# IPv6 and security

*More bits, more vulns!*

# Contents


- Introduction
- Scanning IPv6 ranges
- Fragmentation attacks
- RA flooding
- SLAAC attack

# Introduction - about us

Stef van Dop

- Security consultant at Outpost24
- member of Techinc

Christiaan Ottow

- Project manager at Pine Digital Security
- Likes networking

# Introduction - about IPv6

- Many new features
  - Neighbor Discovery
  - Extension headers
  - Multicast over broadcast
  - Address scopes
- LANs depend on trust
  - No authentication between hosts
  - More features => more trust dependency
- Dual stack problems
  - Security policy discrepancies
  - Unintended dual stack reachability

# Scanning IPV6 ranges

- Address patterns
- Discovery methods
- Address Assignment methods
- Example(s)
- Countermeasures

# Address patterns:

- SLAAC (Interface-ID based on the MAC address)
- IPv4-based (e.g., 2001:db8::192.168.10.1)
- “Low byte” (e.g., 2001:db8::1, 2001:db8::2, etc.)
- Privacy Addresses (Random Interface-IDs)
- “Wordy” (e.g., 2001:db8::dead:beef)
- Related to specific transition-co-existence technologies (e.g., Teredo)

Malone, D. 2008. Observations of IPv6 Addresses. Passive and Active Measurement Conference (PAM 2008, LNCS 4979), 29–30 April 2008.

# Host Discovery - Internal

This is the "easy" part, but even here full ping sweeps are impractical.

- Multicast
  - Send  ICMPv6 echo request packet to the all-nodes link-local multicast address (ff02::1)
- SLAAC
  - Send ICMPv6 RA packet which causes hosts to begin SLAAC and send a solicitation for their newly configured address.

# Host Discovery - External

Turns out to be quite doable too :)

- DNS Based:
  - advertised hostnames/ranges (such as MX records and AS names)
  - common hostnames (such as webmail.domain.tld)
  - patterns in hostnames (colo123.ipv6.domain.tld)
  - reverse lookups (ip6.arpa)
- Public information (google/bing, mailing lists, etc)
- Common/Default ip's (::0, ::1, ::2, ::80, :443, ::babe, ::b00b, ::1000-2000, etc.)

# Examples

- Discovery, AS3265:
  - 2001:0888::/30  Xs4all Internet BV
    - 4300 subnets discovered
    - 1881 ip6.arpa records (partial scan):
      - 52 percent ::1, 46 percent ::2
      - xs4all##.ipv6.xs4all.nl, vlan5.swcolo2.3d2.xs4all.net, etc

- Why do i care?
  - cwi.nl (port 80 on ipv4, port 22,80,443 on v6)
  - mediamatic.nl (p80 on v4, p22,80,873,8080 on v6)
  - etc..

# Solutions?

- The issue is different for servers and clients.

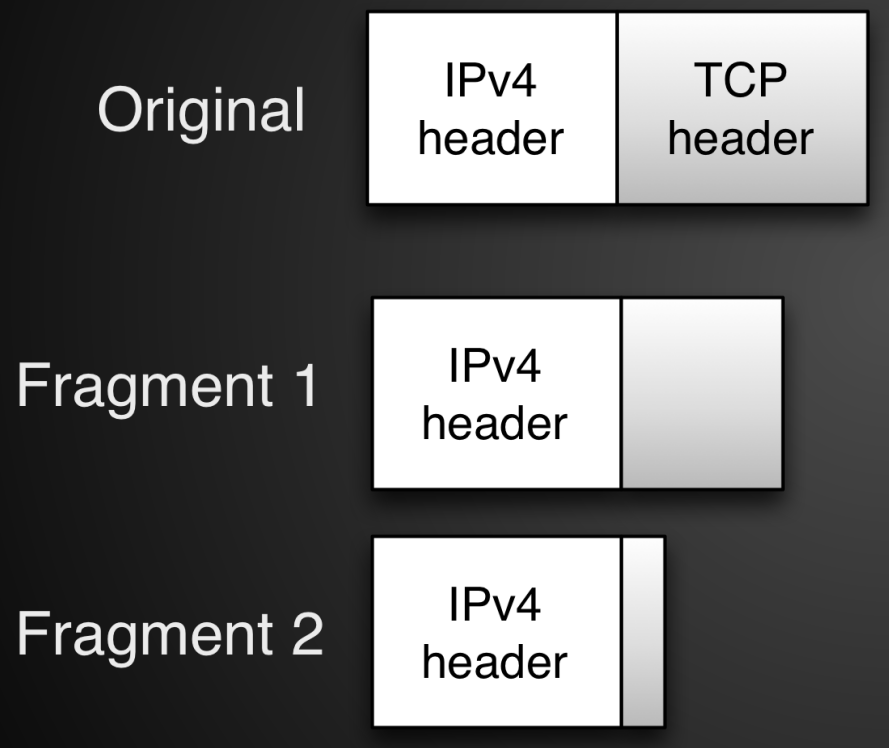
- SLAAC (MAC used as basis for least significant digits)
- DHCPv6 with Temporary adresses

