IPv6 is Internet Standard!

Fernando Gont

LACNOG 2017
Montevideo, Uruguay. September 18-22, 2017

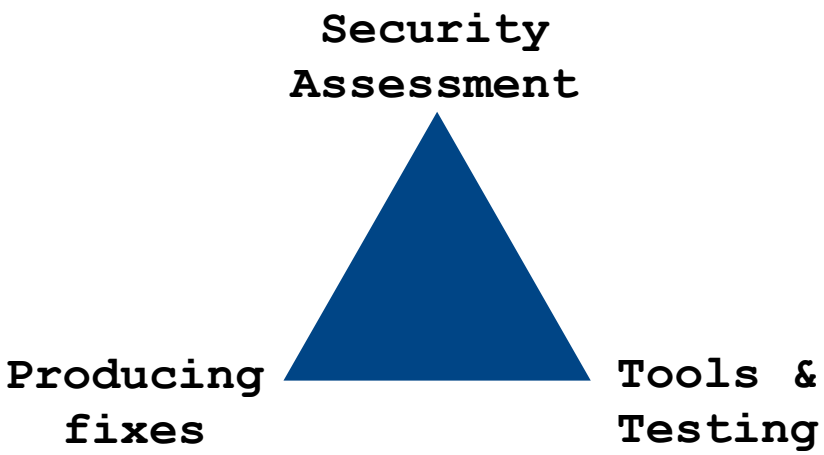
IPv6 is Internet Standard!(?)

Fernando Gont

LACNOG 2017
Montevideo, Uruguay. September 18-22, 2017

About the speaker...

- Security Researcher and Consultant at SI6 Networks
- Author/co-author of 30 IETF RFCs (15+ on IPv6)
- Author of the SI6 Networks' IPv6 toolkit
  - https://www.si6networks.com/tools/ipv6toolkit
- More information at: https://www.gont.com.ar
- Everyday work:

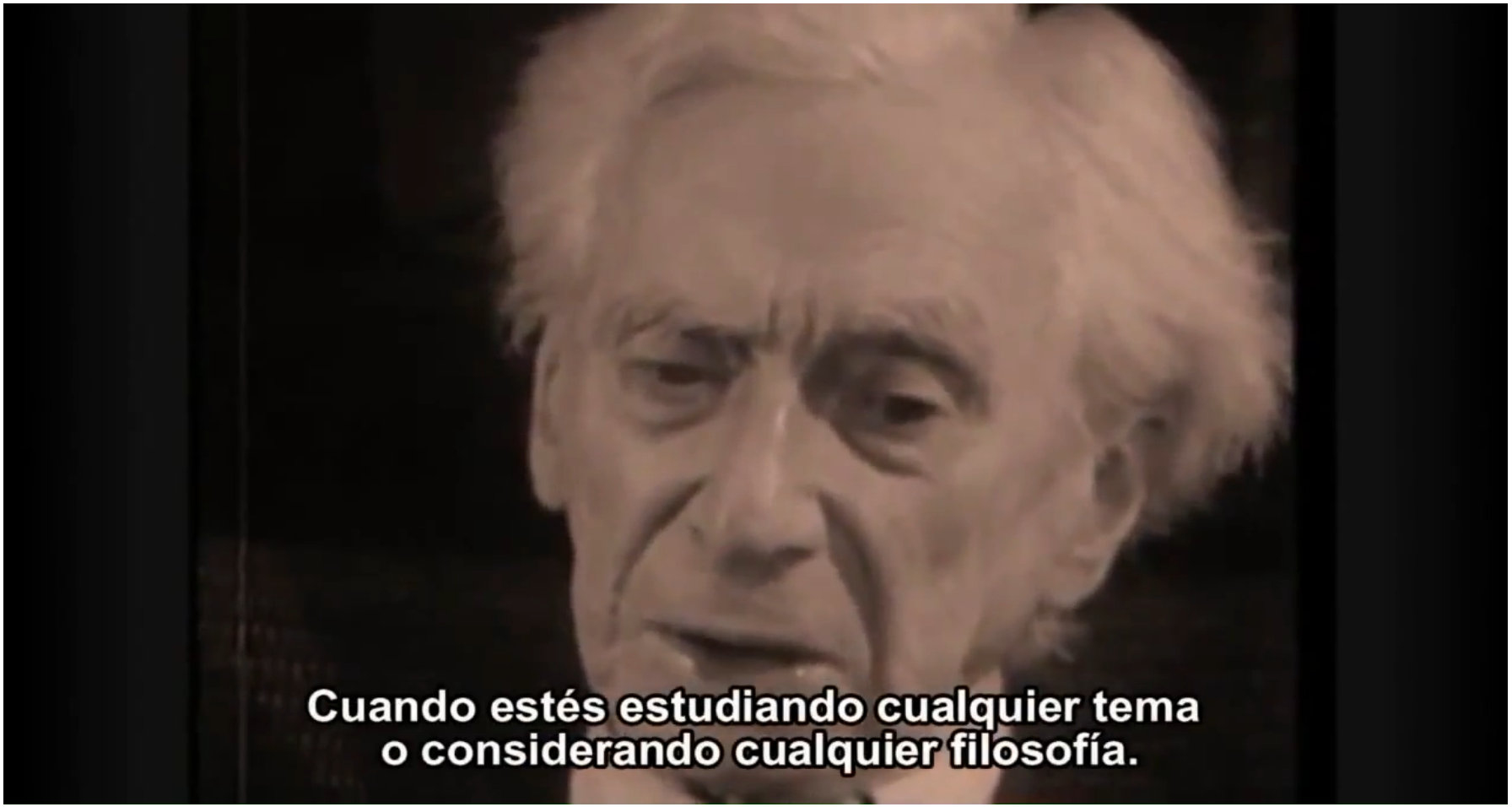


What this presentation is about

What this presentation is about

- Some IPv6-related documents have been recently elevated to “Internet Standard” maturity level
- For some, this is an indication of the level of maturity of IPv6
- To an extent, we challenge/question such belief

A message from Bertrand Russell...



IETF Standards Maturity Levels

IETF standards maturity levels

- IETF “standards track” documents have an associated maturity level (RFC2026)
  - Proposed Standard (PS)
    - Spec is stable and well-understood
  - Draft Standard (DS)
    - PS + 2 independent implementations + successful operational experience
  - Internet Standard (IS)
    - PS ++ (significant implementation an operational experience)

What is IPv6?

What is IPv6?

- On one hand, it is a network-layer protocol
  - RFC 1883 -> RFC 2460 -> now RFC 8200
- In practice, IPv6 is a suite of protocols:
  - IPv6
  - Network-addressing related documents
  - ICMPv6
  - Neighbor Discovery
  - Path-MTU Discovery
  - SLAAC
  - DHCPv6, DHCPv6-PD
  - Transition technologies

What has been progressed to IS?

Progressing IPv6 to IS

- Only the following documents have been progressed to IS:
  - RFC2460 -> RFC8200: Core IPv6 spec
  - RFC1981 -> RFC8201: Path-MTU iscovery
  - RFC4443: ICMPv6
  - RFC3596: DNS extensions for IPv6
- **This is very a small fraction of the whole IPv6 protocol suite**

Core IPv6 spec (RFC2460) to IS

Incorporated changes

Core IPv6 spec (RFC2460) to IS

Deprecation of RHT0

Deprecation of RHT0

- Routing Header Type 0 was IPv6's Source Routing (SR)
  - But allowed for the specification of multiple intermediate points
- Security implications of SR well known from the IPv4 world
- But still IPv6 incorporated this functionality
- Presentation in CanSecWec 2006 raised awareness for the IPv6 case
  - http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf
- RHT0 was formally deprecated by RFC5095

