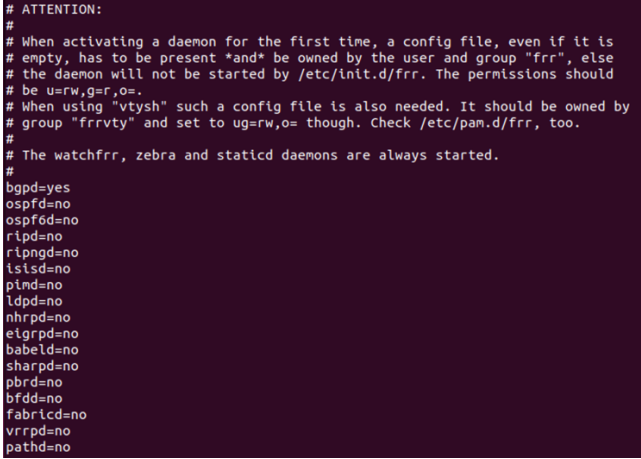


实验名称	BGP 实验		
姓名	刘培源	学号	2023214278
实验步骤	<p>实验环境：Mac Parallel Desktop 19; Ubuntu 22.04</p> <p>注：由于 Ubuntu 22.04 上已经不支持 quagga，因此本实验采用 FRRouting 实现；同时，FRRouting 针对了 Mac 的 Parallel Desktop 进行了适配。</p> <ol style="list-style-type: none">1. 与实验二一样，在 host1 和 host2 上均配置两个网卡，采用桥接模式（Bridge Network: feth8302），用于配置 BGP。2. 重要!!在 cd /etc/frr 和 sudo touch zebra.conf bgpd.conf 配置 zebra.conf 和 bgpd.conf 之前，一定要把/etc/frr/frr.conf 文件删除，因为 frr 默认把所有的 configure 都集成到 frr.conf 里，若要分开配置，就得把它删了，再去分别配置 zebra.conf 和 bgpd.conf（host1 和 host2 都要做同样设置）。3. 在 zebra.conf 中输入 password zebra 配置 zebra，在 bgpd.conf 中输入 password bgp，并且将 daemons 中的 bgpd 设置为 yes，截图如下： 4. 然后在 host1 上通过如下命令进一步配置 zebra：<ol style="list-style-type: none">(1) sudo telnet localhost 2601(2) enable(3) configure terminal(4) interface enp0s5(5) ip address 192.168.0.1/24(6) no shutdown(7) interface enp0s6(8) ip address 192.168.1.1/24(9) no shutdown(10) write配置过程截图如下：		

```

nat@nat-Parallels-ARM-Virtual-Machine:~/Desktop$ sudo telnet localhost 2601
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Hello, this is FRRouting (version 8.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

User Access Verification

Password:
nat-Parallels-ARM-Virtual-Machine> enable
nat-Parallels-ARM-Virtual-Machine# configure terminal
nat-Parallels-ARM-Virtual-Machine(config)# interface enp0s5
nat-Parallels-ARM-Virtual-Machine(config-if)# ip address 192.168.0.1/24
nat-Parallels-ARM-Virtual-Machine(config-if)# no shutdown
nat-Parallels-ARM-Virtual-Machine(config-if)# interface enp0s6
nat-Parallels-ARM-Virtual-Machine(config-if)# ip address 192.168.1.1/24
nat-Parallels-ARM-Virtual-Machine(config-if)# no shutdown
nat-Parallels-ARM-Virtual-Machine(config-if)# write
Configuration saved to /etc/frr/zebra.conf

```

配置完之后 zebra.conf 文件内容如下:

```
nat@nat-Parallels-ARM-Virtual-Machine:~/Desktop$ sudo cat /etc/frr/zebra.conf
!
! Zebra configuration saved from vty
!   2023/12/24 19:49:27
!
frr version 8.1
frr defaults traditional
!
hostname nat-Parallels-ARM-Virtual-Machine
password zebra
!
!
!
!
interface enp0s5
 ip address 192.168.0.1/24
exit
!
interface enp0s6
 ip address 192.168.1.1/24
exit
!
!
!
no ipv6 forwarding
!
!
!
!
!
```

