CSE hands-on-4

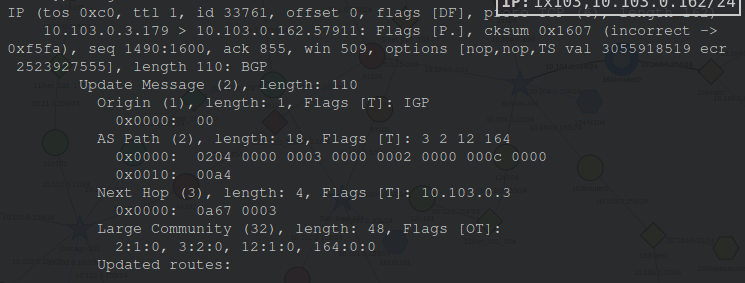
1.

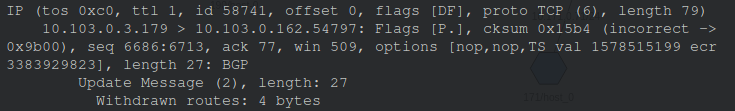
BGP，即边界网关协议，是运行在TCP上的一个协议，他实现自治系统之间的路由可达，并会选择最佳路由的一个矢量性协议。

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**：





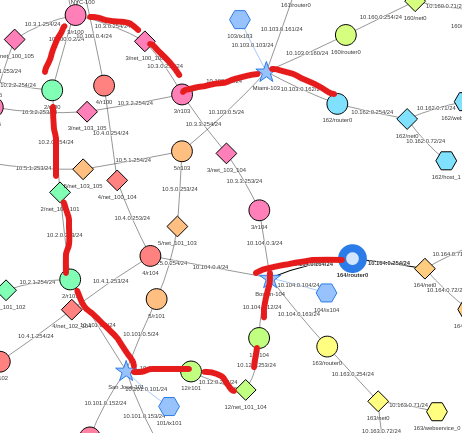
**162为何会接受到这个packet**：因为164节点与as12之间的连接丢失会影响到节点162。同时节点162能够接收as3的消息，而节点164的update message会发送给节点12，之后由于节点12还连接了其他节点，所以节点12会进行消息的广播。节点12有一条到达节点3的路由路径，将update message给节点162，节点162发现164-12的路径的断开对自己有影响，所以更新route table。所以节点162能够接受到第一个new packet。而对于第二个packet，是由于164-12的连接已经断开，所以as12会向节点as162发送一个新的packet，来通知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

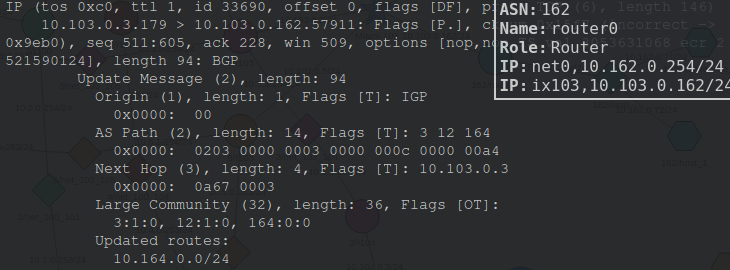
3.

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**。