Carnegie Mellon CyLab
CONFIDENCE FOR A NETWORKED WORLD

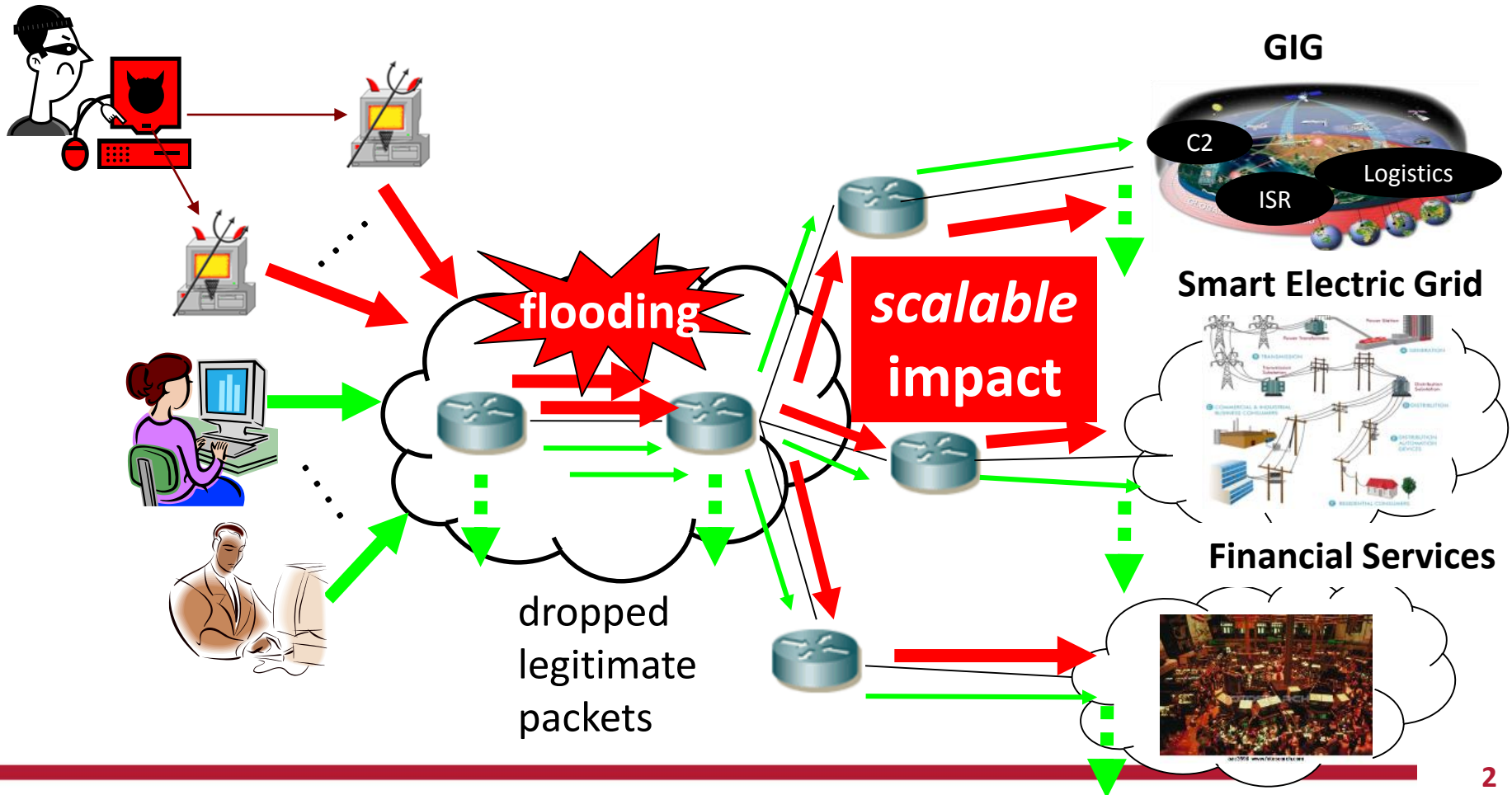
CoDef: Collaborative Defense against Large-Scale Link-Flooding Attacks

Soo Bum Lee*, **Min Suk Kang**, Virgil D. Gligor
CyLab, Carnegie Mellon University
*Qualcomm

Dec. 12, 2013

Large Scale Link-Flooding Attacks

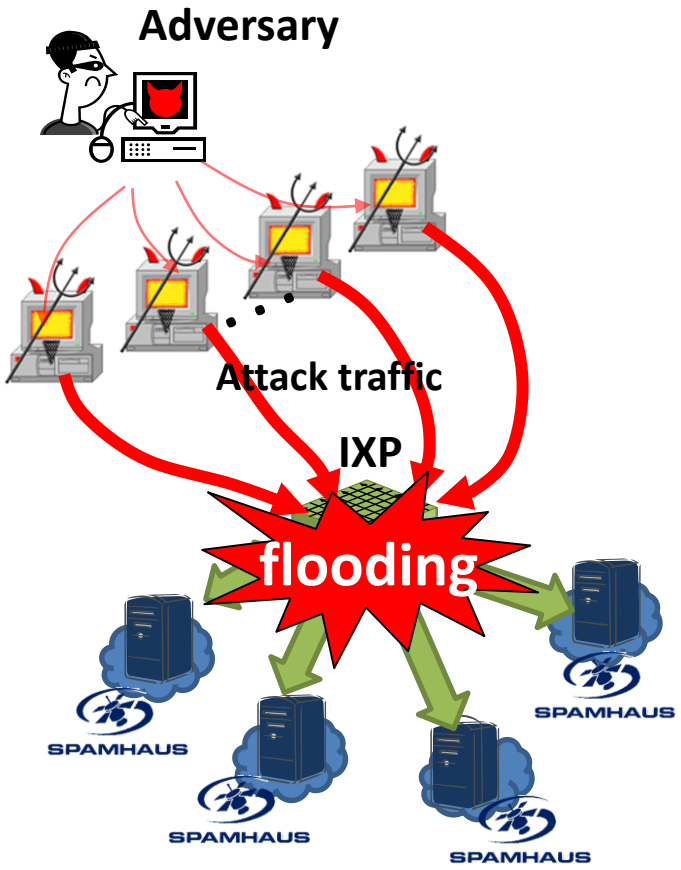
- **Massive DDoS attacks against *chosen targets* in *Internet Infrastructure***



Real World Example: "Spamhaus" Attack (2013)

- **flooding** few links in **4 IXPs**
  - **scalable impact**: regionally degraded connectivity
  - **but easily mitigated**: attack flows are *distinguished* from legitimate flows and filtered

    => lasted only ~ **1 - 1.5 hours**



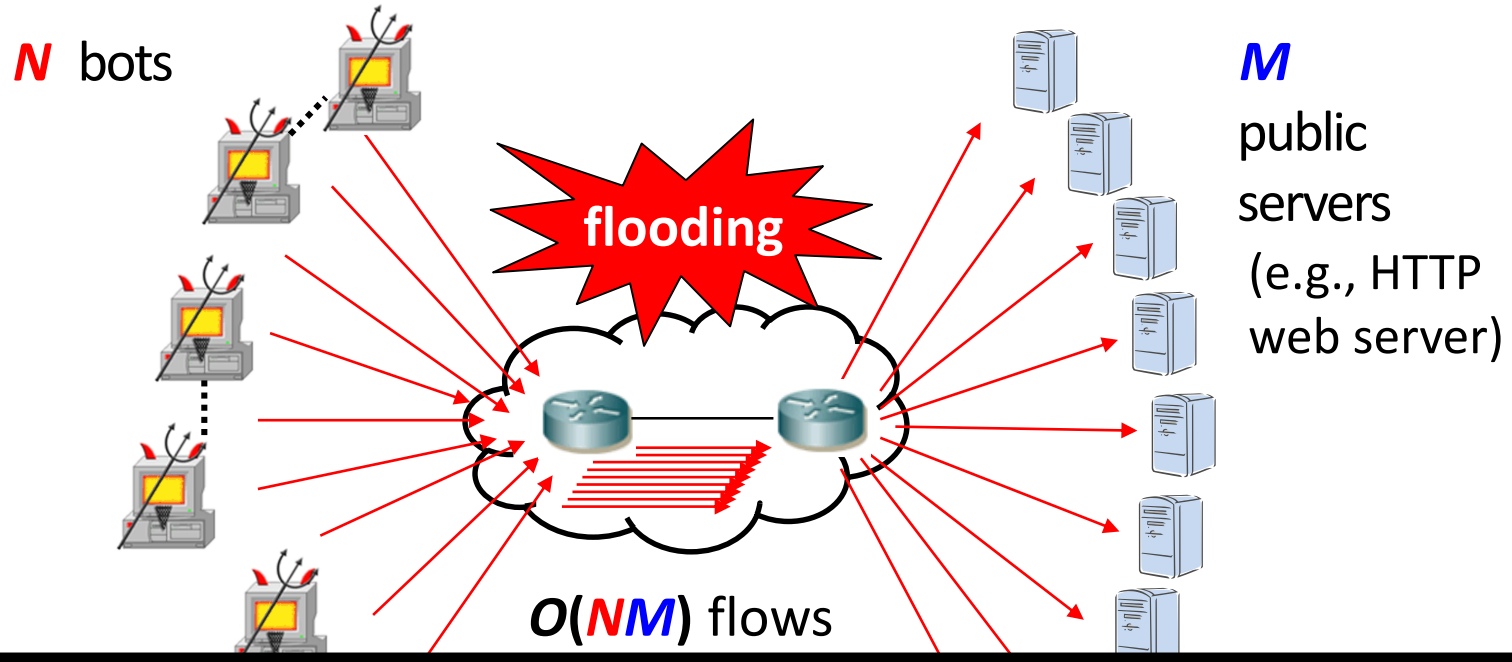
Typical Defenses against Link-Flooding Attacks

