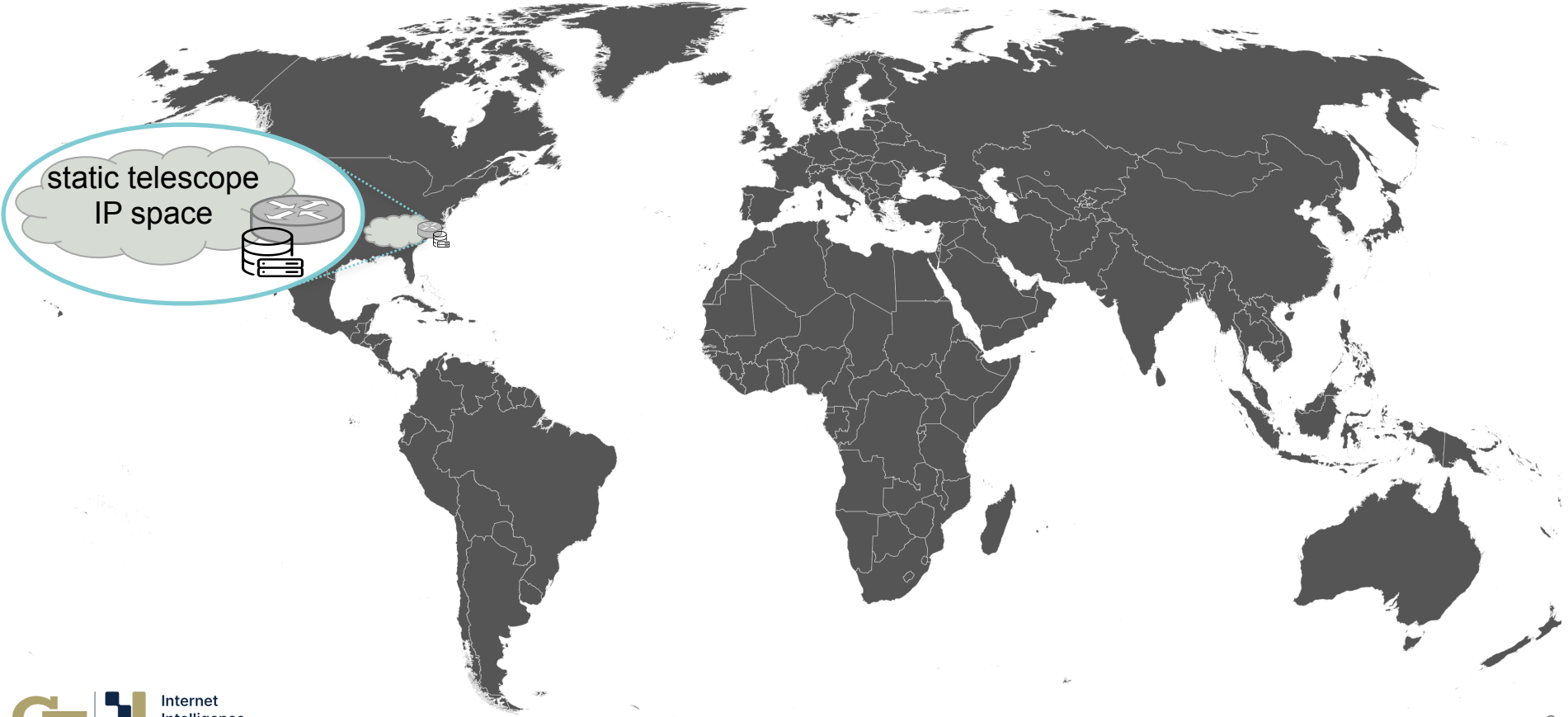
MORP4:
A Dynamic Network Telescope

I. Xygkou, *J. K. Sojan, D. Rauthan, F. Zhu,*
T. Holterbach, S. Alcock, B. Flanagan, A. Saeed, A. Dainotti

NSDI 2026, Renton, U.S.A.

Internet Intelligence Lab

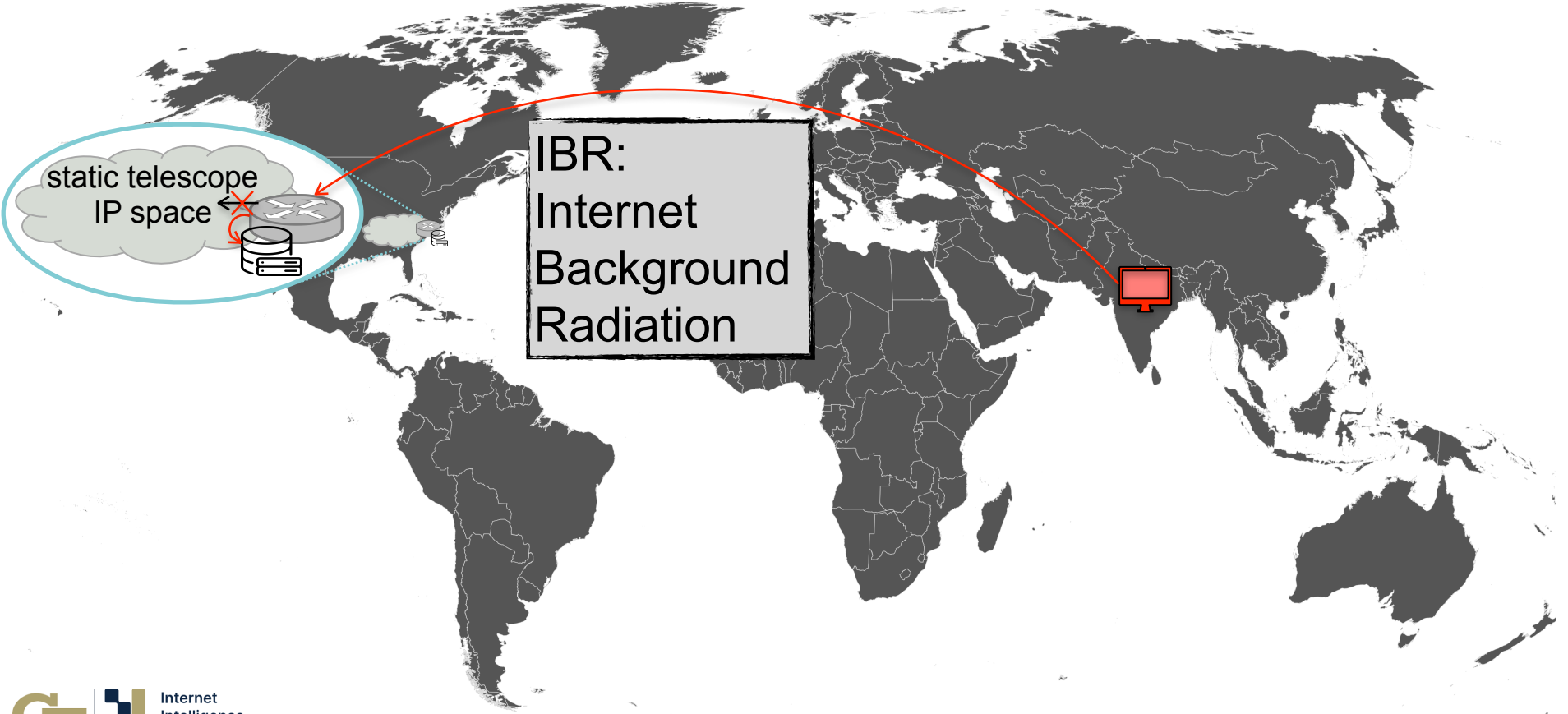
What is a Network Telescope?



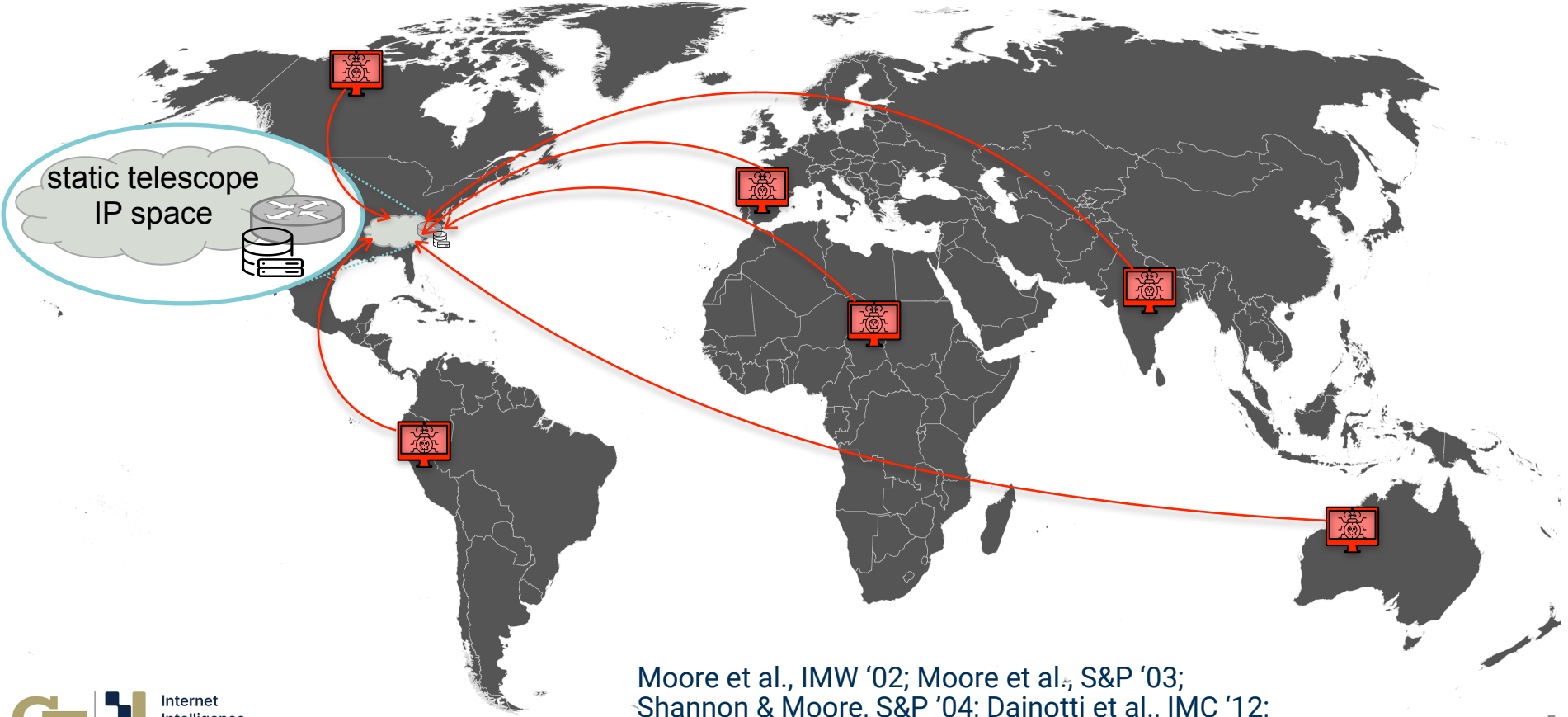
What is a Network Telescope?

Internet Intelligence Lab

What is a Network Telescope?

