BACKGROUND

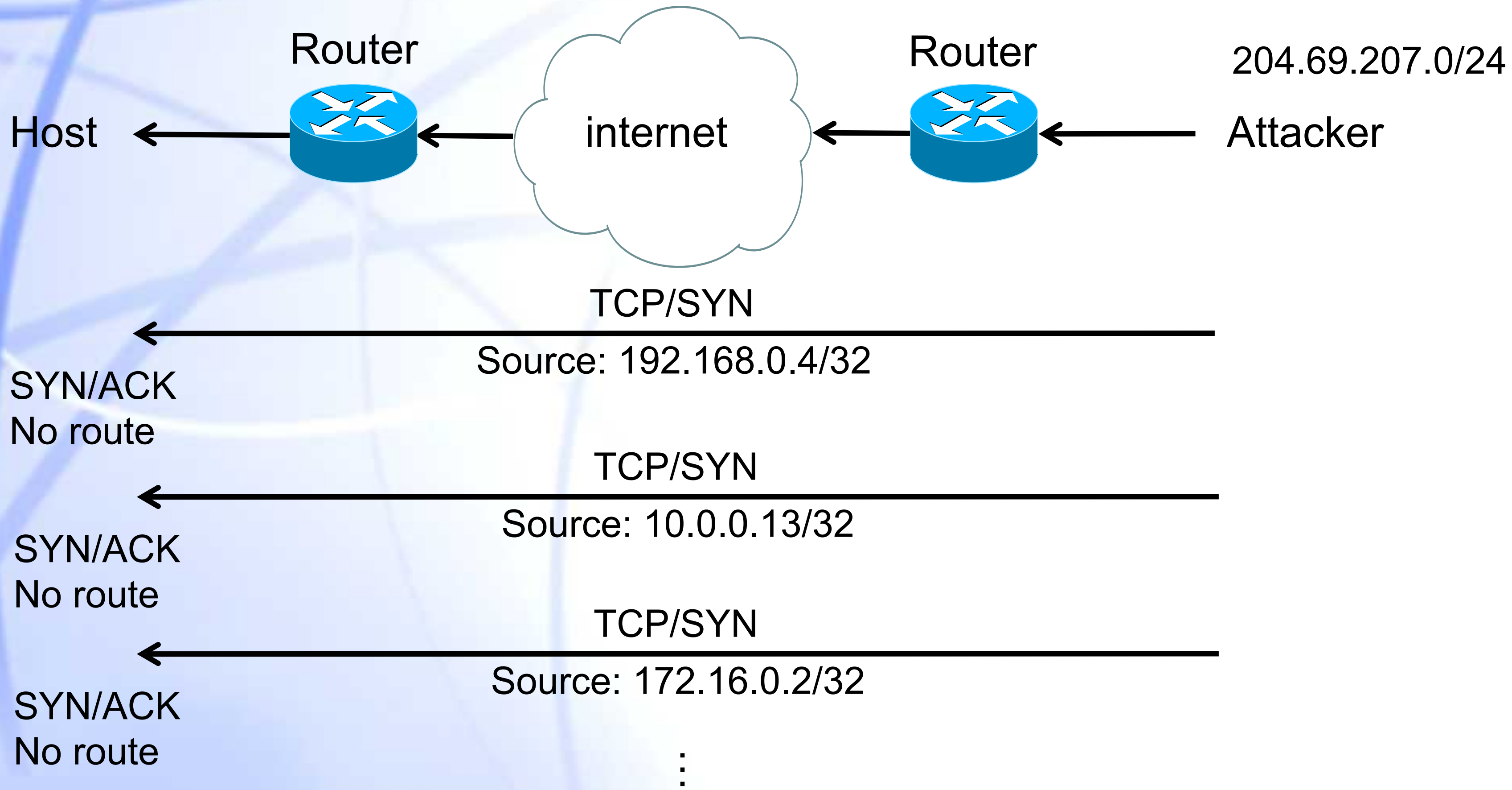
Preliminary filter-based solutions

Ingress filtering

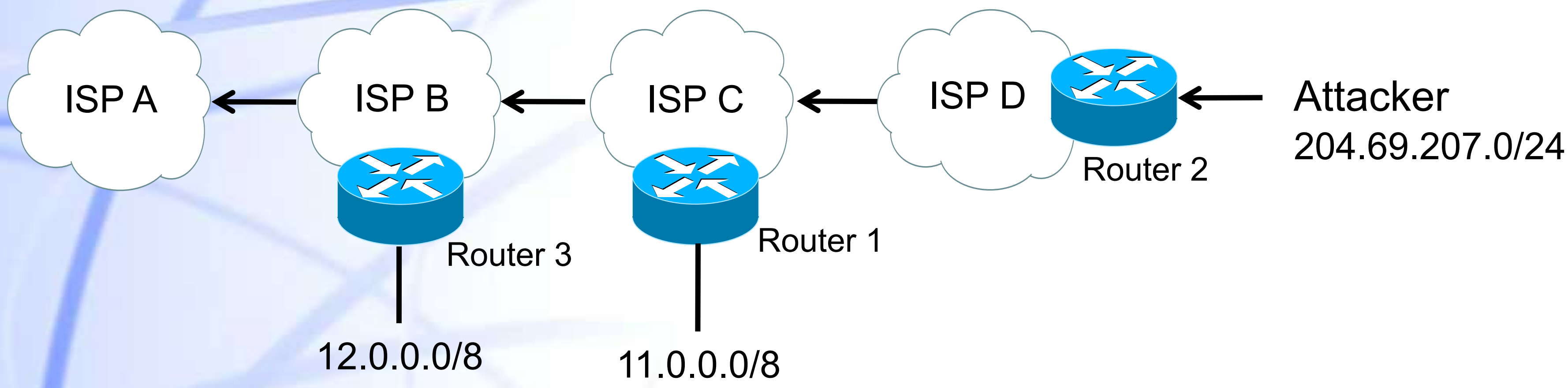
- **Defined in RFC 2827:**
  - **P. Fergusson, D. Senie. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP source address Spoofing*. May 2000**
- **Introduces source address filtering at the network ingress**
  - **Objective: to prohibit DoS attacks which use forged IP addresses**

Ingress filtering (II)

- **TCP SYN flooding attack:**



Ingress filtering (III)



An ingress filter on “Router 2” would check:

IF packet‘s source address from within 204.69.207.0/24
THEN forward as appropriate

IF packet’s source address is anything else
THEN deny packet

Ingress filtering (IV)

- **Drawbacks:**
  - **It becomes effective only with a high degree of deployment**
  - **Source addresses can be spoofed within the network prefix**
  - **It does not prevent attacks that comprise non-spoofed packets**

Traceback

- **Allows to identify the hosts responsible for an attack:**
  - **S. Savage, D. Wetherall, A. Karlin, and T. Anderson. Practical Net- work Support for IP Traceback. In *Proc. ACM SIGCOMM 2000.***
  - ***A. Snoeren, C. Partridge, L. Sanchez, C. Jones, F. Tchakountio, S. Kent, and W. Strayer. Hash-Based IP Traceback. In Proc. ACM SIGCOMM 2001.***
- **Drawbacks:**
  - **Does little to prevent sources from sending traffic**
  - **Once the malicious hosts are identified, it may be too late to prevent the attack**
  - **Limited use in determining the ultimate perpetrators of the attack**

