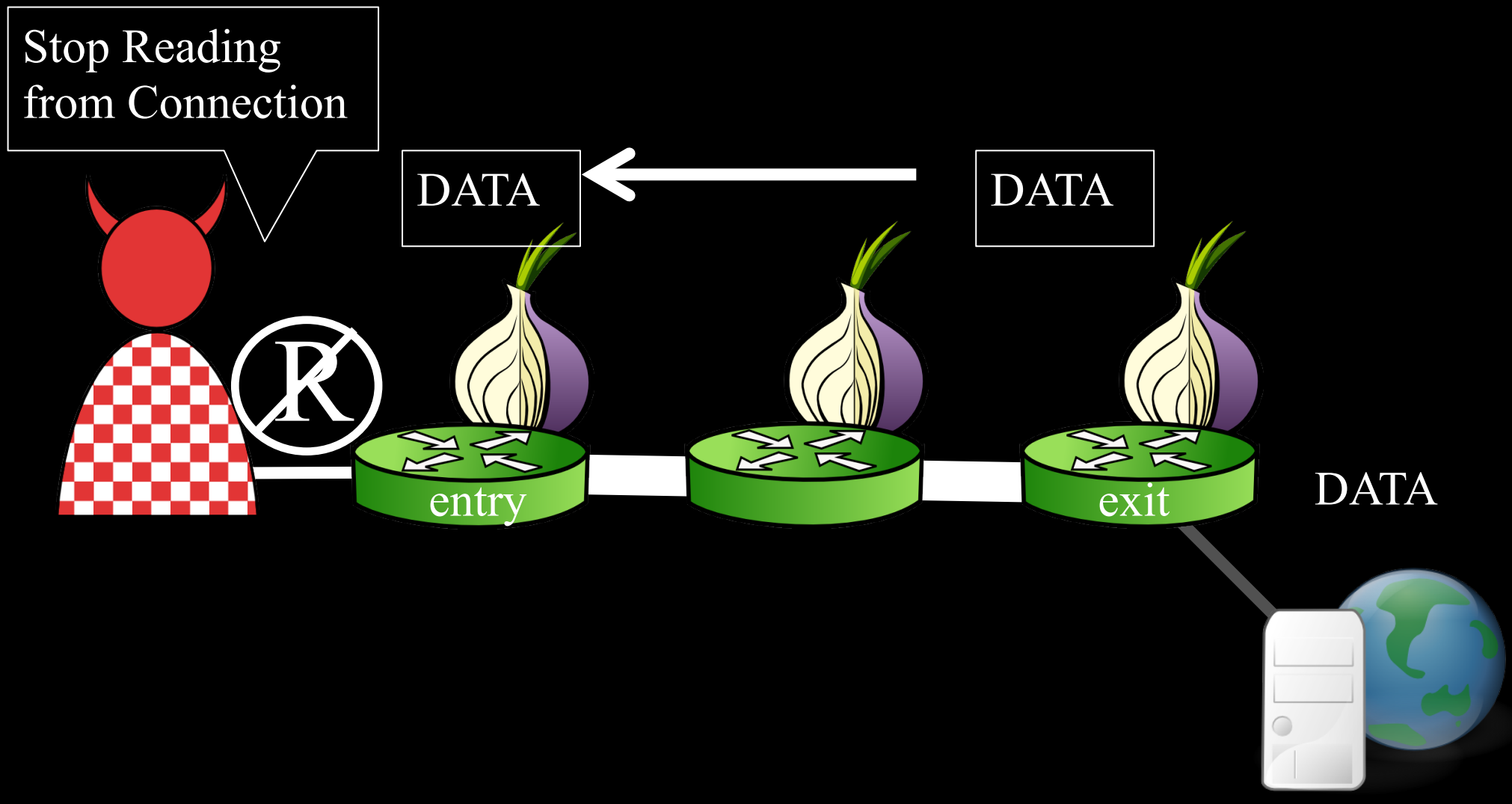
# The Sniper Attack



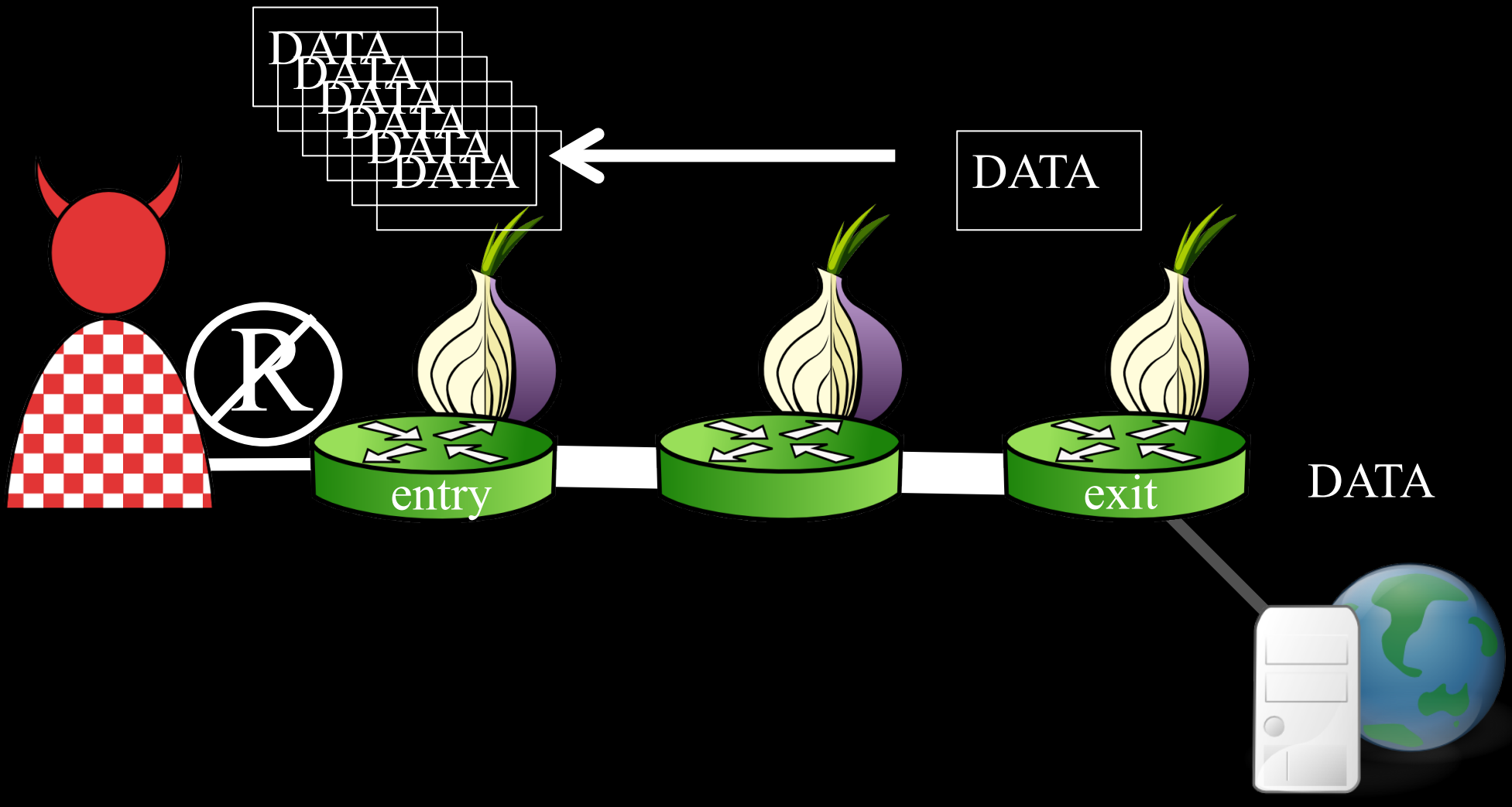
# The Sniper Attack