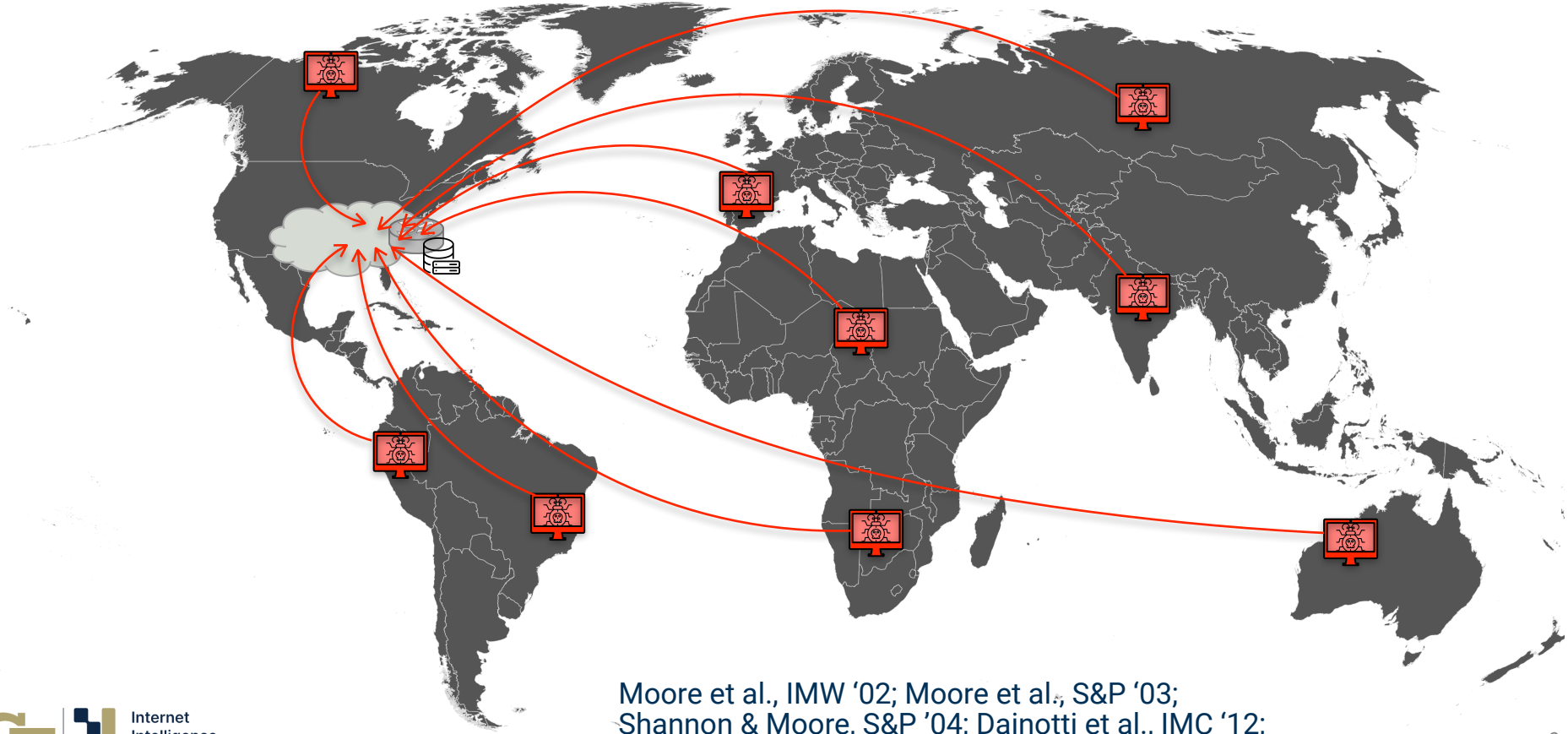


Detecting/Studying Malware & Botnets



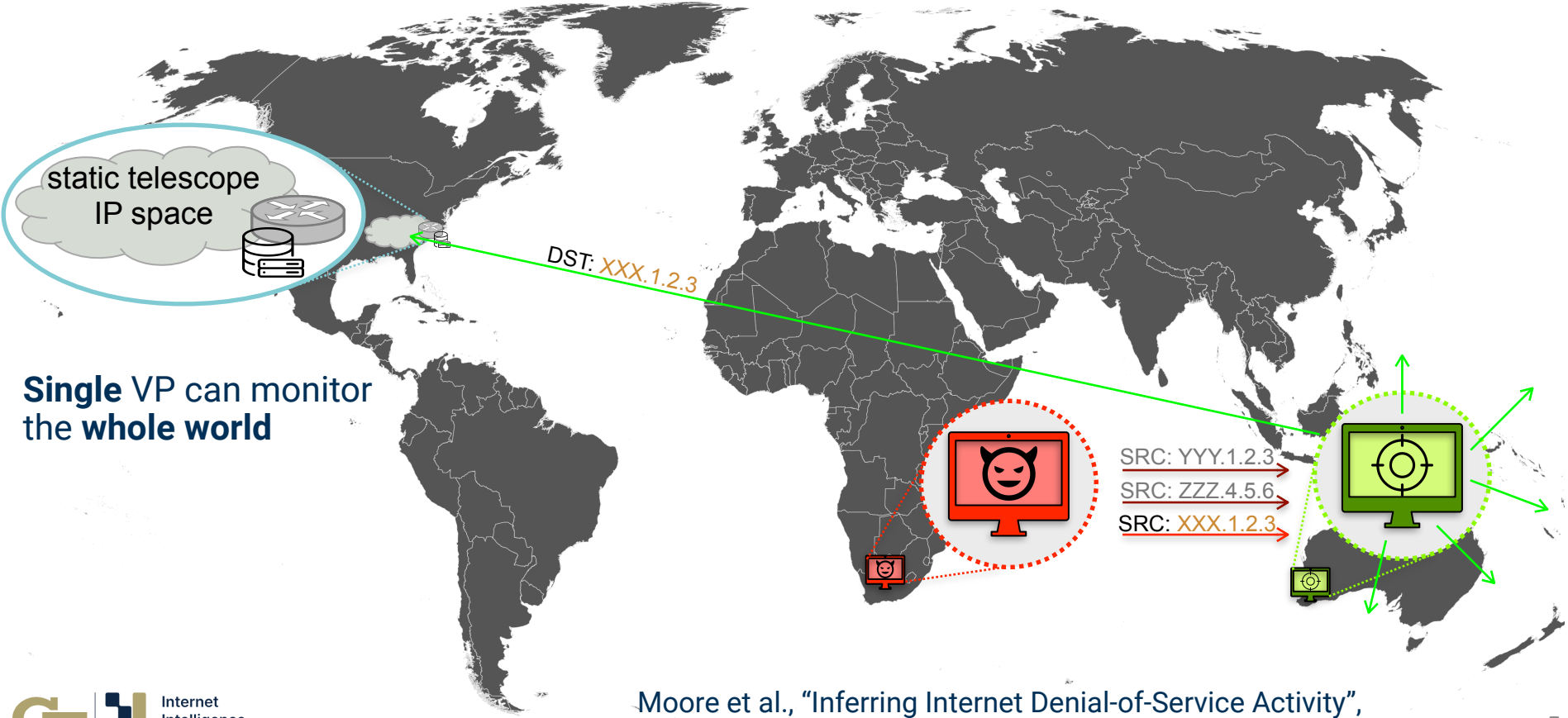
Moore et al., IMW ‘02; Moore et al., S&P ‘03;
Shannon & Moore, S&P ’04; Dainotti et al., IMC ‘12;
Raftopoulos et al., TMA ‘15

Detecting/Studying Malware & Botnets



Moore et al., IMW ‘02; Moore et al., S&P ‘03;
Shannon & Moore, S&P ’04; Dainotti et al., IMC ‘12;
Raftopoulos et al., TMA ‘15

Detecting Spoofed DoS attacks Worldwide



Single VP can monitor the **whole world**

Moore et al., "Inferring Internet Denial-of-Service Activity", USENIX Sec '01 — *USENIX Sec '17 Test of Time Award*

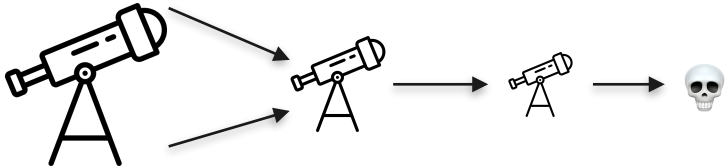
More applications of network telescopes

- Bugs & misconfigurations
  - Benson et al., *IMC ‘15*
- Scanners
  - Durumeric et al., *USENIX Security ’14*
  - Richter et al., *IMC ’19*
  - Hiesgen et al., *USENIX Security ’22*
  - Pauley et al., *USENIX Security '23*
- Large-scale disconnections & shutdowns
  - Dainotti et al., *IMC ’11*
  - Bischof et al., *SIGCOMM ’23*
- …

Limitations of traditional telescopes

LIM.1

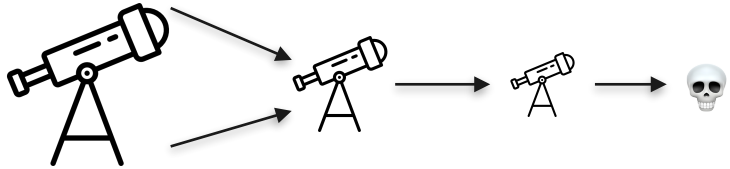
Shrinking / Disappearing



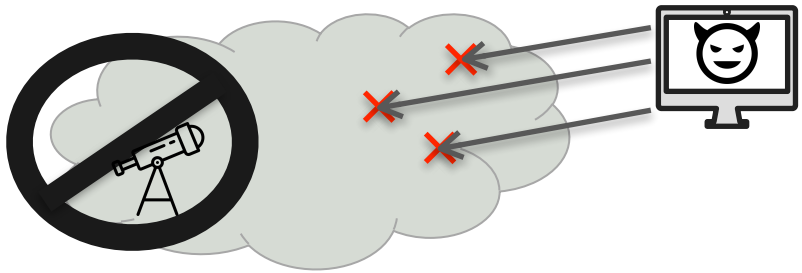
Internet Intelligence Lab

Limitations of traditional telescopes

LIM.1 Shrinking / Disappearing



LIM.2 Blacklisting

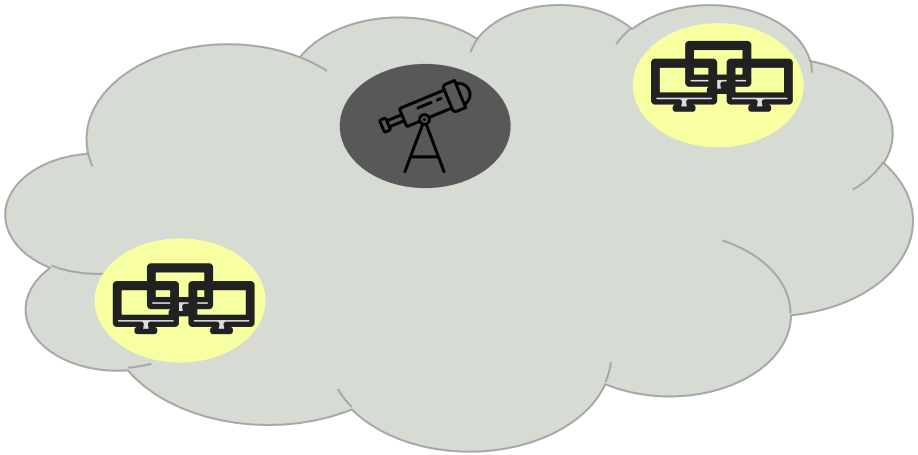


*Manos Antonakakis et al.
“**Understanding the Mirai Botnet**”. USENIX Security ‘17.

Limitations of traditional telescopes

LIM.3

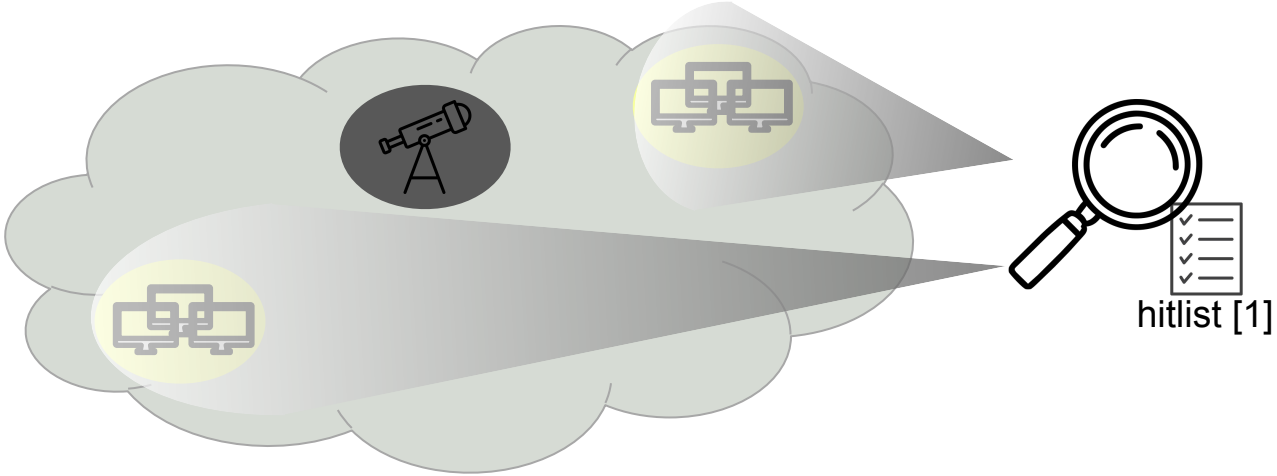
IPv6 IBR is hard to capture



Limitations of traditional telescopes

LIM.3

IPv6 IBR is hard to capture

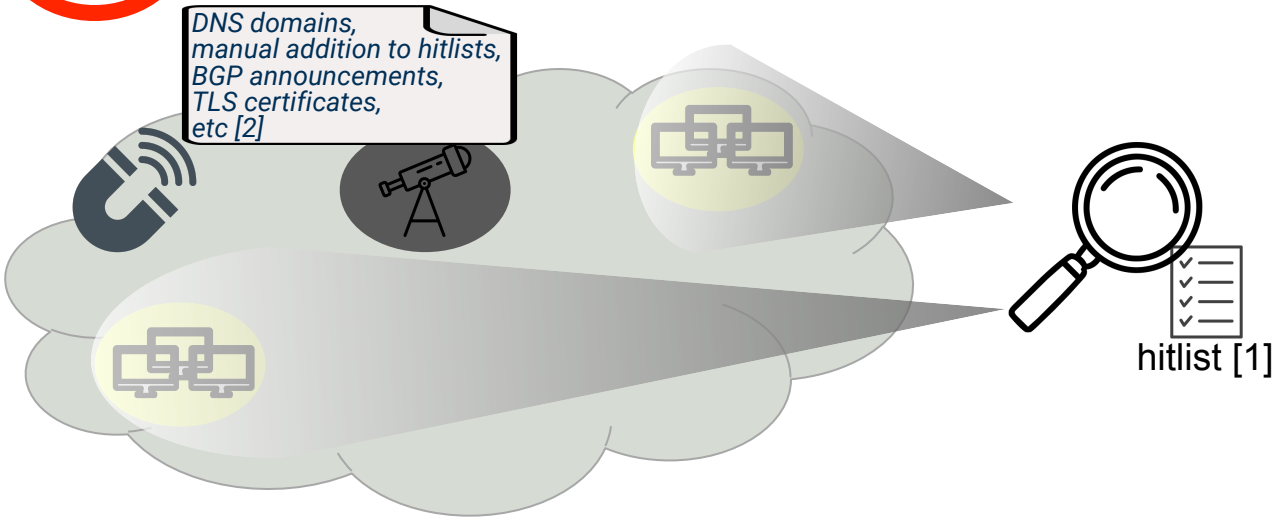


[1] Oliver Gasser et al. “Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists”. IMC ’18.

Limitations of traditional telescopes

LIM.3

IPv6 IBR is hard to capture



[1] Oliver Gasser et al. “Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists”. IMC ’18.
[2] Tanveer et al., USENIX ‘23; Zhao et al., PAM ‘24; Zhao et al., IEICE Trans. Comm. ‘25; Xin et al. SIGCOMM ‘25 (poster); Egloff et al., CoNEXT ‘25; Tanveer et al., CoNEXT ‘25

Limitations of traditional telescopes

LIM.1 Shrinking

LIM.2 Blacklisting

LIM.3 IPv6 IBR locality

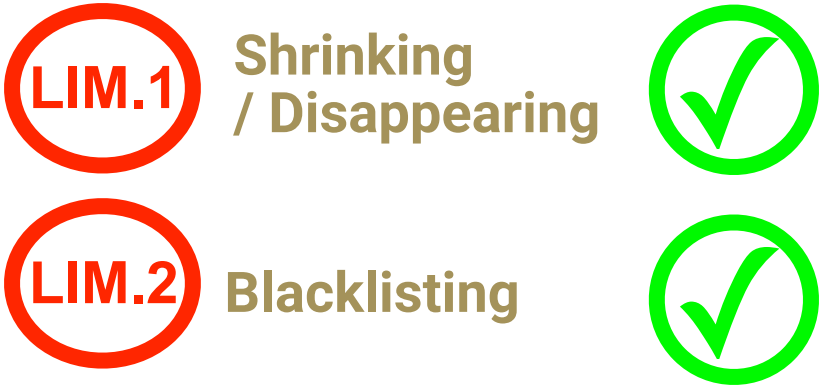
Dynamic Telescope

What is a *dynamic* telescope?

Detect in real time which portions of a network are/become **unutilized** in order to maximize capture of IBR.

What is a *dynamic* telescope?

Detect in real time which portions of a network are/become **unutilized** in order to maximize capture of IBR.



What is a *dynamic* telescope?

Detect in real time which portions of a network are/become **unutilized** in order to maximize capture of IBR.

How do we implement a dynamic telescope?

