ANYCAST
ITS POTENTIAL FOR DDOS MITIGATION

Wouter de Vries
w.b.devries@utwente.nl

Ricardo Schmidt
r.schmidt@utwente.nl

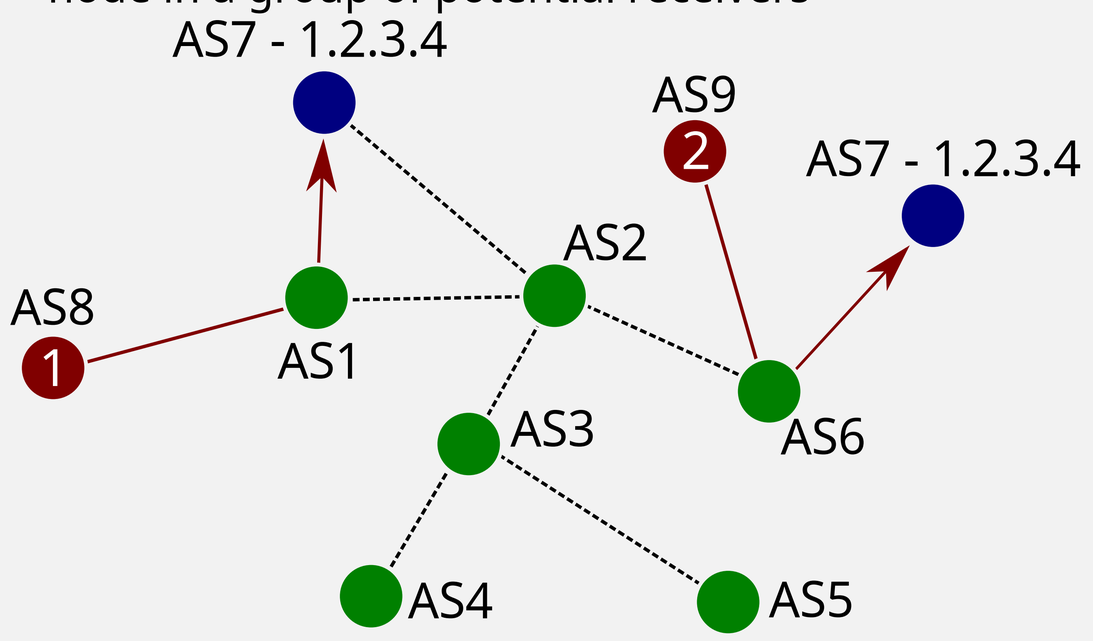
Aiko Pras
a.pras@utwente.nl

IP anycast is widely being used to distribute essential Internet services, such as DNS, across the globe. Our aim is to investigate methods to optimize anycast deployments in order to improve service resilience against DDoS attacks. Is it possible to change the placement of anycast nodes to support DDoS attack mitigation?

Research questions

- What are the current DDoS mitigation strategies?
- Where do DDoS attacks come from, network topology wise?
- What impact does adding/removing nodes have on the overall catchment of an anycast network
- In what way can that catchment be influenced to increase resilience against DDoS attacks
- How can the composition of an anycast network be dynamically influenced in order to improve service resilience against DDos Attacks

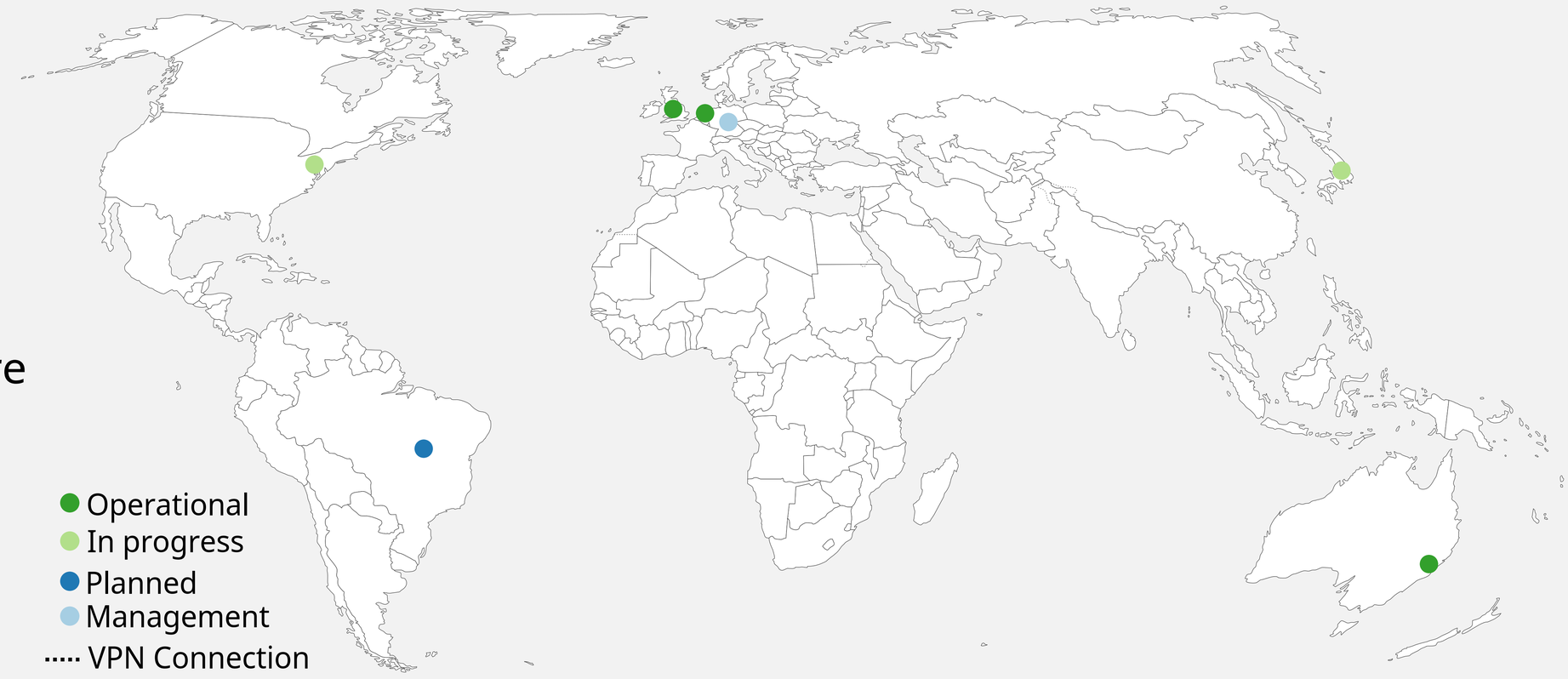
"Anycast is a network addressing and routing methodology in which datagrams from a single sender are routed to the topologically nearest node in a group of potential receivers"



Real-world experience with anycast and BGP within the research community is limited, therefore we are developing an anycast testbed. This testbed will allow us to design and perform large-scale experiments, for example to determine the global catchment of a specific anycast network composition.

Current state of anycast testbed

The testbed currently has 3 operational nodes. 3 additional nodes are being provisioned. Finally, 3 more nodes are planned to become operational in coming months. All nodes are centrally controlled from a management server.



debian ANSIBLE ExaBGP RethinkDB

DACS Design and Analysis of Communication Systems

SURF NET

UNIVERSITY OF TWENTE.