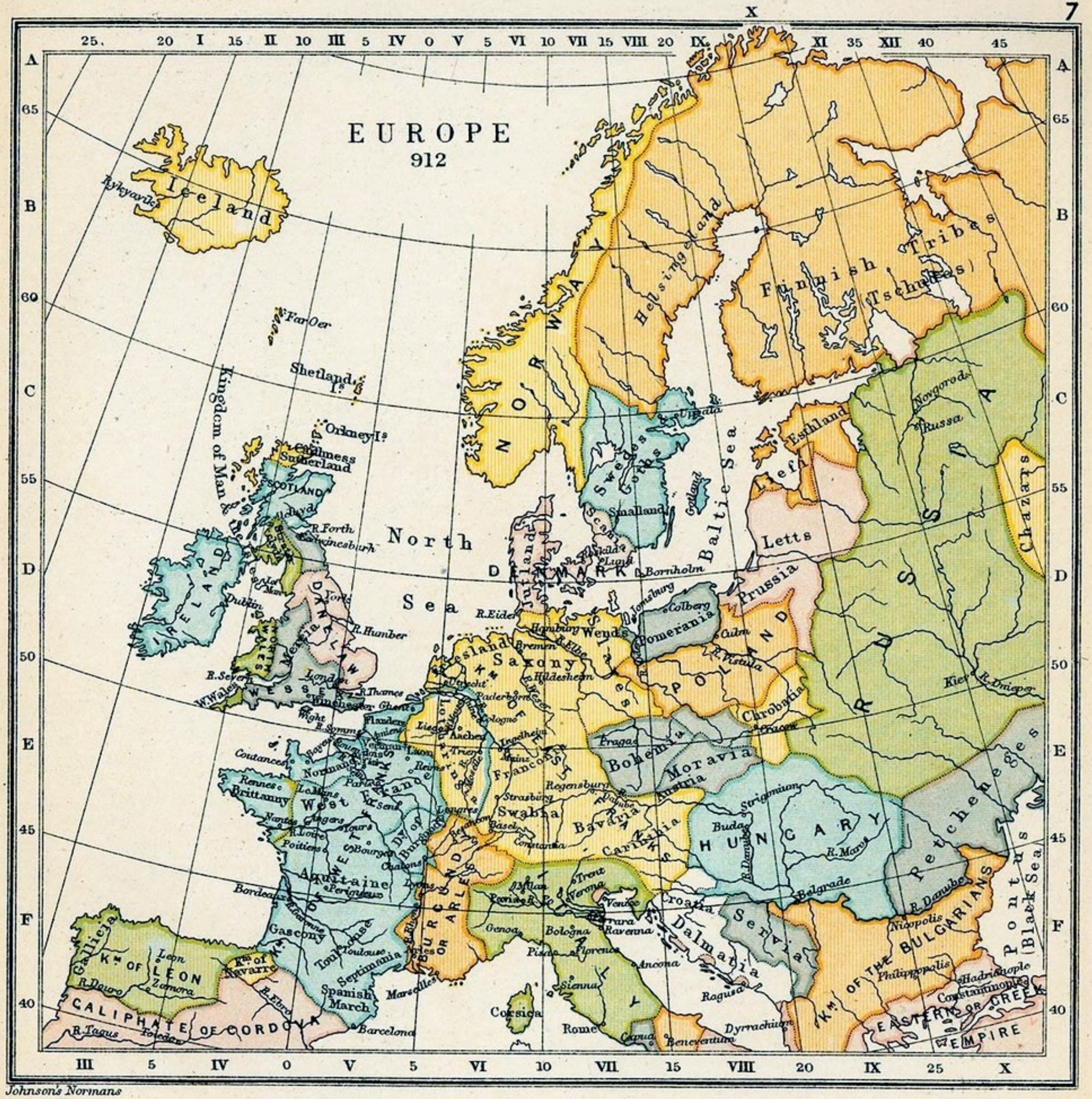
Remotely Triggered Black Holes

UKNOF 24
January 2013

Nick Hilliard
Chief Technical Officer
nick@inex.ie

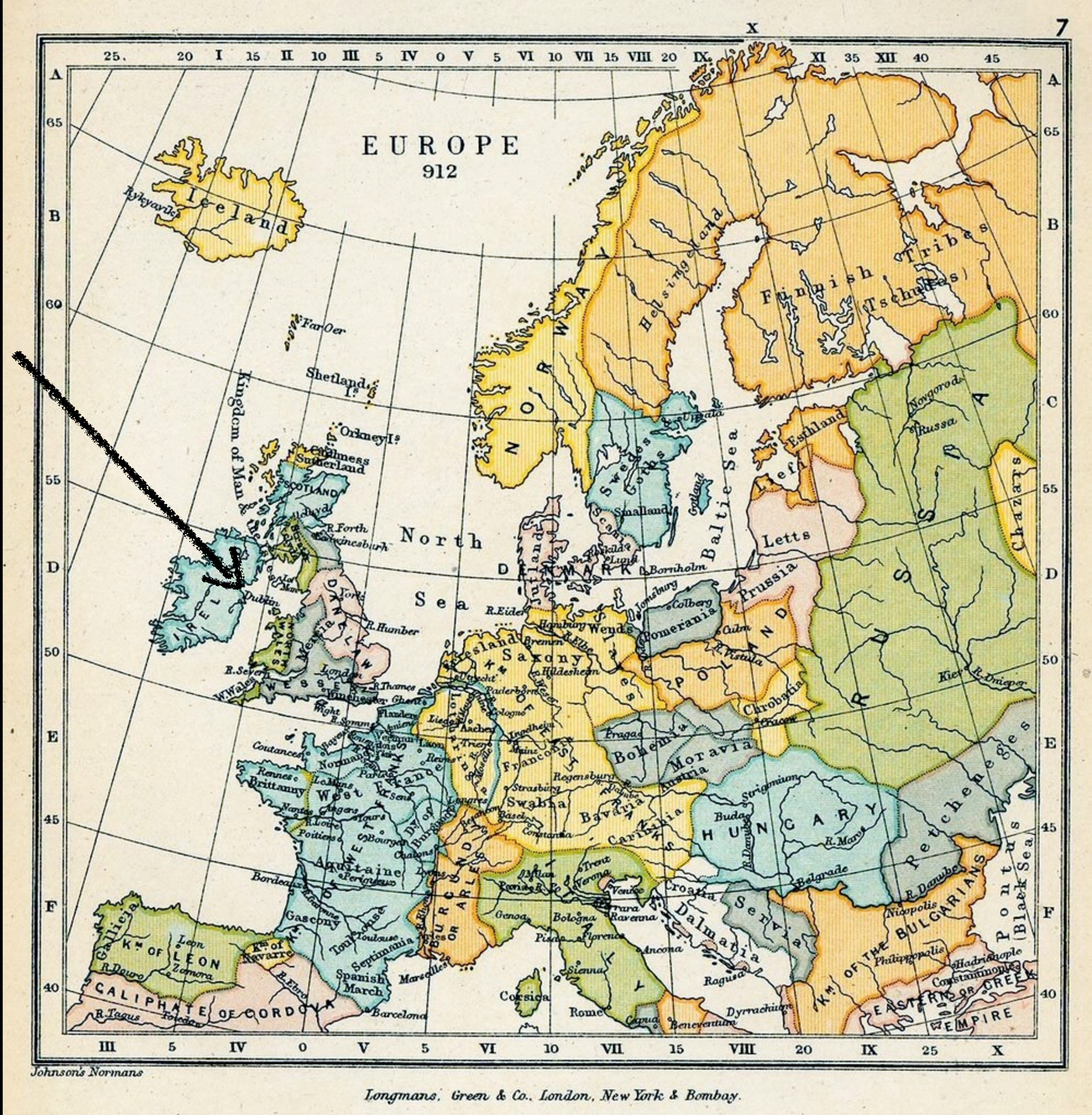


EUROPE
912

Johnson's Normans

Longmans, Green & Co., London, New York & Bombay.

dublin


7
EUROPE
912
Iceland
Rykyavik
Far Oer
Shetland Is
Orkney Is
Caithness
Sutherland
Kingdom of Man & the Isles
SCOTLAND
Lloyd
R. Forth
Edwinesburh
IRELAND
Dublin
Man
WALES
N. Wales
S. Wales
W. Wales
R. Severn
Mercia
DANELAW
York
R. Humber
London
WESSEX
Winchester
R. Thames
Wight
North Sea
NORWAY
Helsingeland
Finnish Tribes
(Tschudes)
Swedes
Gotas
Smalland
Gotland
Upsala
Baltic Sea
Scania
Roskild
Lund
Bornholm
DENMARK
Jutland
R. Eider
Esthland
Liefs
Letts
Prussia
RUSSIA
Novgorod
Russa
Chazars
Kiev
R. Dnieper
Jomsburg
Colberg
Pomerania
Wends
Hamburg
Bremen
R. Elbe
Friesland
Saxony
Hildesheim
Paderborn
Utrecht
Culm
R. Vistula
POLAND
Chrobatia
Cracow
Pragae
Bohemia
Moravia
Austria
Regensburg
R. Danube
Franconia
Mainz
Ingelheim
Trier
Aachen
Liege
Cologne
Ghent
Flanders
R. Somme
Amiens
Rouen
Normandy
Paris
Laon
Reims
Coutances
Rennes
Brittany
Le Mans
Angers
Nantes
R. Loire
Tours
Poitiers
Bourges
West Franks
France
Burgundy
Duchy of Burgundy
Chalons
Langres
Besançon
Lyons
Strasburg
Swabia
Basel
Constantia
Bavaria
Carinthia
Hungary
Strigonium
Buda
R. Maros
Belgrade
Aquitaine
Perigueux
Bordeaux
Gascony
Toulouse
Septimania
Arles
Marseilles
Spanish March
Barcelona
R. Ebro
Kn. of Navarre
Kn. of Leon
Leon
Zamora
Gallicia
R. Douro
R. Tagus
Toledo
CALIPHATE OF CORDOVA
Burgundy or Arles
Milan
Pavia
Verona
Trent
Venice
Genoa
Bologna
Ferrara
Ravenna
Pisa
Florence
Ancona
Sienna
ITALY
Corsica
Rome
Capua
Beneventum
Croatia
Dalmatia
Servia
Ragusa
Dyrrachium
Petchenegs
R. Danube
Nicopolis
Kn. of the Bulgarians
Philippopolis
Hadrianople
Constantinople
EASTERN OR GREEK EMPIRE
Pontus (Black Sea)
Johnson's Normans
Longmans, Green & Co., London, New York & Bombay.