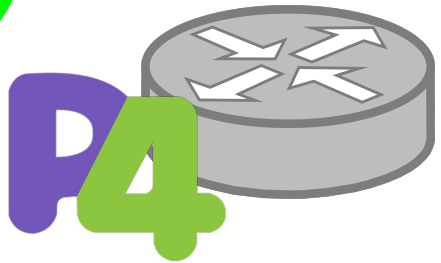
Requirements

- Non-intrusive
  → No address reservation
- Accurate
  → Detect all (and only) utilized IPs
- Line-rate

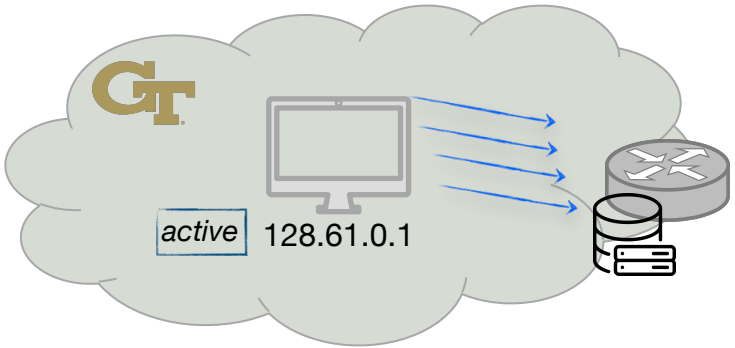
Requirements

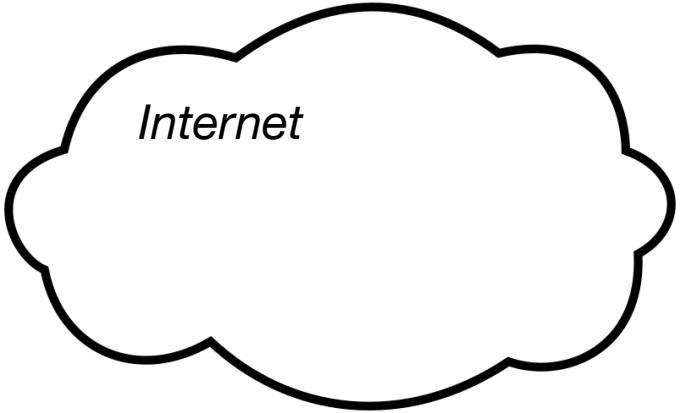
- Non-intrusive
  → No address reservation
- Accurate
  → Detect all (and only) utilized IPs
- Line-rate

MORP4

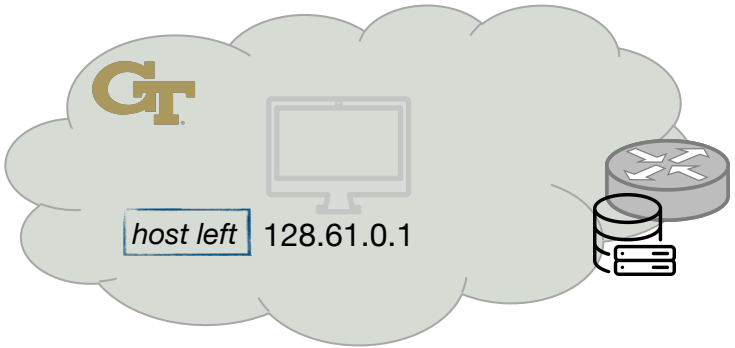


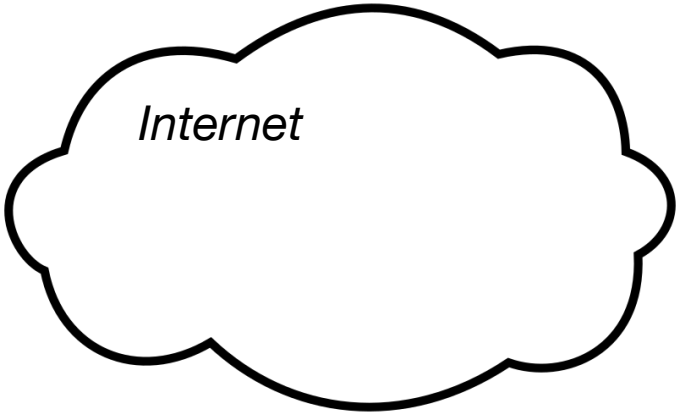
Detecting inactive IPs





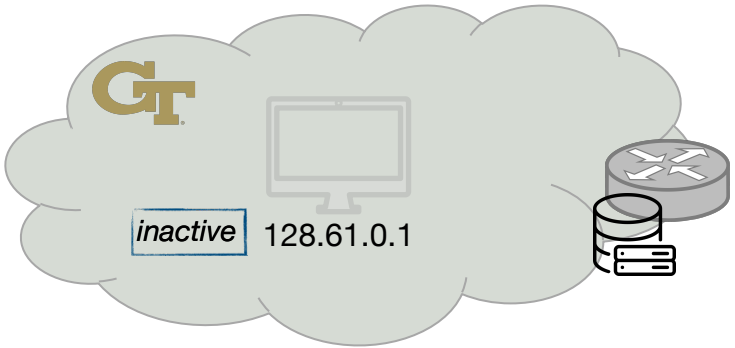
Detecting inactive IPs

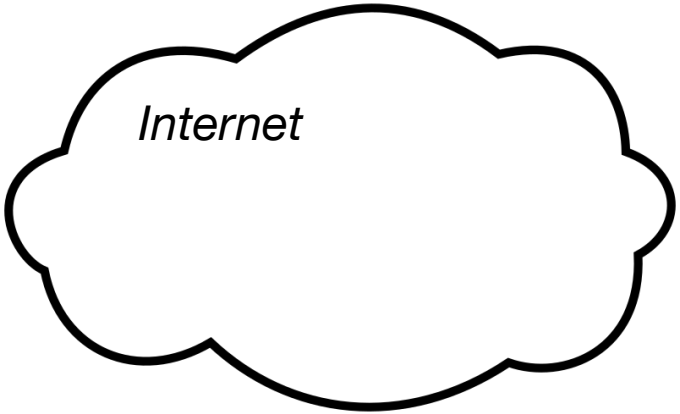




Detecting inactive IPs

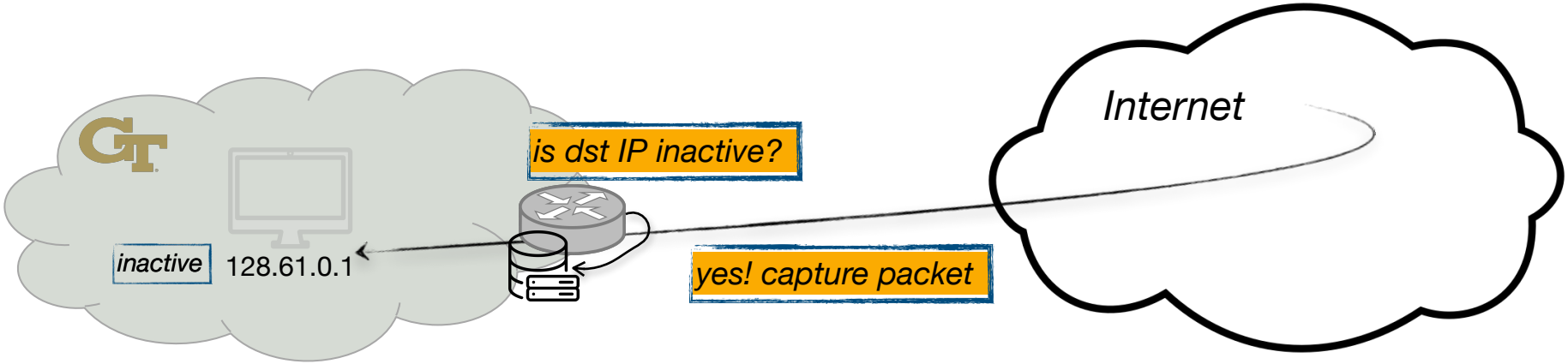
After a *timeout…*



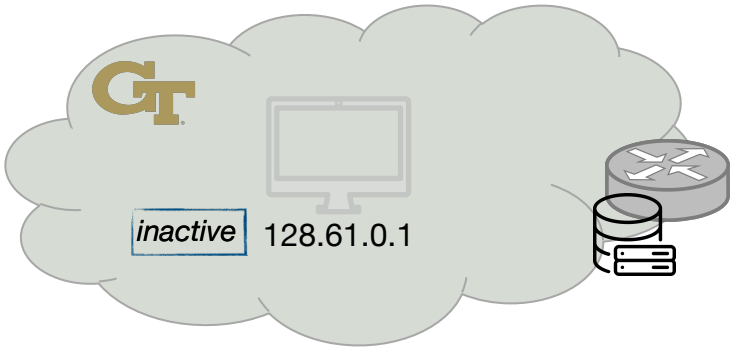


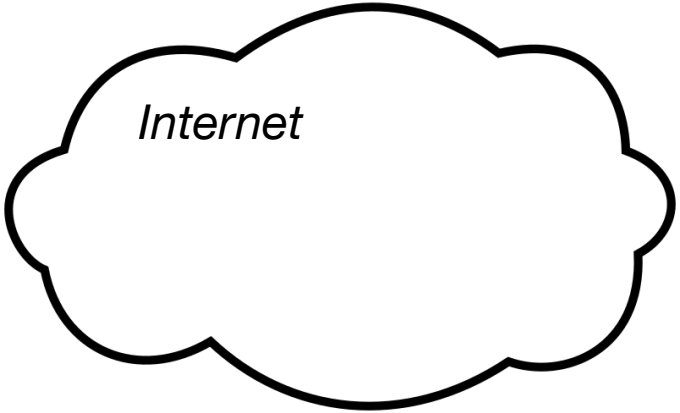
Detecting inactive IPs

After a *timeout…*

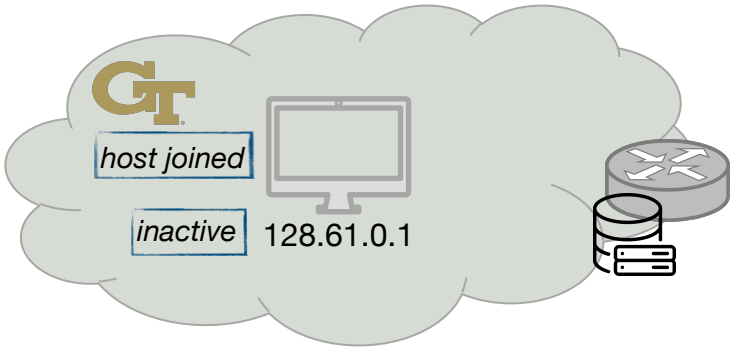


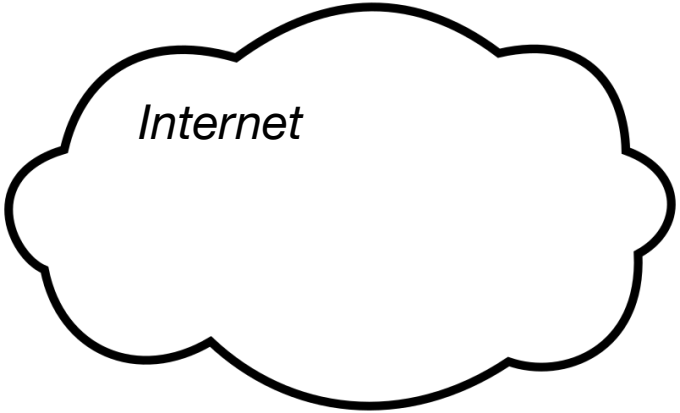
Detecting active IPs



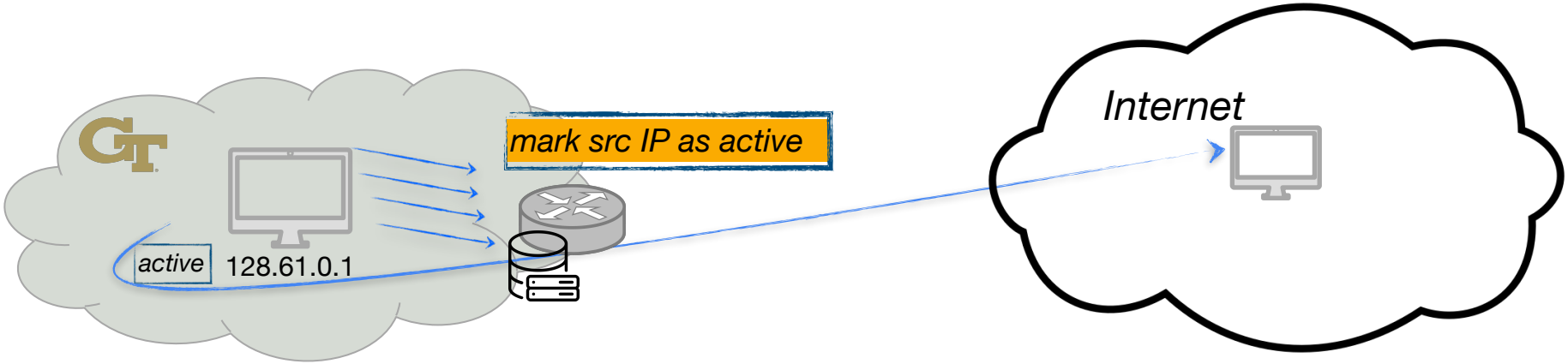


Detecting active IPs

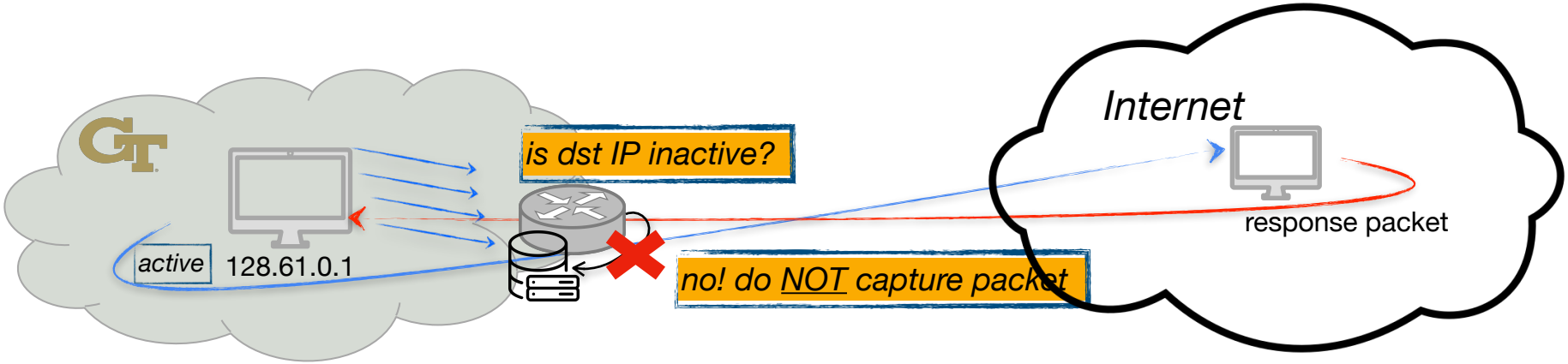




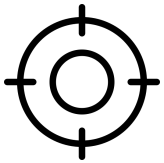
Detecting active IPs



Detecting active IPs



Objectives & Challenges



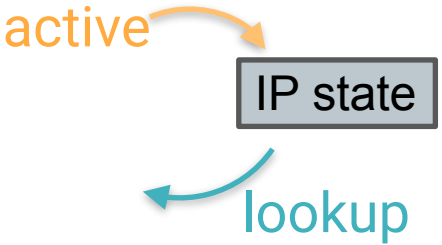
Obj. 1: State consistency

Obj. 1: State consistency

CH.1 At line-rate

Two operations:

- Mark an IP as active (write)
- Check if pkt is to an inactive IP (read)



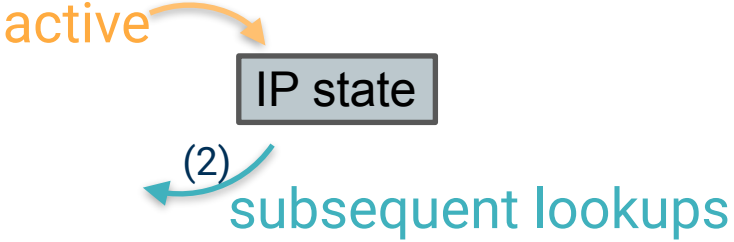
Obj. 1: State consistency

CH.1 At line-rate

Two operations:

- Mark an IP as active (write)
- Check if pkt is to an inactive IP (read)

(1) Order of operations matters!