- ***Distinguish*** **attack flows from legitimate ones**
  - ✓ e.g., flow filtering, pushback, anti-spoof filtering, capability-based solutions

But, ***advanced*** link-flooding attacks can easily ***circumvent*** the ***typical defenses***

"Crossfire" Attack (S&P'13)

use **"bot** to **public server"** attack flows

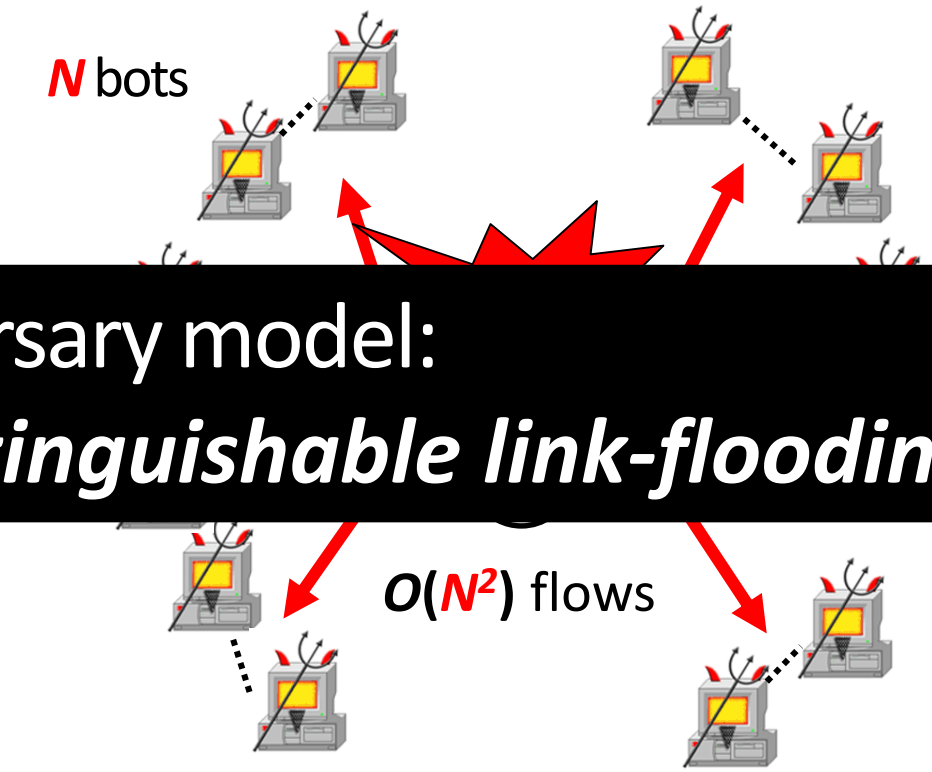


"***indistinguishable***" attack flows from legitimate flows

✓ many, low-rate, diverse source/destination addresses, protocol conforming, destination-wanted

"Coremelt" Attack (ESORICS'09)

use **"bot** to **bot"** ***colluding*** attack flows

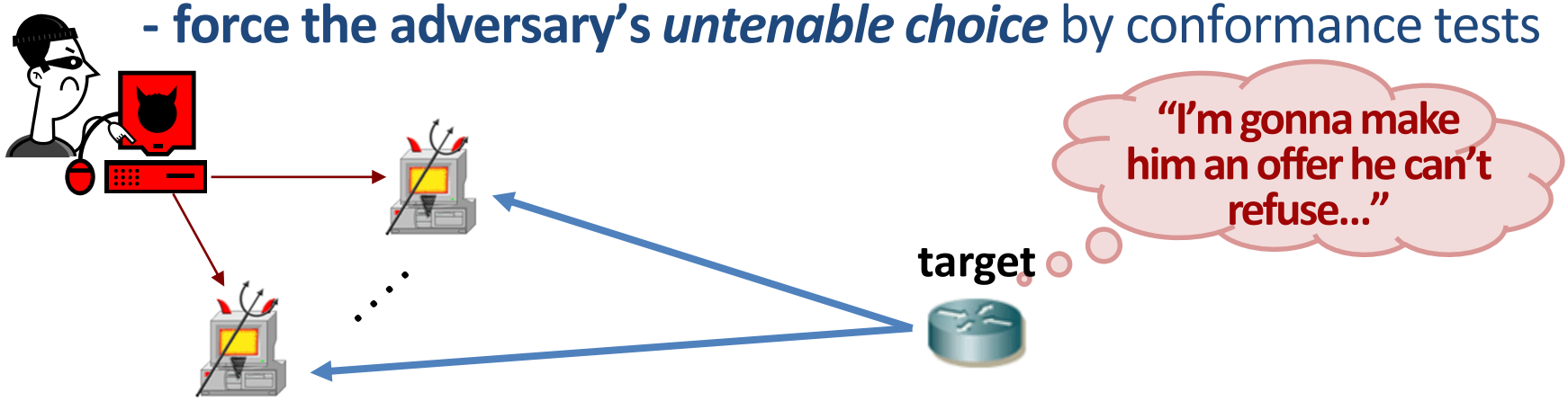


Our adversary model:
"indistinguishable link-flooding attacks"

Problems

I. Identify the *indistinguishable* attack flows?

- **force the adversary's *untenable choice*** by conformance tests



II. Avoid collateral damage to legitimate flows?

- **route separation** (i.e., providing ***detours*** for legitimate flows)

