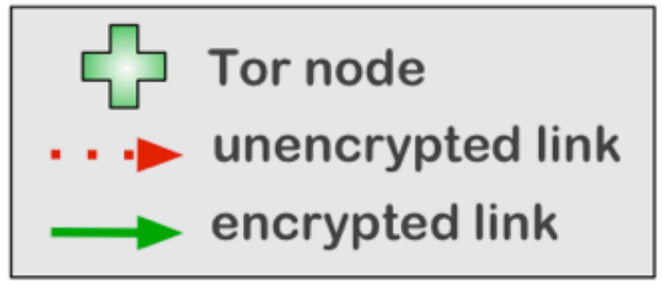
# Hiding Amongst the Clouds

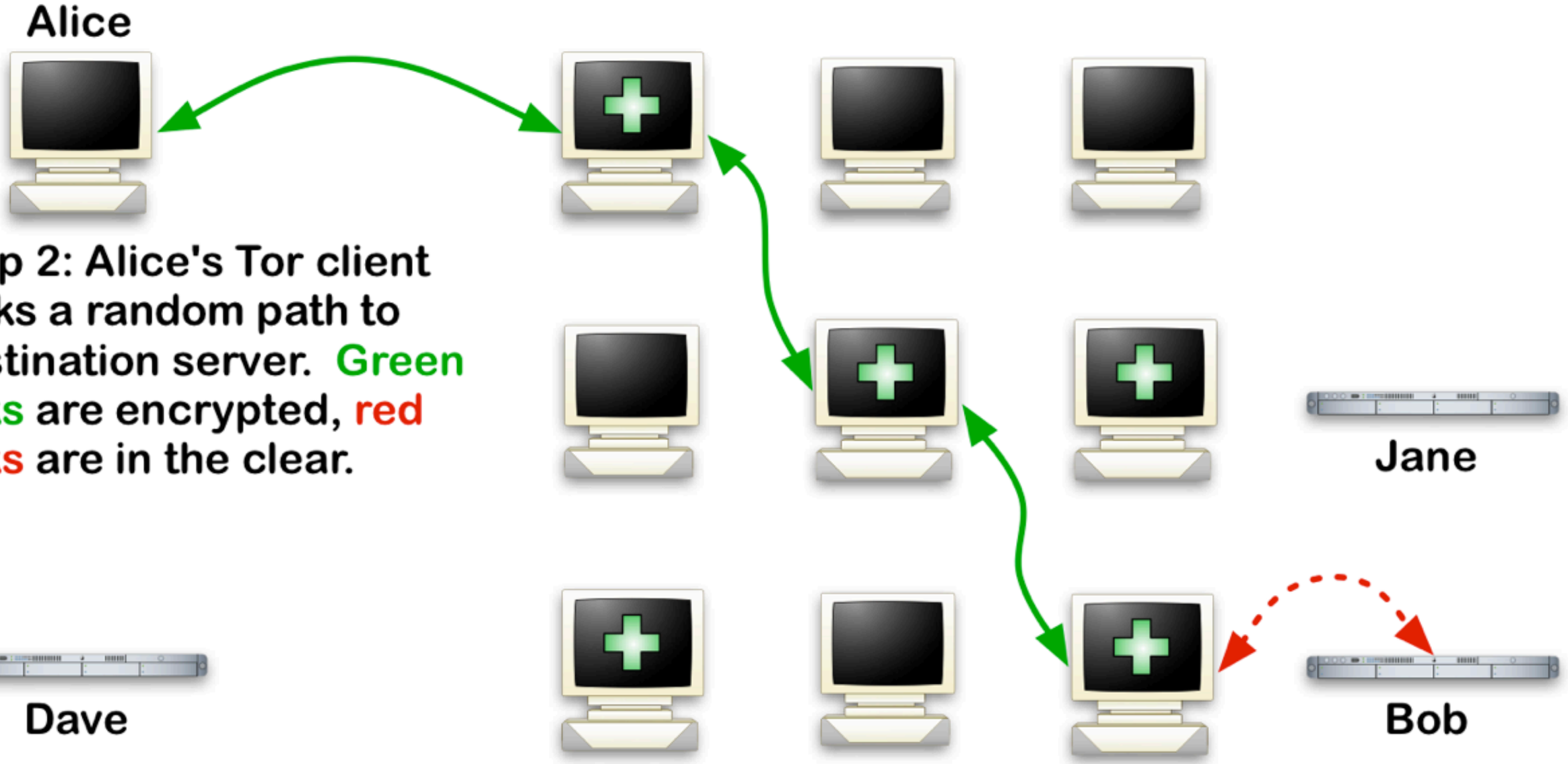
A Proposal for Cloud-based Onion Routing

**Nicholas Jones**
Matvey Arye
Jacopo Cesareo
Michael J. Freedman

Princeton University

# How Tor Works: 2



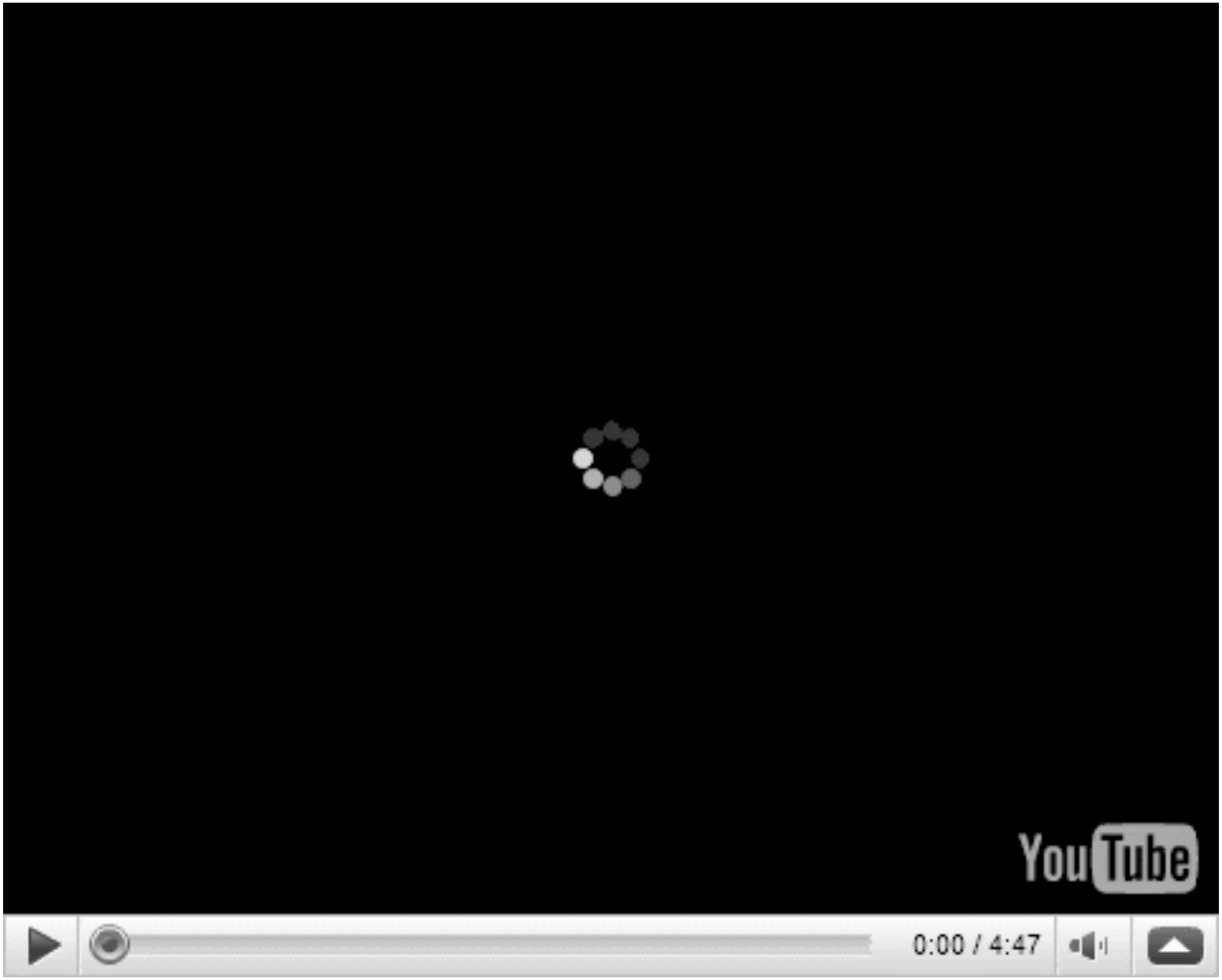

https://www.torproject.org/about/overview.html

We  Tor

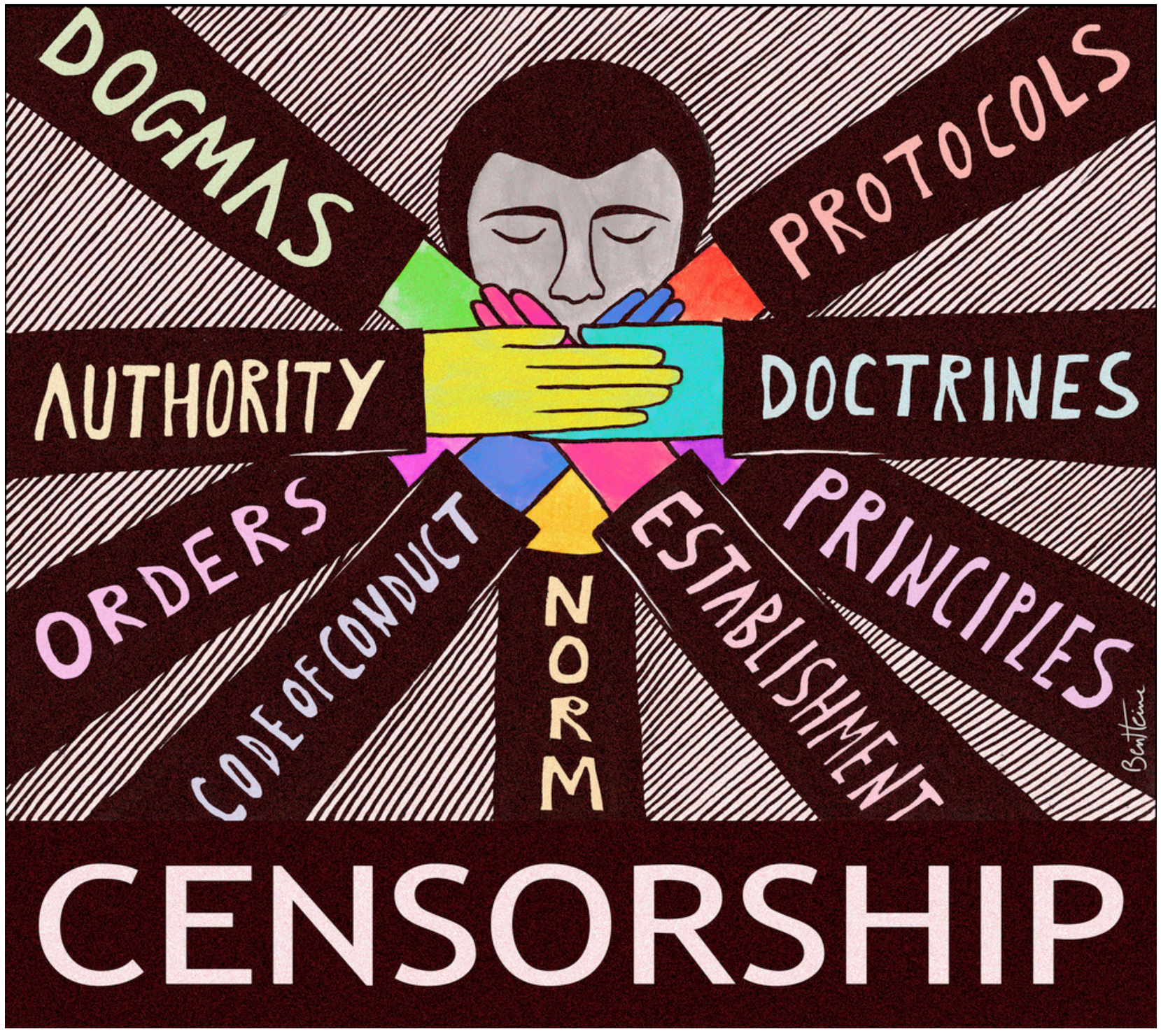
and

AVAILABLE ONLINE FOR FREE

but...


YouTube
0:00 / 4:47

and


DOGMAS
PROTOCOLS
AUTHORITY
DOCTRINES
ORDERS
CODE OF CONDUCT
NORM
ESTABLISHMENT
PRINCIPLES
CENSORSHIP

**C**loud-based

**O**nion

**R**outing

# Benefits, Risks, and Challenges

- Potential benefits of cloud infrastructure
    - High performance
    - Adaptability to censorship
- Economic challenges
- New security problems

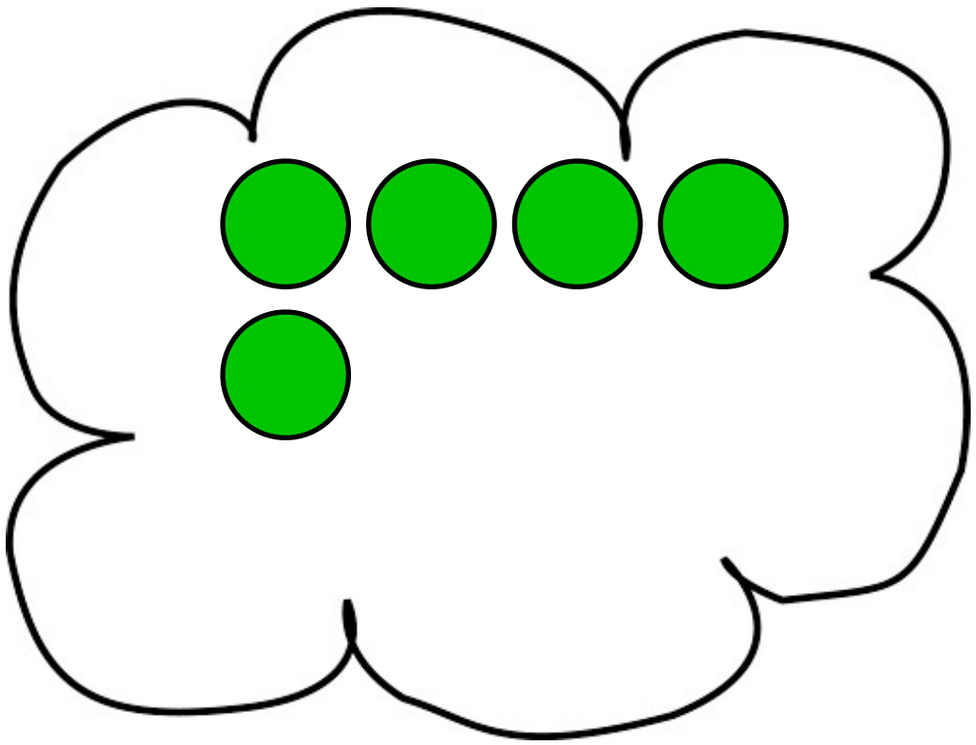
# Benefits of Cloud Infrastructure

Performance (latency, throughput)
Censorship Resistance

# Performance

- Individual nodes are higher bandwidth

- Ability to add and remove nodes to meet demand



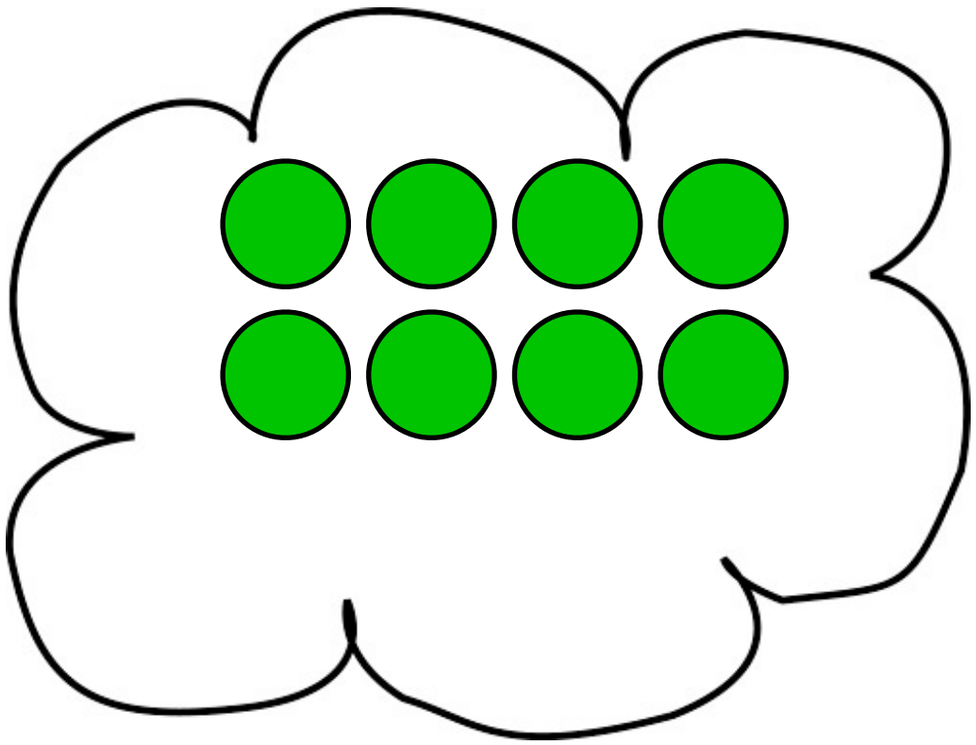
NETFLIX

5:00 P.M.

# Performance

- Individual nodes are higher bandwidth

- Ability to add and remove nodes to meet demand



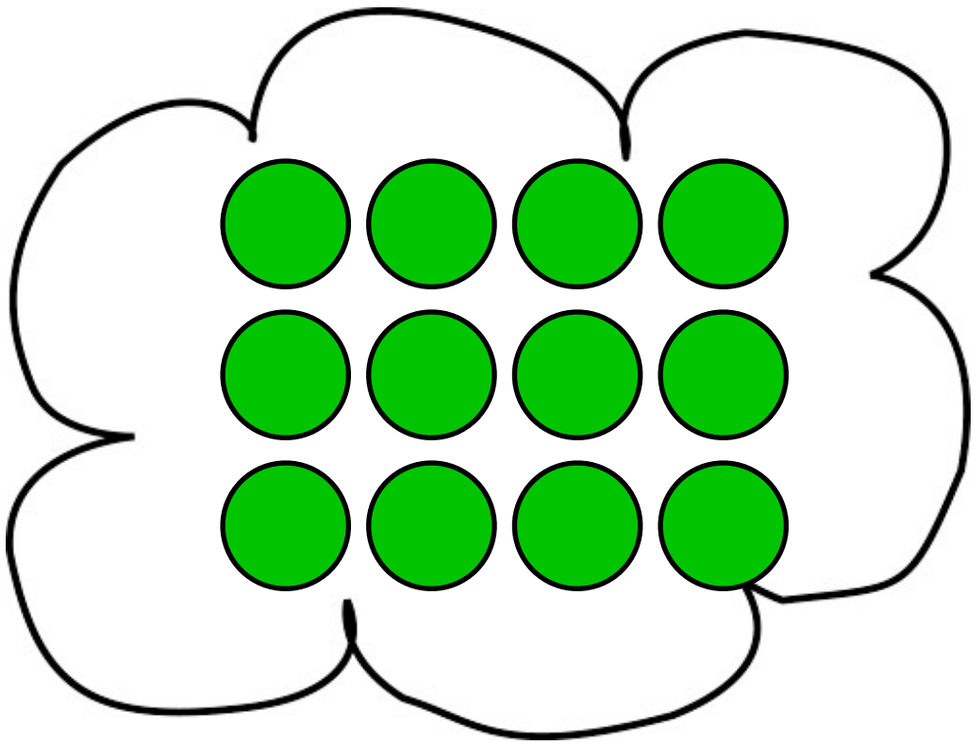
NETFLIX

7:00 P.M.

