

# TCP/IP 网络广播风暴控制技术

崔连春 (济南市电信局 250013)

**摘要:** 本文讨论了控制 TCP/IP 网络广播风暴的两种方法: 广播地址转向和基于

Spanning tree 的控制, 并结合我局 97 网络的具体情况, 找出了这两种控制技术的弊端, 分析原因并给出了解决办法。

**关键词:** BROADCAST TCP/IP STP IRDP HSRP

## 1 网络广播风暴的定义

在计算机网络中, 有很多时候要用到广播技术, 数据链路层和网络层都会用到广播, 前者将广播信息发送到多个物理设备, 后者将广播信息发送到多个逻辑设备。广播 (BROADCAST) 与组播 (MULTICAST) 是两个不同的概念, 其区别在于广播是以网络/子网为目标对象的, 而组播可以以分散在不同网络/子网内的一组主机为目标对象。在此, 只讨论广播。就 TCP/IP 而言, 有如下两种广播:

(1) 全面广播: 将广播数据发送到每一台主机, 如: 使用 255.255.255.255 广播地址进行广播。

(2) 部分广播: 这种情况是将信息广播到一个网络或子网, 如: 134.33.255.255 (网络广播地址), 134.33.81.255 (子网广播地址)。

在广播的过程当中, 如果被接收设备转发, 在多个转发设备之间就有可能出现“广播风暴”现象。一旦出现这种情况, 网络中就会出现大量的广播数据包重复传输, 降低网络性能, 甚至耗尽网络的带宽, 导致网络瘫痪, 严重影响网络上业务数据的传输。

对于这个问题, 必须采取有效的措施加以控制, 以下详细论述几种网络广播风暴的控制技术。

## 2 网络风暴控制技术

对于网络风暴, 有多种控制方法, 目前广泛应用的主要有两种: 即广播地址转向和基于 spanning tree 的控制。

### 2.1 广播地址转向

这种技术是通过在网络设备的端口上, 设置一个 IP 地址, 该端口收到的广播包的目标地址都被替换成指定的 IP 地址, 从而使不必要的广播包转发到指定的主机上。这样, 就有效地保护了网络的带宽资源和设备处理资源。由于网络设备的每个端口都有可能收到广播包, 所以, 必须在每个端口上作相应的配置。其配置方法如下:

```
Router(config)# ip forward-protocol udp
Router(config)# int E0
Router(config-if)# ip helper-address 134.33.81.11
Router(config-if)# ^z
```

广播地址转向的方法对于无冗余、无并行配置的网络, 可以有效地控制广播风暴, 但对于较复杂的网络, 该方法就暴露出一些新的问题:

- 配置繁琐。对于每个路由器上的每个端口都需要配置, 对于双向广播, 每个端口需要配置一个以上的 helper-address, 给网络的管理带来不便;
- 可能导致重复广播。

### 2.2 基于 spanning tree 的控制

这种方法是从网络的底层进行控制的: 网络层 (路由器) 识别出一个地址为广播地址之后, 就会将该广播包发送到相应的网络或子网, 进入到数据链路层。在数据链路层, 各网段通过网桥连接成 LAN, 为了避免两个网段之间有多于一个网桥 (即环路) 出现, 往往采用 spanning tree 算法, 在所有网段之间计算生成一棵无环连接树。因此,

在路由器接口上利用 spanning tree 算法，可以阻止广播数据包被再次发送到发出该数据包的接口，而且可以通过阻塞某些端口来防止广播数据包的重复。

作为 spanning tree 算法工作的前提，每个端口必须配置网桥，否则，该端口将只是接收广播数据包，而不进行转发；因为广播是针对网络而言的，所以应该将待控制网络的所有网络接口所配置的网桥归类到同一组，就如同 LAN 中的所有网桥都属于同一 LAN，只有这样，spanning tree 算法才可能计算出无环树，这是因为 spanning tree 算法计算的实例是确定的、封闭的，对于动态的网络，spanning tree 算法要对网络拓扑的每一次变动都需要重新计算 spanning tree。

具体配置过程如下：

```
Router(config)# ip forward-protocol udp
```

.....

```
Router (config)# bridge 1 protocol ieee {brige group = 1, type = ieee}
```

```
{All routers in the same network must enable the same STP}
```

```
Router (config)# interface E1 { e.g. interface E1}
```

```
Router (config-if)# bridge-group 1
```

```
Router (config-if)# bridge-group 1 input-type-list 10
```

```
Router (config-if)# ip broadcast-address 134.33.81.255
```

```
Router (config)# access-list 10 .....
```

### 3 典型网络配置

下面结合我局 97 网络的情况，具体看一下上述方法存在的弊端。为了便于说明问题，下面给出的网络拓扑图只是从 97 网络中抽取一部分，并作了适当的修改。实际上，这也是在控制网络广播风暴时，会经常遇到的一种典型的网络拓扑。

在图 1 所示的网络中，有两个并行的路由器 R1 和 R2，它们互为冗余备份，对于广播地址转向，只需要将路由器 R1 和 R2 的各端口的广播转向到另一个主机或网络，即能够消除“环路”问题，但却无法控制广播包的重复，问题已经十分直观，所以在此不加赘述。

