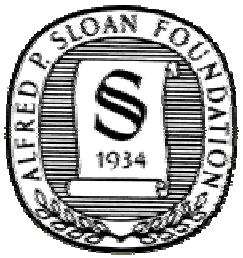
Flooding Attacks by Exploiting Persistent Forwarding Loops

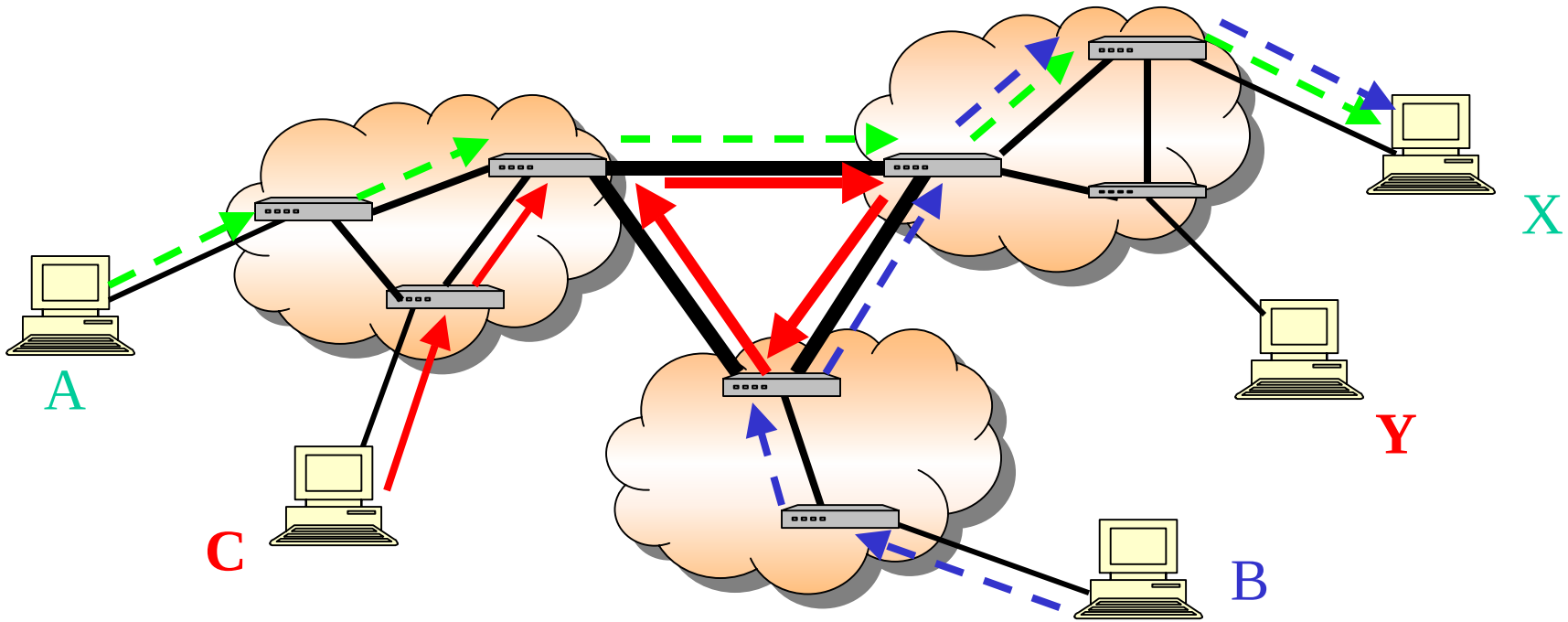
Jianhong Xia, Lixin Gao and Teng Fei

University of Massachusetts, Amherst
MA 01003, USA
Email: {jxia, lgao, tfei}@ecs.umass.edu



