DE·CIX

Awesome for 20 years

Blackholing at IXPs

On the Effectiveness of DDoS Mitigation in the Wild

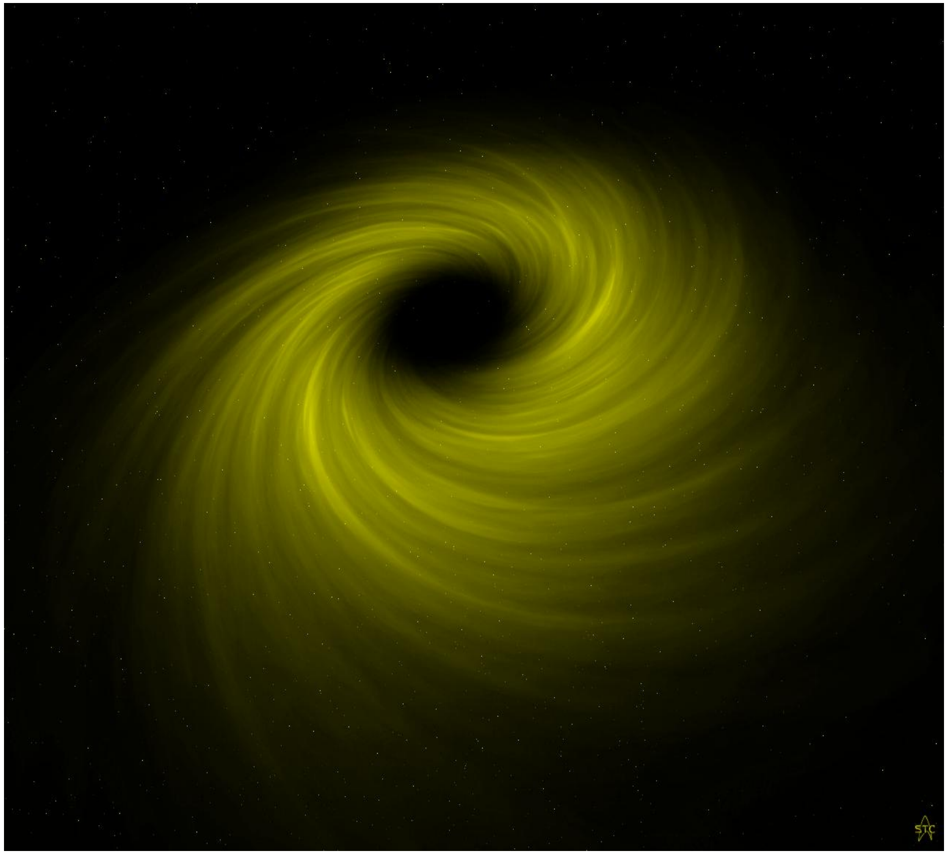
MENOG 16

Christoph Dietzel

R&D DE-CIX / TU Berlin

What is Blackholing?

A **black hole** *is a geometrically defined* **region** *of spacetime* **exhibiting** *such* **strong gravitational effects that nothing***—including particles and electromagnetic radiation such as light—***can escape from inside** *it* [1].



[1] Wald, Robert M. (1984). General Relativity. University of Chicago Press. ISBN 978-0-226-87033-5.