在基于 Spanning tree 的控制方法中，这两个路由器的端口应在同一棵 Spanning tree 中，即所有接口配置的网桥属于同一组，而且都使用同样的协议类型。在每个端口上做类似于 2.2 所示的配置之后，“环路”问题就被解除，但

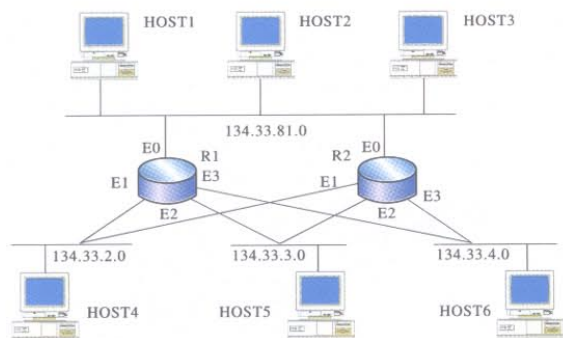


图 1 典型的网络拓扑

是尚不能解决广播包的重复问题，例如：HOST1 向 134.33.81.0 进行广播时，路由器 R1 和 R2 都分别收到三次同样的广播包，这三次广播包分别来自 134.33.2.0、134.33.3.0 和 134.33.4.0。造成此问题的根本原因在于 R1 和 R2 分别转发了来自 HOST1 的广播。如果能够使得 R1 和 R2 中只有一方转发广播，就会消除这种重复现象。同时，因为 R1 和 R2 是互为备份的，只需要一方转发广播包，就已经能够保证网络的正常运行。

为此，可以通过设置到达路由器各端口的 COST 值来控制 Spanning tree 的生成，阻止某些接口，从而减少不必要的广播转发的路径，消除重复广播。如：设定 R1 上各接口的 COST 值为 100，R2 为 80，则生成 Spanning tree 的时候，R2 的接口就被优先选用，而 R1 被阻塞，这样 HOST1 的广播就会只经过 R2 转发。具体配置方法如下：

```
Router (config)# interface e0
```

```
Router (config-if)# bridge-group 1 path-cost 80
```

经过上述配置，有效地解决了重复广播问题，可是这样以来，又出现了一个新问题：R2 的负荷太重了。如果让 R1 承担部分负荷，网络的整体性能岂不更好？基于这一目的，可以让 R1 承担单发数据包的传输工作，有很多办法可以实现这一目标，如：Proxy ARP，RIP，IRDP，HSRP 等，其中，Proxy ARP 方案中对作为 Proxy 的路由器的可靠性要求较高，一旦该路由器发生故障，即使还有别的路径可到达目的地，网络仍要中断，直到手工重新配置；而 RIP 对网络的拓扑变化收敛速度较慢，一般需要 3~10 分钟。因此，这些方案往往不被采用。下面，讨论一下两个常用的负载均衡方案：即

IRDP (ICMP Router Discovery Protocol) 和

HSRP (Hot Standby Routing Protocol)

#### 3.1 IRDP

这种办法首先要求每台主机上运行 IRDP 协议，通过在路由器上设置 IRDP 的有关参数，使 R1 成为主机单发

通信的首选网关，具体操作如下：

```
Router (config-if)# ip irdp
Router (config-if)# ip irdp maxadvertinterval 80
.....
```

```
Router (config-if)# ip irdp preference 80 {default = 100}
```

经过类似的配置后，假设R1的preference比较小，那么，在正常情况下，来自134.33.2.0、134.33.3.0和134.33.4.0的单发数据包，将经过R1，而广播包则经过R2，R1和R2的负载得到了均衡；一旦R1发生故障，网络主机监测不到来自R1的HELLO包时，R2的preference就成为当前最小的，于是单发数据包又会自动发向R2，R1和R2的相互备份功能就体现出来。

### 3.2 HSRP

HSRP引入了虚拟路由器的概念，所谓的“虚拟路由器”是这样—个路由器：它是逻辑意义上的，有自己的虚拟MAC和IP地址。HSRP是利用优先级机制来选择当前活跃状态的路由器的，它把当前优先级最高的路由器当作活跃路由器，当前活跃路由器不断组播HELLO包，一旦发生故障，HELLO包发送终止，于是STANDBY路由器就成为当作活跃路由器。其配置方法如下：

```
Router (config-if)# standby 1 ip 134.33.81.3
```

```
{134.33.81.3 is the virtual router ip address, 1 is Hot
```

```
Standby group #}
```

```
Router (config-if)# standby 1 preempt
```

```
{Become active when no router has higher priority}
```

```
Router (config-if)# standby 1 priority 110
```

```
.....
```

利用HSRP的优先级机制，也可以实现负载均衡的目标。如：将R1的优先级设置为一个较高的值，则单发数据包就会经过R1；一旦此路由器发生故障，原来次高优先级的路由器就成为当前优先级最高的，于是就变成活跃状态，代替原有活跃状态路由器并完成原有活跃路由器的工作。同IRDP一样，也实现了负载均衡和冗余热备的功能。

## 4 结束语

上述内容主要讲述了在TCP/IP网络中对广播风暴的控制技术。在当今网络发展日新月异的形势下，大量的数据业务向计算机网络上转移，这使广播风暴问题变得更加突出。充分利用这些技术，可以有效地控制广播风暴，对于提高网络的健壮性、优化网络的性能等，具有不可低估的作用。■