things we irish believe in

things we irish believe in

things we irish believe in

things we irish believe in

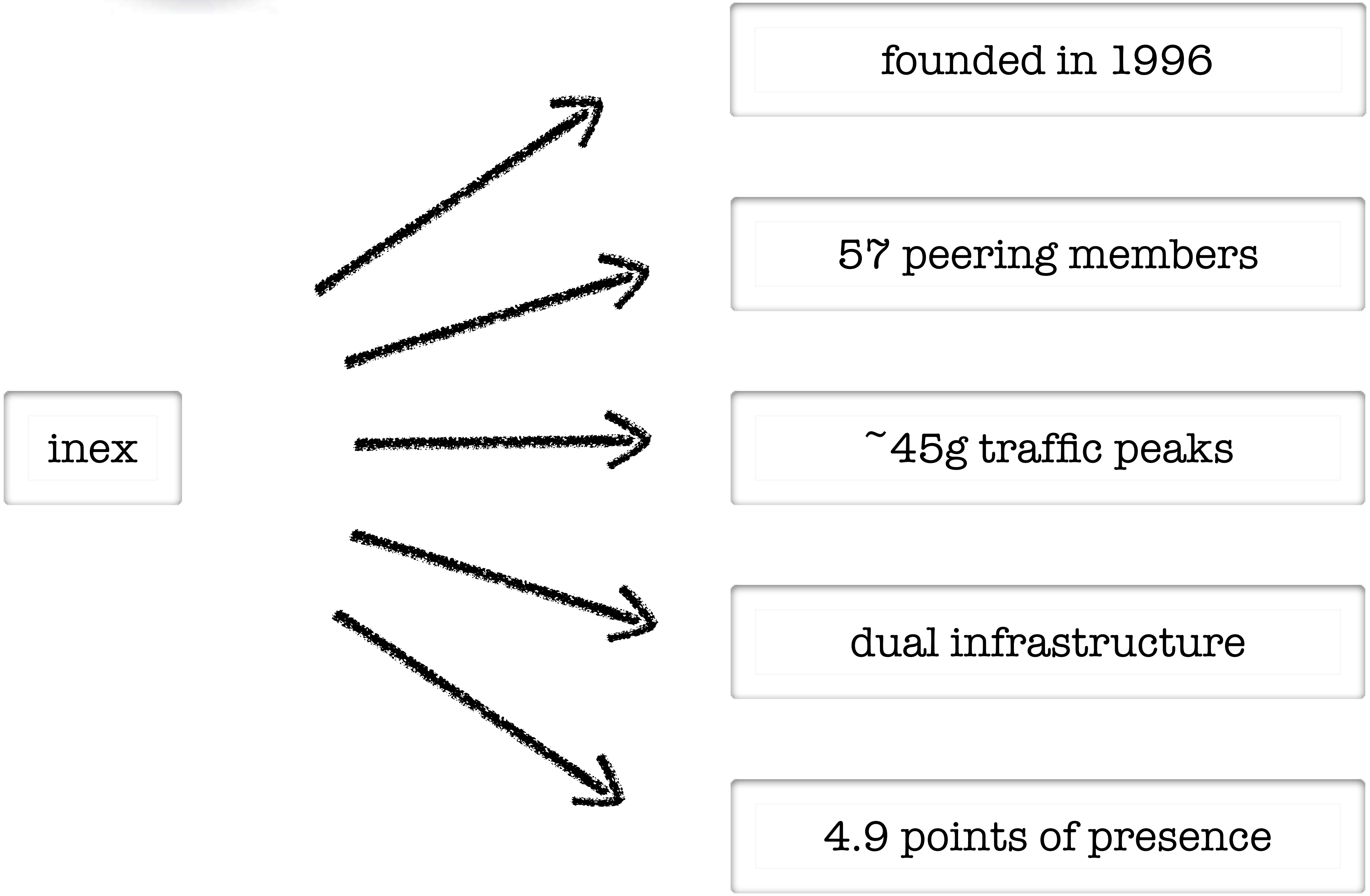
things we irish believe in

http://goo.gl/maps/k9zZL

http://www.flickr.com/photos/15462727@N07/2655010719

IXP Overview

IXP Overview



inex

founded in 1996

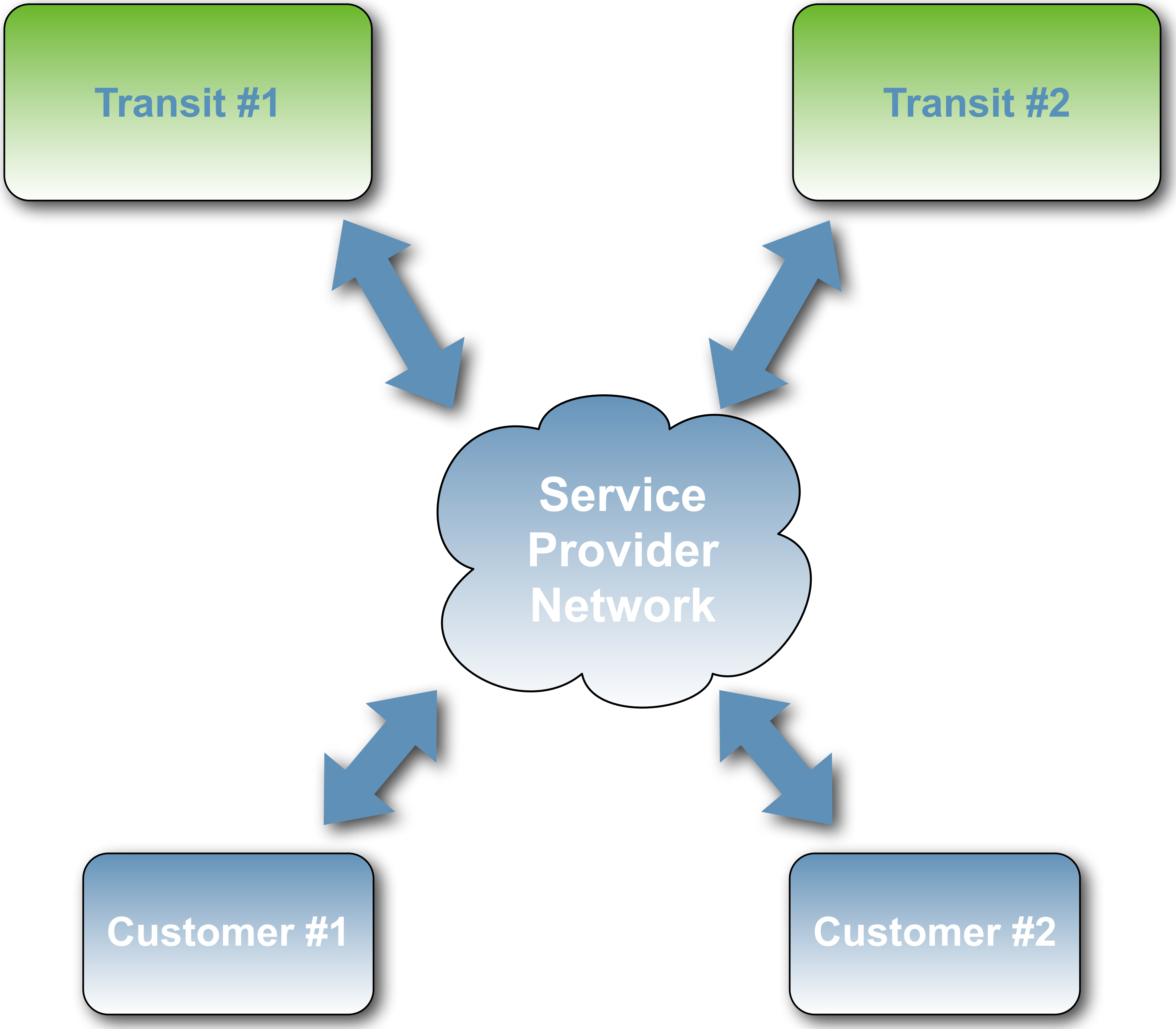
57 peering members

~45g traffic peaks

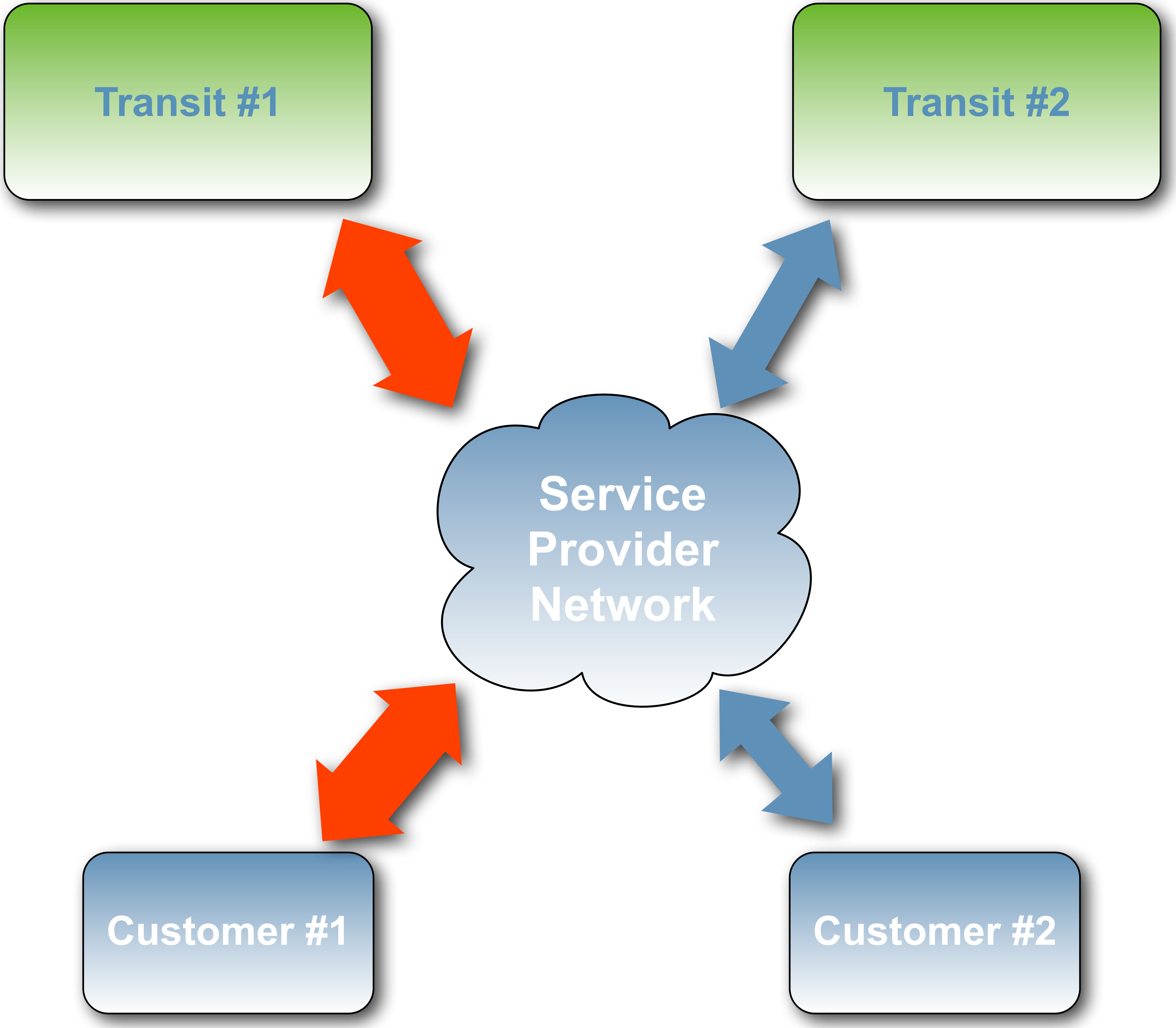
dual infrastructure

4.9 points of presence

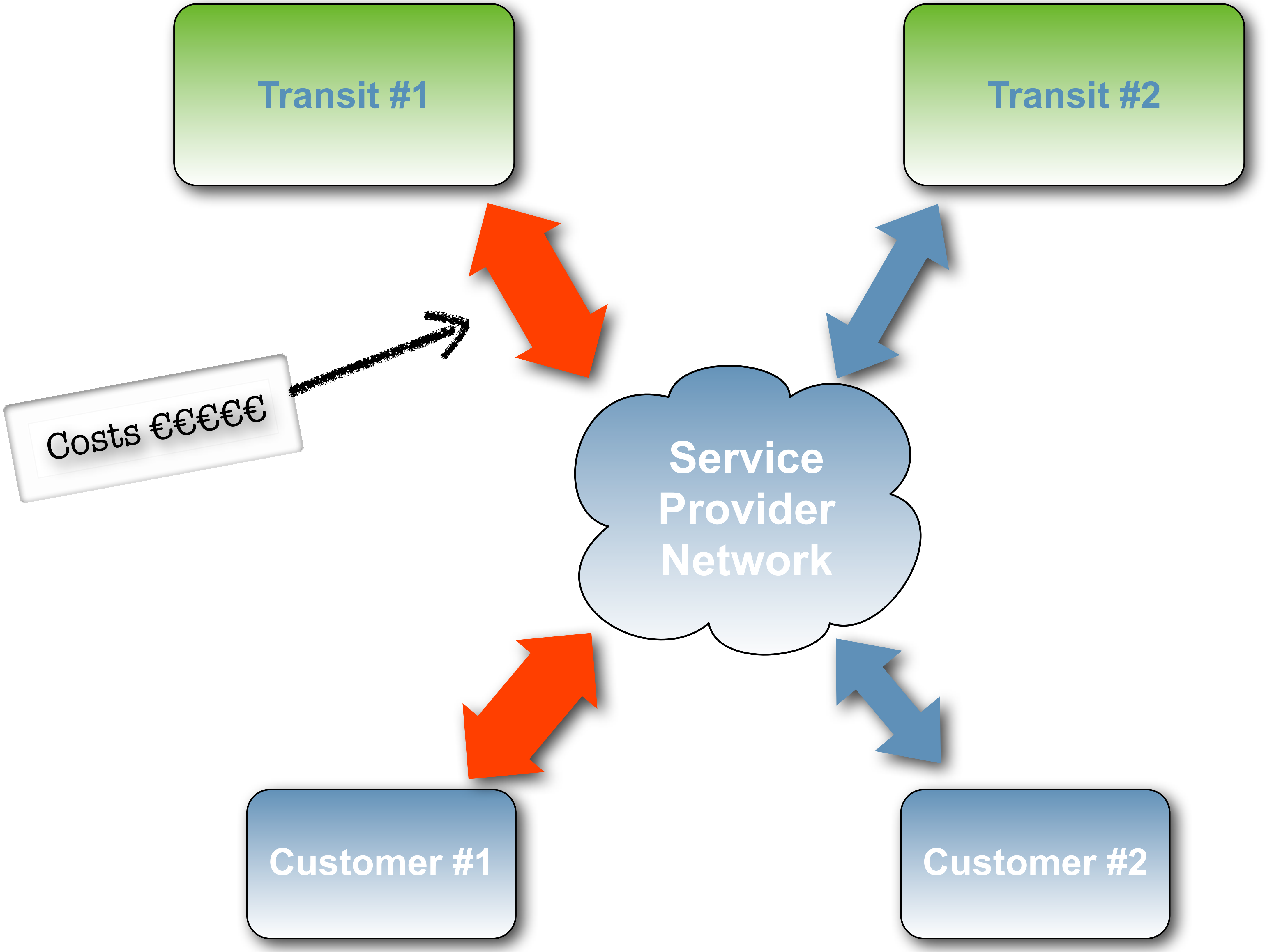
typical isp topology



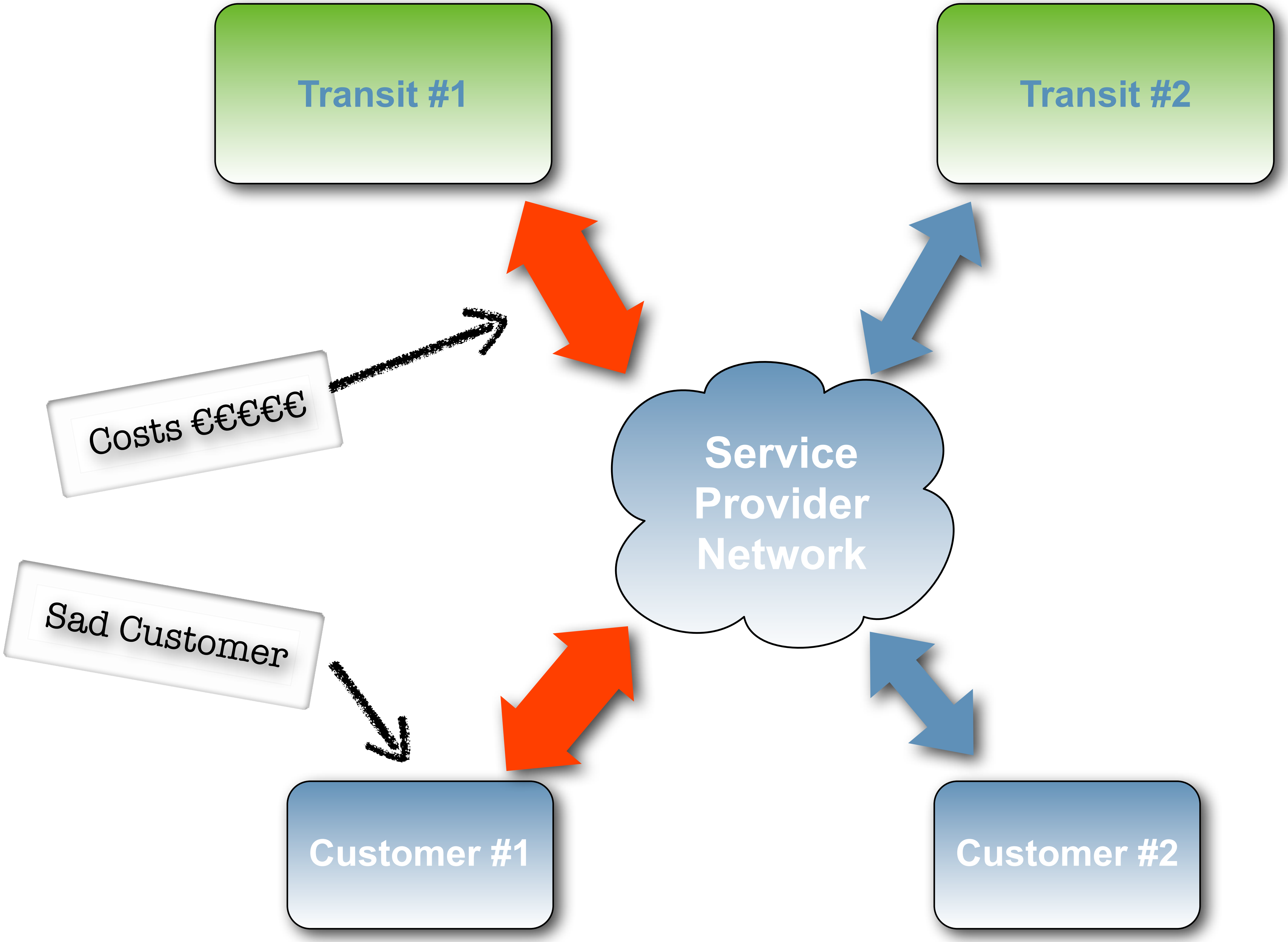
typical isp topology



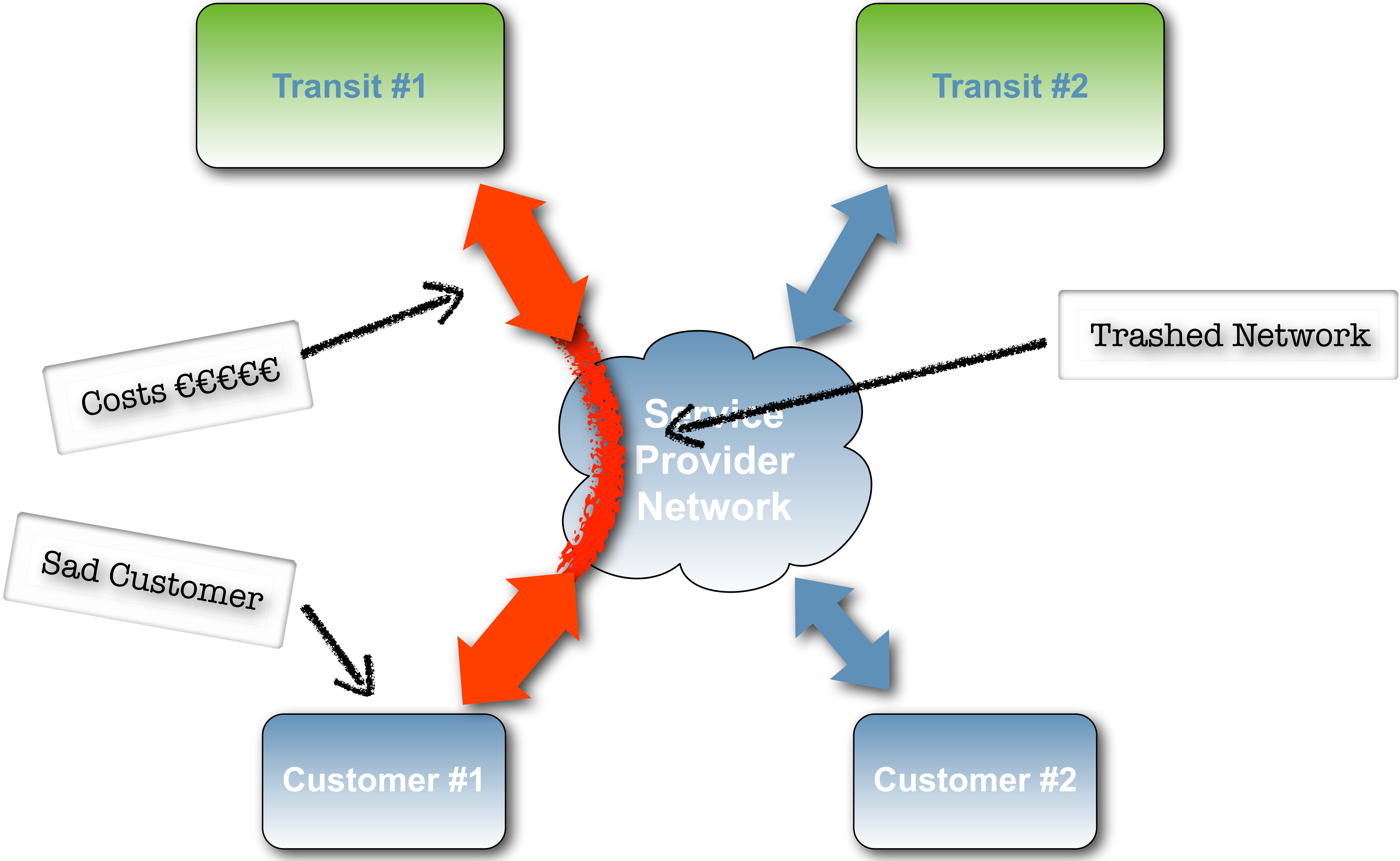
typical isp topology



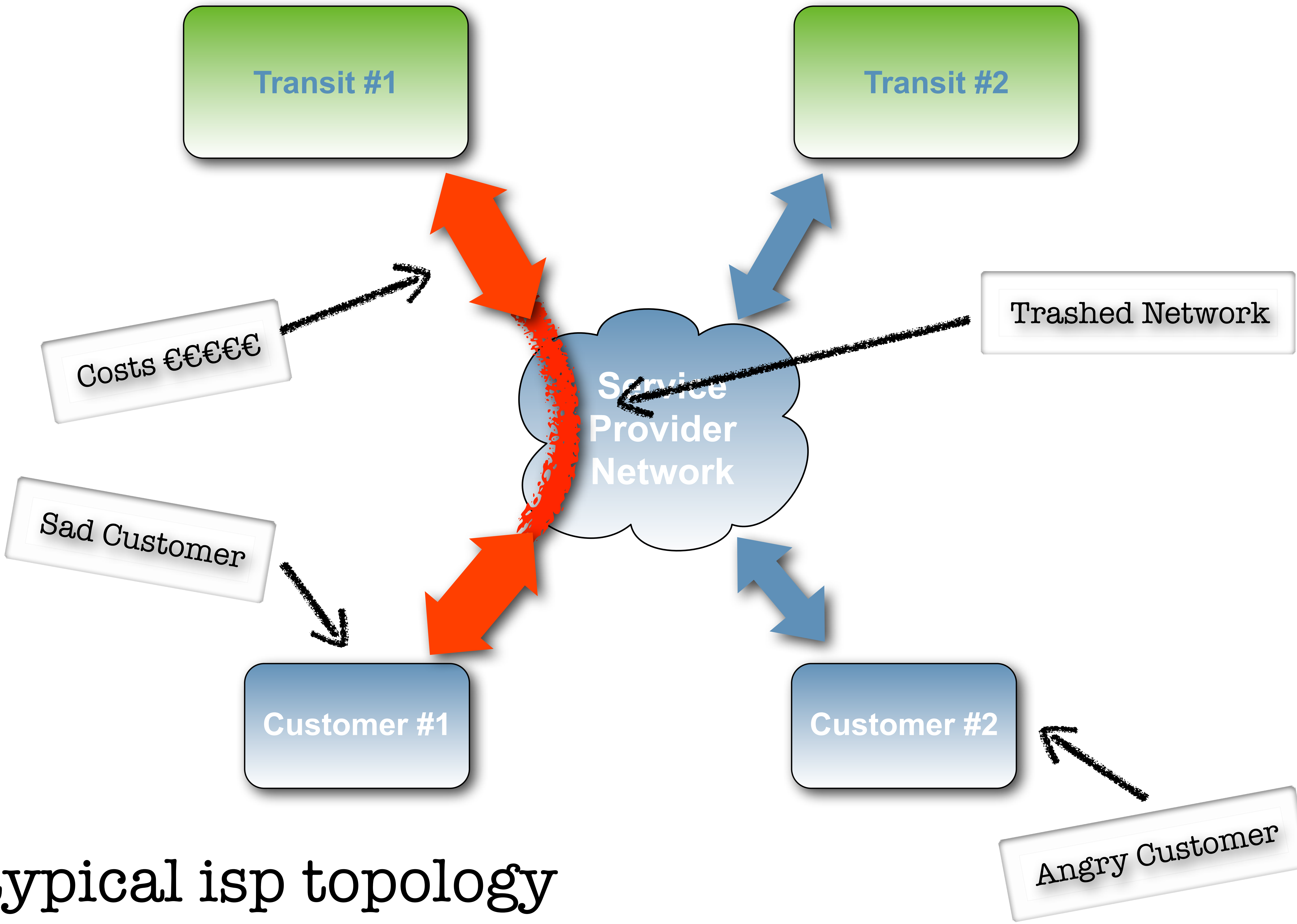
typical isp topology



typical isp topology



typical isp topology



Transit #1

Transit #2

Costs €€€€€

Trashed Network

Service Provider Network

Sad Customer

Customer #1

Customer #2

Angry Customer

typical isp topology

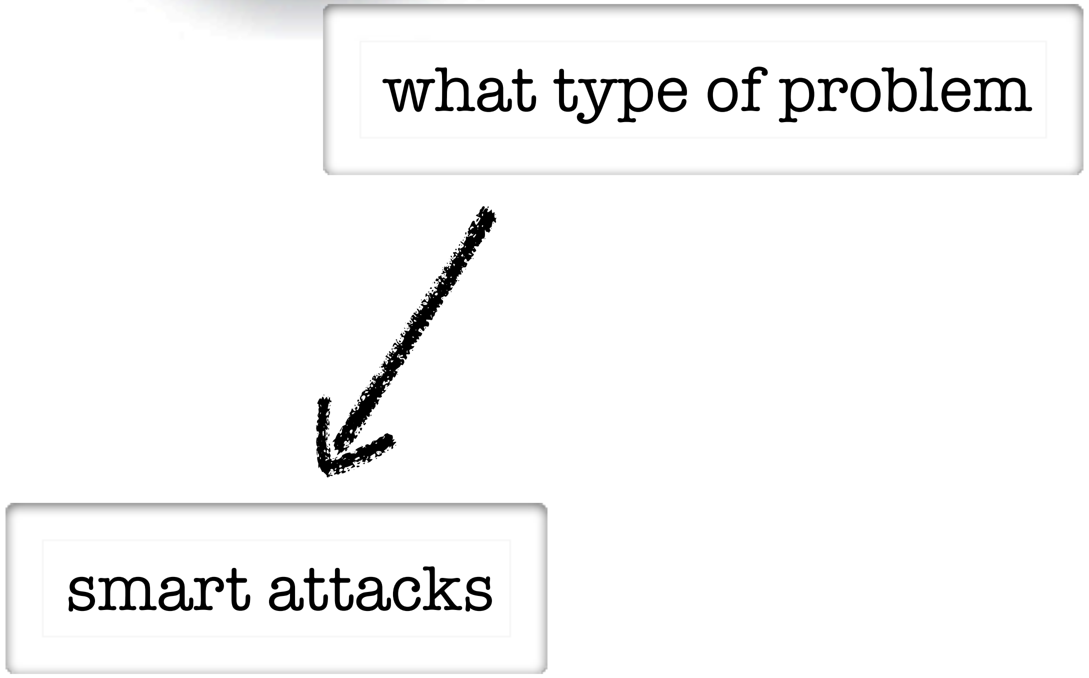
http://flickr.com/photos/crimfants/327861820/

