Remotely Triggered Black Holes

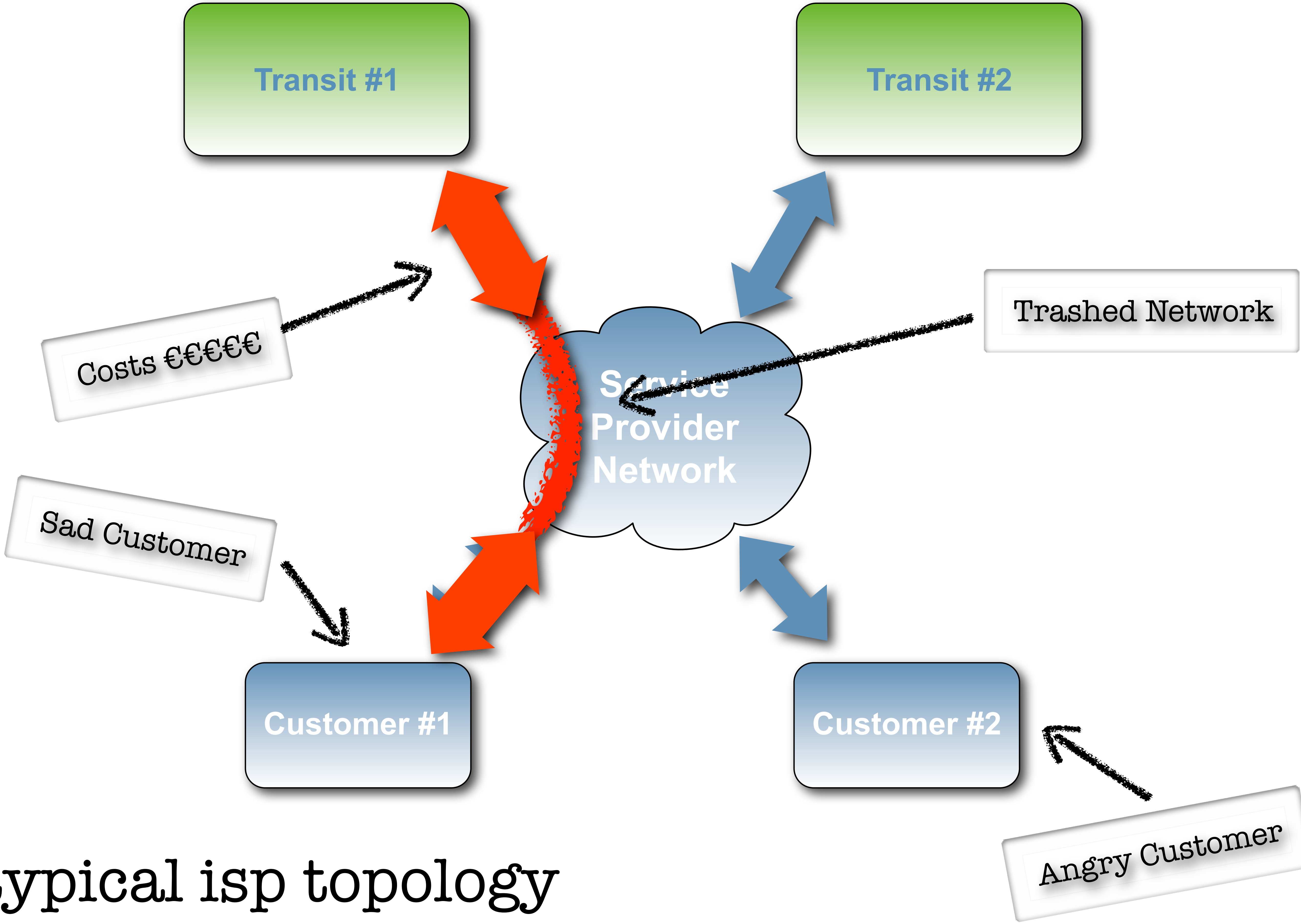
RIPE65 Routing Working Group

Amsterdam 2012

inex

internet neutral exchange

Nick Hilliard
CTO
nick@inex.ie



Transit #1

Transit #2

Costs €€€€€

Trashed Network

Service Provider Network

Sad Customer

Customer #1

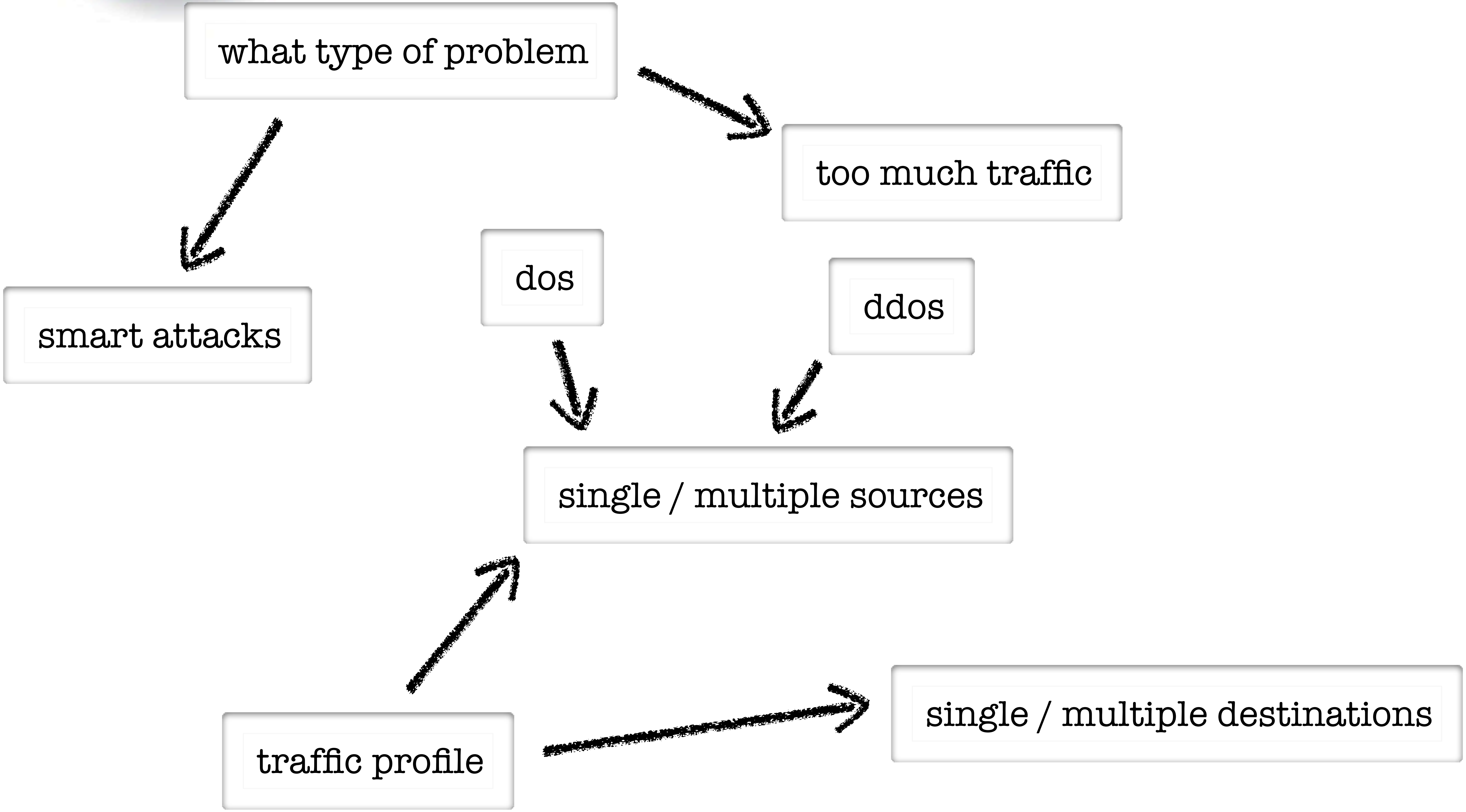
Customer #2

Angry Customer

typical isp topology