# Performance

- Individual nodes are higher bandwidth

- Ability to add and remove nodes to meet demand



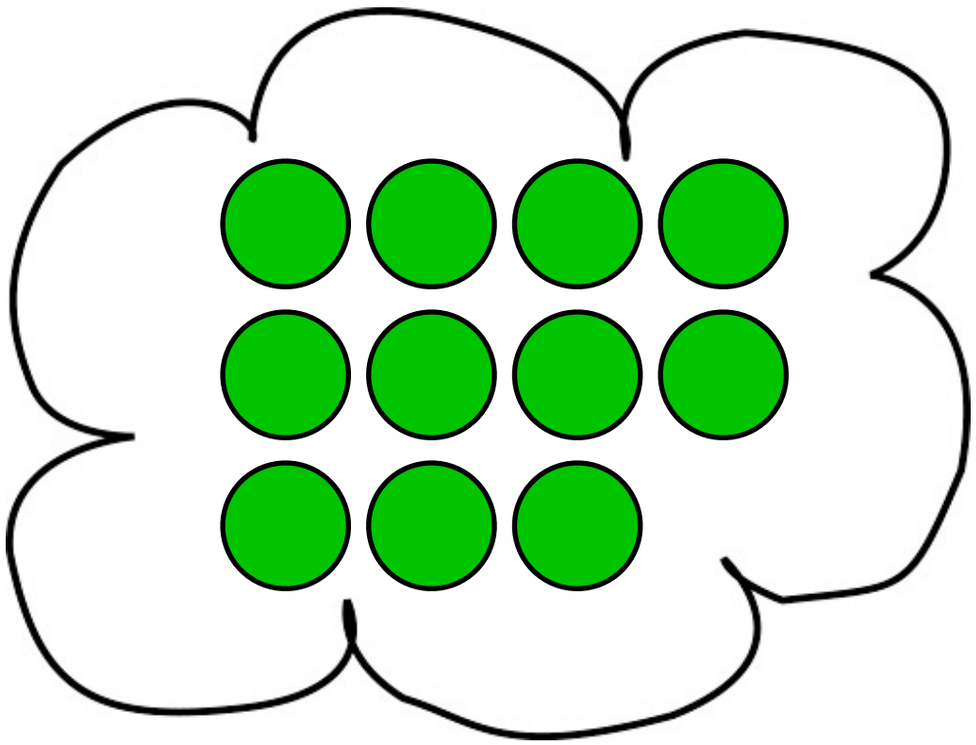
NETFLIX

8:00 P.M.

# Performance

- Individual nodes are higher bandwidth

- Ability to add and remove nodes to meet demand



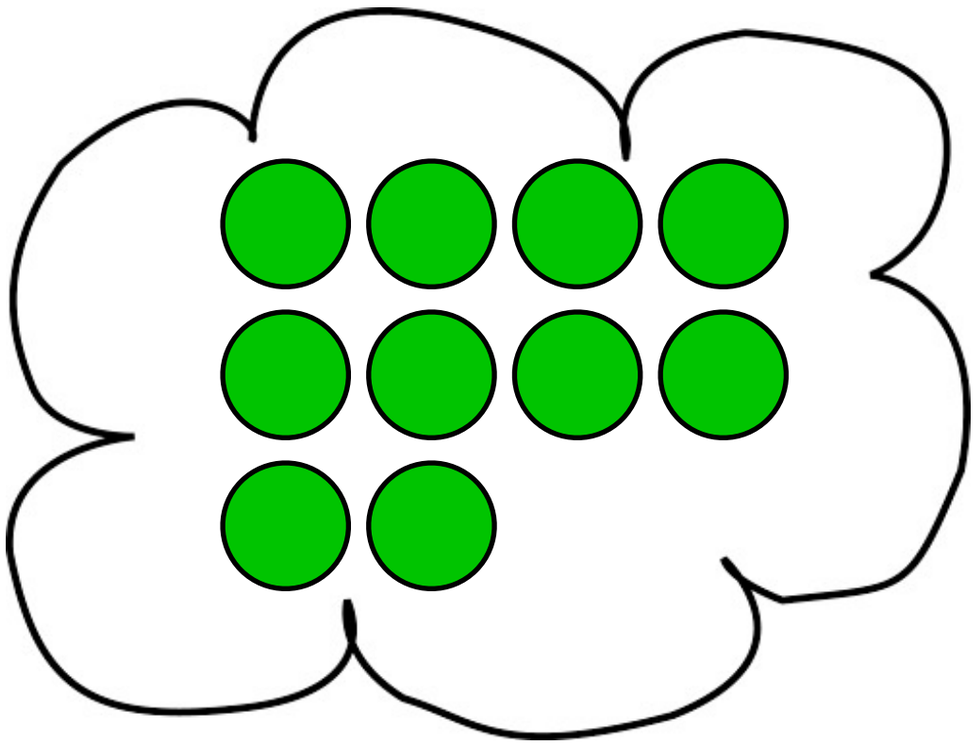
NETFLIX

11:00 P.M.

# Performance

- Individual nodes are higher bandwidth

- Ability to add and remove nodes to meet demand



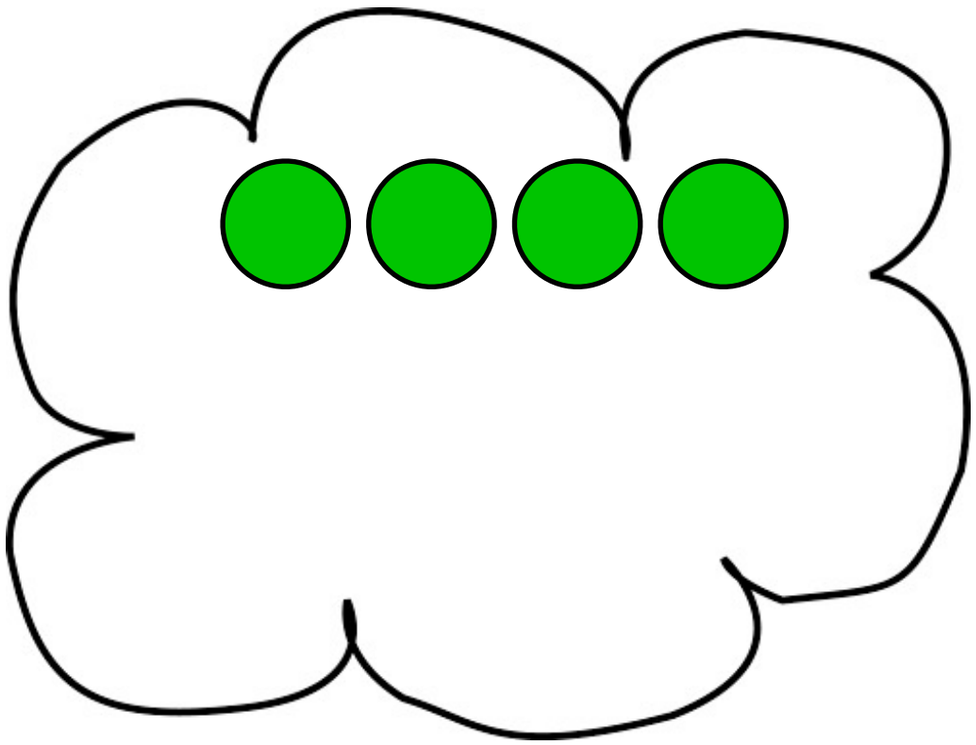
NETFLIX

12:00 A.M.

# Performance

- Individual nodes are higher bandwidth

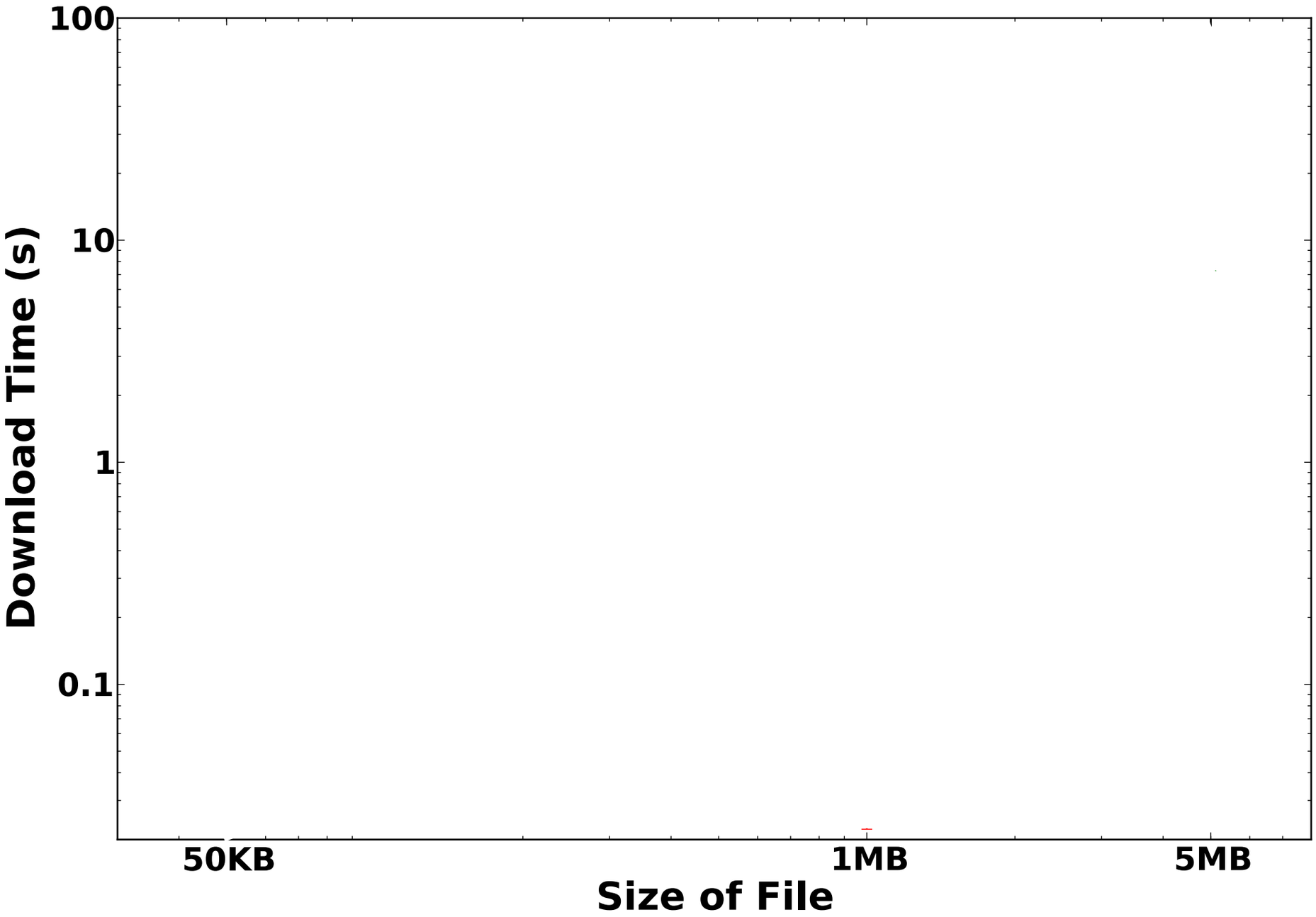
- Ability to add and remove nodes to meet demand



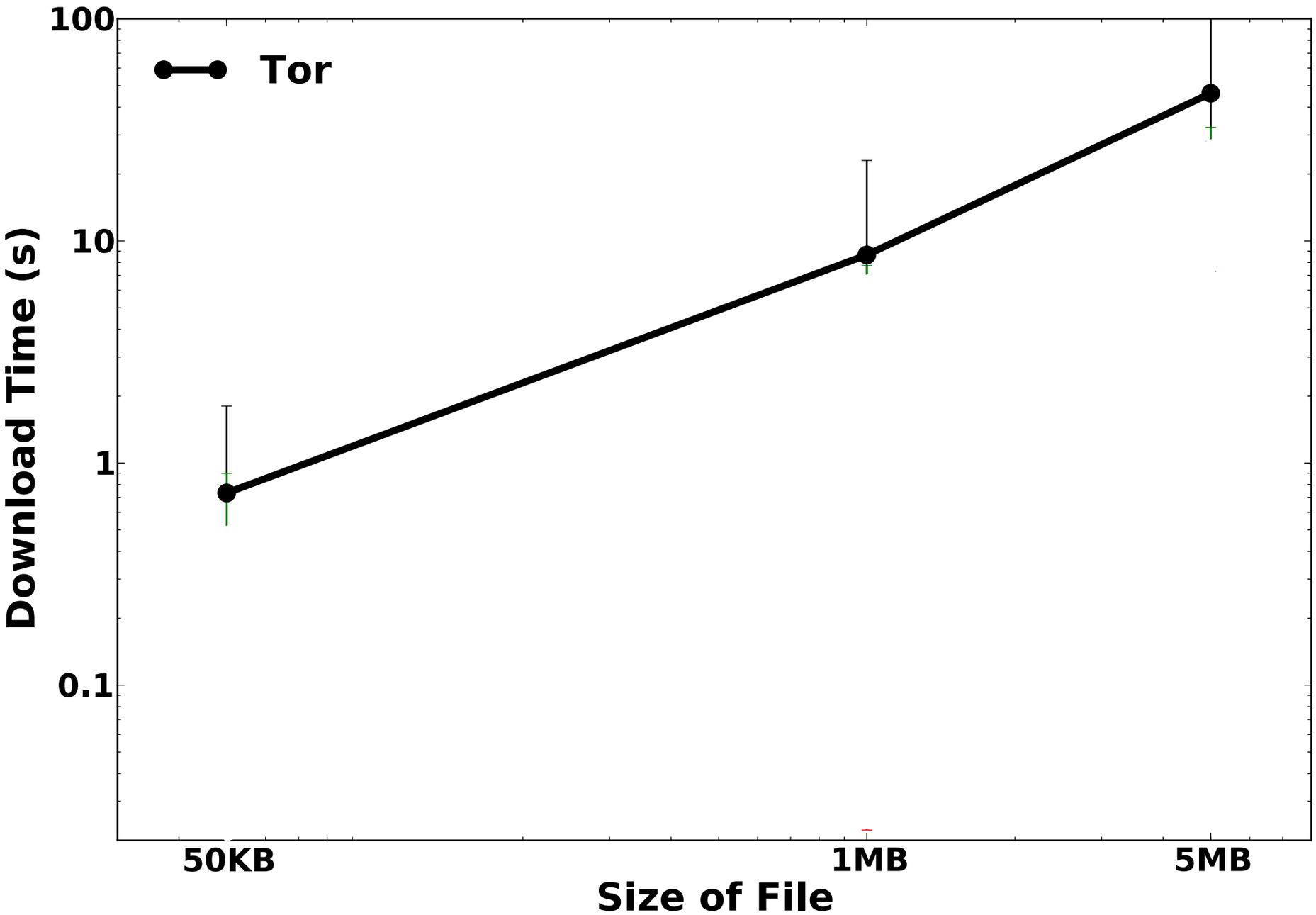
NETFLIX

2:00 A.M.

