CSE hands-on-4

1.

BGP，即边界网关协议，是运行在 TCP 上的一个协议，他实现自治系统之间的路由可达，并会选择最佳路由的一个矢量性协议。

BGP 主要作用是与其他 BGP 系统交换网络可达信息，这些信息会包含每个自治系统(AS)的信息，这些信息有效地构造了自治系统互联的拓扑图，并由此清除了路由环路，同时有利于在自治系统级别上实施策略决策。

2.

Disable 后接收到的 packet 信息：

```
IP (tos 0xc0, ttl 1, id 33761, offset 0, flags [DF], p
    10.103.0.3.179 > 10.103.0.162.57911: Flags [P.], cksum 0x1607 (incorrect ->
0xf5fa), seq 1490:1600, ack 855, win 509, options [nop,nop,TS val 3055918519 ecr
 2523927555], length 110: BGP
        Update Message (2), length: 110
          Origin (1), length: 1, Flags [T]: IGP
            0x0000:  00
          AS Path (2), length: 18, Flags [T]: 3 2 12 164
            0x0000:  0204 0000 0003 0000 0002 0000 000c 0000
            0x0010:  00a4
          Next Hop (3), length: 4, Flags [T]: 10.103.0.3
            0x0000:  0a67 0003
          Large Community (32), length: 48, Flags [OT]:
            2:1:0, 3:2:0, 12:1:0, 164:0:0
          Updated routes:
```

```
IP (tos 0xc0, ttl 1, id 58741, offset 0, flags [DF], proto TCP (6), length 79)
    10.103.0.3.179 > 10.103.0.162.54797: Flags [P.], cksum 0x15b4 (incorrect ->
0x9b00), seq 6686:6713, ack 77, win 509, options [nop,nop,TS val 1578515199 ecr
3383929823], length 27: BGP
        Update Message (2), length: 27
          Withdrawn routes: 4 bytes
```

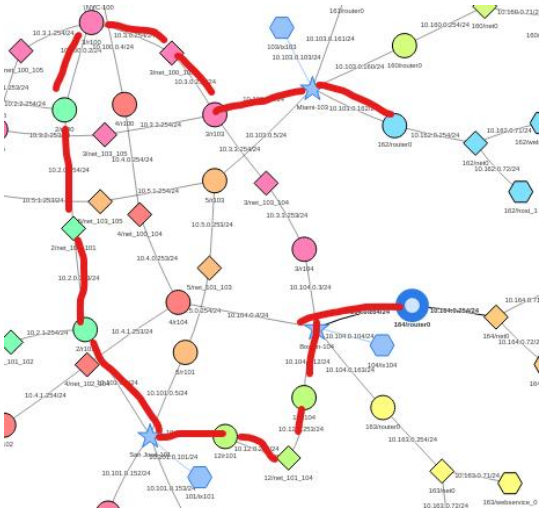
162 为何会接受到这个 packet：因为 164 节点与 as12 之间的连接丢失会影响到节点 162。同时节点 162 能够接收 as3 的消息，而节点 164 的 update message 会发送给节点 12，之后由于节点 12 还连接了其他节点，所以节点 12 会进行消息的广播。节点 12 有一条到达节点 3 的路由路径，将 update message 给节点 162，节点 162 发现 164-12 的路径的断开对自己有影响，所以更新 route table。所以节点 162 能够接受到第一个 new packet。而对于第二个 packet，是由于 164-12 的连接已经断开，所以 as12 会向节点 as162 发送一个新的 packet，来通知节点 as162 虽然新的最短路径已经生成，但是不会真正到达节点 as164，所以会发送这个 withdraw packet。

这个 packet 是如何发送给 162 的：节点 164 的 update message 会先到达图中的 exchange：boston-104，通过这个中转站广播给节点 12，之后沿着 as path 中提供的路径开始传播，最终到达节点 as 3，之后到达节点 162。

