IPv6 security: myths & legends

Paul Ebersman – Paul_Ebersman@cable.comcast.com

01 Sep 2015

NANOG on the Road – Chicago

COMCAST

So many new security issues with IPv6!

Or are there…

IPv6 Security issues

- Same problem, different name
- A few myths & misconceptions
- Actual new issues
- FUD (Fear Uncertainty & Doubt)

COMCAST

Round up the usual suspects!

Remember these?

- ARP cache poisoning
- P2p ping pong attacks
- Rogue DHCP

ARP cache poisoning

- Bad guy broadcasts fake ARP
- Hosts on subnet put bad entry in ARP Cache
- Result: MiM or DOS

Ping pong attack

- P2P link with subnet > /31
- Bad buy sends packet for addr in subnet but not one of two routers
- Result: Link clogs with routers sending packet back and forth

Rogue DHCP

- Client broadcasts DHCP request
- Bad guy sends DHCP offer w/his “bad” router as default GW
- Client now sends all traffic to bad GW
- Result: MiM or DOS

Look similar?

- Neighbor cache corruption
- P2p ping pong attacks
- Rogue DHCP + rogue RA

Solutions?

- Lock down local wire
- /127s for p2p links (RFC 6164)
- RA Guard (RFC 6105)

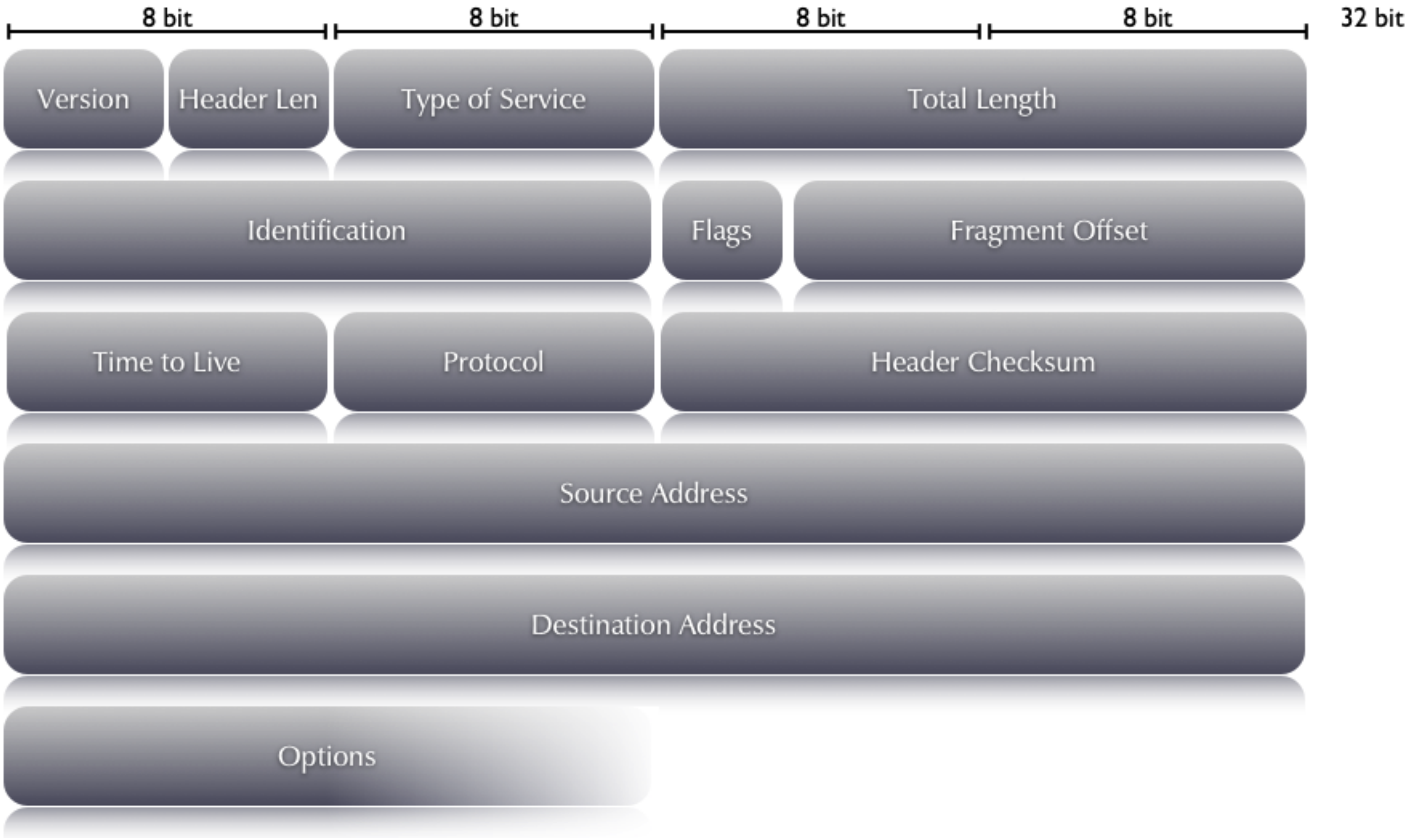
COMCAST

And now for something completely different!

So what *is* new?

- Extension header chains
- Packet/Header fragmentation
- Predictable fragment headers
- Atomic fragments

The IPv4 Packet



8 bit | 8 bit | 8 bit | 8 bit | 32 bit

Version | Header Len | Type of Service | Total Length

Identification | Flags | Fragment Offset

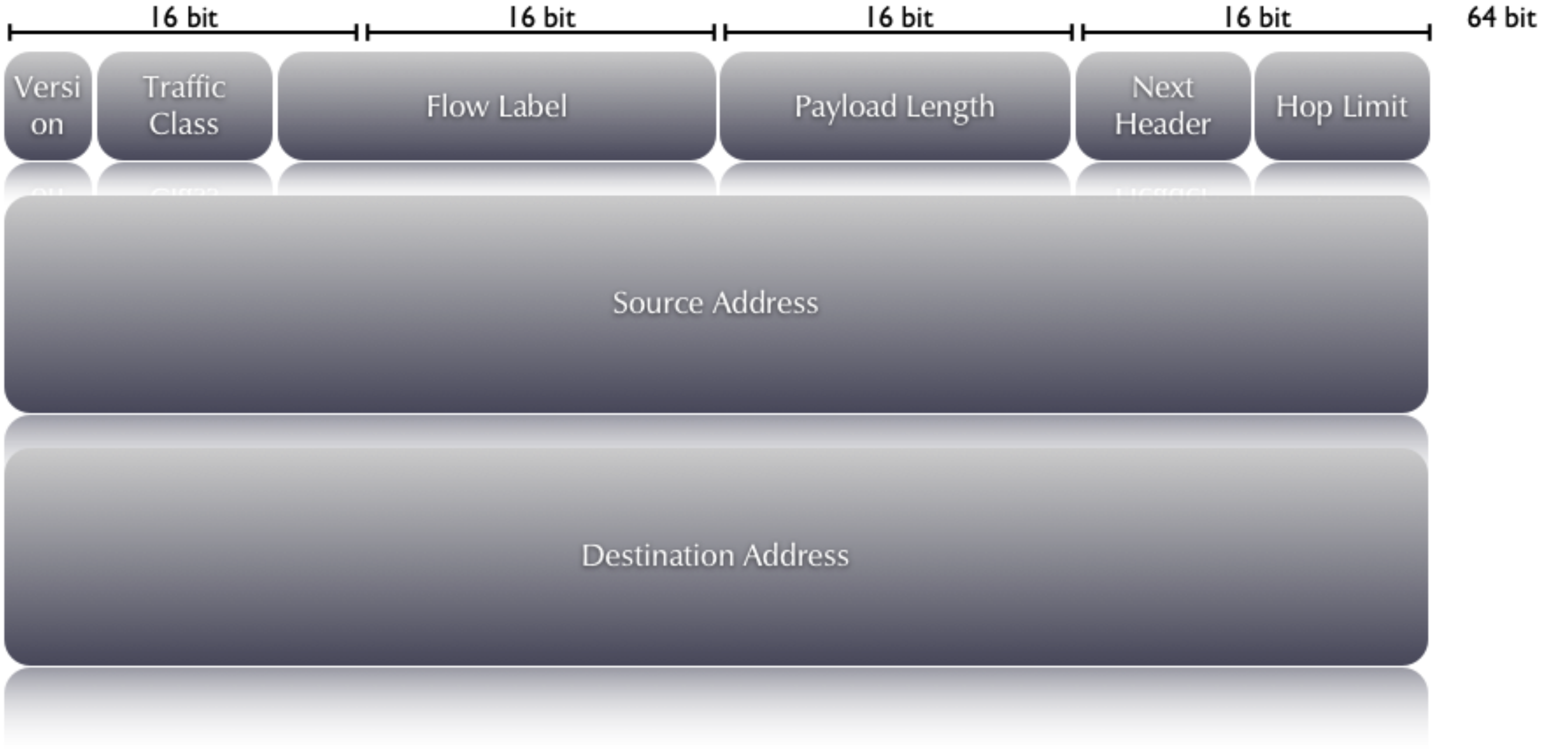
Time to Live | Protocol | Header Checksum