Internet Intelligence Lab

Obj. 1: State consistency

CH.1 At line-rate

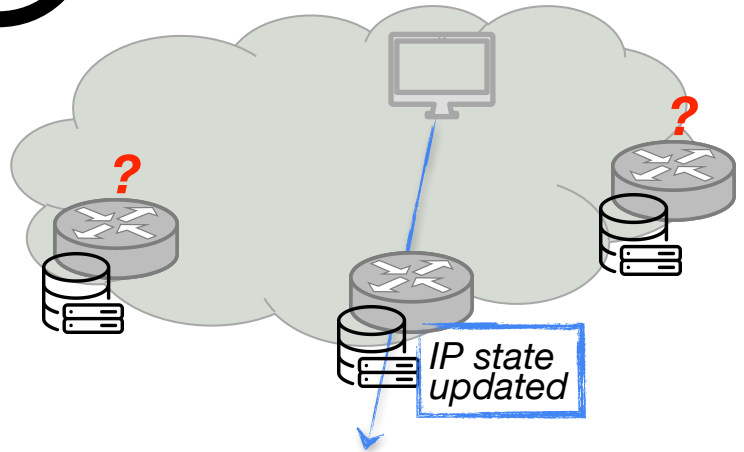
Two operations:

- Mark an IP as active (write)
- Check if pkt is to an inactive IP (read)

(1) Order of operations matters!

active → IP state → (2) subsequent lookups

CH.2 Across multiple points



Obj. 1: State consistency

CH.1 At line-rate

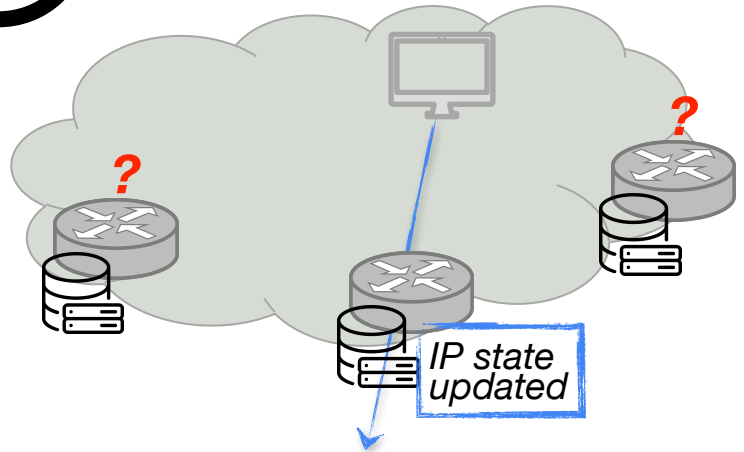
Two operations:

- Mark an IP as active (write)
- Check if pkt is to an inactive IP (read)

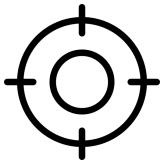
(1) Order of operations matters!

active → IP state → (2) subsequent lookups

CH.2 Across multiple points



CH.3 Limited resources



Obj. 2: Configurability

Different networks have different characteristics.

Network operators can configure parameters:

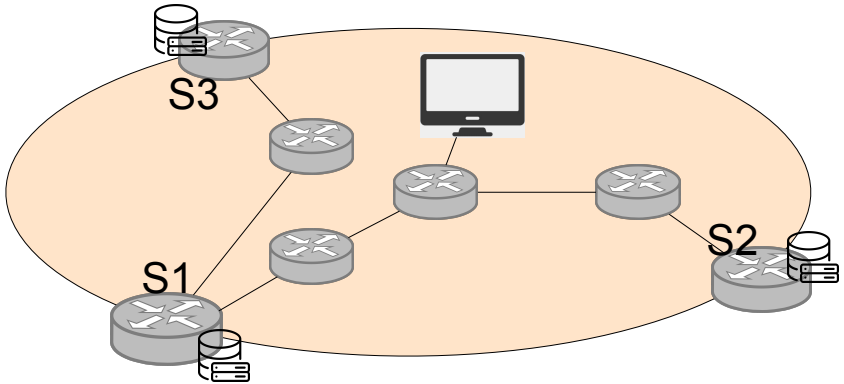
- Monitored subnets
- Monitoring granularity, e.g., in IPv4: /24 or /32
- Timeout, e.g., 6 hrs, or 1 day, or 7 days

State consistency

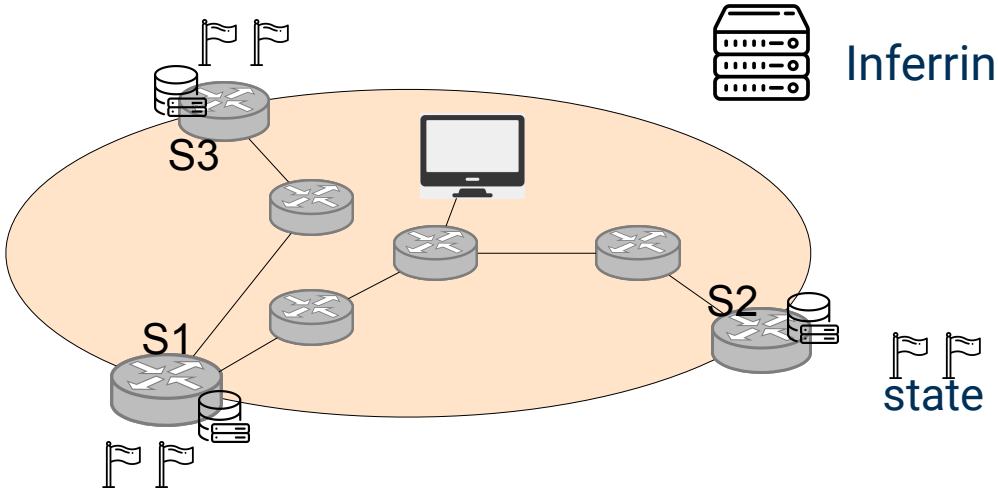
Configurability

MORP4 implements
a *dynamic telescope* in
~430 P4 & ~1,100 C++ lines

Achieving state consistency

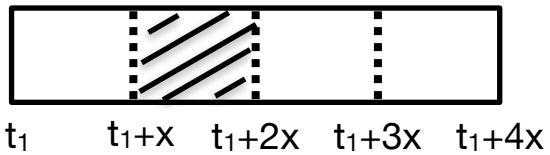


Achieving state consistency through controller

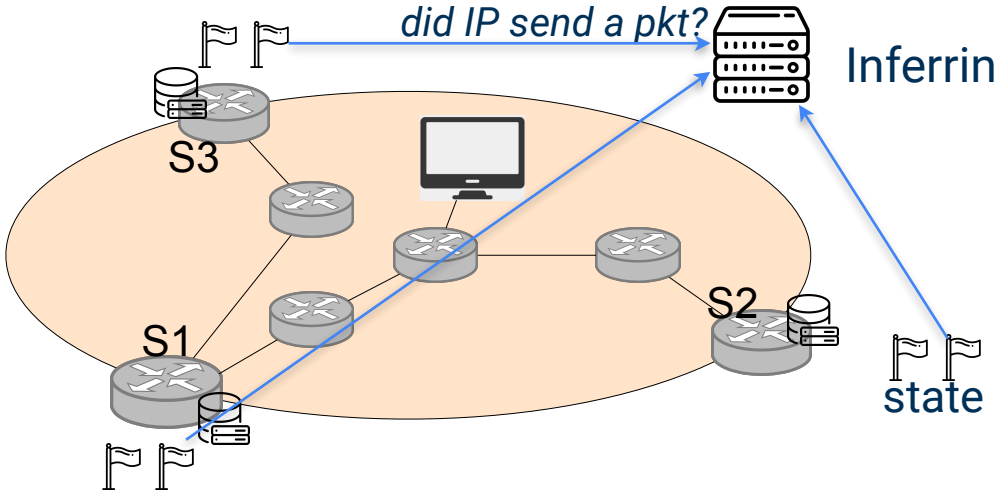


Inferring an IP as inactive is non-time-sensitive

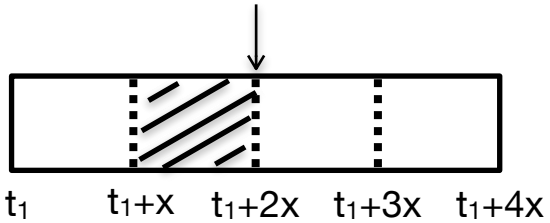
state



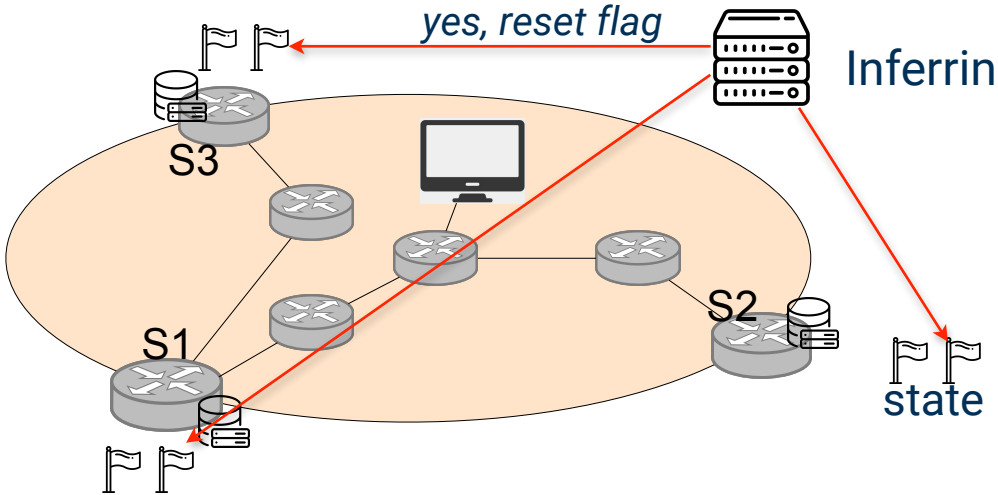
Achieving state consistency through controller



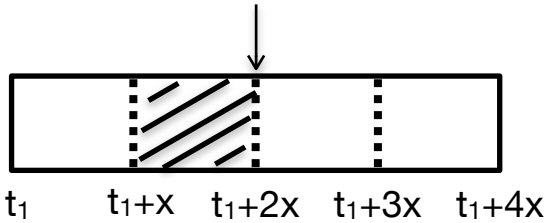
Inferring an IP as inactive is non-time-sensitive



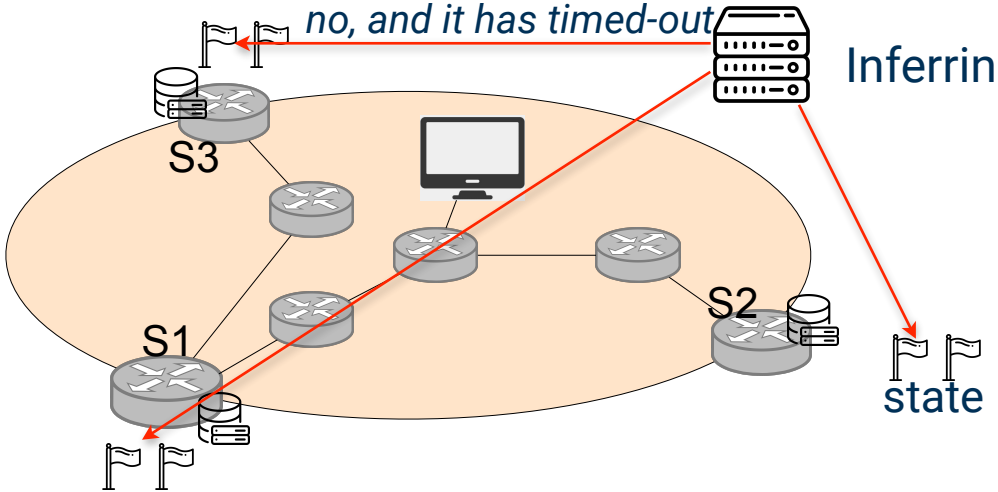
Achieving state consistency through controller



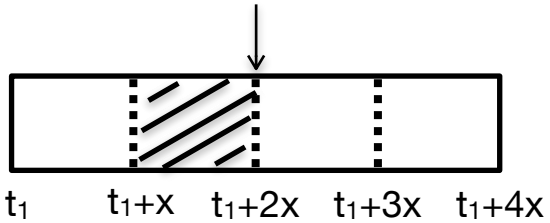
Inferring an IP as inactive is non-time-sensitive



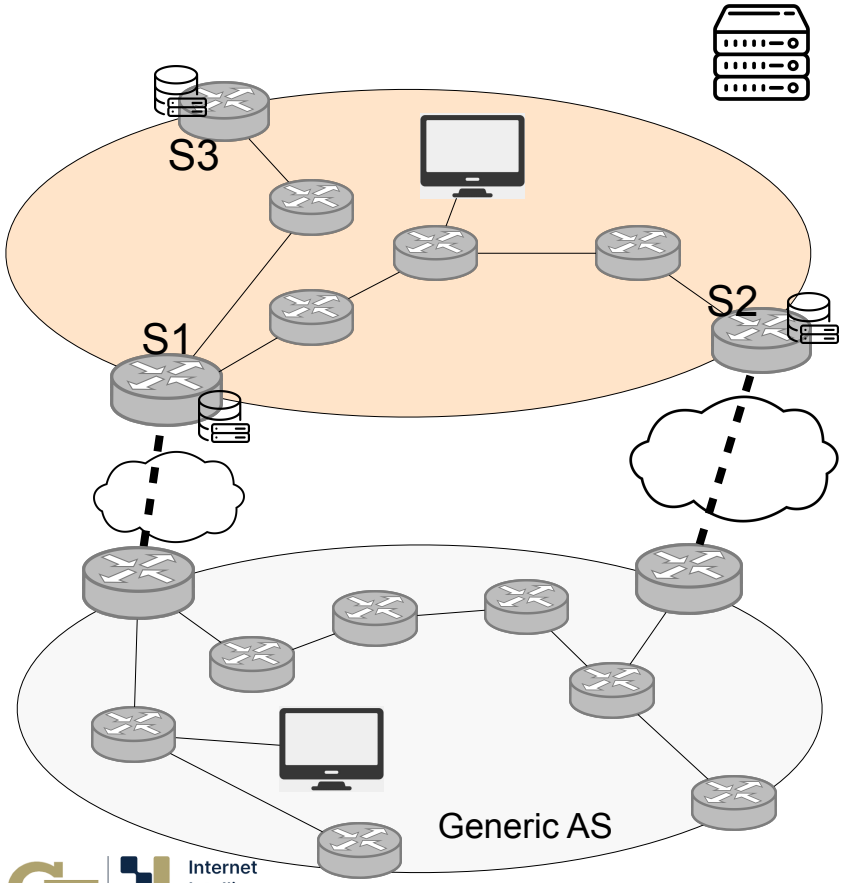
Achieving state consistency through controller

