

基于过滤的转发

Juniper 网络公司，爱立信公司，2001 年 5 月

目录

内容提要.....	2
基于过滤器的转发的概念界定.....	2
分组分类.....	2
过滤器操作.....	2
基于过滤器的转发实例.....	3
语法样本.....	3
基于过滤器的转发应用.....	5
开放接入.....	6
BGP/MPLS VPNs (RFC 2547Bis).....	6
没有 MPLS 的流量工程.....	7
结论.....	8
缩略语.....	8

内容提要

基于过滤器的转发允许配置分组过滤器，根据包头信息对分组分类，如IP信源地址、IP信宿地址、IP协议字段、信源和信宿TCP/UDP端口编号。如果某个分组与过滤器条件相匹配，那么将采用过滤器定义语言中接收操作所规定的路由表，执行传统的基于信宿的转发。基于过滤器的转发提供了一个非常简单而又功能强大的工具—基于策略的路由表选择程序。

基于过滤器的转发的概念界定

基于过滤器的转发允许定义一个分组过滤器，检查分组包头中的字段，来控制客户流量的下站选择。如果一个分组符合过滤器的匹配条件，那么将使用过滤器操作语句中规定的路由表例程转发分组。

可以把基于过滤器的转发只配置成输入分组过滤器，在输出分组过滤器上则不支持使用这种功能。

分组分类

分组过滤器可以根据任何字段对分组进行分类，可以使用JUNOS™ Internet软件过滤器定义语言检查这些字段。这些字段包括：

- 信源和/或信宿IP地址
- 协议号码
- 信源和/或信宿端口编号
- IP 优先值
- DSCP 值
- IP 选项
- TCP 标记
- 分组长度
- ICMP 类型
- 进入和/或输出的逻辑或物理接口

过滤器操作

如果一个分组符合过滤器的条件，那么您可以指定过滤器操作，称为路由例程。这种过滤器操作允许指定路由表例程，用来转发与过滤器的条件相符的流量。一旦确定了路由表，将执行传统的基于信宿的路由操作。除路由例程操作外，您还可以在过滤器指明下述操作修改程序：

- 告警
- 计数
- 日志
- 输出队列
- PLP

- 策略
- 采样

基于过滤器的转发实例

图1 说明了分组流动实例，其中使用输入分组过滤器对分组分类。根据分组分类进程结果，每个分组都采用不同的路由表转发到不同的下站上。

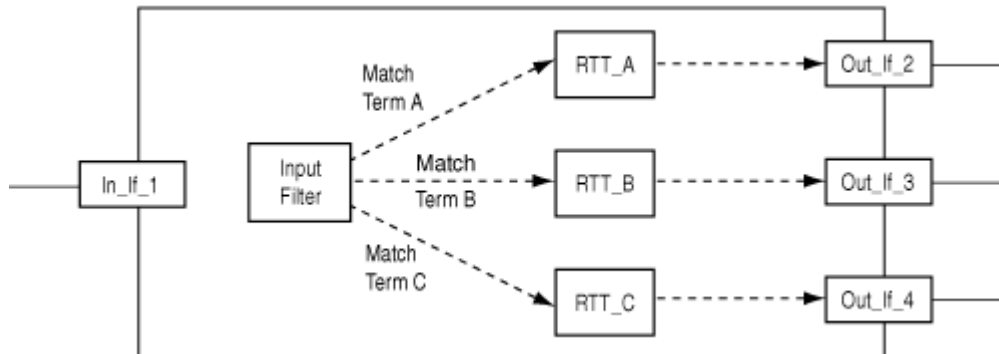


图1：分组流动实例

在本例中，进入的分组到达if_1。Internet Processor II™ ASIC使用进入分组过滤器对每个分组进行检查。如果分组与过滤器上的条件1相符，那么将采用RTT_A执行基于信宿的转发。如果分组与过滤器的条件2相符，那么将采用RTT_B执行基于信宿的转发。如果分组与过滤器上的条件3相符，那么将采用RTT_C执行基于信宿的转发。

注：JUNOS软件目前不支持把通信流量映射到LSP上。

语法样本

本节提供了语法样本，说明了可以怎样配置M系列路由器上基于过滤器的转发。第一个配置部分定义了一个分组过滤器，根据分组的信源地址把客户流量直接指向ISP 1或ISP 2中的下站路由器。图2说明了这一实例的网络拓扑结构。

