《计算机网络实验》实验报告

实验名称: **动态路由协议 RIP，OSPF 和 BGP 观察**

姓名：胡育玮

学号：171860574

邮箱：yeevee@qq.com

班级：17 级计算机科学与技术系 2 班

一、实验目的

1、了解 RIP，OSPF 和 BGP 协议

2、理解自治系统

3、通过实验理解路由选择算法

二、网络拓扑配置

（1）表格：

节点名	虚拟设备名	IP 地址	netmask
Router0	U-571-Router0	eth0: 192.168.0.1	255.255.255.0
		eth1: 192.168.6.1	255.255.255.0
Router1	U-572-Router1	eth0: 192.168.0.2	255.255.255.0
		eth1: 192.168.1.1	255.255.255.0
Router2	U-573-Router2	Eth0: 192.168.2.1	255.255.255.0
		Eth1: 192.168.1.2	255.255.255.0
Router3	U-576-Router3	Eth0: 192.168.2.2	255.255.255.0
		Eth1: 192.168.3.3	255.255.255.0

		Eth2: 192.168.6.2	255.255.255.0
Router4	U-579-Router4	Eth0: 192.168.4.4	255.255.255.0
		Eth1: 192.168.3.4	255.255.255.0
Router5	U-580-Router5	Eth0: 192.168.4.5	255.255.255.0
		Eth1: 192.168.5.5	255.255.255.0
Router6	U-581-Router6	Eth0: 192.168.5.6	255.255.255.0

三、路由配置文件

Zebra.conf：所有 router 均采用“sudo ifconfig eth1 192.168.5.5 netmask 255.255.255.0”这样的指令设置好 IP 地址后再使用

sudo cp /usr/share/doc/quagga/examples/zebra.conf.sample /etc/quagga/zebra.conf

这条指令来复制模板 zebra.conf 文件，故所有 router 的 zebra.conf 都是下面这样的：

zebra.conf

```
! -*- zebra -*-
!
! zebra sample configuration file
!
! $Id: zebra.conf.sample,v 1.1 2002/12/13 20:15:30 paul Exp $
!
hostname Router
password zebra
enable password zebra
!
! Interface's description.
!
!interface lo
! description test of desc.
!
!interface sit0
! multicast

!
! Static default route sample.
!
!ip route 0.0.0.0/0 203.181.89.241
!

!log file /var/log/quagga/zebra.log
```

ripd.conf:

router0:

ripd.conf

```
!-*-rip-*-
hostname ripd
password zebra
router rip
network eth0
network eth1
log stdout
!
```

router3:

ripd.conf

```
!-*-rip-*-
hostname ripd
password zebra
router rip
network eth0
network eth2
log stdout
!
```

ospfd.conf:

router4:

router6:

ospfd.conf

```
!-*-ospf-*-
hostname ospfd
password zebra
router ospf
  network 192.168.4.0/24 area 0
log stdout
!
```

ospfd.conf

```
!-*-ospf-*-
hostname ospfd
password zebra
router ospf
  network 192.168.5.0/24 area 0
log stdout
!
```

Bgpd.conf:

Router3:

bgpd.conf

```
!-*-bgp-*-
hostname bgpd
password zebra
router bgp 30
bgp router-id 192.168.3.3
network 192.168.0.0/24
network 192.168.1.0/24
network 192.168.2.0/24
neighbor 192.168.3.4 remote-as 40
log stdout
!
```

