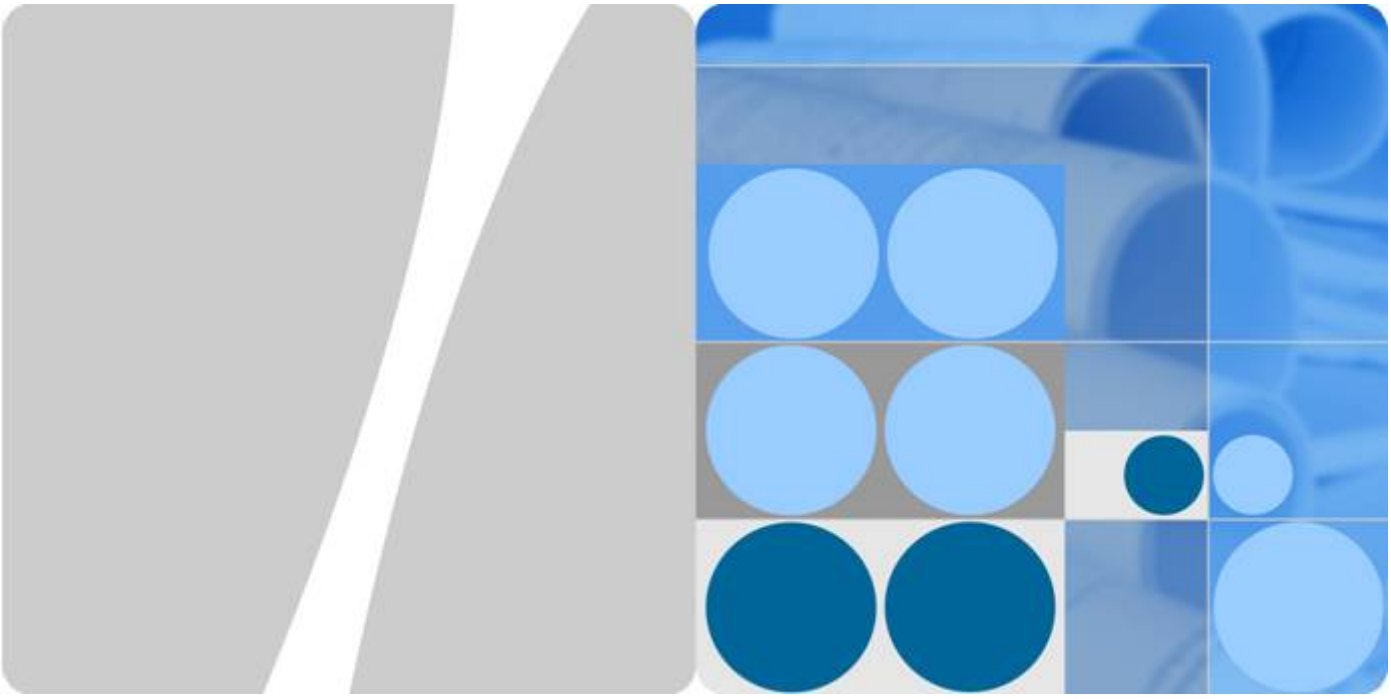


Huawei AR200-S 系列企业路由器

V200R002C00

特性描述-安全

文档版本　01

发布日期　2011-12-30

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： 4008302118

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。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1 ～ n 次。
#	由“#”开始的行表示为注释行。

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 (2011-12-30)

第一次正式发布。

目 录

1 ACL

关于本章

1.1 介绍

定义

访问控制列表 ACL（Access Control List）是由 **permit** 或 **deny** 语句组成的一系列有顺序的规则集合，这些规则根据数据包的源地址、目的地址、源端口、目的端口等信息来描述。ACL 规则通过匹配报文中的信息对数据包进行分类，路由设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

例如可以用 ACL 拒绝任何用户终端使用 Telnet 登录本机，或者允许每个用户终端经由 SMTP（Simple Mail Transfer Protocol）向本机发送电子邮件。

根据不同的划分规则，ACL 可以有不同的类型，如表 1-1 所示。

表 1-1 ACL 分类

划分规则	分类	应用场景	说明
按照命名方式	数字 ACL	传统的 ACL 标识方法，用户创建 ACL 时，指定一个唯一的数字标识，后续的操作可以通过这个唯一的数字标识对 ACL 进行相关的操作。	-
	名字 ACL	用户在创建 ACL 时，可以为 ACL 指定一个名称。后续的操作可以通过这个唯一的名称确定一个 ACL，从而对其进行相关操作。	名称相对于数字来说具有更为直观的标识和记忆的效果，AR200-S 提供了灵活的 ACL 命名方式。 在指定名字 ACL 的同时，也可以同时配置数字标识。如果没有配置数字标识，系统在记录此名字 ACL 会分配一个数字标识给该名字 ACL。 ACL 名称需要全局唯一，互不影响。
按照 ACL 规则的功能	基本 ACL	仅使用报文的源 IP 地址、分片标记和时间段信息来定义规则。	编号范围为 2000 ～ 2999。

划分规则	分类	应用场景	说明
	高级 ACL	既可使用报文的源 IP 地址，也可使用目的地址、IP 优先级、ToS、DSCP、IP 协议类型、ICMP 类型、TCP 源端口/目的端口、UDP 源端口/目的端口号等信息来定义规则。 高级访问控制列表可以定义比基本访问控制列表更准确、更丰富、更灵活的规则。	编号范围为 3000 ～ 3999。
	以太网帧头 ACL	可根据报文的以太网帧头信息来定义规则，如根据源 MAC 地址、目的 MAC 地址、以太帧协议类型等。	编号范围为 4000 ～ 4999。

目的

ACL 是指通过配置的一系列匹配规则对特定的数据包进行过滤，从而识别需要过滤的对象。在识别出特定的对象之后，根据预先设定的策略允许或禁止相应的数据包通过。

AR200-S 通过配置一系列的规则来过滤数据包，这些规则就是通过访问控制列表 ACL 定义的。

ACL 可以作为基础配置被功能模块引用，比如被策略路由、路由过滤、QoS、设备安全、防火墙、IPSec 等功能模块引用。

1.2 参考标准和协议

与 ACL 特性相关的参考标准及协议如下：

文档	描述	备注
RFC 4314	Defines several new access control rights and clarifies which rights are required for different IMAP (Internet Message Access Protocol) commands.	-

1.3 可获得性

涉及网元

无需其他网元的配合。

License 支持

无需获得 License 许可，即可获得该特性的服务。

版本支持

产品	最低支持版本
AR200-S	V200R002C00

特性依赖

不依赖其他特性。

硬件要求

ACL 的查找性能和规则空间与设备的硬件性能有关。

1.4 原理描述

1.4.1 ACL 的基本原理

ACL 负责管理用户配置的所有规则，并提供规则匹配算法。业务根据匹配的规则动作（“允许”或“拒绝”）进行操作。

ACL 的规则管理

每个 ACL 作为一个规则组，可以包含多个规则。规则通过规则 ID 来标识，规则 ID 可以由用户进行配置，也可以由系统自动根据步长生成。一个 ACL 中所有规则均按照规则 ID 从小到大排序。

规则 ID 之间会留下一定的间隔。如果不指定规则 ID 时，具体间隔大小由“ACL 的步长”来设定。例如步长设定为 5，ACL 规则 ID 分配是按照 5、10、15……来分配的。如果步长值是 2，自动生成的规则 ID 从 2 开始。用户可以根据规则 ID 方便地把新规则插入到规则组的某一位置。

ACL 的规则匹配

报文到达设备时，查找引擎从报文中取出信息组成查找键值，键值与规则组中的规则进行匹配，只要有一条规则和报文匹配，就停止查找，称为命中规则，然后根据规则的动作进行处理，“允许”则继续转发报文，“拒绝”则丢弃报文。