Pushback

- **Defined in:**
  - ***R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker. Controlling High Bandwidth Aggregates in the Network. Computer Communications Review, 32(3), July 2002.***
  - J. Ioannidis and S. Bellovin. Implementing Pushback: Router-Based Defense Against DDoS Attacks. In *Network and Distributed System Security Symposium, 2002.*
- **Motivation:**
  - **Internet is vulnerable to DoS attacks and flash crowds**

Pushback (II)

- **Flash crowd:**
  - **A large number of users try to access the same server simultaneously**
  - **Apart from overloading the server, network links can also be overloaded**
  - **Triggered by sudden events of great interest**
    - ✓ **Links from popular web sites (i.e. Slashdot effect)**
    - ✓ **Breaking news stories**

Pushback (III)

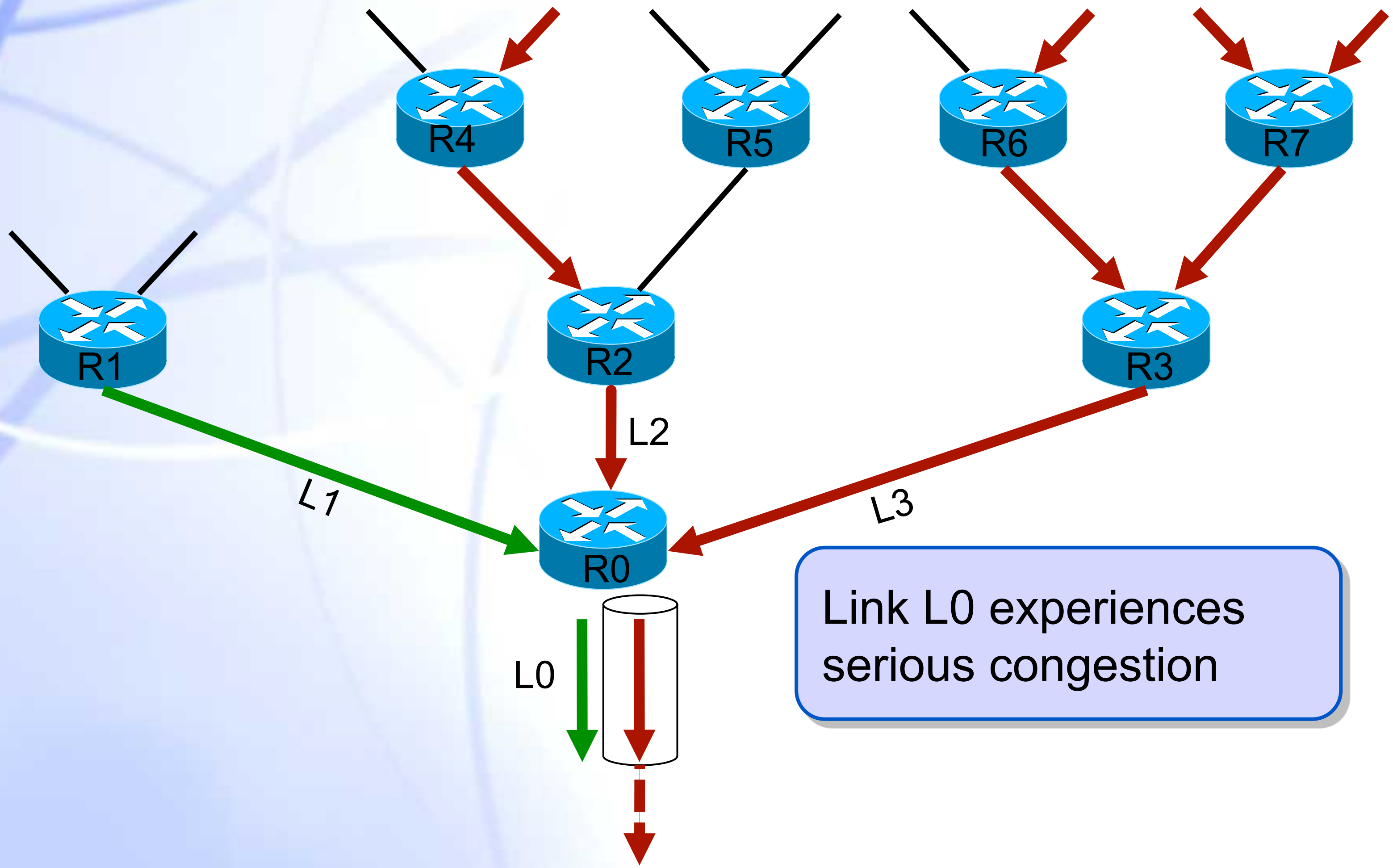
- **In DoS attacks and flash crowds,**
  - **congestion is due to a well-defined subset of the traffic, i.e. an <u>aggregate</u>**
- **<u>Aggregate</u>:**
  - **Collection of packets from one or more flows with some common property:**
    - ✓ **Destination or source address prefix,**
    - ✓ **application type (e.g. streaming video),**
    - ✓ **TCP SYN packets, etc.**
- **The paper proposes mechanisms to detect and control high bandwidth aggregates:**
  - **Local ACC (Aggregate-based Congestion Control)**
  - **Cooperative pushback**

Pushback (IV)

- ACC mechanisms are triggered when a link experiences sustained severe congestion
- Local ACC:
  - Detects and controls aggregates at a single router
  - Consists of two algorithms:
    - ✓ Identification of high bandwidth aggregates
    - ✓ Rate-limit the identified aggregates

Pushback (V)