RTBH Tutorial - Defining the Problem

RTBH Tutorial - Defining the Problem

what type of problem

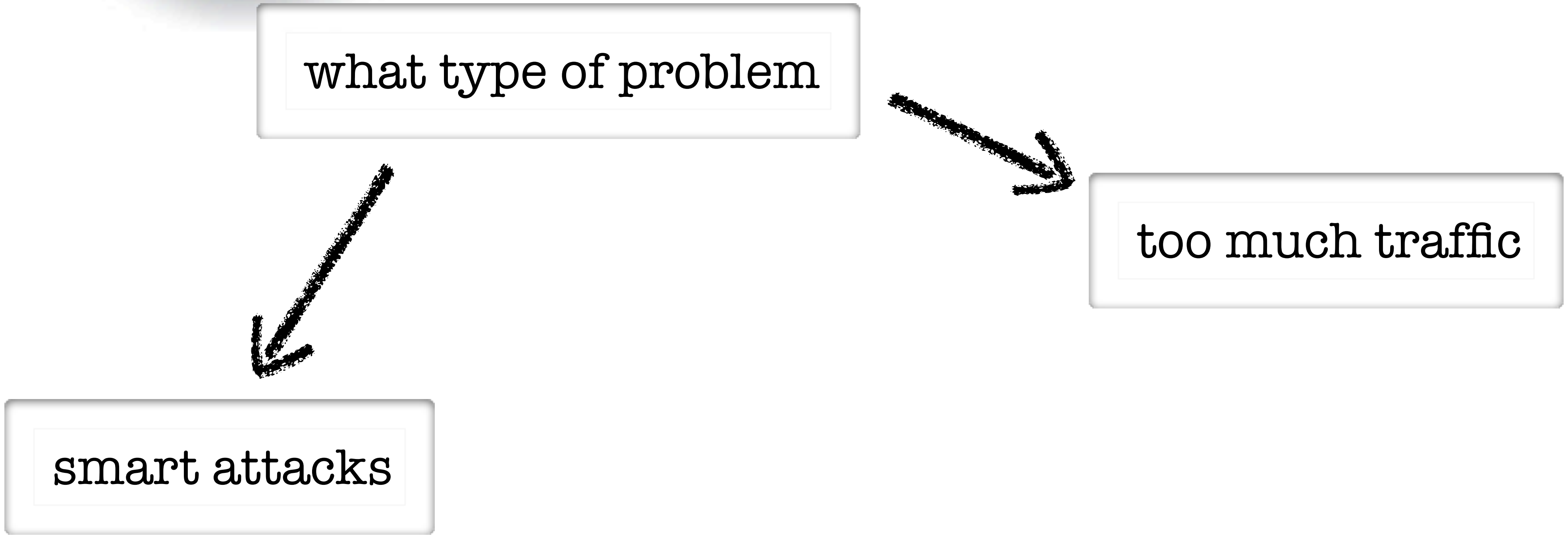
RTBH Tutorial - Defining the Problem



what type of problem

smart attacks

RTBH Tutorial - Defining the Problem

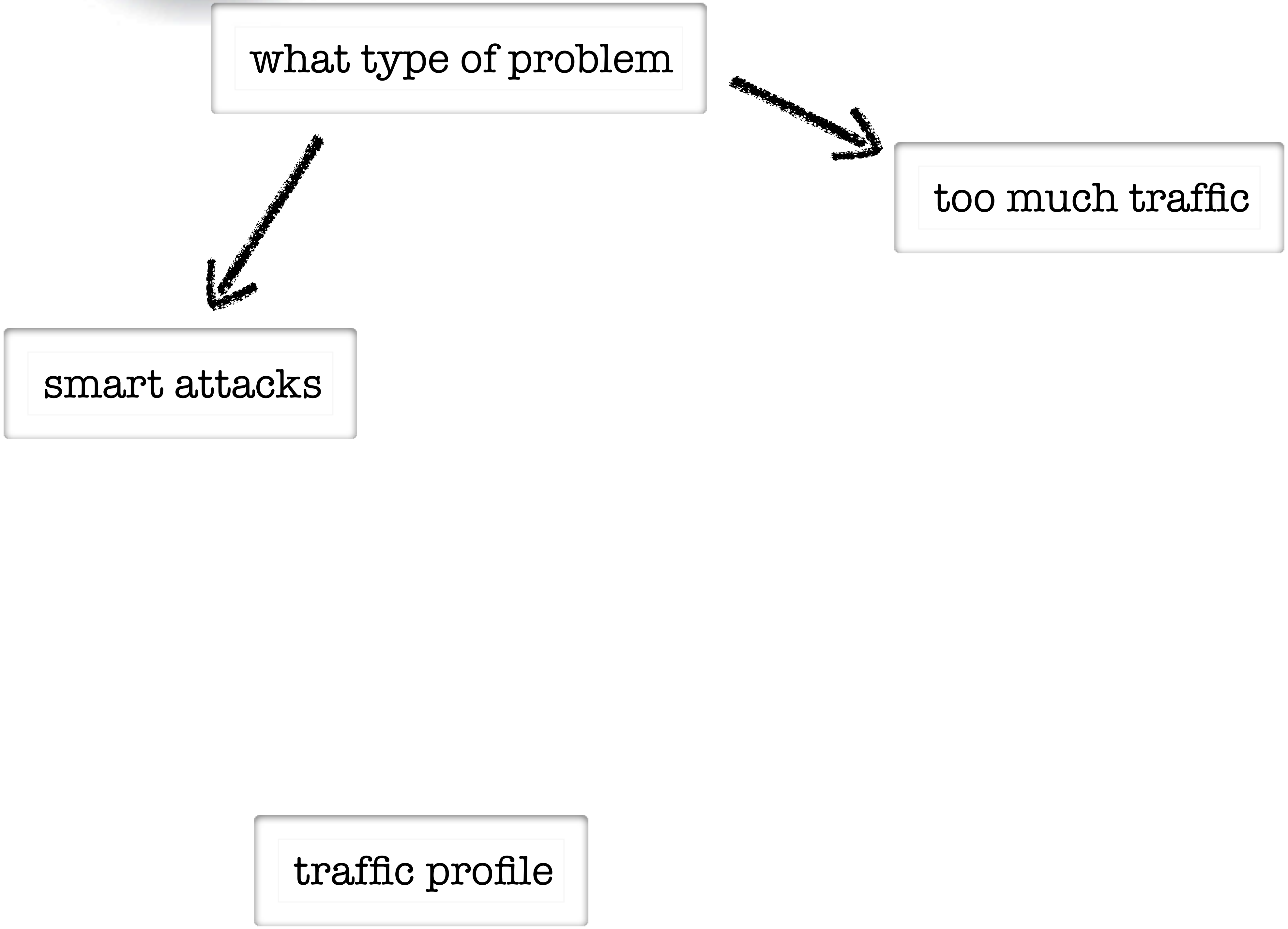


what type of problem

too much traffic

smart attacks

RTBH Tutorial - Defining the Problem



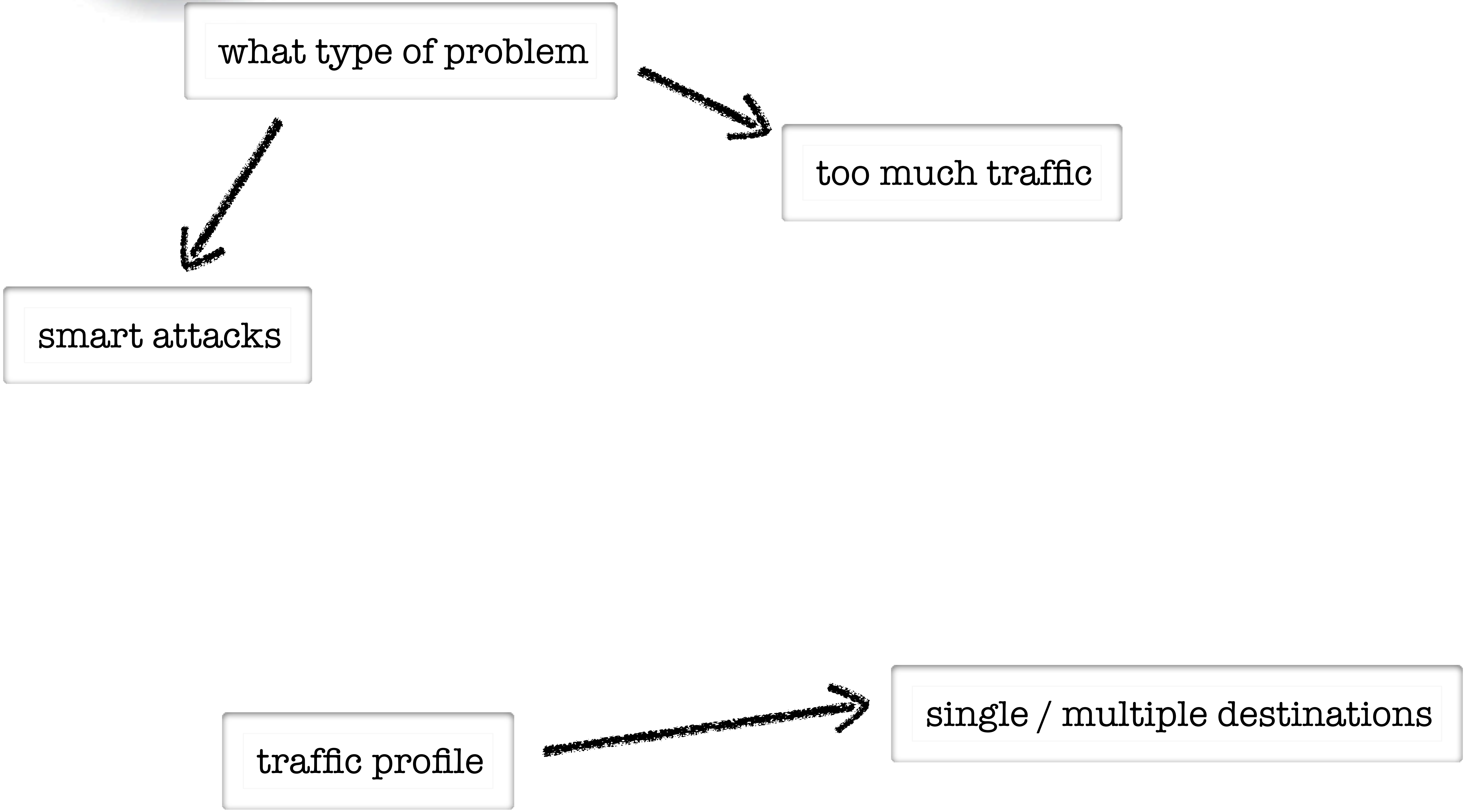
what type of problem

too much traffic

smart attacks

traffic profile

RTBH Tutorial - Defining the Problem



what type of problem

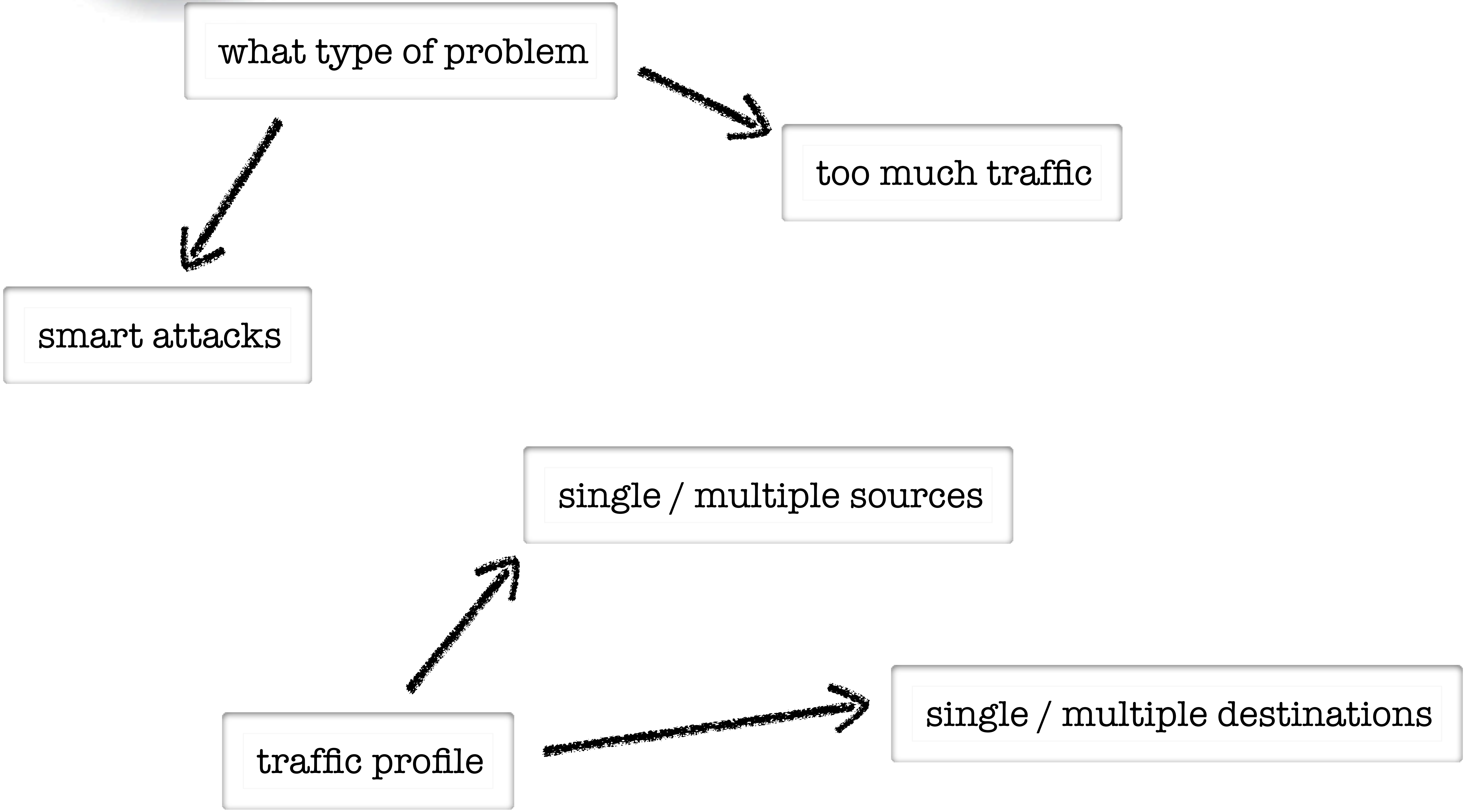
too much traffic

smart attacks

traffic profile

single / multiple destinations

RTBH Tutorial - Defining the Problem



what type of problem

too much traffic

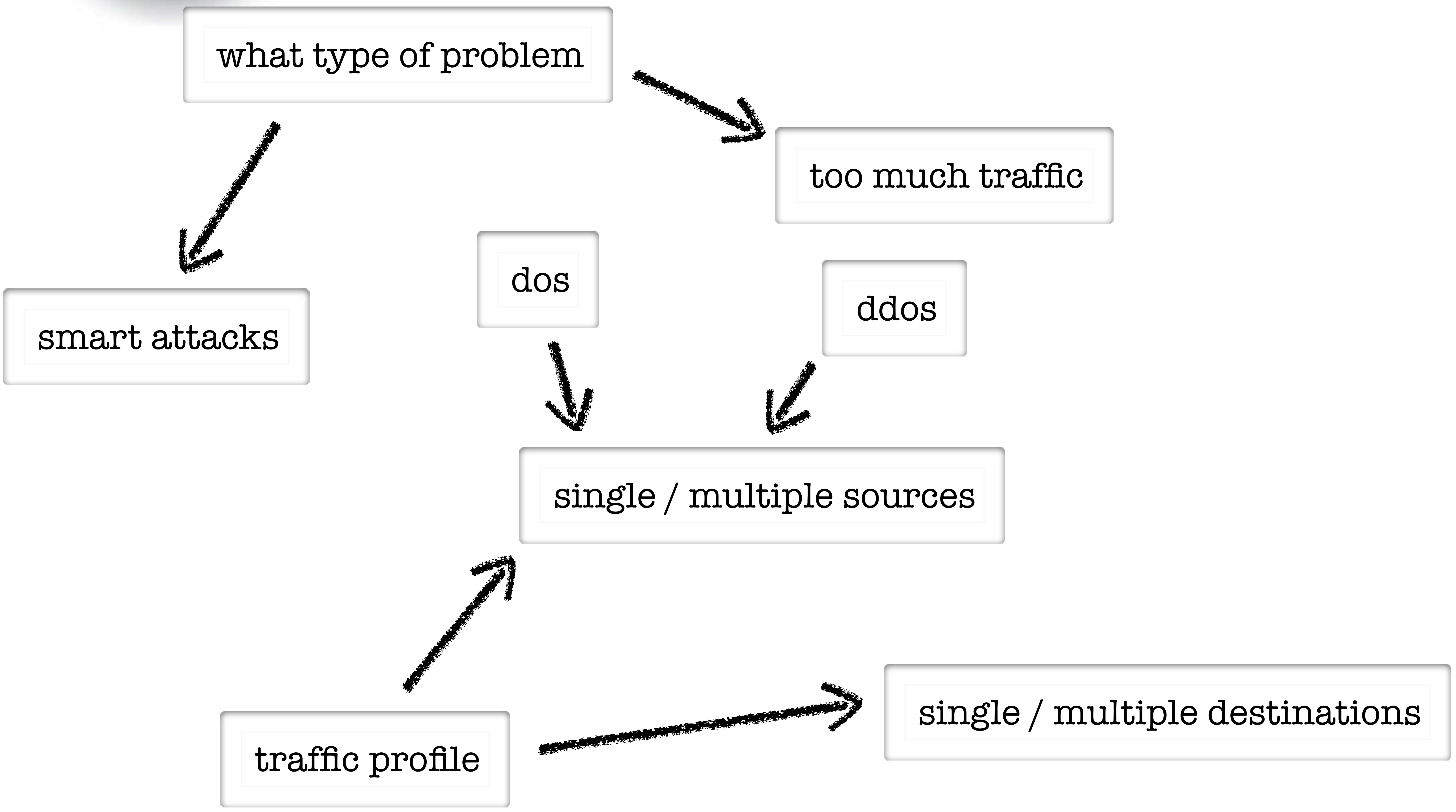
smart attacks

single / multiple sources

traffic profile

single / multiple destinations

RTBH Tutorial - Defining the Problem



what type of problem

too much traffic

smart attacks

dos

ddos

single / multiple sources

traffic profile

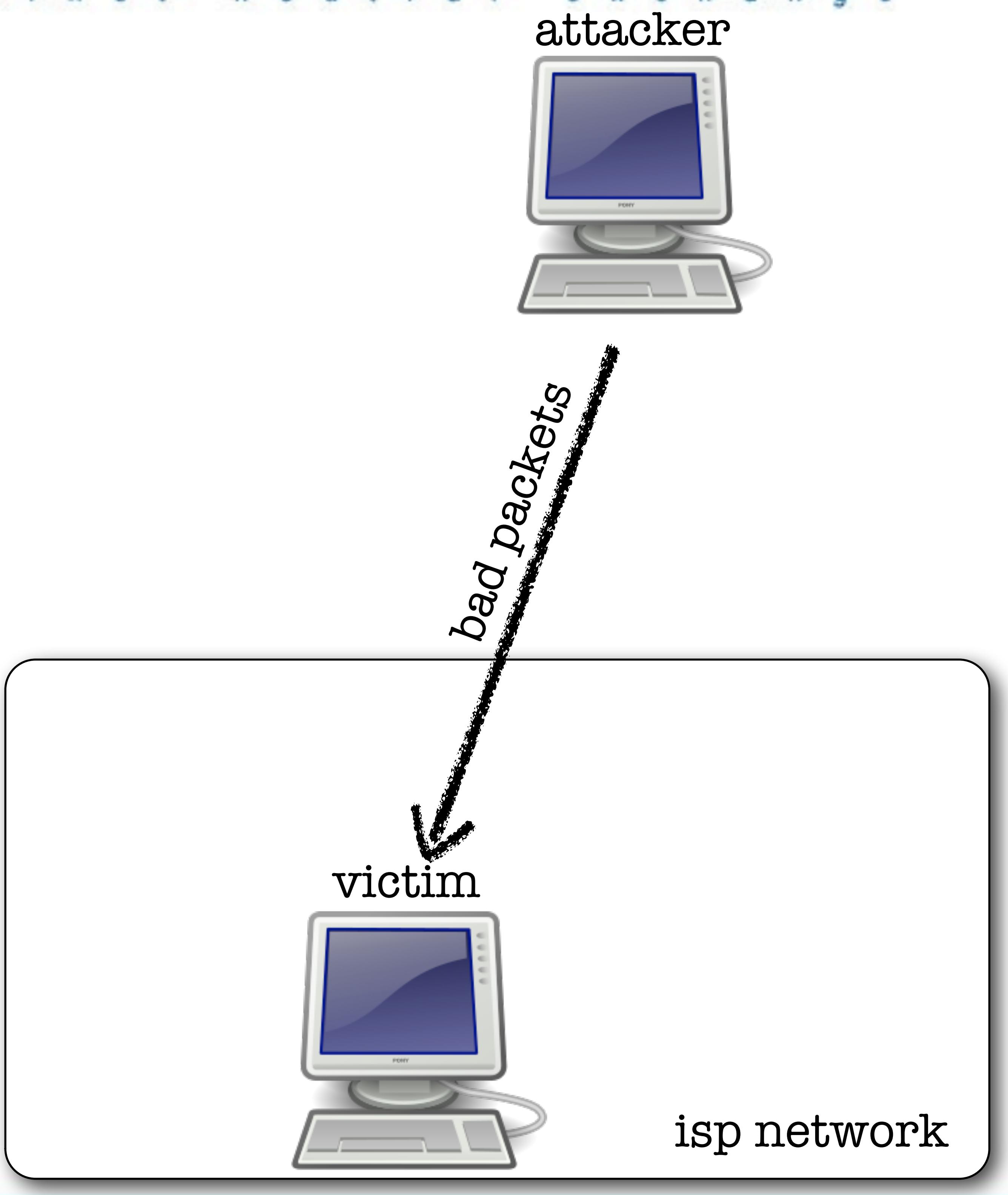
single / multiple destinations

subtle resolution tool

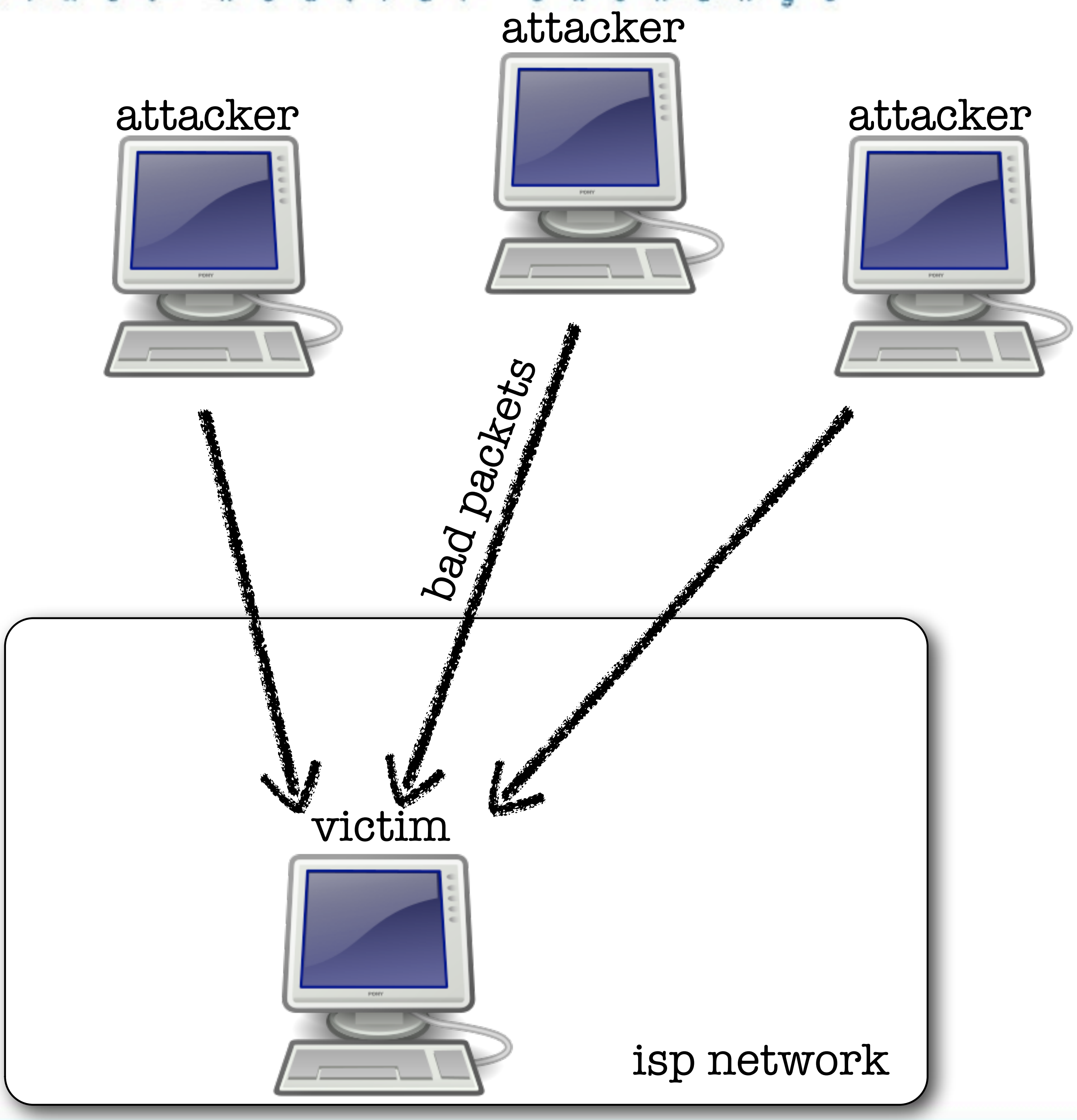
subtle resolution tool

http://www.flickr.com/photos/mrsmagic/6982947352/

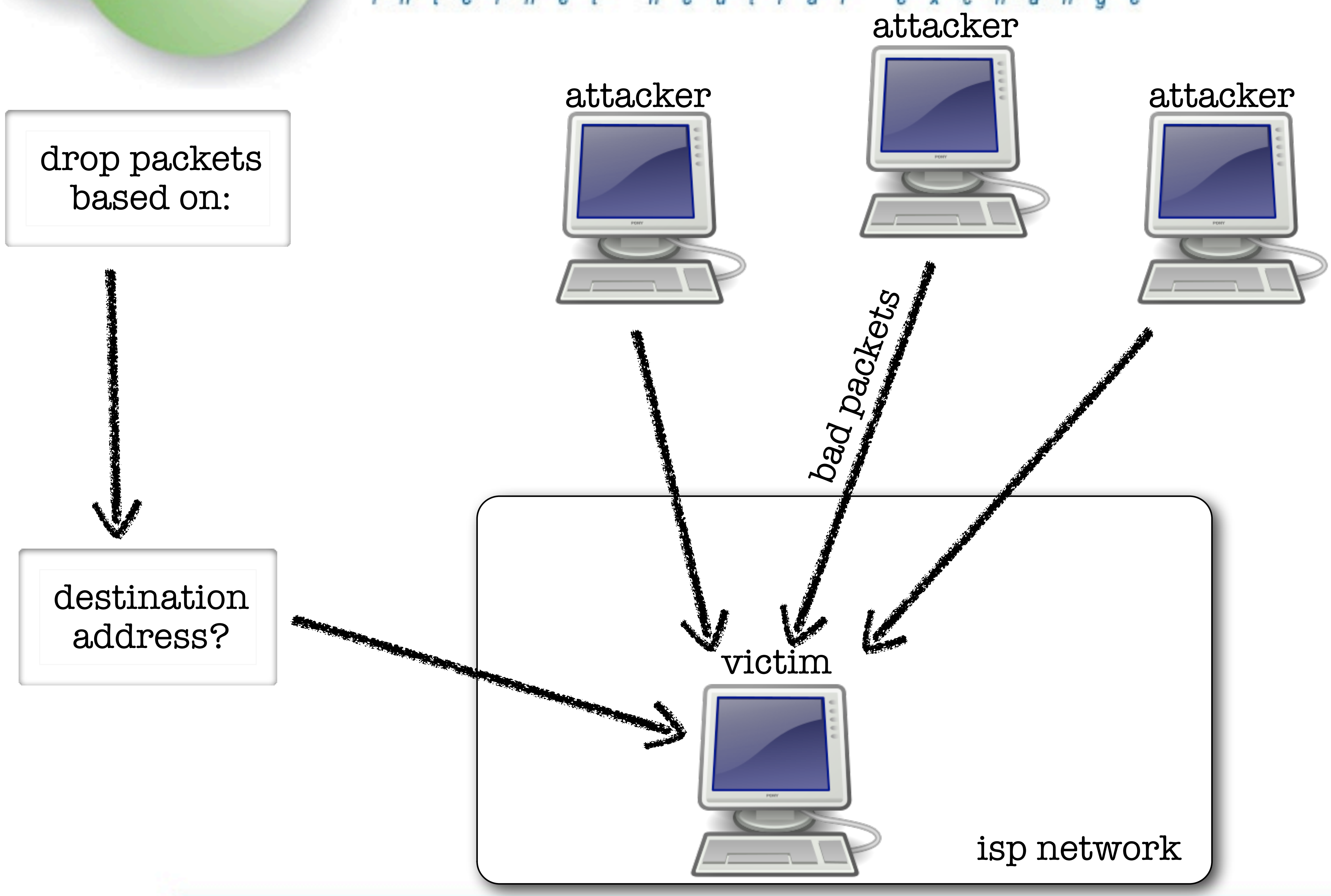
RTBH Tutorial - Dropping Packets in a Hurry



