# Unwanted Traffic: Denial of Service Attacks

Dan Boneh

# Wha i ne D S?

- G a: a e a a ge e i h i e c ing
- H : **Amplification**
  - S a n be f ac e = big effec
- T e f a ifica i n a ac :
  - D S b g:
    - De ign f a a ing ne achine di a e ice
  - D S f d:
    - C and b -ne gene a e f d f e e

# D S can ha en a an a e

- Thi ec e:
  - Sa e D a diffe en a e (b de ):
    - Lin
    - TCP/UDP
    - A ica i
  - D S i iga i n

- Sad n:
  - C en In e ne n de igned hand e DD S a ac

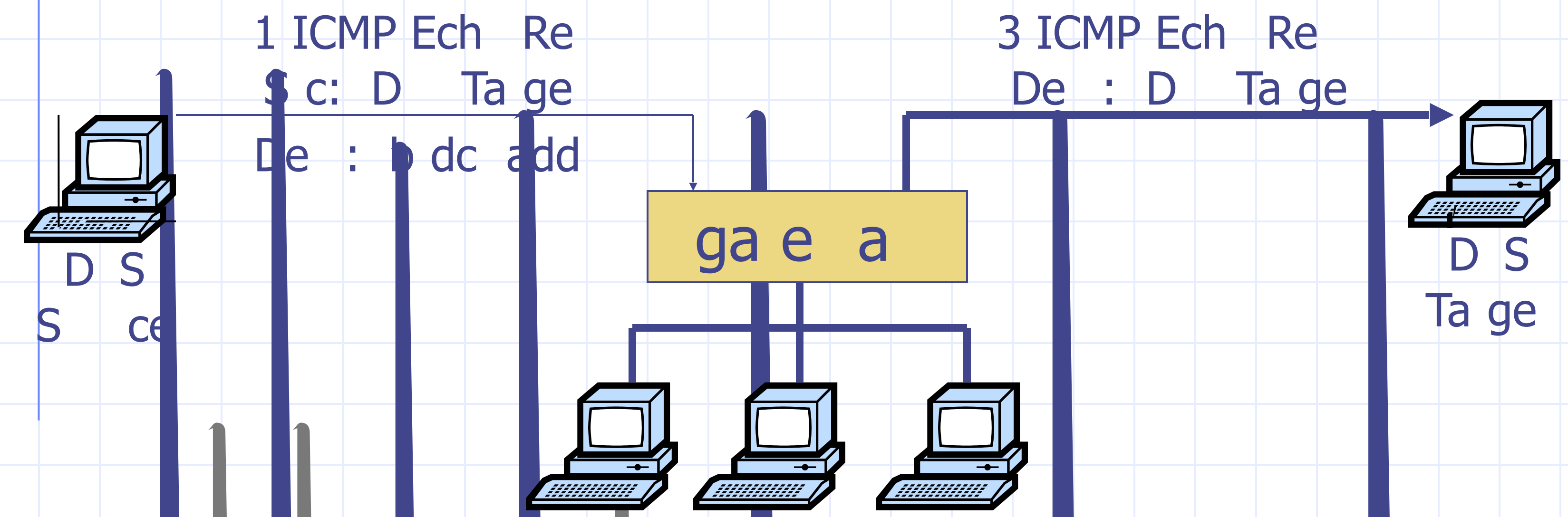
# Wa 802.11b D S b g

- Radi a ing a ac : i ia n f c .
- P c D S b g [B a d , a age, 03]
  - NAV Ne A ca i n Vec ):
    - 15-b fie d. Ma a e 32767
    - A de ca e e e e hanne f NAV ec nd
    - N e e e n d an i d ing NAV e i d b n f ed b 802.11b ca d

  - De-a hen ica i n b g:
    - A n de can e d dea h ac e AP
    - Dea h ac e na hen ica ed

      ⇒ a ac e can e ea ed dea h an ne

# S f a ifica i n D S a ac



1 ICMP Ech Re
S c: D Ta ge
De : b dc add

D S
S ce

ga e a

3 ICMP Ech Re
De : D Ta ge

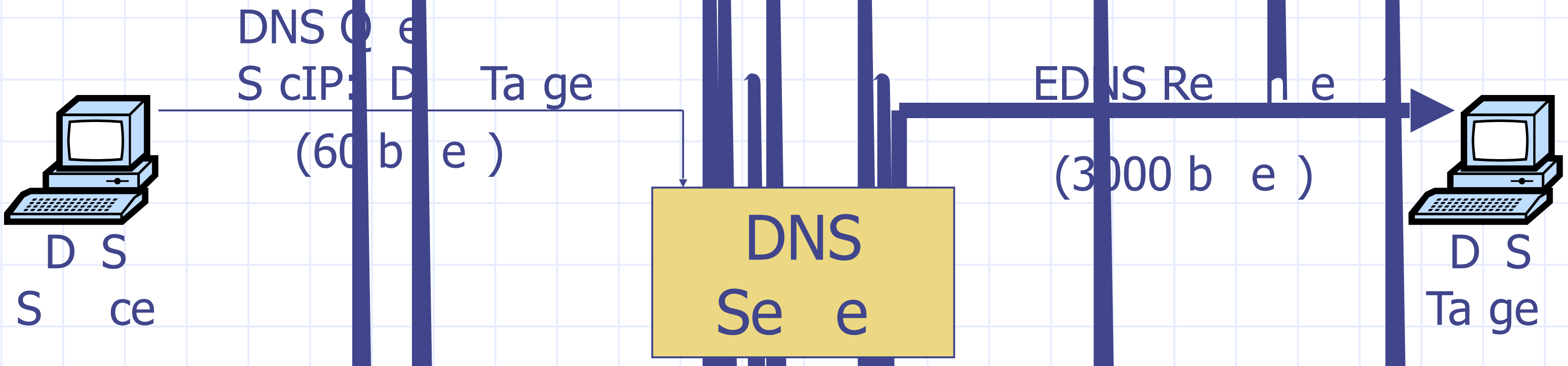
D S
Ta ge

- Send ing e e b adca add (ICMP Ech Re )
- L f e n e :
  - E e h n a ge ne gene a e a ing e (ICMP Ech Re ) ic i

P e en i n: e ec e e na ac e b adca add e

# M de n da e a e (Ma 13

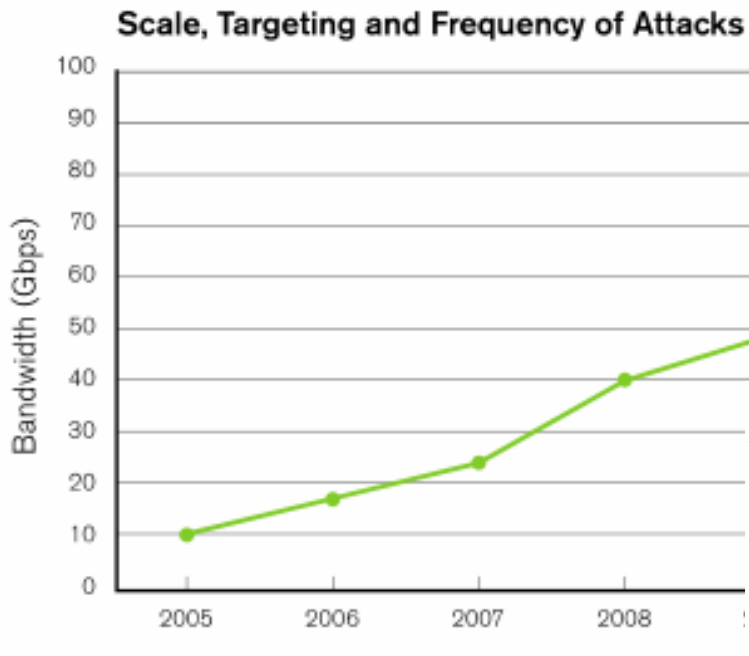
DNS A ifica i n a ac : ( ×50 a ifica i n )



