Surviving DDoS

SANOG X

5 September 2007

ed.lewis@neustar.biz

Theme

- How does a provider of information and services overcome Denial of Service situations?
- An important tradeoff to think about
  - A simple constrained system is easy to control and make efficient
  - A sufficiently capable and reliable system is going to have some complexities

Agenda

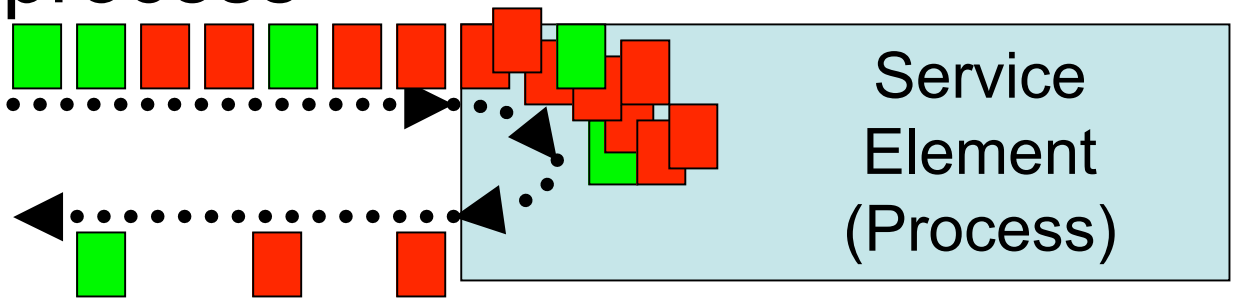
- Know Your Enemy
- Defensive Strategy
- Anycast as a Building Block
- Effective Defense

Know Your Enemy

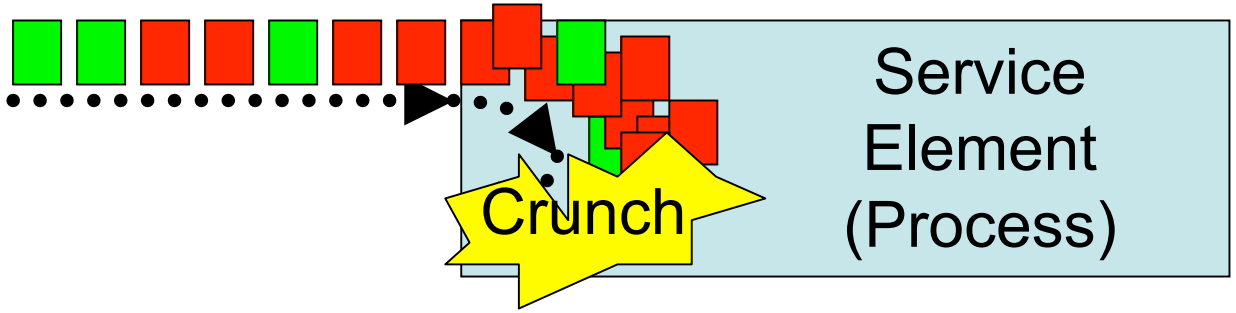
- Denial of Service attack on a process
- DoS attack on a computer
- Dos attack on a network
- DDoS attack

What is a DoS? DDos?

