GÉANT
Networks • Services • People

DDoS Mitigation

Keeping the Business Open

Klaus Möller (orig. Tobias Dussa)
WP8-T1

Webinar, 15th of February 2022

Public

www.geant.org

Game Plan

- Things you can do to defend yourself
- Things others can do to help you
- Some further musings
- Questions/discussion/open mike session

Red Alert, Shields Up!
What You Can Do When Under Attack

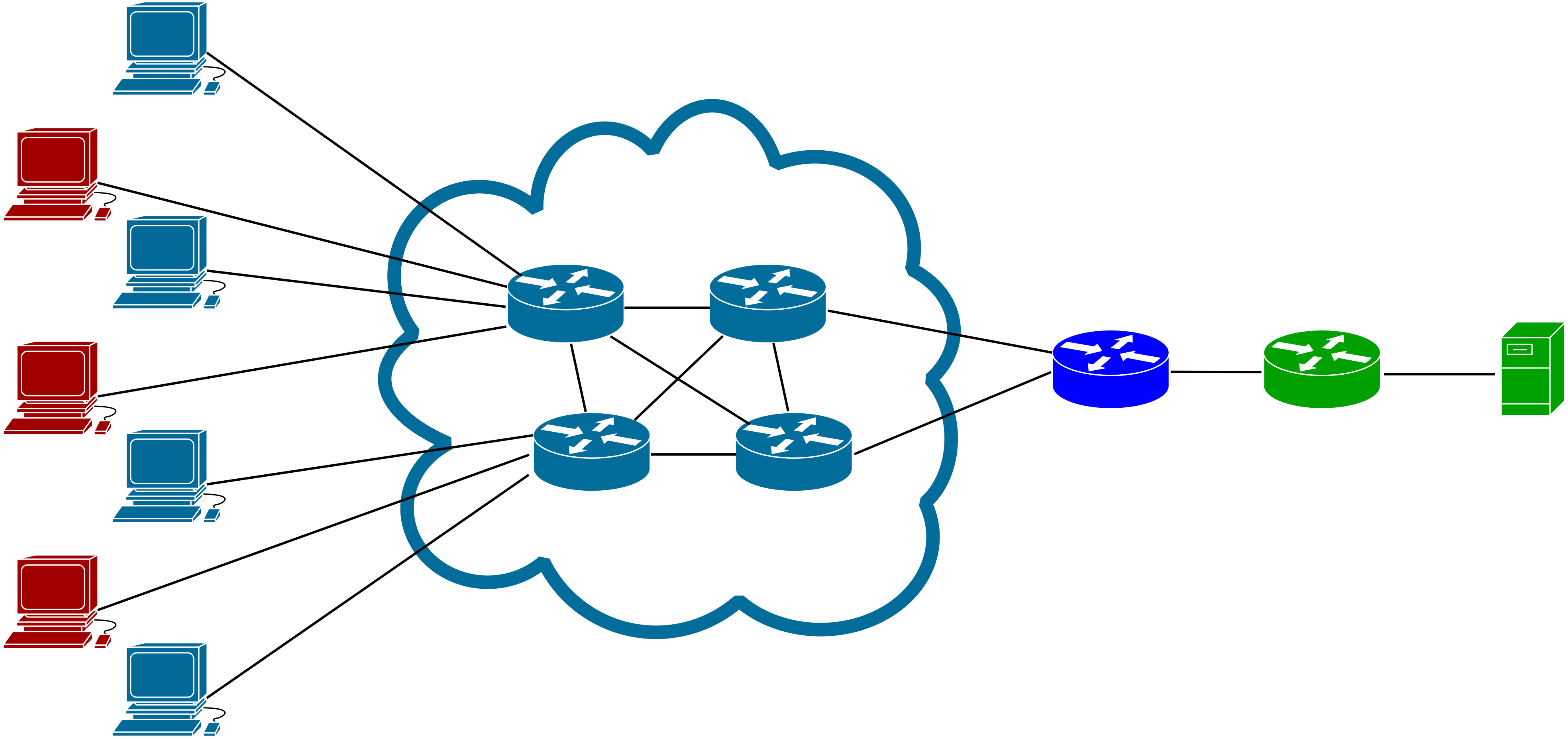
www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

Quick Recap

- A Denial-of-Service (DoS) attack **denies** the **normal usage** of a **service**
- A *Distributed* DoS attack is a DoS attack simultaneously coming from many sources
- For this talk, we assume **you** are running the victim service
- … and have decided you are under attack

General DDoS Overview



What Exactly Is Attacked?