2006: 0.58M en e e n n e ne (Ka in -Shiff a )

2017: 15M en e e ( en e e ec . g)

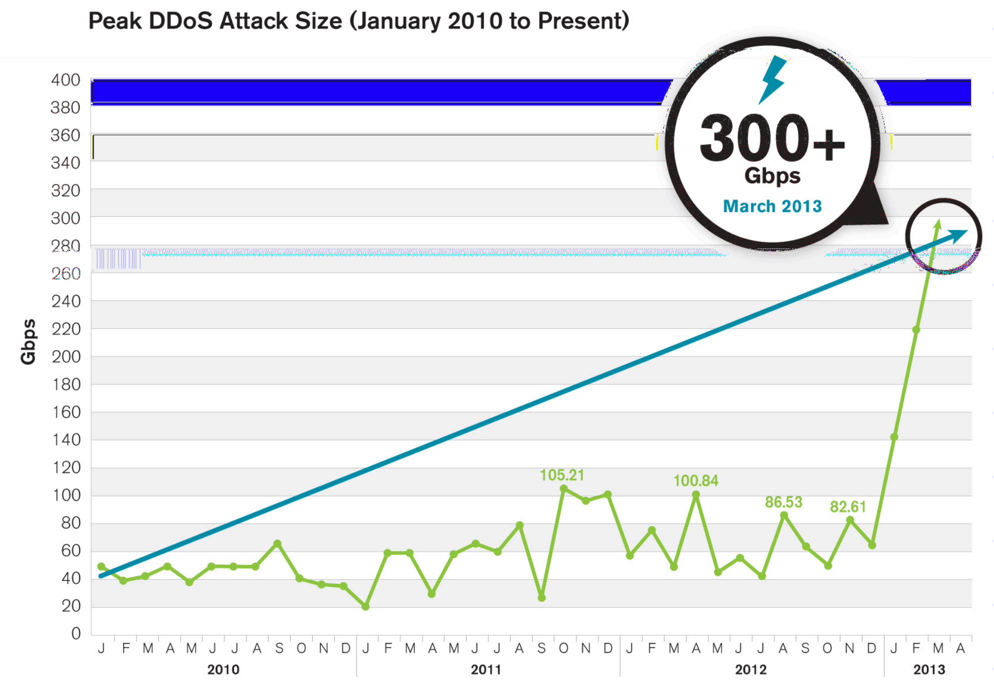
⇒ 3/2013: DD S a ac gene a ing 309 Gb f 28 in .



Scale, Targeting and Frequency of Attacks

*Figure 13*

Source: Arbor Networks, Inc.



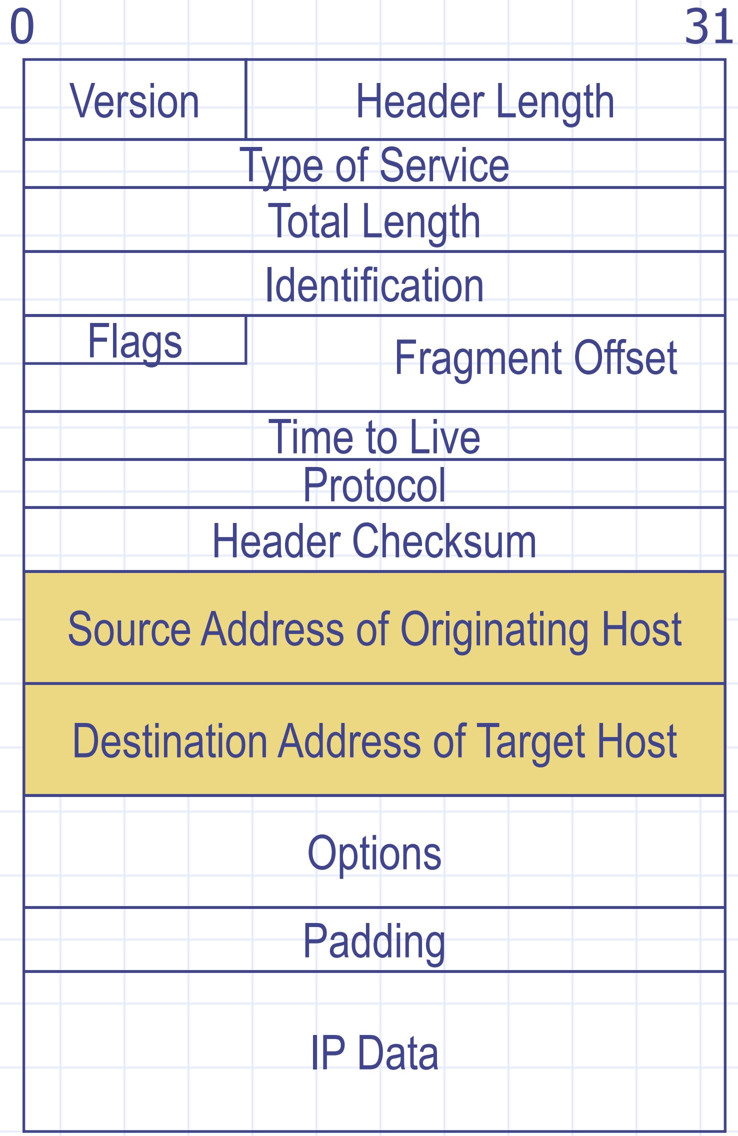
Peak DDoS Attack Size (January 2010 to Present)

Source: Arbor Networks, Inc.

Feb. 2014: 400 Gbps via NTP amplification (4500 NTP servers)

