URPF 技术在防御(D)DoS 攻击方面的应用

邹羽婷

1 URPF 简介

1.1 背景介绍

通常情况下，路由器收到数据报文后，获取到数据包中的目的 IP 地址，针对目的 IP 地址查找本地路由转发表(DstIP, Next Hop)[3]，如果有对应转发表项则转发数据报文；否则，将报文丢弃。由此看来，路由器转发报文时，并不关心数据包的源地址。这就给源地址欺骗攻击有了可乘之机。

(D)DOS 攻击的方法很多，其中使用欺骗的源地址是常见方法。攻击者可以伪造一个源地址，该地址是另一个合法网络的地址，并且在全局路由表中存在。例如，攻击者伪造一个源地址使得被攻击者认为攻击来自于伪造的源地址，但实际上该源地址是完全无辜的，有时候网络管理员会因此而关闭所有来自该源地址的数据流，这样正好使得攻击者的拒绝服务攻击成功实现。更复杂的情形是 TCP SYN 洪泛攻击将使得 SYN-ACK 数据包发送到完全与攻击无关的许多主机，而这些主机就成了牺牲者。这使得攻击者可以同时去欺骗一个或者多个系统。 同样也可以采用 UDP 和 ICMP 洪泛攻击。

1.2 定义和功能

URPF（Unicast Reverse Path Forwarding）是单播逆向路径转发的简称，其主要功能是用于防止基于源地址欺骗的网络攻击行为，对于伪造源 IP 地址的 DoS 攻击非常有效。路由器接口一旦使能 URPF 功能，当该接口收到数据报文时，首先会对数据报文的源地址进行合法性检查，对于源地址合法性检查通过的报文，才会进一步查找去往目的地址的转发表项，进入报文转发流程；否则，将丢弃报文。

1.3 实现原理

URPF 首先获取报文的源 IP 地址和来源接口（入接口），而后以源地址为目的地址[3]，在

路由转发表(FIB 表)中查找相对应的项，找到则转发，否则丢弃。在松散模式下，查找 FIB 表中是否存在该 IP，若存在直接转发，不存在则丢弃；在严格模式下，除了要求 FIB 表中存在该 IP，并且要求转发接口与入接口匹配，若匹配则转发，否则认为该源地址是伪装的，并丢弃报文。

2 工作模式

URPF 有两种工作模式，分别是严格模式和松散模式，部分设备在此基础上，还进一步增加了缺省路由检查以及 ACL 检查功能，进而将 URPF 检查实现的更灵活和全面[4]。

2.1 严格模式

严格模式下，路由器不仅要求报文源地址在 FIB 表存在相应表项，还要求接口匹配才能通过 URPF 检查，即：路由器必须在用于转发返回数据包的接口上接收数据包。

严格模式下若遇到路由不对称的情况，即对端设备记录的路由路径不一样，此时使能 URPF 的路由器可能丢弃合法报文，造成路由器不能正确转发[1]。

如图 2.1.1，PC A 想要发送报文至 PC B。在 SwitchA 的 Interface1 接口上使用了 URPF 的严格模式，当 SwitchA 的 Interface1 接口收到了源地址为 10.1.1.1 的报文，SwitchA 搜索 FIB 表检测 IP 与接口是否匹配，发现 IP 为 10.1.1.1 的报文对应的转发接口为 Interface2（即：如果收到目的地址为 10.1.1.1 的报文则从 Interface2 接口转发），于是 SwitchA 丢弃了该报文。由于从 10.1.1.1 出发的报文和目的地址为 10.1.1.1 的报文的路由为非对称路由，导致合法报文被丢弃。

