Protecting your peering edge.

Graham Beneke
AfPIF 2015

#include std-disclaimer

Peer 3

ISP

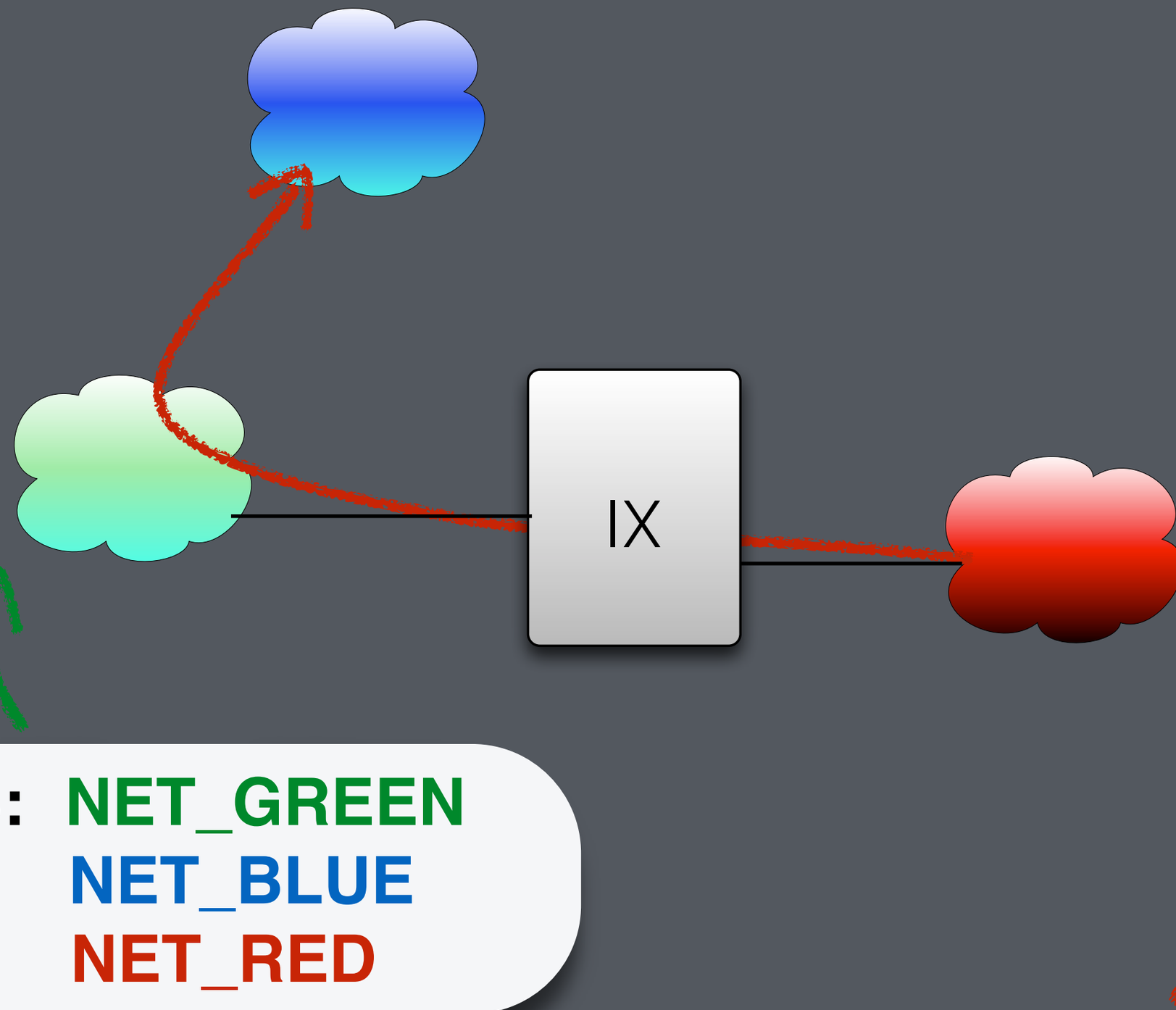
