实验五 动态路由协议RIP, OSPF和BGP观察

161130118 尹浚宇

**实验目的**

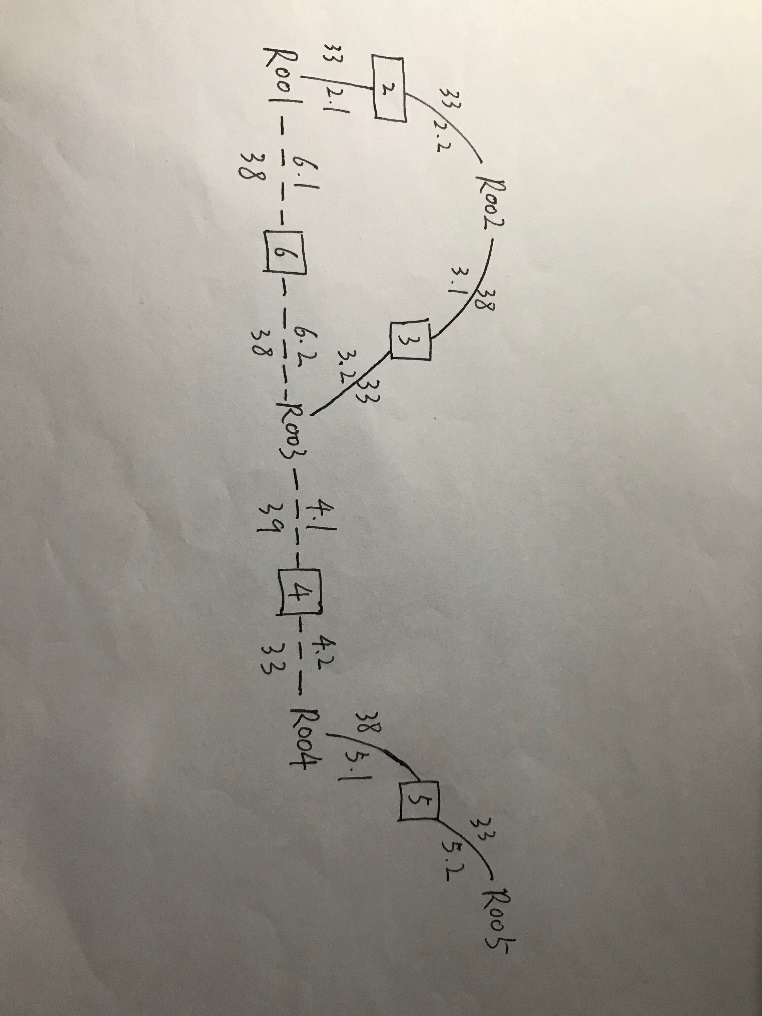
理解自治系统的概念

了解RIP, OSPF, BGP协议的运行过程

掌握距离向量和链路状态的路由选择算法

**网络拓扑配置**

因为电脑配置不够, 这里删去了两个路由器. 拓扑图如下:



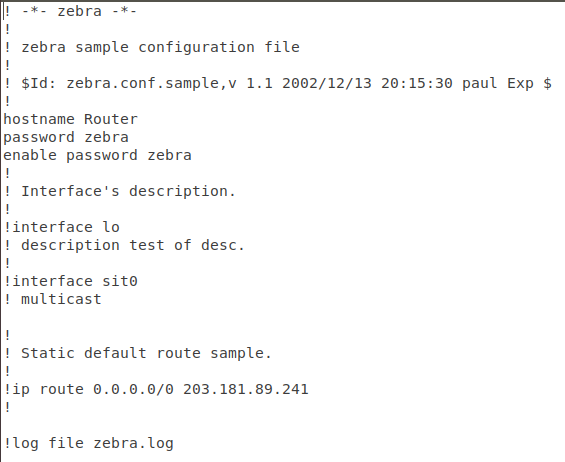
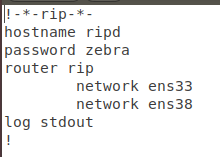
横线上一边表示端口号(省略前缀ens), 一边表示ip地址(省略前缀192.168.), 每个方框代表一个网卡, 子网掩码都是255.255.255.0. R001-R003为AS1, R004-R005为AS2. 虚线表示一开始未使用, 在实验过程中逐步加上去的链路.

