Lab – DDOS Attack Mitigation

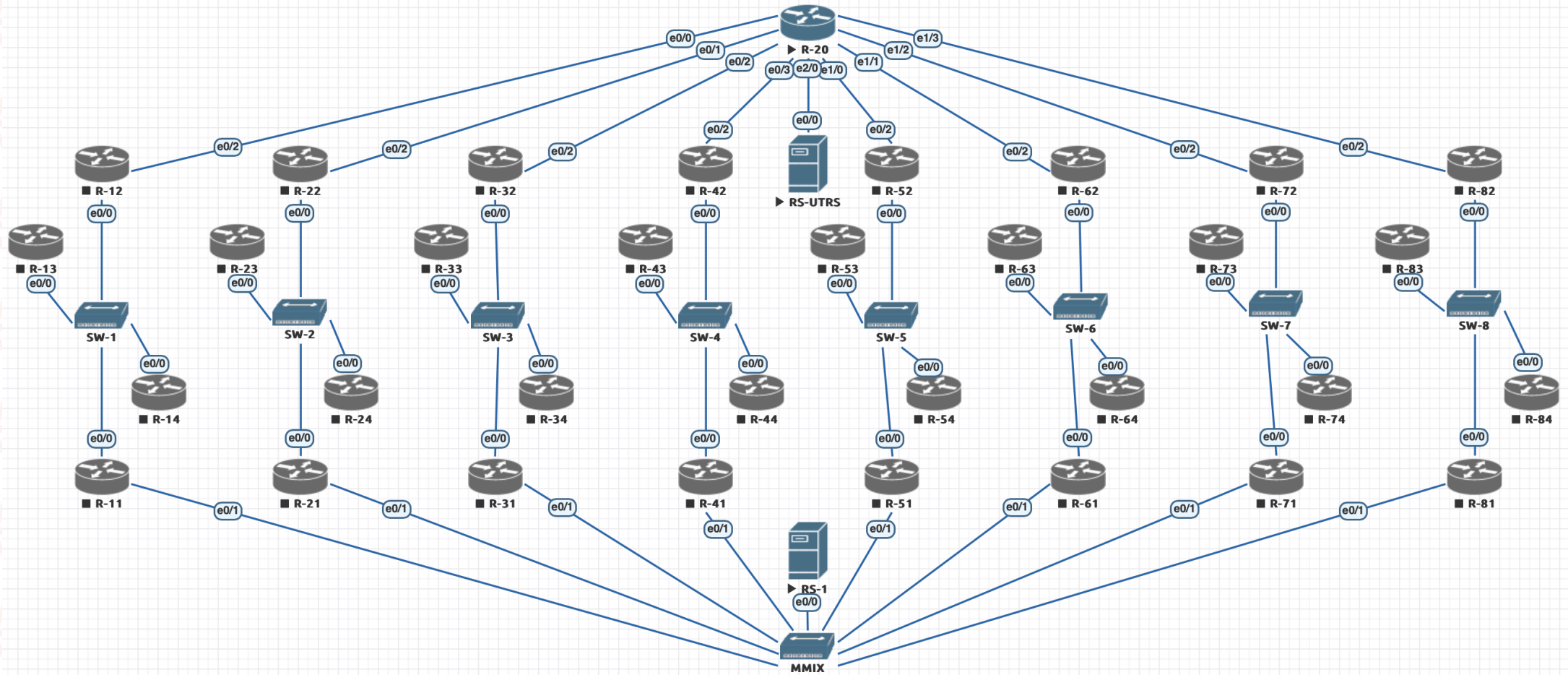
MYANMAR NETWORK OPERATORS GROUP

Author: Thein Myint Khine

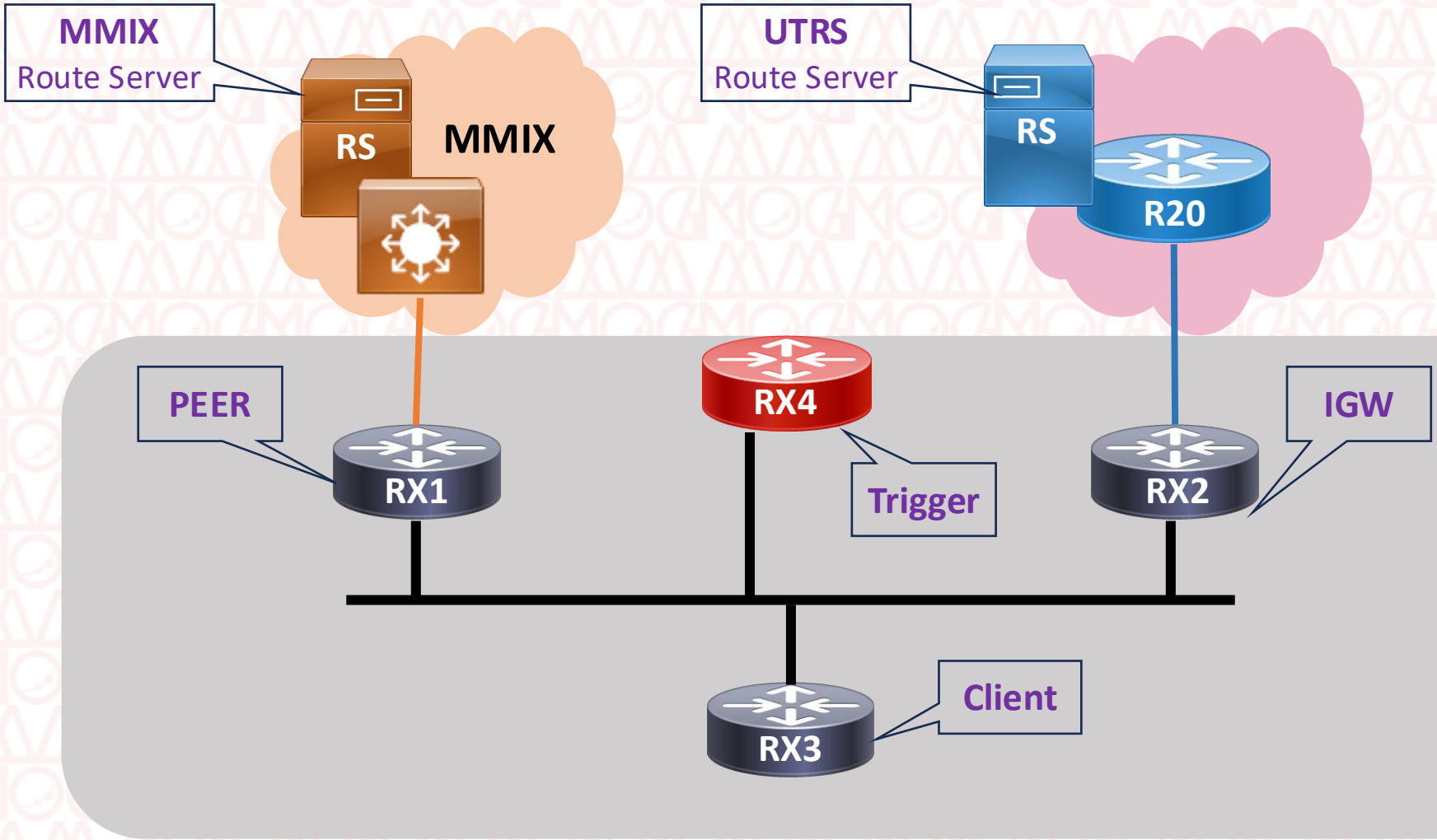
Version: 0.1

Last Update: Mar 18, 2026

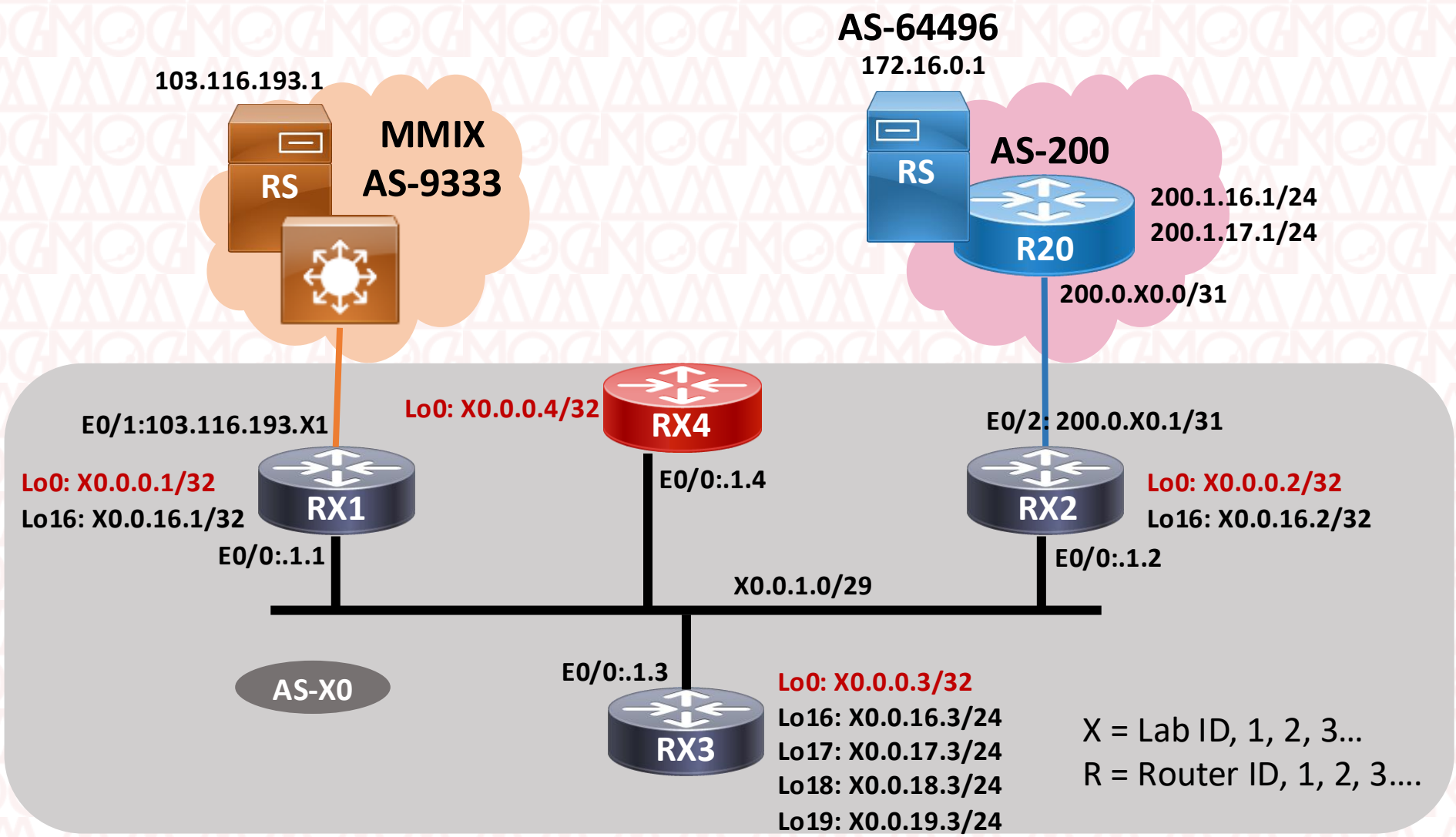
LAB – DDOS Overall Diagram



LAB – DDOS Functioning Diagram



LAB – DDOS Diagram - Details



Basic Configurations

Prefix-list

bgp communities

route-map

1. create prefix-lists of the following

1. allow host only.
2. deny default-gateway.
3. allow all IPs.
4. allow all IP longer than /24 (starting /25)
5. allow prefixes of
   - 10.0.18.0/24
   - 10.0.19.0/24
6. allow prefixes of
   - 10.0.16.0/24
   - 10.0.17.0/24
   - 10.0.18.0/24
   - 10.0.19.0/24

1. create prefix-lists - Answers

1. allow host only.

```
ip prefix-list PRF-HOST permit 0.0.0.0/32
```

2. deny default-gateway.

```
ip prefix-list PRF-DGW deny 0.0.0.0/0
```

3. allow all IPs.

```
ip prefix-list PRF-ALL permit 0.0.0.0/0 le 32
```

4. allow all IP prefixes longer than /24 (starting /25)

```
ip prefix-list PRF-25 permit 0.0.0.0/0 ge 25
```

5. allow prefixes of 10.0.18.0/24 and 10.0.19.0/24

```
ip prefix-list PRF-18-19 permit 10.0.18.0/23 le 24
```

6. allow prefixes of 10.0.16.0/24 to 10.0.19.0/24

```
ip prefix-list PRF-16 permit 10.0.16.0/22 le 24
```

2. BGP community & route-map

```
@Create a standard community list
        ip community-list standard <NAME> permit <aa:nn>
```

```
@Route-map
        route-map <NAME> permit/deny <seq>
         match
         set
