IOAM Loopback & Direct Export (DEX)

Potential Problems
Martin Duke, IETF 110
Loopback & DEX
In order to mitigate the attacks described above, it should be possible for IOAM-enabled devices to limit the exported IOAM data to a configurable rate.

In order to mitigate the attacks described above, as described in Section 7 it should be possible for IOAM-enabled devices to selectively apply the mechanisms that use the flags defined in this document to a subset of the traffic, and to limit the performance of synthetically generated packets to a configurable rate; specifically, network devices should be able to limit the rate of: (i) looped-back traffic (at transit nodes), (ii) replicated active packets (at encapsulating nodes), (iii) packets that are exported to a collector (from either encapsulating nodes or transit nodes), and (iv) synthetically generated packets (at encapsulating nodes).
A bad DEX Corner Case
A bad DEX Corner Case

My Domain

N Hops

Decapsulating Node

Encapsulating Node

Decapsulating Node

Encapsulating Node

My Cloud Provider

Tommy’s Domain
A bad DEX Corner Case

My Domain

Encapsulating Node

N Hops

Decapsulating Node

MxN (!)

Decapsulating Node

My Cloud Provider

Tommy’s Domain

Tommy’s Cloud Provider

M Hops

Encapsulating Node
A bad DEX Corner Case

My Domain

Encapsulating Node

N Hops

Decapsulating Node

MxN (!)

Decapsulating Node

My Cloud Provider

M Hops

Tommy’s Cloud Provider

Tommy’s Domain

\[ M N^2, M^2 N^2, M^2 N^3, \ldots \]
A (less bad) Loopback Corner Case

Encapsulating Node \[\rightarrow\] N Hops \[\rightarrow\] Decapsulating Node

Decapsulating Node \[\rightarrow\] M Hops \[\rightarrow\] Encapsulating Node

Tunneled over...

1 user message = M (N-3) loopback messages
What now?
What now?

• More security considerations?
  • Situation not detectable!
  • Rate limiting not a good solution to infinite traffic
  • Tighter probability bounds?
  • Stronger restriction to a domain?

• Or fundamentally rethink what we’re doing here?