下面给出的附表1是实验全部完成后的配置:

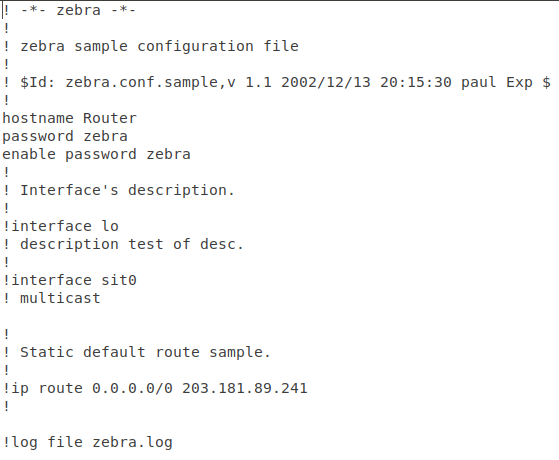
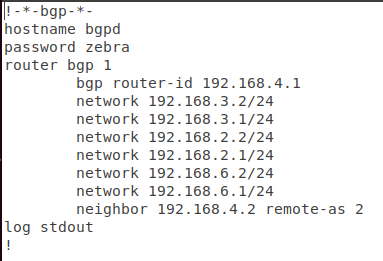
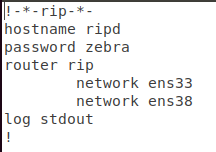
|  |  |  |
| --- | --- | --- |
| 节点名 | ip | netmask |
| R001 | ens33: 192.168.2.1 | 255.255.255..0 |
| ens38: 192.168.6.1 |
| R002 | ens33: 192.168.2.2 |
| ens38: 192.168.3.1 |
| R003 | ens33: 192.168.3.2 |
| ens38: 192.168.6.2 |
| ens39: 192.168.4.1 |
| R004 | ens33: 192.168.4.2 |
| ens38: 192.168.5.1 |
| R005 | ens33: 192.168.5.2 |

**路由配置文件**

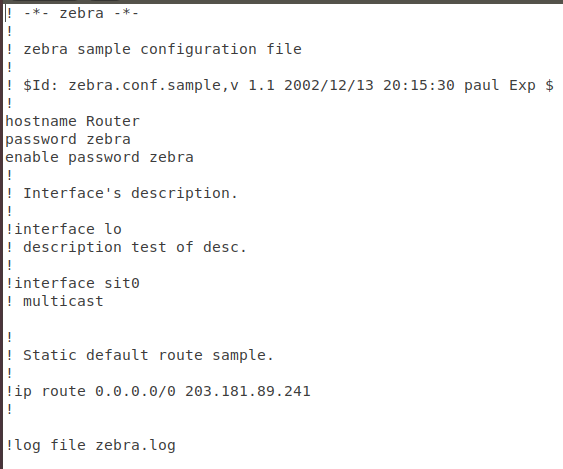
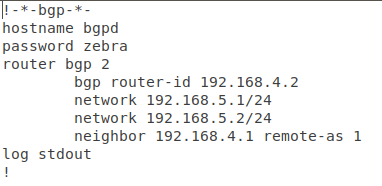
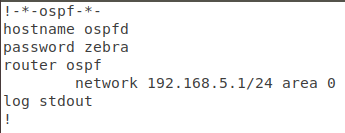
R001:



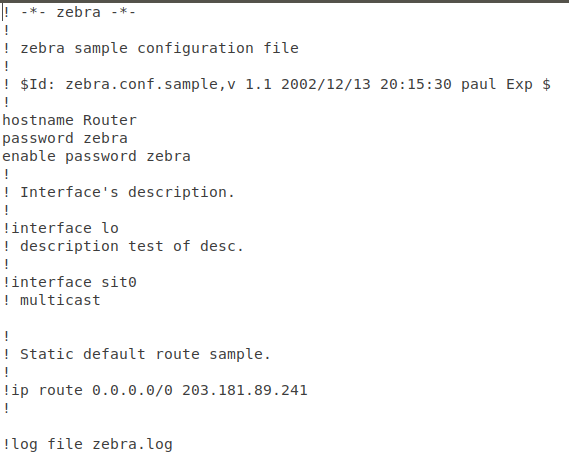
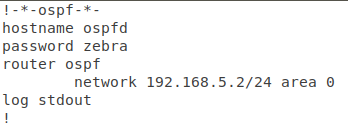
R003:



R004:

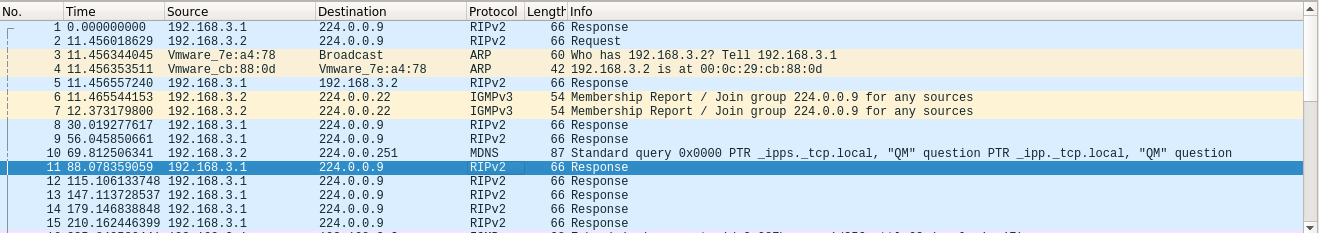


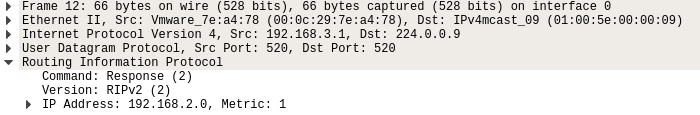
R005:



**数据包截图**

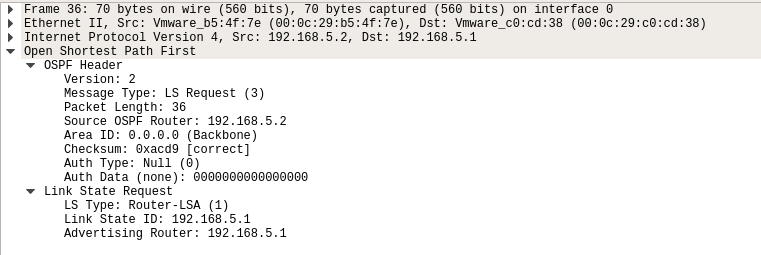
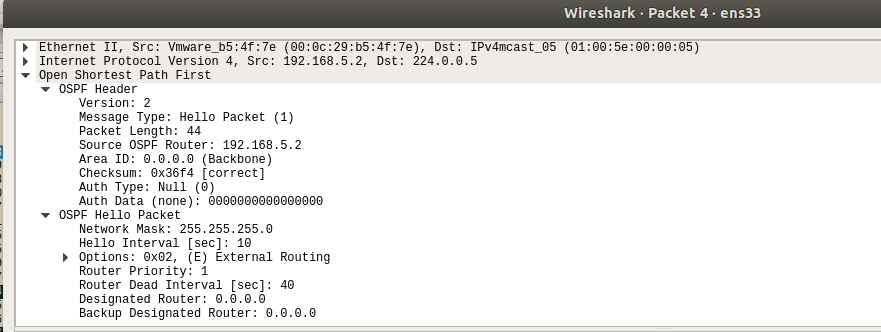
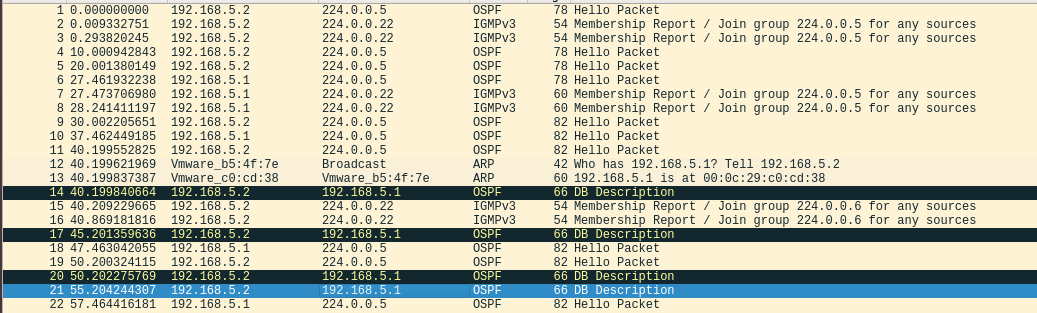
RIP





