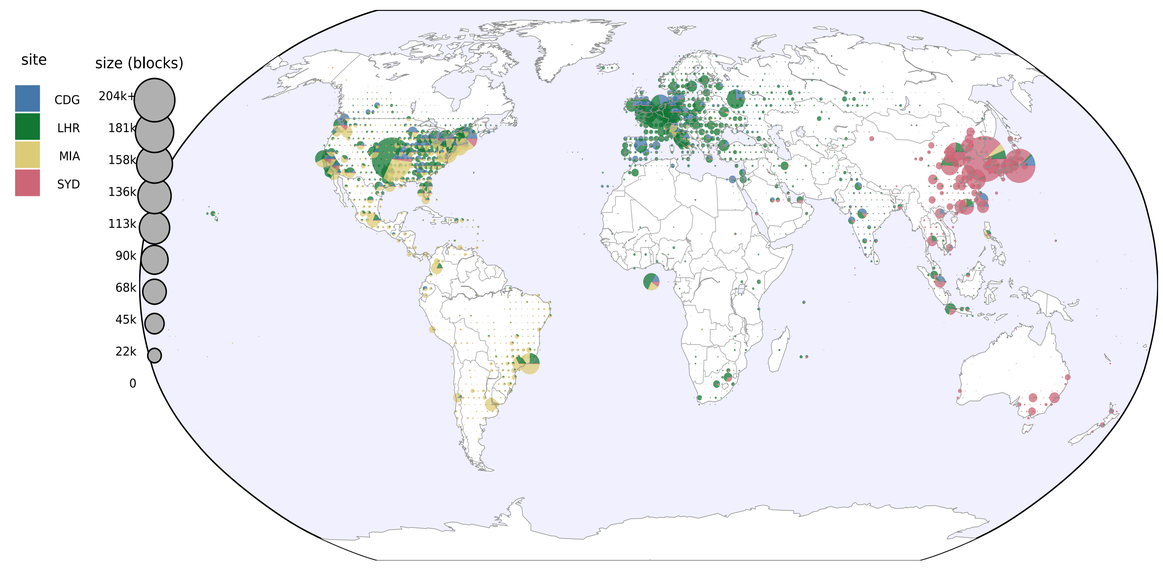
Planning for Anycast as Anti-DDoS

Leandro M. Bertholdo[1], João Ceron[1], Wouter de Vries[1], Roland van Rijswijk-Deij[1]
Aiko Pras[1], John Heidemann[2]
[1]University of Twente [2]University of Southern California

Concepts

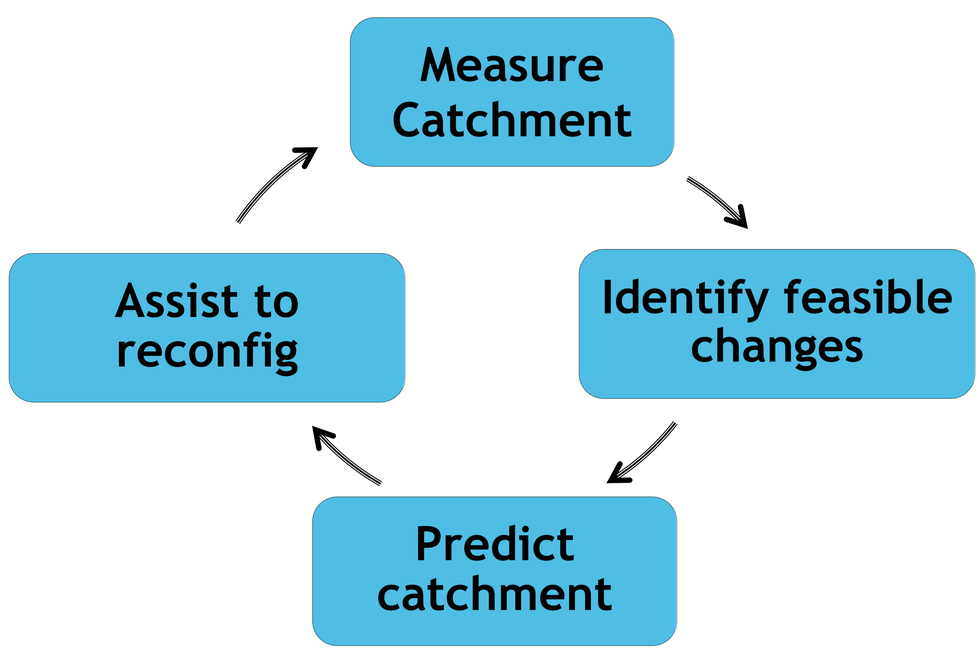
- BGP Anycast is a networking technique where several servers use the same IP Address spread over the world
- Good for performance, resilience, and reliability (ex. DNS root-servers)
- “Catchment control” refers to which site will attract Internet traffic in a specific region