# Re ie : IP Heade f a

- C n ec i n e
  - Un e iab e
  - Be eff



0

31

Version | Header Length

Type of Service

Total Length

Identification

Flags | Fragment Offset

Time to Live

Protocol

Header Checksum

Source Address of Originating Host

Destination Address of Target Host

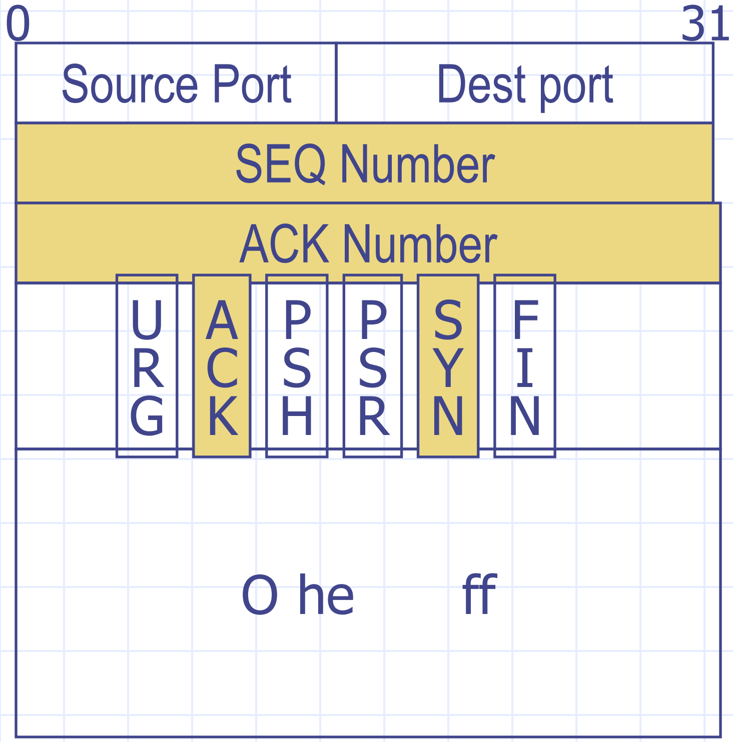
Options

Padding

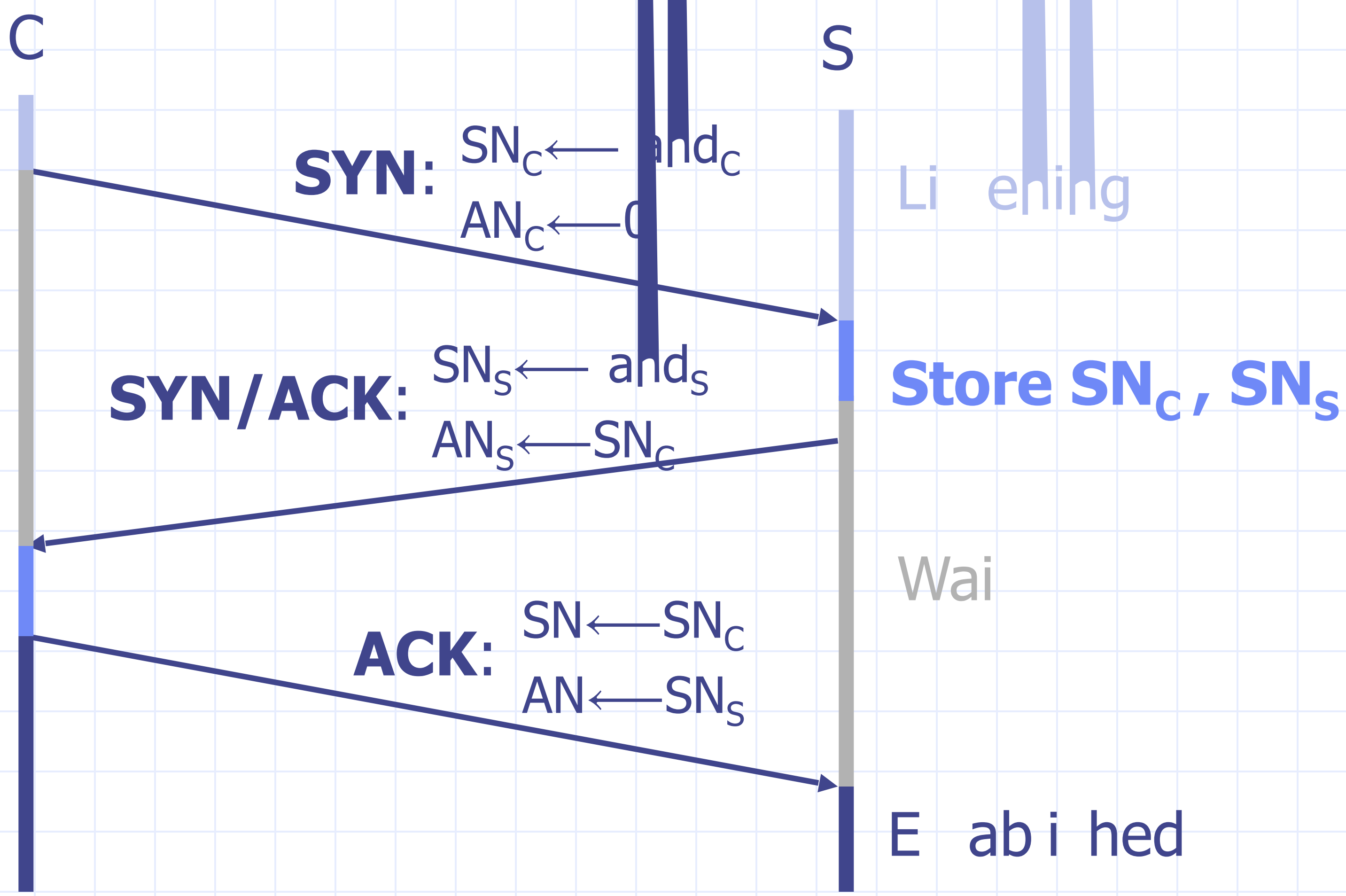
IP Data

# Re ie : TCP Heade f a

- TCP:
  - Se i n ba ed
  - C nge i n c n
  - In de de i e



# Re ie : TCP Hand ha e



C

S

**SYN:** $SN_C \leftarrow$ and$_C$

$AN_C \leftarrow 0$

Li ening

**SYN/ACK:** $SN_S \leftarrow$ and$_S$

$AN_S \leftarrow SN_C$

**Store $SN_C$ , $SN_S$**

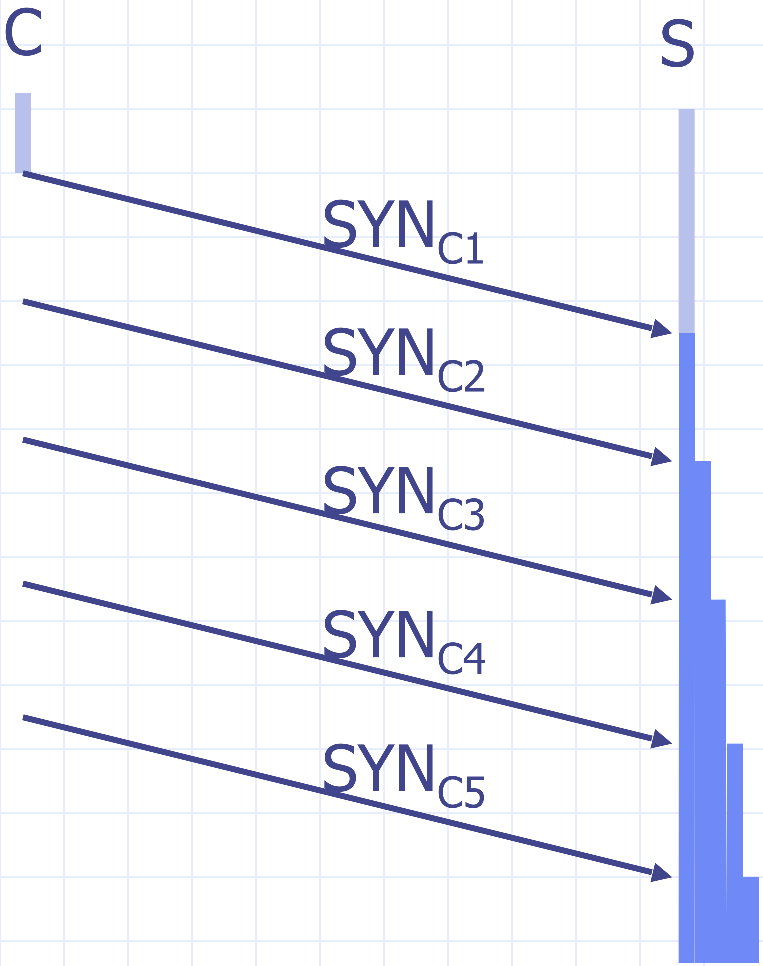
Wai

**ACK:** $SN \leftarrow SN_C$

$AN \leftarrow SN_S$

E ab i hed

# TCP SYN F d I: a e (D S b g)



**Single machine:**

SYN Pac e h **random source IP addresses**

F bac g e e n e e

N f he c nnec i n ib e

# SYN F d ( h ac 48, n 13, 1996)

| OS | Bac g<br>e e i e |
|---|---|
| **Linux 1.2.x** | 10 |
| **FreeBSD 2.1.5** | 128 |
| **WinNT 4.0** | 6 |

