Cyber Demo

Carolyn Lauzon – Department of Energy, Office of Science

Ti Leggett – Argonne Leadership Computing Facility

U.S. DEPARTMENT OF ENERGY

Argonne NATIONAL LABORATORY

What is hacking and why?

Largest-Ever DDoS Campaign Demonstrates Danger of New Attack Method

By: Robert Lemos, eWeek

http://www.eweek.com/security/largest-ever-ddos-campaign-demonstrates-danger-of-new-attack-method

DDOS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world

By: Damien Fletcher, Mirror

https://www.mirror.co.uk/news/world-news/ddos-attack-spamhaus-biggest-cyber-attack-1788942

S Campaign Demonstrates Danger of New Attack Method

By: Robert Lemos, eWeek

http://www.eweek.com/security/largest-ever-ddos-campaign-demonstrates-danger-of-new-attack-method

DDOS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world

By: Damien Fletcher, Mirror

https://www.mirror.co.uk/news/world-news/ddos-attack-spamhaus-biggest-cyber-attack-1788942

S Campaign Demonstrates Danger of New Attack Method

By: Robert Lemos, eWeek

ddos-campaign-demonstrates-danger-of-new-attack-method

Lloyds Bank services hit by denial-of-service attack

By: Danny Palmer, ZDNet

https://www.zdnet.com/article/lloyds-bank-services-hit-by-denial-of-service-attack/

DDOS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world

By: Damien Fletcher, Mirror

https://www.mirror.co.uk/news/world-news/ddos-attack-spamhaus-biggest-cyber-attack-1788942

Mirai variant botnet launches IoT DDoS attacks on financial sector

By: Alison DeNisco Rayome, TechRepublic

https://www.techrepublic.com/article/mirai-variant-botnet-launches-iot-ddos-attacks-on-financial-sector/

Demonstrates Danger of New Attack Method

By: Robert Lemos, eWeek

ddos-campaign-demonstrates-danger-of-new-attack-method

Lloyds Bank services hit by denial-of-service attack

By: Danny Palmer, ZDNet

https://www.zdnet.com/article/lloyds-bank-services-hit-by-denial-of-service-attack/

DDOS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world

By: Damien Fletcher, Mirror

https://www.mirror.co.uk/news/world-news/ddos-attack-spamhaus-biggest-cyber-attack-1788942

Mirai variant botnet launches IoT DDoS attacks on financial sector

By: Alison DeNisco Rayome, TechRepublic

https://www.techrepublic.com/article/mirai-variant-botnet-launches-iot-ddos-attacks-on-financial-sector/

Demonstrates Danger of New Attack Method

By: Robert Lemos, eWeek

ddos-campaign-demonstrates-dange

Lloyds Bank services hit by denial-of-service attack

By: Danny Palmer, ZDNet

https://www.zdnet.com/article/lloyds-bank-services-hit-by-denial-of-service-attack/

Large DDoS attacks cause outages at Twitter, Spotify, and other sites

By: Darrell Etherington, TechCrunch

https://techcrunch.com/2016/10/21/many-sites-including-twitter-and-spotify-suffering-outage/

DDOS attack on Spamhaus: Biggest cyber-attack in history slows down internet across the world

By: Damien Fletcher, Mirror

https://www.mirror.co.uk/news/world-news/ddos-attack-spamhaus-biggest-cyber-attack-1788942

Mirai variant botnet launches IoT DDoS attacks on financial sector

By: Alison DeNisco Rayome, TechRepublic

https://www.techrepublic.com/article/mirai-variant-botnet-launches-iot-ddos-attacks-on-financial-sector/

Demonstrates Danger of New Attack Method

By: Robert Lemos, eWeek

ddos-campaign-demonstrates-dange

Large DDoS attacks cause outages at Twitter, Spotify, and other sites

Crunch

y-sites-including-twitter-and-spotify-suffering-outage/

Lloyds Bank services hit by denial-of-service attack

By: Danny Palmer, ZDNet

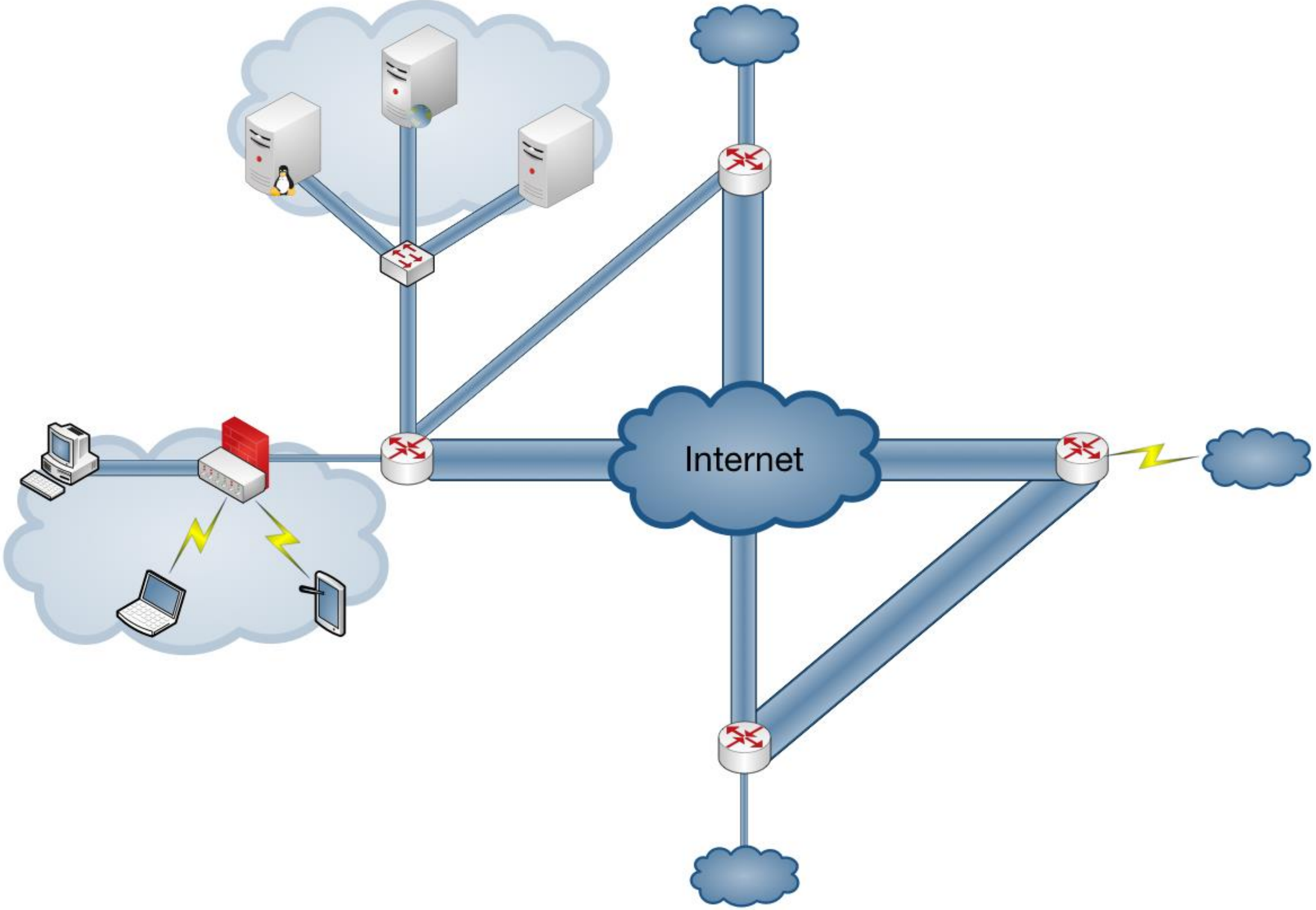
https://www.zdnet.com/article/lloyds-bank-services-hit-by-

Evidence suggests Stuxnet worm set Iran’s nuclear program back

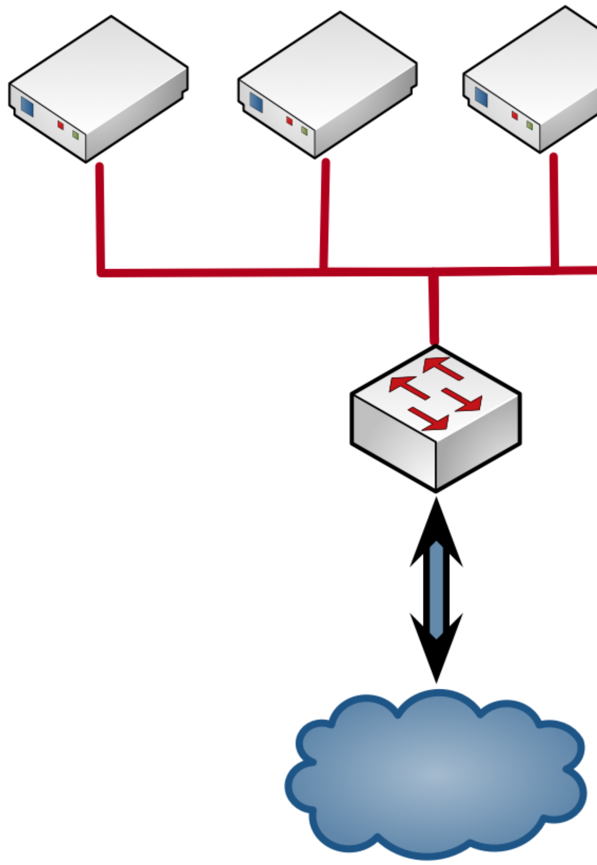
By: Dean Takahashi, VentureBeat

https://venturebeat.com/2011/01/15/evidence-builds-that-stuxnet-worm-was-aimed-at-averting-war-over-irans-nuclear-weapons/