5. 接着在 host1 上通过如下命令配置 bgpd:
 - (1) `sudo telnet localhost 2605`
 - (2) `enable`
 - (3) `configure terminal`
 - (4) `router bgp 100`
 - (5) `network 192.168.0.0/24`
 - (6) `neighbor 192.168.0.2 remote-as 200`
 - (7) `neighbor 192.168.0.2 description "two"`
 - (8) `write`

配置过程截图如下：

```

nat@nat-Parallels-ARM-Virtual-Machine: /Desktop$ sudo telnet localhost 2605
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.

Hello, this is FRRouting (version 8.1).
Copyright 1996-2005 Kunihiko Ishiguro, et al.

User Access Verification

Password:
nat-Parallels-ARM-Virtual-Machine> enable
nat-Parallels-ARM-Virtual-Machine# configure terminal
nat-Parallels-ARM-Virtual-Machine(config)# router bgp 100
nat-Parallels-ARM-Virtual-Machine(config-router)# network 192.168.0.0/24
nat-Parallels-ARM-Virtual-Machine(config-router)# network 192.168.0.2 remote-as 200
% [BGP] Unknown command: network 192.168.0.2 remote-as 200
nat-Parallels-ARM-Virtual-Machine(config-router)# neighbor 192.168.0.2 remote-as 200
nat-Parallels-ARM-Virtual-Machine(config-router)# neighbor 192.168.0.2 description "two"
nat-Parallels-ARM-Virtual-Machine(config-router)# write
Configuration saved to /etc/frr/bgpd.conf

```

配置完之后 bgpd.conf 文件内容如下:

```

nat@nat-Parallels-ARM-Virtual-Machine:~/Desktop$ sudo cat /etc/frr/bgpd.conf
!
! Zebra configuration saved from vty
!   2023/12/24 19:53:40
!
frr version 8.1
frr defaults traditional
!
hostname nat-Parallels-ARM-Virtual-Machine
password bgp
!
!
!
router bgp 100
 neighbor 192.168.0.2 remote-as 200
 neighbor 192.168.0.2 description "two"
!
 address-family ipv4 unicast
   network 192.168.0.0/24
 exit-address-family
!
exit
!
!
!
!

```

6. 对于 host2 的设置，只有 ip 地址的设置有区别，下面直接展示 host2 上配置完之后的 zebra.conf 和 bgpd.conf:

```

host@host-Parallels-ARM-Virtual-Machine:~/Desktop$ sudo cat /etc/frr/zebra.conf
!
! Zebra configuration saved from vty
!   2023/12/24 20:05:15
!
frr version 8.1
frr defaults traditional
!
hostname host-Parallels-ARM-Virtual-Machine
password zebra
!
!
!
interface enp0s5
 ip address 192.168.0.2/24
exit
!
interface enp0s6
 ip address 192.168.2.1/24
exit
!
!
!
no ip forwarding
no ipv6 forwarding
!
!
!
!

```

```

host@host-Parallels-ARM-Virtual-Machine:~/Desktop$ sudo cat /etc/frr/bgpd.conf
!
! Zebra configuration saved from vty
!   2023/12/24 20:07:40
!
frr version 8.1
frr defaults traditional
!
hostname host-Parallels-ARM-Virtual-Machine
password bgp
!
!
!
router bgp 200
 neighbor 192.168.0.1 remote-as 100
 neighbor 192.168.0.1 description "one"
!
 address-family ipv4 unicast
   network 192.168.2.0/24
 exit-address-family
!
exit
!
!
!
!

```

7. 在配置完成之后，分别在 host1 和 host2 上输入 `sudo /etc/init.d/frr restart` 来重启 frr 服务。
8. 在经过一段时间后，观察 host1 的路由表如下：

Kernel IP routing table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use
link-local	*	255.255.0.0	U	1000	0	0
192.168.0.0	*	255.255.255.0	U	0	0	0
192.168.1.0	*	255.255.255.0	U	0	0	0
192.168.2.0	192.168.0.2	255.255.255.0	UG	0	0	0