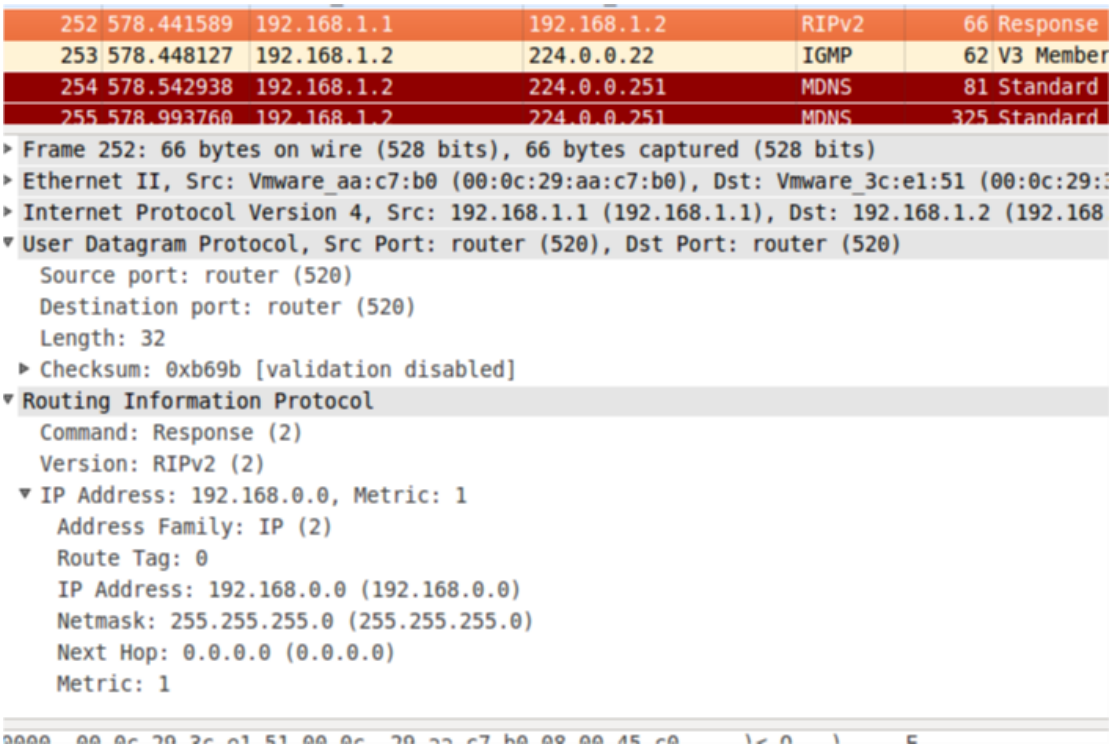
router4:

bgpd.conf

```
!-*-bgp-*-
hostname bgpd
password zebra
router bgp 40
bgp router-id 192.168.3.4
network 192.168.4.0/24
network 192.168.5.0/24
neighbor 192.168.3.3 remote-as 30
log stdout
!
```

