Considerations in Running Active Measurements on RouteViews Collectors

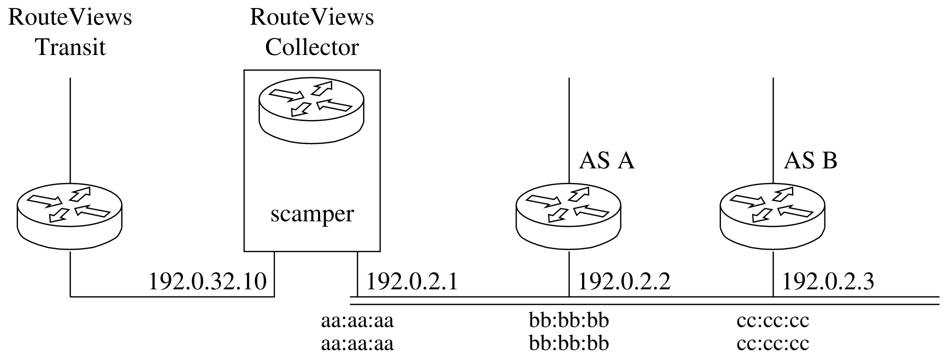

Figure 1: Architecture of scamper use on RouteViews collectors.

We propose to leverage existing BGP collector infrastructure to support active network measurements (ping and traceroute), using CAIDA's Ark measurement software SCAMPER. This capability allows for correlation of data plane and control plane views from the same vantage point, which has been a long-standing visibility gap in the Internet research community. The goal of this document is to describe how SCAMPERcan responsibly conduct data-plane measurements from RouteViews collectors through RouteViews peers, and implications for both collectors and peers. The ability to discover finer-grained (router-level) topology via the RV collector infrastructure offers both operational and research utility (§2).

1 Using Scamper from RouteViews Collector

A RouteViews collector has a transit interface with a globally-routed address configured (192.0.32.10) which the collector uses to transmit archived routing tables to the University of Oregon, as well as an interface in an IXP peering LAN (192.0.2.1) which it uses to establish BGP sessions with members at the exchange (e.g., AS A with 192.0.2.2). To perform an active measurement (ping or traceroute) through AS A in Figure 1, the meassurement software will form an Ethernet frame with the member peer's MAC address (bb:bb:bb:bb:bb:bb, learned through an ARP request) as the *destination* MAC address, and use the collector's MAC address (aa:aa:aa:aa:aa:aa) as the source. Inside the Ethernet frame is an IP packet, with the collector's transit IP address (192.0.32.10) as the source address, so that the RouteViews collector can receive responses from the Internet. Note that *none of the source addresses are spoofed*; they are assigned to the collector. The destination IP address is set to the measurement target IP address, which will vary according to the goals of the measurement.

We use SCAMPER [1] to perform this measurement. SCAMPERis an open-source software measurement tool that implements ping and traceroute among other common active measurement techniques. Many researchers and industry players use SCAMPER to actively probes the Internet in order to analzye topology and performance. SCAMPERis designed to actively probe IP addresses in parallel at a specified packets-per-second rate, to support efficient collection of bulk data. SCAMPER supports TCP, UDP, and ICMP probe packet types, sending small packets by default: 44 bytes for IPv4 UDP probes, 60 bytes for IPv6 UDP probes, and approximately the same for the ICMP responses that SCAMPER receives.

Currently, as part of an NSF-funded collaboration between CAIDA/UCSD and RouteViews, a machine at CAIDA coordinates the measurements. This machine uses SCAMPER's remote control mechanism to request measurements and receive results from RouteViews collectors. No user of this service needs (or will receive) a login to any RouteViews collector or other infrastructure. RouteViews limits SCAMPER's probing rate on the collectors to a maximum of 100 PPS – approximately 6KB/s through the exchange fabric. The responses will not arrive through the exchange; they will arrive at the collector through its transit interface, i.e., from the Internet. In addition to these guard rails, we will implement functionality to allow RouteViews peers to opt-in (for existing peers) or opt-out (for new peers) of use of their peering router for such measurements.

2 Operational and research use cases for this functionality

This functionality is useful for both operations and research. Use cases include:

1. Use traceroute to uncover the router-level path of how traffic from a given member reaches their network.

2. Understand the effect of apparently redundant more-specific prefixes on forwarding behavior.

3. Measure latency to the same destination through different peers

4. Enable a richer view of router-level topology. (A single routeviews collector at an exchange has the ability to measure topology through multiple different networks. The traditional approach requires one vantage point per network.)

References

[1] Scamper. https://www.caida.org/tools/measurement/scamper/.