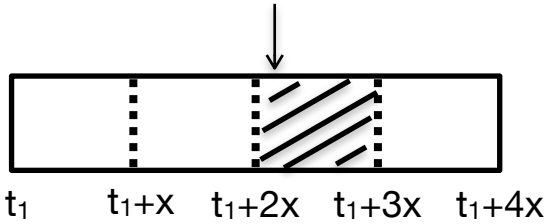


Inferring an IP as inactive is non-time-sensitive



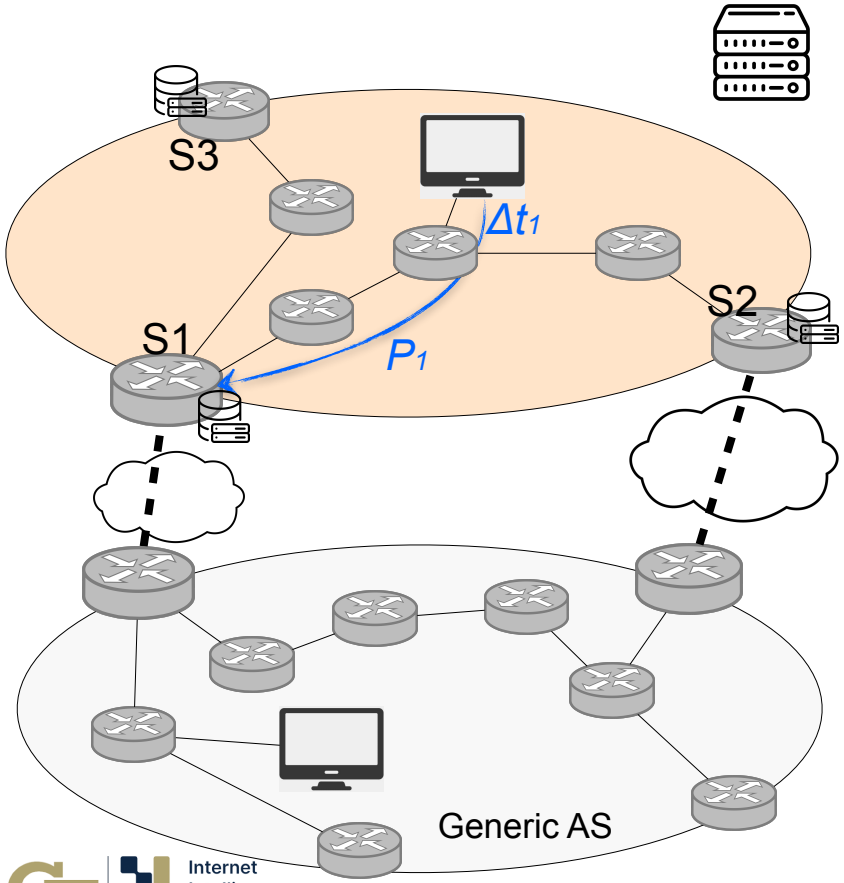
Achieving state consistency through control packets

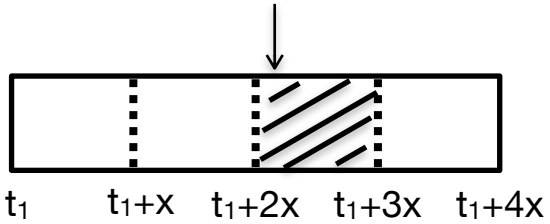




Internet Intelligence Lab

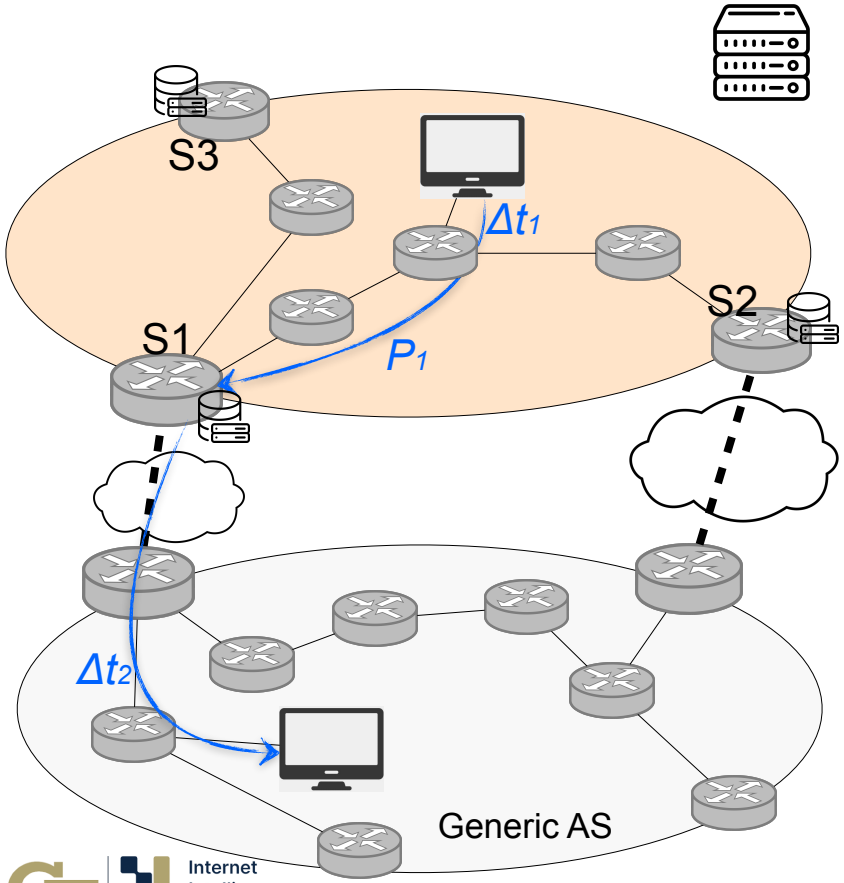
Achieving state consistency through control packets

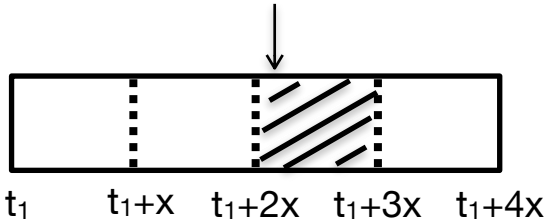




Internet Intelligence Lab

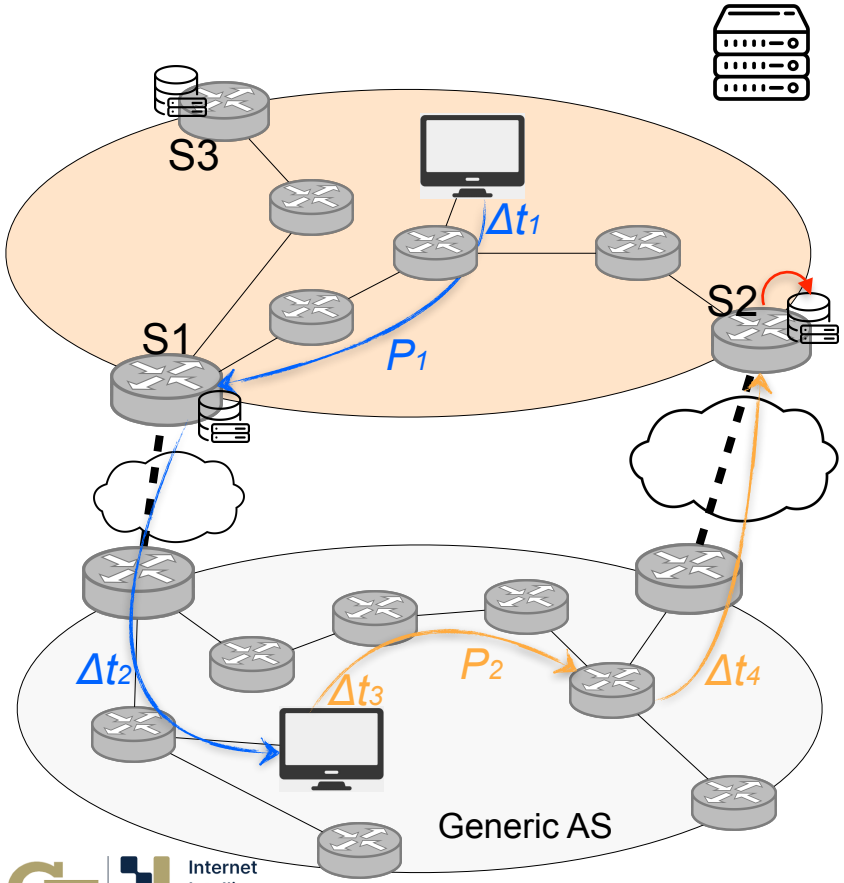
Achieving state consistency through control packets

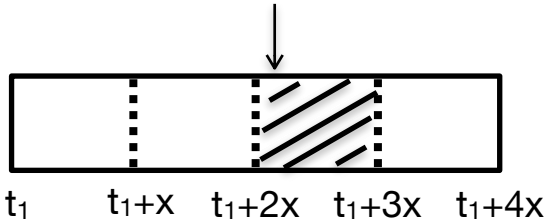




Internet Intelligence Lab

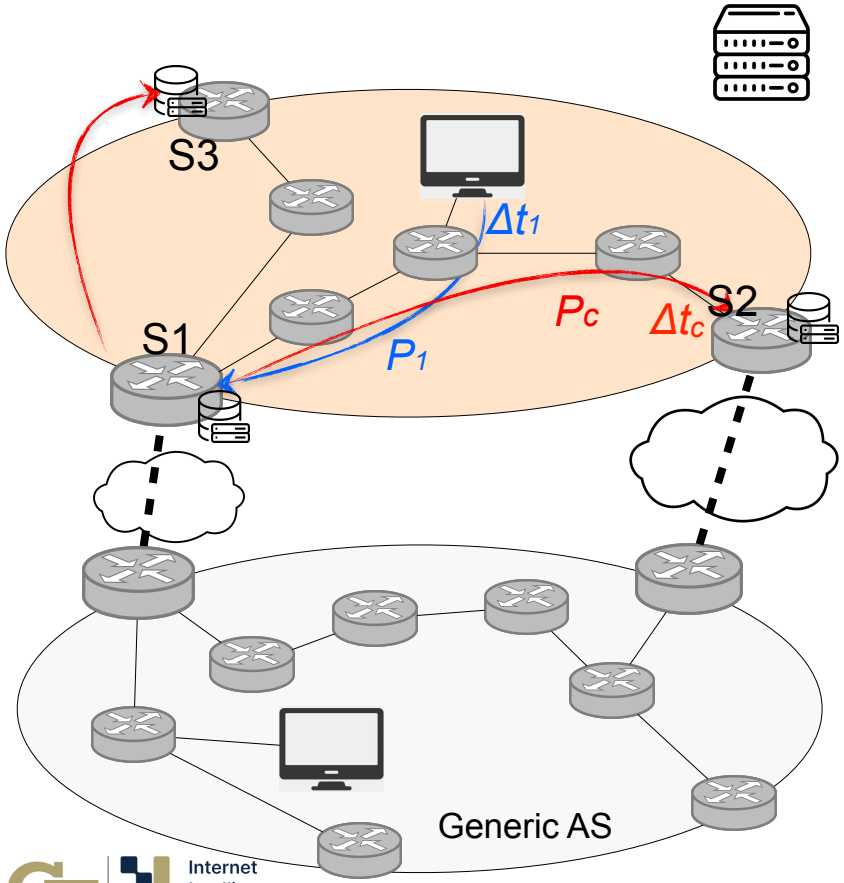
Achieving state consistency through control packets