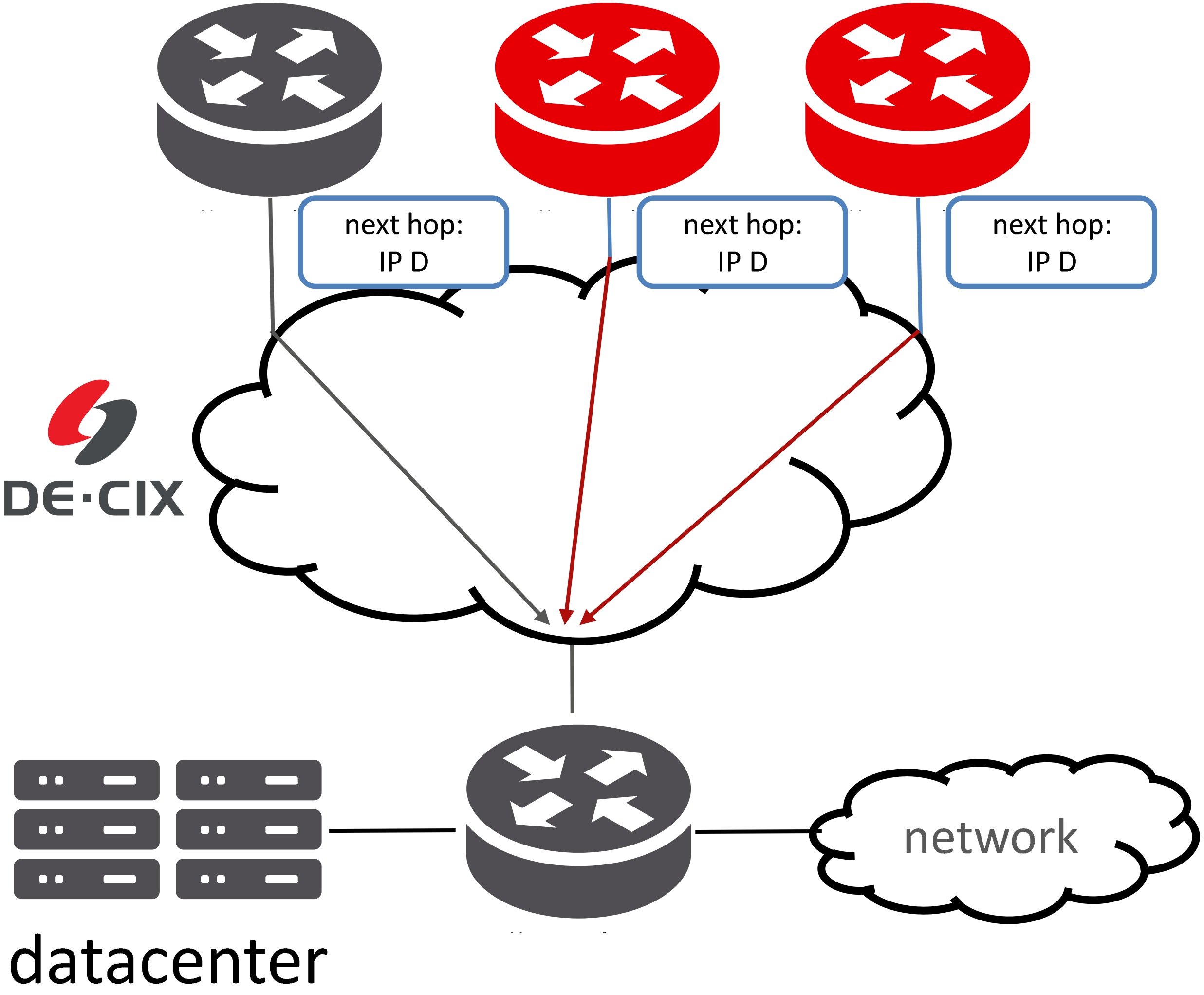
What is Blackholing?

- Operational technique to counter DDoS attacks

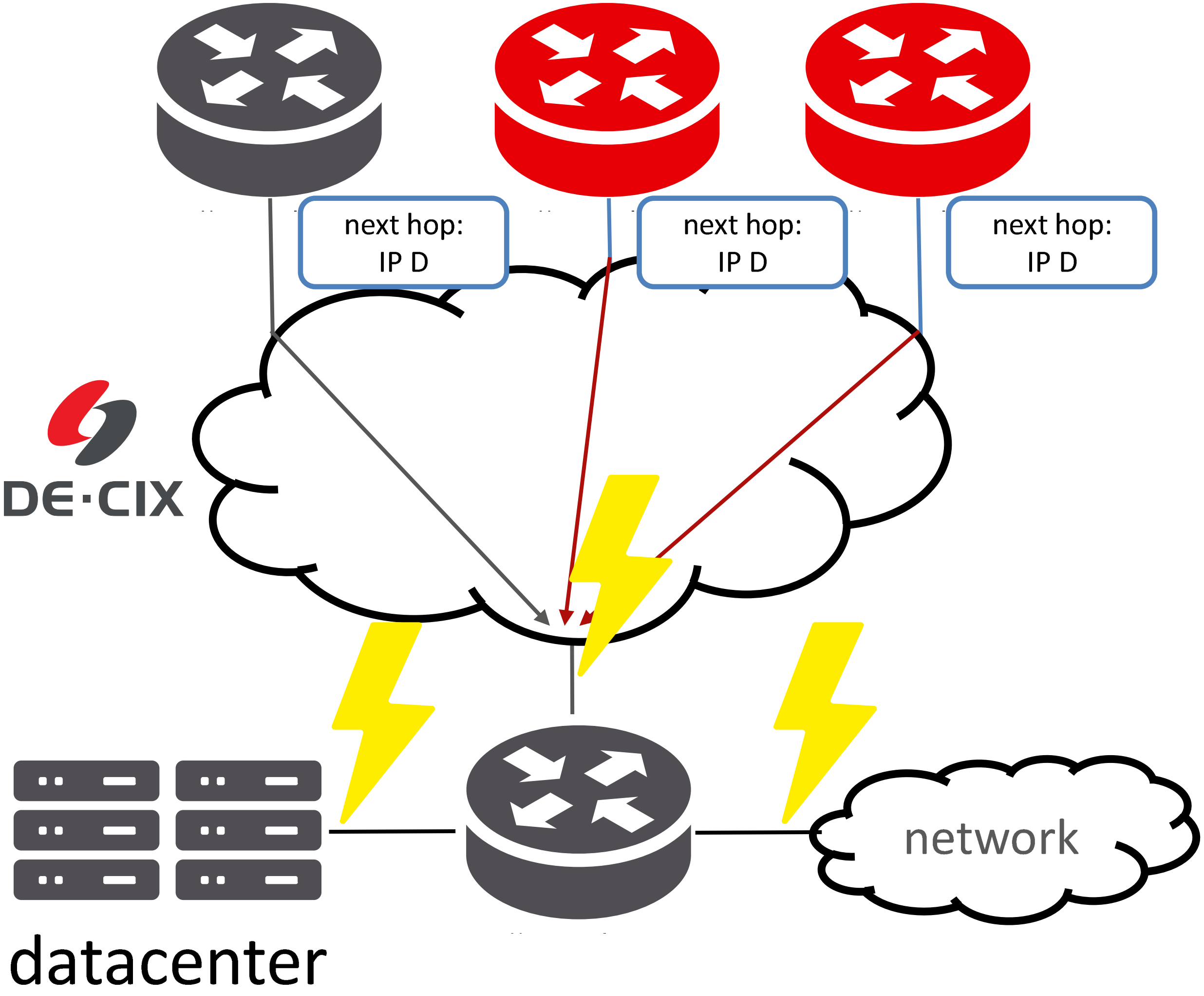
- Last resort to protect peering link or own network