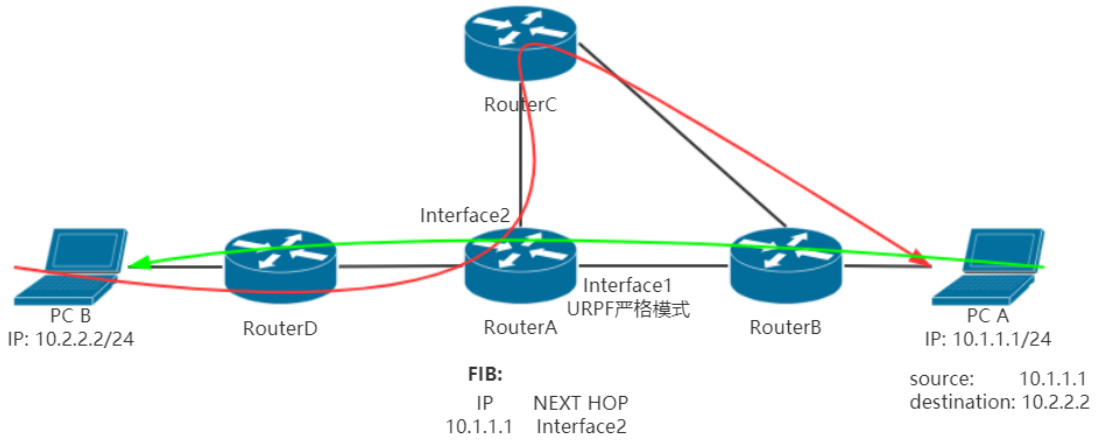

图 2.1.1 非对称路由示例

为了防止合法报文被丢弃，建议在路由对称的环境下使用 URPF 严格模式，例如两个网络边界设备之间只有一条路径。换种说法，只有在保证路由器接口上接收的所有数据包都来自于只分配给该接口的子网（use Unicast RPF in strict mode on network interfaces for which all packets received on an interface are guaranteed to originate from the subnet assigned to the interface[2]），在这种接口上使用 URPF 严格模式，能够最大限度的保证网络的安全性。

严格模式下的 URPF 应用[1]：

如图 2.1.2 所示，AS1 与 AS3、AS2 与 AS3 之间均为单连接。在 SwitchC 的 Interface1 接口和 Interface2 接口上配置 URPF，可以保护 AS3 免受来自 AS1 和 AS2 的源地址欺骗攻击。如果 AS1 中的主机 PC A 伪造了一个源地址为 10.2.2.2 的报文，向 AS3 中的 Server 发送请求。SwitchC 在接收到这个报文后，检查其入接口是否匹配，发现源地址为 10.2.2.2 的报文应该从 Interface2 进入，则 SwitchC 认为该报文源地址是伪造的，直接丢弃该报文。从 AS2 发向 Server 的正常报文，检查通过后，被正常的转发。

上述例子说明现实生活中严格模式一般在通过单链路接入的路由器上实施。

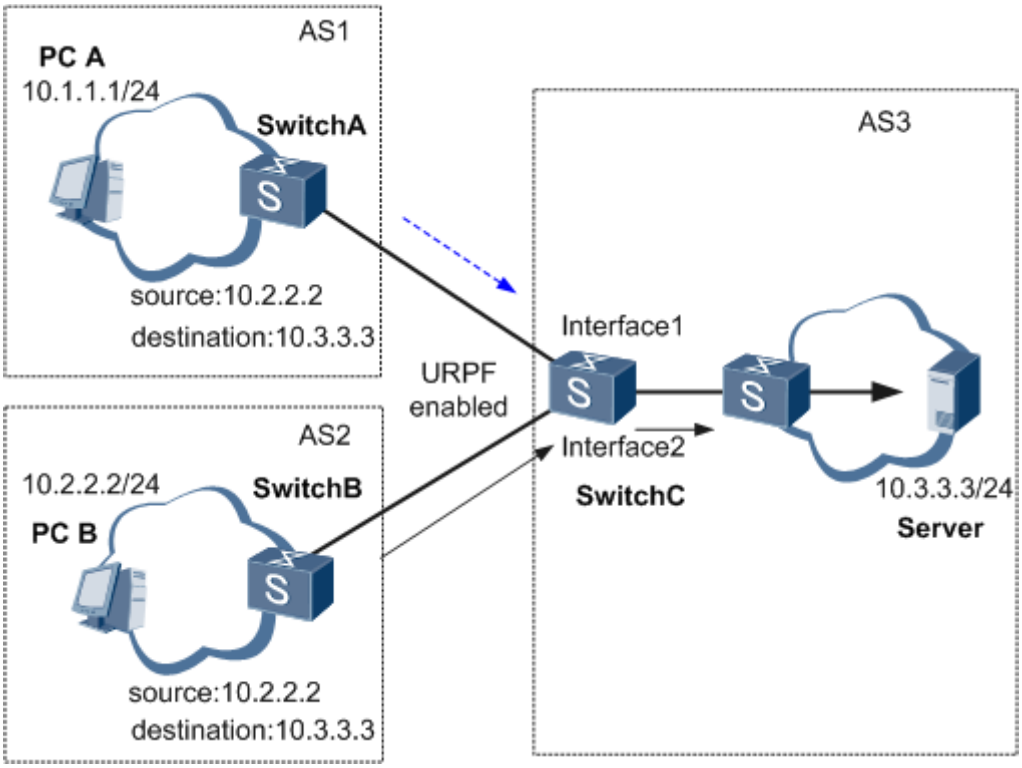

图 2.1.2 URPF 单宿主客户应用环境示意图

2.2 松散模式

松散模式下，路由器不检查接口是否匹配，只要 FIB 表中存在该报文源地址的路由，报

文就可以通过。

如图 2.1.1，在 2.1 小节中描述了在 SwitchA 的 Interface1 接口上使用 URPF 严格模式的情况。现在，我们在 Interface1 接口上使用 URPF 松散模式，当 SwitchA 的 Interface1 接口收到了源地址为 10.1.1.1 的报文，SwitchA 搜索 FIB 表，发现存在 IP 为 10.1.1.1 对应的转发路由，于是 SwitchA 直接转发该报文。报文被成功转发。

