Denial of Service

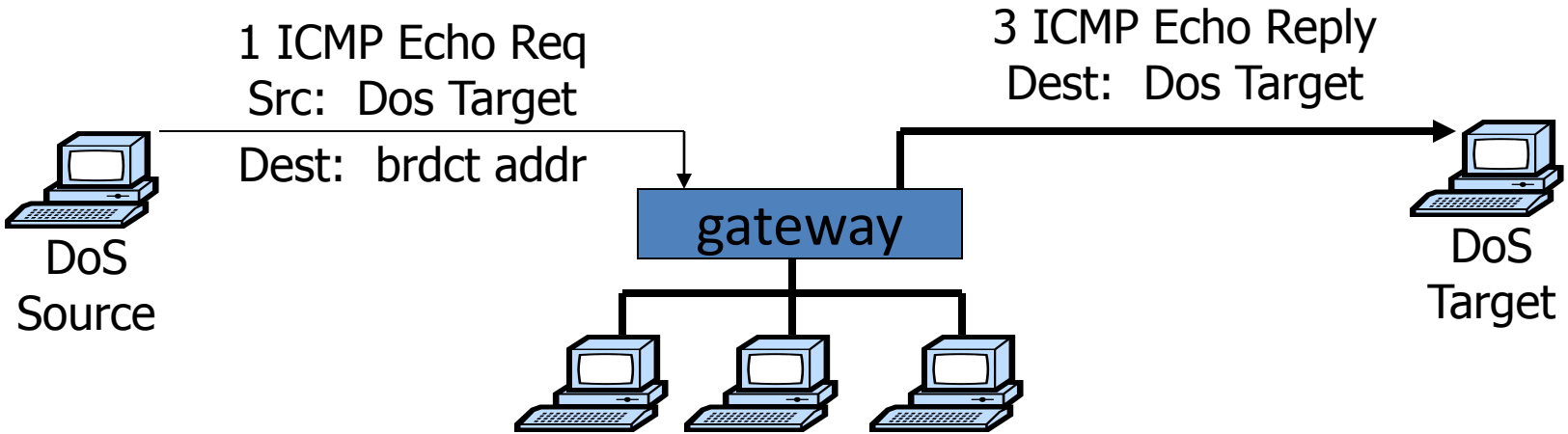
What is network DoS?

- Goal: take out a large site with little computing work
- How: **Amplification**
  - Small number of packets $\Rightarrow$ big effect
- Two types of amplification attacks:
  - DoS bug:
    - Design flaw allowing one machine to disrupt a service
  - DoS flood:
    - Command bot-net to generate flood of requests

DoS can happen at any layer

- This lecture:
  - Sample Dos at different layers (by order):
    - Link
    - TCP/UDP
    - Application
    - Payment
  - Generic DoS solutions
  - Network DoS solutions
- Sad truth:
  - Current Internet not designed to handle DDoS attacks