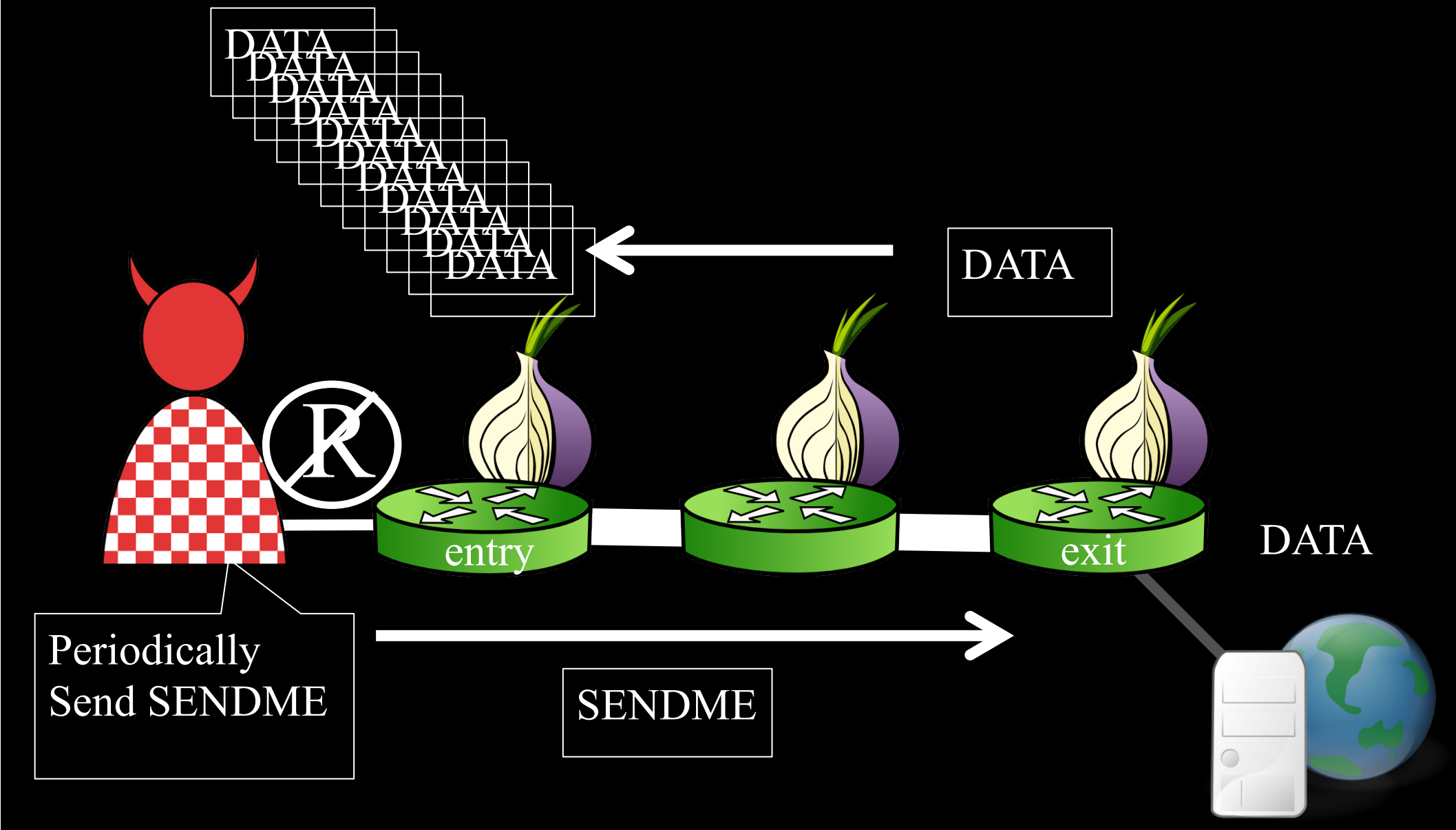
# The Sniper Attack



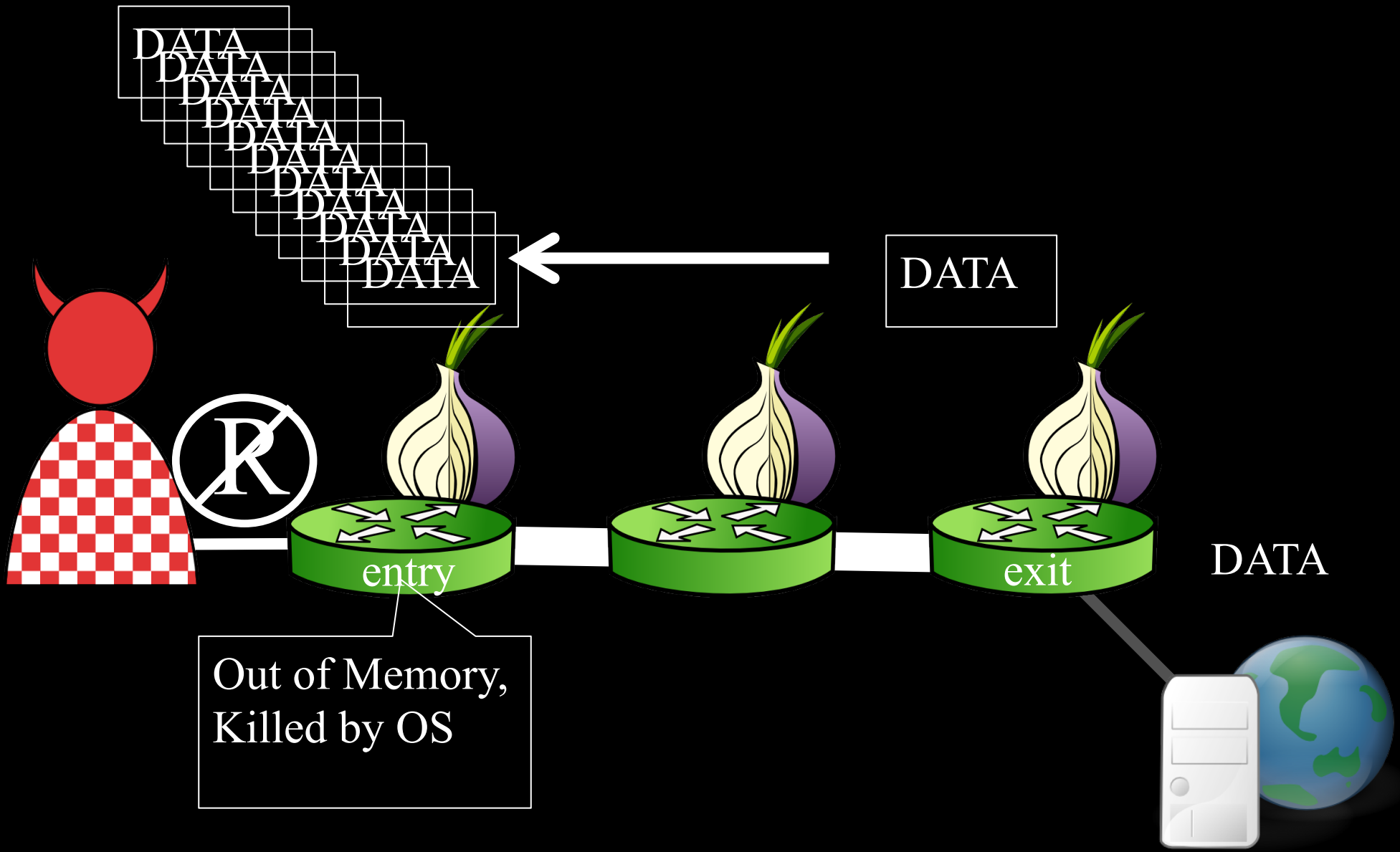
# The Sniper Attack



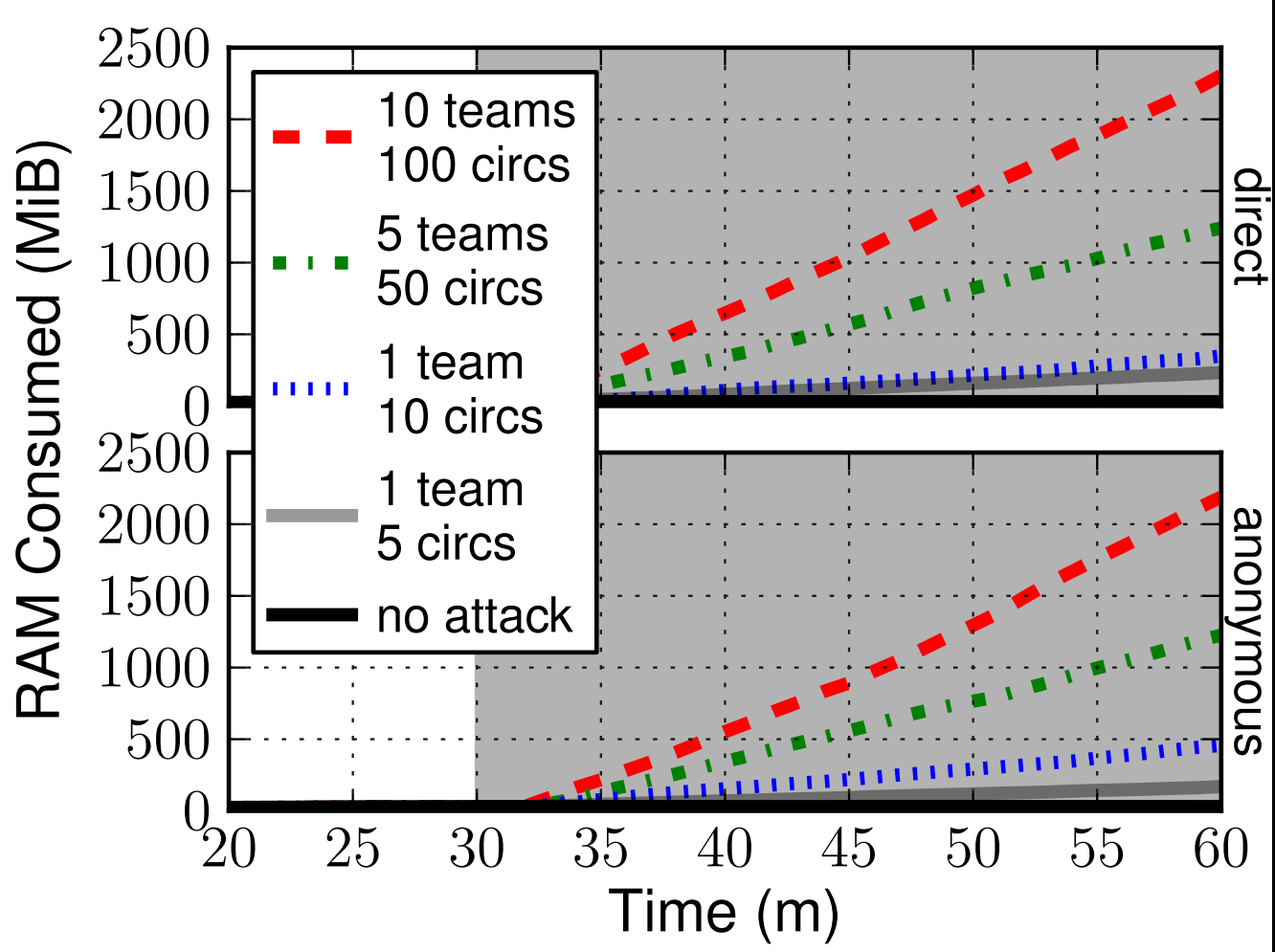