Bac g i e : 3 in e

- Attacker needs only 128 SYN packets every 3 minutes
- Low rate SYN flood

# L a e SYN f d defen e

The b e :

- e e c i e ce ( e ) bef e c ien e nd

N n- i n:

- Inc ea e pac e e i e dec ea e i e

C ec i n ( he nde a ac ) :

- **Syncookies**: e e a e f e e
- S a e f ance e head

# S nc e

[Be n ein, Schen ]

- Idea: e ec e e and da a in ac e gen. e e SN
- Se e e nd Clien i h SYN-ACK c ie:
  - T = 5-bi c n e inc e en ed e e 64 ec
  - L = MAC$_{e}$ (SAdd , SP , DAdd , D , SN$_{C}$, T) [24 bi ]
    - e : ic ed a and d ing o
  - SN$_{S}$ = (T . . L) ( L = 24 bi )
  - **Server does not save state** ( he TCP i n a e )
- H ne c ien e nd i h ACK ( AN=SN$_{S}$ , SN=SN$_{C}$+1 )
  - Se e a ca e ace f c e n if a id SN$_{S}$

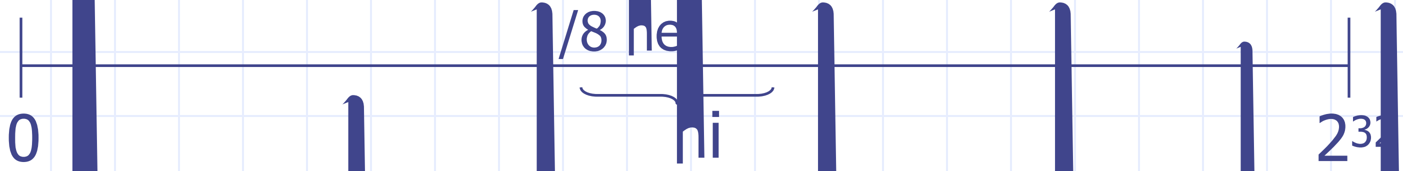
# SYN f d : bac ca e [MVS 01]

- SYN i h f ged ce IP ⇒ SYN/ACK and h

[redacted]

# Bac ca e ea e en

- Li en n ed IP add e ace (da ne )



- L ne SYN/ACK ac e i e be e f SYN a ac
- 2001: **400** SYN a ac / ee
- 2013: **773** SYN a ac /24 h (a b ne ATLAS)
  - La ge e e i en : ( ni an ISP da ne )
    - A b ne

# E nia a ac (ATLAS 07)

- A ac e de ec ed:
  - 115 ICMP f d , 4 TCP SYN f d
- Band id h
  - 12 a ac : **70-95 Mbps for over 10 hours**
- A a ac affic a c ing f ide E nia
  - E nia i n:
    - E nian ISP b c ed a f eign affic n i a ac ed

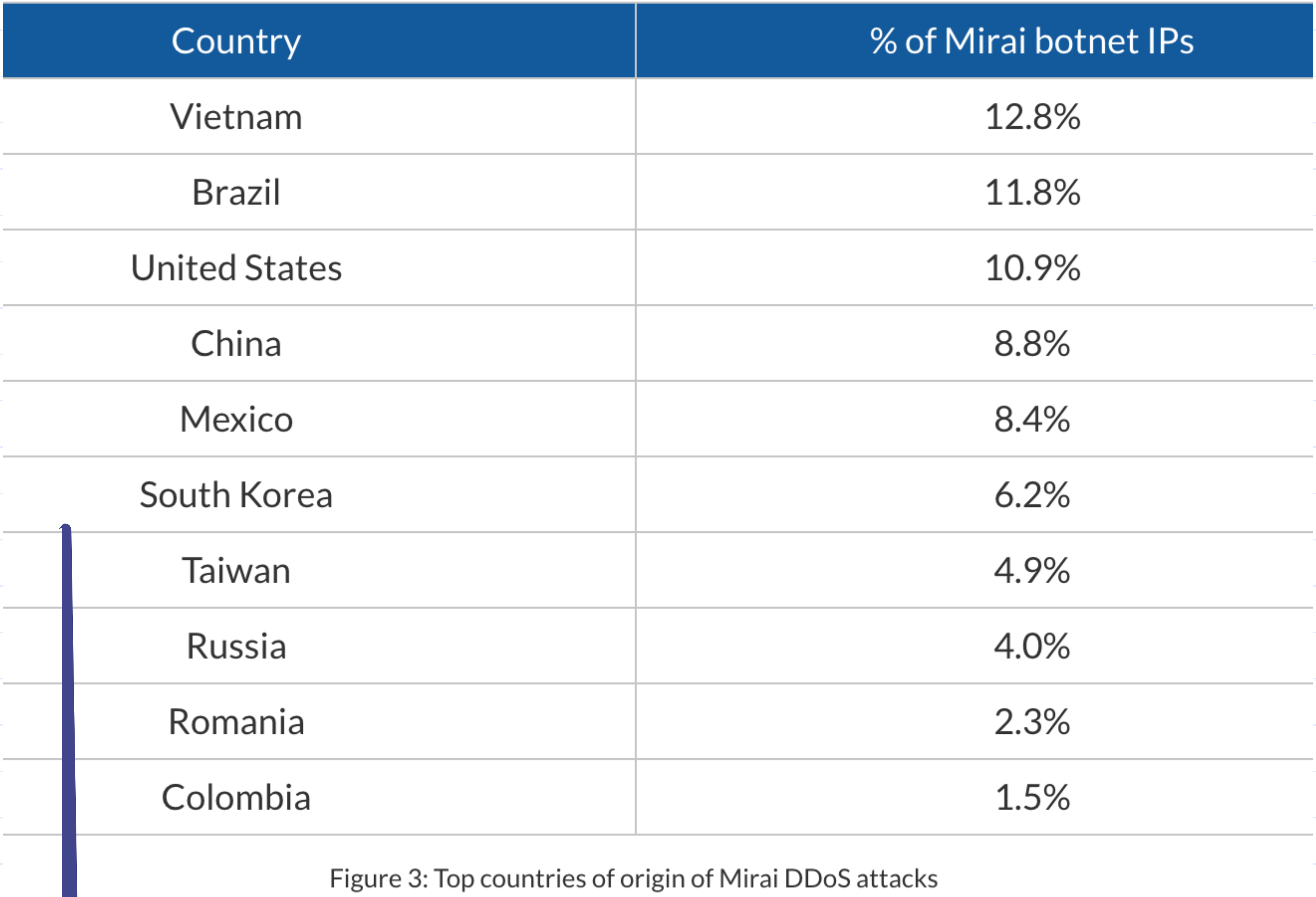
      ⇒ D S a ac had i e i ac in ide E nia

# Ma i e f d (e.g. Mi ai 9/2016 n K eb )

C and b a f d ecific a ge : (DD S)