Smurf amplification DoS attack

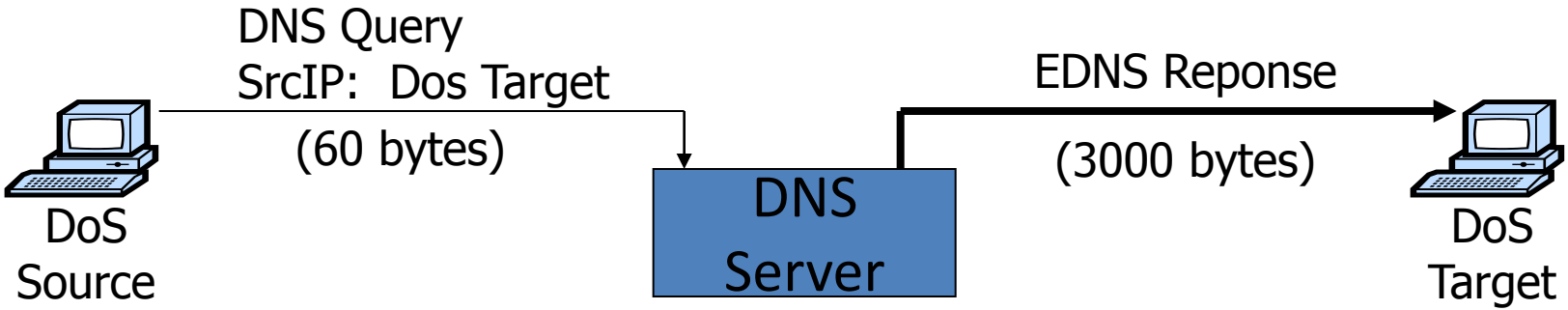


- Send ping request to broadcast addr (ICMP Echo Req)
- Lots of responses:
  - Every host on target network generates a ping reply (ICMP Echo Reply) to victim

Prevention: reject external packets to broadcast address

Modern day example (May ’06)

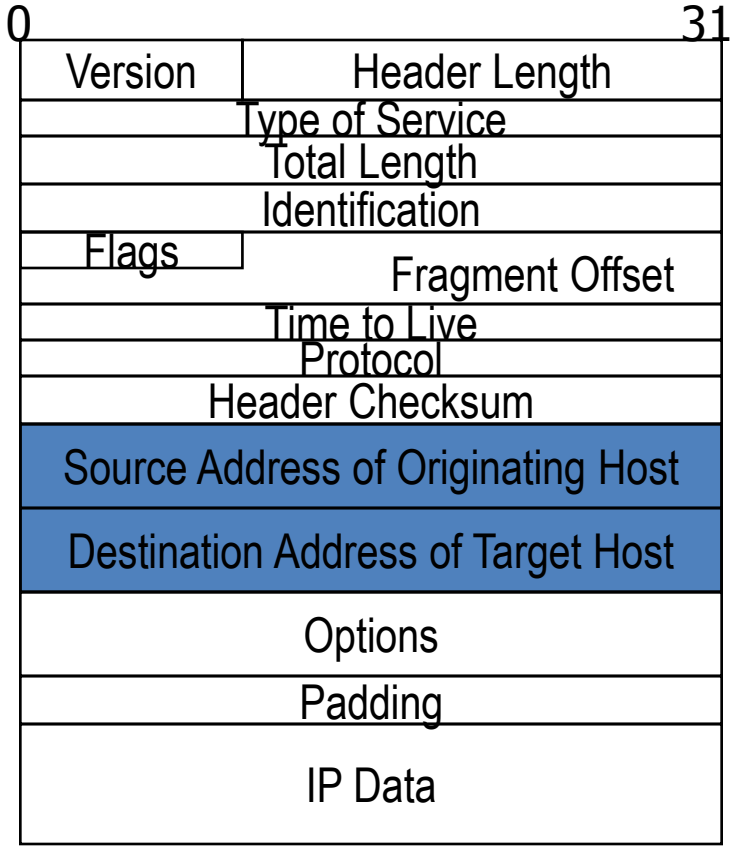
DNS Amplification attack: (×50 amplification)



580,000 open resolvers on Internet (Kaminsky-Shiffman’06)

