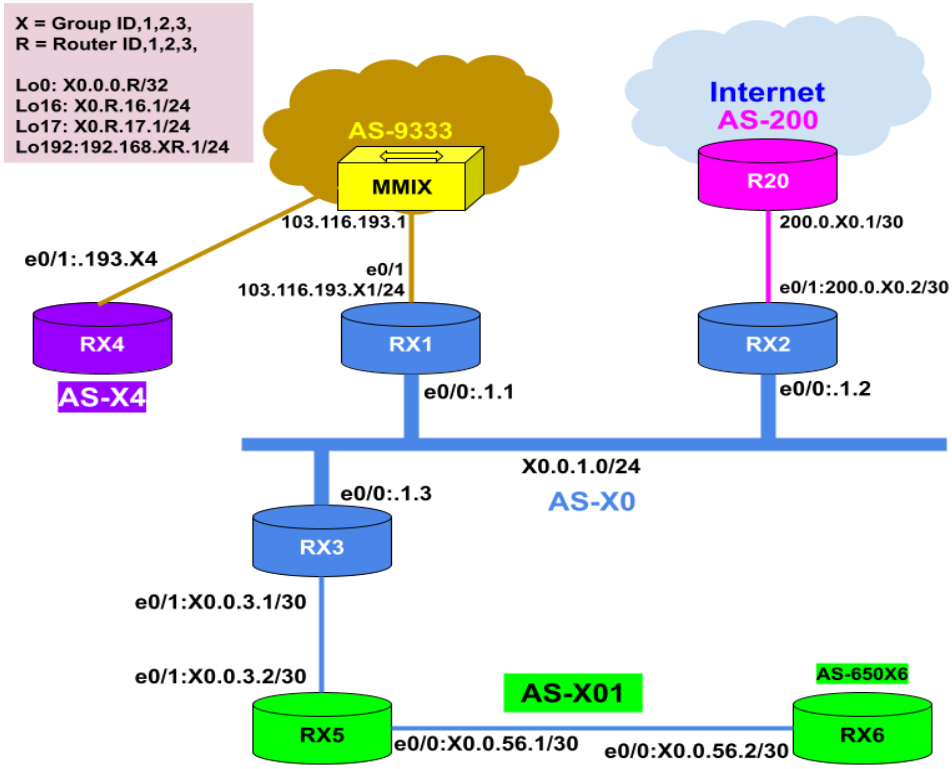
LAB - BGP - Network Security



For your exercise, please refer to the above diagram.

Topology:

Blue ISP with ASX0 is connecting to MMIX and its upstream provider AS200. Green ISP with ASX01 is its downstream. All routers already configured necessary IGP and basic BGP, including route announcement.

In every router, Lo16, Lo17, Lo192 are supposed to be Clients' Prefixes.

MMIX is supporting RTBH (Remote Trigger Black Holding) features with the following parameters.

BGP Community: 9333:66

Next hop address: 103.116.193.66

trigger IP size: /32

Exercise

Configure to meet the following requirements.

1. Check configuration and ping test link IP addresses. Check also OSPF routes, BGP sessions and BGP routes.
2. Activate RTBH at Peer Router Rx1.
3. Considering Rx3, IP X0.3.16.1 is under attack by some MMIX networks, trigger RTBH using the features supported by MMIX.
4. For ASX0 Blue ISP, create inbound filters for
    a. Private IP addresses
    b. Longer prefix length
    c. Default gateway
5. Filter Private ASNs: At Rx2, do not accept Private ASN via AS-200.
6. Outbound Filter: Just advertised prefixes of your owned and downstream.
    - At Rx1, advertise prefixes of AS-X0 and AS-X01 to AS-9333 (MMIX)
    - At Rx2, advertise prefixes of AS-X0 and AS-X01 to AS-200 (Internet)
7. Remove Private AS from AS-X01
8. No default-GW at Peer Router. Filter default gateway at Rx1.
9. Don’t receive owned and downstream prefixes from Global.
    - At Rx2, filter prefixes of AS-X0 and AS-X01 received from global.
10. Null route for unused IP addresses. Also, black IPs.