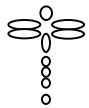


DNS amplification attacks

Matsuzaki Yoshinobu
<maz@iij.ad.jp>

DNS amplification attacks

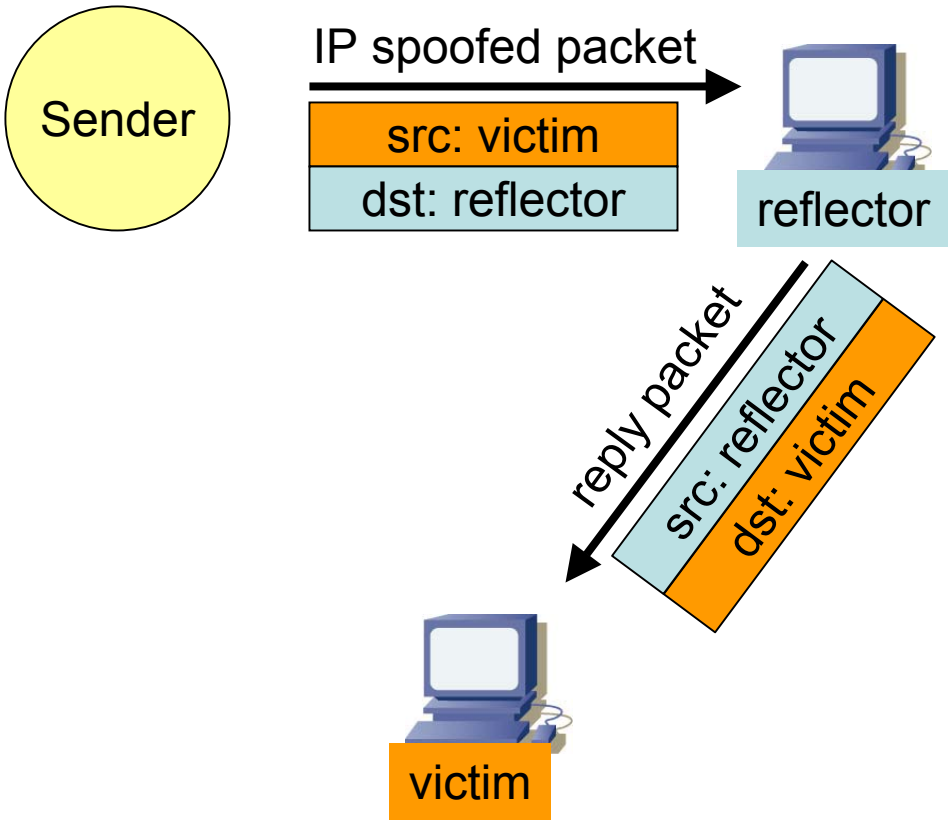
- Attacks using IP spoofed dns query
  - generating a traffic overload
  - bandwidth attack
  - similar to ‘smurf attacks’

- Components are:
  - IP spoofing
  - DNS amp

IP spoofing + DNS amp

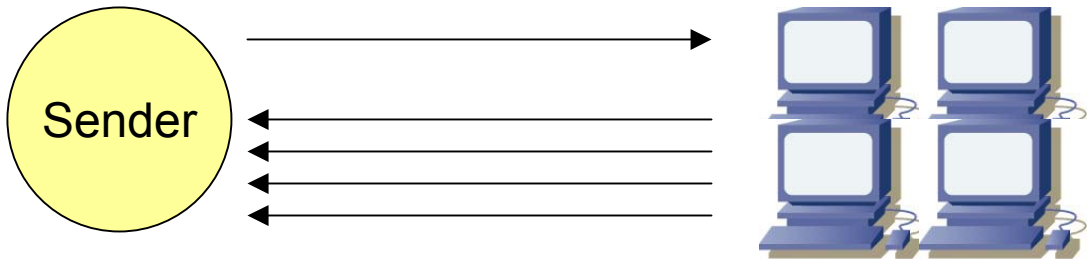
- IP spoofing
  - IP spoofed dns query
  - to use reflections
- DNS amp
  - UDP (no 3way handshake)
  - good amplification ratio =~ 60
  - distributed by full/stub-resolver (dns cache)

