IPv6 Fragmentation and IPv6 Extension Headers in the Real World

Fernando Gont

SI6 NETWORKS

IPv6 Kongress 2014
Frankfurt, Germany. May 22-23, 2014

About...

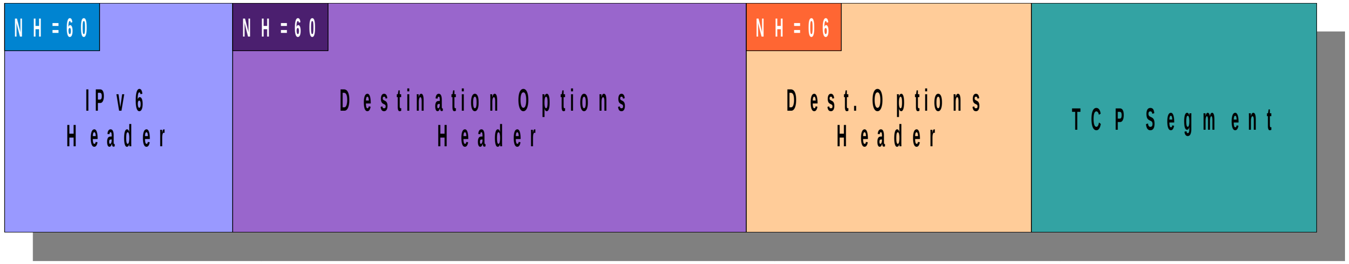
- Currently working as a security researcher for SI6 Networks
- Developer of the SI6 Networks' IPv6 Toolkit
- Active participant at the Internet Engineering Task Force (IETF)
- List administrator of the IPv6 Hackers mailing-list
- More information at:
    - http://www.gont.com.ar
    - http://www.si6networks.com

Some background

(yes... it's inevitably boring :-))

IPv6 Extension Headers

- Fixed-length base header
- Options conveyed in different types of Extension Headers
- Extension Headers organized as a daisy-chain structure