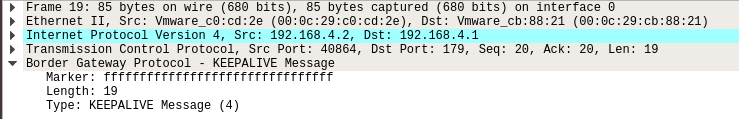
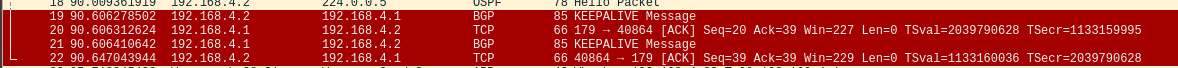
在R003的ens33端口上捕获的.

OSPF



在R005的ens33端口上捕获的.

BGP



在R003的ens39端口捕获的.

**协议报文分析**

对这三种协议的一个大体描述如下表所示:

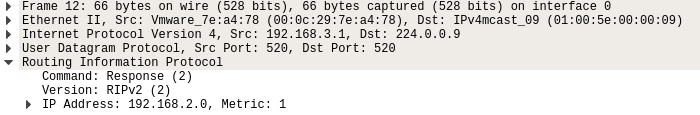
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 协议 | RIP | OSPF | BGP | |
| 类型 | 内部 | 内部 | 外部 | |
| 路由算法 | 距离-向量 | 链路状态 | 距离-向量 | |
| 传递协议 | UDP | IP | TCP | |
| 路径选择 | 跳数最少 | 代价最低 | 较好，非最佳 | |
| 交换节点 | 和本节点相邻 | 网络中所有路由器 | 和本节点相邻的路由器 | |
| 交换内容 | 当前本路由器的路由表 | 与本路由器相邻的所有路由器的链路状态 | 首次 | 整个路由表 |
| 非首次 | 有变化的部分 |

RIP

路由信息协议(Routing Information Protocol)是应用较早、使用较普遍的内部网关协议, 它采用距离向量算法, 适用于小型网络. 在默认情况下, RIP使用跳跃计数(hop count)来衡量路由距离, 跳跃计数是一个包到达目标所必须经过的路由器的数目.

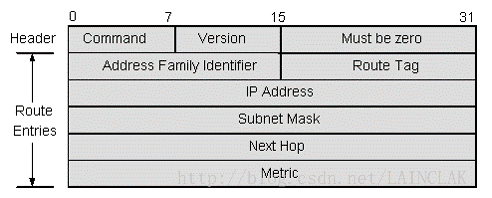
RIP使用UDP的520端口来发送和接收RIP报文. 在RIP中, 如果一个路由在180s内未被刷新, 则相应的距离就被设定成无穷大, 并从路由表中删除该表项. RIP报文分为两种: 请求报文和响应报文.

下图是本实验中抓到的一个RIP包的详细报文.



由于前面部分之前实验已经分析过, 下面只分析报文中的RIP部分.

RIPv2报文格式如下图所示:



其中command字段取值为1或2, 1表示请求信息, 2表示响应信息.

version字段表示版本号, 这里取值为2, 代表是RIPv2.

address family identifier字段表示地址组标识, 于IP该项设置为2. 当消息是对路由器(或主机)整个路由选择表的请求时, 这个字段将被设置为0.

routet tag字段表示路由标志, 这个字段标记外部路由或重分配到RIPv2协议中的路由. 默认情况是使用这个16位的字段来携带从外部路由选择协议注入到RIP中的路由的AS号. 虽然RIP协议自己并不使用这个字段, 但是在多个地点和某个RIP域相连的外部路由, 可能需要使用这个路由标记字段通过RIP域来交换路由信息. 这个字段也可以用来把外部路由编成"组", 以便于在RIP域中更容易地控制这些路由.