- Slowing a process



- Killing a process

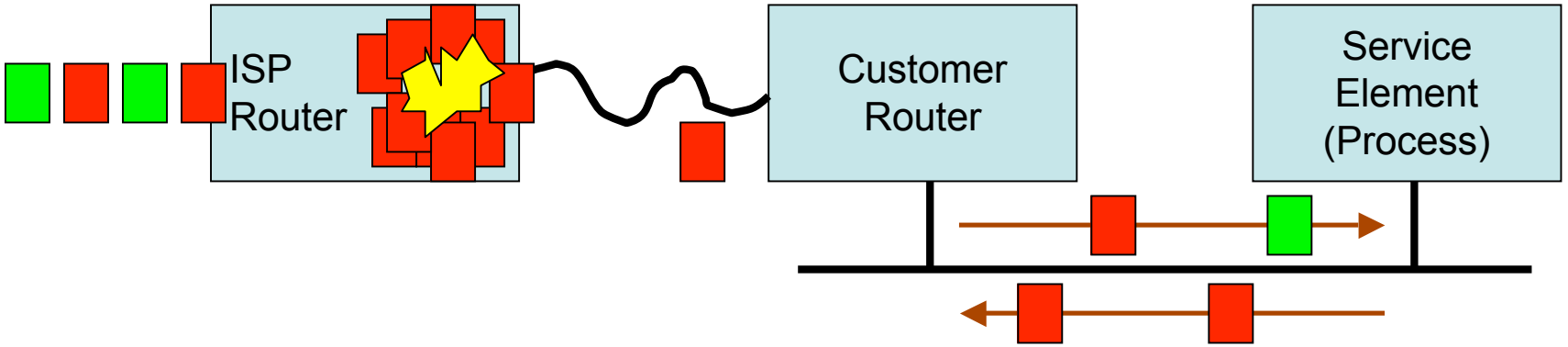


bad packets

good packets

Network Level DoS

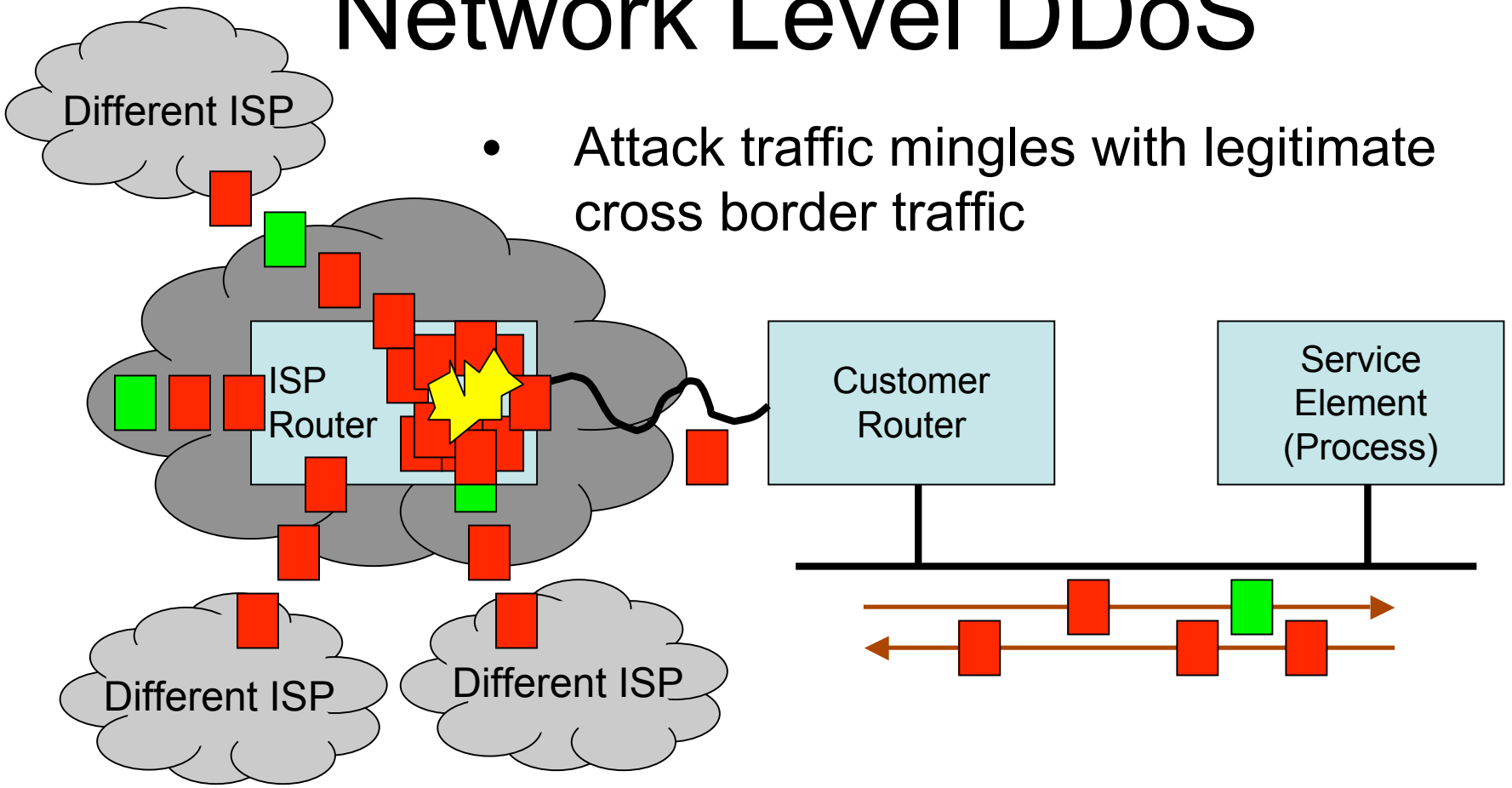
- A Network Denial of Service



- The attack hits in the ISP, not the "victim" site. DDoS - traffic floods from different ISPs