NH=60

IPv6
Header

NH=60

Destination Options
Header

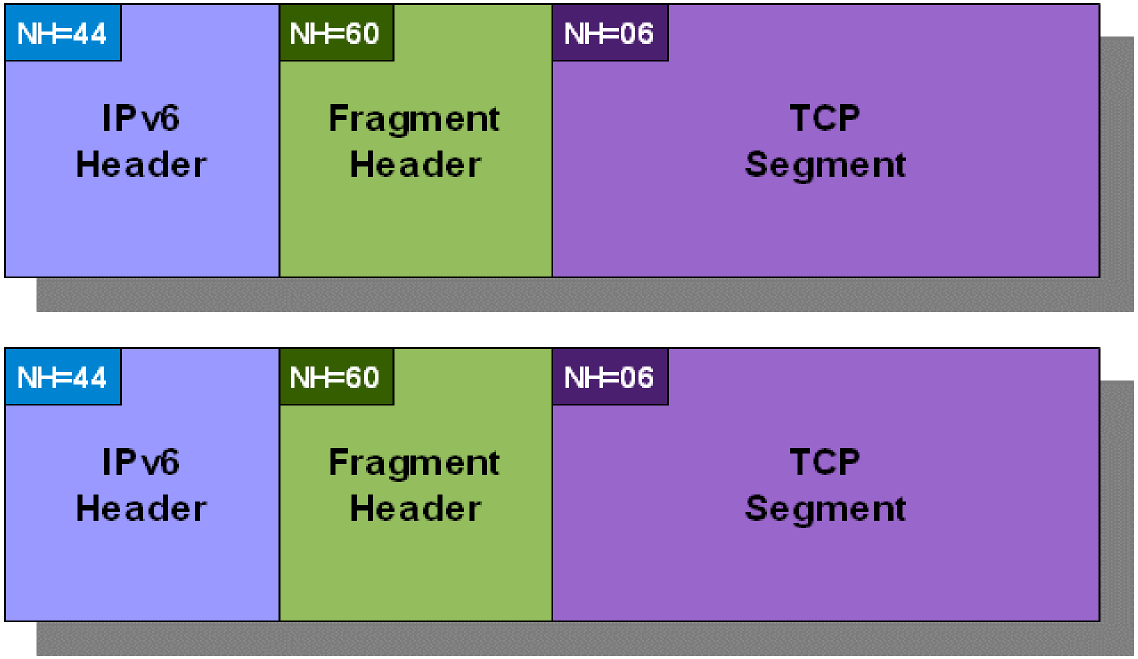
NH=06

Dest. Options
Header

TCP Segment

IPv6 Fragmentation

- Conceptually, same as in IPv4
- Implemented with an IPv6 Fragmentation Header



IPv6 Headers

Theory

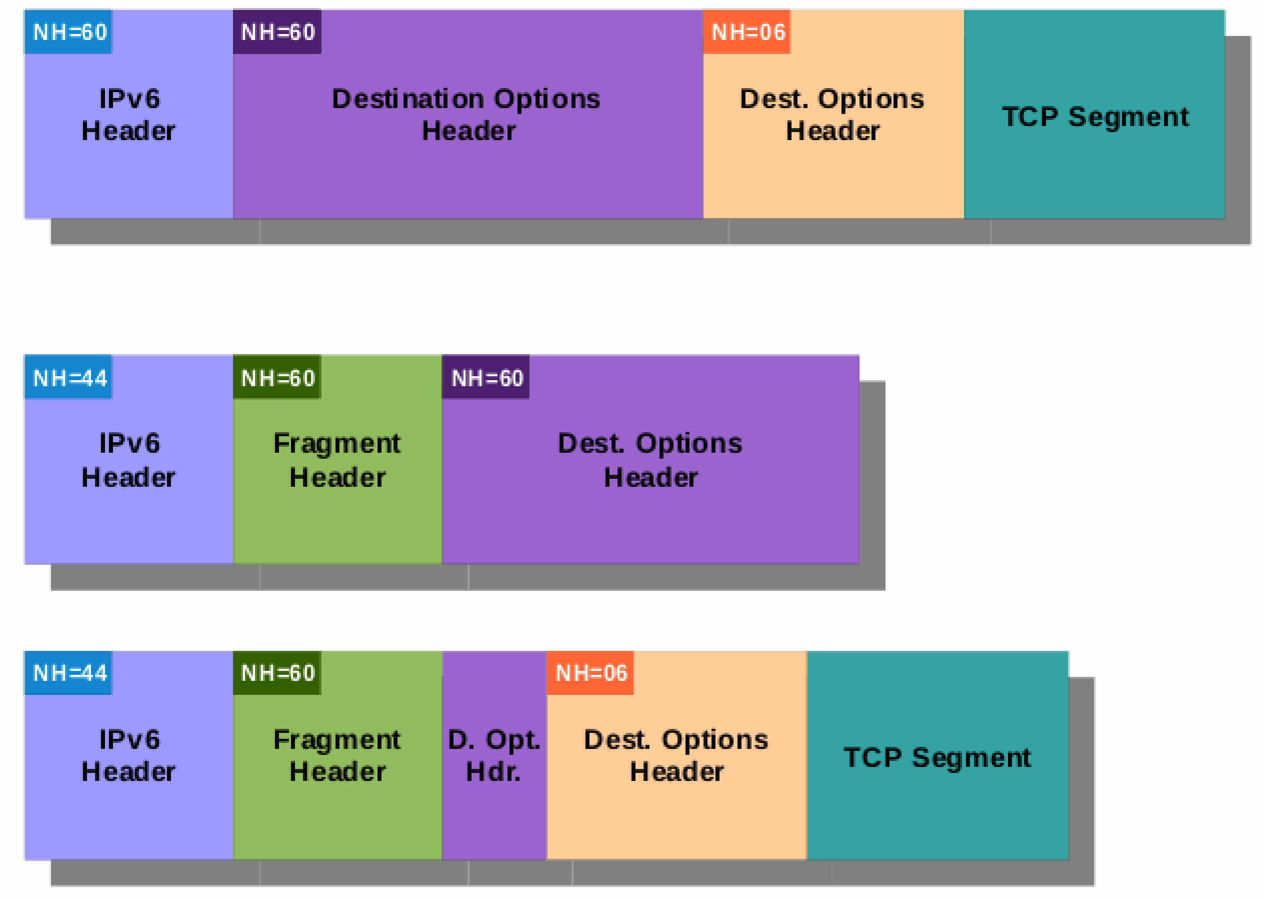
In Theory

- They allow for an arbitrary number of options
- IPv6 routers only need to parse options meant for them
- For non-HbB options, the network should be transparent