//this is not a new problem: nuance.

# Fragmentation attacks

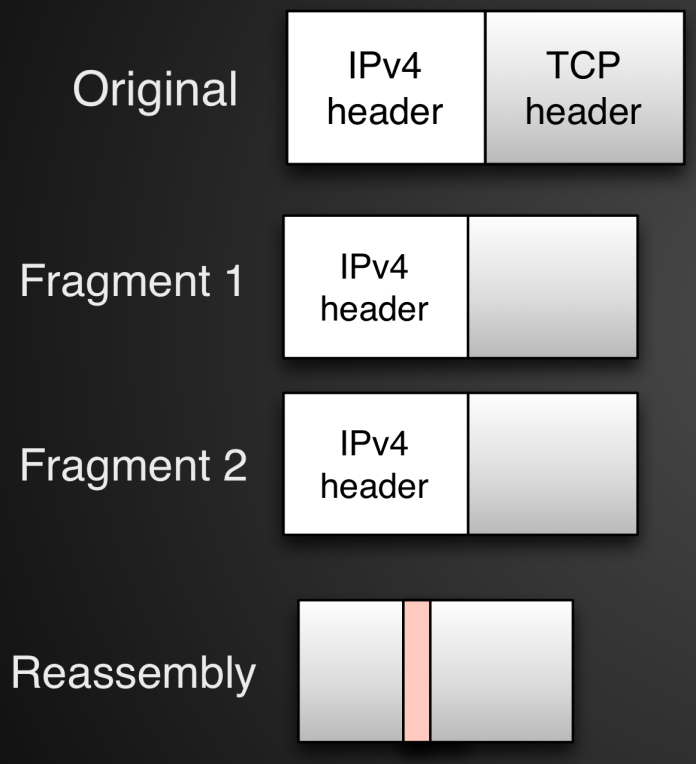
- IPv4 had issues with fragmentation
  - Overlapping fragments
  - Tiny fragments
- Firewalls use 5-tuple
  - src and dst port
  - src and dst addr
  - flags
- Decide on first fragment
  - All info fits in there, right?