查找完所有规则，如果没有符合条件的规则，称为未命中规则，不对报文作任何处理。

1.4.2 ACL 的匹配顺序

一个 ACL 可以由多条“**deny** | **permit**”语句组成，每一条语句描述一条规则，这些规则可能存在重复或矛盾的地方（一条规则可以包含另一条规则，但两条规则不可能完全相同）。

AR200-S 支持两种匹配顺序，即配置顺序（**config**）和自动排序（**auto**）。当将一个数据包和访问控制列表的规则进行匹配的时候，由规则的匹配顺序决定规则的优先级，ACL 通过设置规则的优先级来处理规则之间重复或矛盾的情形。

配置顺序

配置顺序按照用户配置 ACL 规则的先后进行匹配，先配置的规则先匹配。缺省情况下匹配顺序为按用户的配置排序。

自动排序

自动排序（**auto**）使用“深度优先”的原则进行匹配。

“深度优先”根据 ACL 规则的精确度排序，如果匹配条件（如协议类型、源和目的 IP 地址范围等）限制越严格，规则就越先匹配。

比如 129.102.1.1 0.0.0.0 指定了一台主机：129.102.1.1，而 129.102.1.1 0.0.0.255 则指定了一个网段：129.102.1.1 ～ 129.102.1.255，显然前者指定的主机范围小，在访问控制规则中排在前面。具体标准如下。

- 基本 IPv4 ACL 的“深度优先”顺序判断原则如下：
  1. 先看规则中是否带 VPN 实例，带 VPN 实例的规则优先。
  2. 再比较源 IP 地址范围，源 IP 地址范围小（即通配符掩码中“0”位的数量多）的规则优先。
  3. 如果源 IP 地址范围相同，则先配置的规则优先。

  说明

  通配符掩码又称反向掩码，以点分十进制表示。譬如，C 类子网 192.168.1.0 对应的子网掩码为 255.255.255.0，而通配符掩码则为 0.0.0.255。
- 高级 IPv4 ACL 的“深度优先”顺序判断原则如下：
  1. 先看规则中是否带 VPN 实例，带 VPN 实例的规则优先。
  2. 再比较协议范围，指定了 IP 协议承载的协议类型的规则优先。
  3. 如果协议范围相同，则比较源 IP 地址范围，源 IP 地址范围小（即通配符掩码中“0”位的数量多）的规则优先。
  4. 如果协议范围、源 IP 地址范围相同，则比较目的 IP 地址范围，目的 IP 地址范围小（即通配符掩码中“0”位的数量多）的规则优先。
  5. 如果协议范围、源 IP 地址范围、目的 IP 地址范围相同，则比较四层端口号（TCP/UDP 端口号）范围，四层端口号范围小的规则优先。
  6. 如果上述范围都相同，则先配置的规则优先。
- 二层 ACL 的“深度优先”顺序判断原则如下：
  1. 先比较源 MAC 地址范围，源 MAC 地址范围小（即掩码中“1”位的数量多）的规则优先。
  2. 如果源 MAC 地址范围相同，则比较目的 MAC 地址范围，目的 MAC 地址范围小（即掩码中“1”位的数量多）的规则优先。
  3. 如果源 MAC 地址范围、目的 MAC 地址范围相同，则先配置的规则优先。

1.4.3 ACL 的步长设定

设置规则组的步长

通过命令 **step**，可以为一个 ACL 规则组指定“步长”，步长的含义是：自动为 ACL 规则分配编号时，规则编号之间的差值。例如，如果步长设定为 5，规则编号分配是按照 5、10、15…这样的规则分配的。缺省情况下，ACL 规则组的步长为 5。

当步长改变的时候，ACL 规则组下的规则编号会自动重新排列。例如，本来规则编号为：5、10、15、20，如果通过命令 **step 2**，把步长设定改为 2，则规则编号变成：2、4、6、8。

如果本来规则编号不均匀分布，执行 **step** 命令后，规则会变为均匀分布。例如，如果当前步长为 5，规则编号为：1、3、10、12，通过命令 **step 2**，把步长设定为 2，则规则编号自动变成：2、4、6、8。

说明

如果当前步长为 2，规则编号为：1、3、10、12，通过命令 **step 2** 规则编号不发生变化，仍然是：1、3、10、12。如果需要将该规则编号变为：2、4、6、8，可以先执行 **undo step** 命令将规则编号变成：5、10、15、20，再执行 **step 2** 命令，将规则编号变成：2、4、6、8。

恢复步长的缺省值

通过 **undo step** 命令，可以把步长恢复为缺省设定，同时对规则编号进行重新排列。

undo step 命令可以立刻按照缺省步长调整 ACL 规则的编号。例如：ACL 规则组 1，下面有 4 条规则：编号为 1、3、5、7，步长为 2。如果此时使用 **undo step** 命令，则 ACL 规则编号变成：5、10、15、20，步长为 5。

使用步长的作用

通过设置步长，使规则之间留有一定的空间，用户可以在规则之间插入新的规则，以控制规则的匹配顺序。

1.4.4 ACL 对分片报文的支持

传统的包过滤并不处理所有 IP 报文分片，而是只对第一个（首片）分片报文进行匹配处理，后续分片一律放行。这样，网络攻击者可能构造后续的分片报文进行流量攻击，带来安全隐患。

AR200-S 的包过滤提供了对分片报文过滤的功能，包括对所有分片报文进行三层（IP 层）匹配过滤。

在 ACL 规则中，通过参数 fragment 来标识该 ACL 规则对所有分片报文有效，而对非分片报文则忽略此规则；通过参数 none-first-fragment 来标识该规则仅对非首片分片报文有效，而对非分片报文和首片分片报文则忽略此规则。不包含参数 fragment 或 none-first-fragment 的配置规则项对所有报文均有效。

1.4.5 ACL 生效时间段

时间段用于描述一个特殊的时间范围。用户可能有这样的需求，即一些 ACL 规则需要在某个或某些特定时间内生效，而在其他时间段则不生效。例如某单位严禁员工上班时间浏览非工作网站，而下班后则允许通过指定设备浏览娱乐网站，则可以对 ACL 规则约定生效时间段。这时，用户就可以先配置一个或多个时间段，然后通过执行 **rule** 命令引用该时间段，从而实现基于时间段的 ACL 过滤。

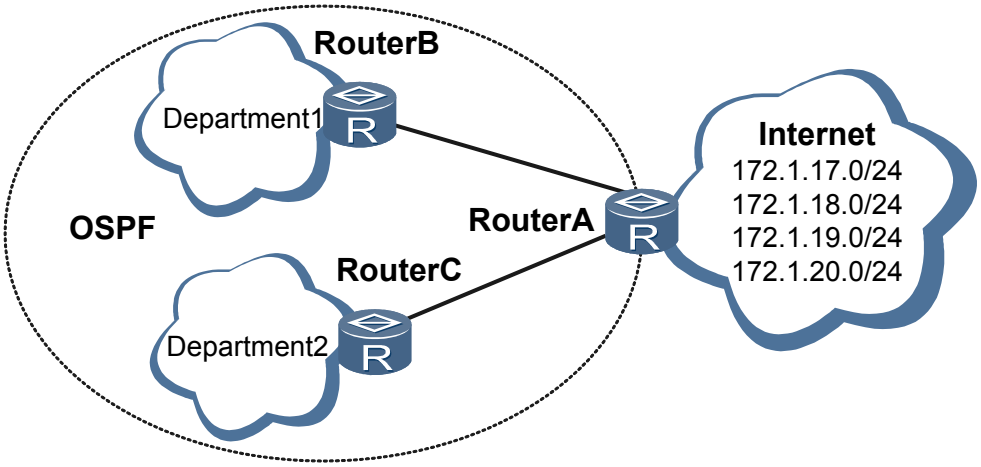
1.5 应用

1.5.1 在路由中使用 ACL 过滤路由信息

ACL 可以应用在各种动态路由协议中，对路由协议发布和接收的路由信息进行过滤。

企业网用户可以通过与 Internet 相连的 AR200-S 访问 Internet 网络。部分用户（如研发部门的员工）需要限制其向外网访问的权限，而有些服务器（如工资查询服务器）不接受来自外网用户的访问，保证本身的信息安全。基于以上所述的企业网的特殊要求，可以在与 Internet 相连的 AR200-S 的出入方向定义 ACL 规则，用来过滤不同路由的报文。

