Exploiting ICMPv6 Error Messages for Reconnaissance

Florian Holzbauer, Markus Maier, Johanna Ullrich

COMET Competence Centers for Excellent Technologies
www.ffg.at/comet
SBA Research

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 message 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.

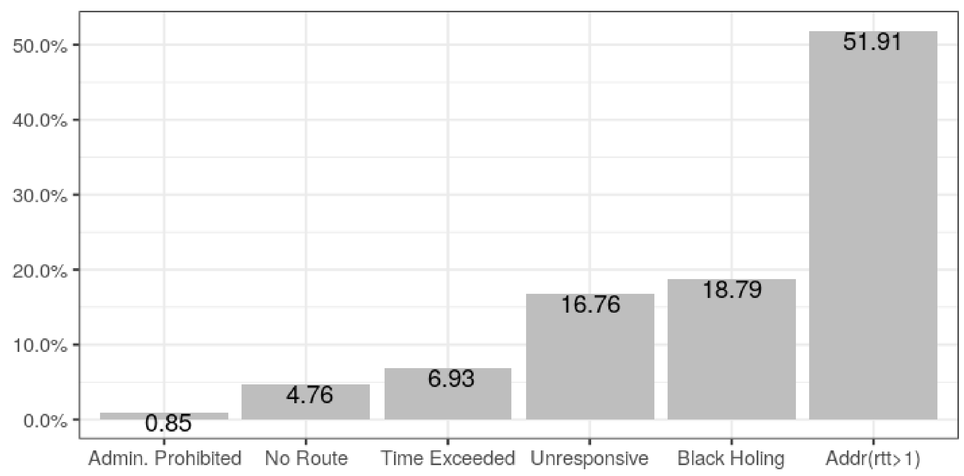

Figure 1: Active network responses

More than 50% of active networks respond with "Address Unreachable" with a RTT > 1s. In contrast, inactive networks react differently. We found requests to 20.8% of inactive networks result in a routing loop.

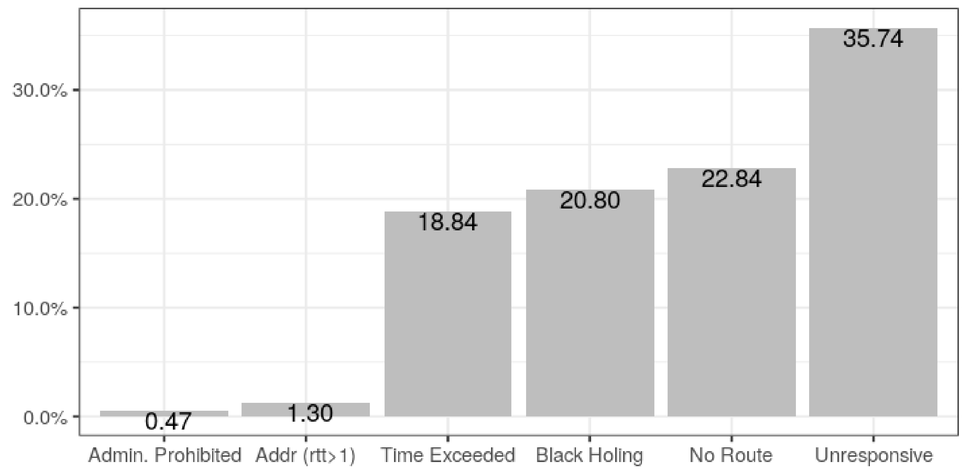

Figure 2: Inactive network responses

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.

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.

	Protocols	Act. NW, Act. Host	Act. NW, Inact. Host	Inact. NW, Inact. Host	Act. ACL	Act. Rej. Route	Rout. to Inc. Interface
Test Case No.		1	2	3	4	5	6
Cisco IOS 15.2.4	All	Reply	Address Unreachable	No Route	Admin. Prohibited	Reject Route	Time Exceeded
Cisco CRS1000V	All	Reply	Address Unreachable	No Route	Admin. Prohibited	Reject Route	-
Juniper VMx 17.1	All	Reply	Address Unreachable	No Route	Admin. Prohibited	Address Unreachable	Time Exceeded
HPE VSR1000	All	Reply	-	-	-	-	Time Exceeded
Mikrotik 6.45	All	Reply	Address Unreachable	No Route	No Route	No Route	Time Exceeded
OpenWRT 19.07	ICMP	Reply	Address Unreachable	Failed Policy	Port Unreachable	Failed Policy	Failed Policy
	TCP/UDP	Reply	Reply	Failed Policy	Reply	Failed Policy	Failed Policy

Table 1: Recorded Message Originating Behavior of Router Operating Systems

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.

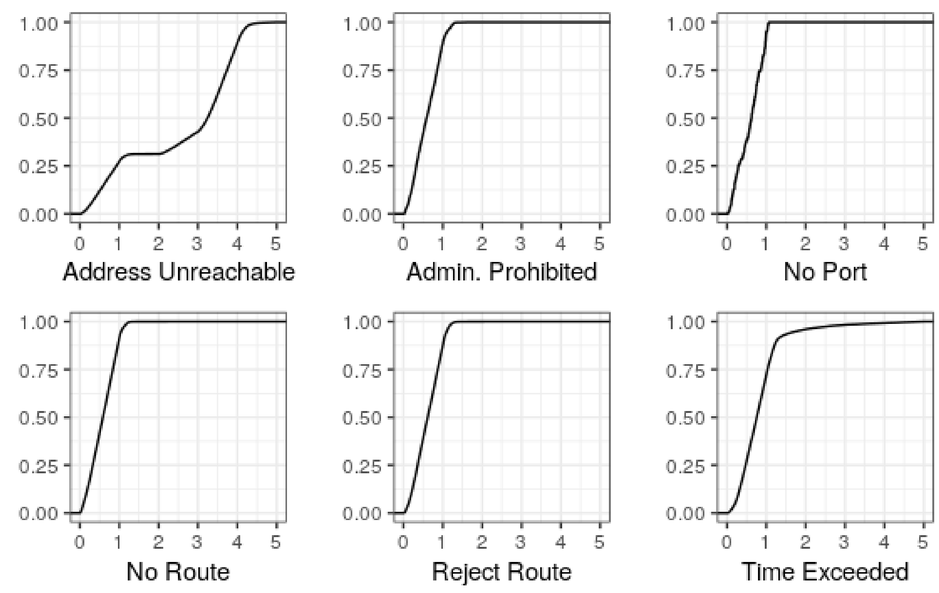

Figure 3: CDF of round-trip times (in seconds) per message type

Demonstration

- *764 Enterprise Networks*: We scanned all directly allocated /48 networks from Gasser's hitlist. Based on Addr (rtt>1) we found around 39.5 active subnets for each network, while the hitlist only shows 3.23 subnets per network.
- *1 ISP Network*: Error Messages allowed us to differentiate between custom home routers and ISP proprietary routers in use. We detected only 0.5% of home connections use custom routers.
- *1 ISP Business Network*: We know from at least one network range of our research partner to be active. While we detected 41 other active networks through Echo Replies, 29 were solely detected by Addr(rtt>1), enhancing the results by about 70%.

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie
Bundesministerium Digitalisierung und Wirtschaftsstandort
FFG Forschung wirkt.
wirtschaftsagentur wien Ein Fonds der Stadt Wien
Europäische Kommission
FWF Der Wissenschaftsfonds.
netidee OPEN INNOVATIONS

SBA Research (SBA-K1) is a COMET Centre within the framework of COMET – Competence Centers for Excellent Technologies Programme and funded by BMK, BMDW, and the federal state of Vienna. The COMET Programme is managed by FFG.