There are many ways to DoS a service. Potentially attacked components include:

- Applications and application resources
- systems and system resources
- network components and resources
- network information
- metadata/prerequisite data

Note: Many of these are not under your control!

How to Respond?

- In order to apply an effective countermeasure, it is necessary to identify the layer that is actually being attacked!
- For a given attack, there may be a number of effective countermeasures on a variety of levels
- Most countermeasures require preparation, and all countermeasures are easier to implement with preparation

Applications and Application Resources

In some ways the easiest to defend against:

- Best chance of truly understanding traffic
- Most targeted attack, therefore little collateral damage in technical terms

Possible problems:

- Application code not under your control
- Application protocol set in stone
- Legitimate-looking traffic hard to separate

Applications and Application Resources – Cont’d

Possible courses of action:

- Make sure the service is appropriately sized (number of threads, buffer sizes and so on)
- Start additional service instances
- Restrict or rate-limit access
- Restrict the service level

Systems and System Resources

Require similar, but more generic defense:

- Concepts apply to many target services
- “Only” general systems insight necessary
- ~~No~~ less need to worry about nitty-gritty service details

Possible problems:

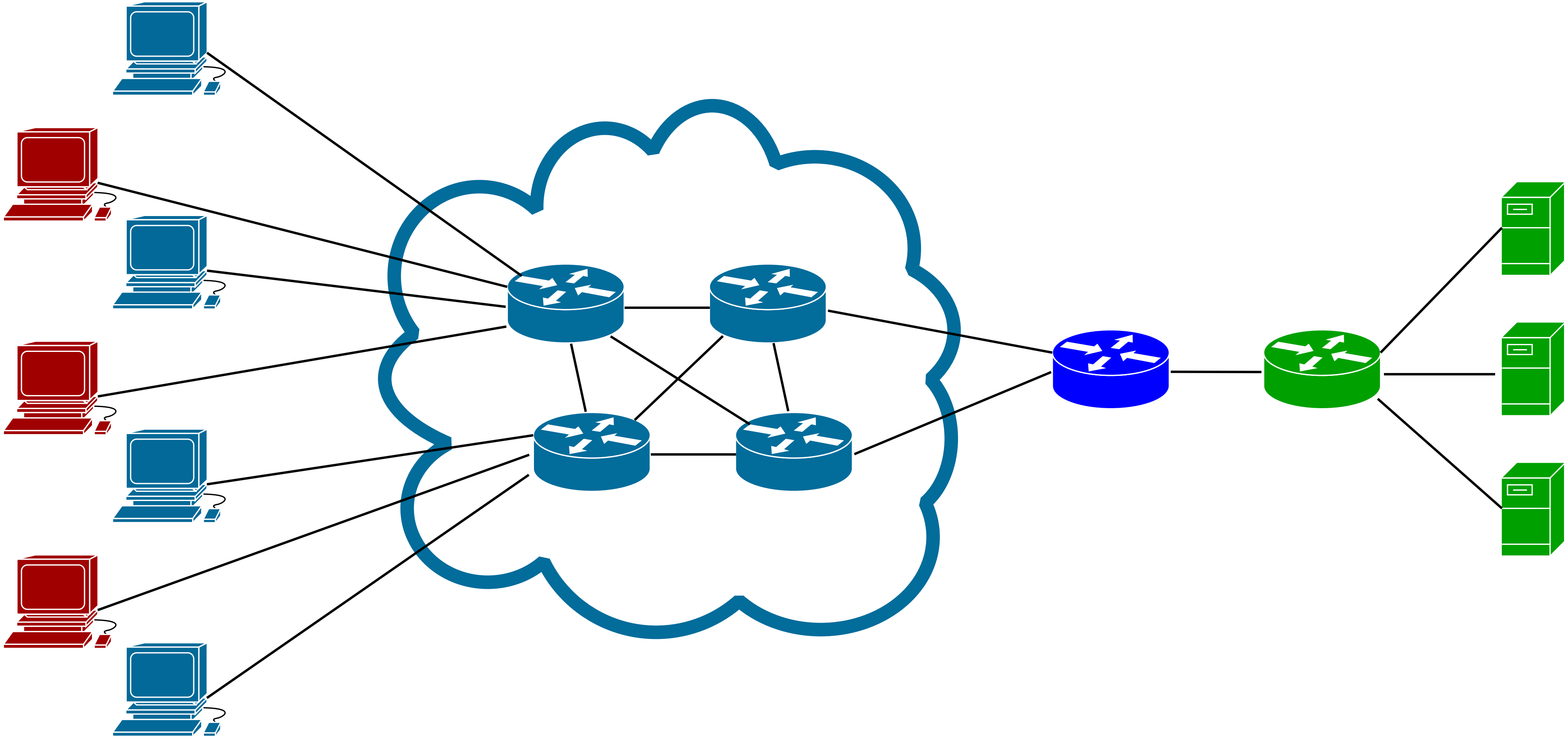
- Less insight into what is happening
- if systems themselves are hit, deploying countermeasures might be hard