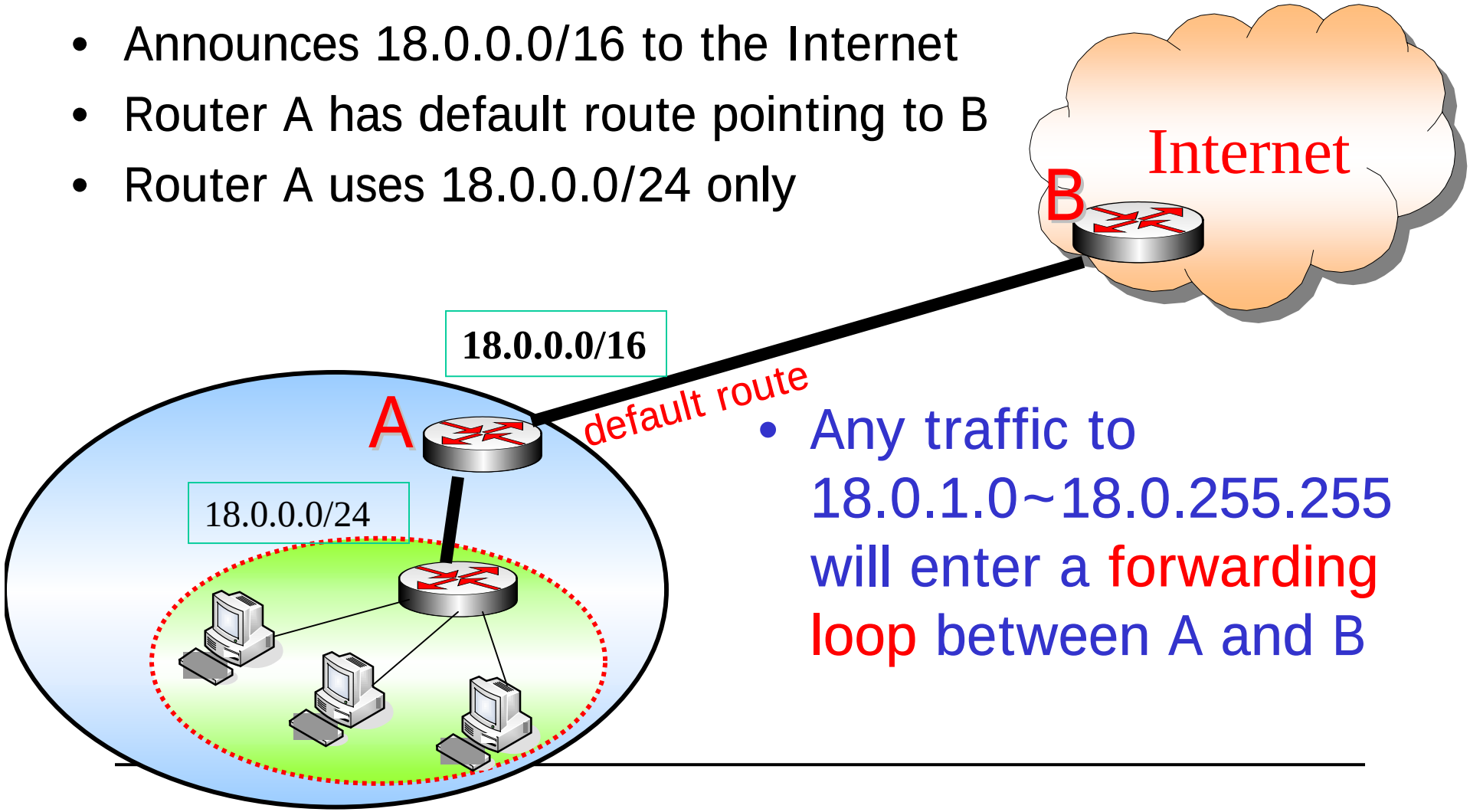
Introduction

- Routing determines forwarding paths



Why Persistent Forwarding Loop Occurs
--- Example on Neglecting Pull-up Route

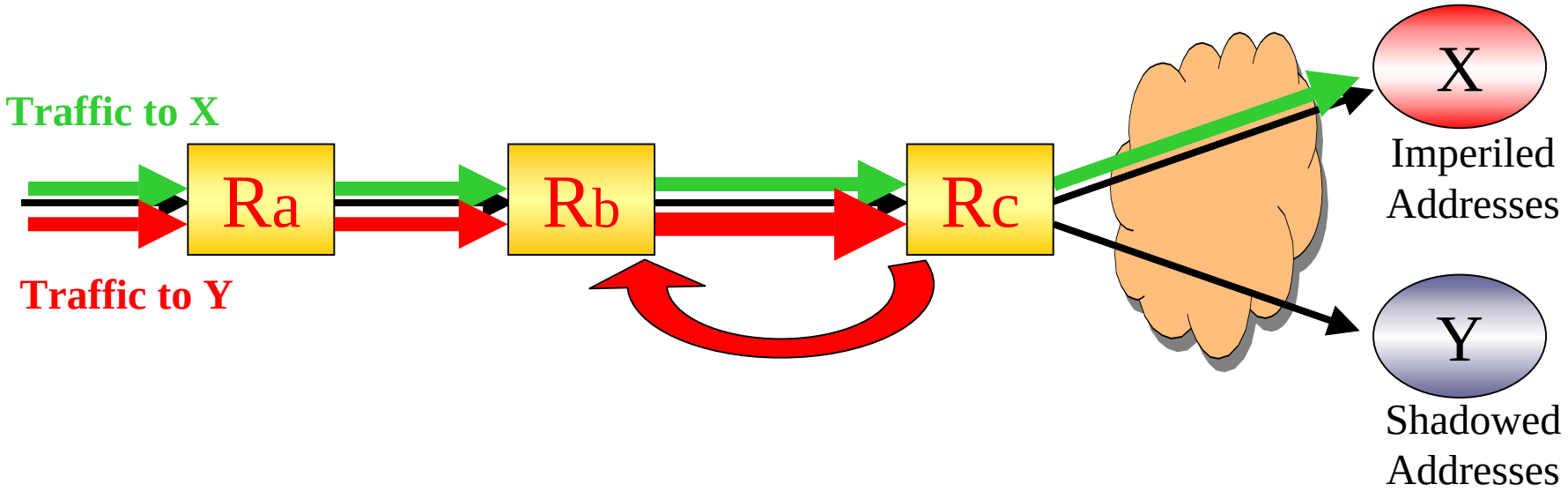
- Announces 18.0.0.0/16 to the Internet
- Router A has default route pointing to B
- Router A uses 18.0.0.0/24 only



- Any traffic to 18.0.1.0~18.0.255.255 will enter a forwarding loop between A and B

Risk of Persistent Forwarding Loops

- Flooding Attacks to legitimate hosts



- How many shadowed addresses in the Internet?
- How many imperiled addresses in the Internet?

Measurement Design

- Design
  - Balancing granularity and overhead
  - Samples 2 addresses in each /24 IP block
- Addresses space collection
  - Addresses covered by RouteView table
  - De-aggregate prefixes to /24 prefixes
    - Fine-grained prefixes
- Data traces
  - Traceroute to 5.5 million fine-grained prefixes
  - Measurement lasts for 3 weeks in Sep. 2005

Shadowed vs. Imperiled Addresses

- Shadowed addresses/prefixes
  - 135,973 shadowed prefixes
  - **2.47%** of routable addresses
  - Located in **5341** ASes
- Imperiled addresses/prefixes
  - 42,887 imperiled prefixes
  - **0.78%** of routable addresses
  - Located in **2117** ASes

Validating Persistent Forwarding Loops

- Validation from various locations
  - From Asia, Europe, West and East coast of US
  - 90% of shadowed prefixes consistently have persistent forwarding loops
- Validation to multiple addresses in shadowed prefixes
  - Sampling ~50 addresses in each shadowed prefix
  - 68% of shadowed prefixes show that
    - All samples have forwarding loops

