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
- github.com/pavel-odintsov
- twitter.com/odintsov_pavel
- IRC, FreeNode, pavel_odintsov
- pavel.odintsov@gmail.com

What kind of DDoS? L3. IPv4?

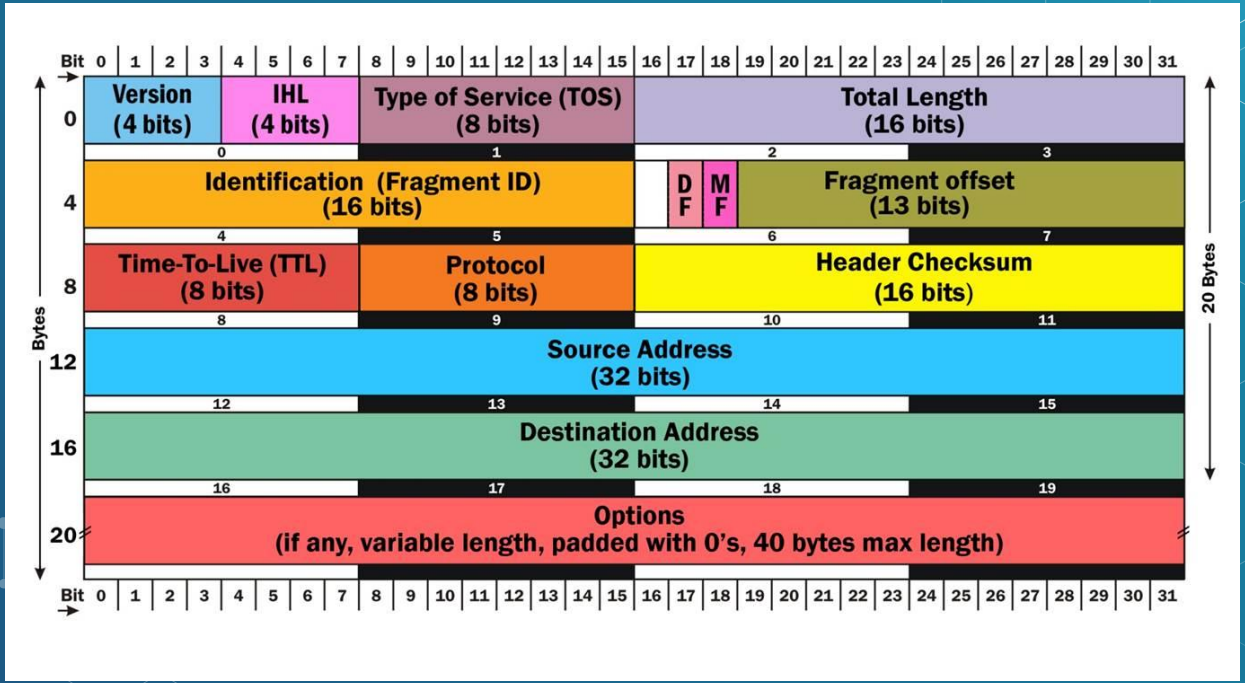


Image from https://thirdinternet.com/ip-packet-syntax/

What kind of DDoS? L3. IPv6?