IP address字段表示路由条目的目的地址, 它可以是主网络地址, 子网地址或主机路由.

subnet mask字段表示子网掩码.

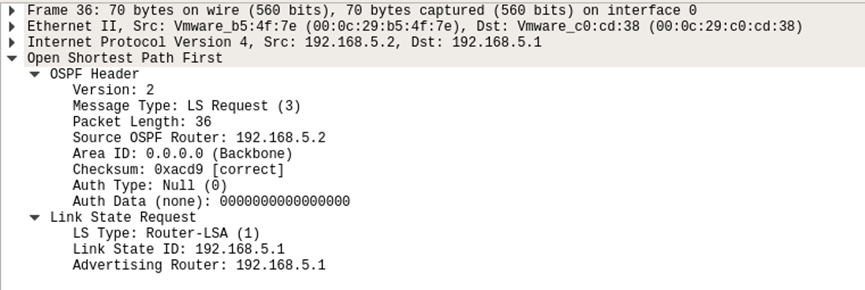
next hop字段如果存在的话，它标识一个比通告路由器更好的下一跳地址. 也就是说, 它指出的下一跳地址, 其度量值比同一个子网上的通告路由器更靠近目的地. 如果这个字段设置为全0, 说明通告路由器的地址就是最好的下一跳地址.

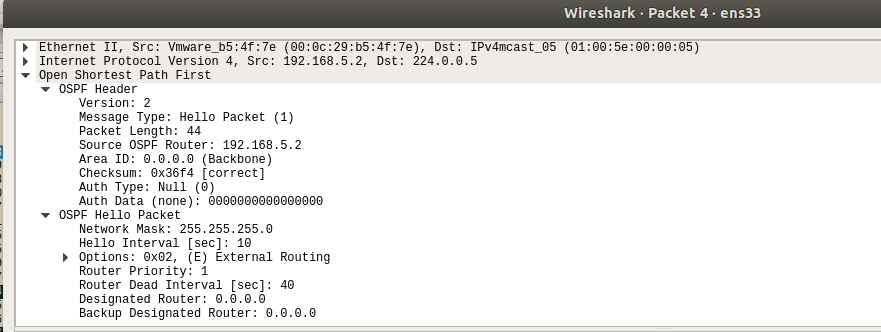
metric字段表示距离的度量值, 它是一个1～16之间的跳数.

OSPF

开放式最短路径优先(Open Shortest Path First)是另一种被广泛使用的内部网关协议. OSPF 根据域中的链路状态来决策路由, 计算出最短路径树, 通常多用于较大型的网络. OSPF协议同时使用单播(unicast)和多播(multicast)来发送Hello包和连接状态更新（link state updates）, 使用的多播地址为224.0.0.5和224.0.0.6. 不同于RIP的是, OSPF协议直接使用IP协议, 并将链路状态广播数据包传送给在某一区域内的所有路由器, 而不是将部分或全部的路由表传递给与其相邻的路由器.

下图是本次实验中捕获的一个link state request包和一个hello包.



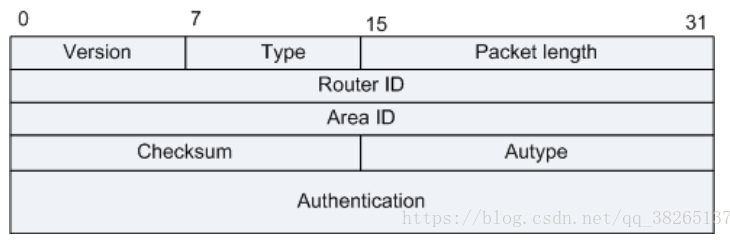


由于前面部分之前实验已经分析过, 下面只分析报文中的OSPF部分.

OSPF用IP报文直接封装协议报文, 协议号为89. OSPF分为5种报文, Hello报文、DD报文、LSR报文、LSU报文和LSAck报文.

OSPF这五种报文具有相同的报文头格式, 长度为24字节.