Network Level DDoS

- Attack traffic mingles with legitimate cross border traffic



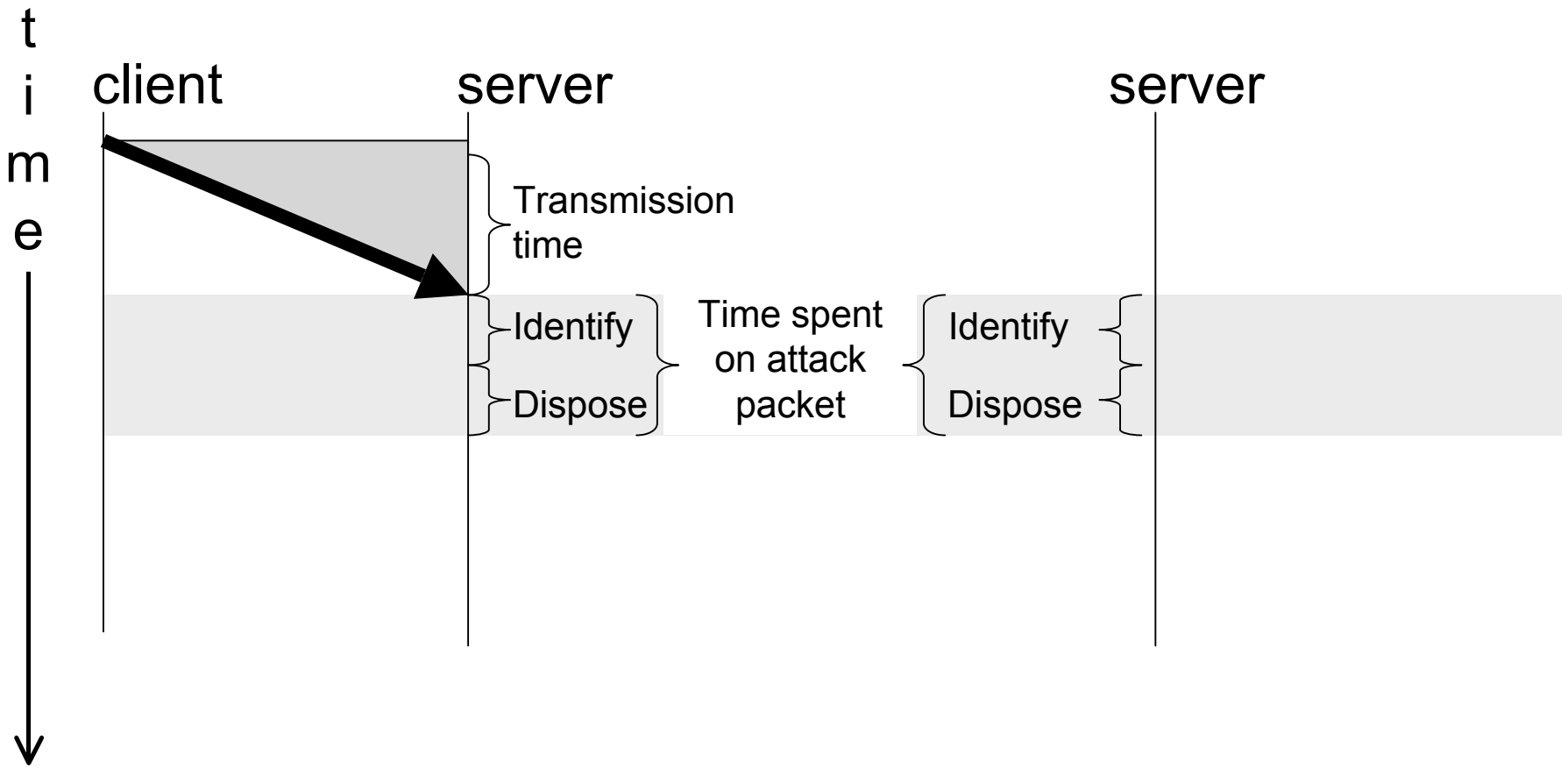
Defensive Strategy

- Toss the bad packets faster than they arrive
  - Identify the bad ones
    - time-to-identify
  - Dispose of them as quickly as possible
    - time-to-dispose
  - Give yourself more time to act
    - time-between-arrivals

