网关多WAN连接实现

培训目的

了解Linux对WAN连接的实现，
了解网关多WAN连接实现原理

培训对象

光通软件研发

培训讲师

方建江

培训课时

2小时

学习重点

1.VLAN与WAN连接
2.Linux下桥/路由WAN连接实现
3.策略路由

- 内容介绍

1. 多WAN连接的引入
2. VLAN简要说明
3. WAN连接实现
4. 策略路由、VLAN绑定

- # 1. 多WAN连接的引入

➢ 家用网关(Home Gateway)，诸多设备和技术的整合，包括通信产品整合、家庭娱乐产品联网整合、智能家电的联网整合等，是家庭网络的中心设备，作为家庭网络中心设备的家庭网关应具备三个方面的功能，即接入功能、业务功能和管理功能。

接入功能：用来实现数字家庭网络与公共网络的连接

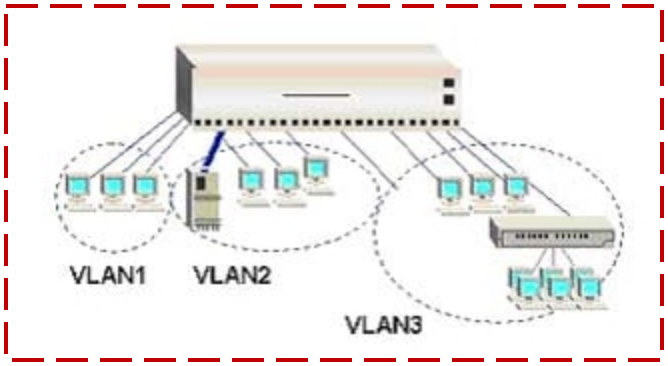
业务功能：完成部分公共网络推进到家庭中的业务功能

管理功能：地址功能、安全功能、服务质量（QOS）功能、远程管理功能、本地管理功能等

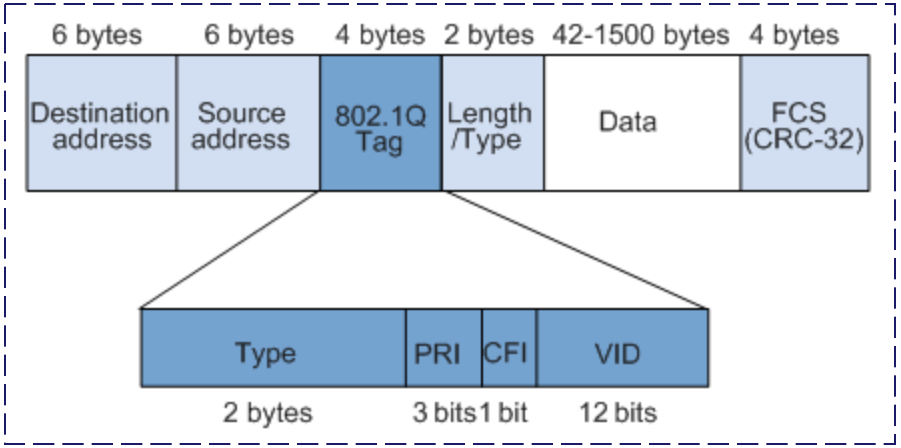
家用网关这种具备多业务及管理功能的特点，决定了其实现方式上的复杂性，一般消费类网关只有一条业务连接，这一连接可能同时具备远程管理(TR069)和网络接入功能，管理起来有很大的限制，多WAN连接业务则可以解决这一问题。

• VLAN（Virtual Local Area Network）

VLAN是一种将局域网（**LAN**）设备从逻辑上划分（注意，不是从物理上划分）成一个个网段（或者说是更小的局域网**LAN**），从而实现虚拟工作组（单元）的数据交换技术。



Type:长度**2Byte**，值为**0x8100**，表示**802.1Q**帧
PRI:长度为**3bit**，范围为**0~7**，表示帧的优先级，值越大优先级越高,主要为**QoS**差分服务提供参考依据
VID:长度**12bits**，可配置
VLAN ID取值范围为**1～4094**
802.1Q总大小为**4**个字节。



