# Multi-homing Considerations for DOTS

https://tools.ietf.org/html/draft-boucadair-dots-multihoming-01

Prague, July 2017

M. Boucadair (Orange)
T. Reddy (McAfee)

# Objectives

- **Complete** the base DOTS architecture with multi-homing specifics
- **Identify** DOTS deployment schemes in a multi-homing context
  - Where the upstream transit provider(s) is offering DDoS mitigation service
  - Without recommending any favorite scheme
- **Sketch** guidelines and recommendations for placing DOTS requests in multi-homed networks, e.g.,:
  - Select the appropriate DOTS server(s)
  - Identify cases where anycast is not recommended

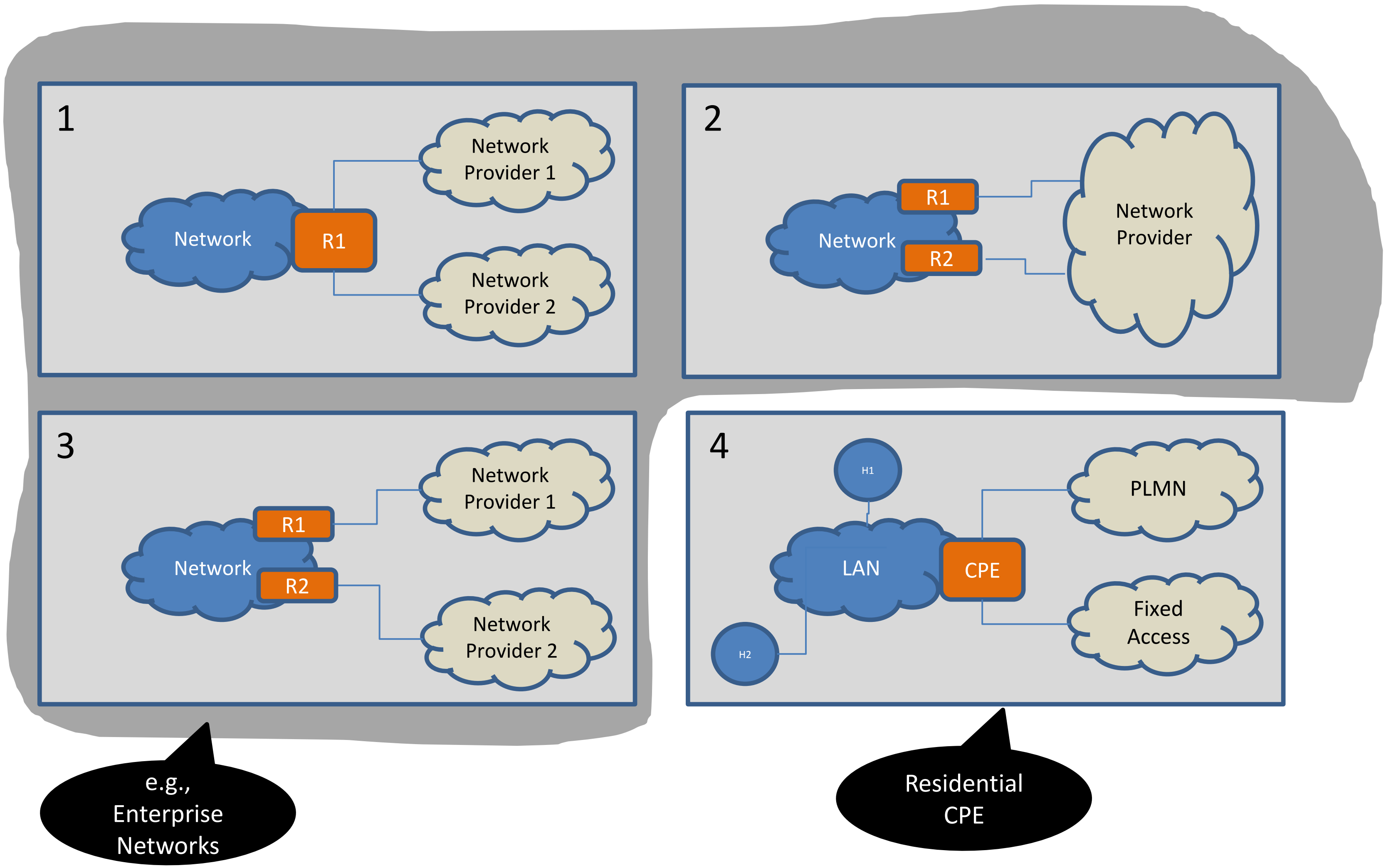
# Why is This Document Needed?

