Exploiting ICMPv6 Error Messages for Reconnaissance

Florian Holzbauer, Markus Maier, Johanna Ullrich

Problem & Motivation
▶ Reconnaissance in IPv6 remains an open problem due to its sheer address space.
▶ However, the amount of error messages usually exceeds the amount of positive replies in IPv6.
▶ We investigate whether error messages allow to infer the deployment status of an IPv6 network.

Methodology
▶ Behaviors of virtual router appliances are monitored in a lab setup.
▶ Results are cross-checked with response behavior in the wild.
▶ Contribution of error messages to active network detection is shown.

Response Behavior in the Wild
Based on a list of addresses known to be active, we generated test cases that represent (I) probing of an active network, and (II) probing of an inactive network.

Lab Environment
We investigated response behavior of routers in a laboratory setup and found error message types to be ambiguous. For example, "Address Unreachable" is used for an inactive host in an active network, but also in case of an active reject route.

Response Timings in the Wild
There is a difference in timing of “Address Unreachable” messages that allows to gain insight into the remote network’s status.

Conclusion
▶ Error messages can be used to infer the deployment status of an IPv6 network. Therefore we recommend a two-step approach for IPv6 measurements: 1) Detect active subnets. 2) Investigate active subnets for active hosts.
▶ We detected numerous routing loops in IPv6.