BGP 状态机实验

一、实验目的

通过 BGP 协议状态机实验，使学生加深对协议状态机描述的理解，并掌握协议状态机的设计实现方法。本实验状态机取材于 BGP 路由协议，学生也可以加深对于 BGP 路由协议的理解。

二、实验说明

<1> BGP 协议简述

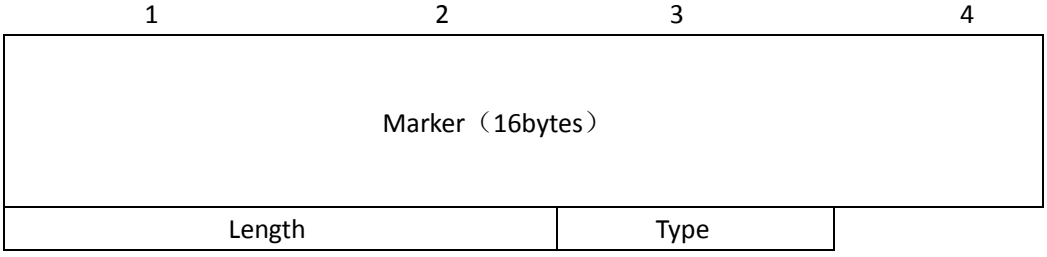
BGP 协议是在 EGP 协议的基础上发展起来的。EGP 协议曾经作为自治系统间的路由协议，广泛应用于 NSFNET 等网络上，但是 EGP 被路由环路问题所困扰。BGP 通过在路由信息中增加自治系统（AS）路径的属性，消除了路由环路。BGP 协议还支持路由策略配置。随着互联网的飞速发展，路由表的表项数也迅速增加，自治系统间路由信息的交换量越来越大，严重影响了网络的性能。BGP 支持无类域间路由和路由聚集，可以有效的减少日益增大的路由表。

BGP 路由器可以与本自治系统内或者自治系统外的路由器建立 BGP 连接。与自治系统内的路由器建立的连接成为 iBGP 连接，与自治系统外的路由器建立的连接成为 eBGP 连接。iBGP 和 eBGP 的处理机制不同。BGP 路由器通过 TCP 协议建立可靠的连接。