图 1-1 在路由过滤中使用 ACL



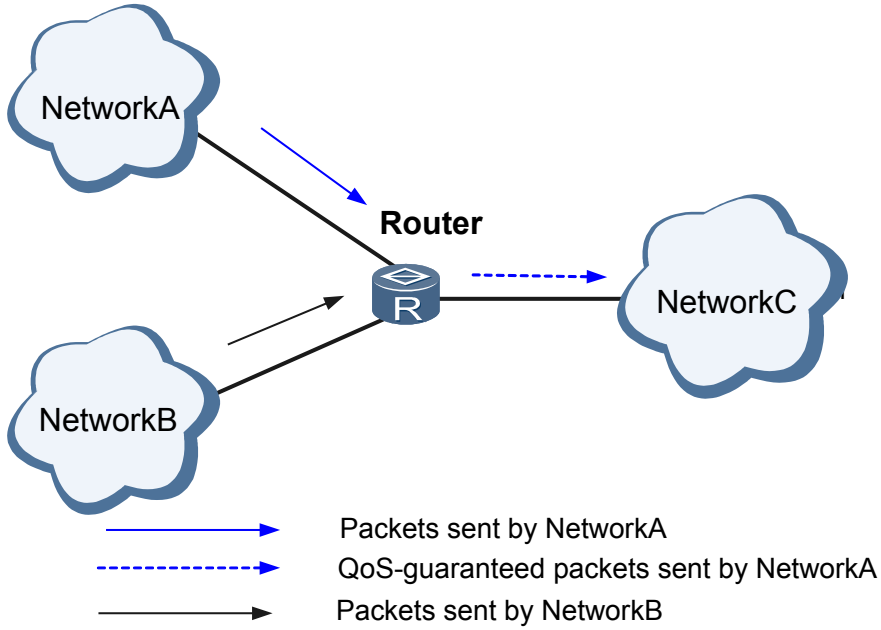
如图 1-1 所示，在运行 OSPF 协议的网络中，RouterA 作为内外网的连接路由器，在 RouterA 上定义 ACL 列表，并在 OSPF 协议中应用 ACL 过滤，可控制路由的发布和接收，如：

- RouterA 仅提供 172.1.17.0/24、172.1.18.0/24 和 172.1.19.0/24 给 RouterB。
- RouterC 仅接收路由 172.1.18.0/24。

1.5.2 在 QoS 中使用 ACL 进行流分类

如图 1-2 所示，NetworkA、NetworkB 通过 Router 访问 NetworkC，NetworkA、NetworkB 对语音、视频、数据有不同的访问需求。如 NetworkA 对视频的访问需求比较强烈，为了保证 NetworkA 的访问质量，可以在 Router 上使用 ACL，然后在 QoS 策略中引用这个 ACL，这样，所有来自 NetworkA 的报文都会被 Router 进行 QoS 处理后转发，以保证质量。而来自其它网络的所有报文，因为没有匹配 ACL 而正常的转发，没有 QoS 的保障。

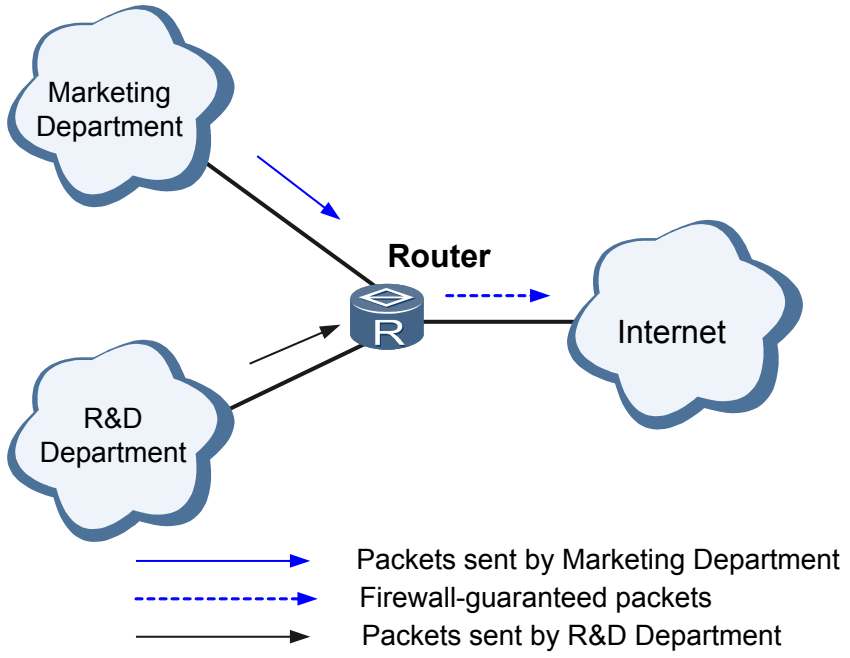
图 1-2 在 QoS 中使用 ACL



1.5.3 在防火墙中使用 ACL

在企业网中，不同的部门对外访问 Internet 的权限和安全措施需求不一样，因此所采取的防火墙策略是不一样的，在防火墙中使用 ACL，可以将 ACL 中过滤出的报文进行一系列的安全处理。

图 1-3 在防火墙中使用 ACL

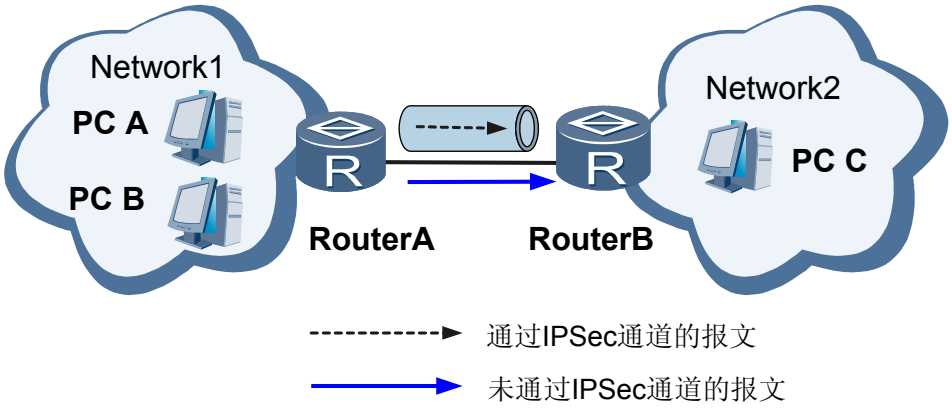


如图 1-3 所示，某企业的两个部门市场部和研发部，如果要求市场部的员工可以访问 Internet 网络并且具有一定的安全保证，研发部的员工不能访问 Internet 网络，在 Router 上部署ACL 并配置防火墙，就可以达到这个要求。