III. Prevent the attack from being ***dispersed*** and causing ***unanticipated*** damage to legitimate flows?

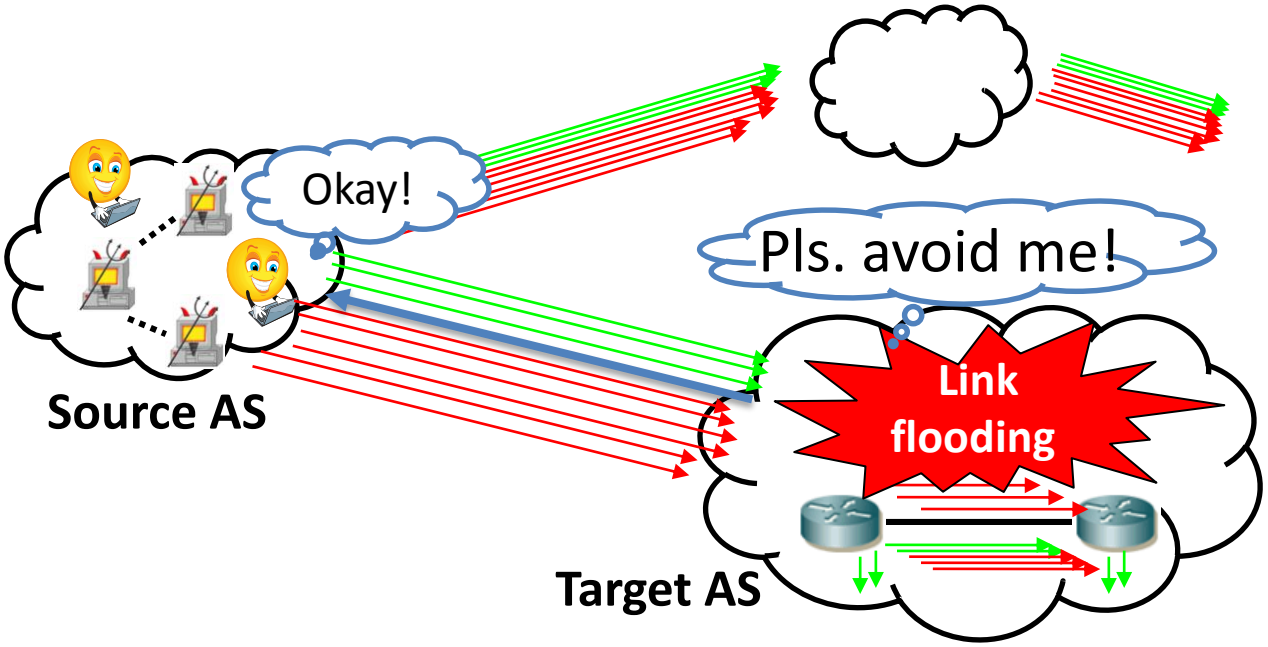
- **pin down** potential attack flows

CoDef: Collaborative Defense

1. Collaborative Rerouting

Target AS sends ***reroute requests*** to source ASes

=> provides detours around the flooded link

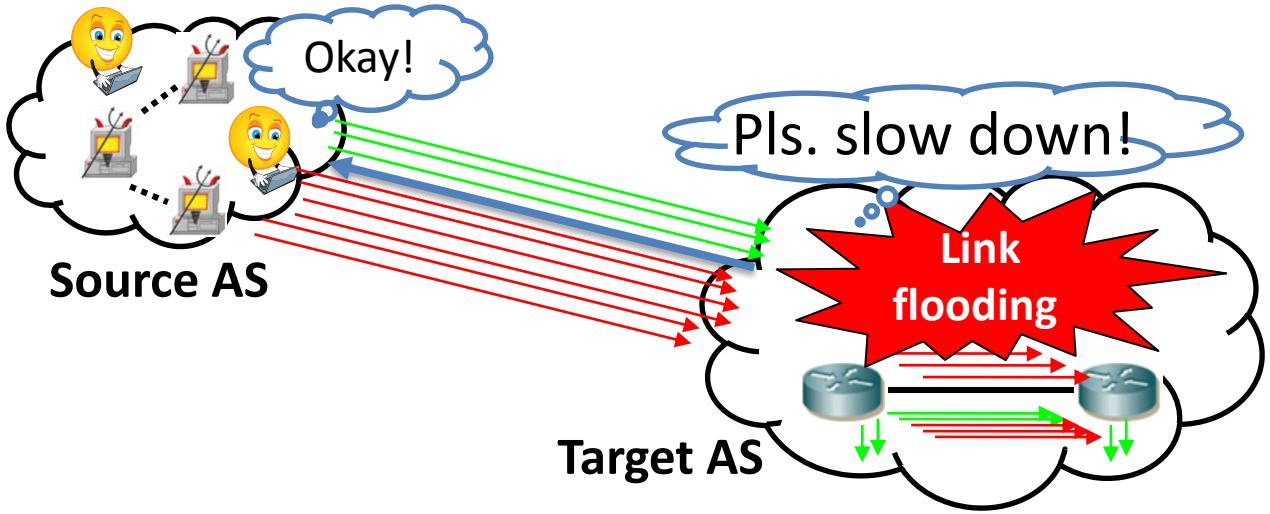


CoDef: Collaborative Defense

2. Collaborative Rate Control

Target AS sends ***rate-control requests*** to source ASes

=> allows source AS to prioritize flows



Motivations of Collaborative Defense

Target AS

- ✓Has no way to distinguish attack flows by itself
- ✓Has limited control over the incoming traffic

  e.g., end-to-end AS-paths, traffic rate

Source AS

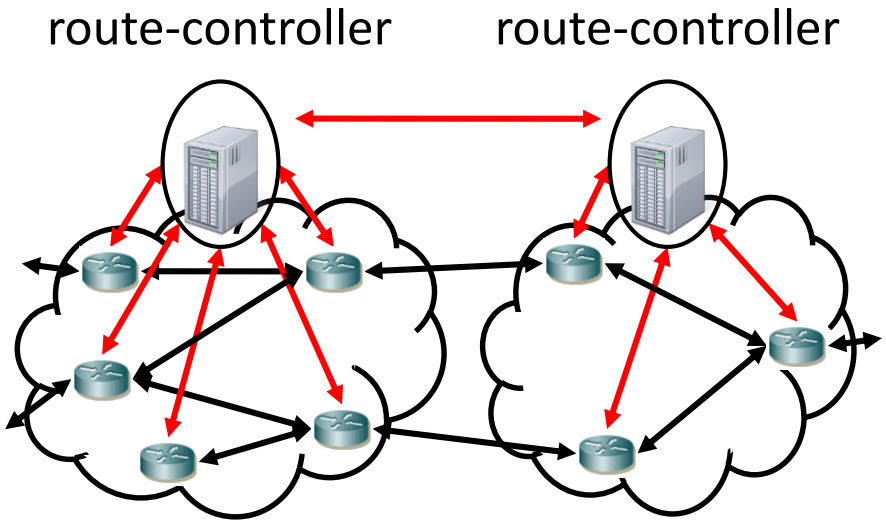
- ✓Has no idea about the flooding at the remote target
- ✓Has good reason for collaboration to circumvent flooding

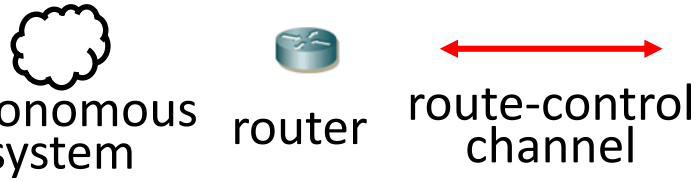
Transit ASes

- ✓Has no incentive/motivation for changing (optimized/complex) routing policies

CoDef Architecture

- CoDef ***adds complementary*** routing functions
  - ***route controllers, secure route-control channels***