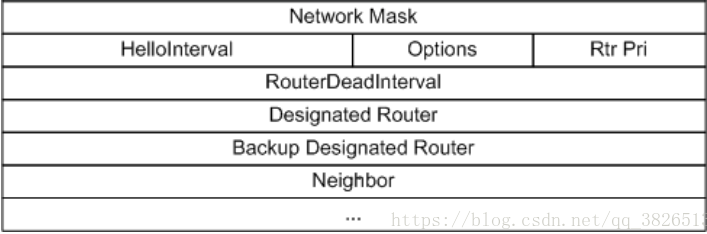
OSPF报头格式如下图所示:



各字段解释如下:



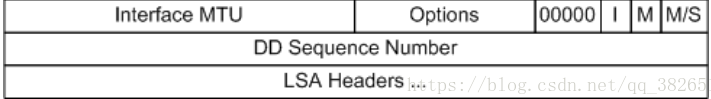
Hello报文格式如下:



各字段解释如下:



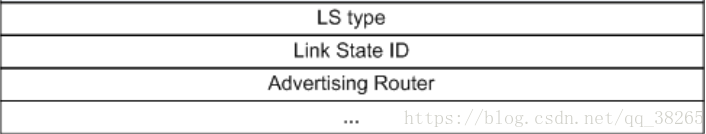
DD报文格式如下:



各字段解释如下:



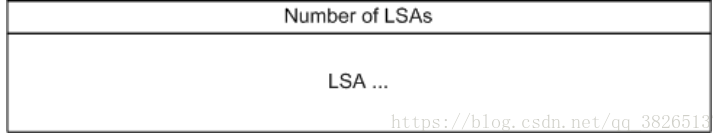
LSR报文格式如下:



各字段解释如下:



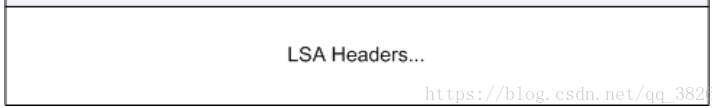
LSU报文格式如下:



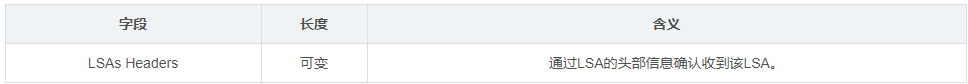
各字段解释如下:



LSAck报文格式如下:



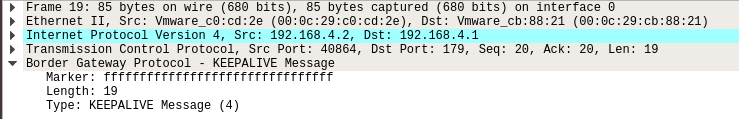
各字段解释如下:



BGP

边界网关协议(Border Gateway Protocol)是互联网的核心路由协议. 它通过维护路由表来实现自治系统之间的可达性, 属于向量路由协议. BGP不使用传统域内路由协议的距离度量, 而是基于路径、网络策略和规则集来决定路由. BGP通过在路由器上手工设置来使用TCP的 179号端口来发送和接收报文. BGP路由器会周期地发送19字节的保持存活报文来维护连接. 当BGP在一个AS内部运行时, 它被称作内部边界网关协议(iBGP, Interior Border Gateway Protocol); 当BGP在AS之间运行时, 它被称作外部边界网关协议(eBGP, Exterior Border Gateway Protocol).

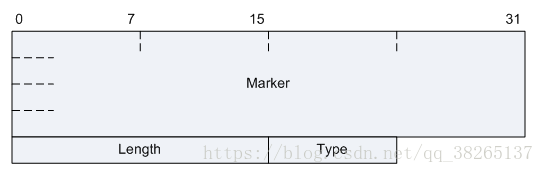
下图是本实验中捕获的一个BGP报文.



由于前面部分之前实验已经分析过, 下面只分析报文中的BGP部分.

BGP报文由BGP报文头和具体报文两部分组成.

BGP报文头包括三个部分, 总长19字节. 具体格式如下图所示:



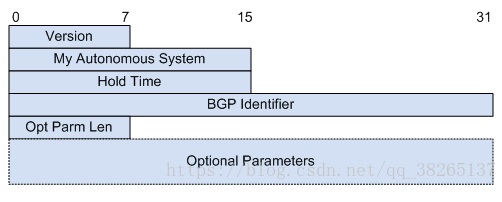
其中marker字段占16字节, 用于检查BGP对等体的同步信息是否完整, 以及用于BGP验证的计算. 不使用验证时所有比特均为1.

length字段占2字节, 表示包括报文头在内的BGP消息总长度(以字节为单位).