IXP

Peer 2

Peer 1

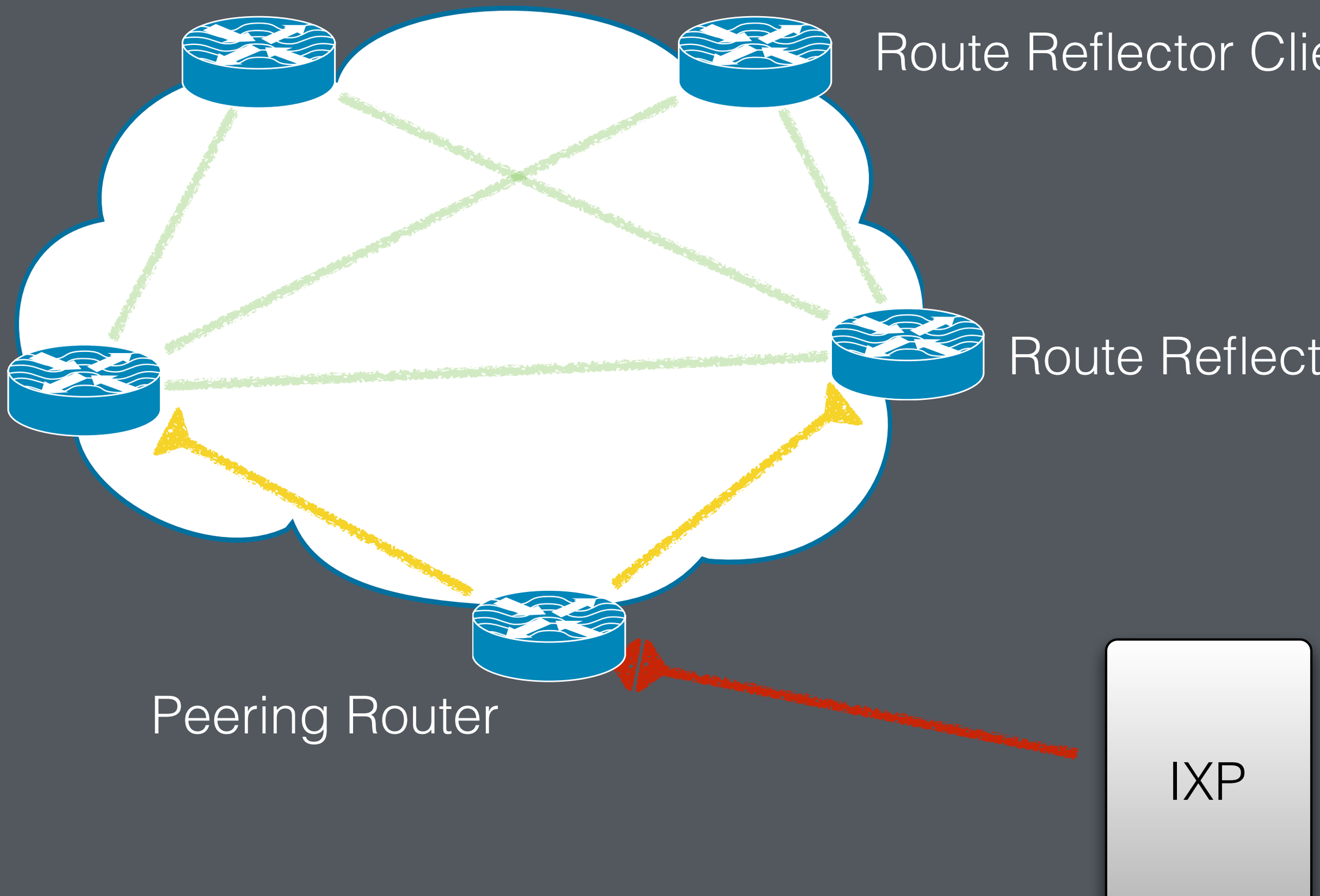
Expect to receive
traffic not destined
to your network.