reflection



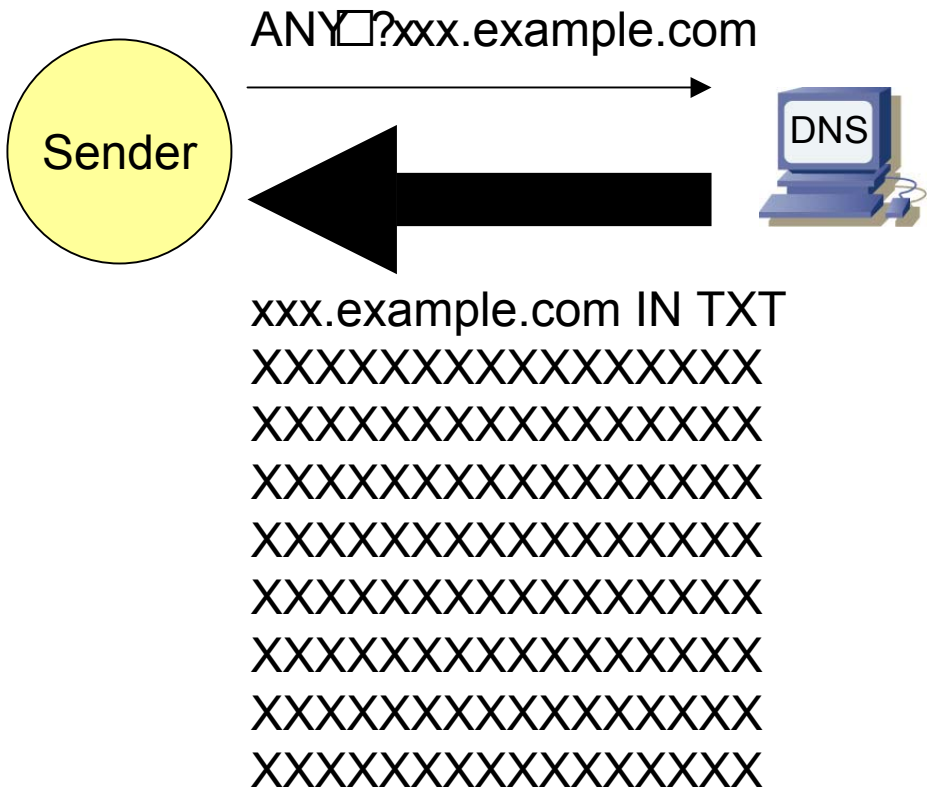
amplification

1. multiple replies

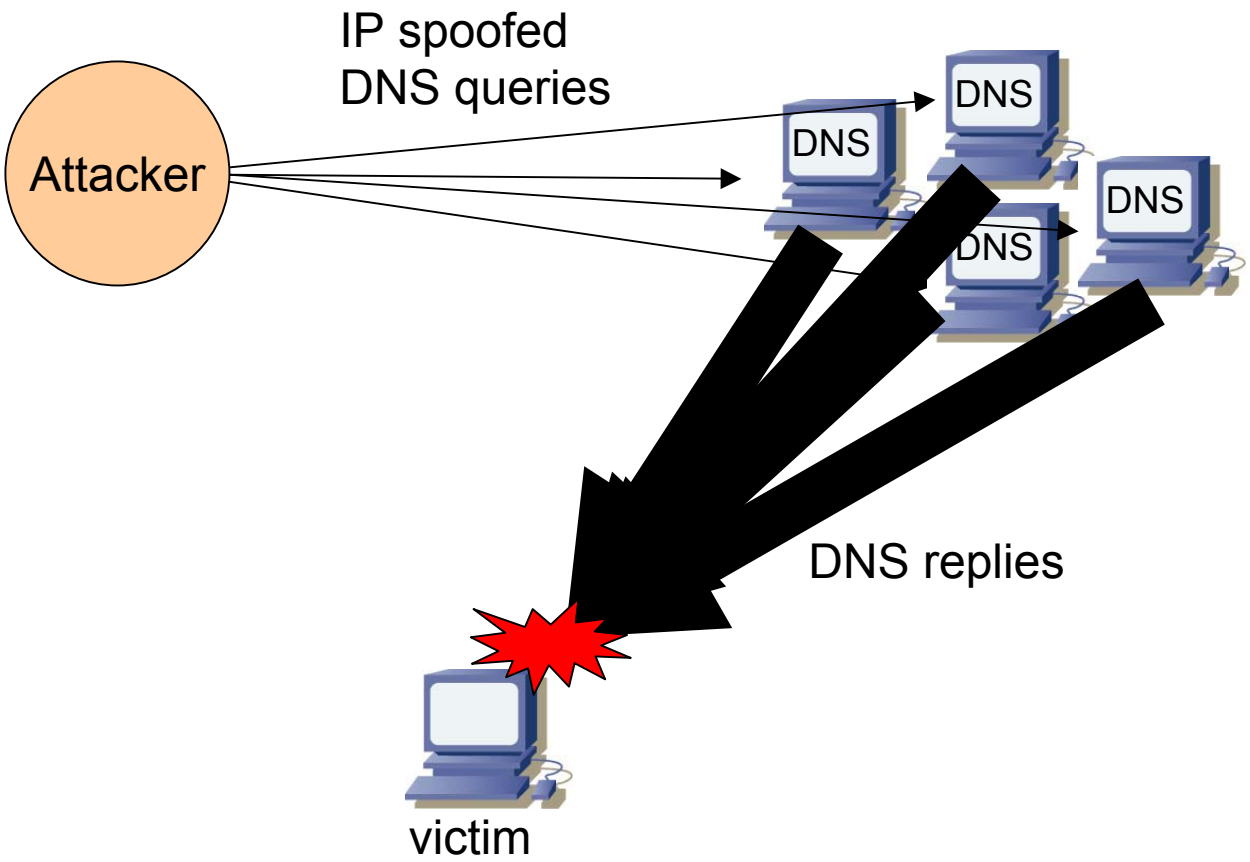