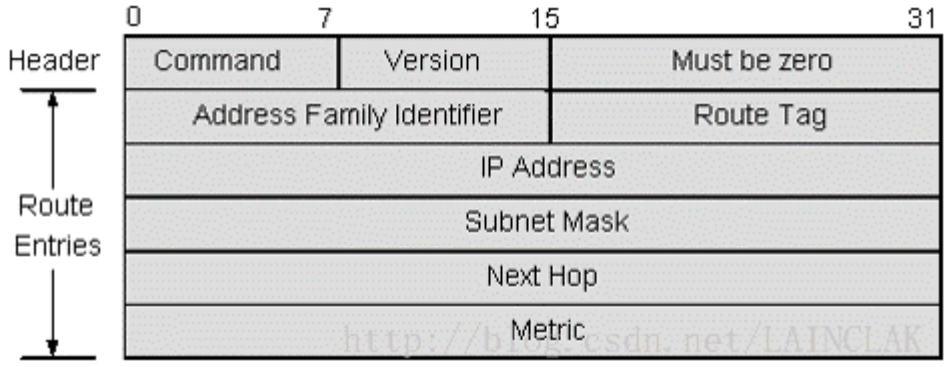
四、数据包截图和协议报文分析

（1）RIP 协议报文



上图为 router2 eth1 抓取的 RIPv2 response 包。

RIPv2 协议的字段：



Command：表明是 response 还是 request. 取值 1 或 2，当取值为 1 时表示该消息为请求消息；当取值为 2 时表示该消息为响应消息。

Version：当取值为 1 时表示该消息为 RIPv1 消息；当取值为 2 时表示该消息为 RIPv2 消息

Address Family Identity：对于 IPv4 协议，该字段取值为 2。当该消息是对整张路由表的请求消息时，该字段取值为 0。

Route Tag：用于标记外部路由或者路由引入到 RIPv2 协议中的路由。

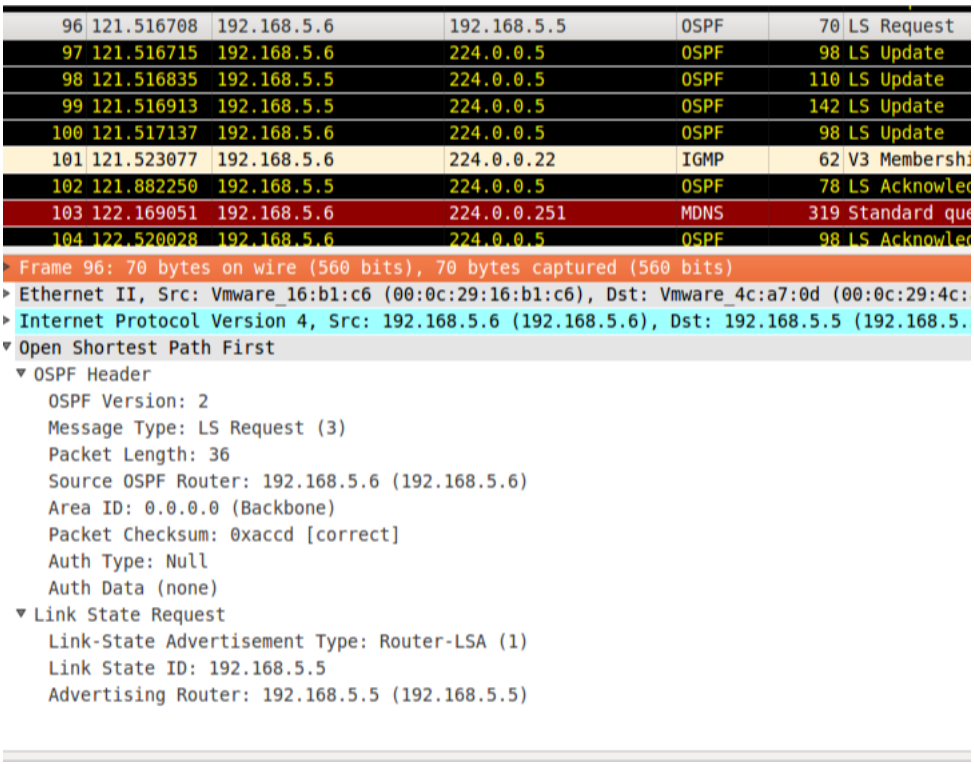
IP Address：该字段表示路由的目的地址

Subnet Mask：用来标识使用 IPv4 地址的网络的掩码

NextHop：表示比通告路由器地址更好的下一跳地址。如果该字段为 0.0.0.0，**则说明通告路由器地址为最优下一跳地址。**

Metric：该字段是指 RIP 中的跳数。在 RIP 中，该字段的取值范围为 1-16

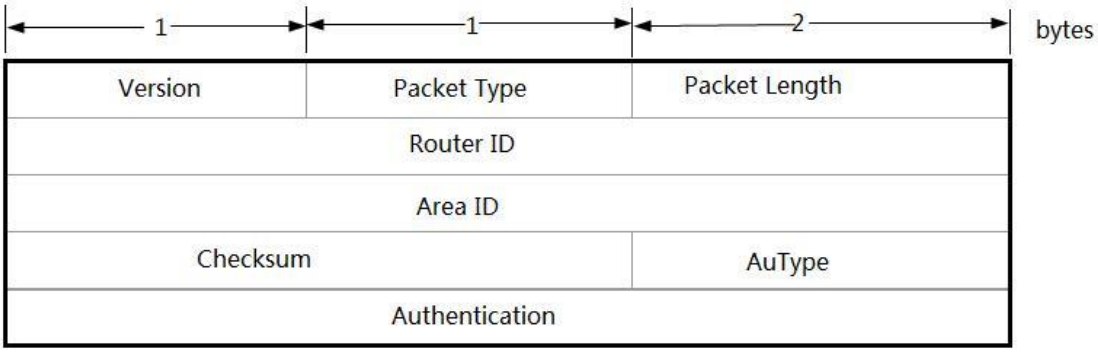
（2）OSPF 协议报文



上图为 router5 eth1 抓取的 OSPF LS request 报文。

OSPF 报文主要有 5 种：Hello 报文、DD （Database Description，数据库描述）报文、LSR （LinkState Request，链路状态请求）报文、LSU（LinkState Update，链路状态更新）报文和 LSAck（LinkState Acknowledgment，链路状态应答）报文。它们各自在 OSPF 路由更新中所担当的用途不一样，报文格式也存在比较大的差别。