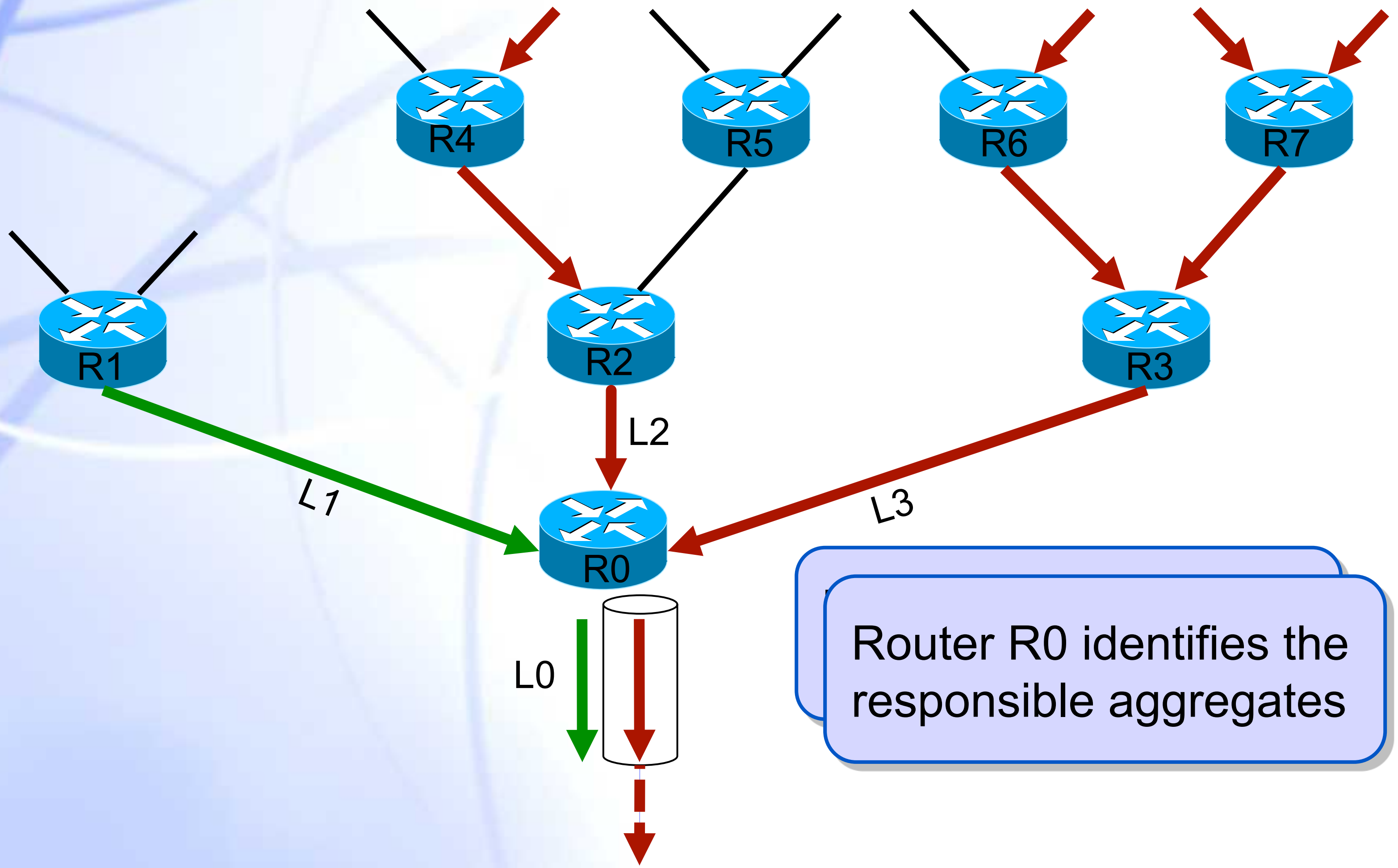
- **Local ACC: example**



Link L0 experiences serious congestion

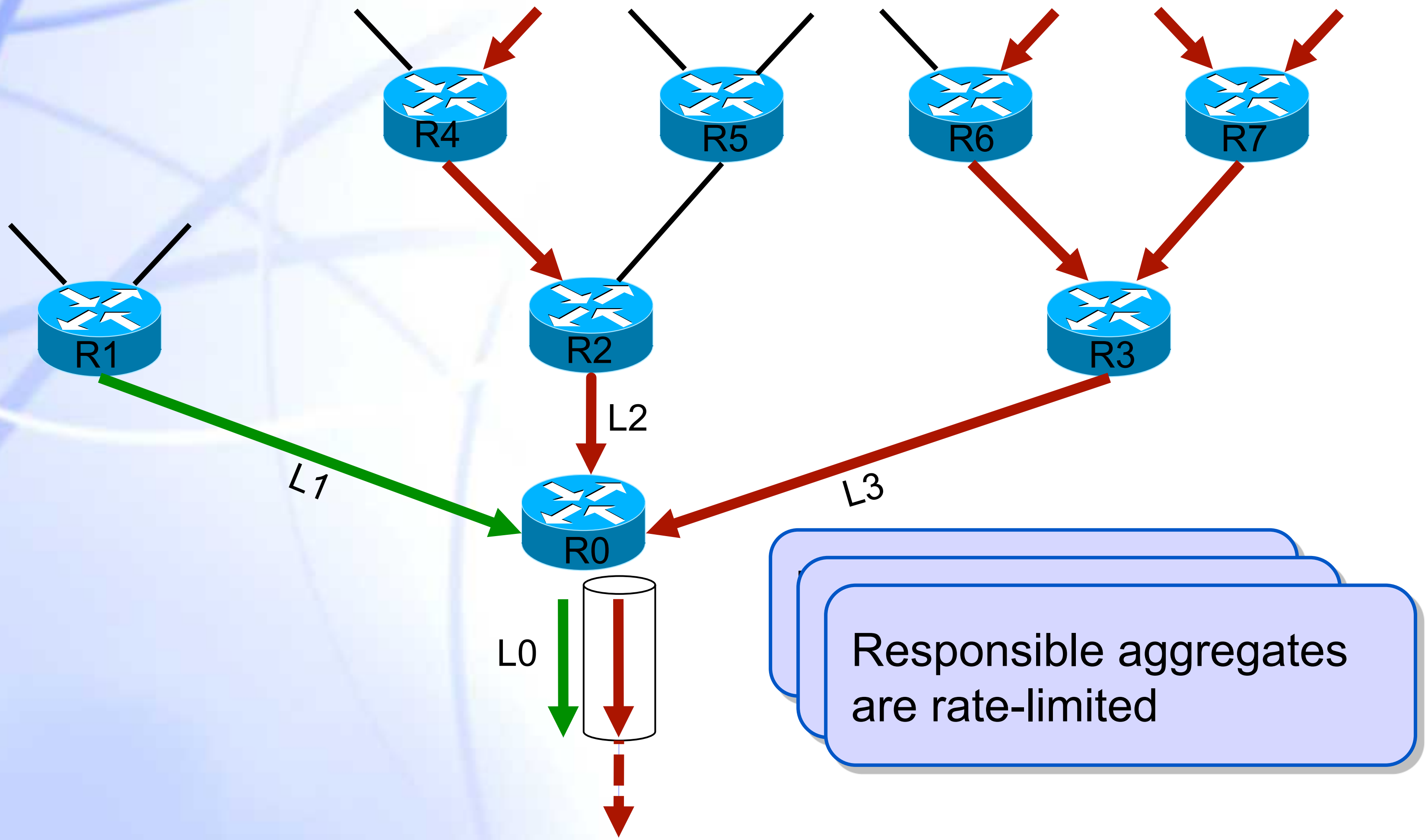
Pushback (V)

- **Local ACC: example**



Pushback (V)