2. bigger reply

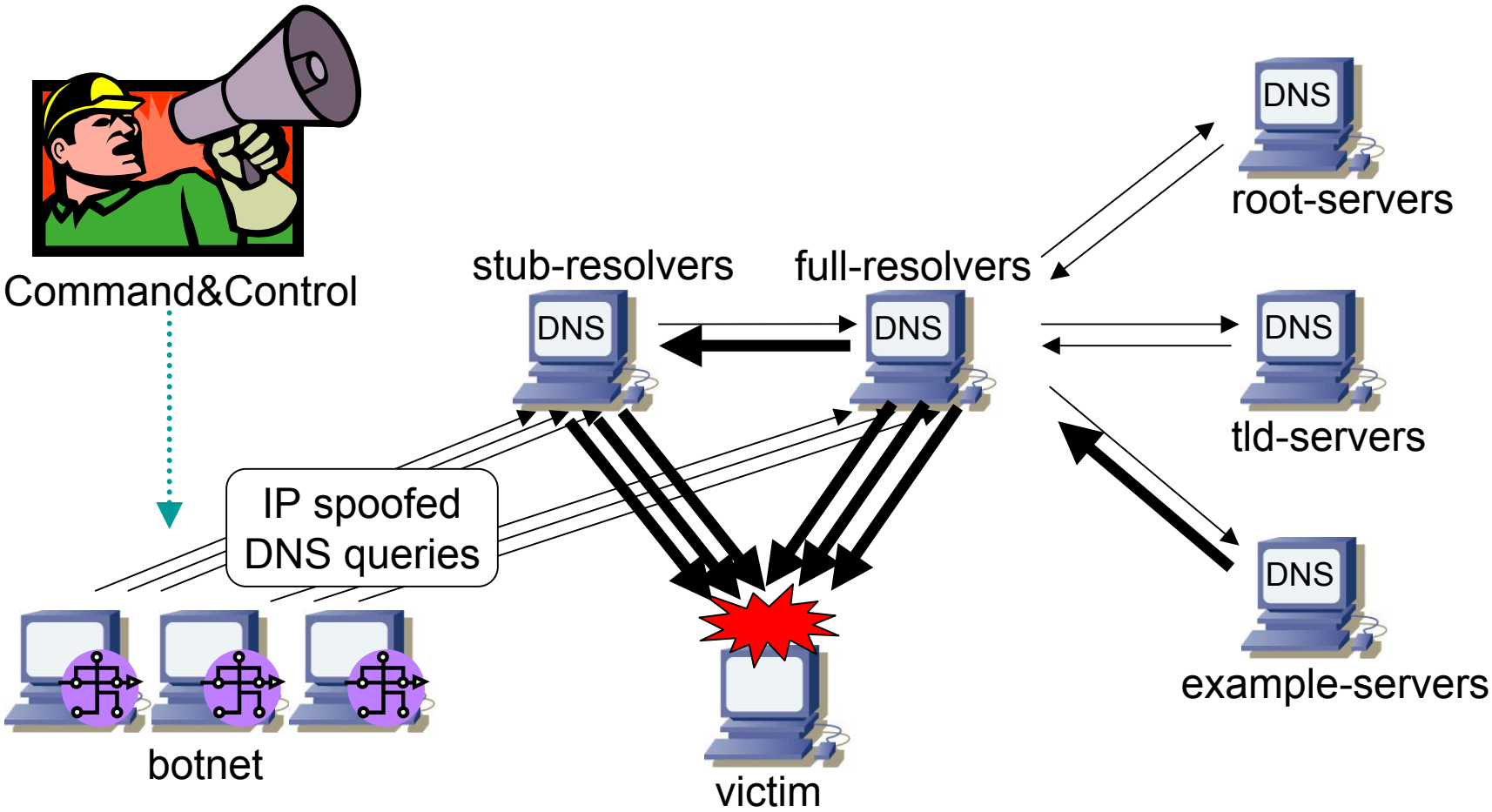
DNS amplification



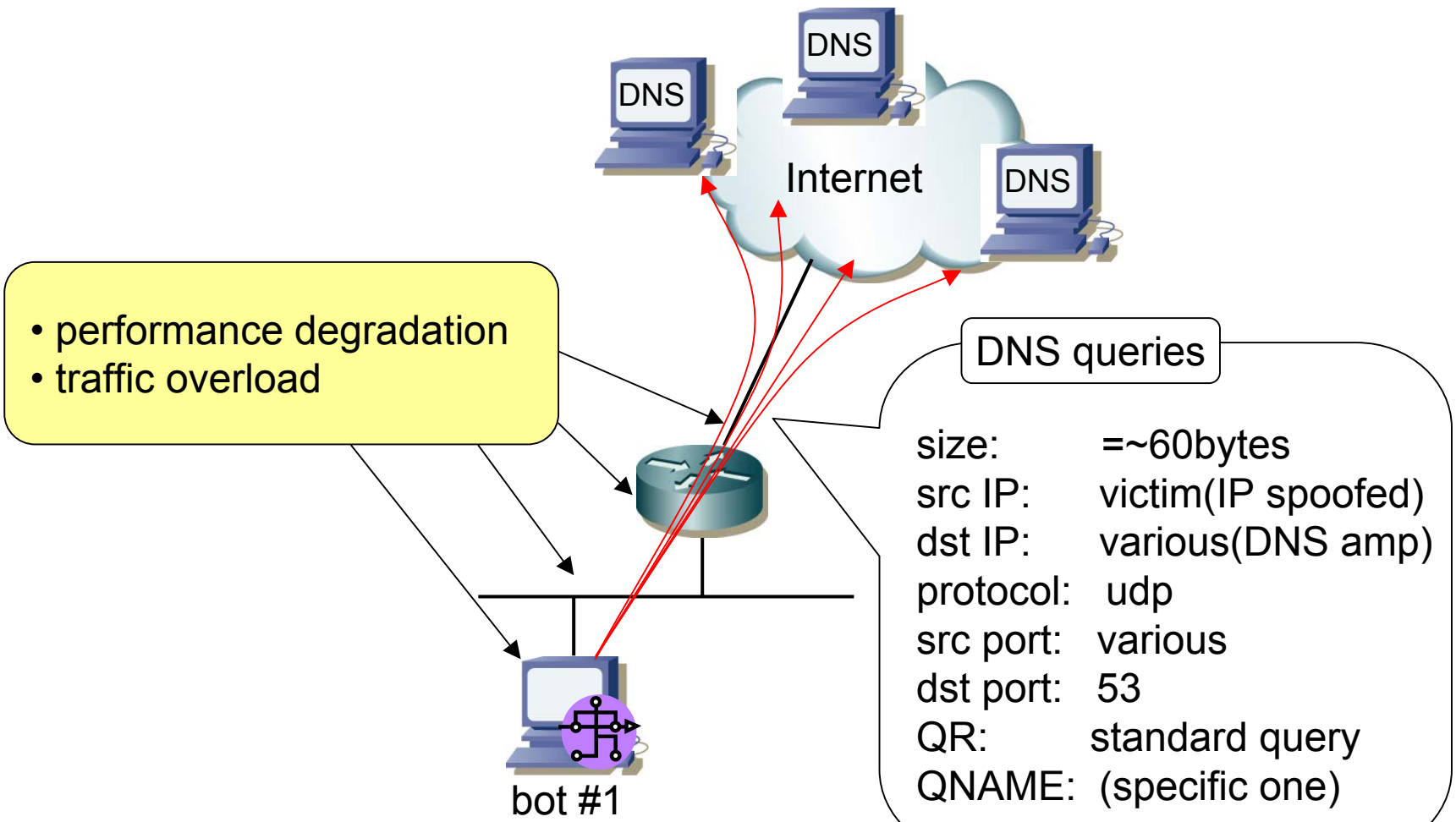
DNS amplification attack