<2> BGP 协议的消息类型

BGP 有 4 种类型的消息，分别为 OPEN，UPDATE，KEEPALIVE 和 NOTIFICATION 消息，它们有相同的消息头。

a> 消息头结构



Maker：（16B）鉴权信息

Length：（2B）消息的长度

Type：（1B）消息的类型

1：OPEN

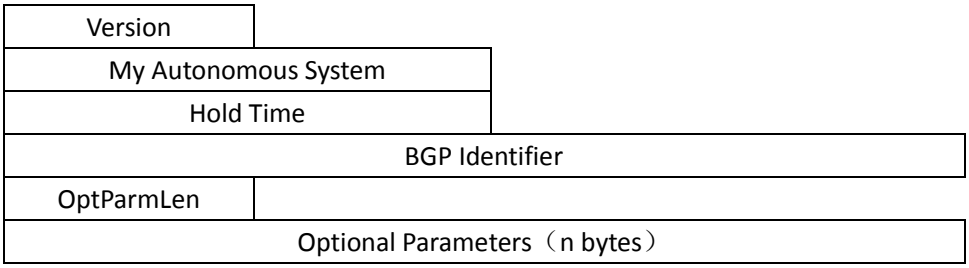
2：UPDATE

3：NOTIFICATION

4：KEEPALIVE

b> OPEN 消息结构

OPEN 消息在上述消息头的基础上，再添加如下字段。



Version：（1B）发起方 BGP 版本号

My Autonomous System：（2B 无符号整数）本地 AS 号

Hold Time：（2B 无符号整数）发起方建议的保持时间

BGP Identifier：（4B）发起方的路由器标识符

OptParmLen：（1B）可选参数长度

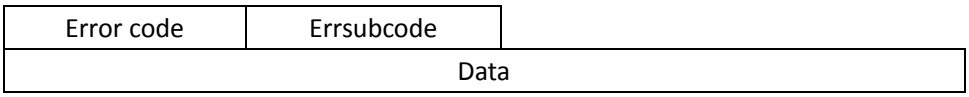
Optional Parameters：（变长）可选参数。

c> KEEPALIVE 消息结构

KEEPALIVE 消息只有一个消息头。

d> NOTIFICATION 消息结构

NOTIFICATION 消息在上述消息头的基础上，再添加如下字段。



Errorcode：（1B）错误代码

错误代码	错误类型
1	消息头错
2	OPEN 消息错
3	UPDATE 消息错
4	保持时间超时
5	状态机错
6	退出

Errsubcode：（1B）辅助错误代码，略

Data：（变长）依赖于不同的错误代码和辅助错误代码。用于诊断错误原因。

e> UPDATE 消息结构

UPDATE 消息在上述消息头的基础上，再添加如下字段：

Unfeasible Routes Len：（2B 无符号整数）不可达路由长度

Withdrawn Routes：（变长）撤销路由列表

Path Attribute Len：（2B 无符号整数）路径属性长度

Path Attribute：（变长）路径属性（以下详细说明）

NetWork Layer Reachability Information：（变长）网络层可达性信息

BGP 使用二元组<length,prefix>来表示所撤销的路由和网络层可达性信息。Length 为 1B，指示地址前缀的长度。Prefix 为地址前缀，长度为 1B~4B。