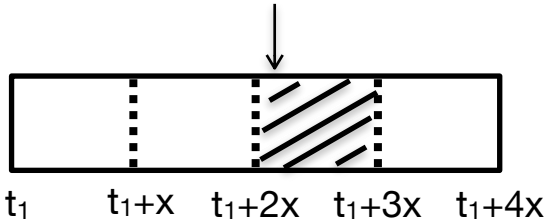


Internet Intelligence Lab

Achieving state consistency through control packets

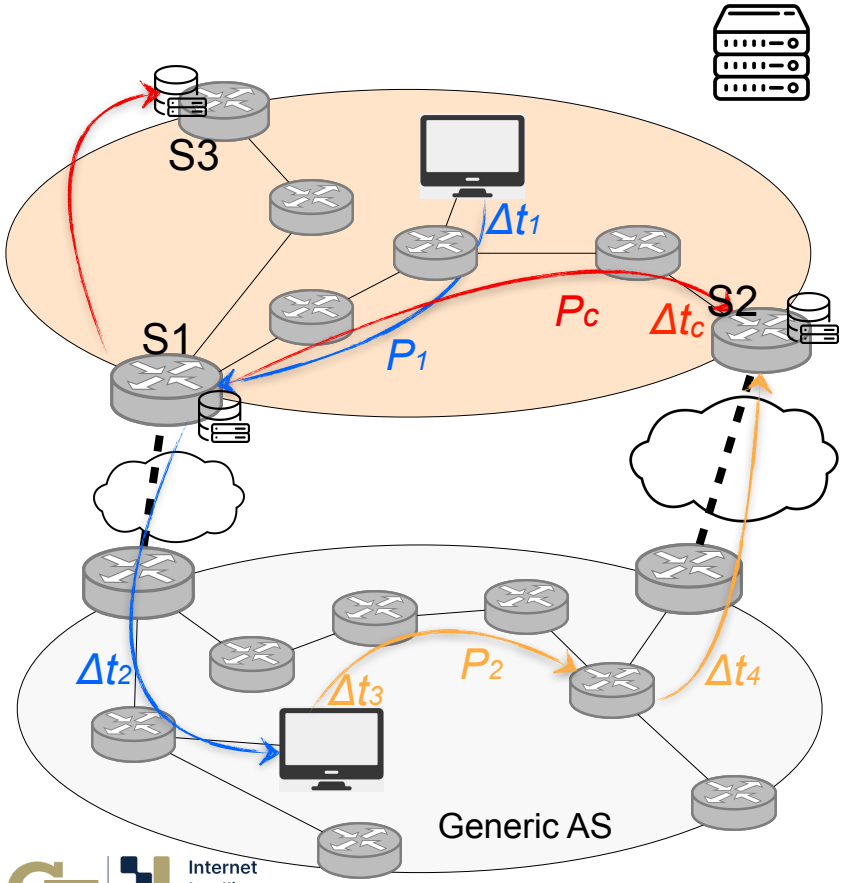


Switch sends control packet to
all other switches to notify of state change



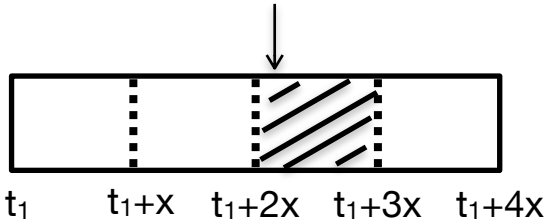
Internet Intelligence Lab

Achieving state consistency through control packets



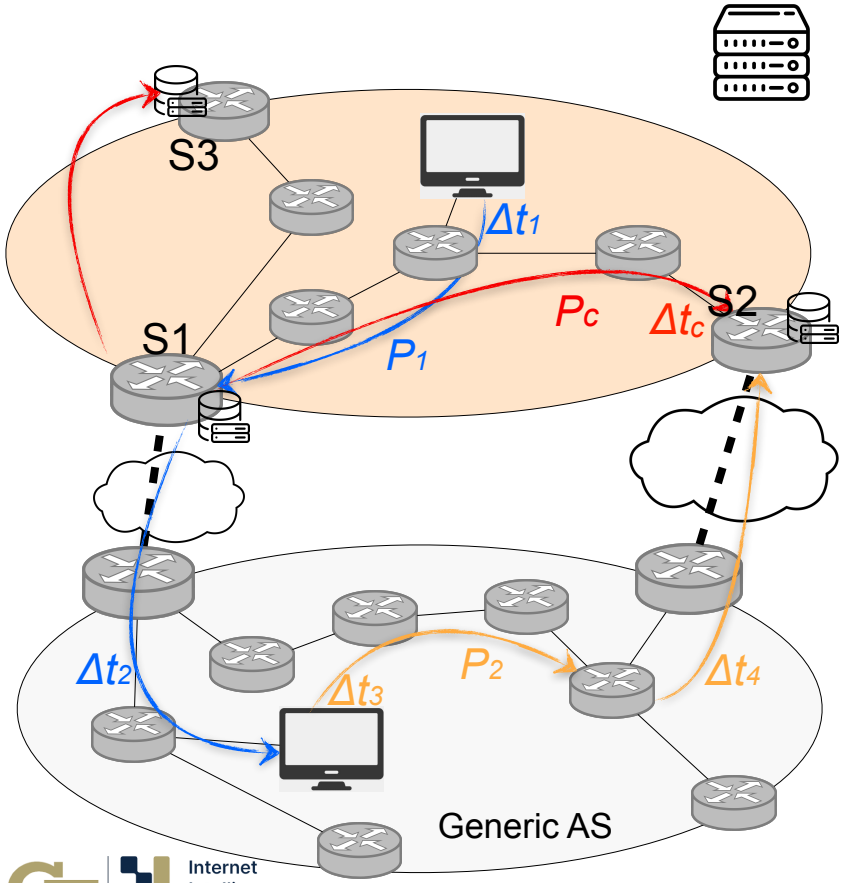
Switch sends control packet to
all other switches to notify of state change:

$$\Delta t_c < \Delta t_2 + \Delta t_3 + \Delta t_4$$



Internet Intelligence Lab

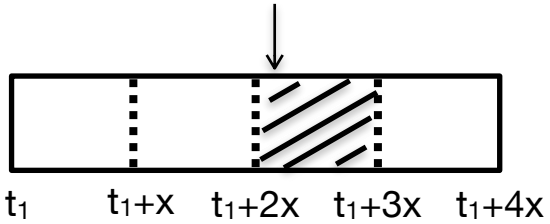
Achieving state consistency through control packets



Switch sends control packet to all other switches to notify of state change:

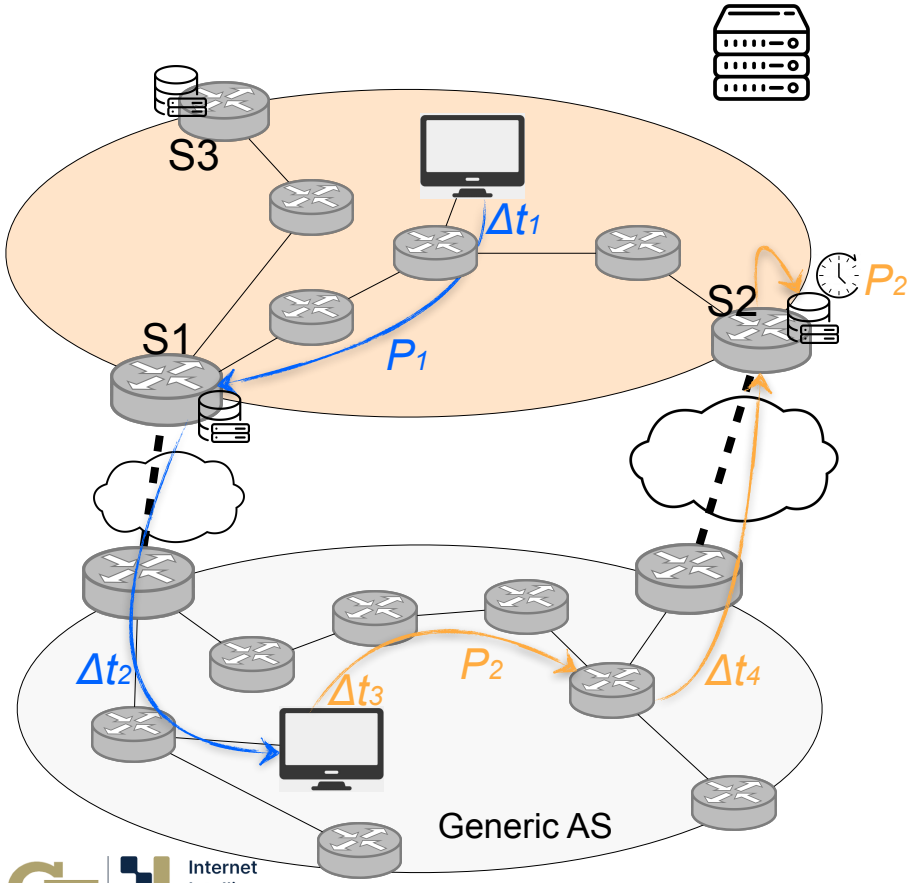
$$\Delta t_c < \Delta t_2 + \Delta t_3 + \Delta t_4$$

Packet loss: *Pc* x3



Internet Intelligence Lab

Achieving state consistency through control packets



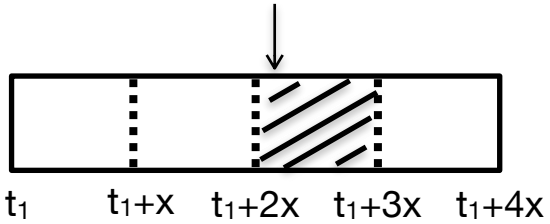
Switch sends control packet to all other switches to notify of state change:

$$\Delta t_c < \Delta t_2 + \Delta t_3 + \Delta t_4$$

Packet loss: *Pc* x3

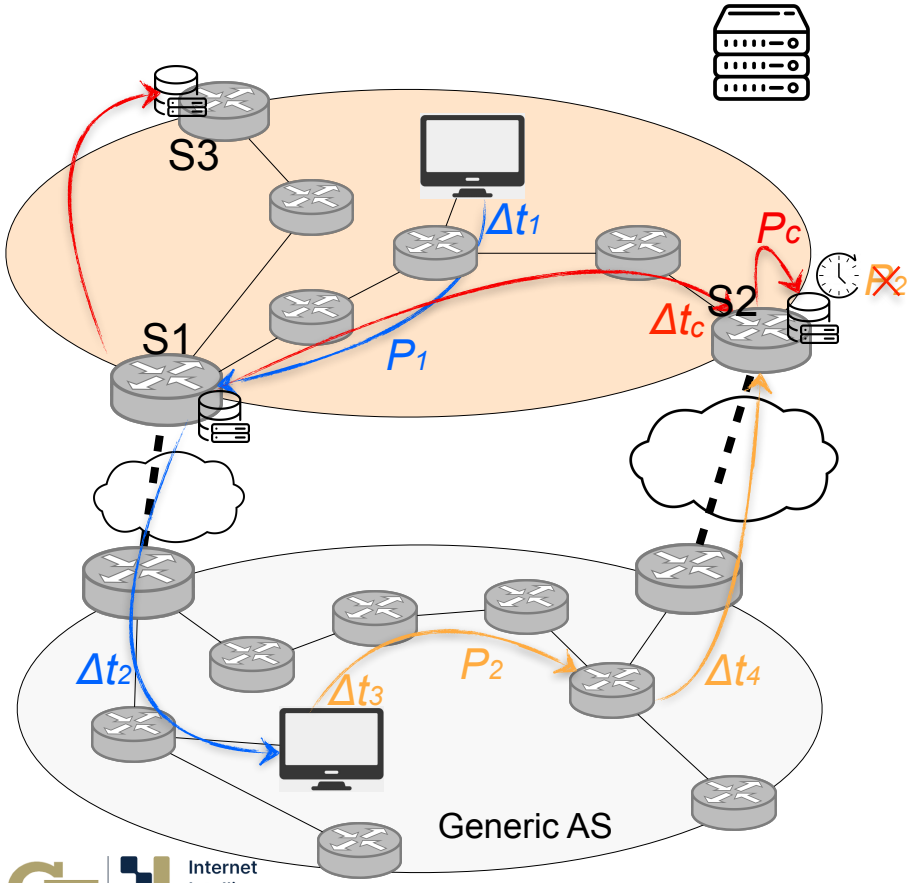
Delay: buffer IBR in capture host for 1sec

$$\Delta t_2 + \Delta t_3 + \Delta t_4 < \Delta t_c < 1s$$



Internet Intelligence Lab

Achieving state consistency through control packets



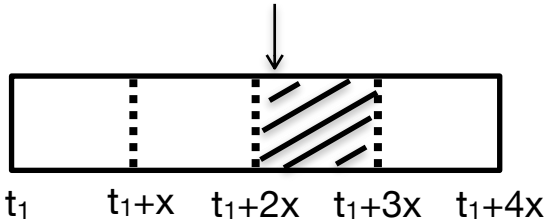
Switch sends control packet to all other switches to notify of state change:

$$\Delta t_c < \Delta t_2 + \Delta t_3 + \Delta t_4$$

Packet loss: *Pc* x3

Delay: buffer IBR in capture host for 1sec

$$\Delta t_2 + \Delta t_3 + \Delta t_4 < \Delta t_c < 1s$$



Internet Intelligence Lab

Evaluating MORP4

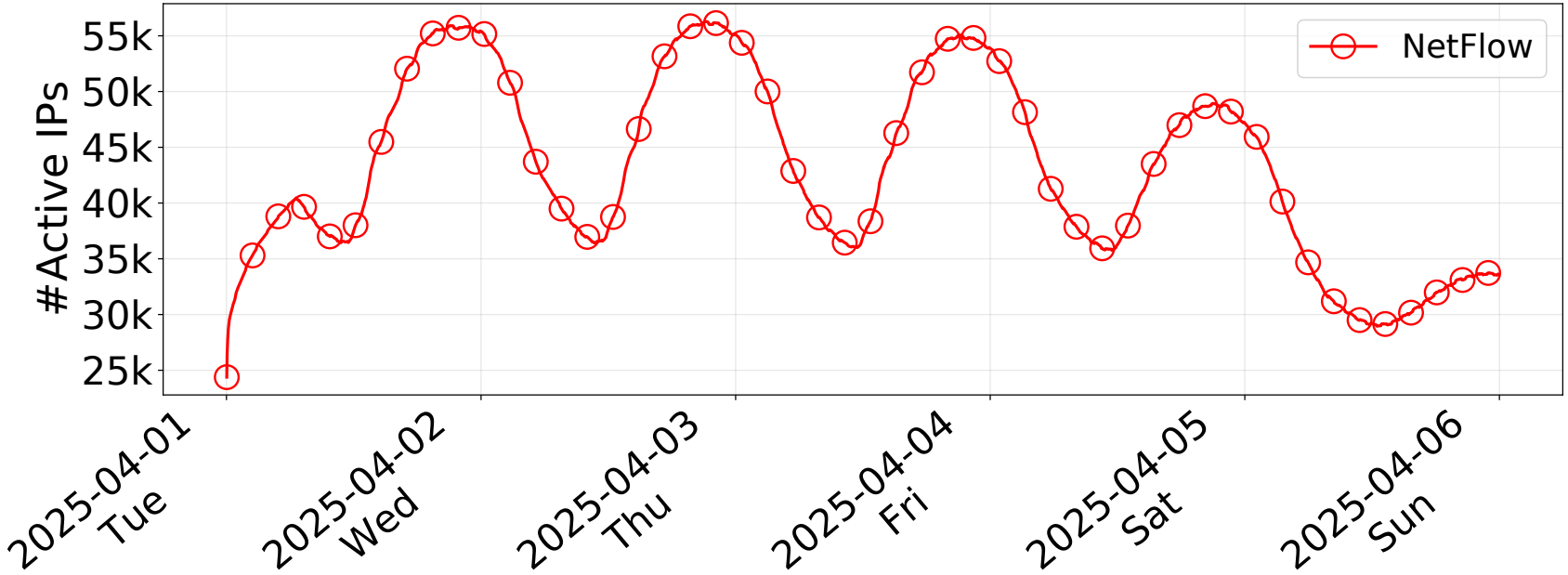
- Does MORP4 accurately detect active IPs?
- Does MORP4 increase our visibility into IBR?