OSPF 报文封装在为 IP 报文里。以上所说到的五种 OSPF 报文使用相同的 OSPF 报头格式：



上图为 OSPF 报头格式。

Version: 版本字段，占 1 个字节，指出所采用的 OSPF 协议版本号，目前最高版本为 OSPF v4，即值为 4。

Packet Type：报文类型字段，标识对应报文的类型。

Packet Length：包长度字段，占 2 个字节。它是指整个报文（包括 OSPF 报头部分和后面各报文内容部分）的字节长度。

Router ID：路由器 ID 字段，占 4 个字节，指定发送报文的源路由器 ID。

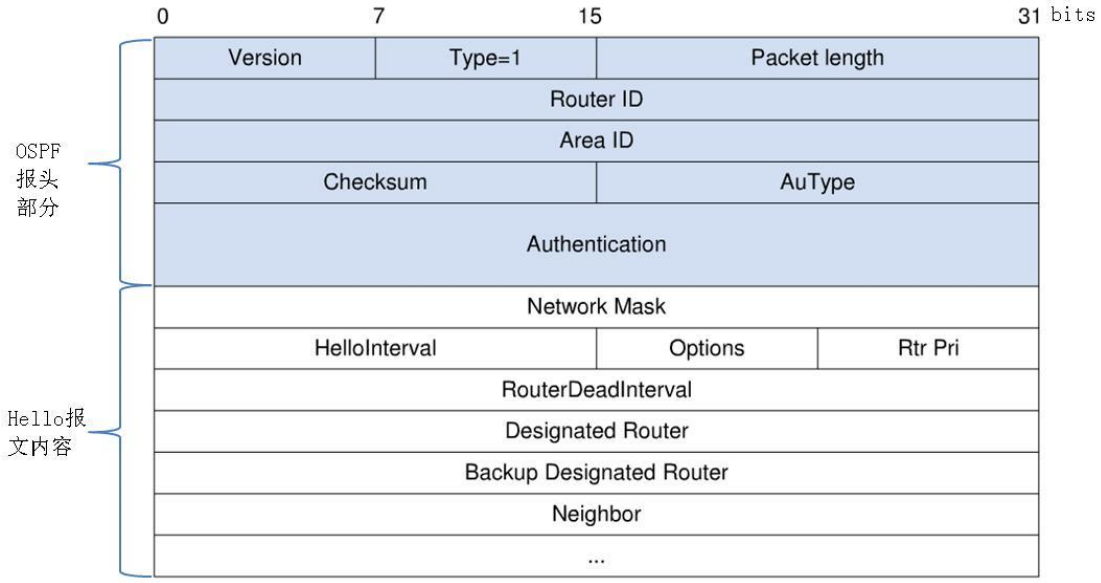
Area ID：区域 ID 字段，占 4 个字节，指定发送报文的路由器所对应的 OSPF 区域号。

Checksum：校验和字段，占 2 个字节，是对整个报文（包括 OSPF 报头和各报文具体内容，**但不包括下面的 Authentication 字段**）的校验和。

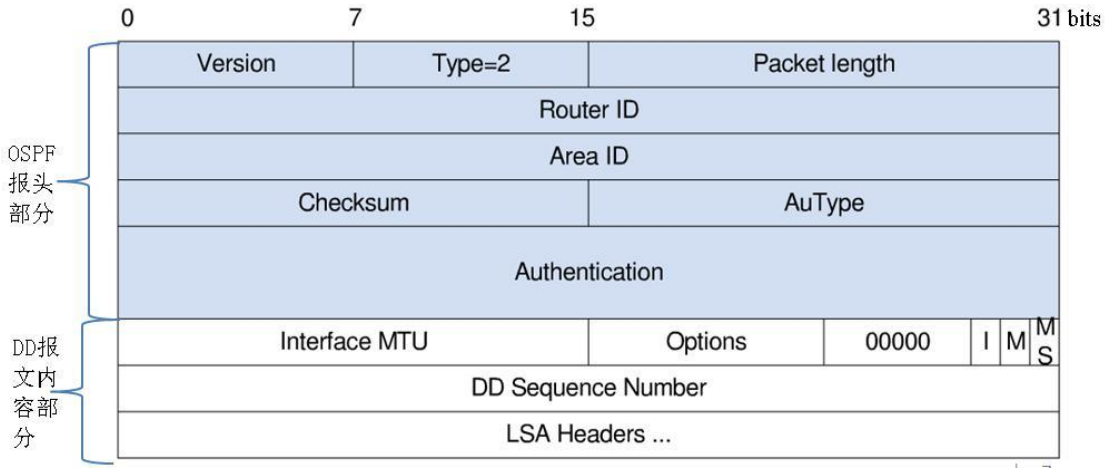
AuType：认证类型字段，占 2 个字节，指定所采用的认证类型，0 为不认证，1 为进行简单认证，2 采用 MD5 方式认证。