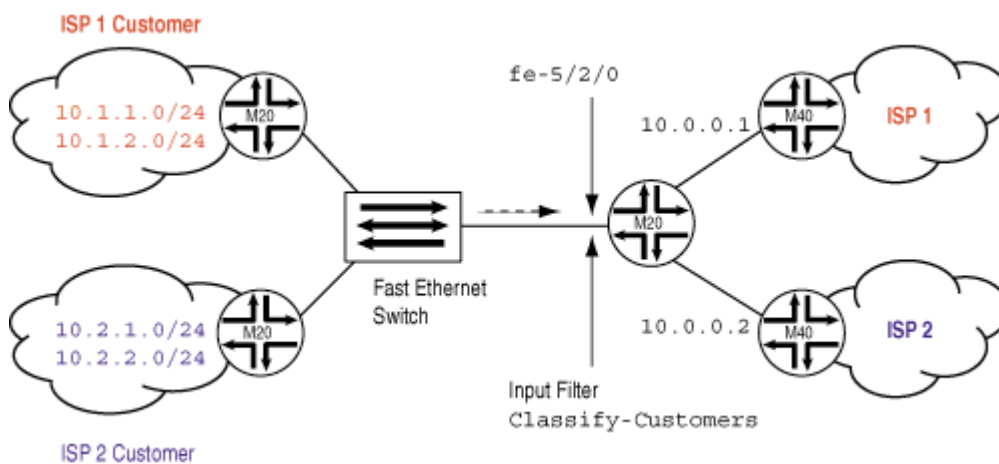


图2：语法样本实例的网络拓扑结构图

如果分组带有一个分配给ISP 1客户的信源地址，那么将采用isp1路由表执行基于信宿的转发。如果分组带有一个分配给ISP 2客户的信源地址，那么将采用isp2路由表执行基于信宿的转发。如果分组没有符合任何条件，那么过滤器将接收分组，然后使用标准inet.0路由表执行基于信宿的转发。

```
filter classify-customers {
  term isp1-customers {
    from {
      source-address { /* ISP 1 customer prefixes */
        10.1.1.0/24;
        10.1.2.0/24;
      }
    }
    then {
      routing-instance isp1-route-table;
    }
  }
  term isp2-customers {
    from {
      source-address { /* ISP 2 customer prefixes */
        10.2.1.0/24;
        10.2.2.0/24;
      }
    }
    then {
      routing-instance isp2-route-table;
    }
  }
  term default { /* Accept all other traffic */
    then {
      accept; /* Forward using inet.0 */
    }
  }
}
```

下面的配置部分定义了classify-customers (对客户分类) 过滤器中参考的路由例程。

```
routing-instance {
  isp1-route-table {
    instance-type forwarding;
    static {
      route 0.0.0.0/0 nexthop 10.0.0.1; /* Static default route */
    }
  }
}
```

```
isp2-route-table {
  instance-type forwarding;
  static {
    route 0.0.0.0/0 nexthop 10.0.0.2; /* Static default route */
  }
}
```

下面的配置部分分解路由例程中安装的接口路由，把分组转发到该接口上直接连接的下一站。

```
routing-options {
  interface-routes {
    rib-group inet fbf-group;
  }
  rib-groups {
    fbf-group {
      import-rib [inet.0 isp1-route-table.inet.0
                 isp2-route-table.inet.0];
    }
  }
}
```

下面的配置部分把classify-customers过滤器作为进入分组过滤器分配给路由器接口fe-5/2/0。

```
interfaces fe-5/2/0 {
  unit 0 {
    family inet {
      filter {
        input classify-customers;
      }
    }
  }
}
```

基于过滤器的转发应用

您可以使用基于过滤器的转发支持大量的服务供应商应用，包括：

- 开放接入
- BGP/MPLS VPNs (RFC 2547bis)
- 没有 MPLS 的流量工程

开放接入

基于过滤器的转发的最大的应用之一是满足开放接入要求。开放接入是一种Internet同等功能，允许用户选择自己的长话运营商，而不一定是提供本地环路的市话供应商。与电话网类似，Internet接入供应商必需允许竞争对手接入其基础设施，以允许客户选择自己的ISP转接供应商。图3说明了采用基于过滤器的转发来满足服务供应商开放接入要求的一种方式。