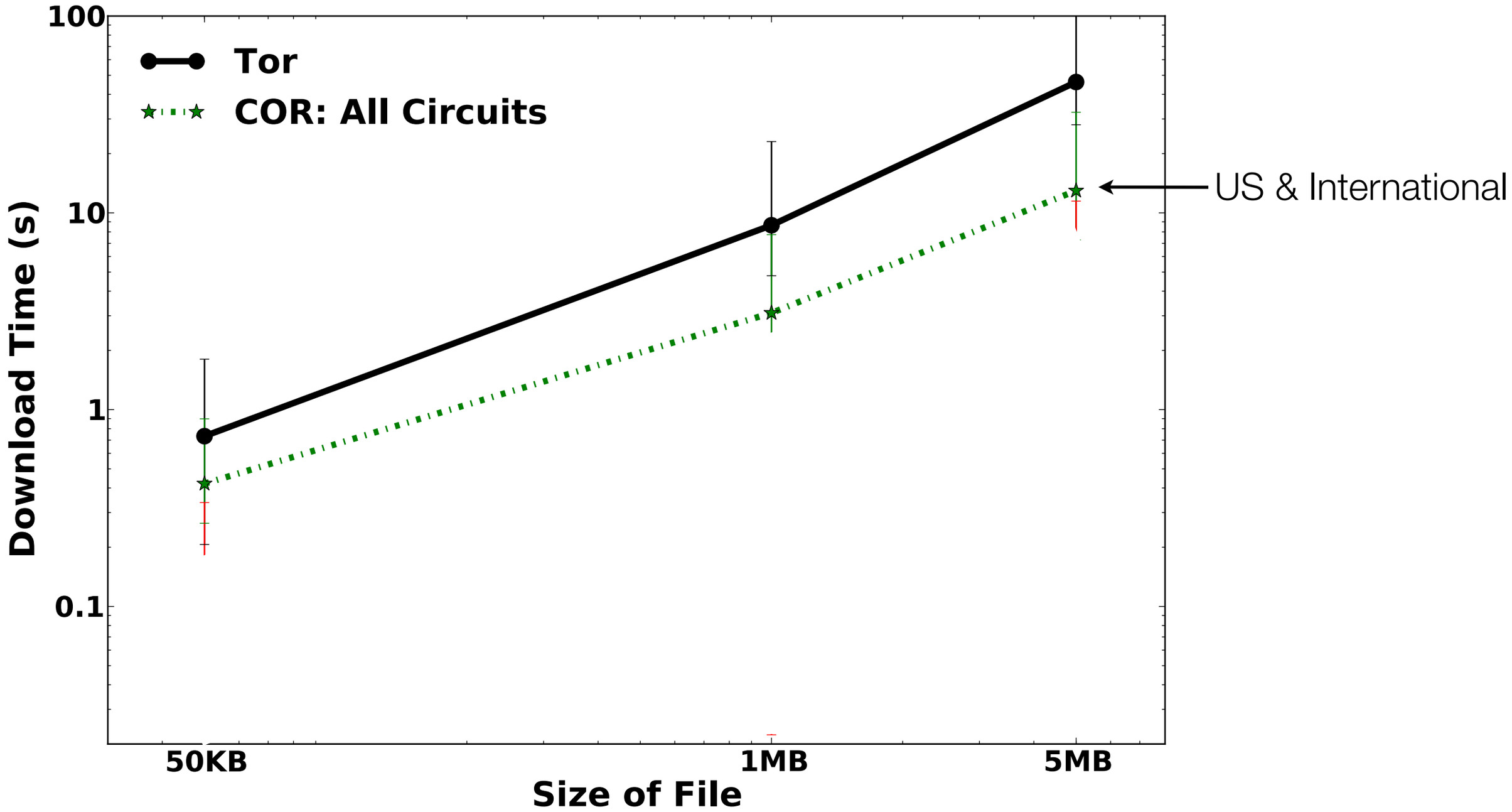
# COR has higher throughput than Tor



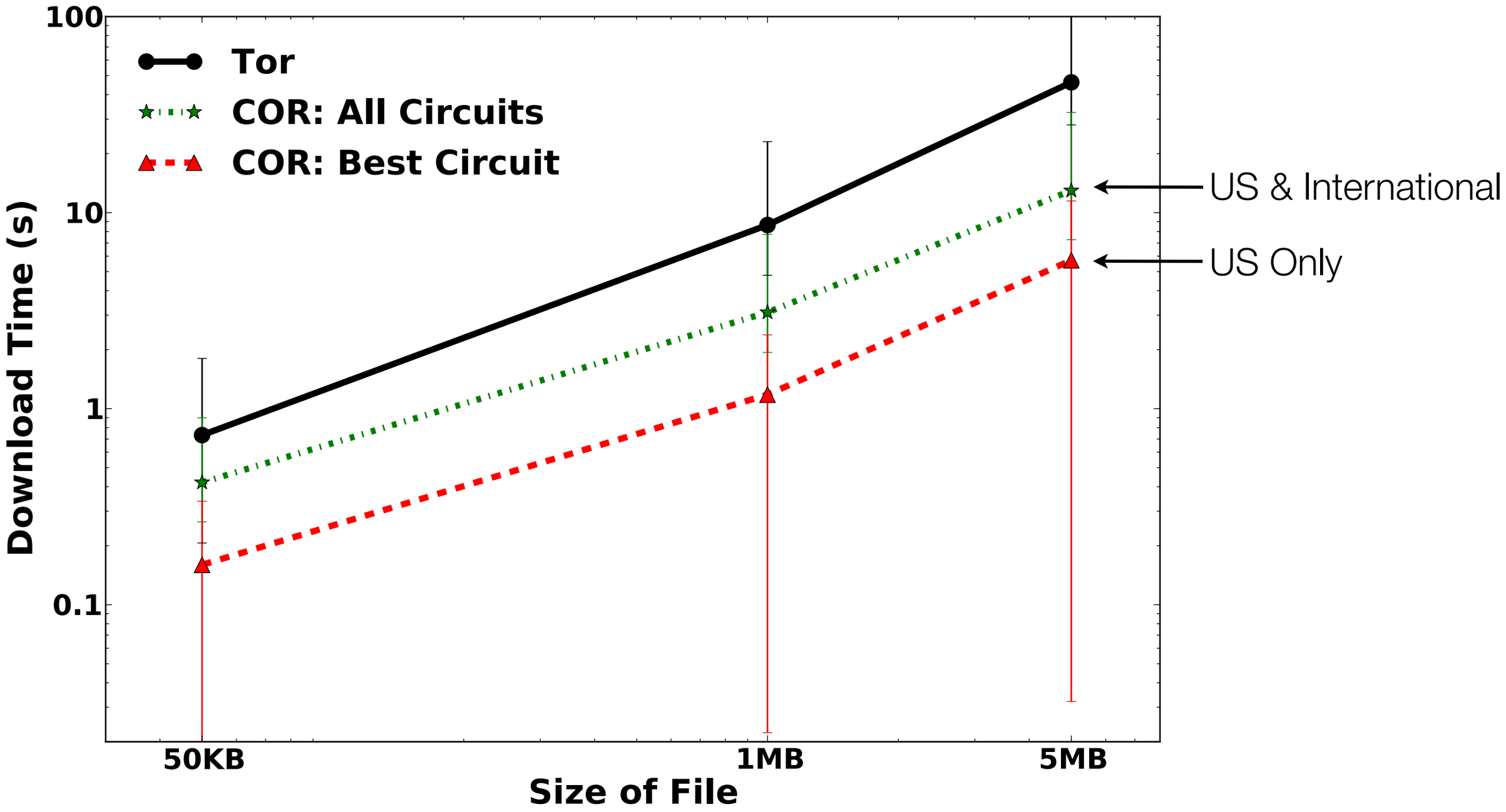
# COR has higher throughput than Tor



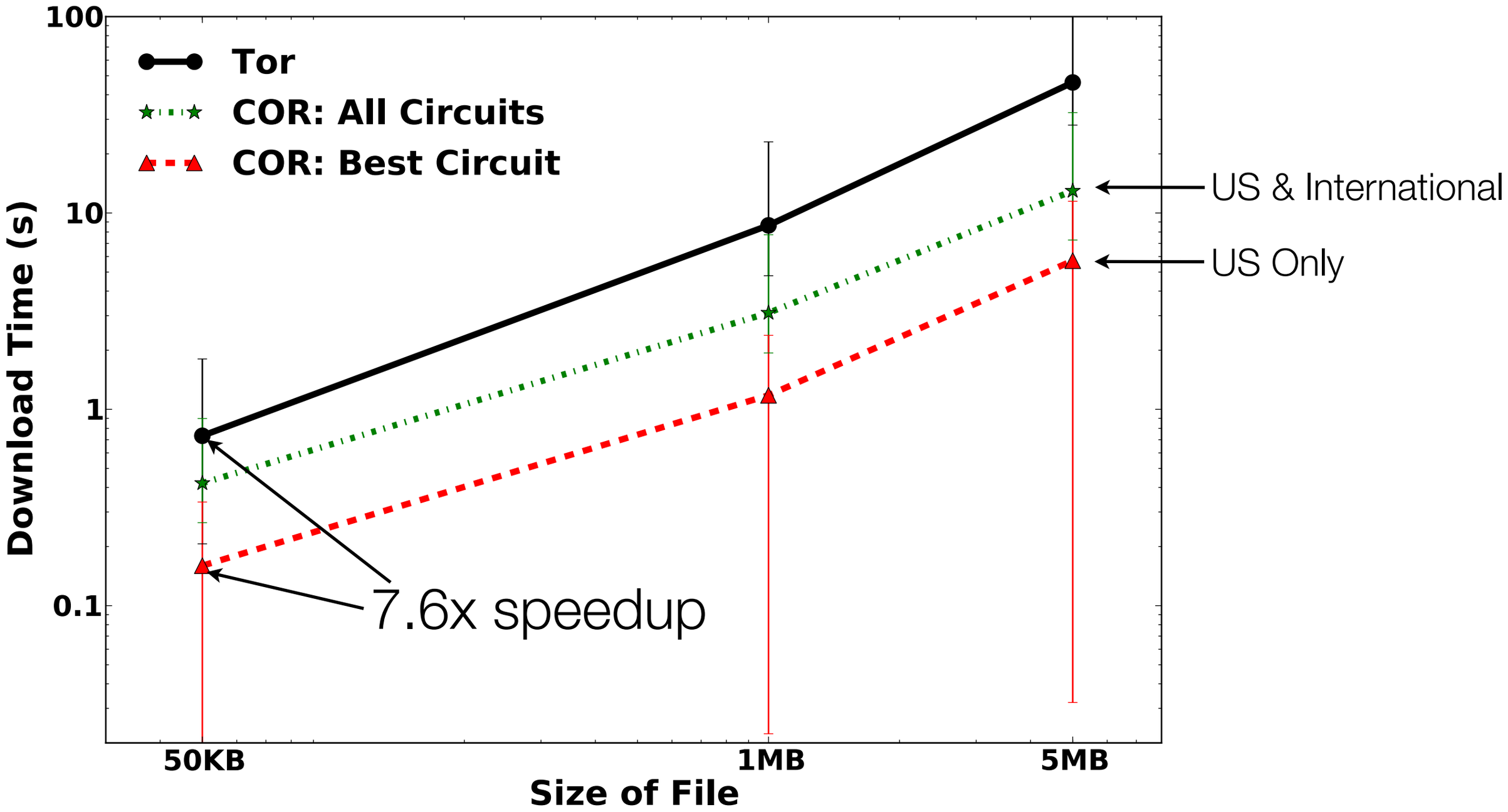
# COR has higher throughput than Tor



# COR has higher throughput than Tor

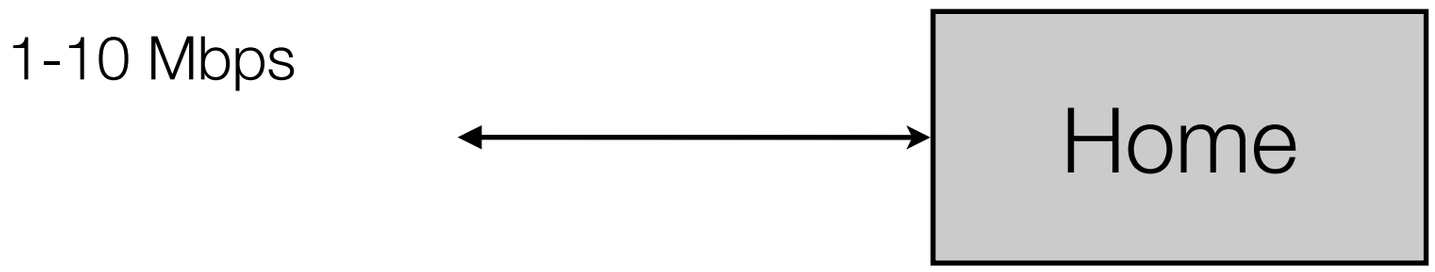


# COR has higher throughput than Tor



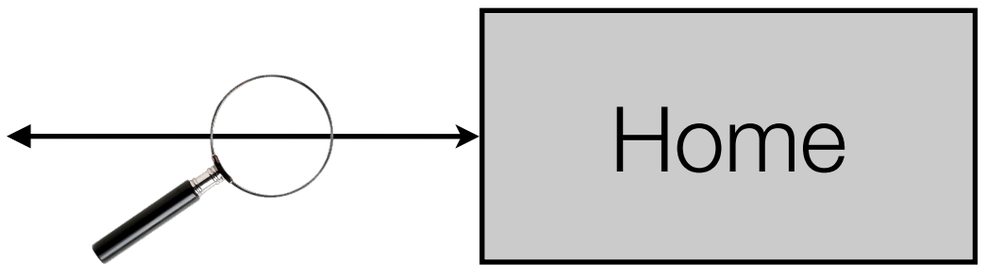
# Multi-homed Datacenters are Harder to Monitor

# Multi-homed Datacenters are Harder to Monitor



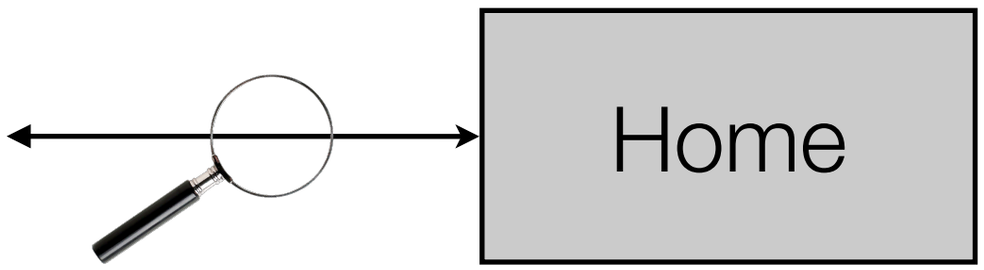
# Multi-homed Datacenters are Harder to Monitor