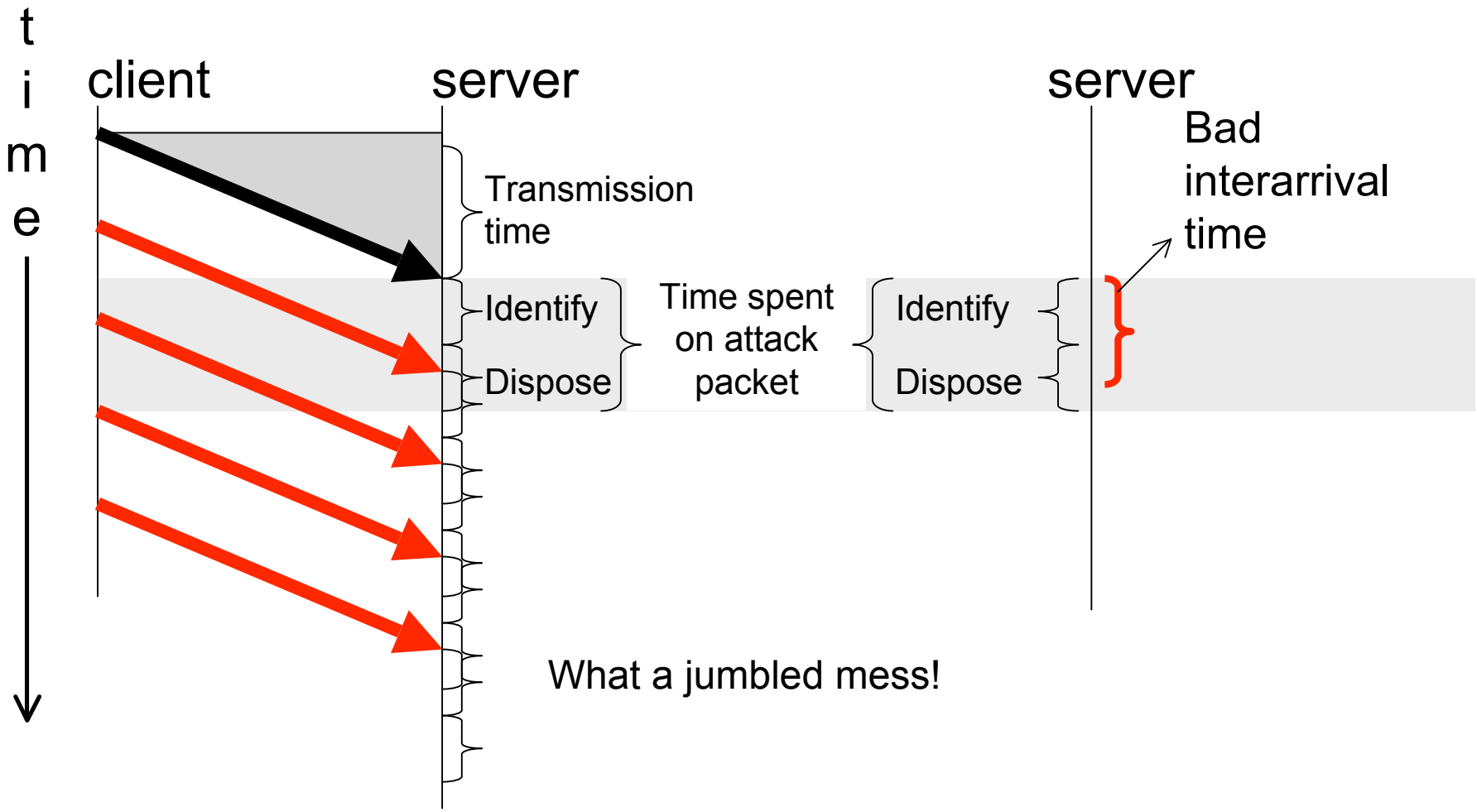
Applying some math

- Queuing Theory
  - "average service time must be less than the inter-arrival rate or the system is unstable"
  - If queues always grow longer, it is bad
- If (time-to-identify + time-to-dispose) > (time-between-arrivals) then you have a problem

