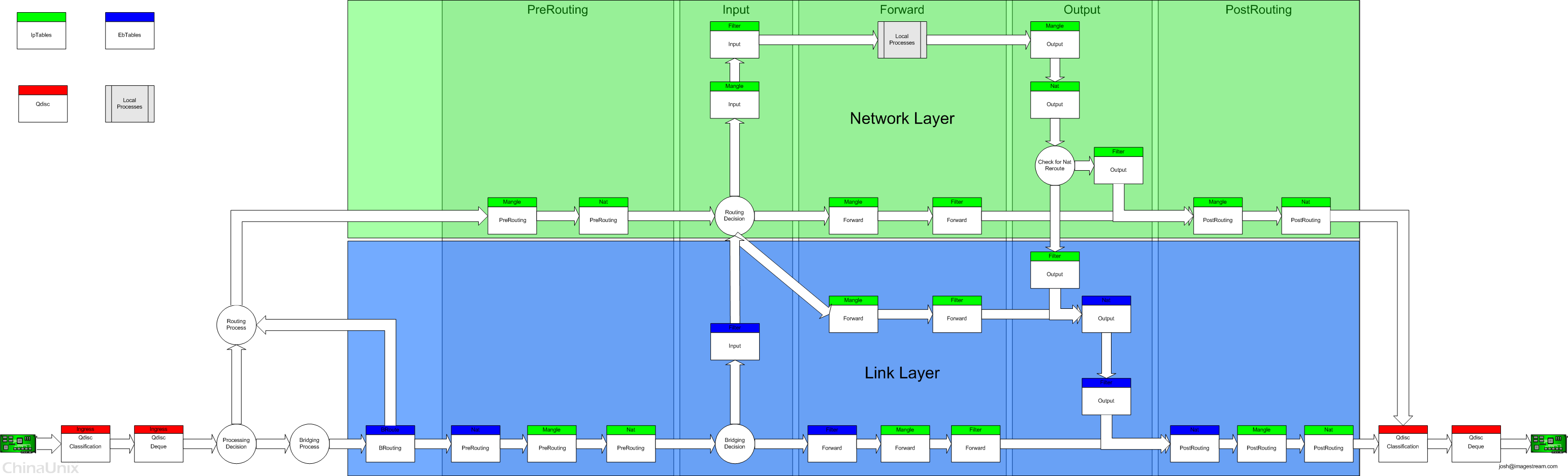
**[ebtables基本使用](http://www.cnblogs.com/peteryj/archive/2011/07/24/2115602.html)**

ebtables和iptables类似，都是Linux系统下网络数据包过滤的配置工具。既然称之为配置工具，就是说过滤功能是由内核底层提供支持的，这两个工具只是负责制定过滤的rules.

这里主要介绍ebtables，iptables类似。  
一、过滤时机  
要了解过滤时机，首先得了解网络数据包进入网卡后，在系统中的转换流程，见图：



从上图可以看到数据包从进入到离开系统，要经过PreRoute，Input，Forward，Output，PostRoute这五个阶段。每个阶段中包括了一些节点，每个节点就是一个过滤时机。当数据包行进到某个节点时，系统就是检测对应节点的过滤规则并进行过滤。从图中还可以发现，对于每个阶段，ebtables的过滤时机都比iptables要早。

二、ebtables配置  
ebtables的配置分为表、链和规则三级。  
1. 表  
表是内置且固定的，共有三种: filter, nat, broute，用-t选项指定。最常用的就是filter了，所以不设-t时默认就是这个表。nat用于地址转换，broute用于以太网桥。  
2.  链  
链有内置和自定义两种 。不同的表内置的链不同，这个从数据包的流程图中就可以看出来。所谓自定义的链也是挂接在对应的内置链内的，使用-j让其跳转到新的链中。  
3. 规则  
每个链中有一系列规则，每个规则定义了一些过滤选项。每个数据包都会匹配这些项，一但匹配成功就会执行对应的动作。

所谓动作，就是过滤的行为了。有四种，ACCEPT，DROP，RETURN和CONTINUE。常用的就是ACCEPT和DROP，另两种就不细述了。

三、ebtables基本命令  
有了上面的简单介绍，再熟悉一些基本命令就可以使用了。  
1. 列表：  
ebtables -L  
ebtables -L –Lc , 查看各rule的匹配次数以及字节数  
2. 新建/删除链  
ebtables -N <chain\_name>  
ebtables -X <chain\_name>  
3. 新建规则  
ebtables -A <chain\_name> [ rules ]  
[rules]有几种  
-s 源MAC -d 目标MAC -i 入接口 -o 出接口

参考文档: ebtables User Manual  
<http://ebtables.sourceforge.net/misc/ebtables-man.html>

Ebtables即是以太网桥防火墙，以太网桥工作在数据链路层，Ebtables来过滤数据链路层数据包。 2.6内核内置了Ebtables，要使用它必须先安装Ebtables的用户空间工具（ebtables-v2.0.6），安装完成后就可以使用ebtables来过滤网桥的数据包。 参照用户实际要求，设置ebtables规则如下：

1:对所有的数据包默认通过   
2:分清楚源地址和目的地址和源端口和目的端口   
3:对TCP,UDPP数据包分别过滤

Ebtables使用规则如下：

ebtables [-t table] -[ADI] chain rule-specification [match-extensions] [watcher-extensions]

-t table :一般为FORWARD链。

－ADI：A添加到现有链的末尾；D删除规则链（必须指明规则链号）；I插入新的规则链（必须指明规则链号）。

-P:规则表的默认规则的设置。可以DROP,ACCEPT,RETURN。

-F:对所有的规则表的规则链清空。

-L:指明规则表。可加参数，--Lc,--Ln

-p:指明使用的协议类型，ipv4,arp等可选（使用时必选）详情见/etc/ethertypes

--ip-proto:IP包的类型，1为ICMP包，6为TCP包，17为UDP包，在/etc/protocols下有详细说明

--ip-src:IP包的源地址

--ip-dst:IP包的目的地址

--ip-sport:IP包的源端口

--ip-dport:IP包的目的端口

-i:指明从那片网卡进入

-o:指明从那片网卡出去

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

简单配置规则如下：

#!/bin/bash

echo "The ebtables start !"

ebtables -P FORWARD ACCEPT

ebtables -P INPUT ACCEPT

ebtables -P OUTPUT ACCEPT

ebtables -F

ebtables -A FORWARD -p ipv4 -i eth0/eth1 --ip-proto (6/17) --ip-dst(目的IP)  --ip-dport(目的端口) -j DROP

ebtables -A FPRWARD -p ipv4 -i eth0/eth1 --ip-proto (7/17) --ip-src(源IP) --ip-sport(源端口) -j

DROP