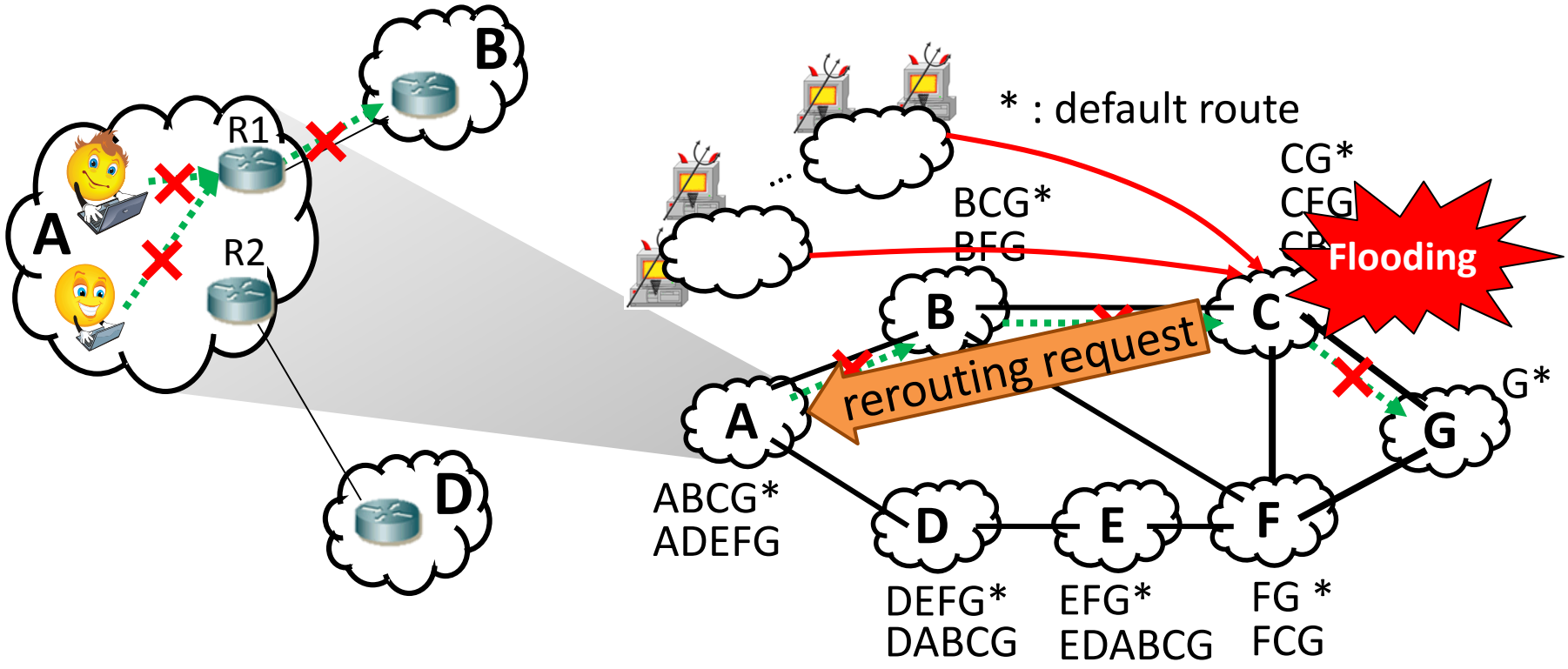




Collaborative Rerouting

C is ***flooded*** and **A**'s packets to **G** are dropped

(1) **C** sends re-route message to **A**: "Please avoid me (i.e., **C**)"

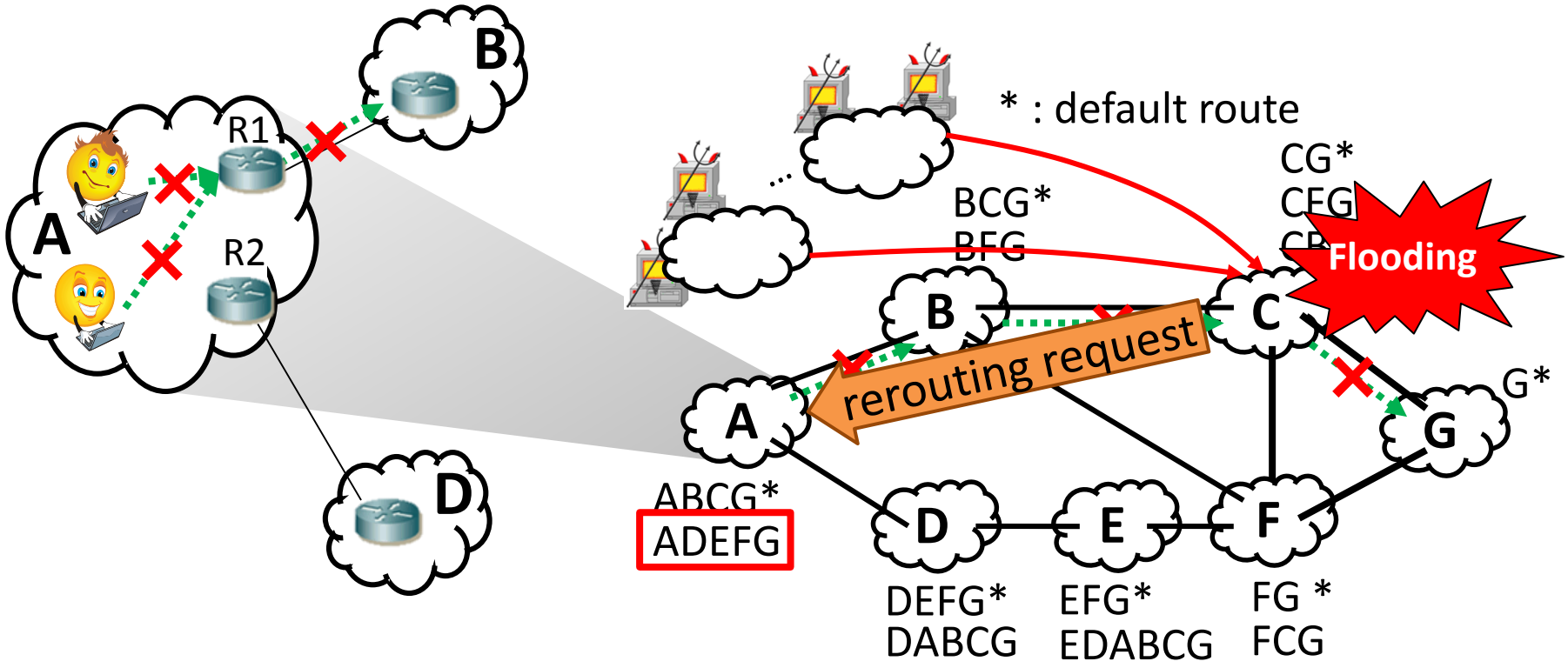


Collaborative Rerouting

C is ***flooded*** and **A**'s packets to **G** are dropped

(1) **C** sends re-route message to **A**: "Please avoid me (i.e., **C**)"

(2) **A** refers to its routing table and finds alternate route: **ADEFG**



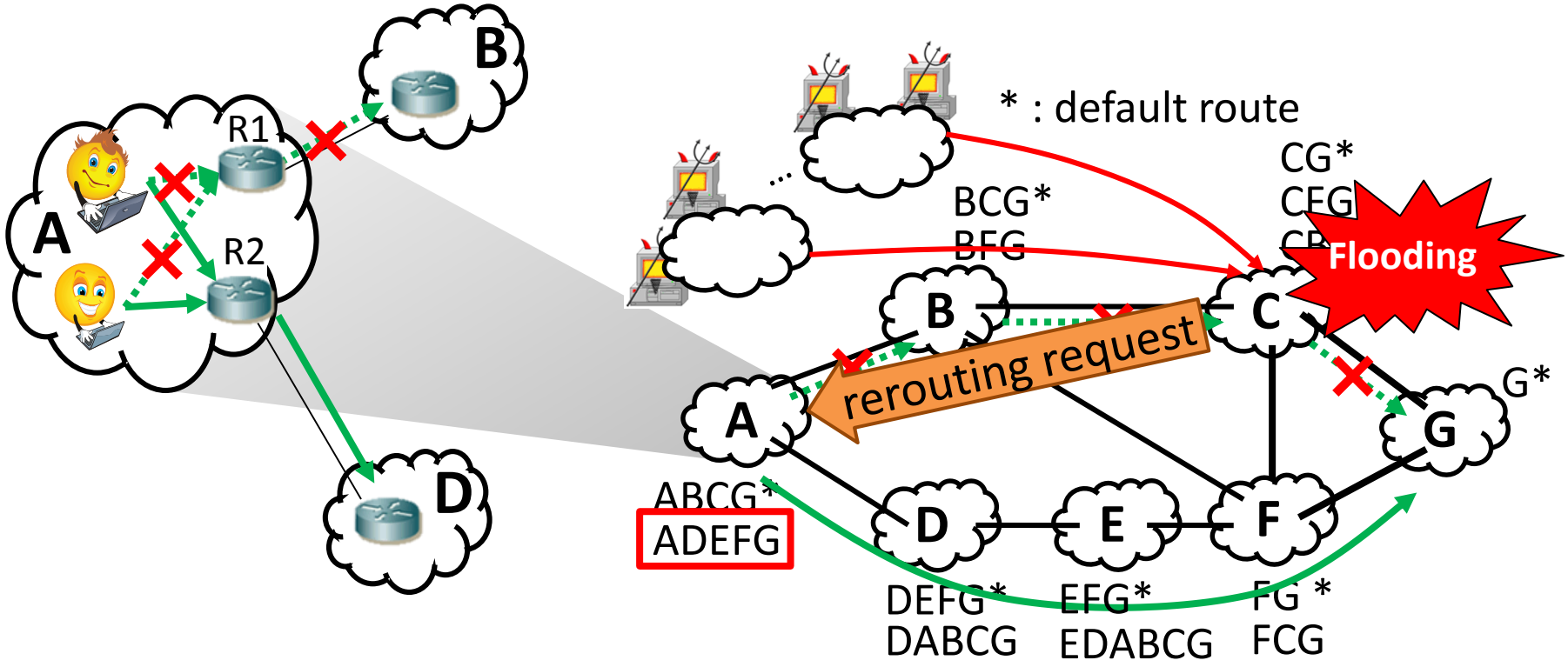
Collaborative Rerouting

C is ***flooded*** and **A**'s packets to **G** are dropped

(1) **C** sends re-route message to **A**: "Please avoid me (i.e., **C**)"