- **Local ACC: example**

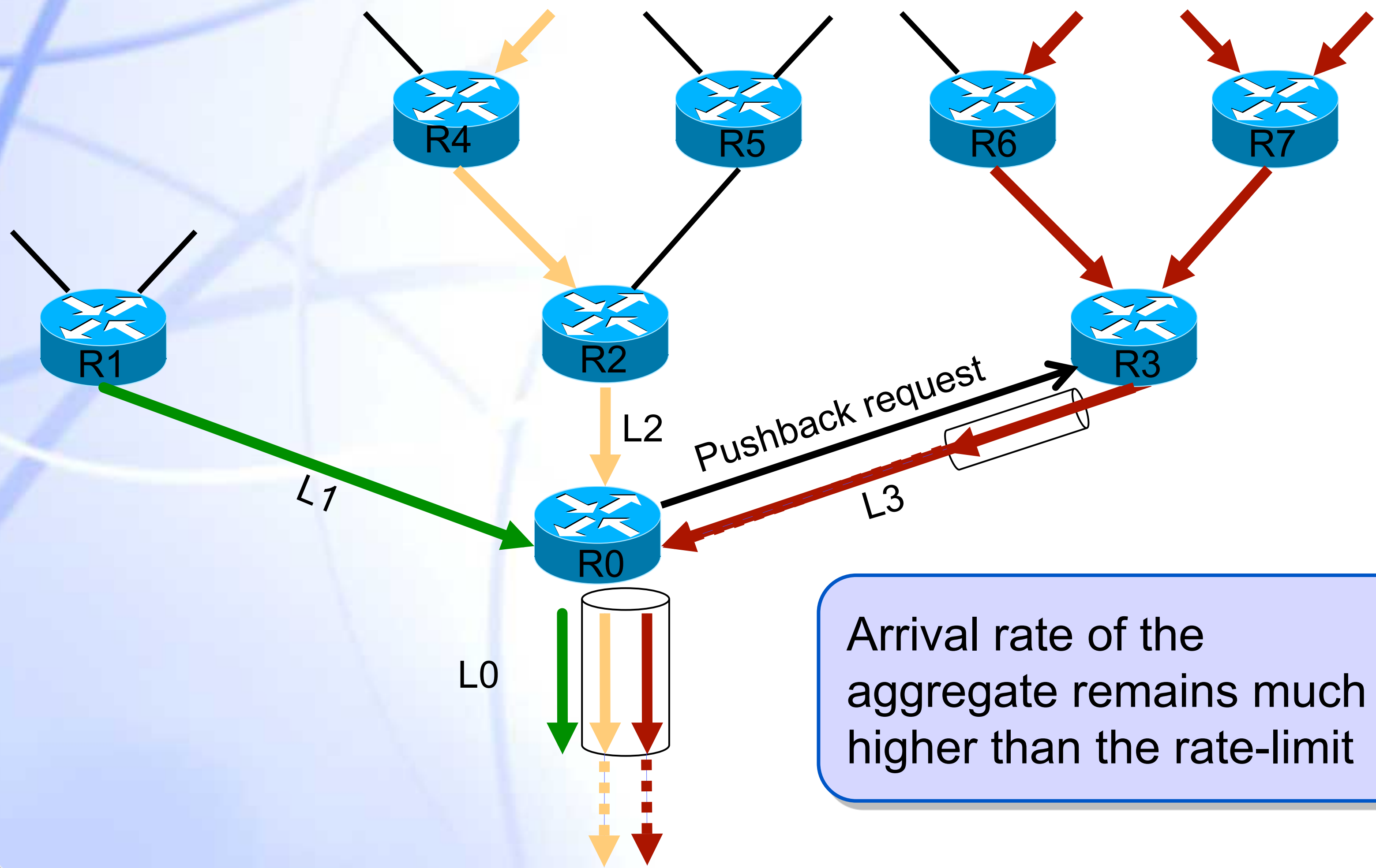


Pushback (VI)

- **Pushback**
  - Invoked if the drop rate for a rate-limited aggregate remains high for several seconds
  - Enables a router to cooperate with adjacent routers to control an aggregate
  - Benefits:
    - ✓ Saving upstream bandwidth
    - ✓ Focus rate-limiting on the attack traffic within the aggregate

Pushback (VII)

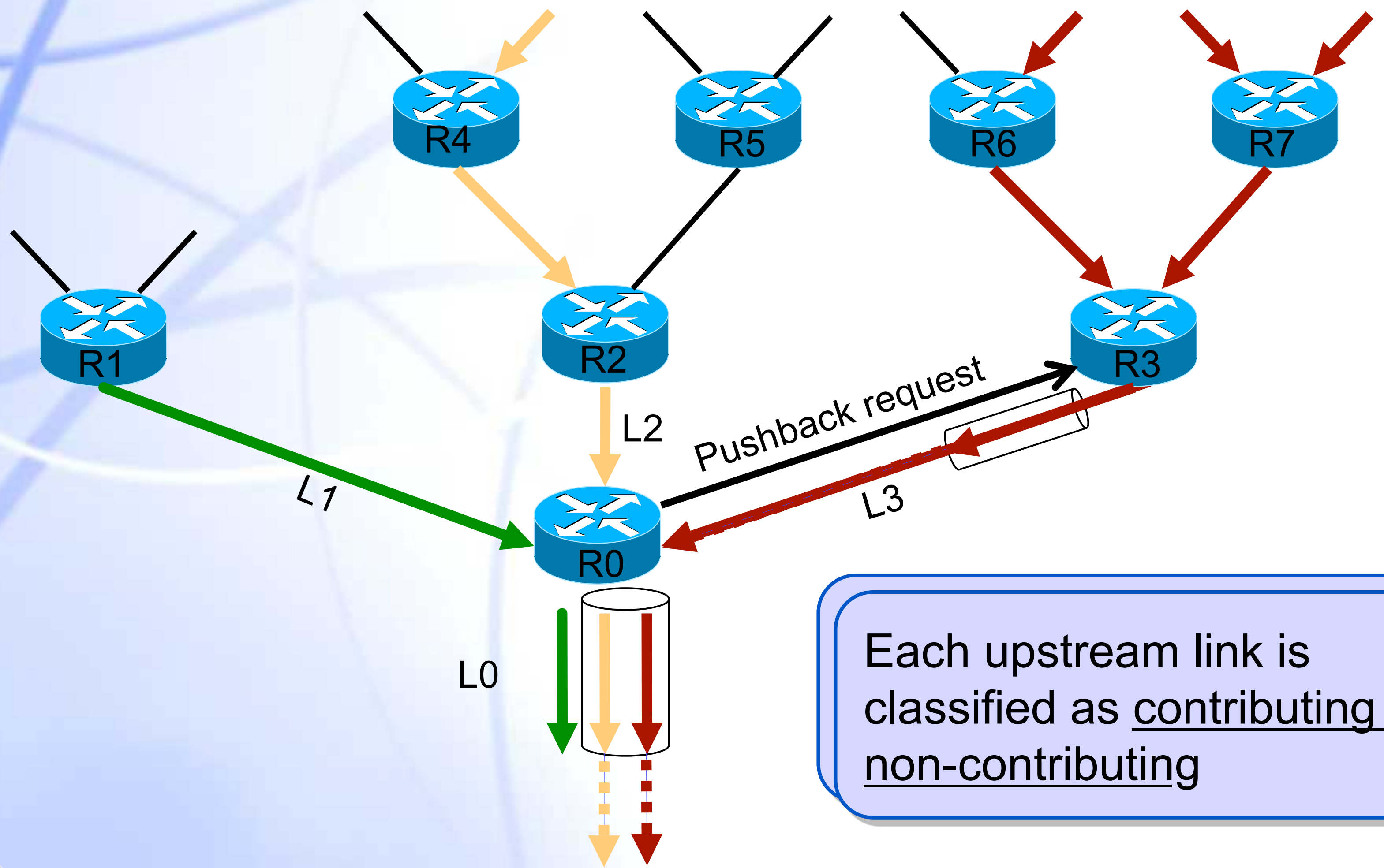
- **Pushback: example**



Arrival rate of the aggregate remains much higher than the rate-limit

Pushback (VII)