多WAN连接与VLAN的关系

➢VLAN的作用

(1) 端口的分隔。即便在同一个交换机上，处于不同VLAN的端口也是不能通信的。这样一个物理的交换机可以当作多个逻辑的交换机使用

(2) 隔离广播域，安全性也提高。不同VLAN不能直接通信，杜绝了广播信息的不安全性，控制广播风暴的产生

(3) 管理灵活。更改用户所属的网络不必换端口和连线，只更改软件配置就可以了

➢WAN连接：用于接入外部网络，通常指的是出口，转发来自内部 LAN 接口的 IP 数据包。

通过将数据包加上不同的VLAN TAG，可以进入不同的网络，对WAN连接而言，就可以获得不同的IP地址，也就可以在路由器中建立多个不同的逻辑网络链路，提供不同的服务。

VLAN 的配置命令是什么？如何创建一个VLAN设备用于处理VLAN报文？

- 2. WAN连接实现

- WAN连接类型

  - ROUTE(路由)

    - DHCP(Dynamic Host Configuration Protocol 动态主机配置协议)
    - STATIC
    - PPPOE(Point to Point Protocol over Ethernet)

  - BRIDGE(桥接)

- 建立路由WAN连接步骤
  - 获取WAN连接IP地址、子网掩码、网关地址、DNS信息
  - 设置WAN接口的IP/DNS/MASK/GATEWAY信息并且UP

echo 0 0 10.188.101.1 pon.1> /var/dproxy.conf

ifconfig pon.1 10.188.101.18 netmask 255.255.255.0 broadcast 10.188.101.255 up

  - 设置路由

增加一条默认路由：

route add default gw 10.188.101.1 dev pon.1

如果不设置为默认路由而是为目标网络：

route add -net 224.0.0.0 netmask 240.0.0.0 dev pon.1

  - 设置NAT规则

iptables -t nat -A nat_post_wan_conn -o pon.1 -s 192.168.1.0/255.255.255.0 -j MASQUERADE

MASQUERADE，地址伪装，算是**SNAT**中的一种特例，可以实现自动化的**SNAT**，配置 **MASQUERADE**就不用指定**SNAT**的目标**ip**了

- 问题
  - 1. 多条WAN连接存在时，数据包如何确定走哪一条WAN连接？
  - 2. 如何使特定的报文只走特定的WAN连接？
  - 3. 如何限制某一端口的用户侧数据包只走某一条WAN连接？

- 路由表

```
~ # route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 br1
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 br0
10.188.101.0    0.0.0.0         255.255.255.0   U     0      0        0 pon.1
10.188.102.0    0.0.0.0         255.255.255.0   U     0      0        0 pon.2
127.0.0.0       0.0.0.0         255.255.0.0     U     0      0        0 lo
224.0.0.0       0.0.0.0         240.0.0.0       U     0      0        0 eth0
0.0.0.0         10.188.101.1    0.0.0.0         UG    0      0        0 pon.1
```

数据包的转发根据目的网络从路由表中查找确定走哪一条路由，当一个数据包的目的网段不在你的路由记录中，那么路由器该把那个数据包发送到哪里？

- 策略路由(Policy Route)

➢ 策略路由根据实际的应用需求来进行报文的转发，可以是协议类型、应用、报文大小、或IP源地址中的一个或多个的组合。当数据包经过路由器转发时，路由器根据预先设定的策略对数据包进行匹配，当匹配到一条策略，就根据该条策略指定的路由进行转发；当没有匹配到任何策略，就使用路由表中的各项数据目的地址对报文进行路由。

➢ Linux对策略路由的支持

从Linux-2.2开始，内核把路由归纳到许多路由表中，这些表都进行了编号，编号数字的范围是1到255。另外，为了方便，还可以在/etc/iproute2/rt_tables中为路由表命名。默认情况下，所有的路由都会被插入到表main(编号254)中。在进行路由查询时，内核只使用路由表main。

- Linux下的高级网络管理工具

➢ Iproute2是一个在Linux下的高级网络管理工具软件，Linux下的一些网络配置工具可完成大量的工作，实际上它是通过rtnetlink sockets方式动态配置内核，如route和ifconfig，实际上这些工具都调用了非常强大的iproute2的底层基本功能。