(2) **A** refers to its routing table and finds alternate route: **ADEFG**

(3) **A** changes "Import Policy" of its BGP router (i.e., R2)



Collaborative Rerouting

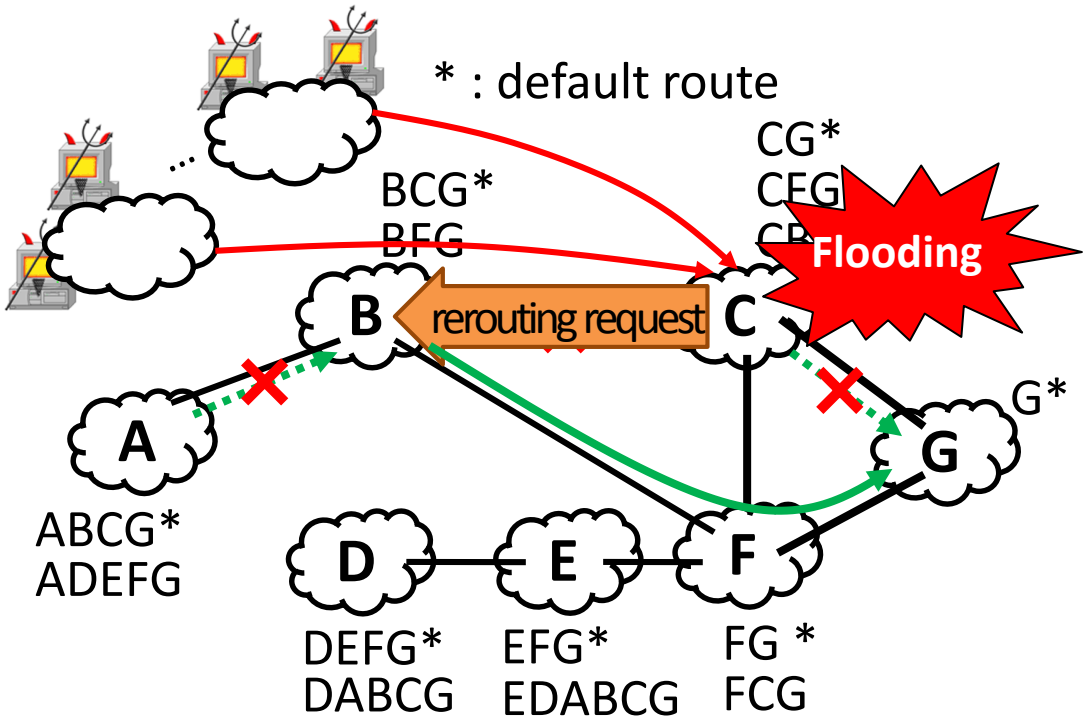
C is ***flooded*** and **A**'s packets to **G** are dropped

(1) **C** sends re-route message to **A**: "Please avoid me (i.e., **C**)"

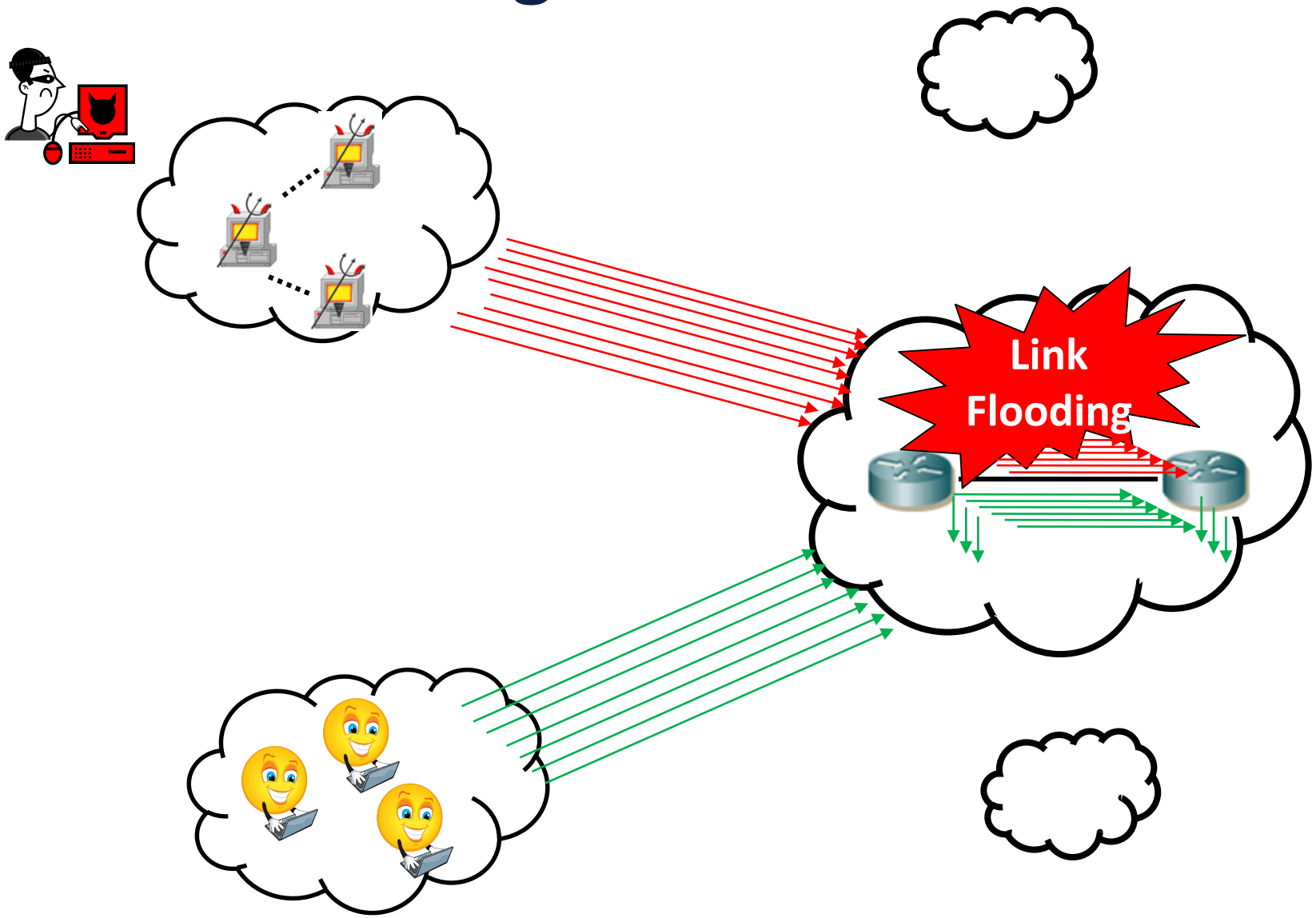
(2) **A** refers to its routing table and finds alternate route: **ADEFG**

(3) **A** changes "Import Policy" of its BGP router (i.e., R2)