http://flickr.com/photos/crimfants/327861820/

RTBH Tutorial - Defining the Problem



what type of problem

too much traffic

smart attacks

dos

ddos

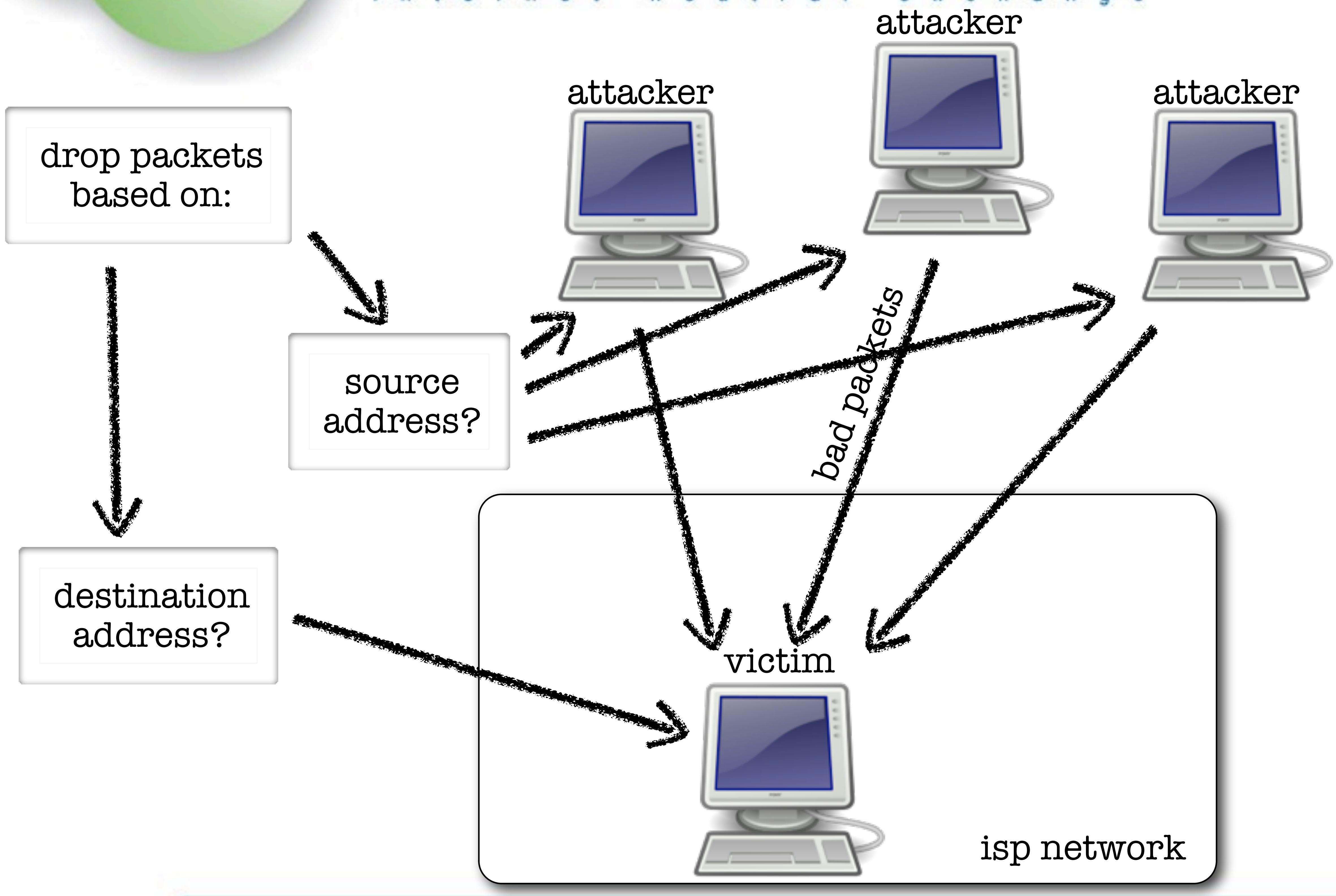
single / multiple sources

traffic profile

single / multiple destinations

resolution tools

RTBH Tutorial - Dropping Packets in a Hurry



drop packets based on:

source address?

destination address?