- Since a few years also at IXPs (DE-CIX, MSK-IX, NETIX, NIX-CZ, …)

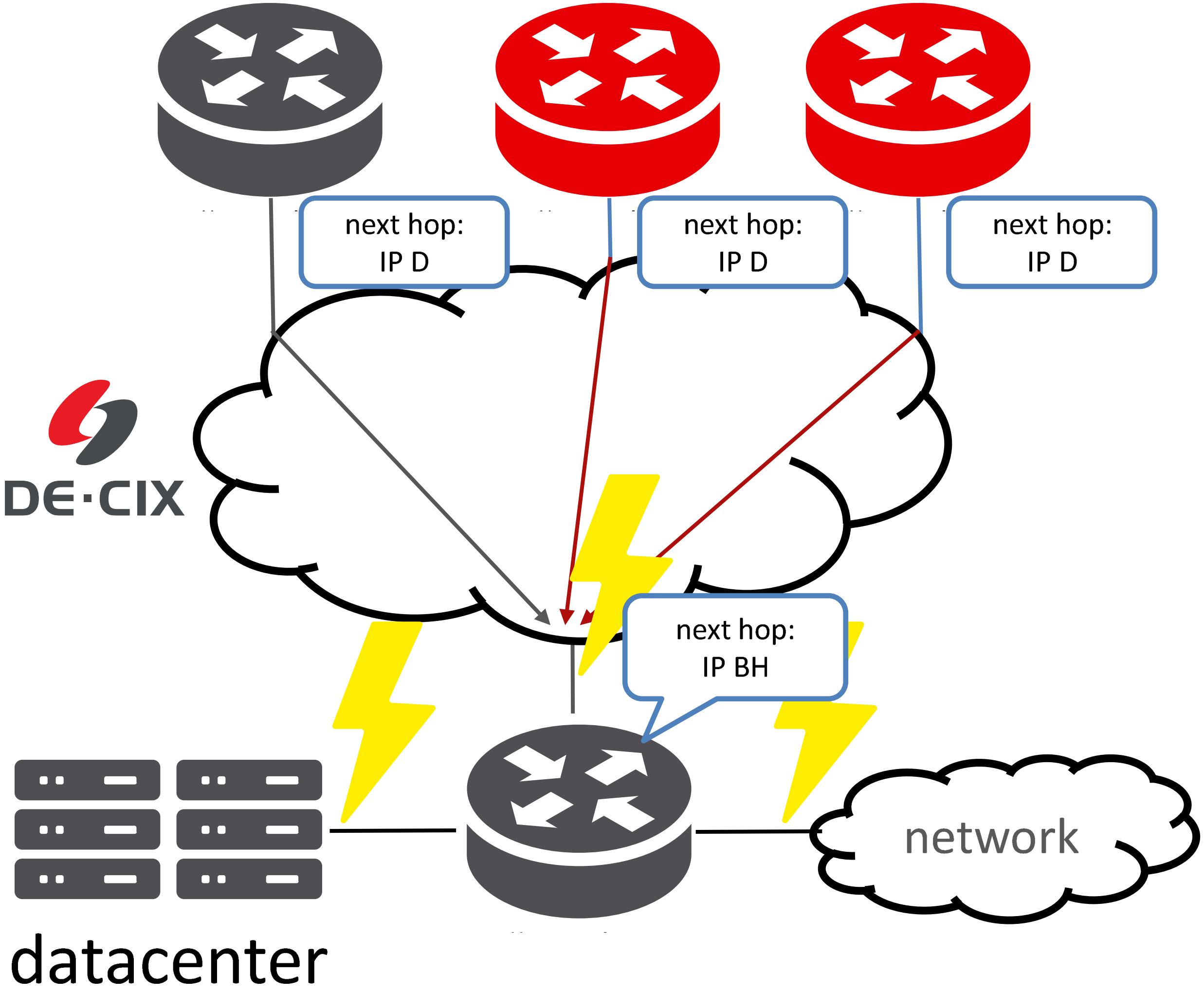
Blackholing – DDoS Attack



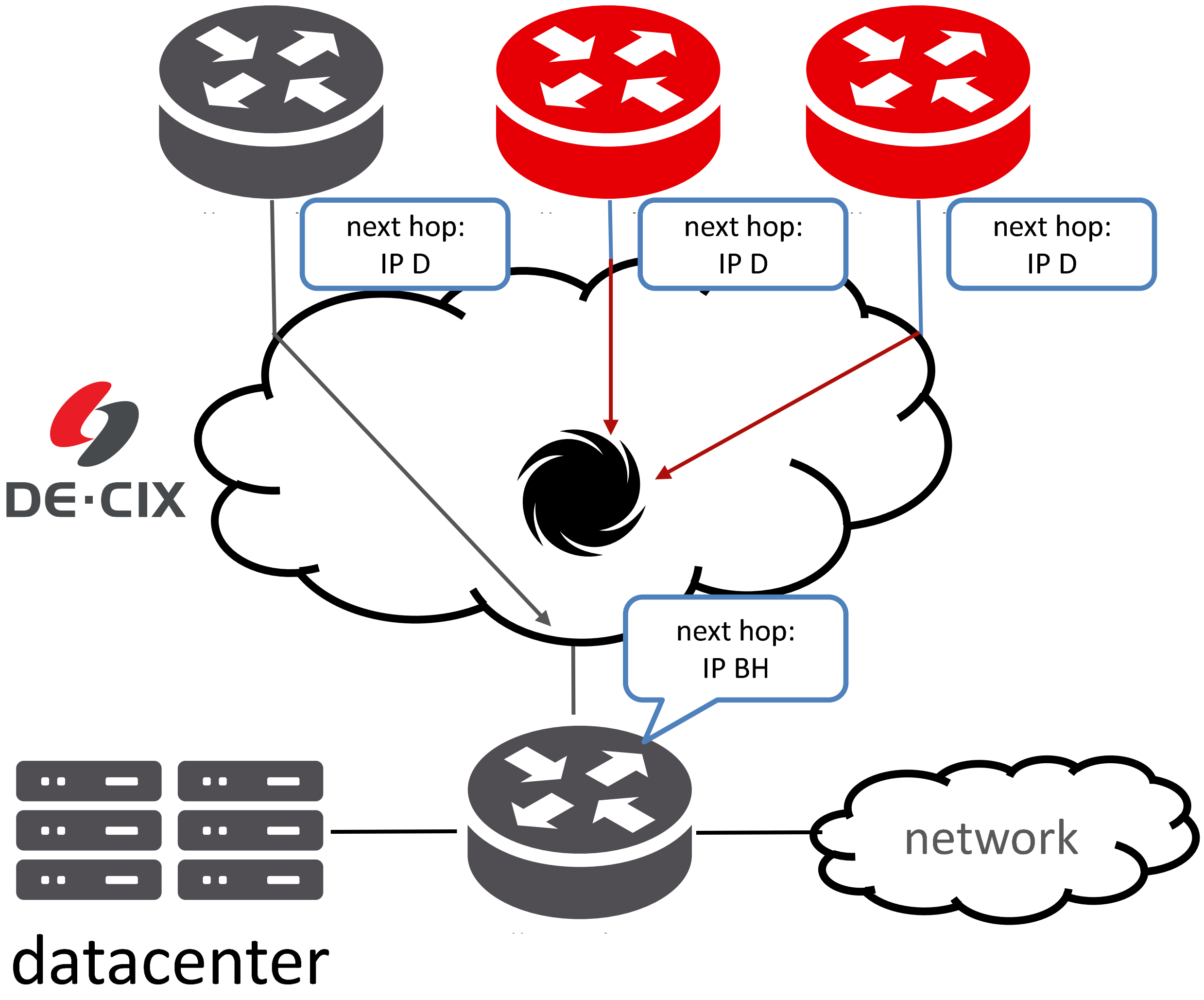
Blackholing – Port and Network Congestion