Authentication：认证字段，占 8 个字节，具体值根据不同认证类型而定：认证类型为不认证时，此字段没有数据，认证类型为简单认证时，此字段为认证密码，认证类型为 MD5 认证时，此字段为 MD5 摘要消息。

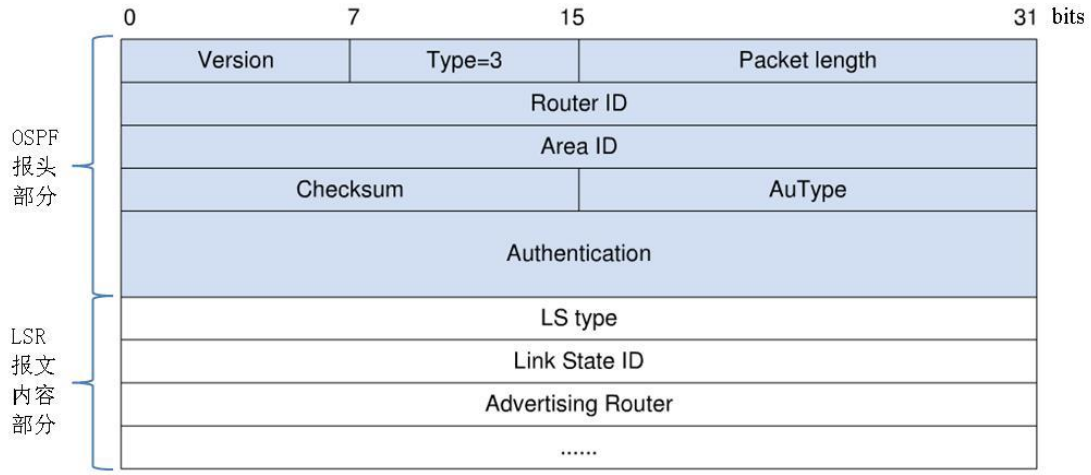
Hello 报文：



DD 报文：



LSR 报文：也即上面给出的 router5 抓取的报文：

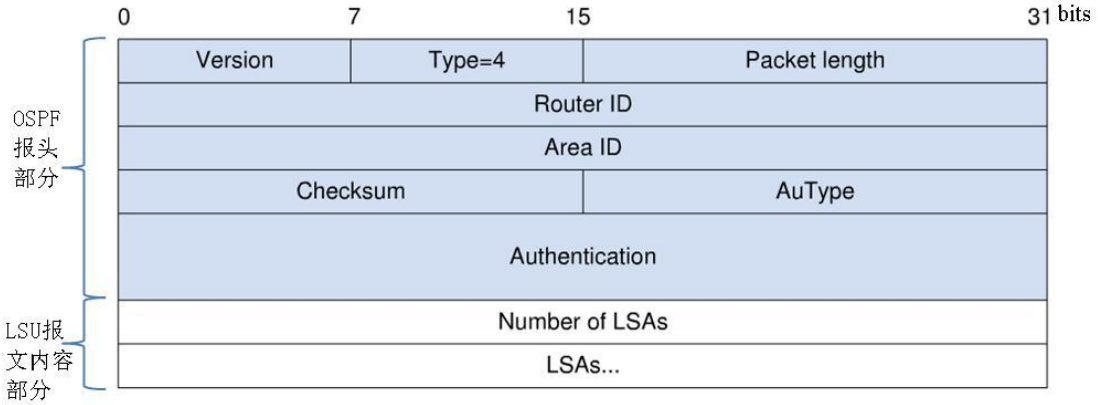


LSR 报文用于请求相邻路由器链路状态数据库中的一部分数据。当两台路由器互相交换完 DD 报文后，知道对端路由器有哪些 LSA 是本 LSDB 所没有的，以及哪些 LSA 是已经失效的，则需要发送一个 LSR 报文，向对方请求所需的 LSA。