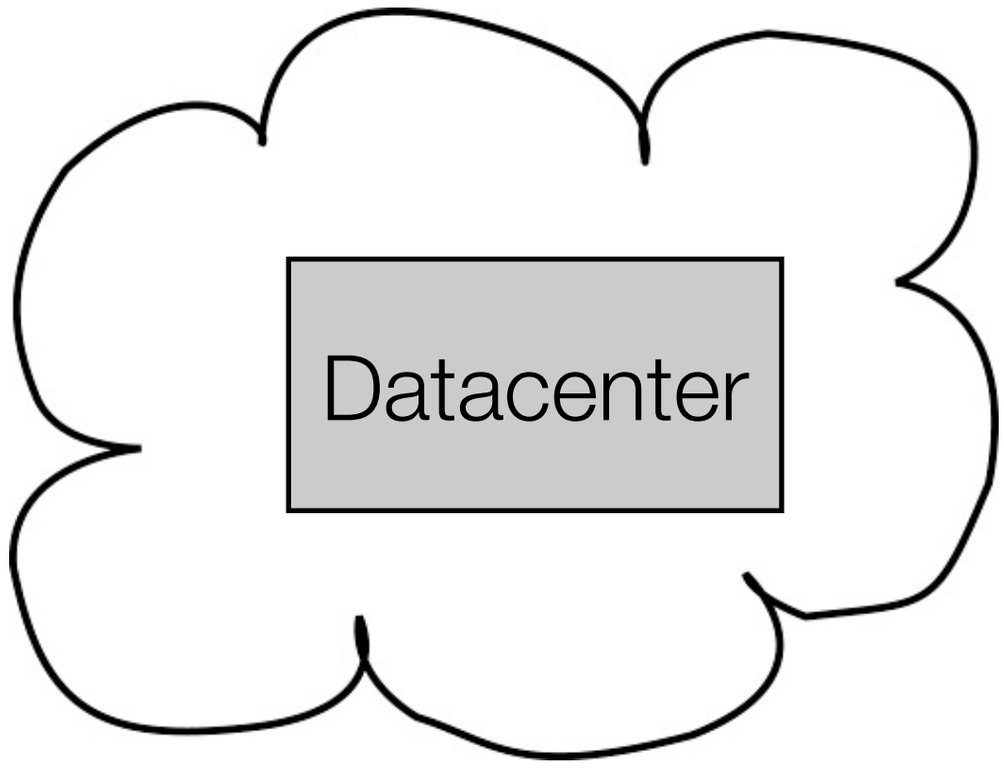
1-10 Mbps



# Multi-homed Datacenters are Harder to Monitor

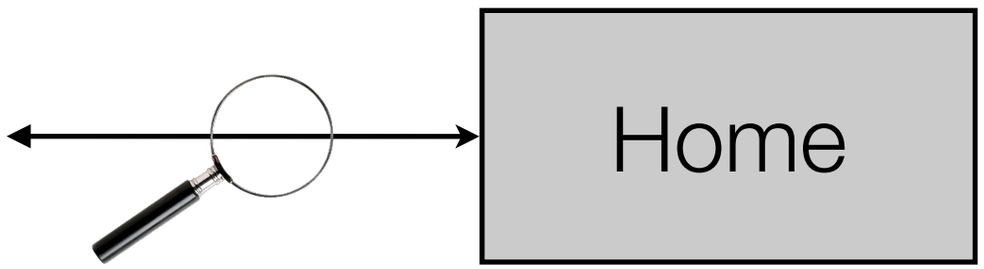
1-10 Mbps



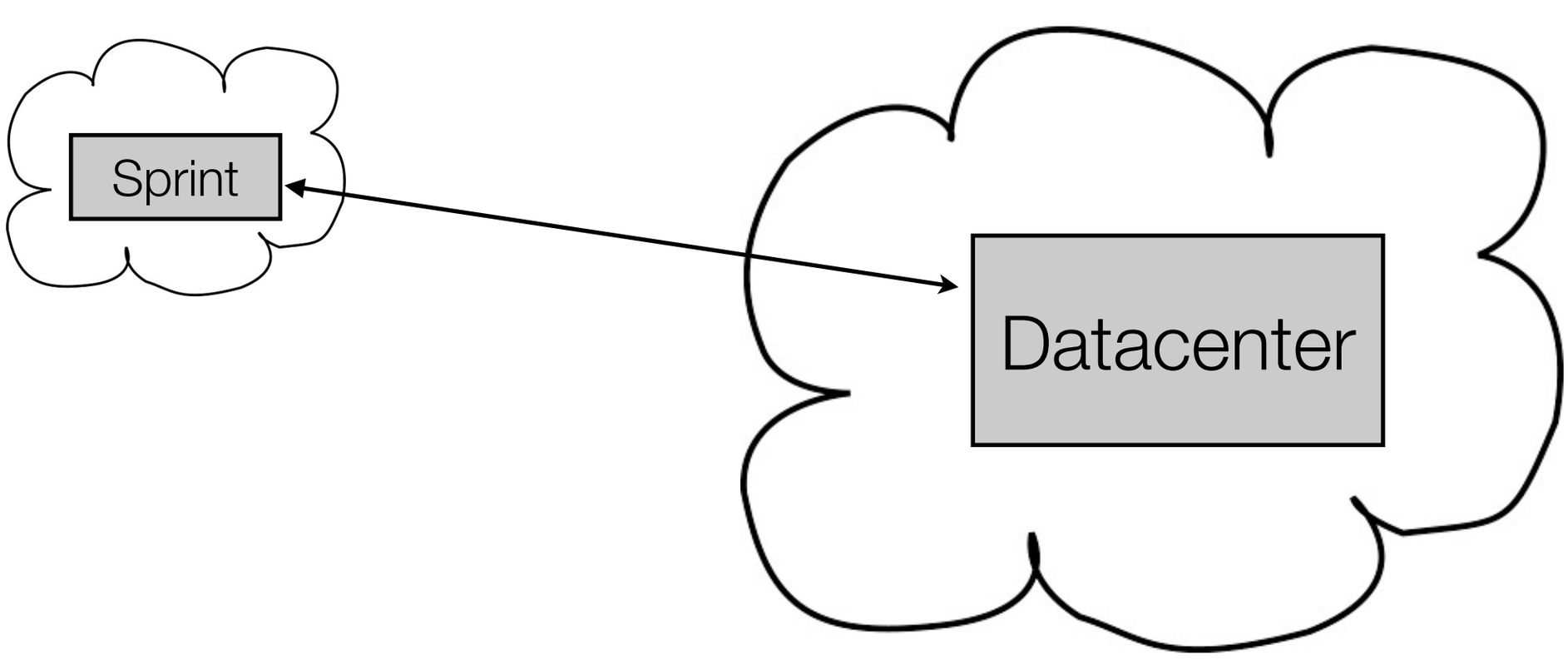



# Multi-homed Datacenters are Harder to Monitor

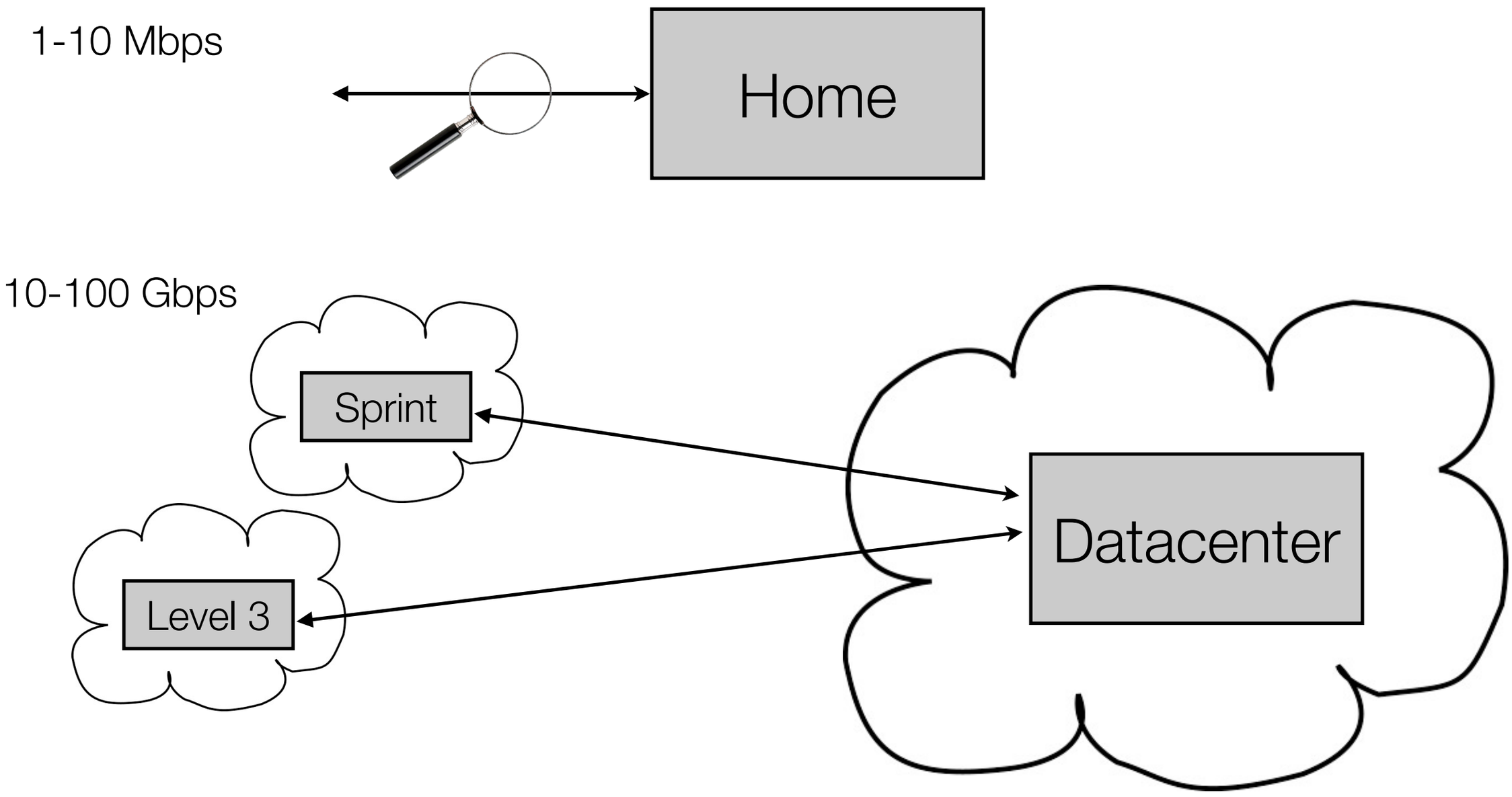
1-10 Mbps



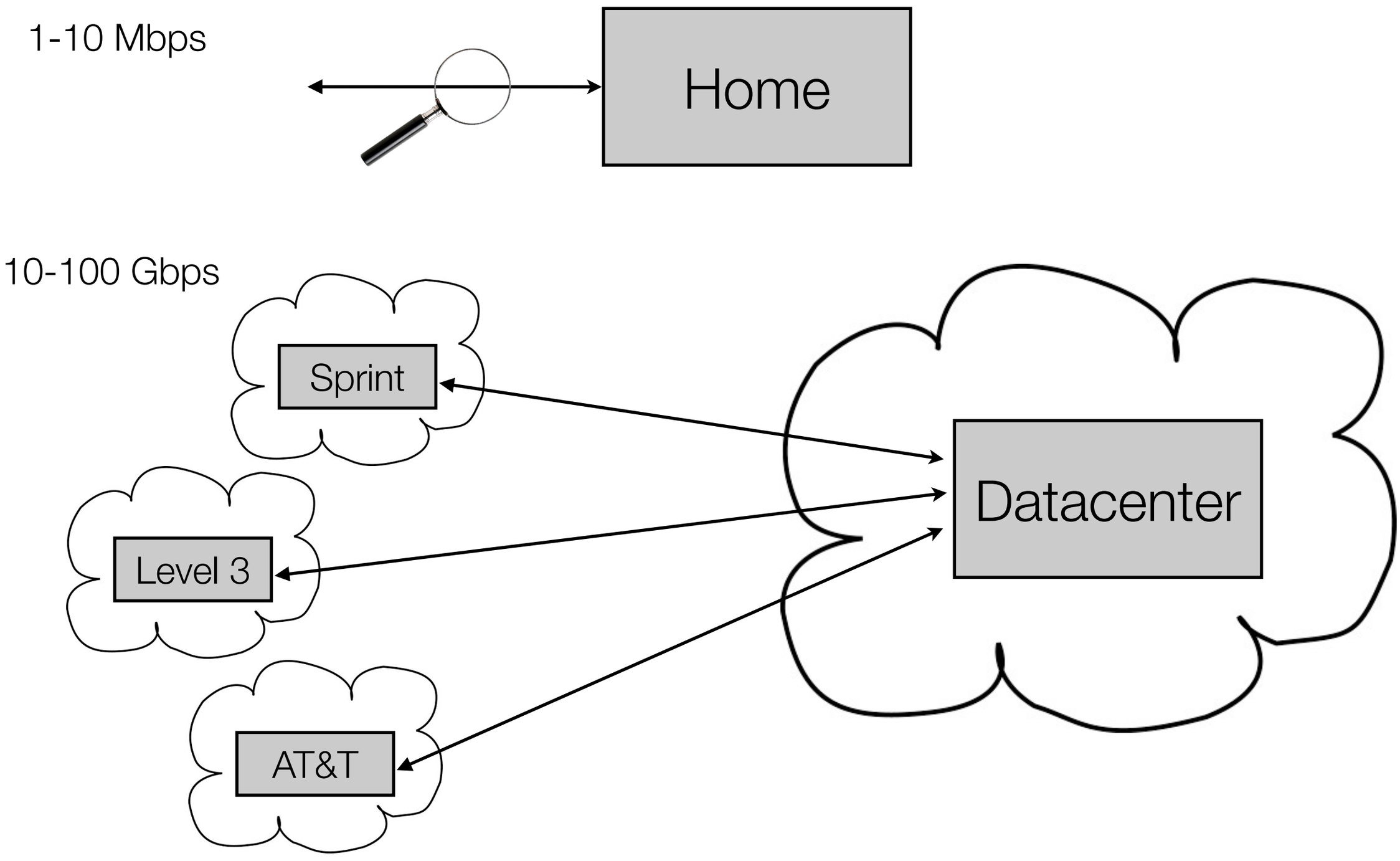

10-100 Gbps



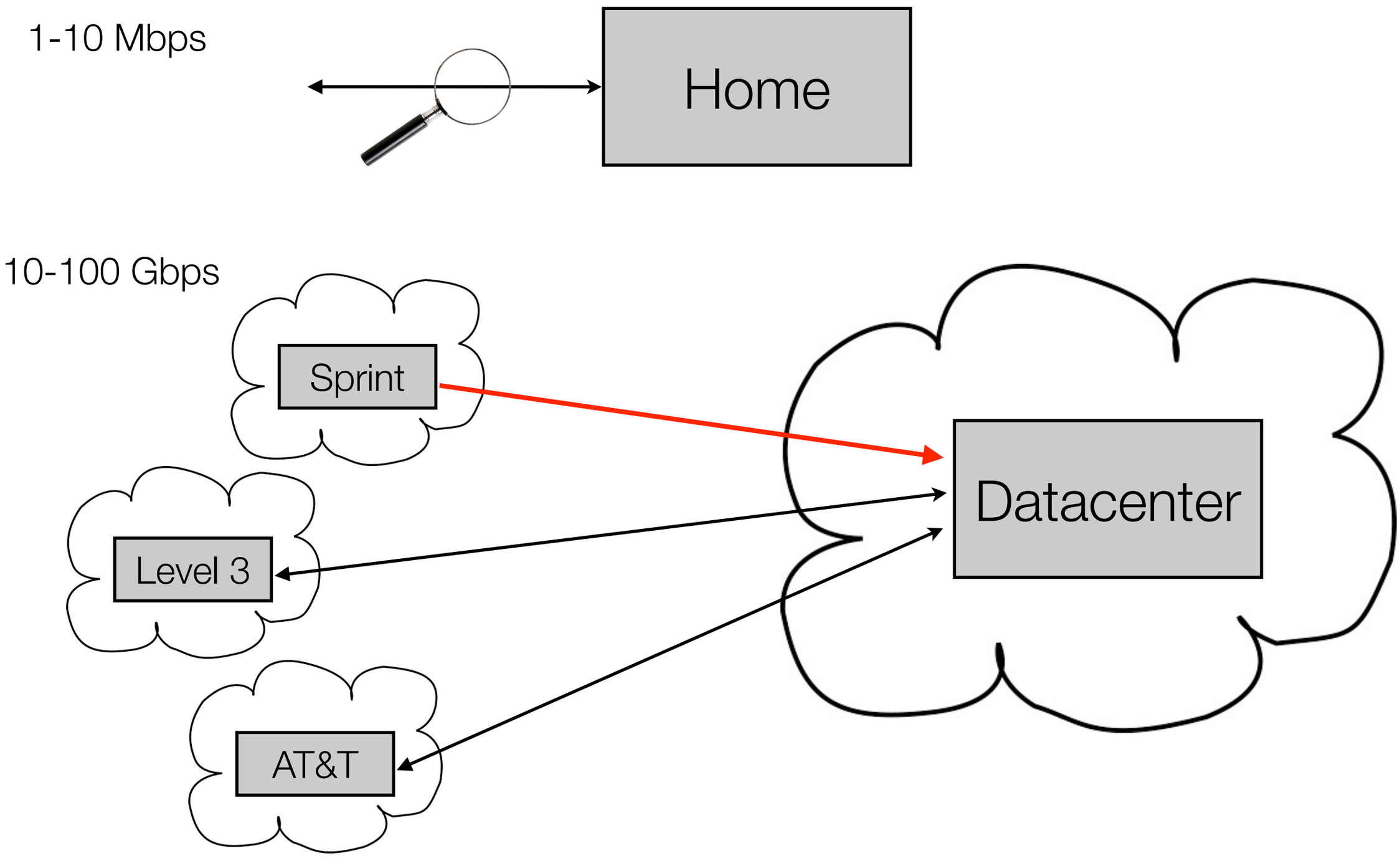
# Multi-homed Datacenters are Harder to Monitor



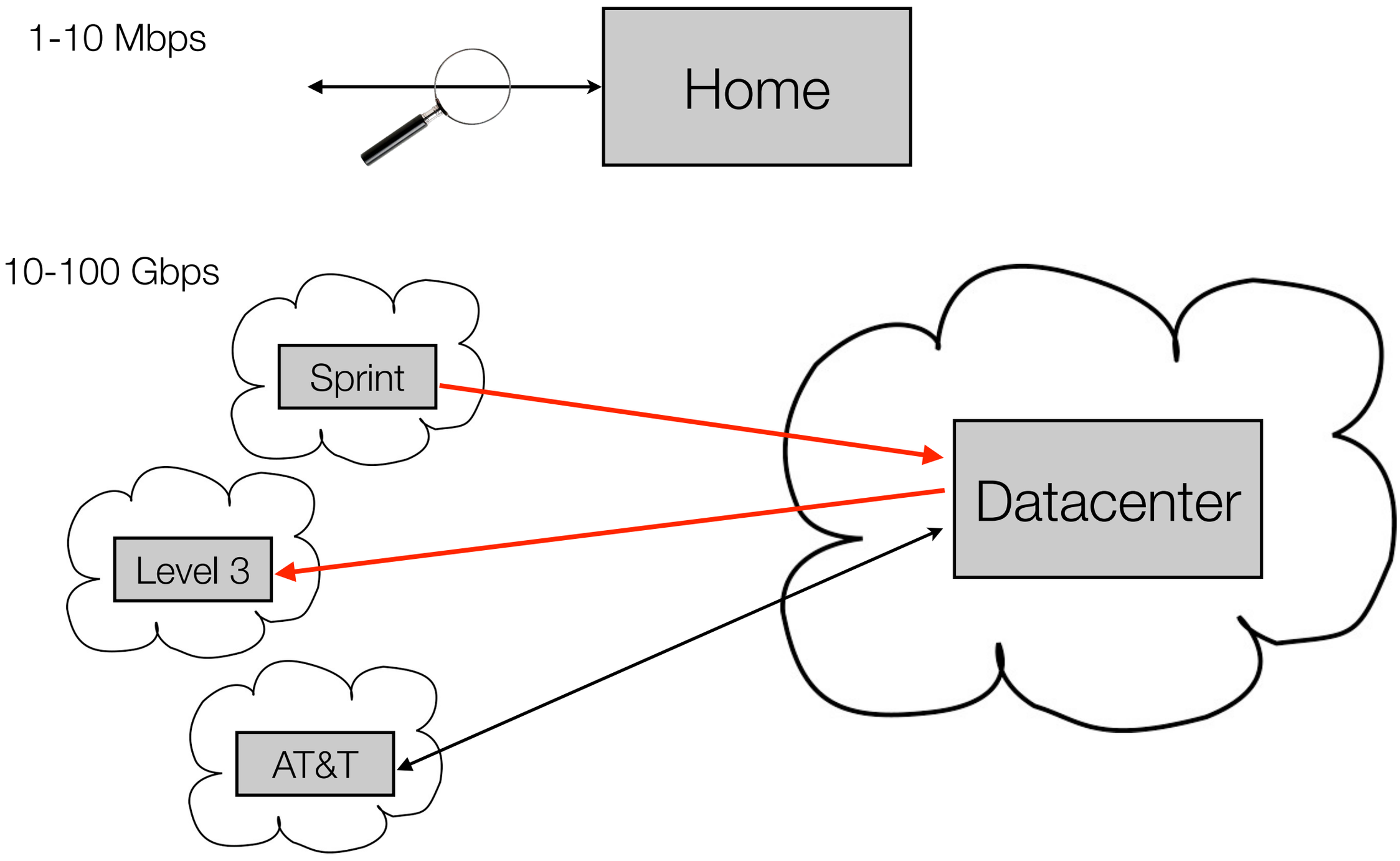
# Multi-homed Datacenters are Harder to Monitor