attack relations

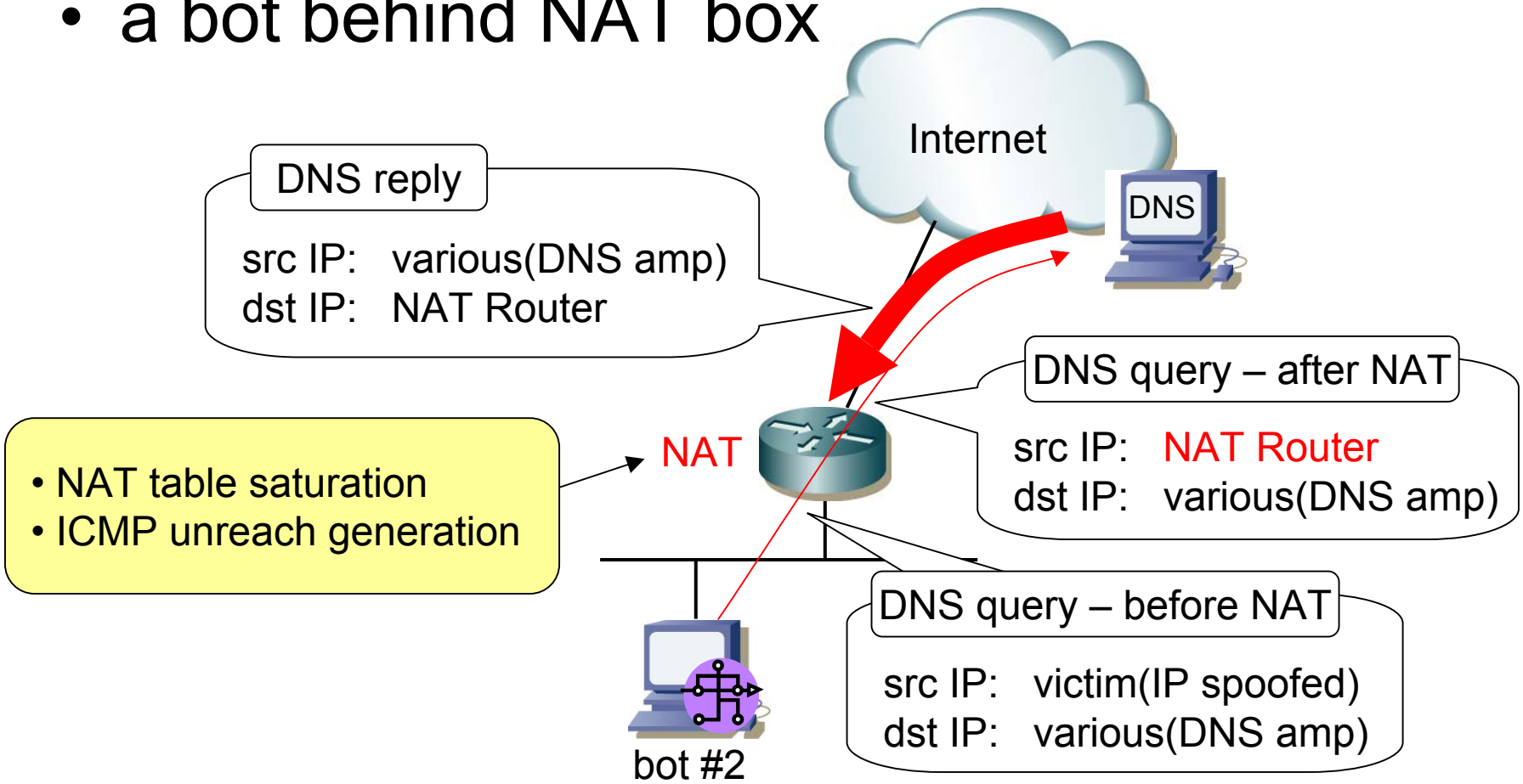


view of bot #1

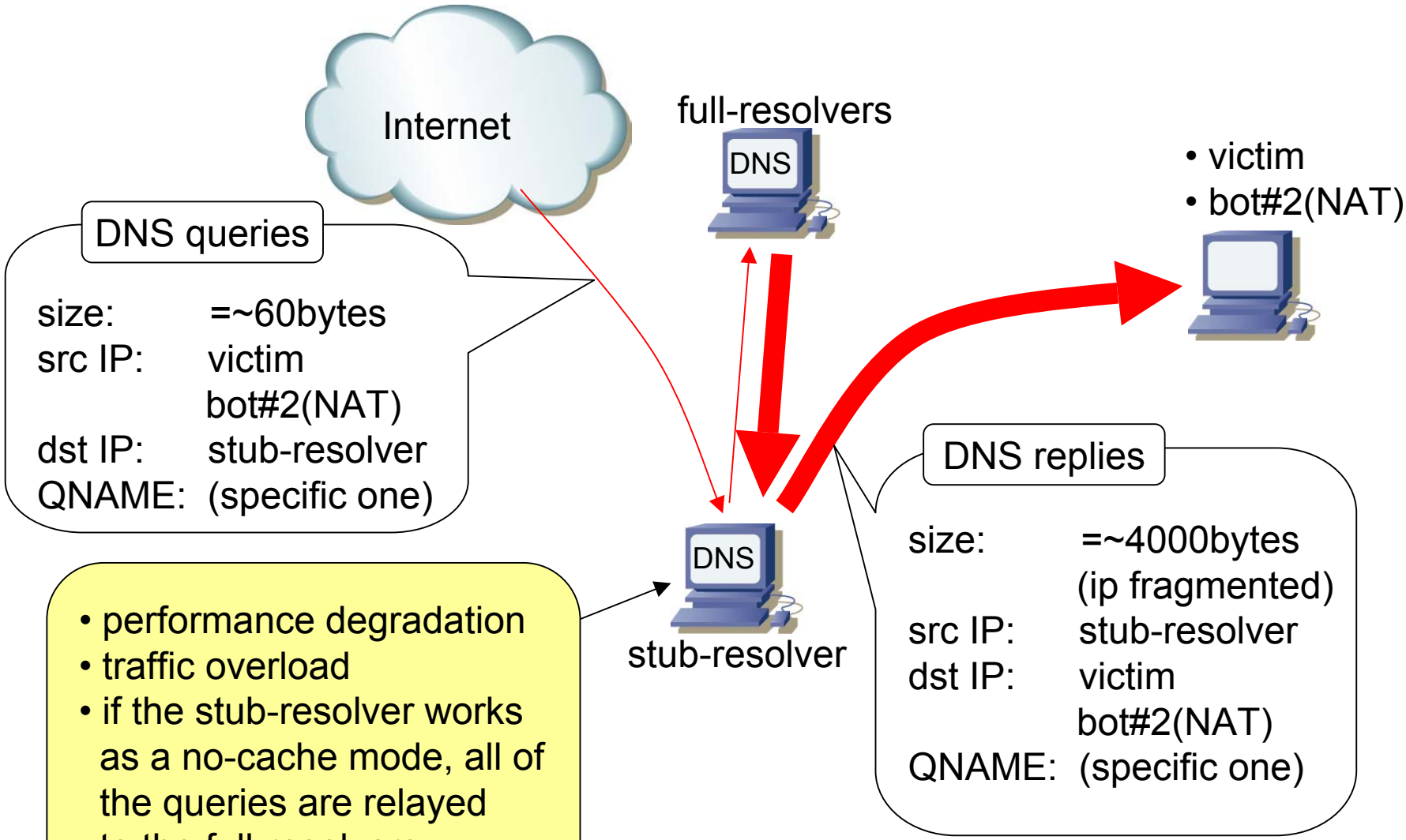