- F d i h SYN, ACK, UDP, and GRE ac e
- 623 Gb ( ea ) f ≈100K c i ed I T de ice
- A eb i e:
  - Sa a e ne in ne e
  - Rand ce IP ⇒

    a ac SYN he a e a ea SYN
- Wha d ???



| Country | % of Mirai botnet IPs |
|---|---|
| Vietnam | 12.8% |
| Brazil | 11.8% |
| United States | 10.9% |
| China | 8.8% |
| Mexico | 8.4% |
| South Korea | 6.2% |
| Taiwan | 4.9% |
| Russia | 4.0% |
| Romania | 2.3% |
| Colombia | 1.5% |

Figure 3: Top countries of origin of Mirai DDoS attacks

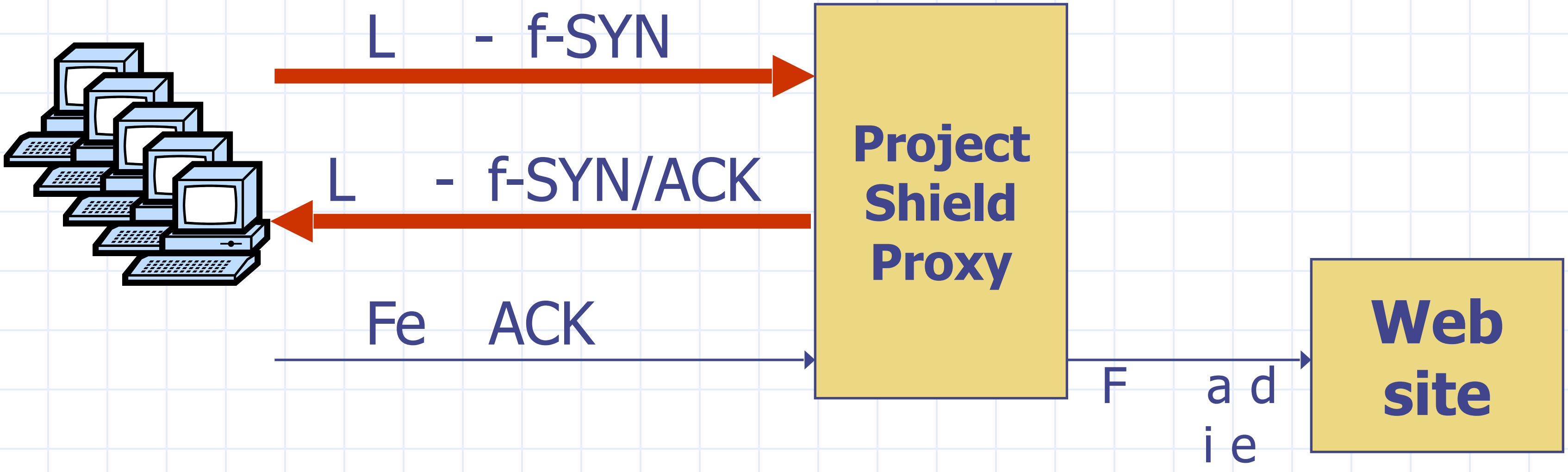
c: inca a.c

# G g e ec hie d

P ec ing ne gani a i n .

(C e cia e ice: A a ai, C d a e, )

Idea: n f a d e ab i hed TCP c nnec i n i e



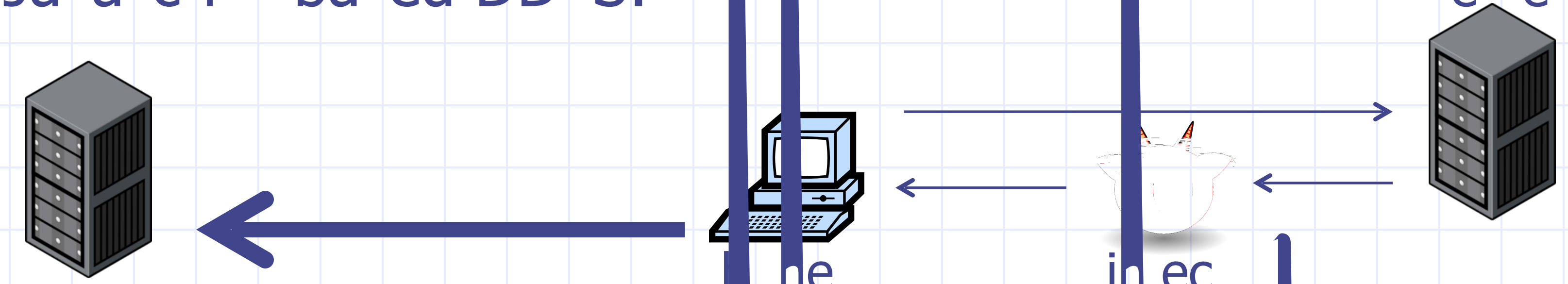
# S nge a ac : GET f d

- C and b a :
  - C e e TCP c nnec i n eb i e
  - Send h HTTP GET e e
  - Re ea
- Wi b a S N f c ec i n
- b :
  - A ac e can n ge e and ce IP .
    - Re ea ca i n f b bie
  - P can n b c a e-i i b .

# A ea - d e a e: Gi H b (3/2015)

Ja a c i -ba ed DD S:

a
e e



gi h b.c

ne
end e

in ec
i ageF d.

i ageF d.

```
f nc i n i gf d()
   a TARGET = ' ic i - eb i e.c /inde . h ?
   a and = Ma h.f (Ma h. and () * 1000)
   a ic = ne I age()
   ic c = 'h ://'+TARGET+ and+'= a '

 e In e a (i gf d, 10)
```

W d HTTPS
e en hi DD S?

# DNS D S A ac (e.g. D n a ac 10/2016)

DNS n n UDP 53

- DNS en f ic i .c h ed a DNSP ide .c

DD S a ac

- f d DNSP ide .c i h DNS e ie
- **Random source IP address** in UDP ac e
- Ta e en i e DNS e e (c a e a da age)

D n a ac : ed e Mi ai-ba ed o

- A ea 100,000 a ci end in

⇒ D n cann an e an egi DNS e ie

⇒ Di ed e ice a Ne f i , Gi h b, T i e,

# D S Mi iga i n

# 1. Cien e

- Idea: c n a ac e
- M de e ha d be :
  - G en cha enge C find X ch ha

$$LSB_n ( SHA\text{-}1( C \| X ) ) = 0^n$$

  - A n: a e e ec ed $2^n$ i e e
  - F =16 a e ab .3 ec n 1GhZ achine
  - Main in : chec ing e i i ea .
- D ing D S a ac :
  - E e ne b i e i n i h e e
  - When n a ac : d n e i e e i n

# E a e

- GET f d (RSA 99)
  - E a e cha enge: C = TCP e e - e -
  - Fi da a ac e c a e i
    - C e i e TCP c nnec i i ed
- SSL hand ha e D S: SD 03)
  - Cha enge C ba ed TLS e i ID
  - Se e : chec e i bef e RSA dec .

# Benefi and i i a i n

- Ha dne f cha enge: n
  - Decided ba ed n D S a ac e.