# Multi-homed Datacenters are Harder to Monitor

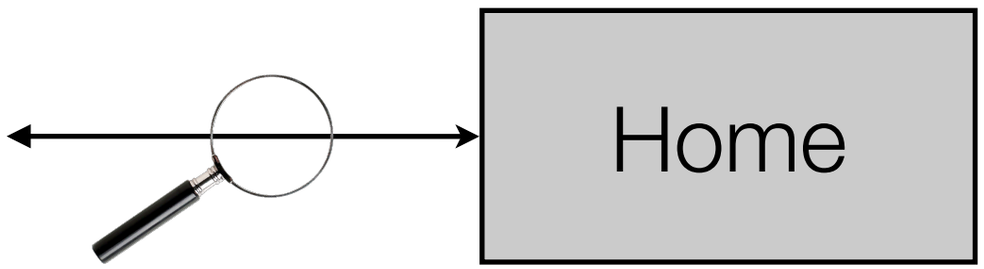


# Multi-homed Datacenters are Harder to Monitor

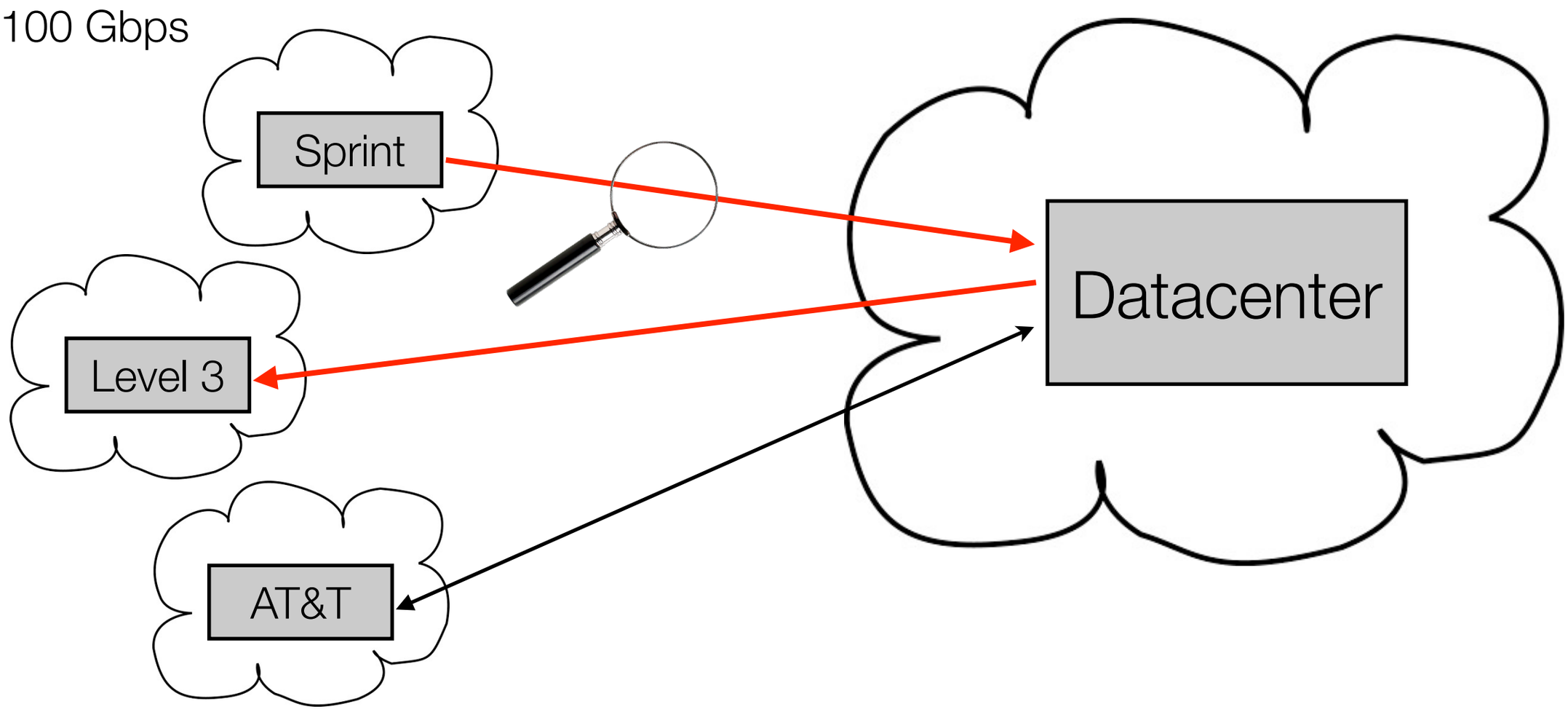


# Multi-homed Datacenters are Harder to Monitor

1-10 Mbps

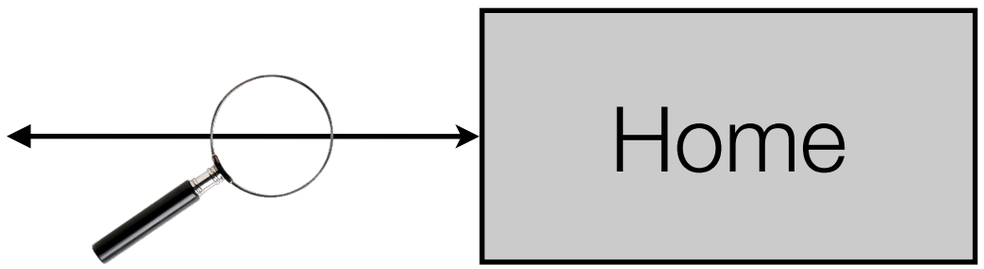



10-100 Gbps

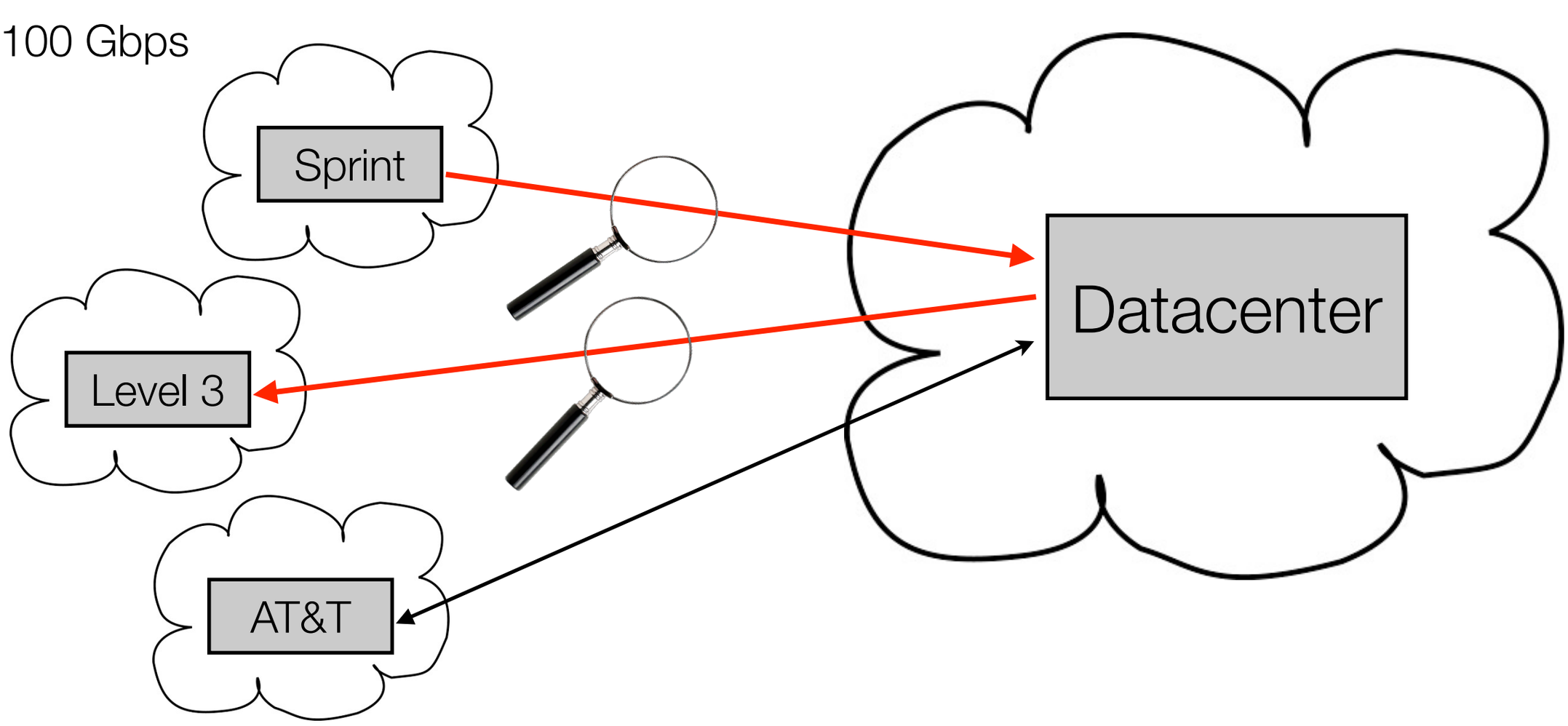


# Multi-homed Datacenters are Harder to Monitor

1-10 Mbps

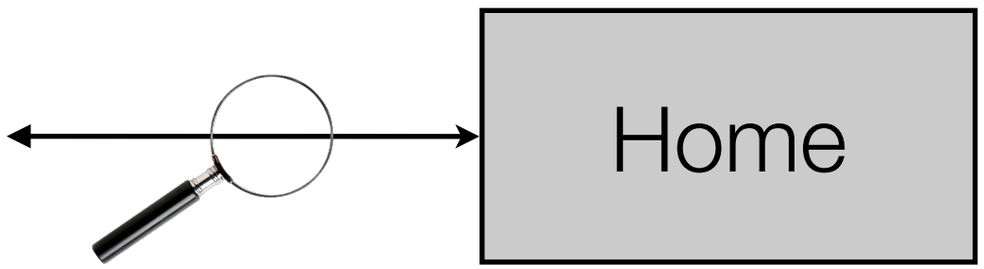



10-100 Gbps

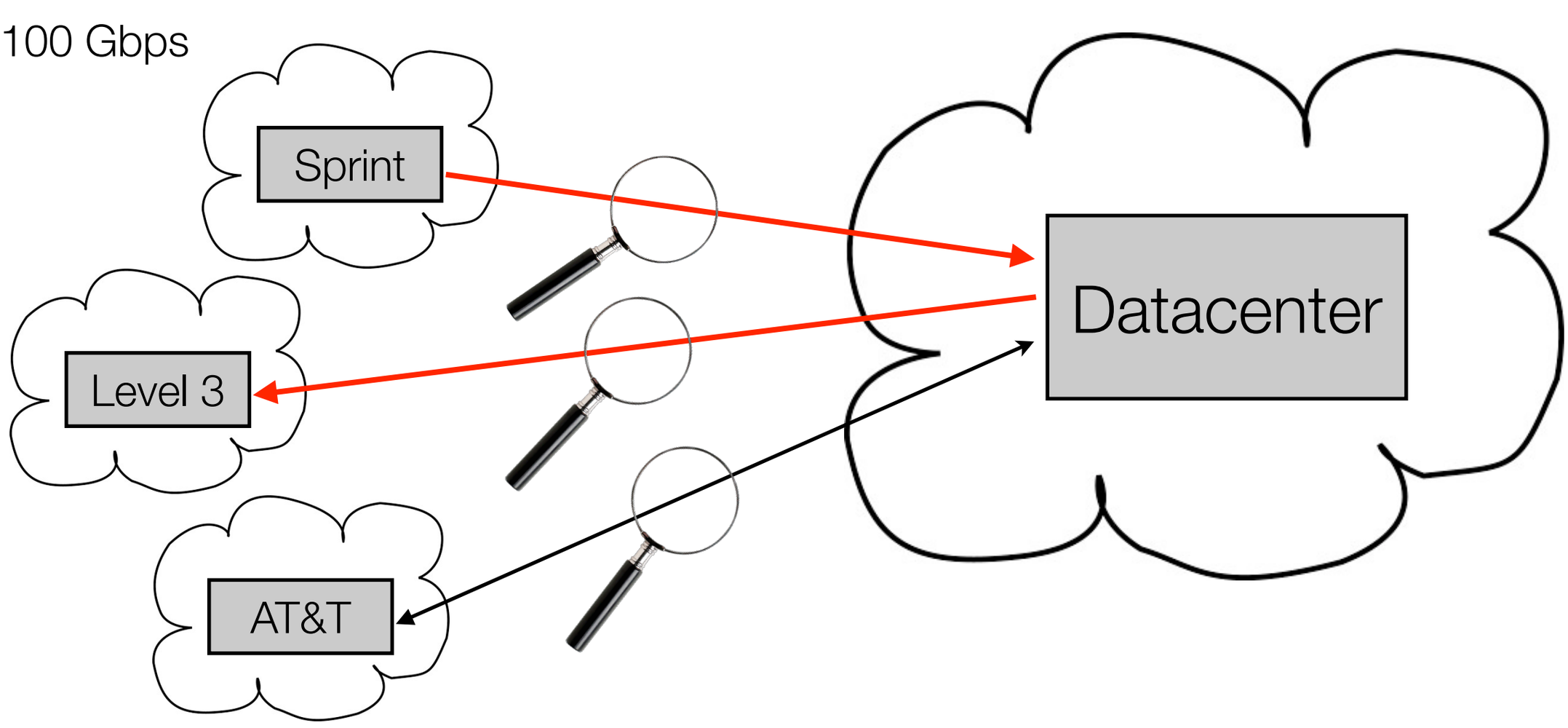


# Multi-homed Datacenters are Harder to Monitor

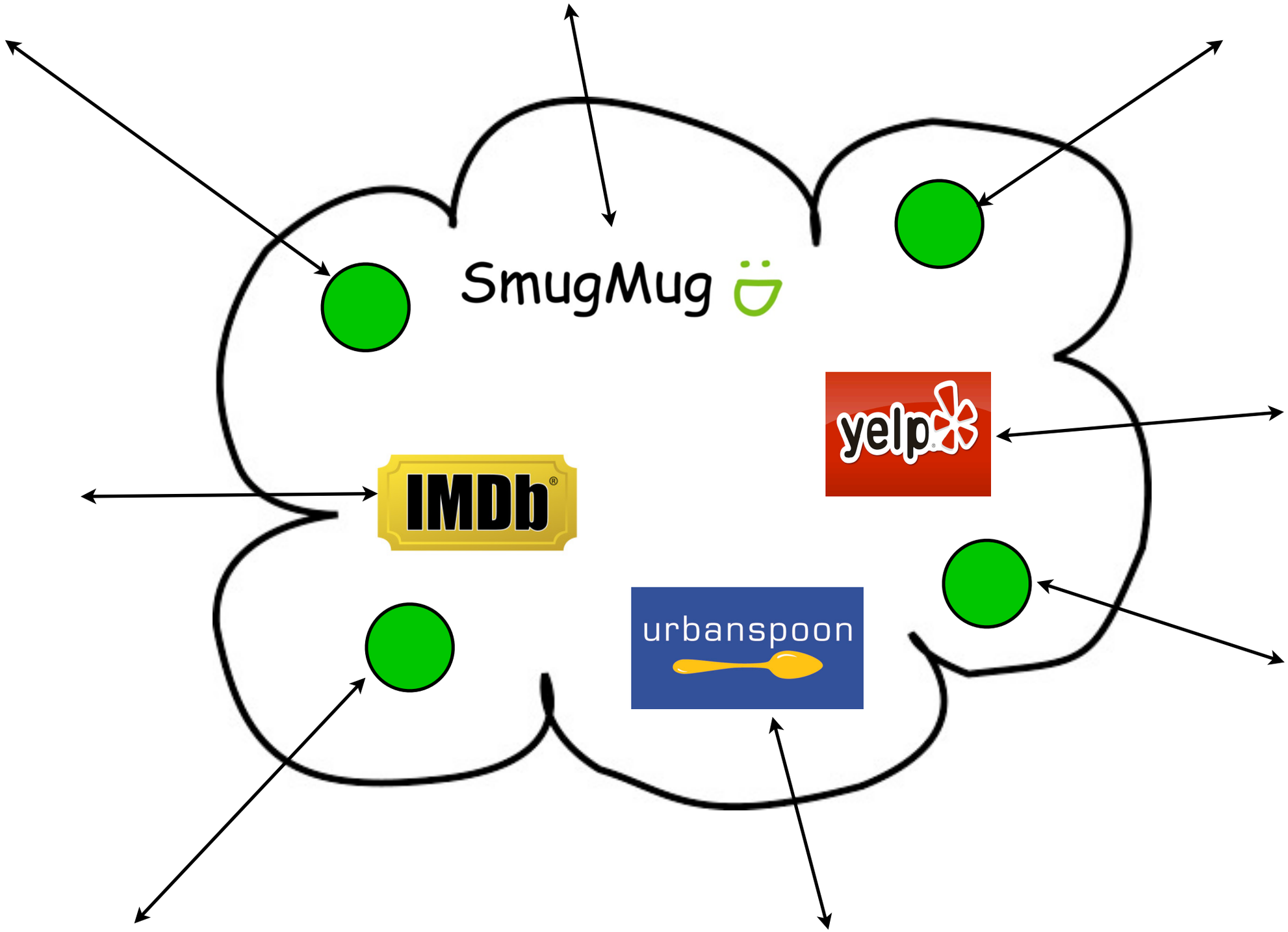
1-10 Mbps



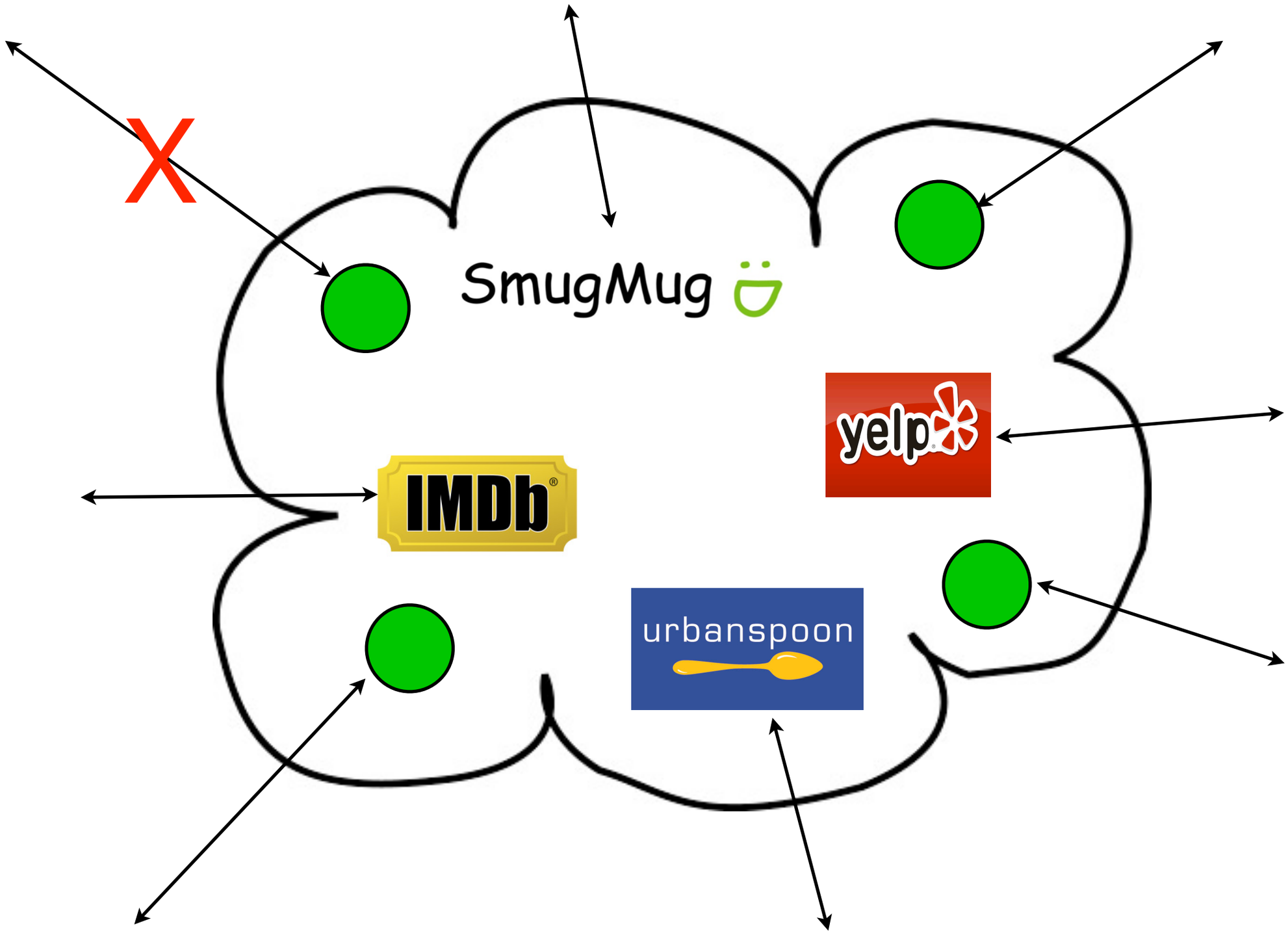

10-100 Gbps



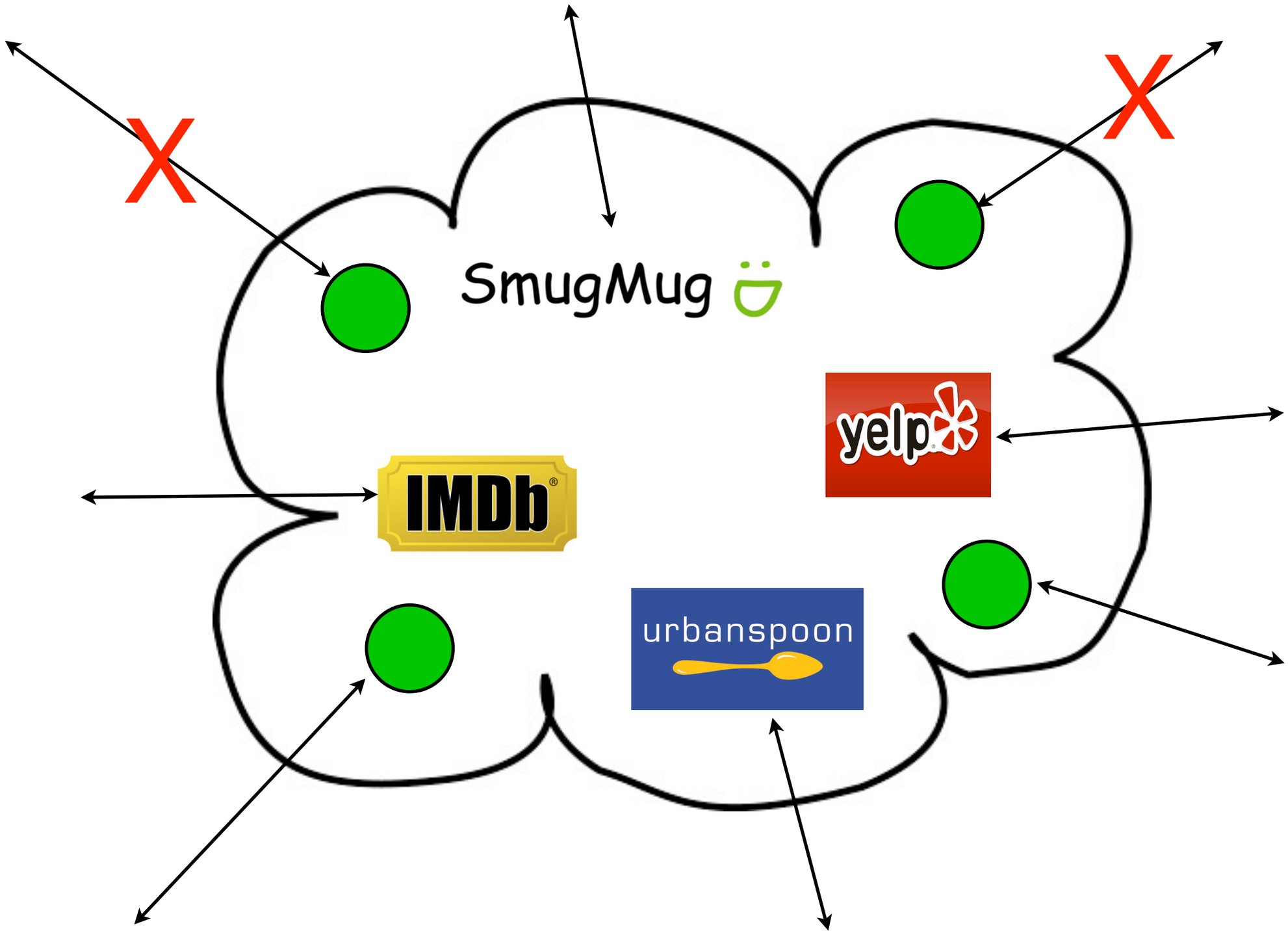
# Blocking Clouds Causes Collateral Damage



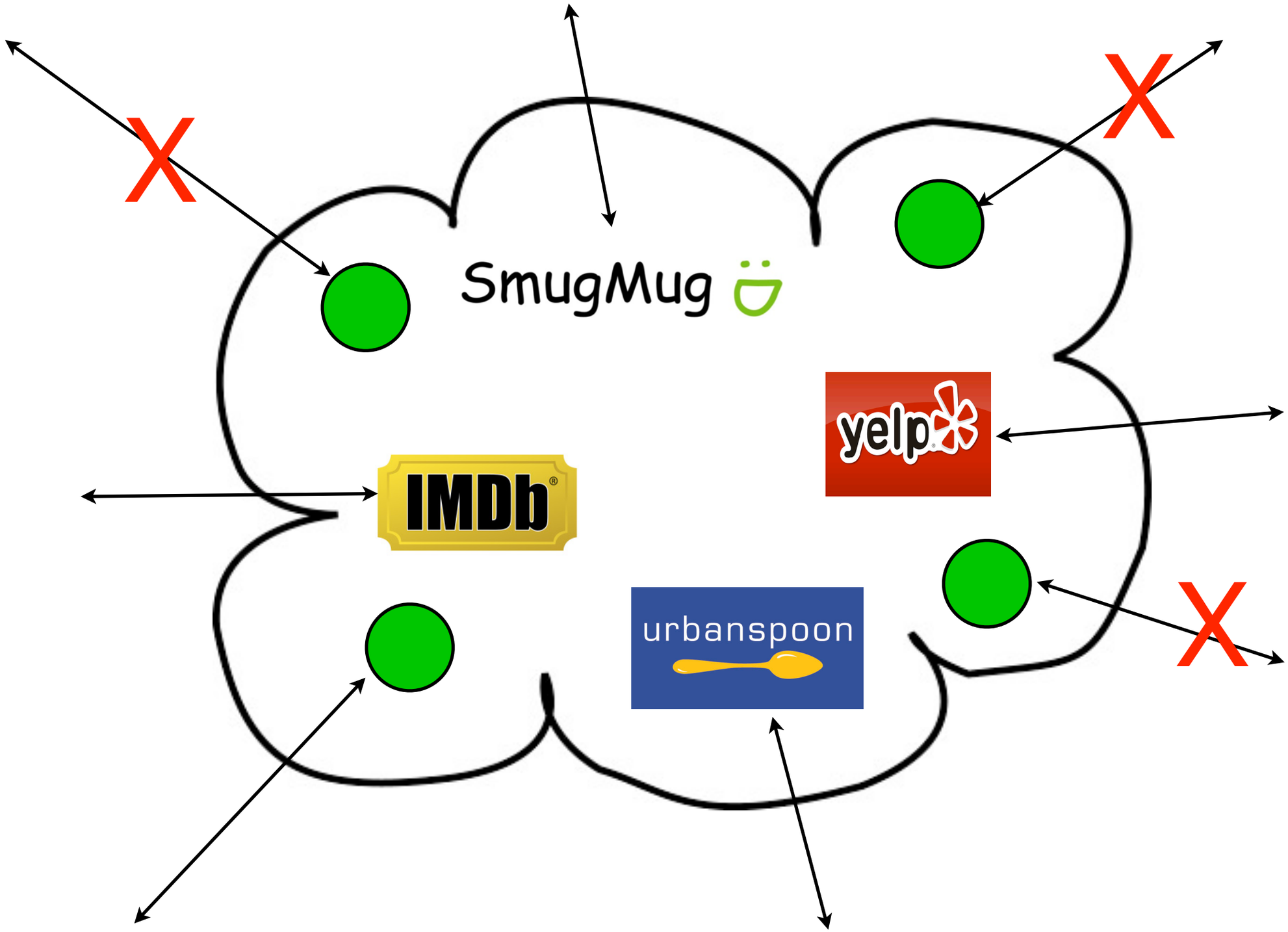
# Blocking Clouds Causes Collateral Damage