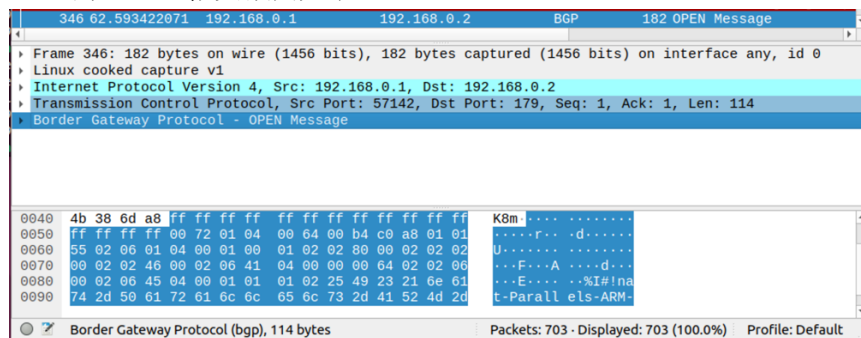
host2 的路由表如下：

Kernel IP routing table						
Destination	Gateway	Genmask	Flags	Metric	Ref	Use
link-local	*	255.255.0.0	U	1000	0	0
192.168.0.0	*	255.255.255.0	U	0	0	0
192.168.1.0	192.168.0.1	255.255.255.0	UG	0	0	0
192.168.2.0	*	255.255.255.0	U	0	0	0

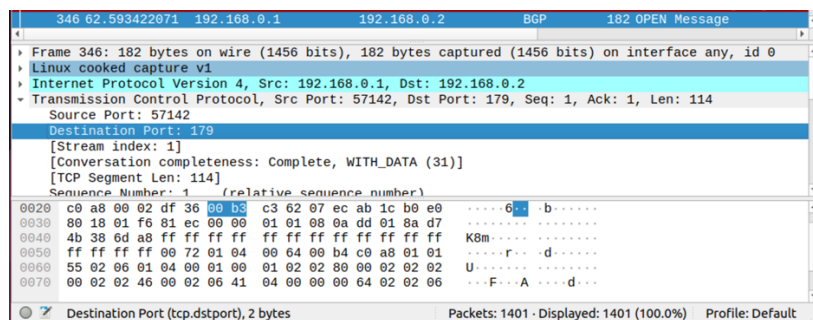
- 至此 BGP 已经配置完成，wireshark 的数据分析在后面给出。

1. 观察 OPEN 报文

BGP 的 OPEN 报文截图如下

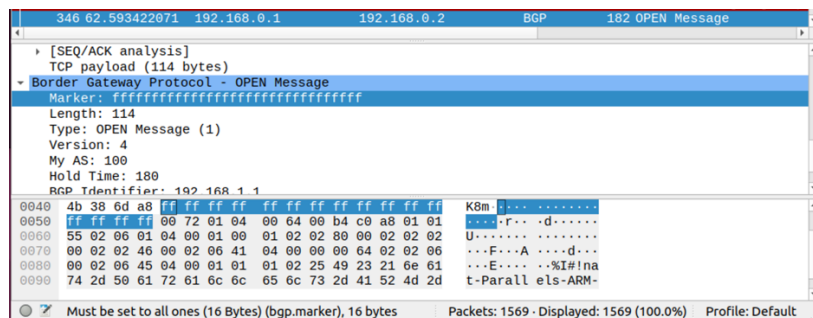


(1) 传输协议层 TCP 中的端口号是否为 179?



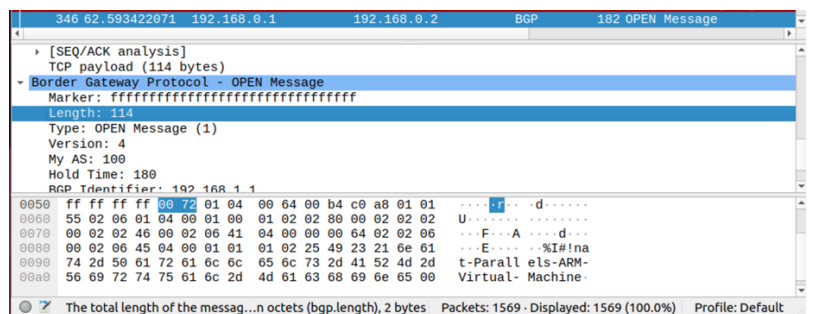
是的

(2) Marker 字段的值是否全为 1?所观察到的值代表什么含义?