<3> BGP 有限状态机

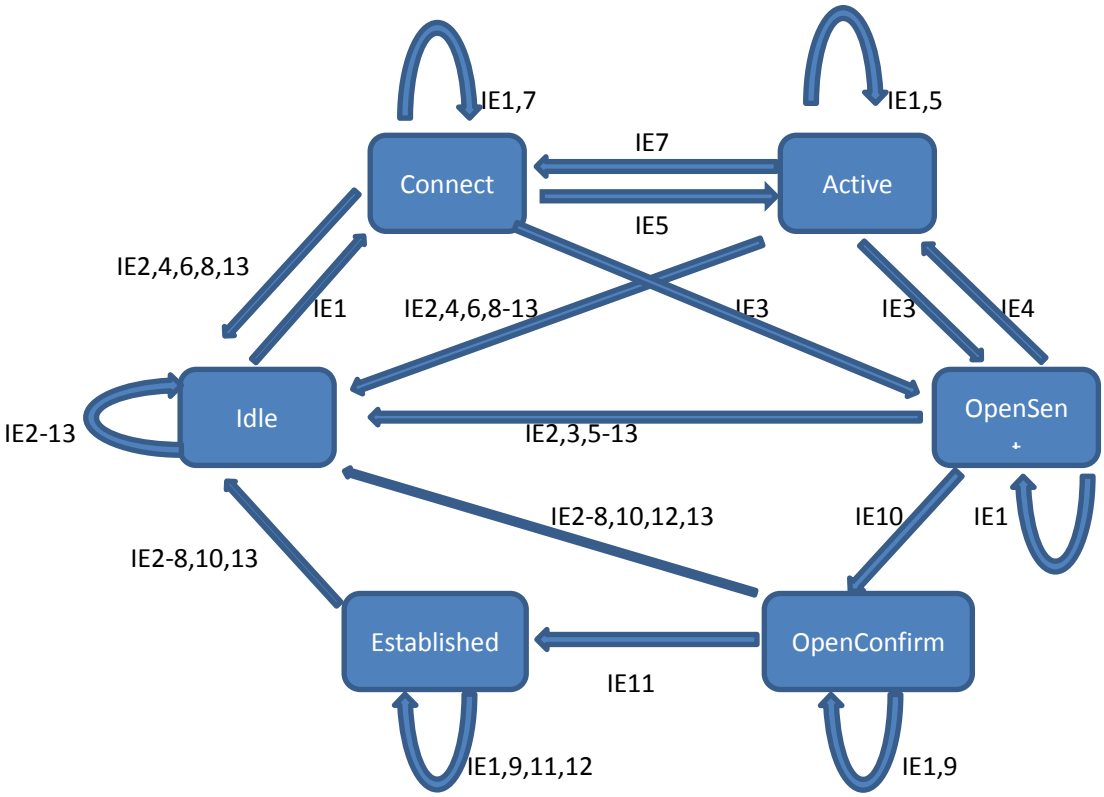
BGP 有限状态机具有以下 6 种状态：

1)Idle 2)Connect 3)Active 4)OpenSent 5)OpenConfirm 6)Established

BGP 有限状态机中引起状态变迁的 BGP 事件包括以下 13 种：

1)BGP Start 2)BGP Stop 3)BGP Transport connection open
4)BGP Transport connection closed 5)BGP Transport connection open failed
6)BGP Transport fatal error 7)ConnectRetry timer expired
8)Hold Timer expired 9)KeepAlive timer expired 10)Receive OPEN message
11)Receive KEEPALIVE message 12)Receive UPDATE message
13)Receive NOTIFICATION message

BGP 状态机如下图所示。一个典型的过程为：Idle（启动消息）—>Connect（TCP 连接成功，发 OPEN）—>OpenSent（收到 OPEN 消息，协商成功）—>OpenConfirm（收到 KEEPALIVE 消息）—>Established（TCP 连接关闭，有错误，或处理 UPDATE 消息失败，或收到 NOTIFICATION 消息）—>Idle。



1> Idle 状态

BGP 总是从 IDLE 状态开始，此时拒绝所有外来连接。当一个 Start 事件（IE1）发生（如操作者手动配置 BGP 进程或复位现有的 BGP 进程等），BGP 进程将初始化所有 BGP 资源，启动计时器，并初始化与邻居 BGP 路由器之间的 TCP 连接，监听来自邻居路由器的 TCP 初始化，并将自己的状态置为 Connect。

2> Connect 状态

在此状态，BGP 进程等待 TCP 建立连接完成。若 TCP 建立连接成功，BGP 进程将清除 ConnectRetry 计时器，完成初始化，并向邻居发送 OPEN 消息，且将自己状态置为 OpenSent 状态。若 TCP 建立连接不成功，BGP 进程将继续监听来自邻居的连接，复位 ConnectRetry 计时器，并将自己状态转为 Active。

若在此状态 ConnectRetry 计时器超时，此计时器将被复位，进程将再次试图与邻居建立 TCP 连接，状态仍保持在 Connect 状态。在该状态下，出 IE1 外的其他事件都将使 BGP 状态回到 Idle 状态。

3> Active 状态

在此状态，BGP 进程试图初始化与邻居的 TCP 连接，若 TCP 建立连接成功，BGP 进程清除 ConnectRetry 计时器，完成初始化，并向邻居发送 OPEN 消息，且将自己状态置为 OpenSent 状态。

若在此状态 ConnectRetry 计时器超时，进程将回到 Connect 状态，并复位 ConnectRetry 计时器，且初始化 TCP 连接，监听 TCP 连接。在该状态下，出 IE1 外的其他事件都将使 BGP 状态回到 Idle 状态。

4> OpenSent 状态

在此状态，Open 消息已经被发送，BGP 进程将等待来自邻居的 OPEN 消息。当收到来自邻居的 Open 消息时，BGP 进程将检查消息的所有域，若存在错误，则发送 Notification 消息，并将自己状态置为 Idle。若 Open 消息中没有错误，则发送一个 KeepAlive 消息，置 KeepAlive 计时器。并将自己状态置为 OpenConfirm。

若发生 TCP 断连，本地进程将关闭 BGP 连接，重置 ConnectRetry 计时器，并开始监听新的连接。自己的状态被置为 Active。在该状态下，出 IE1 外的其他事件都将使 BGP 状态机回到 Idle 状态。

5> OpenConfirm 状态

在此状态，BGP 进程等待 KeepAlive 消息或 Notification 消息。若收到 KeepAlive 消息，则将自己状态转到 Estabilished 状态。