RTBH Tutorial - Dropping Packets in a Hurry

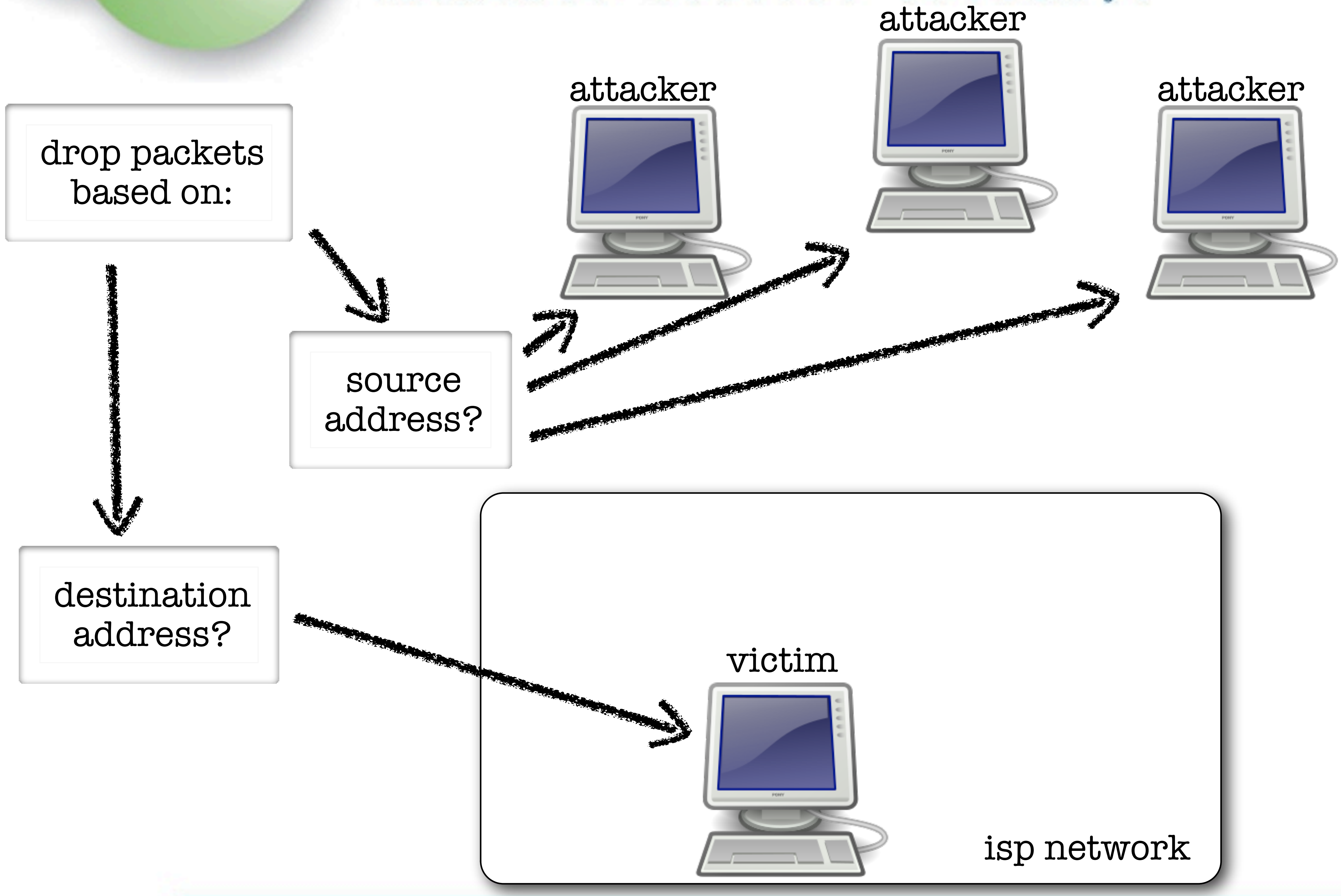


RTBH Tutorial - Dropping Packets in a Hurry


drop packets based on:

destination address?

RTBH Tutorial - Dropping Packets in a Hurry



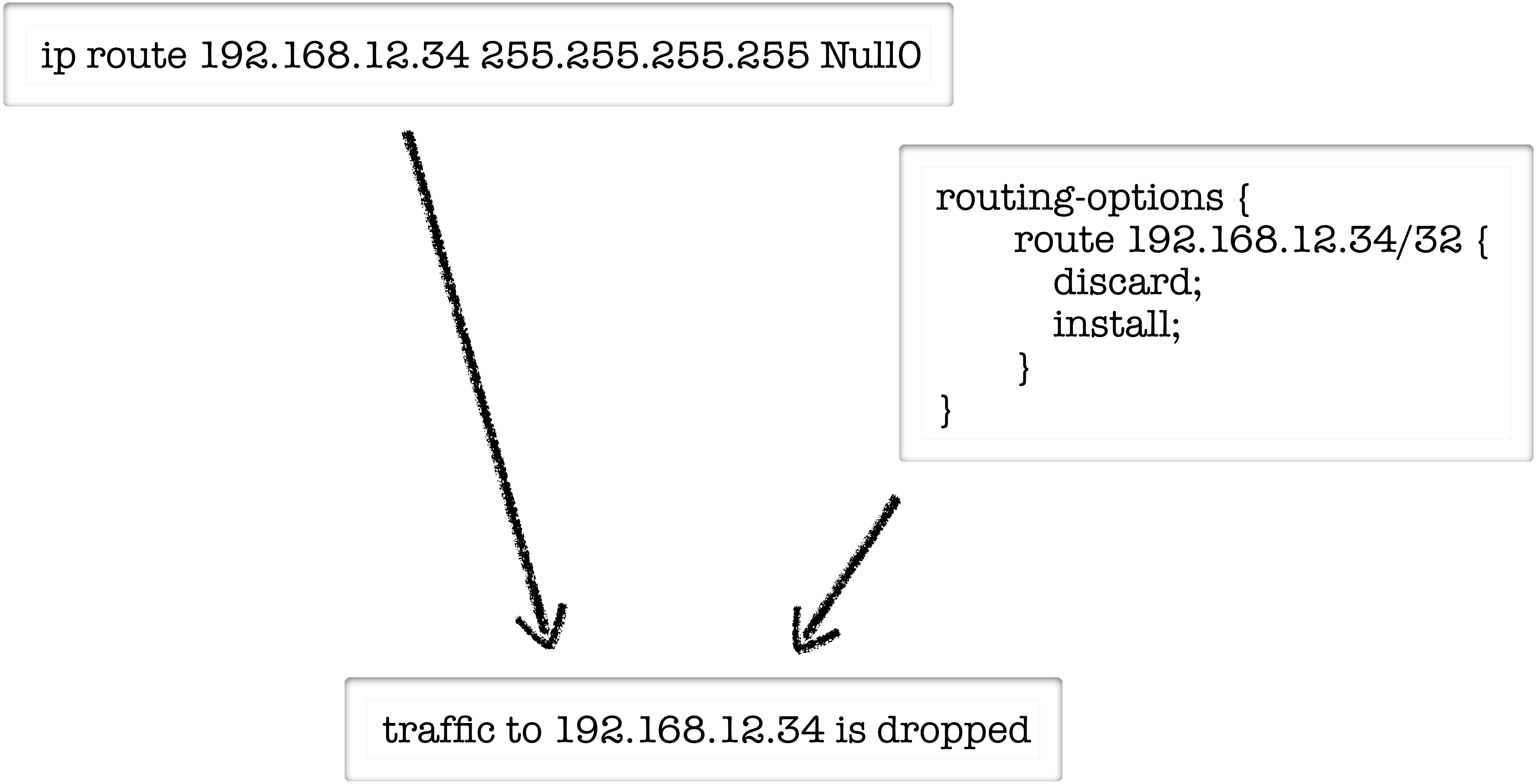
drop packets based on:

source address?

destination address?

RTBH Tutorial - Naive Destination Drops

RTBH Tutorial - Naive Destination Drops

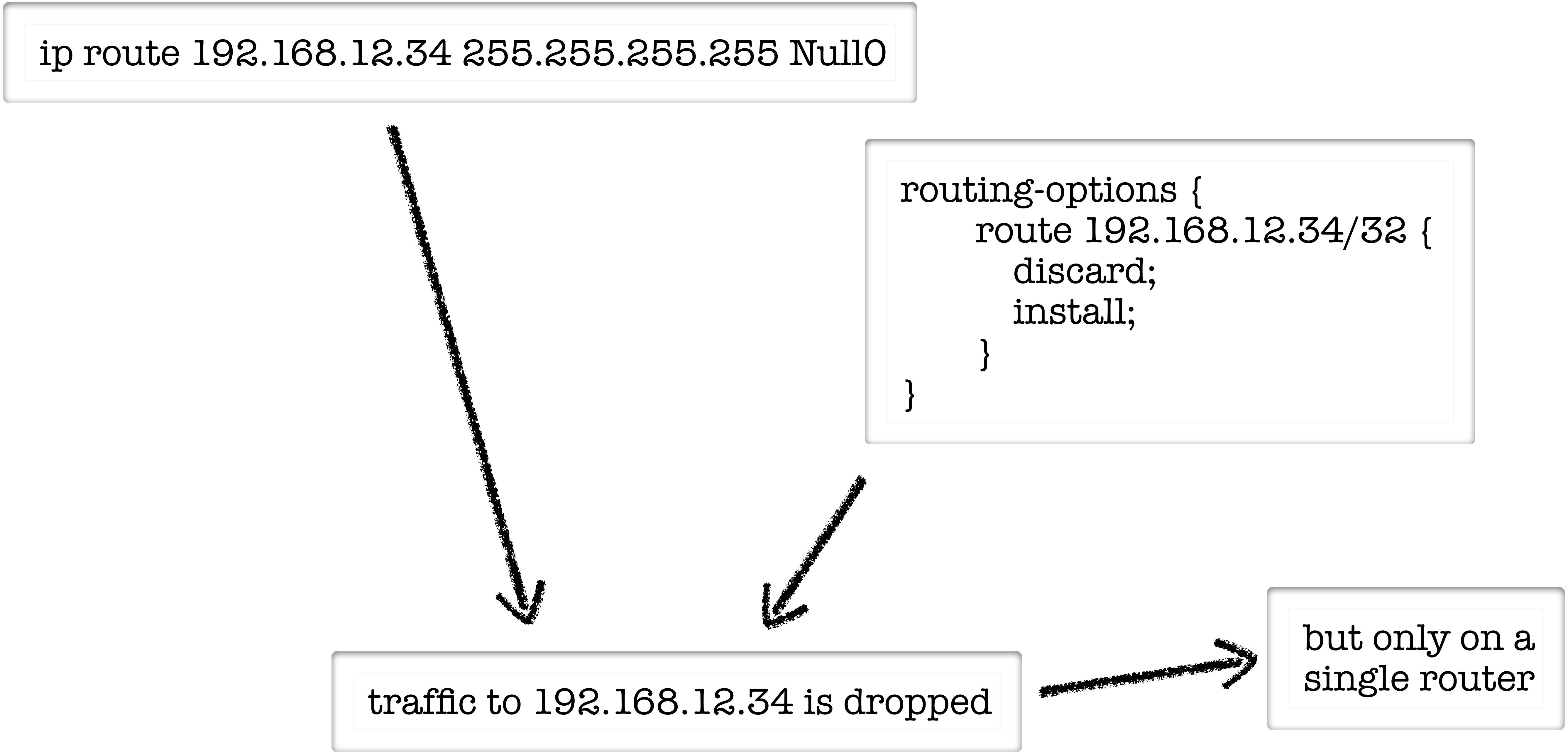


```
ip route 192.168.12.34 255.255.255.255 Null0
```

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

traffic to 192.168.12.34 is dropped

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

RTBH Tutorial - Naive Destination Drop Problems

need mechanism to propagate a null route throughout an entire network

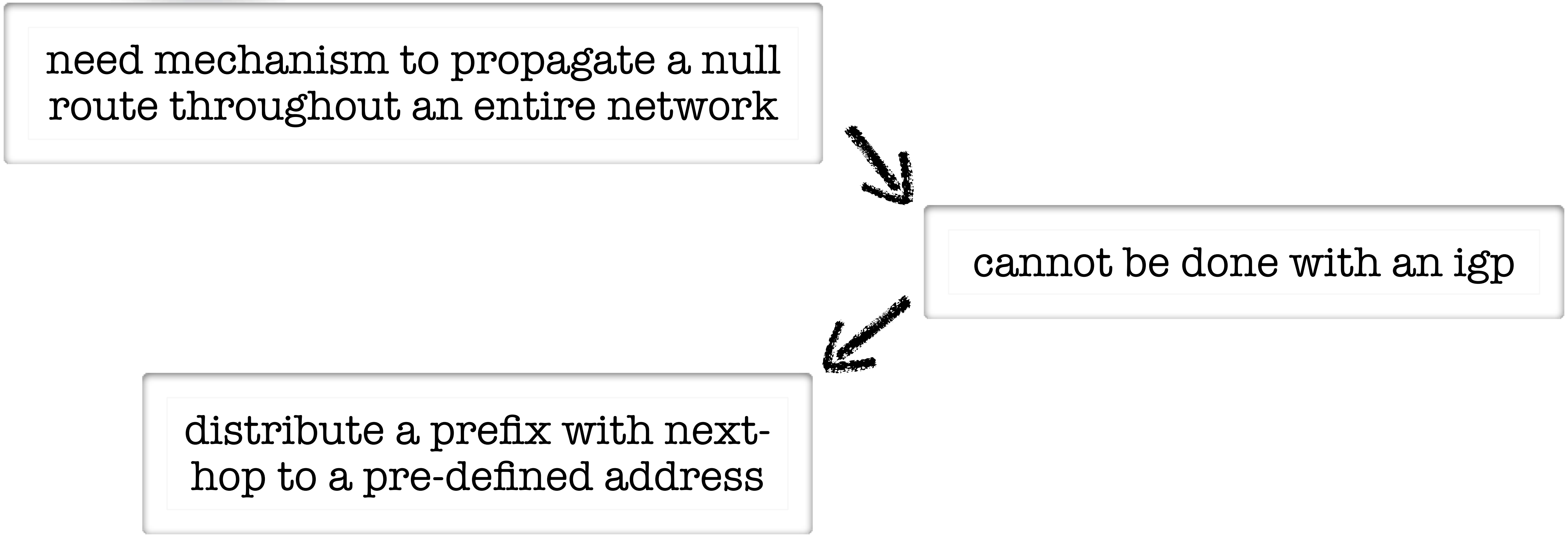
RTBH Tutorial - Naive Destination Drop Problems

need mechanism to propagate a null route throughout an entire network

↘

cannot be done with an igp

RTBH Tutorial - Naive Destination Drop Problems

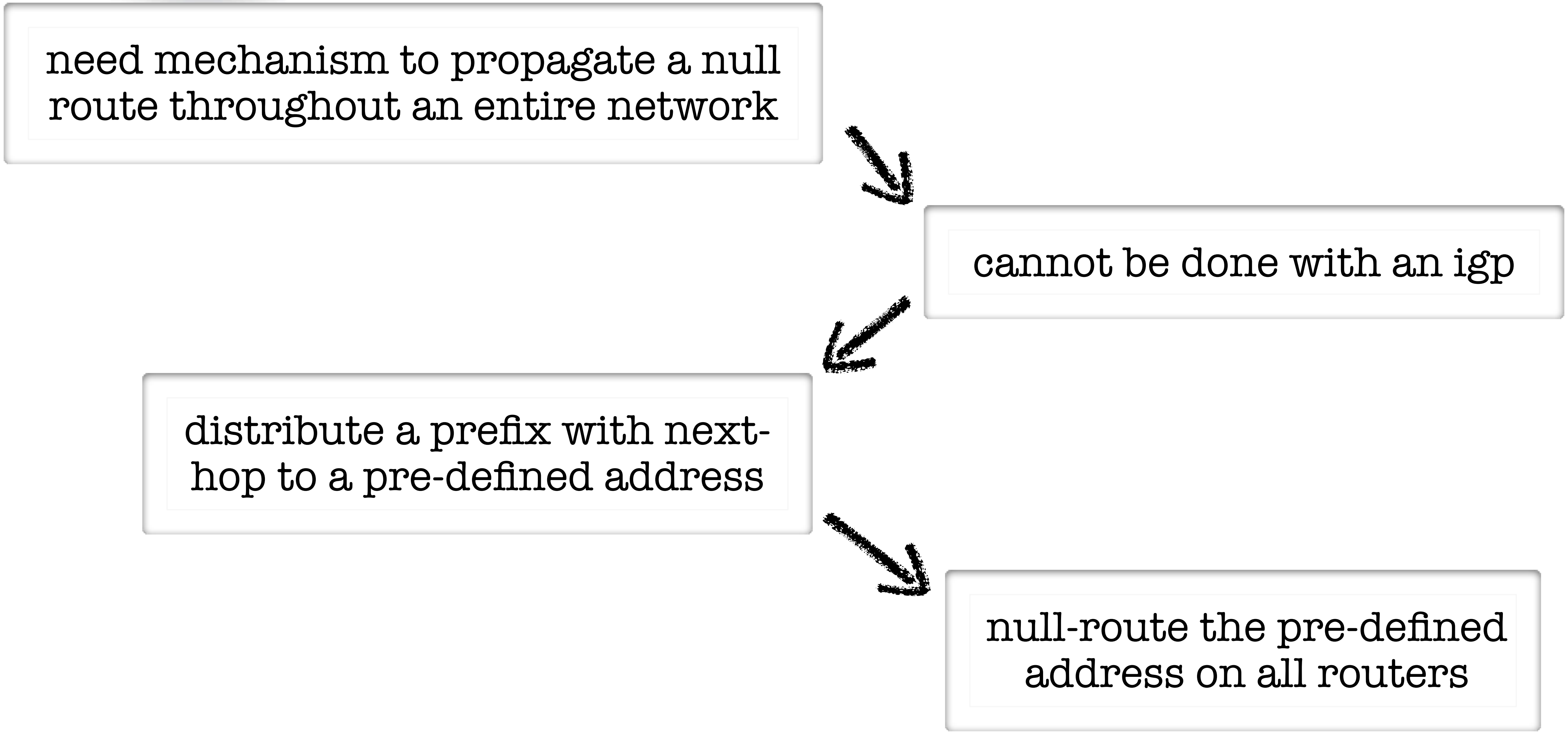


need mechanism to propagate a null route throughout an entire network

cannot be done with an igp

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

RTBH Tutorial - Naive Destination Drop Problems



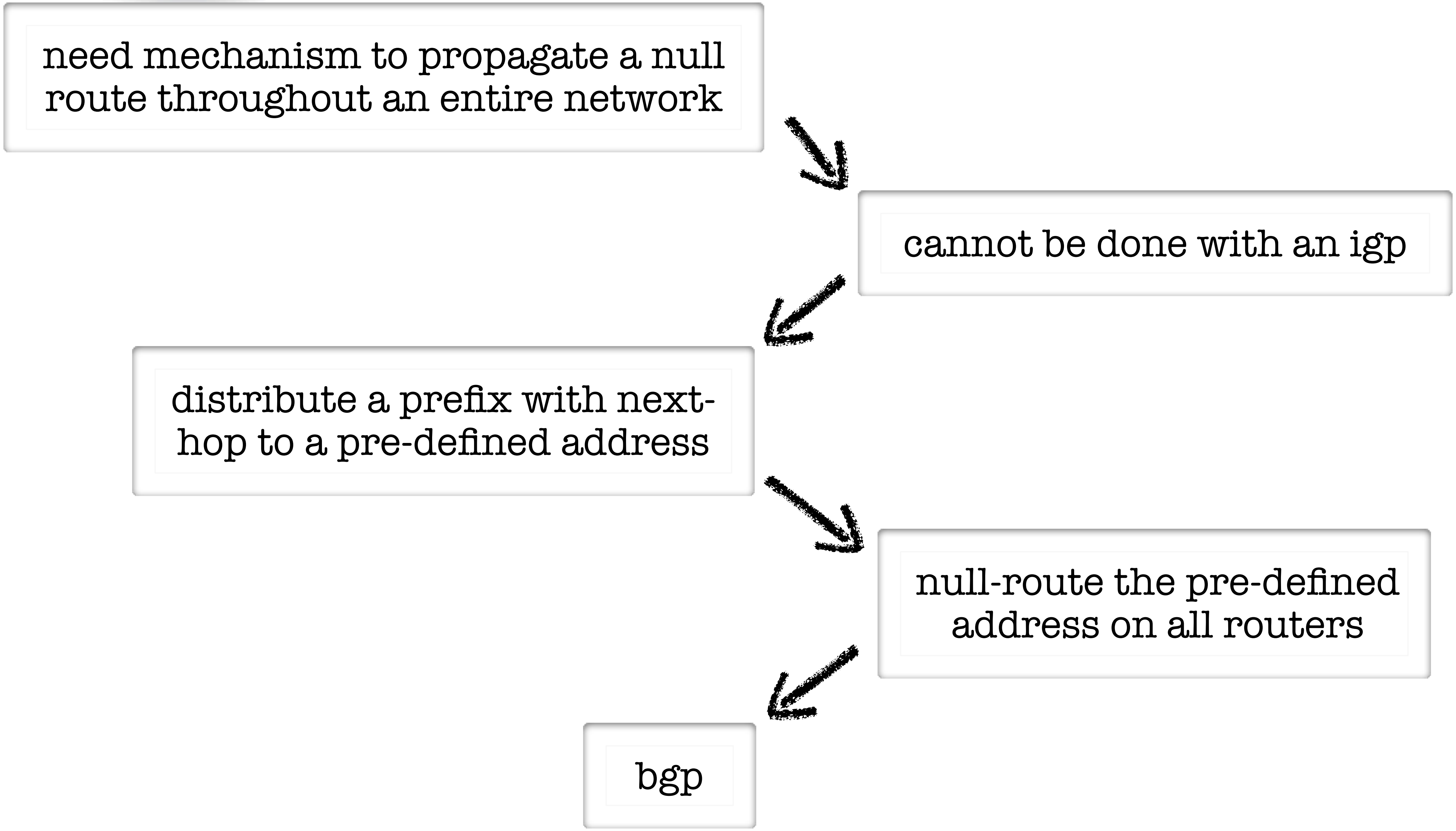
need mechanism to propagate a null route throughout an entire network

