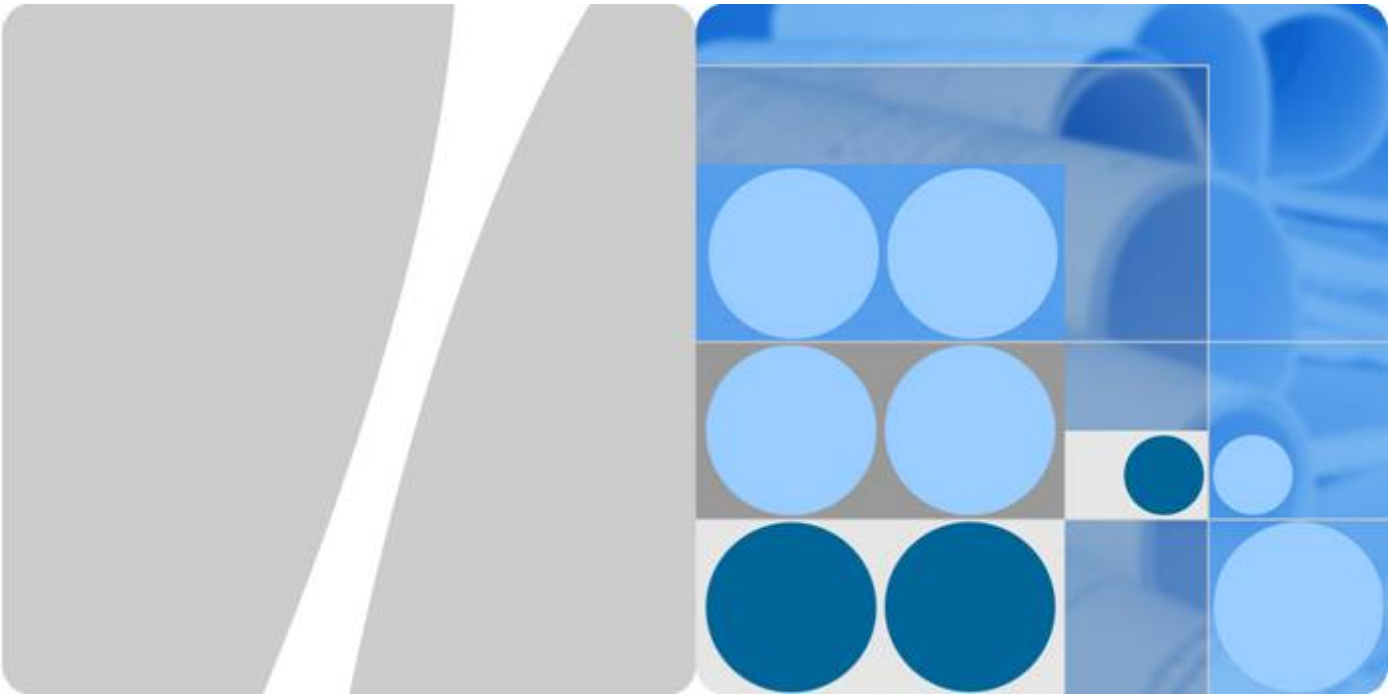


HUAWEI NetEngine20E-X6 高端业务路由器

V600R003C00

特性描述-安全

文档版本　01

发布日期　2011-05-15

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 0755-28560000 4008302118

客户服务传真： 0755-28560111

前 言

读者对象

本文档针对安全特性，从简介、原理描述和应用三个方面介绍了安全特性。

本文档与其它类型手册相结合，便于读者深入掌握安全特性的实现原理。

本文档主要适用于以下工程师：

- 网络规划工程师
- 调测工程师
- 数据配置工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2011-05-15)

第一次正式发布。

目 录

插图目录

表格目录

1 BOD

关于本章

1.1 介绍

定义

BOD（Bandwidth On Demand）特性是一种针对用户实现动态分配带宽的增值业务，在用户有带宽调整需求时，可以通过 Portal Server 自助选择 BOD 业务，业务动态激活和注销，不需要运营商通过更改配置完成带宽更改，同时也给运营商提供了更为灵活的基于业务的计费方式。

目的

随着 VoIP、IPTV、等网络应用的多样化，客户对网络带宽的需求也越来越多样化。BOD 是为客户提供多样化服务的有效方案。

受益

运营商收益

通过部署 BOD 业务，运营商可以：

- 开展差异化服务，对不同的目标客户群推出灵活的业务和资费政策，提高 ARPU 值，增加运营收入；
- 快速部署新业务，避免同质化竞争，降低用户离网率；
- 利用资费政策调节用户对带宽的占用，充分利用现有带宽，保护投资；
- 开展用户自助服务，降低运维成本；

1.2 参考标准和协议

文档	描述	备注
RFC 2748	The COPS (Common Open Policy Service) Protocol.	
RFC 2940	Definitions of Managed Objects for Common Open Policy Service (COPS) Protocol Clients.	
RFC 3483	Framework for Policy Usage Feedback for Common Open Policy Service with Policy Provisioni	

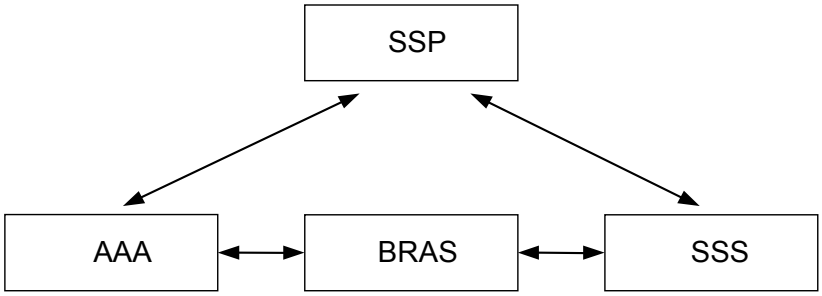
1.3 原理描述

1.3.1 增值业务控制

BOD 作为增值业务的一种，我们通过介绍增值业务的流程来讲解 BOD。

增值业务系统组成

图 1-1 增值业务系统组成图



增值业务通常由以下几个系统和设备组成：

- AAA：即 AAA 服务器，用于接入业务的认证、授权和计费。
- SSS（Service Select Server）：作为策略决策点（Policy Decision Point，简称 PDP），主要完成增值业务的配置、管理、策略决策、计费等功能。如 COPS（Common Open Policy Service）服务器、AAA 服务器。
- BRAS：作为策略执行点（Policy Enforcement Point，简称 PEP），用于业务策略的执行、业务流的转发，并提供每种业务的原始话单，用于按业务计费。
- SSP（Service Select Portal）：为基于 WEB 的自助服务门户，用户可以通过 Portal 浏览、订购和搜索业务，是运营商演示业务和引导用户使用业务的窗口。如 Portal 服务器。
- BRAS 与 AAA 之间使用 RADIUS 或 HWTACACS 协议接口，与 SSS 之间采用 COPS 协议接口。

增值业务处理过程

增值业务的开展基于接入业务，当用户接入时，策略服务器已经针对该用户下发了接入业务的业务策略。当用户使用增值业务时，需要动态修改业务策略。

- 增值业务策略 BOD 的安装

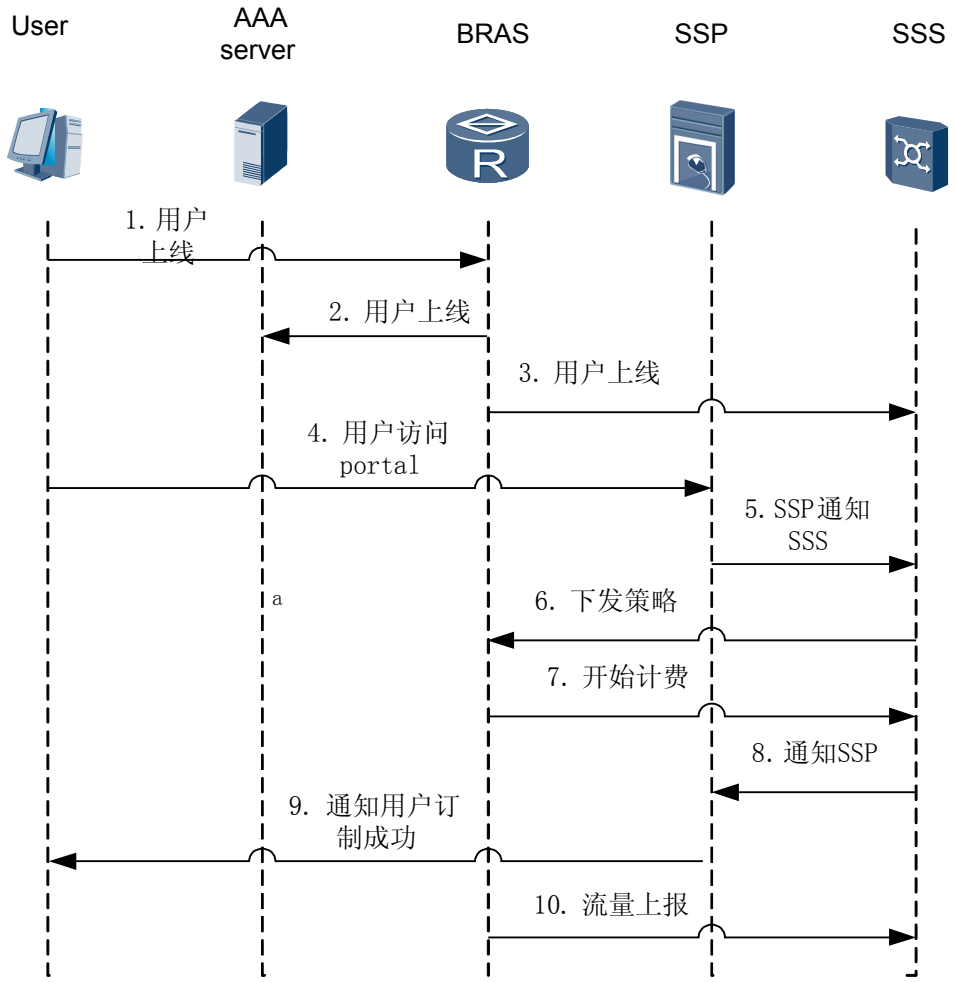
  用户通过 COPS 策略服务器动态下发的增值业务策略 BOD 来使用增值业务，这种方式的增值业务称为动态增值业务。

  用户可以访问 Portal 页面，在 Portal 页面上选择自己感兴趣的业务，Portal 服务器将用户选择的业务通知给 COPS 策略服务器，COPS 策略服务器将业务对应的策略下发给策略执行点。

- BOD 动态增值业务流程

  下面以用户访问 Portal 页面自助选择增值业务为例，介绍 BOD 动态增值业务下发流程，如图 1-2 所示。

图 1-2 动态增值业务流程



1. 用户发起上线。
2. AAA 服务器认证通过，授权用户上线。
3. BRAS 将用户信息通知给 SSS。
4. 用户访问 Portal 页面，并在 Portal 页面选择感兴趣的增值业务。
5. SSP 将用户及其业务信息传给 SSS。
6. SSS 根据用户业务定制业务策略，下发给 BRAS。
7. BRAS 执行下发的增值业务策略，并通知 SSS 计费开始。
8. SSS 收到计费开始消息，通知 SSP。
9. SSP 通过 Portal 页面告知用户业务已激活，用户可以使用增值业务。
10. 用户使用增值业务，BRAS 根据增值业务策略对业务进行计费和控制，并向 SSS 上报流量。

1.3.2 COPS

增值业务最常用的方式就是通过策略服务器，又叫 COPS 服务器下发业务。COPS 服务器与 BRAS 之间采用 COPS 协议进行数据的传输。

说明

NE20E-X6 当前支持的策略服务器是 RM9000。

COPS 是一种请求、应答型协议，采用 Client/Server 模型。一般策略执行点(PEP)作为 Client，策略决定点(PDP)作为 Server。COPS 协议使用 TCP 传输协议，使 Client 与策略 Server 进行可靠的数据传输， 该协议是可扩展的，可以在不修改协议的情况下支持多种 Client 类型。

COPS 协议实现支持 RFC2748，RFC3084。

图 1-3 COPS 模型

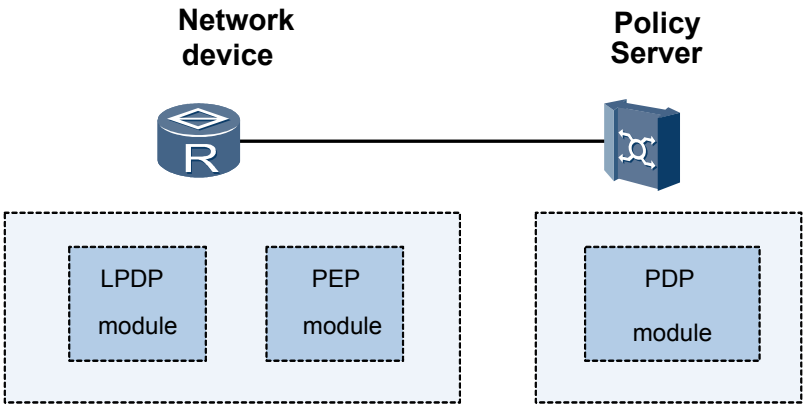


图 1-3 是一个典型的 COPS 模型，包括 PDP、PEP、LPDP 三种 COPS 元素。其中 LPDP 可选，在 PDP 缺席的情况下被 PEP 用来本地决策，PEP 和 LPDP 之间的通信可以不使用 COPS 协议。

PEP 负责建立到 PDP 的 TCP 连接，通过该连接，PEP 负责向 PDP 发送请求、接收远端 PDP 的决策、上报决策执行结果、通报请求状态的改变、无用状态的删除，另外出于计费和监视等目的，PEP 应具有上报本地策略执行结果的能力。PDP 通过该连接下发响应 PEP 请求的决策，当然也可以主动下发策略。

当 PEP 发送一个配置请求（configuration request）时，期望 PDP 以决策消息的形式连续下发命名配置数据。当 PEP 成功安装一个命名配置数据后，PEP 应当向服务器发送一个报告消息进行确认。服务器可以以决策消息的形式更新或删除一个命名配置信息，PEP 删除一个服务器指定的命名配置信息后将向 PDP 应答一个报告消息。

COPS 协议通过自识别的 COPS 对象传送必要的数据，通过这些数据可以识别请求状态、建立请求上下文、识别请求的类型、刷新已安装的请求、转发策略、报告错误、保证消息完整性、传送客户特定信息。每一个消息中都包含了客户类型信息，用于区分不同的客户类型，客户类型不同，其要求的决策和客户特定数据的含义也不同。COPS 上下文对象中的消息类型和请求类型字段标识了触发策略的外部事件。有以下三种：

- 收到消息
- 本地资源分配
- 转发消息。

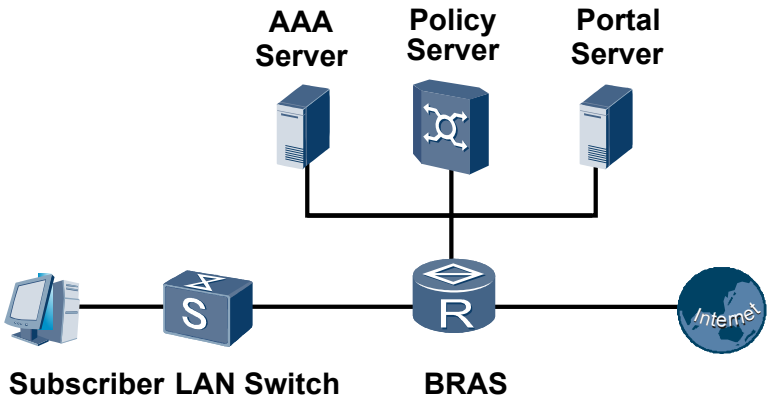
PEP 具有通过 LPDP 进行本地决策的能力，但 PDP 是最终的决策权威者。即 PEP 通过 LPDP 决策对象必须将所有相关的本地决策信息转发给 PDP，PEP 必须遵守 PDP 根据这些信息做出的最终决策。

PDP 和 PEP 利用心跳探测消息保证连接。如果连接出现故障，PEP 必须尽力重新建立与 PDP 之间的连接或转向备份 PDP。如果连接断掉，PEP 应该使用 LPDP 进行本地决策。当连接重新建立后，PEP 应通知 PDP 自从连接断掉后被删除的状态或通过的允许进入控制事件。PDP 可以查询需要进行同步的所有 PEP 内部状态（所有已被安装的请求必须重新发布）。PEP 也可以通过缓存和在有限时间内继续使用以前通过的 PDP 决策减少因为连接丢失造成的服务中断。

1.4 应用

BOD 业务应用组网图

图 1-4 图 4 BOD 业务组网图



动态增值业务都可以使用 COPS 服务器下发，用户按照某种接入认证方式上线，上线过程中获得基本的带宽。

上线后，用户访问 Portal 服务器，在 Portal 页面上选择自己需要的带宽类别，Portal 服务器把用户的选择提交给 Policy 服务器。Policy 服务器根据用户的选择，给 BRAS 下发用户的带宽，用户的带宽生效后，用户即可按照新的带宽使用网络。

BRAS 提供的 BOD 业务不仅可以动态分配带宽，也可以更改用户的 ACL 组、用户优先级、计费策略等一些基本用户属性。

1.5 术语与缩略语

缩略语

缩略语	英文全称	中文全称
BOD	Bandwidth on Demand	订制带宽
AAA	Authentication, Authorization and Accounting	认证、授权和计费
BoD	Bandwidth On Demand	按需带宽

缩略语	英文全称	中文全称
COPS	Common Open Policy Service	公共开放策略业务
RADIUS	Remote Authentication Dial in User Service	远端用户拨入鉴权服务
BRAS	Broadband Remote Access Server	宽带接入服务器
SSP	Service Selection Portal Server	业务选择使用的门户服务器
SSS	Service Selection Server	业务选择服务器

2 MAC 学习限制

关于本章

2.1 介绍

定义

MAC 地址学习限制，通过限制接口或者 VSI 等的 MAC 地址学习的数量，能够将针对 MAC 表项资源所遭受的攻击限制在一定范围内，使其他用户不受影响。

目的

二层网络中 MAC 表项是一种用于报文转发的关键资源，当网络中存在 MAC 攻击行为时，MAC 表项资源会被非法挤占，造成表项资源不足或者被耗尽，从而影响合法用户正常使用网络。为了防止这种情况出现，可以进行 MAC 学习限制，将 MAC 攻击的影响限定在一定范围内。

受益

运营商受益

通过限制接口或者 VSI 等的 MAC 地址学习的数量，能够将攻击限制在一定范围内，使其他用户不受影响。

用户受益

由于将攻击限制在一定的范围，提高了用户的安全性，降低了带宽的浪费。

2.2 参考标准和协议

无

2.3 原理描述

MAC 限制，用户报文通过路由器学习用户报文里的源 MAC，当学习到的 MAC 达到了限制阈值：如果用户报文的源 MAC 在 MAC 表中存在，用户报文会继续转发下去；如果用户报文的源 MAC 不在 MAC 表中存，那么报文会根据 MAC 限制动作 Action（动作 Action 分为 Forward 转发和 Discard 丢弃）进行相应的处理。比如 action 动作为 discard 丢弃，那么用户报文入端口丢弃。

2.3.1 MAC 限制的基本原理

2.3.2 流量抑制基本原理

2.3.1 MAC 限制的基本原理

MAC 限制是在 MAC 学习的过程中，通过限制 MAC 学习的数目来进行的。基本原理如下：

- 基于端口或端口+VLAN 的 MAC 限制

1、用户报文当通过配置了基于端口或端口+vlan 的 MAC 限制端口时，路由器会学习用户报文里的源 MAC 地址和转发信息，在学习时，判断进入的端口是否配置了 MAC 限制，如果配置了，进入限制流程。

2、限制流程：判断要学习的源 MAC 是否存在于 MAC 表中，如果存在，不学习正常转发出去；如果不存在，判断之前学习到的 MAC 数是否达到 MAC 限制阈值，如果没有达到限制阈值，进行学习；如果已经达到限制阈值，根据限制的 action 动作类型，discard 进行丢弃，forward 进行转发。

- 基于广播域 VLAN 或 VSI 的 MAC 限制

用户报文通过配置了 MAC 限制的广播域进行转发时，路由器会在报文转发的出端口处学习用户报文中的源 MAC；如果源 MAC 已经存在于 MAC 表中，不再进行学习正常转发出去；如果不存在，判断之前学习到的 MAC 数是否达到 MAC 限制阈值，如果没有达到限制阈值，进行学习；如果已经达到限制阈值，根据限制的 action 动作类型，discard 进行丢弃，forward 进行转发。

2.3.2 流量抑制基本原理

二层网络中的流量分类

二层网络中的流量分为以下几种：

- 单播流量：目的 MAC 已经存在于 MAC 表中的单播流量，交换机根据 MAC 表中的信息对这种报文进行单播发送。
- 未知单播流量：目的 MAC 不在 MAC 表中的单播流量，交换机对此种流量进行广播发送。
- 组播流量：目的 MAC 为组播的流量，交换机对此种流量一般进行广播发送。
- 广播流量：目的 MAC 为广播的流量，交换机对此种流量进行广播发送。

为了保证单播流量的发送，交换机中可以对未知单播、组播、广播流量允许转发的带宽大小分别进行限制。

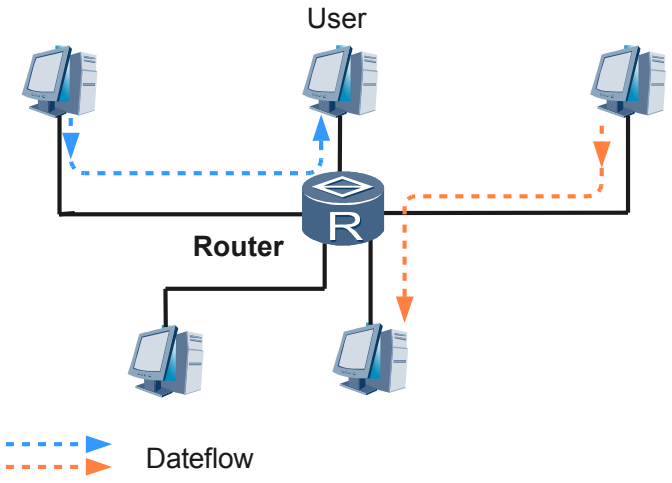
广播流量的产生和危害

为了提高传统 LAN 的通信效率，接入更多计算机，同时尽量避免冲突，出现了二层交换机。二层交换机通过 MAC 学习，将共享介质的冲突限定在了其每个下行端口中，如图 2-1 所示。

说明

本手册中 NE20E-X6 作为交换机使用。

图 2-1 流量限制组网图



交换机接收网段上的所有数据帧。根据数据帧中的源 MAC 地址进行学习，构建 MAC 地址表，存放 MAC 地址和端口的对应关系。

对于收到的数据帧，交换机如果能够在 MAC 地址表中查到目的 MAC 地址，则把帧基于目的 MAC 地址进行二层转发，因此具有隔离冲突的作用。

如果目的地址不在 MAC 地址表中，交换机会向除了接收端口之外的所有端口发送广播，这就有可能导致网络中发生广播风暴。

在交换机收到组播或广播报文时，由于根据它们的目的 MAC 并不能明确的指定出端口，所以交换机也会向除了接收端口之外的所有端口转发这些组播或广播流量，这同样可能导致发生广播风暴。