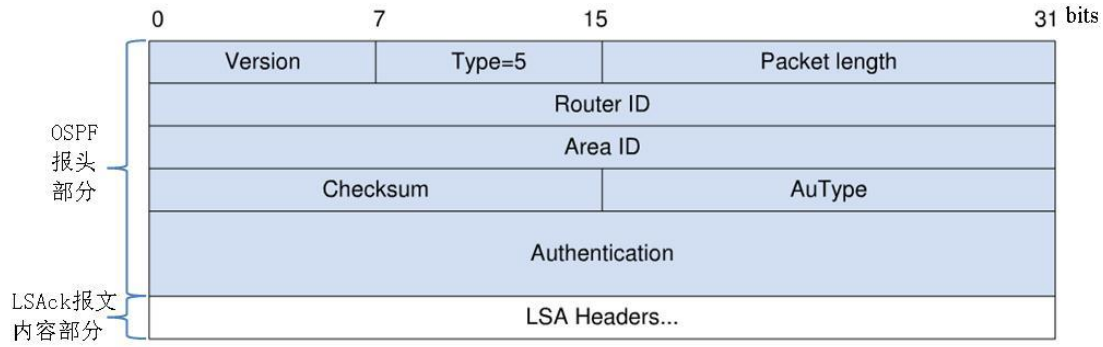
LSR 报文内容包括所需的 LSA 摘要。LSR 报文内容部分各字段说明：

字段名	长度	功能
LS type	4字节	指定所请求的LSA类型，主要共7类，具体参见9.2.5节
Link State ID	4字节	用于指定ospf所描述的部分区域，该字段的使用方法根据不同的LSA类型而不同：当为LSA 1时，该字段值是产生LSA 1的路由器的Router-ID，当为LSA 2时，该字段值是DR的接口地址，当为LSA 3时，该字段值是目的网络的网络地址，当为LSA 4时，该字段值是ASBR的Router-ID，当为LSA 5时，该字段值是目的网络的网络地址
Advertising Router	4字节	指定产生此所要请求的LSA的路由器ID

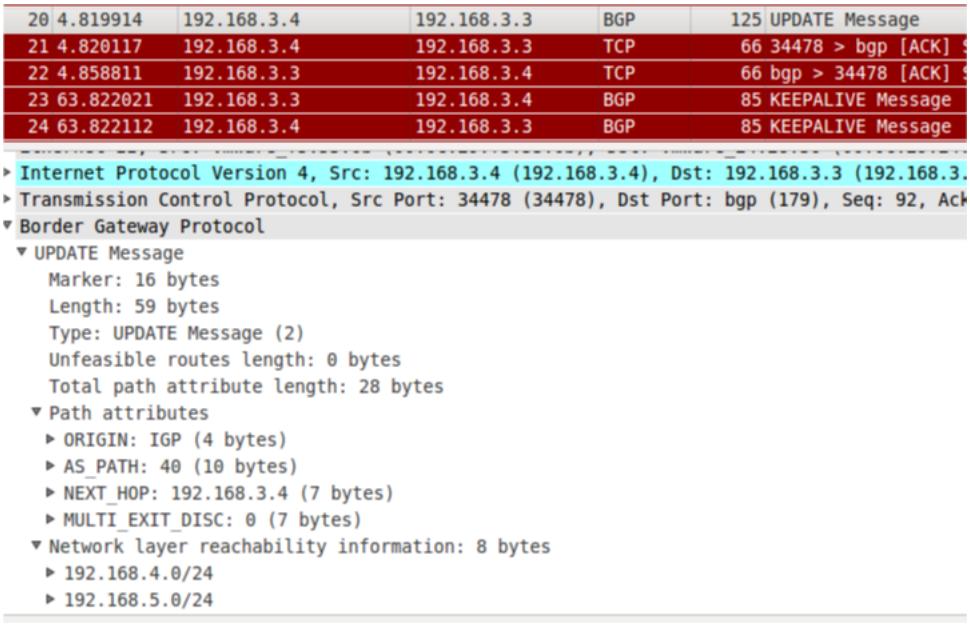
LSU 报文:



LSAck 报文：



（3）BGP 协议报文



上图为 router3 eth1 抓取的 BGP update 报文。

BGP 是建立在 TCP 之上的协议，端口号是 179，共有 4 种报文类型：

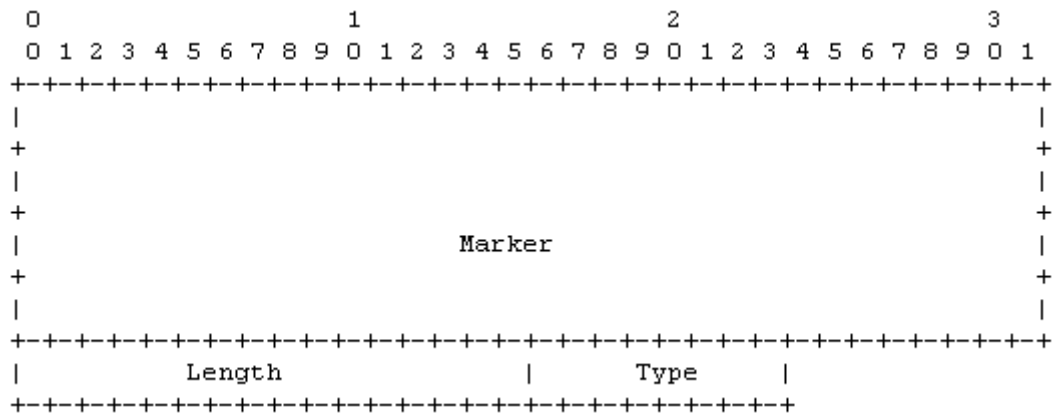
1:open(打开消息)