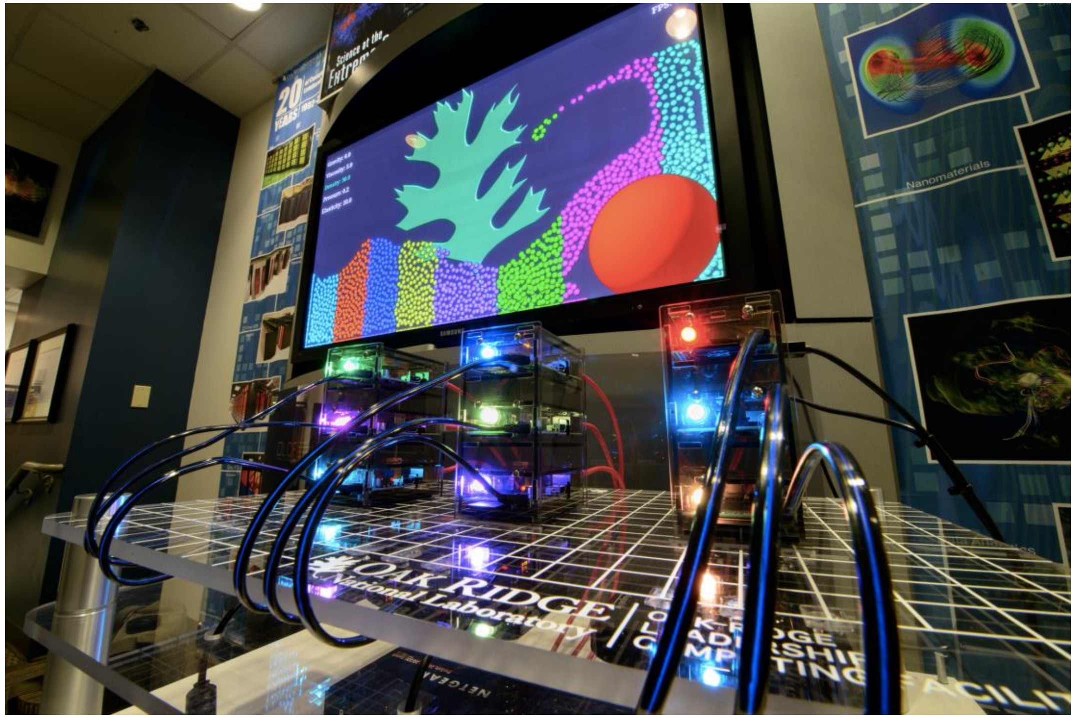
The Internet and Cyber Security



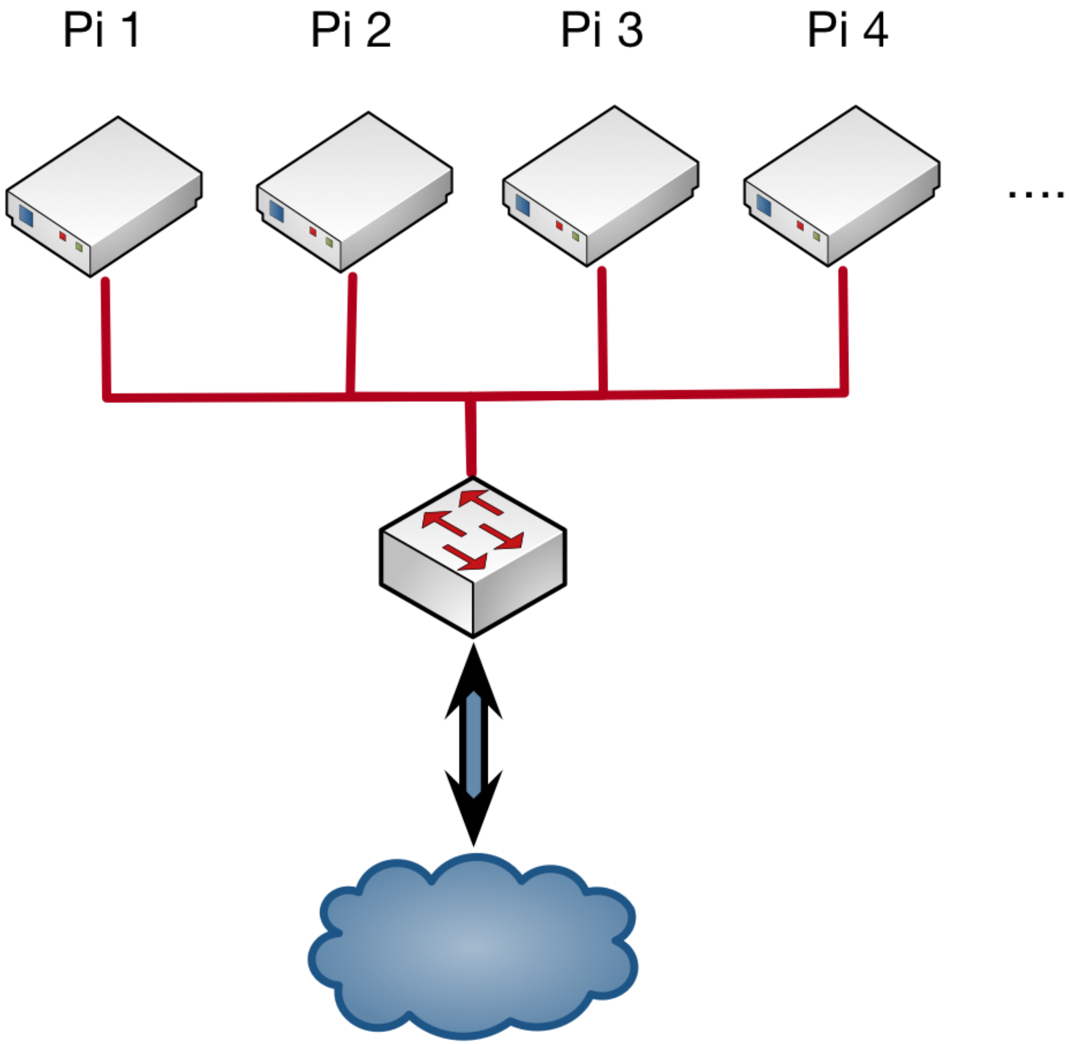
A Simple Network of Computers Talking



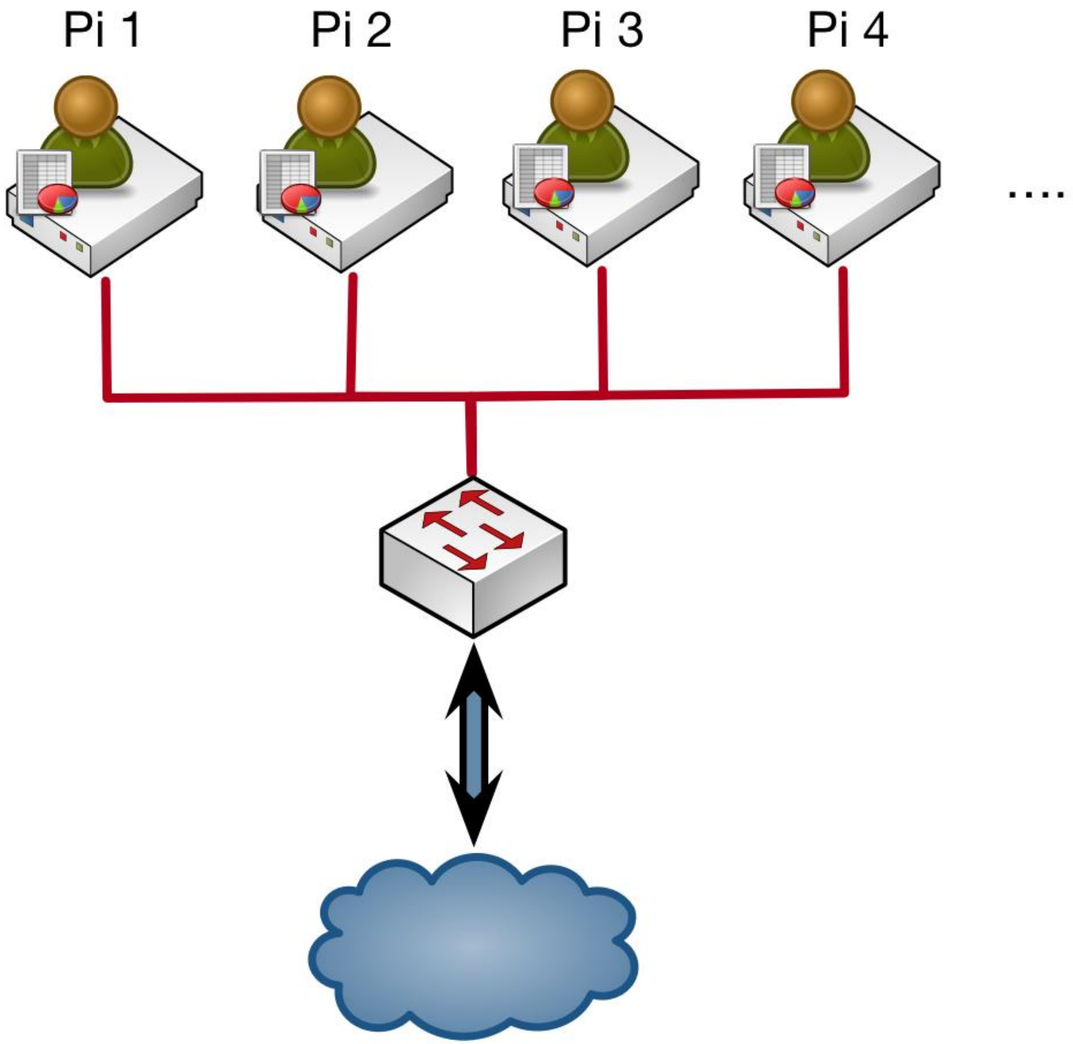
Mini Demo:
TinyTitan = Shows Computers Talking to Each Other Over a Network



Tiny Titan: A Simple Network of Computers Talking

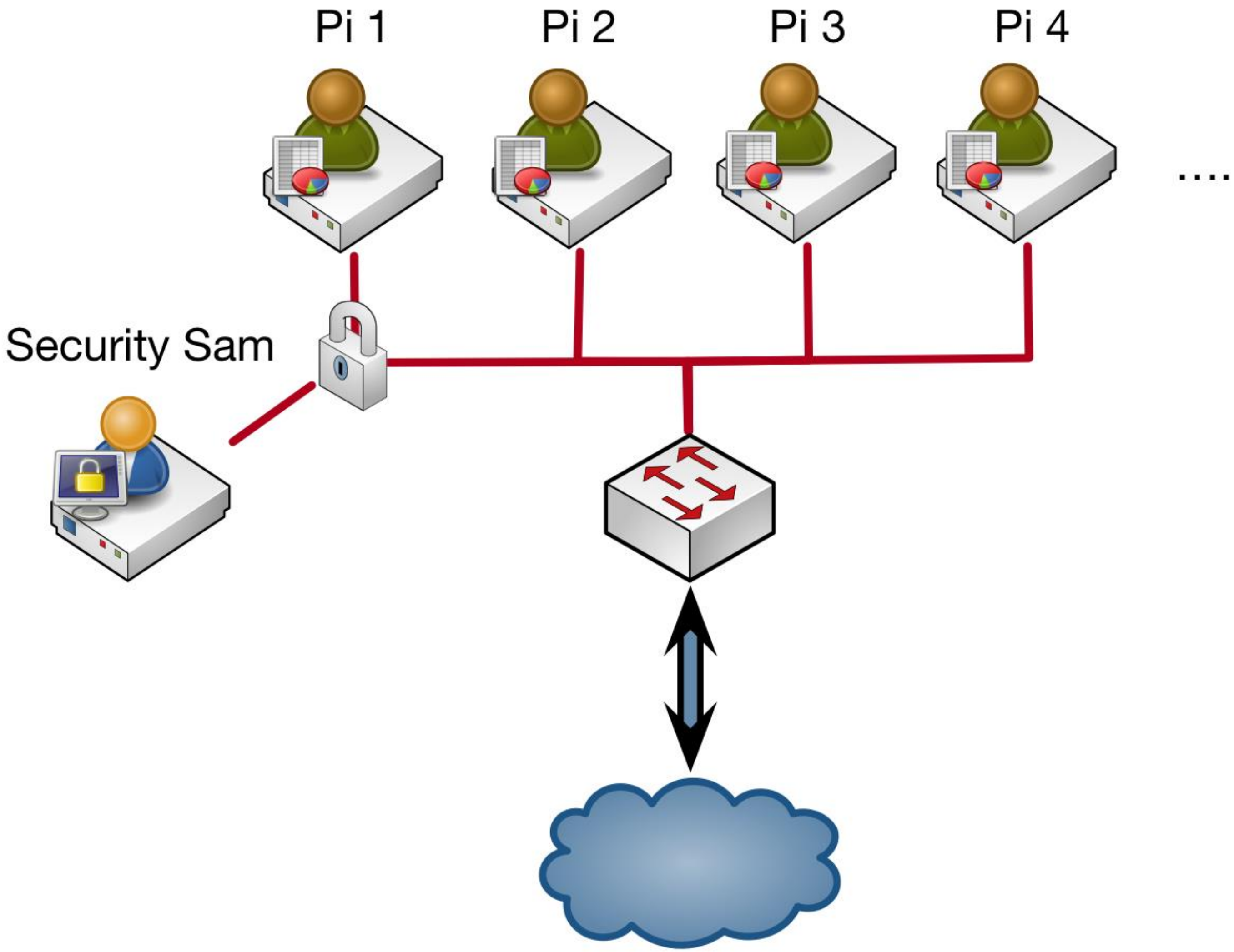


Tiny Titan: A Simple Network of Computers Talking

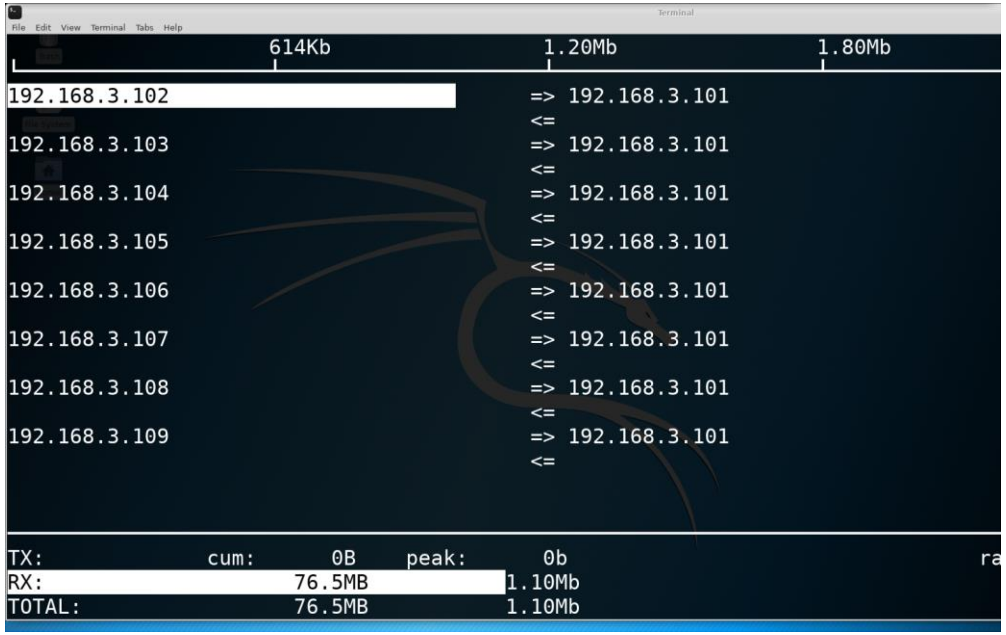


Security Sam

Monitors Pis Traffic



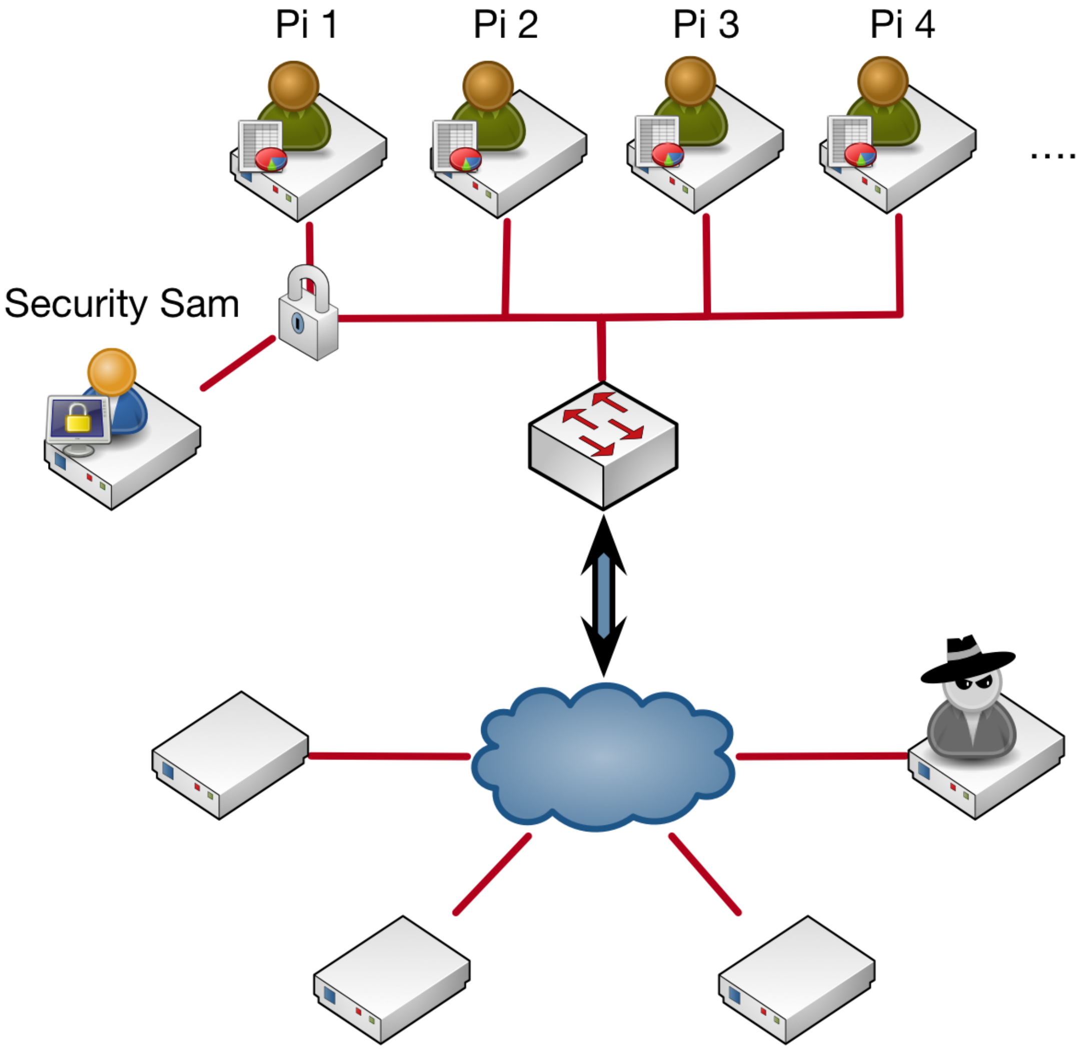
Mini Demo:
Security Sam Traffic Monitoring on Pi1



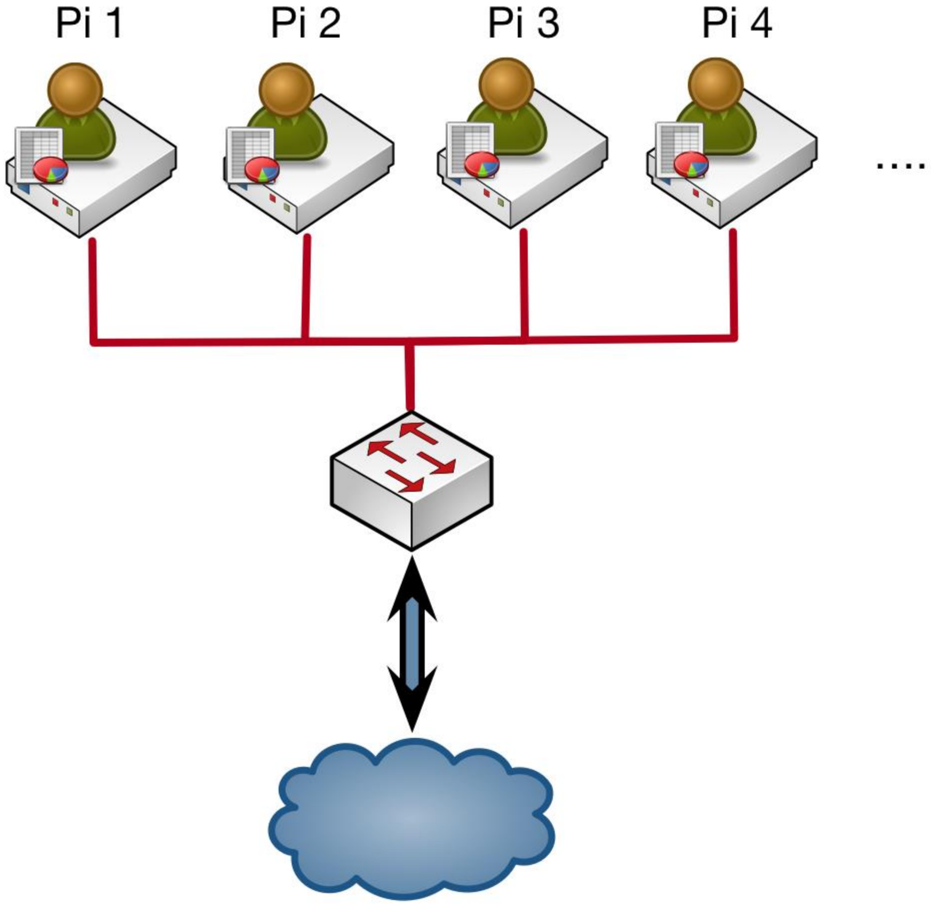
```
                         614Kb                 1.20Mb                1.80Mb
192.168.3.102                                 => 192.168.3.101
                                              <=
192.168.3.103                                 => 192.168.3.101
                                              <=
192.168.3.104                                 => 192.168.3.101
                                              <=
192.168.3.105                                 => 192.168.3.101
                                              <=
192.168.3.106                                 => 192.168.3.101
                                              <=
192.168.3.107                                 => 192.168.3.101
                                              <=
192.168.3.108                                 => 192.168.3.101
                                              <=
192.168.3.109                                 => 192.168.3.101
                                              <=

TX:             cum:       0B   peak:      0b                             ra
RX:                     76.5MB          1.10Mb
TOTAL:                  76.5MB          1.10Mb
```