# The Sniper Attack



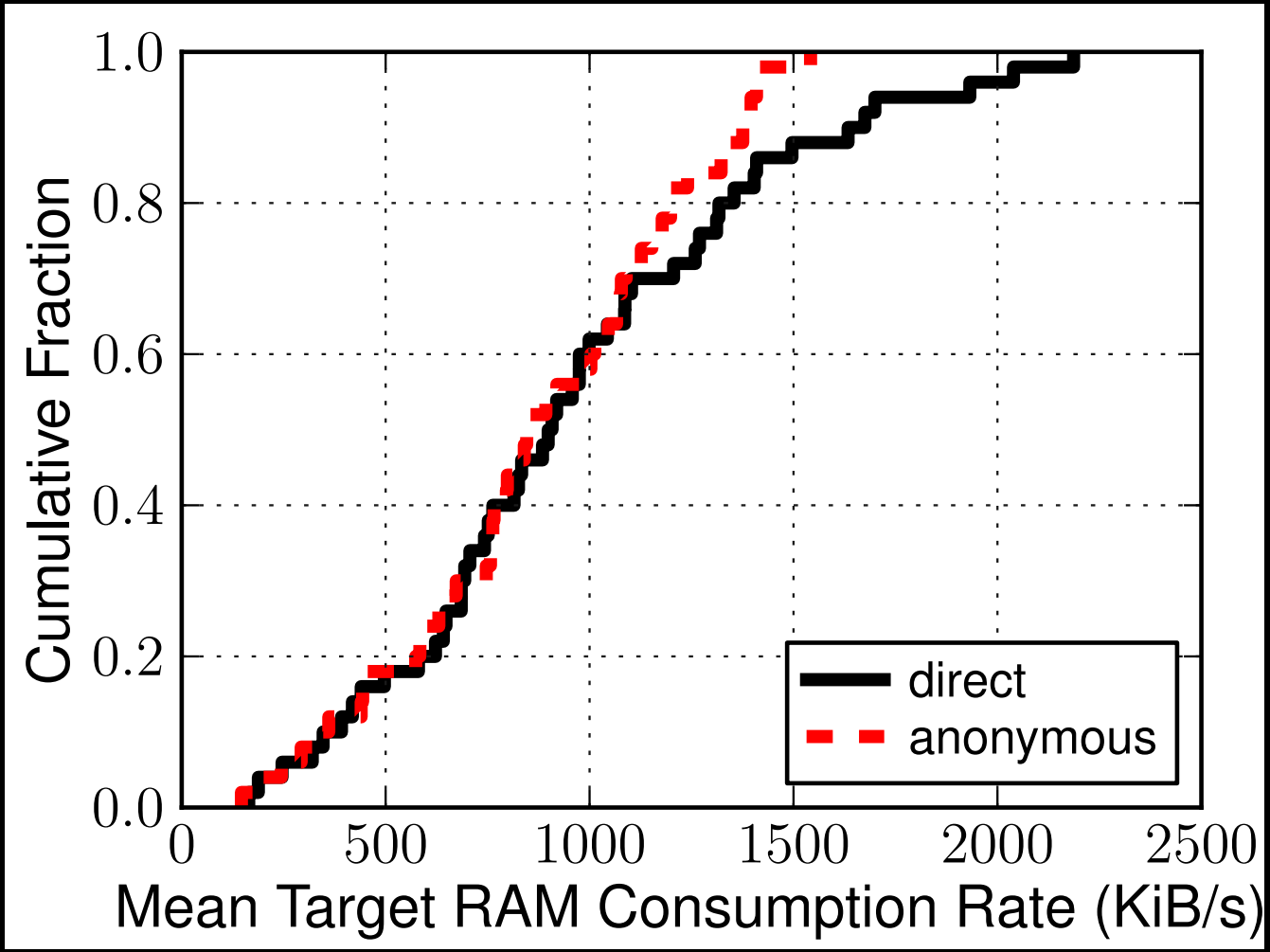
# The Sniper Attack



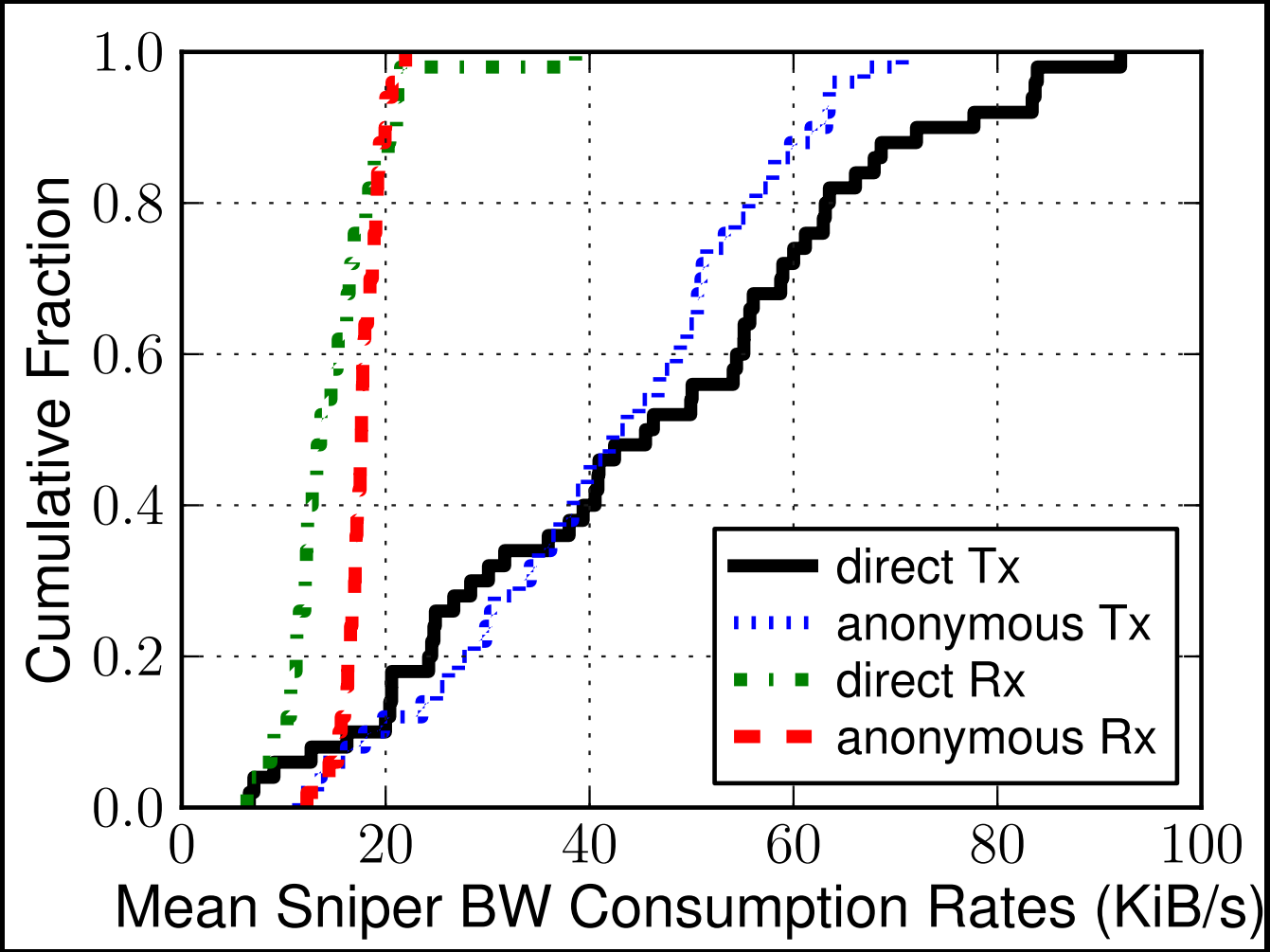