attacker

attacker

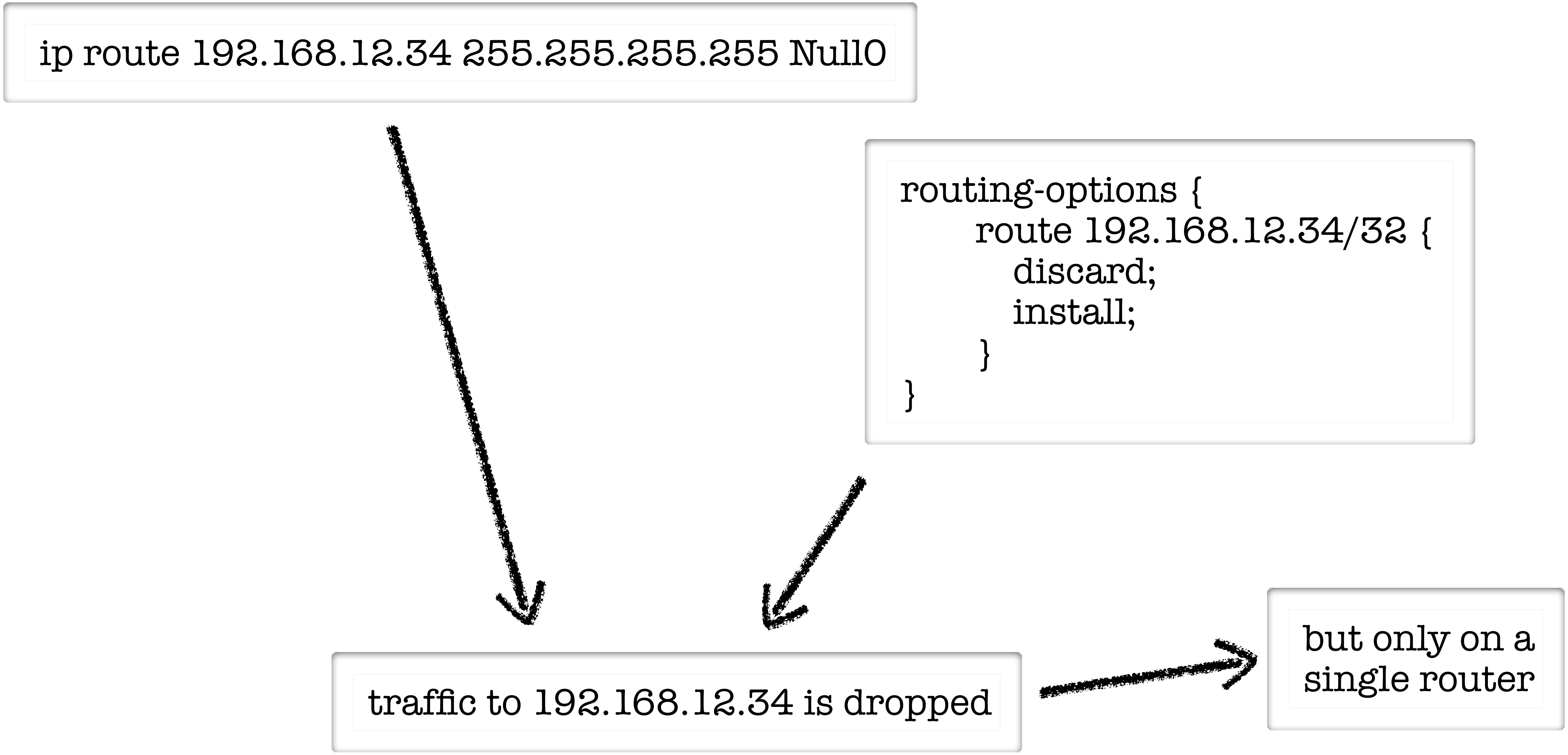
attacker

bad packets

victim

isp network

RTBH Tutorial - Naive Destination Drops



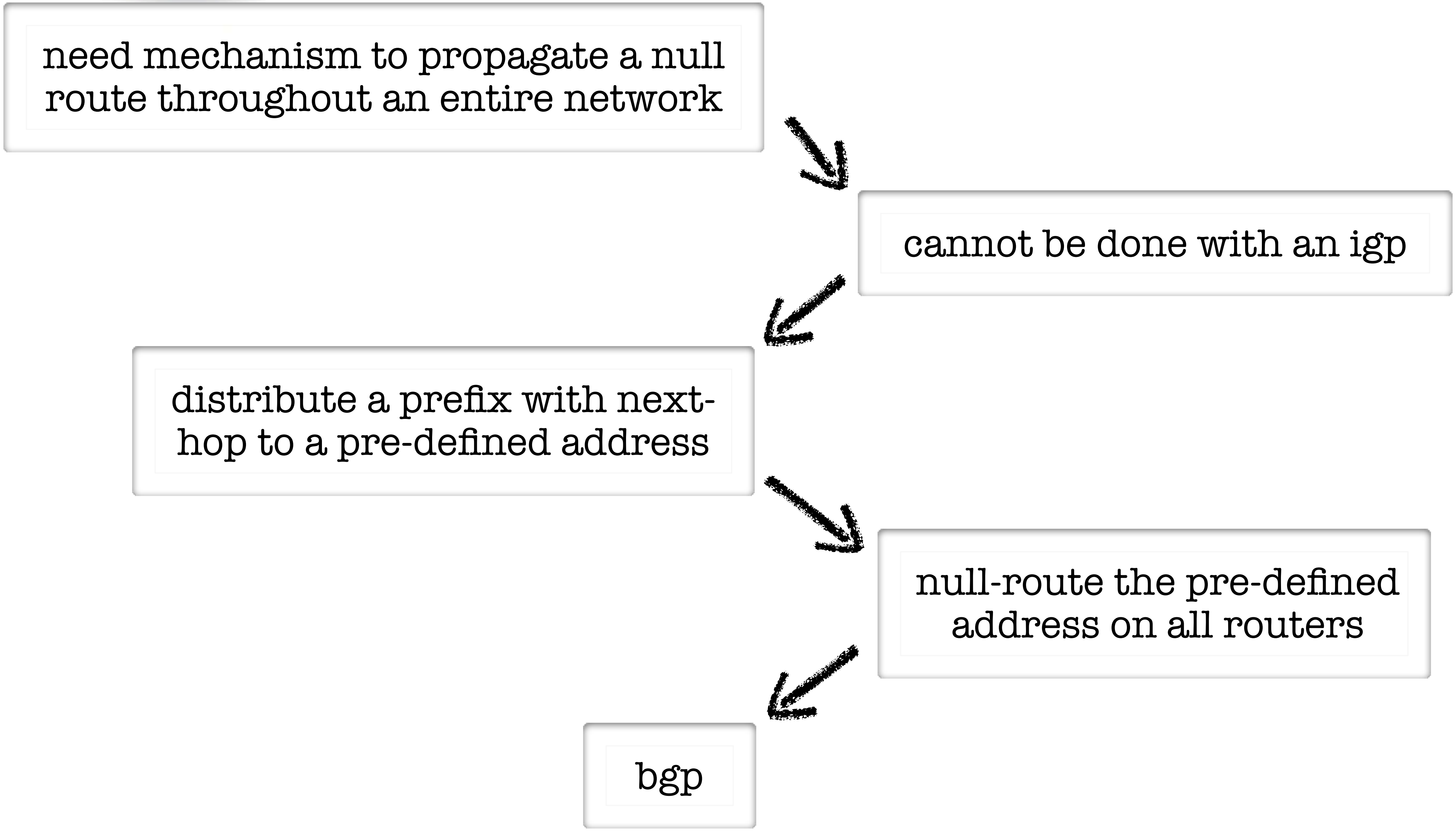
```
ip route 192.168.12.34 255.255.255.255 Null0
```

```
routing-options {
      route 192.168.12.34/32 {
         discard;
         install;
      }
}
```