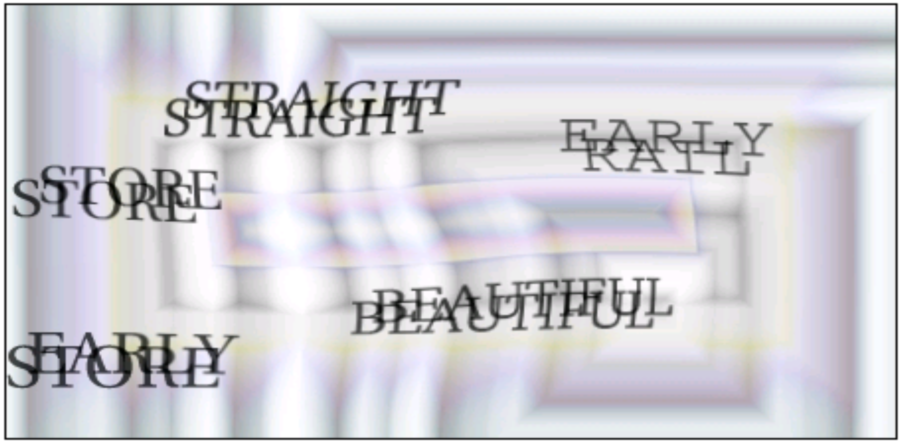
- Li i a i n :
  - Re i e change b h c ien and e e
  - H e egi i a e c ien d ing a ac
    - C ien n ce h ne and ab e can n c nnec

# Me -b nd f nc i n

- CPU e a i :
  - high end e e / -end I T de ice = 8000
  - ⇒ I ib e ca e ha d e
- In e e ing b e a i n
  - Main e acce i e i :
    - high end e e / -end I T de ice = 2
- Be e e :
  - S i e i e an ain e acce e
    - D -G dbe g-N , C 03
    - Abadi-B -Mana e-W bbe , ACM T IT 05

# 2. CAPTCHA

- Idea: e if ha c nnec i n i f a h an



- A ie a ica i a e DD S [Ki 05]
  - D in a ac : gene a e CAPTCHA and ce e e if a id i n
  - P e en ne CAPTCHA e ce IP add e .

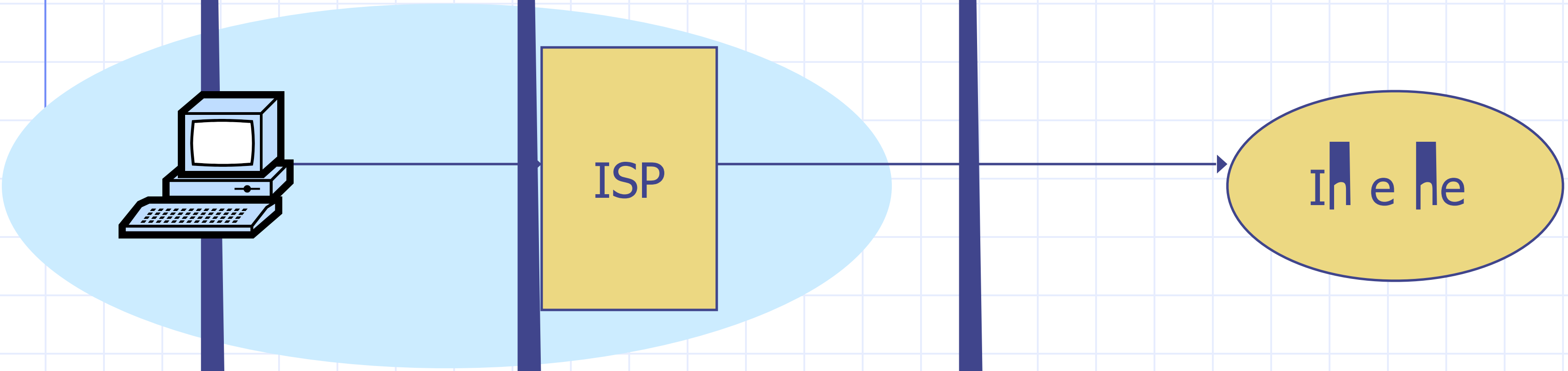
# 3. S ce iden ifica i n

G a : iden if ac e ce

U i a e g a : b c a ac a he ce

# 1. Ing e fi e ing (RFC 2827, 3704)

- Big b e : DD S i h fed ce IP



- Ing e fi e ing ic : ISP n f a d ac e i h egi i a e ce IP ( ee a SAVE c )

# I e en a i n be

ALL ISP d hi . Re i e g ba .

- If 10% f ISP d n i e en ⇒ n defen e
- N incen e f de e

<u>2017</u>:

- 33% f A . S e a e f fab e
  ( fe .caida. g)
- 23% f ann nced IP add e ace i fab e

Reca : 309 Gb a ac ed n 3 ne (3/2013)

# 2. T acebac [Sa age e a . 00]

- G a :
  - Gi en e f a ac ac e
  - De e i e a h ce
- H : change e ec d inf i ac e
- A i n :
  - M e e ai nc i ed
  - A ac e end an ac e
  - R e f a ac e ic i e ai e a i e ab e

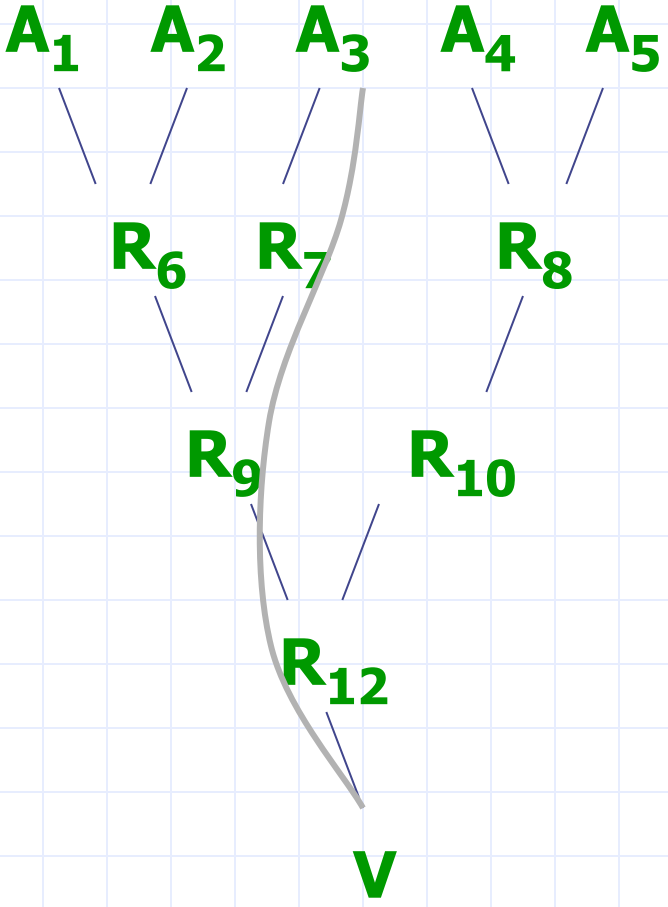
# Si e e h d

- W i e a h in ne ac e
  - Each e add i n IP add e ac e
  - Vic i ead a h f ac e

- P b e :
  - Re i e ace in ac e
    - Pa h can be ng
    - N e a fie d in c en IP f a
      - Change ac e f a ch e ec

# Be e idea

- DD Si e an ac e n a e a h
- S e ne i in each ac e
  - Each e abi i ica e n add e
  - Fi ed ade ega d e f a h eng h