Core IPv6 spec (RFC2460) to IS

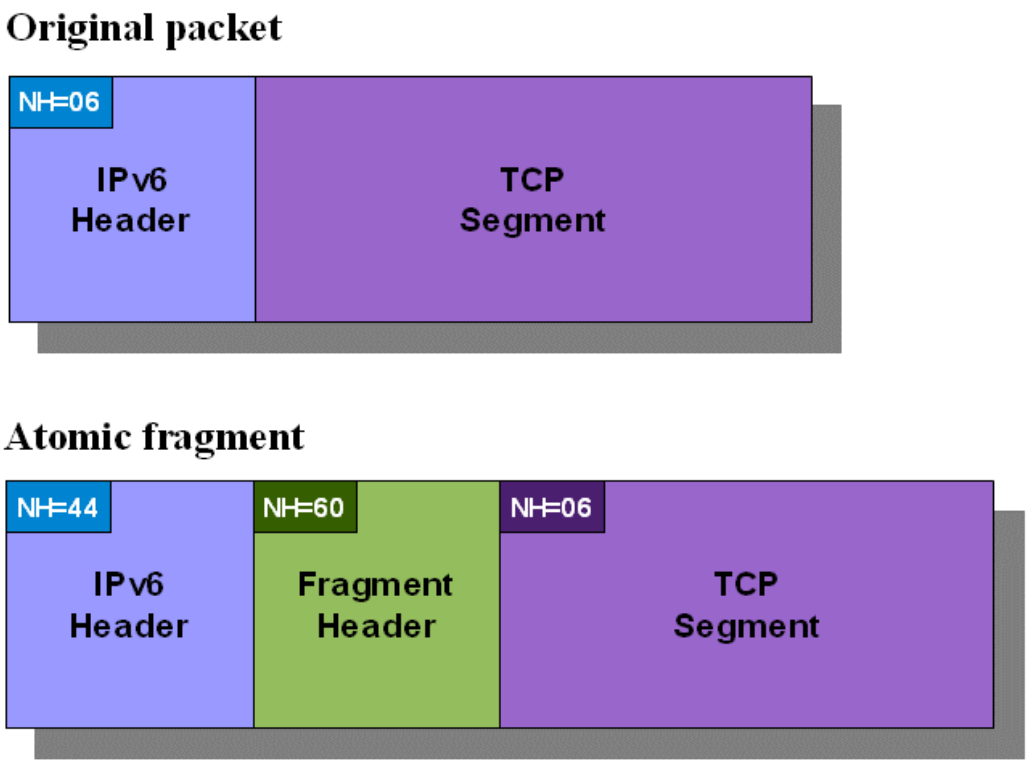
Fragmentation-related changes

Overlapping fragments

- Use of overlapping fragments for circumventing security controls known since (at least) 1998:
  - “Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection” (Ptacek and Newsham, 1998)
  - http://cs.unc.edu/~fabian/course_papers/PtacekNewsham98.pdf
- No legitimate use of overlapping fragments in IPv6
- But core IPv6 spec (RFC2460) allowed it
- RFC5722 banned overlapping fragments

Generation of atomic fragments

- RFC2460 stated that upon receipt of an ICMPv6 PTB message < 1280, hosts should generate atomic fragments:



Generation of atomic fragments (II)

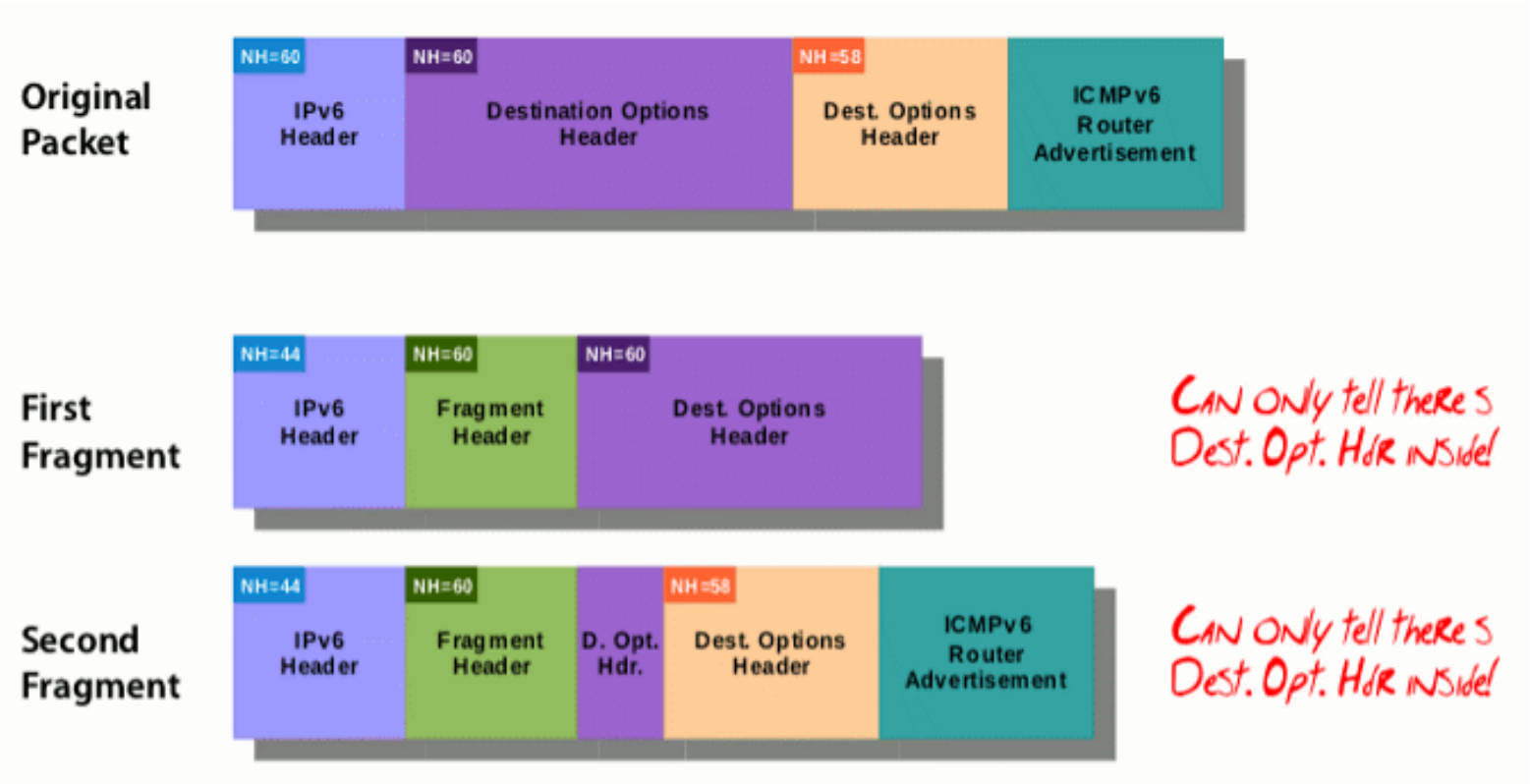
- While apparently harmless, atomic fragments can lead to DoS:
  - A single ICMPv6 PTB message can trigger atomic fragments
  - Widespread dropping of packets with EHs would lead to DoS
- Generation of atomic fragments was removed from RFC2460 (now RFC8200) and RFC6145 (now RFC7915)
  - Rationale in RFC8021