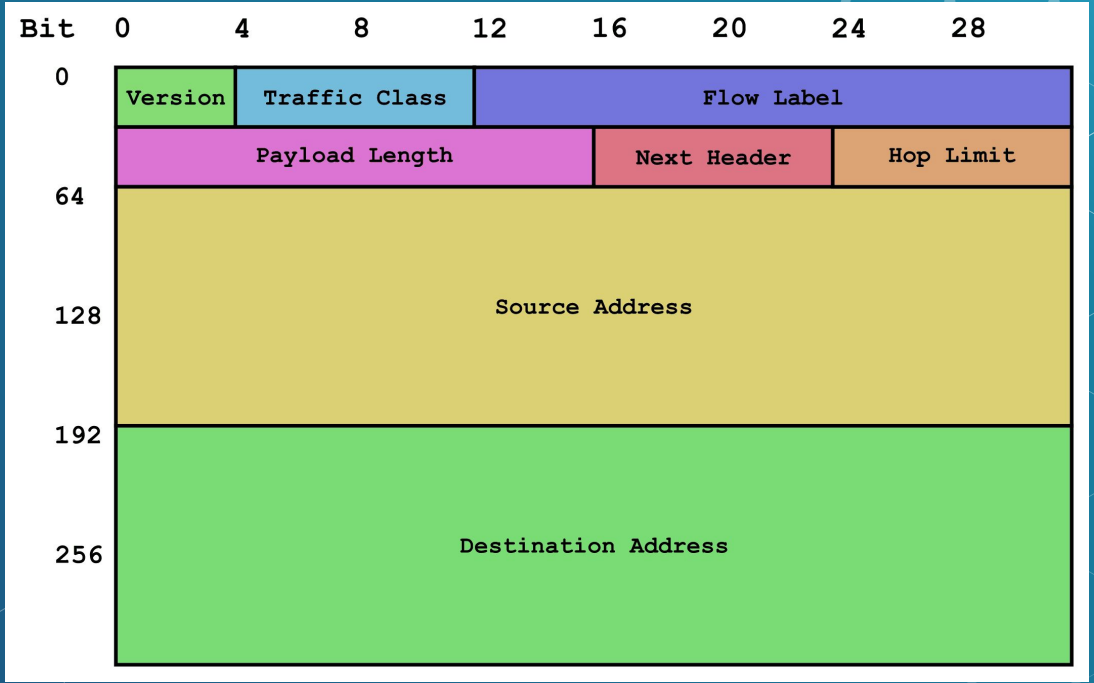


Image from https://networkel.com/ipv6-overview-communication-types/

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?