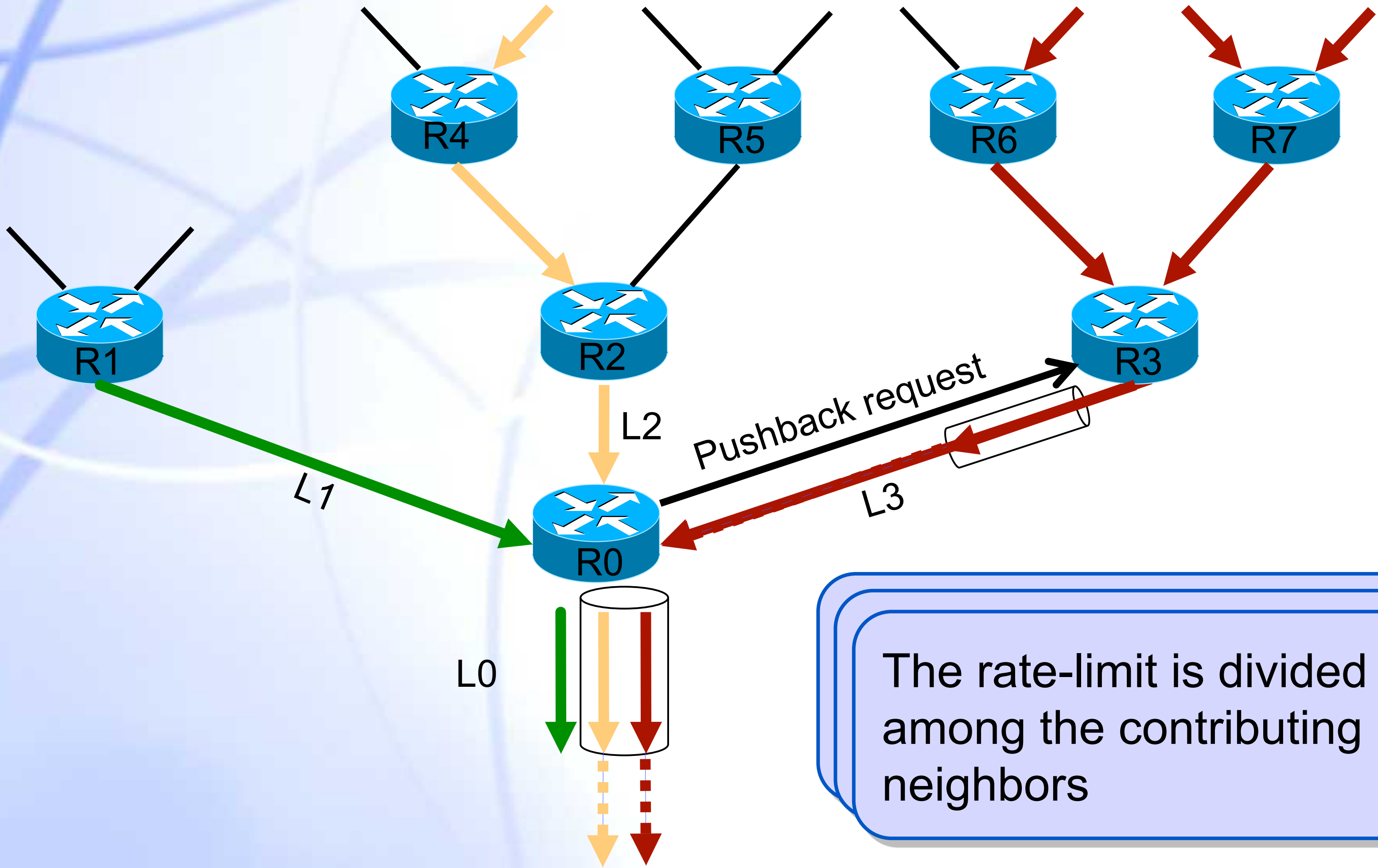
- **Pushback: example**



Each upstream link is classified as contributing or non-contributing

Pushback (VII)

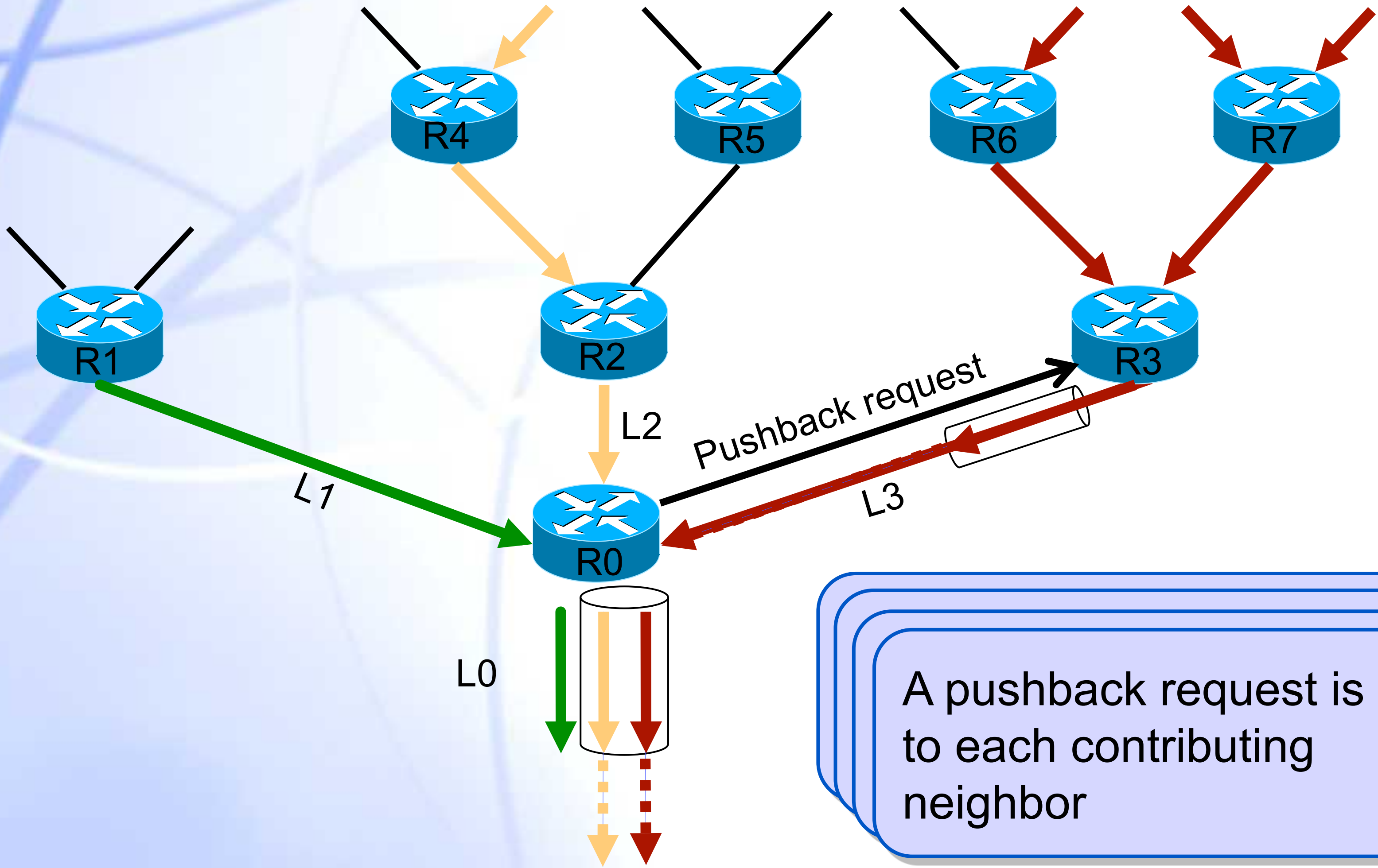
- **Pushback: example**



The rate-limit is divided among the contributing neighbors

Pushback (VII)