2:keepalive(存活消息)

3:update(更新消息)

4:notification(报错消息)

BGP 包头格式：



Maker(16 字节)——全为 1，标识 BGP 报文边界

Length(2 字节)——BGP 包全长，长度的值最少 19 字节，最大 4096 字节。

Type(1 字节)—

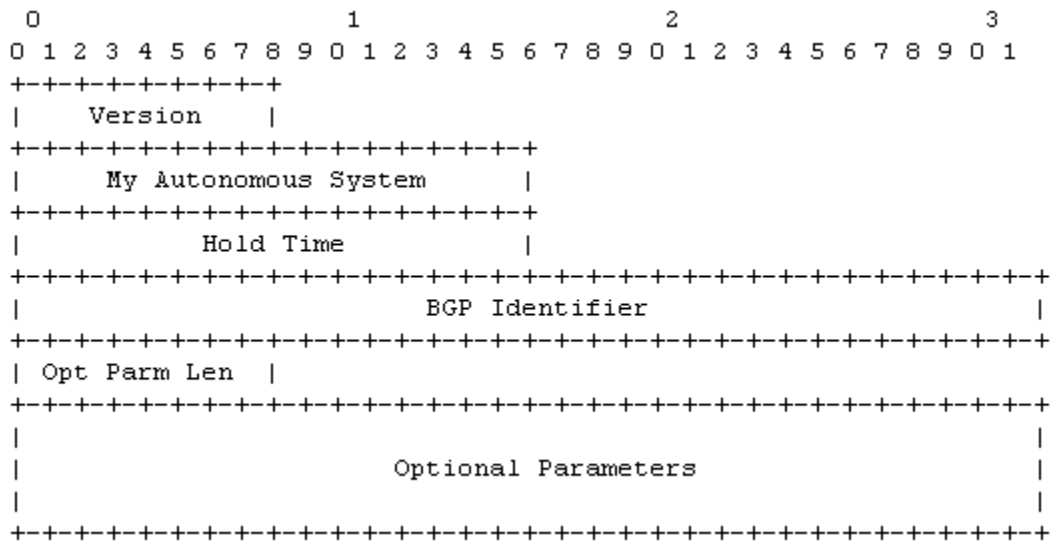
1 - OPEN

2 - UPDATE

3 - NOTIFICATION

4 – KEEPALIVE

OPEN 报文：



Version(1 字节)—﹣当前的 BGP 版本号为 4

My Autonomous System（2 字节）—发送者自制系统号

Hold Time（2 字节）—BGP hold time 默认为 180 秒。如果 180 秒内，没有收到 keepalive 消息，则删除 bgp 邻居。

BGP Identifier（4 字节）—发送者的 BGP router-ID.