Real-world Deployment

- Real-world deployment on a campus network
  - Monitor
    - 166k IPv4 addresses at /32 granularity
    - 1 /32 IPv6 network at /53 granularity on the same switch
  - 6 hours timeout to consider an IP/subnet inactive

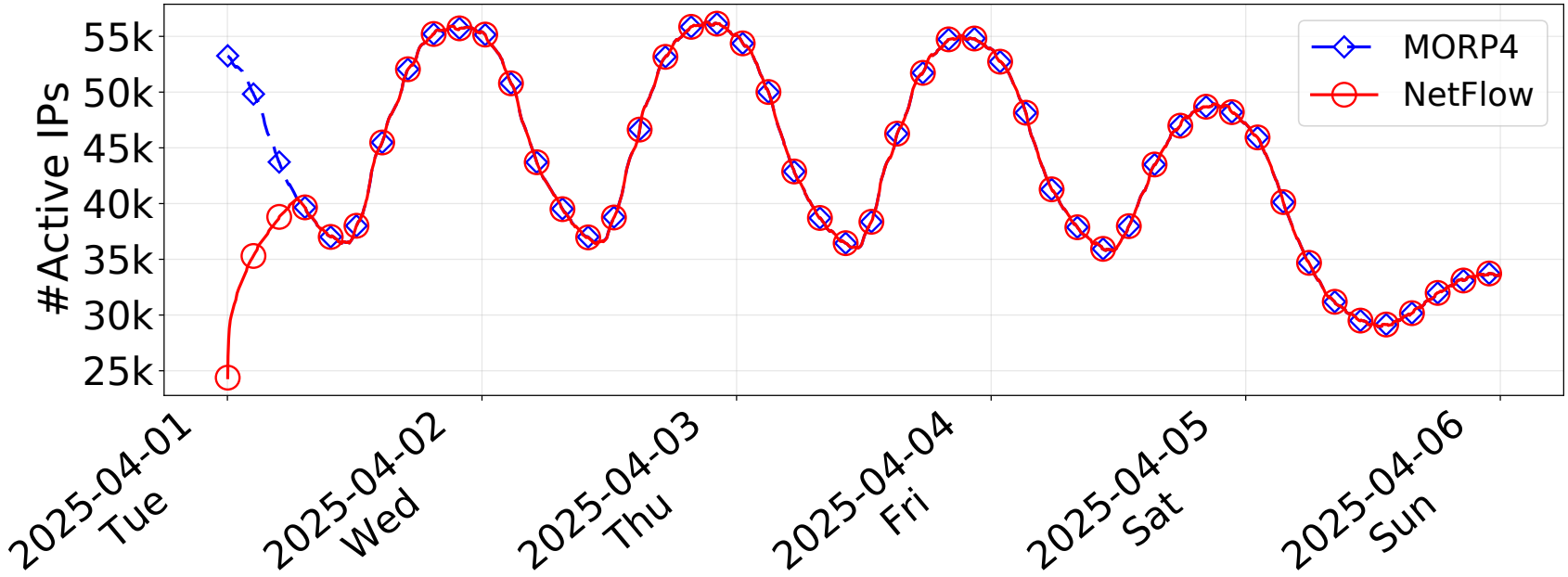
Does MORP4 accurately detect active IPs?

- Ground truth: unsampled NetFlow data



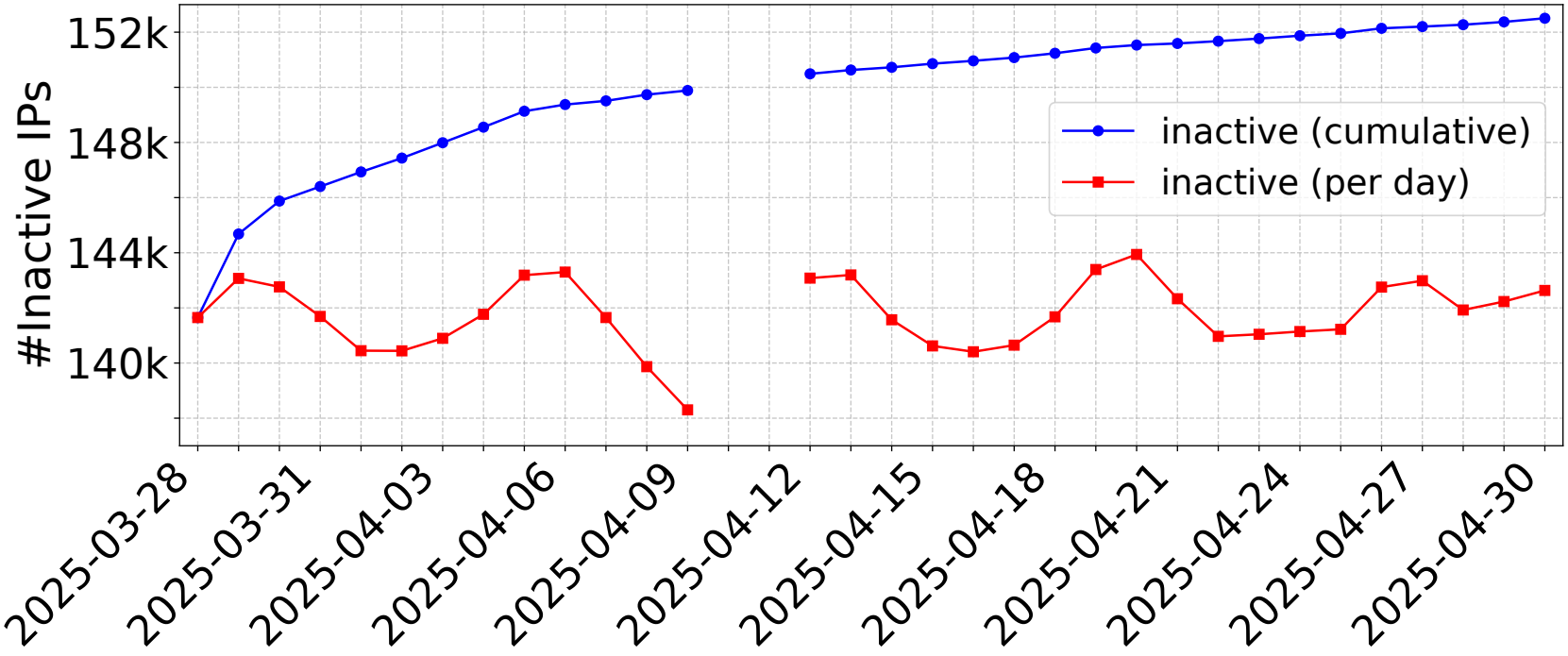
Does MORP4 accurately detect active IPs?

