RFC6145: The IPv6 addresses in the ICMPv6 header may not be IPv4-translatable addresses. … A mechanism by which the translator can instead do stateless translation is left for future work.
Requirements (1)

- uRPF $\rightarrow$ cannot use RFC1918 addresses
- IPv4 address depletion $\rightarrow$ hard to use public IPv4 addresses
Requirements (2)

- IPv4 recipient of the ICMP message should be able to distinguish between different IPv6 ICMPv6 origination → needs a pool
Progress

• IANA reversed prefix 192.70.192.0/24
  – Scope: Addresses from the assigned address prefix are intended to be used as source addresses and not as destination addresses in the context of the public network.

• According to the comments received from the mailing-list and in the Taipei meeting. The major updates are:
  – Add RFC5837 requirements for identify the source IPv6 address in ICMP.
  – Only propose hop count mapping algorithm
  – Add filtering and rate-limiting recommendations
RFC5837 issue

• When translator is configured to use the IANA-assigned /24 to map non IPv4-translatable address, the translator **MUST** implement ICMP extension defined by [RFC5837].

• The resulting ICMP extension **MUST** include the IP address Sub-Objects that specify the source IPv6 addresses in the original ICMPv6.
Filtering and rate-limiting recommendations

• **Filtering Recommendations**
  – SHOULD allow ICMP type 3 - Destination Unreachable (incl PTB).
  – SHOULD allow ICMP type 11 - Time Exceeded.
  – MAY allow ICMP type 12 - Parameter Problem.
  – SHOULD NOT allow any of the various ICMP request messages.

• **Rate-limiting Recommendations**
  – The rate limiting of traffic from the prefix SHOULD also be enabled as additional countermeasure against abuse of this prefix.
  – The methods presented in [RFC4443] [RFC5597] [RFC6192] [RFC6398] [RFC6450] can be used.

• **RFC5837 Recommendations**
  – Advanced filtering and rate-limiting techniques which can process the ICMP extension defined in [RFC5837] MAY also be used to control the source of the ICMP.
Remarks

• When setting up the ACL correctly
  – The network only allows ICMP packets using this block as the source address.
  – No responses will be generated from any network device in the network.

• The original IPv6 address is traceable
  – RFC5837 is a MUST requirement

• Rate-limiting can be used as additional protection scheme