Source Address

Destination Address

Options

The IPv6 Packet



Fragmentation

- Minimum 1280 bytes
- Only source host can fragment
- Destination must get all fragments
- What happens if someone plays with fragments?

IPv6 Extension Header Chains

- No limit on length
- Deep packet inspection bogs down
- Confuses stateless firewalls
- Fragments a problem
- draft-ietf-6man-oversized-header-chain-09

Predictable Fragments

- Fragment Header ID field
- No requirement other than “unique”
- Some implementations predictable
- draft-gont-6man-predictable-fragment-id

Results of predicting ID

- Determine the packet rate
- Perform stealth port scans
- Uncover the rules of a number of firewalls
- Count the # of systems behind a middle-box
- Perform a Denial of Service (DoS) attack

Atomic Fragments

- Packet w/Fragment Header but not fragmented
- Usually forced by forged “Packet too big” msg
- Fragments can overlap
- Results: various fragmentation attacks possible
- See RFC 6946

Reality

- Most of these attacks are complicated
- Most attackers are lazy and will find easier vectors of attack
- But, there are toolsets out there

You're already running IPv6…

“I’m not using IPv6”

- Are you running:
  - Windows 8, Server 2012, Vista or newer
  - Windows clustering
  - Mac OSX
  - Any modern LINUX or FreeBSD

Guess again

Congratulations,
you’re running IPv6

Get used to it…

- Test now
- Train your staff
- Beat on your vendors
- Monitor it, don’t try to disable it

COMCAST

But everybody says…

IPSEC: the myth

IPSEC in IPv6 is better than IPv4 because it was designed in and mandated.

IPSEC: the reality

- RFCs said “MUST” support IPSEC (but softening to “SHOULD”…)
- Didn’t define “support”, let vendors do it
- Vendors shipped, didn’t enable
- No PKI…

IPv6 is *HUGE!*

- So big you can’t scan it…
- Unless you don’t really use it…

COMCAST

Use the space we have

- Give the whole /64 to DHCP pools
- Randomize address assignments across the whole /64
- Avoid EUI-64

COMCAST

It’s the end of the world as we know it!

IPv6 will destroy the Internet!

- Apps will break
- Firewalls won’t work
- ICMP is scary
- We don’t understand it so it must be insecure

Apps

- Yes, you will need to test and possibly rewrite all your code
- You need to reach everyone, including mobile devices
- Most bad ideas also in IPv4 code

If it was wrong in IPv4…

- Hard coding IP addresses
- Not checking inputs/sizes
- Using relative DNS labels
- No longer have source
- Not tested since Y2K

Where to read more

- RIPE presentation:
  - https://ripe66.ripe.net/presentations/134-Making_an_application_fully_IPv6_compliant_(2).pdf

Firewalls won’t work

- What do you do if your gear doesn’t meet your needs?
  - Beat on your vendors until it does…
  - But you need to know what to ask for

ICMP is scary, turn it off!

- ICMPv4 wasn’t that scary…
- ICMPv6 is much more tightly defined
- Read RFC 4890

We don’t understand it, so…

- If someone is telling you that IPv6 is evil incarnate, it’s because:
  - **They are a vendor that doesn’t support IPv6 but their competitors do**
  - **They are trying to sell you a security product**

COMCAST

Q & A

COMCAST

Thank you!