



Conex IPv6 format

Suresh Krishnan
Mirja Kuehlewind
Carlos Ralli Ucendo

















Requirements for marking IPv6 packets

- › R-1: The marking mechanism needs to be visible to all conex-capable nodes on the path.
- › R-2: The mechanism needs to be able to traverse nodes that do not understand the markings. This is required to ensure that conex can be incrementally deployed over the Internet.
- › R-3: The presence of the marking mechanism should not significantly alter the processing of the packet. This is required to ensure that conex marked packets do not face any undue delays or drops due to a badly chosen mechanism.
- › R-4: The markings should be immutable once set by the sender. At the very least, any tampering should be detectable.

Candidate solutions

- › Extension headers
- › Hop-by-Hop Options
- › Destination Options
- › Bits in the IPv6 header

Scorecard

	R1	R2	R3	R4
Extension headers				
Hop-by-Hop Options				
Destination Options				
Header Bits				

Destination Options

- › Seem to be the best way forward
- › The conex-aware nodes on path that inspect these options are not exactly standards compliant
 - RFC2460 does not use RFC2119 wording and hence it is hard to say one way or another
- › The conex-aware nodes will
- › The destination options are encrypted by IPsec ESP and this will make them opaque to conex-aware nodes on the path
 - We can decide to leave out encrypted packets out of scope of conex



ERICSSON