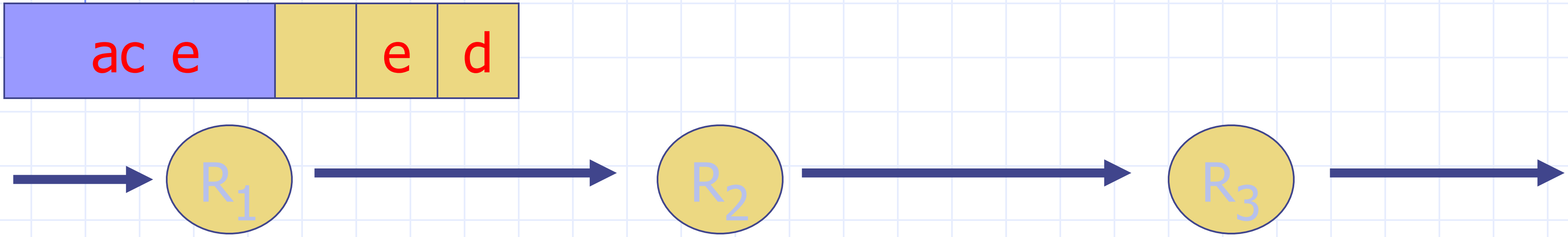
# Edge Sa ing

- Da a fie d e ac e :
  - Edge a and end IP add e e e
  - Di a ce: n be f h ince edge ed
- Ma ing ced e f e R

```
if c in n head i h babi i ) he n
        i e R i a add e
        i e 0 i di ance fie d
e e
        i di a e == 0 i e R i end
fie d
        inc e en di ance fie d
```

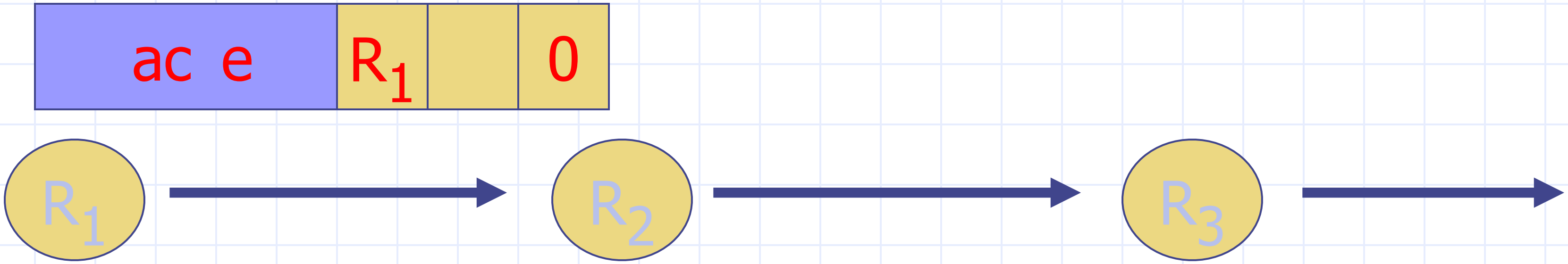
# Edge Sa ing: ic e

- Pac e ecei ed
  - $R_1$ ecei e ac e f ce an he e
  - Pac e c n ain ace f a , end, di ance



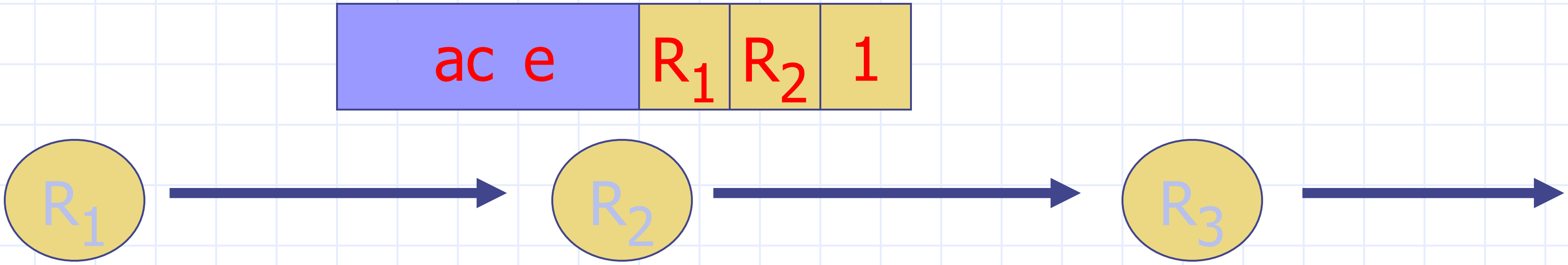
# Edge Sa ing: ic e

- Begin i ing edge
  - $R_1$ ch e i e a f edge
  - Se di ance 0



# Edge Sa ing

- Fini h i ing edge
  - $R_2$ ch e n e i e edge
  - Di ance i 0
    - W i e end f edge, inc e en di ance 1



ac e

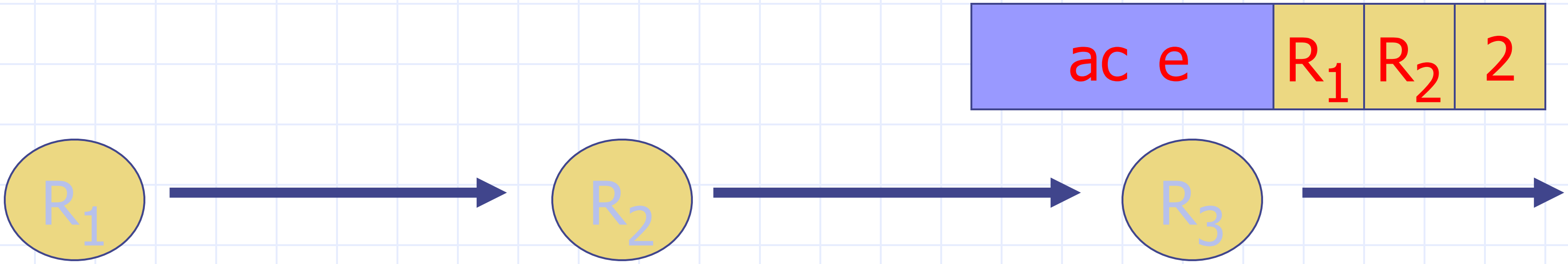
$R_1$

$R_2$

1

# Edge Sa ing

- Inc e en di ance
  - $R_3$ c e n e i e edge
  - Di ance >0
    - Inc e en di ance 2