➢ 路由策略数据库在**/etc/iproute2/rt_tables**中描述，它可以支持255张路由表，其中有3张路由表是内置的，分别为本地路由表(local)描述本地接口地址、广播地址都放在这个表，主表(main)，如果没有指明路由所属的表，所有的路由都默认放在这个表里；默认路由表(default)，一般来说默认的路由都放在这张表，但是如果特别指明放的也可以是所有的网关路由。表0保留。

```
~ # ip ru list
0:      from all lookup local
32700:  from all iif br0 lookup RT_L_TO_W
32766:  from all lookup main
32767:  from all lookup default
32768:  from all lookup pon.1
32769:  from all lookup pon.2
~ #
```

```
~ # ip ro ls tab main
192.168.2.0/24 dev br1  proto kernel  scope link  src 192.168.2.1
192.168.1.0/24 dev br0  proto kernel  scope link  src 192.168.1.1
10.188.101.0/24 dev pon.1  proto kernel  scope link  src 10.188.101.18
10.188.102.0/24 dev pon.2  proto kernel  scope link  src 10.188.102.102
127.0.0.0/16 dev lo  scope link
224.0.0.0/4 dev eth0  scope link
default via 10.188.101.1 dev pon.1
~ #
```

- 配置策略路由
  - 添加路由记录

    ip route replace default dev pon.1 via 10.188.101.1 table pon.1

    修改默认路由为经过网关10.188.101.1，使其经过设备pon.1

    ip route add 10.0.0/24 via 193.233.7.65

    设置到网络10. 0. 0/24的路由经过网关193. 233. 7. 65

  - 增加路由策略规则

    ip ru add from all table pon.1 prio 32768

    通过路由表pon. 1来路由所有的包(from all)，规则优先级为32768

    ip ru add from 193.233.7.83 nat 192.203.80.144 table 1 prio 320

    把源地址为193. 233. 7. 83的数据报的源地址转换为192. 203. 80. 144，并通过表1进行路由

    IP命令使用方法请参考ip 命令手册

- 策略路由结合**Netfilter**

➢ 在Linux操作系统上，控制IP转发的机构除了路由外，还有重要的一个部分Netfilter。Netfilter对指定类型的IP数据报进行标记，加上策略路由的功能可以达到特定报文的特定路由转发。

➢ 实现方法

✓ 针对不同的策略建立各自的路由表

✓ 给满足不同条件的IP 数据报打上相应的标记

✓ 让带有不同标记的IP 数据报，使用相对应的路由表进行路由转发

- 策略路由结合**Netfilter**实例

➢ 设置从eth1进入的数据报必须走路由表pon.3：

➢ Netfilter中Ebtables规则

ebtables -t filter -A in_wan_conn -p IPv4 -i eth1 -j mark --mark-or 0x10 --mark-target CONTINUE

➢ 策略路由规则

ip rule add pref 32699 fwmark 16 table pon.3

```
~ # ip ru
0:      from all lookup local
32699:  from all fwmark 0x10 lookup pon.3
32700:  from all iif br0 lookup RT_L_TO_W
32766:  from all lookup main
32767:  from all lookup default
32768:  from all lookup pon.1
32769:  from all lookup pon.2
32770:  from all lookup pon.3
~ #
```

注意DNS报文：DNS解析IP地址时也必须走对应的WAN连接，否则会导致DNS解析失败

- # 桥接WAN
- 网桥工作在数据链路层，将两个LAN连起来，根据MAC地址来转发帧，可以看作一个“低层的路由器”。

- 网桥的配置步骤
  - 创建网桥设备 **br0**：

    brctl addbr br0
  - 向**br0**中添加网卡：

    brctl addif br0 eth0

    brctl addif br0 eth1

```
~ # brctl show
bridge name     bridge id               STP enabled     interfaces
br0             8000.008909081000       yes             eth0
                                                        eth1
br1             8000.000000000000       no
~ # brctl showmacs br0
port no mac addr                is local?       ageing timer
  1     00:89:09:08:10:00       yes                0.00
  1     20:f4:1b:80:01:7c       no                 1.25
~ #
```

- # VLAN绑定

- 对于路由WAN连接来说，不考虑VLAN的影响
- 对桥WAN连接来说，因为VLAN工作在链路层，会考虑VLAN对于转发的选择
- 实现原理
  - 创建一个VLAN设备用于处理带该VLAN的报文
  - LAN侧带VLAN的报文如果直接交由软桥br0进行处理，则会被丢弃，Kernel中收发包的位置对于是否存在该VLAN设备需要进行判断，如果存在则需要将该报文去掉vlan tag后，再交由桥处理
  - LAN侧带VLAN的报文被去掉TAG后，从WAN口发送出去前需要加上该绑定的WAN连接的VLAN头部

小结

- ✓ WAN连接建立过程
- ✓ 策略路由原理+Netfilter使用
- ✓ 桥接以及VLAN绑定

Thanks