



DDoS Challenges In IPv6 environment



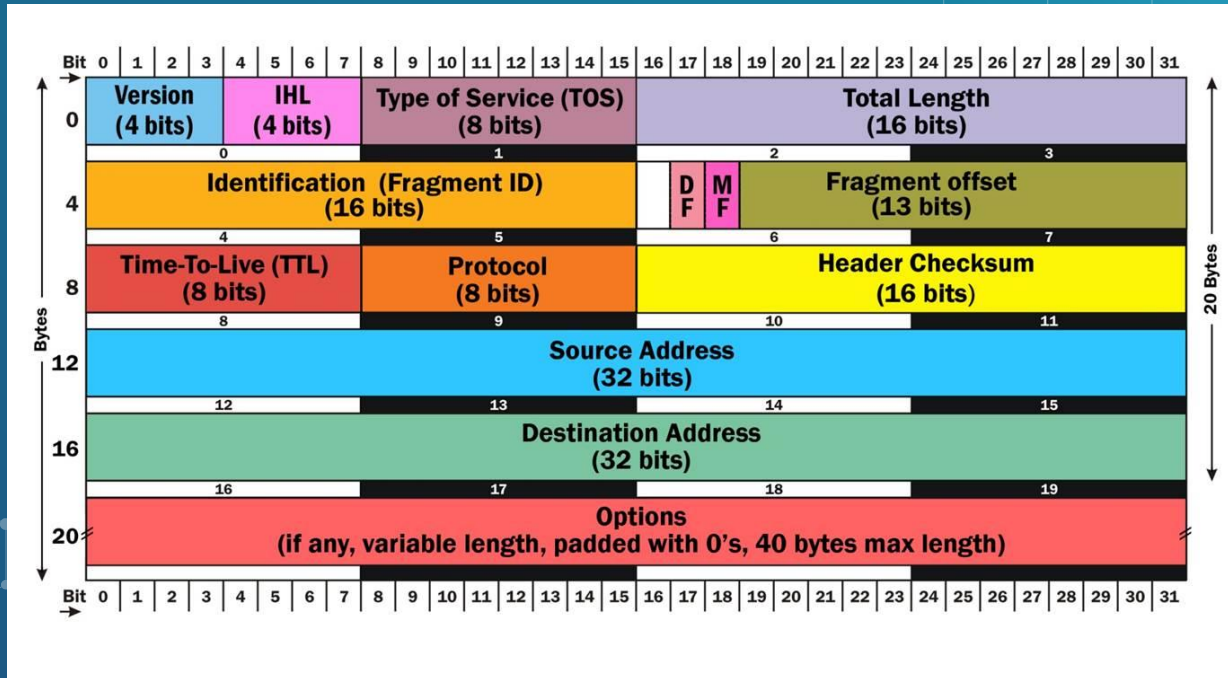
Hello

I'm Pavel Odintsov, the author of open source DDoS detection tool,
FastNetMon: <https://github.com/pavel-odintsov/fastnetmon>