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

RTBH Tutorial - Naive Destination Drop Problems



need mechanism to propagate a null route throughout an entire network

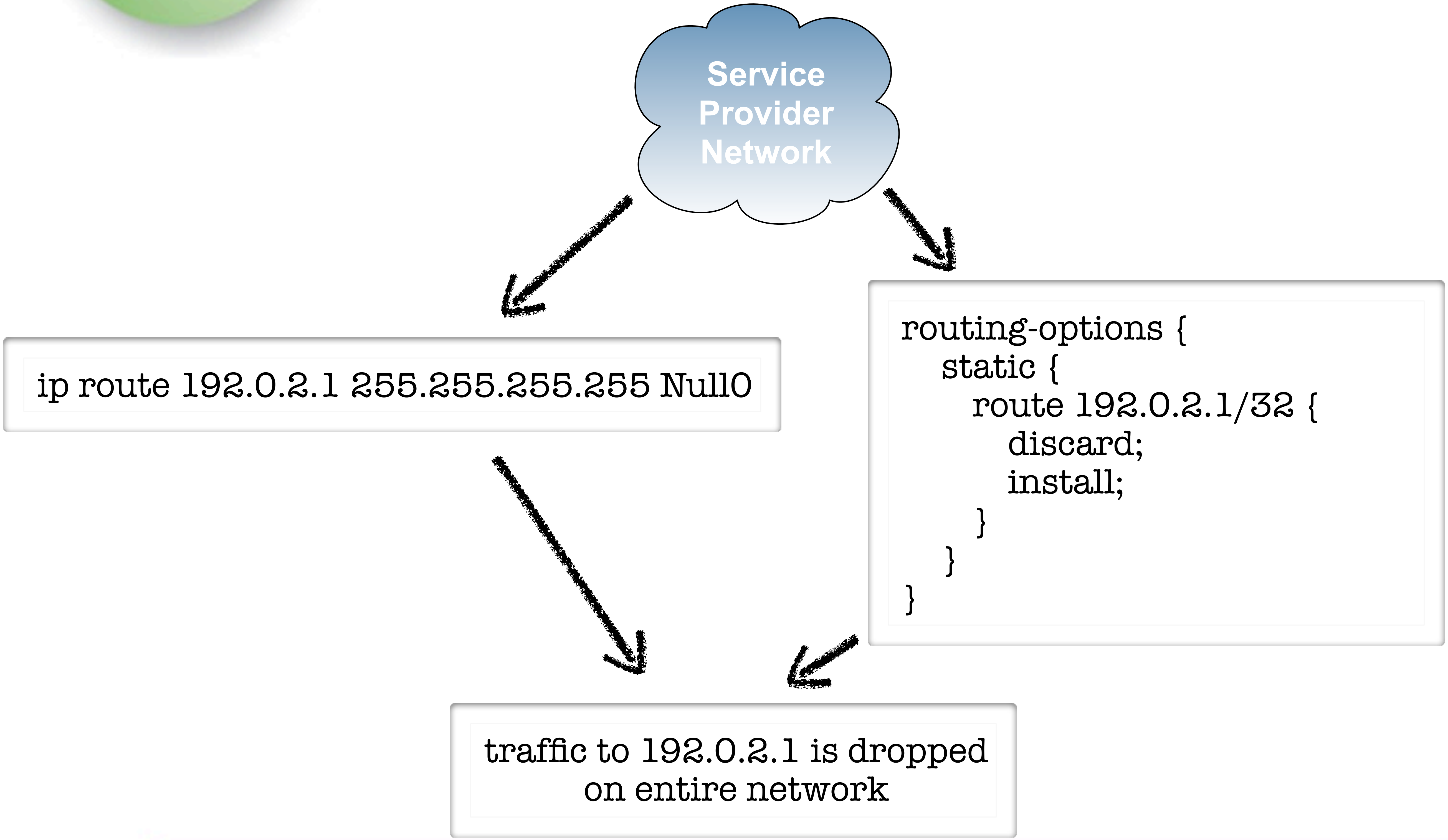
cannot be done with an igp

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;
     }
   }
}
```

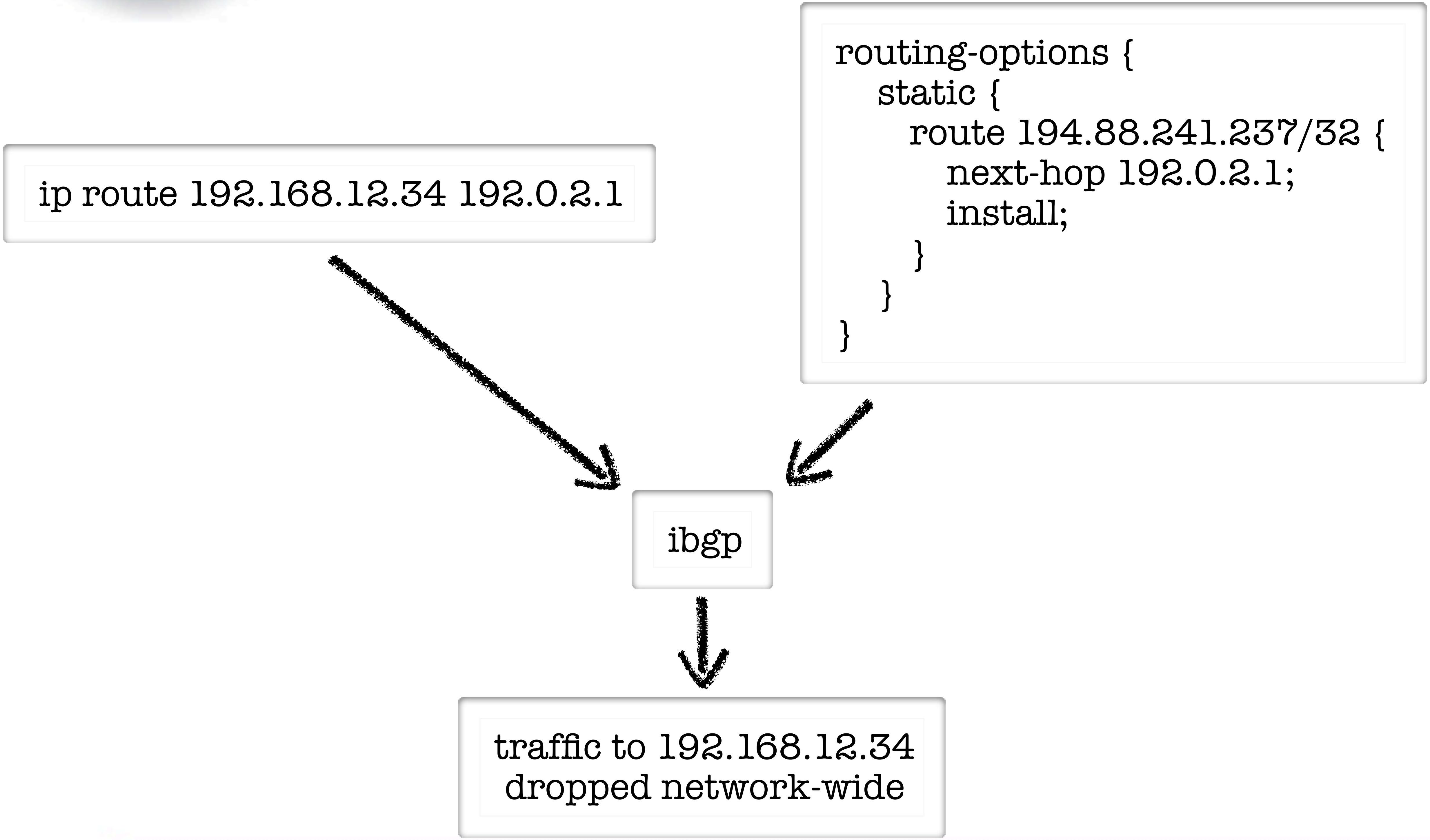
traffic to 192.0.2.1 is dropped
on entire network

RTBH Tutorial - Distribution via iBGP

```
ip route 192.168.12.34 192.0.2.1
```

```
routing-options {
   static {
      route 194.88.241.237/32 {
         next-hop 192.0.2.1;
         install;
      }
   }
}
```

RTBH Tutorial - Distribution via iBGP



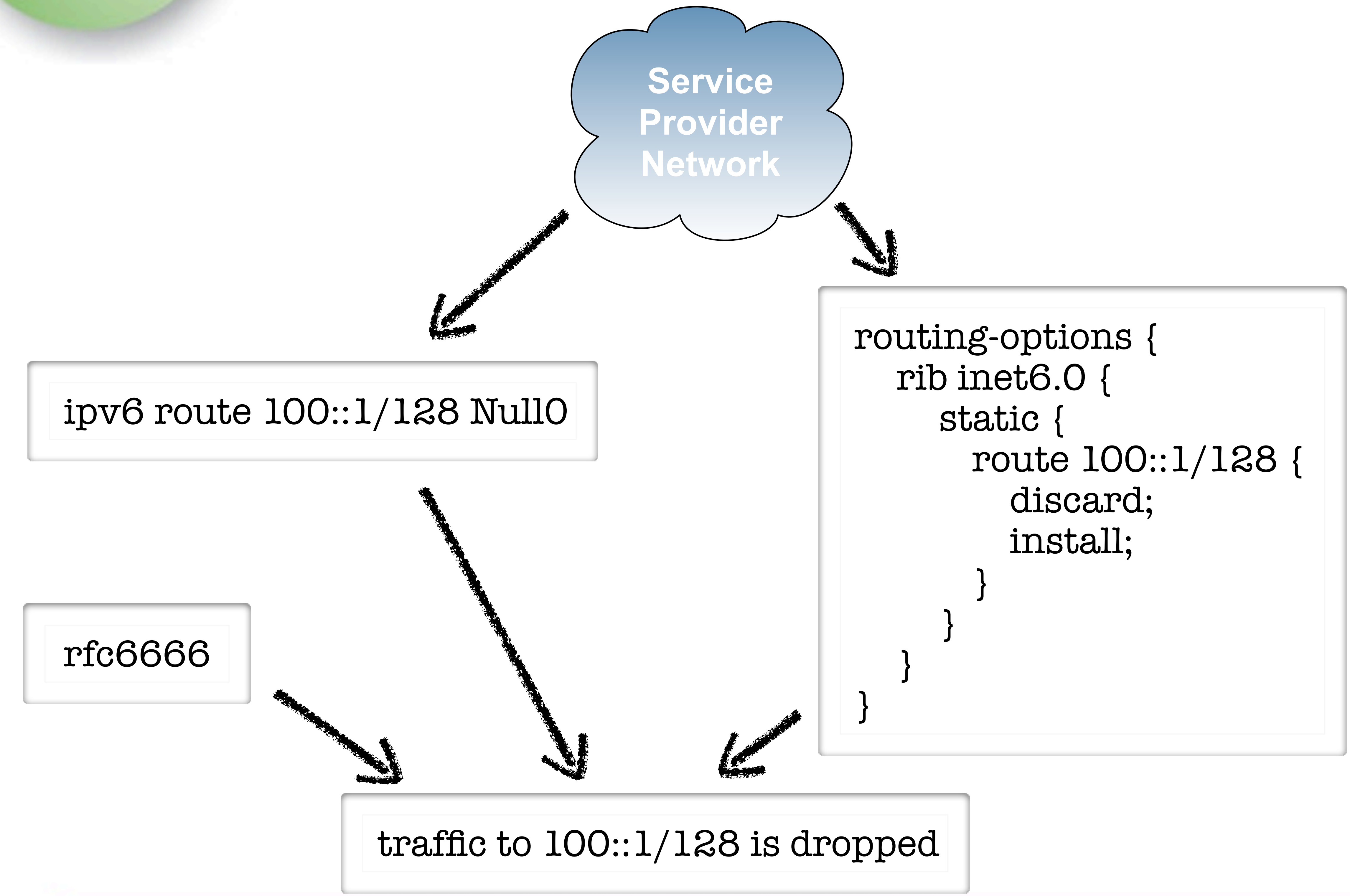
```
ip route 192.168.12.34 192.0.2.1
```

```
routing-options {
   static {
      route 194.88.241.237/32 {
         next-hop 192.0.2.1;
         install;
      }
   }
}
```

ibgp

traffic to 192.168.12.34
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;
            }
        }
    }
}
```

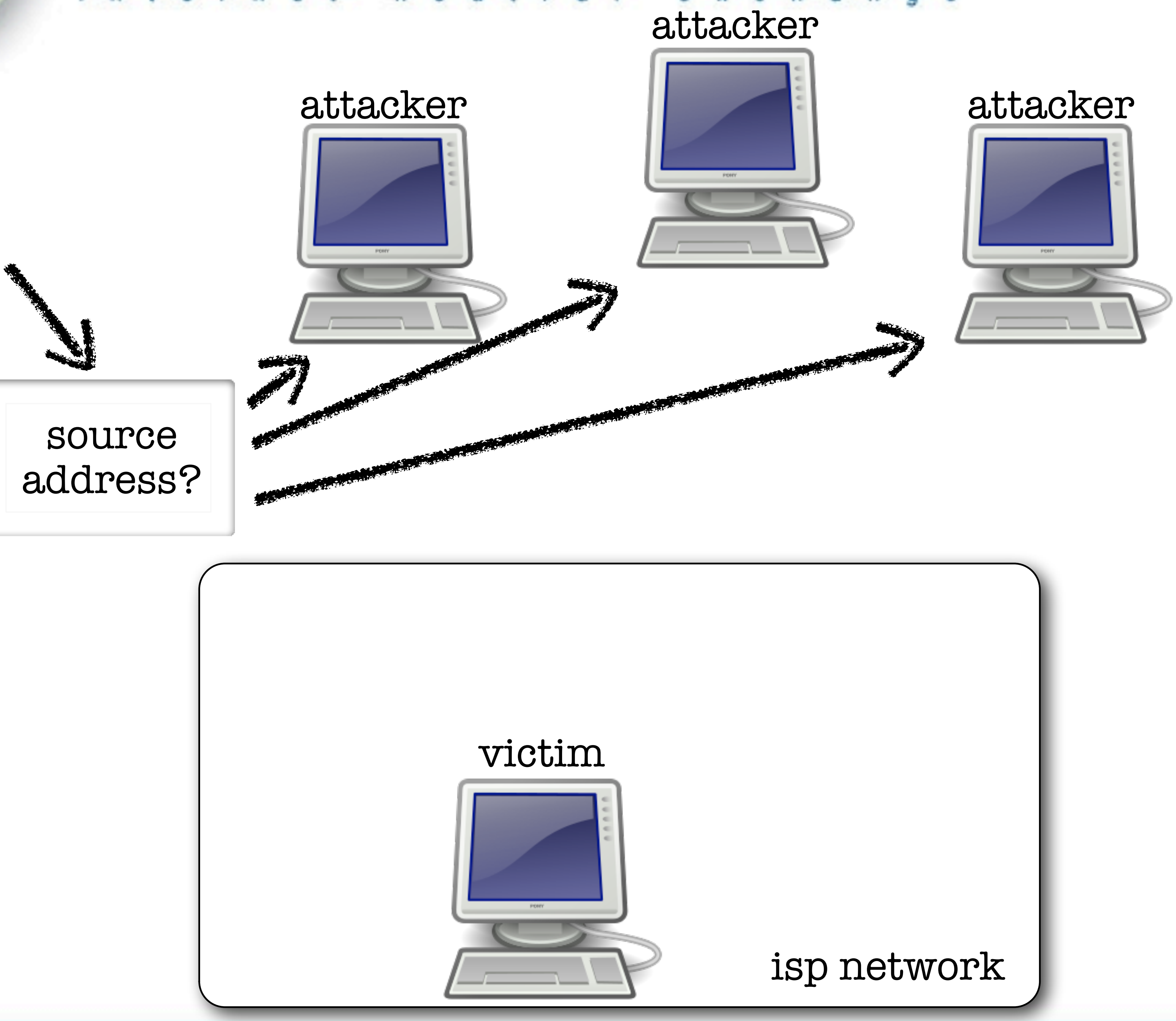
rfc6666

traffic to 100::1/128 is dropped

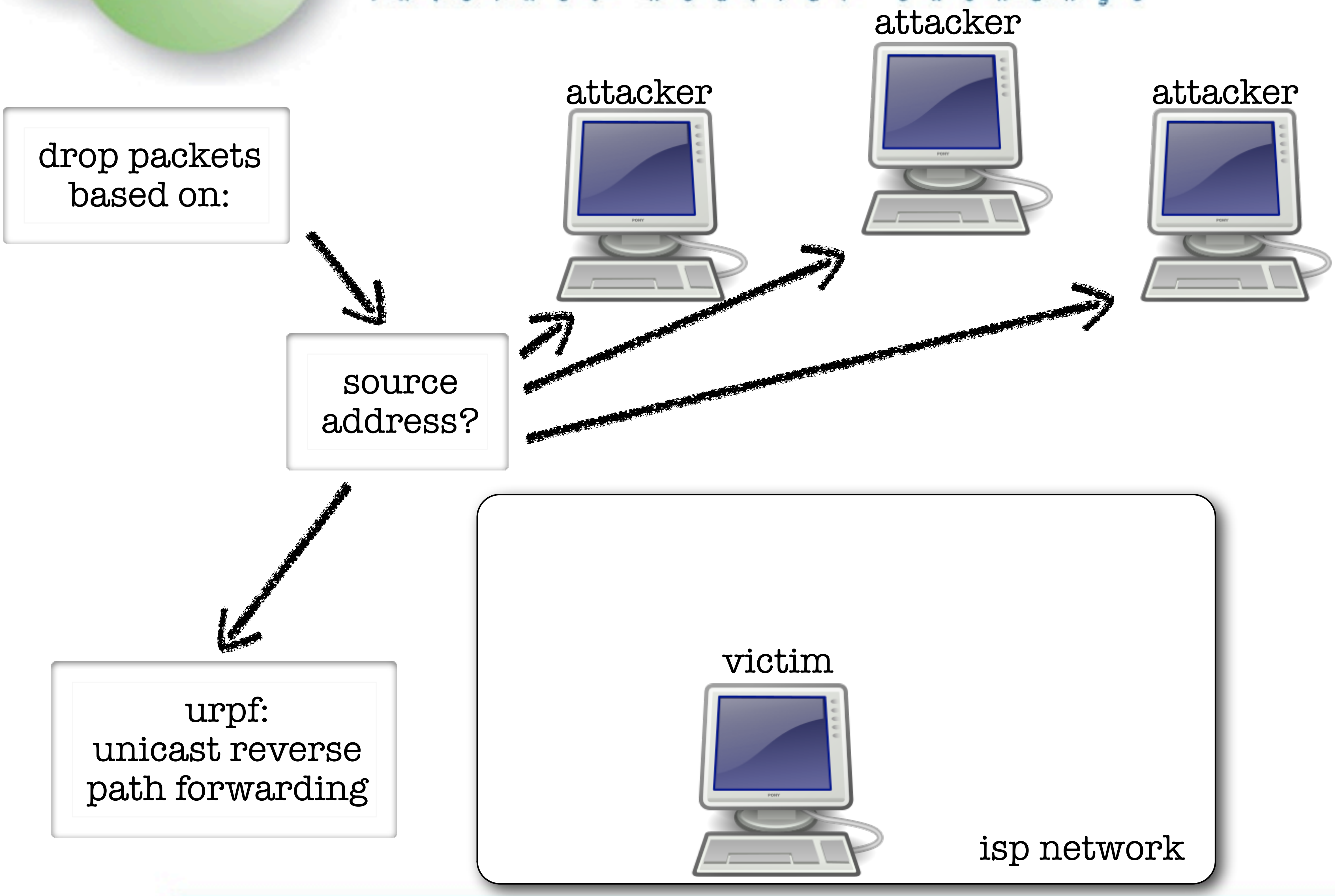
RTBH Tutorial - Source Filtering

drop packets based on:

source address?