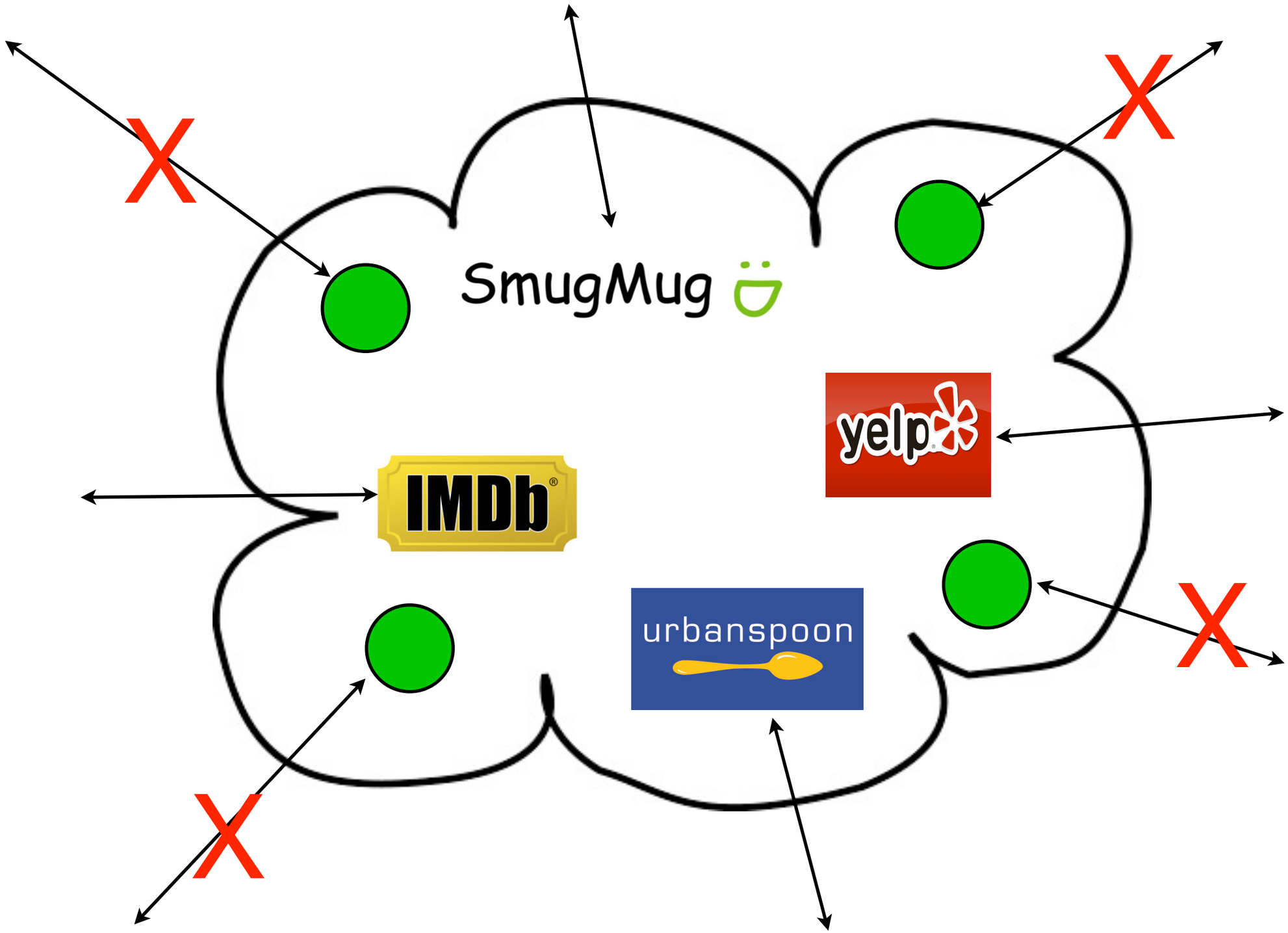
# Blocking Clouds Causes Collateral Damage



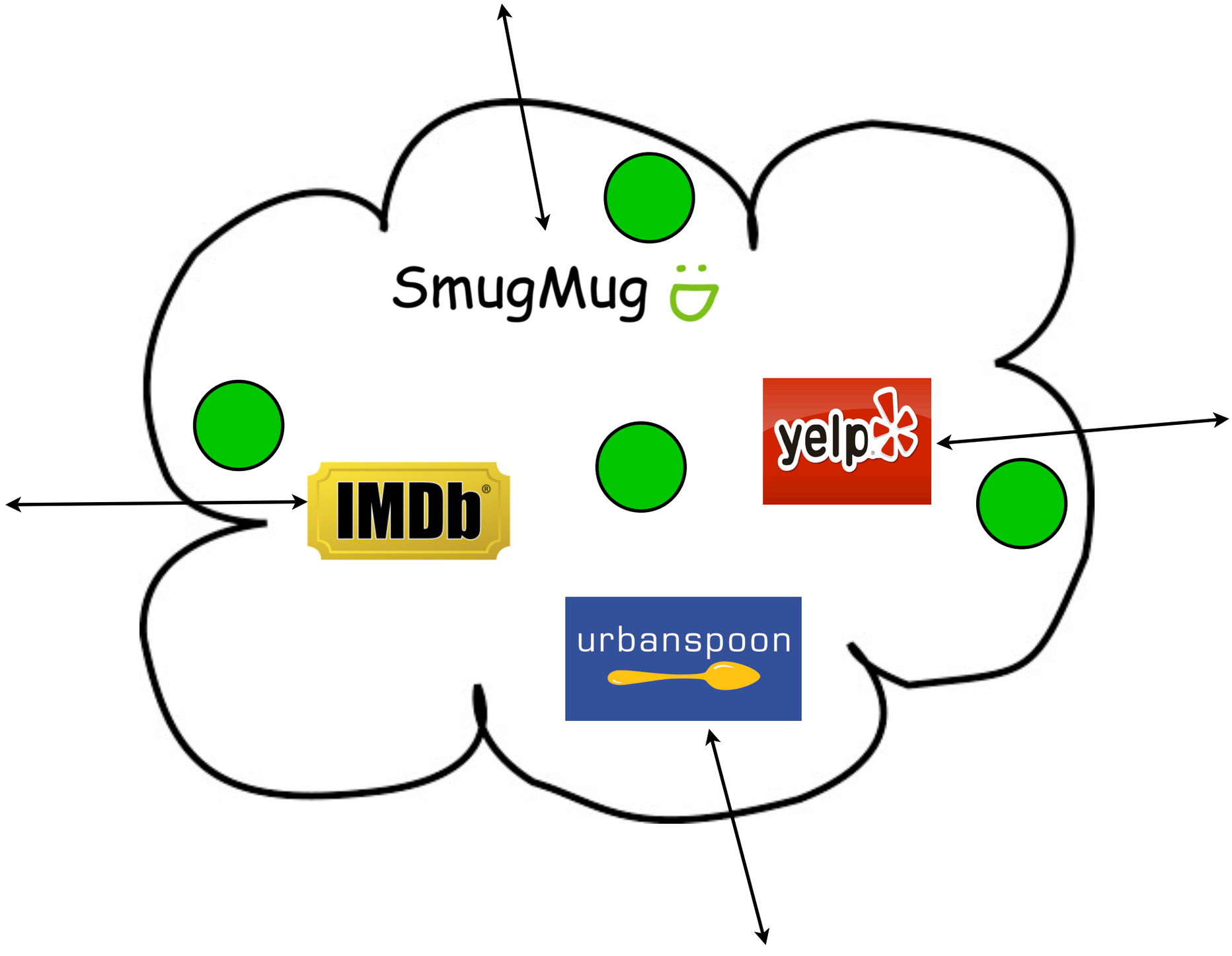
# Blocking Clouds Causes Collateral Damage



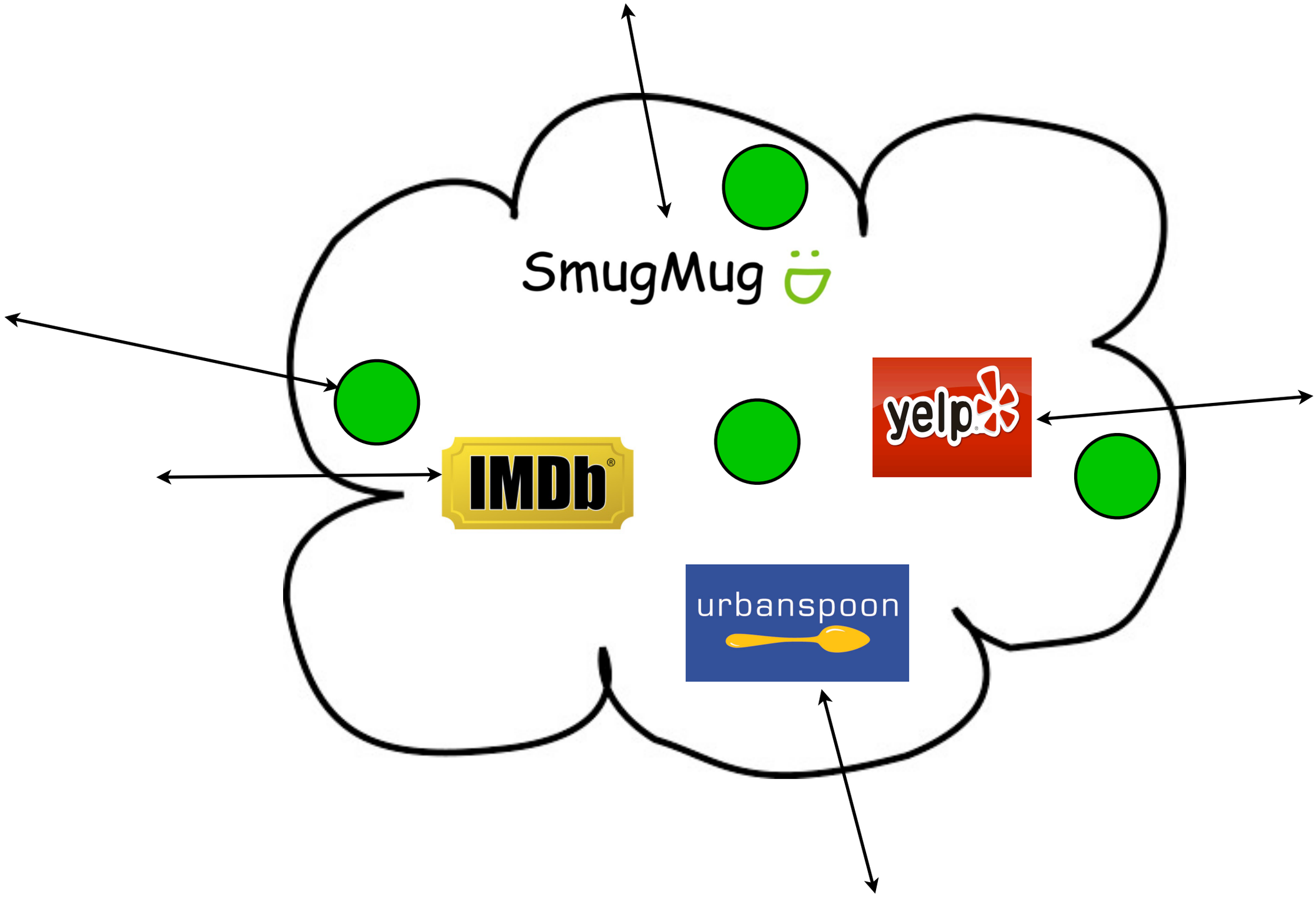
# Blocking Clouds Causes Collateral Damage



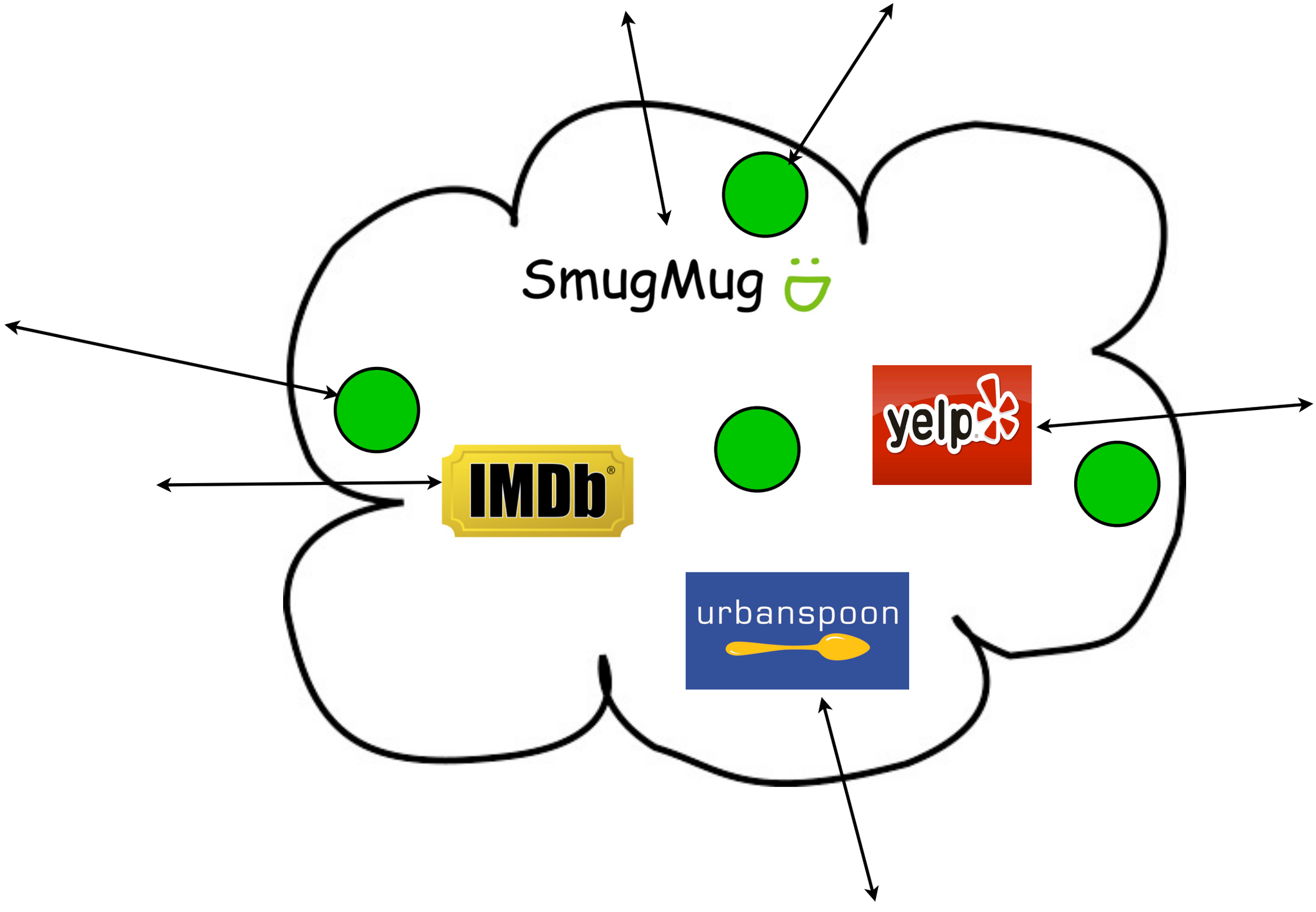
# Blocking Clouds Causes Collateral Damage



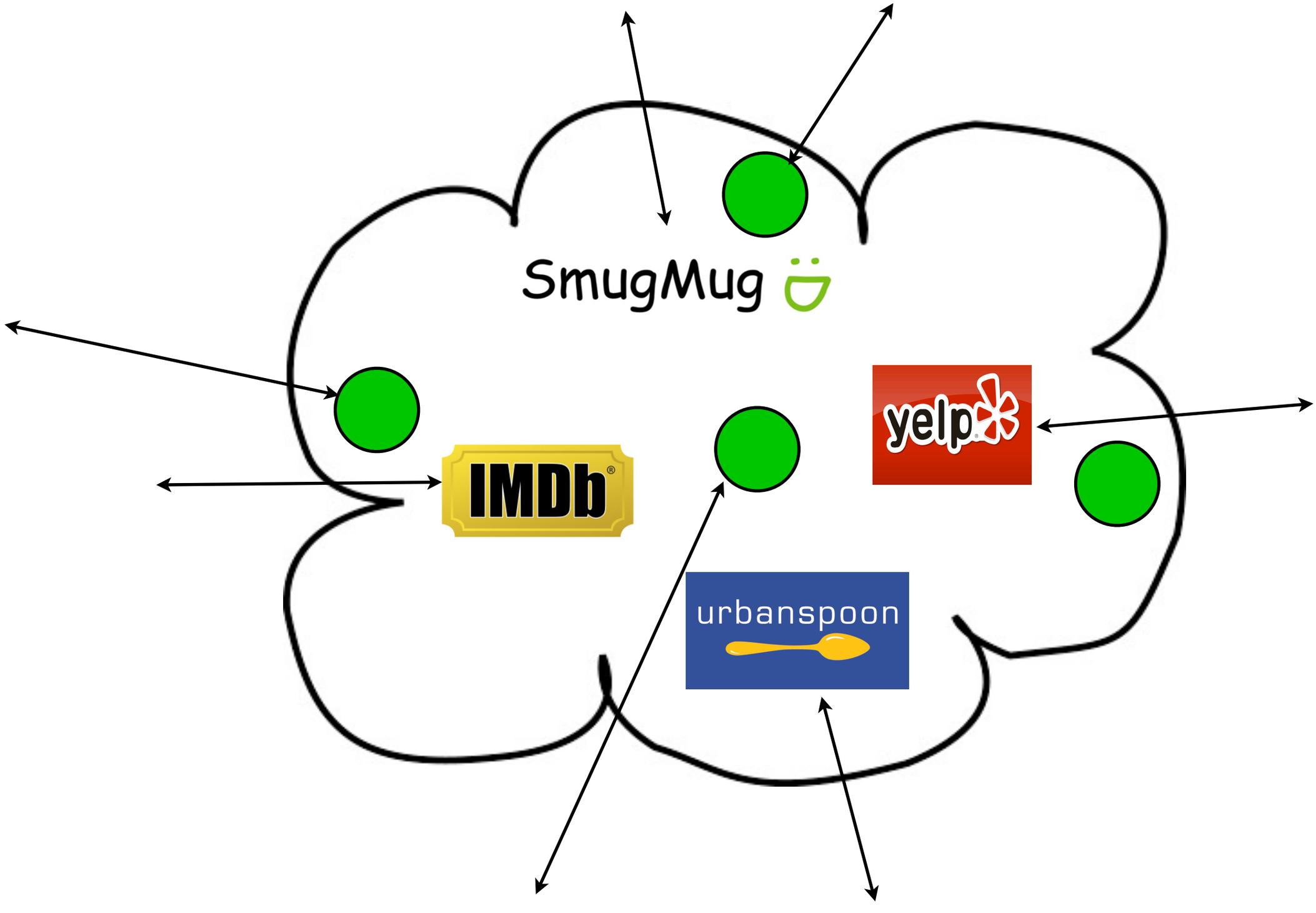
# Blocking Clouds Causes Collateral Damage



