

ISP Network Workshop Module 3 :

Configuring the network for RTBH

Objective : To configure and test the RTBH technique in Provider network.

Pre-requisite : Module 2

RTBH (Remote Triggered Blackhole) is a technique to use BGP propagation to send specific routes to all routers in the network in order to black hole them or send them to sinkholes. We'll use the basic network built in the Module 2 for this lab.

We'll use the 'optional router' in this exercise as the Trigger Router in each Network.

1. Configure iBGP with the Trigger Router

We'll first configure all routers in the network to run iBGP with the Trigger Router. The trigger router must also be configured for iBGP with all the other routers in the same ASN.

Use examples from Module 2 for help.

2. Configure the network router with trigger

Each router in the network must be pre-configured to understand triggers sent by the trigger router. So they must be configured.

Example Configuration for R14

```
Router14(config)#ip route 192.0.2.1 255.255.255.255 Null0 254
Router14(config)#ip route 192.0.2.2 255.255.255.255 Null0 199
```

3. Configure the trigger

The trigger router is the main component in the RTBH technique. You insert specific routes into the Trigger router to propagate for action.

Example Configuration for Router 15

```
Router15(config) #router bgp 1
Router15(config-router)#redistribute static route-map static-
to-bgp
```

```
Router15(config) #^Z
```

```
Router15(config) #route-map static-to-bgp permit 10
Router15(config) #match tag 66
Router15(config) #set up next-hop 192.0.2.1
Router15(config) #set local-preference 50
Router15(config) #set community no-export
Router15(config) #set origin igp
```

! Add an empty route-map for other traffic.

```
Router15(config) #route-map static-to-bgp deny 20
Router145(config)#ip route 192.0.2.1 255.255.255.255 Null0 254
```

4. **Black holing Prefixes**

Now that the triggers are configured, you can insert routes in your network to blackhole specific routes.

Each group can blackhole these IPs, assuming that the customer routers are configured with these IP address internally.

Alpha Net	10.0.3.254
Beta Net	10.0.1.254
Charlie Net	10.0.2.254

Example for R15 in Alphanet

```
Router15(config)#ip route 10.0.3.254 255.255.255.255 Null0 tag 66
```

5. **Now you can simulate attacks across the network by sending continous ping packets.**

ISP Network Workshop Module 3.1 :
Configuring the network for RTBH using community triggers