- Send a DOTS mitigation request to an arbitrary DOTS server **won’t help** mitigating a DDoS attack
- Blindly forking all DOTS mitigation requests among all available DOTS servers is **suboptimal**
- Sequentially contacting DOTS servers may **increase the delay** before a mitigation plan is enforced
- Guidance is therefore needed for DOTS client/gateway implementations

# Methodology

- Rely upon draft-ietf-dots-use-case to identify and **extract viable** deployment candidates
- **Augment** the description with multi-homing technicalities, e.g.,
  - One vs. multiple upstream network providers
  - One vs. multiple interconnect routers
  - Provider-Independent (PI) vs. Provider-Aggregatable (PA)
- Describe the **recommended behavior** of DOTS clients and gateways for each case

# Sample Multi-Homing Scenarios

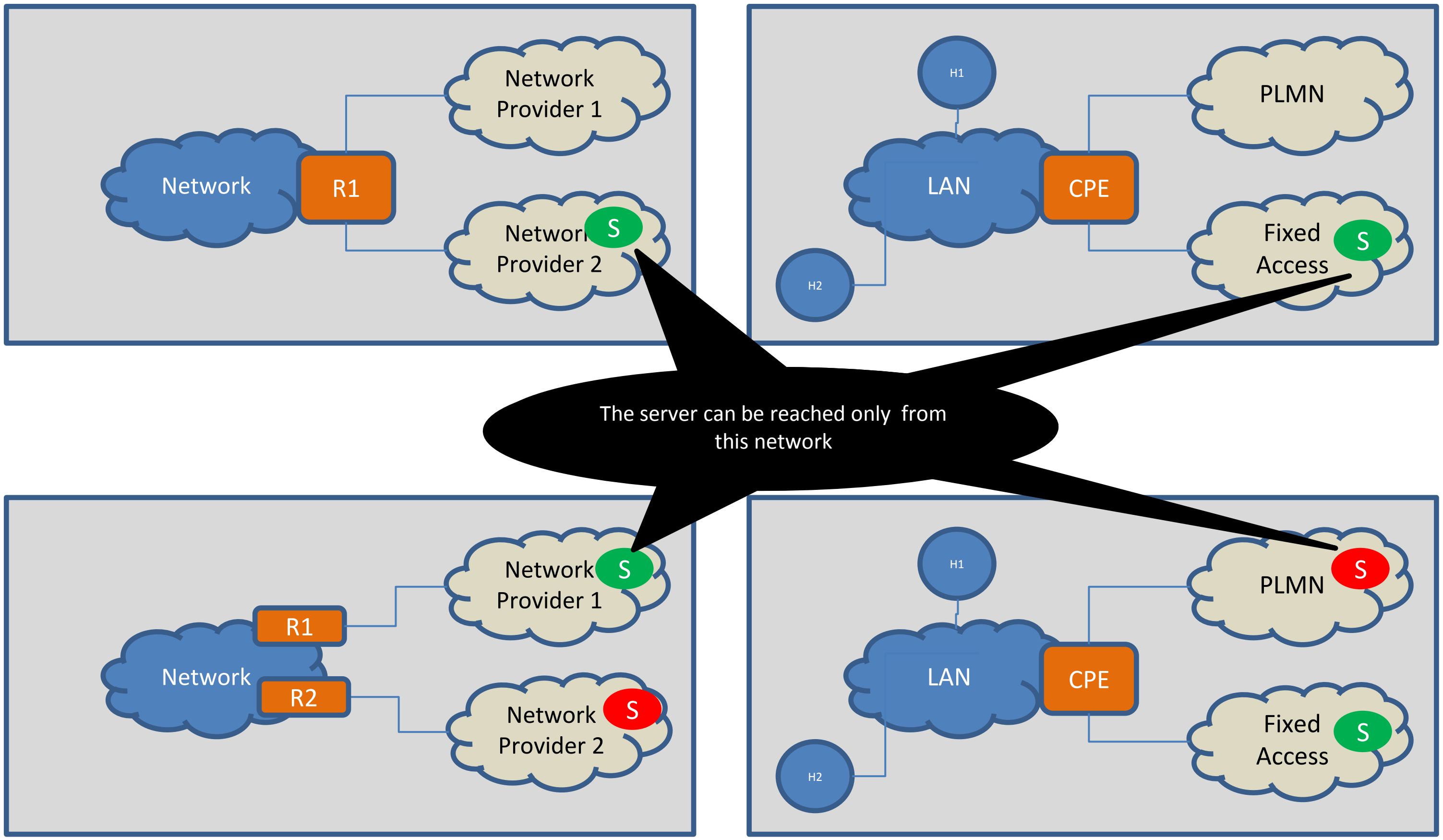


e.g., Enterprise Networks

Residential CPE

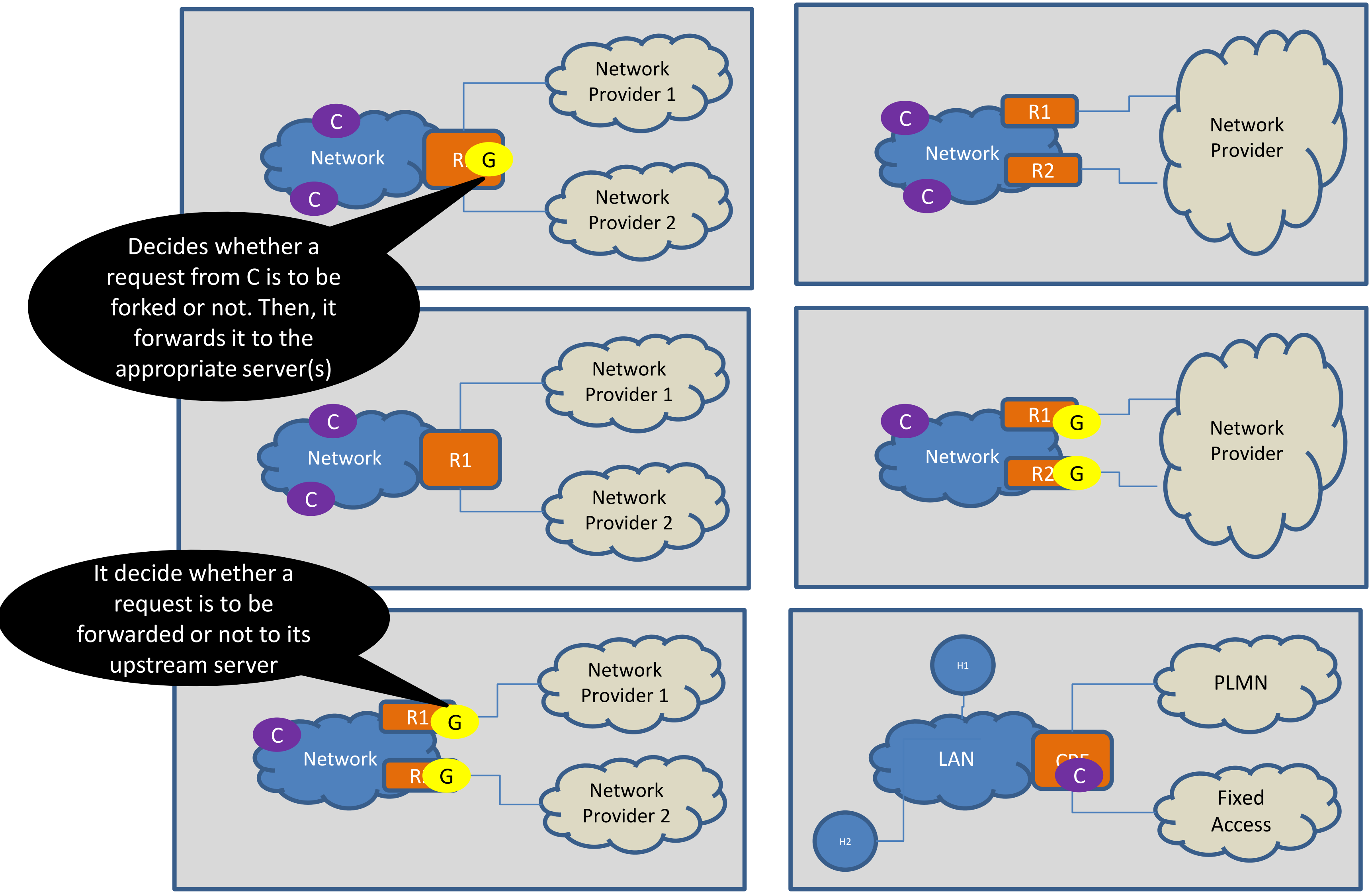
# DOTS in Multi-Homed Networks: Server Side