Objective

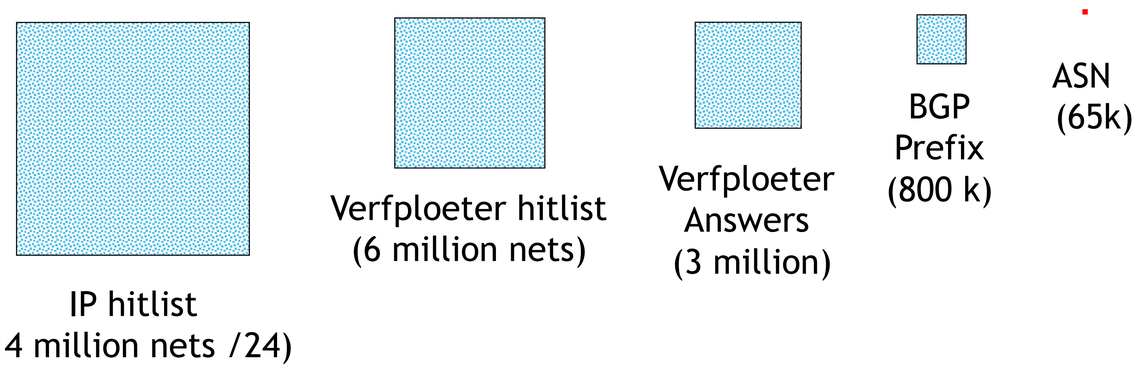
- Better defence against large-scale Distributed Denial-of-Service (DDoS) attacks by making anycast more effective than today

Our Approach



If you want control, you need to measure it!

We use a tool called Verfploeter and an IP-Hitlist to measure and have a better control over anycast nodes, collecting catchment data in terms of volume, proximity (RTT) or georeferencing.



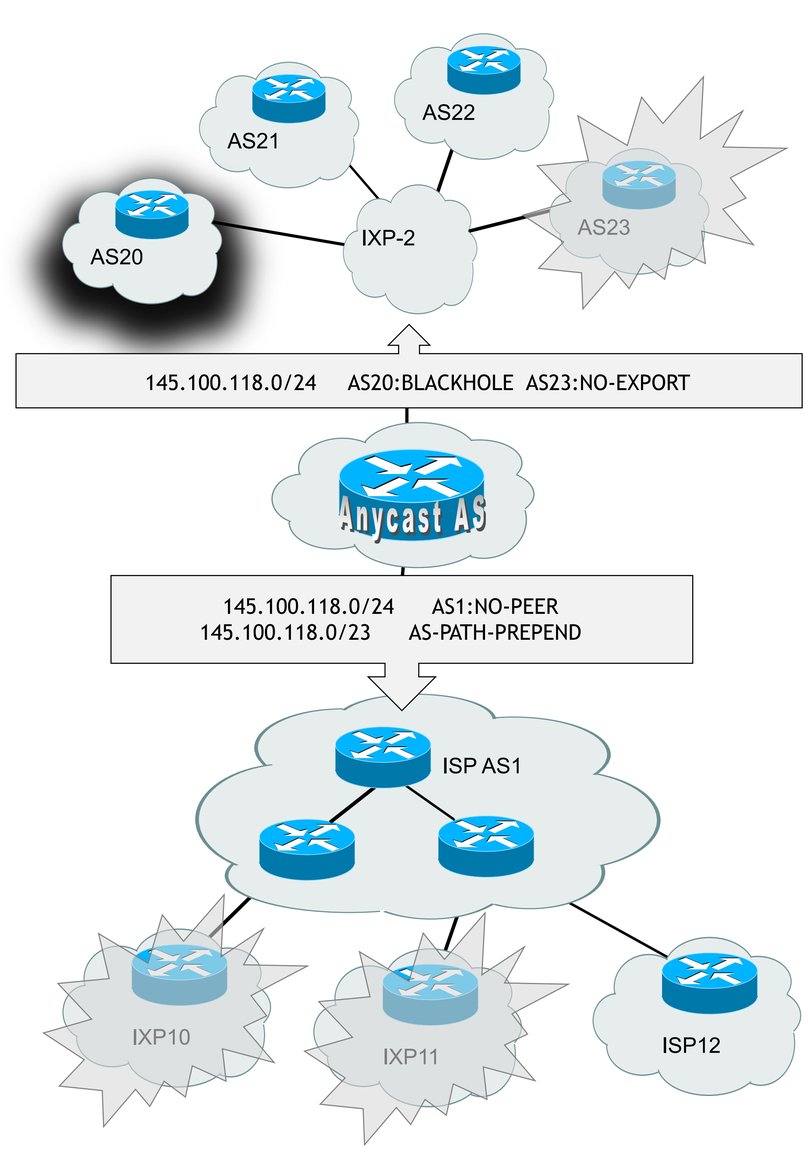
Map anycast catchments and baseline load

Project changes and predicts effects on catchments

Estimate attack load and assist in anycast reconfiguration

BGP & Catchment Manipulation

We are implementing fine-grained catchment control through BGP attribute manipulation (AS-Path, Aggregation and Communities).



https://paaddos.nl

This work has received funding from CONCORDIA, the Cybersecurity Competence Network supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.