Hacker Hal

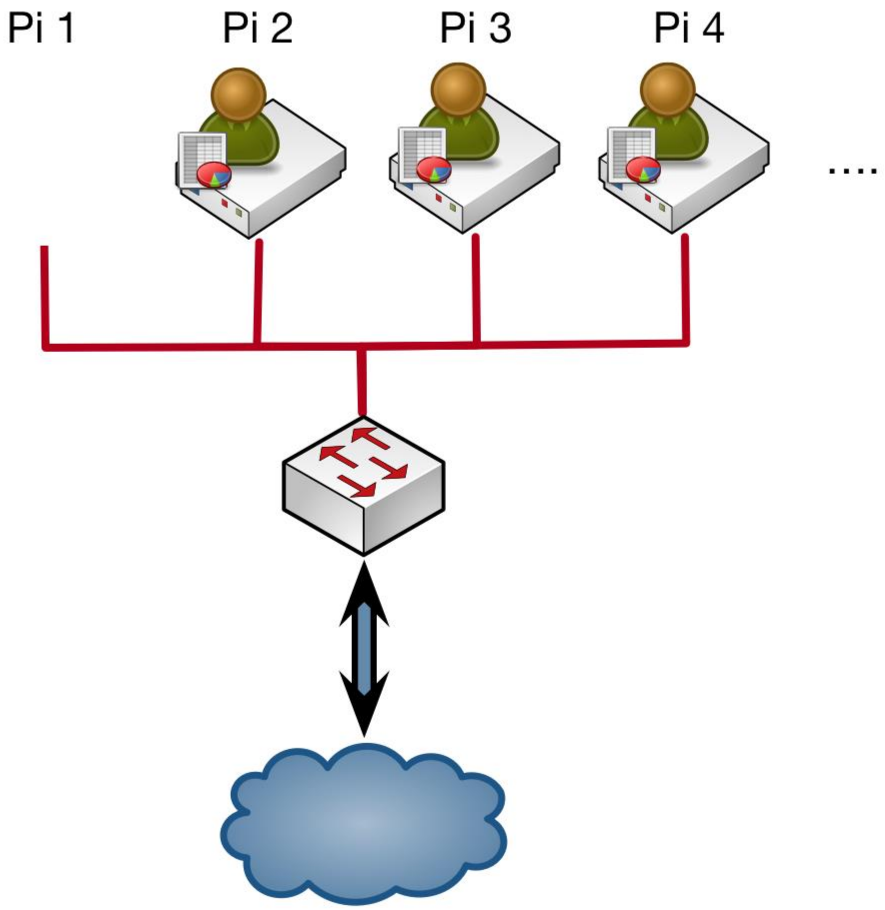
Wants to Stop Pis from Sharing Secrets



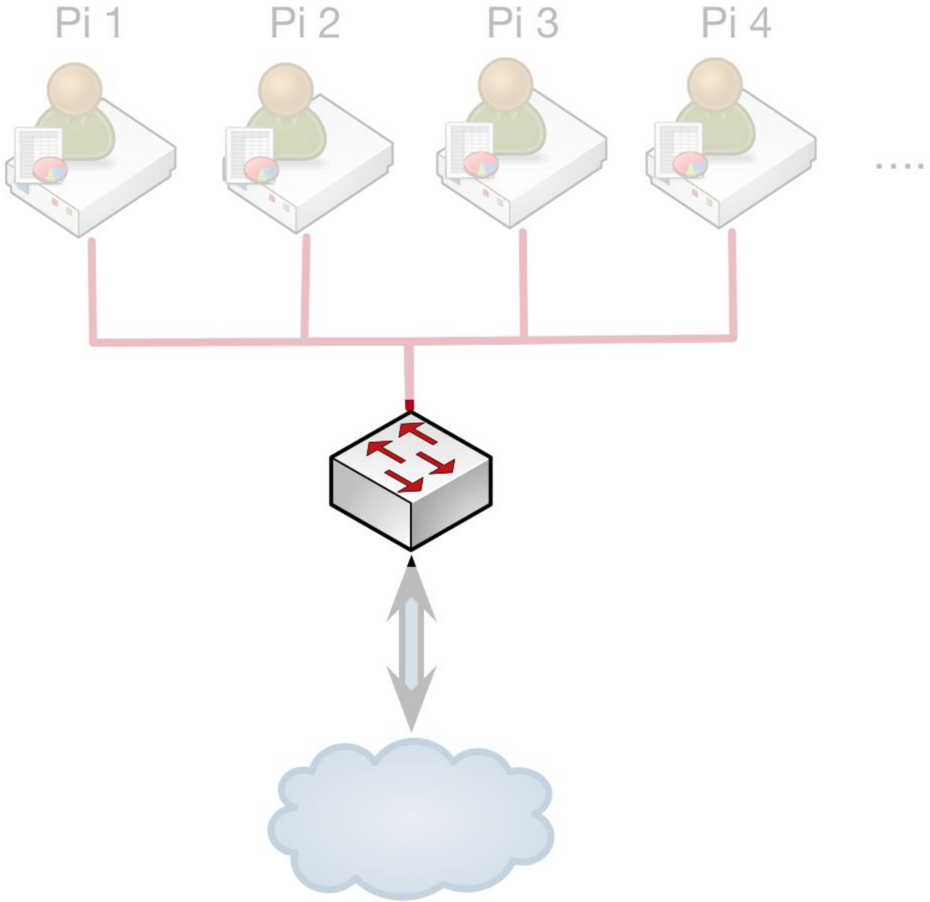
What things might Hal do to stop Pis from sharing secrets?



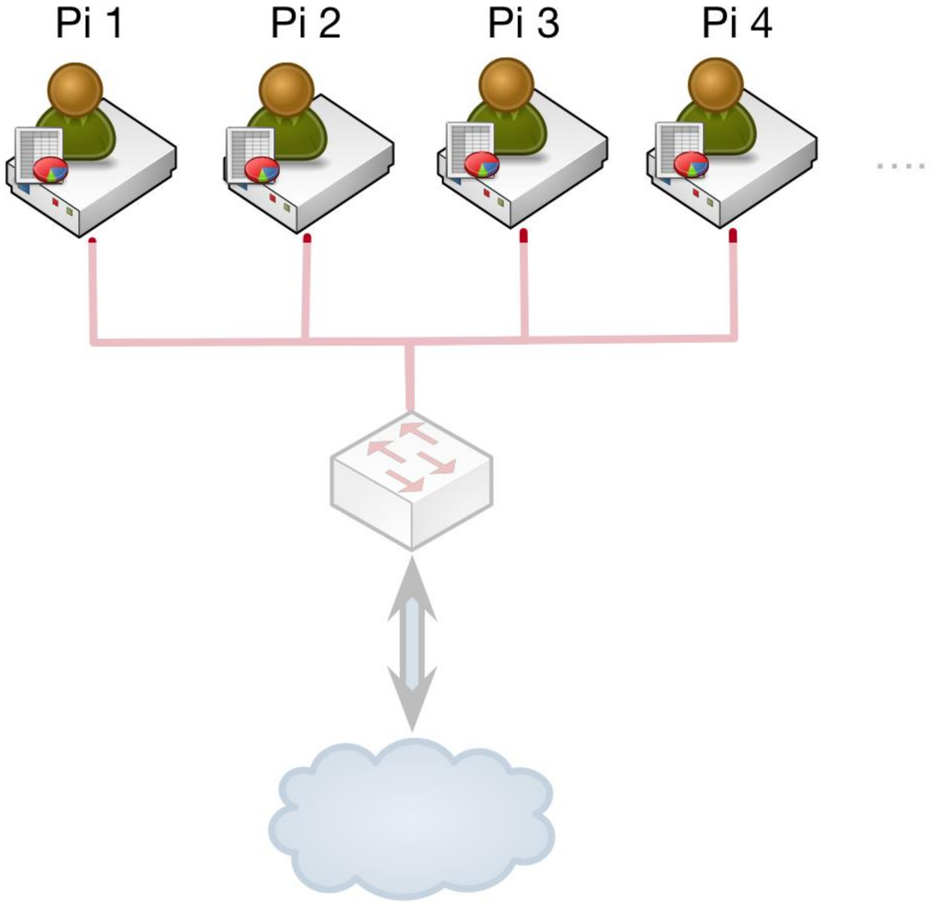
What things might Hal do to stop Pis from sharing secrets?



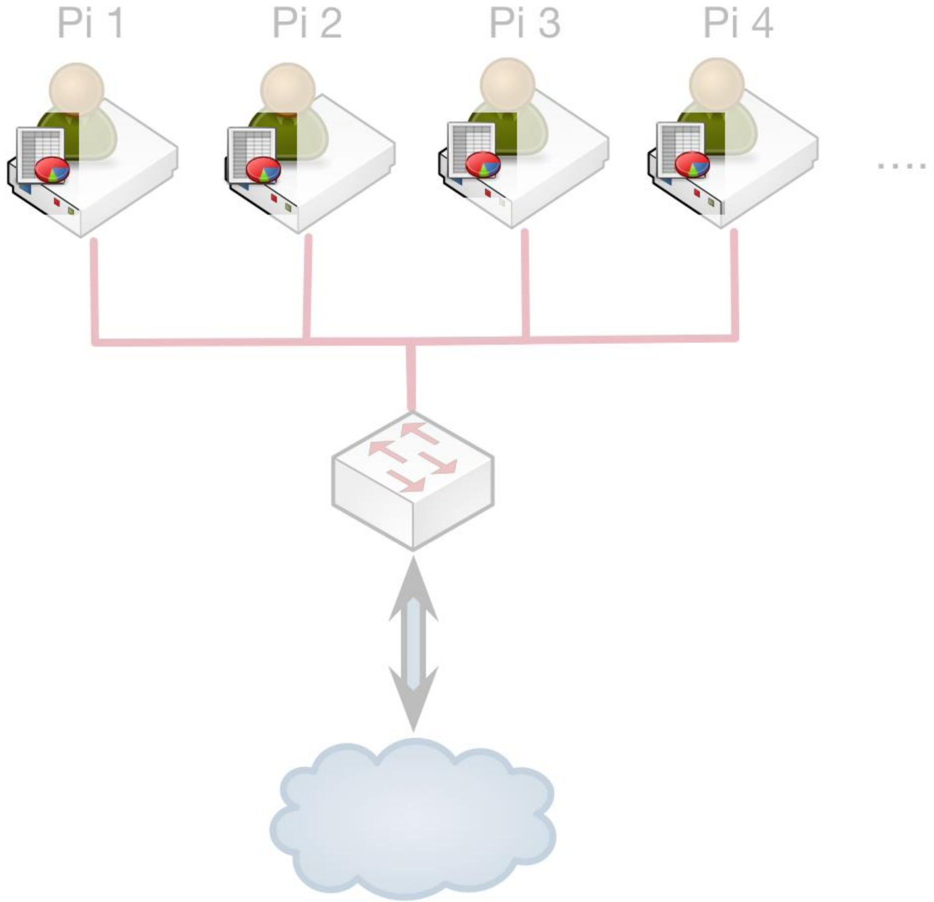
What things might Hal do to stop Pis from sharing secrets?



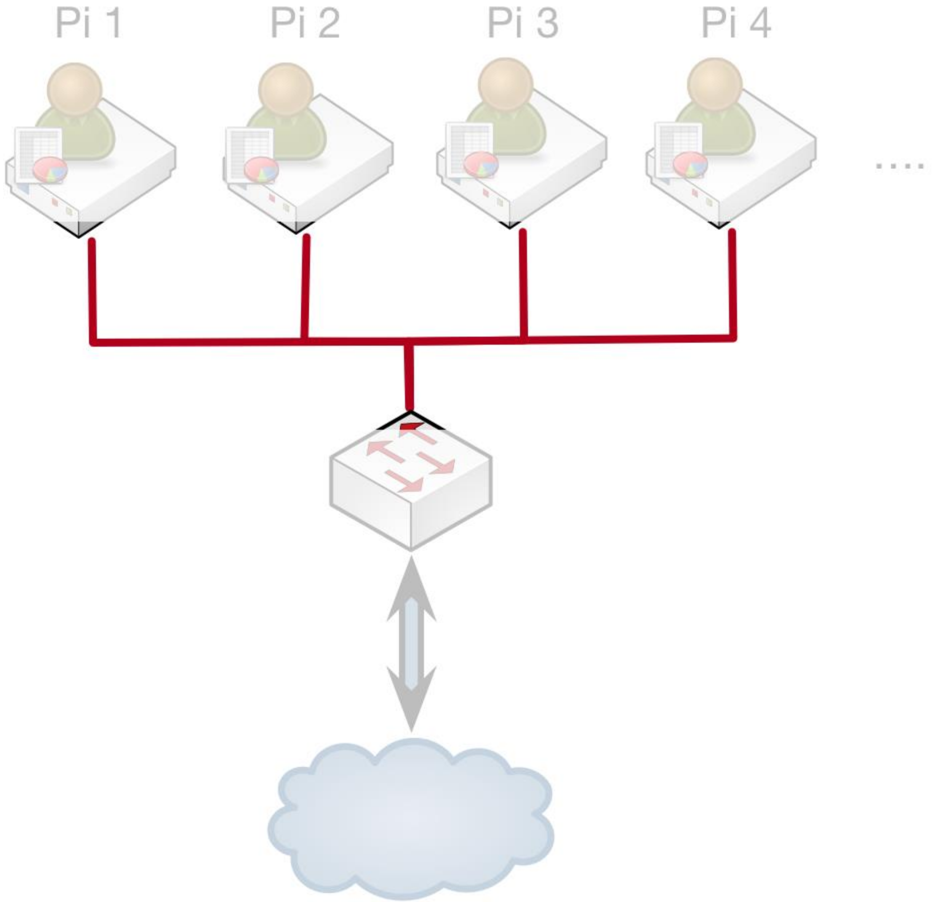
What things might Hal do to stop Pis from sharing secrets?