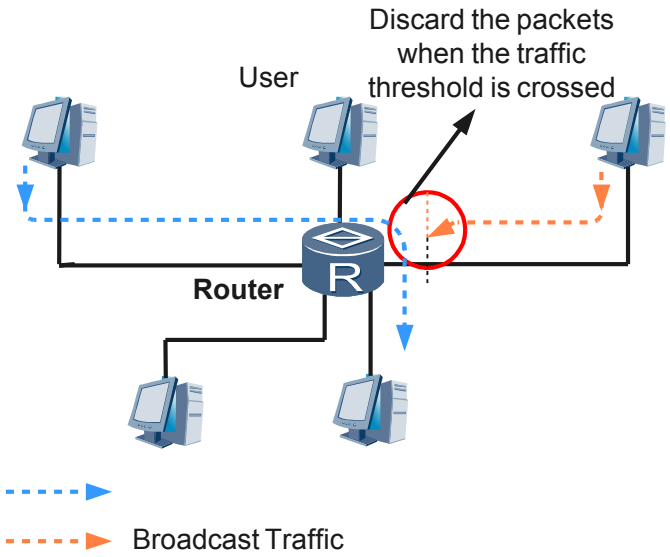
因此，使用交换机进行组网，通过二层快速交换提高了单播转发效率，但是广播流量的存在降低了交换机的效率，故而需要进行流量限制。

流量限制

在二层网络中的大多数场景中，单播流量都应该远大于广播流量，这也是使用交换机进行组网的一个前提。而如果不对广播流量进行限制，当广播流量大量存在时，会耗费大量的网络带宽，造成网络性能的下降，甚至达到造成通信中断。

在交换机中对产生的广播流量进行限制，则能在广播流量激增时依然保证交换机能够剩下一部分带宽给普通的单播转发使用。

图 2-2 流量限制示意图



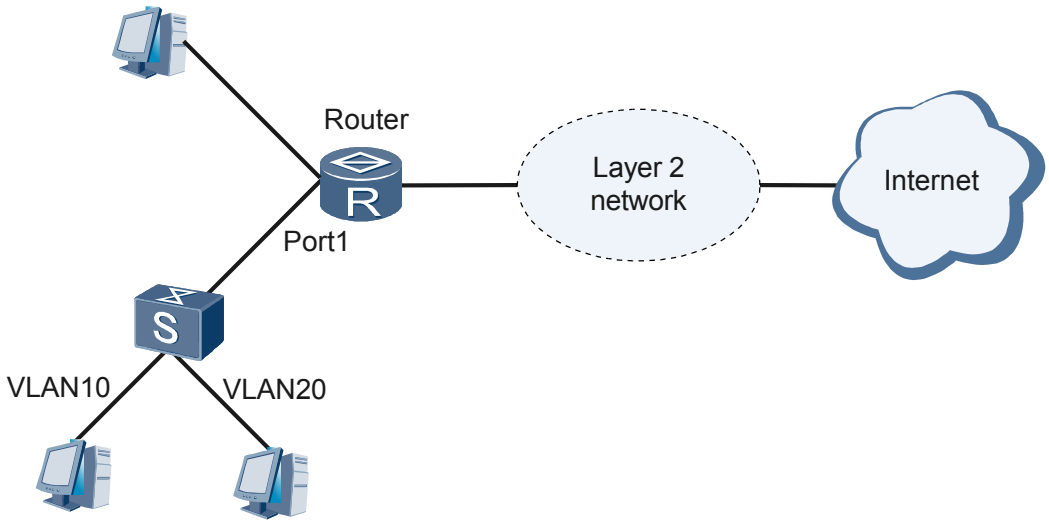
2.4 应用

根据入接口限制 MAC 学习数量

目前 NE20E-X6 支持二层交换接口的使用，而二层交换接口下根据接入 VLAN 的不同，可以接入多个不同 VLAN 的二层用户网络。

NE20E-X6 可以为此二层交换接口下，所有接入的二层用户网络设定一个总的 MAC 学习限制数量，而不区分具体的 VLAN。如图 2-3 所示，路由器 的 port1 可以配置基于接口的 MAC 学习限制，不区分 VLAN。

图 2-3 基于接口的 MAC 学习示意图



根据入接口＋ VLAN 限制 MAC 学习数量

除了可以在二层交换接口下为所有用户的二层网络配置一个总的 MAC 学习限制数量，还可以同时为二层交换接口下的一个或多个特定 VLAN，设定 MAC 学习的最大限制数量。

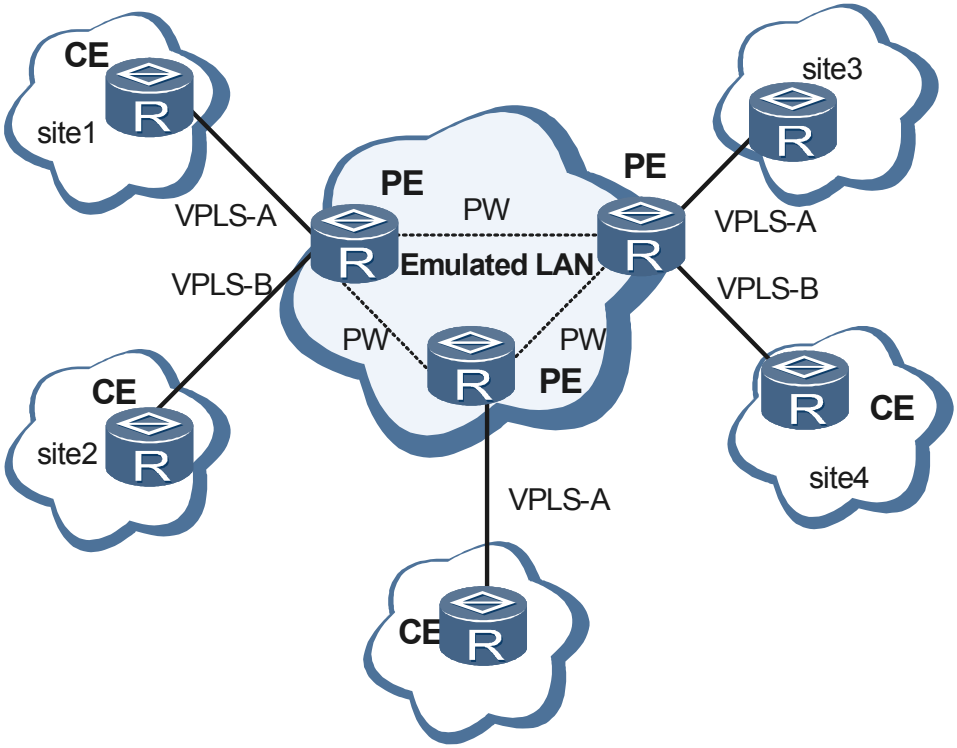
如图 2-3 所示，在路由器 的 port1 可以基于 port+VLAN 的方式设置 MAC 限制，只对 VLAN10 或者只对 VLAN20 做 MAC 限制。

根据入子接口限制 MAC 学习数量

目前 NE20E-X6 支持主接口或者子接口绑定 VSI，在 VPLS 中，服务提供商网络模拟网桥设备，由 PE 进行 MAC 地址学习，在 PE 设备上可以对 VSI 的 AC 接口配置 MAC 学习限制。

如图 2-4 所示，可以在 PE 上的 AC 接口配置基于接口的 MAC 限制，限制 VSI 相应 Site 的 MAC 所能学习到的 MAC 表项数量。

图 2-4 接口绑定 VSI 时基于接口的 MAC 学习限制示意图



根据入 QinQ 子接口限制 MAC 学习数量

和普通的子接口类似，QinQ 子接口在接入 VPLS 业务时，也需要进行二层转发，需要限制 MAC 地址学习数量。NE20E-X6 支持在 QinQ 子接口上设定 MAC 学习的上限，和达到上限后的转发行为。如图 2-4 所示。

2.5 术语与缩略语

术语(Terms)

术语	解释
MAC 学习	路由器或者交换机通过学习用户报文里的源 MAC，达到指导用户报文的转发。
MAC 学习限制	通过在 MAC 学习过程中限制所学习的 MAC 数量，来达到安全性的提高。
MAC 学习限制阈值	MAC 学习在限制时的最大数目。
动作	MAC 学习的数量达到限制阈值时，对用户报文的转发行为的处理，目前有 discard 丢弃，forward 转发。

缩略语(Abbreviations)

缩略语	英文全称	中文全称
MAC	Mac address	MAC 地址

3 DHCP Snooping

关于本章

3.1 介绍

定义

DHCP Snooping 是一种 DHCP 安全特性。通过 MAC 地址限制，DHCP Snooping 安全绑定、IP+MAC 绑定、Option82 特性等功能过滤不信任的 DHCP 消息，解决了设备应用 DHCP 时遇到 DHCP DoS 攻击、DHCP Server 仿冒攻击、ARP 中间人攻击及 IP/MAC Spoofing 攻击的问题。DHCP Snooping 的作用就如同在 Client 和 DHCP Server 之间建立的一道防火墙。

目的

DHCP Snooping 功能用于防止：

- DHCP 饿死攻击
- DHCP Server 仿冒者攻击
- 中间人攻击与 IP/MAC Spoofing 攻击

根据不同的攻击类型，DHCP Snooping 提供不同的工作模式，见表 3-1。

表 3-1 攻击类型与 DHCP Snooping 工作模式对应表

攻击类型	DHCP Snooping 工作模式
DHCP 饿死攻击	MAC 地址限制
DHCP Server 仿冒者攻击	信任（Trusted）/不信任（Untrusted）
中间人攻击/IP/MAC Spoofing 攻击	DHCP Snooping 绑定表
改变 CHADDR 值的 DoS 攻击	检查 DHCP 报文的 CHADDR 字段

3.2 参考标准和协议

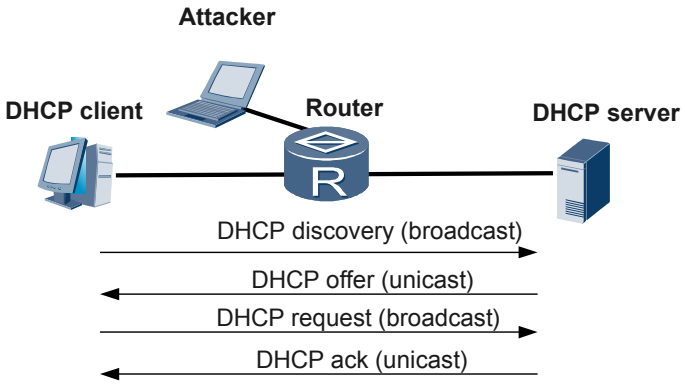
文档编号	描述
RFC 3046	DHCP Relay Agent Information Option
RFC 2132	DHCP Options and BOOTP Vendor Extensions

3.3 原理描述

3.3.1 DHCP 饿死攻击

在 DHCP 饿死攻击方式中，攻击者不断变换物理地址，尝试申请一个 DHCP 域中所有的 IP 地址，直到耗尽 DHCP Server 地址池中的地址，导致其他正常用户无法获得地址。如图 3-1 所示。

图 3-1 DHCP 饿死攻击示意图



可以通过 MAC 地址限制来防止 DHCP 饿死攻击。

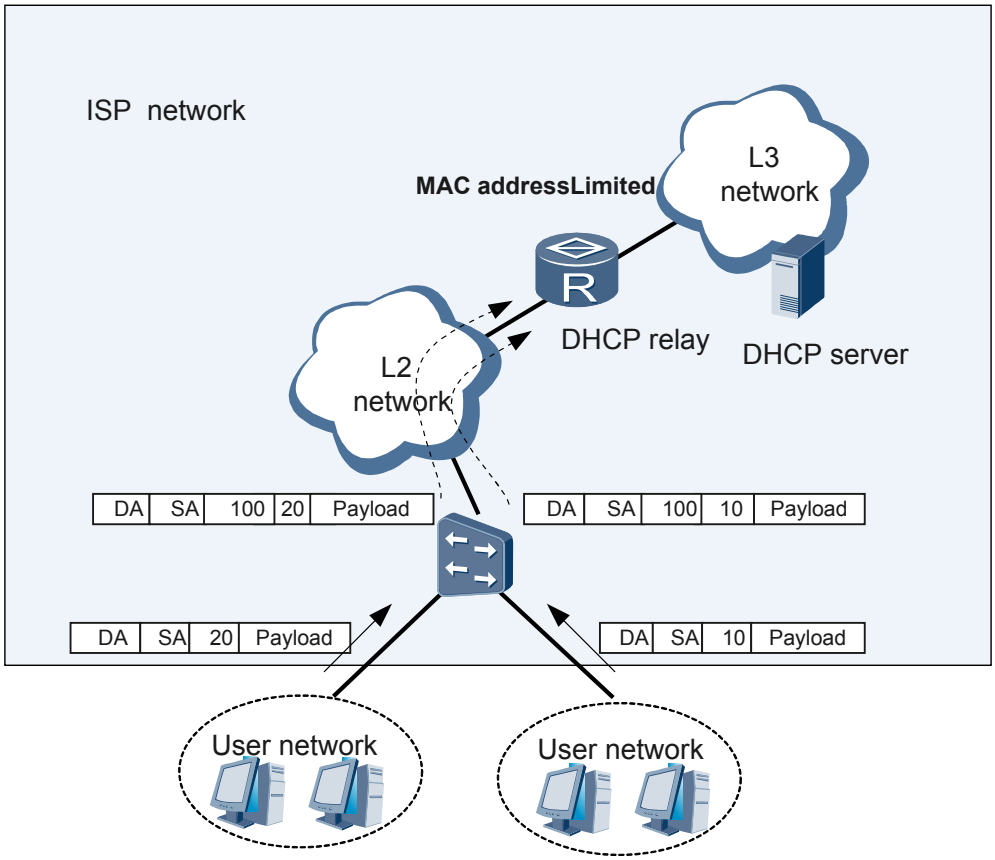
普通 MAC 地址限制

MAC 地址限制功能主要用于防止 DHCP 饿死攻击，一般部署在二层设备上。通过限制设备接口上允许学习到的最多 MAC 地址数目，防止用户通过变换 MAC 地址，大量发送 DHCP 请求，同时也限制了一个接口上的用户数目。

QinQ 方式下的 MAC 地址限制

在实际的应用中，用户通过 DSLAM（Digital Subscriber Line Access Multiplexer）设备接入网络，通过给不同的用户配置不同的 VLAN 来隔离用户。同时为了规避 VLAN 总数（4094）的限制，使用 QinQ 特性，给用户报文封装两层 Tag 标签。这时如果在网关上部署了 MAC 地址限制功能，就需要能够基于两层 Tag 对 MAC 数进行限制。如图 3-2 所示。

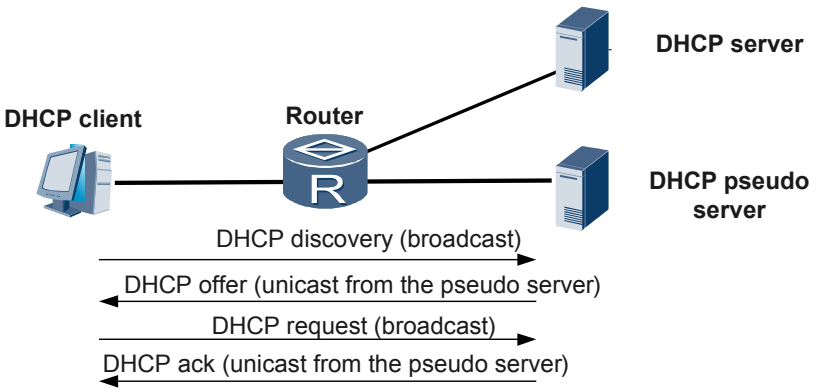
图 3-2 基于 QinQ 的 MAC 地址数量限制



3.3.2 DHCP Server 仿冒者攻击

由于 DHCP 请求报文以广播形式发送，所以 DHCP Server 仿冒者可以侦听到此报文。DHCP Server 仿冒者回应给 DHCP Client 仿冒信息，如错误的网关地址、错误的 DNS 服务器、错误的 IP 等，达到 DoS（Deny of Service）的目的。如图 3-3 所示。

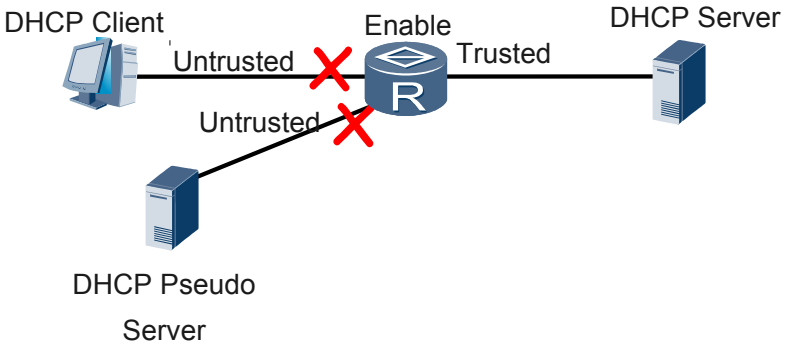
图 3-3 DHCP Server 仿冒者攻击示意图



为防止 DHCP Server 仿冒者攻击，可使用 DHCP Snooping 的“信任（Trusted）/不信任（Untrusted）”工作模式。

把某个物理接口或者 VLANIF 设置为“信任（Trusted）”或者“不信任（Untrusted）”。凡是从“不信任（Untrusted）”接口上收到的 DHCP Reply（Offer、ACK、NAK）报文直接丢弃，这样可以隔离 DHCP Server 仿冒者攻击。如图 3-4 所示。

图 3-4 Trusted/Untrusted 工作模式示意图



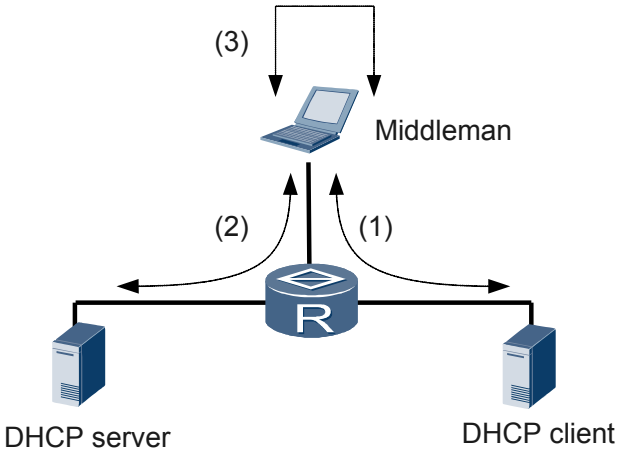
3.3.3 中间人攻击与 IP/MAC Spoofing 攻击

中间人攻击

首先，中间人向客户端发送带有自己 MAC 和服务器 IP 的报文，让客户端学到中间人的 IP 和 MAC，达到仿冒 DHCP Server 的目的。达到目的后，客户端发到服务器的报文都会经过中间人；然后，中间人向服务器发送带有自己 MAC 和客户端 IP 的报文，让服务器学到中间人的 IP 和 MAC，达到仿冒客户端的目的。达到目的后，服务器发到客户端的报文都会经过中间人，如图 3-5 所示。

中间人完成服务器和客户端的数据交换。在服务器看来，所有的报文都是来自或者发往客户端；在客户端看来，所有的报文也都是来自或者发往服务器端。但实际上这些报文都是经过了中间人的“二手”信息。

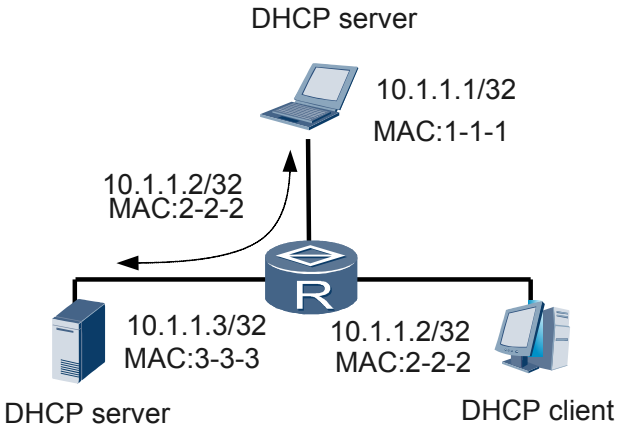
图 3-5 中间人攻击示意图



IP/MAC Spoofing 攻击

攻击者向服务器发送带有合法用户 IP 和 MAC 的报文，令服务器误以为已经学到这个合法用户的 IP 和 MAC，但真正的合法用户不能从服务器获得服务。如图 3-6 所示。

图 3-6 IP/MAC Spoofing 攻击示意图



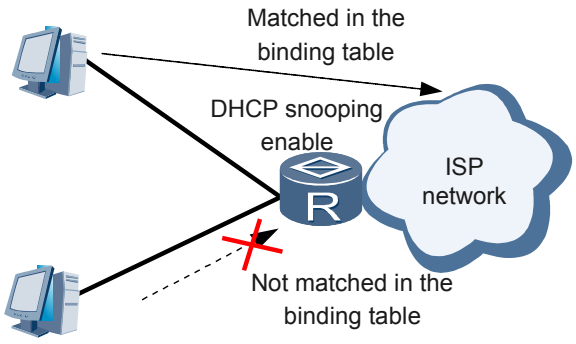
为隔离中间人攻击与 IP/MAC Spoofing 攻击，可使用 DHCP Snooping 绑定表工作模式。

NE20E-X6 默认是强策略。当接口接收到 ARP 或者 IP 报文，使用 ARP 或者 IP 报文中的“源 IP+源 MAC”匹配 DHCP Snooping 绑定表。如果匹配就进行转发，如果不匹配就丢弃。如图 3-6 所示。

对于配置静态 IP 的用户，由于没有通过 DHCP 请求而获得 IP，所以，没有对应的 DHCP Snooping 绑定表项，该用户发出的 ARP、IP 报文会被丢弃，从而防止该用户非法使用网络。

对于盗用其他合法用户 IP 地址的用户，同样由于不是自己通过 DHCP 请求而获得 IP 的，IP 对应的 DHCP Snooping 绑定表项中的 MAC 以及接口与盗用者的不一致，盗用者发出的 ARP、IP 报文会被丢弃，从而防止该盗用者非法使用网络。

图 3-7 应用 IP 与 MAC 绑定表示意图



DHCP Snooping 绑定表中的表项分为两种：

- 通过命令行配置的静态表项，只能通过命令行删除。
- 通过 DHCP Snooping 功能自动学习到的动态表项，并根据 DHCP 租期进行老化。

DHCP Snooping 绑定表中的动态表项是根据 DHCP server 回的 ACK 报文自动生成的。根据网络设备层次不同，动态表项的建立过程也不同：

- 在二层设备上
  - 如果使能了 Option82 选项，二层设备通过监听 DHCP 报文，在 DHCP 请求报文中插入 Option82，DHCP Server 会在 Reply 报文中携带 Option82 选项。二层设备分析 Option82 选项即可确定 DHCP Reply 报文回应给哪个接口，从而建立对应的 DHCP Snooping 绑定表项。
  - 如果未使能 Option82 选项，二层设备根据 MAC 地址表来识别不同的接口信息。
- 在三层设备上