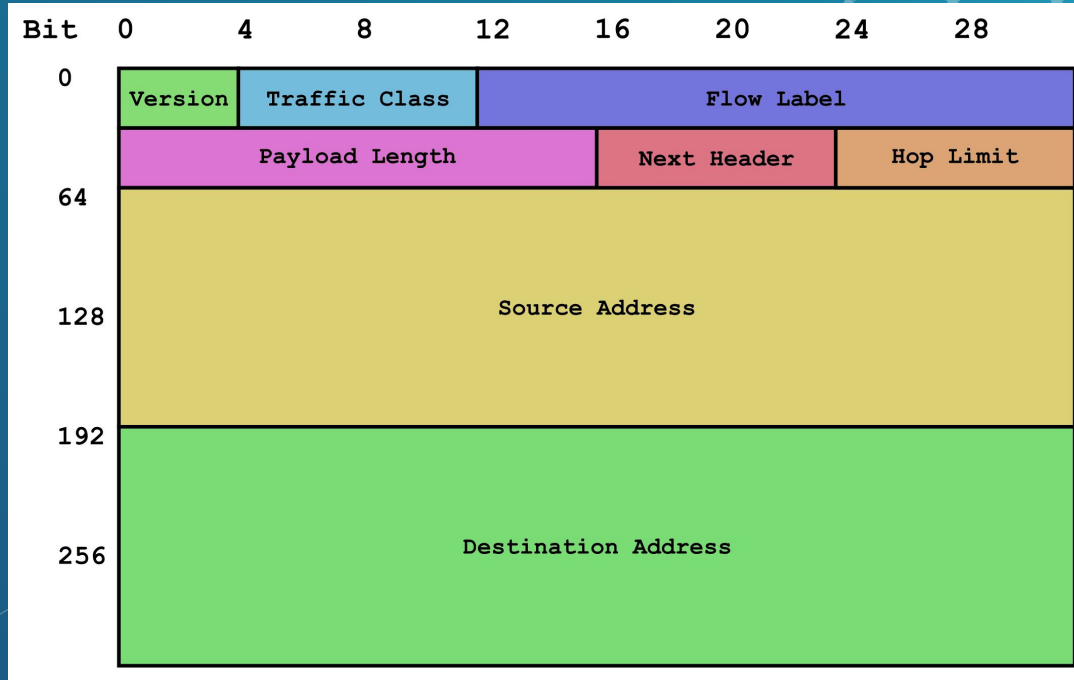
Ways to contact me:

- [linkedin.com/in/podintsov](https://www.linkedin.com/in/podintsov)
- github.com/pavel-odintsov
- twitter.com/odintsov_pavel
- IRC, FreeNode, [pavel_odintsov](#)
- pavel.odintsov@gmail.com

What kind of DDoS? L3. IPv4?



What kind of DDoS? L3. IPv6?



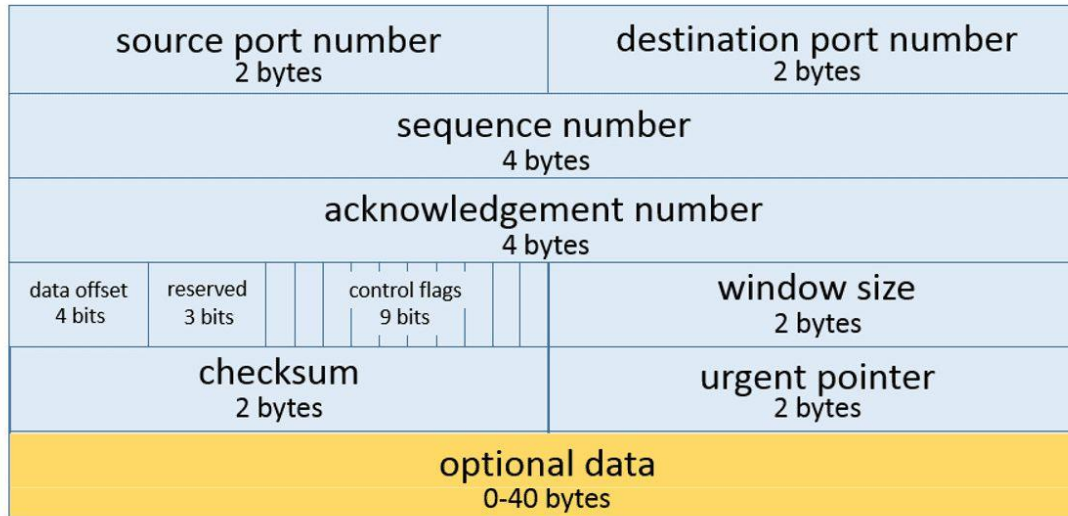
What kind of DDoS? L3

- Protocol flood (UDP, ICMP, GRE, TCP). Just keep the protocol field static.
- Fragmentation attack (just set fragment flags: DF, MF and Fragment Offset).
- Spoofing attack type (just randomize source IP)
- Options flood (just add more options)
- Empty packet flood (set length to 0)
- TTL expiration attack (very low or even zero TTL)
- ToS flood, just set random values here

What kind of DDoS? L4. TCP?