RTBH Tutorial - Source Filtering

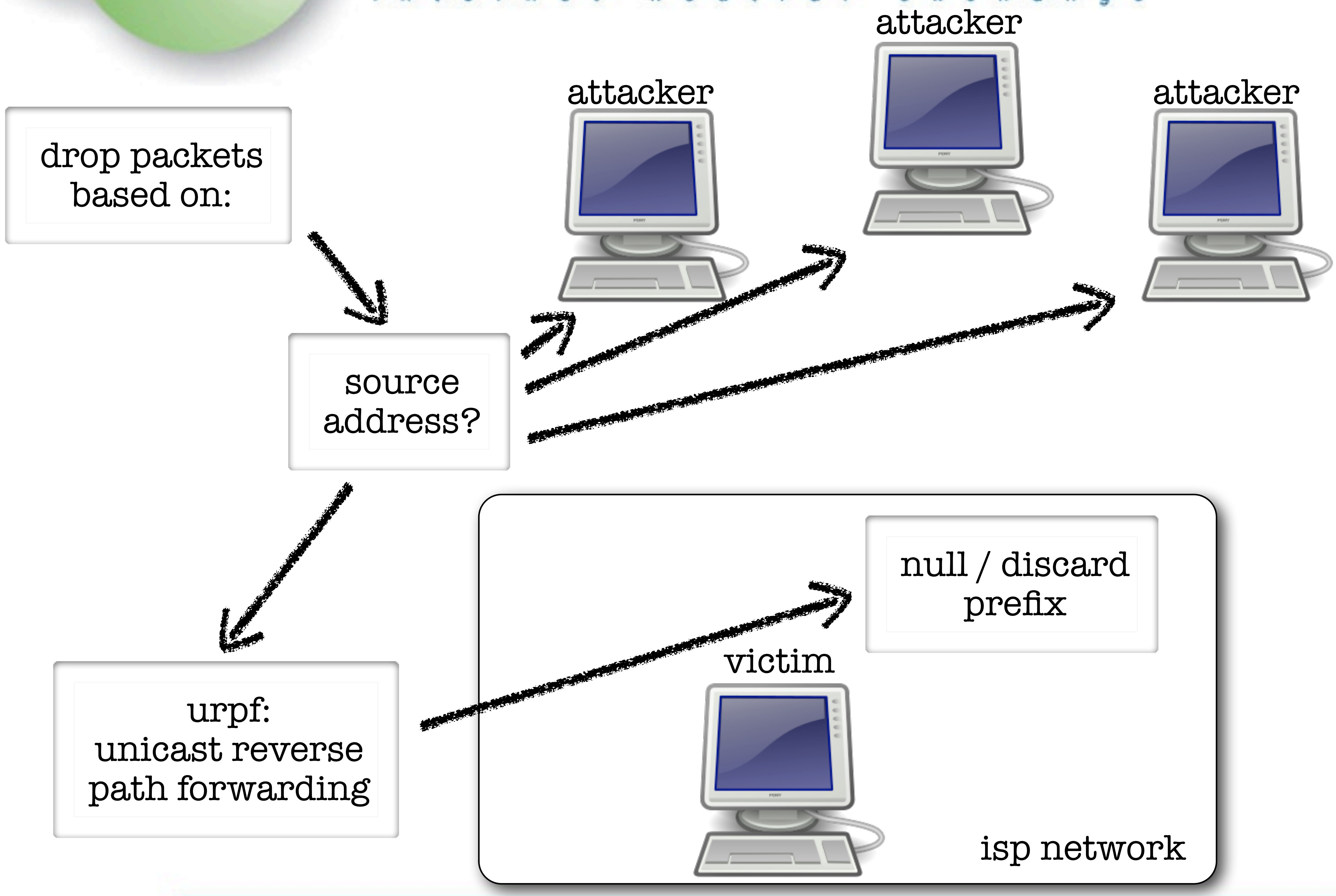


drop packets based on:

source address?

urpf:
unicast reverse path forwarding

RTBH Tutorial - Source Filtering



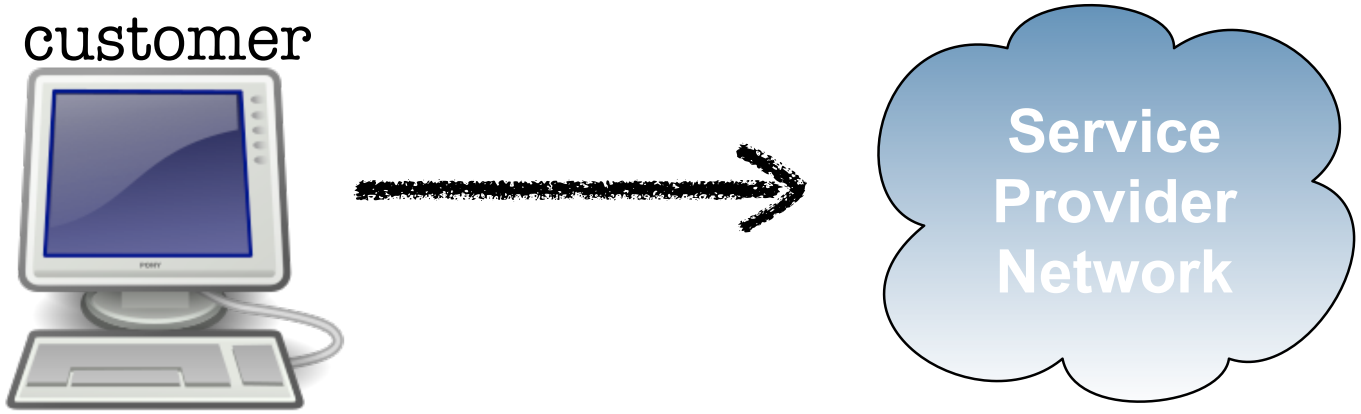
drop packets based on:

source address?