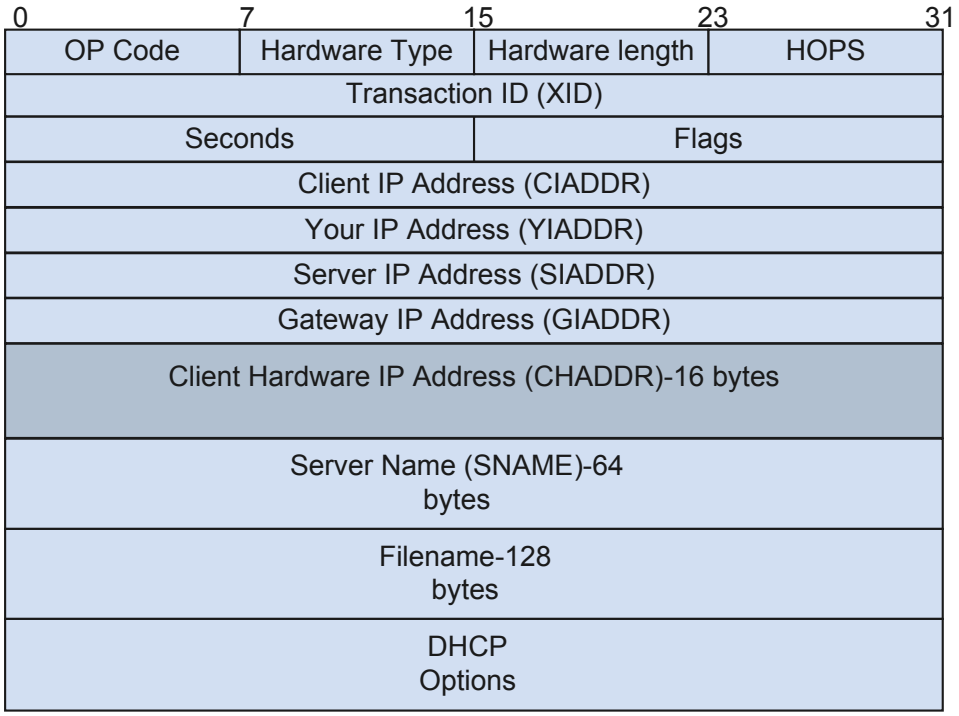
  对于配置为“不信任”的接口，通过监听 DHCP Reply 消息，获取 DHCP Server 分配给用户的 IP 地址、用户 MAC 地址、报文通过的接口等信息，建立不信任侧的 IP 与 MAC 绑定表项。该表项与分配给用户的 IP 地址具有同样的租约期，租约到期或者用户释放该 IP 地址则自动删除该表项。

用户申请到 IP 地址后发生异常下线，这样用户就无法发出 DHCP Release 报文来释放已申请的 IP 地址。此时可以使能 ARP 与 DHCP 的联动功能。系统将对 DHCP Snooping 表项中到达老化时间并且 ARP 表项中也不存在的 IP 地址进行 ARP 探测。在规定的探测次数内探测不到用户，则系统会删除 DHCP 绑定表中的绑定关系并通知 DHCP Server 释放 IP 地址。

3.3.4 改变 CHADDR 值的 DoS 攻击

在 DHCP 饿死攻击方式中，如果攻击者改变的不是数据帧头部的源 MAC，而是改变 DHCP 报文中的 CHADDR（Client Hardware Address）值来不断申请 IP 地址，如图 3-8 所示，而路由器仅根据数据帧头部的源 MAC 来判断该报文是否合法，那么“MAC 地址限制”方案不能起作用。

图 3-8 改变 CHADDR 的 DOS 攻击



这时，可以使用 DHCP Snooping 检查 DHCP 请求报文中 CHADDR 字段的功能。如果该字段跟数据帧头部的源 MAC 相匹配，便转发报文；否则，丢弃报文。

3.3.5 我司 Option82 报文格式

Option82 报文格式

Option82 是 DHCP 报文的一个特殊字段，供 DHCP Relay 设置，用来标识 DHCP Request 报文的发送路径。

客户端发送的 DHCP 请求报文，经过 DHCP Relay 时，DHCP Relay 为 DHCP 请求报文填充 Option82 字段，DHCP Server 收到含有 Option82 字段的 DHCP 请求报文时，在 DHCP Realy 报文中原样添加该字段返回给 DHCP Relay，DHCP Relay 根据 DHCP Relay 报文中携带的 Option82 字段确定发送给那个接口。

如图 3-9 所示，Option82 的 Code 字段为 82，Length 字段标识代理信息字段的字节数，iN 为代理信息字段子选项，子选项由子选项编号/长度值/子选项值”的元组序列组成，如图 3-9 所示，SubOpt 为子选项的编号，Length 字段标识代理信息子选项内容的长度，不包括子选项编号/长度值。在 Option82 字段中，必须要定义一个子选项，子选项可以为空，因此 Option82 字段最短长度为 2。

最初分配的 DHCP 中继代理子选项为：

- 1：代理路径 ID 子选项。
- 2：代理远程 ID 子选项。

DHCP 服务器可以根据上面的路径 ID 作为 IP 地址分配和其他参数指定的策略。

路由器除了支持上面的子选项 1 之外，还支持子选项 9。用来标识华为设备添加的路径 ID 信息。

子选项 9 的作用：

- 对于接口转发的 DHCP 应答报文，如果 Option82 中含有子选项 9，并且子选项 9 中有华为厂商信息，华为设备就可以解析该字段，解析成功后，取出接口信息，把子选项 9 中的华为厂商信息字段剥掉，进行报文转发；如果 Relay 接口是 QINQ 子接口，DHCP Relay 利用取到的两层 VLAN TAG，封装报文进行转发。
- 对于建立 DHCP Snooping 绑定表，首先解析该 DHCP 报文是不是 DHCP 应答报文，如果是 DHCP 应答报文，根据子选项 9 中取到的接口信息建立 DHCP Snooping 绑定表；否则，不能建立 DHCP Snooping 绑定表。

图 3-9 option82 报文格式

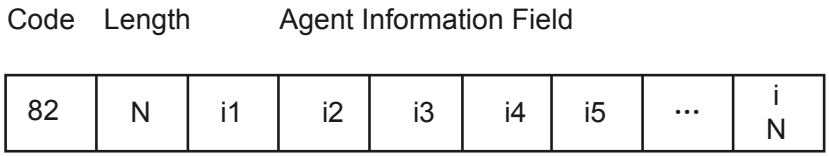
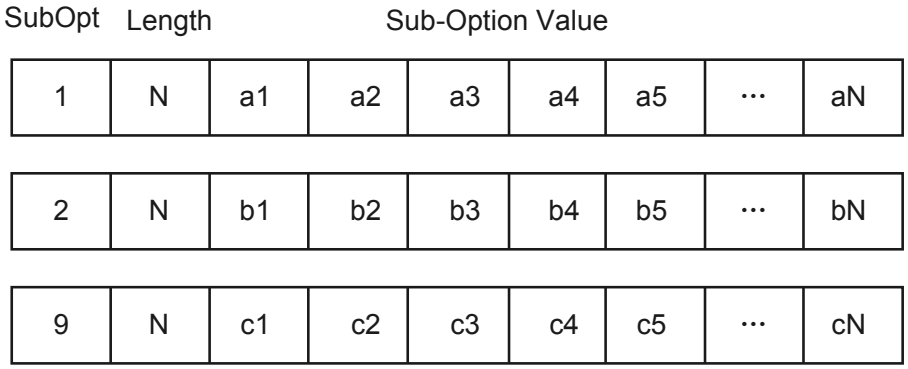


图 3-10 option82 报文格式



Option82 既可应用在二层设备上，又可应用在三层设备上。三层设备可以通过 DHCP 服务器使用 Option82 选项执行地址分配策略或其他策略；二层设备可以通过分析 Option82 选项确定 DHCP Reply 报文回应给哪个接口，从而建立对应的 IP 与 MAC 绑定表项。下面分别描述这两种情况。

在二层设备上插入 Option82

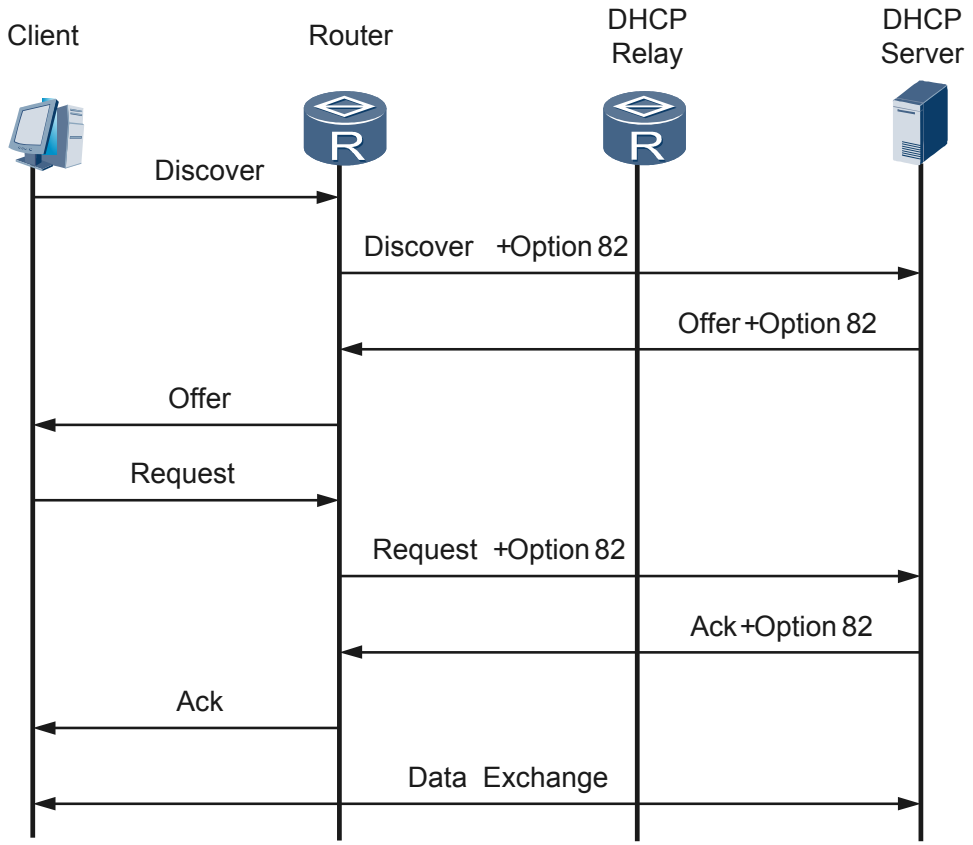
如图 3-11 图 3-12 所示，用户设备首先接入二层设备，然后通过一个二层网络连接到 DHCP Relay 或者 DHCP Server。

如果在这个二层设备上启用了 DHCP Snooping，DHCP Reply 报文可能是广播报文。二层设备可以根据报文的 MAC 地址查找 VLAN，确定 DHCP 回应报文应该回给哪个接口，建立对应的 IP 与 MAC 地址绑定表项。

如果需要在二层设备上监听 DHCP 报文，在 DHCP Discover 报文中插入 Option82，DHCP Server 会在回应报文中携带 Option82 选项。二层设备可以通过分析 Option82 选

项确定 DHCP Offer 报文回应给哪个接口，从而建立对应的 IP 与 MAC 绑定表项。并且将 DHCP Reply 报文中的 Option82 剥离后发给用户。

图 3-11 在二层设备上插入 Option82



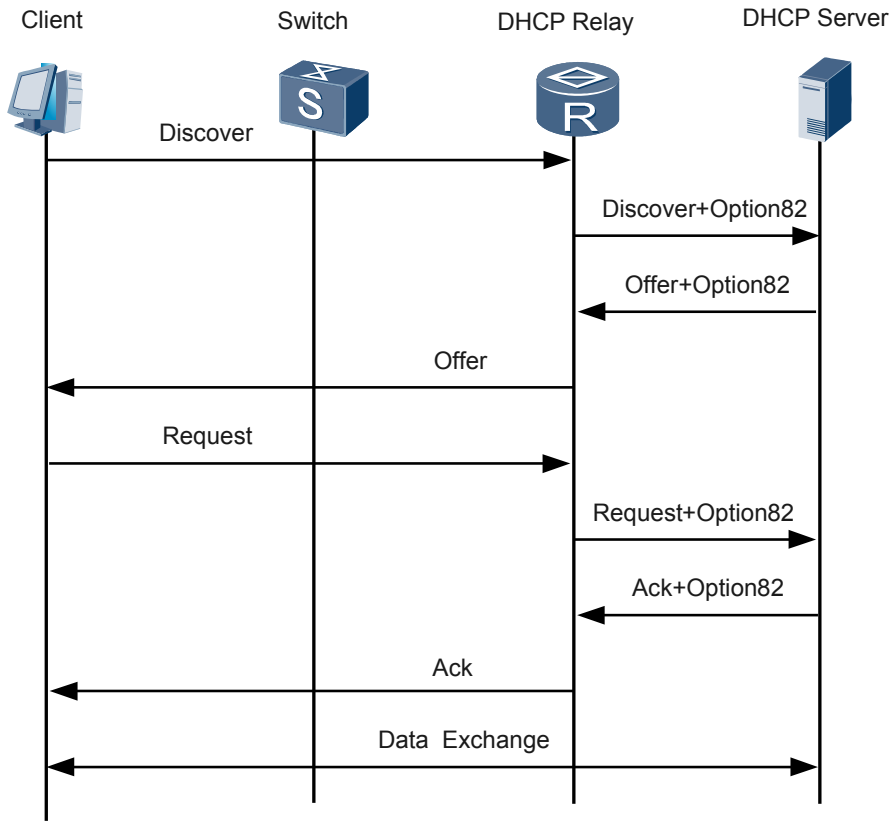
在三层设备上插入 Option82

在三层设备上插入 Option82 时，三层设备通常是指 DHCP Relay Agent。

如图 1-12 所示，DHCP Relay Agent 使能 Option82 功能后将 Option82 插入到用户发送的 Discover 和 Request 报文中，DHCP 服务器通过识别 Option82 来执行 IP 地址分配策略或其它策略。

DHCP 服务器的响应报文也带有 Option82，DHCP Relay Agent 收到带有 Option82 的响应报文后，将 Option82 剥离，然后发给用户。

图 3-12 在三层设备上插入 Option82



Option82 的实现

客户端发送的 DHCP 请求报文，DHCP Realy 检查其是否携带 Option82 域。

- 如果有 Option82 域。

  检查其插入配置，插入 Option82 的配置分为 Insert 和 Rebuild 两种：

  - 如果当前接口配置是 Option82 Rebuild，说明该接口对已经携带的 Option82 不信任，修改 Option82，修改后的 Option82 子选项为 1。
  - 如果当前接口配置是 Option82 Insert，说明该接口对已经携带的 Option82 信任，不能对于该 Option82 的子选项 1 修改。需要检查 Option82 中是否有子选项 9，如果没有子选项 9，构造子选项 9。如果已有子选项 9，检查是否有华为厂商信息字段，如果没有华为厂商信息字段，构造华为厂商信息字段，添加到其它厂商信息字段的后面。

- 如果没有 Option82 域。

  不区分接口针对 Option82 的插入配置是 Insert 还是 Rebuild，都插入子选项 1 的 Option82。

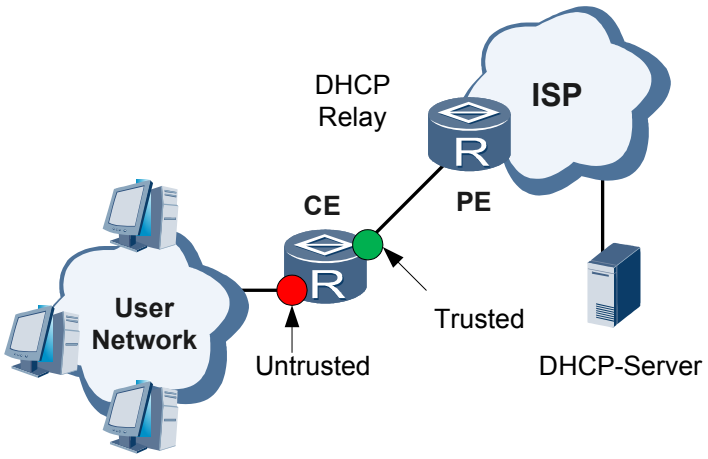
DHCP 应答报文转发过程中，如果有子选项 1 或 9，并且子选项 1 或 9 中有华为厂商信息字段，设备成功解析该字段后，把子选项 1 或 9 中的华为厂商信息字段剥掉，然后转发。

3.4 应用

在路由器二层模式下防止攻击的应用

用户网使用 NE20E-X6 作为二层设备络接入 ISP，在设备上应用 DHCP Snooping 功能。将用户侧的接口配置为 untrusted 模式，把运营商网络侧的接口配置为 trusted 模式。此时设备判断接收到的报文信息和绑定表中的内容一致后才会被转发，否则报文将被丢弃，同时告警，保证运营商网络安全。

图 3-13 DHCP Sooping 的应用典型组网



3.5 术语与缩略语

缩略语

缩略语	英文全称	中文全称
PPP	Point-to-Point Protocol	点到点协议
MP	MultiLink PPP	多链路 PPP
PAP	Password Authentication Protocol	密码验证协议
CHAP	Challenge-Handshake Authentication Protocol	挑战握手验证协议
LCP	Link Control Protocol	链路控制协议
NCP	Network Control Protocol	网络层控制协议
MRU	Maximum Receive Unit	最大接收单元
RTP	Real-time Transport Protocol	实时传输协议

缩略语	英文全称	中文全称
CCP	Compression Control Protocol	压缩控制协议

4 URPF 特性

关于本章

4.1 介绍

定义

URPF 是 Unicast Reverse Path Forwarding 的简称，又称单播逆向路径转发，是一种用于防止基于源地址欺骗的网络攻击行为的技术。

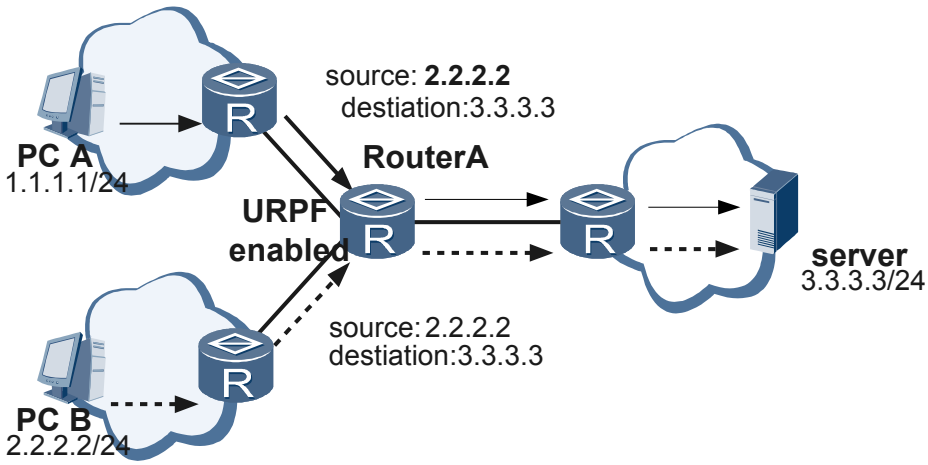
一般情况下，路由器接收到报文，获取报文的目的地址，针对目的地址查找转发表，如果找到了就转发报文，否则丢弃该报文。而 URPF 通过获取报文的源地址和入接口，在转发表中查找源地址对应的接口是否与入接口匹配，如果不匹配，则认为源地址是伪装的，直接丢弃该报文。通过这种方式，URPF 能够有效地防范网络中通过修改报文源 IP 地址而进行恶意攻击行为的发生。

要保证 URPF 正常的工作，必须确保从客户流向 Internet 上某主机的报文与该主机流向客户的报文在客户路由器和 ISP 路由器之间所经过的链路一致，也就是要保持路由的对称性。否则，URPF 将因为接口不匹配而丢掉某些正常的报文

目的

当前，基于源地址欺骗发起的网络攻击，已经成为 Internet 上一种非常普遍的攻击形式，造成源地址欺骗造成的网络安全问题。

图 4-1 源地址欺骗攻击示意图



如图 4-1 所示，PC A 伪造了源地址为 2.2.2.2 的报文，向 Server 发起请求，Server 在收到请求报文后就向 PC B（2.2.2.2）发送回应报文。PC A 发起的这种伪造报文对 Server 以及 PC B 都造成了攻击。

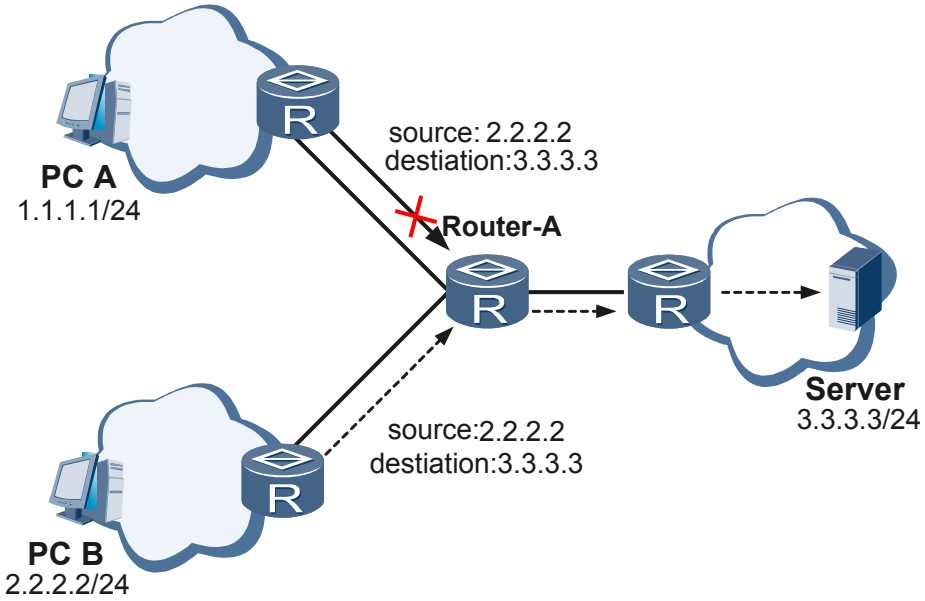
大量的这种伪造报文会造成 DOS（Denial of Service）攻击，对网络的影响极大。

在网络入口处解决源地址欺骗，使用单播逆向路径转发（URPF）技术可以解决源地址欺骗造成的网络安全问题。

说明

URPF 支持对 IPv4/IPv6 报文 DOS 攻击的防护。

图 4-2 URPF 防止基于源地址欺骗示意图



如图 4-2 所示，在 Router A 上使能 URPF 功能后，PC A 发送的伪造报文就会在 Router A 处被直接丢掉，而 PC B 的报文的被正常的转发。