# Fragmentation in IPv4



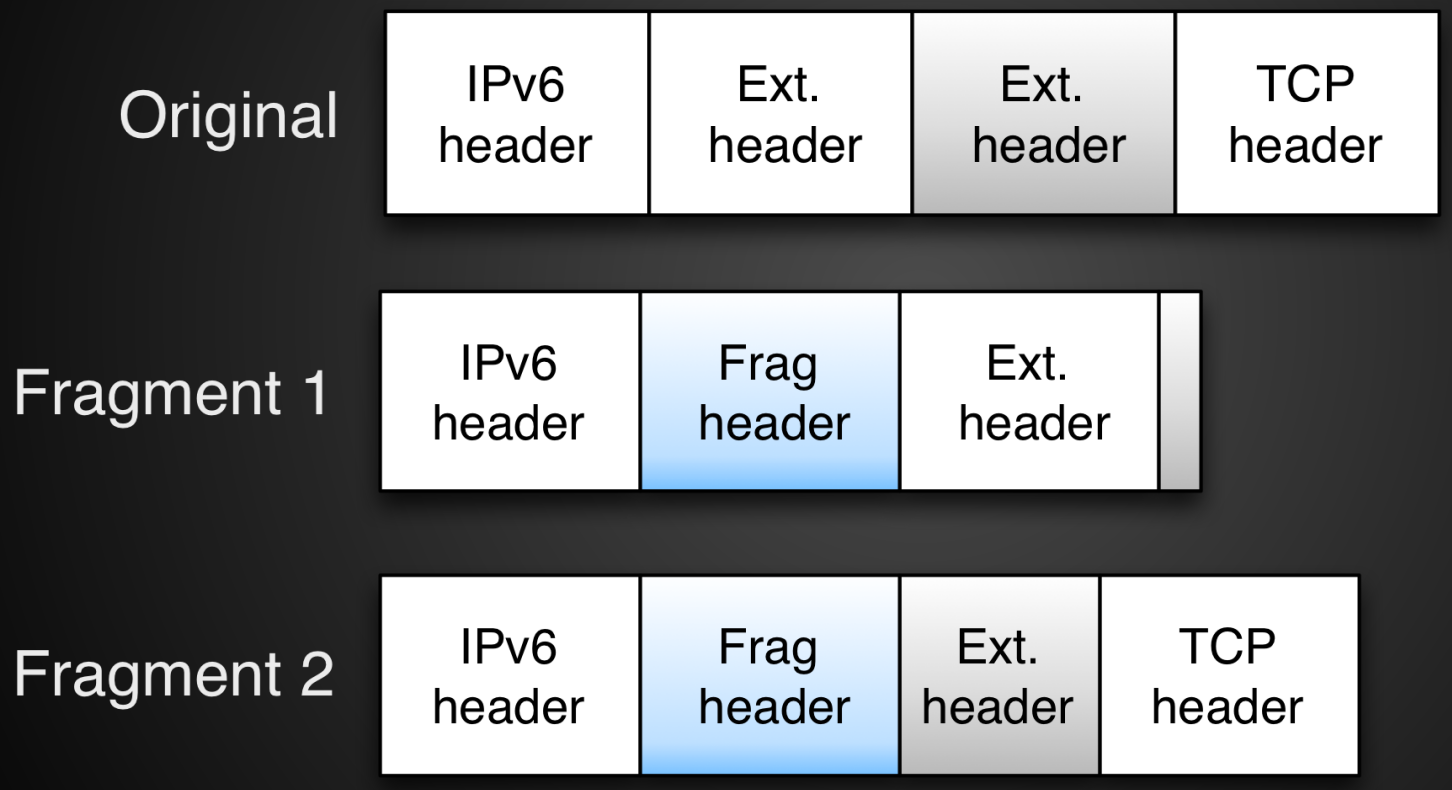

Tiny fragment attack

# Fragmentation in IPv4




Overlapping fragment attack

# Fragmentation in IPv6



# RA flooding

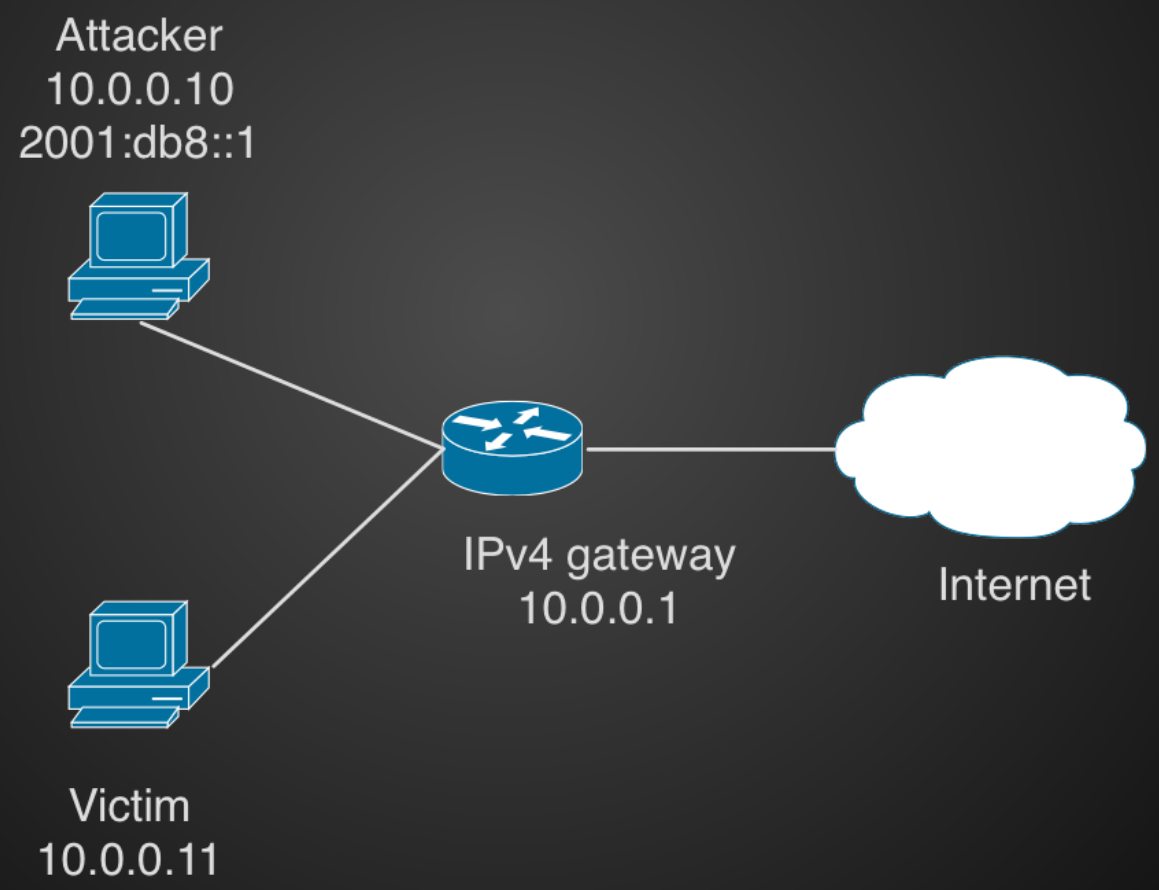
I did not have enough time to finish this, and since all of you are using linux (the one OS that doesn't halt/slow down on RA floods) this slide is here so we can have a short discussion about how vendors are not acknowledging ipv6 issues.