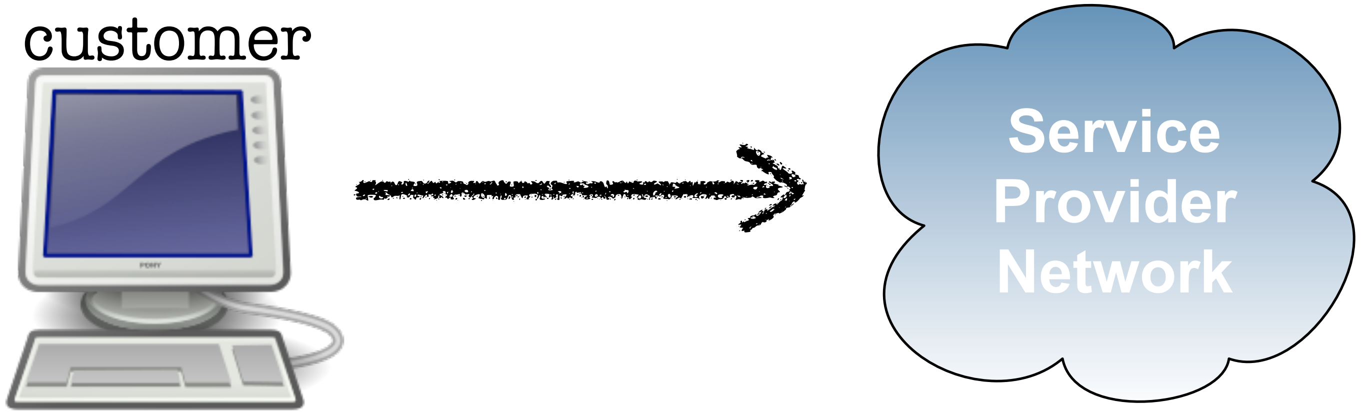
urpf: unicast reverse path forwarding

null / discard prefix

RTBH Tutorial - Refresher on uRPF



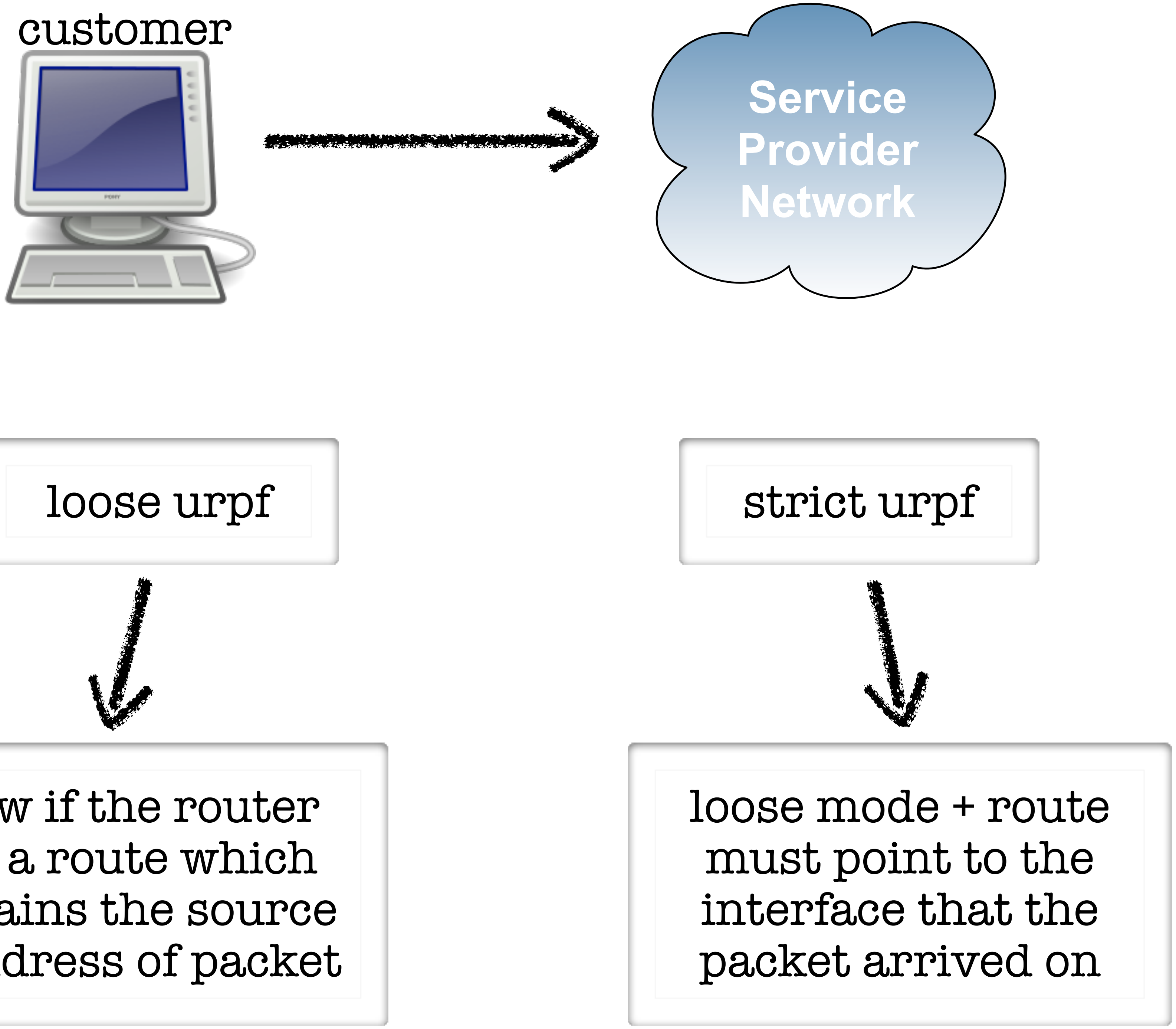
RTBH Tutorial - Refresher on uRPF



loose urpf

allow if the router has a route which contains the source ip address of packet

RTBH Tutorial - Refresher on uRPF



customer

Service Provider Network

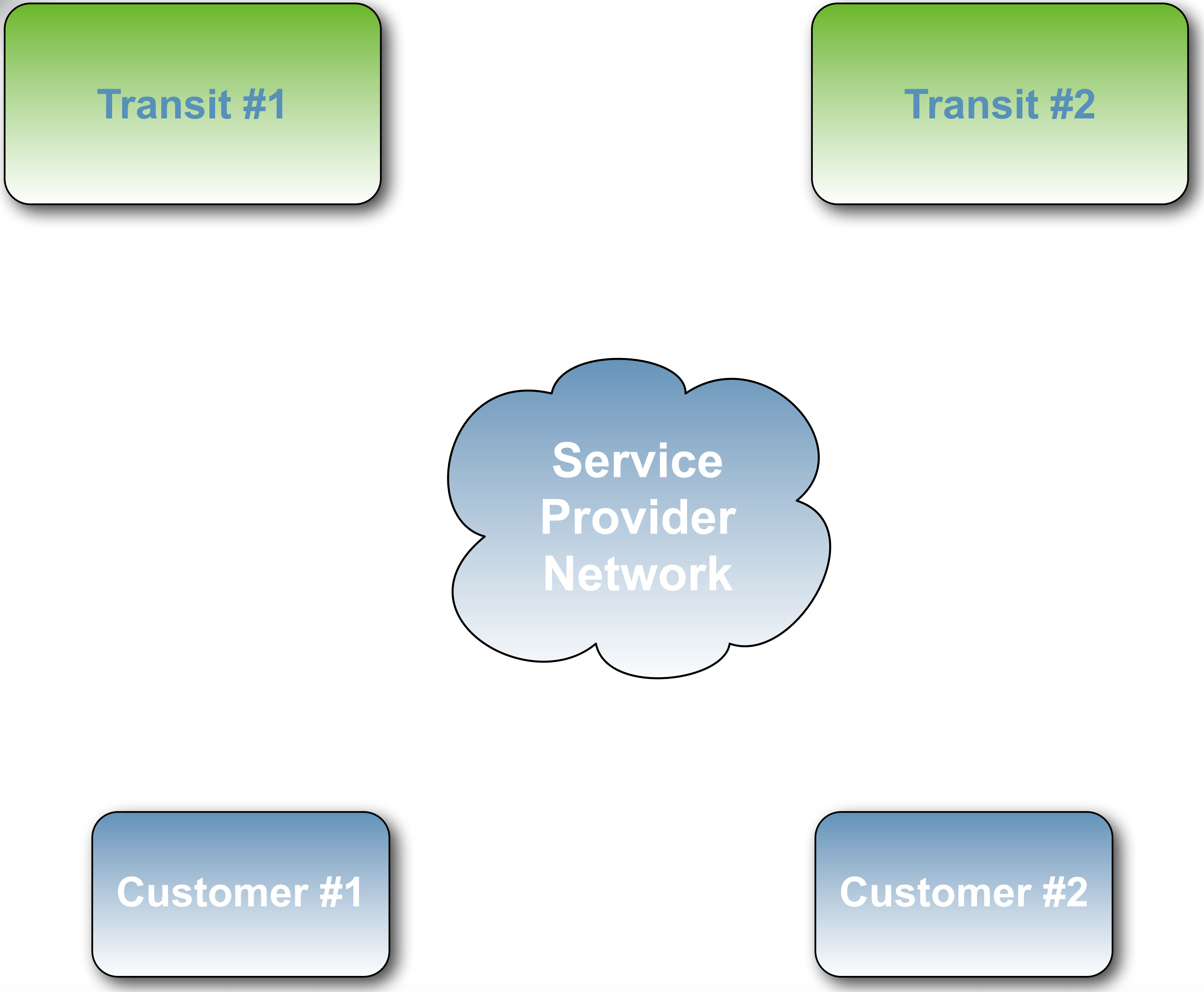
loose urpf

allow if the router has a route which contains the source ip address of packet

strict urpf

loose mode + route must point to the interface that the packet arrived on

RTBH Tutorial - Refresher on uRPF



Transit #1

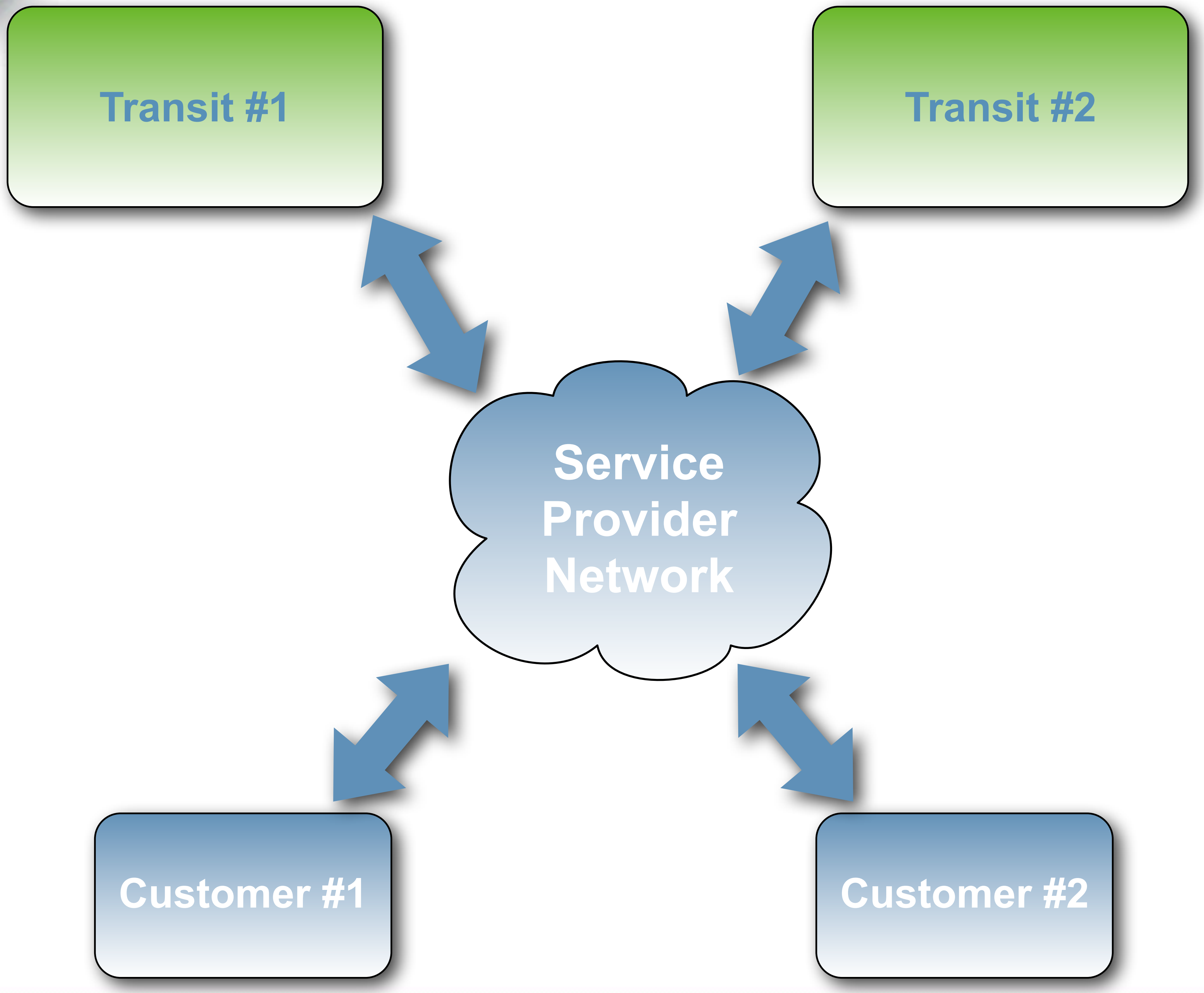
Transit #2

Service Provider Network

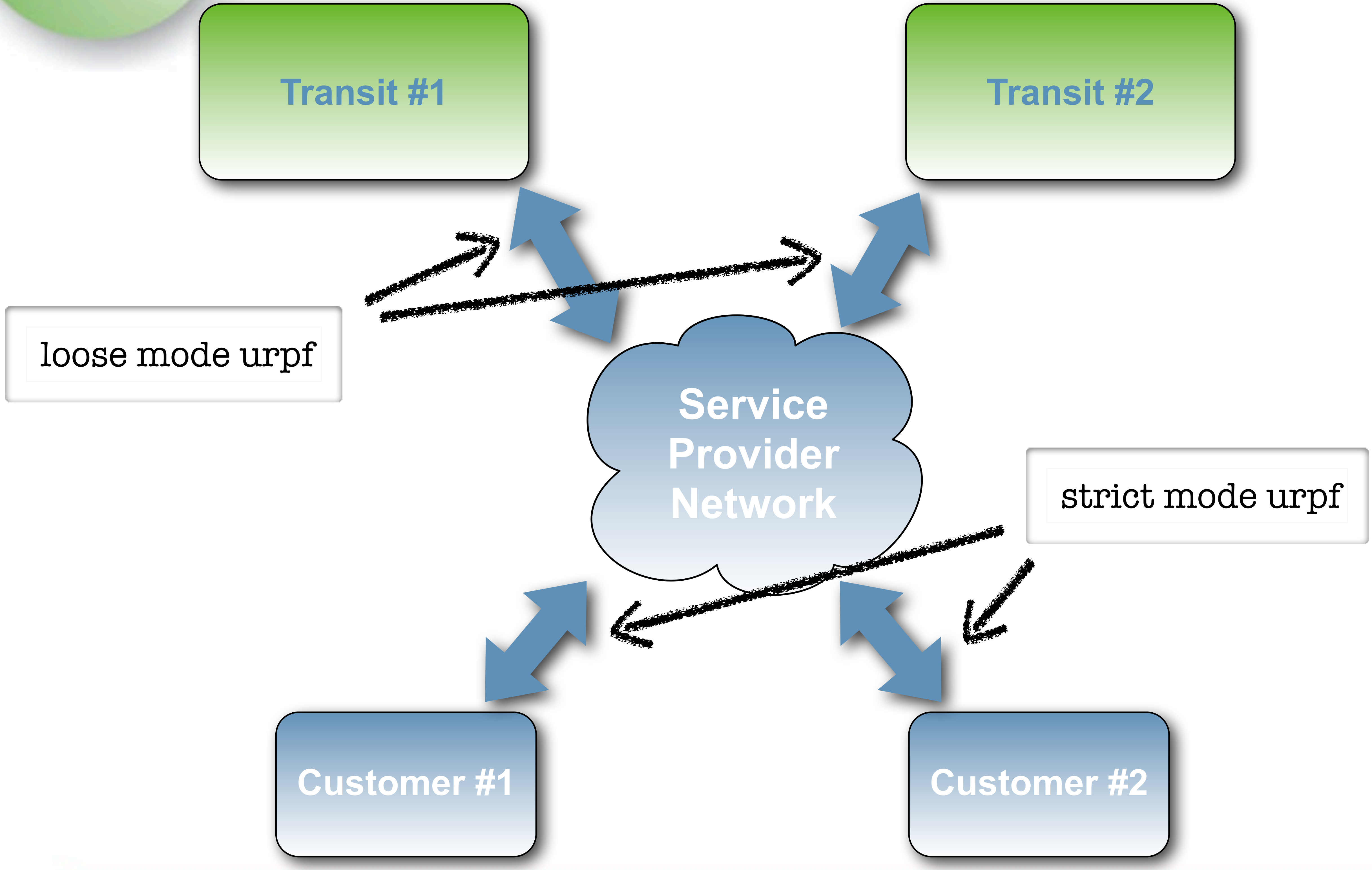
Customer #1

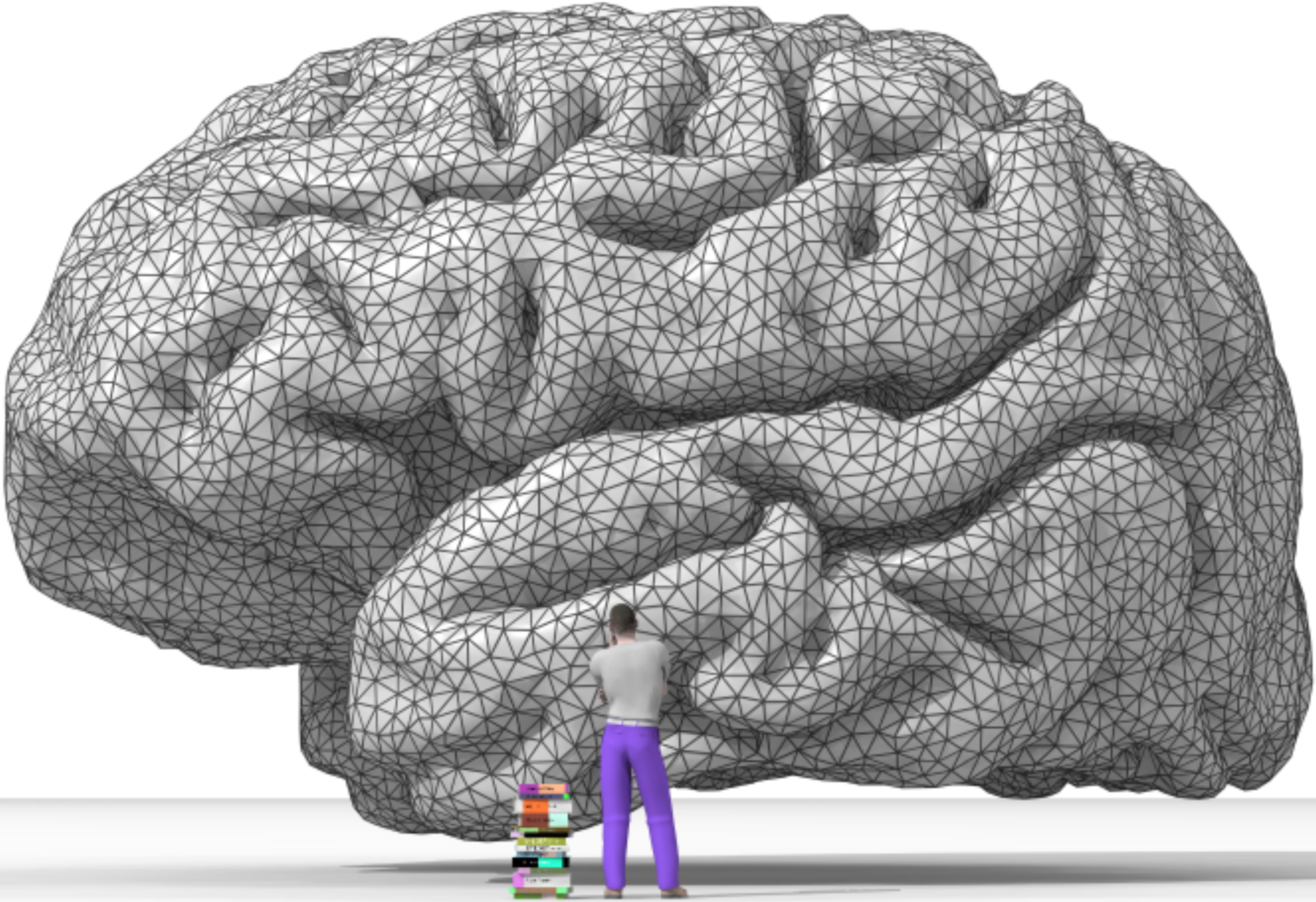
Customer #2

RTBH Tutorial - Refresher on uRPF



RTBH Tutorial - Refresher on uRPF



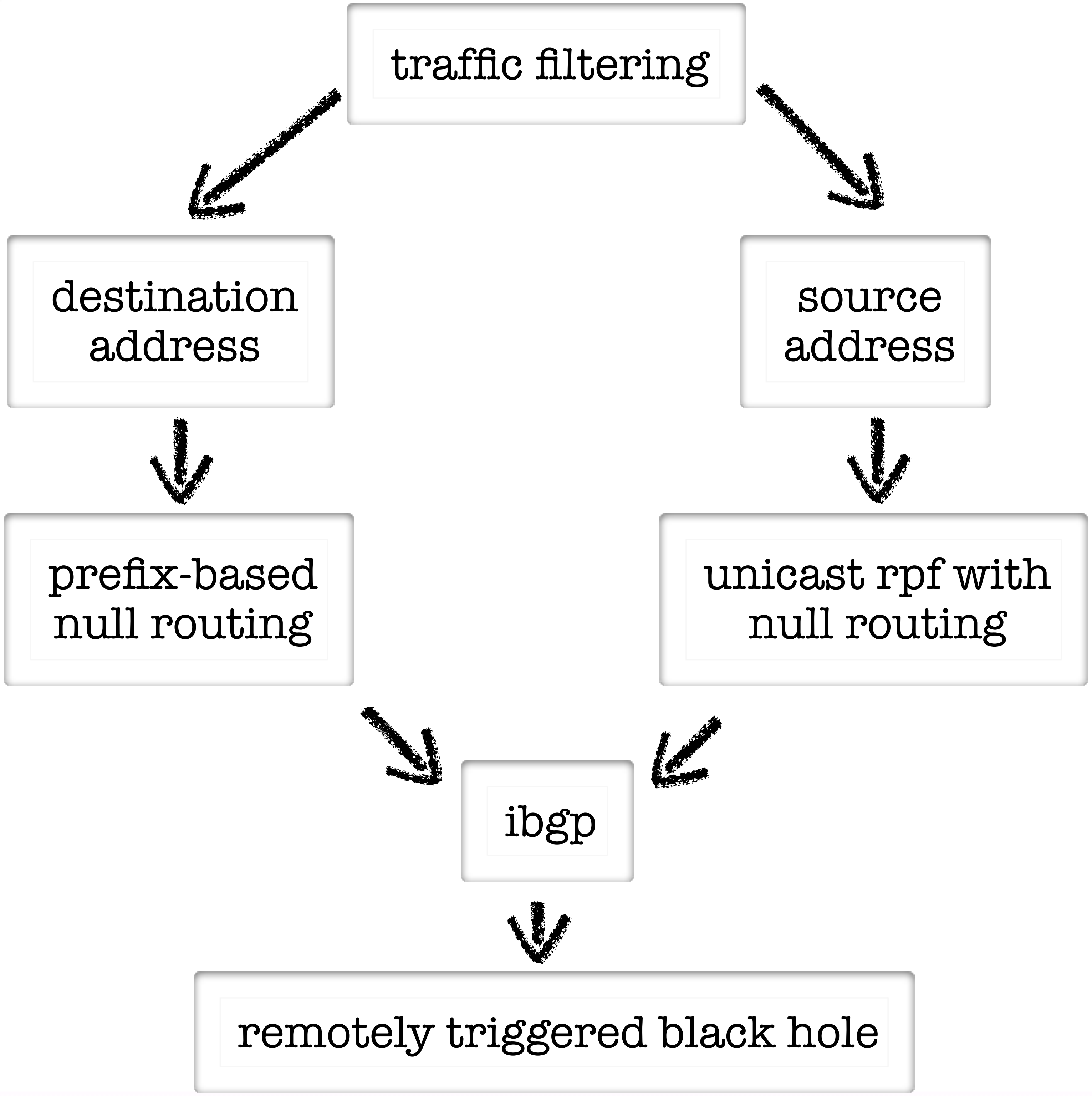


http://www.loria.fr/~rougier

RTBH Tutorial - Methodology

traffic filtering

RTBH Tutorial - Methodology



traffic filtering

destination address

source address

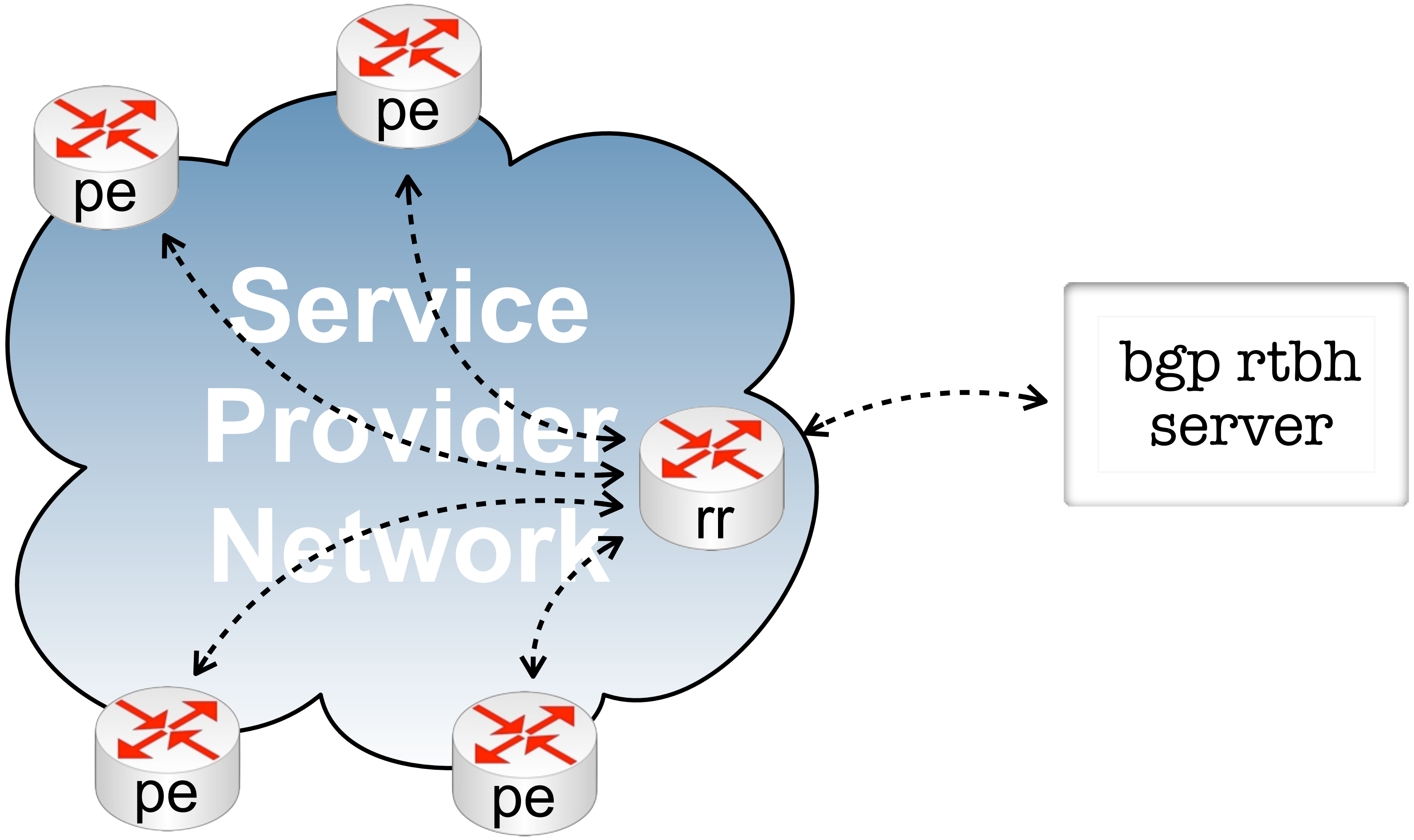
prefix-based null routing

unicast rpf with null routing

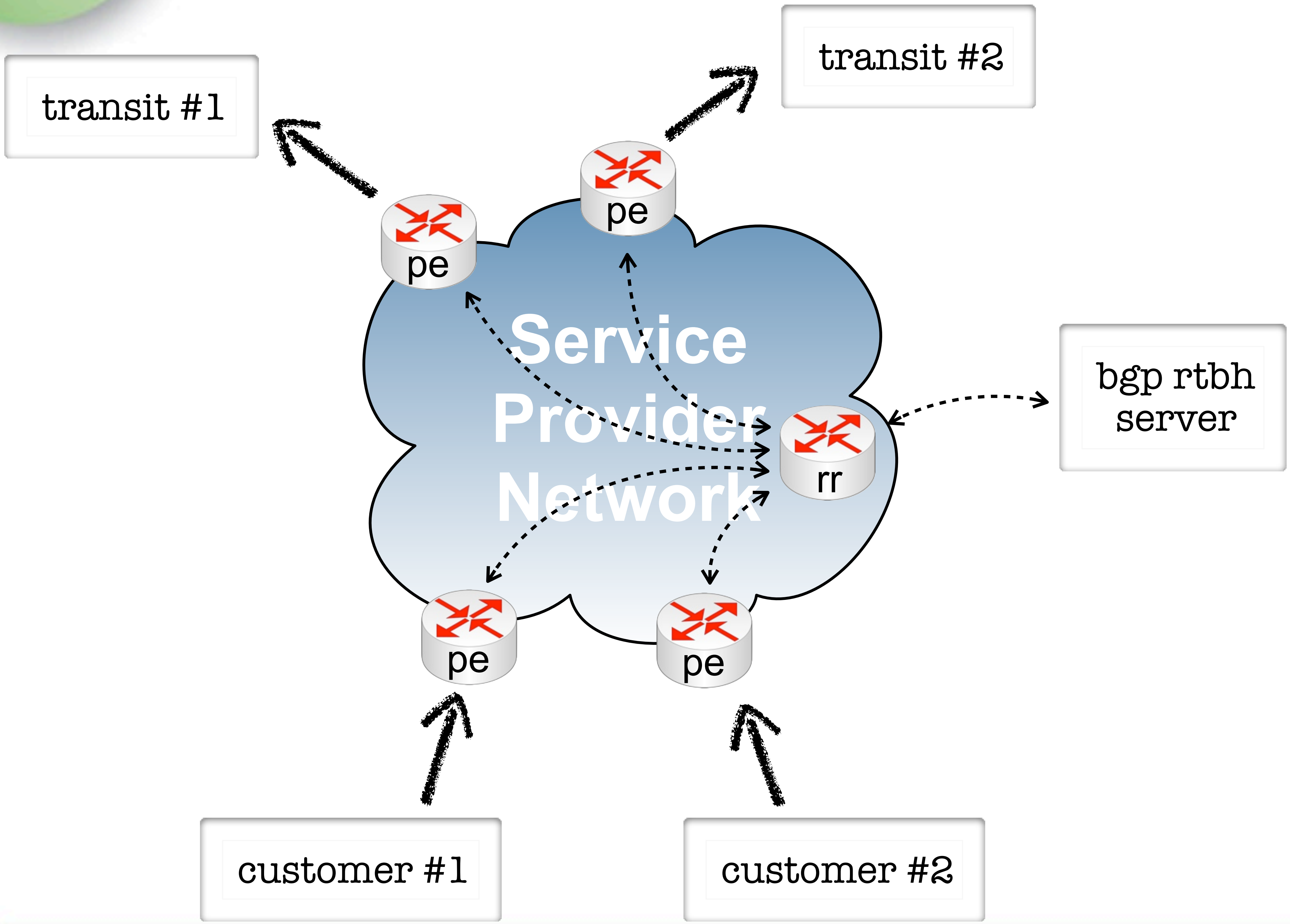
ibgp

remotely triggered black hole

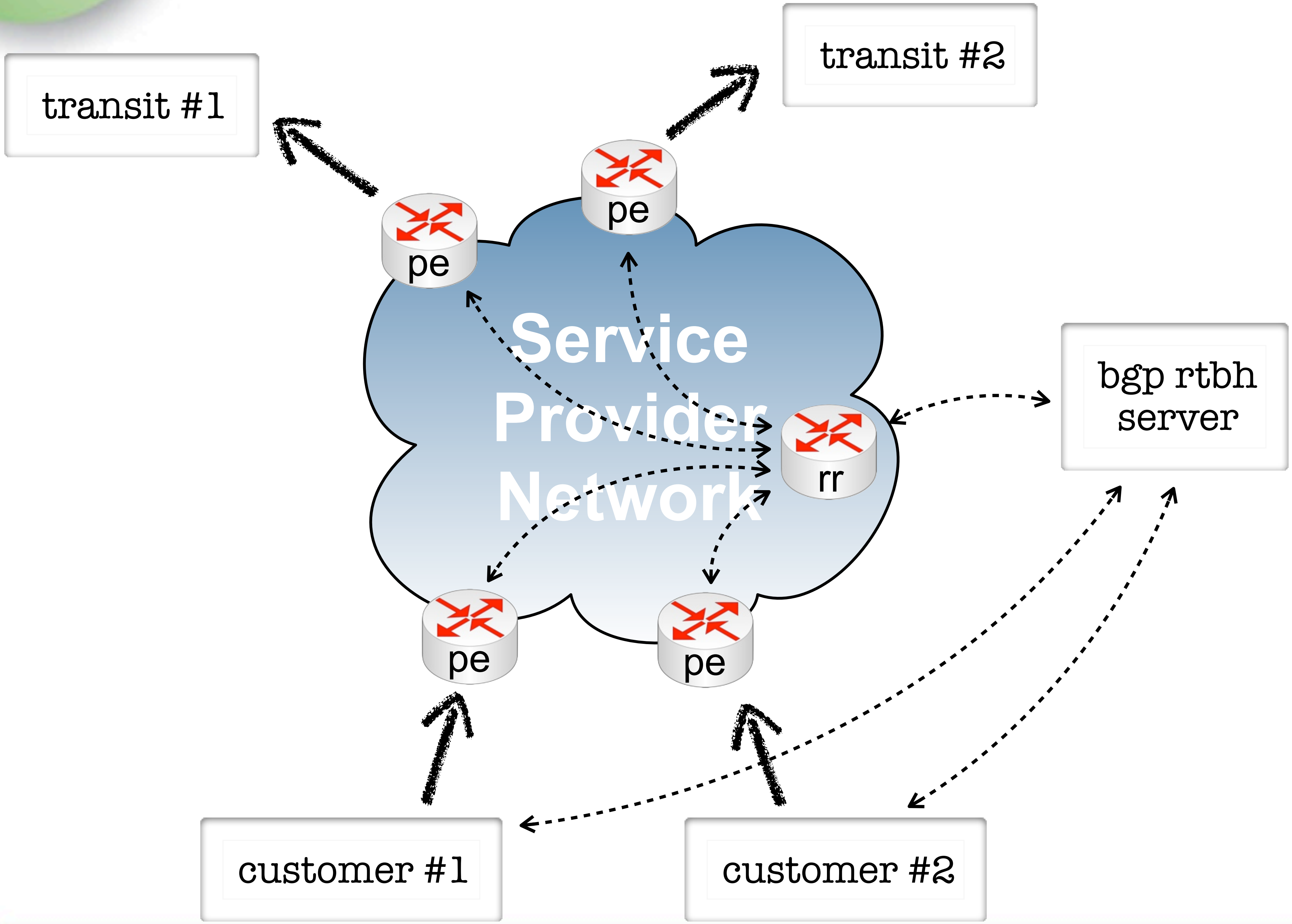
RTBH Tutorial - Integration Design



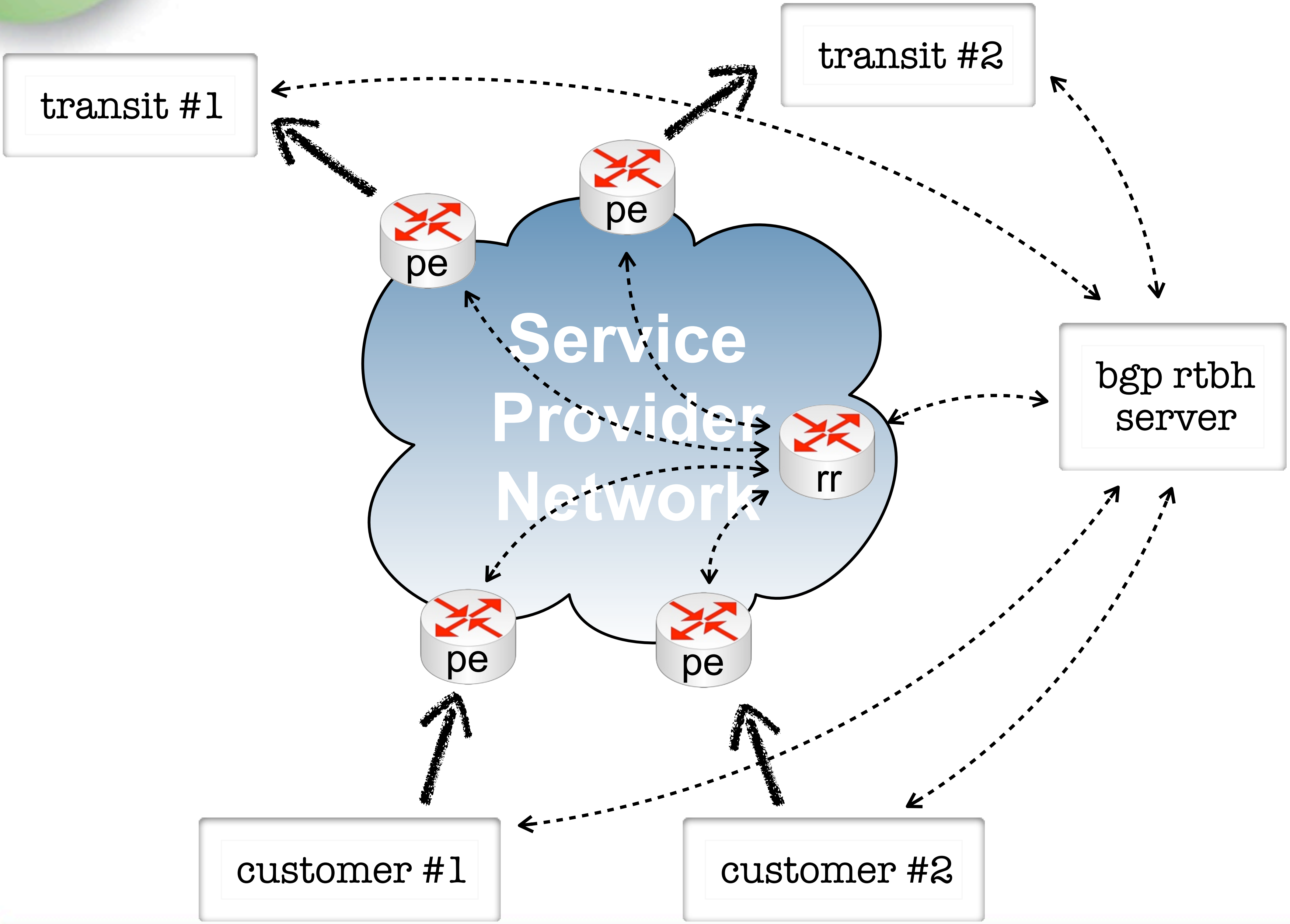
RTBH Tutorial - Integration Design



RTBH Tutorial - Integration Design



RTBH Tutorial - Integration Design



RTBH Tutorial - Can Work Anywhere

fully standards compliant

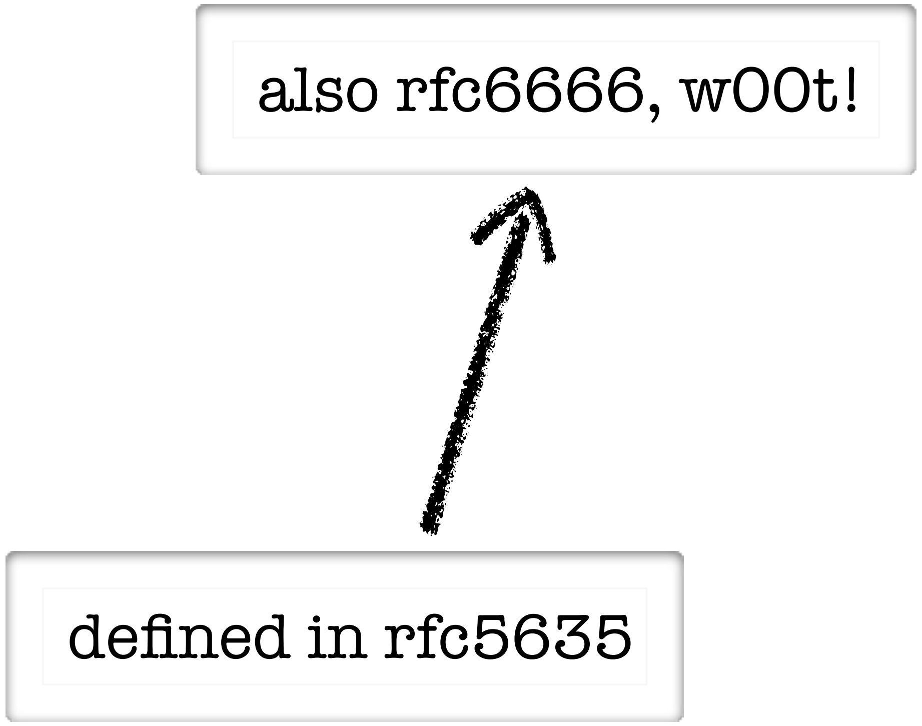
RTBH Tutorial - Can Work Anywhere

fully standards compliant

defined in rfc5635

RTBH Tutorial - Can Work Anywhere

fully standards compliant



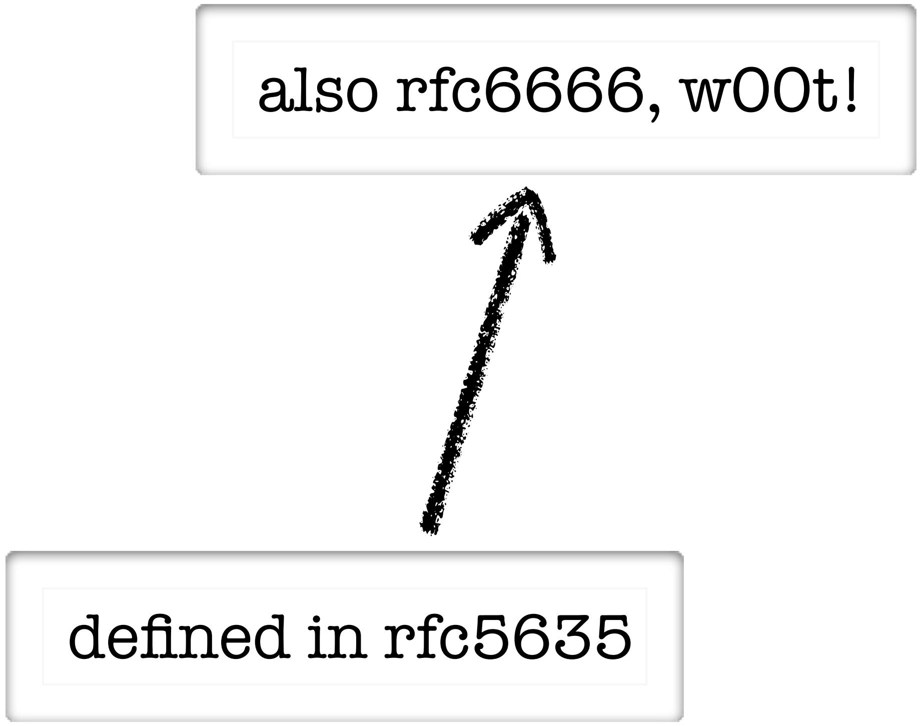
also rfc6666, w00t!

defined in rfc5635

RTBH Tutorial - Can Work Anywhere

fully standards compliant

fast, efficient means of black-holing

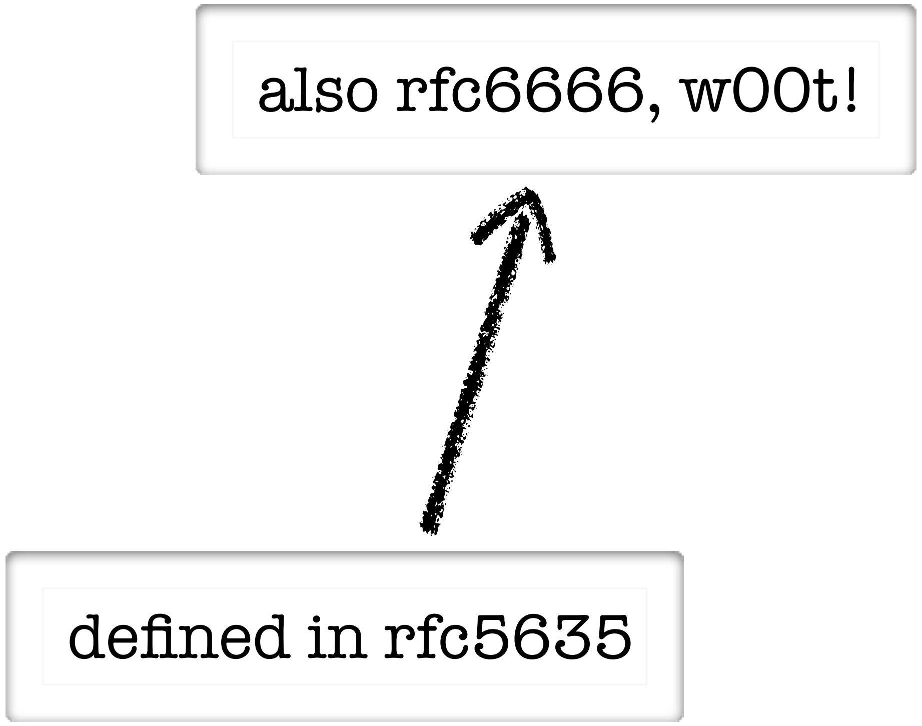


defined in rfc5635

