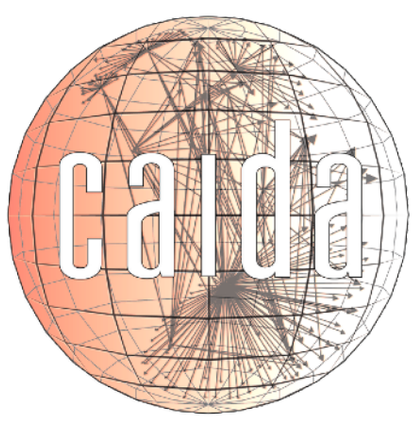
# An Alias Resolution Service for the Community

Young Hyun
CAIDA
SDSC/UCSD

Mar 14, 2018
AIMS 2018




# talk goals

- give heads up to community
  - work in progress
  - early stages of implementation
  - solicit feedback and requests
  - look for beta testers

# alias resolution

- identify which interfaces belong to the same router
- useful for ...
  - identifying border links (bdrmap-IT)
  - producing router-level and pop-level topology
    - understanding full complexity of AS peering arrangements
    - redundancy and resilience of ASes
  - identifying traceroute path anomalies/artifacts
    - Luckie et al, "A Second Look at Detecting Third-Party Addresses in Traceroute Traces with the IP Timestamp Option"
  - decipher MDA traceroute results

# project goals

- provide a community service for performing alias resolution
  - large-scale: thousands to millions of targets
- focus on techniques that aren't practical for researchers
  - complex software
  - high infrastructure and/or CPU requirements
  - high operational costs dealing with host/network failures

# why?

- re-use knowledge, experience, expertise
  - strengths, weaknesses, nuances, and pitfalls of each technique
  - best practices
  - for example, Mercator has a lot of false positives at Internet scale O(millions of targets)
    - unpublished work with Ken Keys: algorithm to prune false positives
- integrate multiple techniques, data sources, and tools
  - challenging to combine results with different accuracy
  - example tie-in: query for traces by router in Henya
  - seed aliases from one technique into others; for example, MIDAR to kapar

# techniques

- planned
  - MIDAR: check IPID-based monotonic bounds test
- possibly
  - Matthew's DNS-based technique
  - prespecified timestamps (Justine Sherry)
  - iffinder: look for common source address in responses (Mercator)
  - speedtrap: look for similar IPv6 fragment identifiers
  - kapar: APAR + extensions (passive technique; need traceroute paths)

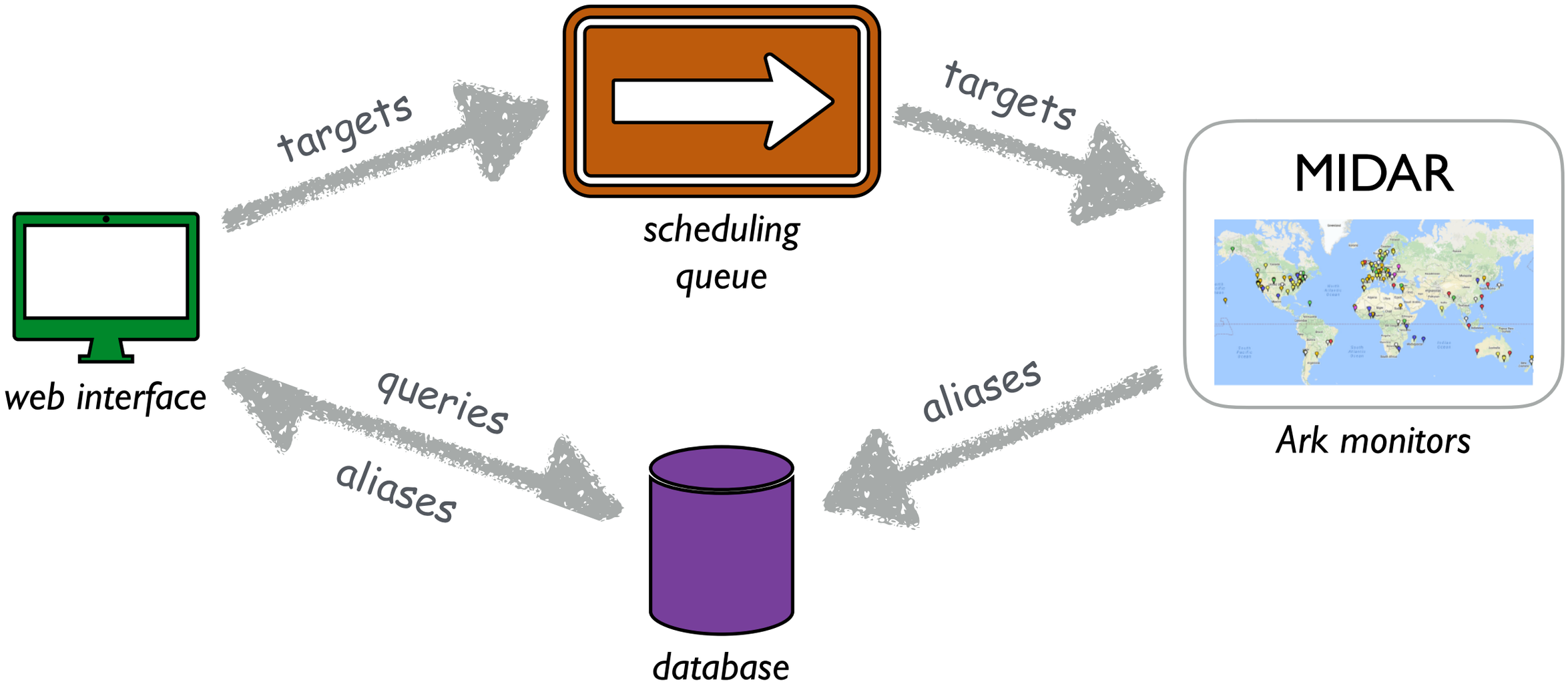
# user interfaces

- API over HTTP
  - for example, submit targets with POST request
  - query for aliases
- web interface (for humans)
  - paste targets into a text area
  - upload a file with targets
  - query for aliases with web form

# querying

- queryable archive of all resolved aliases
  - aliases from past ITDK runs
  - results of user-submitted runs
- sample queries:
  - show which submitted targets are aliases of each other
  - return all known interfaces for a given target
  - show all alias sets (that is, routers) in a given prefix/AS?

# architecture




Thanks! Potential user? ark-info@caida.org