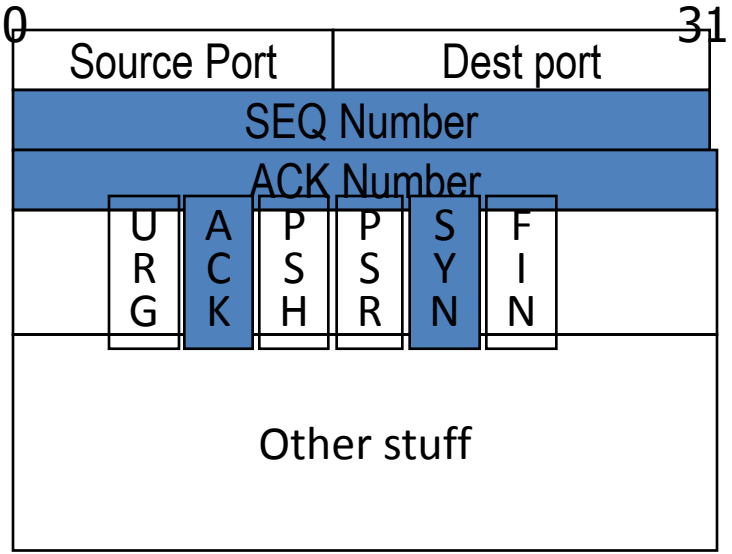
Review: IP Header format

- Connectionless
  - Unreliable
  - Best effort

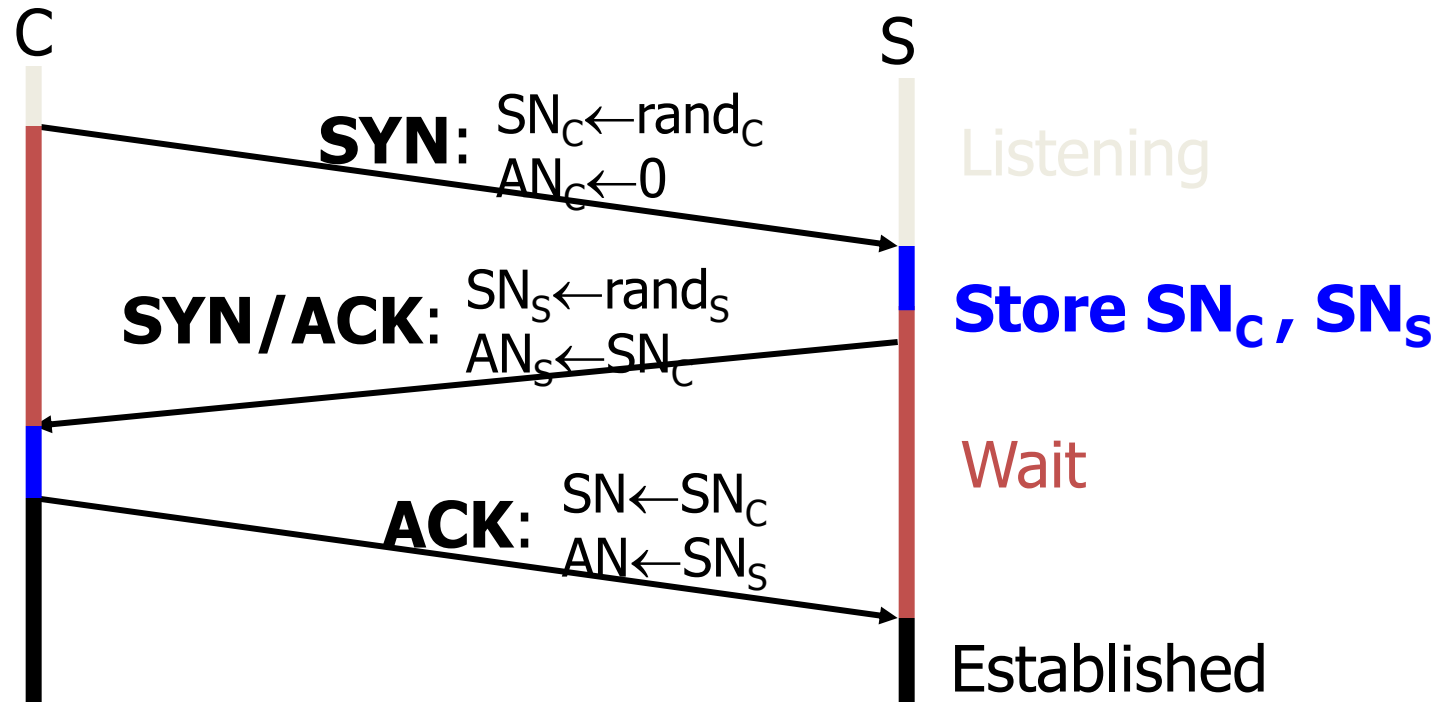


Review: TCP Header format

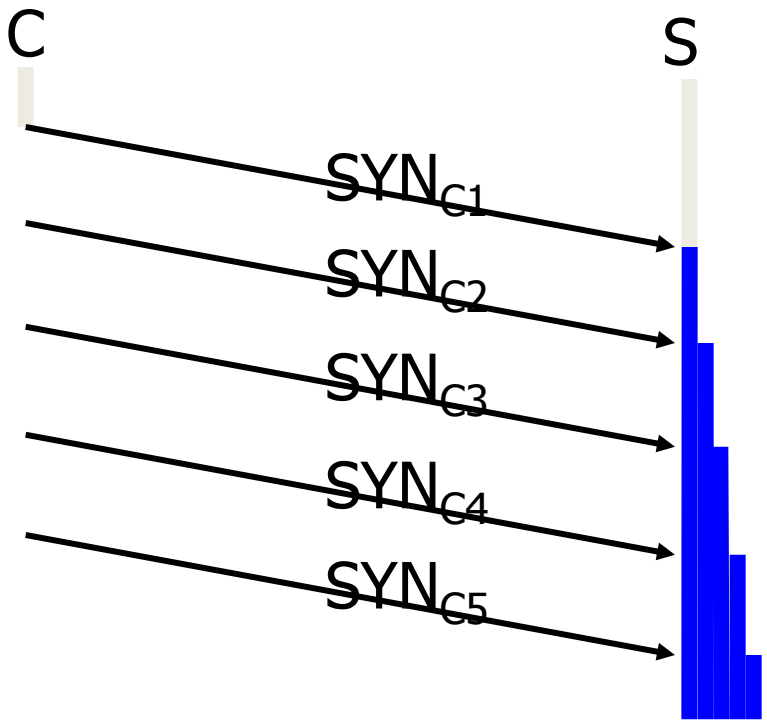
- TCP:
  - Session based
  - Congestion control
  - In order delivery



Review: TCP Handshake



TCP SYN Flood I: low rate (DoS bug)



Single machine:

- SYN Packets with **random source IP addresses**
- Fills up backlog queue on server
- No further connections possible

SYN Floods (phrack 48, no 13, 1996)

OS	Backlog queue size
Linux 1.2.x	10
FreeBSD 2.1.5	128
WinNT 4.0	6

Backlog timeout: 3 minutes

⇒ Attacker need only send 128 SYN packets every 3 minutes.

⇒ Low rate SYN flood

A classic SYN flood example

- MS Blaster worm (2003)
  - Infected machines at noon on Aug 16th:
    - SYN flood on port 80 to **windowsupdate.com**
    - 50 SYN packets every second.
      - each packet is 40 bytes.
    - Spoofed source IP: a.b.X.Y where X,Y random.
- MS solution:
  - new name: windowsupdate.microsoft.com
  - Win update file delivered by Akamai

Low rate SYN flood defenses

- Non-solution:
  - Increase backlog queue size or decrease timeout
- Correct solution (when under attack) :
  - **Syncookies**: remove state from server
  - Small performance overhead