Issues with IPv6 Extension Headers and IPv6 Fragmentation

Finding Upper-layer information

- Finding upper-layer information is painful (if at all possible)



Processing the IPv6 header chain

- Processing the IPv6 header chain is expensive
  - Processing the header chain may be CPU-intensive
  - Some implementations can inspect only up to 128 bytes (or even some smaller number)

Fragmentation deemed as 'insecure'

- DoS vector:
  - Some are afraid about stateful-ness of IPv6 fragments
- Evasion:
  - It becomes harder (if at all possible) to implement ACLs
- Buggy implementations:
  - e.g. some boxes crash when a malformed fragment traverses it

Problems Found In the Real World

IPv6 Fragmentation and EH reliability

- Operators filter them, as a result of:
  - Perceived issues with IPv6 Fragmentation and EH
  - Almost no current dependence on them
- IPv6 Extension Headers result in unreliability

Previous measurements

Previous measurements

- Probes against web addresses
- Obtained some stats:
  - > 40% packet drop rates for fragmented packets
  - > 50% packet drop rates for simple EHs (Destination Options)
- Obtained some data about location of packet drops:
  - Drops from 1 hop away (from destination) to more than 10 hops away
- Some remaining questions:
  - Do packet drops occur in the same AS as the destination?

Testing Methodology

(IPv6 Kung Fu)

Probing methodology

- List of IPv6-enabled domains from WIPv6 Day site (~ 3K)
- Obtained:
  - Domain -> AAAA records (web)
  - Domain -> MX records -> AAAA records (mail)
  - Domain -> NS records -> AAAA records (DNS)
- Then discarded invalid addresses:
  - non-global addresses
  - non-unicast addresses

Probing methodology (II)

- Tools: SI6 Networks' IPv6 Toolkit
    - http:///www.si6networks.com/tools
- addr6 for address filtering
- path6 for EH-enabled traceroute
- Custom Perl scripts

Probing methodology (III)

1) Run “normal” path6 to target (D), and save route (ROUTE)
2) Check that last “hop” in route is D
3) Run EH-enabled path6, and find last responding address (L)
4) Find “L” in “ROUTE” -> dropping system (X) is next in ROUTE
5) Compare AS(X) with AS(D), and produce other stats

Real World Data

(Brand-new data)

Web addresses: Dst. Opt Header 256B

- Probe packets include Dst. Opt. Hdr of 256 bytes
- Alexa's Top 500:
  - Packet drop rate: 96.07%
  - 77.55% of packet drops by different Autonomous System
- WIPv6 Day:
  - Packet drop rate: 77.44%
  - 83.18% of packet drops by different Autonomous System

Mail addresses: Dst. Opt Header 256B

- Probe packets include Dst. Opt. Hdr of 256 bytes
- Alexa's Top 500:
  - Packet drop rate: 91.42%
  - 96.87% of packet drops by different Autonomous System
- WIPv6 Day:
  - Packet drop rate: 73.16%
  - 86.85% of packet drops by different Autonomous System

DNS addresses: Dst. Opt Header 256B

- Probe packets include Dst. Opt. Hdr of 256 bytes
- Alexa's Top 500:
  - Packet drop rate: 82.53%
  - 94.16% of packet drops by different Autonomous System
- WIPv6 Day:
  - Packet drop rate: 81.15%
  - 87.03% of packet drops by different Autonomous System

Web addresses: Fragmented payload

- 500B probe packets sent as 256B fragments
- Alexa's Top 500:
  - Packet drop rate: 0%
- WIPv6 Day:
  - Packet drop rate: ~0%
  - 0% of packet drops by different Autonomous System

Mail addresses: Fragmented Payload

- 500B probe packets sent as 256B fragments
- Alexa's Top 500:
  - Packet drop rate: 0%
- WIPv6 Day:
  - Packet drop rate: ~0%
  - 0% of packet drops by different Autonomous System

DNS addresses: Fragmented Payload

- 500B probe packets sent as 256B fragments
- Alexa's Top 500:
  - Packet drop rate: 0%
- WIPv6 Day:
  - Packet drop rate: 0%

Future work

Future work

- Test more IPv6 Extension Headers
  - Hop by Hop Options
  - IPsec
- Test return traffic (servers -> clients)

Some conclusions

Some conclusions

- Think twice before employing IPv6 EHs, then don't
- Support for IPv6 fragmentation seems to have improved (!?)

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

www.si6networks.com