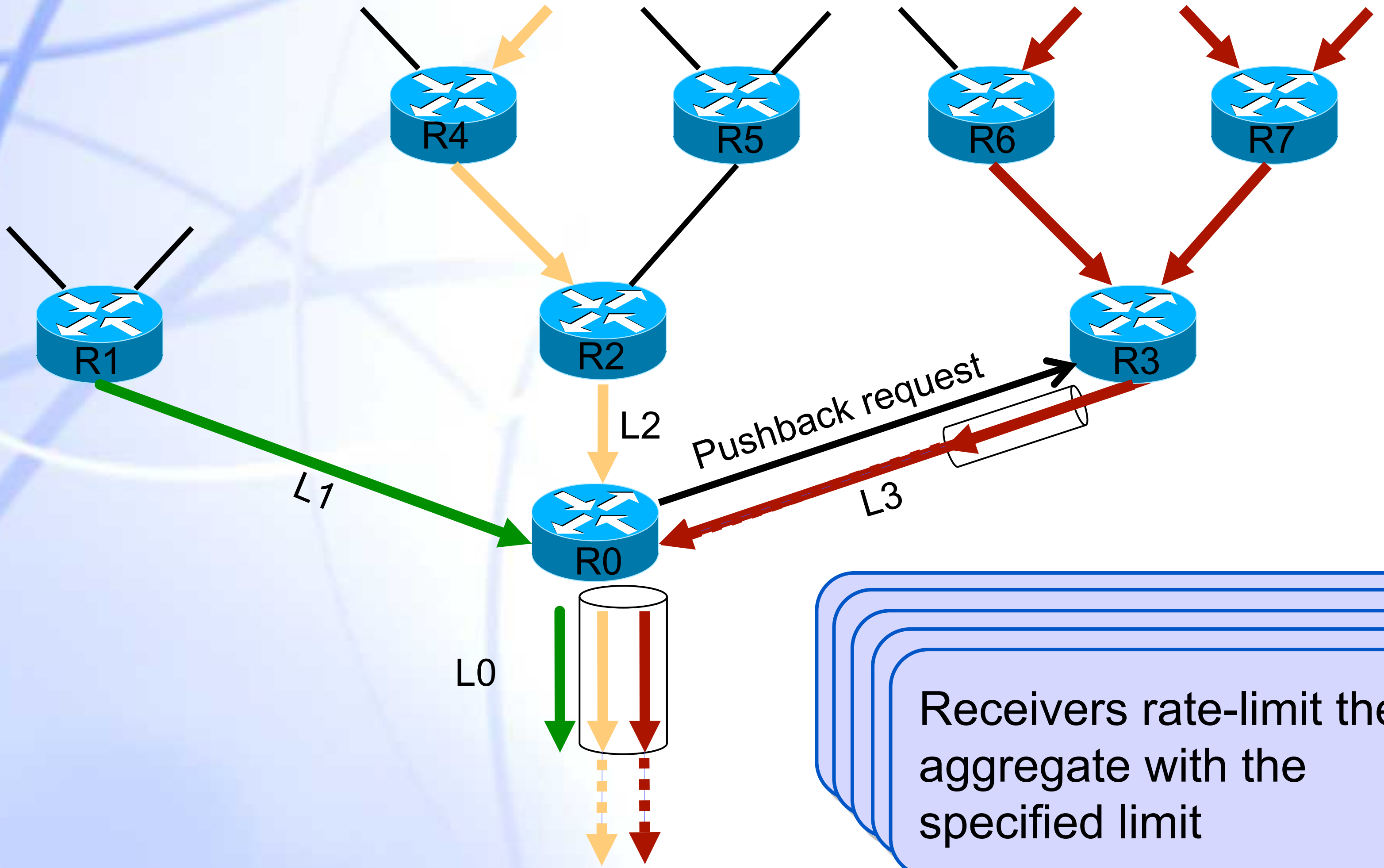
- **Pushback: example**



A pushback request is sent to each contributing neighbor

Pushback (VII)

- **Pushback: example**



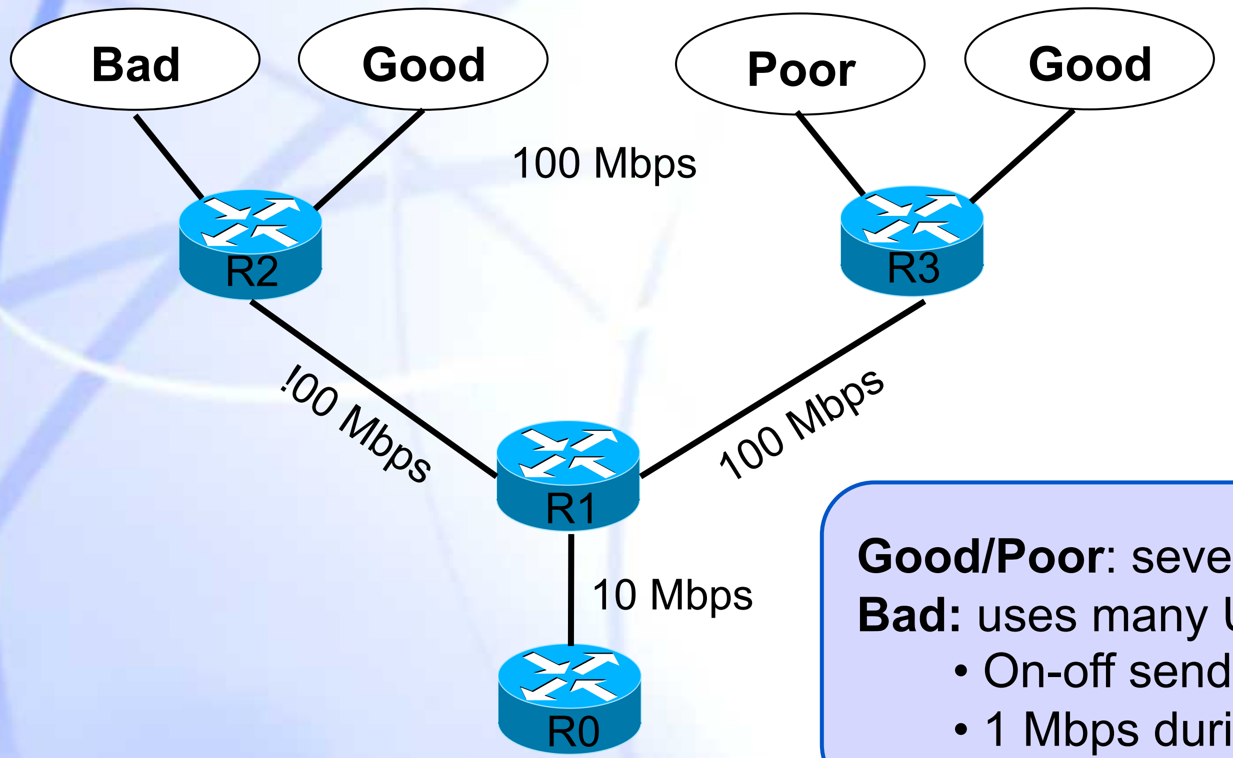
Receivers rate-limit the aggregate with the specified limit

Pushback (VIII)

- **Identifying high bandwidth aggregates:**
  - **Most of DoS attacks and flash crowds have a common source or destination prefix**
  - **Algorithm to identify high bandwidth aggregates (based on the destination address):**
    1. From the drop history, extract a list of high-bandwidth addresses
    2. Cluster the addresses into 24-bit prefixes
    3. For each cluster, try to obtain a longer prefix that contains most of the drops
    4. Merge closely related prefixes
    5. Each prefix describes a high-bandwidth aggregate

Pushback (IX)