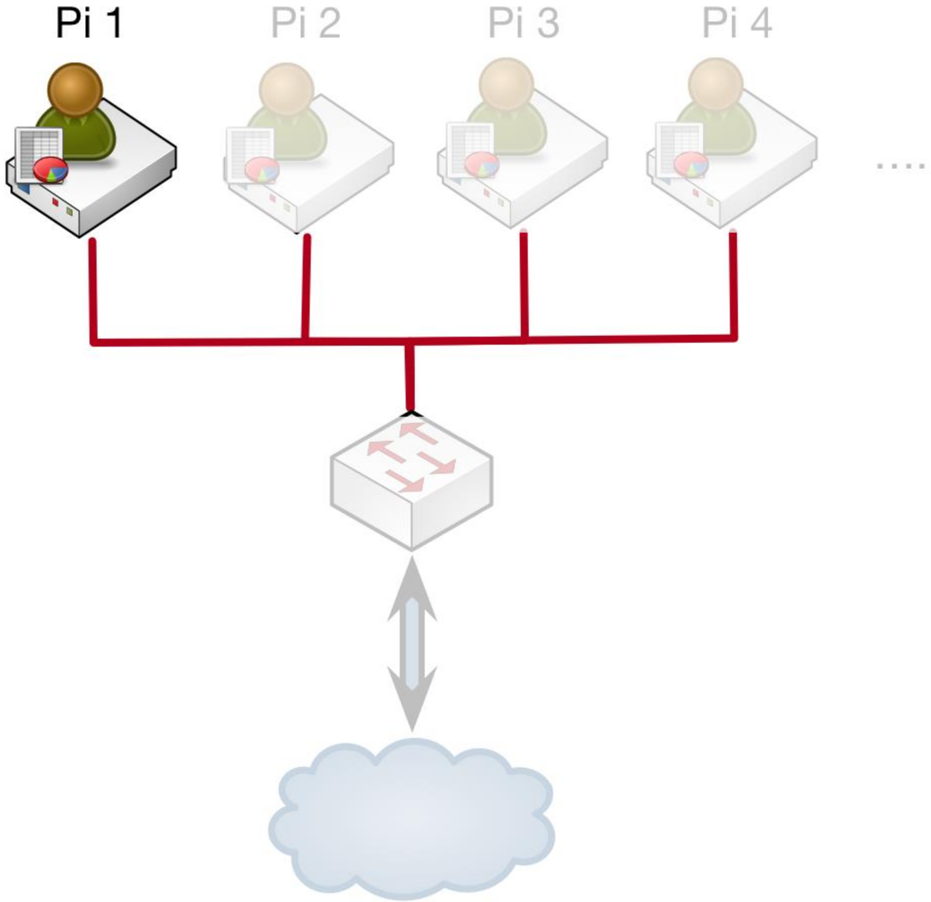
What things might Hal do to stop Pis from sharing secrets?



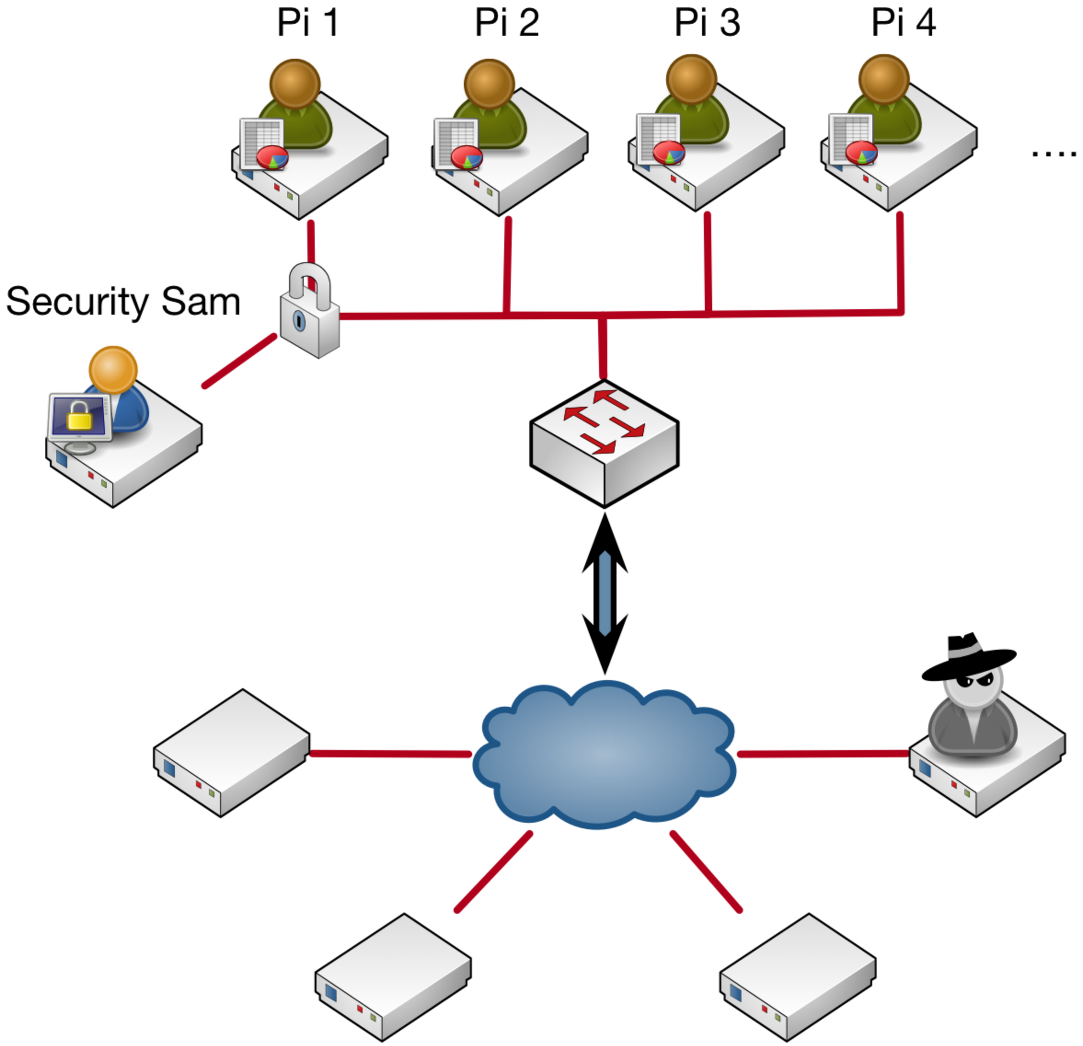
What things might Hal do to stop Pis from sharing secrets?



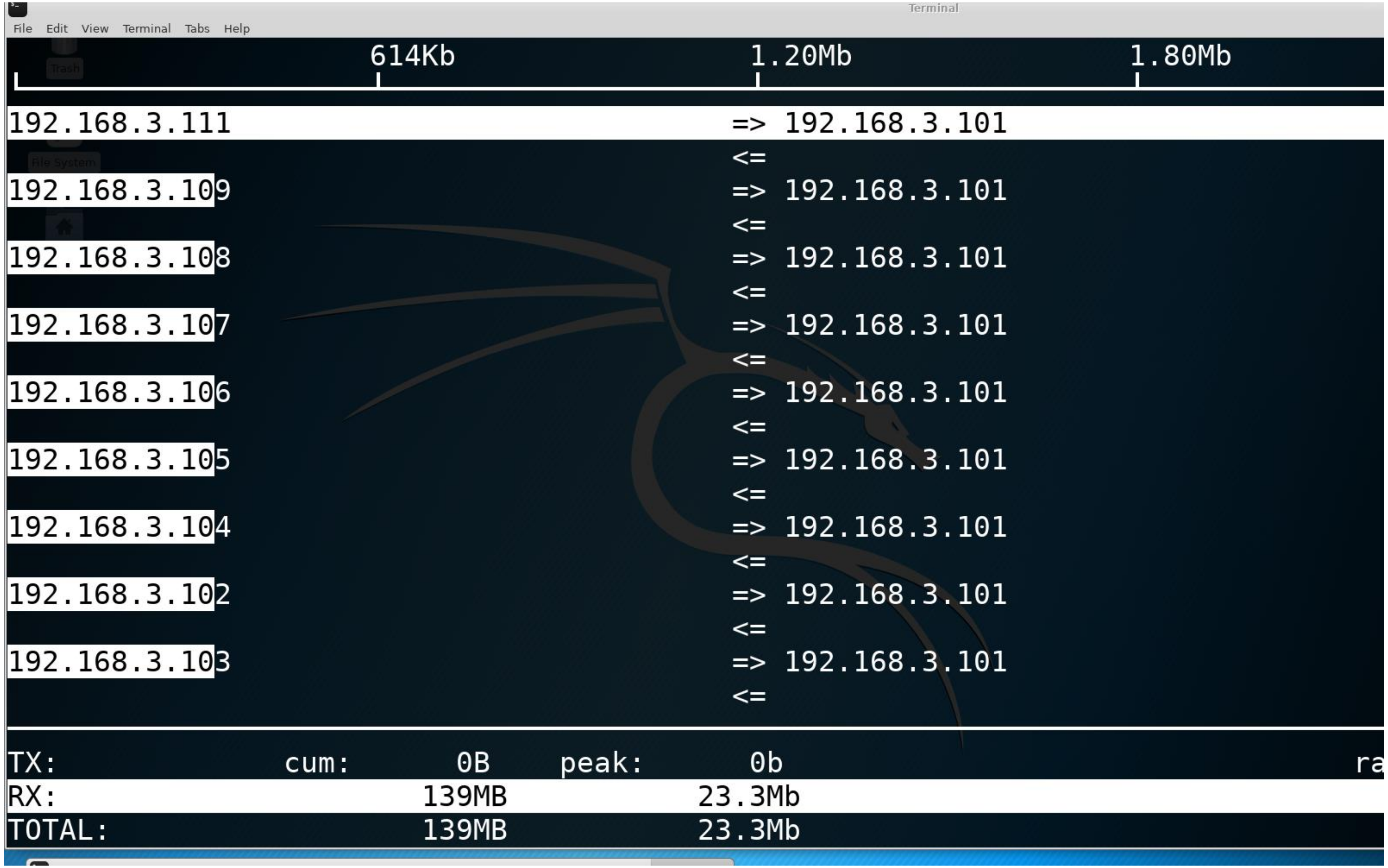
What things might Hal do to stop Pis from sharing secrets?



Mini Demo:
Hacker Hal Strikes - Denial of Service (DoS)



Hacker Hal Strikes - Denial of Service (DoS)

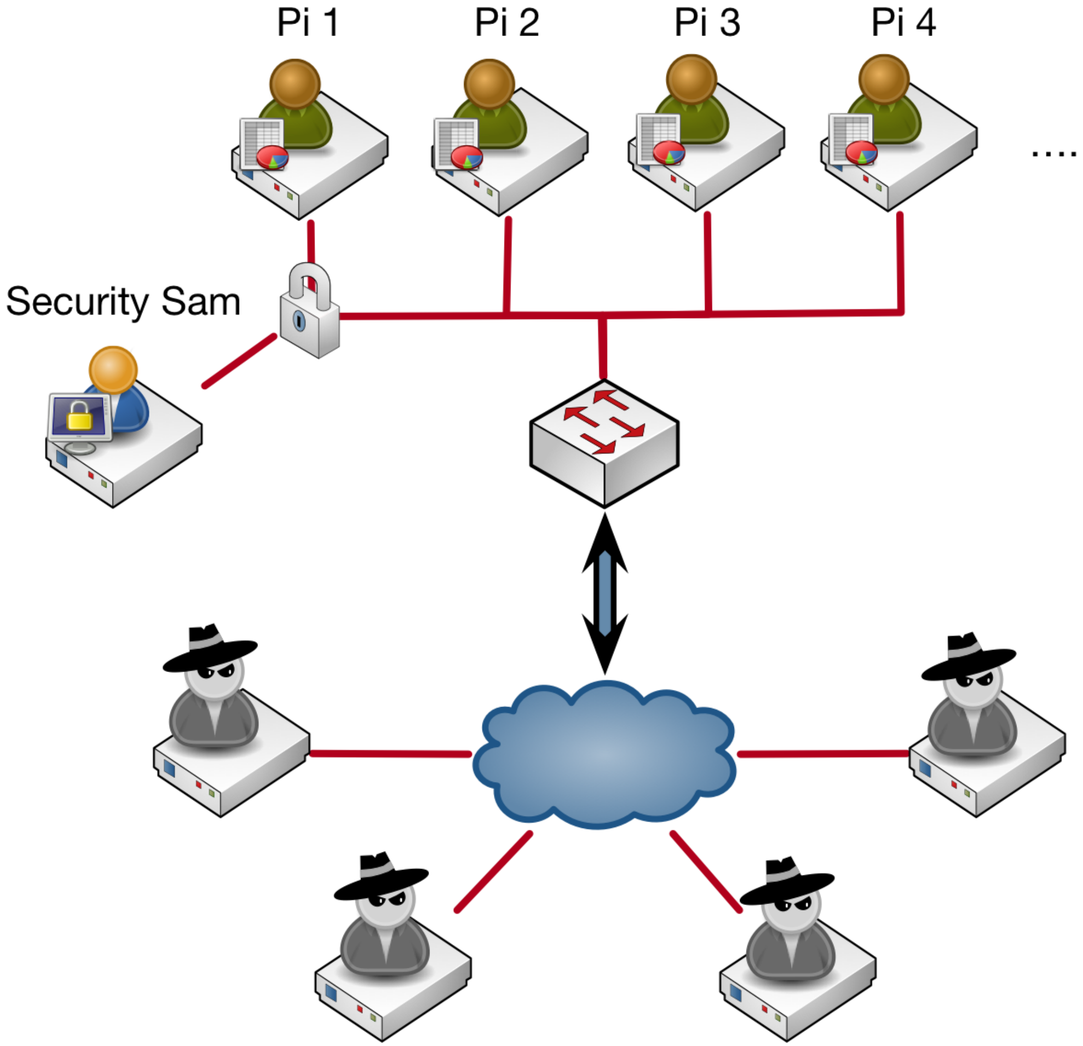


```
                    614Kb                1.20Mb               1.80Mb
192.168.3.111                         => 192.168.3.101
                                      <=
192.168.3.109                         => 192.168.3.101
                                      <=
192.168.3.108                         => 192.168.3.101
                                      <=
192.168.3.107                         => 192.168.3.101
                                      <=
192.168.3.106                         => 192.168.3.101
                                      <=
192.168.3.105                         => 192.168.3.101
                                      <=
192.168.3.104                         => 192.168.3.101
                                      <=
192.168.3.102                         => 192.168.3.101
                                      <=
192.168.3.103                         => 192.168.3.101
                                      <=

TX:             cum:     0B     peak:     0b                        ra
RX:                    139MB           23.3Mb
TOTAL:                 139MB           23.3Mb
```

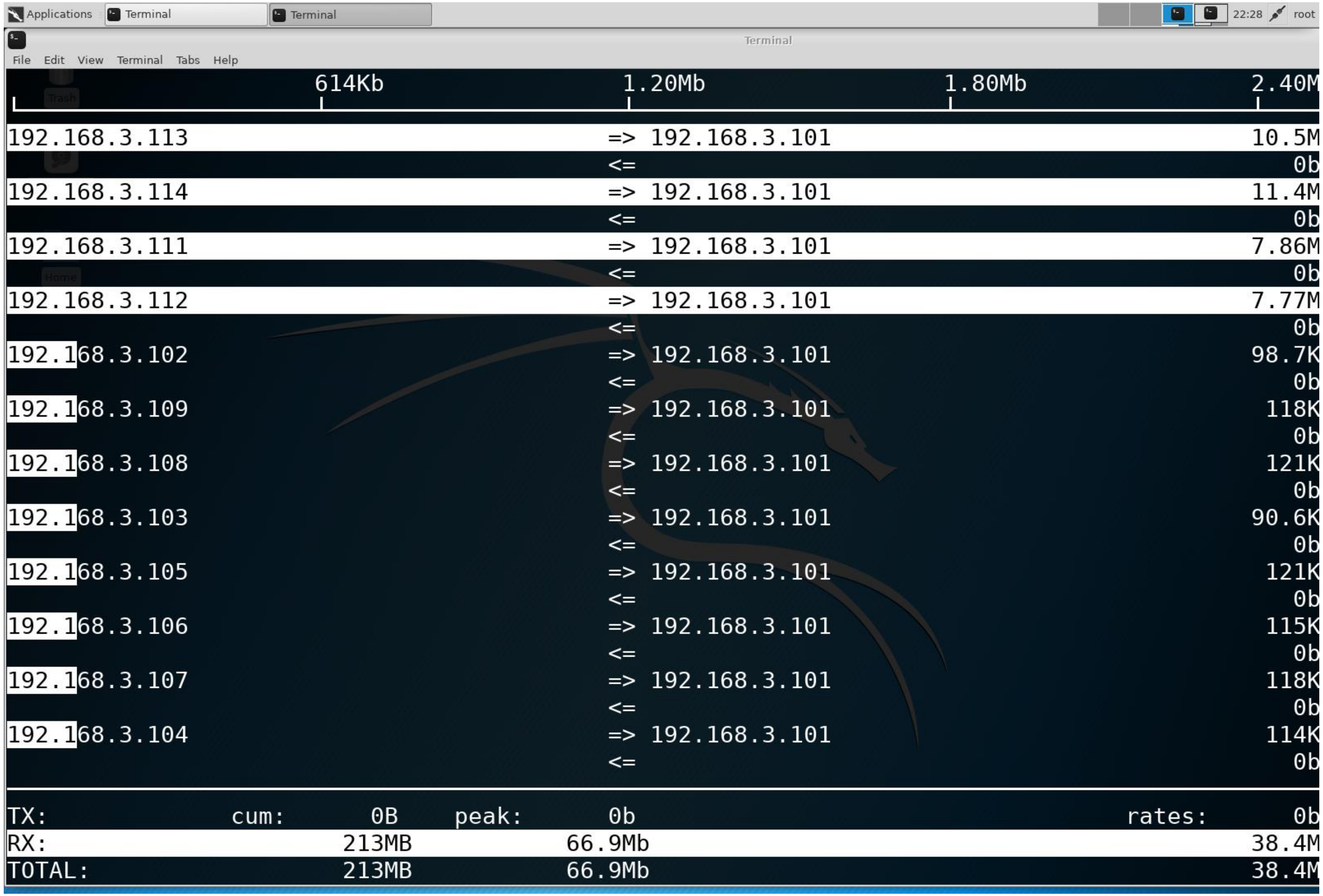
Hacker Hal Not Effective

- What could Hal do to have an impact?