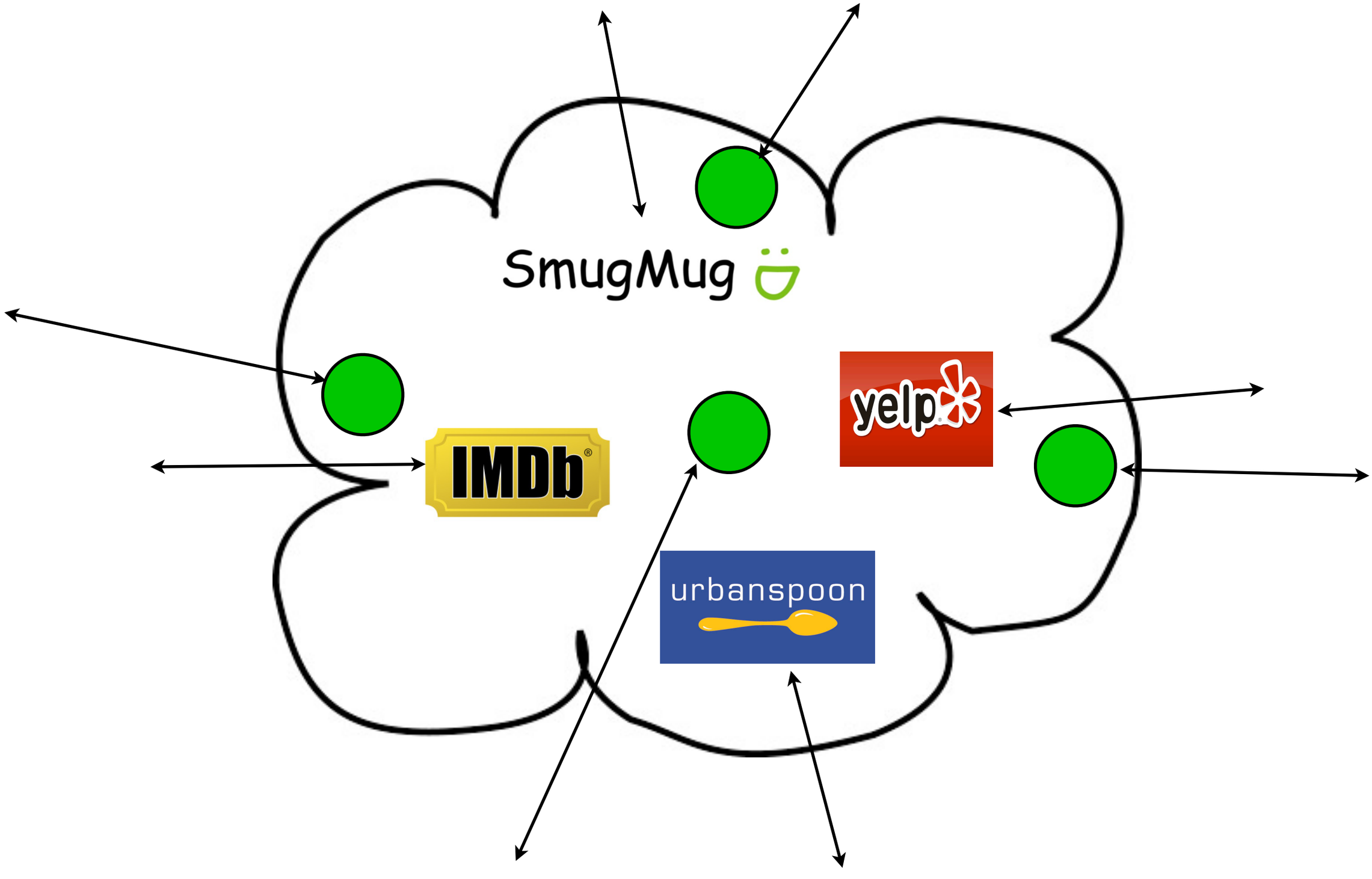
# Blocking Clouds Causes Collateral Damage



# Blocking Clouds Causes Collateral Damage



# Blocking Clouds Causes Collateral Damage



# Benefits of Clouds

- Higher performance

- Elasticity to scale to demand

- Multi-homing and scale makes eavesdropping difficult

- Elasticity forces censors to make hard choices: collateral damage or unblocked access

# Economics

Cloud pricing is affordable for end users

# Cost of running COR in the cloud

- Cloud providers charge for CPU and bandwidth

# Cost of running COR in the cloud

- Cloud providers charge for CPU and bandwidth

- CPU is cheap

# Cost of running COR in the cloud

- Cloud providers charge for CPU and bandwidth

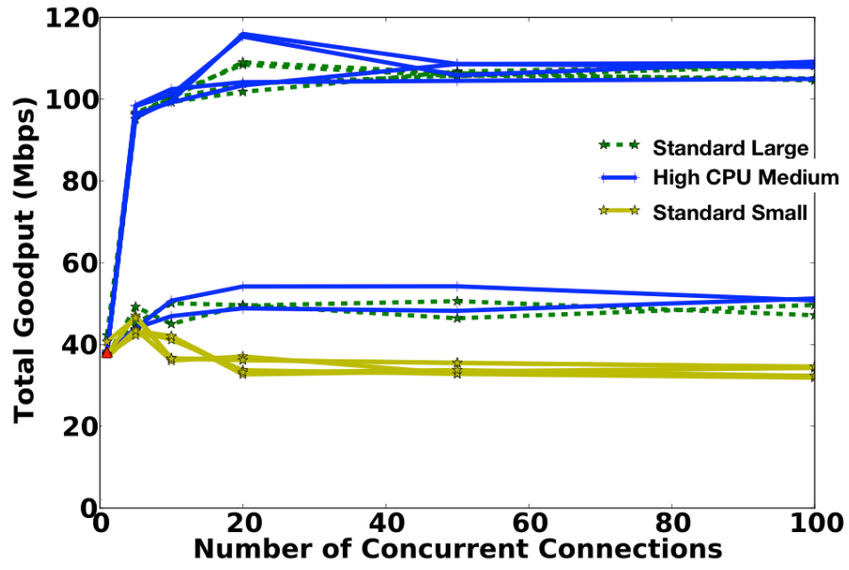
- CPU is cheap
  - 100+ users on a 34¢/hr node

# Cost of running COR in the cloud

- Cloud providers charge for CPU and bandwidth

- CPU is cheap

  - 100+ users on a 34¢/hr node



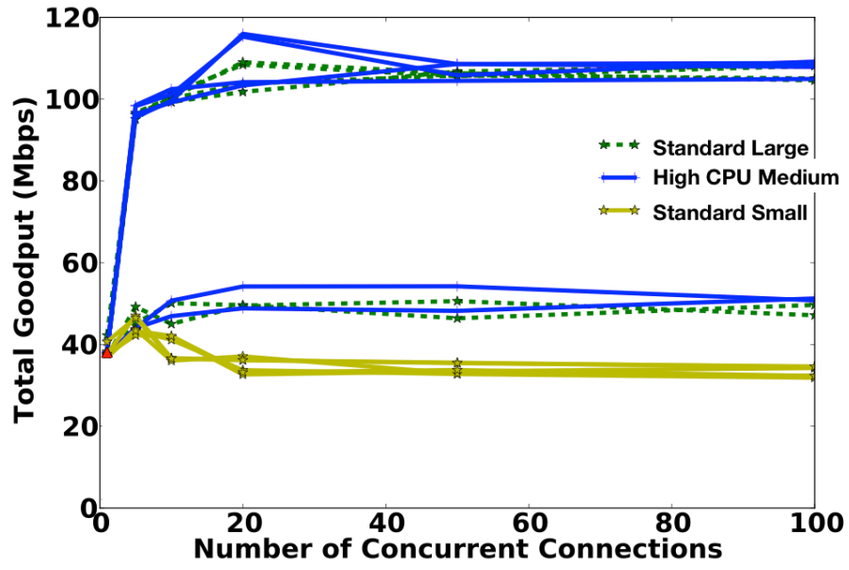
# Cost of running COR in the cloud

- Cloud providers charge for CPU and bandwidth

- CPU is cheap

  - 100+ users on a 34¢/hr node

- Bandwidth is dominant cost

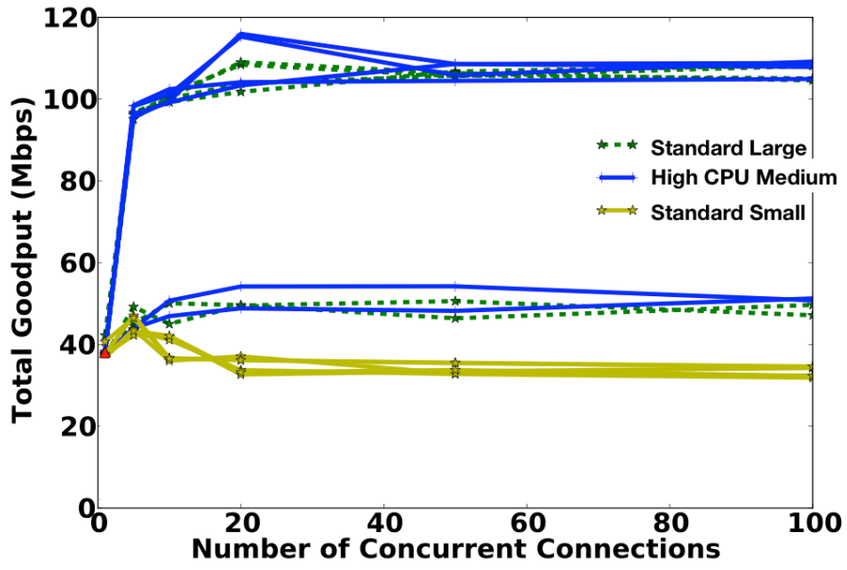


# Cost of running COR in the cloud

- Cloud providers charge for CPU and bandwidth

- CPU is cheap
  - 100+ users on a 34¢/hr node

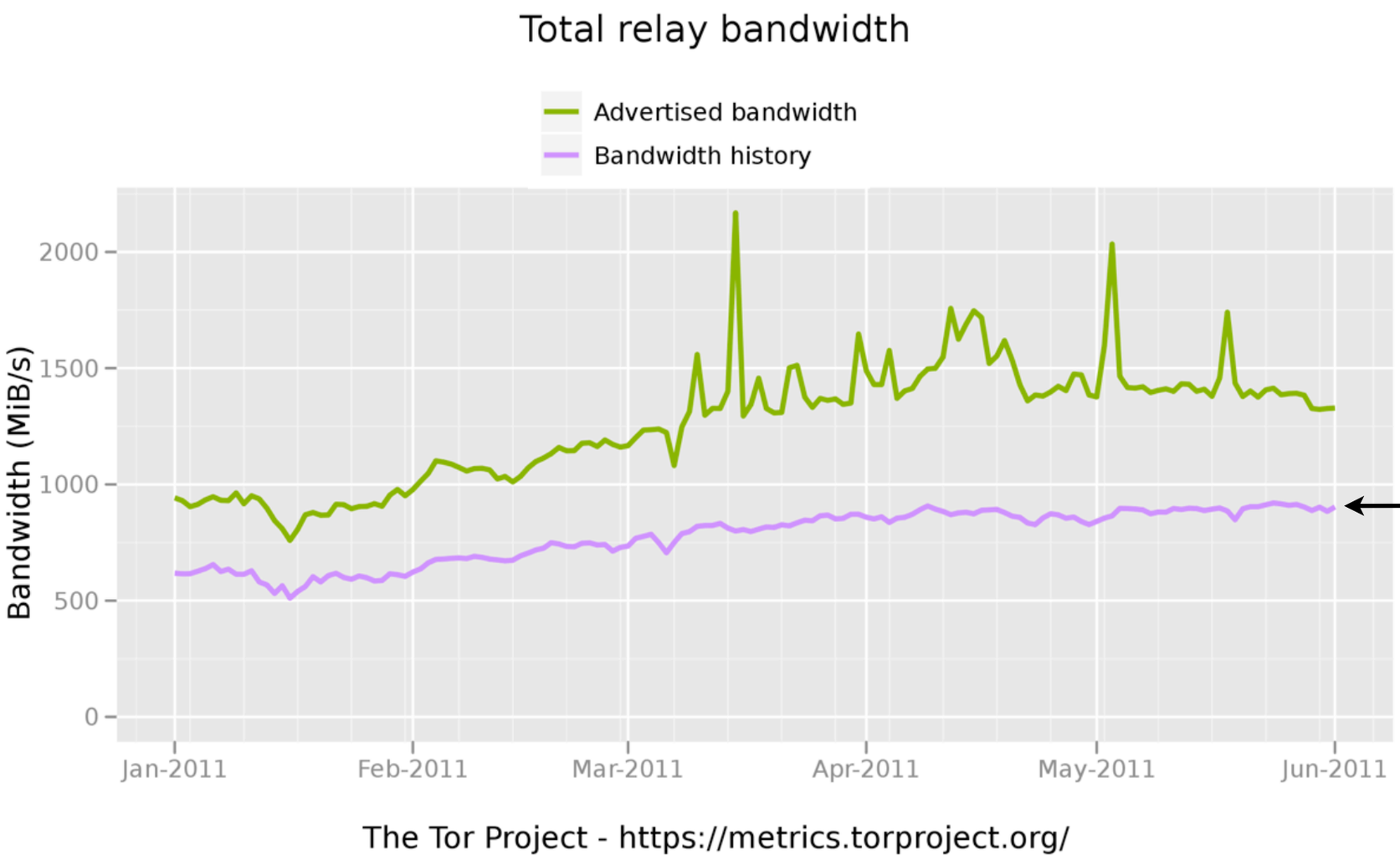
- Bandwidth is dominant cost
  - 100MB as low as 1¢




| **Data Transfer IN** | |
|---|---|
| All data transfer in | $0.000 per GB |
| **Data Transfer OUT** | |
| First 1 GB / month | $0.000 per GB |
| Up to 10 TB / month | $0.120 per GB |
| Next 40 TB / month | $0.090 per GB |
| Next 100 TB / month | $0.070 per GB |
| Next 350 TB / month | $0.050 per GB |

Amazon EC2 Pricing

# Tor’s Total Bandwidth Cost in the Cloud




← Approximately 900 MB/s

376 TB/month

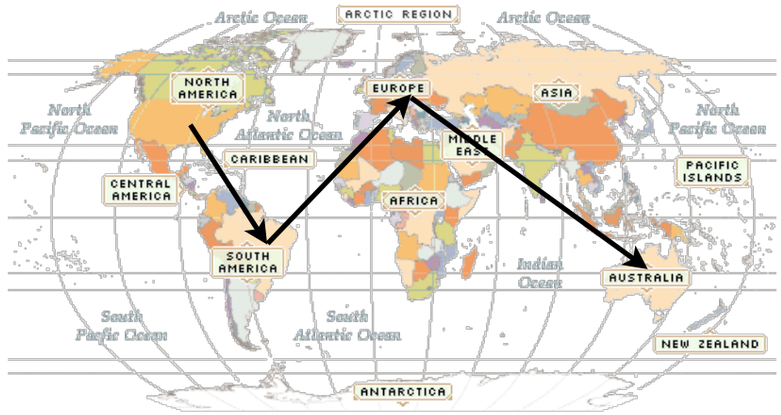
COR Cost: $61,200/month

# Security Challenges and Solutions

- Involved Parties and Trust Model
- Building Tunnels
- Paying for Tunnels
- Learning About Relays

# Distributing Trust

- Tor
    - Tunnels between volunteer relays




- COR
    - Tunnels between clouds from different providers

# Is that sufficient?

- Should users pay cloud providers directly?
    - Not anonymous: Credit cards and Paypal leak info

# Is that sufficient?

- Should users pay cloud providers directly?
    - Not anonymous: Credit cards and Paypal leak info
- Another layer of indirection: Anonymity Service Providers
    - Operate relays and pay cloud providers
    - Mask users’ identities
    - Accept anonymous payment for access

# System Roles

- Cloud Hosting Providers (CHPs)
  - Provide infrastructure for COR relays

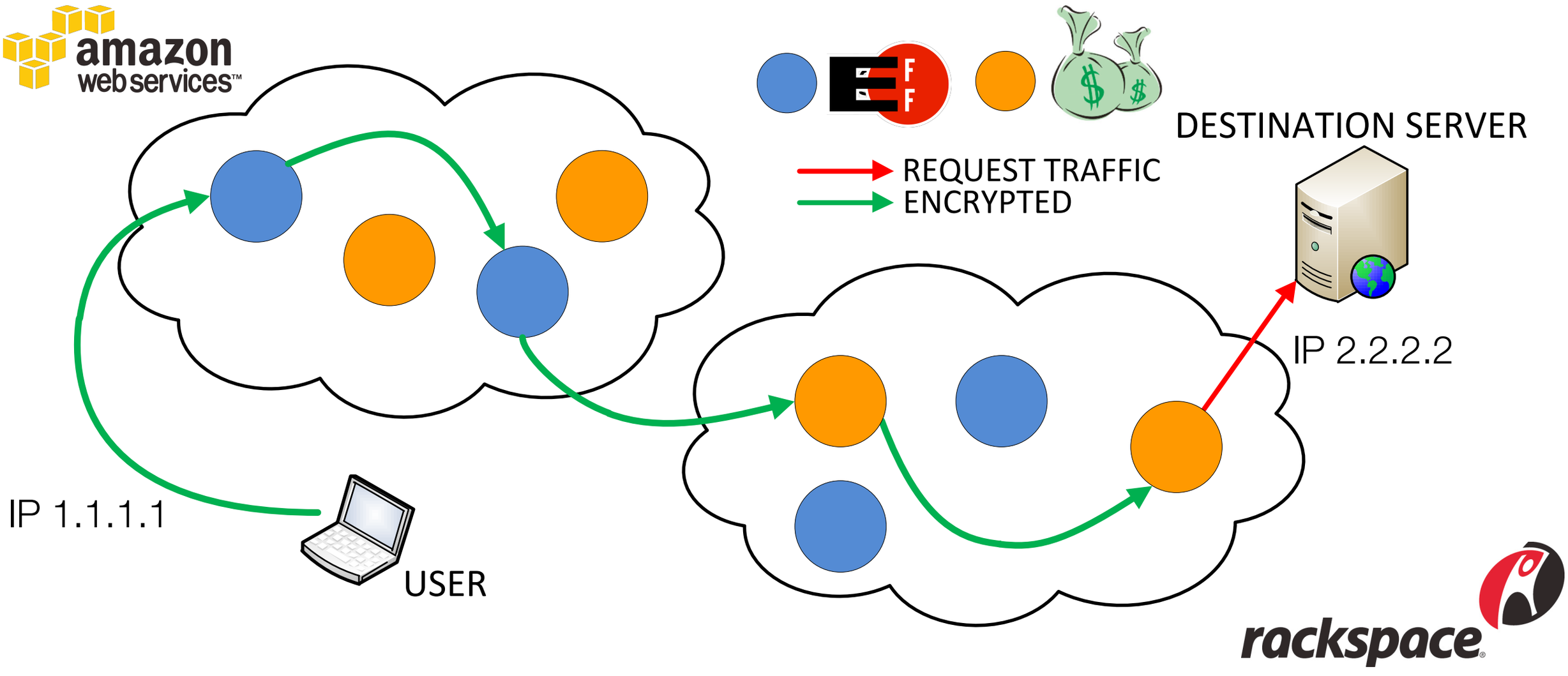


Windows Azure

- Anonymity Service Providers (ASPs)
  - Run relays and directory servers
  - Sell tokens
    - Redeemable for XX MB of connectivity or XX amount of time