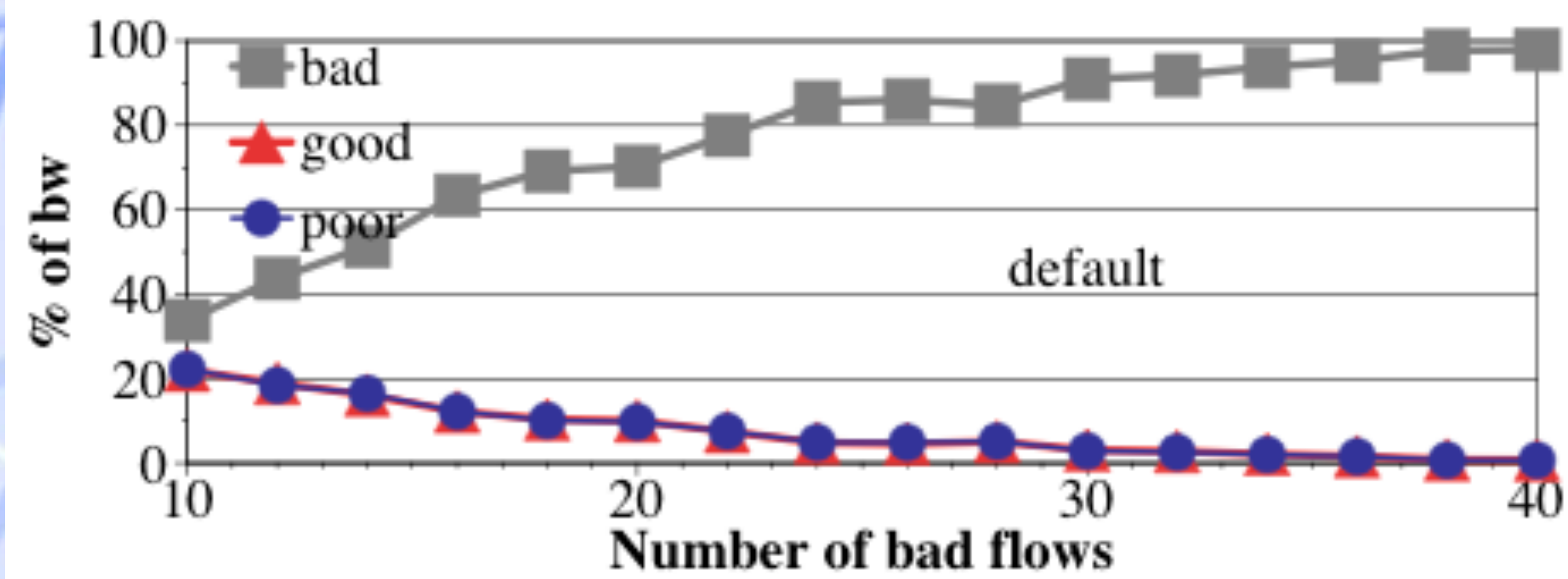
- **Simulation topology:**



Good/Poor: seven TCP connections
Bad: uses many UDP flows. Each flow:
- On-off sending pattern (0-40 sec)
- 1 Mbps during on periods

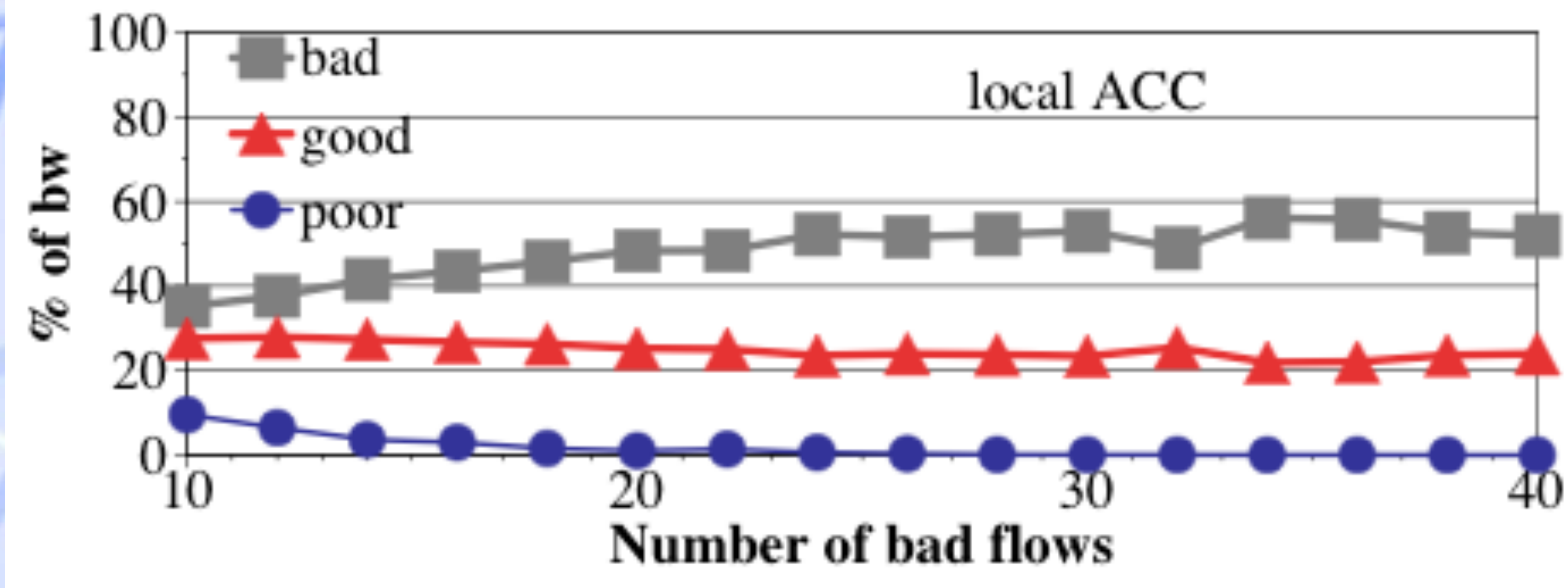
Pushback (X)

- Results:



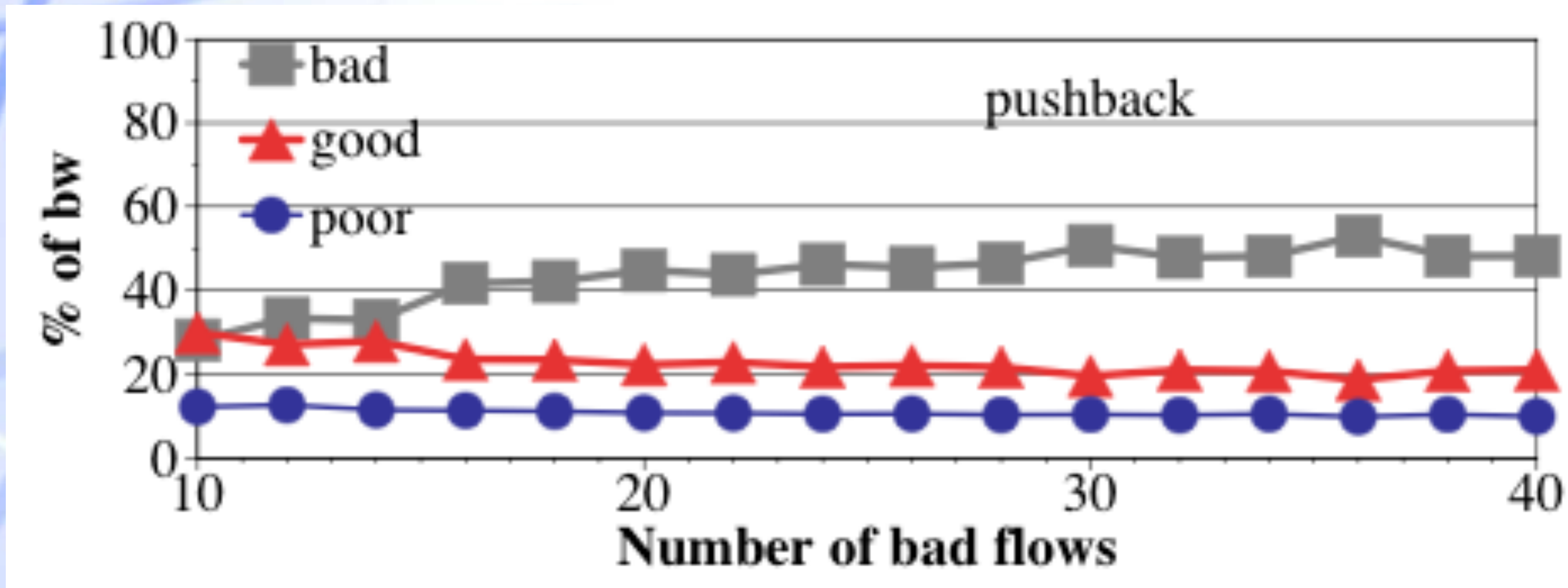
Pushback (X)

- **Results:**



Pushback (X)

- **Results:**



Pushback (XI)

- **Drawbacks:**
  - It is difficult to identify responsible aggregates
  - Discrimination based on packet headers is vulnerable to spoofing
  - Discrimination based on packet content can be frustrated by end to end encryption
  - Sophisticated attacks can infer a filter in order to evade it

Overlay filtering

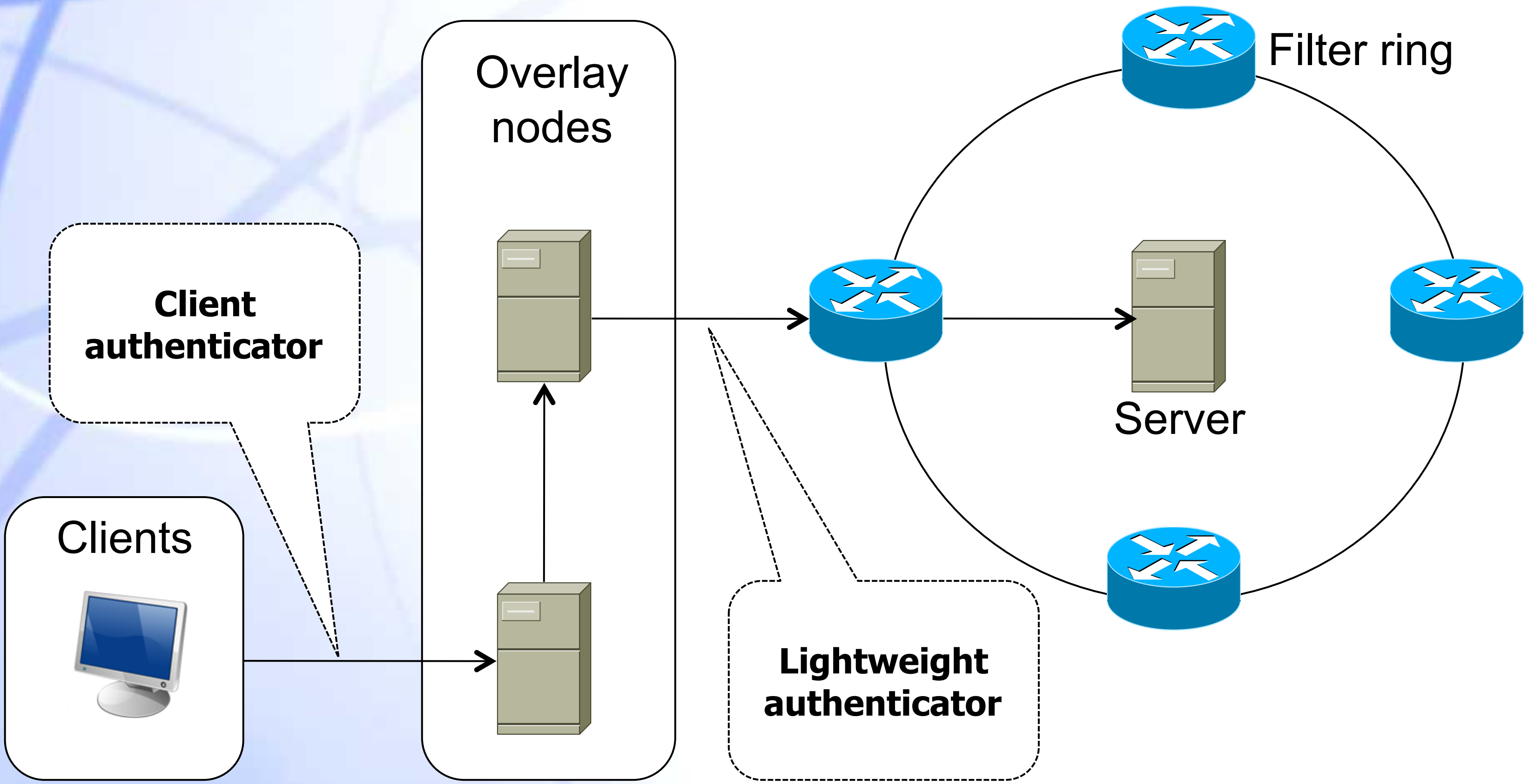
- **Proposals:**
  - **D. G. Andersen. Mayday: Distributed Filtering for Internet Services. In Proc. of USITS 2003**
  - A. Keromytis, V. Misra, and D. Rubenstein. SOS: Secure Overlay Services. In Proc. ACM SIGCOMM 2002

"Using existing network capabilities, how do we protect a server from DDoS attacks while ensuring that legitimate clients can still use the services it provides?"

- **Mayday:**
  - **Combines overlay networks with lightweight packet filtering to defend DDoS**

Overlay filtering (II)

- **Mayday architecture:**



Overlay filtering (III)

- To protect the server against DDoS:
  - Mayday prevents clients from communicating directly with the server
  - It imposes a router-based, network layer filter ring around the sever
- Clients communicate with the overlay nodes, which:
  - Authenticate the client
  - Verify that the client is permitted to use the service
- Overlay nodes use a lightweight authenticator to get through the filter ring

Overlay filtering (IV)

- **Examples of overlay routing:**
  - **Singly-Indirect routing**
  - **Doubly-Indirect routing**
  - **Random routing**
  - **Etc.**
- **Examples of lightweight authenticators:**
  - **Egress Source Address**
  - **Server destination port**
  - **Server destination address**
  - **Etc.**

Overlay filtering (V)

- **Drawbacks:**
  - **It is vulnerable to an attacker discovering the secret:**
    - ✓ **It is shared among all the traffic through the overlay to the same destination**
  - **The scheme does not use regular Internet routes**

Anomaly detection

- Classify the traffic patterns as normal or anomalous
- Malicious traffic causes actions to be performed:
  - Raising alarms, installing network filters, etc.
- Drawbacks:
  - Anomaly detection is not a sufficient response to the problem
  - Leads to closed systems