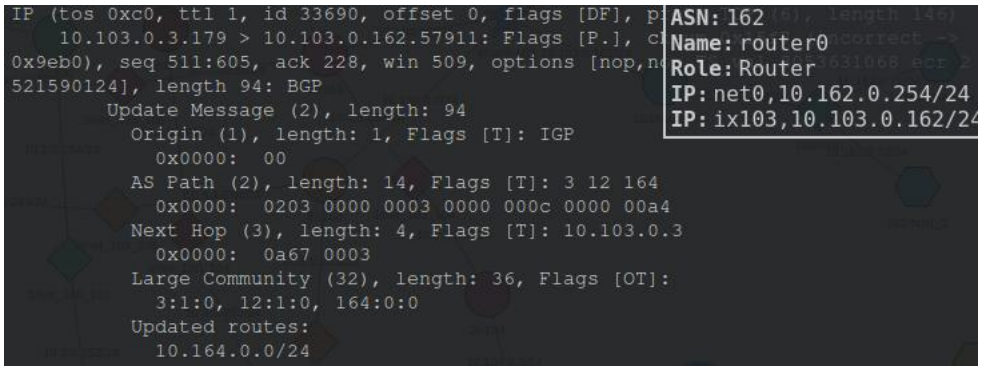
3.

AS Path 指的是一个 update meeage 在发送过程中经过了哪些 AS 路径，并会按照一定顺序记录从本地到目标地址经过的所有 AS 编号。

路径截图：



4.



162 为何会接受到 new packet：因为 164 节点与 as12 之间的连接丢失会影响到节点 162。同时节点 162 能够接收 as3 的消息，而节点 164 的 update message 会发送给节点 12，之后由于节点 12 还连接了其他节点，所以节点 12 会进行消息的广播。节点 12 有一条到达节点 3 的路由路径，将 update message 给节点 162，节点 162 发现 164-12 的路径的断开对自己有影响，所以更新 route table。所以节点 162 能够接受到 new packet。

新的 packet 是如何发送到节点 162 去的：节点 164 的 update message 会先到达图中的 exchange：boston-104，通过这个中转站广播给节点 12，之后沿着 as path 中提供的路径开始传播，最终到达节点 as 3，之后到达节点 162。

5.

没有接受到 new packet。

原因：因为 as150 与 as151 之间的连接中断对于节点 as162 到达节点 as151 的路由路径不会产生影响，所以节点 162 就不会接受到新的 update message。

6.

在节点 as153 进行 hijack 之后，由于对于相同的 IP 10.154.0.0，节点 153 的提供的掩码长度更长，则根据 BGP 的最长前缀匹配规则，可以知道会优先选择节点 as153 作为目标。同时 as153 向外发送 update message，节点 as160 在接收到这个消息的时候发现现在连接 10.154.0.0 的路由路径变得更短，所以就会把访问对应网络的路由路径重定向到节点 as153 处，所以成功实施了 hijack。

7.

由于原来的 as154 节点使用的是 24 位的掩码，只有使用比他更长的掩码才能够使得 BGP 将 as153 作为消息发送的目的地，所以至少要使用 25 位掩码。

可以使用 10.154.0.0/24，因为当 as153 节点使用 10.154.0.0/24 的时候，则 BGP 会发现两个相同的目的地。这时候会选择路径较短的一个作为最终的目的地。而在这个例子中，as160 到 as153 的路由距离小于 as160 到 as154 的路由距离，所以还是会选择 as153 作为最终目标。**不可以使用 10.154.0.0/23**，因为使用 23 掩码的时候，由于 as154 节点的掩码位数为 24 位，那么 BGP 会根据最长前缀匹配规则选择 as154 作为目的地而不是 as153。

8.

在 as153 断开连接之后，会向外发送新的 update message，这时候根据最长前缀匹配规则可以知道 10.154.0.0 只剩下 as154 一个目的地了，所以节点 as160 发现找到对应 ip 的路由路径改变了，会更新 route table，所以又重新连接到了 as154 节点。

9.

可以使得节点 as160 通过匹配长度比 25 位更长的掩码长度来拒绝掉 as153，因为掩码长度的优先级高于路径长度的优先级。**所以可以通过将 as154 节点的掩码位数修改为 26 位来进行防御**。