@route-map - Example
        route-map RM-TRANSIT-IN permit 10
         match ip address prefix-list PRF-MINE
         match as-path 10
         set community no-advertise
         set local-preference 200
@route-map – binding
        router bgp 10
         neighbor 200.0.2.1 route-map RM-TRANSIT-IN out
         redistribute static route-map RTBH
```

2. show bgp using regular expressions

```
@ show bgp all prefixes from local AS

@ show bgp prefixes originated from AS200 that is directly connect to our AS.

@ show bgp prefixes that transit directly connected AS200.

@ show bgp prefixes that transit AS200.
```

2. show bgp using regular expressions

@ show bgp all prefixes from local AS

```
R11# show ip bgp regexp ^$
```

@ show bgp prefixes originated from AS200 that is directly connect to our AS.

```
R11# show ip bgp regexp ^200$
```

@ show bgp prefixes that transit directly connected AS200.

```
R11# show ip bgp regexp ^200_
```

@ show bgp prefixes that transit AS200.

```
R11# show ip bgp regexp _200_
```

Exercises

Sr.	Exercises
1	RTBH, Global Black Hole, within an ISP
2	RTBH, Community Method, Regional Black Hole, within an ISP
3	RTBH, Black Hole with IX Peers at MMIX
4	UTRS,
5	Next-hop
6	Sinkhole

1

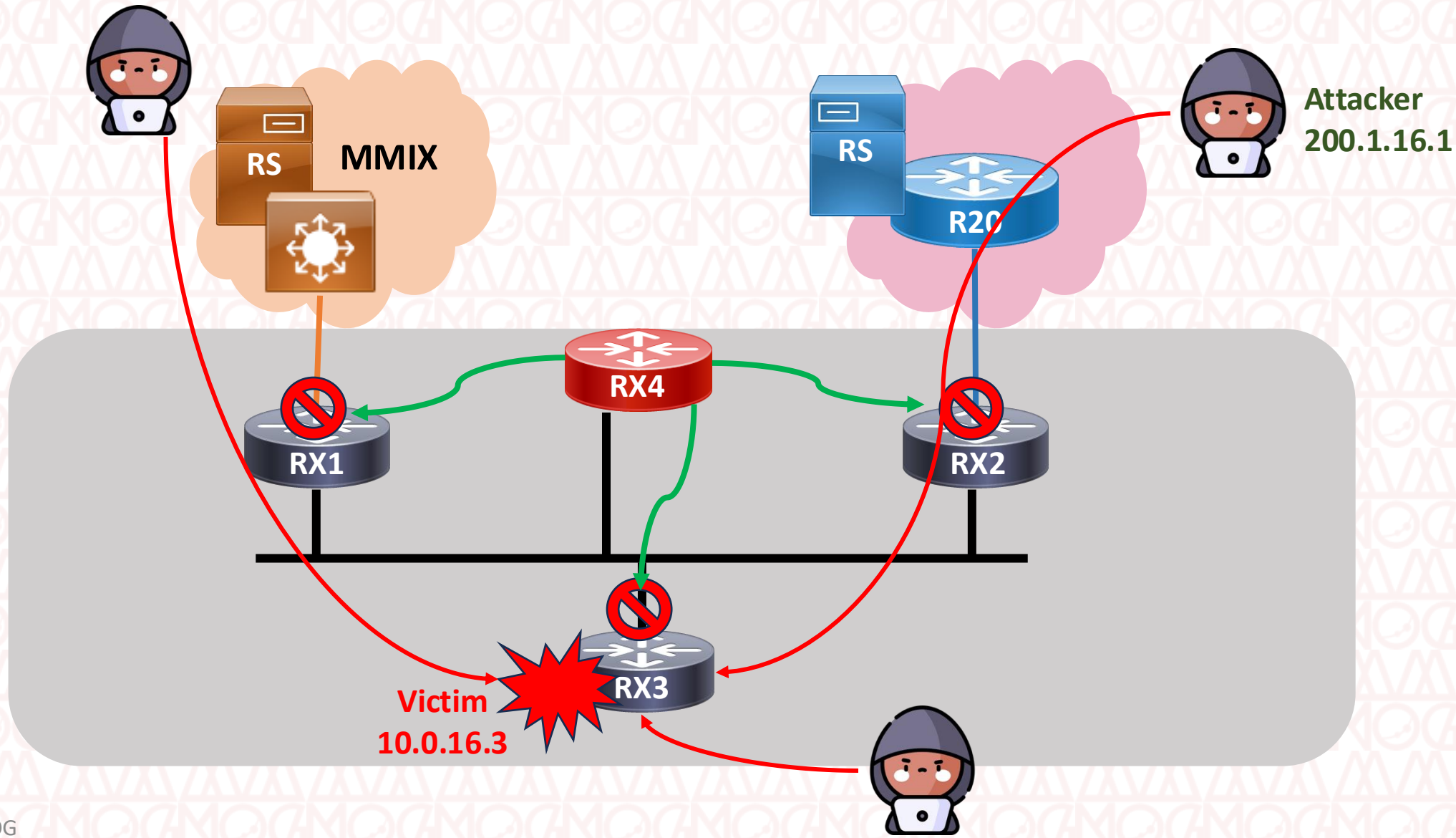
RTBH

Remote Trigger Black Hole

Global Black Hole

within an ISP

LAB – Global Defense



Using Trigger Machine

The route map black-hole-trigger is applied prior to redistributing static routes into BGP. The following occurs in the route map before