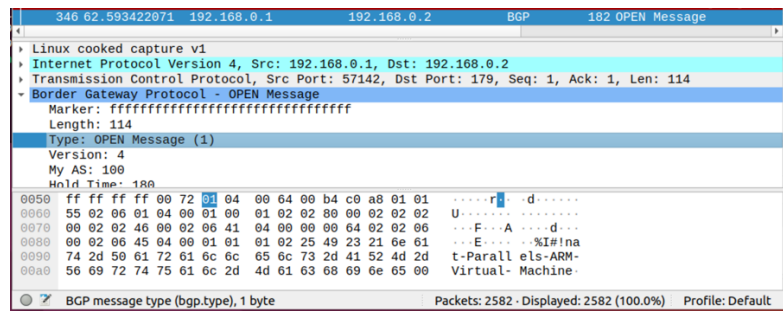
是的，代表不使用验证。

(3) Length 字段的值?OPEN 报文各个字段的总长度?二者是否相等。



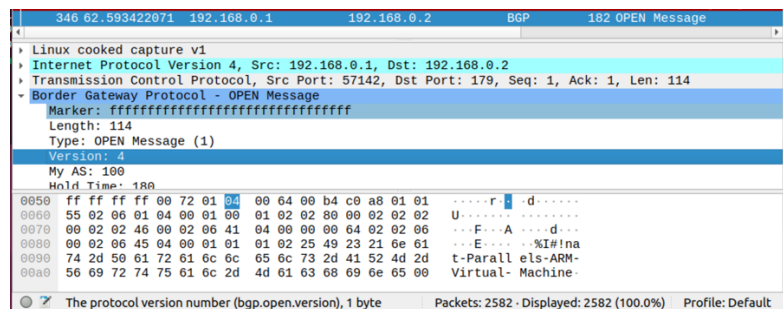
Length 字段的值为 114；总长度也是 114，二者相等。

(4) Type 字段的值是否与 OPEN 报文的类型值对应?



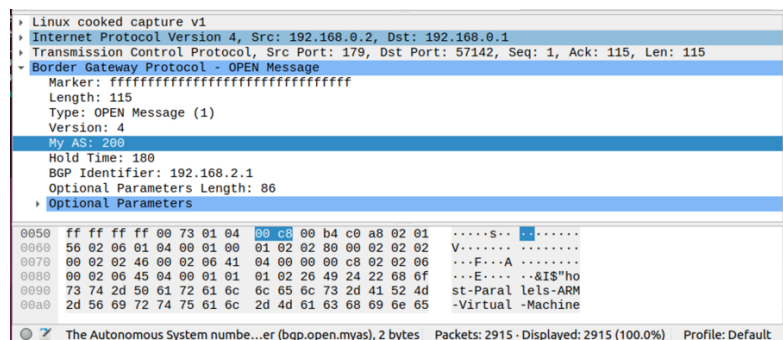
由图可知，二者相对应。

(5) Version 字段是否为 4?



是的。

(6) 观察 MyAs 字段, Hold Time 字段, IP 地址字段, 确认这个 OPEN 报文发送者所在的 AS 号, 建议的保持时间, 以及 IP 地址。