建议在不能保证路由对称的环境下使用 URPF 的松散模式，例如两个网络边界设备之间如果有多条路径连接的话，路由的对称性就不能保证，在这种情况下，URPF 的松散模式也可以保证较强的安全性[1]。

松散模式下的 URPF 应用[1]：

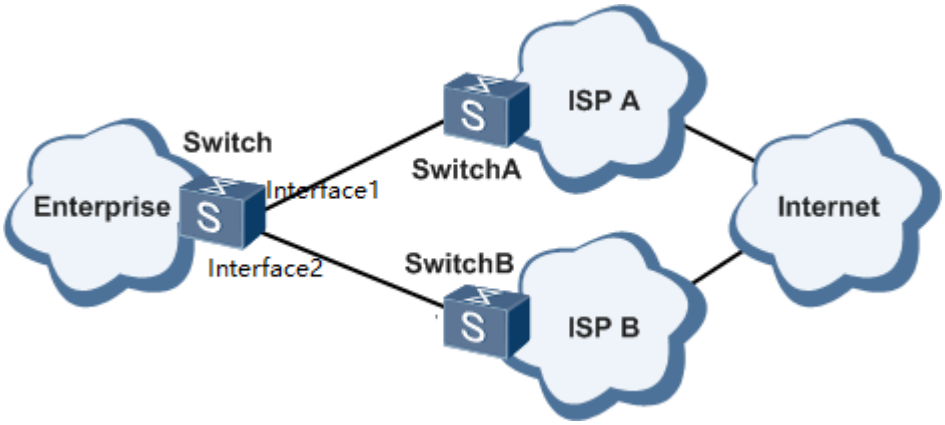

图 2.2.1 URPF 多宿主多 ISP 客户应用环境示意图

在图 2.2.1 所示环境中，客户与多个 ISP 连接，很难保证 Enterprise 和两个 ISP 之间路由的对称性，必须使用 URPF 松散模式。

比如说，假如从 Enterprise 出发的包通过 ISP A 到达 Internet，而从 Internet 到 enterprise 的包则通过 ISP B，这时 Enterprise 出口 Switch 的 Interface2 接口必须使用松散模式，若使用严格模式，查 FIB 表发现源 IP 对应的转发接口为 Interface1，从 Internet 到 enterprise 的包就会被丢弃。同理可证，Interface2 也需要使用松散模式。

上述例子说明现实生活中松散模式一般在多链接出口路由器上实施。

2.3 URPF 的高级特性[4]

严格型和松散型检查是 URPF 两个基本检查机制；部分设备在此基础上，还进一步增加了缺省路由检查以及 ACL 检查功能，进而将 URPF 检查实现的更灵活和全面[4]。如图 2.3.1 所