RA flooding effectively halts windows 8, windows server 2008, and slows down OSX.

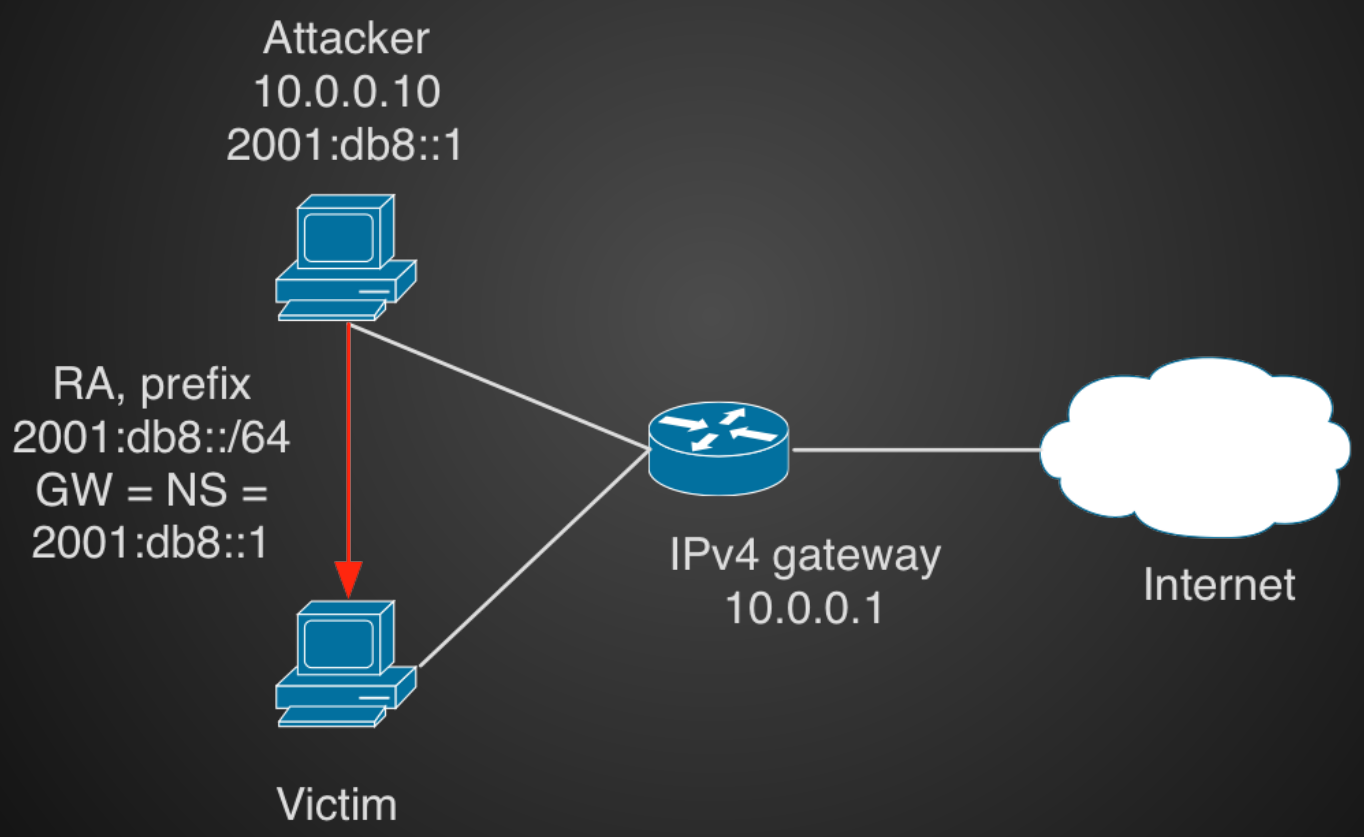
# SLAAC attack

- Example of dual-stack badness
- Doesn't require IPv6 network!
- Create IPv6 layover network
- Most OSs choose IPv6 by default
- Offer connectivity
- MitM away!