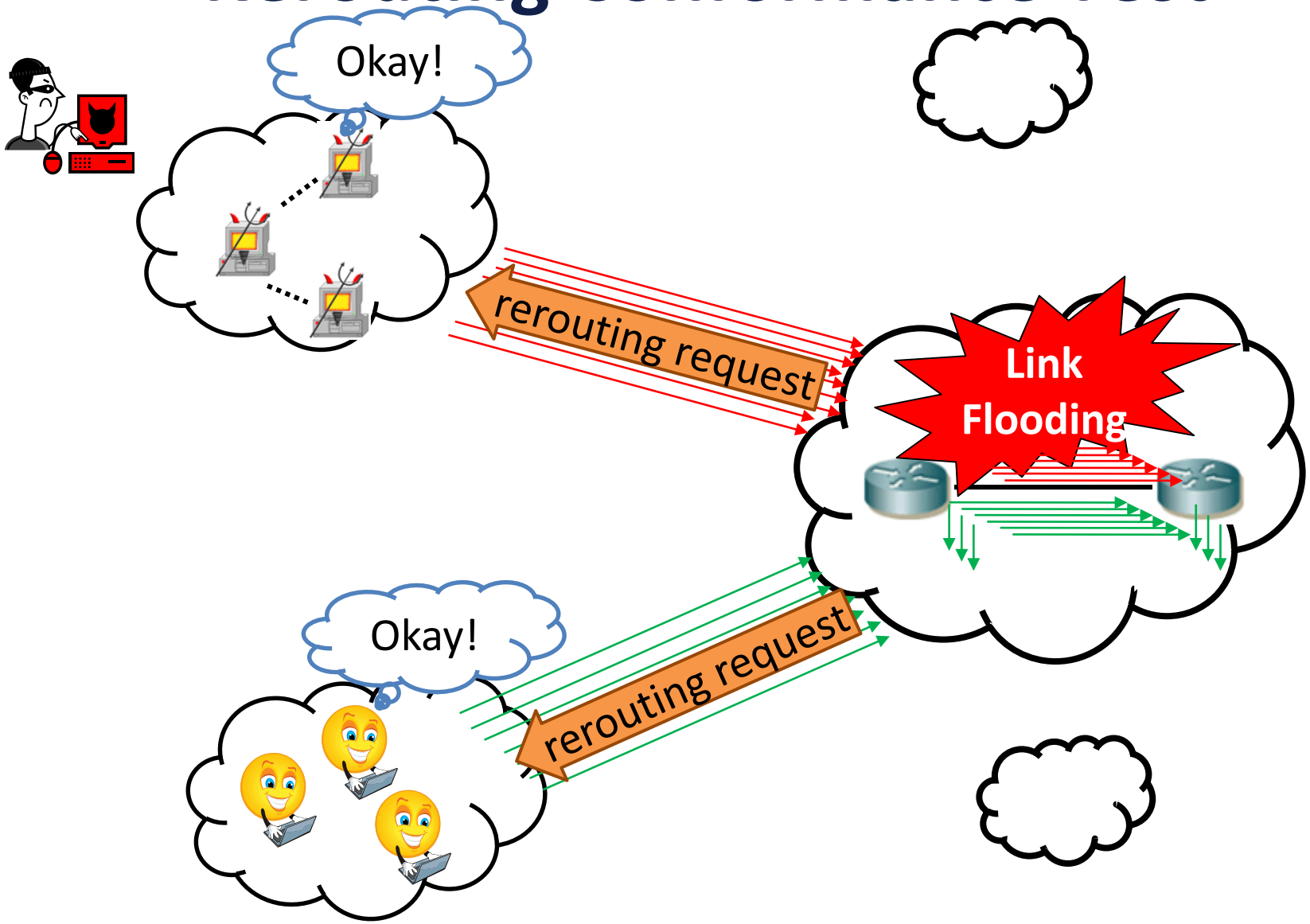
"What if domain **A** is ***single-homed*** exclusively to **B**?"
=> rerouting at B