Systems and System Resources – Cont'd

Possible courses of action:

- Make sure the system is properly sized (CPU, RAM, HDD, sockets)
- Start additional system instances (potentially at backup site)
- Restrict or rate-limit traffic (e. g., the number of TCP connections)
- Restrict service level

Local Mitigation



Network Components and Resources

Defense on this level is a different game and very problematic:

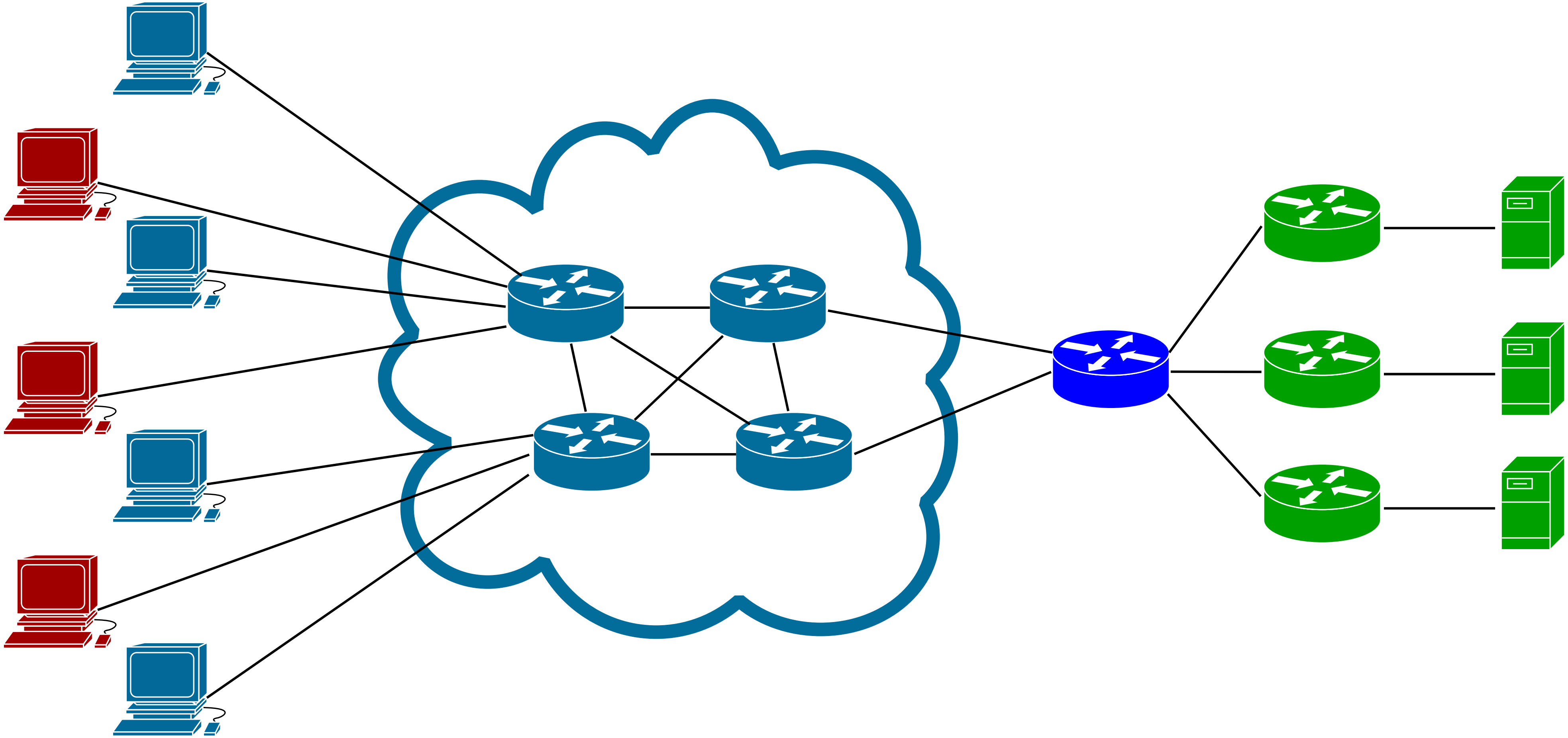
- Adding networking resources or components ad-hoc is often very hard or impossible
- Attacks often take down entire sites, severely limiting response capabilities
- Collateral damage is often substantial
- Affected components or resources only partially under your control, if at all!