Properties of Persistent Forwarding Loops

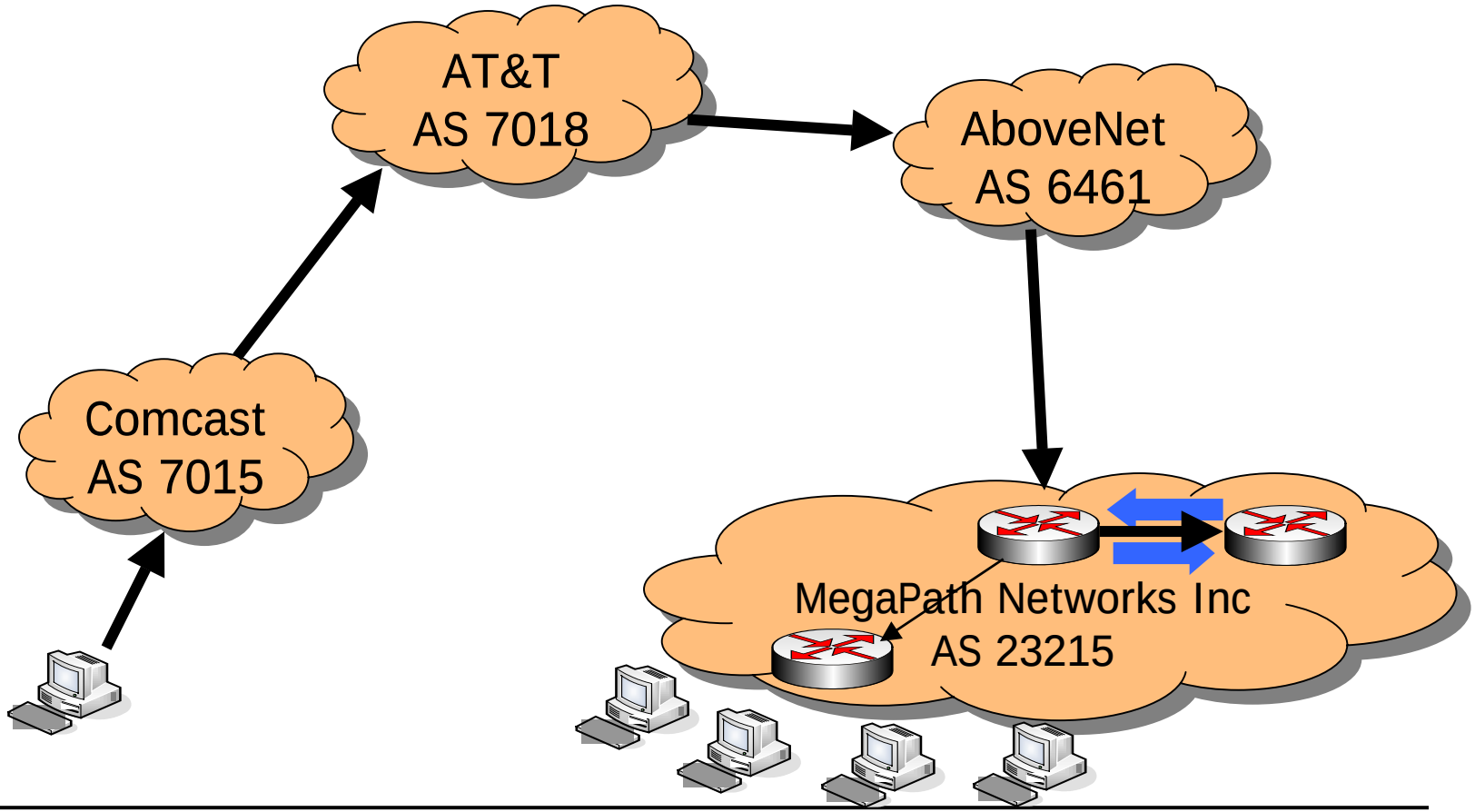
- Length
  - 86.6% of persistent loops are two hops long
  - 0.4% are more than 10 hops long
    - Some are more than 15 hops long
- Location
  - 82.2% of persistent loops occur within destination domains
- Implications
  - Significantly amplify attacking traffic
  - Can be exploited from different places