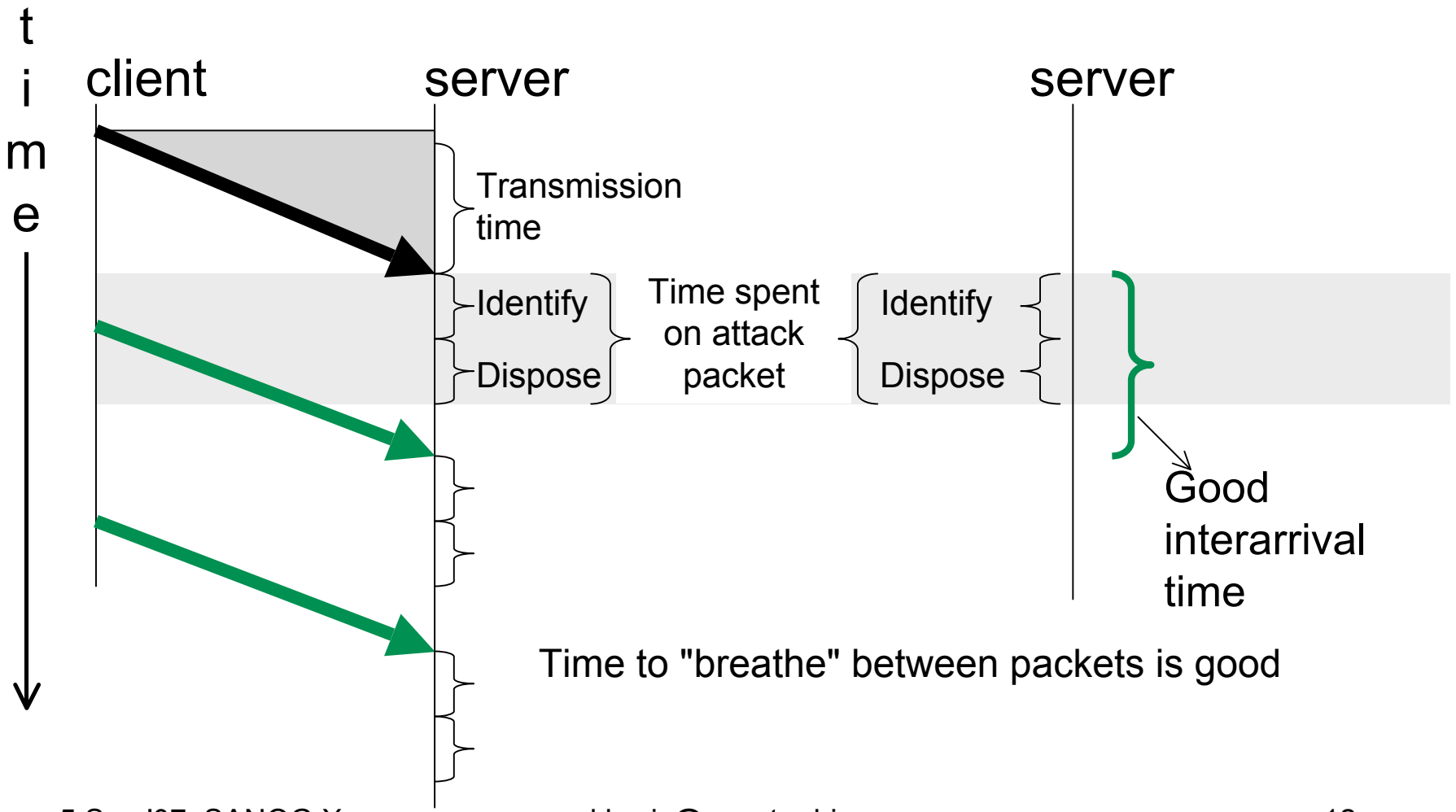
Time diagram



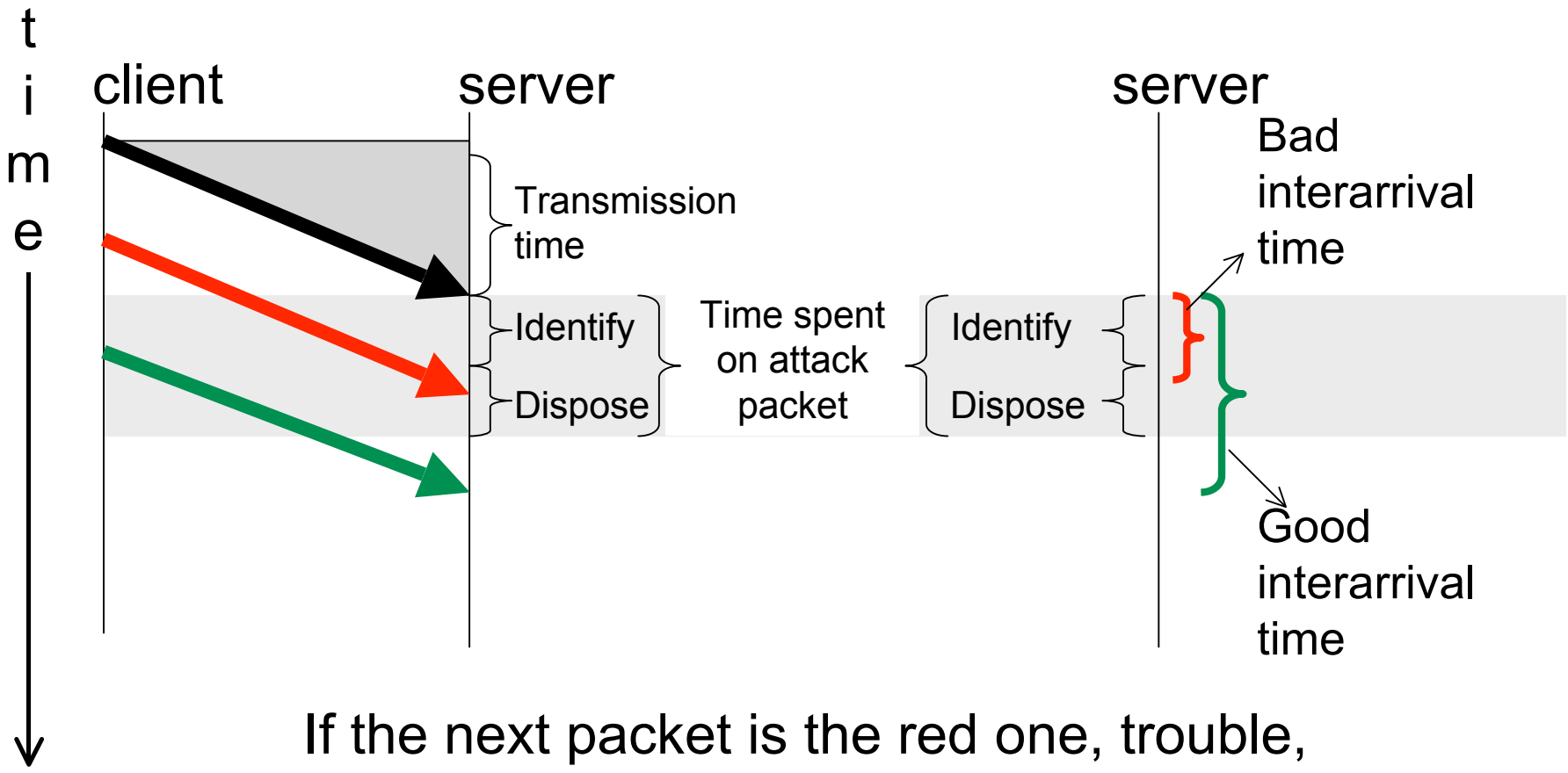
Time diagram - "red"



Time diagram - "green"



Time diagram



If the next packet is the red one, trouble,
if it is green, you are okay.