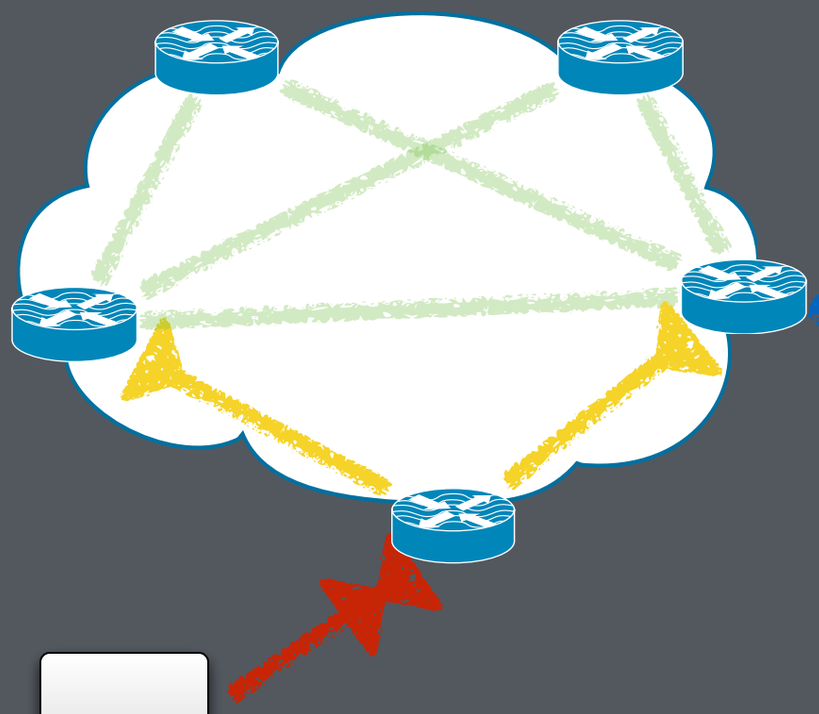
You **will** need to protect your network!