1.5.4 在 IPSec 中使用 ACL

在 IP 网络中，对等体间通过 IPSec、加密与数据源认证等方式，来保证数据报在网络上传输时的私有性、完整性和真实性。这个安全通道往往是在链接两个网络的两台设备上建立的，而局域网内部的用户由于安全性要求不一样，有些需要安全保护，有些不需要，也就是对于 IPSec 的需求是有差异的。这时在局域网的出口设备配置 ACL，过滤需要进入 IPSec 通道的报文，ACL 允许（perimt）的报文将被保护，ACL 拒绝（deny）的报文将不被保护。

图 1-4 在 IPSec 中使用 ACL



如图 1-4 所示，RouterA 和 RouterB 之间建立了 IPSec 通道。在 RouterA 上使用 ACL，Permit 来自 PC A 的所有报文，然后在 IPSec 策略中引用这个 ACL，这样，所有来自 PC A 的报文都会被 RouterA 加密后转发，而来自 PC B 的所有报文，因为没有匹配 ACL 而正常的转发。

1.6 术语与缩略语

术语

术语	解释
基本 ACL	基本访问控制列表使用源 IP 地址、分片标记和时间段等信息作为定义访问控制列表规则的元素。
高级 ACL	高级访问控制列表可以使用数据包的源地址信息、目的地址信息、IP 承载的协议类型、针对协议的特性，例如 TCP 的源端口、目的端口，ICMP 协议的类型、code 等内容定义规则。
以太网帧头 ACL	基于二层的访问控制列表，是一种特殊的访问控制列表，可以根据接收报文的以太网帧头信息定义规则。

缩略语

缩略语	英文全称	中文全称
ACL	Access Control List	访问控制列表

2 流量抑制

关于本章

2.1 介绍

定义

AR200-S 的接口支持对本接口接收的广播报文、组播报文和未知单播报文的最大流量进行限制。当上述任意一种报文的最大流量超过配置的阈值时，系统将丢弃超过阈值的该种报文，使该种报文的流量降低到阈值之内，从而保证网络业务的正常运行。

目的

当 AR200-S 的某个二层以太接口接收到广播报文、组播报文或未知单播报文时，会在同一个 VLAN 内的其他的二层以太接口转发这些报文，如果该类报文过多，会占用大量宝贵的接口带宽资源，并且影响 AR200-S 的安全性能，因此需要对该类报文的流量进行抑制，最大限度的保证通过 AR200-S 二层以太接口的该类报文的流量控制在一定的阈值之内。

受益

企业受益

- 通过流量控制，减少广播风暴，保证 AR200-S 的转发性能。

2.2 参考标准和协议

文档编号	描述
IEEE 802.1d	Media Access Control (MAC) Bridges Specifies an architecture and protocol for the interconnection of IEEE802 LANs below the MAC service boundary.

2.3 可获得性

涉及网元

无需其他网元的配合。

License 支持

无需获得 License 许可，即可获得该特性的服务。

版本支持

表 2-1 版本支持

产品	最低支持版本
AR200-S	V200R002C00

特性依赖

不依赖其他特性。

硬件要求

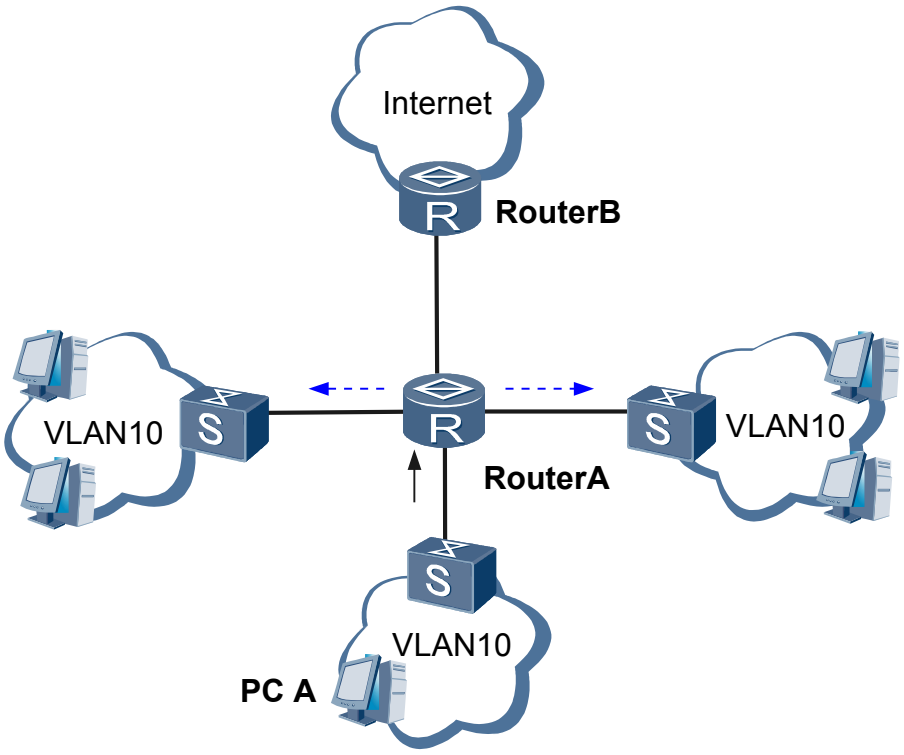
二层接口支持以太接口，三层接口不支持。

2.4 原理描述

当 AR200-S 的某个二层以太接口接收到广播报文、组播报文或未知单播报文时，会在同一个 VLAN 内的其他的二层以太接口转发这些报文。通过在接口上配置流量抑制功能，可以将广播报文、组播报文或未知单播报文的流量限制在一定范围之内，从而保证网络业务的正常运行。

如图 2-1 所示，RouterA 的有 3 个二层以太接口加入 VLAN10，当 PC A 发送大量广播报文，广播报文将在其他加入 VLAN10 的二层以太接口转发，在整个 VLAN 内形成广播风暴，从而占用大量宝贵的带宽资源。可以在连接 PC A 的二层以太接口上配置流量抑制功能，对该接口接收的广播报文的流量进行抑制。

图 2-1 流量抑制组网图

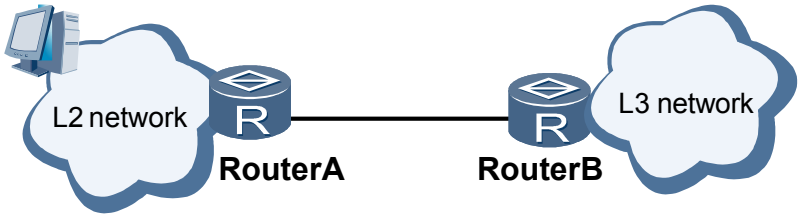


缺省情况下，接口对广播、组播和未知单播流量不做限制。

2.5 应用

如图 2-2 所示，RouterA 作为二层网络到三层路由器 RouterB 的衔接点，当需要限制二层网络转发的来自用户的广播、组播或者未知单播报文时，可以通过在 RouterA 的二层以太接口上配置流量抑制功能来实现。

图 2-2 配置流量抑制组网图



2.6 术语与缩略语

术语

无

缩略语

无

3 本机防攻击

关于本章

3.1 介绍

定义

本机防攻击包括 CPU 防攻击、攻击溯源和应用层联动。

AR200-S 的本机防攻击特性针对的对象是上送 CPU 的报文，主要用于保护路由设备自身安全，使设备在受到攻击时保证已有业务可以正常运转。

CPU 防攻击包括以下特性：

- CAR 系列特性

  CAR 系列特性主要包括黑名单、CPCAR、Deny 以及统一限速等功能。其中，黑名单指非法用户的集合，通过 ACL 把符合特定特征的用户纳入到黑名单中，被纳入黑名单的用户所发的报文到达 AR200-S 后均会被丢弃；CPCAR 按照协议类型对报文做 CAR 值限速；Deny 直接丢弃某种协议类型的报文；统一限速是指对上送 CPU 的报文统一限速，保证整体上送 CPU 的报文不会过多，保护 CPU 安全。