traffic to 192.168.12.34 is dropped

but only on a single router

RTBH Tutorial - Naive Destination Drop Problems



need mechanism to propagate a null route throughout an entire network

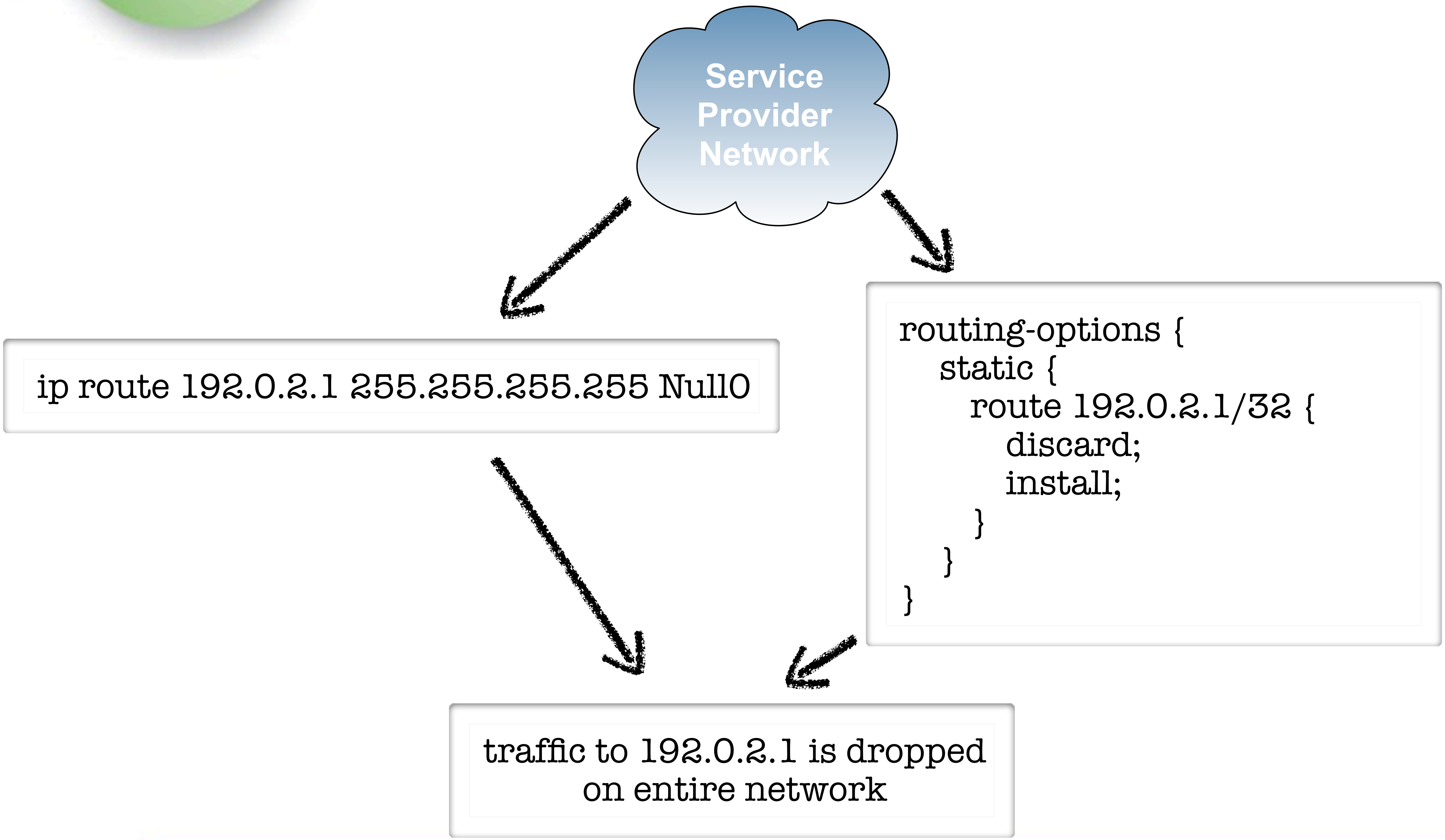
cannot be done with an igp

distribute a prefix with next-hop to a pre-defined address

null-route the pre-defined address on all routers

bgp

RTBH Tutorial - Smart Destination Drops



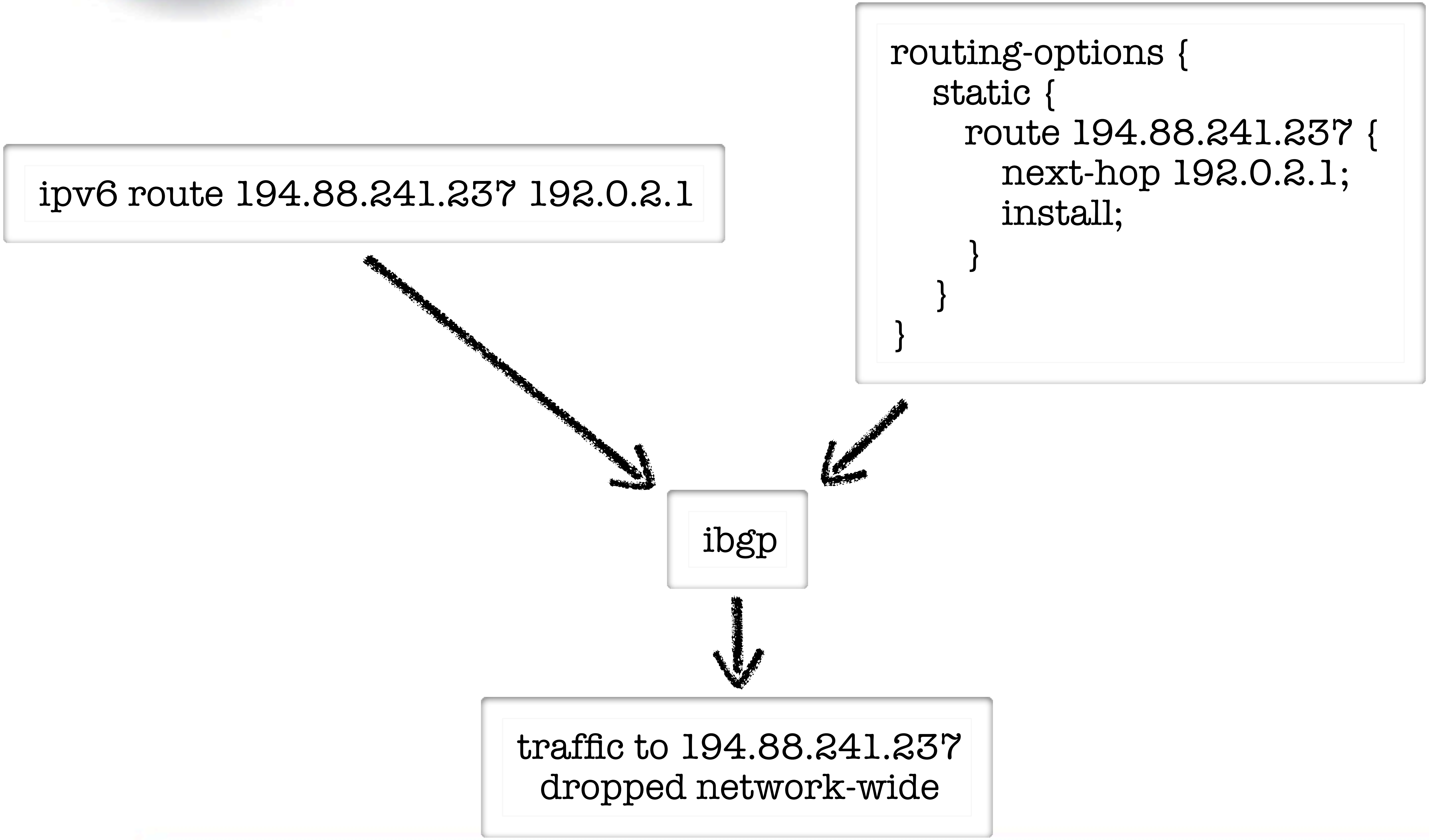
Service Provider Network

```
ip route 192.0.2.1 255.255.255.255 Null0
```

```
routing-options {
   static {
      route 192.0.2.1/32 {
         discard;
         install;
      }
   }
}
```