URPF 作为网络入口安全机制防范攻击，在性能上优于传统的防火墙。

受益

运营商受益

URPF 业务给运营商带来了明显的收益：

有效解决网络入口处源地址欺骗问题。网路入口处启用 UFPF 过滤伪造源的 IP 地址的攻击报文，剩下的攻击报文的源 IP 地址都是合法，轻而易举寻找攻击源。

用户受益

无

4.2 参考标准和协议

不涉及

4.3 原理描述

4.3.1 URPF 的基本原理

4.3.1 URPF 的基本原理

URPF 是解决网络中源地址欺骗攻击。使能 URPF 后，设备会根据报文的源 IP 的反查路由，确定用户源地址的合法性。若不匹配，则认为非法报文直接丢弃。

在复杂的网络环境中应用 URPF 时，会遇到路由不对称的情况，这时，URPF 不能正常的工作。

为了解决复杂网络中应用 URPF 的问题，NE20E-X6 中实现了 URPF 的两种模式：

- 严格模式
- 松散模式

严格模式

URPF 严格模式，不仅要求在转发表中存在相应表项，还要求接口一定匹配的数据报文才能通过 URPF 检查。

基于接口使能 URPF 的严格模式，IP（IPv6）数据报文从接口进入路由器，使用报文的源 IP（IPv6）地址+ VRF（VPN 的索引）查找路由表，命中表项后取路由表的出接口信息与报文入接口信息比较，结果相同则认为通过 URPF 检查，按正常流程转发数据报文。如果查路由表未命中，或者命中路由表的出接口信息与数据报文入接口信息比较的结果不完全相同，则认为是非法数据报文，存在源地址欺骗，丢弃数据报文。

如果两个网络边界路由器 之间只有一条路径的话，这时，路由能够保证是对称的， 建议使用 URPF 严格模式。使用严格模式能够最大限度的保证网络的安全性。

松散模式

URPF 松散模式，不检查接口是否匹配，只要存在针对源地址的路由能，数据报文就通过 URPF 检查。

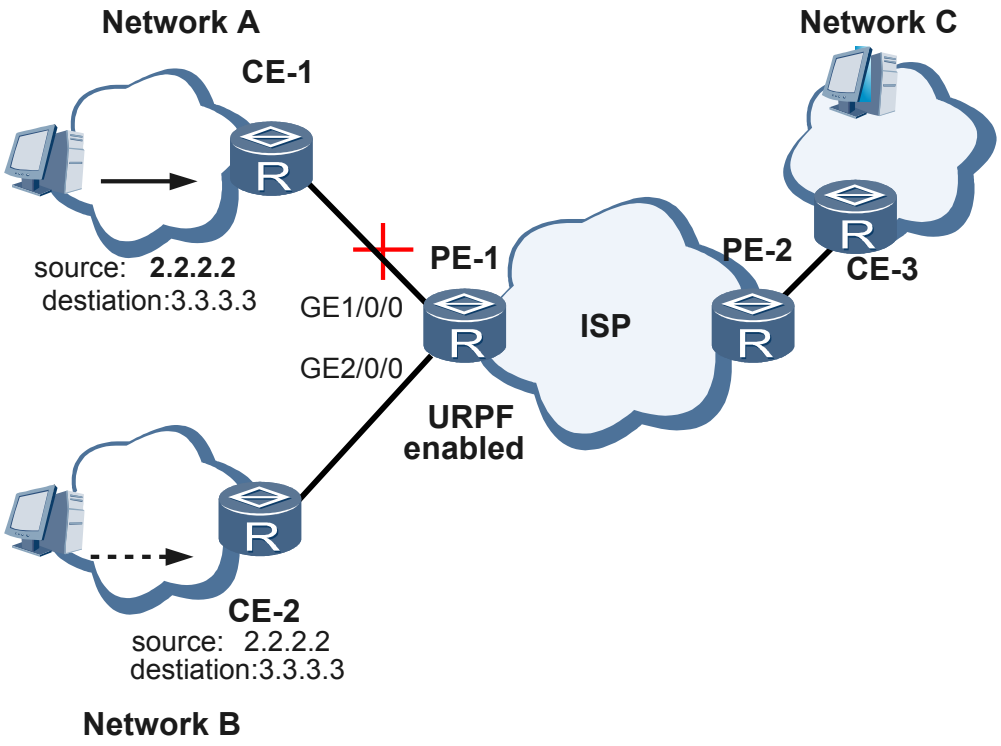
基于接口使能 URPF 的松散模式，IP（IPv6）数据报文从接口进入路由器，使用报文的源 IP（IPv6）地址+ VRF（VPN 的索引）查找路由表，命中表项则认为通过 URPF 检查，按正常流程转发数据报文。如果查路由表未命中，，则认为是非法数据报文，存在源地址欺骗，丢弃数据报文。

两个网络边界之间如果有多个连接的话，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。

4.4 应用

URPF 严格模式在运营商网络中的应用

图 4-3 URPF 单宿主客户应用环境示意图



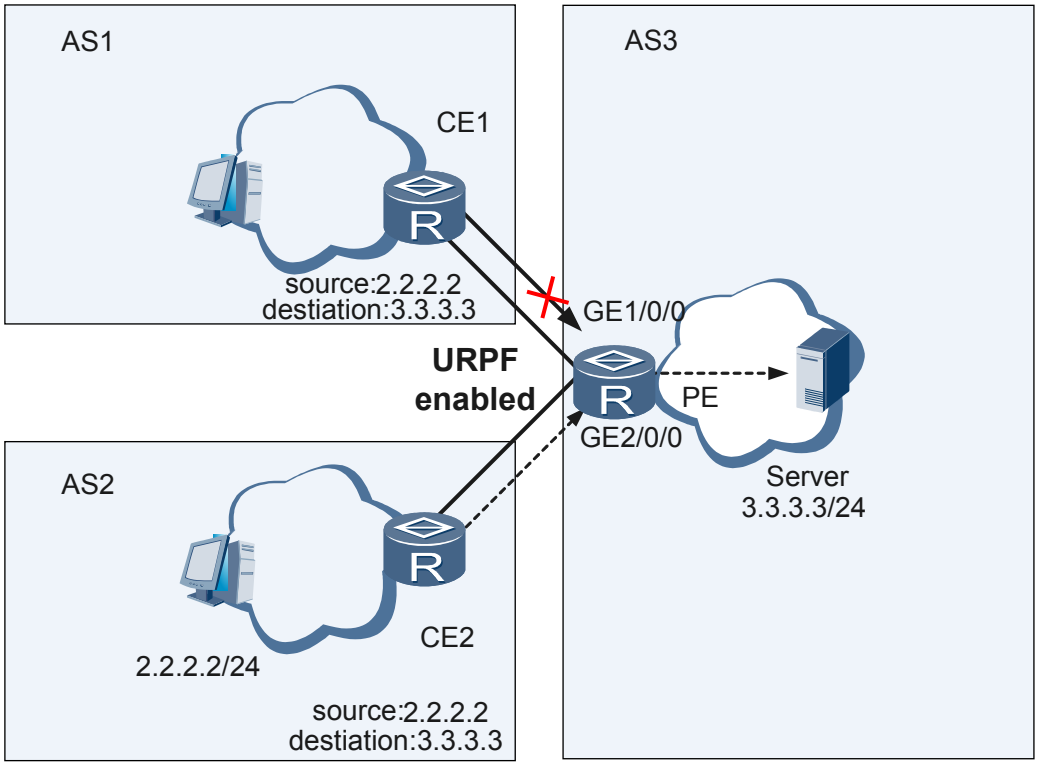
如图 4-3 所示，用户网络 A 和用户网络 B 与 PE 直连。在 PE 的 GE1/0/0 接口和 GE2/0/0 接口上启动 URPF，可以保护运营商网络免受来自用户网络 A 和用户网络 B 的源地址欺骗攻击。

如果，用户网络 A 中的一台 PC 伪造了一个源地址为 2.2.2.2 的报文，通过运营商网络向网络 C 中发送请求。PE 在接受到这个报文后，对其进行入接口和源地址检查，发现源地址为 2.2.2.2 的报文应该从 GE2/0/0 进入，而不应该从 GE1/0/0 进入。PE 认为该报文源地址是伪造的，直接丢弃该伪造报文，导致免于攻击。

从用户网络发向 Server 的正常报文，执行 URPF 检查通过后，正常转发。

URPF 严格模式在运营商跨域网络中的应用

图 4-4 URPF 单宿主单 ISP 客户应用环境示意图



如图 4-4 所示，AS1 和 AS2 与 AS3 之间为单连接。在 RouterC 的 GE1/0/0 接口和 GE2/0/0 接口上启动 URPF，可以保护 AS3 免受来自 AS1 和 AS2 的源地址欺骗攻击。

如果，网络中的一台 PC 伪造了一个源地址为 2.2.2.2 的报文，向运营商中的 Server 发送请求。RouterC 在接受到这个报文后，对其进行入接口和源地址检查，发现源地址为 2.2.2.2 的报文应该从 GE2/0/0 进入，而不应该从 GE1/0/0 进入。RouterC 认为该报文源地址是伪造的，直接丢弃该伪造报文。

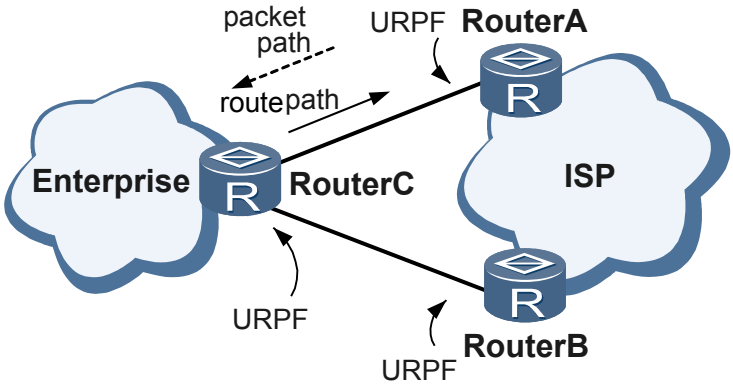
用户 2 发向 Server 的正常报文，检查通过后，被正常的转发。

URPF 松散在运营商网络中的应用

两个网络边界之间多个连接有两种情况，即：单宿主单 ISP 客户和多宿主多 ISP 客户，如下。

- 单宿主单 ISP 客户

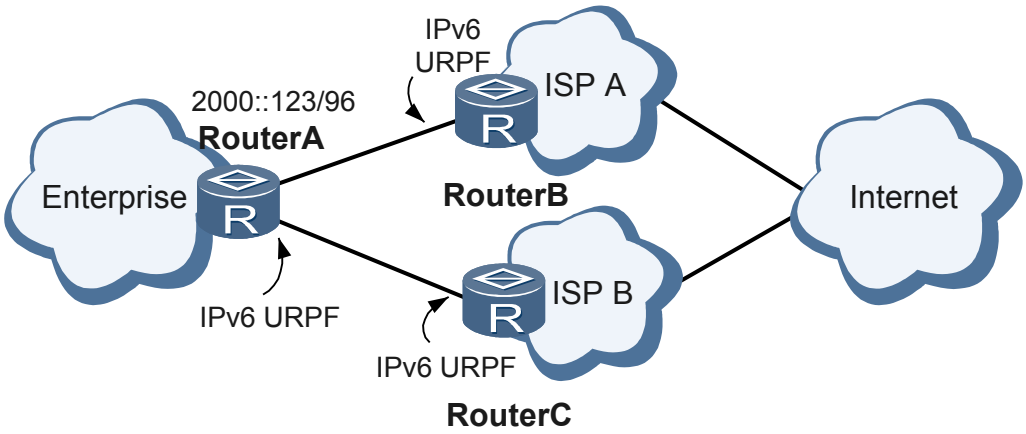
图 4-5 URPF 单宿主单 ISP 客户应用环境示意图



- 如图 4-5 所示，一个公司网络和某个 ISP 之间，为了保证可靠性，有多条连接。这时，就不能够保证 Enterprise 和 ISP 之间路由的对称性，必须使用松散模式。

URPF 松散在运营商网络中多宿主多 ISP 客户应用

图 4-6 URPF 多宿主多 ISP 客户应用环境示意图



在图 4-6 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。

客户与多 ISP 连接下的 URPF 应用具有以下特点：

- 如果用户希望某些特殊报文任何情况都可以通过 URPF 的检查，可以在 ACL 中指定这些特殊的源地址。
- 许多用户的路由器 可能只有一条缺省路由指向 ISP，此时，需要配置允许匹配缺省路由选项。

4.5 术语与缩略语

无

5 设备安全

关于本章

5.1 介绍
介绍设备安全特性的定义、目的和受益。

5.2 参考标准和协议
查阅其他的参考资料。

5.3 原理描述
介绍设备安全特性的基本原理。

5.4 术语与缩略语
术语与缩略语。

5.1 介绍

介绍设备安全特性的定义、目的和受益。

5.1.1 定义

通过本机 URPF、TCP/IP 防攻击对上送 CP 处理的欺骗、畸形报文过滤，通过 GTSM 检测上送 CP 报文的 TTL 并丢弃 TTL 非法的报文，然后通过应用层联动对上送的报文按协议粒度分类做带宽限制和优先级调度（实现上层未开启服务时底层对应报文不上送），通过管理&业务平面防护实现管理口和业务口保护，使得最终上送到 CP 集中处理的报文在流量和报文格式上都合理合法，减少不必要的 CPU 处理，实现设备安全提升。支持特性如下所列：

- 应用层联动
- 管理&业务平面防护
- TCP/IP 防攻击
- 本机 URPF
- 攻击溯源
- 动态链路保护
- GTSM
- CP-CAR
- 白名单
- 黑名单
- 用户自定义流
- 最小包补偿
- 告警

5.1.2 目的

当设备接入 Internet 时，面对网上众多的攻击，有必要提升设备的自我防护能力，以保障设备在攻击发生时可以主动过滤攻击流量，或者能及时分析攻击流量以便消除攻击威胁，或者能提供事后溯源手段避免攻击重复发生。诸如此类的能力，以提供设备持续工作时间，保障现有运行业务，提升供应商的满意度。面临的威胁包括如下几个方面：

- 非法用户通过远程访问路由器。
- 黑客利用 TCP/IP 协议栈的漏洞攻击路由器的协议栈。
- 通过泛洪流量占用路由器的上送通道。
- DOS（Deny of Service）攻击消耗 CPU 和系统的存储资源。
- 通过伪造源 IP 地址欺骗路由器造成转发表项、CPU 处理能力的无谓消耗。

5.1.3 受益

运营商受益

设备安全能给运营商带来明显的收益：

设备受攻击不中断业务、业务不受影响，提升了设备持续工作时间，提升了运营商的服务能力。

用户受益

用户得到的服务增强。以往我司数通设备受攻击用户业务中断、无法上线的情况将得到改善。

5.2 参考标准和协议

查阅其他的参考资料。

本特性的参考资料清单如下：

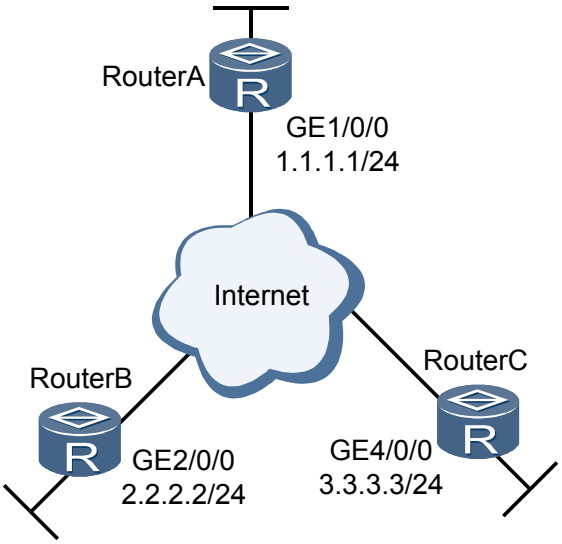
- TCP/IP Illustracted Volume 1:The Protocols, Publisher Addison Wesley/Pearson , Author W.Richard Stevens
- RFC 3682 Generalized TTL Security Mechanism(GTSM)
- RFC 959 File Transfer Protocol(FTP)
- RFC1267/1268 Border Gateway Protocol 3 (BGP-3)
- RFC 2328 Open Shortest Path First(OSPF)
- RFC 854 Telnet Protocol(TELNET)

5.3 原理描述

介绍设备安全特性的基本原理。

防攻击特性一般在如下场景发挥作用：

图 5-1 防攻击特性场景示意图



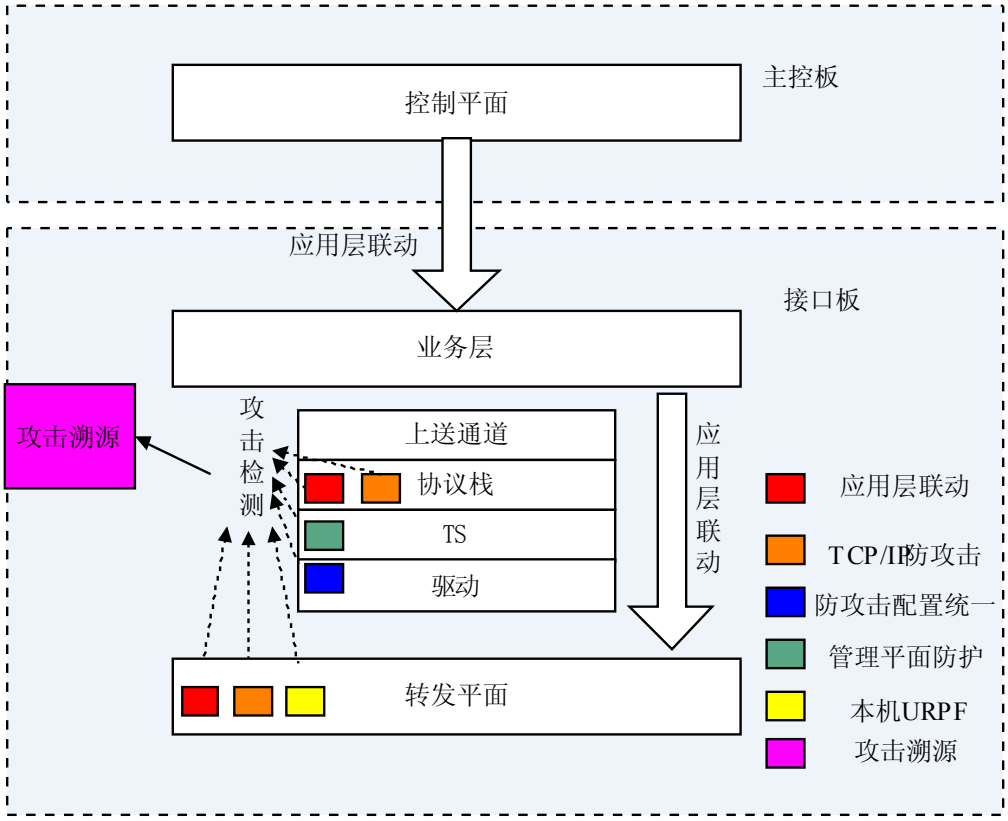
Router A 面对来自 Internet 的攻击，需要安全特性来保证设备在受攻击状态下仍然保持设备的持续服务能力，并且需要保护与 Router B、Router C 之间的通信不受影响。

5.3.1 实现原理

通过本机 URPF、TCP/IP 防攻击对上送 CP 处理的欺骗、畸形报文过滤，通过 GTSM 检测上送 CP 报文的 TTL 并丢弃 TTL 非法的报文，然后通过应用层联动对上送的报文按协议粒度分类做带宽限制和优先级调度）实现上层未开启服务时底层对应报文不上送），通过管理&业务平面防护实现管理口和业务口保护，使得最终上送到 CP 集中处理的报文在流量和报文格式上都合理合法。

如果上送过程中有丢弃报文，将激活攻击溯源，攻击溯源模块将根据自己的统计计数以及配置的采样比对同类型上送报文进行记录。如果丢弃的报文数量超过阈值，将激活告警，提醒客户当前的报文丢弃数量和丢弃模块信息。

图 5-2 设备安全示意图



5.3.2 应用层联动

应用层联动指的是将控制层面的协议开关状态和底层转发引擎的协议上送关联起来。通过在上层和底层建立联系，在协议开关状态上保持一致，对于设备没有开启业务的协议，底层硬件默认是以小带宽上送其协议报文，也可以配置为完全不上送，这样就将攻击者的攻击范围尽可能缩小，增加了攻击的成本，减少了设备的安全风险。

以 BGP 业务为例，如果 R1 上没有配置 BGP 业务，那么 BGP 报文即使上送到主控 CPU 也是要丢弃，因此应用层联动根据上层的配置在 NP 就将 BGP 报文丢弃，减少无用的处理。

5.3.3 管理&业务平面防护

管理&业务平面防护有两个作用，一个是指定某几个端口为管理端口，其他的端口收到的管理报文一概丢弃，可以防止攻击者通过网络接口远程控制路由器。另外一个作用是在软件层面再对协议报文做一次控制。管理业务平面防护模块通过三级策略的配置（接口级，板级，全局级）能够方便的指定路由器的某一个端口能够处理哪几种类型的协议报文。

5.3.4 TCP/IP 防攻击

对于基于 TCP/IP 协议的一些畸形报文或是一些典型的攻击报文，主要是利用 TCP/IP 防攻击模块进行防护。通过构造一系列的 ACL，将畸形报文和攻击报文的特征下发到 ACL

中进行报文的识别，然后可以采取直接丢弃或者是采取 CAR 带宽限流的方式防护。TCPIP 防攻击模块的关键在于灵活和可扩展，因为攻击的方式总是在改变，所以攻击报文的特征识别需要不断更新。

5.3.5 本机 URPF

URPF(Unicast Reverse Path Find)是单播反向路径检查的缩写，分为严格模式和松散模式，其原理是数据报文从网络接口进入到 NP，对于三层 IP 报文，查找路由表 FIB，如果是本机路由则上送 CP 处理，在上送之前需要做 URPF 检查，检查数据报文的源 IP 地址是否合法，检查的原理是根据数据包的源 IP 地址查路由表。

支持配置检查模式为严格模式和松散模式，以及允许匹配缺省路由的方式。

- 对于严格模式：如果报文能匹配明细路由，并且入接口跟匹配路由的出接口一致，则允许报文上送，否则丢弃报文。
- 对于松散模式：如果报文匹配上明细路由，则运行报文上送，否则丢弃报文。默认情况下，会认为缺省路由不存在，不会去匹配缺省路由，只有进行了配置时候，才会去匹配缺省路由的。

对允许匹配缺省路由的模式，必须和严格模式一起配置，报文匹配明细路由或者缺省路由，并且报文入接口跟匹配路由的出接口一致才上送，否则丢弃。不支持缺省路由与松散模式一起配置，因为这样无法达到防攻击的效果。松散模式和严格模式互斥，只能配置一种模式。

本机 URPF 的防护主要是针对变源 IP 攻击，一般攻击者会构造大量的变源 IP 地址的攻击，对于本设备的 IP 报文在上送 CPU 之前做一次本机 URPF 检查，可以减少受到变源 IP 攻击的可能性。