- 动态链路保护特性

  AR200-S 通过动态链路保护特性保护基于会话的应用层数据，如 FTP Session 数据和 BGP Session 数据。动态链路保护特性保证已有业务受到攻击时能够正常运行。

  当 AR200-S 检测到 FTP Session 或 BGP Session 建立时，会启动对此 Session 的动态链路保护功能，后续上送报文如匹配此 Session 特征信息，此类数据将会享受高速率上送的权利，由此保证了此 Session 相关业务的运行可靠性、稳定性。

攻击溯源

攻击溯源基于流量分析和统计，自动识别攻击源，然后通过告警通知管理员，以便对攻击源进行抑制，保证网络安全。

应用层联动

应用层联动模块为部分协议和业务提供开关，当协议开关关闭时，将针对该协议的报文直接丢弃，避免对系统造成攻击。如果协议开关打开，AR200-S 可以通过 CPU 防攻击的限速功能，使协议报文以指定的速率上送 CPU，保证 CPU 的资源不被耗尽，保证网络的正常运行。

目的

随着互联网技术的不断演进、网络规模的不断扩大以及网络应用日益普及，越来越多的企业通过借助网络来实现自身的快速发展。如何在一个开放的网络应用环境中保卫自身的机密数据、信息安全，这个问题为越来越多的企业所关注。

保护 CPU，保证 CPU 对正常业务的处理和响应具有重要意义。但是在网络中，存在正常的需要上送 CPU 处理的报文，也存在针对 CPU 的恶意攻击报文。针对 CPU 的恶意攻击报文会引发正常业务的中断甚至系统的瘫痪，大量突发性的正常报文也会导致 CPU 占用率过高，使 CPU 性能下降，从而影响 CPU 对正常业务的处理。

AR200-S 的本机防攻击功能针对的对象是上送 CPU 的报文，主要用于保护路由设备自身安全，使设备在受到攻击时保证已有业务可以正常运转以及在设备遭受攻击时屏蔽各业务之间的相互影响。

受益

企业受益

通过配置本机防攻击功能，保护网络安全，保证设备的稳定运行。

3.2 参考标准和协议

无。

3.3 可获得性

涉及网元

无需其他网元的配合。

License 支持

无需获得 License 许可，即可获得该特性的服务。

版本支持

表 3-1 版本支持

产品	最低支持版本
AR200-S	V200R002C00

特性依赖

不依赖其他特性。

硬件要求

对硬件无特殊要求。

3.4 原理描述

3.4.1 CPU 防攻击

AR200-S 支持多级安全机制，保证设备的安全，实现了对设备的分级保护。

AR200-S 通过以下策略实现对设备的分级保护：

- 第一级：通过黑名单来过滤上送 CPU 的非法报文。
- 第二级：对上送 CPU 的报文按照协议类型进行速率限制，保证每种协议上送 CPU 的报文不会过多。

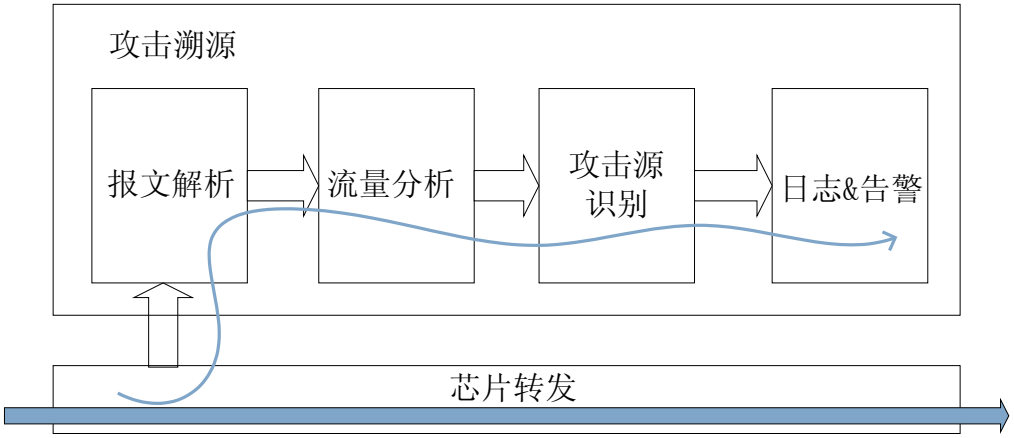
- 第三级：对上送 CPU 的报文，按照协议优先级进行调度，保证优先级高的协议先得到处理。
- 第四级：对上送 CPU 的报文统一限速，对超过统一限速值的报文随机丢弃，保证整体上送 CPU 的报文不会过多，保护 CPU 安全。

3.4.2 攻击溯源

攻击溯源针对设备 CPU 的 DOS 攻击进行防御。通过对上送 CPU 的报文进行分析统计，对统计的报文设置一定的阈值，超过阈值的报文即认为是攻击报文，对这些攻击的报文根据报文信息找出攻击源用户、或者攻击源接口，然后通过日志、告警等方式提醒管理员，以便管理员采用一定的措施来保护设备。

如图 3-1 所示，攻击溯源包括报文解析、流量分析、攻击源识别和发送日志告警通知管理员四个过程。

图 3-1 攻击溯源原理



通过图 3-1 所示的四个过程，找出攻击源，然后管理员通过 ACL 或配置黑名单的方式限制攻击源，以保护设备 CPU。

3.4.3 应用层联动

应用层联动模块为部分协议和业务提供开关，当协议开关关闭时，将该协议的报文直接丢弃，避免对系统造成攻击。如果协议开关打开，AR200-S 可以通过 CPU 防攻击的限速功能，使协议报文以指定的速率上送 CPU，保证 CPU 的资源不被耗尽，保证网络的正常运行。

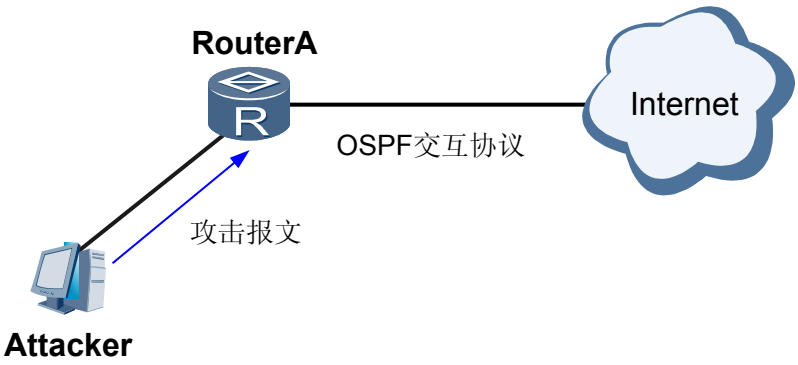
应用层联动主要应用于 AR200-S 启用多种功能和业务时，通过关闭某些协议防止攻击者对 AR200-S 进行攻击。