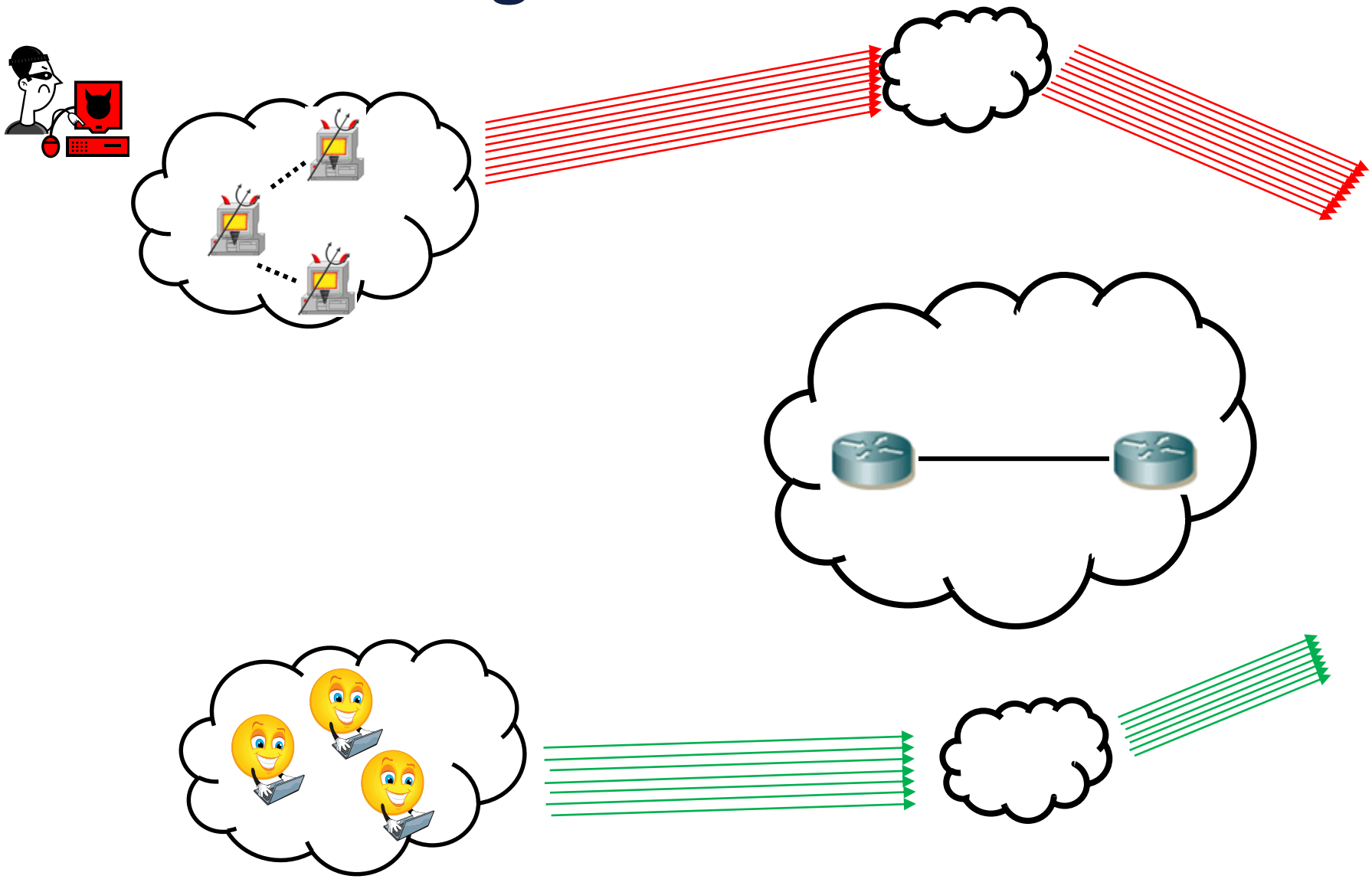
Rerouting Conformance Test



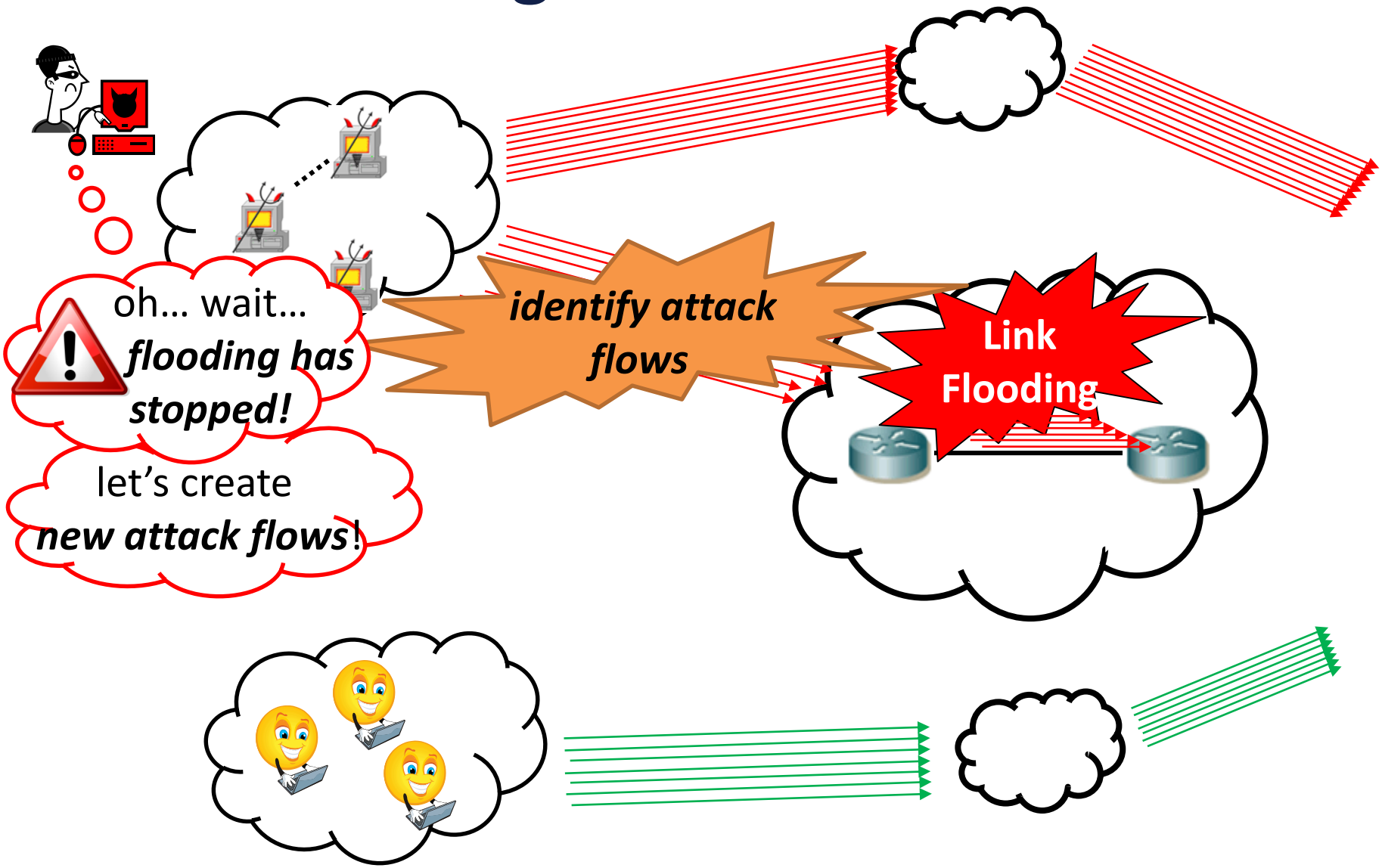
Rerouting Conformance Test



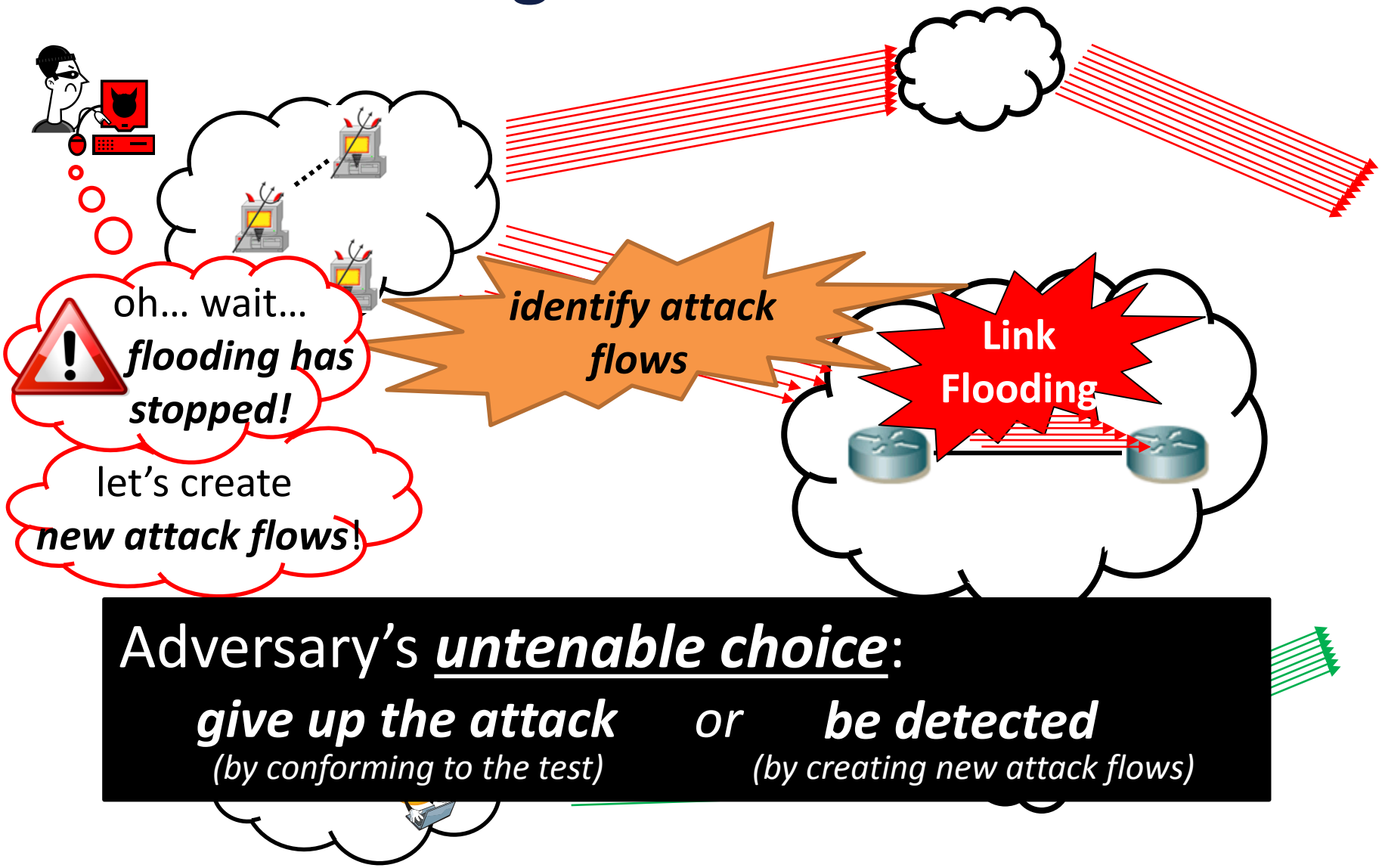
Rerouting Conformance Test



Rerouting Conformance Test



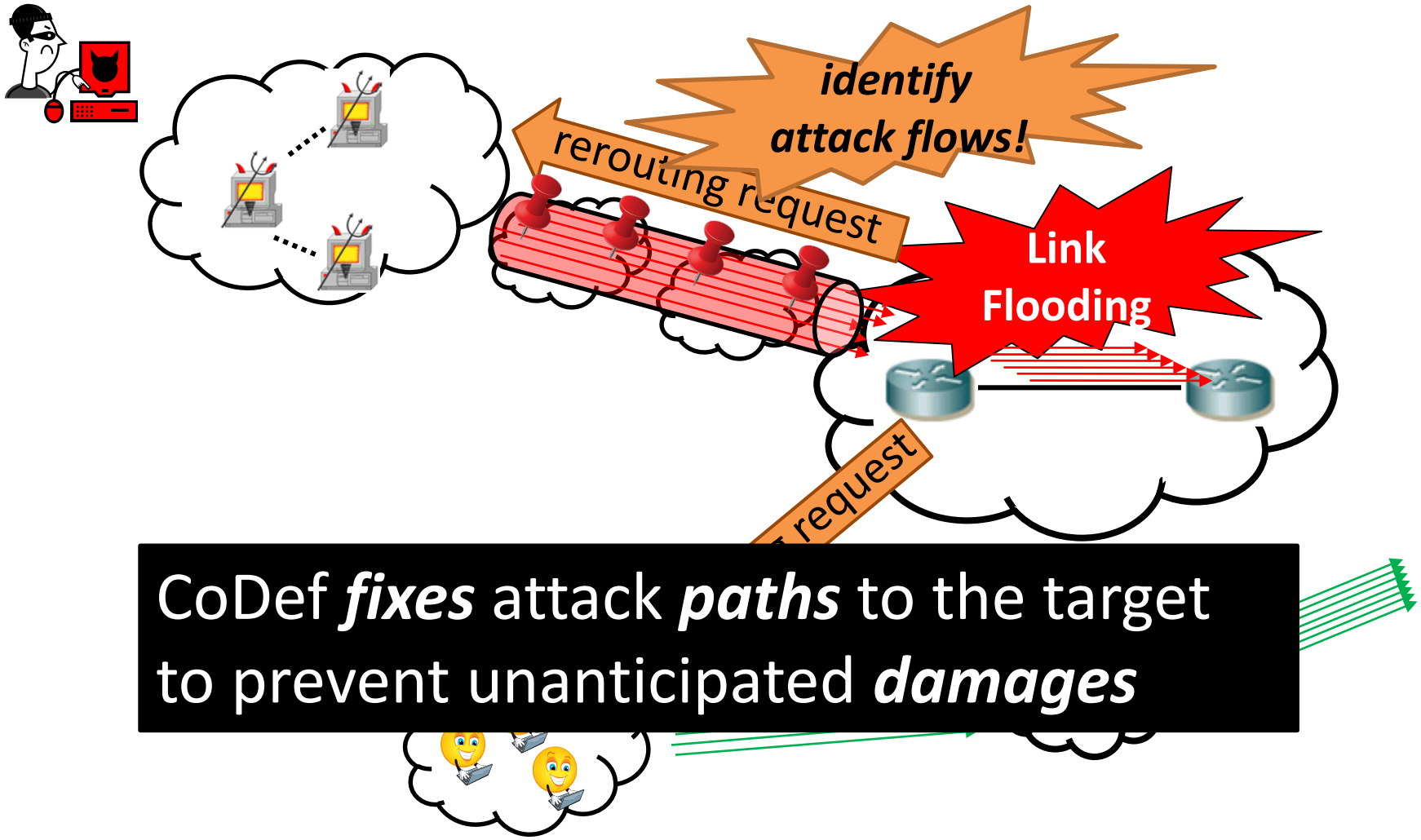
Rerouting Conformance Test



Adversary's ***untenable choice***:

give up the attack *(by conforming to the test)* *or* ***be detected*** *(by creating new attack flows)*

Path Pinning



CoDef ***fixes*** attack ***paths*** to the target to prevent unanticipated ***damages***

Evaluation of Collaborative Rerouting

- **Internet AS topology**
  - ✓ **40K+ ASes** and their **business relationships** from CAIDA (e.g., customer-provider, peer-peer)
  - ✓ **538 attack ASes** selected based on real spam bot distribution

- **Forwarding path decision model**
  - ✓ **preference:** (i) ***cheaper*** paths; (ii) ***shorter*** paths

Evaluation of Collaborative Rerouting

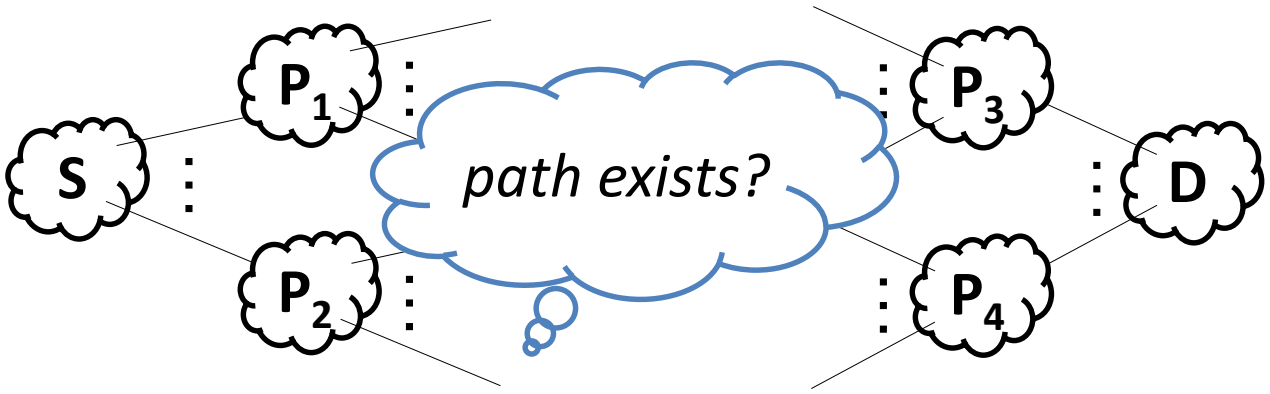
evaluate the **"availability** of **alternate paths"**