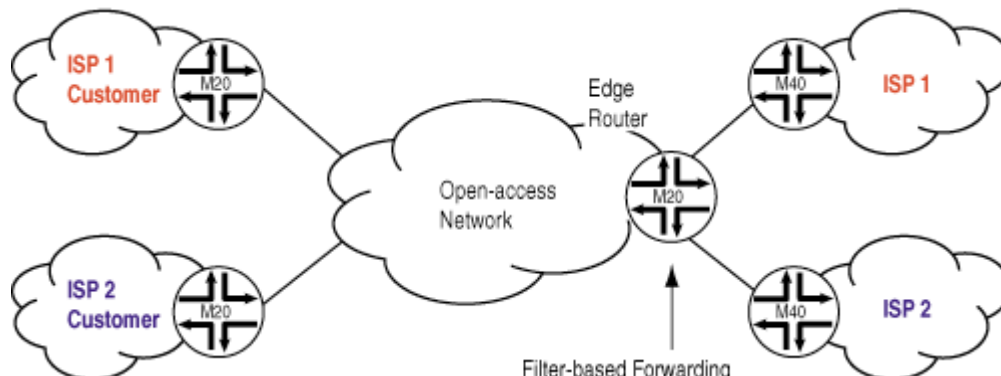


图3：满足供应商开放接入的要求

开放接入网络供应商(拥有共享线缆调制解调器、DSL或以太网基础设施) 必须拥有一个IP地址池，其中包括其提供客户接入的每个不同ISP的IP地址。开放接入供应商为每个特定ISP的客户分配这些地址。由于这些用户发出的流量必须转发到相应的ISP，因此离开开放接入网络的流量转发决策不能仅基于每个包头中携带的信宿地址。

在这一解决方案中，开放接入网元发出的所有客户流量都采用默认的路由，路由到接入供应商的边缘路由器上。在客户分组到达接入供应商边缘路由器的进入端口时，将根据每个分组的信源地址执行基于过滤器的转发分析，然后把分组转发到分组过滤器结果决定的相应的ISP转接供应商上。

BGP/MPLS VPNs (RFC 2547bis)

基于过滤器的转发的一种新兴应用是支持客户通过开放接入网络接入第三层BGP/MPLS VPN。在典型的RFC 2547bis VPN中，每台PE路由器采用与分组进入接口相关的VPN路由和转发(VRF)表转发客户流量。一般来说，通过在VPN路由例程的配置中包括接口，可以把一个或多个路由器接口关联到或绑定到一个VPN上。通过把一个接口绑定到一个VPN上，可以使用VPN的VRF表为到达该接口上的任何分组制订转发决策。

如果属于不同VPN的不同CE路由获准使用开放接入网络接入一台公共PE路由器，那么必需采用一种机制，把每个进入分组与其VRF表映射起来，这样才可以正确地进行转发。基于过滤器的转发提供了一种非典型的解决方案，允许PE路由器根据物理或逻辑接口绑定之外的属性，确定为一个VPN分配哪些流量(图4)。

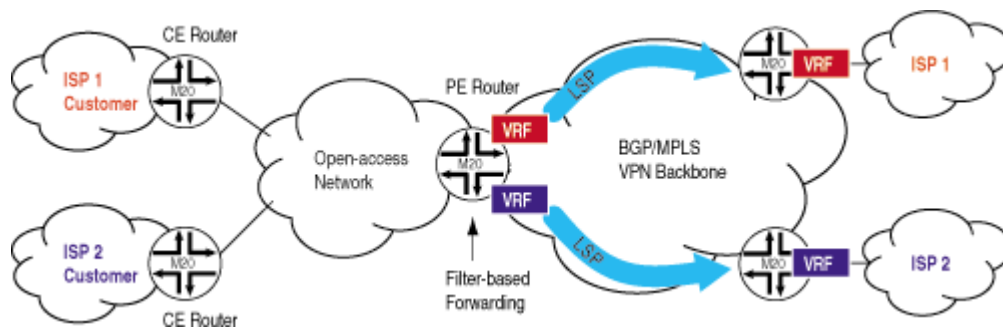


图4：支持BGP/MPLS VPN

在本例中，假设VPN_Red与ISP 1相关，VPN_Blue与ISP 2相关。连接开放接入网络的PE路由器配有一个入站分组过滤器，决定使用VRF_Red (ISP 1的客户)转发哪些流量，根据VRF_Blue (ISP 2的客户)转发哪些流量。

作为服务供应商，基于过滤器的转发允许您以巨大的灵活性提供BGP/MPLS VPN服务。

- 您可以提供一个单向VPN，其中客户站点发出的出局流量流经BGP/MPLS VPN基础设施，返回流量则沿着尽力而为的IP路由路径传送。
- 您可以配置一台PE路由器，使到达开放接入网络接口的某些流量沿着BGP/MPLS VPN路径传送，到达同一个接口上的其它流量则采用inet.0中包含的尽力而为的路由转发。
- 如果一台CE路由器的开放接入网络接口在物理上没有映射到一个VRF表，那么可以在物理上把连接到其它PE路由器的其它CE路由器的接口映射到一个VRF表上。