Classifying Persistent Forwarding Loops

- Within one AS (94.3%)
  - 82.2% in destination domains
- Within two ASes (5.3%)
- Within three or more ASes (0.4%)
  - As many as 7 or 8 ASes

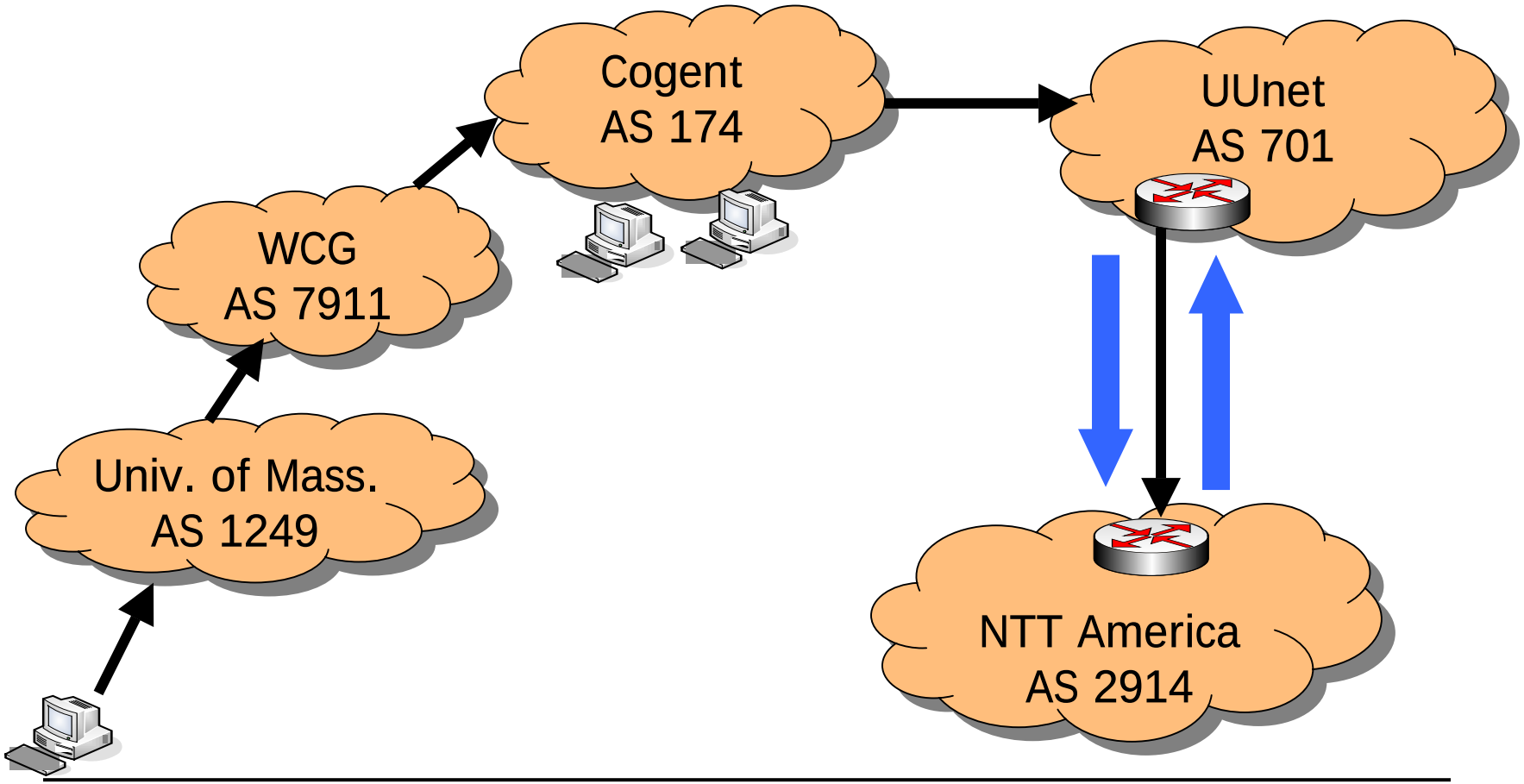
Example: Loop Occurs in One Domain

- Traceroute to 69.33.53.1



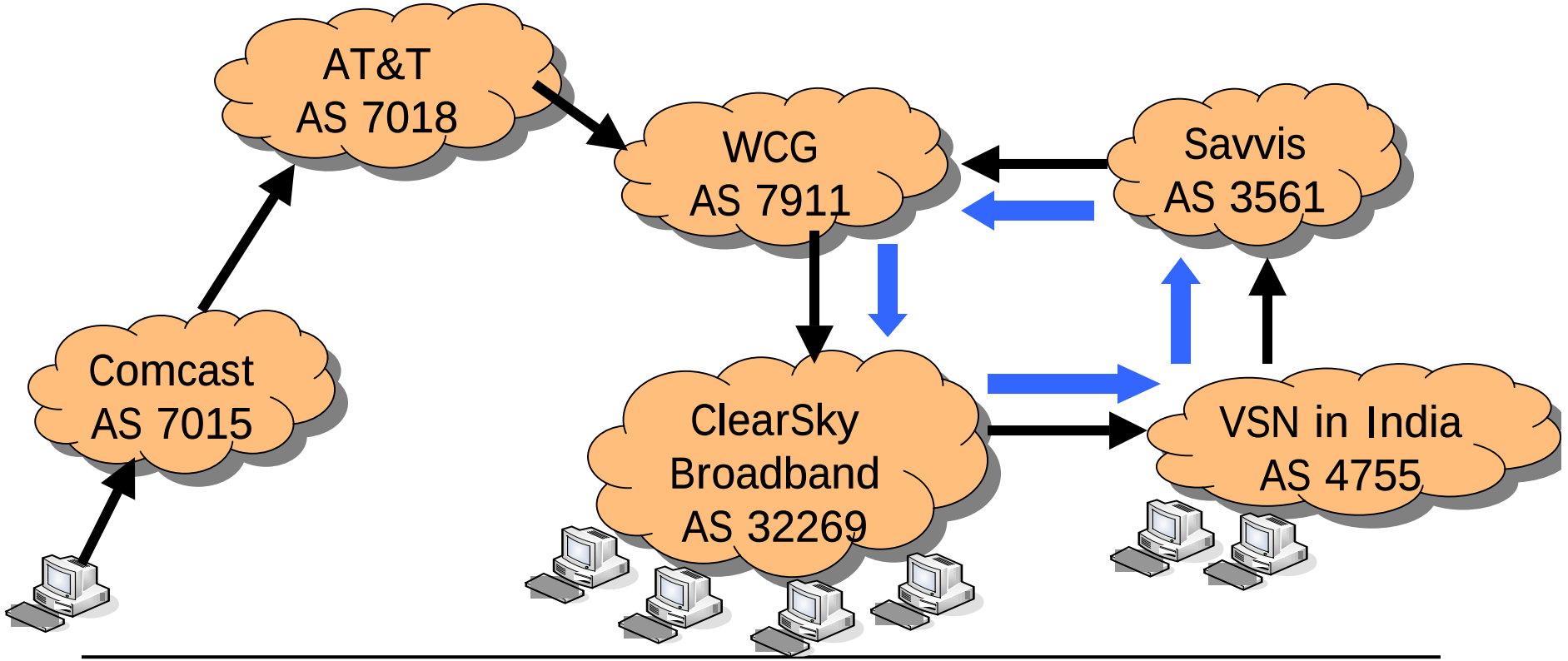
Example: Loop Occurs in Two Domains