5.3.6 攻击溯源

攻击溯源可以看成是一个处理能力较强的日志处理中心。对于各个模块检测到攻击，会将攻击报文的信息发送到攻击溯源模块进行记录，通过维护一个较大的缓冲区，攻击溯源模块可以根据时间戳对攻击的的报文按照时间戳进行排序。支持方便的精确查询和模糊查询，并且当接口板重启后信息不会丢失，通过命令行还可以按照标准文件格式将其导入到主控板的 CF 卡保存。

目前攻击溯源不支持将记录输出到单独的服务器。

5.3.7 动态链路保护

设备安全的一个重要目标就是对已经建立起来的业务，需要保障其不受攻击的影响。动态链路保护特性通过白名单特性保护基于会话的应用层数据，如 BGP Session 数据，保护已有业务在攻击发生时的正常运行。

利用防攻击特性里面的白名单，当设备检测到 BGP Session 建立时，会将此 Session 信息同步下发到白名单中，后续上送报文如匹配此 Session 特征信息，此类数据将会享受高带宽高优先级上送的权利，由此保证了此 Session 相关业务的运行可靠性、稳定性。反之当设备检测到 BGP Session 拆除时需将此 Session 信息从白名单中删除。

5.3.8 GTSM

GTSM(Generalized TTL Security Mechanism)是通用跳数检测机制的缩写，即通过检测上送的 TTL 值合法与否，来保护 CPU 免受 CPU-utilization（CPU overload）类型的攻击。

5.3.9 CP-CAR

CP-CAR 用来设置上送 CPU 的报文的分类限速上送规则，针对每类报文可设置均值速率、承诺突发尺寸、优先级信息等。通过对不同的报文设置不同的 CAR 规则，可以降低报文的相互影响，达到保护 CPU 的目的。CAR 还可以设置上送 CPU 报文的整体速率，当整体上送速率超过阈值后，报文将被丢弃，避免 CPU 过载。

5.3.10 白名单

白名单指合法用户或者是高优先级用户的集合。通过设定白名单信息可主动保护现有业务、高优先级用户业务。可将确定为正常使用设备的合法用户或者是高优先级用户业务设置到白名单中，后续匹配白名单特征的报文会被采用高速率高优先级上送。

5.3.11 黑名单

黑名单指非法用户的集合。通过设定 ACL，可将确定为攻击的非法用户设置到黑名单中，后续匹配黑名单特征的报文会被丢弃或者低优先级上送。

5.3.12 用户自定义流

用户自定义流指用户自定义防攻击 ACL 规则。主要应用于当后续网络中出现不明攻击时，用户可灵活指明攻击流数据特征，将符合此特征的数据流进行上送限制。

5.3.13 最小包补偿

NE20E-X6 支持最小包补偿功能，可以解决小报文攻击的问题。路由器收到上送 CPU 的报文后，进行长度检测：

- 如果报文的实际长度小于预设的最小包长，使用设定的长度计算报文的上送速率。
- 如果报文的实际长度大于预设的最小包长，使用实际的报文长度计算报文的上送速率。

5.3.14 告警

如果一定时间内的丢包超过阈值限制，则安全特性会通过 MIB 向网管发送告警，提示用户当前有大量丢包，需要处理。

如果丢包现象消失，则告警取消。

5.4 术语与缩略语

术语与缩略语。

5.4.1 缩略语

5.4.1 缩略语

缩略语	英文全称	中文全称
ACL	Access Control List	访问控制列表
CAR	Committed Access Rate	接入速率限制
CP	Central Process	集中处理
CPU	Center Process Unit	中央处理器
DOS	Deny of Service	拒绝服务(攻击)
GTSM	Generalized TTL Security Mechanism	通用 TTL 安全机制
IP	Internet Protocol	网际协议
ISP	Internet Service Provider	Internet 服务提供商
NP	Network Processor	网络处理器
TCP	Transmission Control Protocol	传输控制协议
TTL	Time to live	存活时间(指报文能在路由器间传递的跳数)
URPF	Unicast Reverse Path Find	单播反向路径查找

6 GTSM

关于本章

6.1 介绍

定义

GTSM（Generalized TTL Security Mechanism），即通用 TTL 安全保护机制，是一种通过检查 IP 报文头中的 TTL 值是否在一个预先定义好的特定范围内，从而实现对 IP 上的业务进行保护的机制。

目的

GTSM 主要用于保护建立在 TCP/IP 基础上的控制层面协议免受 DoS（Deny of Service）攻击。例如，攻击者模拟真实的路由协议，对一台设备不断发送报文，导致设备因处理这些“合法”报文（攻击报文）而使系统异常繁忙，CPU 占用率过高。为了避免 CPU 过载，采用 GTSM 策略，通过检查 IP 报文头中的 TTL 值是否在一个预先定义好的范围内以实现对采用 IP 转发的业务进行保护。

6.2 参考标准和协议

本特性的参考资料清单如下：

文档	描述	备注
RFC3682	The Generalized TTL Security Mechanism (GTSM) is designed to protect a router's TCP/IP based control plane from CPU-utilization based attacks.	不支持基于 TUNNEL 邻居，如：IP in IP 和 IP in MPLS。

6.3 原理描述

GTSM 是 TTL 安全机制，通过 TTL 的检测来达到防止攻击的目的。TTL 字段存在于 IP 报文头里，用于设置数据包可以经过的最多设备数。如果某个协议或者业务满足 TTL 范围这个限制条件就可以使用该机制保护设备不受攻击。

GTSM 应用的前置条件

GTSM 应用的前置条件如下：

- 路由协议（BGP/BGP4+/OSPF）的邻居都是建立在相邻或者相近设备之间。
- 报文转发过程中 TTL 不易被篡改。

说明

需要在协议作用范围内的所有设备上部署 GTSM 策略。

GTSM 的实现

GTSM 是一种利用 TTL 防止以上类型攻击的通用化技术，主要手段如下：

- 对于直连的协议邻居：将需要发出的协议报文的 TTL 值设定为 255，这样部署了 GTSM 功能的邻居收到时，邻居转发层面会将 TTL 值非 255 的协议报文直接丢弃，避免了对控制层面的攻击。
- 对于多跳的邻居：可以定义一个合理的 TTL 范围，例如 251 ～ 255，邻居转发层面将超出这个 TTL 范围的协议报文直接过滤掉，从而避免了控制层面受到攻击。

GTSM 的使用范围

GTSM 的应用范围如下：

- GTSM 对于 IPv4 的 TTL 机制以及 IPv6 的 Hop Limit 机制同样适用。GTSM 的 TTL 就是泛指 TTL 和 Hop Limit。
- GTSM 对于单播报文有效，对组播报文无效。因为组播报文本身具有 TTL 是 255 的限制，不需要使用 GTSM 进行保护。

GTSM 处理流程

GTSM 保护的是 CPU 资源，转发层面发送给本机的协议报文，该报文上送 CPU 时：

- 如果设备使能了 GTSM 功能，首先进行 GTSM 策略匹配，如果匹配了 GTSM 策略，再判断报文的 TTL 是否在策略允许的范围内，超过则认为是攻击报文，丢弃；如果不匹配 GTSM 策略的报文按照缺省动作处理。
- 如果设备没有使能 GTSM 功能，报文直接上送控制层面。

6.3.1 BGP/BGP4+ GTSM

6.3.2 OSPF GTSM

6.3.3 LDP GTSM

6.3.1 BGP/BGP4+ GTSM

GTSM 机制通过对 IP 报文头中 TTL 的检测来达到防止攻击的目的。

如果攻击者模拟真实的 BGP/BGP4+协议报文，对一台设备不断地发送报文，设备转发层面接收到报文后，检测是否是 BGP 报文：

1. 对于非 BGP 报文，将按照配置的缺省处理策略进行转发或丢弃。
2. 对于 BGP 报文:
   (1) 如果设备使能了 GTSM 功能，首先进行 GTSM 策略匹配，如果匹配了 GTSM 策略，再判断报文的 TTL 是否在策略允许的范围内，超过则认为是攻击报文，丢弃；不匹配 GTSM 策略，按照缺省策略丢弃或者上送。
   (2) 如果设备没有使能 GTSM 功能，报文直接上送控制层面。

BGP/BGP4+策略基于邻居粒度，建立多少 BGP 的邻居，可以启用相应的 GTSM 策略数。

6.3.2 OSPF GTSM

GTSM 机制通过对 IP 报文头中 TTL 的检测来达到防止攻击的目的。

如果攻击者模拟真实的 OSPF 协议报文，对一台设备不断地发送报文，设备转发层面接收到报文后，首先判断是否是 OSPF 报文：

1. 对于非 OSPF 报文，将按照配置的缺省处理策略进行转发或丢弃。
2. 对于 OSPF 报文:
   (1) 如果设备使能了 GTSM 功能，首先进行 GTSM 策略匹配，如果匹配了 GTSM 策略，再判断报文的 TTL 是否在策略允许的范围内，超过则认为是攻击报文，丢弃；不匹配 GTSM 策略，按照缺省策略丢弃或者上送。
   (2) 如果设备没有使能 GTSM 功能，报文直接上送控制层面。

OSPF 支持协议粒度。公网只能有一种 GTSM 的策略，私网基于 VPN 实例的策略，每个 OSPF VPN 均可以配置相应的 GTSM 策略。

6.3.3 LDP GTSM

GTSM 机制通过对 IP 报文头中 TTL 的检测来达到防止攻击的目的。

如果攻击者模拟真实的 LDP 协议报文，对一台设备不断地发送报文，设备转发层面接收到报文后，首先判断是否是 LDP 报文：

1. 对于非 LDP 报文，将按照配置的缺省处理策略进行转发或丢弃。
2. 对于 LDP 报文:
   (1) 如果设备使能了 GTSM 功能，首先进行 GTSM 策略匹配，如果匹配了 GTSM 策略，再判断报文的 TTL 是否在策略允许的范围内，超过则认为是攻击报文，丢弃；不匹配 GTSM 策略，按照缺省策略丢弃或者上送。
   (2) 如果设备没有使能 GTSM 功能，报文直接上送控制层面。

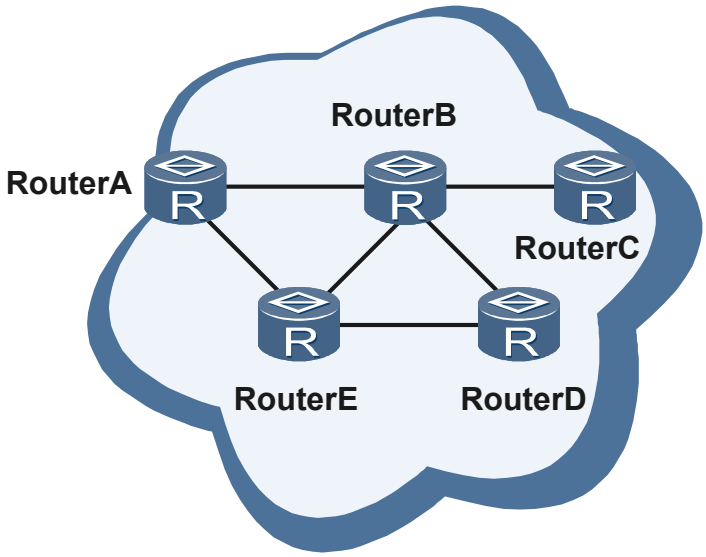
LDP GTSM 基于邻居粒度，建立多少 LDP 邻居，可以启用相应数目的 GTSM 策略。

6.4 应用

如图 6-1 所示：

- RouterA 和 RouterB 是相邻设备，通过直连接口互连，RouterB 发出报文 TTL 为 255，RouterA 设备收到报文也为 255。
- RouterA 和 RouterC，是相近设备，通过 RouterB 互连，RouterC 发出的报文 TTL 为 255，到 RouterA 接收的时候 TTL 为 254。
- 设备 RouterD 通过网络连接到设备 RouterA 上，网络固定 RouterD 到 RouterA 的跳数为 n，RouterD 发出的报文 TTL 为 255，到 RouterA 接收的时候 TTL 为 255-n。

图 6-1 GTSM 应用组网图



对于以上组网，通过在所有设备上启动 GTSM 保护。

- 在 RouterA 上收到 RouterB 发送过来报文的 TTL 合法值为 255。
- 在 RouterA 上收到 RouterC 发送过来报文的 TTL 合法范围为 254 到 255。
- 在 RouterA 上收到 RouterD 发送过来报文的 TTL 合法范围为 (255-n)到 255。

只有满足以上条件的报文才上送 CPU，否则报文将被直接丢弃。

6.5 术语与缩略语

缩略语

缩略语	英文全称	中文全称
GTSM	Generalized TTL Security Mechanism	通用 TTL 安全机制
TTL	Time To Live	存活时间

7 镜像

关于本章

7.1 介绍
介绍镜像特性的定义、目的和受益。

7.2 参考标准和协议
查阅其他的参考资料。

7.3 原理描述
介绍本地镜像和远端镜像的基本原理以及组网应用。

7.1 介绍

介绍镜像特性的定义、目的和受益。

7.1.1 定义

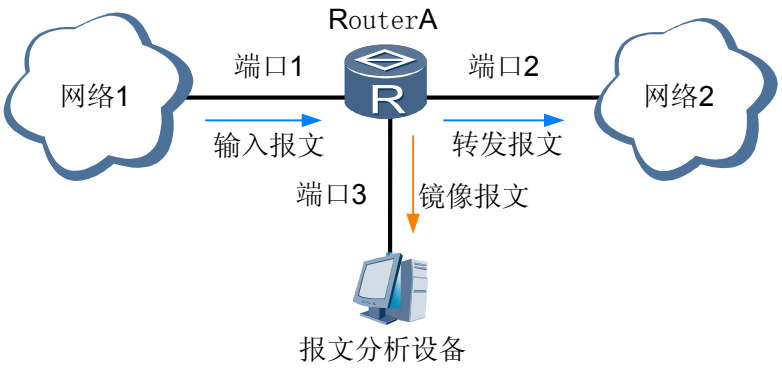
镜像是一种捕获接口输入或者输出报文的方式，捕获报文的过程不影响报文的转发处理，这一特性通常用来定位网络问题。

按照镜像口和观察口的位置可以分为：

- 本地镜像

  本地镜像指：将本设备一个接口的流量复制一份，从本设备一个接口输出。 如图 7-1 所示，端口 1 为“本地镜像端口”、端口 3 为“本地观测端口”。

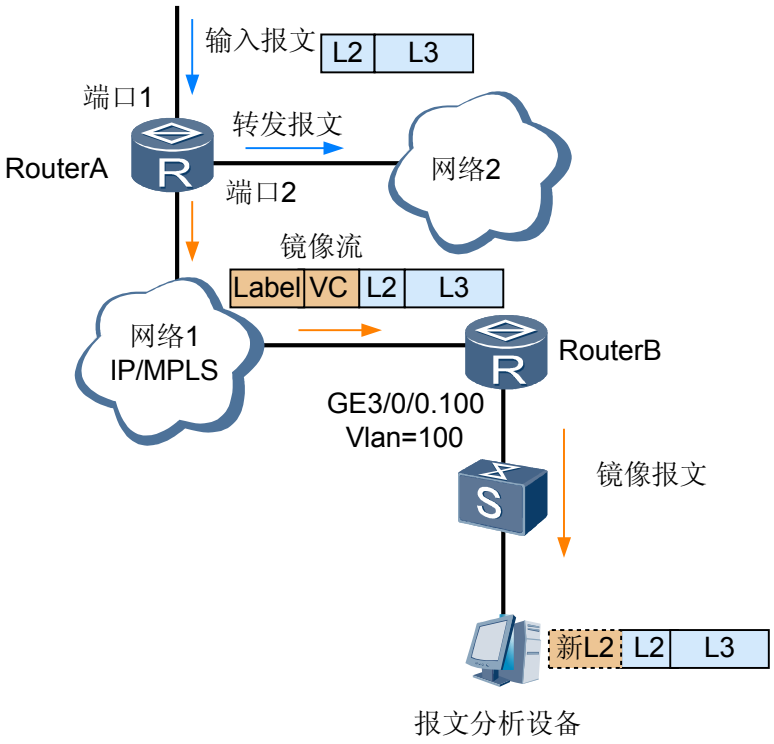
  图 7-1 本地镜像示意图



- 远端镜像

  远端镜像：指将 RouterA 上一个接口的流量复制后，通过隧道传输到 RouterB，从 RouterB 上的一个接口输出到观测设备。如图 7-2 所示，RouterA 端口 1 为“远端镜像口”，RouterB 的端口 3 为“远端观察口”。

  图 7-2 远端镜像示意图

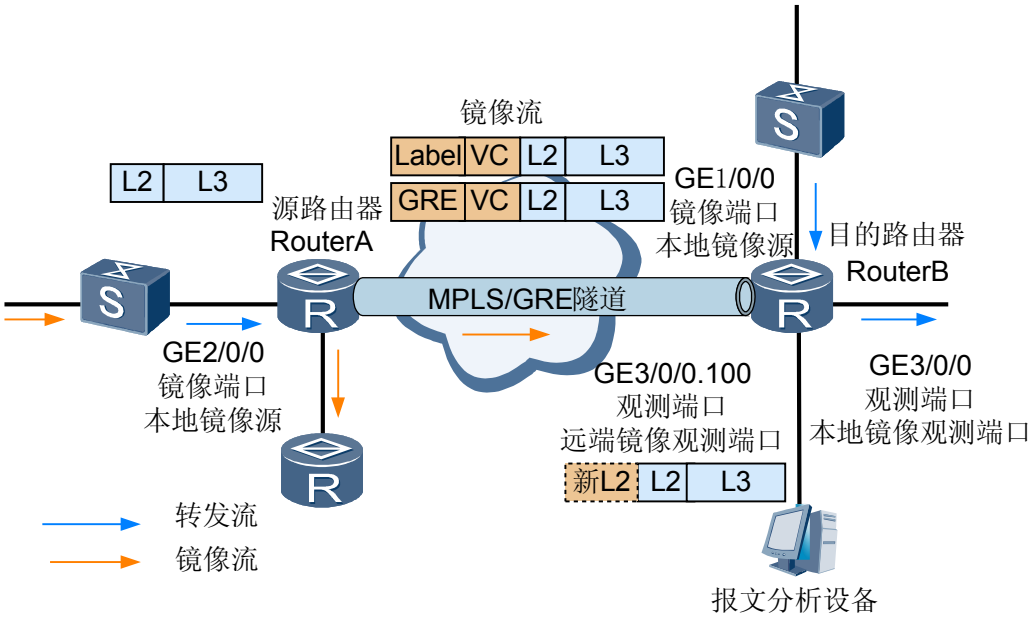


按照镜像策略可以分为：

- 端口镜像：镜像端口输入或输出的所有流量；
- 流镜像：通过配置过滤原则，只镜像符合条件的流量。

为了下文的描述方便，我们统一如下名词术语：

图 7-3 “本地镜像”和“远端镜像”应用及名词示意图



- 本地镜像源：在本地镜像中，作为镜像端口的接口，该接口的数据会被拷贝一个副本从本地指定的观测端口发送出去。例如图 7-3 中 RouterB 上的 G1/0/0。
- 本地镜像观测端口：输出本地某个接口上镜像数据的接口。例如图 7-3 中 RouterB 上的 G3/0/0。
- 源路由器：远端镜像源所在的路由器；例如图 7-3 中 RouterA。
- 目的路由器远端镜像观测端口所在的路由器；例如图 7-3 中 RouterB。
- 远端镜像源：在远端镜像中，作为镜像的接口，该接口的数据会被拷贝一个副本从指定的隧道发出，到达远端的一个目的路由器，并从目的路由器指定的接口输出。例如图 7-3 中 RouterA 上的 G2/0/0。
- 远端镜像观察口：输出由远端路由器发送过来的镜像数据的接口。例如图 7-3 中 RouterB 上的 G3/0/0.100

本地镜像和远端镜像都支持的功能：

- 支持基于物理接口镜像输入报文、输出报文；
- 支持基于子接口（VLAN）镜像输入报文、输出报文；
- 支持基于流分类镜像报文；
- 支持对镜像流量做 CAR；
- 支持镜像上送 CPU 的报文；

远端镜像特有的：

- 截取报文长度；
- 只镜像三层部分；
- 设定镜像流的调度优先级；
- 支持使用 MPLS LSP、GRE、MPLS TE 隧道传输镜像流。

7.1.2 目的

在网络运行过程中，要对网络设备的端口状况进行观测及分析。可以通过配置镜像功能，在不影响端口转发的前提下，将数据包完整的复制一份到指定端口，提供给网管，对当前的数据流进行监控与分析。

7.1.3 受益

用户受益

- 方便客户和用服的人员定位和分析网络问题。
- 通过远端镜像的方式，还可以省去用户奔波之苦，通过简单的配置，就可以将远端上的数据捕获到本地进行分析。

7.2 参考标准和协议

查阅其他的参考资料。

无

7.3 原理描述

介绍本地镜像和远端镜像的基本原理以及组网应用。

7.3.1 本地镜像基本原理

本地镜像支持的功能点原理介绍

- 支持基于物理接口镜像输入报文、输出报文；
  - 对从镜像口输入的二层报文完整镜像，从指定的端口输出。
  - 对从镜像口输出的二层报文完整镜像，从指定的端口输出。
- 基于子接口（Vlan）镜像输入报文、输出报文；
  - 可以通过 Vlan 过滤镜像报文，只完整镜像以太报文外层 Tag==指定 VlanID 的报文，并从指定接口输出。
- 支持基于流分类镜像报文；
  - 可以基于 QoS 的复杂流分类策略，比如 Source IP、DestIP、过滤符合条件的报文，完整镜像并从指定的端口输出。
- 支持对镜像流量做 Car；
  - 为减轻镜像流量对正常转发流量的影响，可以设置镜像 Car 参数，Cir 范围 100kbps 到 2500,000,000bps。
- 支持镜像上送 CPU 的报文；
  - 可以配置只镜像上送 CPU 处理的报文，将镜像报文从指定端口输出。

注意

本地镜像时，一个物理单板所有接口的镜像流量只能从指定一个本地观察口输出。

本地镜像的配置步骤

1. 配置一个本地观察口，指定其索引；
2. 配置本地镜像口；
3. 在镜像口的 Slot 视图下配置将镜像流送达的观察口索引；

7.3.2 远端镜像基本原理

远端镜像支持的基本功能点原理介绍

- 支持基于物理接口镜像输入报文、输出报文；
  - 对从镜像口输入的二层报文完整镜像，从指定的隧道输出。
  - 对从镜像口输出的二层报文完整镜像，从指定的隧道输出。
- 基于子接口（Vlan）镜像输入报文、输出报文；
  - 可以通过 Vlan 过滤镜像报文，只完整镜像以太报文外层 Tag==指定 VlanID 的报文，并从指定隧道输出。
- 持基于流分类镜像报文；
  - 可以基于 QoS 的复杂流分类策略，比如 Source IP、DestIP、过滤符合条件的报文，完整镜像并从指定的隧道输出。
- 支持对镜像流量做 Car；
  - 为减轻镜像流量对正常转发流量的影响，可以设置镜像 Car 参数，Cir 范围 100kbps 到 2500,000,000bps。
- 支持镜像上送 CPU 的报文；
  - 可以配置只镜像上送 CPU 处理的报文，将镜像报文从指定隧道输出。
- 支持设定截取报文长度，只镜像部分报文
  - 从头部开始取指定长度的部分，对其镜像，并从指定隧道输出。
- 支持设定只镜像三层部分；
  - 从链路层之后的部分开始镜像。
- 支持设定镜像流的调度优先级；
  - 对镜像的数据设置指定的调度优先级，默认为 BE 级别。
- 支持使用 MPLS LSP、GRE、MPLS TE 隧道传输镜像流。
  - 镜像的数据报文可以从 MPLS LSP 隧道或者 GRE 隧道，或者 MPLS TE 隧道输出。