from **legitimate** ASes to a **destination**

conservative attack scenario

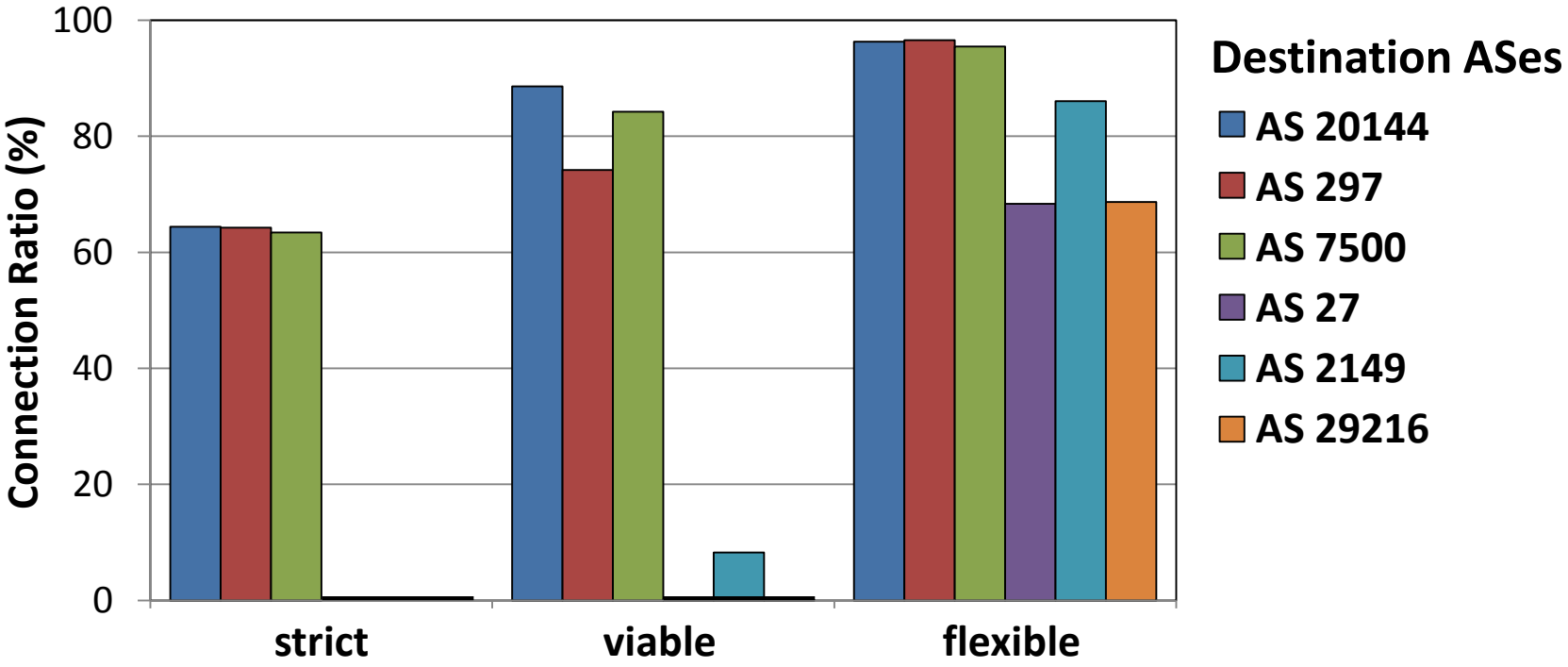
- ***all ASes*** on the ***attack paths*** (i.e., paths from attack ASes to destination) are the ***flooding targets***

Finding alternate paths: "***avoid*** target ASes"

- three ***evaluation policies***
  - ✓ ***strict***
  - ✓ ***viable***
  - ✓ ***flexible***



Availability of Alternate Paths



Ease of Deployment

- **No significant** deployment **cost**
  - ***no*** changes to **existing** systems (e.g., BGP and OSPF)
    - honors routing policies of individual ASes
    - requires no disclosure of internal topology/policies
- **Significant deployment incentives**
  - **technical** advantage
    - detects and mitigates large-scale link-flooding attacks
  - **economical** advantages
    - provides premium services

Conclusion

- ***CoDef***: a practical mechanism for ***defending*** against large-scale link-flooding attacks
- Test to ***identify the attack flows*** exploiting adversary's untenable choices
- ***Significant deployment incentives***

Thank You