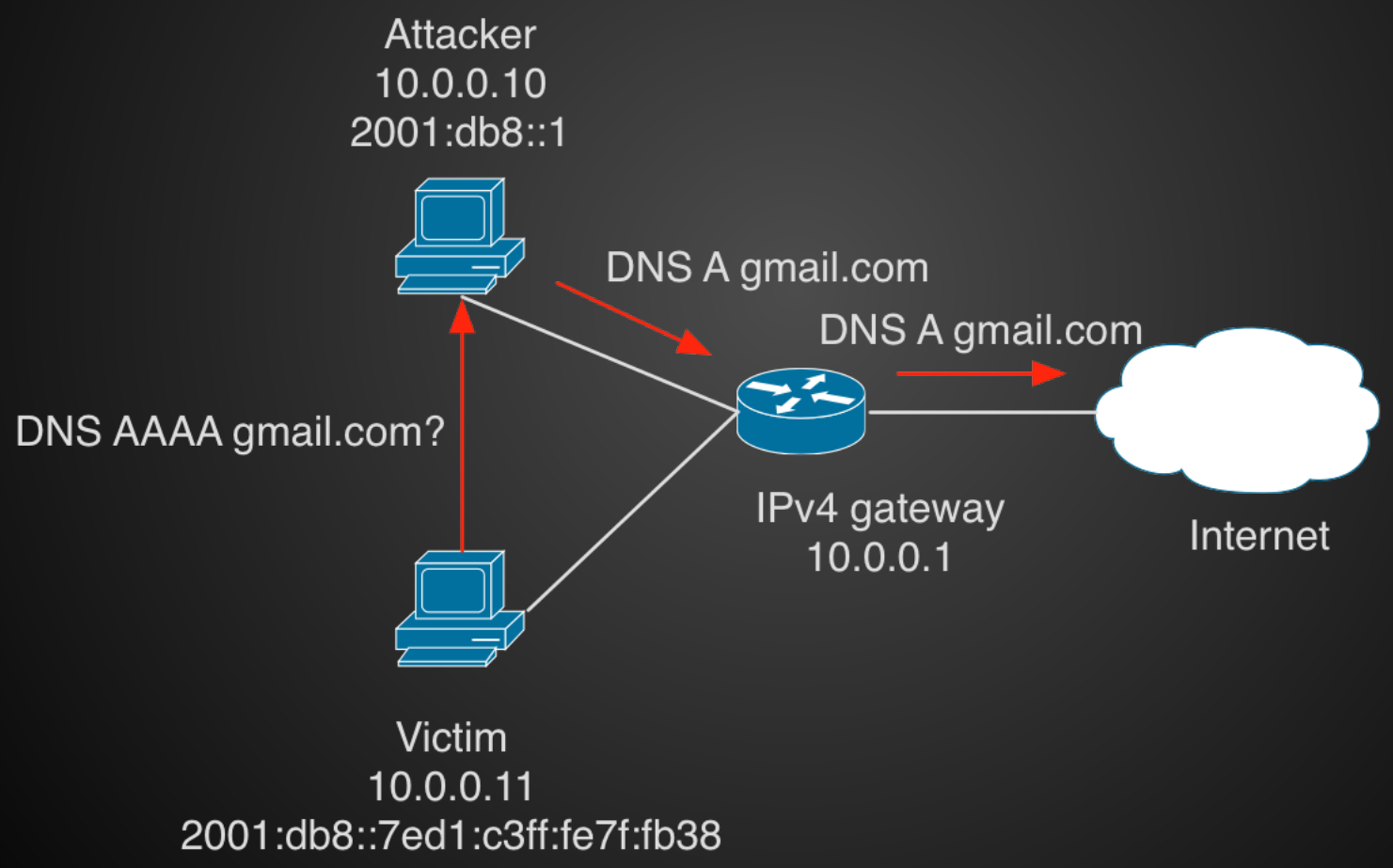
# SLAAC attack



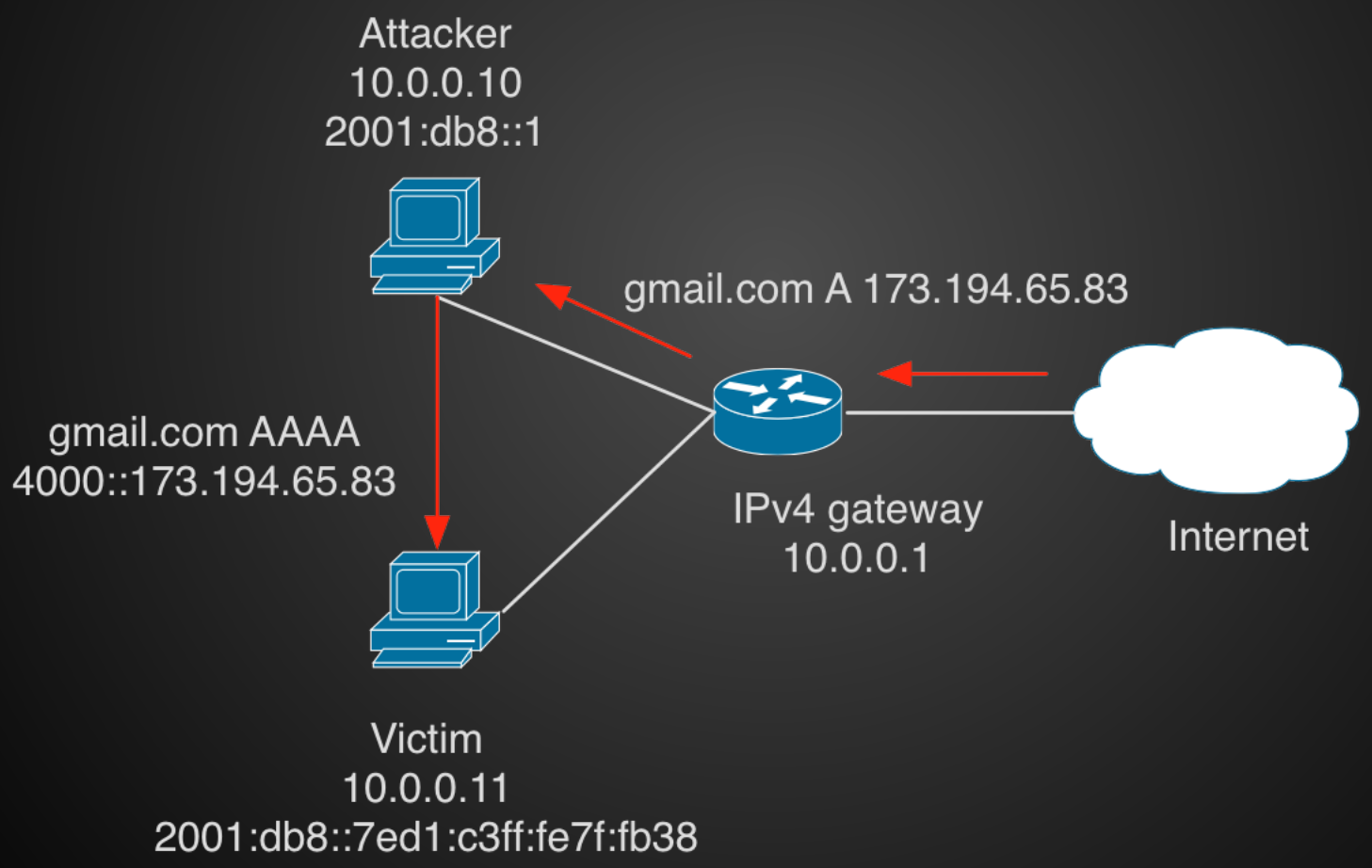