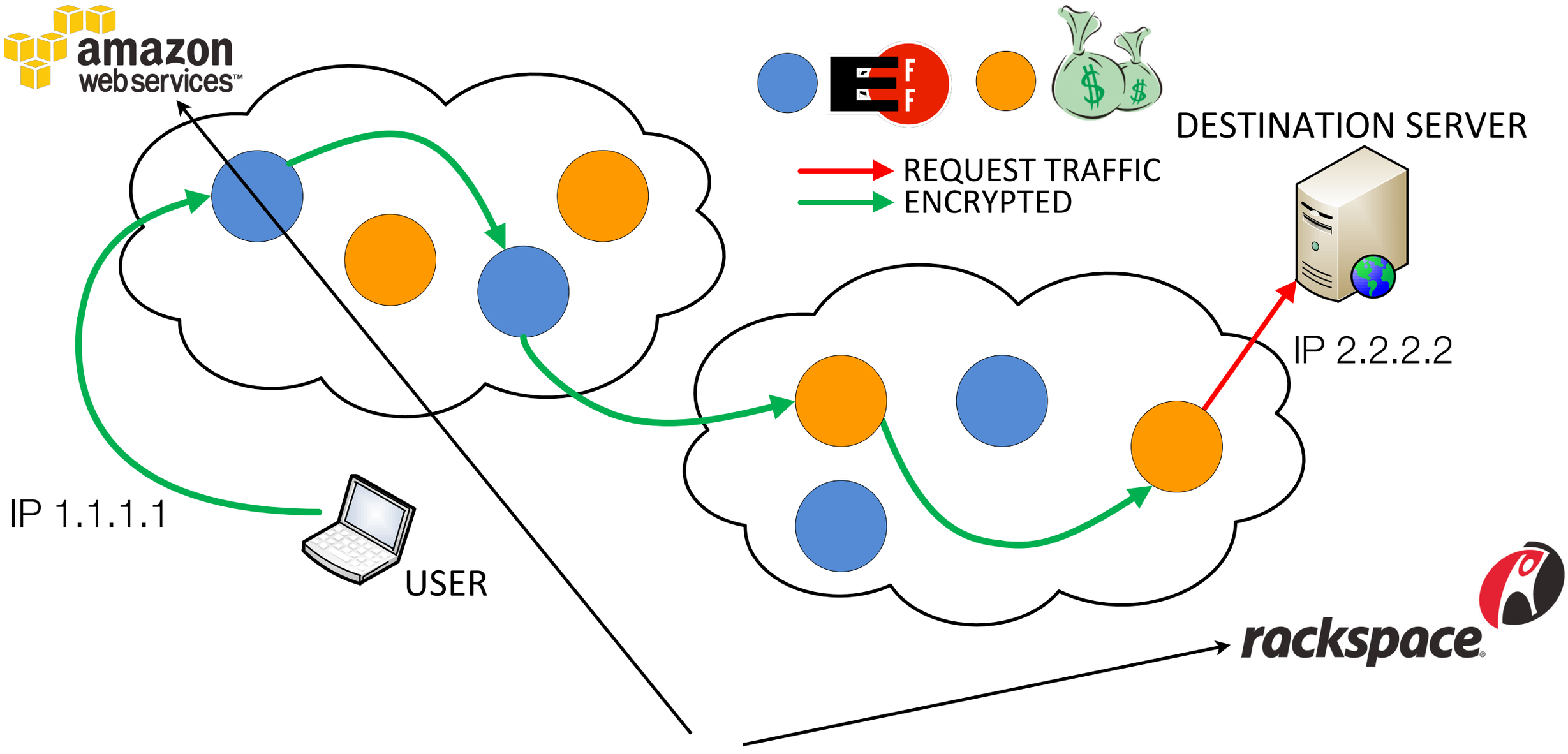


# System Architecture Example




Organizations used above are examples only

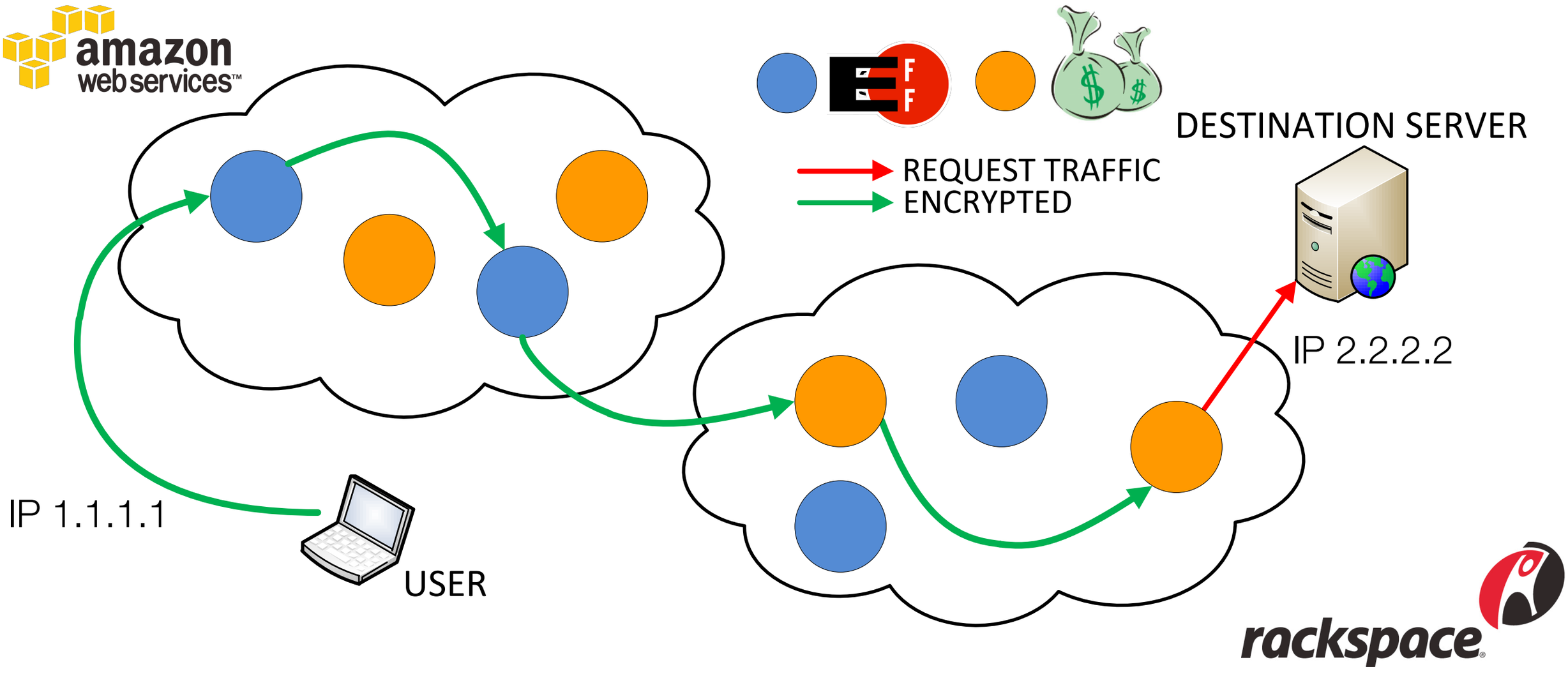
# System Architecture Example




Cloud Hosting Providers

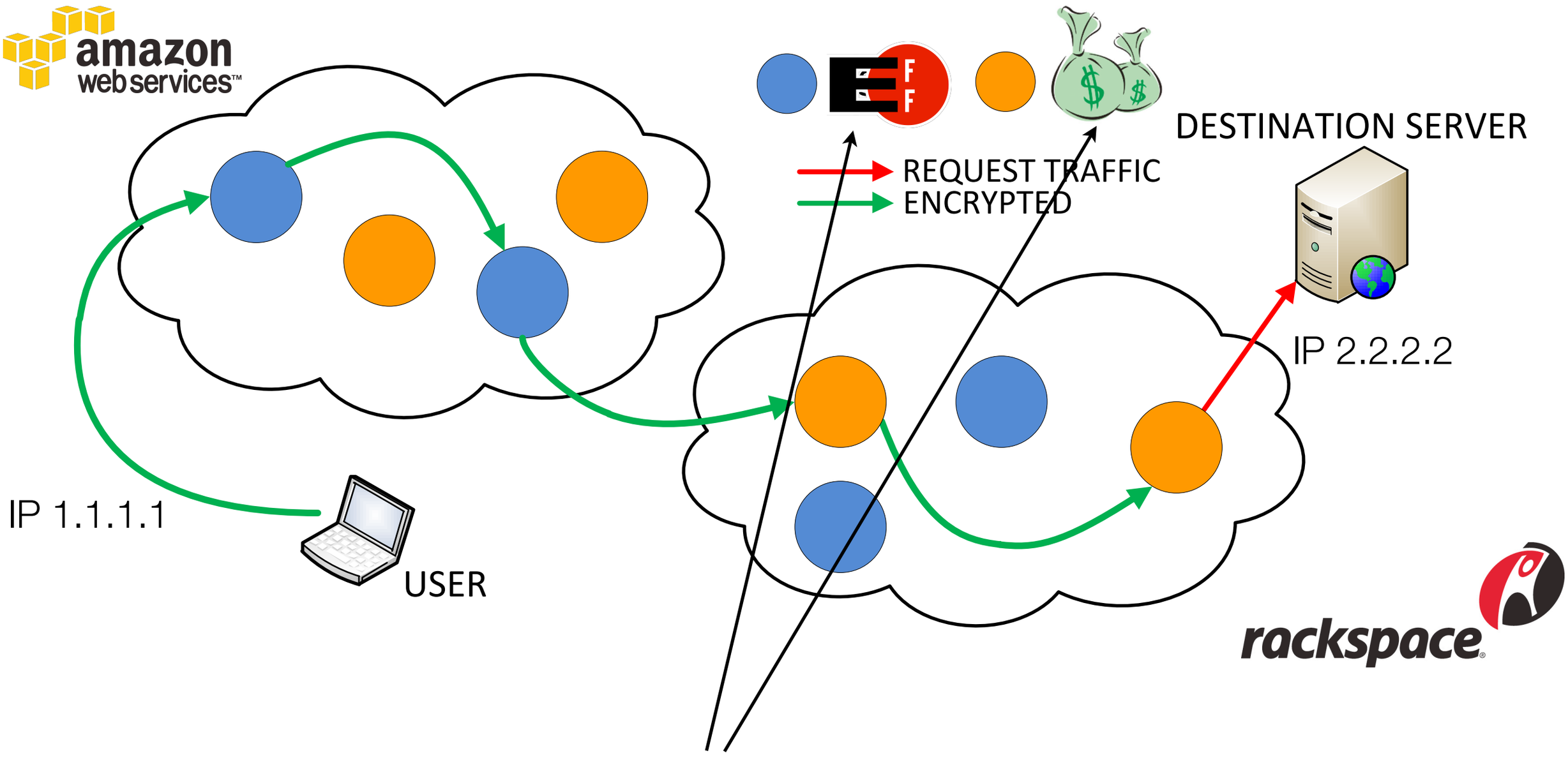
Organizations used above are examples only

# System Architecture Example




Organizations used above are examples only

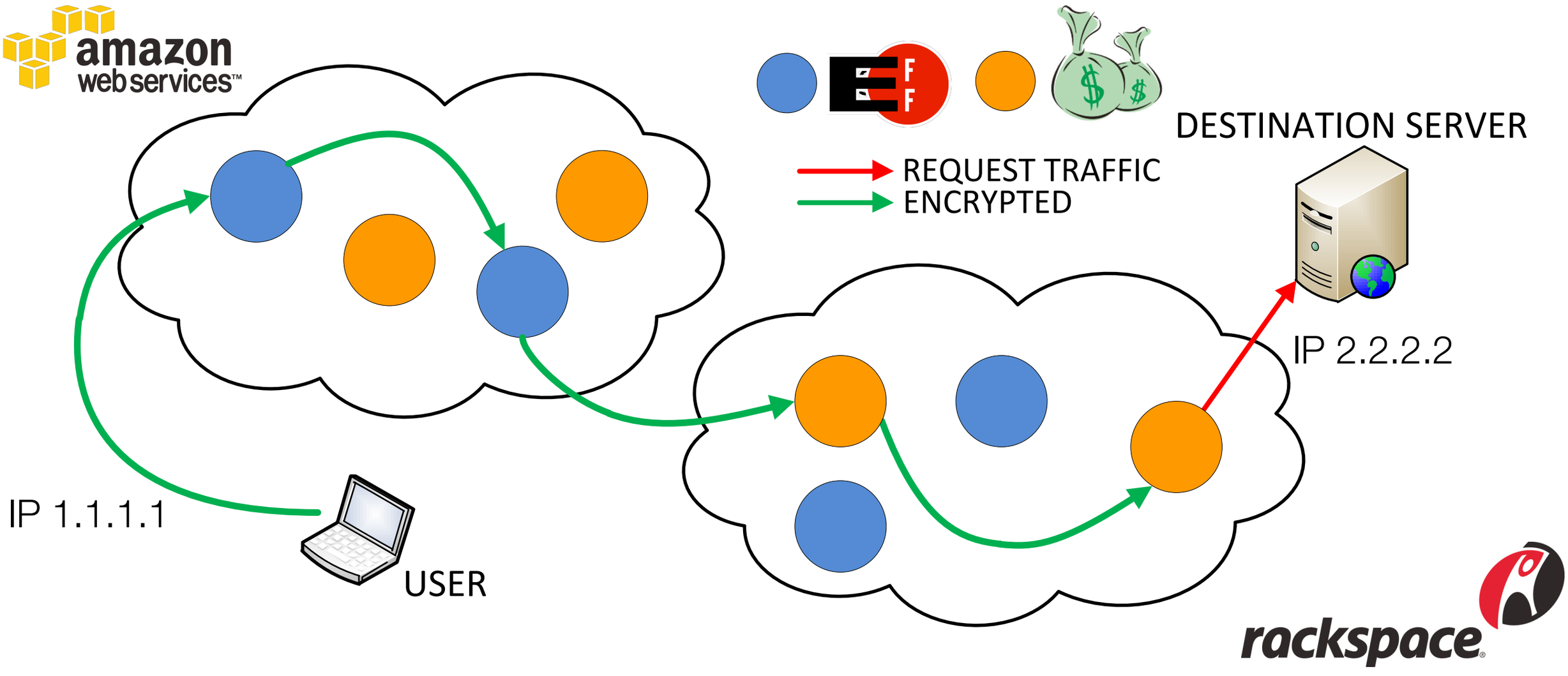
# System Architecture Example




Anonymity Service  Providers

Organizations used above are examples only

# System Architecture Example

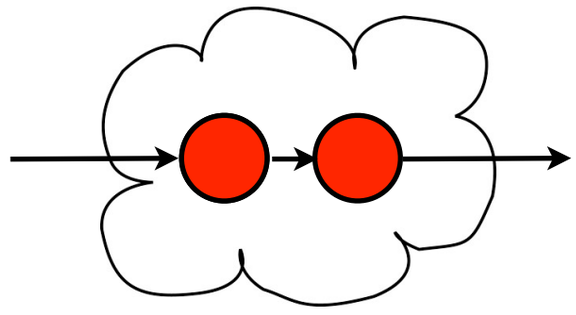



Organizations used above are examples only

# Circuit Construction Must be Policy Aware

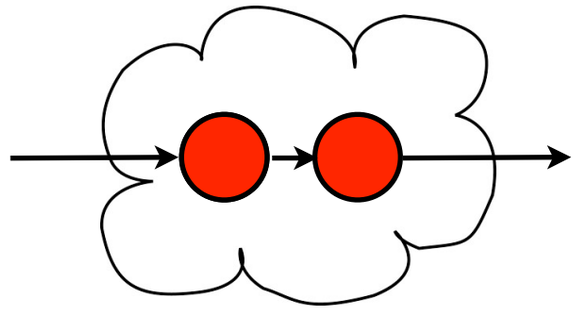
# Circuit Construction Must be Policy Aware

- Two relays within each datacenter

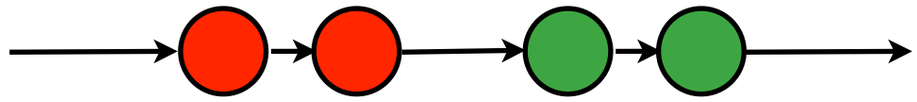


# Circuit Construction Must be Policy Aware

- Two relays within each datacenter

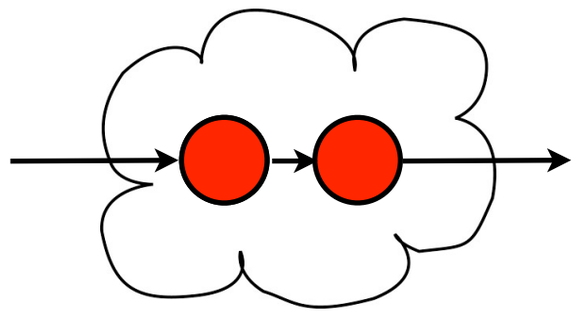


- Different entry and exit ASPs

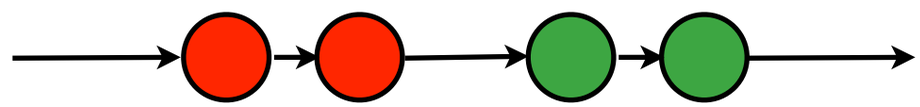


# Circuit Construction Must be Policy Aware

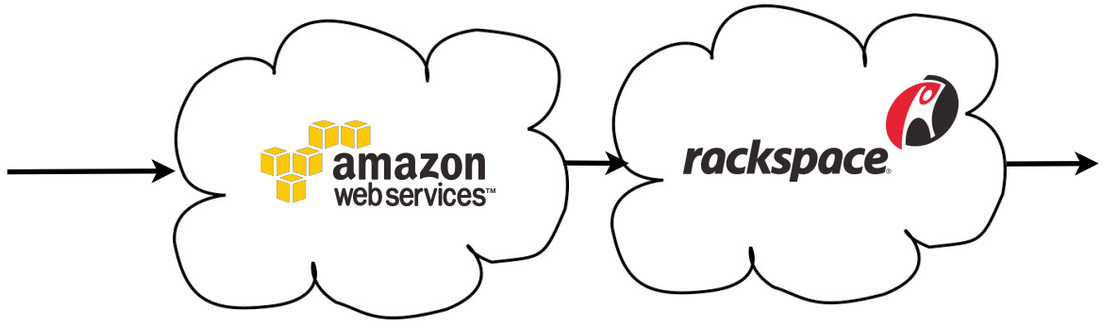
- Two relays within each datacenter



- Different entry and exit ASPs

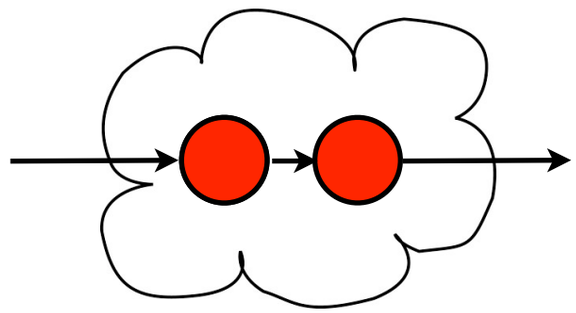


- Different entry and exit CHPs

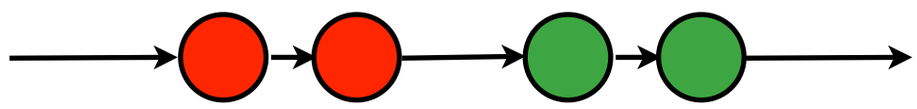


# Circuit Construction Must be Policy Aware

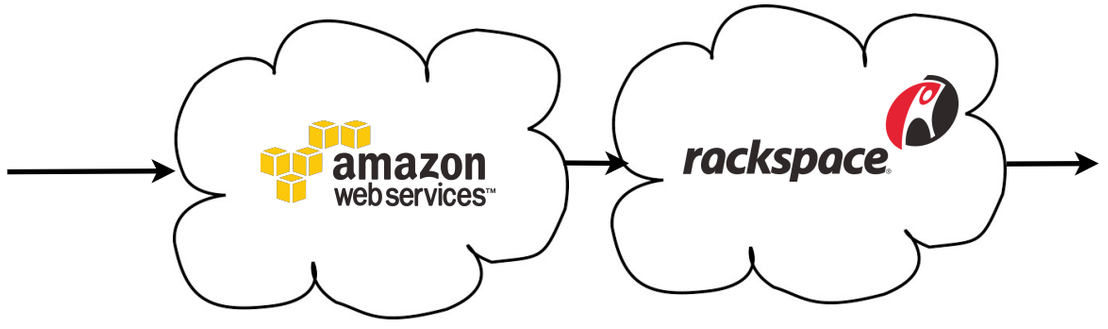
- Two relays within each datacenter



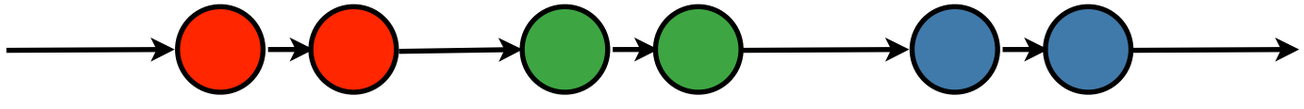
- Different entry and exit ASPs



- Different entry and exit CHPs




- ASP and CHP relays are contiguous within a circuit



# Paying for Access

- Users purchase tokens

- Redeem tokens for access (bandwidth or time)

- Chaum's e-cash:

  - Cryptographically untraceable

# How do users gain access?

- Users need two things:
  - Tokens
  - COR Directory

# How do users gain access?

- Users need two things:
  - Tokens
  - COR Directory
- Solution: Bootstrapping Network
  - Low speed
  - High Latency
  - Free

# Adversaries enumerate and block ingress

- Current technologies
    - Tor Bridges

- Two separate problems:
    - COR Relays
        - High speed, low latency, not free
    - Bootstrapping
        - Low speed, high latency, free

| Summary | Tor | COR |
| --- | --- | --- |

| Summary | Tor | COR |
| --- | --- | --- |
| Secure | ✔ | ✔ |

| Summary | Tor | COR |
| --- | --- | --- |
| Secure | ✅ | ✅ |
| High Speed | ❌ | ✅ |

| Summary | Tor | COR |
|---|---|---|
| Secure | ✓ | ✓ |
| High Speed | ✗ | ✓ |
| Dynamic Scaling | ✗ | ✓ |

| Summary | Tor | COR |
|---|---|---|
| Secure | ✓ | ✓ |
| High Speed | ✗ | ✓ |
| Dynamic Scaling | ✗ | ✓ |
| Adaptive to censorship | ✗ | ✓ |

| Summary | Tor | COR |
|---|---|---|
| Secure | ✓ | ✓ |
| High Speed | ✗ | ✓ |
| Dynamic Scaling | ✗ | ✓ |
| Adaptive to censorship | ✗ | ✓ |
| Free | ✓ | ✗ |