若在收到 KeepAlive 消息之前 Hold 计时器超时，则发送一个 Notification 消息，其中错误代码为 Hold Timer Expired，并将状态转为 Idle。若收到 Notification 消息，则转换状态到 Idle 状态。若 Hold 计时器超时，或发生错误，或发生 Stop 事件，则发送一个 Notification 消息到邻居，关闭 BGP 连接，并转换状态到 Idle 状态。

6> Established 状态

在此状态，BGP 对等体之间的连接被完全建立，此时可以交互各种 BGP 消息。若 KeepAlive 计时器超时，则发送一个 Keepalive 消息，并复位 KeepAlive 计时器。

若收到 Notification 消息，则转换状态到 Idle 状态。若 Hold 计时器超时，则发送一个 Notification 消息，其中错误代码为“Hold Timer Expired”，并将自己状态转为 Idle。在该状态下，出 IE1 外的其他事件都将使 BGP 路由器发送 Notification 消息，其中错误代码为 Finate State Machine Error，并将 BGP 状态转换到 Idle 状态。

三、实验内容

<1> 实验要求

本实验要求学生根据系统的各种输入事件，进行 BGP 状态的变迁，并根据 BGP 协议进行相应的处理。

<2> 接口函数说明

本实验中需要学生实现的接口函数包括收到 Open 消息事件处理函数、收到 KeepAlive 消息事件处理函数、收到 Notification 消息事件处理函数、收到 Update 消息事件处理函数、TCP 连接异常事件处理函数、计时器超时事件处理函数、BGP 开始事件处理函数、BGP 结束事件处理函数和收到连接结果事件处理函数。

1> 收到 Open 消息事件处理函数：

BOOLEAN stud_bgp_FsmEventOpen (BgpPeer *pPeer, BYTE *pBuf, unsigned int len)

2> 收到 KeepAlive 消息事件处理函数：

BOOLEAN stud_bgp_FsmEventKeepAlive (BgpPeer *pPeer, BYTE *pBuf, unsigned int len)

3> 收到 Notification 消息事件处理函数：
BOOLEAN stud_bgp_FsmEventNotification (BgpPeer *pPeer, BYTE *pBuf, unsigned int len)

4> 收到 Update 消息事件处理函数：
BOOLEAN stud_bgp_FsmEventUpdate (BgpPeer *pPeer, BYTE *pBuf, unsigned int len)

5> TCP 连接异常事件处理函数：
Void stud_bgp_FsmEventTcpException (BgpPeer *pPeer, BYTE msgType)

6> 计时器超时事件处理函数：
Void stud_bgp_FsmEventTimerProcess (BgpPeer *pPeer, BYTE msgType)

7> BGP 开始事件处理函数：
Void stud_bgp_FsmEventStart (BgpPeer *pPeer)

8> BGP 结束事件处理函数：
Void stud_bgp_FsmEventStop (BgpPeer *pPeer)

9> 收到连接结果事件处理函数：
Void stud_bgp_FsmEventConnect (BgpPeer *pPeer)

系统提供的函数如下：

1> 试图建立连接函数：
Void bgp_FsmTryToConnectPeer()

2> TCP 段发送函数：
Void bgp_FsmSendTcpData (char *pBuf, DWORD dwLen)

<3> 数据结构定义

本实验中，实验系统定义了如下 BGP 对等体结构

```
Struct BgpPeer
{
    DWORD bgp_dwMyRouterID;     //本路由器的路由器 ID
    WORD bgp_wMyAS;             //本路由器所属的 AS
    DWORD bgp_dwCfgHoldtime;    //设置的 holdtime 时间值
    BYTE bgp_byState;           //协议状态机
    BYTE bgp_bAuth;             //是否有认证信息
}
```

四、实验代码

见附件。

五、实验收获

刚开始做实验的时候对实验内容的理解还不是很深刻，只是按照实验指导书的状态转移图来一点点的实现，在检查时通过和助教的交流，更加深刻的理解了 TCP 建立连接的状态和 BGP 建立连接的状态，对 BGP 协议的整体有了更深的体会。