- Traceroute to 199.239.153.1



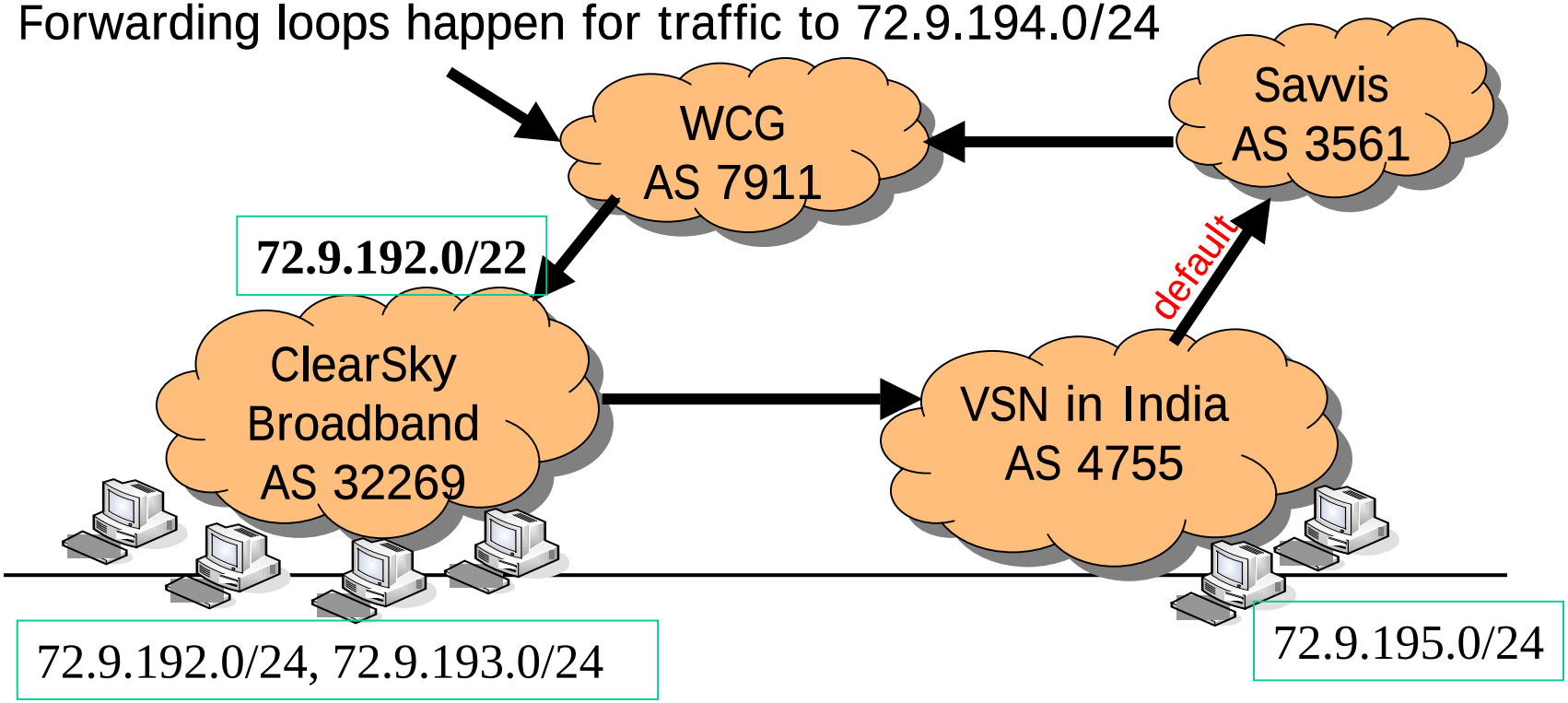
Example: Loop Occurs in 4 Domains

- Traceroute to 72.9.194.20
  - As many as 17 routers are involved in the forwarding loops