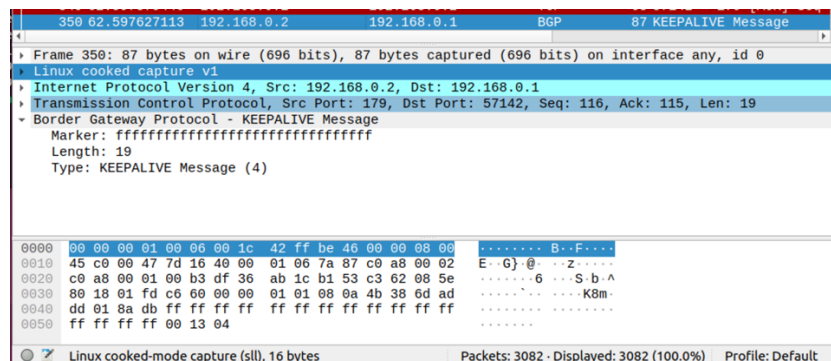


AS 号: 200

建议保持时间: 180

IP 地址: 192.168.2.1

2. 观察 KEEPALIVE 报文



3. 观察 UPDATE 报文, 重启 fir。

372	65.393138073	192.168.0.2	192.168.0.1	BGP	91 UPDATE Message
Frame 372: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface any, id 0 Linux cooked capture v1 Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1 Transmission Control Protocol, Src Port: 41386, Dst Port: 179, Seq: 135, Ack: 134, Len: 23 Border Gateway Protocol - UPDATE Message					
Marker: ffffffffffffffffffffffffffffffff Length: 23 Type: UPDATE Message (2) Withdrawn Routes Length: 0 Total Path Attribute Length: 0					
0000	00 00 00 01 00 06 00 1c 42 ff be 46 00 00 08 00 B..F....			
0010	45 c0 00 4b e6 bf 40 00 01 06 10 da c0 a8 00 02	E..K..@..z.....			
0020	c0 a8 00 01 a1 aa 00 b3 f6 29 2a 09 01 d6 0a d8) *i.....			
0030	80 18 01 f6 ee f5 00 00 01 01 08 0a 4b 38 78 98K8x.....			
0040	dd 01 91 d6 ff ff ff ff ff ff ff ff ff ff ff ffK8x.....			
0050	ff ff ff ff 00 17 02 00 00 00 00			
Must be set to all ones (16 Bytes) (bgp.marker), 16 bytes Packets: 3469 - Displayed: 3469 (100.0%) Profile: Default					

4. 观察 NOTIFICATION 报文。

355	63.080009697	192.168.0.2	192.168.0.1	BGP	89 NOTIFICATION Message
Frame 355: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0 Linux cooked capture v1 Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1 Transmission Control Protocol, Src Port: 179, Dst Port: 57142, Seq: 156, Ack: 134, Len: 21 Border Gateway Protocol - NOTIFICATION Message					
Marker: ffffffffffffffffffffffffffffffff Length: 21 Type: NOTIFICATION Message (3) Major error Code: Cease (6) Minor error Code (Cease): Administratively Shutdown (2)					
0000	00 00 00 01 00 06 00 1c 42 ff be 46 c0 a8 08 00 B..F....			
0010	45 c0 00 49 7d 19 40 00 01 06 7a 82 c0 a8 00 02	E..I}..@..z.....			
0020	c0 a8 00 01 00 b3 df 36 ab 1c b1 7b c3 62 08 716...{-b.q...			
0030	80 18 01 fd c3 38 00 00 01 01 08 0a 4b 38 6f 8f8...K8o.....			
0040	dd 01 8a dc ff ff ff ff ff ff ff ff ff ff ff ffK8o.....			
0050	ff ff ff ff 00 15 03 06 02			
Must be set to all ones (16 Bytes) (bgp.marker), 16 bytes Packets: 3309 - Displayed: 3309 (100.0%) Profile: Default					

思考题	<p>1. 重启 quagga 出现的 UPDATE 消息都是成对的，即两个 bgp 对等体都向对方那个发送了一个 UPDATE 消息。请结合这个具体的例子，思考产生这个现象的原因。</p> <p>答：在重启 Quagga 时观察到的 BGP UPDATE 消息成对出现的现象，即两个 BGP 对等体相互发送了一个 UPDATE 消息，可以归因于 eBGP 的对等体特性和 TCP 协议的传输机制。具体而言，eBGP 协议要求两个对等体间的通信是互相独立的，这意味着每个对等体都需要主动发送信息以维持协议的状态和数据的同步。同时，BGP 协议运行在 TCP 之上，这要求在数据传输前必须完成 TCP 的三次握手过程，确保连接的可靠性。因此，在 Quagga 重启过程中，两个 BGP 对等体都会通过发送 UPDATE 消息来重新建立连接并同步路由信息，从而形成了成对的 UPDATE 消息现象。</p> <p>2. 如何验证 BGP 声明的正确性？</p> <p>答：验证 BGP 声明的正确性主要依赖于 BGP 消息中的 Marker 字段。BGP 协议设计了 Marker 字段作为一种安全机制，以确保接收到的消息是有效和完整的。在 BGP 消息结构中，Marker 字段通常位于消息的开始位置，用于标识消息的开始并提供一种方法来验证消息的完整性。通过检查这个字段，可以确认收到的 BGP 声明是否符合协议规范，从而确保 BGP 通信的可靠性和数据的正确性。</p>
经验总结	<p>1. 在 Parallel Desktop 上使用 Ubuntu 22.04 的 MacOS 用户注意实验步骤中的重要!!部分。</p>