traffic to 192.0.2.1 is dropped
on entire network

RTBH Tutorial - Distribution via iBGP



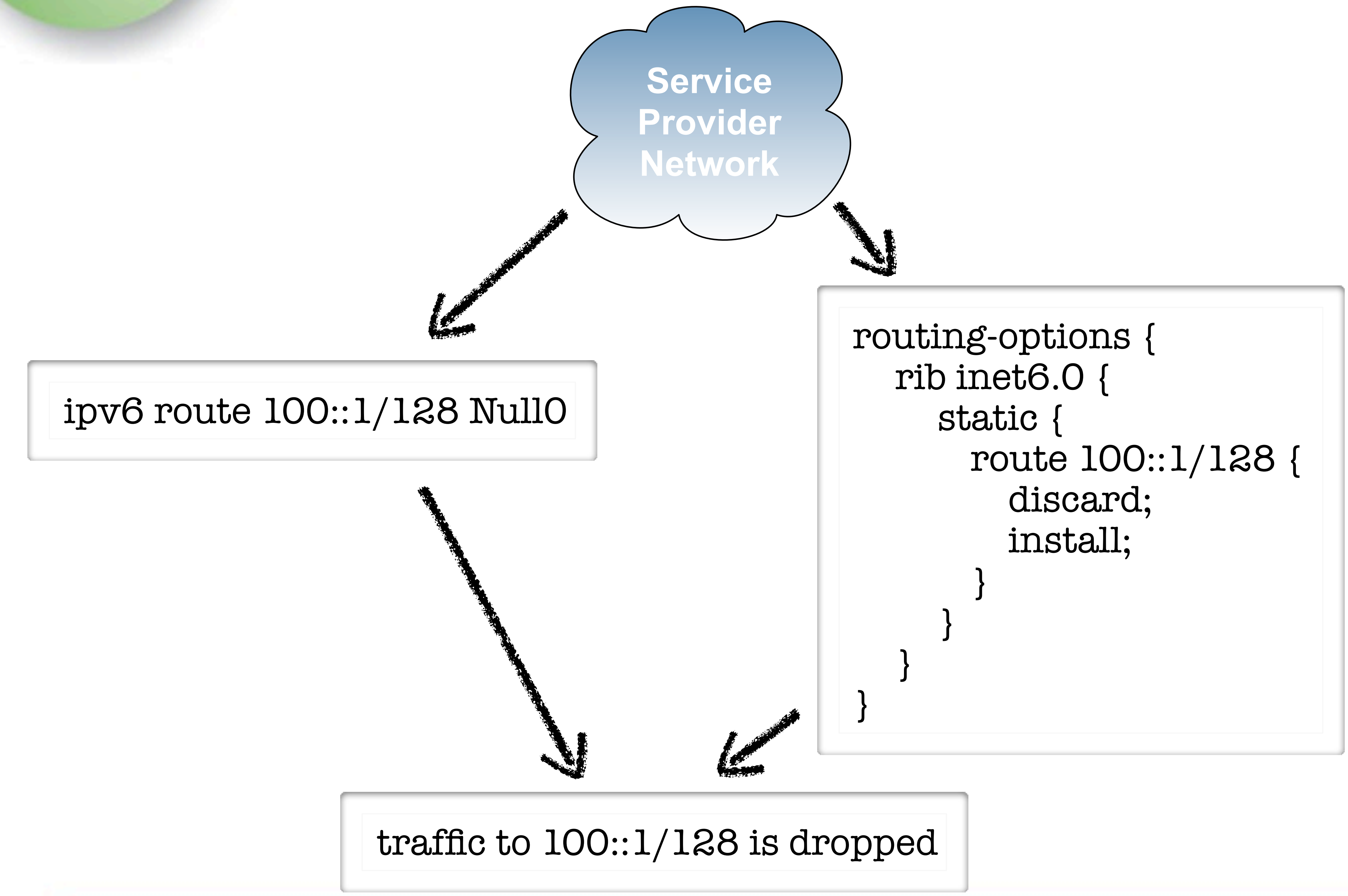
```
ipv6 route 194.88.241.237 192.0.2.1
```

```
routing-options {
   static {
      route 194.88.241.237 {
         next-hop 192.0.2.1;
         install;
      }
   }
}
```

ibgp

traffic to 194.88.241.237
dropped network-wide

RTBH Tutorial - Works on IPv6 Too



Service Provider Network

ipv6 route 100::1/128 Null0

```
routing-options {
   rib inet6.0 {
      static {
         route 100::1/128 {
            discard;
            install;
         }
      }
   }
}
```