Transmission Control Protocol (TCP) Header

20-60 bytes





What kind of DDoS? L4

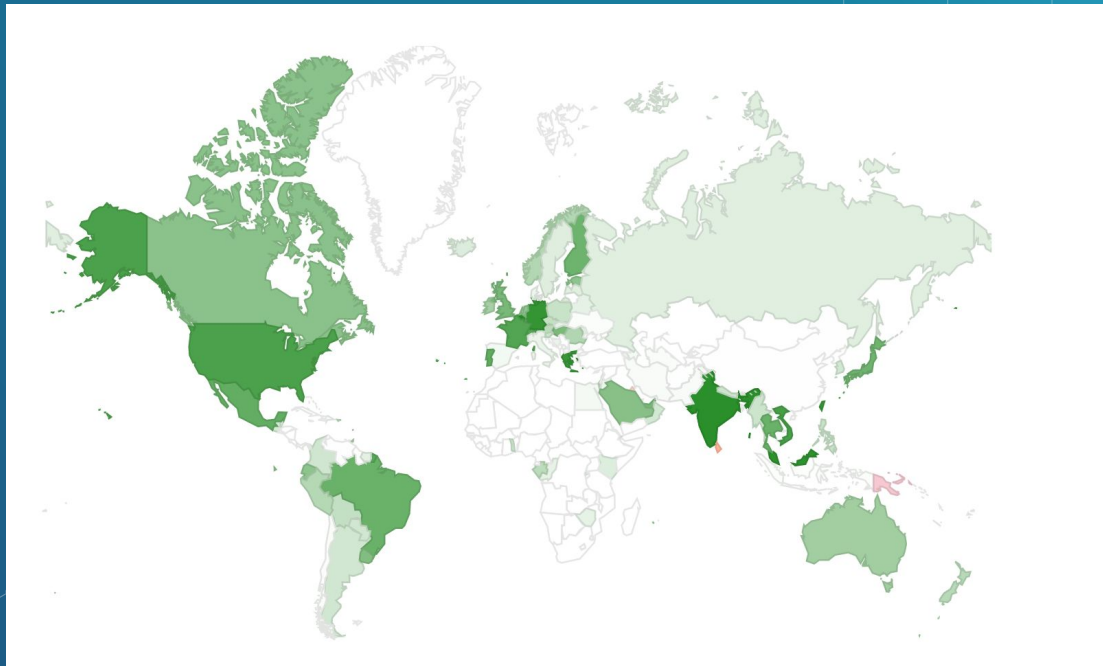
- Source port flood (including zero port)
- Destination port flood (including zero port)
- TCP Sequence flood
- TCP Ack field flood
- TCP Flag flood (TCP, ACK)
- TCP Window size flood (including 0)