Network Components and Resources – Cont’d

Possible courses of action:

- Restrict or rate-limit traffic (e. g., the rate of inbound ICMP packets)
- Move service to backup site with different address and update DNS etc.
- Ask your ISP (or upstream entity) for help

Off-Site Mitigation



Network Components and Resources – Cont'd Cont'd

What if you **are** the ISP/upstream entity?

- Blackhole traffic as far upstream as possible.
- If possible, based on traffic sources; if necessary, based on traffic destination.

Network Information

If someone manages to attack this successfully, there is almost certainly not a whole lot you can do about it:

- Routing and peering information is done outside of your control.
- … unless you are running your own Autonomous System, in which case you should already know what to do.

Network Information – Cont'd

Possibly courses of action:

- Contact your ISP or upstream entity for help.

If you are the ISP/upstream entity: Fix/reclaim your BGP advertisements and peering info.

Metadata/Prerequisite Data

This is somewhat of a “catch-all” category. What you can sensibly do depends a lot on what exactly has been attacked:

- Services you depend on but that are outside your control (e. g., most of DNS, OCSP, NTP) or
- services you depend on that *are* under your control (e. g., some DNS, LDAP, Kerberos).

Metadata/Prerequisite Data – Cont'd

Possible courses of action:

- If the service that is not available is outside of your control: Contact the service provider and tell them they have a problem. (Although they will likely know this already.)
- Otherwise, go fix your own service.
- Or, indeed, **have** your own service – for instance, a local NTP server.