- redistributing the route to iBGP peers:
- Match on a tag value of 66.
- Set the next hop to 192.0.2.1.
- The local-preference is set to 200.
- The origin is set to IGP.
- The community is set to no-export.

1. Prepare Null Interfaces and Trigger Machine

```
Rx1(config)#
ip route 192.0.2.1 255.255.255.255 null 0
interface Null0
 no ip unreachable

Rx2(config)#
ip route 192.0.2.1 255.255.255.255 null 0
interface Null0
 no ip unreachable

Rx3(config)#
ip route 192.0.2.1 255.255.255.255 null 0
interface Null0
 no ip unreachable

Rx4(config)#
ip route 192.0.2.1 255.255.255.255 null 0
interface Null0
 no ip unreachable
```

```
! Create a route-map for Trigger
Rx4(config)#
route-map RTBH permit 10
 match tag 66
 set local-preference 200
 set origin igp
 set community no-export
 set ip next-hop 192.0.2.1
! Config BGP
router bgp 10
  redistribute static route-map RTBH
```

2. Trigger Test (Destination Attack & Source Attack)

! Assume IP X0.0.16.3 is under attack. Trigger that IP for black hole.

```
!check ping test by outside router to this victim IP before config.
!Trigger null routing.
Rx4(config)#
ip route 10.0.16.3 255.255.255.255 null 0 tag 66
!Check routing tables of the Routers.  Should noticed null routed route.
!AT Rx1, Rx2, Rx3
show ip bgp
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 10.0.16.0/24     10.0.0.3                 0    100      0 i
 *>i 10.0.16.3/32     192.0.2.1                0    200      0 i
```

! Assuming IP 200.1.16.1 is an attacker. Cut packets responding to source IP of attacker.

```
!check ping test to 200.1.16.1 before config.
Rx4(config)#
ip route 200.1.16.1 255.255.255.255 null 0 tag 66
```

2

RTBH

Community Method

Regional Black Hole

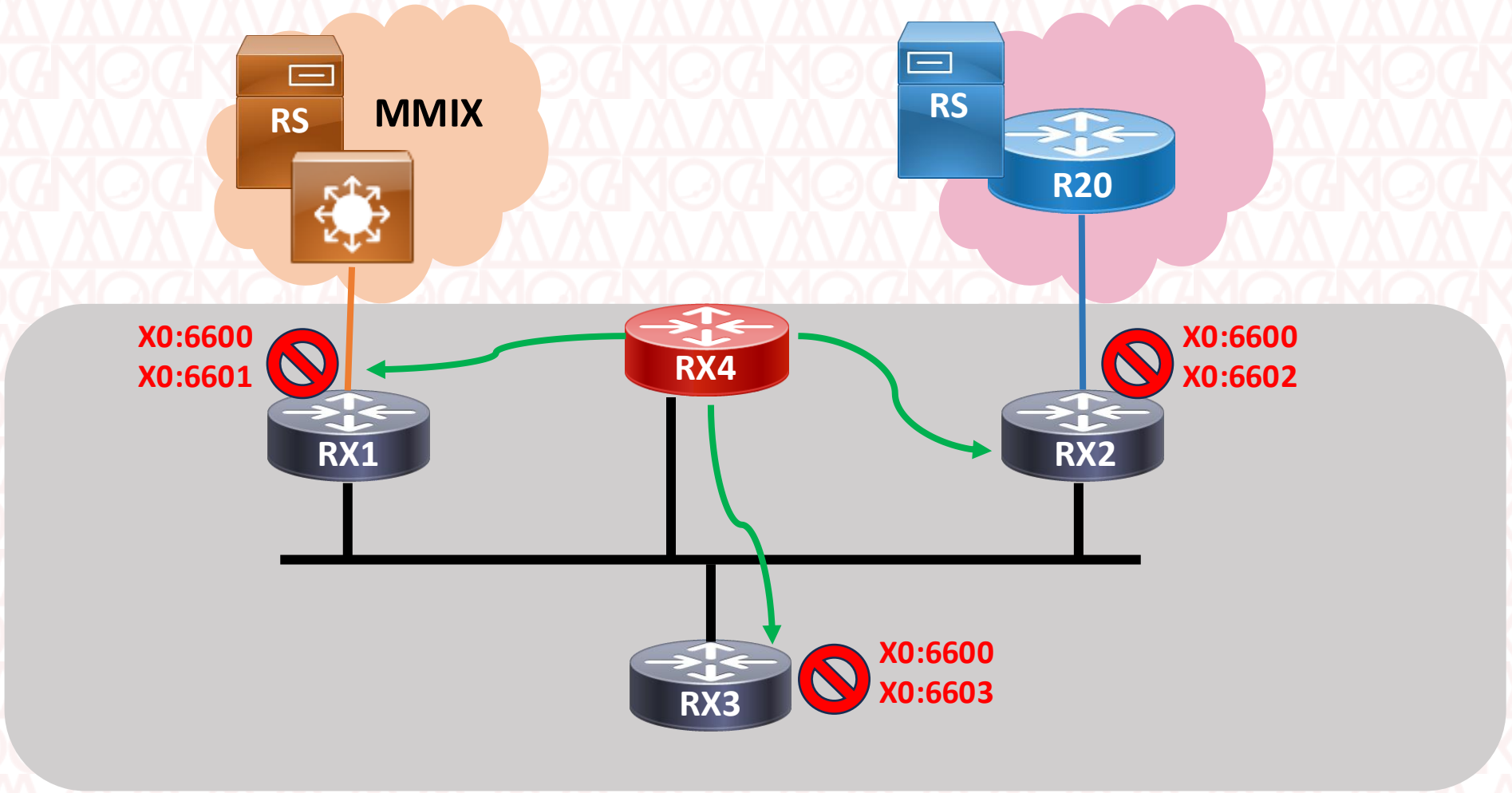
within an ISP

RTBH with community for regionalize

We will define the following community value for regional Black hole filtering.

Description	Communty	Remark
Black Hole at All	X0:6600	Drop Attack at all edge Routers
Black Hole at RX1	X0:6601	Drop Attack at Peer Router
Black Hole at RX2	X0:6602	Drop Attack at Gateway Router
Black Hole at RX3	X0:6603	Drop Attack at Client Router