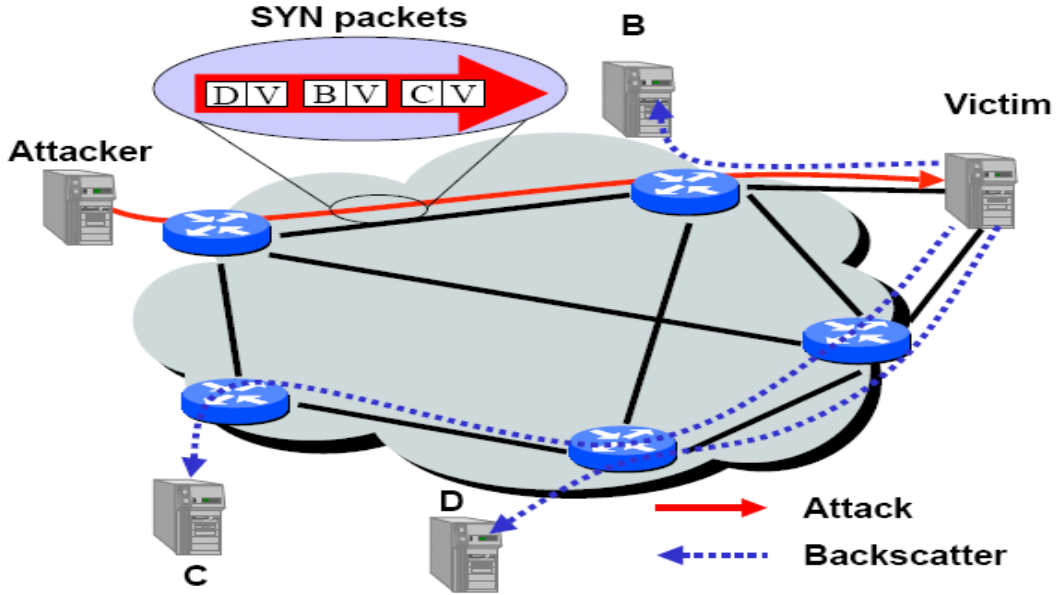
Syncookies

[Bernstein, Schenk]

- Idea: use secret key and data in packet to gen. server SN
- Server responds to Client with SYN-ACK cookie:
  - T = 5-bit counter incremented every 64 secs.
  - $L = MAC_{key}$ (SAddr, SPort, DAddr, DPort, SN_C, T) [24 bits]
    - key: picked at random during boot
  - SN_S = (T . mss . L) (|L| = 24 bits)
  - **Server does not save state** (other TCP options are lost)
- Honest client responds with ACK ($AN=SN_S$, $SN=SN_C+1$)
  - Server allocates space for socket only if valid SN_S.

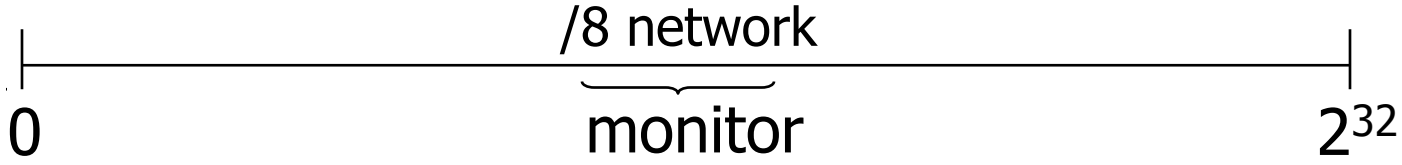
SYN floods: backscatter [MVS' 01]

- SYN with forged source IP ⇒ SYN/ACK to



Backscatter measurement [MVS' 01]

- Listen to unused IP addresss space (darknet)



- Lonely SYN/ACK packet likely to be result of SYN attack

- 2001: **400** SYN attacks/week
- 2008: **4425** SYN attacks/24 hours (arbor networks ATLAS)