Radio for Backup - How Others Can Help You

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

ISP/Upstream Entity

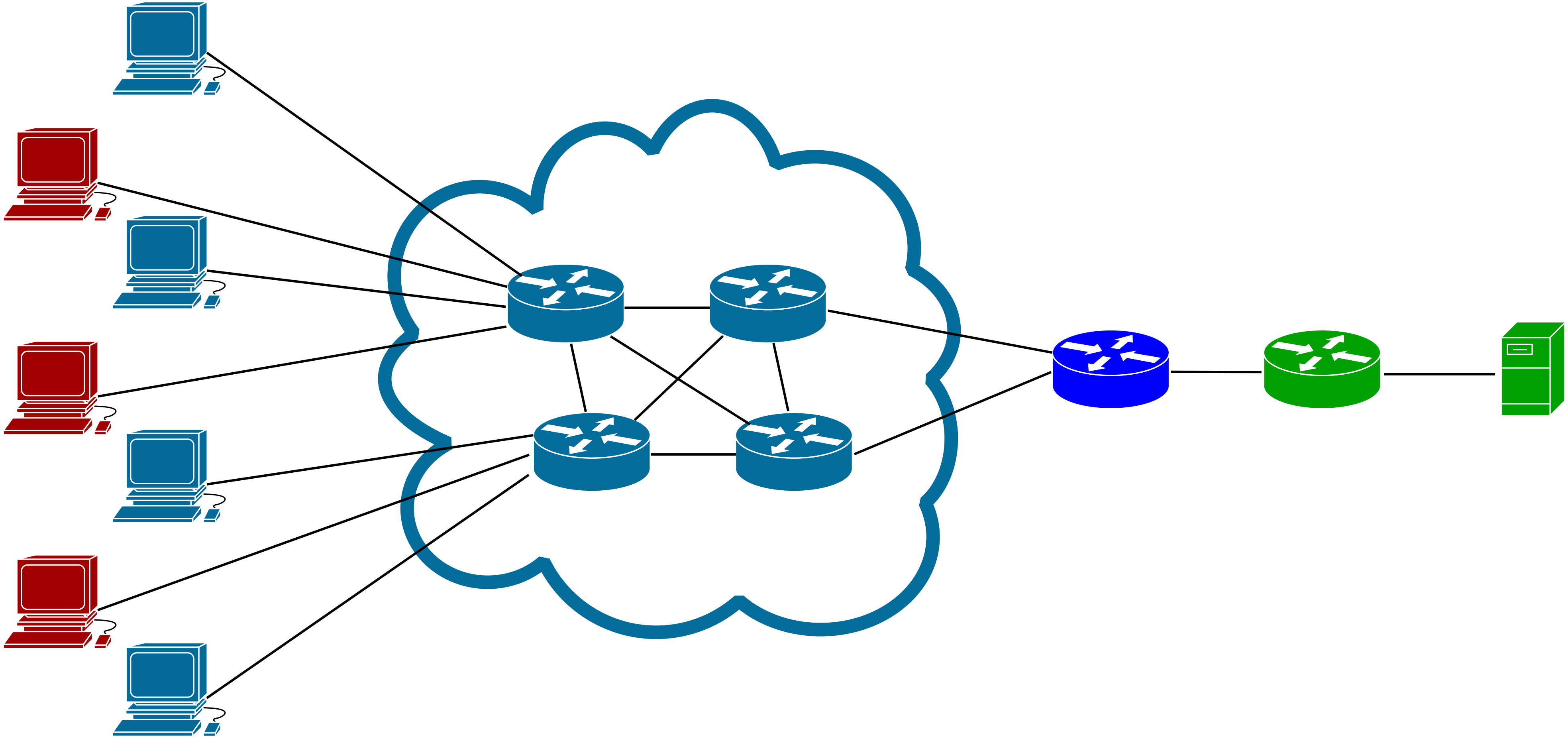
Uniquely, your ISP can blackhole traffic **before** it becomes a problem for your uplink

- Blackhole routing is the name of the game
- Preferably as much upstream as possible
- This will likely take the victim service offline
- … from the outside, that is
- Furthermore, key connections might even be kept “open” with static explicit routing

ISP/Upstream Entity – Cont'd

- Much easier if you have discussed this beforehand with your ISP
- Having a prepared emergency backup instance of the victim service off-site also helps

Blackhole Routing



DDoS Mitigation Providers

Commercial companies that offer “cleaning” of network traffic. Two flavors: Always-on and On-demand

- Always-on: All traffic is permanently routed through the mitigation provider resources. Adds latency because of longer routes
- On-demand: Traffic is re-routed through mitigation provider resources when an attack is detected. Takes a bit of time to switch over, and mitigation provider might be bypassed by a clever attacker