# Memory Consumed over Time



# Mean RAM Consumed, 50 Relays



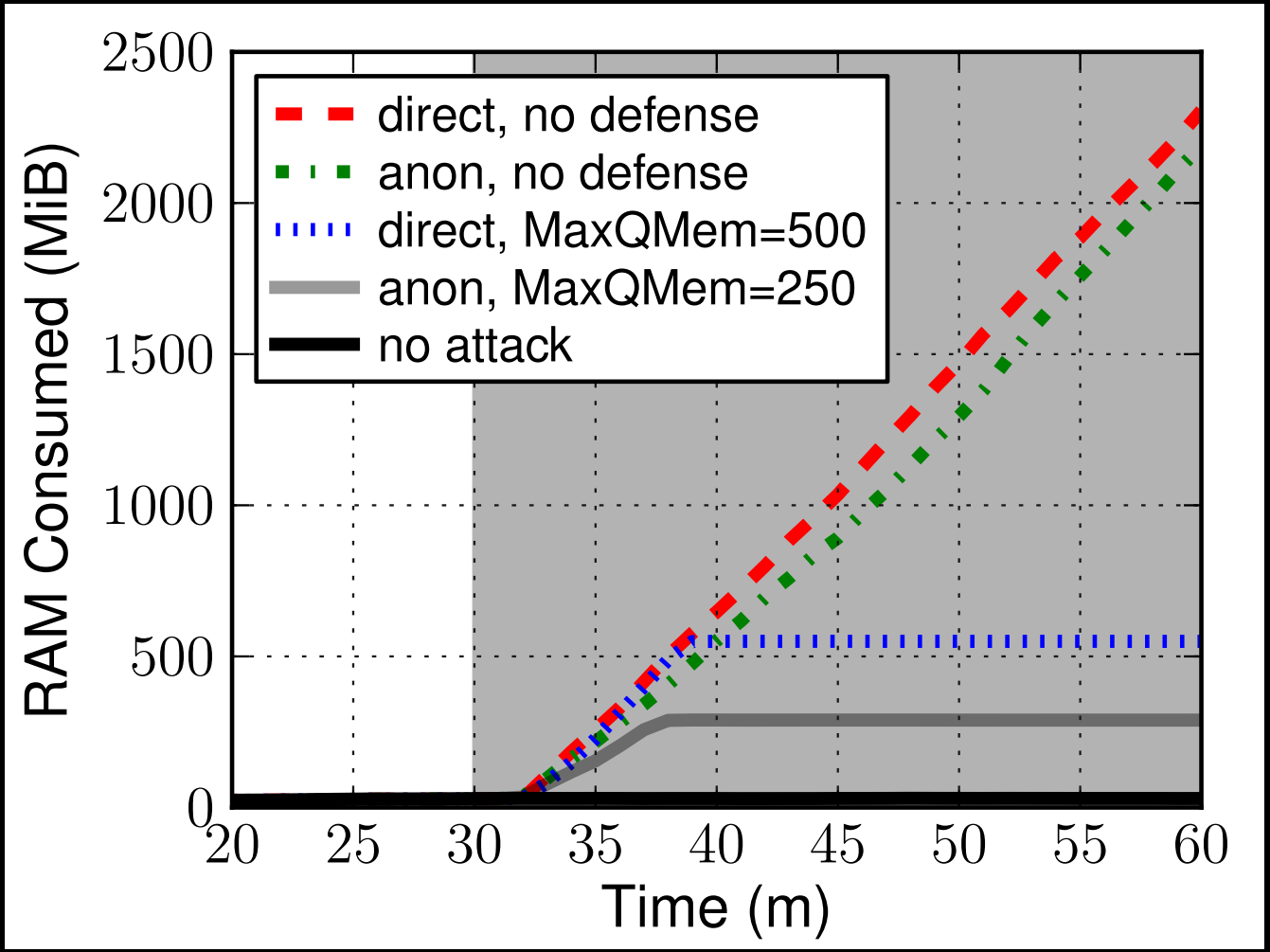
# Mean BW Consumed, 50 Relays



# Sniper Attack Defenses

- Authenticated SENDMEs
- Queue Length Limit
- Adaptive Circuit Killer

# Circuit-Killer Defense



# Sniper Attack Implications

- Reduce Tor's capacity
- Network Denial of Service
- Influence path selection (selective DoS)
- Deanonymization of hidden services

# Outline

- Experimentation Ideology
- Shadow and its Design
- Use case:
  - Overview: the Distributed Tor Network
  - Research: the Sniper Attack Against Tor

# Questions?

shadow.github.io

github.com/shadow

cs.umn.edu/~jansen

rob.g.jansen@nrl.navy.mil

*think like an adversary*