示：

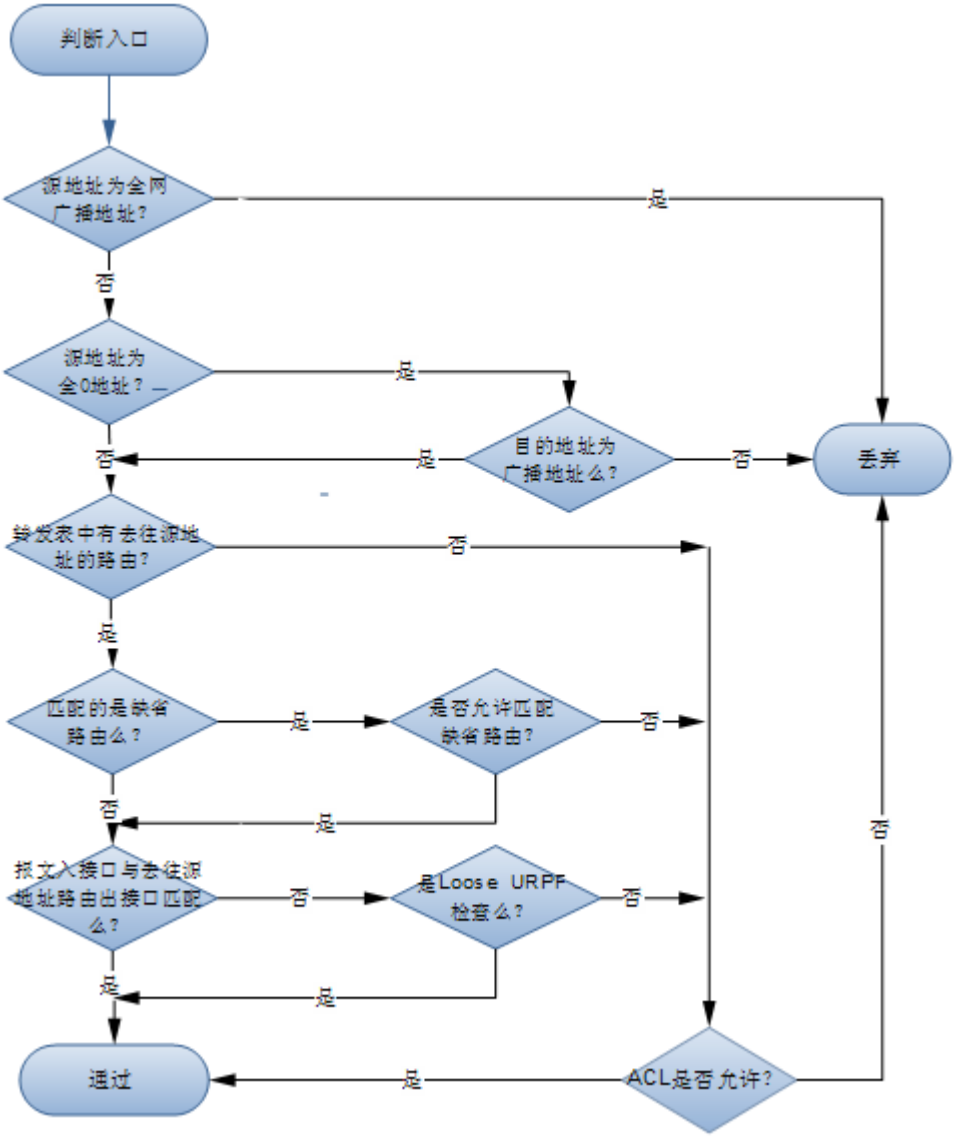

图 2.3.1 URPF 检查流程

特别情况下，设备在严格型 URPF 检查的基础上再增加链路层检查，即在确认路由转发表中存在去往源地址的路由以及出接口后，再增加检查 ARP 表项，确保报文的源 MAC 地址和查到的 ARP 表项中的 MAC 地址一样才允许报文通过。链路层检查功能对于运营商用单个三层以太网接口接入大量 PC 机用户时较适合部署。

3 总结

通过上述分析，可以看出在路由器上部署 URPF 对于防范伪造源 IP 地址的(D)DoS 攻击还是很有效的，所以其也能大大缓解基于伪造源 IP 的反射放大 DDoS 攻击带来的危害。但是

在路由器上部署 URPF 或多或少会降低路由器转发效率。

uRPF 的基本原理是如果 IP 地址不属于应该来自的子网网络就阻断出口业务，当(D)DoS 攻击伪造的数据包来自同一子网的 IP 地址，如果没有检查链路层，URPF 这种解决方案就会失效。但检查链路层又会增大路由器开销，降低转发效率。

对于 URPF 的使用，各大运营商需要在安全和效率之间进行权衡。

参考资料：

[1] 华为，*S9300&S9300E V200R008(C00&C10) 配置指南-安全：14 URPF 配置*，Retrieved November 12, 2018, from http://support.huawei.com/enterprise/zh/doc/DOC1000089026?section=j00h

[2] Cisco, *Understanding Unicast Reverse Path Forwarding*, Retrieved November 12, 2018, from https://www.cisco.com/c/en/us/about/security-center/unicast-reverse-path-forwarding.html

[3] *URPF - 单播逆向路径转发*，Retrieved November 12, 2018, from http://blog.sina.com.cn/s/blog_6617106b01011jc4.html

[4] *网络安全技术之 URPF 技术介绍*，Retrieved November 12, 2018, from http://www.h3c.com.cn/MiniSite/Technology_Circle/Technology_Column/ICG/ICG_Technology/201209/753898_97665_0.htm

[5] *浅谈 TCP/IP 协议栈(六)路由表与 FIB 表*, Retrieved November 12, 2018, from https://blog.csdn.net/u012155923/article/details/52089869