Optional Parameters Length（可选参数长度）（1 字节）:如果这个域是 0，说明没有可选参数。

Optional Parameters（可选参数）:这里总长度是和 Optional Parameters Length 指定的值是一致的。

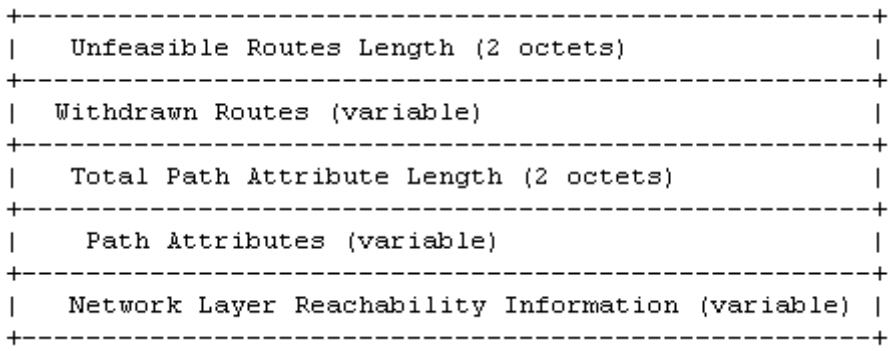
keepalive 报文：

该报文比较简单，只有 BGP 的固定头。默认每 60 秒发送一次，对等体收到后，会更新保活消息计时，如果联系三

次发送的消息，都没到达对等体，对方则删除 bgp 邻居。

建立邻居时，BGP 先尝试与对等体建立一个 TCP 连接。如果 TCP 连接建立成功，BGP 发送一个 OPEN 消息给对端，并等待从对端发来的 OPEN 消息。收到一个 OPEN 消息后，BGP 检查该消息的所有字段，如果没有发现错误，则向对端发送一个 KEEPALIVE 消息并启动 KEEPALIVE 定时器。收到 KEEPALIVE 消息，则邻居建立。

update 报文格式：所有路由的添加，更新，删除都、依赖此消息完成：



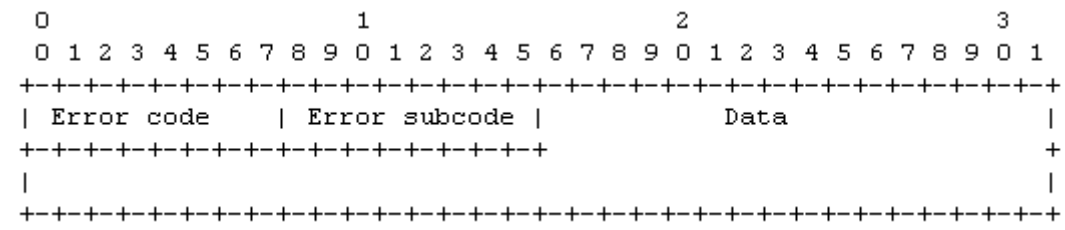
Unfeasible Routes Length—-2 字节，指示了撤销路由的字节总长度。0 说明没有撤销路由。

Withdrawn Routes —-之前发布过，不再有效的路由。总长度与 Unfeasible Routes Length 值对应。

Total Path Attribute Length—-2 字节，0 代表在 UPDATE 消息中没有网络层可达信息域。

Path Attributes（路径属性）：总长度和 Total Path Attribute Length 值对应。

NOTIFICATION 报文格式：



Error code：占 1 个字节（无符号位），定义错误的类型，非特定的错误类型用零表示。

Error subcode：占 1 个字节（无符号位），指定错误细节编号，非特定的错误细节编号用零表示。

Data：指定错误数据内容。

五、观察动态路由

网络变更前 router0 的路由表和到 router3 的 IP 路径：

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.1.0     192.168.0.2     255.255.255.0   UG    2      0        0 eth0
192.168.2.0     192.168.0.2     255.255.255.0   UG    3      0        0 eth0
user@ubuntu:~$
```

```
user@ubuntu:~$ tracepath 192.168.2.2
 1:  ubuntu-2.local                                        0.055ms pmtu 1500
 1:  ubuntu.local                                          0.322ms
 1:  ubuntu.local                                          0.210ms
 2:  192.168.1.2                                           0.512ms
 3:  192.168.2.2                                           1.049ms reached
     Resume: pmtu 1500 hops 3 back 62
user@ubuntu:~$
```

可见变更前到 router3 的 IP 为 192.168.2.2 的网卡需要经过 3 跳，且网关为 192.168.0.2，即需要通过 router1 来路由。

网络变更后 router0 的路由表和到 router3 的 IP 路径：

```
user@ubuntu:/etc/quagga$ tracepath 192.168.2.2
 1:  ubuntu-2.local                                        0.065ms pmtu 1500
 1:  192.168.2.2                                           0.333ms reached
 1:  192.168.2.2                                           0.226ms reached
     Resume: pmtu 1500 hops 1 back 64
user@ubuntu:/etc/quagga$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.1.0     192.168.6.2     255.255.255.0   UG    3      0        0 eth1
192.168.2.0     192.168.6.2     255.255.255.0   UG    2      0        0 eth1
192.168.6.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
user@ubuntu:/etc/quagga$
```

可见变更后，到 router3 仅需 1 跳，路由表也发生了变化，从 router0 路由到 router3 的 IP 为 192.168.2.2 的网卡时，网关为 192.168.6.2，正好对应 router3 的连到 router0 的网卡。

六、参考资料

BGP：

https://blog.csdn.net/younkerjqb/article/details/72867987

RIP：

https://blog.csdn.net/LAINCLAK/article/details/77266828

OSPF：

https://blog.csdn.net/lycb_gz/article/details/9662965