What kind of DDoS? L3 and L4

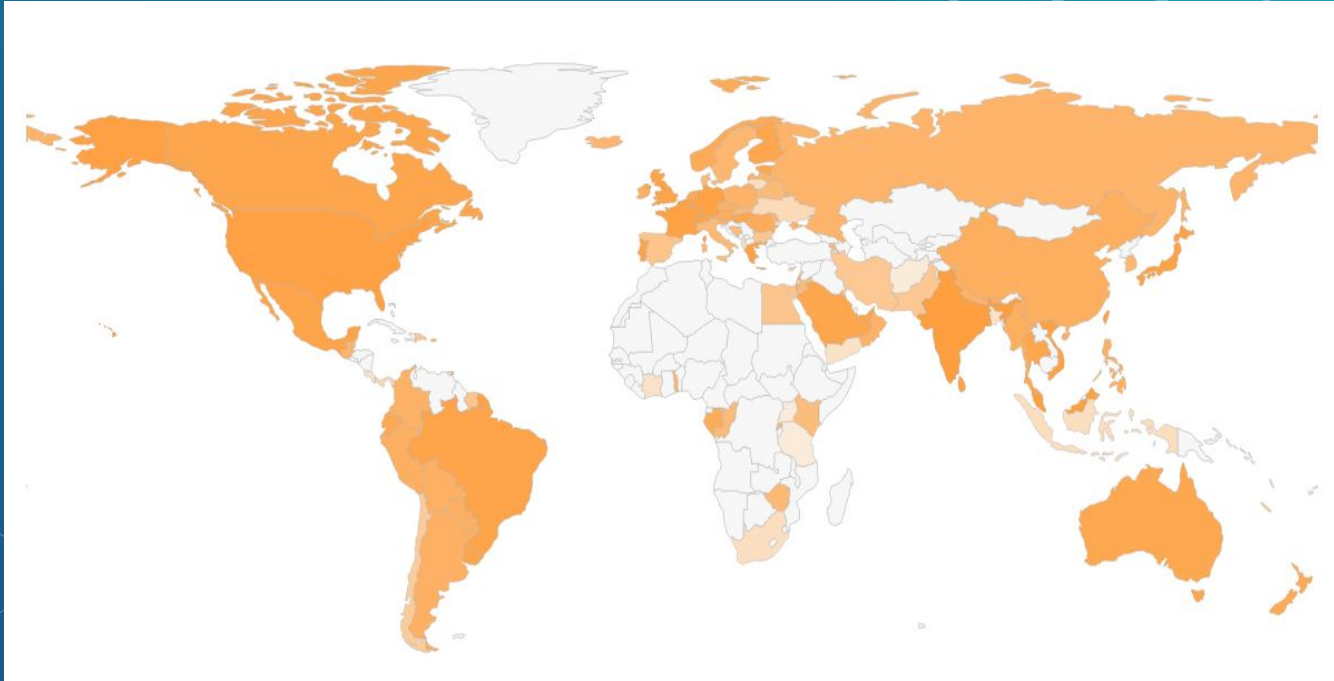
- TCP flag flood (i.e. SYN, ACK flood)
- UDP flood
- GRE flood
- UDP amplification (DNS, NTP, SSDP, SNMP)
- Fragmentation attack
- Spoofed source attacks

DDoS Over IPv6? Is it a thing? Google?



Data from <https://www.google.com/intl/en/ipv6/statistics.html>

DDoS Over IPv6? Is it a thing? Akamai?



Data from <https://www.akamai.com/uk/en/resources/our-thinking/state-of-the-internet-report>

DDoS Over IPv6? Is it a thing? China!





DDoS challenges

- ◇ Telemetry about IPv6
- ◇ BGP for IPv6
- ◇ Blackhole RFC 7999 for IPv6
- ◇ Traffic engineering for IPv6

The background of the slide is a solid blue color with a subtle, repeating pattern of light blue hexagons. Some hexagons are filled with a lighter shade, while others are just outlines. In the top left corner, there is a small, solid blue hexagon.

What's wrong with telemetry?

- ◇ Netflow v5, no fields for IPv6 addresses
- ◇ No ways to send Netflow, IPFIX, sFlow v5 to IPv6 only collector

Telemetry for IPv6

◆ Netflow v9, IPFIX, sFlow v5

```
case NF9_IPV6_SRC_ADDR:
    // It should be 16 bytes only
    if (record_length == 16) {
        memcpy(&packet.src_ipv6, data, record_length);
        // Set protocol version to IPv6
        packet.ip_protocol_version = 6;
    }

    break;
case NF9_IPV6_DST_ADDR:
    // It should be 16 bytes only
    if (record_length == 16) {
        memcpy(&packet.dst_ipv6, data, record_length);
        // Set protocol version to IPv6
        packet.ip_protocol_version = 6;
    }

    break;
```