- Ground truth: unsampled NetFlow data

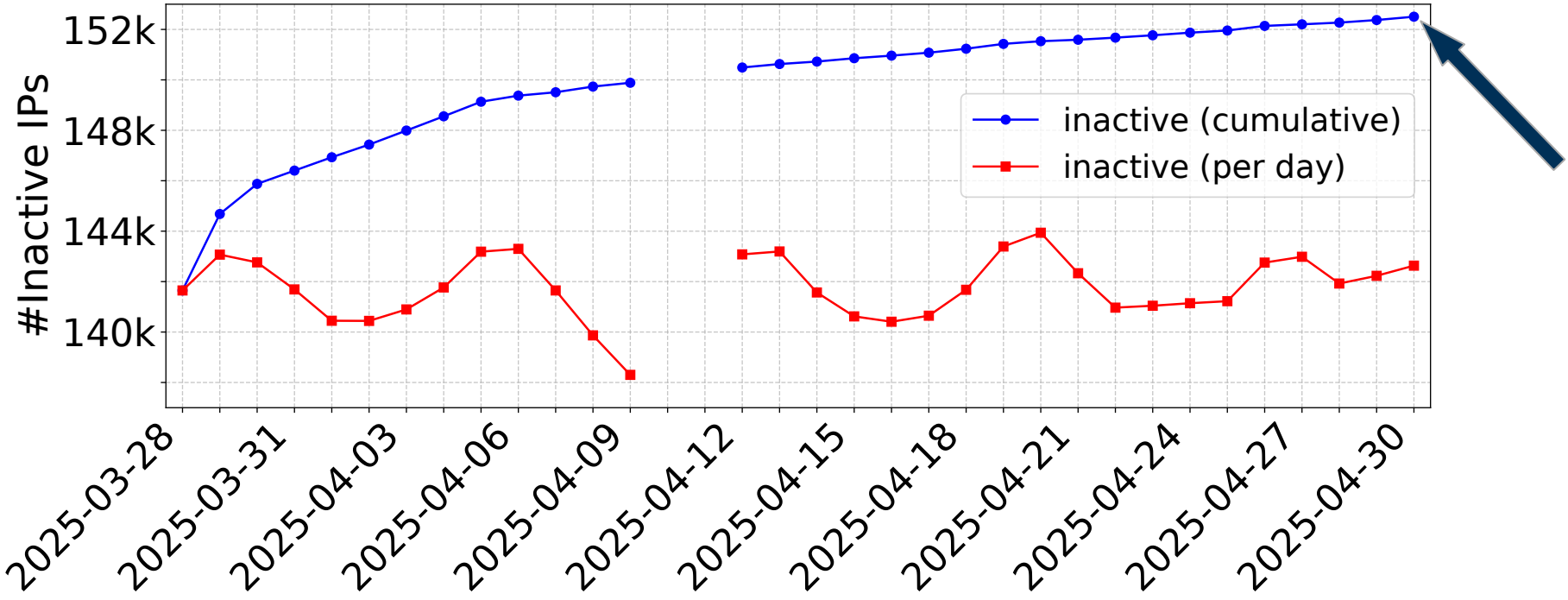


✓ MORP4 == NetFlow simulation

MORP4 recovers unutilized space



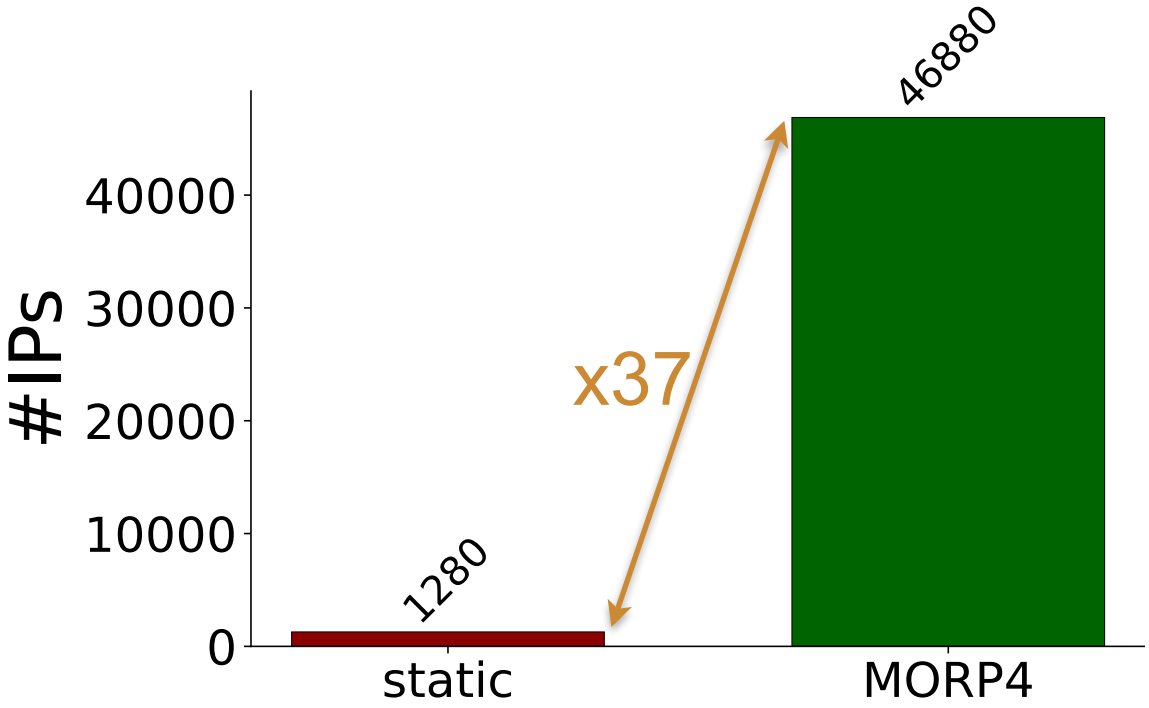
MORP4 recovers unutilized space



Found 152k out of 166k (~92%) IPs being inactive at some point

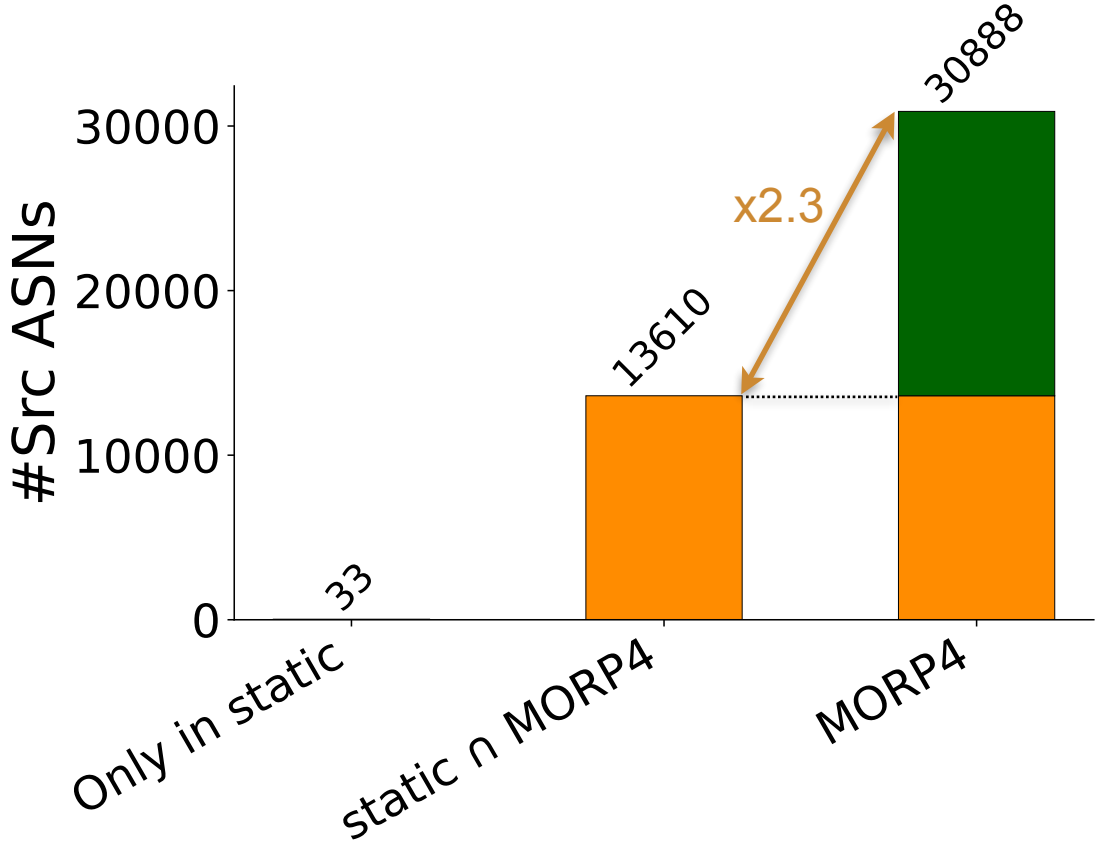
MORP4 expands the telescope size

Our network engineers have dedicated 5 /24s to static telescope



during ~34 days

MORP4 increases visibility into IBR sources

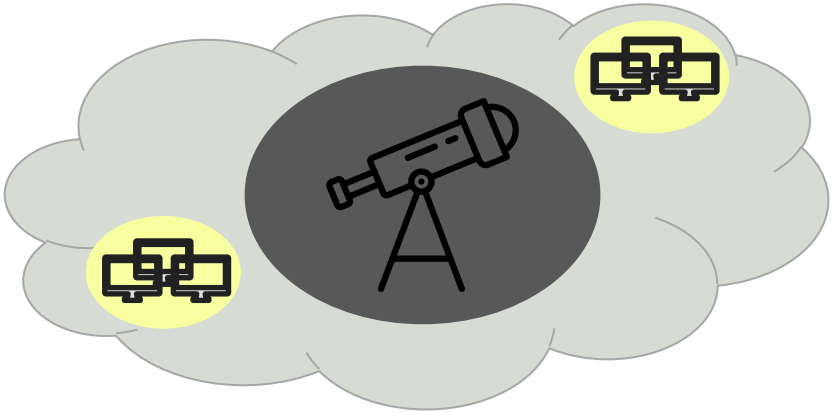


during ~34 days

MORP4 automatically infers candidate useful IPv6 telescope space

Static telescope

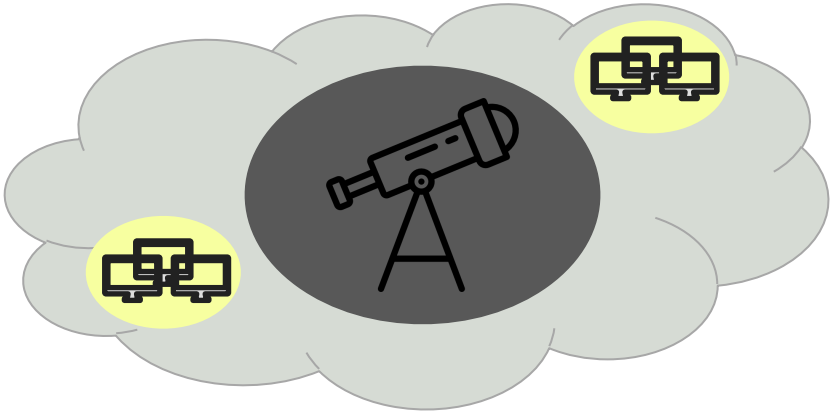
TotallyDark subnets



MORP4 automatically infers candidate useful IPv6 telescope space

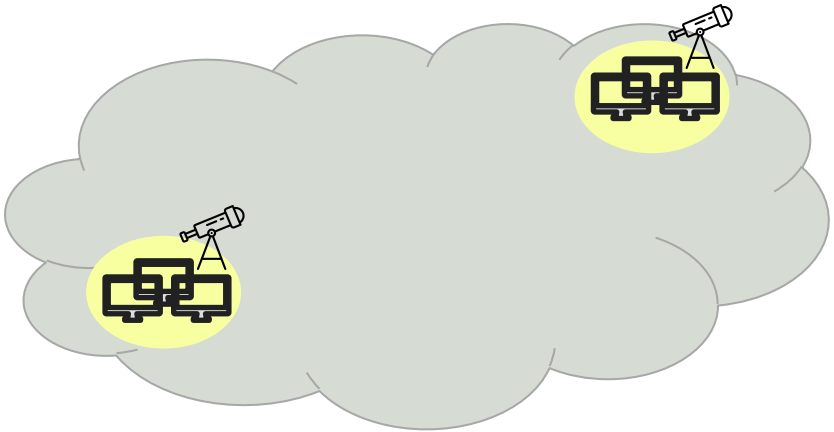
Static telescope

TotallyDark subnets

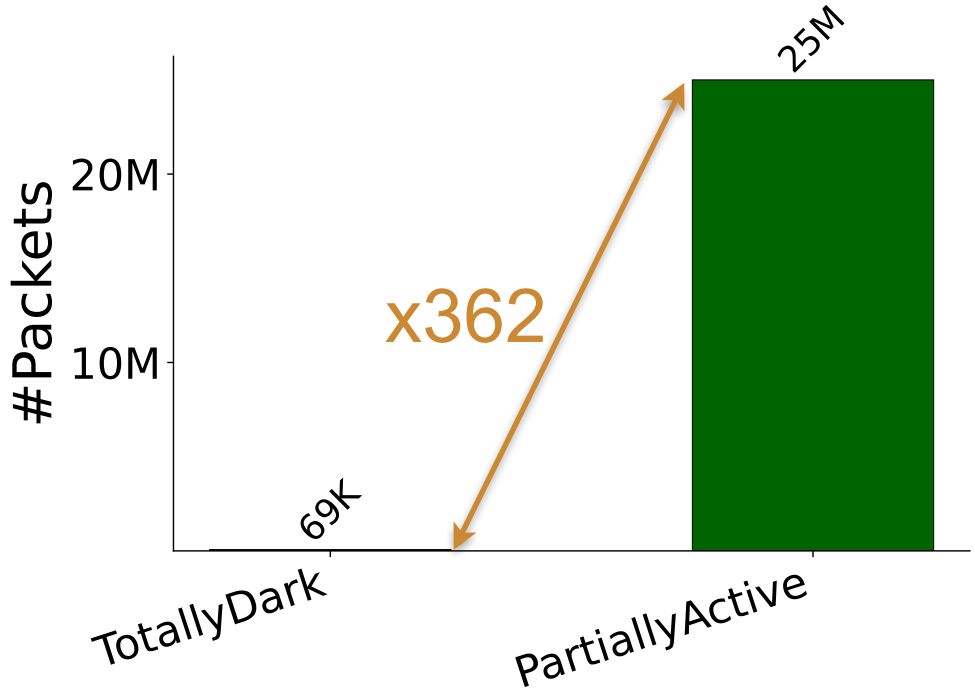


Dynamic telescope

PartiallyActive subnets

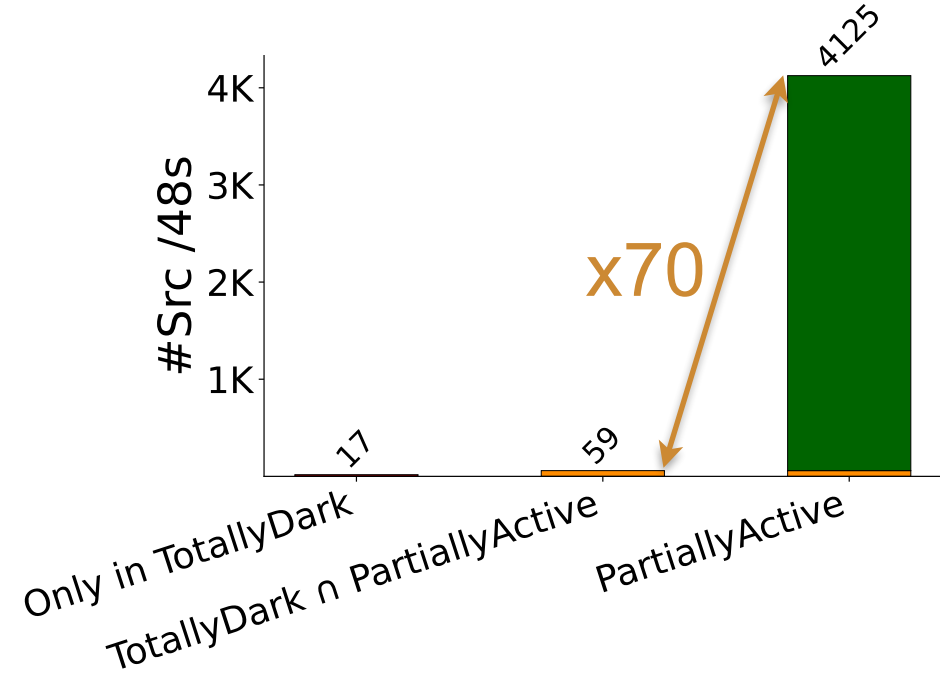


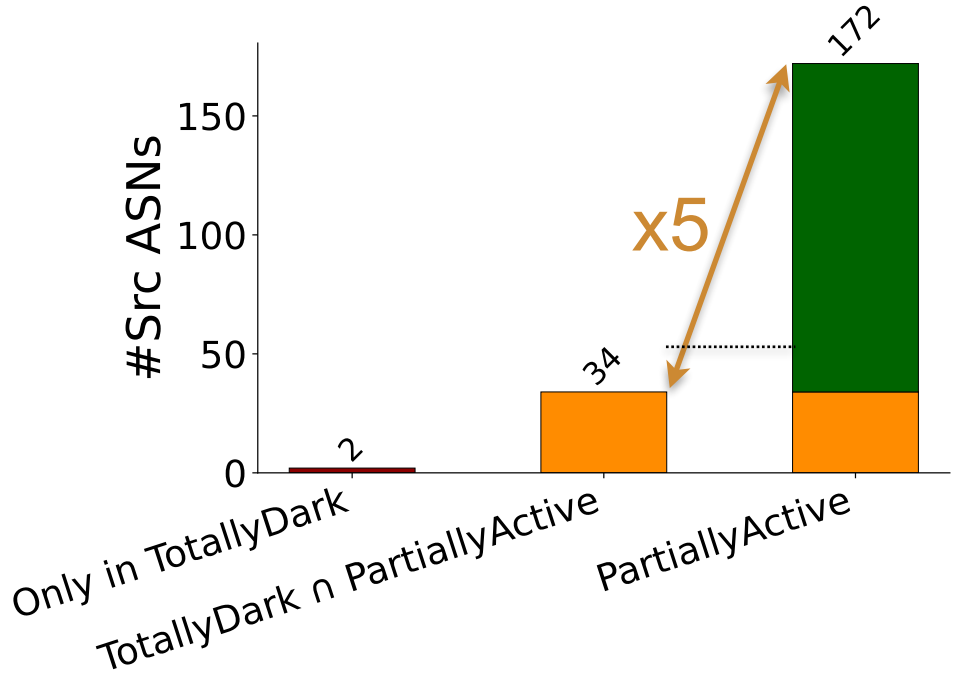
MORP4 collects more IPv6 IBR close to real operational subnets



during ~34 days

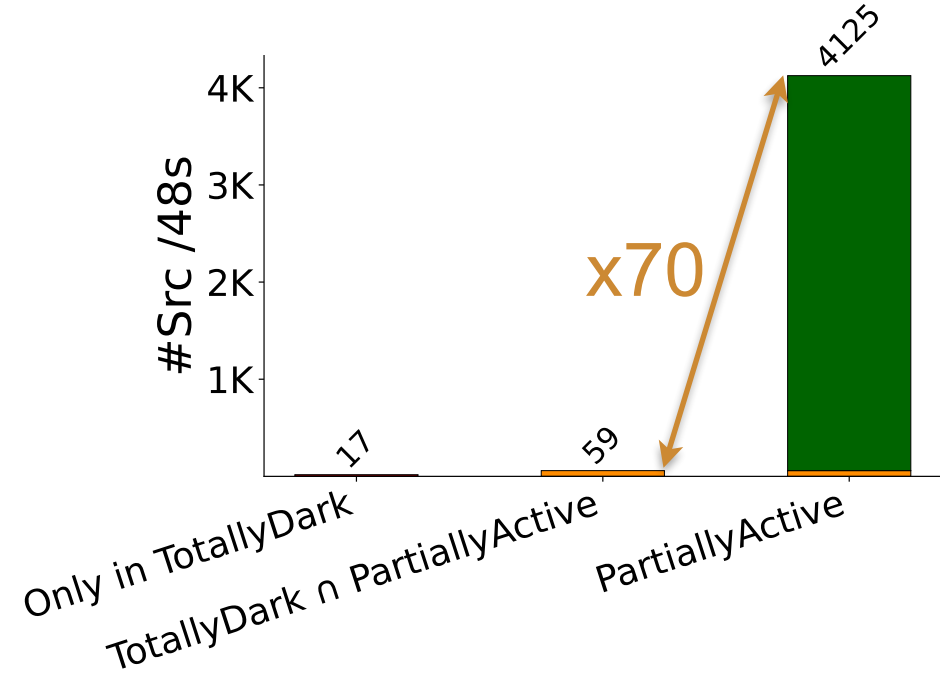
MORP4 collects more diverse IPv6 IBR close to real operational subnets

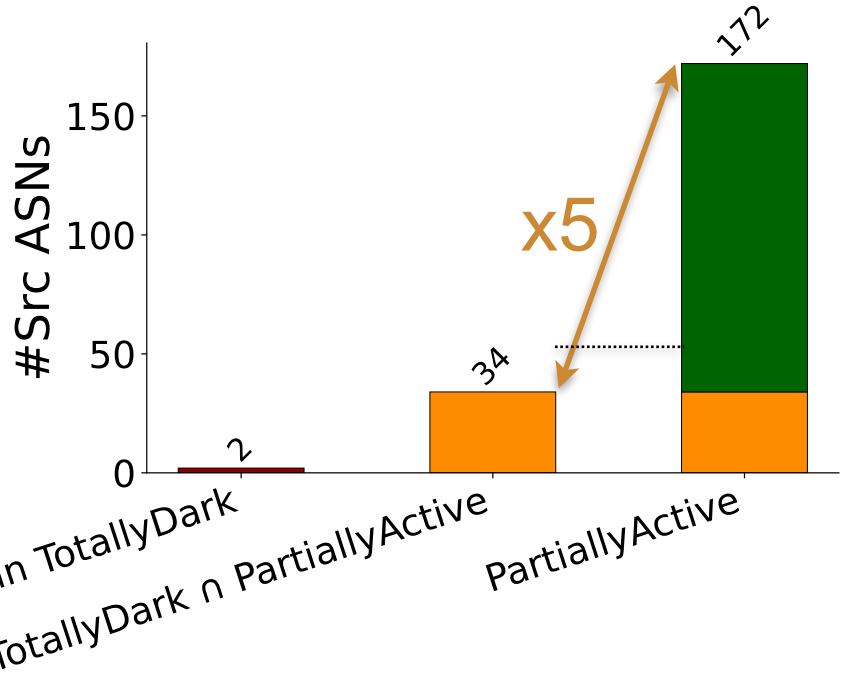




during ~34 days

MORP4 collects more diverse IPv6 IBR close to real operational subnets





Realistic IBR without artificially attracting scanners

during ~34 days

Conclusions

With MORP4:

✓ Large IPv4 network telescope

✓ Effective IPv6 network telescope

Conclusions

With MORP4:

✓ Large IPv4 network telescope

✓ Effective IPv6 network telescope

Ongoing work

- Deployment at another major Research and Educational network
- Comparison of IBR between major static telescope vs MORP4
  - Increased visibility == greater insights?

Conclusions

With MORP4:

✓ Large IPv4 network telescope

✓ Effective IPv6 network telescope

Ongoing work

- Deployment at another major Research and Educational network
- Comparison of IBR between major static telescope vs MORP4
  - Increased visibility == greater insights?

Thank you!