Traffic Control Mechanisms

- Filtering
  - Source address filtering
  - Other forms of filtering
- Rate limits
- Protection against traffic analysis
  - Padding
  - Routing control

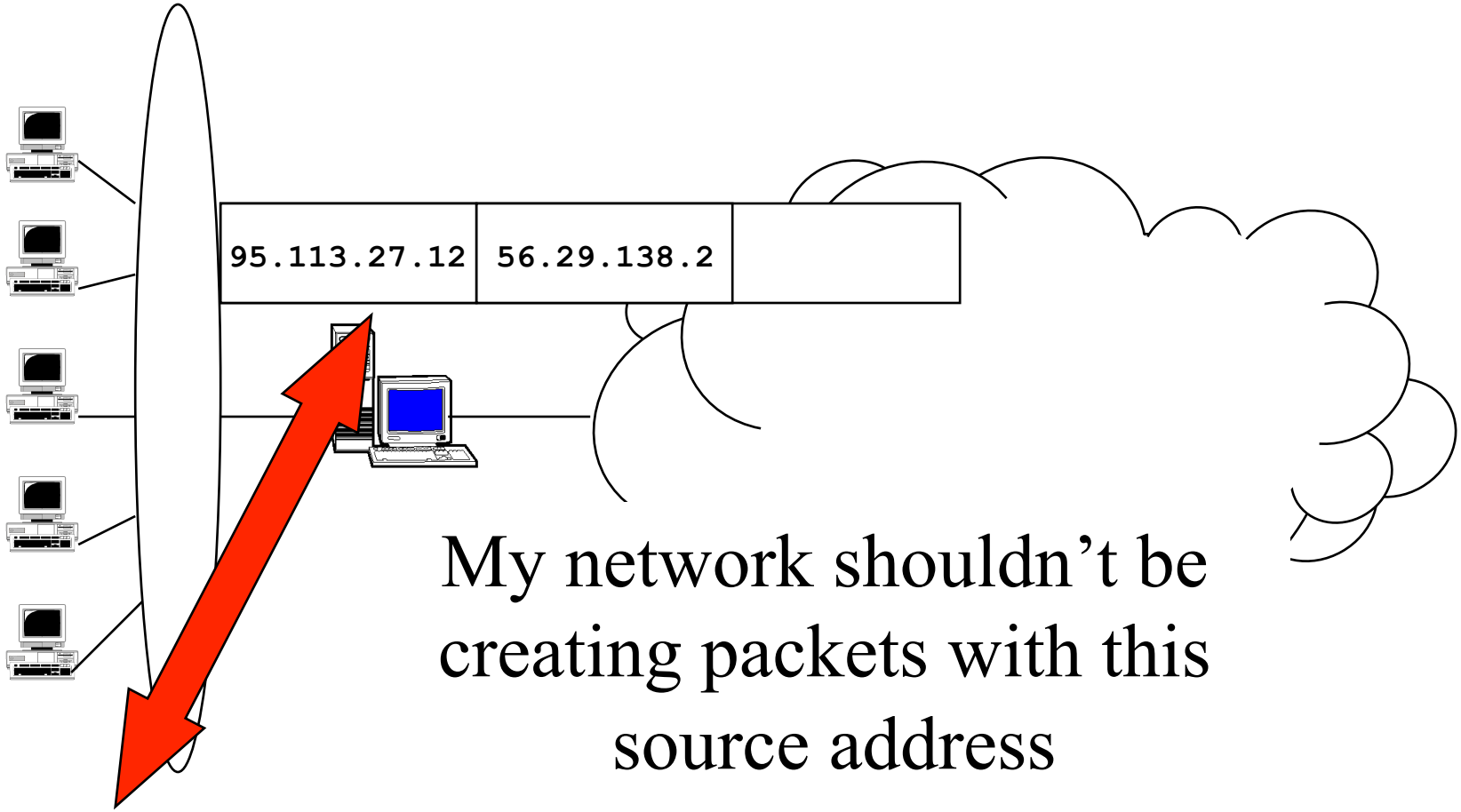
Source Address Filtering

- Filtering out some packets because of their source address value
  - Usually because you believe their source address is spoofed
- Often called ingress filtering
  - Or egress filtering . . .

Source Address Filtering for Address Assurance

- Router "knows" what network it sits in front of
  - In particular, knows IP addresses of machines there
- Filter outgoing packets with source addresses not in that range
- Prevents your users from spoofing other nodes' addresses
  - But not from spoofing each other's