What do we do?

- Time to identify
  - Look for the attack's pattern
- Time to dispose
  - Filter, drop fast
- Inter-arrival time
  - More service points (e.g., load balancing)

Looking at "Service Points"

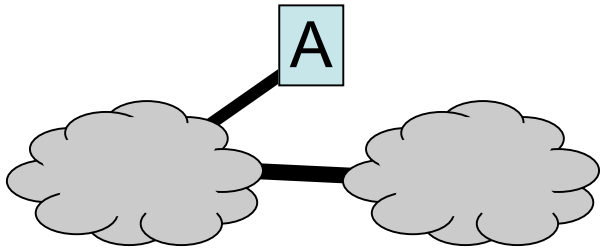
- More than just "add capacity"
  - Attacks can scale more cheaply than defenses
  - Well placed capacity needed
- Important building block: Anycast

Anycast

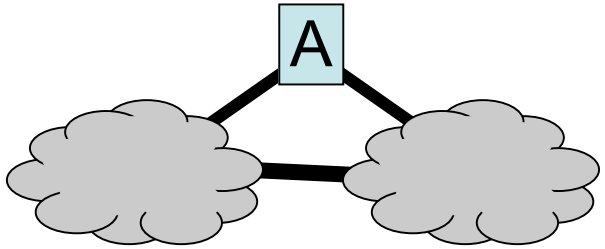
- Anycast basics
- Why it works
- When does it break?

Single-Multihomed-Anycast

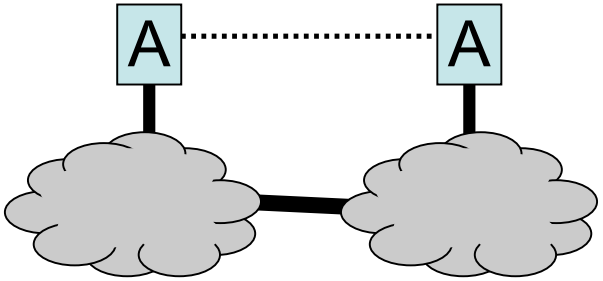
- Single Homed



- Multi-homed



- Anycast

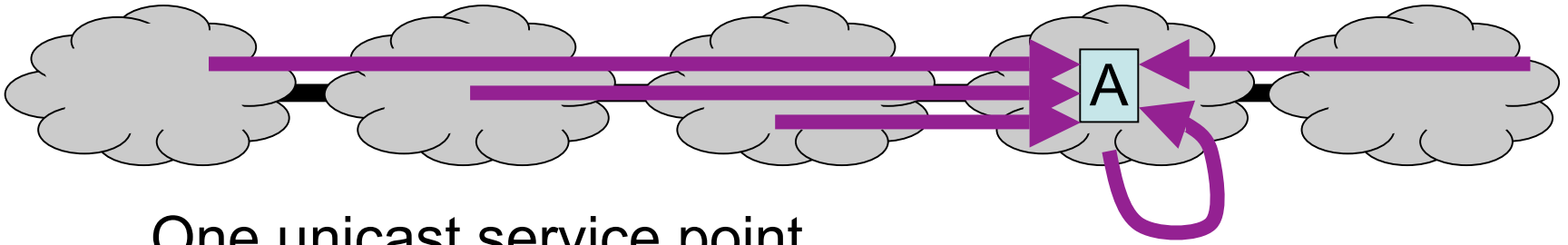


Anycast

- More instances, serving network localities
- Coordinated, best if servers are "stateless"
  - DNS is ideal
  - eCommerce not so ideal