Processing of atomic fragments

- Since IPv6 atomic fragments are...“atomic”!
- No need to “reassemble” them
- Still, some implementations tried to reassemble atomic fragments with other queued fragments
- RFC6946 clarified the processing of IPv6 atomic fragments

Pathological first fragments

- RFC2460 allowed for first fragments that failed to include the entire IPv6 header chain:



Pathological first fragments (II)

- Such pathological fragmentation prevented, e.g., statelss packet inspection:
  - No single packet contains upper protocol info
  - Fragment reassembly is needed
- RFC7112 prohibits this pathological fragmentation
  - First fragment required to obtain entire IPv6 header chain

Core IPv6 spec (RFC2460) to IS

”Omissions”

Operational experience with EHs

- Operational experience with EHs at Internet scale boils down to:

  "IPv6 packets containing EHs are widely dropped"

  - See RFC7872
- Use of EHs including fragmentation and IPsec becomes challenging
- RFC8200 is moot on this topic
- Was it really possible to progress IPv6 to IS, considering EHs?

Requirements for Frag IDs

- Fragments of an original IPv6 packet are identified by means of an “Identification” value in the Fragment header
- RFC2460 suggested use of a global counter to generate these identifiers
  - But security implications of predictable IDs have been known for **decades**
  - See: draft-gont-predictable-numeric-ids
- IPv6 Frag IDs discussed in RFC7739 (Informational!)
- RFC8200:
  - Removes recomendation of global counter, and points to RFC7739
  - No formal security requirements for Frag IDs

Core IPv6 spec (RFC2460) to IS

”Controversy”

Insertion of IPv6 Extension Headers

- IPv6 is an end-to-end protocol
- A proposal for Segment Routing with IPv6 (SRv6) (draft-ietf-6man-segment-routing-header) proposed the insertion of EHs at middleboxes:
  - Proponents argued that RFC2460 was ambiguous in this respect
  - The WG had consensus **against** EH insertion

Insertion of IPv6 Extension Headers (II)

- Proponents of SRv6 pushed to keep alledged ambiguty in RFC2460bis
  - Idea backed (mostly) by employees of the same single vendor
- WG shipped document with alleged ambiguity
- Issue raised again during IETF LC
  - Decision of WG was reverted -> EH insertion banned
- Idea of EH insertion was pushed once more during IESG review
- RFC8200 was published with explicit ban of EH insertion