- DOTS service can be offered by **all** or **a subset** of upstream providers, e.g.,



The server can be reached only from this network

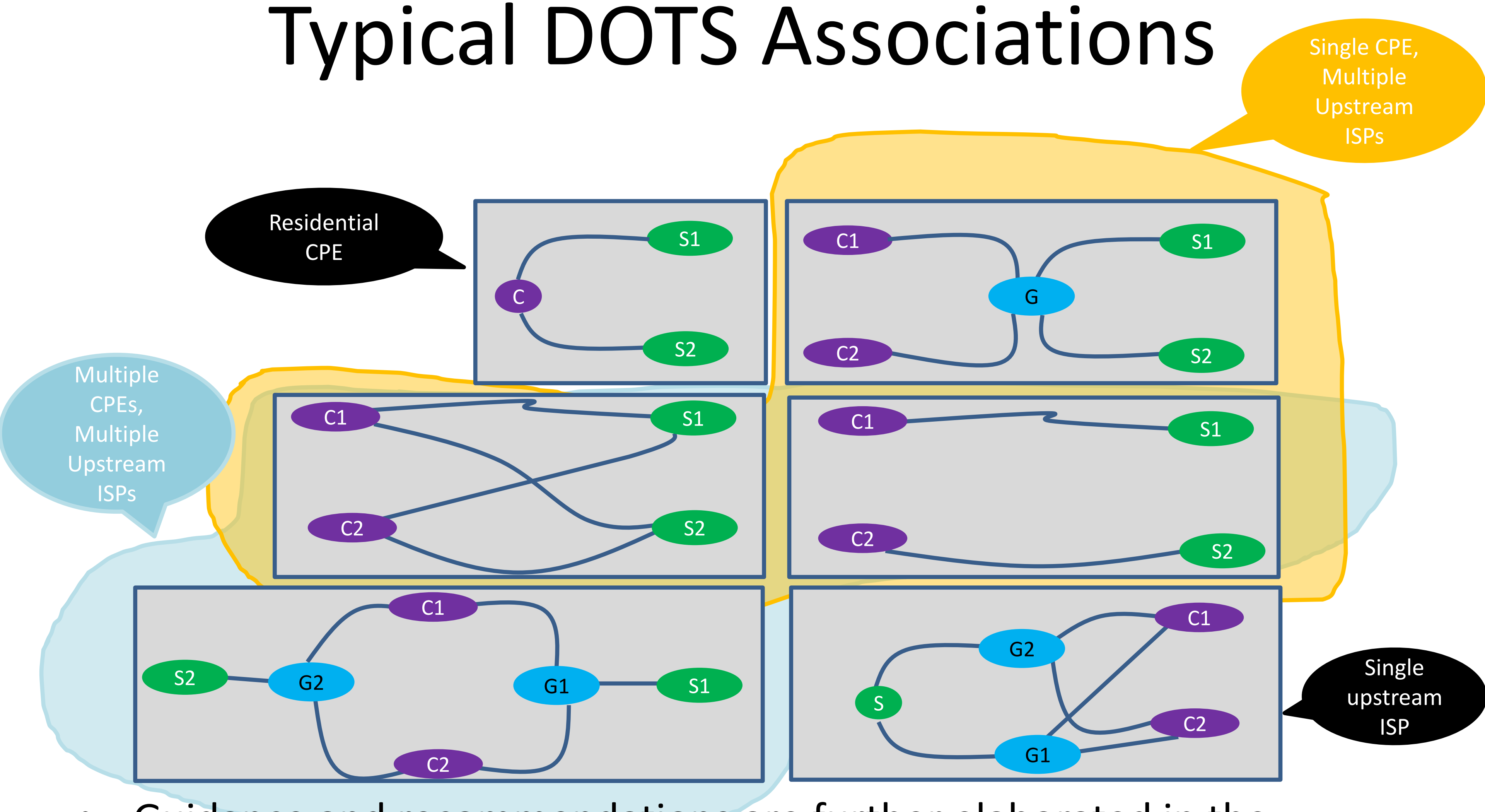
# DOTS in Multi-Homed Networks: Client Side