LAB – Regional Defense



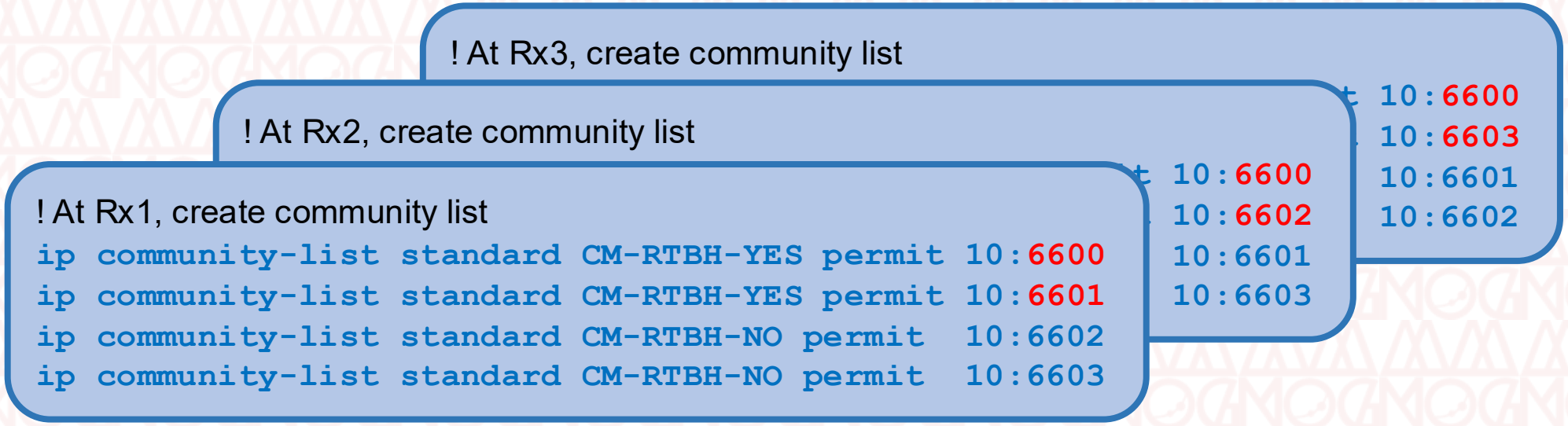
1. Community Based route-map at Trigger Machine

```
RX4(config)#
route-map RTBH permit 60
 match tag 6600
 set local-preference 200
 set origin igp
 set community 10:6600 no-export
 set ip next-hop 192.0.2.1
route-map RTBH permit 61
 match tag 6601
 set local-preference 200
 set origin igp
 set community 10:6601 no-export
 set ip next-hop 192.0.2.1
```

```
route-map RTBH permit 62
 match tag 6602
 set local-preference 200
 set origin igp
 set community 10:6602 no-export
 set ip next-hop 192.0.2.1
route-map RTBH permit 63
 match tag 6603
 set local-preference 200
 set origin igp
 set community 10:6603 no-export
 set ip next-hop 192.0.2.1
```

```
router bgp 10
  neighbor IBGP send-community
```

2. Preparation at Edged Machines



! Create route-map

```
route-map RM-IBGP-IN deny 10
 match community CM-RTBH-NO
route-map RM-IBGP-IN permit 20
 match community CM-RTBH-YES
 set community no-advertise
route-map RM-IBGP-IN permit 1000
```

! Bind route-map to BGP session

```
router bgp 10
 neighbor IBGP route-map RM-IBGP-IN in
```

3. Test Trigger for Black holes

```
! Create static routes for trigging.
Rx4(config)#
 ip route 10.0.16.60 255.255.255.255 null 0 tag 6600  ! Black hole at all Routers
 ip route 10.0.16.61 255.255.255.255 null 0 tag 6601  ! Black hole at Peer Router
 ip route 10.0.16.62 255.255.255.255 null 0 tag 6602  ! Black hole at IGW
 ip route 10.0.16.63 255.255.255.255 null 0 tag 6603  ! Black hole at Client Router
! Check the result
R11#sh ip bgp 10.0.16.60
BGP routing table entry for 10.0.16.60/32, version 74
Paths: (1 available, best #1, table default, not advertised to any peer)
  Not advertised to any peer
  Refresh Epoch 14
  Local
    192.0.2.1 from 10.0.0.4 (10.0.0.4)
      Origin IGP, metric 0, localpref 200, valid, internal, best
      Community: no-advertise
      rx pathid: 0, tx pathid: 0x0
```

4. Check Results

```
R11#sh ip bgp
     Network          Next Hop            Metric LocPrf Weight
Path
 *>  10.0.16.60/32    192.0.2.1                0    200  32768 i
 *>  10.0.16.61/32    192.0.2.1                0    200  32768 I
```

```
R12#sh ip bgp
     Network          Next Hop            Metric LocPrf Weight
Path
 *>  10.0.16.60/32    192.0.2.1                0    200  32768 i
 *>  10.0.16.62/32    192.0.2.1                0    200  32768 I
```

```
R13#sh ip bgp
     Network          Next Hop            Metric LocPrf Weight
Path
 *>  10.0.16.60/32    192.0.2.1                0    200  32768 i
 *>  10.0.16.63/32    192.0.2.1                0    200  32768 I
```

```
R14#sh ip bgp
     Network          Next Hop            Metric LocPrf Weight
Path
 *>  10.0.16.60/32    192.0.2.1                0    200  32768 i
 *>  10.0.16.61/32    192.0.2.1                0    200  32768 i
 *>  10.0.16.62/32    192.0.2.1                0    200  32768 i
 *>  10.0.16.63/32    192.0.2.1                0    200  32768 i
```

3

RTBH

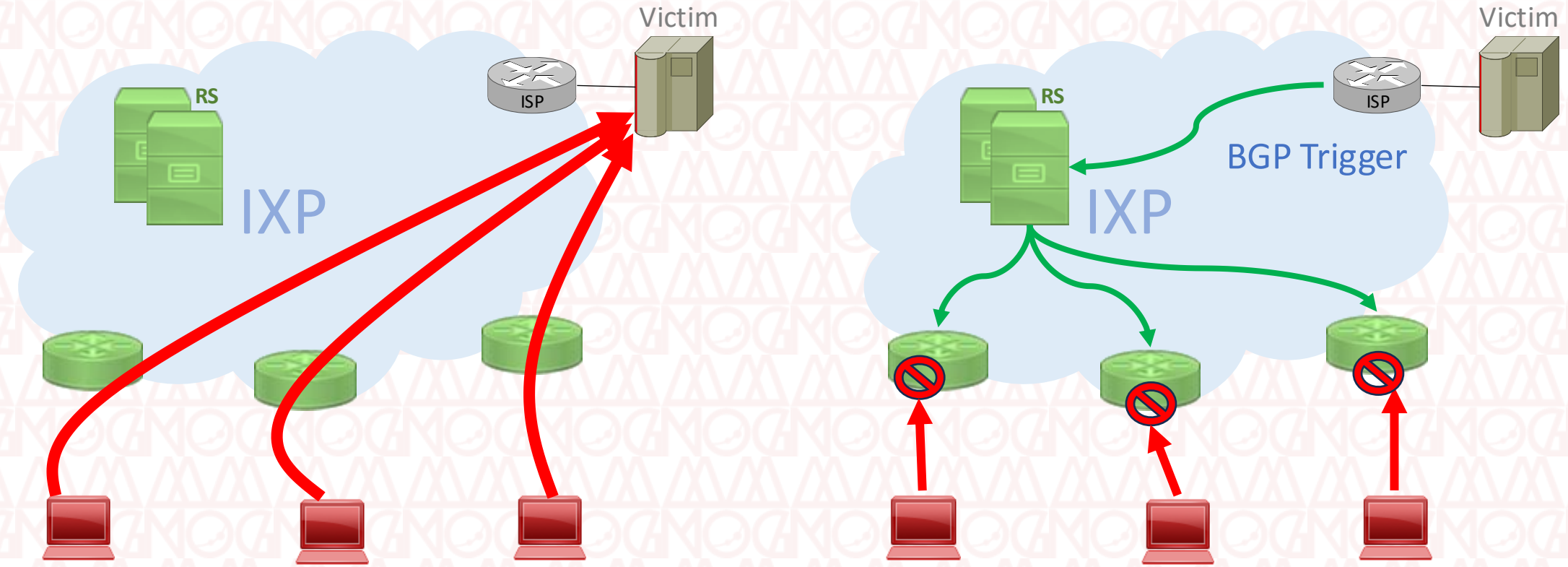
Community Method

Black Hole with IX peers

MMIX

RTBH – with an Exchange

MMIX Supports Remote Trigger, black-hole filtering (RTBH)



RTBH BGP Communities supported by MMIX

IXP	Community	Next-Hop Address	Trigger IP Size
Yangon	9654:66	103.116.194.66	/32
Mandalay	9333:66	103.116.193.66	/32

1. Prepare at Peer Machine RX1

! Activate RTBH at Peer Router Rx1. – done on previous exercise.

```
!## If there is no inbound filtering on peering session with MMIX,
! just need to configure a static null route and stop retransmission

Rx1(config)#
ip route 103.116.193.66 255.255.255.255 null 0
!
interface Null0                                  ! Done on previous exercise
 no ip unreachable
!Create Prefix, community list and inbound route-map
ip prefix-list PRF-HOST permit 0.0.0.0/0 ge 32
ip community-list standard CM-RTBH-MMIX permit 9333:66
!
```

1. Prepare at Peer Machine RX1 - Continue

```
RX1(config)#
```

```
! Modify MMIX Inbound route-map
route-map RM-MMIX-IN permit 10
 match ip address prefix-list PRF-HOST
 match community CM-RTBH-MMIX
 set community no-advertise
route-map RM-MMIX-IN permit 100
```

```
! Modify MMIX outbound route-map
route-map RM-MMIX-OUT permit 5
 match ip address prefix-list PRF-HOST
 match community CM-RTBH-MMIX
route-map RM-MMIX-OUT permit 10
 match ip address prefix-list PRF-MMIX
```

```
! Modify BGP session
router bgp 10
 neighbor 103.116.193.1 send-community
 neighbor 103.116.193.1 route-map RM-MMIX-OUT out
 neighbor 103.116.193.1 route-map RM-MMIX-IN in
```