view of bot #2

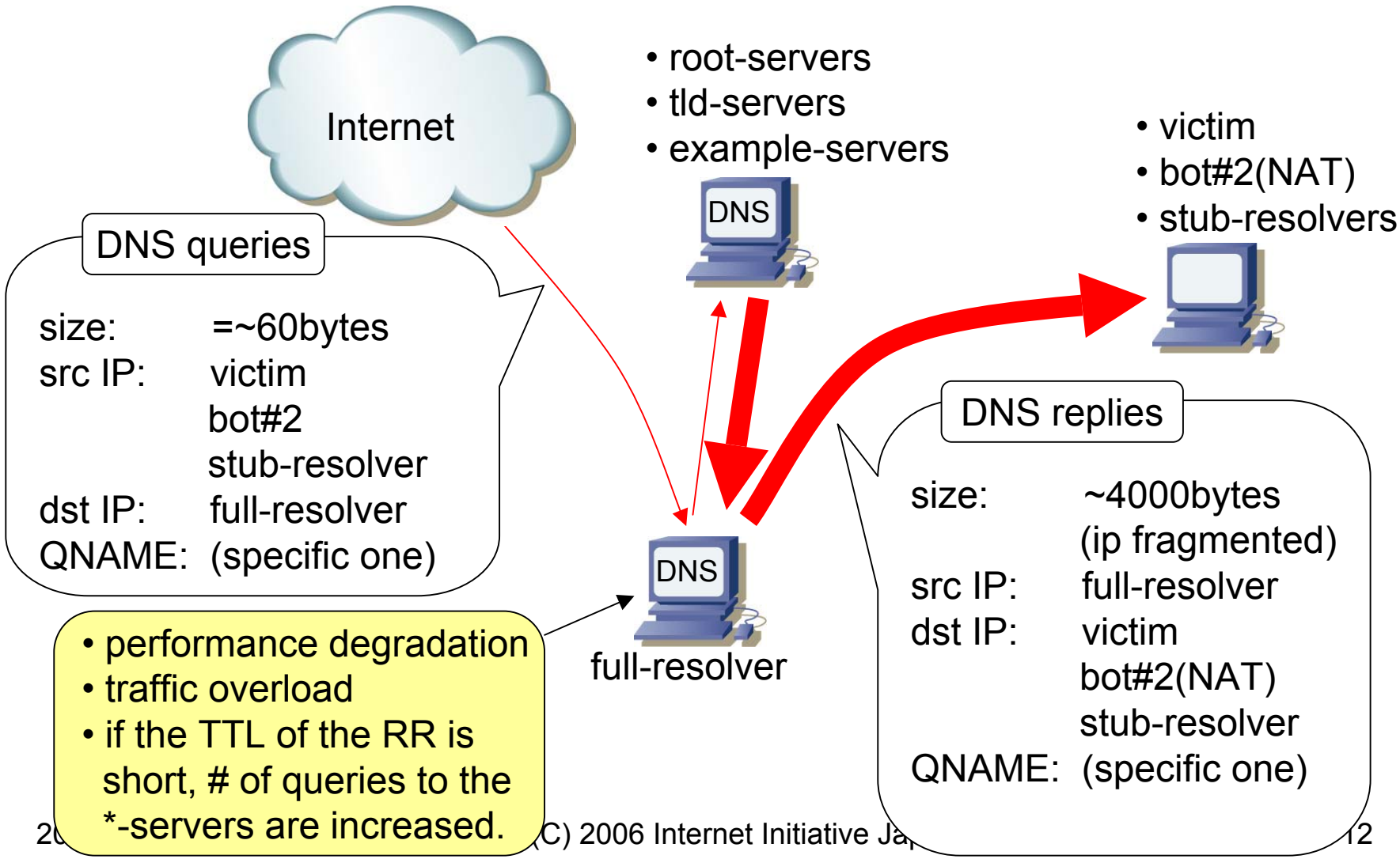
- a bot behind NAT box



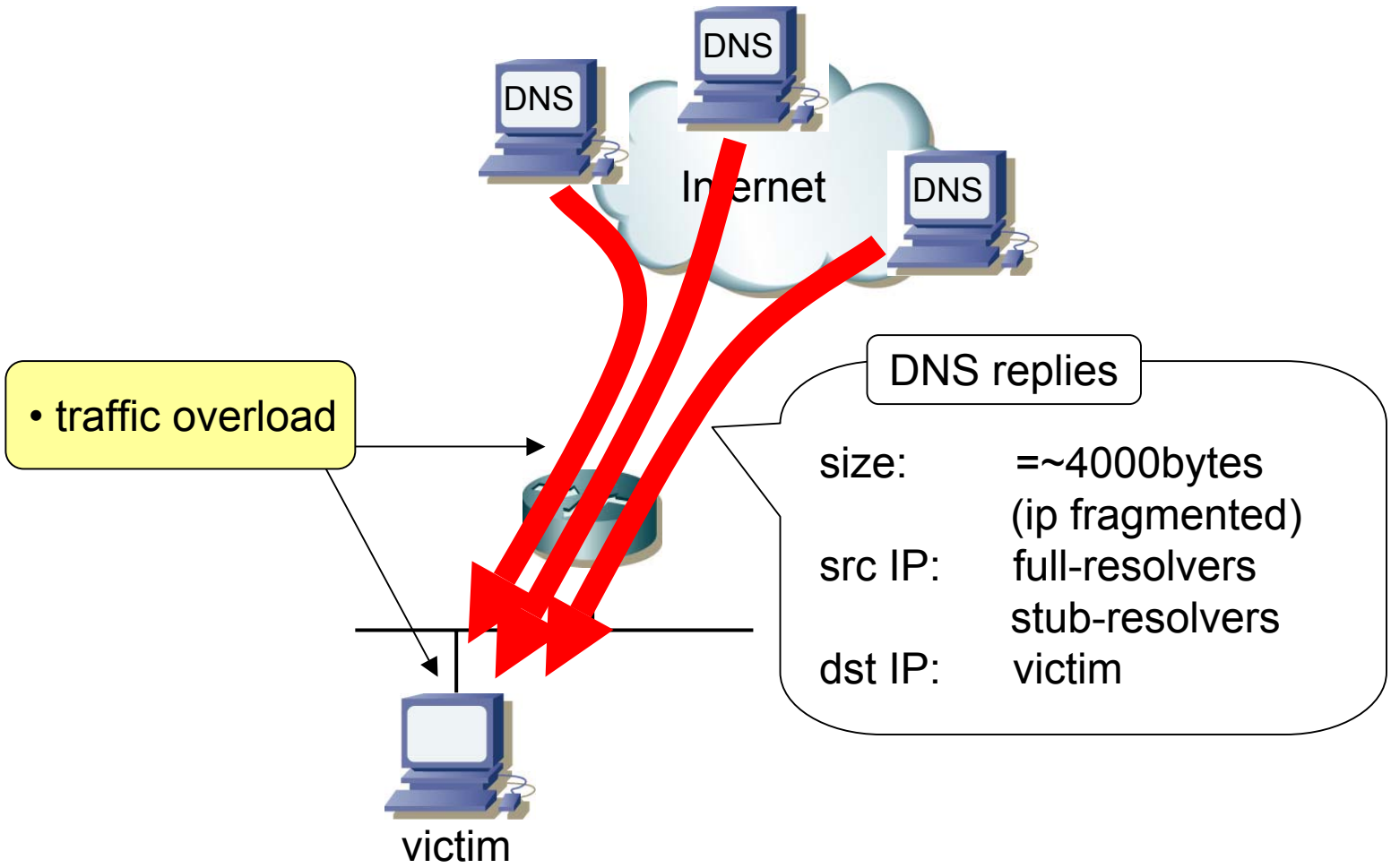
view of stub-resolver