Hacker Hal Super Strike
Distributed Denial of Service (DDoS)

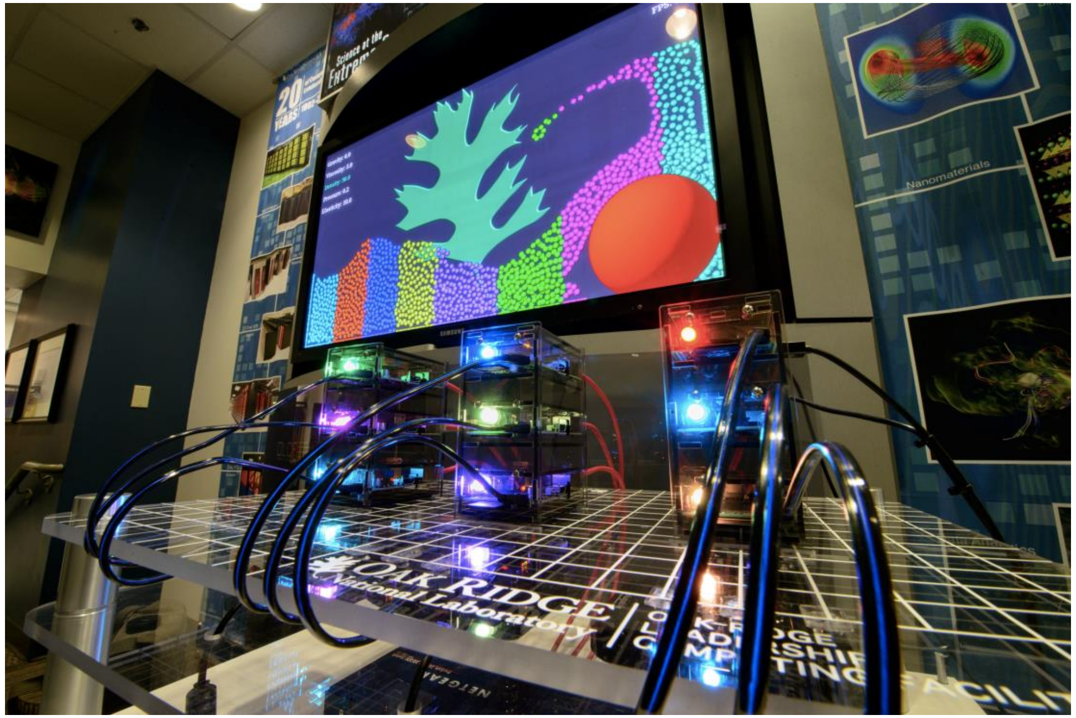


Hacker Hal Strikes Again- Distributed Denial of Service



```
                   614Kb                1.20Mb               1.80Mb               2.40M
192.168.3.113                        => 192.168.3.101                              10.5M
                                     <=                                               0b
192.168.3.114                        => 192.168.3.101                              11.4M
                                     <=                                               0b
192.168.3.111                        => 192.168.3.101                              7.86M
                                     <=                                               0b
192.168.3.112                        => 192.168.3.101                              7.77M
                                     <=                                               0b
192.168.3.102                        => 192.168.3.101                              98.7K
                                     <=                                               0b
192.168.3.109                        => 192.168.3.101                               118K
                                     <=                                               0b
192.168.3.108                        => 192.168.3.101                               121K
                                     <=                                               0b
192.168.3.103                        => 192.168.3.101                              90.6K
                                     <=                                               0b
192.168.3.105                        => 192.168.3.101                               121K
                                     <=                                               0b
192.168.3.106                        => 192.168.3.101                               115K
                                     <=                                               0b
192.168.3.107                        => 192.168.3.101                               118K
                                     <=                                               0b
192.168.3.104                        => 192.168.3.101                               114K
                                     <=                                               0b

TX:            cum:      0B    peak:      0b                               rates:     0b
RX:                   213MB           66.9Mb                                       38.4M
TOTAL:                213MB           66.9Mb                                       38.4M
```

Mini Demo:
TinyTitan DDOS Impact


Science at the Extreme
20 YEARS
Nanomaterials
OAK RIDGE National Laboratory
OAK RIDGE LEADERSHIP COMPUTING FACILITY
NETGEAR

7 Iranians Indicted for DDoS Attacks Against U.S. Banks

By: Eric Chabrow, Bank Info Security

https://www.bankinfosecurity.com/7-iranians-indicted-for-ddos-attacks-against-us-banks-a-8989

Overwhelm an Amazon distribution center
DDOS

- Amazon verifies:
  - Every delivery (3-way handshake)
    - Checks every truck and driver
  - Each package (integrity)
    - Scans package barcode
- You could send:
  - A few big trucks with lots of packages each, OR
    - Amazon is designed to handle this
  - Lots of cars with one package each
    - ”Valid” deliveries, but not how Amazon was designed

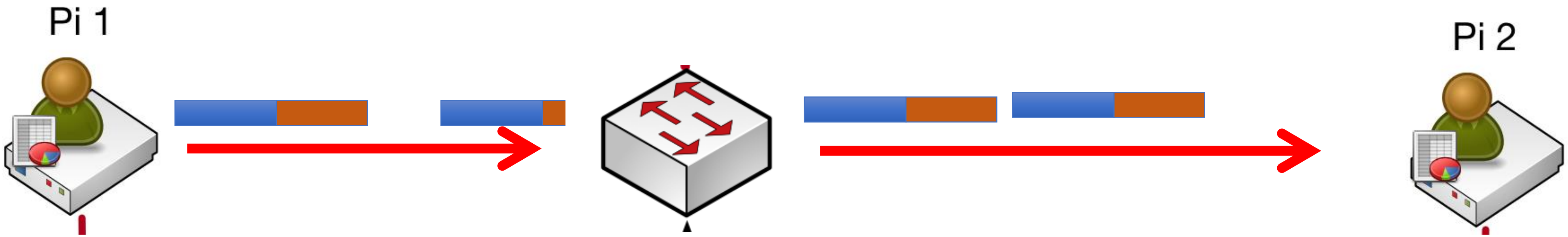
Extra

ARP

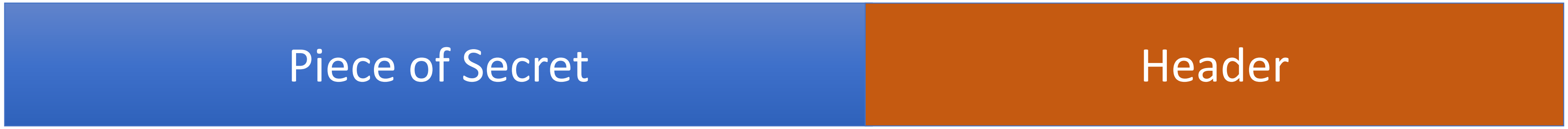
Mac Address and IP Address

Name	Mac Address	IP Address
pi1	b8 : 27 : eb : 9f : 4e : c5	192.168.3.101
pi2	b8 : 27 : eb : be : 80 : c1	192.168.3.102
pi3	b8 : 27 : eb : 89 : 58 : fd	192.168.3.103
pi4	b8 : 27 : eb : 53 : 6a : eb	192.168.3.104
pi5	b8 : 27 : eb : dc : c0 : 0c	192.168.3.105
pi6	b8 : 27 : eb : c5 : 4f : 8f	192.168.3.106
pi7	b8 : 27 : eb : f2 : 3c : a9	192.168.3.107
pi8	b8 : 27 : eb : 7f : 25 : 09	192.168.3.108
pi9	b8 : 27 : eb : 79 : a1 : f8	192.168.3.109

Pi1 sends ‘secret’ to Pi2



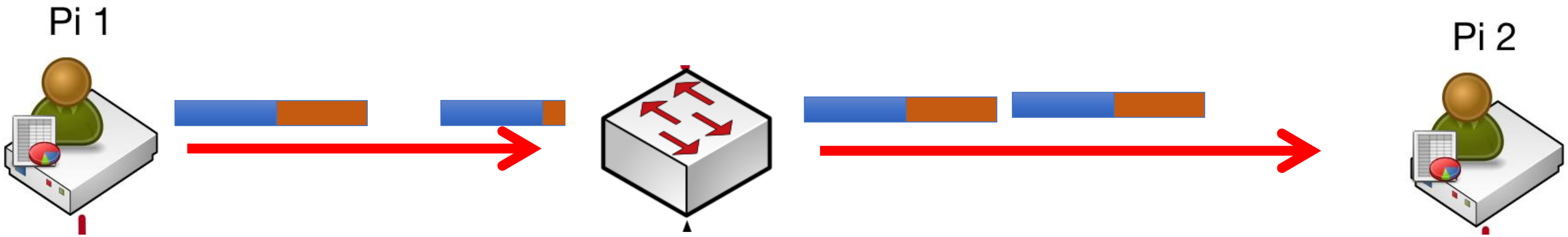
A packet



Piece of Secret

Header

Pi1 sends ‘secret’ to Pi2

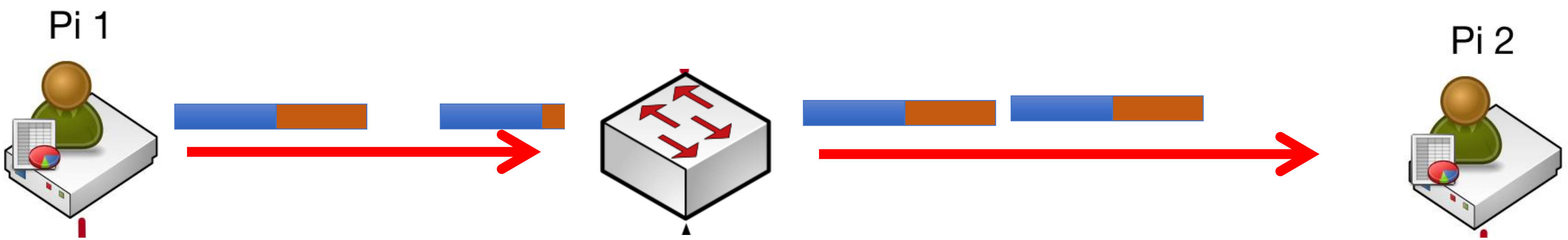


A packet

Piece of Secret	MAC address	IP address	+

Name	Mac Address	IP Address
pi1	b8 : 27 : eb : 9f : 4e : c5	192.168.3.101
pi2	b8 : 27 : eb : be : 80 : c1	192.168.3.102
pi3	b8 : 27 : eb : 89 : 58 : fd	192.168.3.103
pi4	b8 : 27 : eb : 53 : 6a : eb	192.168.3.104
pi5	b8 : 27 : eb : dc : c0 : 0c	192.168.3.105
pi6	b8 : 27 : eb : c5 : 4f : 8f	192.168.3.106
pi7	b8 : 27 : eb : f2 : 3c : a9	192.168.3.107
pi8	b8 : 27 : eb : 7f : 25 : 09	192.168.3.108
pi9	b8 : 27 : eb : 79 : a1 : f8	192.168.3.109