Source Address Filtering Example



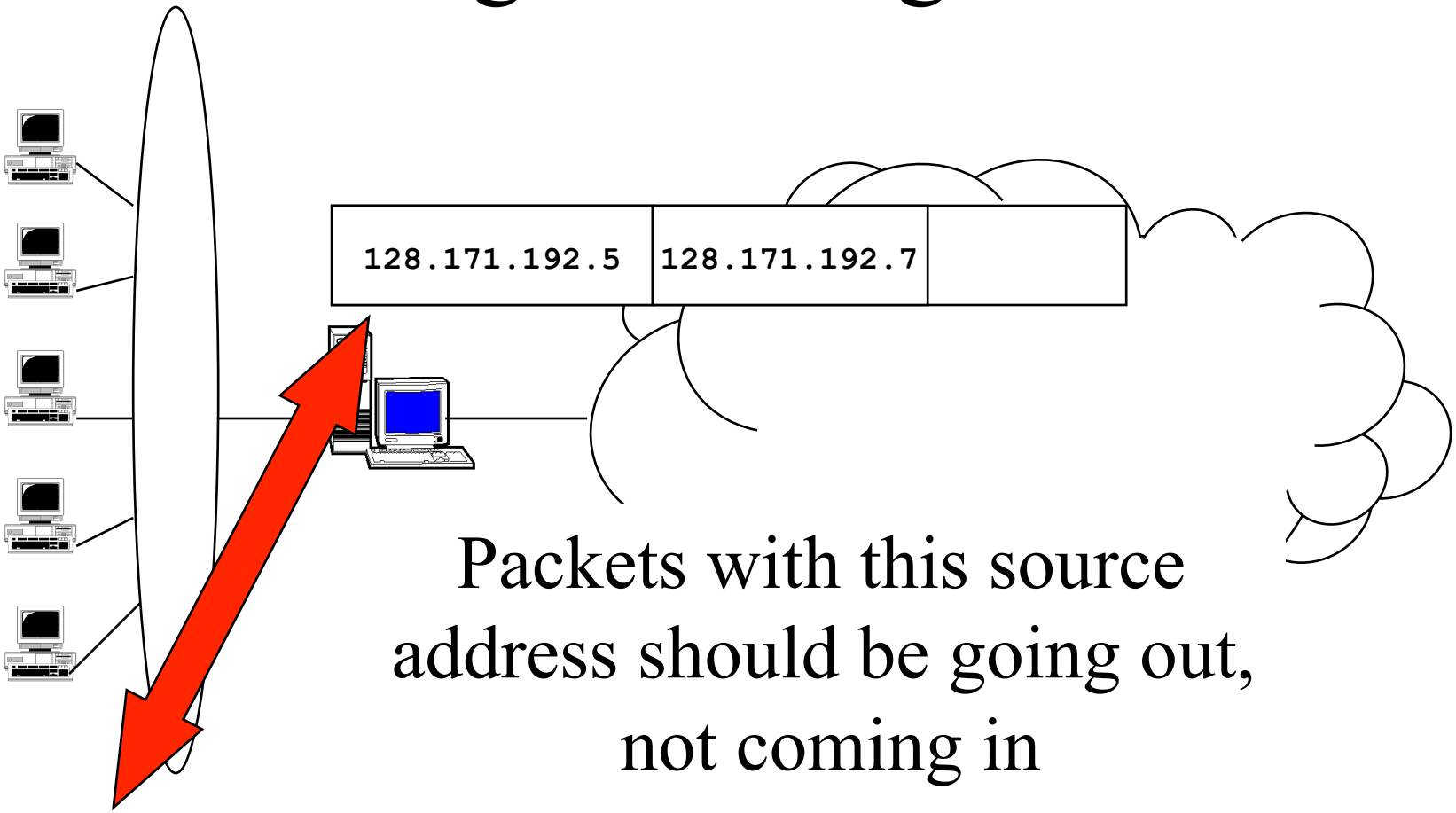
My network shouldn't be creating packets with this source address

So drop the packet

Source Address Filtering in the Other Direction

- Often called egress filtering
  - Or ingress filtering . . .
- Occurs as packets leave the Internet and enter a border router
  - On way to that router's network
- What addresses shouldn't be coming into your local network?

Filtering Incoming Packets



Other Forms of Filtering

- One can filter on things other than source address
  - Such as worm signatures, unknown protocol identifiers, etc.
- Also, there are unallocated IP addresses in IPv4 space
  - Can filter for packets going to or coming from those addresses
- Some source addresses for local use only
  - Internet routers can drop packets to/from them

Realistic Limits on Filtering

- Little filtering possible in Internet core
  - Packets being handled too fast
  - Backbone providers don't want to filter
  - Damage great if you screw it up
- Filtering near edges has its own limits
  - In what's possible
  - In what's affordable
  - In what the router owners will do

Rate Limits

- Many routers can place limits on the traffic they send to a destination
- Ensuring that the destination isn't overloaded
  - Popular for denial of service defenses
- Limits can be defined somewhat flexibly
- But often not enough flexibility to let the good traffic through and stop the bad

Padding

- Sometimes you don't want intruders to know what your traffic characteristics are
- Padding adds extra traffic to hide the real stuff
- Fake traffic must look like real traffic
  - Usually means encrypt it all
- Must be done carefully, or clever attackers can tell the good stuff from the noise

Routing Control

- Use ability to control message routing to conceal the traffic in the network
- Used in *onion routing* to hide who is sending traffic to whom
  - For anonymization purposes
- Routing control also used in some network defense
  - To hide real location of a machine
  - E.g., SOS DDoS defense system