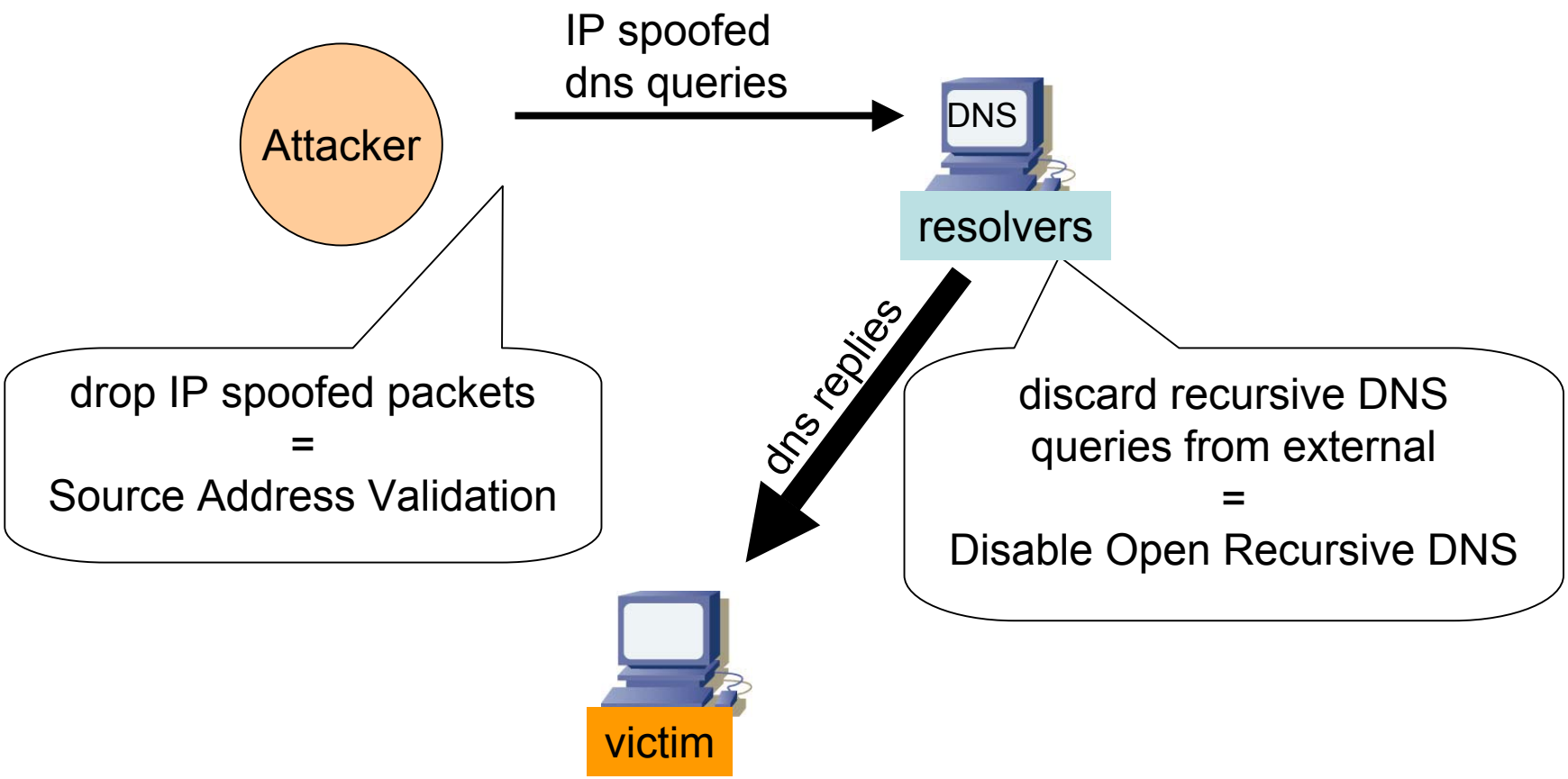
view of full-resolver



view of victim



solutions



Disable Open Recursive DNS

- There are many ‘open relay’ resolvers.
  - ISP cache servers
  - customers’ dns servers
  - DSL routers (dns proxy as stub-resolver)