2. Prepare for MMIX RTBH at Trigger Machine

```
RX4 (config)#
! Modify existing route-map for MMIX remote trigger.
route-map RTBH permit 93
 match tag 9333
 set local-preference 200
 set origin igp
 set community 9333:66
 set ip next-hop 192.0.2.1
```

! Be aware that no more ‘no-export’ bgp community in this route-map

3. Test Trigger for Black holes

```
! Create static routes for trigging.
Rx4(config)#
 ip route 10.0.18.93 255.255.255.255 null 0 tag 9333  ! RTBH announce to IX Peers

! Check the result
RX1#sh ip bgp nei 103.116.193.1 advertised-routes
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 10.0.18.93/32    192.0.2.1                0    200      0 i
 *>i 10.0.18.0/24     10.0.0.3                 0    100      0 i
 *>i 10.0.19.0/24     10.0.0.3                 0    100      0 i

Total number of prefixes 3
```

4

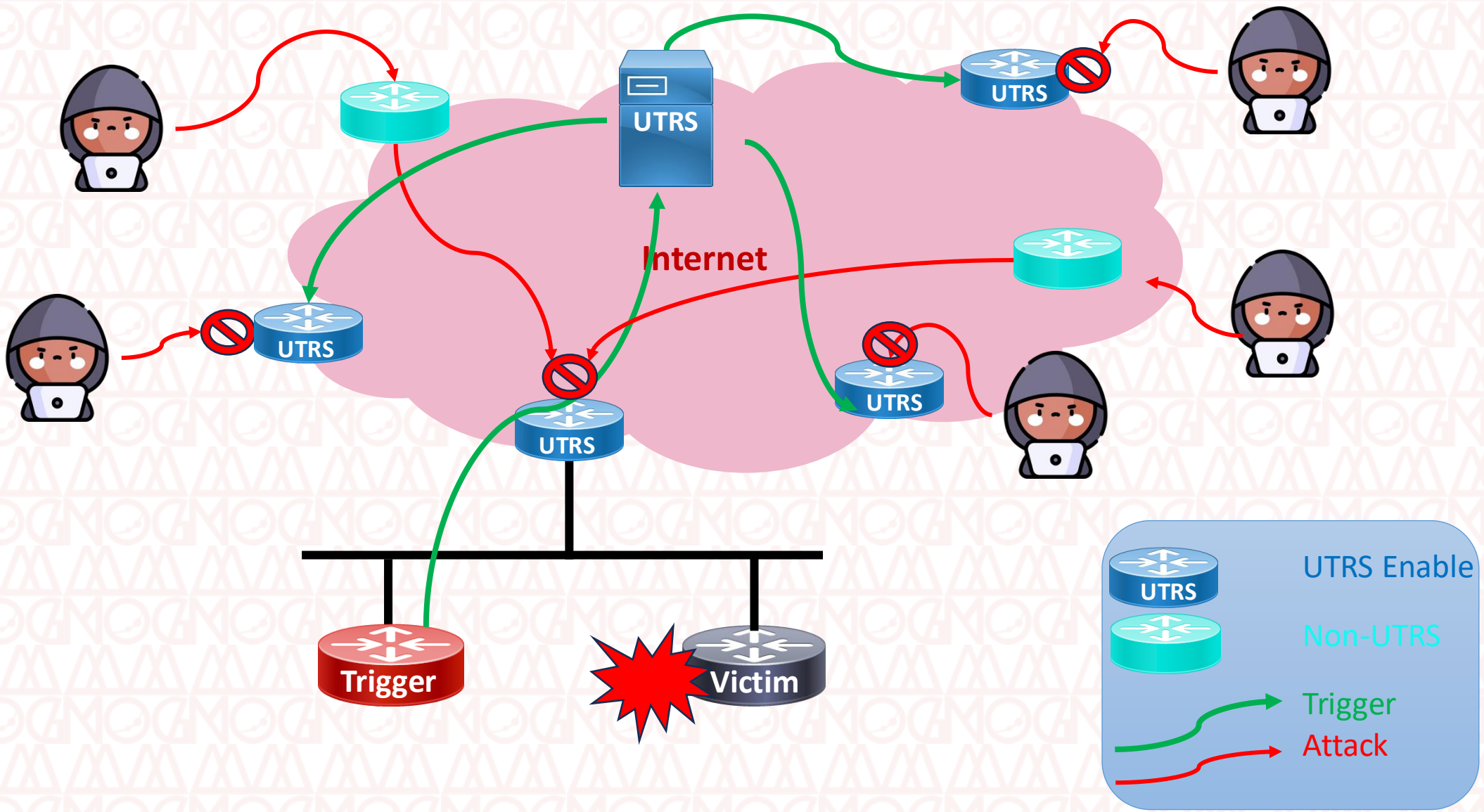
UTRS

Unwanted Traffic Removal Service

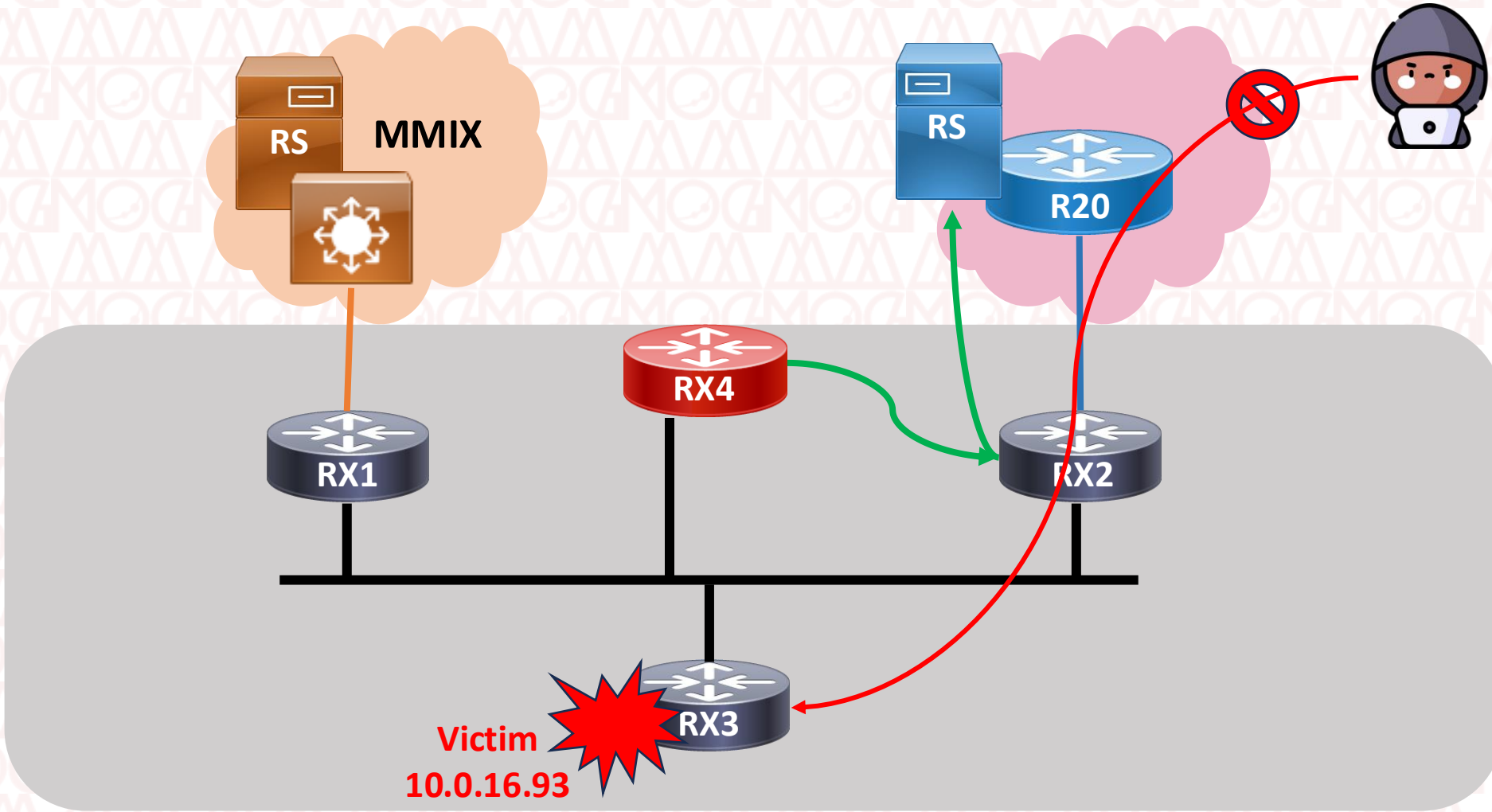
Global Back Hole

International community

UTRS Concept Topology Diagram



LAB – Global Defense



Team CYMRU's defined Parameters

- UTRS local AS number: 64496
- UTRS local addresses: [provided at provisioning]
- TCP MD5 password: [provided at provisioning]
- Next-hop: 192.0.2.1
- Community: NO_EXPORT
- Community: 64496:0
- Multi-hop
- passive