Either flavor must be established beforehand

Content Delivery Networks

Content Delivery Networks (CDNs) provide decentralized service delivery

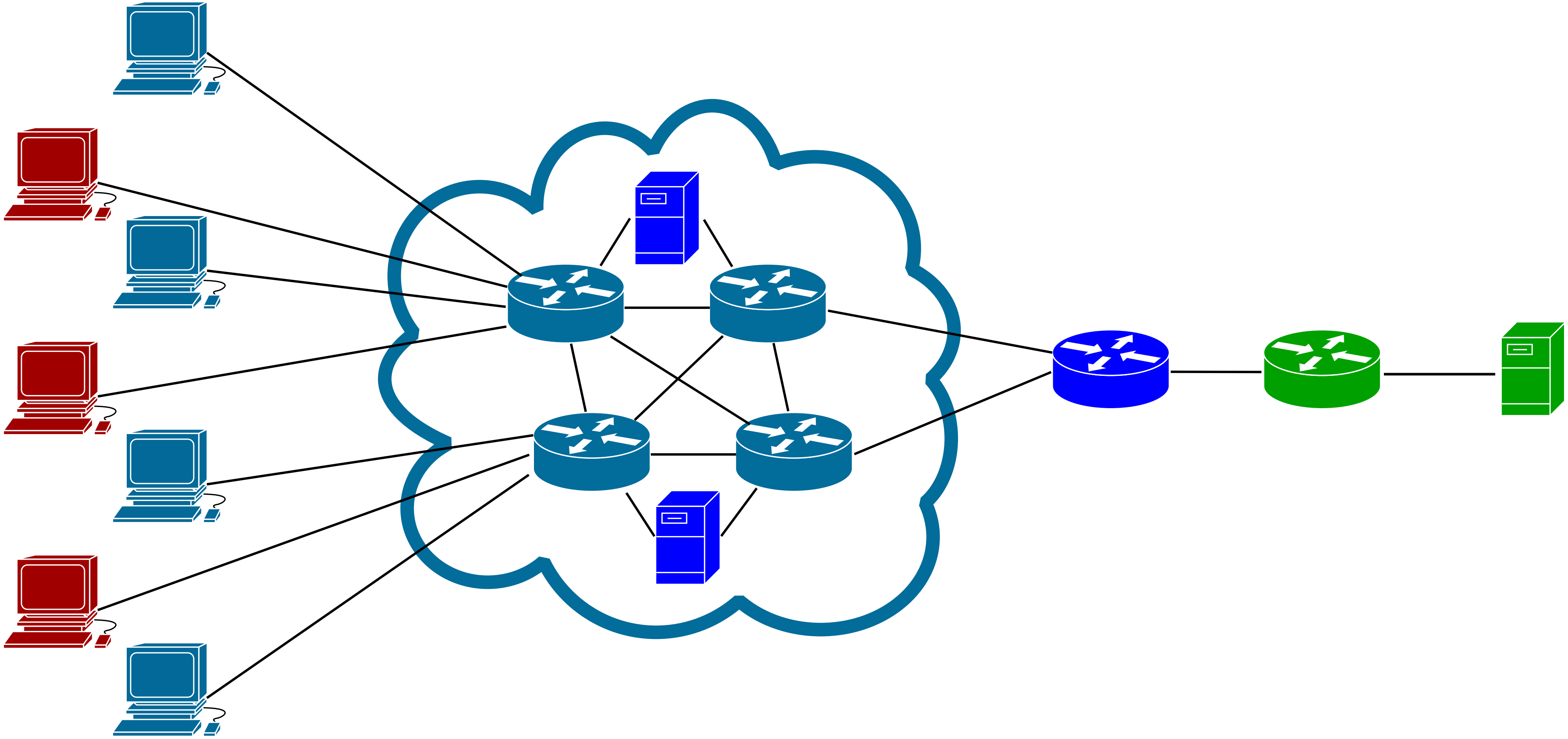
- Primary benefit are quicker deliveries because the CDN servers are “closer” to the client, topologically speaking
- But this also means that it is very hard to attack the service as a whole because there are a lot of delivery endpoints
- Only helps if deployed beforehand

Security Teams

Depending on the context and attack details, external security teams might be able to help:

- Insight into botnet operations
- ability to contact third parties
- assistance in incident coordination

DDoS Mitigation Provider/CDN



DFN DEUTSCHES FORSCHUNGSNETZ DFN CERT

Miscellaneous Observations

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union’s Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).

Every Bit Helps

- It is crucial to be able to start working again. Working with your ISP/upstream entity to restore connectivity to your most important communications partners goes a long way
- So does restoring local basic service so that people can start working again internally
- Also realize that losing internet connectivity means losing VoIP telephony!

Be a Good Neighbor

Successfully defending yourself on your own is **very** hard, if not impossible. It is key that everybody keeps their own turfs clean, especially when not under attack, so that DDoS attacks are made as difficult as possible

- Monitor outbound traffic for bots
- Be sure not to be a reflector/amplifier
- Consider rate-limiting outbound ICMP traffic

Keep the Right People in the Loop

Remember that one of the goals of a DDoS attack is likely to make the target (presumably you) look bad.

If you are attacked, your public reaction is key

- This means that your PR people should probably be briefed on what is happening
- Also consider informing users of the problem so they do not have to guess what is wrong

Collaborative Effort

- Successful DDoS mitigation is a team effort that cannot be pulled off by the victim alone
- The deliberate distribution and dislocation of the attack means that many players are potentially involved

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

© GÉANT Association on behalf of the GN4 Phase 2 project (GN4-2).
The research leading to these results has received funding from
the European Union's Horizon 2020 research and innovation
programme under Grant Agreement No. 731122 (GN4-2).