FIB: **NET_GREEN**
NET_BLUE
NET_RED

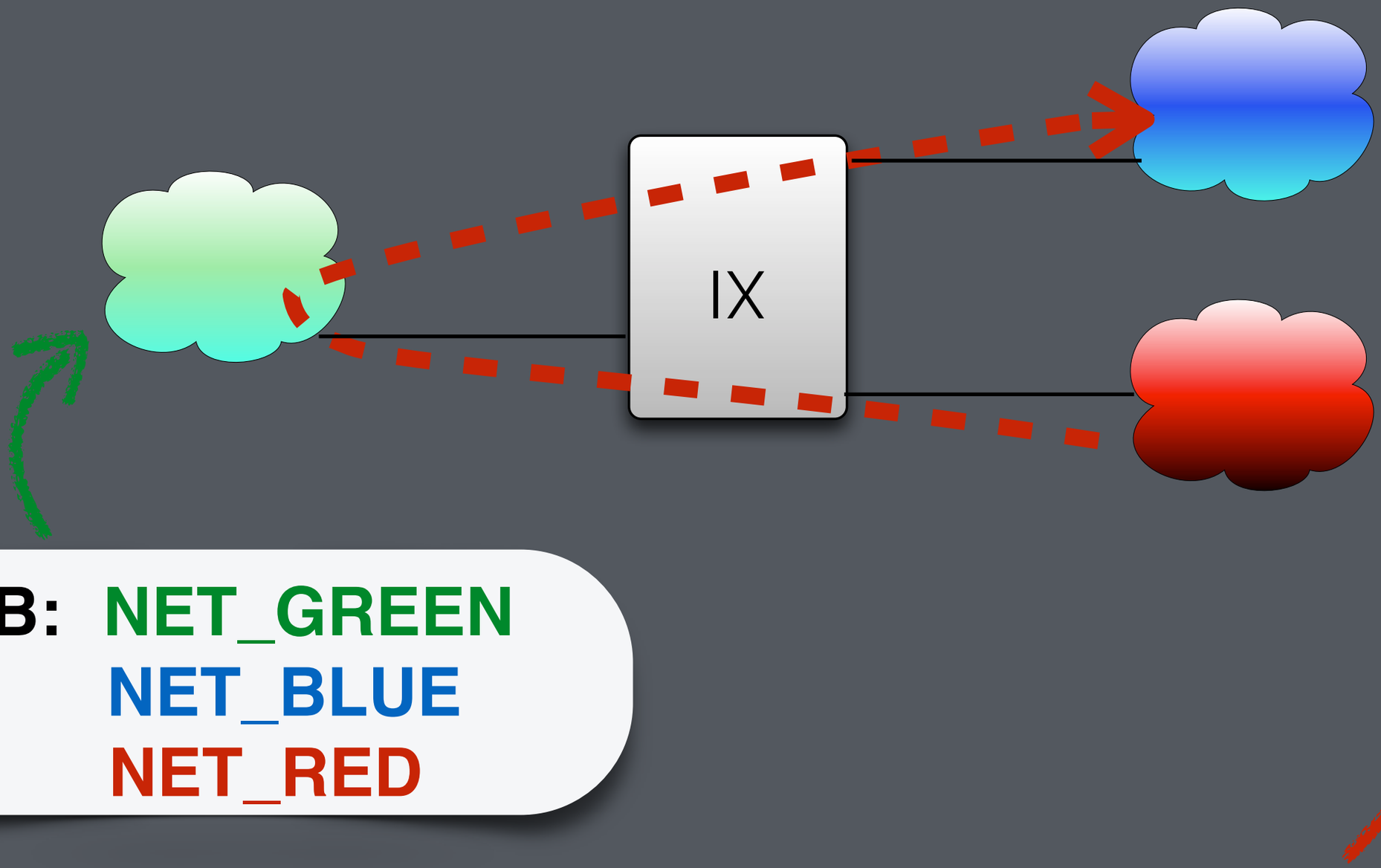
FIB: **NET_GREEN**
NET_RED


Route Reflector Client
Route Reflector
Peering Router
IXP



```
route-map filter-to-my-peering-router
        match criteria only_my_customers
                permit only_my_customers
```

Whom are you protecting against?



FIB: NET_GREEN
NET_BLUE
NET_RED

FIB: NET_GREEN
NET_RED

1

2

3

- BGP advertisement classification
- QoS Policy Propagation via BGP (QPPB).

Step 1: Tag peer prefixes uniquely within BGP and FIB tables

- peer prefixes set with community attribute (P) and tag (P)

- customer prefixes are set with community attribute (C) and tag (C)

Step 2: Tag external packets at peering locations based upon longest prefix match within FIB:

- tag (P) for packets received from peer and **destined** to a prefix in the FIB with tag (P),
- tag (C) for packets received from peer and **destined** to a prefix in the FIB with tag (C).

```
int Gig 0/0
 ipv4 bgp policy propagation input qos-group destination
```

```
nd-cla
class-map match-any
match qos-group 7
end-class-map
!
policy-map qppb_set_dscp
class TWO
set dscp af21
!
class EXT
police rate 1000000 bps burst
31250 bytes peak-burst 31250 bytes
conform-action drop
```

Step 3 (Packet classification via MQC):

ISP forwards or discards packets that ingress peering interconnects based upon associated packet tag value:

- Packets with tag (B) are discarded
- Packets with tag (C) are forwarded

```
int Gig 0/0
 ipv4 bgp policy propagation input qos-group destination
  service-policy input qppb_set_dscp
```

handouts available for IOS, IOS-XR and JunOS

- Hardware forwarding platform.

- Classification is a key requirement.

graham@inx.net.za