Decides whether a request from C is to be forked or not. Then, it forwards it to the appropriate server(s)

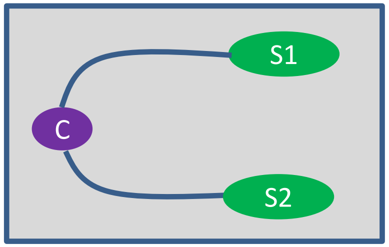
It decide whether a request is to be forwarded or not to its upstream server

# Typical DOTS Associations



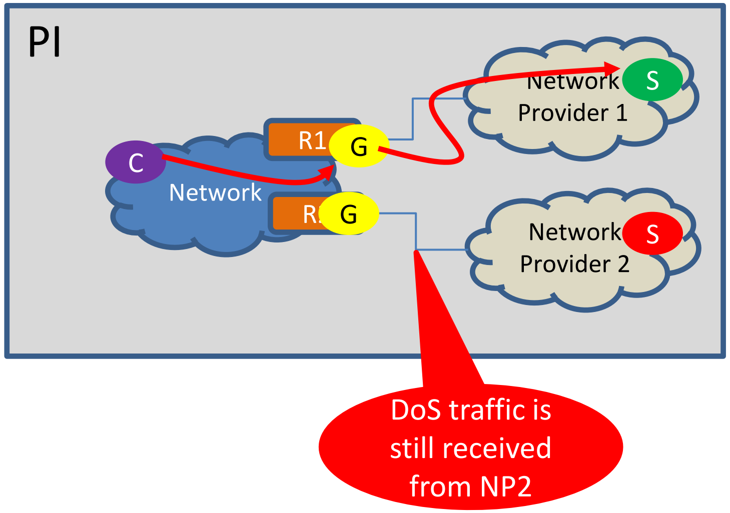
- Guidance and recommendations are further elaborated in the draft…
- See the sample in the next slide

# Sample Recommendations

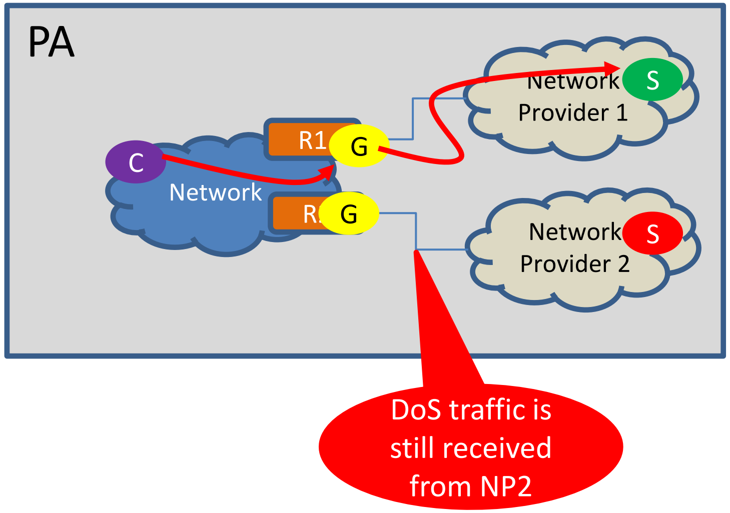


- The DOTS client MUST be able to **associate a DOTS server with each upstream** network
- The DOTS client MUST **resolve the DOTS server's** name provided by an upstream network using the DNS servers learned from **the same network**
- The DOTS client MUST use the **source address selection** algorithm as per RFC6724 to select the candidate source addresses to contact each of these DOTS servers
- DOTS signaling sessions MUST be **established and maintained with each of the DOTS servers** because the mitigation scope of these servers is restricted
- When conveying a mitigation request to protect the attack target(s), the DOTS client among the DOTS servers available **MUST select a DOTS server** whose network has assigned the prefixes from which target prefixes and target IP addresses are derived

# Samples where Anycast is not Recommended



DoS traffic is still received from NP2



DoS traffic is still received from NP2

# Next Steps

- Contributions are welcome
- Consider adopting this document as a WG to complement the DOTS Architecture
- Questions?