3.5 应用

3.5.1 CPU 防攻击

CPU 防攻击主要用于对设备 CPU 的防护，保证在有攻击的情况下 CPU 仍然能够正常运转。

图 3-2 CPU 防攻击应用



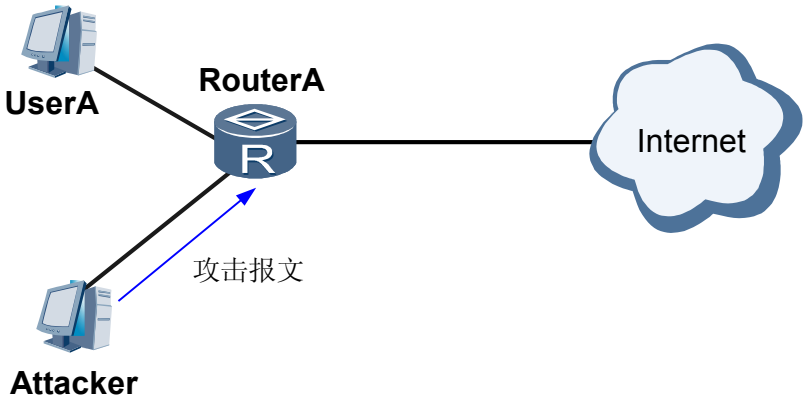
如图 3-2 所示，攻击者发送大量的攻击报文，占用过多的 CPU 资源，导致网络侧 OSPF 路由协议无法交互，协议无法建立。

在 RouterA 上配置 CPU 防攻击，限制用户的攻击报文，攻击报文被限制在一个很小的速率，不会影响 CPU 的正常处理，保证 CPU 可以有效的处理 OSPF 协议，OSPF 可以正常协商，从而使合法用户可以正常访问网络。

3.5.2 攻击溯源

攻击溯源主要防止大流量协议报文对设备的攻击，保护设备的 CPU。

图 3-3 攻击溯源应用



如图 3-3 所示，攻击者发送大量的攻击报文，导致设备 CPU 繁忙，无法处理其它业务。在 RouterA 上配置攻击溯源，通过报文分析统计找出攻击者的 MAC 地址，设备发送告警给管理员，然后由管理员登录到 RouterA 上，配置攻击者的黑名单，丢弃攻击者的攻击报文，保护设备的 CPU。

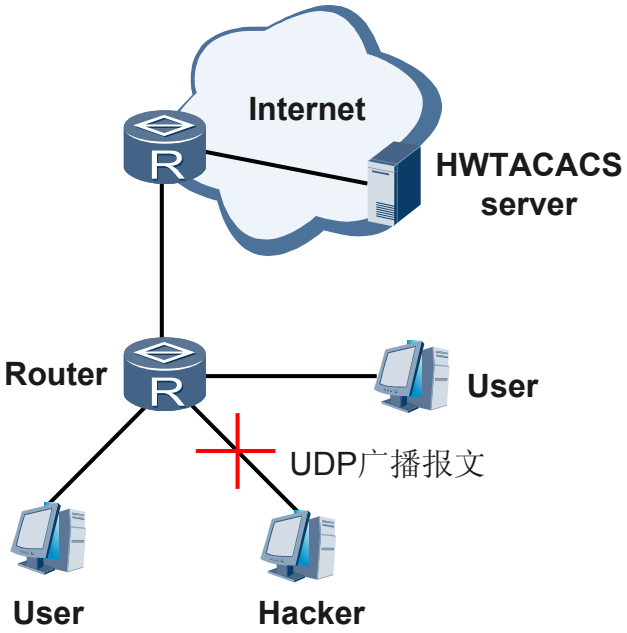
3.5.3 应用层联动

应用层联动主要过滤接收到的未启用业务的报文，防止 AR200-S 遭受攻击。

如图 3-4 所示，Router 启用很多业务，比如 BGP 和 VRRP 等，但不需要启用 UDP Helper。为了防止 Hacker 发送大量的 UDP 广播报文，导致 Router 耗费很多资源处理这

些攻击报文，可以在 Router 上关闭掉 UDP Helper，这样无论攻击者发送多少 UDP 广播报文，Router 都不进行处理，直接丢弃，保证了系统和资源的正常工作。

图 3-4 应用层联动组网



对于已经开启的业务和协议，Router 通过 CPU 防攻击的限速功能限制其上送速率，使其以指定的速率上送，保证 CPU 不受攻击，保证业务正常运行。

3.6 术语与缩略语

缩略语

缩略语	英文全称	中文全称
CAR	Committed Access Rate	承诺接入速率

4 IP 源防攻击

关于本章

4.1 介绍

定义

URPF（Unicast Reverse Path Forwarding）是单播逆向路径转发的简称，其主要功能是防止基于源地址欺骗的网络攻击行为。

单播逆向路径转发之所以称为“逆向”，是针对正常的路由查找而言的。一般情况下，AR200-S 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。

目的

URPF

现在，基于源 IP 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。URPF 可以用来防止基于源地址欺骗的网络攻击行为。

受益

企业受益

- 防御网络上的 IP 源攻击，降低对 IP 源攻击的维护成本。

用户受益

- 更安全的网络环境，不用担心 IP 源攻击的骚扰，获取到更稳定的网络服务。

4.2 参考标准和协议

无。

4.3 可获得性

涉及网元

无需其他网元的配合。

License 支持

无需获得 License 许可，即可获得该特性的服务。

版本支持

表 4-1 版本支持

产品	最低支持版本
AR200-S	V200R002C00

特性依赖

无

硬件要求

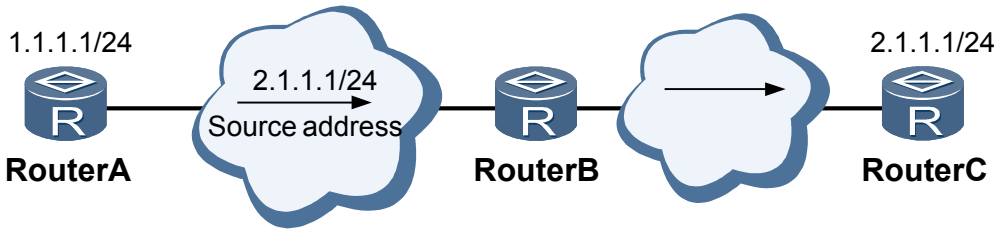
对硬件无特殊要求。

4.4 原理描述

4.4.1 URPF

URPF 通过获取报文的源地址和入接口，以源地址为目的地址，在转发表中查找源地址对应的接口是否与入接口匹配。如果不匹配认为源地址是伪装的，丢弃该报文。通过这种方式 URPF 就能有效地防范网络中通过修改源地址而进行的恶意攻击行为的发生。

图 4-1 URPF 原理



如图 4-1 所示，在 RouterA 上伪造源地址为 2.1.1.1 的报文向服务器 RouterB 发起请求，RouterB 响应请求时将向真正的“2.1.1.1”即 RouterC 发送报文。这种非法报文对 RouterB 和 RouterC 都造成了攻击。

如果在 RouterB 上启用 URPF，则 RouterB 在收到源地址为 2.1.1.1 的报文时，URPF 检查到以此报文源地址的路由不在收到该报文的接口上，则报文会被丢弃。

4.5 应用

4.5.1 URPF

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，AR200-S 中实现了 URPF 的两种模式

- 严格模式
- 松散模式

URPF 严格模式的应用

建议在路由对称的环境下使用 URPF 严格模式，即：不仅要求在转发表中存在相应表项，还要求接口一定匹配才能通过 URPF 检查。

如果两个网络边界 AR200-S 之间只有一条路径的话，这时，路由能够保证是对称的，使用严格模式能够最大限度的保证网络的安全性。

如图 4-2 图 4-3 所示，AS1 和 AS2 与 AS3 之间为单连接。在 RouterC 的 Eth1/0/0Vlanif 10 接口和 Eth2/0/0Vlanif 20 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 AS1 中的主机 PC A 伪造了一个源地址为 2.2.2.2 的报文，向 AS3 中的 Server 发送请求。RouterC 在接受到这个报文后，对其进行入接口检查，发现源地址为 2.2.2.2 的报文应该从 Eth2/0/0Vlanif 20 进入，而不应该从 Eth1/0/0Vlanif 10 进入，则 RouterC 认为该报文源地址是伪造的，直接丢弃该伪造报文。