注意

一个镜像报文只从一个隧道输出，不支持 1 to N 的输出模式。

远端镜像配置

1. 配置镜像实例
   (1) 创建实例。
   (2) 指定目的 路由器 IP 地址以及镜像流的标识。
2. 配置远端观察口，与镜像实例中指定的标识要相同
3. 配置远端镜像源

远端镜像源的处理

- 接收到报文后，镜像报文，并获取报文进入隧道的信息；
- 将报文封装为 MPLS 或者 GRE，最内层封装特定标签，标识这是镜像报文；
- 将报文从隧道入口发出。

远端目的设备的处理

- 镜像报文到达目的 路由器后，弹出外层的隧道标签。通过最内层的特定标签，识别出该报文输出的观察口；
- 在输出时，根据配置将镜像报文直接从观察口输出，或者对该报文增加二层封装再输出。

支持远程镜像的隧道

远程镜像的报文支持通过 MPLS LSP、MPLS TE、GR 隧道传送到目的 路由器，用户在配置目的 路由器的时候，只需要指定目的 路由器上的 IP 地址， 路由器会按照优选 LSP、TE 次之、GRE 最次的顺序选择隧道。用户亦可指定隧道的类型，方式如下：

配置隧道策略

```
[HUAWEI]tunnel-policy lsp
Info: New tunnel-policy is configured.
```

指定隧道类别为 LSP

```
[HUAWEI-tunnel-policy-lsp] tunnel select-seq lsp load-balance-number 1
```

在镜像实例下指定隧道类别

```
[HUAWEI-mirror-instance-A] remote-destination 12.0.0.1 identifier 10 tunnel-policy lsp
```

查看镜像实例下的配置

```
[HUAWEI-mirror-instance-a] display mirror instance a
Instance a
  Peer IP               : 12.0.0.1
  Identifier            : 10
  Tunnel Policy         : lsp
  Tunnel Type           : -
  Tunnel Index          : 0
  Tunnel Status         : DOWN
  Tunnel Outport        : -
  Slice-Size            : None
  With-Linklayer-Header : No
  Flow-Class            : be
```

远程镜像的其他可选配置项

远程镜像还可以选择配置：截取报文的长度、是否镜像链路层、流量的优先级。配置命令如下：

```
[HUAWEI-mirror-instance-a]slice-size 256
[HUAWEI-mirror-instance-a] with-linklayer-header
[HUAWEI-mirror-instance-a] flow-class af1
[HUAWEI-mirror-instance-a]display this
#
remote-destination 12.0.0.1 identifier 10 tunnel-policy lsp
 flow-class af1
 with-linklayer-header
 slice-size 256
#
```

表 7-1 是否含二层头配置对镜像处理的示意

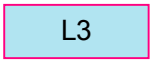
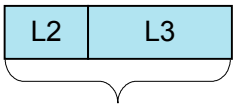
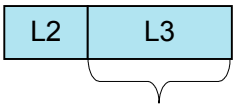
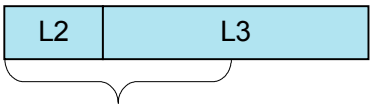
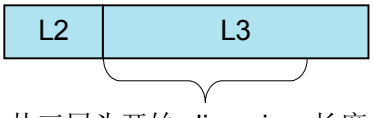
原始报文格式	镜像端口配置	观察端口配置	输出报文格式
	undo with-Linklayer-Header	undo with-Linklayer-Header	
	undo with-Linklayer-Header	with-Linklayer-Header	
	with-Linklayer-Header	undo with-Linklayer-Header	
	with-Linklayer-Header	with-Linklayer-Header	

表 7-2 镜像报文复制与“Slice-size、with-Linklayer-Header”参数的关系

Slice-size	with-Linklayer-Header	复制报文方式
= 0	*with-Linklayer-Header*	
= 0	*undo with-Linklayer-Header*	
> 0	*with-Linklayer-Header*	
> 0	*undo with-Linklayer-Header*	

说明

上 slice-size 最小为 256 字节，如果在镜像实例下配置的 slice-size 小于 256 字节，那么当应用到接口板上时，将按照 256 字节截取。

flow class 的配置是控制镜像流在设备上调度的优先级别，默认为 be 级别。镜像流量的限速，为了防止镜像流量影响业务流量。

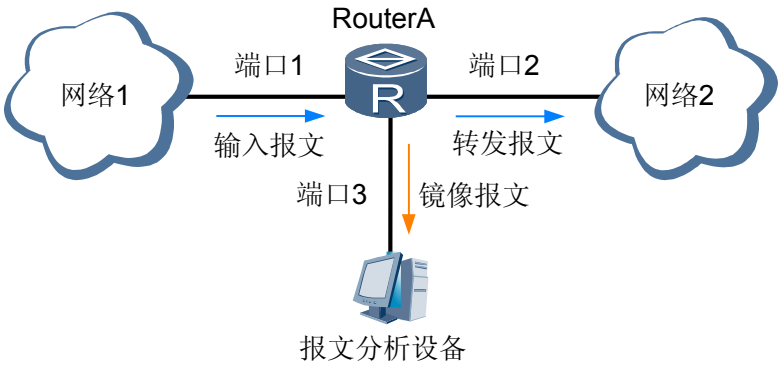
远端镜像报文的输出选择

远端观察口是子接口时，在输出镜像报文时，默认给报文再增加一个二层封装，目的 MAC 为广播 MAC，源 MAC 为接口 MAC，Tag 为子接口的 Vlan。用户也可以配置不做封装，将原始报文直接从接口输出。

7.3.3 组网应用

本地镜像应用

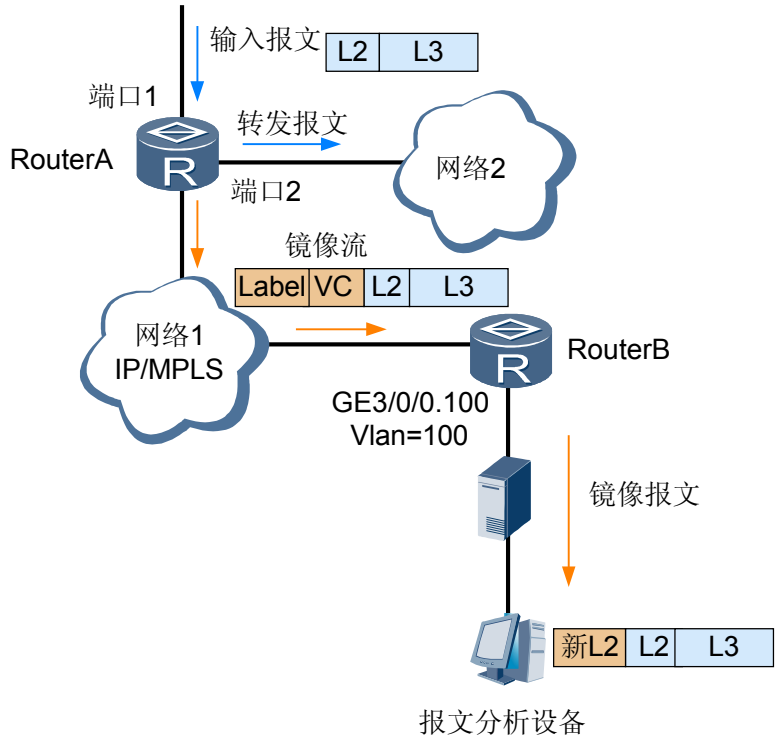
图 7-4 本地镜像应用组网图



如图 7-4 所示，Router A 的端口 1 为镜像端口，做输入报文的镜像；端口 3 为观测端口。

远端镜像应用

图 7-5 远端镜像组网图



如图 7-5 所示，报文分析设备通过交换机接入到 Router B 的观察口上，这样可以将观察口配置为子接口，如图 7-5 所示，输出的镜像报文通过 VLAN 100 输出到分析设备上。

8 合法监听

关于本章

8.1 介绍

定义

合法监听是由执法机构（LEA:Law Enforcement Agency）和运营商（ISP:Internet Service Provide）配合完成的监听系统。

执法机构根据国家相关法律向针对运营商合法监听业务进行合法授权。运营商向执法机构提供合法监听业务的支持。

目的

随着 Internet 的日渐成熟，网页浏览、即时通讯，电子邮件和各种视频应用越来越普及。信息化使人们享受到了通信的便利，同时也出现了不法分子利用通信工具实施的违法犯罪活动情况。

通过在运营商网络部署合法监听业务，执法部门可以针对网络信息内容进行监听、审计，识别违法犯罪活动进行有效打击。因此合法监听业务对于国家维护网络信息安全、打击网络犯罪，有着重要的意义。

受益

运营商收益：为执法部门提供合法监听功能。识别网络中的非法信息用于打击利用网络进行的违法犯罪活动。

8.2 参考标准和协议

文档	描述	备注
IETF： RFC3924	Cisco Architecture for Lawful Intercept in IP Networks	定义合法监听在 IP 网络中的架构

8.3 原理描述

8.3.1 合法监听的基本原理

合法监听信息

合法监听过程可以通过运营商的网络设备来获取**表 8-1** 中的信息。

表 8-1 合法监听的信息分类

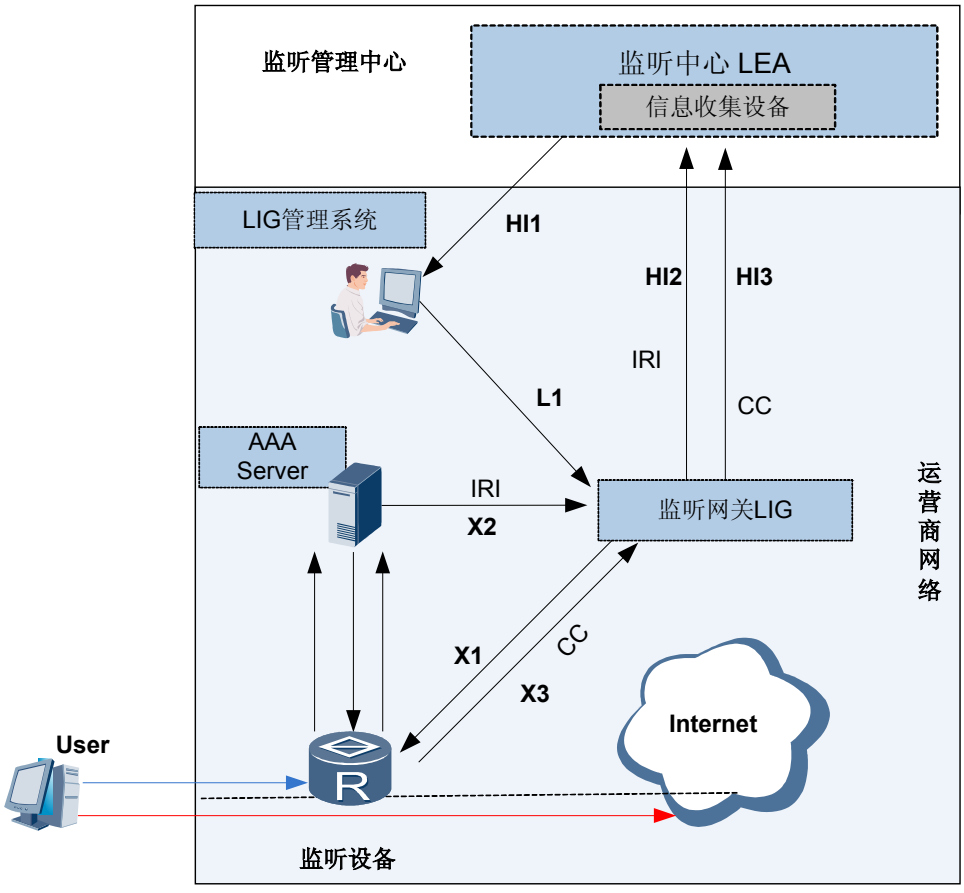
信息类型	内容	获取设备
内容信息 CC（Content of Communication）	被监听者的通讯内容本身，如 E-mail 邮件内容、VoIP 语音包等。	RADIUS、DHCP 服务器
监听相关通讯 IRI（Intercept Related Information）	通讯相关的地址、时间、网络位置等信息。	部署合法监听的设备

说明

当前 NE20E-X6 不支持 IRI。

合法监听系统模型

图 8-1 合法监听系统模型示意图



如图 8-1 所示，合法监听涉及到以下角色：

- 监听中心

执法机构通过监听中心监听上网用户的活动。因此，监听中心是监听行为的发起者和监听结果的最终接收者。其主要功能为：

定义监听目标

发起或终止监听行为

接收并记录监听结果

分析监听结果

- 监听管理中心

  监听中心的代理机构，负责接收监听中心的监听请求，并将其转换为网络中的具体位置信息和服务的标识，之后将监听配置部署到运营商的网络设备中。

- 监听网关 LIG（Lawful Interception Gateway）

  监听管理中心和运营商设备之间的代理，在合法监听功能的应用中有重要作用，具体如下：

  - 通过 L1 接口和 HI1 接口间接接收监听管理中心的监听请求
  - 通过 X 接口向不同网络设备部署监听配置并获取监听内容
  - 通过 HI2、HI3 接口向监听管理中心传送监听内容

- LIG 管理系统

  接受来自监听管理中心的监听请求，并发放给 LIG。一个 LIG 管理系统可以管理多个 LIG。

  说明

  LIG 管理系统通过 L1 接口配置 LIG。LIG 设备位于运营商侧，LIG 管理系统则由监听管理中心负责操作。

- 运营商

  负责在其维护的网络中部署合法监听功能，支持监听设备直接从监听管理中心接收配置信息并将监听流量传送回监听管理中心。

  主要功能如下：

  - 通过 X1 接口获取 LIG 发送的监听目标等信息。
  - 通过 X3 接口向 LIG 传送 CC 信息。

合法监听在实现过程中，涉及到的各个接口的含义及作用如表 8-2 所示。

表 8-2 合法监听相关的接口

接口	连接的设备角色	功能	说明
L1	连接 LIG 管理系统和 LIG	通过该接口将监听管理中心的监听控制命令向 LIG 发布。	当 LIG 呈分布式部署于运营商网络中时，可以通过多个 L1 接口发布监听命令，便于对 LIG 统一进行控制。
HI1	连接监听管理中心和 LIG 管理系统	通过该接口监听管理中心向 LIG 管理系统部署管理命令以及接受命令响应等。	无

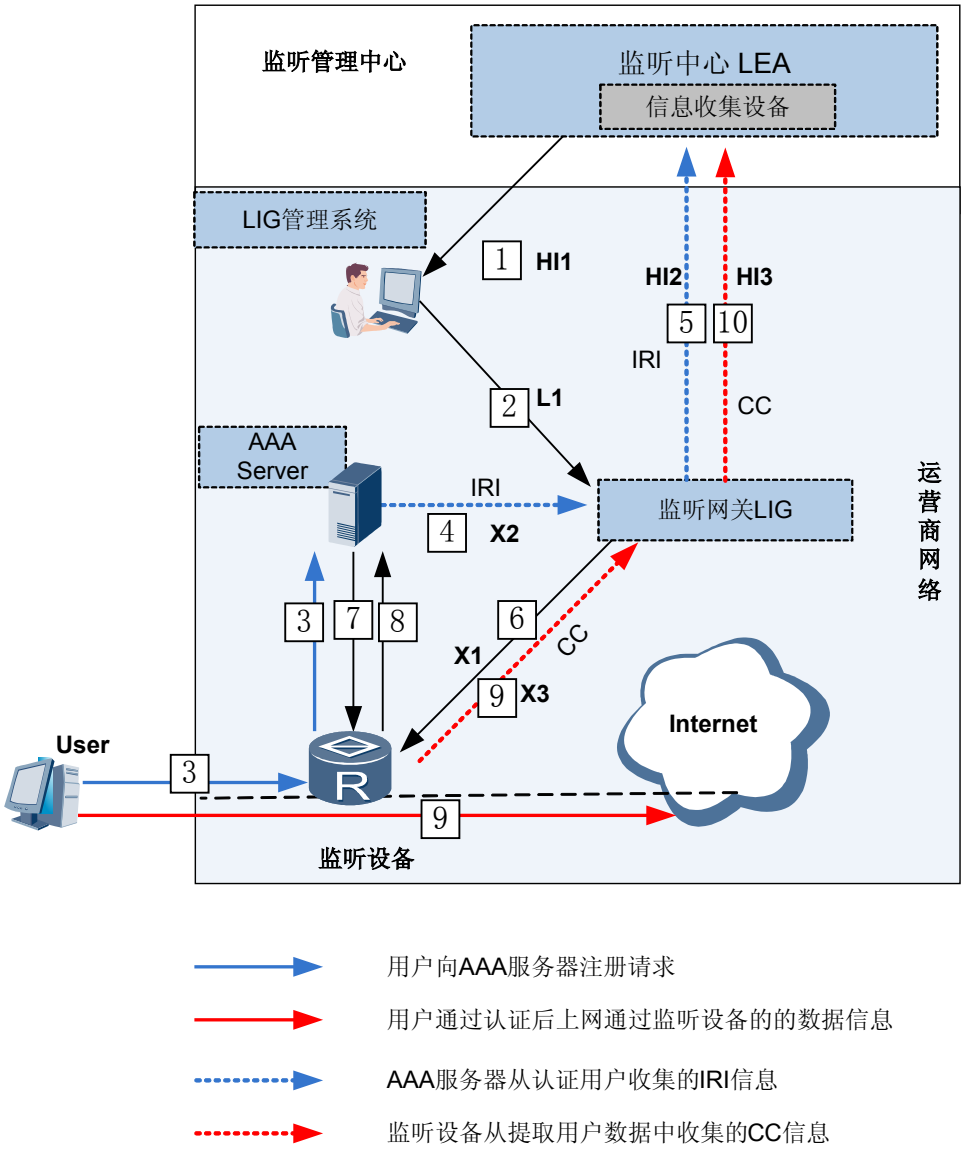
接口	连接的设备角色	功能	说明
HI2	连接监听管理中心和 LIG	通过该接口 LIG 向监听管理中心传送 IRI 信息。	无
HI3	连接监听管理中心和 LIG	通过该接口 LIG 向监听管理中心传送 CC 信息。	无
X1	连接 LIG 和运营商设备的信令接口。	通过该接口 LIG 向运营商网络设备部署监听配置，包括设定监听目标、查询监听信息并维护 X2、X3 接口。	常用的 X1 接口的实现技术为 SNMPv3，专用 MIB 方式。
X2	连接 LIG 和运营商网络设备的数据接口	通过该接口运营商网络向 LIG 传送 IRI 信息并发送告警。	该接口需要保证数据的可靠性和私密性，可以通过 TCP、UDP、IPSec 方式实现。
X3	连接 LIG 和运营商网络设备的数据接口。	通过该接口运营商网络向 LIG 传送 CC 信息和心跳信息。	无

NE20E-X6 在合法监听业务中作为运营商网络中的监听设备。支持提供 X1 与 X3 接口与 LIG 设备的信令接口和数据接口连接。

NE20E-X6 的 X3 接口可以与多个 LIG 设备共用，最多连接 10 个 LIG 设备。

合法监听的监听过程

图 8-2 合法监听的监听过程示意图



NE20E-X6 的监听的过程如下：

1. 监听中心根据监听需要，向监听管理中心下发合法监听授权书。
2. 监听管理中心将合法监听授权书的内容输入到监听网关。
3. 用户上线时，向 AAA 服务器发起认证请求。
4. 监听网关和服务器的上的监听设备（如 IP Probe、Sniffer）根据预设置的监听目标，监听流量，将用户上线时生成最初的 IRI 信息上送监听网关 LIG。
5. 监听网关 LIG 加工用户的 IRI 信息，并将 IRI 信息发送到 LEA。
6. 监听网关 LIG 向 NE20E-X6 设置监听目标。
7. AAA 服务器通知 NE20E-X6，用户已认证通过，已接入 Internet 网络。

8. NE20E-X6 向 AAA 发送计费信息。
9. NE20E-X6 复制用户上网信息流量，并发送到监听网关 LIG。
10. 监听网关 LIG 将 CC 流量发往 LEA 的信息收集设备。

当用户退出网络或者监听到期时，监听网关 LIG 删除 NE20E-X6 上设置的监听，监听结束。

8.4 应用

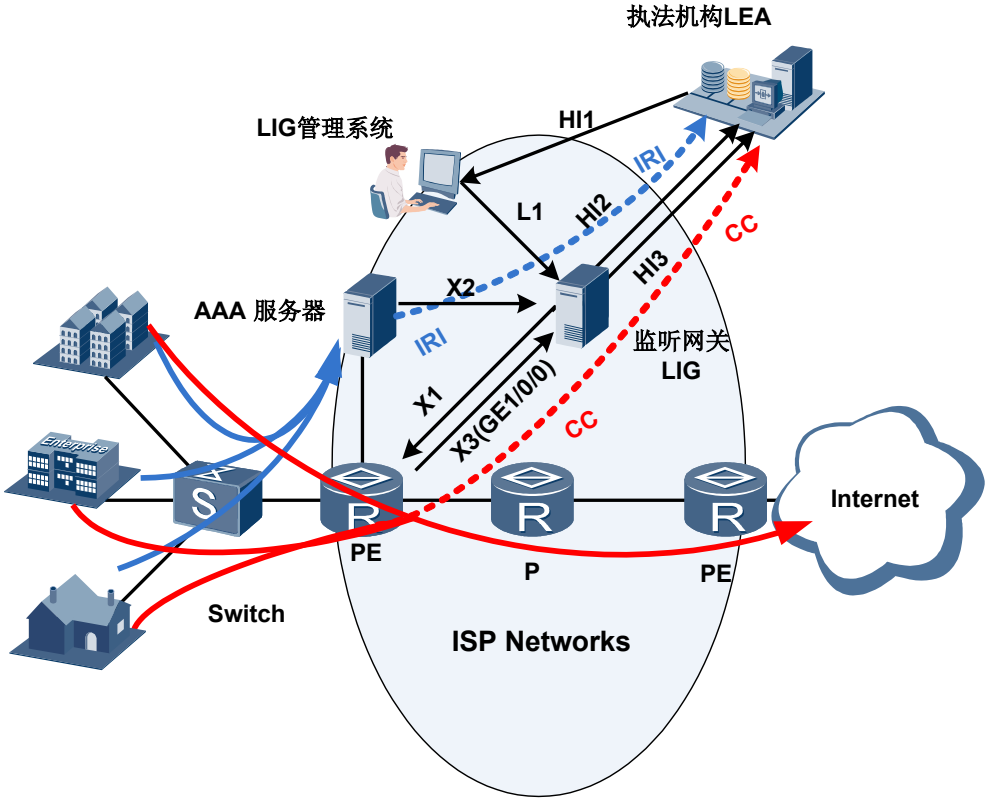
Internet 业务的合法监听应用场景

在 Internet 业务网络中，运营商为了配合执法部门 LEA 识别 Internet 中的违法犯罪活动相关信息，在承载网中网元设备上部署合法监听业务。其中：

- AAA 服务器部署合法监听业务，将认证通过用户的 IAI 信息发送到监听网关 LIG。
- 路由器部署合法监听业务，按照监听网关 LIG 获取的监听目标，将目标的 CC 信息通过 X3 接口发送到监听网关 LIG。
- 监听网关 LIG 将收集到的 Internet 用户 CC 和 IRI 信息发送到监听管理中心统一监控。