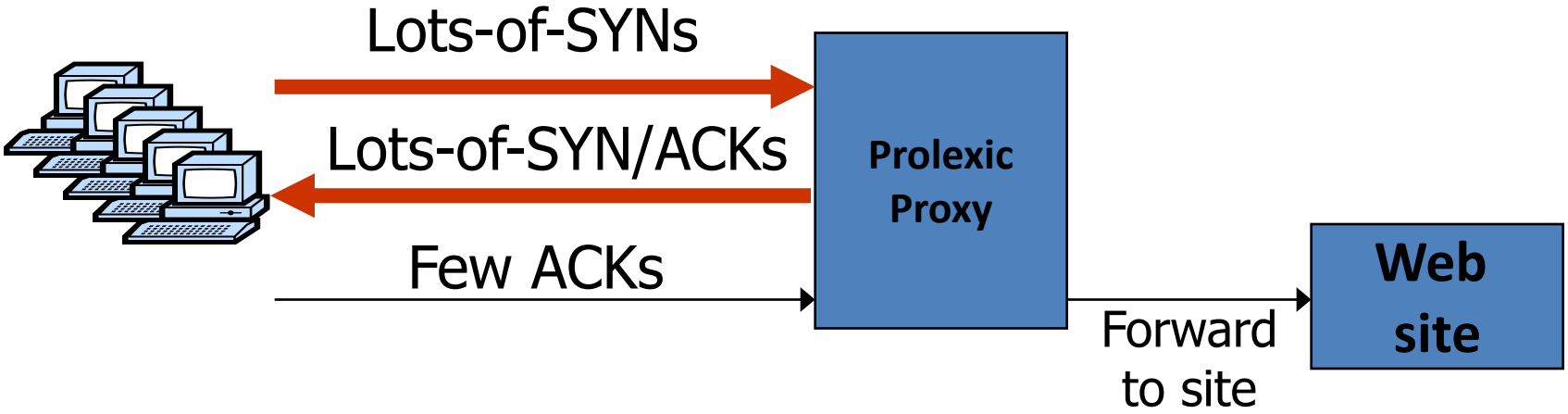
  - Larger experiments: (monitor many ISP darknets)
    - Arbor networks
    - Network telescope (UCSD)

SYN Floods II: Massive flood (e.g BetCris.com '03)

- Command bot army to flood specific target: (DDoS)
  - **20,000** bots can generate **2Gb/sec** of SYNs (2003)
  - At web site:
    - Saturates network uplink or network router
    - Random source IP $\Rightarrow$
      attack SYNs look the same as real SYNs

Prolexic

- Idea: only forward established TCP connections to site



- Prolexic capacity: 20Gb/sec link

  can handle $40 \cdot 10^6$ SYN/sec

Stronger attacks: TCP connection flood

- Command bot army to:
  - Complete TCP connection to web site
  - Send short HTTP HEAD request
  - Repeat
- Will bypass SYN flood protection proxy
- … but:
  - Attacker can no longer use random source IPs.
    - Reveals location of bot zombies
  - Proxy can now block or rate-limit bots.

DNS DoS Attacks (e.g. bluesecurity ’06)

- DNS runs on UDP port 53
  - DNS entry for victim.com hosted at victim_isp.com
- DDoS attack:
  - flood victim_isp.com with requests for victim.com
  - **Random source IP address** in UDP packets
- Takes out entire DNS server: (collateral damage)
  - bluesecurity DNS hosted at Tucows DNS server
  - DNS DDoS took out Tucows hosting many many sites

Root level DNS attacks

- Feb. 6, 2007:
  - Botnet attack on the 13 Internet DNS root servers
  - Lasted 2.5 hours
  - None crashed, but two performed badly:
    - g-root (DoD), l-root (ICANN)
    - Most other root servers use anycast

Attack in Oct. 2002 took out 9 of the 13 TLD servers

DoS via route hijacking

- YouTube is 208.65.152.0**/22** (includes 2^{10} IP addr)
  youtube.com is 208.65.153.238, …

- Feb. 2008:
  - Pakistan telecom advertised a BGP path for
    208.65.153.0**/24** (includes 2^8 IP addr)
  - Routing decisions use most specific prefix
  - The entire Internet now thinks
    208.65.153.238 is in Pakistan

- Outage resolved within two hours
  … but demonstrates huge DoS vuln. with no solution!