Blackholing – Announcement



Blackholing – Attack Mitigation



Blackholing – Brief History

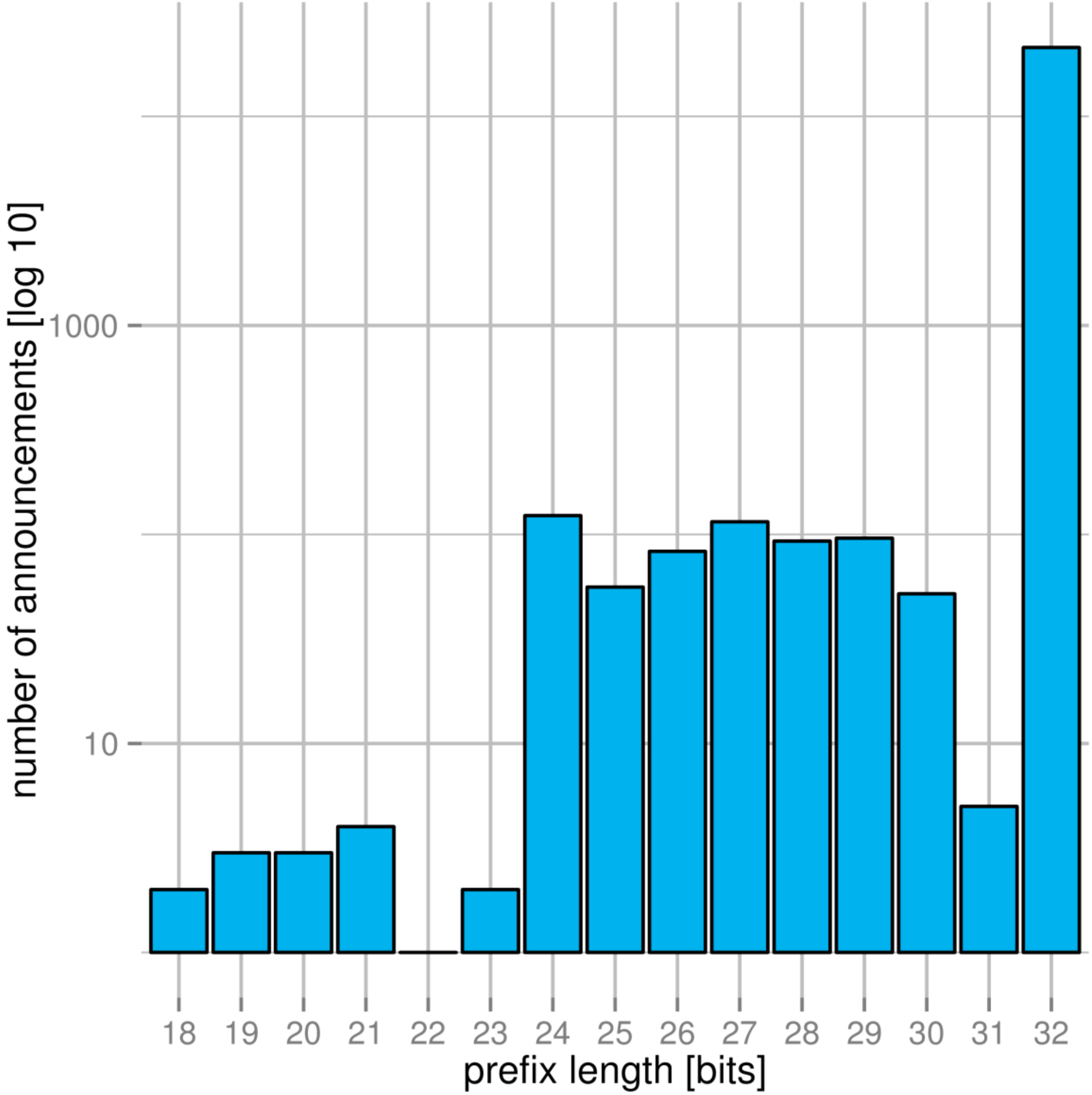
- Late 1980s: used on a per device basis
- 2002: within ASes, see RFC 3882
- 2005 – 2007: major ISPs offer blackholing as a service