这样执法部门 LEA 作为监听管理中心可以针对指定的 Internet 用户进行监听。

图 8-3 Internet 业务的合法监听示意图



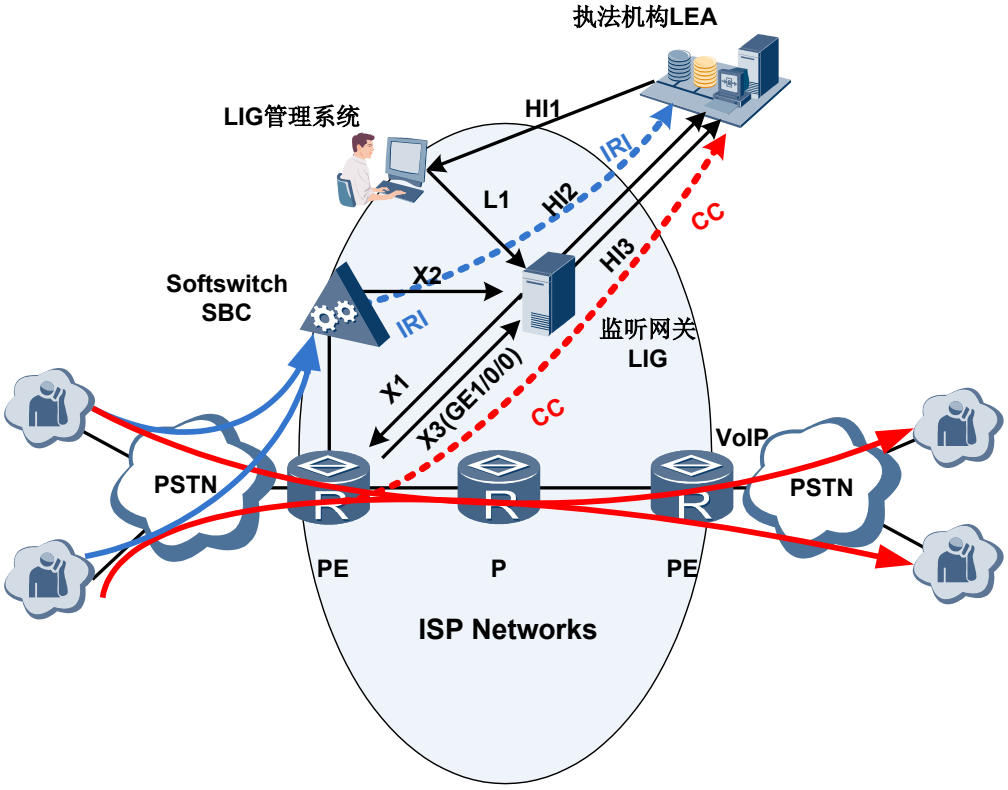
VoIP 业务的合法监听应用场景

在 VoIP 业务网络中，运营商为了配合执法部门 LEA 识别 Internet 中的违法犯罪活动相关信息，在承载网中网元设备上部署合法监听业务。其中：

- 软交换设备部署合法监听业务，将认证通过用户的 IAI 信息发送到监听网关 LIG。
- 路由器部署合法监听业务，按照监听网关 LIG 获取的监听目标，将目标的 CC 信息通过 X3 接口发送到监听网关 LIG。
- 监听网关 LIG 将收集到的 VoIP 用户 CC 和 IRI 信息发送到监听管理中心统一监控。

这样执法部门 LEA 作为监听管理中心可以针对指定的 VoIP 业务用户进行监听。

图 8-4 Internet 业务的合法监听示意图



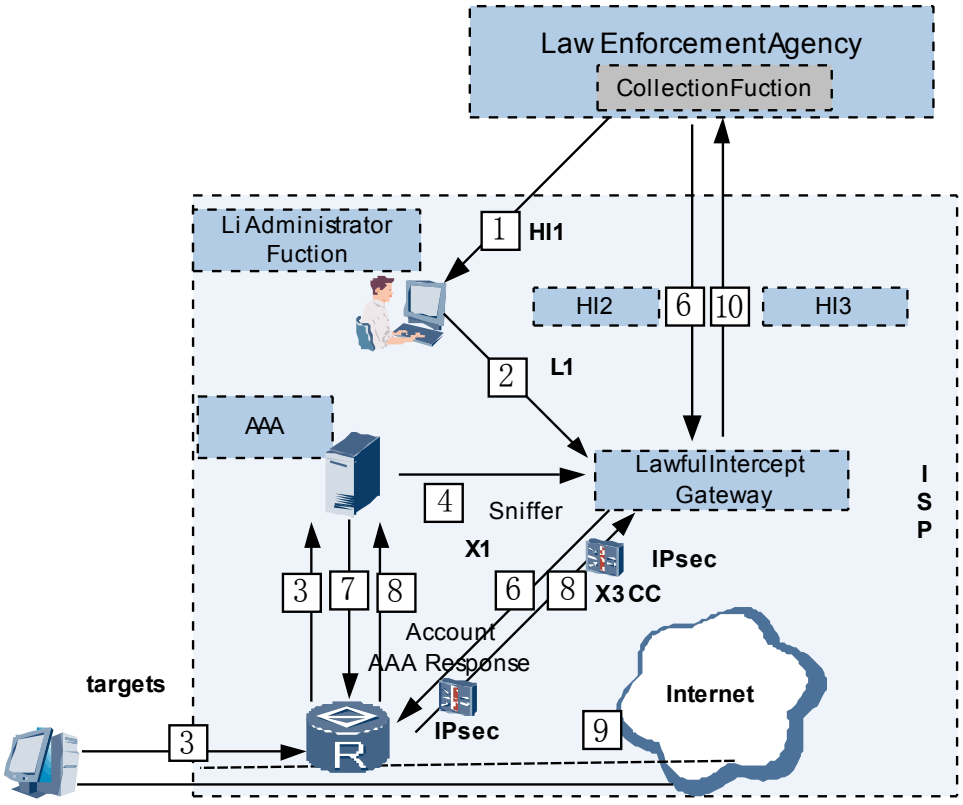
8.4.1 Internet 业务的合法监听

8.4.2 VoIP 业务的合法监听

8.4.1 Internet 业务的合法监听

Internet 业务的合法监听是与 AAA 服务器配合完成的。

图 8-5 Internet 业务的合法监听示意图



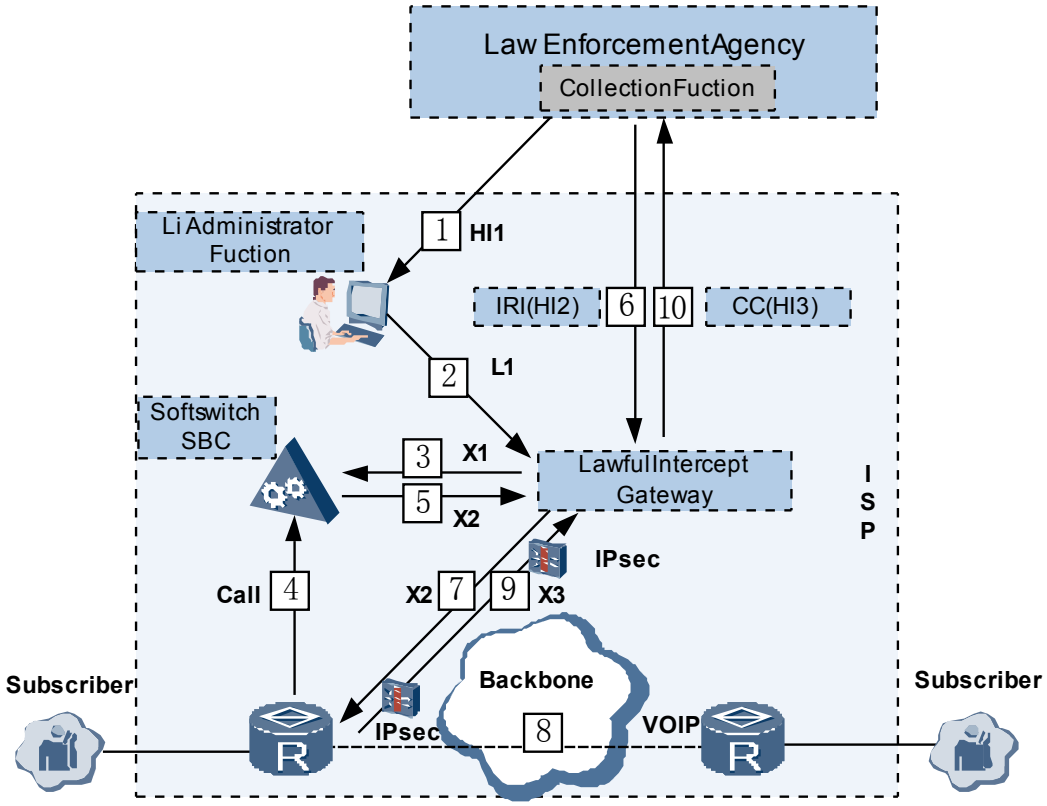
如图 8-5Internet 业务的合法监听流程步骤如下：

1. LEA 通过纸件或电子接口向监听管理中心发起监听请求
2. 监听管理中心通过图形界面在 LIG 上进行监听设置
3. 用户上线时，向 AAA 服务器发起认证请求
4. IP Probe 或 sniffer 设备根据预设置的监听目标，监听 AAA 流量，用户上线时，通知 LIG，并发送 IRI 信息
5. LIG 加工用户的 IRI 信息，并将 IRI 信息发送到 LEA
6. LIG 向 MSCG 设置监听目标
7. AAA 服务器通知 MSCG，用户已认证通过，已接入 Internet 网络
8. MSCG 向 AAA 发送计费信息
9. MSCG 复制用户上网信息流量，并发送到 LIG
10. LIG 将 CC 流量发往 LEA 的信息收集设备

用户下线时，Sniffer 或 IP Probe 设备通知 LIG，LIG 删除 MSCG 上配置的监听目标，MSCG 停止流量监听。

8.4.2 VoIP 业务的合法监听

图 8-6 VoIP 业务的合法监听示意图



如图 8-6 所示与软交换设备、SBC 配合，完成 VOIP 业务的合法监听。

具体步骤如下：

1. LEA 通过纸件或电子接口向监听管理中心发起监听请求
2. 监听管理中心通过图形界面在 LIG 上进行监听设置
3. LIG 向软交换设备设置监听目标
4. 用户发起呼叫
5. 软交换设备捕获用户呼叫信息，发送 IRI 信息到 LIG
6. LIG 将 IRI 信息发送到 LEA 的收集设备
7. LIG 向 MSCG 设置监听目标
8. 用户使用 Internet 资源，建立了通话 session，进行通话
9. MSCG 监听用户通话流量，复制用户流量报文，发向 LIG
10. LIG 转发用户通话流量，LEA 收集器汇总用户流量信息

用户下线时，软交换设备通知 LIG，LIG 删除 MSCG 上配置的监听目标，MSCG 停止流量监听。

9 NAT

关于本章

9.1 介绍（Introduction）

定义

NAT 是 Network Address Translation 的简称，即网络地址转换。

目的

NAT 是将 IP 数据报报头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问外部网络的功能。这种通过使用少量的公有 IP 地址映射多数的私有 IP 地址的方式，可以在一定程度上缓解 IP 地址空间枯竭的压力。

受益

运营商受益

NAT 给运营商带来以下收益：

- NAT 在一定程度上缓解了 IPV4 地址枯竭的压力，允许使用少量的共有 IP 地址为大量用户提供服务，保护现有投资。
- NAT 也能够保护用户信息不被泄露。

9.2 参考标准和协议

文档	描述	备注
RFC 1661	The IP Network Address Translator (NAT)	
RFC 2663	IP Network Address Translator (NAT) Terminology and Considerations	
RFC 2709	Security Model with Tunnel-mode IPsec for NAT Domains	
RFC 2766	Network Address Translation - Protocol Translation (NAT-PT)	
RFC 2993	Architectural Implications of NAT	
RFC 3022	Traditional IP Network Address Translator (Traditional NAT)	
RFC 3235	Network Address Translator (NAT)-Friendly Application Design Guidelines	
RFC 3489	STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)	
RFC 3519	Mobile IP Traversal of Network Address Translation (NAT) Devices	

文档	描述	备注
RFC 3715	IPsec-Network Address Translation (NAT) Compatibility Requirements	
RFC 3947	Negotiation of NAT-Traversal in the IKE	
RFC 4008	Definitions of Managed Objects for Network Address Translators (NAT)	

9.3 原理描述

9.3.1 NAT 的基本概念

如 RFC1631 所描述，NAT 是将 IP 数据报报头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问外部网络的功能。这种通过使用少量的公有 IP 地址映射多数的私有 IP 地址的方式，可以在一定程度上缓解 IP 地址空间枯竭的压力。

私有网络地址和公有网络地址

私有网络地址（以下简称私网地址）是指内部网络或主机的 IP 地址，公有网络地址（以下简称公网地址）是指在互联网上全球唯一的 IP 地址。IANA（Internet Assigned Number Authority）规定将下列的 IP 地址保留用作私网地址，不在 Internet 上被分配，可在任何单位或公司内部使用。

- A 类私有地址：10.0.0.0 ～ 10.255.255.255
- B 类私有地址：172.16.0.0 ～ 172.31.255.255
- C 类私有地址：192.168.0.0 ～ 192.168.255.255

各企业在预见未来内部主机和网络的数量后，选择合适的内部网络地址。不同企业的内部网络地址可以相同。如果一个公司选择上述三个范围之外的其它网段作为内部网络地址，则当与其他网络互通时有可能会造成混乱。

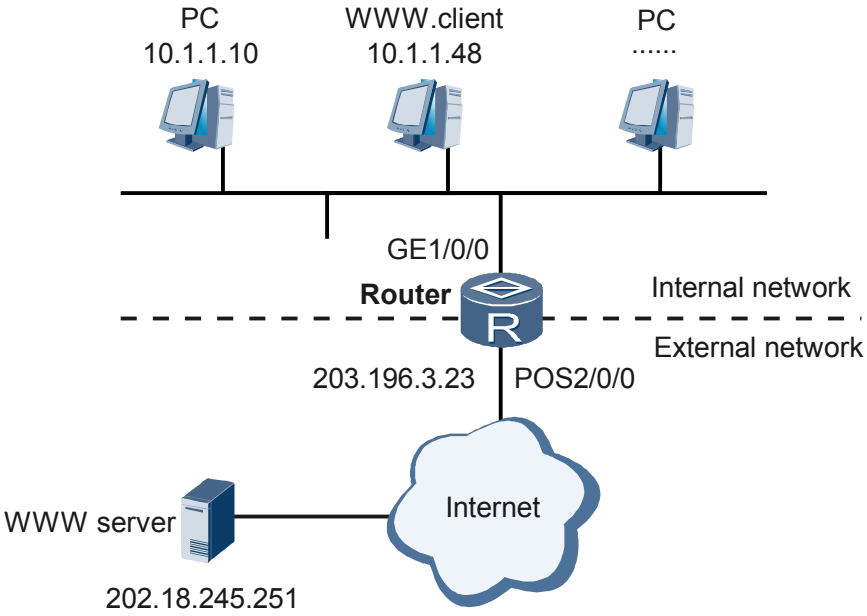
说明

上述三个范围内的地址不会在因特网上被分配，因而可以不必向 ISP 或注册中心申请而在公司或企业内部自由使用。

NAT 基本原理

如图 9-1 所示，当内部网络的主机访问互联网或与公有网络的主机通信时，需要进行网络地址转换。

图 9-1 NAT 示意图



内部网络的地址是 10.0.0.0 网段，而对外的公有网络 IP 地址是 203.196.3.23。内部的主机 10.1.1.48 以 WWW 方式访问外部网络的服务器 202.18.245.251。

主机 10.1.1.48 发出一个数据报文，选择一个源端口 6084，目的端口为 80。在通过 NAT 后，该报文的源地址和端口可能改为 203.196.3.23:32814，目的地址与端口不做改变。在路由器中维护着一张地址和端口对应表。

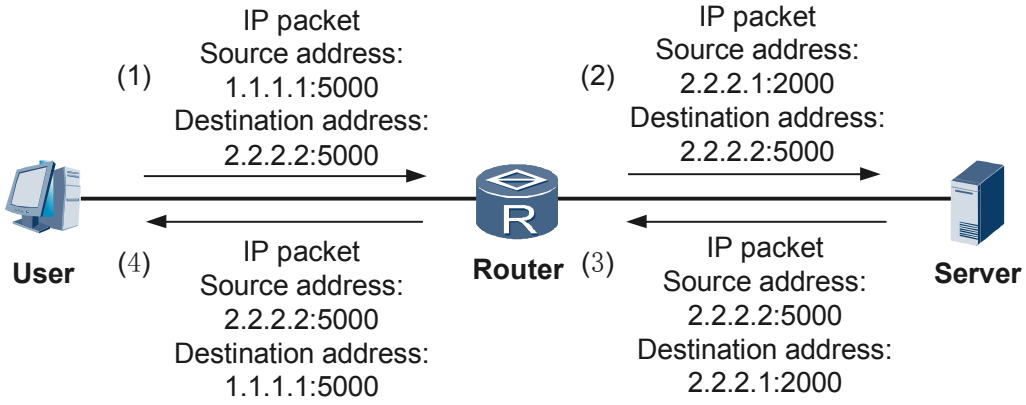
当外部网络的 WWW 服务器返回结果时，路由器会将结果数据报文中目的 IP 地址及端口转化为 10.1.1.48:6084。这样内部主机 10.1.1.48 就可以访问外部服务器了。

9.3.2 NAT 的转换机制

路由器中维护着一张地址端口对应表，所有经过路由器且需要进行地址转换的报文，都会通过这个对应表做相应的修改，进行<私有地址+端口>与<公有地址+端口>之间的转换。转换过程如下所示：

1. 内部网络主机向外发送报文时，路由器报文的源 IP 地址和端口替换为路由器的外部网络地址和端口。
2. 当外部的报文进入内部网络时，路由器会查找地址端口对应表，将报文的目的地址和端口进行转换，转换为真正的目的地址。

图 9-2 NAT 转换示意图



如图 9-2 所示。内部用户访问外部服务器的流程如下：

1. 用户向服务器发送源地址为 1.1.1.1：5000、目的地址为 2.2.2.2：5000 的报文。
2. 用户发至服务器的报文，在经过路由器的时候，经过地址转换，报文的源地址由 1.1.1.1：5000 改变为 2.2.2.1：2000。
3. 服务器收到用户的报文后，向用户回送报文，报文的源地址为 2.2.2.2：5000，目的地址为 2.2.2.1：2000。
4. 服务器发至用户的报文，在经过路由器的时候，经过地址转换，目的地址由 2.2.2.1：2000 改变为 1.1.1.1：5000。

上述的地址转换过程对终端（如图中的用户和服务器）来说是透明的。对外部服务器而言，它认为客户的 IP 地址就是 2.2.2.1，并不知道有 1.1.1.1 这个地址。因此，NAT“隐藏”了企业私有网络的拓扑。

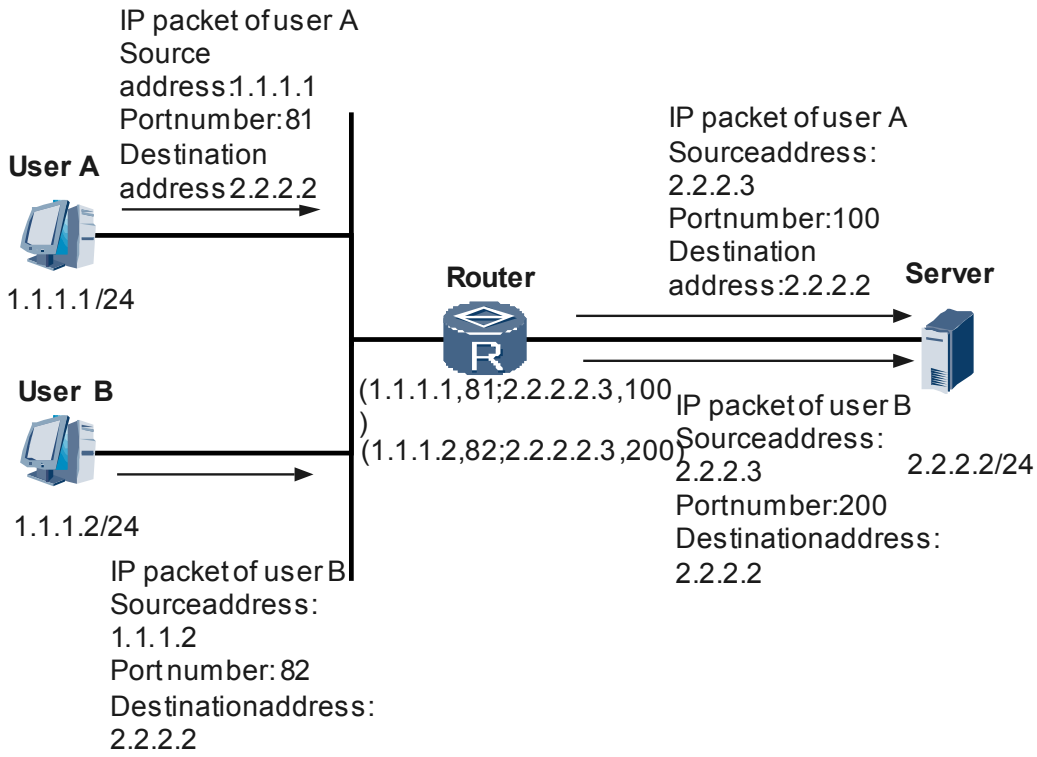
9.3.3 NAT 地址转换模式

内部网络的主机访问外部网络时，如内部网络的主机非常多、外部 IP 地址却只有一个，地址转换可能就会显得效率比较低。解决这个问题需要一个私有网络拥有多个外部地址，可以通过两种方式来实现多对多地址转换。

PAT 地址转换

该方式通过 IP 地址与端口号绑定的方式来实现一对多或多对多的地址转换。几个私网地址转换后可以对应同一个公网地址，但是端口号不同。在连接内部网络和外部网络的路由器上，存在一张内部网络和外部网络的（IP 地址，端口号）地址端口对应表。当主机从内部网络访问外部网络时，路由器 IP 地址和端口号分别进行转换。如图 9-3 所示。