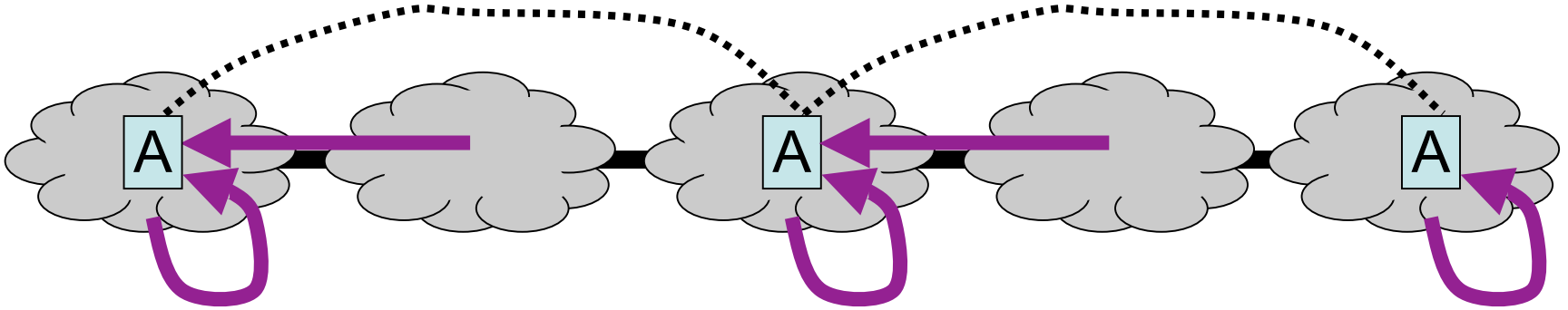
With/Without Anycast

Showing request flows



One unicast service point

Three anycast service points



Traffic increasingly isolated one ISP

Anycast Tradeoffs

- Saves Addresses
- Divide and Conquer strategy to handle large audiences
  - One large network looks like many simple
- Many points - higher costs of operation
- Must coordinate routing and application load balancing strategies

Routing Magic

- Anycast is about routing "magic"
  - Lets routing system determine the set of clients (the "audience") for a server
- To make this reliable, the routing determination must be "controlled."
  - Otherwise, instability and unpredictability take over

Effective Defense

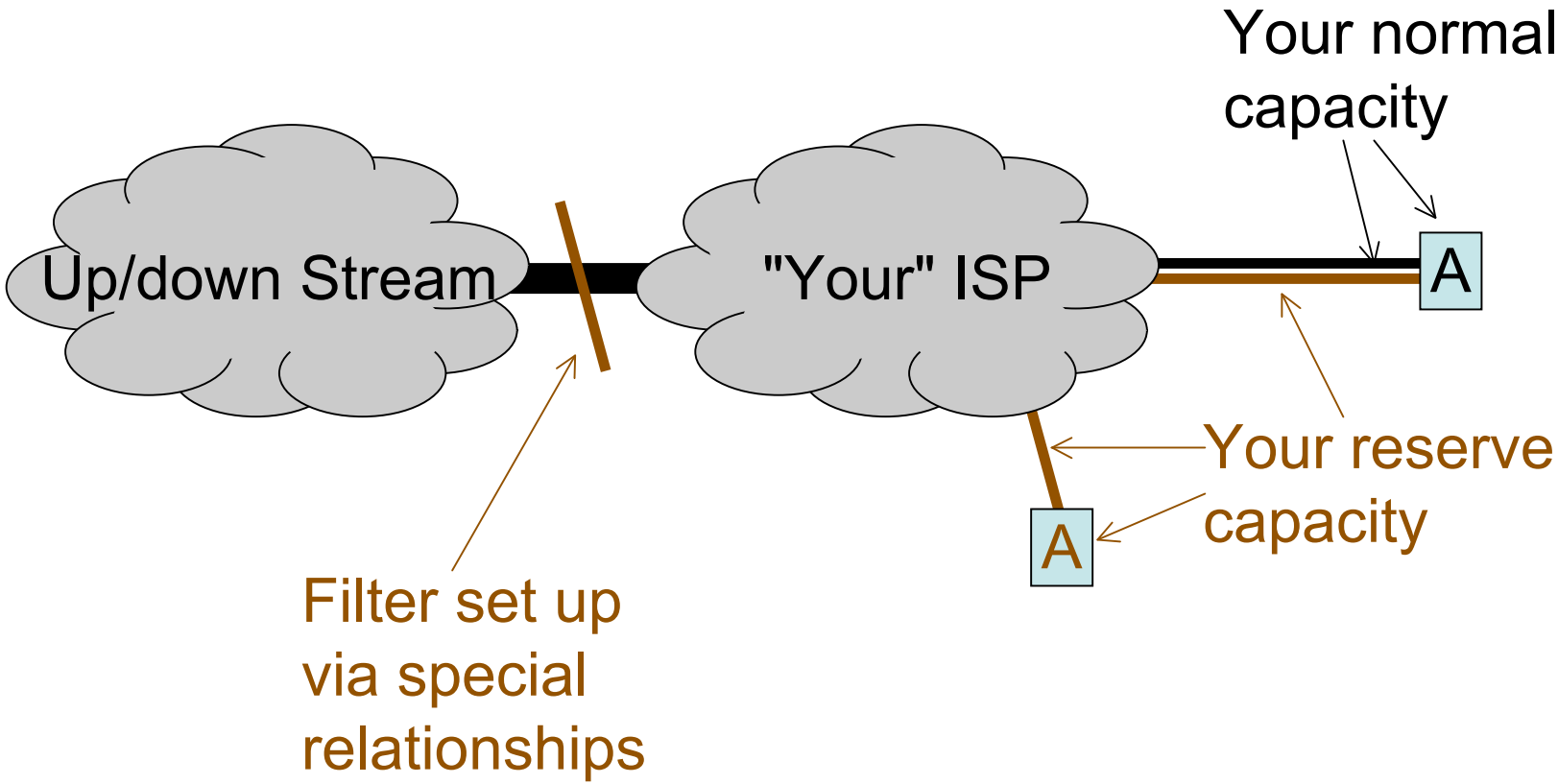
- Excess Provisioning
- Pre-positioning

- Anycast is a tool of each, but more work is still needed by each defensive strategy

Excess Provisioning

- One approach is to have more capacity than any attack
  - Resources that can be put into service only when needed (to cut cost of always "up")
  - Relationships to get help from the different ISPs through which all attack traffic flows.