Type字段占1字节, 表示BGP消息的类型. Type有5个可选值, 表示BGP报文头后面所接的5类报文, 具体定义如下:



Open类型报文格式如下:



各字段解释如下:

version: 表示协议的版本号.

My autonomous System: 发送者自己的AS号.

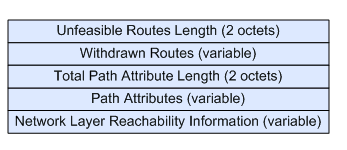
Hold Time: 发送者自己设定的hold time值, 用于协商BGP对等体间保持建立连接关系时发送KEEPALIVE或UPDATE等报文的时间间隔.

BGP Identifier: 发送者的router id.

Opt Parm Len: 表示Optional Parameters的长度. 如果此值为0, 表示没有可选参数.

Optional Paramters: 此值为BGP可选参数列表, 每一个可选参数是一个TLV格式的单元.

Update类型报文格式如下:



各字段解释如下:

Unfeasible Routes Length: 标明Withdrawn Routes部分的长度. 其值为零时, 表示没有撤销的路由.

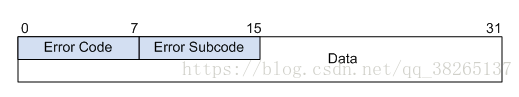
Withdrawn Routes: 包含要撤销的路由列表, 列表中的每个单元包含1字节的Length域和可变长度的Prefix域.

Total Path Attribute Length: 标明Path Attributes部分的长度. 其值为零时, 表示没有路由及其路由属性要通告.

Path Attributes: 包含要更新的路由属性列表, 按其类型号从小到大的顺序排序, 填写更新的路由的所有属性. 每一个属性单元包括属性类型, 属性长度, 属性值三部分. 其编码采用TLV格式.

Network Layer Reachability Information: 包含要更新的地址前缀列表, 每一个地址前缀单元由一个LV二元组组成, 其编码填写方法与Withdrawn Routes的填写方法相同.

Notification类型报文格式如下:



各字段解释如下:

Error code: 占1个字节, 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, 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.

Keepalive类型报文用于保持BGP连接. 其报文只有BGP报文头, 没有具体内容, 故其报文长度应固定为19个字节.

Refresh类型报文格式如下:



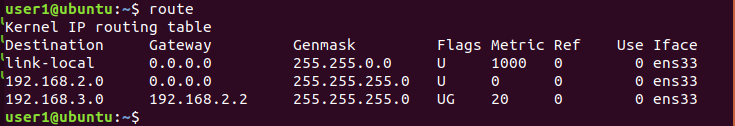
各字段解释如下:



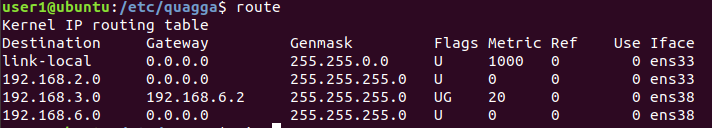
**观察动态路由**

R001路由表变化

在R001和R003之间没有链路之前

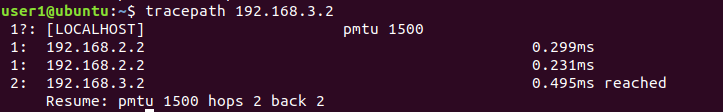


在R001和R003之间有链路之后

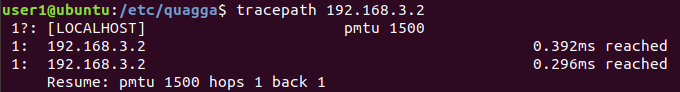


R001到R003的包传输路径变化

在R001和R003之间没有链路之前



在R001和R003之间有链路之后



可以观察到在网络变更之前, 从R001到R003的下一跳为R002, 一个包从R001到R003必须要经过2跳. 在网络变更之后, RIP协议使用距离向量算法得到了新的跳数最少的路径, 即R001到R003的包直接从新加链路发包即可.