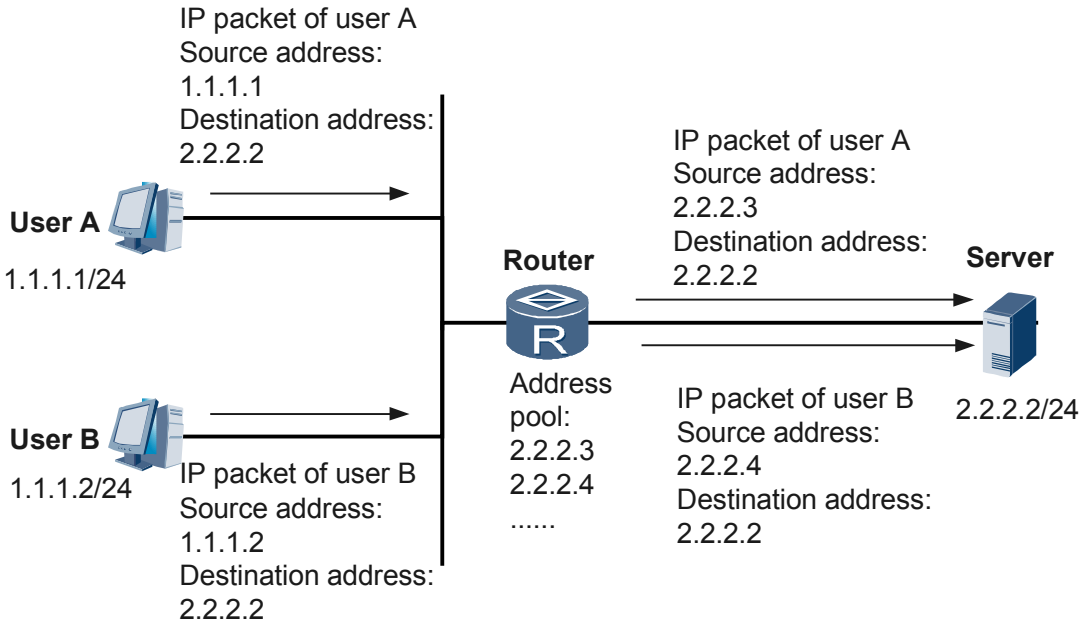
图 9-3 基于 NAT PAT 的地址转换



NoPAT 地址池转换

顾名思义，地址池就是一些合法 IP 地址（公有网络 IP 地址）的集合。用户可根据自己拥有的合法 IP 地址的多少、内部网络主机的多少、以及实际应用情况，配置合适的 IP 地址池。当主机从内部网络访问外部网络时，将会从地址池中挑选一个 IP 地址做为转换后的报文源地址。如图 9-4 所示。

图 9-4 NAT 利用地址池的多对多地址转换



说明

NAT 服务器拥有的公有 IP 地址数目要远少于内部网络的主机数目，因为所有内部主机并不会同时访问外部网络。公有 IP 地址数目的确定，应根据网络高峰期可能访问外部网络的内部主机数目的统计值来确定。

9.3.4 NAT 的种类

根据 NAT 的应用情况，主要有以下四种类型。

全圆锥形 NAT

私网主机向外部发起访问，相同的源地址和源端口的报文做 NAT 映射得到相同的外部网络地址和端口；任何外部主机可以通过访问映射后的外部网络地址和端口来访问内部地址和端口。

限制圆锥形 NAT

私网主机向外部发起访问，相同的源地址和源端口的报文做 NAT 映射得到相同的外部网络地址和端口；与全圆锥不同，只有与私网主机访问的目的地址相同的外部主机可以通过访问映射后的外部网络地址和端口来访问内部地址和端口。

限制端口圆锥形 NAT

私网主机向外部发起访问，相同的源地址和源端口的报文做 NAT 映射得到相同的外部网络地址和端口；与全圆锥不同，任何外部主机可以通过访问映射后的外部网络地址和端口来访问内部地址和端口，但外部主机发出的报文的源端口必须要与私网主机发起访问时的目的端口相同。

对称式 NAT

私网主机向外部发起访问，只有源地址、源端口、协议类型（TCP/UDP/ICMP）、目的地址和目的端口完全相同的 IP 报文做 NAT 才能映射到相同的外部网络地址和端口；只有目的地址与私网主机访问的目的地址相同的外部主机可以通过访问映射后的外部网络地址和端口来访问内部地址和端口，且外部主机发出的报文的源端口必须要与私网主机发起访问时的目的端口相同。

9.3.5 NAT 的优缺点

地址转换的优点如下：

- 使内部网络的大量主机可以使用少量公网 IP 地址就可以访问外部网络资源。
- 为内部主机提供了“隐私”（Privacy）保护。

地址转换的缺点如下：

- 由于 NAT 是对数据报文进行 IP 地址的转换，涉及 IP 地址的数据报的报头不能被加密。在应用层协议中，如果报文中有地址或端口需要转换，则报文不能被加密。例如，不能使用加密的 FTP 连接，否则 FTP 的 port 命令不能被正确转换。
- 网络调试变得更加困难。比如，某一台内部网络的主机试图攻击其它网络，则很难指出究竟是哪一台机器是恶意的，因为主机的 IP 地址被屏蔽了。

9.3.6 应用级网关 ALG

NAT 只能对 IP 地址和 TCP/UDP 头部的端口信息进行转换。对于一些特殊协议，例如 ICMP、FTP 等，它们报文的数据部分可能包含 IP 地址或端口信息。如果对这些报文进行地址转换，就会出现不一致的情况，导致错误。例如，一个使用内部 IP 地址的 FTP 服务器可能在和外部网络主机建立会话的过程中需要将自己的 IP 地址发送给对方。而这个地址信息是放到 IP 报文的数据部分，NAT 无法对它进行转换。外部网络主机接收了这个私有地址并使用它，这时 FTP 服务器将表现为不可达。

解决这些特殊协议的 NAT 转换问题的方法就是在 NAT 实现中使用应用级网关 ALG（Application Level Gateway）功能。ALG 是特定的应用协议的转换代理，它和 NAT 交互以建立状态，使用 NAT 的状态信息来改变封装在 IP 报文数据部分中的特定数据，并完成其他必需的工作以使应用协议可以跨越内外网运行。

例如，内网某主机的数据包 A 发送到外网后出现错误，外网返回一个“目的站点不可达”的 ICMP 报文，该报文数据部分包含了造成错误的数据报 A 的首部（注意，NAT 发送 A 之前进行了地址转换，所以源地址不是内部主机的真实地址）。如果开启了 ICMP ALG 功能，在 NAT 转发 ICMP 报文之前，它将与 NAT 交互，打开 ICMP 报文并转换其数据部分的报文 A 首部的地址，使这些地址表现为内部主机的确切地址形式，并完成其他一些必需工作后，由 NAT 将这个 ICMP 报文转发给内部主机。

9.3.7 NAT 在设备上的实现

利用访问控制列表控制地址转换

在实际应用中，我们可能希望某些内部的主机具有访问 Internet（外部网络）的权利，而某些主机不允许访问。

利用访问控制列表，可以控制地址转换的使用范围。只有满足访问控制列表条件的数据报文才可以进行地址转换，这样就能够使内部网络的特定主机能够有权访问 Internet。

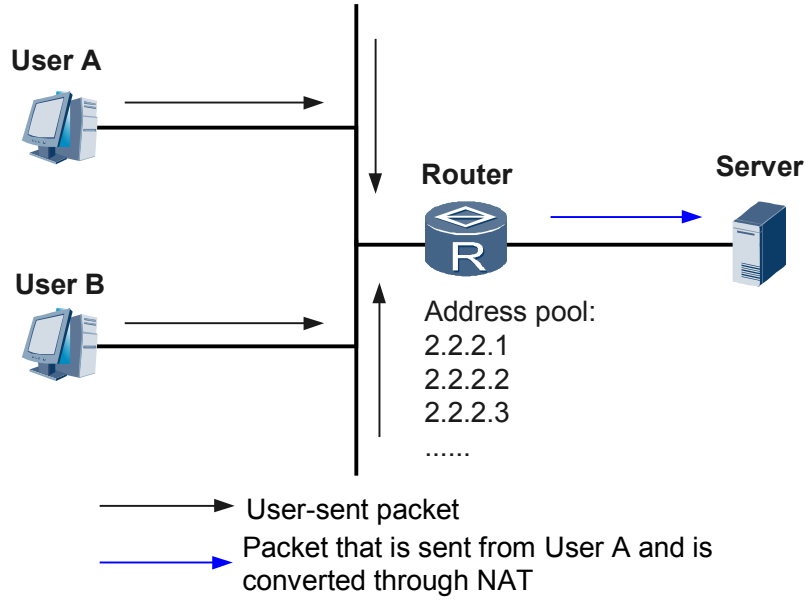
访问控制列表是由命令 **acl** 生成的，它依据数据包的 IP 头及其承载的上层协议数据包头的格式定义了一定的规则，表示允许或是禁止具有某些特征的数据包。地址转换按照这样的规则判定哪些包是被允许转换或者是被禁止转换，这样可以禁止一些内部的主机访问外部网络，保证具有一定特征的数据包才可以被允许进行地址转换，提高网络的安全性。

“转换关联”就是将一个地址池和一个访问控制列表关联起来，这种关联指定了“具有某些特征的 IP 报文”才可以使用“这样的地址池中的地址”。当内部网络有数据包要发往外部网络时，首先根据访问列表判定是否是允许的数据包，然后根据转换关联找到与之对应的地址池，这样就把源地址转换成这个地址池中的某一个地址，完成了地址转换。

设备在处理报文时，如果发现该报文是需要从内网发往外网的数据，并且允许进行地址转换，根据“转换关联”可以利用地址池将内部网络主机的 IP 地址和端口替换为路由器的外部网络地址和端口。对于外网需要发往内网的数据，通过查找地址端口对应表，把路由器外部网络地址和端口转换为内部网络主机的 IP 地址和端口。

如图 9-5 所示。路由器配置了外部地址池，池中的地址有 2.2.2.1、2.2.2.2 等。同时，路由器上也配置了 ACL 规则，允许用户 A 的报文通过，并进行地址转换，不允许 B 的报文进行地址转换，即对于 B 的报文不予处理。这样，就使得用户 B 不能访问网络。

图 9-5 多对多地址转换及地址池

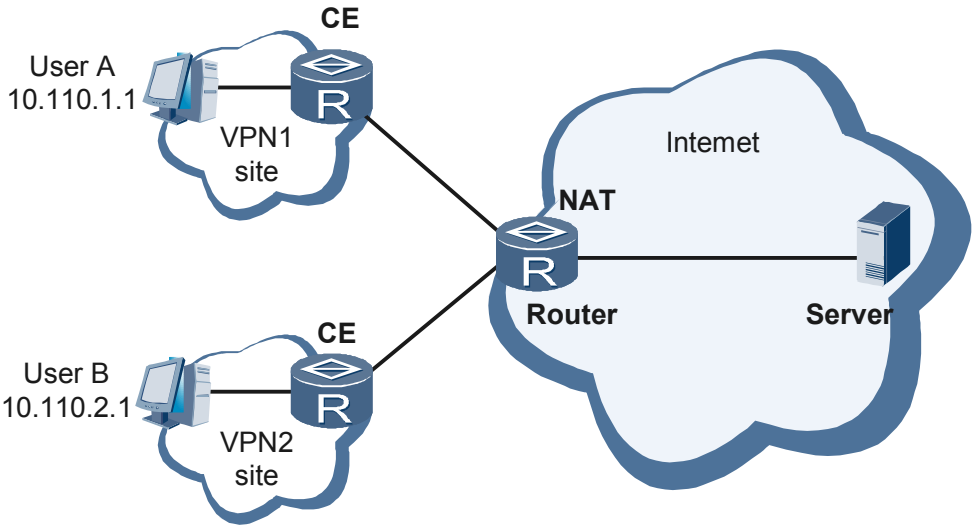


支持 VPN

NAT 不仅可以使内部网络的用户访问外部网络，还允许分属于不同 VPN（Virtual Private Network）的用户通过同一个出口访问外部网络。

当 VPN 用户访问 Internet 时，NAT 将内部网络主机的 IP 地址和端口替换为路由器的外部网络地址和端口，同时还记录了用户的 VPN 信息。报文还原时，NAT 将外部网络地址和端口还原为内部网络主机的 IP 地址和端口，同时获得了 VPN 用户信息。如图 9-6 所示。

图 9-6 地址转换支持 VPN



内部服务器

地址转换具有“屏蔽”内部主机的作用，但是在实际应用中，可能我们需要提供给外部一个访问内部服务器的机会，如提供给外部一个 WWW 服务器，或是一台 FTP 服务器。

使用地址转换可以灵活地添加内部服务器，例如可以使用 202.110.10.10 作为 WEB 服务器的外部地址，使用 202.110.10.11 作为 FTP 服务器的外部地址，甚至还可以使用 202.110.10.12:8080 这样的地址作为 WEB 服务器的外部地址，还可为外部用户提供多台同样的服务器，如提供多台 WEB 服务器。

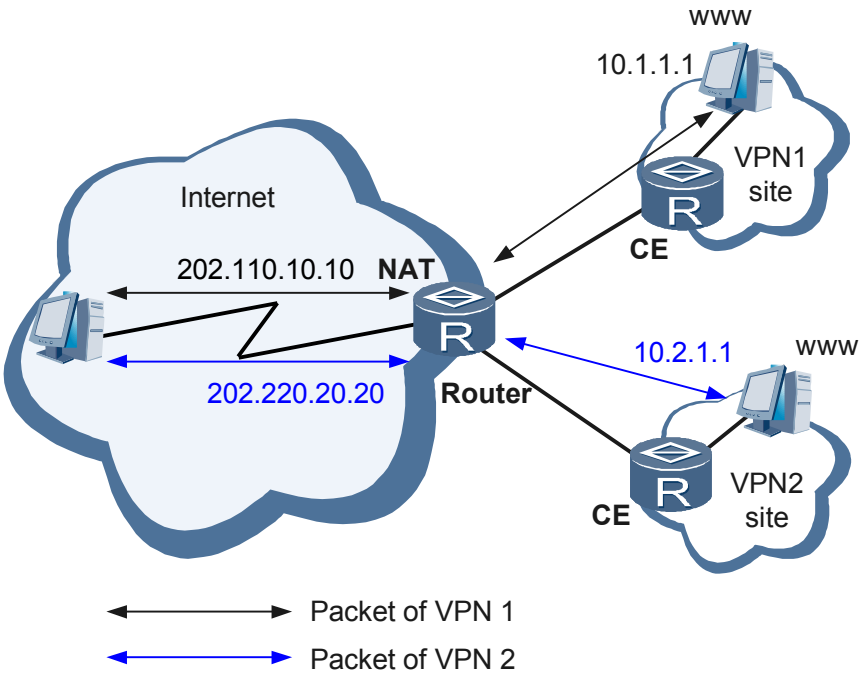
通过配置内部服务器，可将相应的外部地址、端口等映射到内部的服务器上，提供了外部网络主机访问内部服务器的功能。

在外部网络主机访问内部服务器时，根据用户的配置查找外部数据包的目的地址，如果要访问的是内部服务器，则转换成相应的内部服务器的私有地址和端口，达到访问内部服务器的目的；在内部服务器向外部网络主机发送报文时，对源地址进行查找，判断是否是从内部服务器发出去的报文，如果是则将源地址转换成相应的外部地址。

内部服务器的多实例

NAT 支持内部服务器的多实例，提供给外部访问 MPLS VPN 内主机的机会。例如，VPN1 内提供 WWW 服务的主机地址是 10.1.1.1，VPN2 内提供 WWW 服务的主机地址是 10.2.1.1；使用 202.110.10.10 做为 VPN1 的 WEB 服务器外部地址，使用 202.110.20.20 做为 VPN2 的 WEB 服务器外部地址。这样，Internet 的用户使用 202.110.10.10 就可以访问 VPN1 提供的 WWW 服务，使用 202.110.20.20 就可以访问 VPN2 提供的 WWW 服务。如图 9-7 所示。

图 9-7 内部服务器的多实例



说明

设备支持地址重叠的 MPLS VPN 用户访问同一个公网。

端口映射

应用层协议通常使用知名端口号进行通信。端口映射允许用户对不同的应用层协议定义一组新的端口号，还可以指定使用非知名端口的主机范围。

端口映射只有和 NAT 等针对业务敏感的特性联合使用的时候才具有实际意义。

例如在一个企业私网中，内部 FTP 服务器 10.10.10.10 通过 2121 端口提供 FTP 服务。用户通过支持 NAT 业务的 NE20E-X6 访问 FTP 服务器时，只能使用 2121 做为端口号。由于默认情况下 FTP 报文的端口号是 21，这时 FTP 服务器无法将 2121 端口的报文识别为 FTP 应用。此时就需要支持 NAT 业务的 NE20E-X6 通过端口映射功能将 2121 端口的报文识别为 FTP 协议报文转发给 FTP 服务器，实现用户对 FTP 服务器的访问。

目的地址转换

目的地址转换功能，可以用来匹配地址转换业务的流量策略的报文将根据策略内容做目的地址替换。

购买地址转换业务的运营商通过一个特定的用户域上线，这些用户的报文通过匹配 ACL 选择特定的服务器的 IP 地址替换其 IP 报文头中的目的地址。

IP 连接数限制

基于 IP 地址的连接数限制，用于统计和监控安全区域中单个 IP 地址所建立的 TCP/UDP 连接。通过分析源 IP 地址发起或目的地址接收的 TCP 或 UDP 连接总数是否超过设定的

阈值，可以确定是否需要限制该方向的新的连接的发起，以防止系统受到恶意的攻击或因系统太忙而发生拒绝服务的情况。

当 TCP/UDP 连接数降至阈值以下后，源 IP 地址或目的地址可以重新发起或者接受 TCP 或 UDP 连接。

NAT 会话表项老化时间的调整

NAT 功能可以支持不同协议的会话表老化时间可配置。通过调整各个协议的 NAT 会话表项的老化时间，可以使过期的 NAT 会话表项尽快老化，释放系统资源。

9.3.8 NAT 日志简介

NAT 日志的作用

对于通过 NAT 设备接入的用户，由于源 IP 地址经过地址转换，难以精确定位某次访问网络的操作是从哪台主机、哪个用户发起的，这使得网络的安全性降低。

NAT 日志（UserLog）就是为了解决这一安全问题而实现的。它可以记录 NAT 数据流信息，从而使管理员能够了解 NAT 转换前的地址信息，进而查询、跟踪网络活动和操作，提高网络的可用性和安全性。

NAT 日志功能只用于 NAT 的出方向，不记录外部用户对内部服务器的访问。

NAT 日志的实现

对于通过 NAT 访问 Internet 的私网用户，NAT 日志信息通过以下步骤输出：

- 路由器按照 IP 报文的源 IP 地址、源端口、目的 IP 地址、转换后的源 IP 地址、转换后的源端口、协议号来对 IP 报文进行分类；
- 每一类 IP 报文作为一条 NAT 流，缓存在 NAT 的会话表中；
- 当会话表中的流老化时，将会话表表中的流按特定格式封装 UDP 报文发送到指定的日志主机。

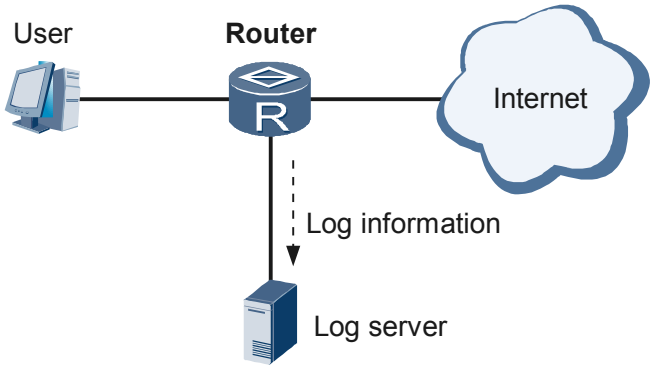
NAT 日志的输出

日志采用 UDP 报文方式输出。

如图 9-8 所示，系统统计每一条老化的流，当统计到一定数量后，将统计信息生成一条 UDP 报文发送出去，供网上的日志服务器接收处理。

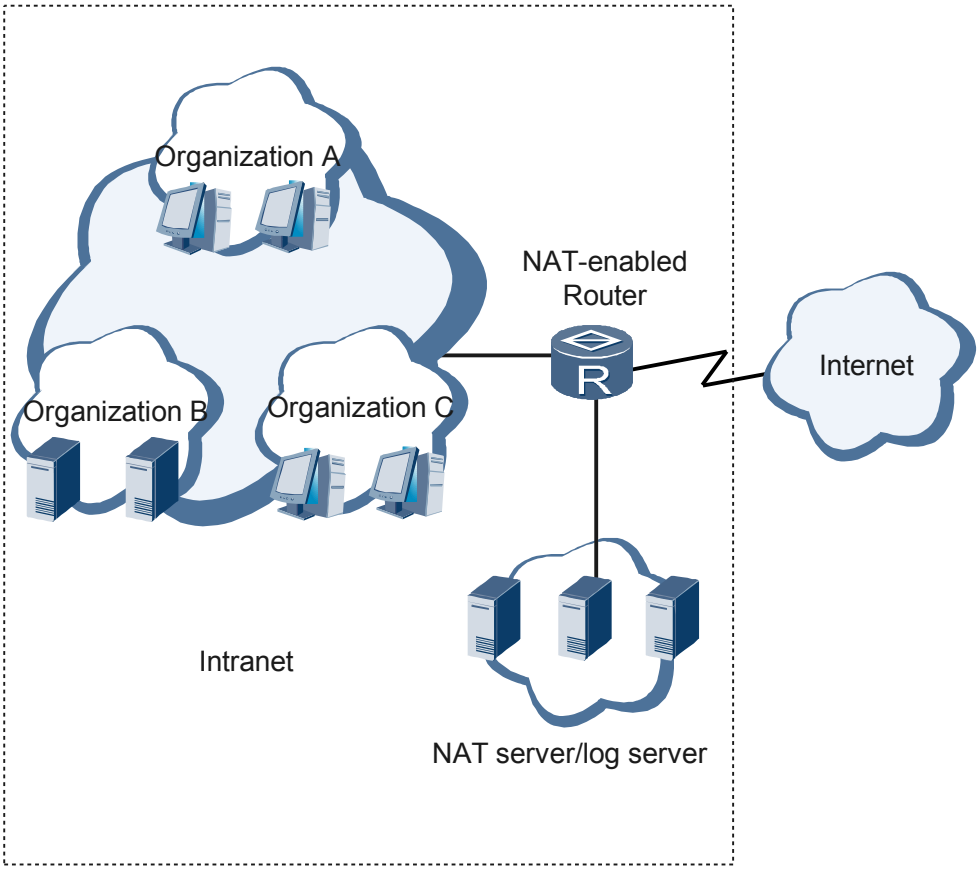
UDP 报文中包含多条 NAT 数据流的原始信息，由一个报文头和若干条记录组成，每条记录分别对应一条被记录的数据流。

图 9-8 日志信息输出示意图



9.4 应用

图 9-9 NAT 的应用



如图 9-9 所示，企业网络在出口处配置 NAT，可以使整个企业只用少量的公网 IP 就可以访问 Internet。内部网络访问外部网络的日志会被路由器发送到日志服务器。

9.5 术语与缩略语

缩略语

缩略语	英文全称	中文全称
NAT	Network Address Translation	网络地址转换
PAT	Port Address Translation	端口地址转换
VPN	Virtual Privaty Network	虚拟专用网络