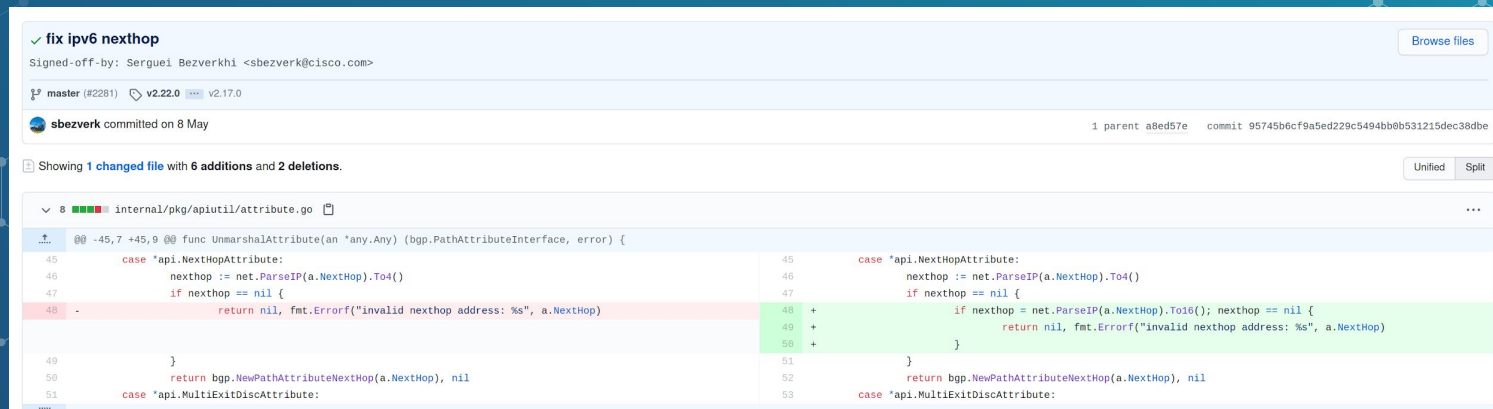
```
case NF10_IPV6_SRC_ADDR:
    // It should be 16 bytes only
    if (record_length == 16) {
        memcpy(&packet.src_ipv6, data, record_length);
        // Set protocol version to IPv6
        packet.ip_protocol_version = 6;
    }

    break;
case NF10_IPV6_DST_ADDR:
    // It should be 16 bytes only
    if (record_length == 16) {
        memcpy(&packet.dst_ipv6, data, record_length);
        // Set protocol version to IPv6
        packet.ip_protocol_version = 6;
    }

    break;
```

Issues with BGP for IPv6

- ❖ MPReach instead of old good NLRI for IPv4
- ❖ BGP Daemon implementation



The screenshot shows a GitHub pull request interface. At the top, the title is 'fix ipv6 nexthop' with a green checkmark icon. Below the title, it says 'Signed-off-by: Serguei Bezverkhii <sbezverk@cisco.com>'. There are two tabs: 'master (#2281)' and 'v2.22.0' (selected). The commit message is 'sbezverk committed on 8 May'. On the right, it shows '1 parent a8ed57e' and 'commit 95745b6cf9a5ed229c5494bb0b531215dec38dbe'. Below this, it says 'Showing 1 changed file with 6 additions and 2 deletions.' and has 'Unified' and 'Split' buttons. The file path is 'internal/pkg/apiutil/attribute.go'. The code diff shows changes to the 'UnmarshalAttribute' function. Line 48 is highlighted in red, indicating a deletion. Lines 48-50 are highlighted in green, indicating additions. The diff shows that the original code (line 48) returned nil and an error for an invalid nexthop address. The new code (lines 48-50) adds a check for IPv6 addresses using 'net.ParseIP(a.NextHop).To16()' and returns nil and an error if the address is not a valid IPv6 address.

```
45 case "api.NextHopAttribute":
46     nexthop := net.ParseIP(a.NextHop).To4()
47     if nexthop == nil {
48 -         return nil, fmt.Errorf("invalid nexthop address: %s", a.NextHop)
49     }
50     return bgp.NewPathAttributeNextHop(a.NextHop), nil
51 case "api.MultiExitDiscAttribute":
52
53     case "api.NextHopAttribute":
54         nexthop := net.ParseIP(a.NextHop).To4()
55         if nexthop == nil {
56 +             if nexthop = net.ParseIP(a.NextHop).To16(); nexthop == nil {
57 +                 return nil, fmt.Errorf("invalid nexthop address: %s", a.NextHop)
58 +             }
59         }
60         return bgp.NewPathAttributeNextHop(a.NextHop), nil
61 case "api.MultiExitDiscAttribute":
```

BGP for IPv6

✓ Added stub conf options for IPv6 BGP implementation

master v1.1.9

pavel-odintsov committed 2 days ago

Showing 1 changed file with 11 additions and 0 deletions.