- 2009: extended community usage, see RFC 5635
- **2010: First IXPs adopt the concept**

Is it frequently used and how is it used?

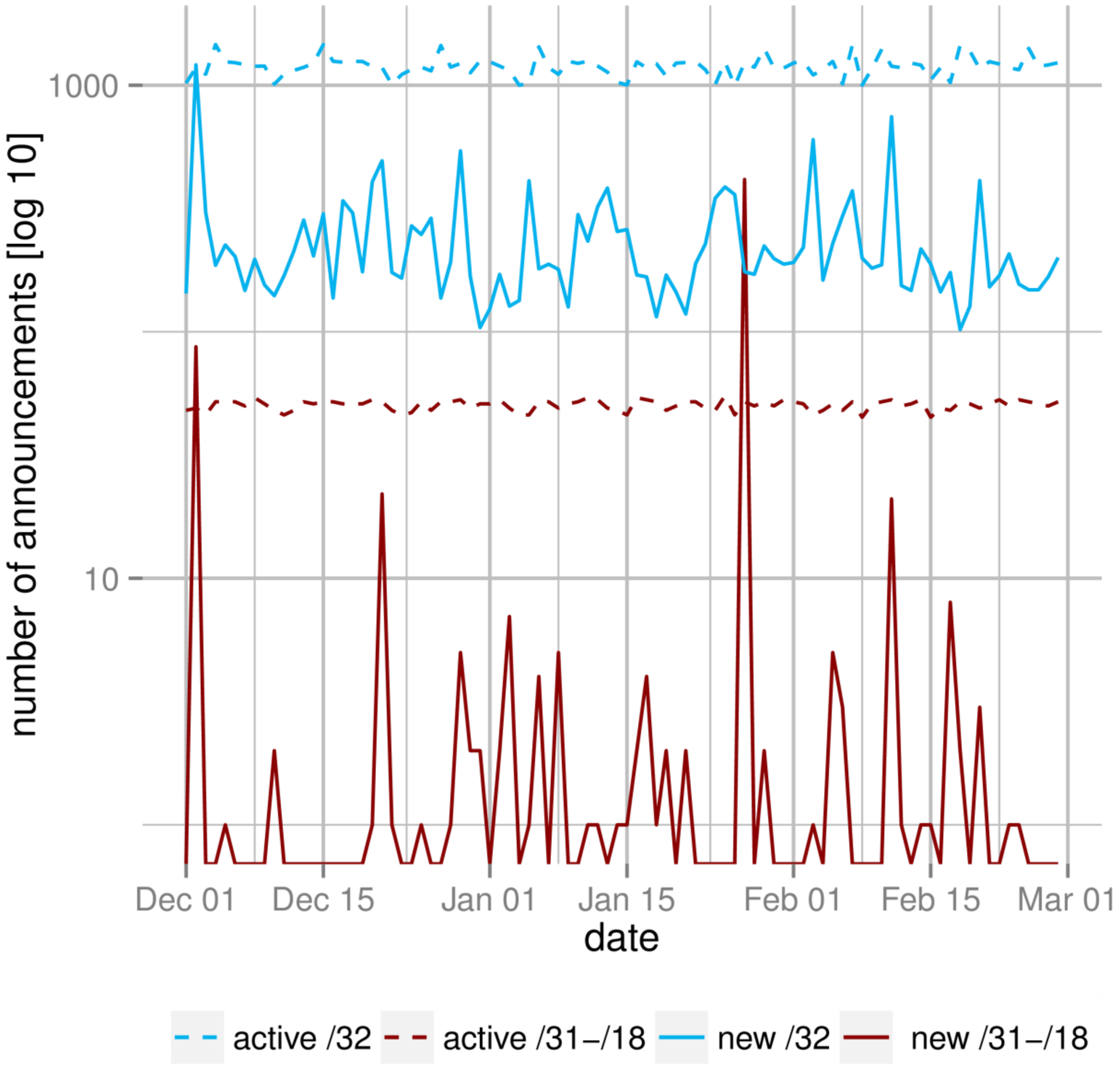
What the impact on traffic? How can we improve blackholing?