1. Configuration @RX2 (International Gateway Router)

RX2(config)#

```
ip prefix-list PRF-25 permit 0.0.0.0/0 ge 25
ip community-list standard CM-UTRS permit 64496:0
!
route-map RM-UTRS-IN permit 10
 match ip address prefix-list PRF-25
 match community CM-UTRS
 set community no-advertise
!
route-map RM-UTRS-OUT permit 10
 match ip address prefix-list PRF-25
 match community CM-UTRS
!
```

RX2(config)#

```
router bgp 10
 neighbor 172.16.0.1 remote-as 64496
 neighbor 172.16.0.1 update-source loopback 16
 neighbor 172.16.0.1 ebgp-multihop 255
 neighbor 172.16.0.1 password utrs
 neighbor 172.16.0.1  transport connection-mode passive
 neighbor 172.16.0.1 route-map RM-UTRS-OUT out
 neighbor 172.16.0.1 route-map RM-UTRS-IN in
```

Note: UTRS' RS_IP and Password are not real ones but only for this exercise.

This Lab doesn't include 'flowsec' feature supported by UTRS

2. Configuration @ RX4 (Trigger Machine)

RX4(config)#
route-map RTBH permit 96
 match tag 64496
 set local-preference 200
 set origin igp
 set community 64496:0
 set ip next-hop 192.0.2.1

3. Trigger to UTRS

```
RX4(config)# ip route 10.0.16.96 255.255.255.255 null 0 tag 64496

! After other LAB advertise, you will see the route
R12#sh ip bgp regexp ^64496_
     Network          Next Hop            Metric LocPrf Weight Path
 *>  20.0.16.96/32     192.0.2.1                              0 64496 20 i
```