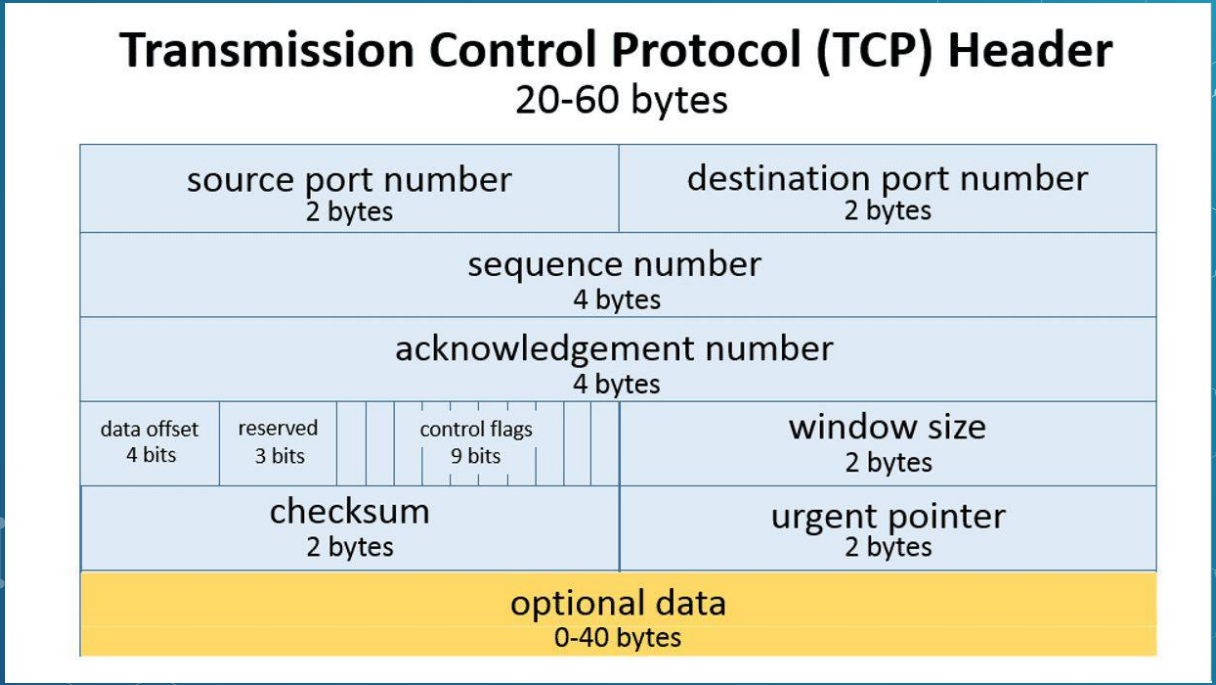


Image from https://www.lifewire.com/tcp-headers-and-udp-headers-explained-817970

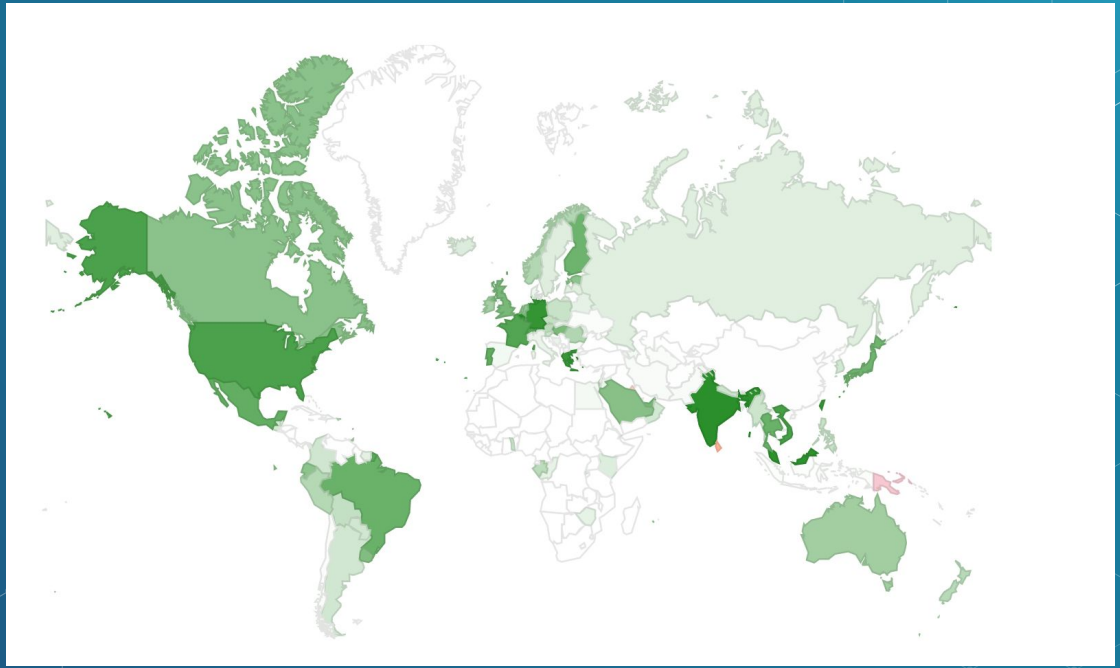
What kind of DDoS? L4

- 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

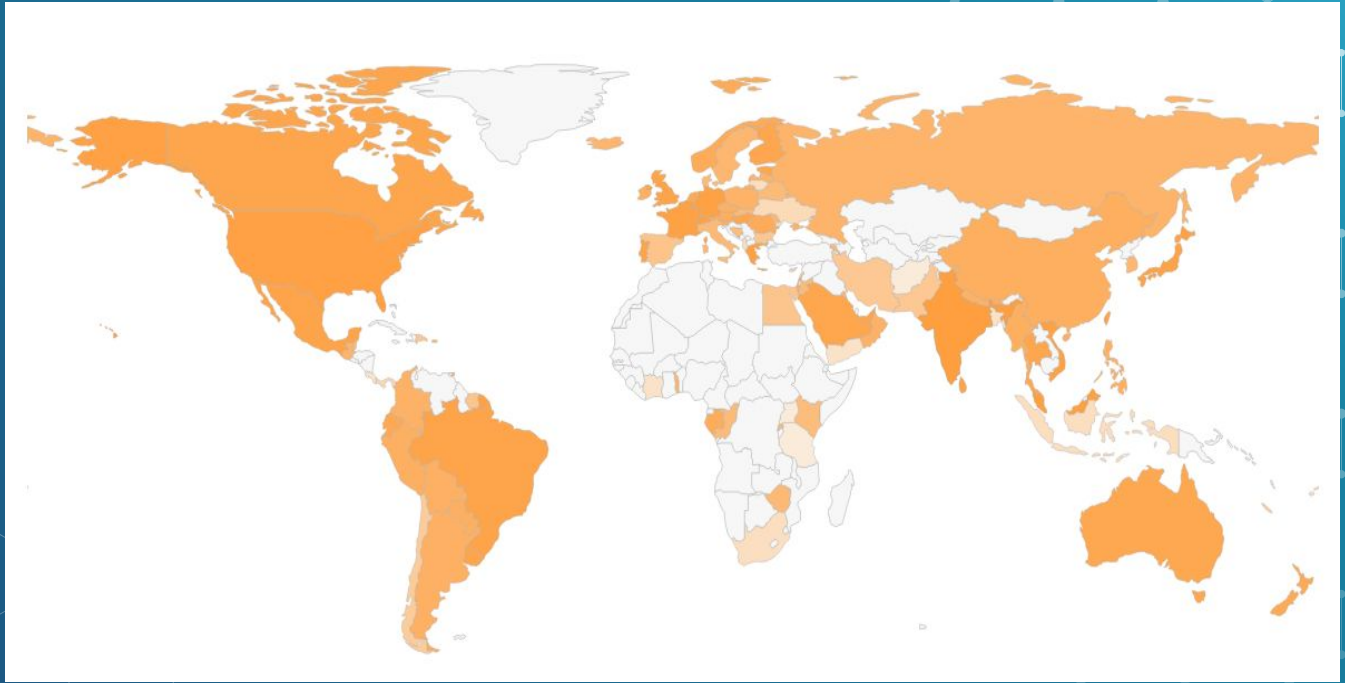
- TCP flag flood (i.e. SYN, ACK flood)
- UDP flood
- GRE flood
- UDP amplification (DNS, NTP, SSDP, SNMP)
- Fragmentation attack
- Spoofed source attacks

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!

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

DDoS challenges

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

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

fix ipv6 nexthop

Browse files

Signed-off-by: Serguei Bezverkhi <sbezverk@cisco.com>

master (#2281) v2.22.0 ··· v2.17.0

sbezverk committed on 8 May

1 parent a8ed57e commit 95745b6cf9a5ed229c5494bb0b531215dec38dbe

Showing **1 changed file** with **6 additions** and **2 deletions**.

Unified Split

8 internal/pkg/apiutil/attribute.go

```
@@ -45,7 +45,9 @@ func UnmarshalAttribute(an *any.Any) (bgp.PathAttributeInterface, error) {
 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)
+48                         if nexthop = net.ParseIP(a.NextHop).To16(); nexthop == nil {
+49                                 return nil, fmt.Errorf("invalid nexthop address: %s", a.NextHop)
+50                         }
 49                 }
 50                 return bgp.NewPathAttributeNextHop(a.NextHop), nil
 51         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

```diff
@@ -233,12 +233,23 @@ exabgp_flow_spec_announces = off

 # GoBGP intergation
 gobgp = off
+
+ # Configuration for IPv4 announces
 gobgp_next_hop = 0.0.0.0
 gobgp_announce_host = on
 gobgp_announce_whole_subnet = off
+
 gobgp_community_host = 65001:666
 gobgp_community_subnet = 65001:777

+ # Configuration for IPv6 announces
+ gobgp_next_hop_ipv6 = 100::1
+ gobgp_announce_host_ipv6 = off
+ gobgp_announce_whole_subnet_ipv6 = off
+
+ gobgp_community_host_ipv6 = 65001:666
+ gobgp_community_subnet_ipv6 = 65001:777
+
```

What is the issue with BGP RTBH?

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

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