Blackholing Usage Analysis – Prefix View I

- » Mainly /32 announcements (97%)
- » /24 - /30 account for 2.5%
- » 9 announcements for < /24
- » **Accept more specifics for blackholing!**



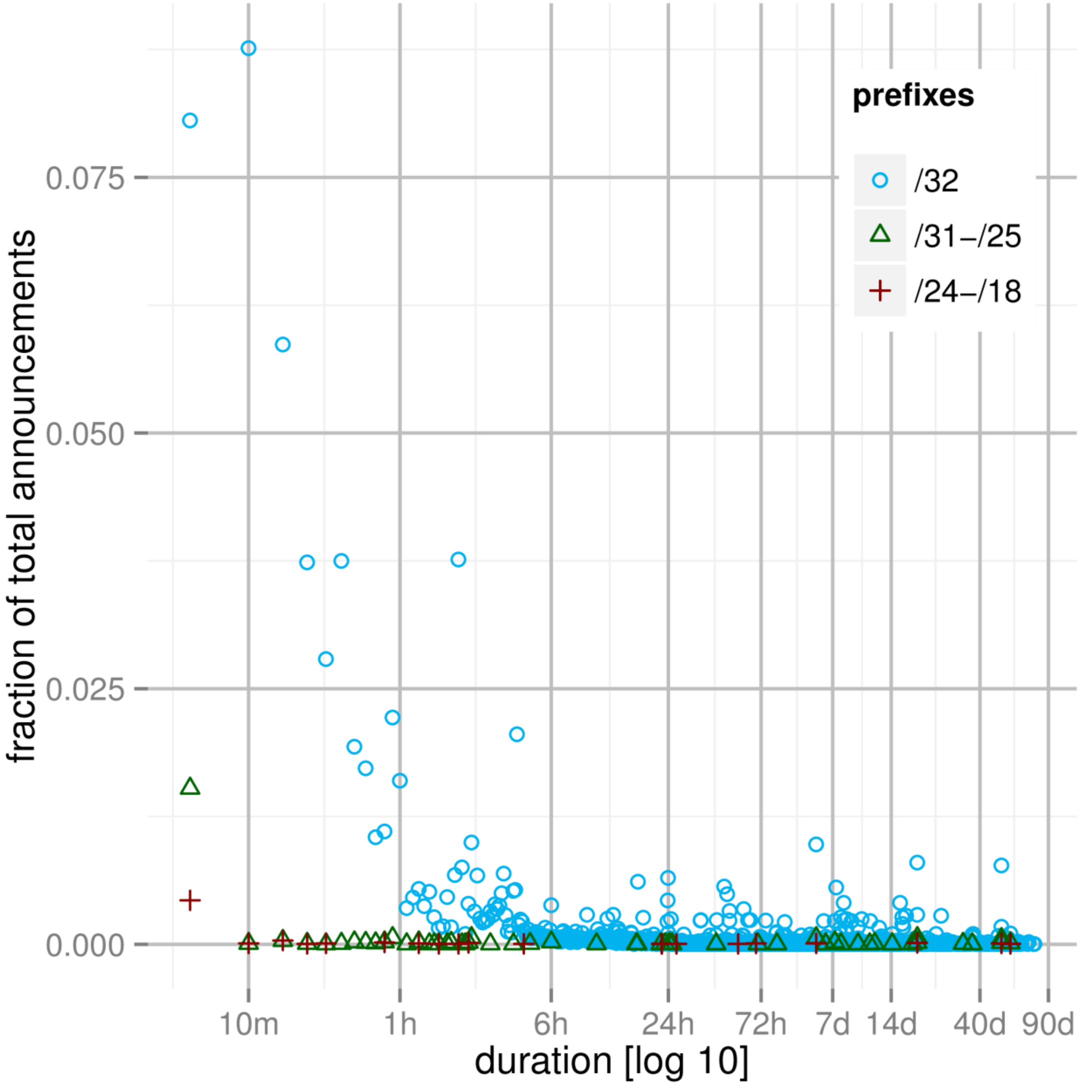
Blackholing Usage Analysis – Prefix View II