traffic to 100::1/128 is dropped

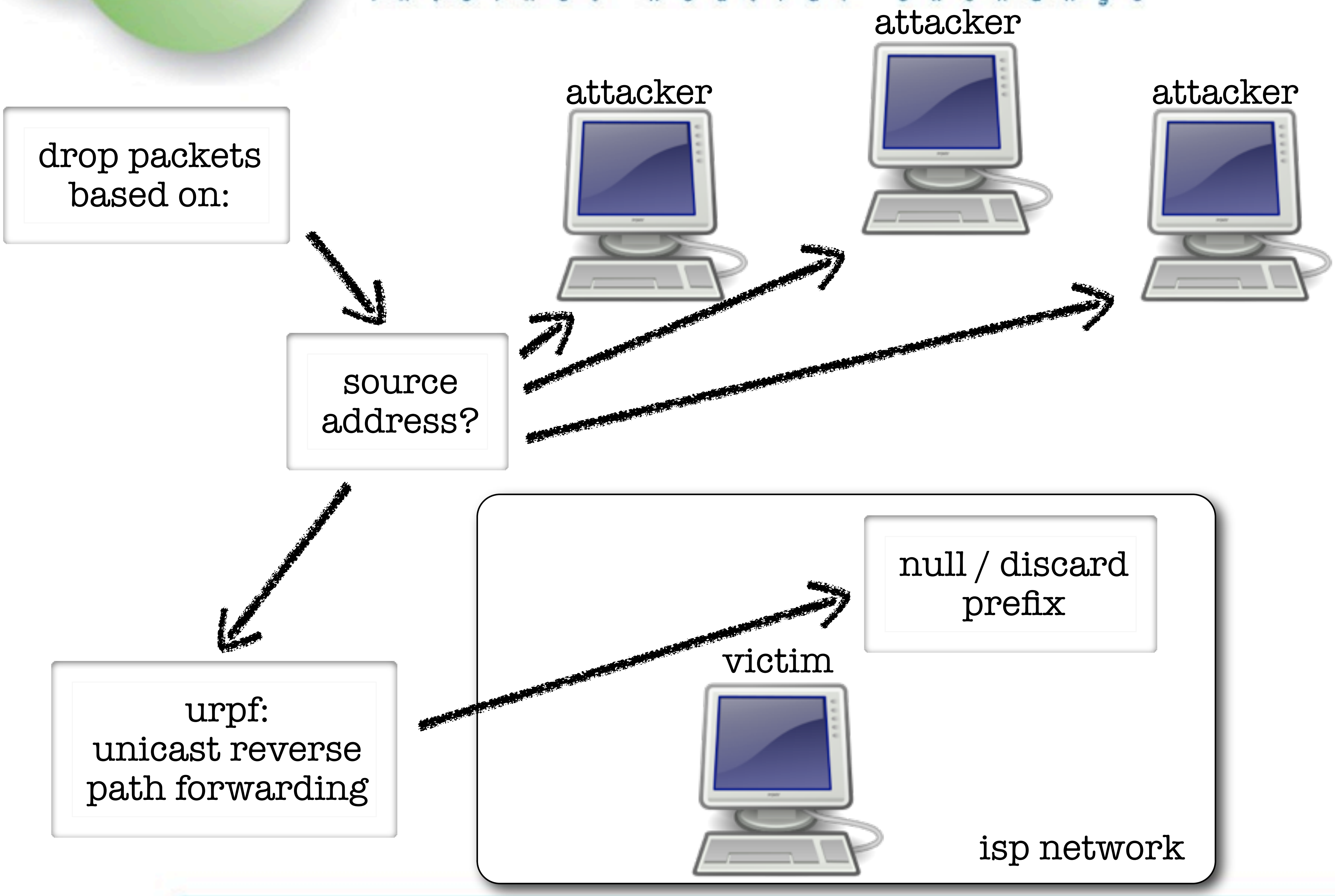
RTBH Tutorial - Commercial Break

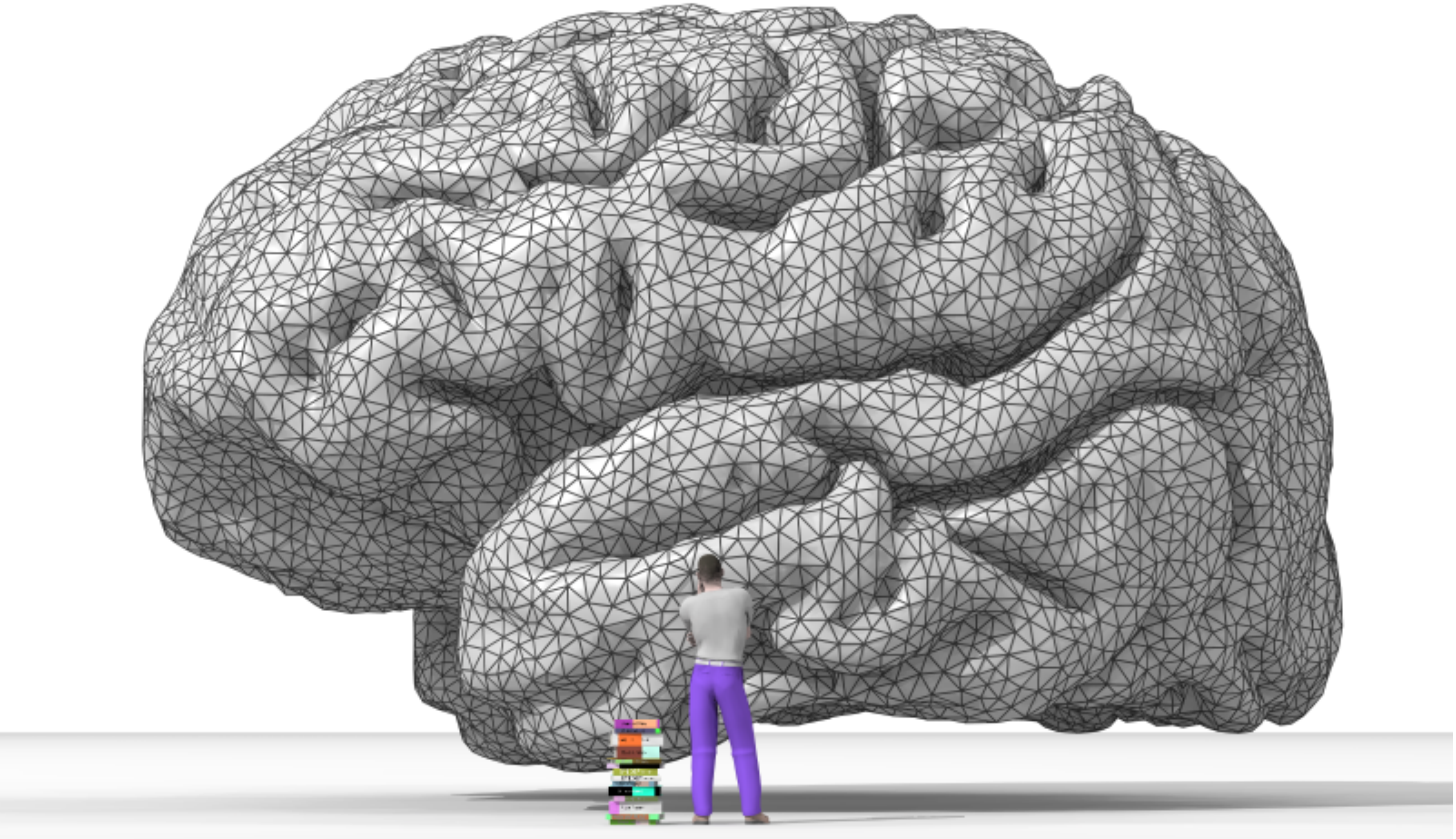
shameless plug

RFC 6666

100::/64

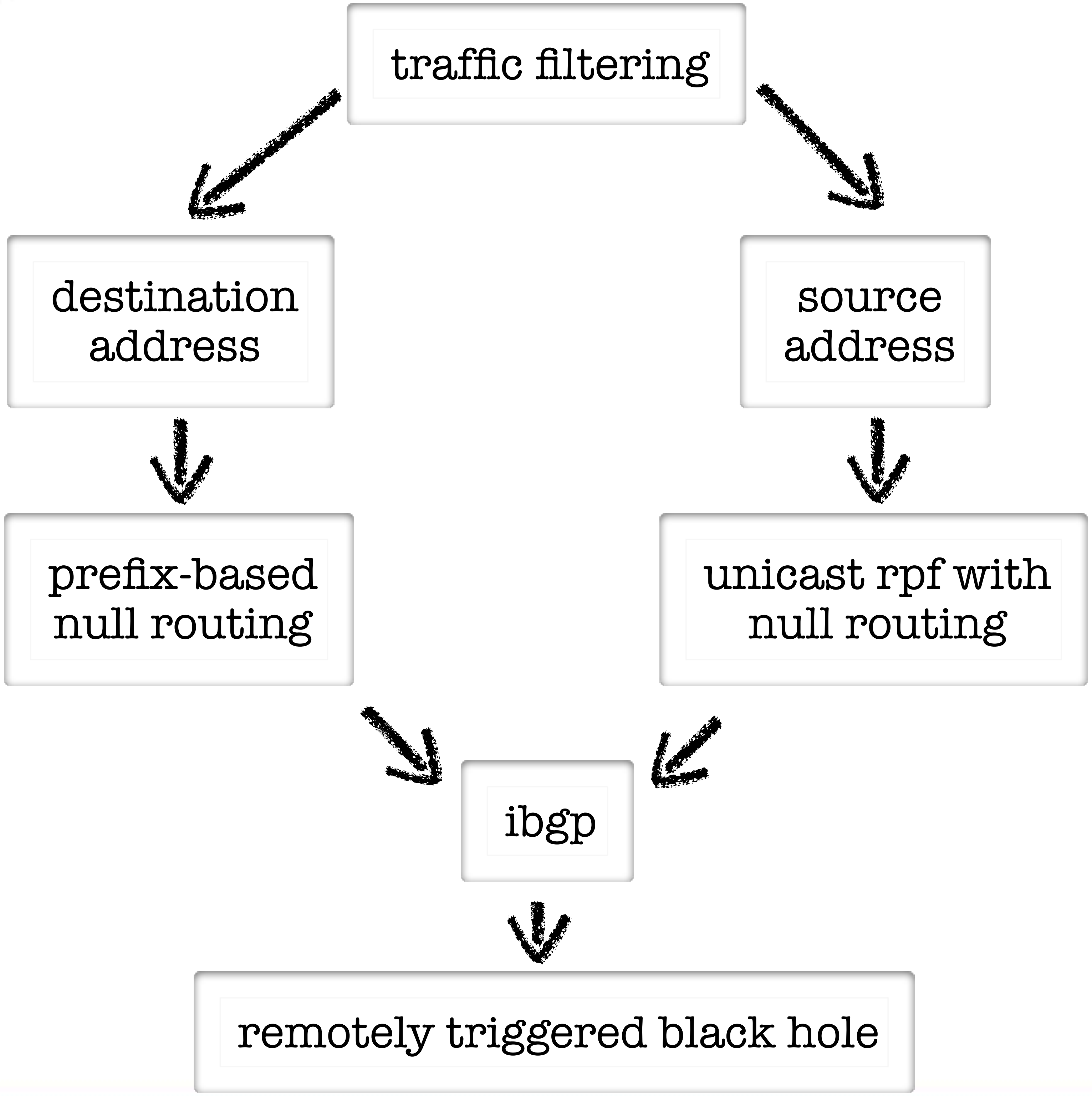
RTBH Tutorial - Source Filtering





http://www.loria.fr/~rougier

RTBH Tutorial - Methodology



traffic filtering

destination address

source address

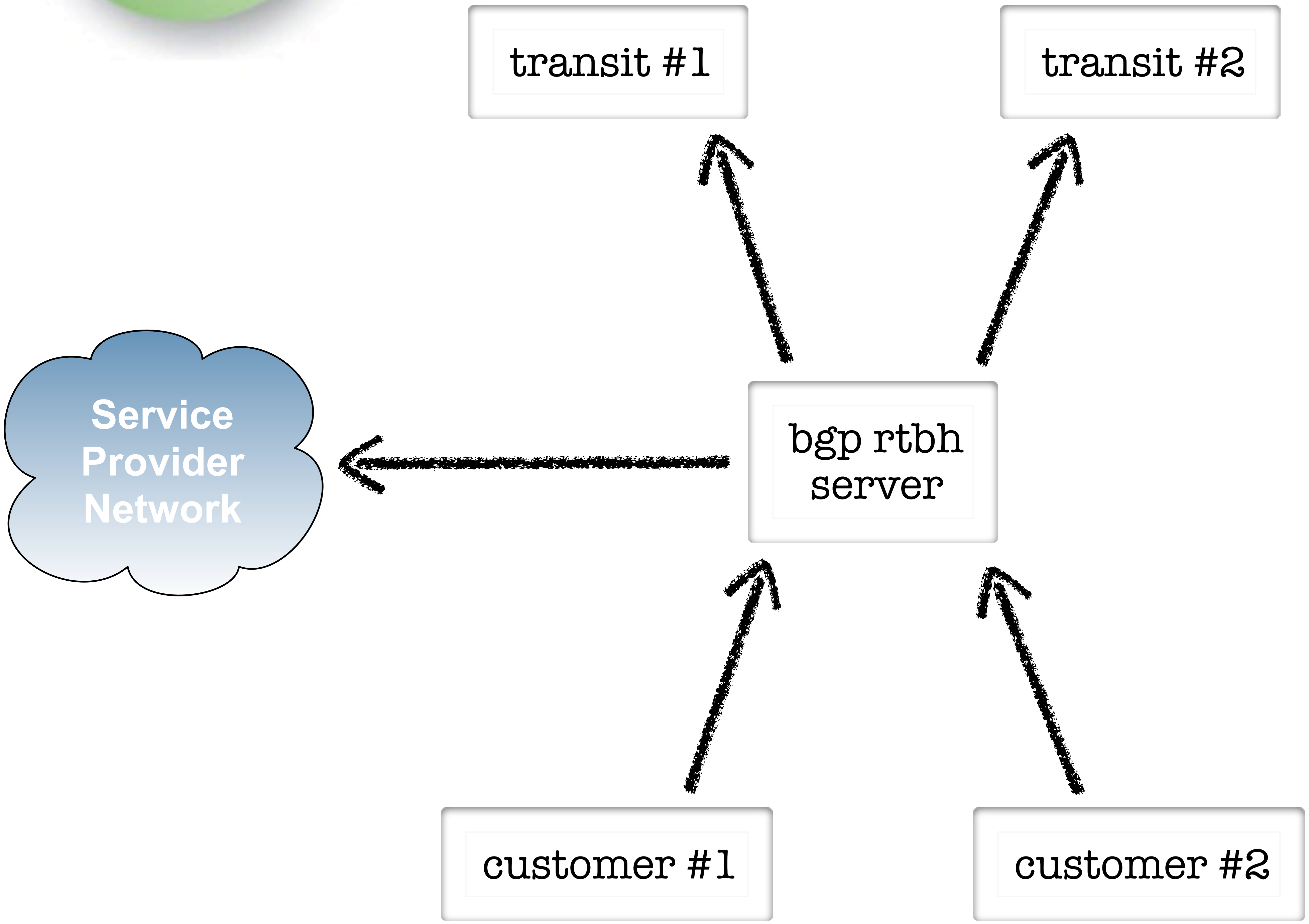
prefix-based null routing

unicast rpf with null routing

ibgp

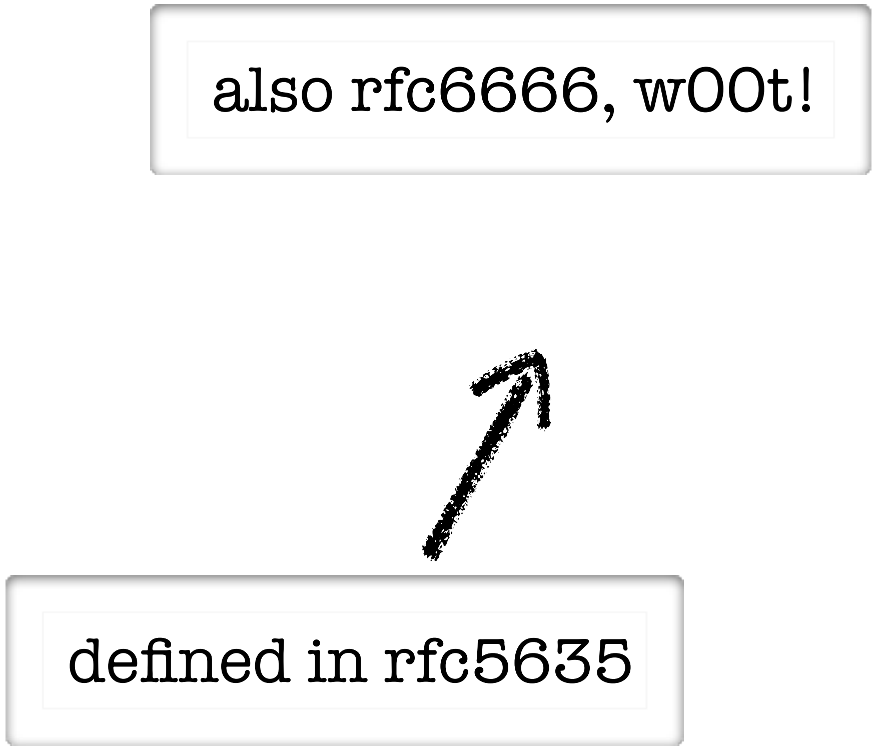
remotely triggered black hole

RTBH Tutorial - Methodology



RTBH Tutorial - It’s Good Stuff

fully standards compliant



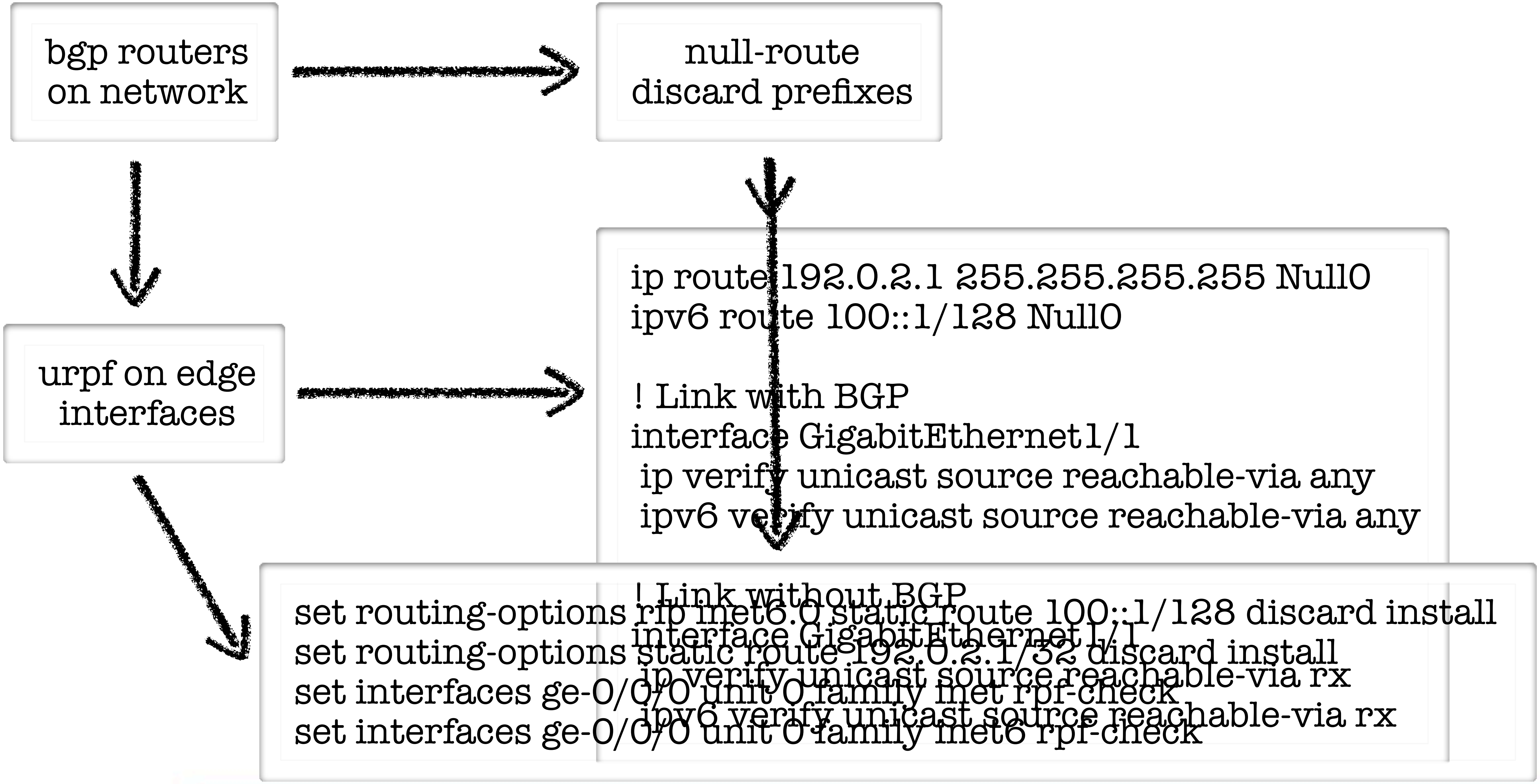
defined in rfc5635

also rfc6666, w00t!