从 AS2 发向 Server 的正常报文，检查通过后，被正常的转发。

图 4-2 URPF 严格模式应用环境示意图

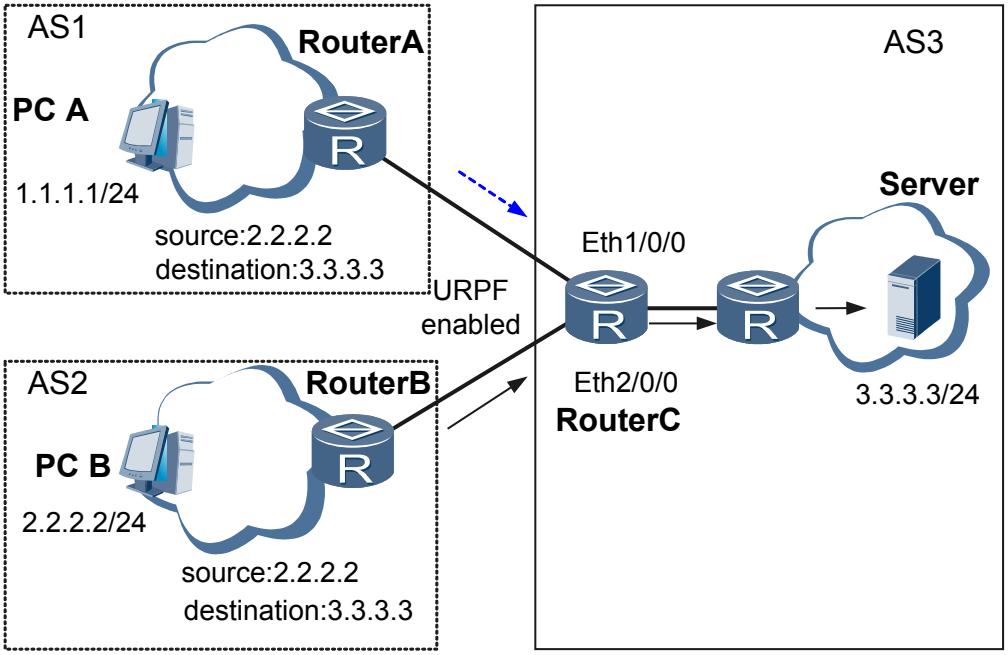
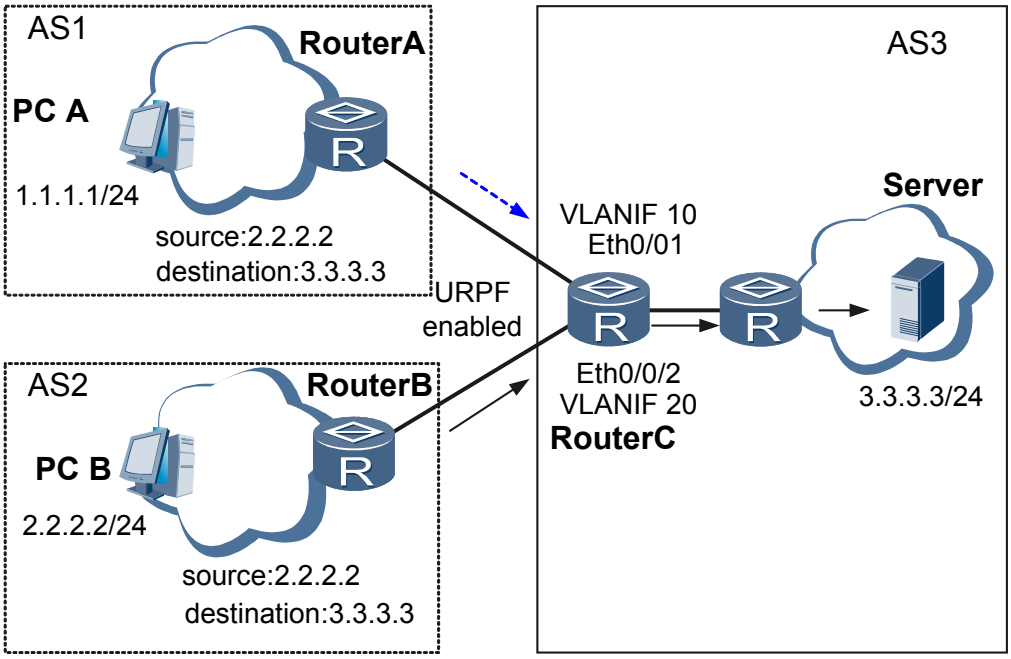


图 4-3 URPF 严格模式应用环境示意图



松散模式

可以在不能保证路由对称的环境下使用 URPF 的松散模式，即：不检查接口是否匹配，只要存在针对源地址的路由，报文就可以通过。

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。

4.6 术语与缩略语

术语

无

缩略语

缩略语	英文全称	中文全称
URPF	Unicast Reverse Path Forwarding	单播逆向路径转发

5 ARP 安全

关于本章

5.1 介绍

定义

ARP 安全是基于 ARP 的安全特性，通过 ARP 严格学习、ARP 表项保护和 ARP 报文速率限制等措施，不仅能够防范针对 ARP 协议的攻击，还可以防范网段扫描攻击等基于 ARP 协议的攻击。

目的

可以防范针对 ARP 表项的攻击。

常见的 ARP 攻击包括 ARP 欺骗和 ARP 泛洪攻击。

- ARP 欺骗指攻击者通过发送伪造的 ARP 报文，恶意修改设备或网络内其他主机的 ARP 表项，造成用户或网络的报文转发异常。ARP 欺骗可以分为：
  - 仿冒用户主机
  - 仿冒网关
- ARP 泛洪攻击是指攻击者向设备发送大量虚假的 ARP 请求报文或免费 ARP 报文，造成设备的计算资源长期忙于 ARP 处理，影响其他业务的处理，或者造成设备上的 ARP 表项超过规格，表项溢出，无法缓存正常用户的 ARP 表项，从而阻碍正常的报文转发。ARP 泛洪攻击可以分为：
  - 拒绝服务攻击
  - 缓存溢出攻击
  - 扫描攻击

受益

企业受益

- 防御网络上的 ARP 攻击，降低对 ARP 攻击的维护成本。

用户受益

- 更安全的网络环境，不用担心 ARP 攻击的骚扰，更稳定的网络服务。

5.2 参考标准和协议

本特性的参考资料清单如下：

文档	描述
RFC826	Ethernet Address Resolution Protocol
RFC903	Reverse Address Resolution Protocol
RFC1027	Using ARP to Implement Transparent Subnet Gateways
RFC1042	Standard for the Transmission of IP Datagrams over IEEE 802 Networks

5.3 可获得性

涉及网元

无需其他网元的配合。

License 支持

无需获得 License 许可，即可获得该特性的服务。

版本支持

表 5-1 版本支持

产品	最低支持版本
AR200-S	V200R002C00

特性依赖

不依赖其他特性。

硬件要求

对硬件无特殊要求。

5.4 原理描述

根据不同的攻击类型，可以配置不同的 ARP 安全特性来解决。如表 5-2 所示。

表 5-2 ARP 安全针对不同攻击类型的解决方法

攻击类型	ARP 安全特性
ARP flood	基于源 IP 或端口的 ARP 抑制 基于源 IP 的 ARP Miss 抑制
ARP 欺骗	ARP 严格学习 ARP 表项学习保护 防 ARP 网关冲突

5.4.1 ARP 报文抑制

收到大量 ARP 报文可能导致设备忙于进行 ARP 学习和 ARP 响应，无法处理其它业务，因此需要对 ARP 报文进行抑制，以保护 CPU 资源。ARP 报文抑制包括 ARP 报文源抑制和 ARP 报文速率抑制，其中 ARP 报文速率抑制基于全局或端口。