Pi1 sends ‘secret’ to Pi2



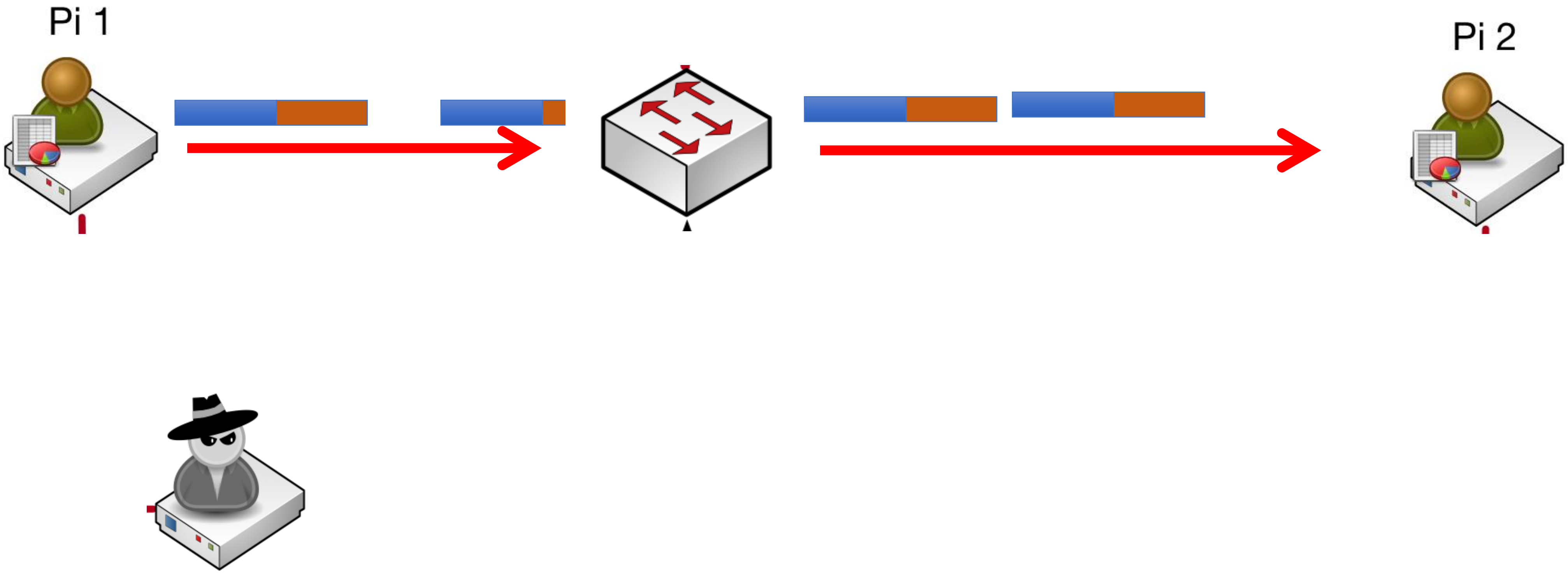
A packet

Piece of Secret	b8 : 27 : eb : be : 80 : c1	192.168.3.102	+

Pi1’s ARP table

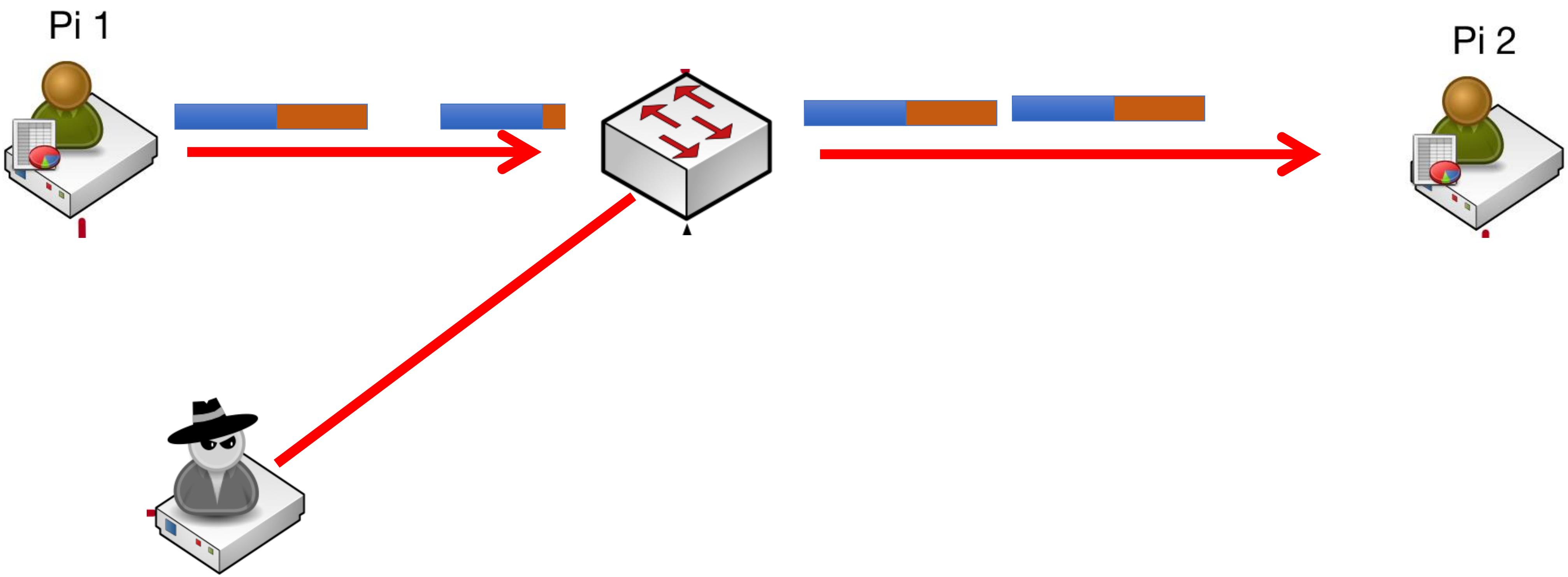
Mac Address	IP Address
b8 : 27 : eb : be : 80 : c1	192.168.3.102
b8 : 27 : eb : 89 : 58 : fd	192.168.3.103
b8 : 27 : eb : 53 : 6a : eb	192.168.3.104
b8 : 27 : eb : dc : c0 : 0c	192.168.3.105
b8 : 27 : eb : c5 : 4f : 8f	192.168.3.106
b8 : 27 : eb : f2 : 3c : a9	192.168.3.107
b8 : 27 : eb : 7f : 25 : 09	192.168.3.108
b8 : 27 : eb : 79 : a1 : f8	192.168.3.109

Evil Eve Evesdropper wants to spy on Pi1 and Pi2 secrets



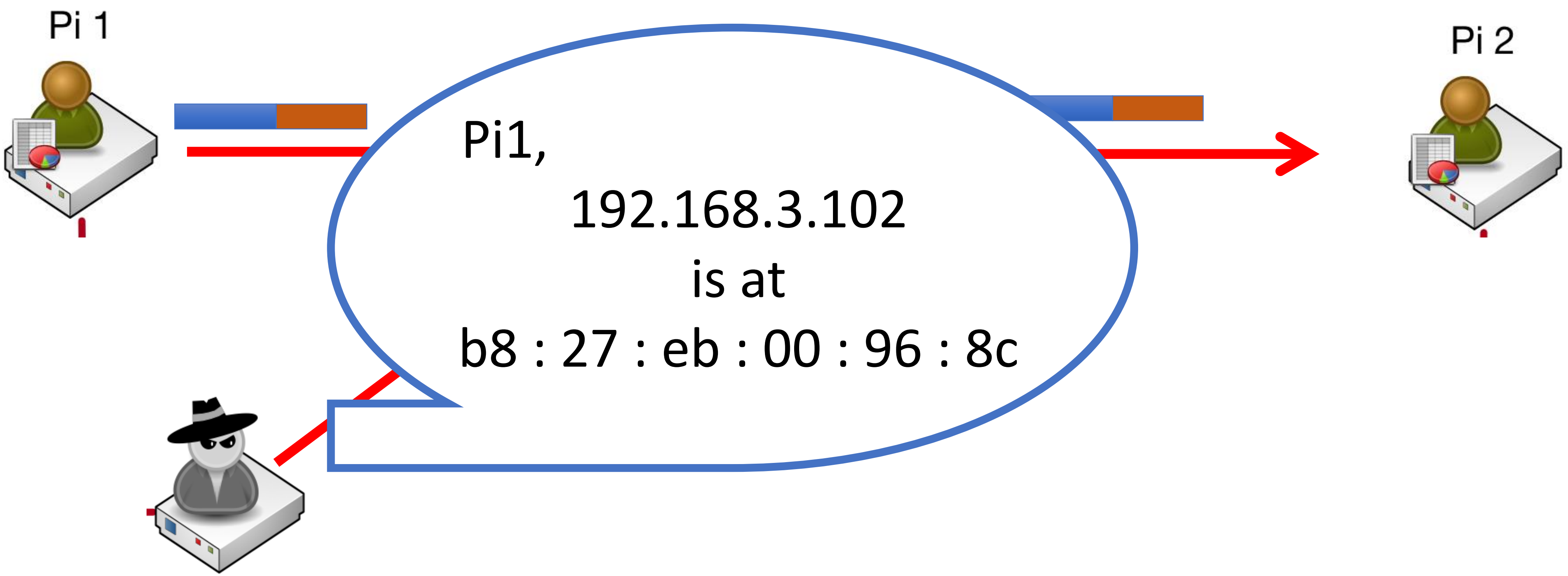
MAC| b8 : 27 : eb : 00 :96 : 8c

Evil Eve Evesdropper wants to spy on Pi1 and Pi2 secrets



MAC| b8 : 27 : eb : 00 :96 : 8c
IP| 192.168.3.120

Evil Eve Evesdropper wants to spy on Pi1 and Pi2 secrets



Pi1,

192.168.3.102

is at

b8 : 27 : eb : 00 : 96 : 8c

MAC| b8 : 27 : eb : 00 :96 : 8c
IP| 192.168.3.120

P1’s ARP Table

192.168.3.120
b8 : 27 : eb : 00 :96 : 8c

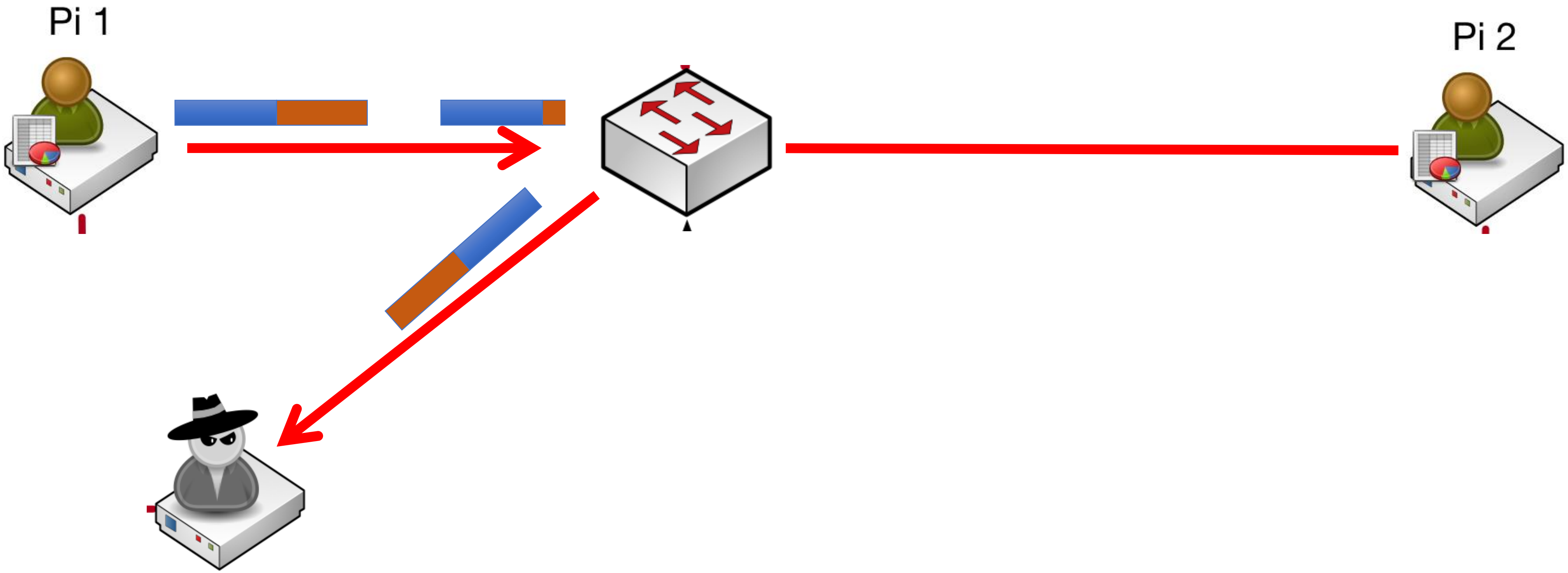
Mac Address	IP Address
b8 : 27 : eb : be : 80 : c1	192.168.3.102
b8 : 27 : eb : 89 : 58 : fd	192.168.3.103
b8 : 27 : eb : 53 : 6a : eb	192.168.3.104
b8 : 27 : eb : dc : c0 : 0c	192.168.3.105
b8 : 27 : eb : c5 : 4f : 8f	192.168.3.106
b8 : 27 : eb : f2 : 3c : a9	192.168.3.107
b8 : 27 : eb : 7f : 25 : 09	192.168.3.108
b8 : 27 : eb : 79 : a1 : f8	192.168.3.109

P1’s ARP Table

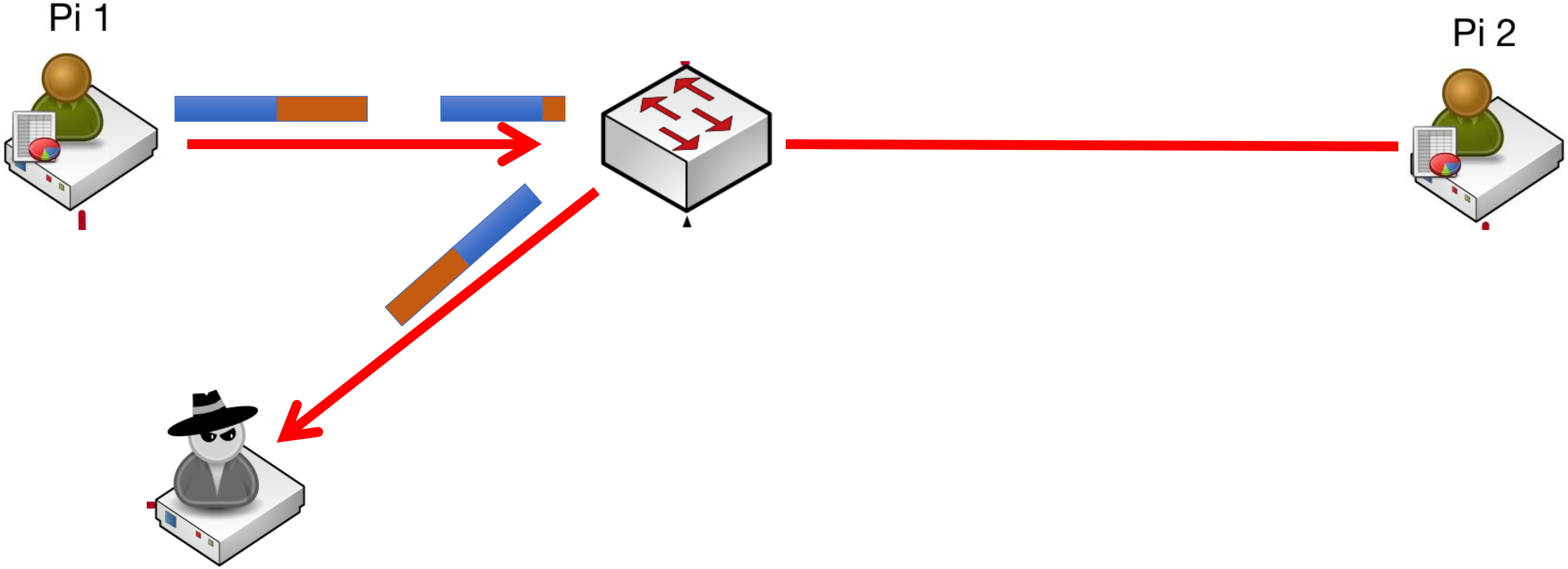
192.168.3.120
b8 : 27 : eb : 00 :96 : 8c

Mac Address	IP Address
b8 : 27 : eb : 00 : 96 : 8c	192.168.3.102
b8 : 27 : eb : 89 : 58 : fd	192.168.3.103
b8 : 27 : eb : 53 : 6a : eb	192.168.3.104
b8 : 27 : eb : dc : c0 : 0c	192.168.3.105
b8 : 27 : eb : c5 : 4f : 8f	192.168.3.106
b8 : 27 : eb : f2 : 3c : a9	192.168.3.107
b8 : 27 : eb : 7f : 25 : 09	192.168.3.108
b8 : 27 : eb : 79 : a1 : f8	192.168.3.109