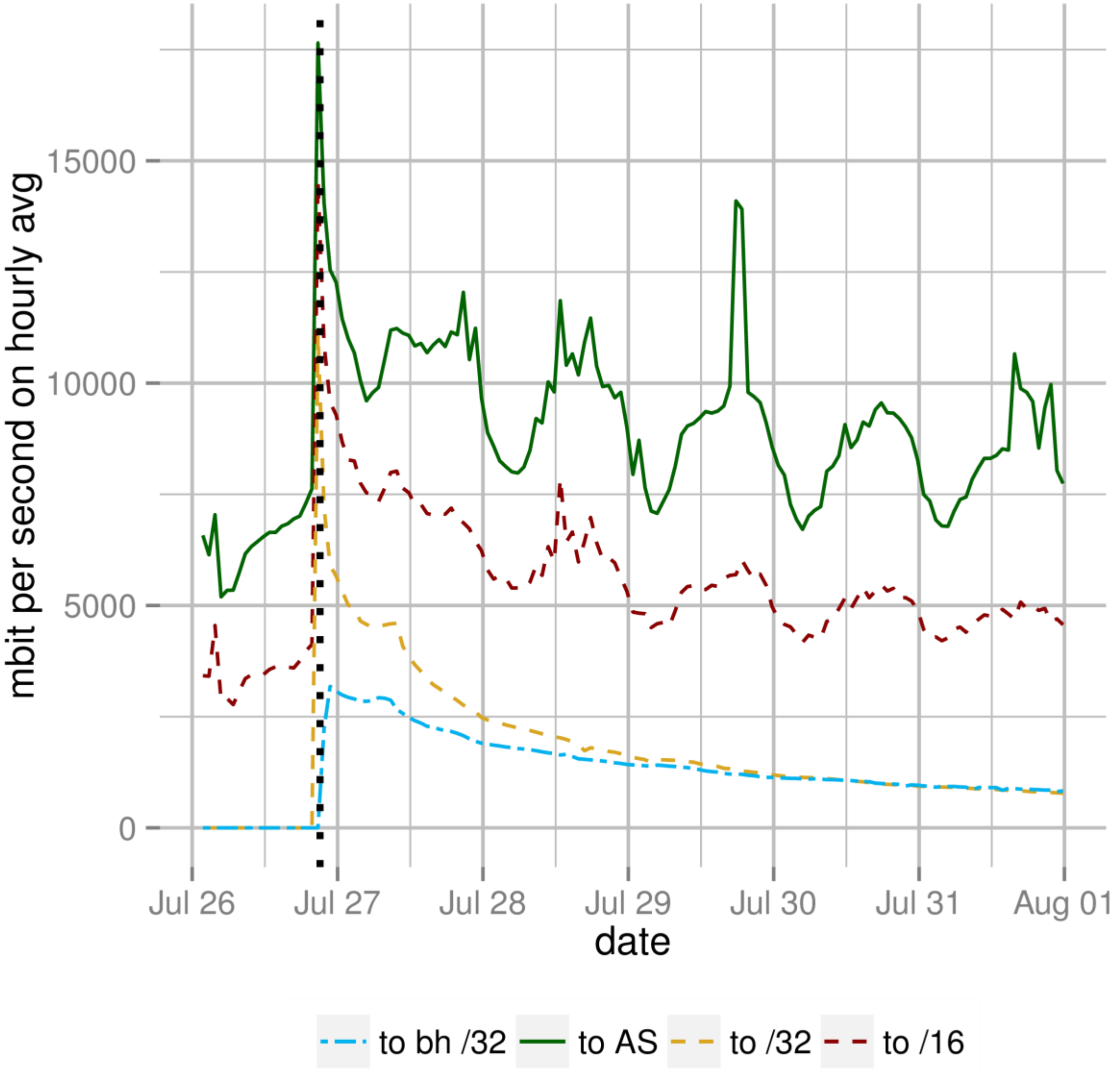
- Stable number of active blackholes
- High variance in new announcements
- Spikey less specifics (/31 - /18)
- **Blackholing is indeed widely used!**

Blackholing Usage Analysis – Prefix View III

- Active duration per prefix by prefix length
- Majority is short-lived (~10% = 5 min)
- Longest observed announcement 76.31 days