5

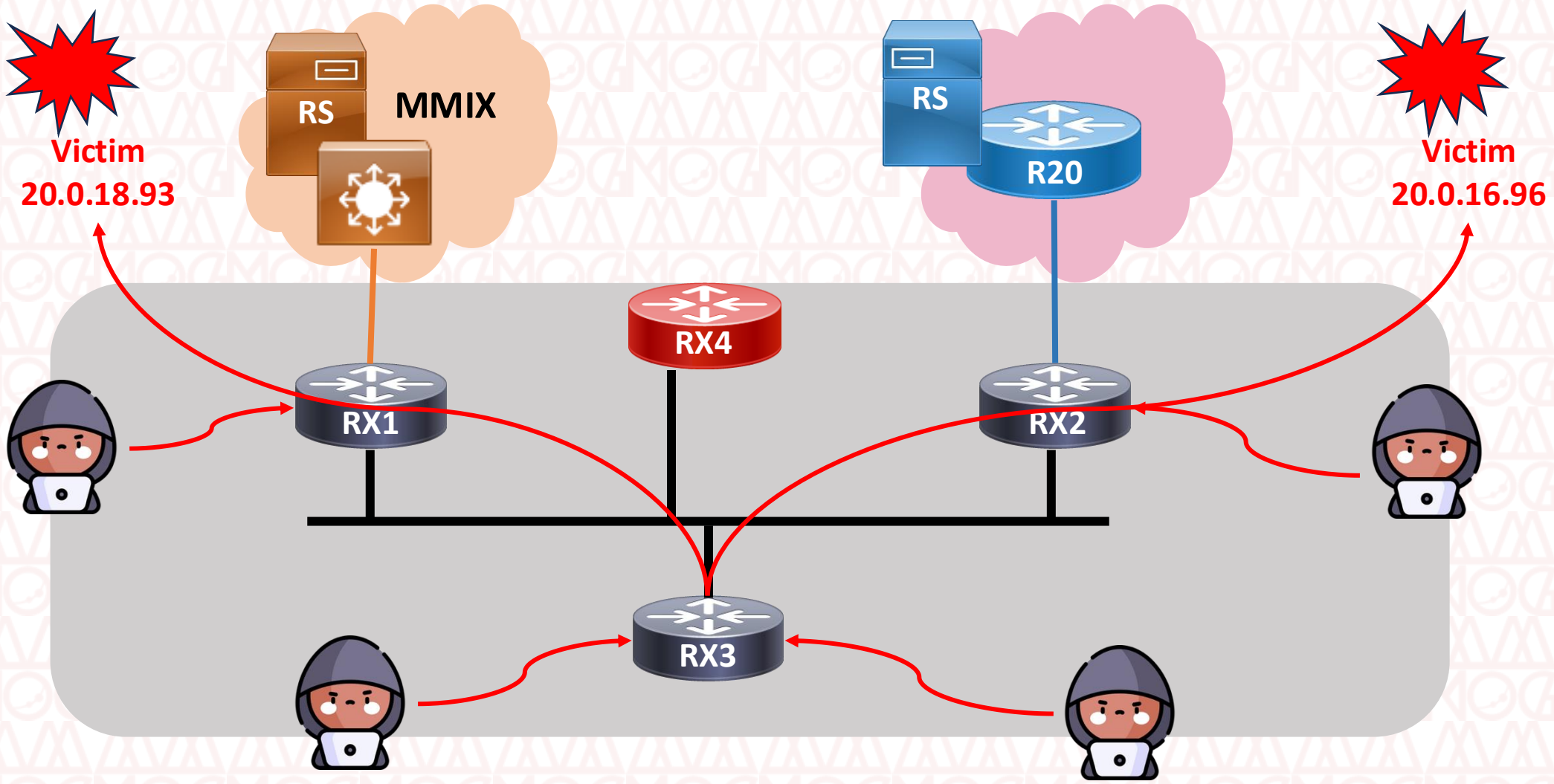
External Trigger

next-hop update

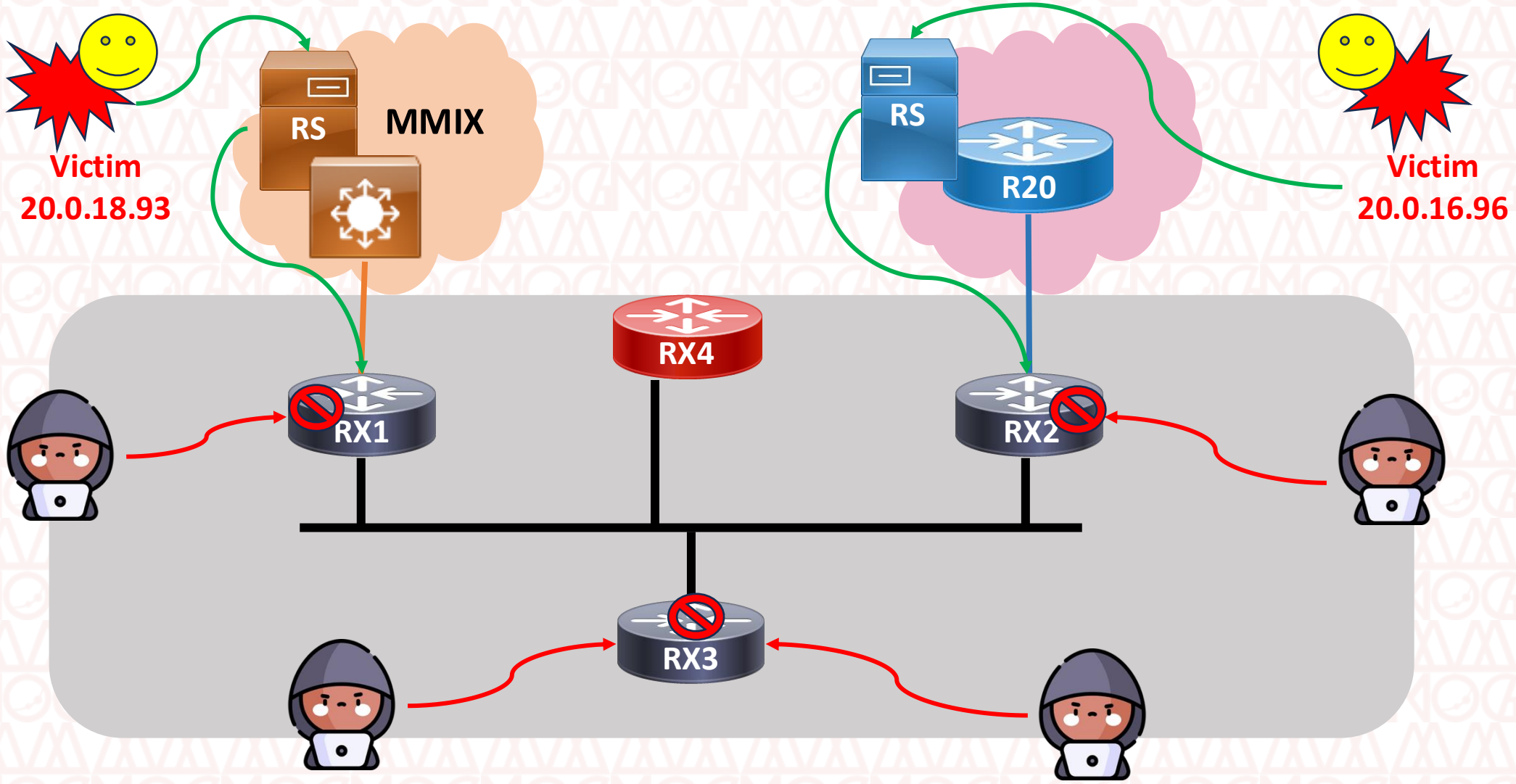
IBGP

Edge Routers defense

Attack to others from inside network



Global defense



1. Remove regional defense

```
! Exiting Config of RX1
route-map RM-MMIX-IN permit 10
 match ip address prefix-list PRF-HOST
 match community CM-RTBH-MMIX
 set community no-advertise
! Remove 'no-advertise'
route-map RM-MMIX-IN permit 10
 no set community
```

```
! Exiting Config of RX2
route-map RM-UTRS-IN permit 10
 match ip address prefix-list PRF-25
 match community CM-UTRS
 set community no-advertise
! Remove 'no-advertise'
route-map RM-UTRS-IN permit 10
 no set community
```

```
! Check Result at RX3, will notice next-hops are not null IPs.
RX3# sh ip bgp regexp _20_
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 20.0.18.93/32    10.0.0.1                 0    100      0 20 i
 *>i 20.0.16.96/32    10.0.0.2                 0    100      0 64496 20 i
! Why?  iBGP 'Next-Hop-Self'.
! Need to change next-hop for RTBH.
```

2. Exclude Trigger IPs from 'next-hop-self'

```
!Need to change next-hop
RX1(config)#
route-map RM-IBGP-OUT permit 10
 match ip address prefix-list PRF-HOST
 match community CM-RTBH-MMIX
 set ip next-hop 192.0.2.1
route-map RM-IBGP-OUT permit 100
!
router bgp 10
 neighbor IBGP route-map RM-IBGP-OUT out
```

```
!Need to change next-hop
RX2(config)#
route-map RM-IBGP-OUT permit 10
 match ip address prefix-list PRF-25
 match community CM-UTRS
 set ip next-hop 192.0.2.1
route-map RM-IBGP-OUT permit 100
!
router bgp 10
 neighbor IBGP route-map RM-IBGP-OUT out
```

! Check Result at RX3, will notice next-hops are changed.

```
R13#sh ip bgp regexp _20_
     Network          Next Hop            Metric LocPrf Weight Path
 *>i 20.0.16.0/24     10.0.0.2                 0    100      0 200 20 i
 *>i 20.0.18.93/32    192.0.2.1                0    100      0 20 i
 *>i 20.0.16.96/32    192.0.2.1                0    100      0 64496 20 i
 *>i 20.0.17.0/24     10.0.0.2                 0    100      0 200 20 i
 *>i 20.0.18.0/24     10.0.0.1                 0    100      0 20 i
 *>i 20.0.19.0/24     10.0.0.1                 0    100      0 20 i
```