在支持这些连接选项时，如果采用迂回方法，则要求两台路由器的解决方案。第一台路由器执行基于策略的路由，对分组进行分类，然后把分组转出某个物理或逻辑接口。第二台路由器作为PE路由器使用，根据进入的物理或逻辑接口把流量映射到一个VRF表上(图5)。

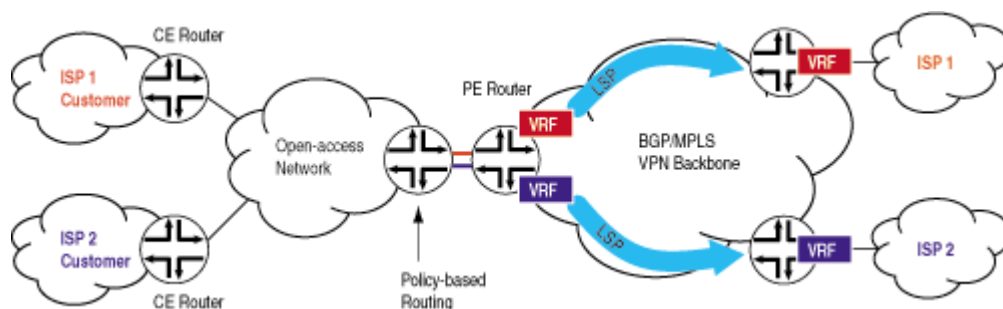


图5：基于策略的迂回路由解决方案

没有 MPLS 的流量工程

您还可以使用基于过滤器的转发，支持初步的流量工程形式，而不必部署MPLS。本例还说明了可以怎样采用基于过滤器的转发来支持基于应用的转发。看一下图6中的网络拓扑图。

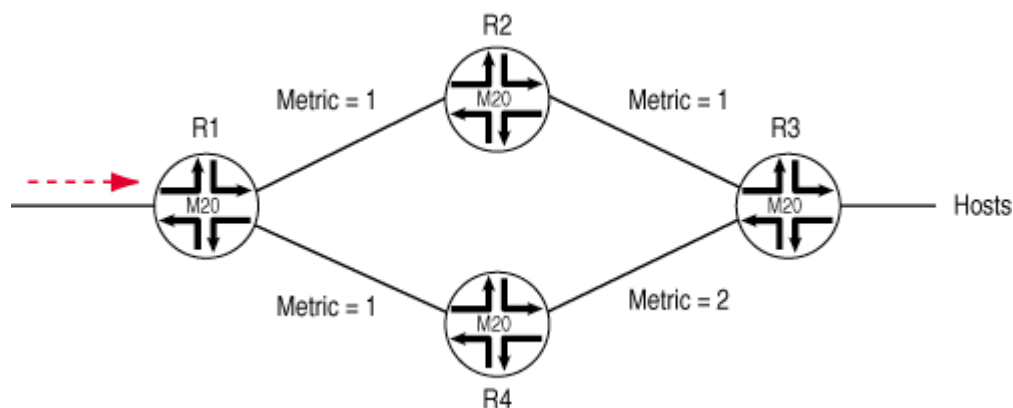


图6：支持初步流量工程

通过使用传统的基于宿的IP路由，到达R1（地址为R3下行主机）的所有流量都沿着从R1到R2到R3的成本最低的IGP量度路径传送。但是，为了满足特定的客户要求，假设您可能希望沿着从R1到R4到R3的拥塞程度最低、但成本较高的IGP量度路径转发所有VoIP流量。通过在R1上配置基于过滤器的转发，把地址为R3某个下行主机所有VoIP流量转发到R4的下站（而不是R2）上，您可以实现上述模式。

尽管执行基于过滤器的转发硬件具有性能上的优势，但必须指出，流量工程/基于应用的转发应用具有扩充能力限制，在下站消失或试图在多站中重定向时，这些局限性就会显现出来。这些局限性与JUNOS实现技术无关，相反，它们是部署静态路由的必然结果。

结论

基于过滤器的转发提供了一种基于策略的路由表选择工具，您可以使用这种工具支持大量的关键应用，包括开放接入、BGP/MPLS VPN和流量工程。基于过滤器的转发为控制服务提供商网络中的用户流量流动提供了另一种机制。

缩略语

ASIC	专用集成电路
BGP	边界网关协议
CE	客户边缘
DSL	数字用户线
DSCP	Diffserv编码点
ICMP	网际控制报文协议
IP	网际协议
ISP	互联网服务供应商
MPLS	多协议标记交换
PE	供应商边缘
PLP	丢包优先权
RFC	请求评论
TCP	传输控制协议
UDP	用户数据报协议

VPN 虚拟专用网
VRF VPN路由和转发