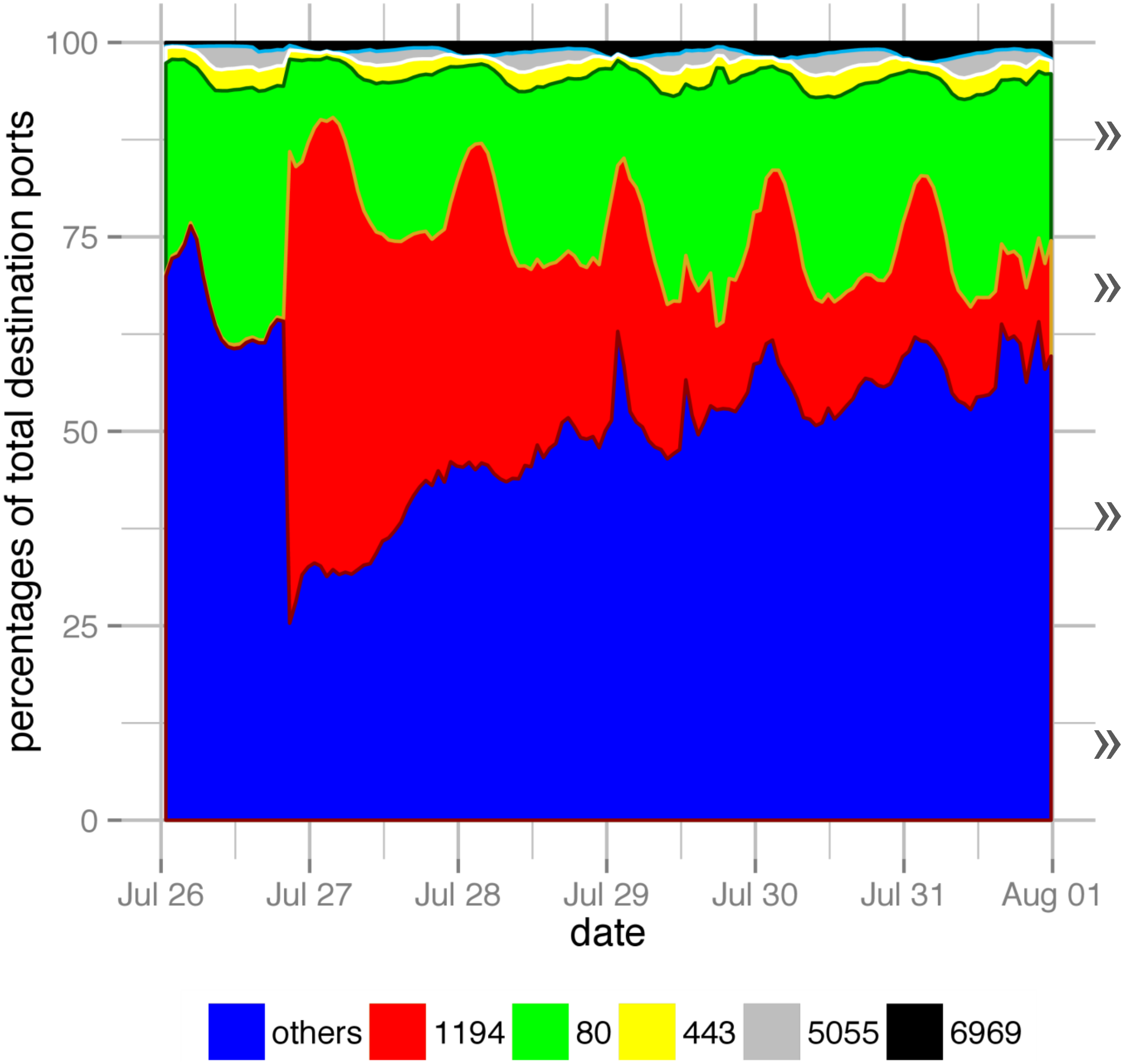


Impact on Traffic - Case Study I



- Traffic for one /32
- Traffic rises after announcement to 17.6 Gbit/s
- Traffic is reduced by one third

Impact on Traffic - Case Study II



» Effectiveness indicator

» Port mix of customer port traffic

» Port 1194 (OpenVPN) share increases to ~50%

» Blackhole takes effect, port mix converges to initial distribution

Summary and Outlook

» 23,000 announced blackholes (over a three month period)

» Least observed specific was a /18

» Stable number of 1200 active blackholes

» Succeeds in mitigating large DDoS attacks

» **Find all details in the paper (to appear next week at PAM’16) [2]**

[2] http://www.net.t-labs.tu-berlin.de/papers/DFK-BIXPO-16.pdf

Standardized Triggering of Blackholing

- Well-defined community for triggering blackholing
- First version of Internet Draft available [3]
- Extended beyond IXPs and more Operational Recommendations added
- Will become RFC status this year

[3] https://tools.ietf.org/html/draft-ymbk-grow-blackholing-01

DE·CIX

Awesome for 20 years

Comments? Questions?

rnd@de-cix.net

Christoph Dietzel

R&D DE-CIX / TU Berlin