11 src/fastnetmon.conf

```
@@ -233,12 +233,23 @@ exabgp_flow_spec_announces = off
233 233
234 234 # GoBGP intergation
235 235 gobgp = off
236 +
237 + # Configuration for IPv4 announces
238 238 gobgp_next_hop = 0.0.0.0
239 239 gobgp_announce_host = on
240 240 gobgp_announce_whole_subnet = off
241 +
242 242 gobgp_community_host = 65001:666
243 243 gobgp_community_subnet = 65001:777
244 244
245 + # Configuration for IPv6 announces
246 + gobgp_next_hop_ipv6 = 100::1
247 + gobgp_announce_host_ipv6 = off
248 + gobgp_announce_whole_subnet_ipv6 = off
249 +
250 + gobgp_community_host_ipv6 = 65001:666
251 + gobgp_community_subnet_ipv6 = 65001:777
252 +
```

The background of the slide features a repeating pattern of hexagons. Some hexagons are solid blue, while others are white outlines. The pattern is more dense in the top right and bottom left corners, fading towards the center.

What is the issue with BGP RTBH?

- ◇ Only /128 support
- ◇ No support
- ◇ Non RFC community number, please use RFC7999

The background of the slide features a dark blue gradient with a subtle, repeating pattern of light blue hexagons and connecting lines, resembling a molecular or network structure. A small, solid teal hexagon is positioned to the left of the main title.

What about traffic engineering / diversion?

- ◇ Diversion can be implemented on customer basis
- ◇ Ability to localise customer for RTBH purposes
- ◇ Anycast is affordable



Automate it!

FastNetMon Community 1.1.8 and 1.1.9

- ◇ Complete IPv6 support for mirror, Netflow and IPFIX modes
- ◇ Added logic to ban / unban IPv6 hosts manually via API and `fastnetmon_api_client`
- ◇ Added logic to announce / withdraw announces about IPv6 hosts

Screenshot

FastNetMon 1.1.8 master git-c6a1c98582b9409c552a8be5f3637e1482725b7c

IPs ordered by: packets

Incoming traffic

| | | | | |
|-------|----------------|----------|----------|---------|
| | | 3124 pps | 129 mbps | |
| 2a00: | c554:abf6:d337 | 3124 pps | 129 mbps | 0 flows |

Outgoing traffic

| | | | | |
|-------|---------------|----------|--------|---------|
| | | 2218 pps | 1 mbps | |
| 2a00: | 554:abf6:d337 | 2218 pps | 1 mbps | 0 flows |

Internal traffic

0 pps 0 mbps

Other traffic

0 pps 0 mbps

Subnet load:

| | | | | | |
|-----------|--------------|--------------|-----------|--------------|--------|
| 2a00: | 97e4:520c/64 | pps in: 3124 | out: 2218 | mbps in: 129 | out: 1 |
| :0000/128 | | pps in: 0 | out: 0 | mbps in: 0 | out: 0 |

FastNetMon Community Installation

- ◇ `wget`
`https://raw.githubusercontent.com/pavel-odintsov/fastnetmon/master/src/fastnetmon_install.pl`
`-Ofastnetmon_install.pl`
- ◇ `sudo perl fastnetmon_install.pl`

THANKS!

ANY QUESTIONS?

You can find me at:

- ◇ @odintsov_pavel
- ◇ pavel.odintsov@gmail.com
- ◇ linkedin.com/in/podintsov