Normal and Reserve Capacity



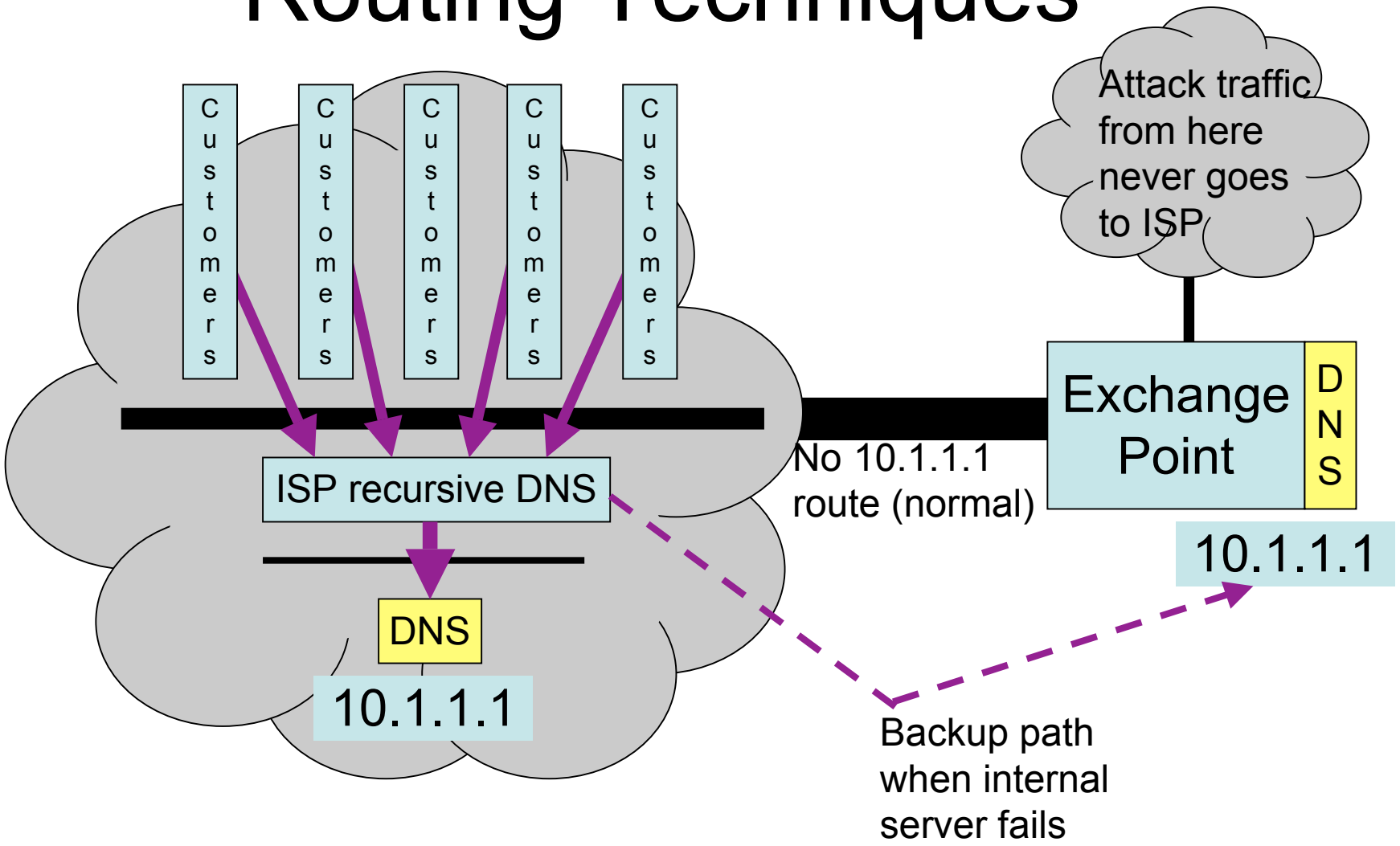
Limits

- Available "excess" capacity
  - There's a cost when unutilized
- Scale of (human) relationships
  - Requesting filters is not automated
  - Have to maintain global relations with ISPs

Pre-positioning

- Two part strategy
- Put data where it needs to be ahead of time
  - Good strategy for something like DNS
- Use routing to control where data is accessed
  - Try to minimize traffic between ISPs

Routing Techniques



Advantages of Pre-positioning

- Puts more control in hands of ISP
  - If attack traffic happens, it comes from within ISP, source is apparent
  - Makes network performance more stable
- Better access in "non-attack" times
  - Closer servers mean faster roundtrips

Conclusion

- DDoS attacks are part of the Internet
- Defense can't count on scaling past size of attack
- Data servers in ISP benefits service provider, ISP, and customers
  - And simplifies the network
  - Needs ISP to trust service provider!

The last slide

- Discussion?