# Pa h ec n c i n

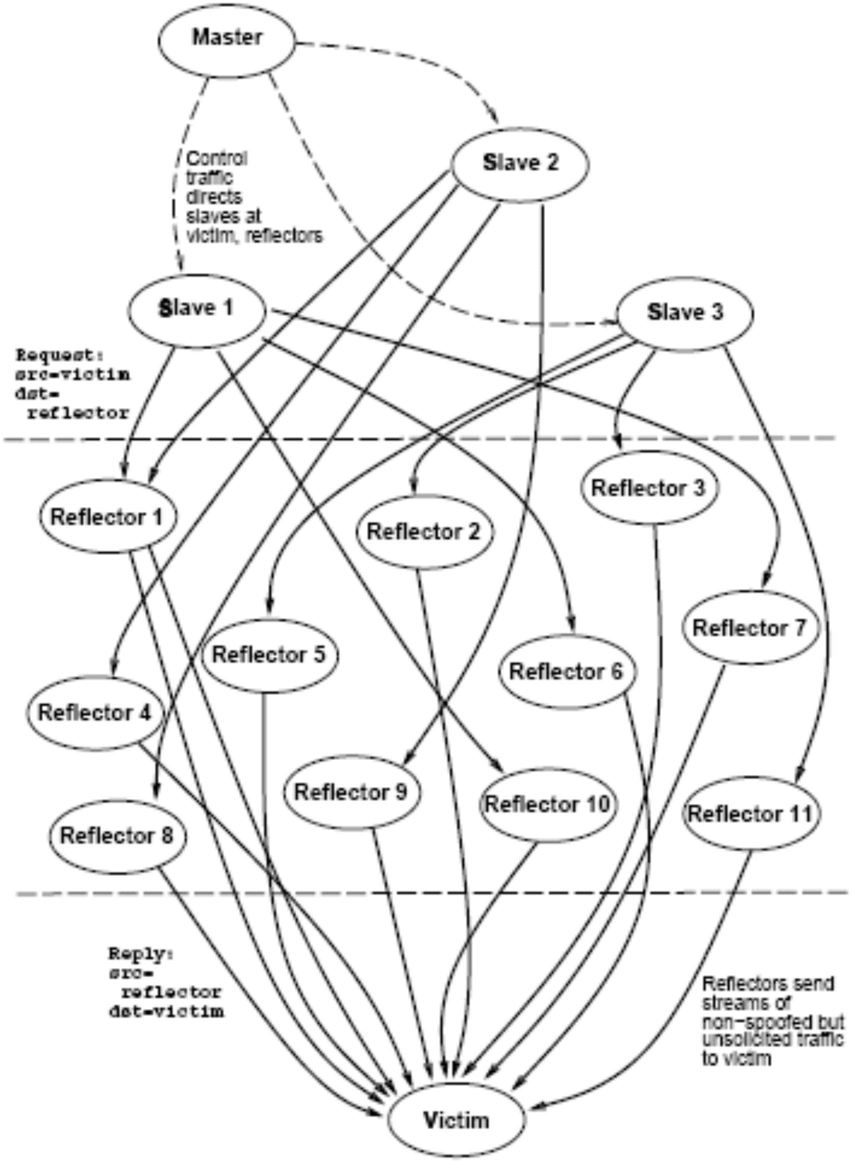
- E ac inf a i n f a ac ac e
- B i d g a h ed a ic i
  - Each ( a ,end,di ance) e ide an edge
- # ac e needed ec n c a h

$$E(X) < \frac{\ln(d)}{p(1-p)^{d-1}}$$

he e i a ing babi i , d i eng h f a h

# D S A ac

- Si e Ma e
- Ma b gene a e f d
- Zi i n f ef ec hide b
  - Ki acebac and hbac e h d


Master
Control traffic directs slaves at victim, reflectors
Slave 1
Slave 2
Slave 3
Request: src=victim dst=reflector
Reflector 1
Reflector 2
Reflector 3
Reflector 4
Reflector 5
Reflector 6
Reflector 7
Reflector 8
Reflector 9
Reflector 10
Reflector 11
Reply: src=reflector dst=victim
Reflectors send streams of non-spoofed but unsolicited traffic to victim
Victim

# Ca abi i ba ed defen e

# Ca abi i ba ed defen e

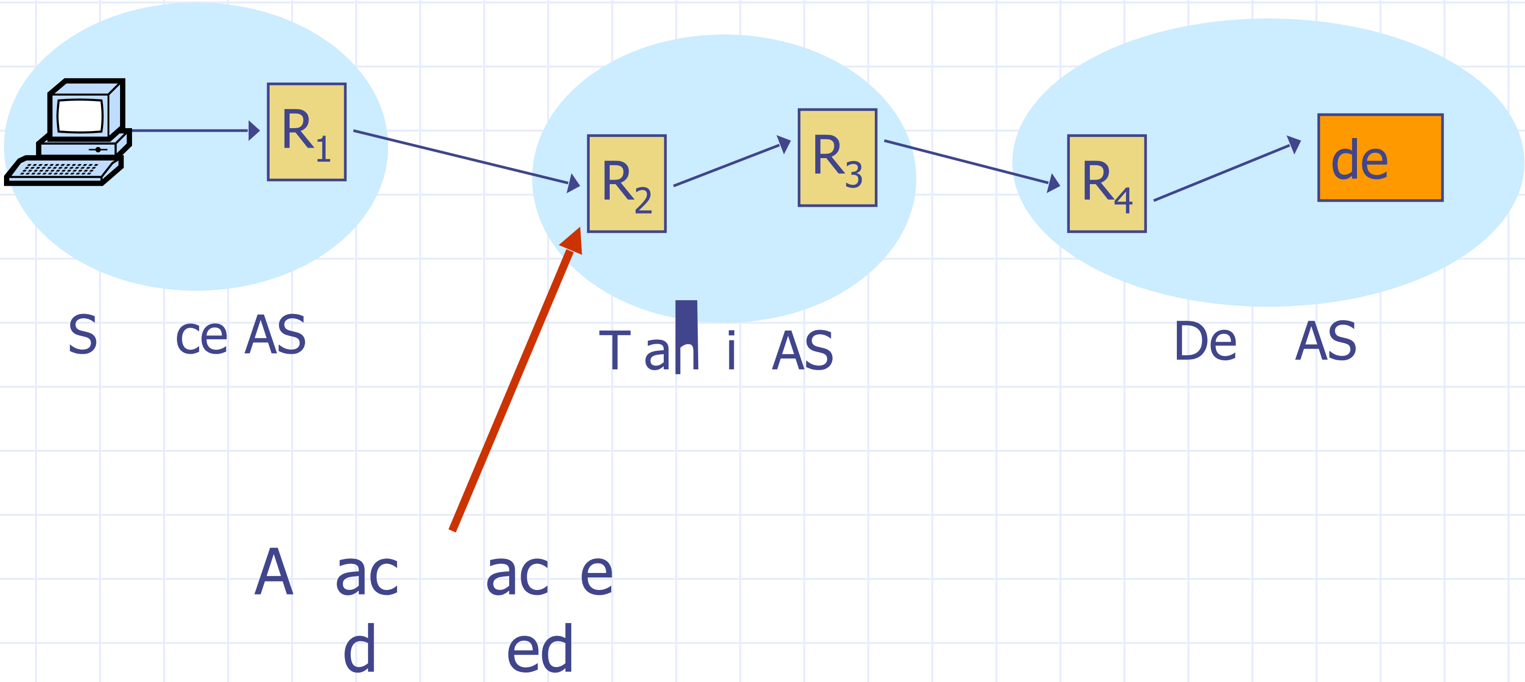
- Ande n, R e, We he a .
  - P e en ing n e e de ia - f- e ice i h ca abi i ie . SIGCOMM 04.
- Ya , Pe ig, and S ng.
  - Siff: A a e e n e ne f fi e i iga e DD S ding a ac . IEEE S&P 04.
- Yang, We he a , Ande n.
  - A D S- i i ing ne a chi ec e. SIGCOMM 05

# Ca abi i ba ed defen e

- Ba ic idea:
  - Re ei e ca n ecif ha ac e he an
- H :
  - Se de e e ca abi i in SYN ac e
    - Pa h iden ifie ed i i # e f ne ce
  - Re ei e e nd i h ca abi i
  - Se de inc de ca abi i in a f e ac e
  - **Main point:** R e n f a d:
    - Re e ac e , and
    - Pac e i h a id ca abi i

# Ca abi i ba ed defen e

- Ca abi i ie can be e ed if ce i a ac ing
  - B c a ac ac e c e ce



# Ta e h e e age:

- De ia f Se ice a ac a e ea :
  M be c ide ed a de ign i e
- Sa n:
  - In e ne i i -e i ed hand e DD S a ac
  - Man c e cia i n : C dF a e, A a ai,
- Man a f c e ede ign