Example: Loop Occurs in 4 Domains --- Detailed Investigation

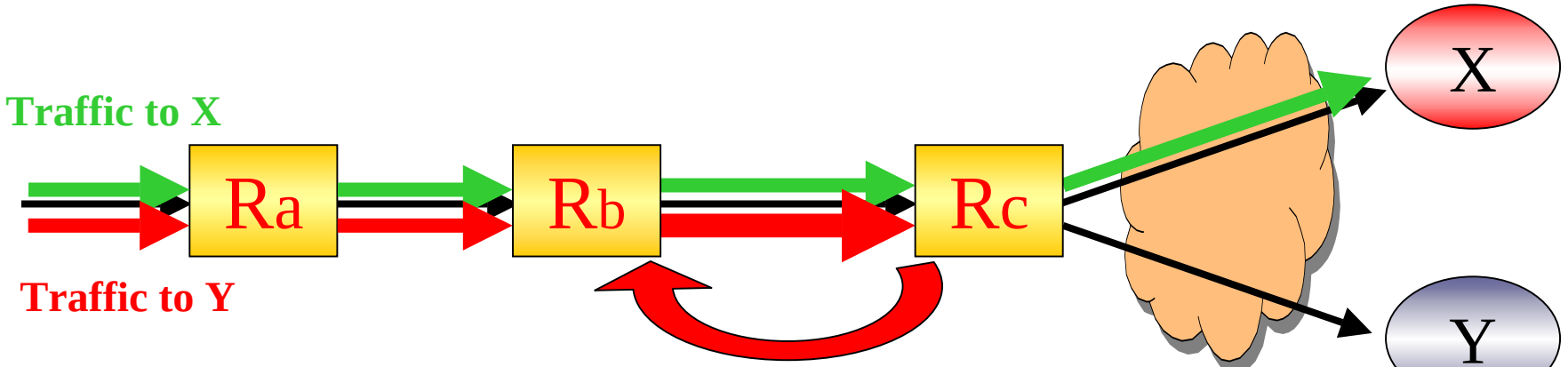
- ClearSky announces 72.9.192.0/22 to the Internet
  - Traffic to 72.9.192.0/24, 72.9.193.0/24, route locally
  - Traffic to 72.9.194.0/24, 72.9.195.0/24, forward to VSN in India
- VSN in India
  - Traffic to 72.9.195.0/24, route locally
  - Traffic to 72.9.194.0/24, use default to SAVVIS
- Forwarding loops happen for traffic to 72.9.194.0/24



Impact on Tier-1 ASes and Large ISPs

- All Tier-1 ASes will be impacted
- 52.4% of routers involved in the loops are resolved by DNS
  - Exist in all Tier-1 ASes and most large ISPs
    - UUNET Technologies, Inc (AS 701)
    - AT&T WorldNet Services (AS 7018)
    - Sprint (AS 1239)
    - Level 3 Communications, LLC (AS 3356)
    - And more, such as Qwest, Verio, SBC Global, Savvis, GLBX
  - Distributed in about 129 countries
    - US, Japan, Brazil, Russian, Germany, Italy, Mexico ...

Launching Flooding Attacks



$$Amplification = \frac{TTL_0 - N_{hops}}{L_{loop}} = \frac{255-14}{2} \approx 120$$

- Overloading a link with available bandwidth 100Mbps
  - Number of compromised hosts: 25
  - Average traffic rate needed: $\frac{100Mbps}{120*25} = 33.3Kbps$
- Even for a long loop with 16 hops
  - Still amplify attacking traffic about 15 times

Pull-Up Route and Validation

- Neglecting pull-up route can cause persistent forwarding loops
- Validation:
  - For each forwarding loop,
    - Identify the prefix announced by destination domain
    - Classify corresponding traces to that prefix into two parts
      - traces with forwarding loops
      - traces without forwarding loops
    - Pull-up route exists if
      - Traces in two parts share a same router
      - The shared router is involved in the forwarding loop
- Result:
  - About 68% of persistent forwarding loops are caused by misconfigurations on pull-up route

Summary

- Persistent forwarding loops
  - Large number of shadowed prefixes
  - Distributed in a large number of domains
- Affect legitimate hosts
  - Large number of imperiled prefixes
  - Spread widely in various domains
- Can be exploited to launch flooding attacks
  - Amplifying attacking traffic significantly
  - Can be launched from different locations
- Tier-1 ASes and large ISPs can be impacted

Thanks

- Any questions or comments?