Evil Eve Evesdropper spies on Pi1 and Pi2 Secrets

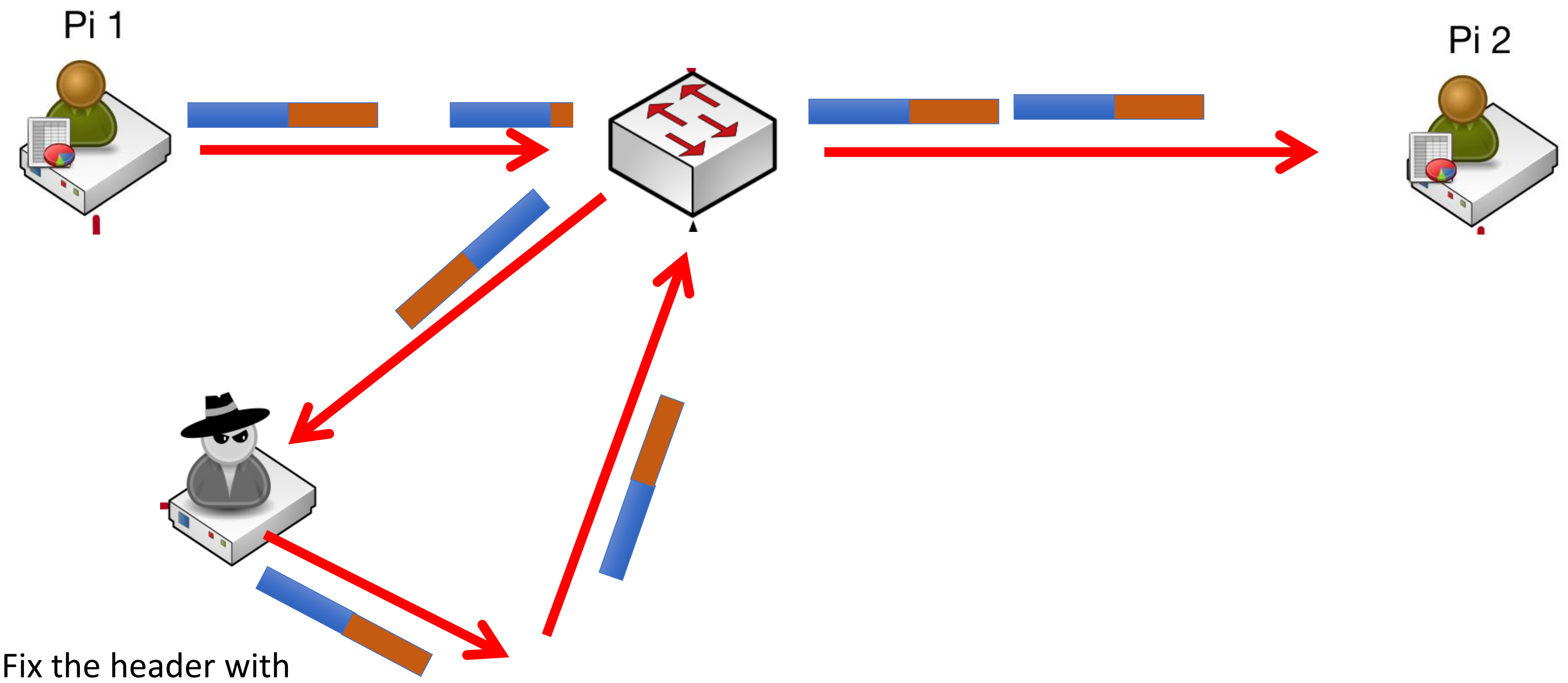


Evil Eve Evesdropper spies on Pi1 and Pi2 Secrets



Fix the header with
correct MAC address

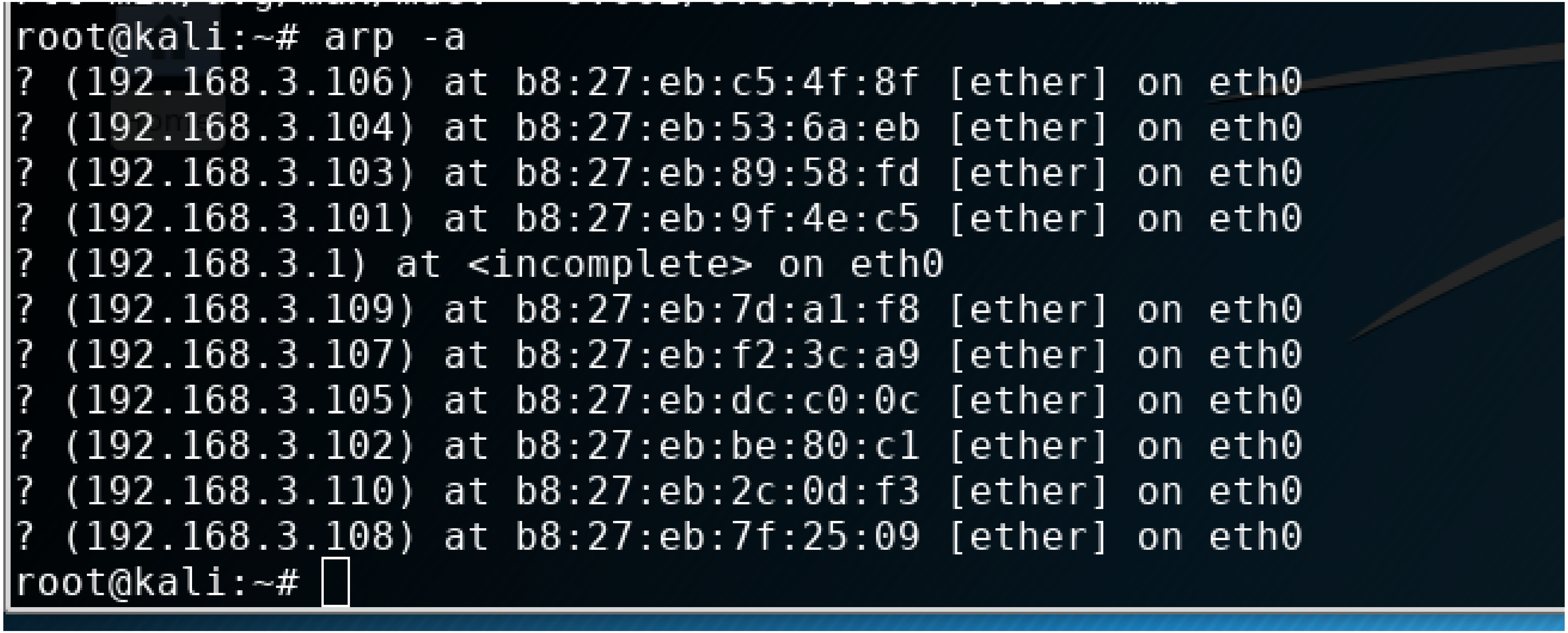
Evil Eve Evesdropper spies on Pi1 and Pi2 Secrets



Fix the header with
correct MAC address

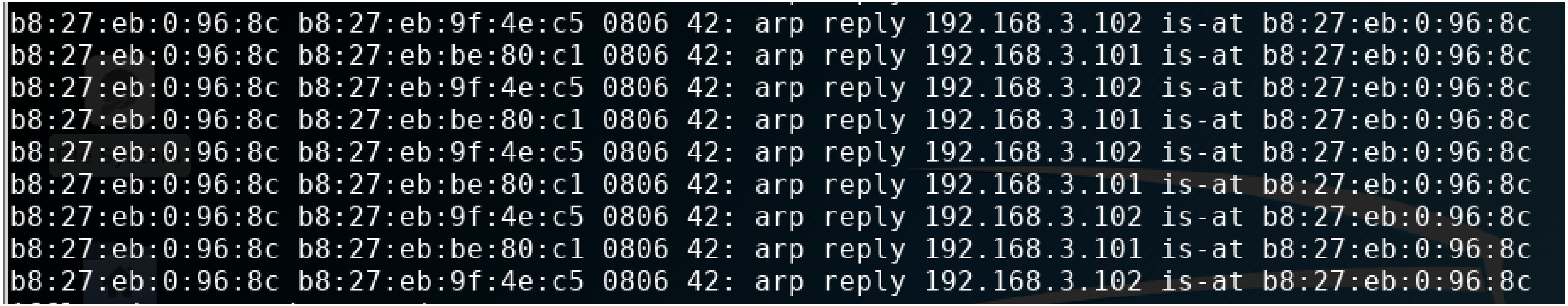
Screen Shots from “Evil Eve

Evil Eve ARP Table



```
root@kali:~# arp -a
? (192.168.3.106) at b8:27:eb:c5:4f:8f [ether] on eth0
? (192.168.3.104) at b8:27:eb:53:6a:eb [ether] on eth0
? (192.168.3.103) at b8:27:eb:89:58:fd [ether] on eth0
? (192.168.3.101) at b8:27:eb:9f:4e:c5 [ether] on eth0
? (192.168.3.1) at <incomplete> on eth0
? (192.168.3.109) at b8:27:eb:7d:a1:f8 [ether] on eth0
? (192.168.3.107) at b8:27:eb:f2:3c:a9 [ether] on eth0
? (192.168.3.105) at b8:27:eb:dc:c0:0c [ether] on eth0
? (192.168.3.102) at b8:27:eb:be:80:c1 [ether] on eth0
? (192.168.3.110) at b8:27:eb:2c:0d:f3 [ether] on eth0
? (192.168.3.108) at b8:27:eb:7f:25:09 [ether] on eth0
root@kali:~# 
```

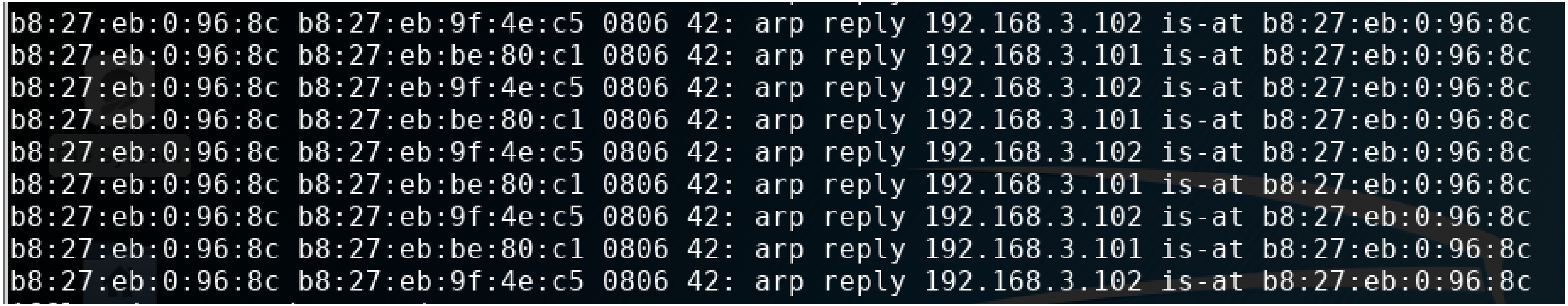
Evil Eve ARP Spoof



```
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
```

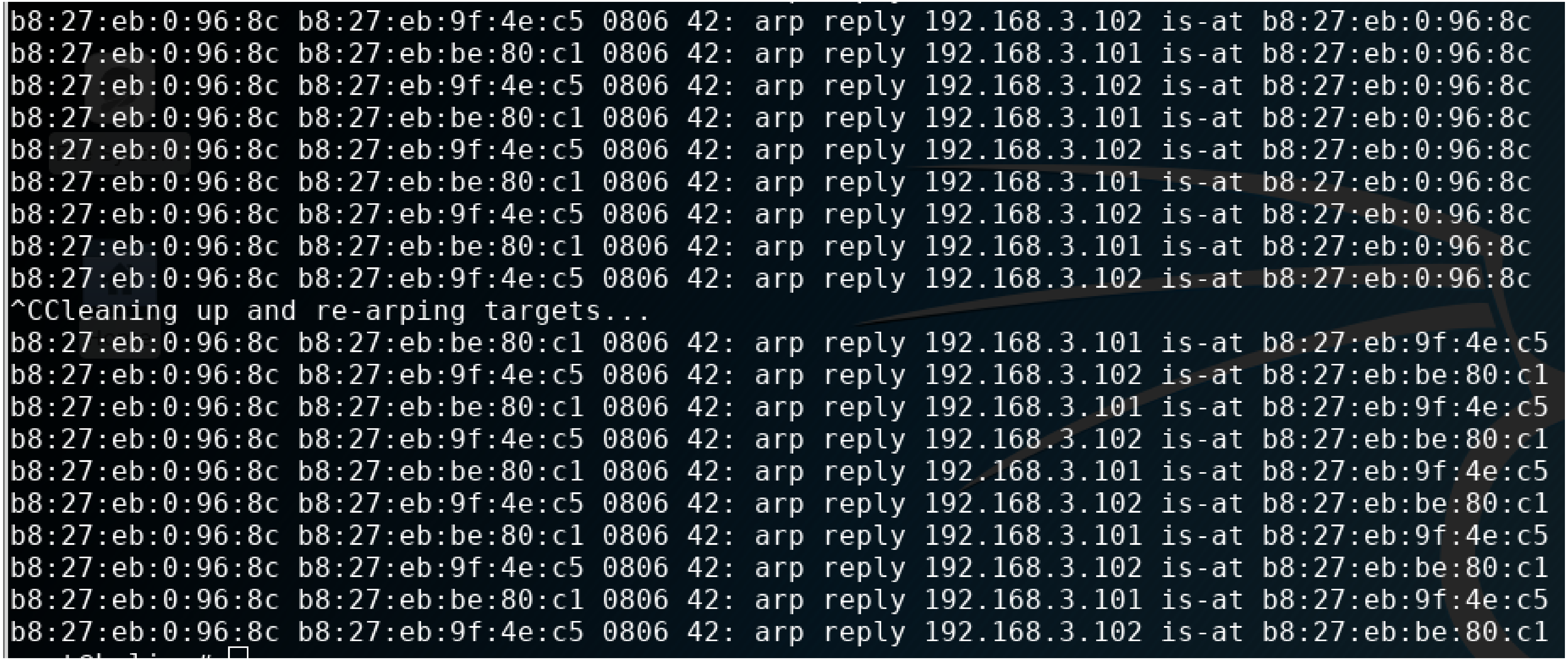
Line 1 translation

Evil Eve Mac   pi1 mac   arp reply   pi2 IP   is – at   Evil Eve Mac



```
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
```

Evil Eve ARP Spoof and Unspoof



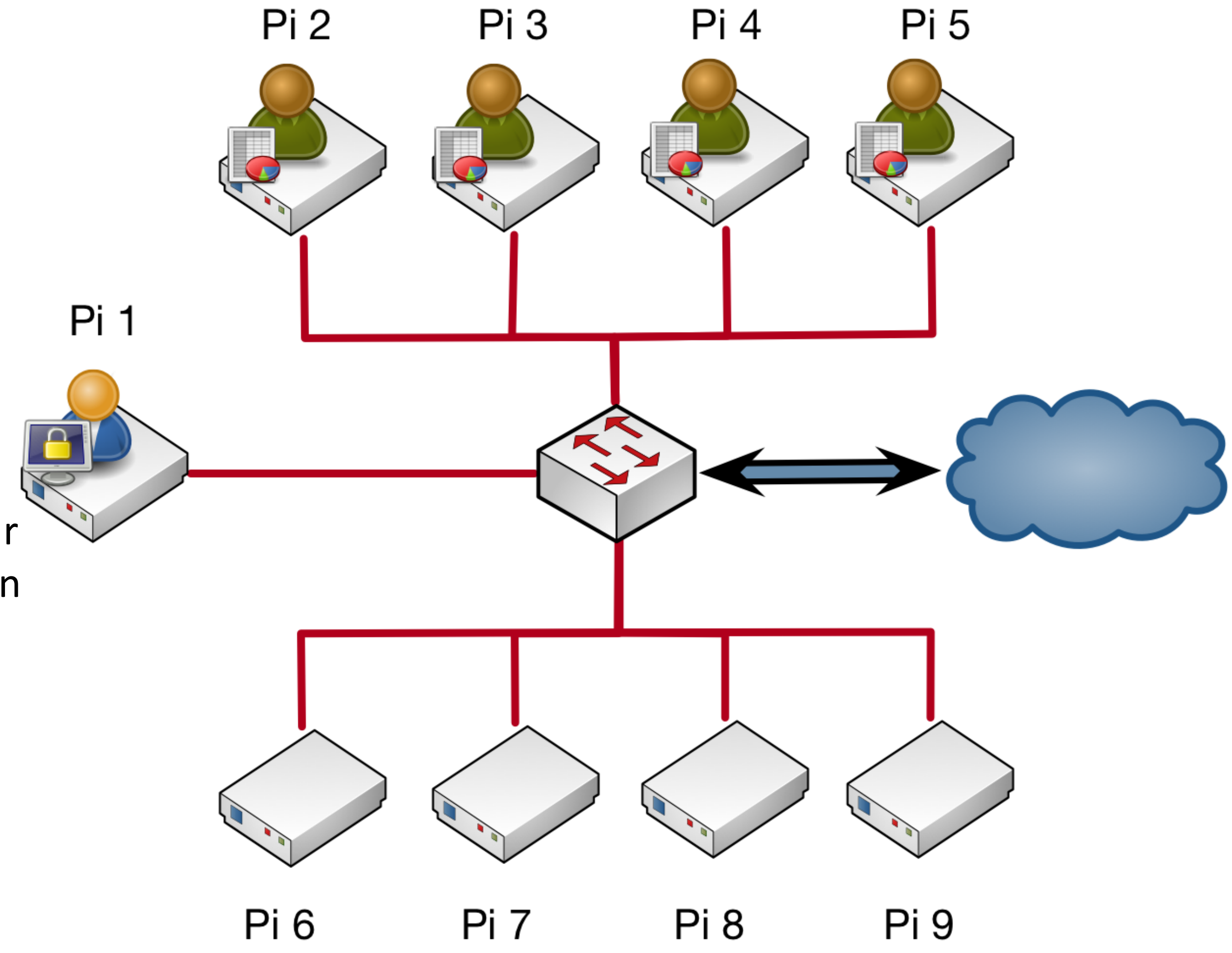
```
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:0:96:8c
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:0:96:8c
^CCleaning up and re-arping targets...
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:9f:4e:c5
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:be:80:c1
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:9f:4e:c5
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:be:80:c1
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:9f:4e:c5
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:be:80:c1
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:9f:4e:c5
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:be:80:c1
b8:27:eb:0:96:8c b8:27:eb:be:80:c1 0806 42: arp reply 192.168.3.101 is-at b8:27:eb:9f:4e:c5
b8:27:eb:0:96:8c b8:27:eb:9f:4e:c5 0806 42: arp reply 192.168.3.102 is-at b8:27:eb:be:80:c1
```