6

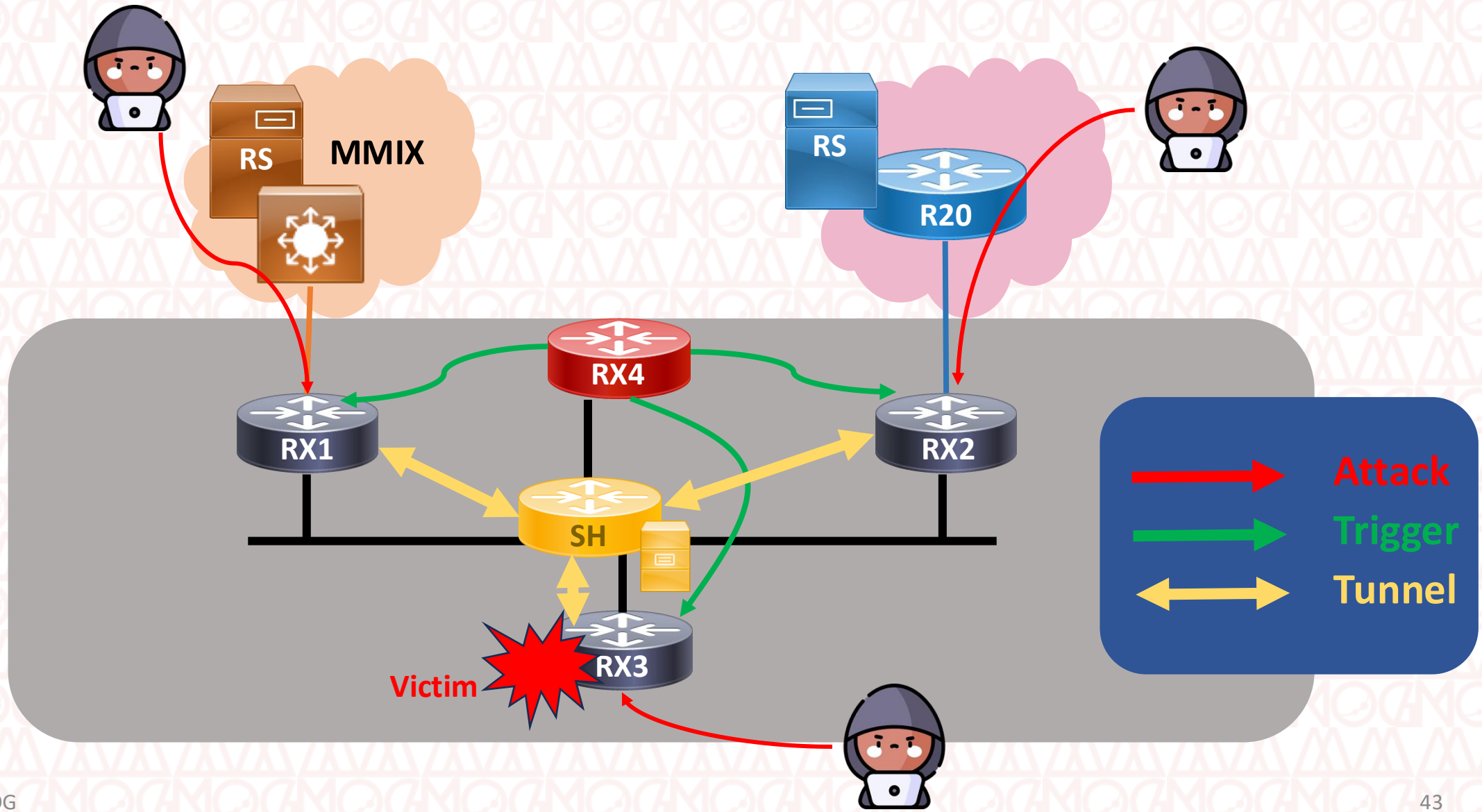
Sinkhole

Quarantine or Redirection

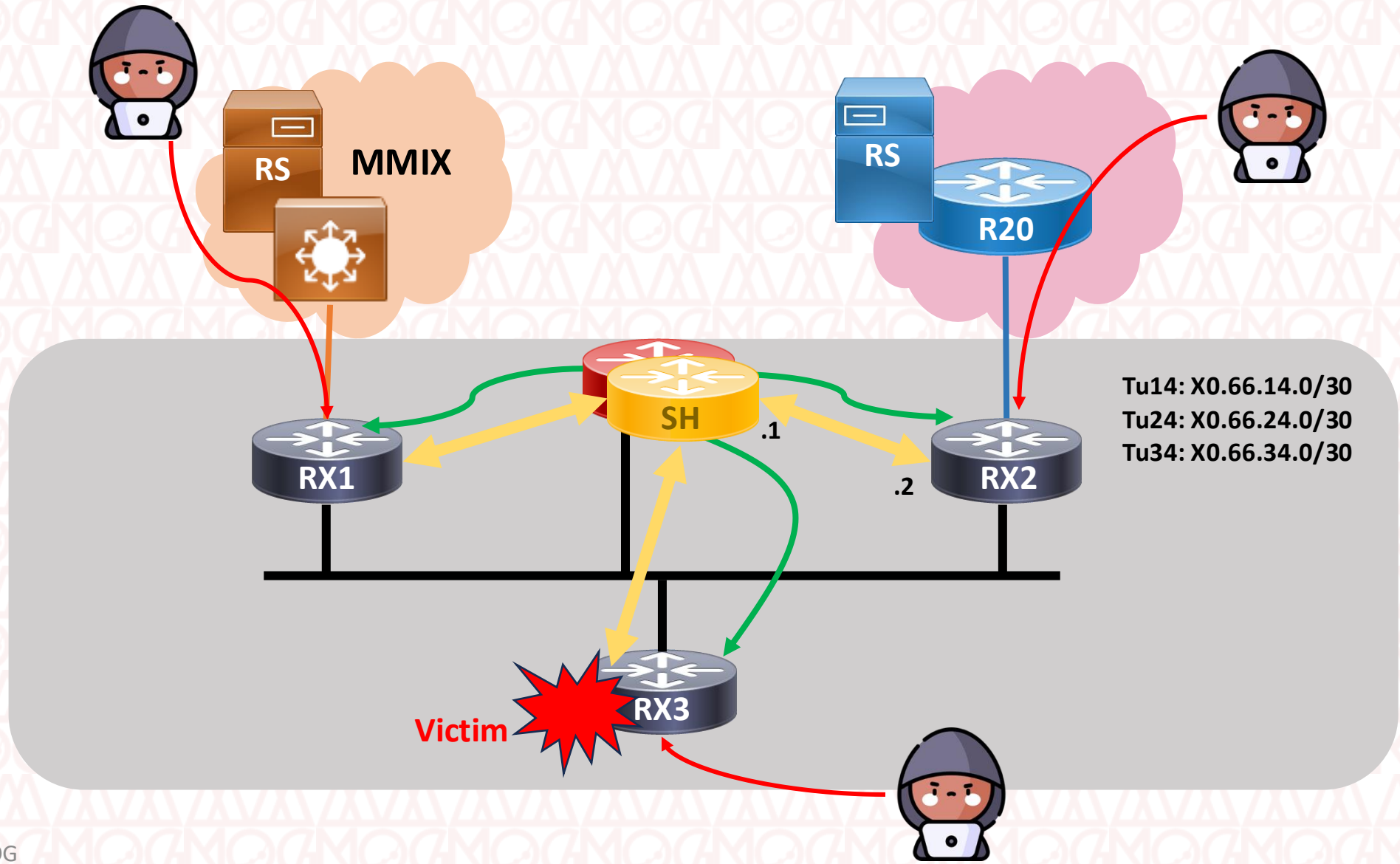
of

Attack Traffic

Sinkhole Network



Sinkhole Network - LAB



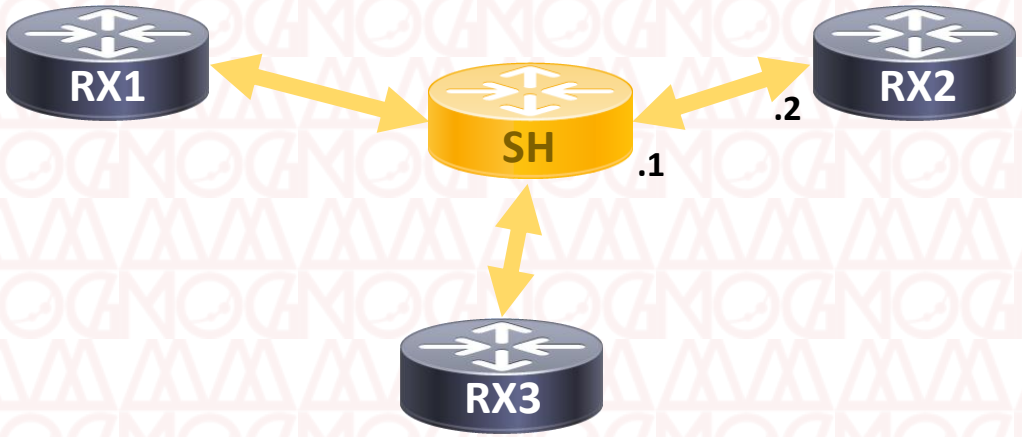
1. Setup Tunnel interfaces

```
! Tunnel interface @RX2
RX2(config)#
interface Tunnel24
 ip address 10.66.24.2 255.255.255.252
 tunnel source Loopback0
 tunnel destination 10.0.0.4
```

```
! Tunnel interface @RX4
RX4(config)#
interface Tunnel24
 ip address 10.66.24.1 255.255.255.252
 tunnel source Loopback0
 tunnel destination 10.0.0.2
```

```
! Rate limit @Rx2
RX2(config)#
rate-limit output 8000 17916 17916 conform-action transmit exceed-action drop
```

Same for Rx1 & Rx3

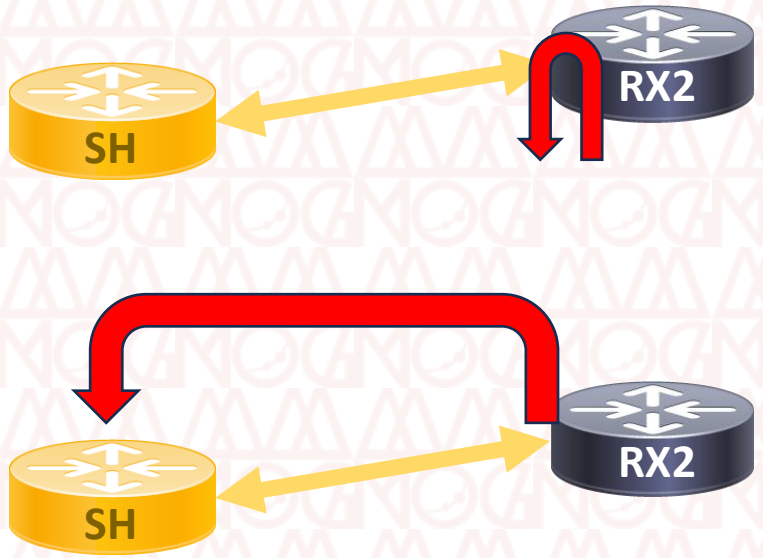


2. Next-Hop advertisement changes

```
! Existing route-map of RX4
route-map RTBH permit 62
 match tag 6602
 set local-preference 200
 set origin igp
 set community 10:6602 no-export
 set ip next-hop 192.0.2.1
```

```
! Next-hop Config after changes
route-map RTBH permit 62
 match tag 6602
 set local-preference 200
 set origin igp
 set community 10:6602 no-export
 set ip next-hop 10.66.24.1
```

```
! Next-Hop to be interface of SH
RX4(config)#
route-map RTBH permit 62
 no set ip next-hop 192.0.2.1
 set ip next-hop 10.66.24.1
```



Result

```
! Next-hop Config after changes
R12#sh ip bgp 10.0.16.62
BGP routing table entry for 10.0.16.62/32, version 174
! skipped
    192.0.2.1 from 10.0.0.4 (10.0.0.4)
      Origin IGP, metric 0, localpref 200, valid, internal, best
      Community: no-advertise
      rx pathid: 0, tx pathid: 0x0
```

```
! Next-hop Config after changes
R12#sh ip bgp 10.0.16.62
BGP routing table entry for 10.0.16.62/32, version 174
! skipped
    10.66.24.1 from 10.0.0.4 (10.0.0.4)
      Origin IGP, metric 0, localpref 200, valid, internal, best
      Community: no-advertise
      rx pathid: 0, tx pathid: 0x0
```

References & Learning

References:

Cisco White Paper :

"REMOTELY TRIGGERED BLACK HOLE FILTERING—DESTINATION BASED AND SOURCE BASED"

Team CYMRU:

"DDOS MITIGATION SERVICE – UTRS – SERVICE THREAT HUNTING"

More Learning:

Flowsec – DDOS protection for ISP

RPF – Reverse Path Forwarding

Sinkhole

Thank you

Q&A

Thein Myint Khine
theinmyintkhine@mm-ix.net

www.mmnog.net.mm

event@mm-ix.net