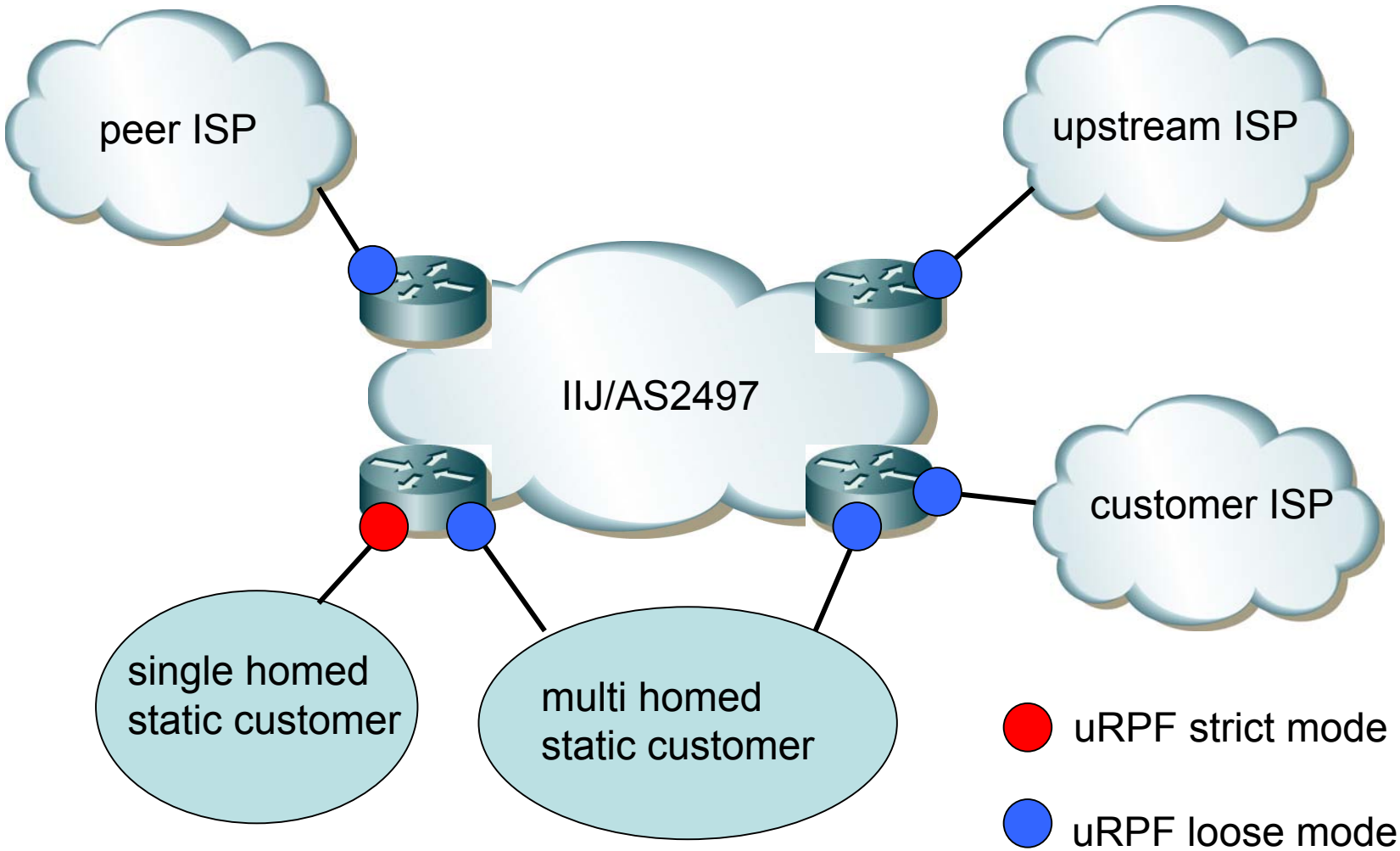
Source Address Validation

- BCP38/RFC2827
  - All providers of Internet connectivity are urged to implement filtering described in this document to prohibit attackers from using forged source addresses...

IIJ/AS2497's case

- **IIJ to Introduce Source Address Validation to all its Connectivity Services**
  - http://www.iij.ad.jp/en/pressrelease/2006/0308.html
- IIJ is adopting uRPF and ACLs.

IIJ's policy



CISCO uRPF configuration

uRPF strict mode

```
interface GigabitEthernet0/0
 ip verify unicast source reachable-via rx
```

uRPF loose mode

```
interface GigabitEthernet0/0
 ip verify unicast source reachable-via any
```

Juniper uRPF configuration

uRPF strict mode

```
interface { ge-0/0/0 { unit 0 { family inet {
 rpf-check;
} } } }
```

uRPF loose mode

```
interface { ge-0/0/0 { unit 0 { family inet {
 rpf-check { mode loose; }
} } } }
```

reference

- AL-1999.004 – DoS attacks using the DNS
  - http://www.auscert.org.au/render.html?it=80
- The Continuing DoS Threat Posed by DNS Recursion
  - http://www.us-cert.gov/reading_room/DNS-recursion033006.pdf
- SAC008 – DNS Distributed DDoS Attacks
  - http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf

END