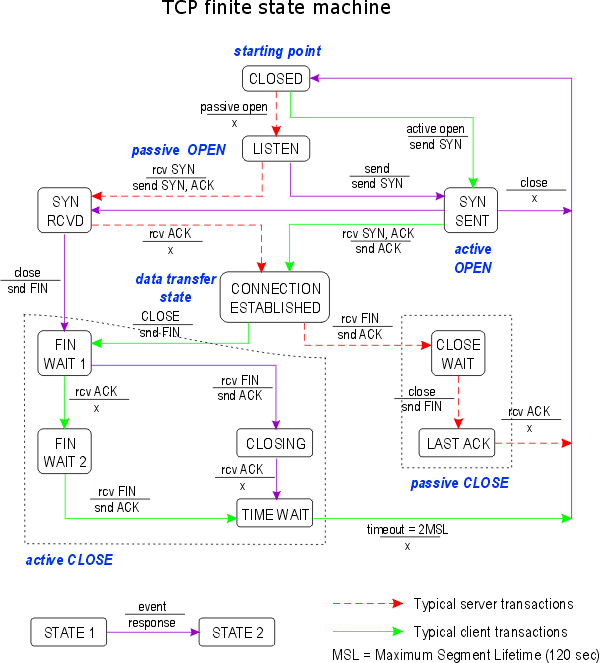
更详细的解释 [请点击](../select%20file扩展性阅读/网络相关/防火墙/iptables.docx)

·1 TCP有限状态机。TCP finite state machine



服务器端一般为被动打开passive open，而客户端一般为主动打开active open。

ESTABLISHED

SYN SEND

SYN RCVD

SYN=1 ACK=1

SYN=1 ACK=0

S

C

**·下面为三次握手阶段的TCP状态类型**。

SYN=0 ACK=1

**· 下面为四次断开阶段的TCP状态类型。**

LAST ACK

CLOSE-WAIT

TIME-WAIT

FIN-WAIT2

FIN-WAIT1

ACK=1

FIN=1

ACK=1

FIN=1

# ·2 Netfilter 数据报文过滤框架

**· 共有5个hook function（钩子函数），每个钩子函数都可以添加诸多规则，并被调用。**

1 input

2 output

3 forward 转发

4 prerouting

5 postrouting

**·每条规则被匹配到后，立刻进行相应动作，而不会理会接下来的规则了。**

**· 相同函数组成的诸多规则可组成链，每条连可以被分为不同的功能。**

**功能：**

Filter(过滤)：表

INPUT 应用于进入当前主机的数据包

OUTPUT 应用于当前主机传输出去的数据包

FORWARD 应用于数据包目的地非本机，也就是该包将要被转发的情况

Nat（地址转换）：表

PREROUTING 进行路由判断之前所进行的规则

POSTROUTING 进行路由判断之后所进行的规则。

OUTPUT

Mangle（修改报文，破坏者）：表

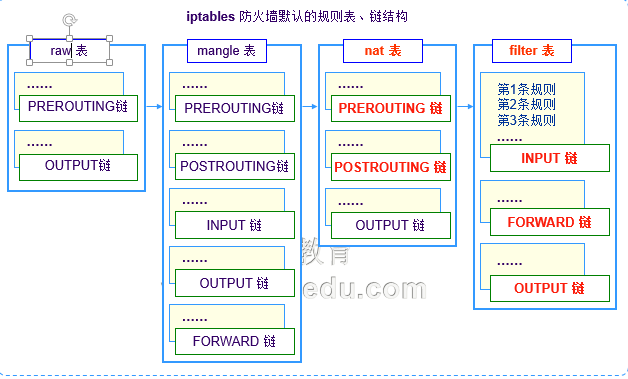
All

Raw（原始，不修改）：表

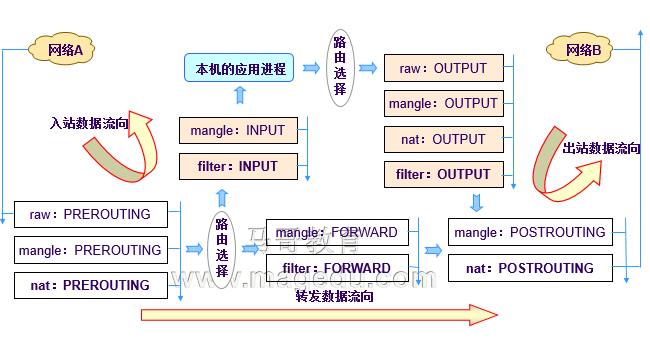
OUTPUT

PREROUTING

用户也可以自定义链，在某些链中被调用，方便用户管理。用户可以删除自定义的空链，但默认链无法删除。



**· 数据包过滤匹配流程**



3 数据包状态

NEW状态的数据包说明这个数据包是收到的第一个数据包。比如收到一个SYN数据包，它是连接的第一个数据包，就会匹配NEW状态。第一个包也可能不是SYN包，但它仍会被认为是NEW状态。

ESTABLISHED：

只要发送并接到应答，也就是S端收到SYN=0,ACK=1,C端收到SYN=1,ACK=1时，一个数据连接就从NEW变为ESTABLISHED,而且该状态会继续匹配这个连接后继数据包。

RELATED：

当一个连接和某个已处于ESTABLISHED状态的连接有关系时，就被认为是RELATED，也就是说，一个连接想要是RELATED的，首先要有个ESTABLISHED的连接，这个ESTABLISHED连接再产生一个主连接之外的连接，这个新的连接就是RELATED。

INVALID：

INVALID状态说明数据包不能被识别属于哪个连接或没有任何状态。