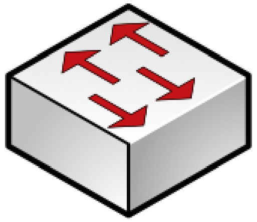
DEMO

EXTRA EXTRA

Tiny Titan: A Simple Network of Computers Talking

Security Sam
Monitors Pis Traffic

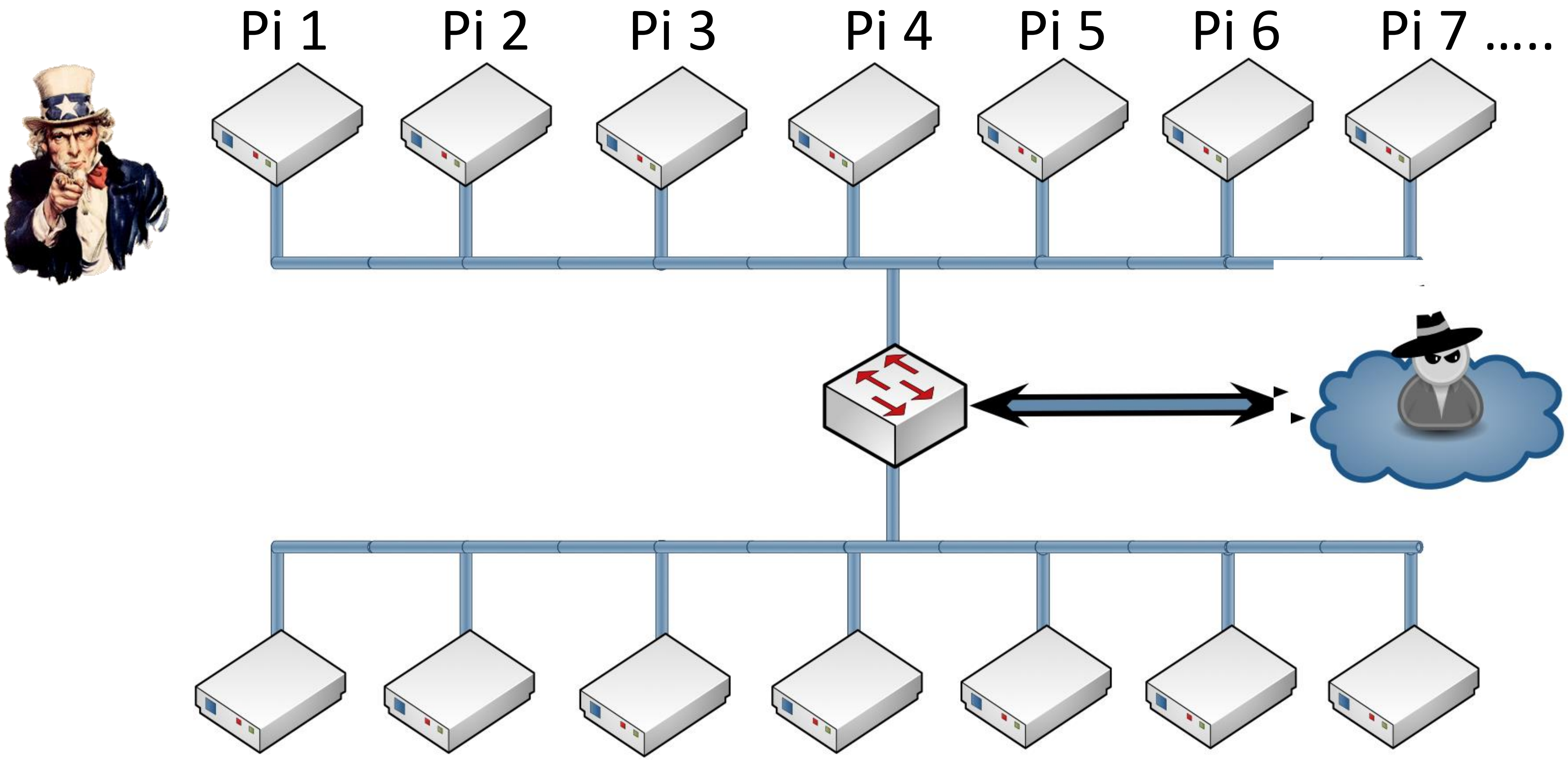




“Need to add ‘Secur
is a Pi and has tap in
all traffic INTO Pi1

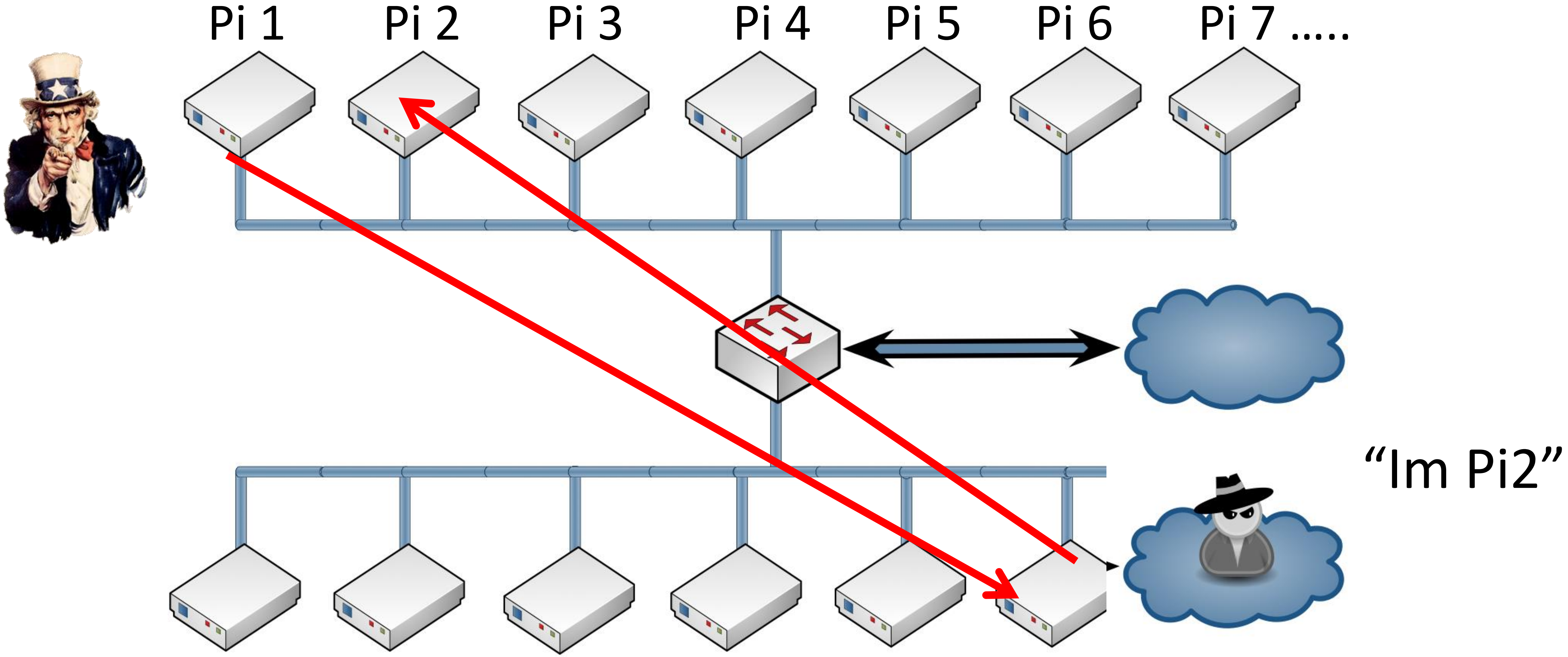
Hacker Hal

Wants to Steal Secrets from Pi1 and Pi2



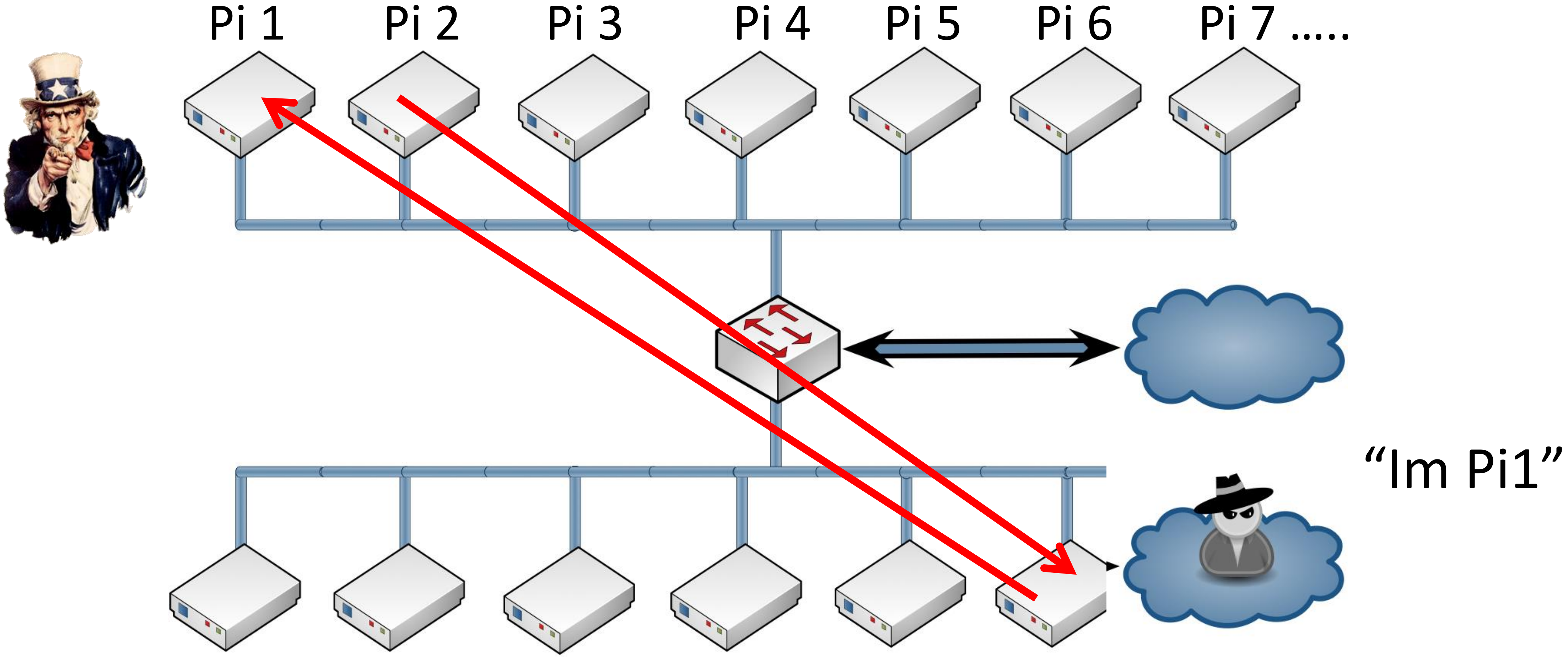
Hacker Hal

Tricks Pi1 into thinking HH is Pi2

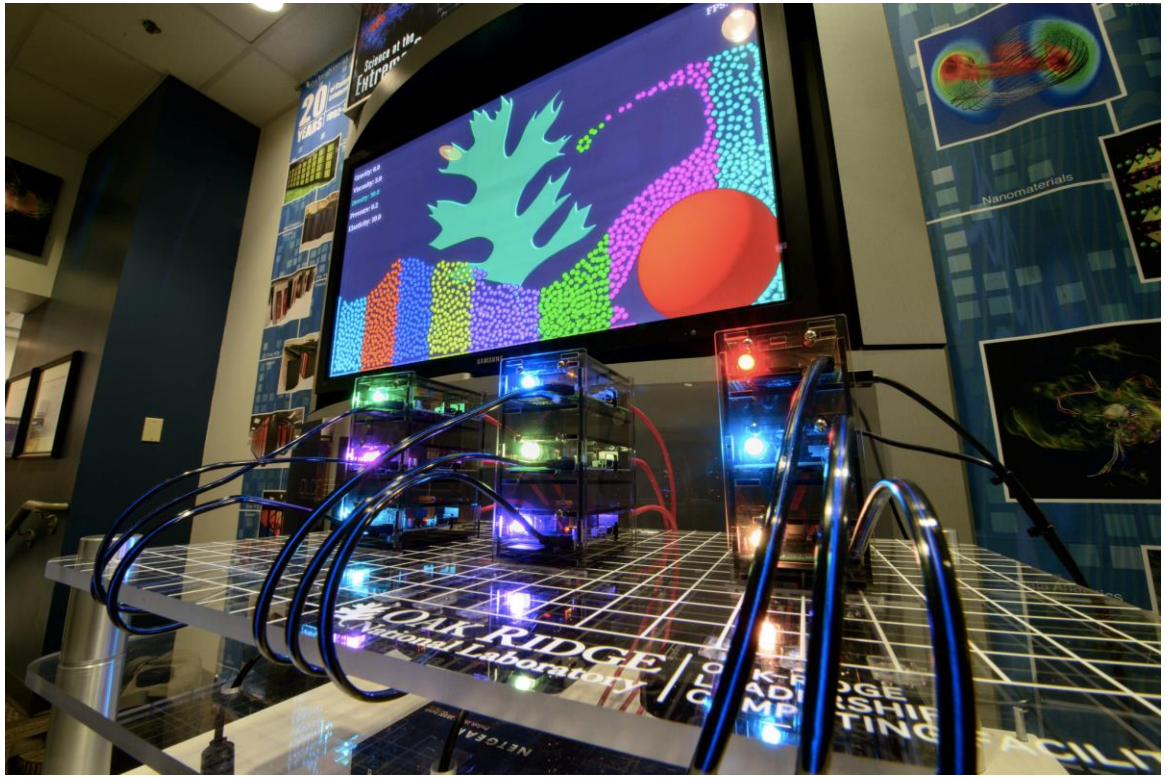


Hacker Hal

Tricks Pi2 into thinking HH is Pi1



Mini Demo:
Stealing Secrets: “ARP” Poisoning



Acknowledgement

Adam Simpson (Oak Ridge National Laboratory, NVIDIA) and Robert French (Oak Ridge National Laboratory) for support with Tiny Titan.

This presentation used resources of the Argonne Leadership Computing Facility at Argonne National Laboratory, which is supported by the Office of Science of the U.S. Department of Energy, Office of Science, under contract number DE-AC02-06CH11357.