Core IPv6 spec (RFC2460) to IS

Security Considerations

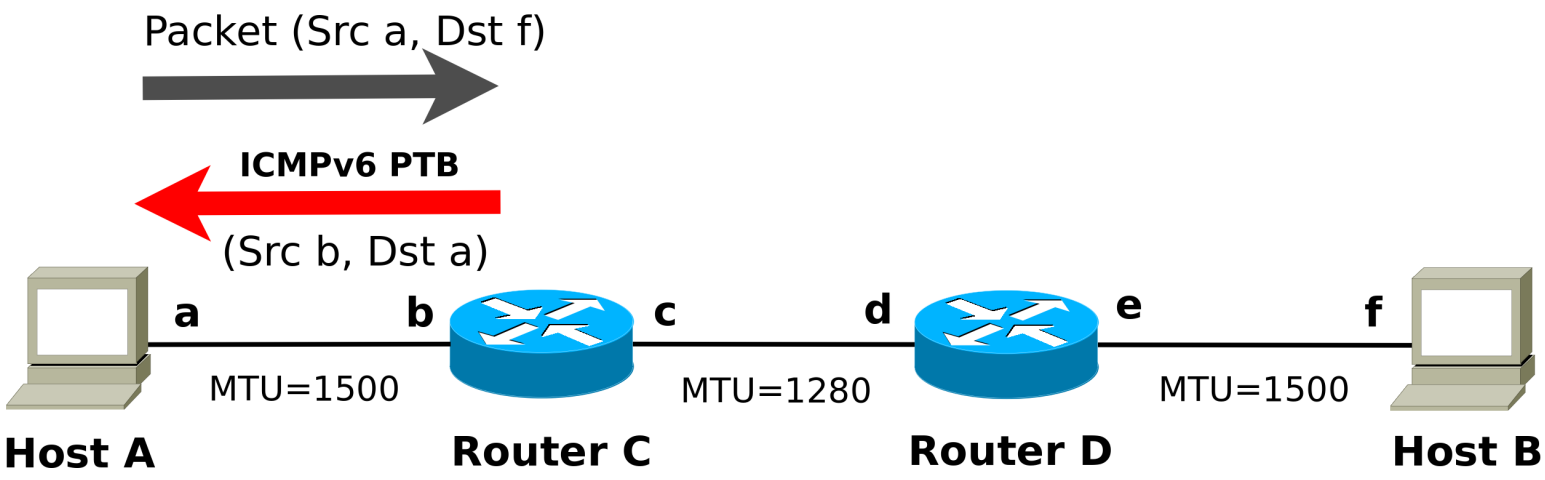
Security Considerations

- RFC2460 lacked a proper “Security Considerations” section
- RFC8200 includes a more proper discussion of the security implications of IPv6
- It also includes pointers to some of the work carried out in the last 10 years:
  - Security and Privacy implications of IPv6 addresses (RFC7721 & RFC7707)
  - Some mention of issues associated with EHs (references missing, though)

Path-MTUD to (RFC1981) to IS

Path MTU Discovery

- Path-MTU Discovery relies on ICMPv6 messages to discover the minimum MTU towards a destination



Path MTU Discovery to IS

- Controversy happened when elevating Path-MTU Discovery (RFC1981) to IS
  - We should elevate RFC4821 to IS, rather than RFC1981
  - But RFC4821 wasn't ready for IS
- End result:
  - Traditional Path-MTU Discovery (RFC1981) elevated to IS via publication of RFC8201
  - Rationale: “if ICMPv6 error messages are not dropped, it works”

IPv6 Addr. Arch. (RFC4291) to IS

(“Failure to move...”)

Addressing architecture to IS

- IPv6 Addressing Architecture (RFC4291) mandates use of /64 for IPv6 subnets
  - There has been a heated debate on this hardcoded size
- Some see it as a constraint:
  - Allowing subnets smaller than /64 provides extra flexibility for the operator
  - A network can always be further extended (without NAT) by using smaller subnets
- Others think that it guarantees hosts can obtain multiple addresses:
  - If there's no lower limit on the subnet size, ISPs could start assigning only one address per host

Addressing architecture to IS (II)

- The 6man WG failed to achieve consensus
- There is no clear path to progress RFC4291 to IS

Conclusions

Conclusions

- Only a tiny part of the IPv6 protocol suite has been formally elevated to “Internet Standard”
- Despite hopes, there are aspects of the protocol for which we lack wide-scale successful operational experience
- At times, the maturity level of a spec is used as an excuse for not changing it (including patching flaws)
- All the above says nothing about the maturity of IPv6 implementations
  - Which is close to that of IPv4 implementations in the 90's

Acknowledgements

Ivan Arce (@4Dgifts)

- An Argentina-based maradonian

Enno Rey (@Enno_Insinuator)

- A Germany-based maradonian

Diego Armando Maradona

- “The influence of Maradona's game is the third of the important feelings that drive mankind” -- Emir Kusturika

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com