also rfc6666, w00t!

RTBH Tutorial - Can Work Anywhere

fully standards compliant



defined in rfc5635

also rfc6666, w00t!

fast, efficient means of black-holing

rtbh uplink supported by many transit providers

RTBH Tutorial - Can Work Anywhere

fully standards compliant

defined in rfc5635

also rfc6666, w00t!

fast, efficient means of black-holing

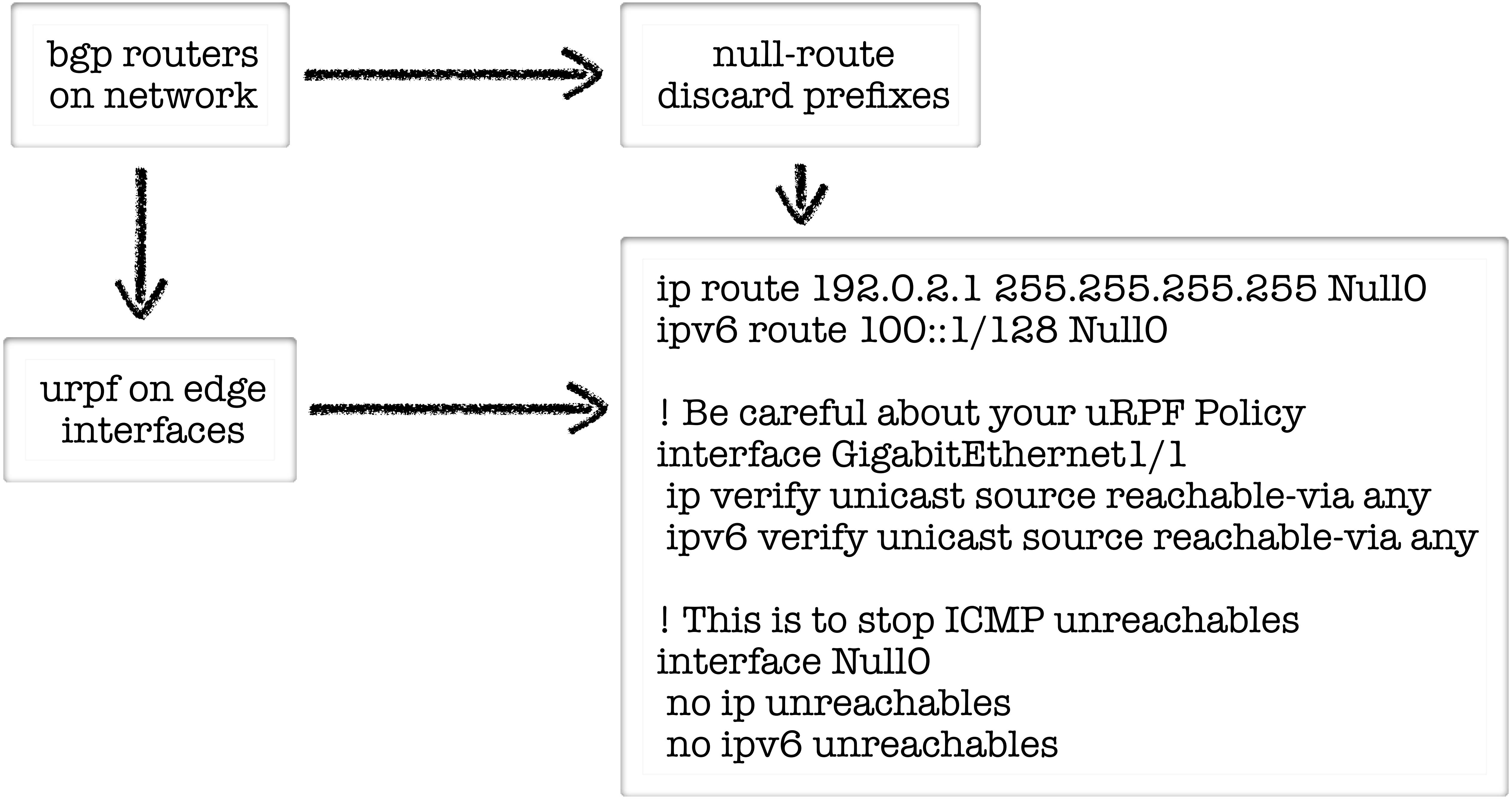
gives good excuse to implement bcp38

rtbh uplink supported by many transit providers

RTBH Tutorial - PE Configuration

bgp routers on network

RTBH Tutorial - PE Configuration



bgp routers on network

null-route discard prefixes

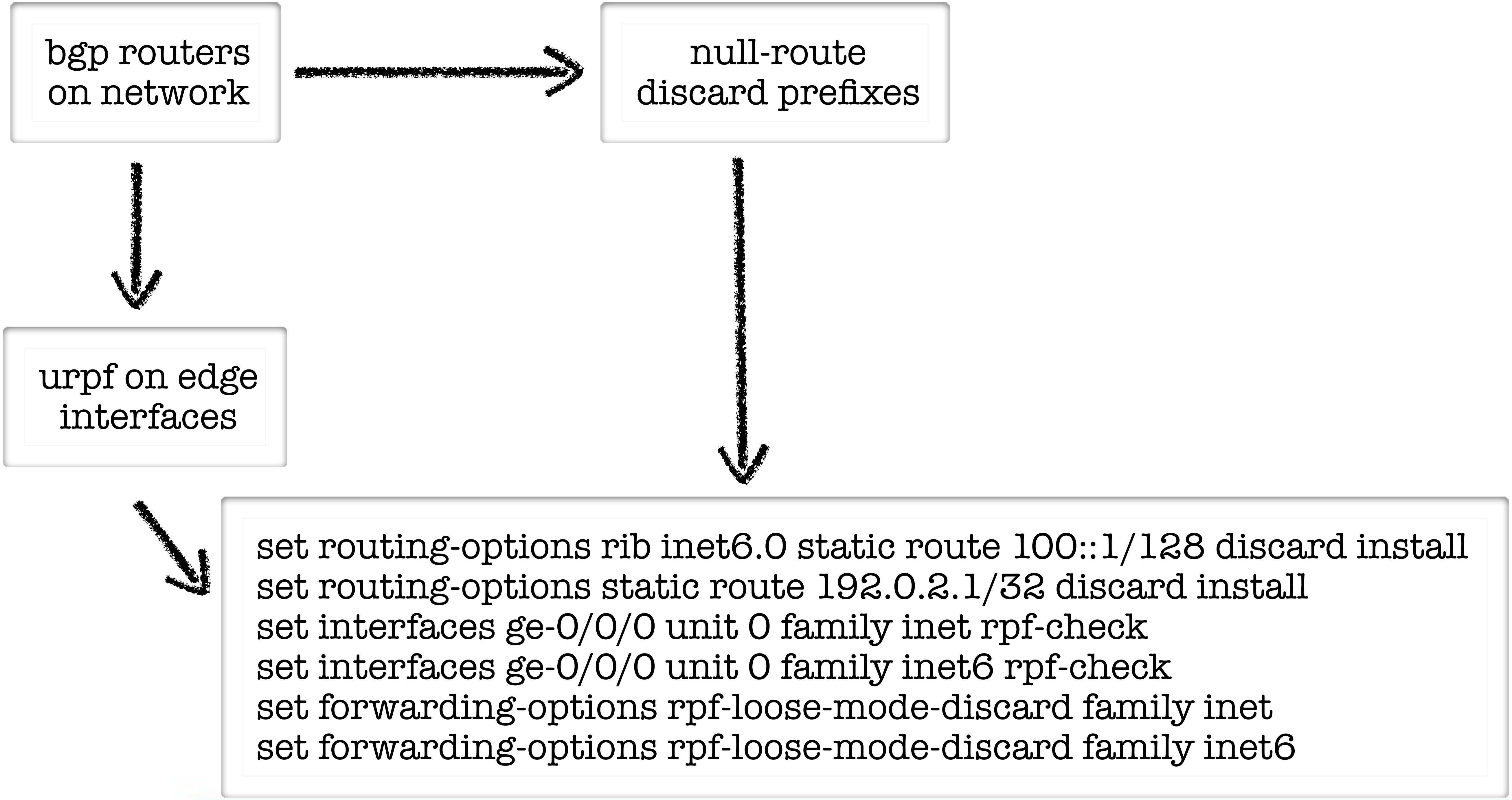
urpf on edge interfaces

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

! Be careful about your uRPF Policy
interface GigabitEthernet1/1
 ip verify unicast source reachable-via any
 ipv6 verify unicast source reachable-via any

! This is to stop ICMP unreachables
interface Null0
 no ip unreachables
 no ipv6 unreachables
```

RTBH Tutorial - PE Configuration



bgp routers on network

null-route discard prefixes

urpf on edge interfaces

```
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
set forwarding-options rpf-loose-mode-discard family inet
set forwarding-options rpf-loose-mode-discard family inet6
```

RTBH Tutorial - Implementation Notes

RTBH Tutorial - Implementation Notes

be careful that your hardware supports unicast rpf properly

don’t run ipv6 unicast rpf on a sup720

asr9k requires IOS XR >= 4.1.1

loose urpf discard requires junos 12.1 + MX/T series

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

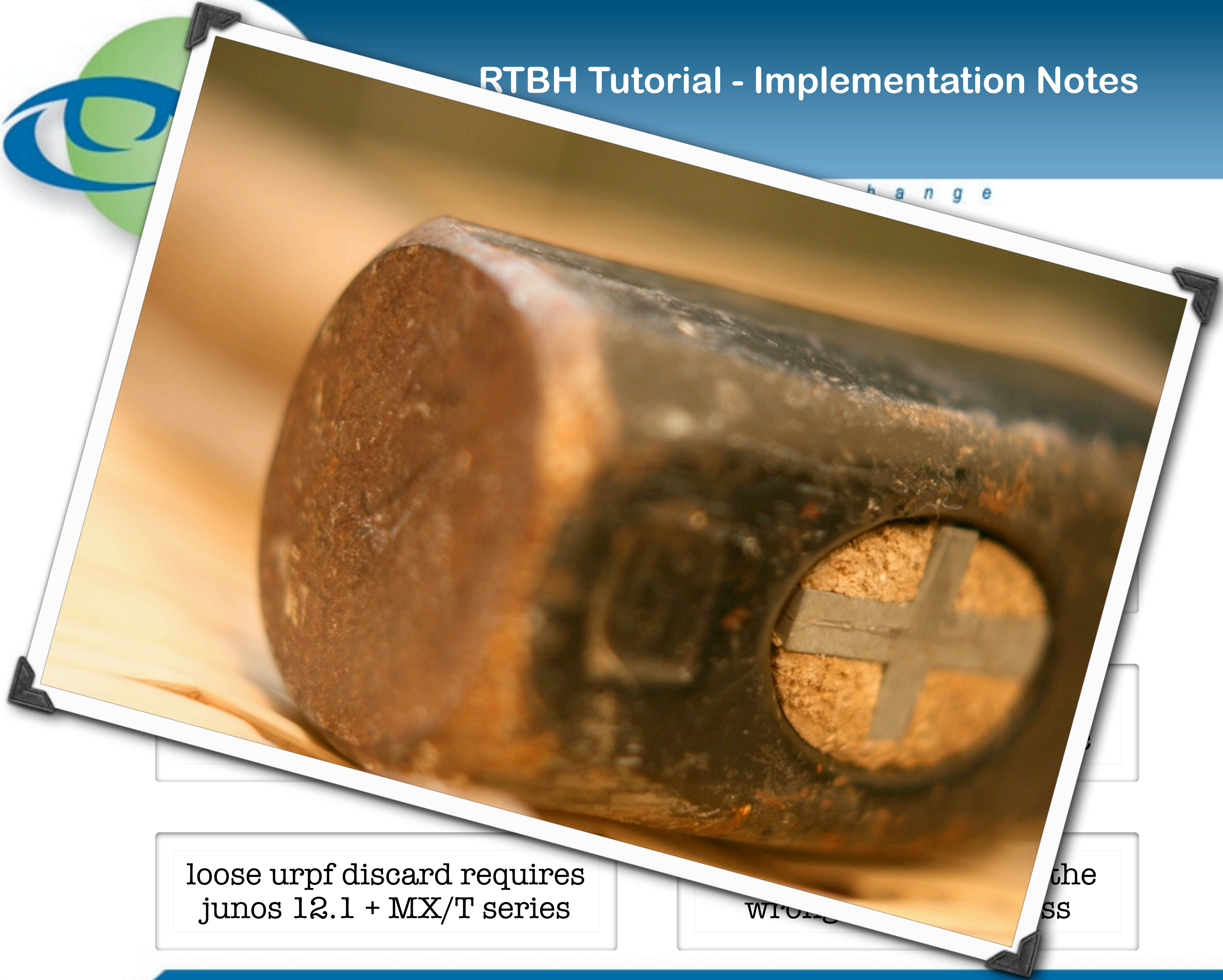
asr9k requires IOS XR >= 4.1.1

can also run rtbh using quagga, bird, exabgp, etc

loose urpf discard requires junos 12.1 + MX/T series

be careful not to filter the wrong source address

RTBH Tutorial - Implementation Notes



loose urpf discard requires
junos 12.1 + MX/T series

the
wrong ss

RTBH Tutorial - Server Configuration

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