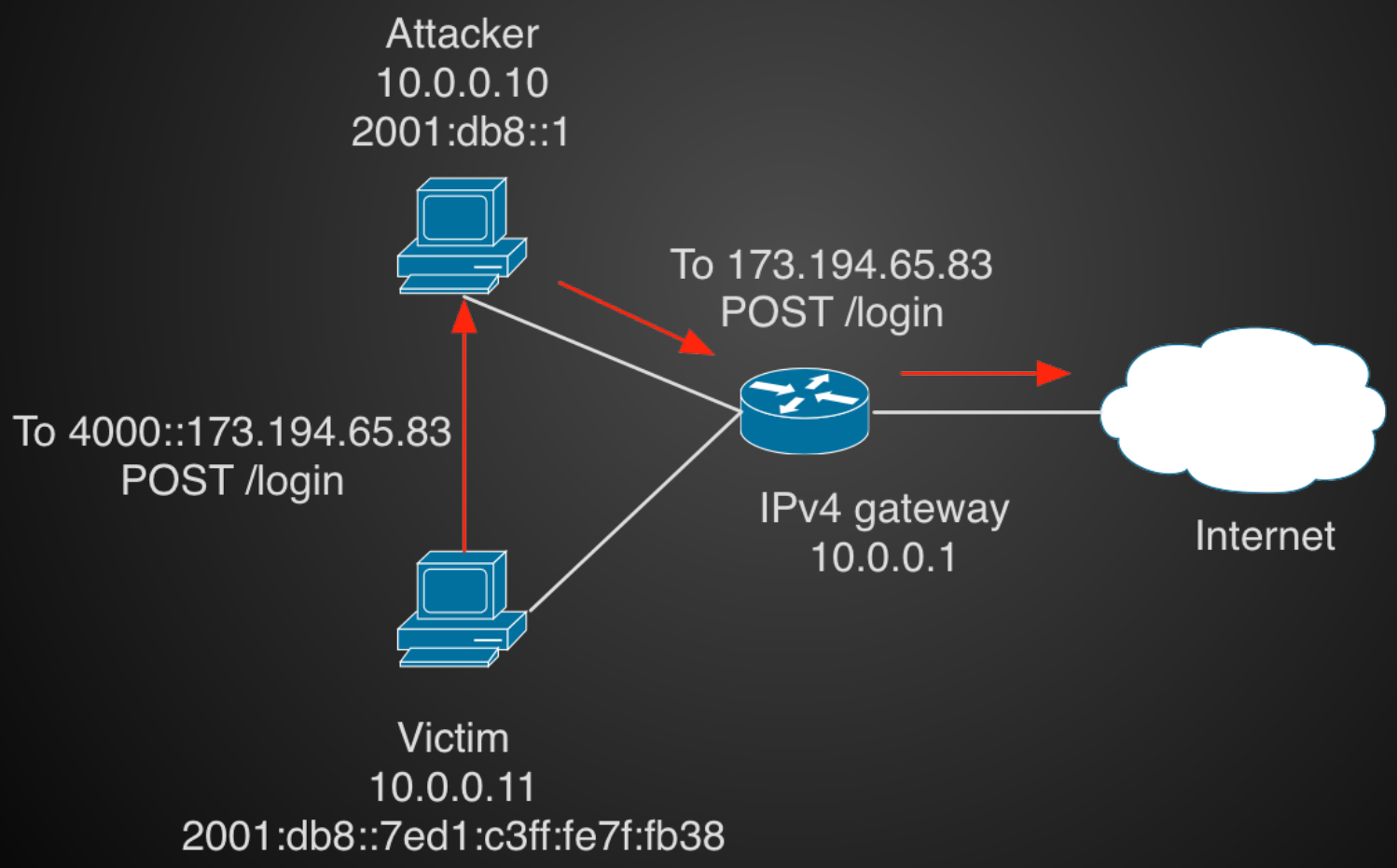
# SLAAC attack



# SLAAC attack



# SLAAC attack



# SLAAC attack