fast, efficient means of black-holing

supported by most transit providers

RTBH Tutorial - Client Configuration



bgp routers on network

null-route discard prefixes

urpf on edge interfaces

```
ip route 192.0.2.1 255.255.255.255 Null0
ipv6 route 100::1/128 Null0

! Link with BGP
interface GigabitEthernet1/1
 ip verify unicast source reachable-via any
 ipv6 verify unicast source reachable-via any

! Link without BGP
interface GigabitEthernet1/1
 ip verify unicast source reachable-via rx
 ipv6 verify unicast source reachable-via rx
```

```
set routing-options rib inet6.0 static route 100::1/128 discard install
set routing-options static route 192.0.2.1/32 discard install
set interfaces ge-0/0/0 unit 0 family inet rpf-check
set interfaces ge-0/0/0 unit 0 family inet6 rpf-check
```

RTBH Tutorial - Implementation Notes

be careful that your hardware supports unicast rpf properly

if you use next-hop-self in your ibgp policy, best to have separate rtbh box

don’t run ipv6 unicast rpf on a sup720

separate rtbh works well with route reflector config

asr9k requires IOS XR >= 4.1.1

can also run rtbh server on quagga, bird, etc

RTBH Tutorial - Server Configuration

- mechanism to inject prefixes
- uplink configuration to transits
- tags to control injection policy
- downlink configuration to isp customers
- policy of accepting host prefixes only
- juniper and cisco configuration
- ipv4 and ipv6 configuration examples
- includes trigger configuration

https://www.inex.ie/rtbh