对于某一个用户，一般不会在短时间内发送大量的 ARP 报文，如果出现这种情况，可以认为是攻击。当设备检测到这种攻击后，可以通过对这个用户的 ARP 源抑制来保护设备的 CPU 资源，保证 CPU 可以正常处理业务。

基于全局的 ARP 速率抑制是为了保证设备出现 ARP 攻击时，限制上送主控板的 ARP 报文，从而保护设备的 CPU 资源，保证其他业务的正常运行

基于端口的 ARP 速率抑制是为了保证在某个端口出现 ARP 攻击时，不影响其他端口的 ARP 学习，同时还可以保护设备的 CPU 资源，保证其他业务的正常运行。

5.4.2 ARP Miss 消息抑制

ARP Miss 是指设备在转发时因匹配不到对应的 ARP 表项而上报的 Miss 消息，触发大量 ARP Miss 消息，对设备造成攻击。ARP Miss 消息抑制包括 ARP Miss 消息源抑制和 ARP Miss 消息速率抑制，其中 ARP Miss 消息速率抑制基于全局。

对于某一个用户，如果其发送的报文在短时间内触发大量的 ARP Miss 消息，如果出现这种情况，可以认为是攻击。当设备检测到这种攻击后，可以通过对这个用户的 ARP Miss 源抑制来保护设备的 CPU 资源，保证 CPU 可以正常处理业务。

基于全局的 ARP Miss 消息速率抑制是为了保证设备触发大量的 ARP Miss 消息时，限制上送主控板的 ARP Miss 报文，从而保护设备的 CPU 资源，保证其他业务的正常运行。

5.4.3 不学习免费 ARP 报文

免费 ARP 报文是主机使用自己的 IP 地址作为目的 IP 地址发送 ARP 报文，其主要目的有两个：

- 用于检查重复的 IP 地址：正常情况下不会收到 ARP 回应，如果收到，则表明本网络中存在与自身 IP 地址重复的地址。
- 用于通告一个新的 MAC 地址：发送方更换了网卡，MAC 地址变了，为了能够在 ARP 表项老化前通告所有主机，发送方可以发送一个免费 ARP 报文。

由于收到免费 ARP 报文并不需要身份验证，任何一个用户都可以发送免费 ARP 报文，如果此免费 ARP 报文使用其他用户的 IP 地址，则会将设备上对应用户的 ARP 修改为错误的 ARP，形成 ARP 欺骗。同时，大量的免费 ARP 报文也可能造成设备 CPU 超载，影响其他业务。

当设备通过 ARP 请求和响应学习 ARP 时，设备不支持 WAN 侧接口学习免费 ARP 报文，以降低 ARP 欺骗的可能性。

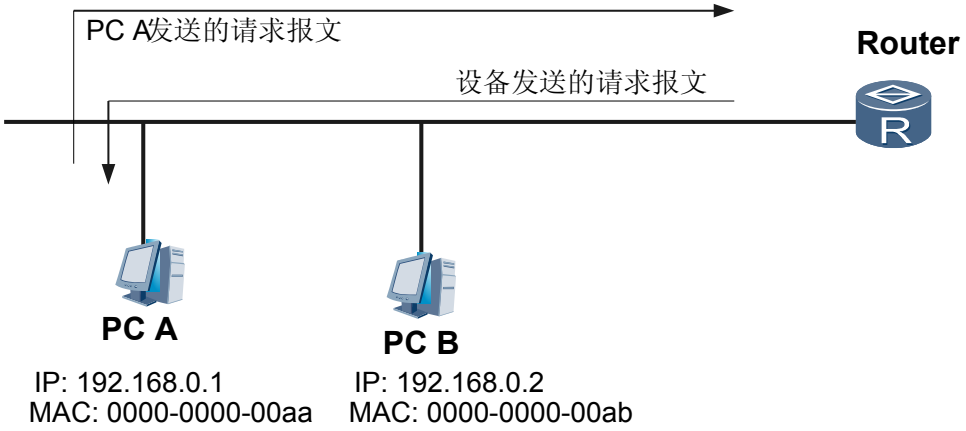
说明

设备只支持 Vlanif 接口学习免费 ARP 报文。

5.4.4 严格学习 APR 表项

严格学习 ARP 表项是指 AR200-S 仅仅学习自己发送的 ARP 请求报文的应答报文，并不学习其它设备向 AR200-S 发送的 ARP 请求报文。这样，可以拒绝掉大部分的 ARP 请求和应答报文攻击。

图 5-1 ARP 的严格学习



如图 5-1 所示，PC A 向 AR200-S 发送 ARP 请求报文，正常情况下，AR200-S 会向 PC A 发送 ARP 应答报文，并且 AR 将 PC A 的 MAC 地址加入对应的 ARP 表项（或者更新对应的 ARP 表项）。但是 AR200-S 配置了严格学习 APR 表项之后，AR200-S 会正常的向 PC A 发送 ARP 应答报文，但 AR200-S 并不将 PC A 的 MAC 地址加入对应的 ARP 表项（或者更新对应的 ARP 表项）。当收到的 ARP 请求报文和原来的 ARP 表项不一致的时候，AR200-S 会再向 PC A 发送一个 ARP 请求，待收到该请求对应的 PC A 发出的应答报文后，AR200-S 才会将 PC A 的 MAC 地址加入对应的 ARP 表项（或者更新对应的 ARP 表项）。

5.4.5 ARP 表项保护

设备在收到用户的第一个 ARP 报文时，会在 ARP 表中添加一个 ARP 表项，后续如果再收到此用户的 ARP 报文，会根据新的 ARP 报文更新原来的表项，包括更新 MAC 地址、端口、VLAN 信息和老化时间。如果存在攻击用户，故意发送错误的 ARP 报文以更新合法用户的 ARP 表，会导致设备上的 ARP 表项错误，合法用户的报文无法正常转发。

为了防御这种 ARP 攻击，设备可以在第一次学习到 ARP 以后，不再允许其他用户更新此表项或只能更新此表项的部分信息。

AR200-S 提供三种防御模式：fixed-all、fixed-mac 和 send-ack。

- 对于 fixed-all 模式，设备在收到 ARP 报文时，仅更新老化时间，其他项均不允许更新，如果收到报文中的 MAC 地址、端口、VLAN 信息和 ARP 表中的信息不匹配，报文直接被丢弃。
- 对于 fixed-mac 模式，设备在收到 ARP 报文时，仅不允许用户更新 MAC 信息，可以更新端口、VLAN 和老化时间，主要应用于用户端口会切换的场景。
- 对于 send-ack 模式，设备收到一个涉及 MAC 地址、VLAN、接口修改的 ARP 报文时，不会立即进行修改，而是先对原 ARP 表中与此 ARP 报文中的 MAC 地址对应的用户发一个单播确认。

5.4.6 防 ARP 网关冲突

当设置作为网关时，如果某个攻击者发送 ARP 来仿冒网关，会导致其下连的所有用户的网关 ARP 表被修改为错误的 ARP，所有用户发往网关的流量均发送到攻击者，攻击者可以轻易的窃听到用户的信息。

ARP 网关冲突防攻击功能使能后，系统生成 ARP 防攻击表项，在后续一段时间内对收到具有相同源 MAC 地址的报文直接丢弃，这样可以防止与网关地址冲突的 ARP 报文在 VLAN 内广播。AR200-S 支持发送免费 ARP 报文功能，此时可以使能此功能，发送正确的免费 ARP 报文，该报文广播发送到所有用户，可以迅速将已经被攻击的用户的 ARP 修改为正确 ARP，保证用户的安全性。

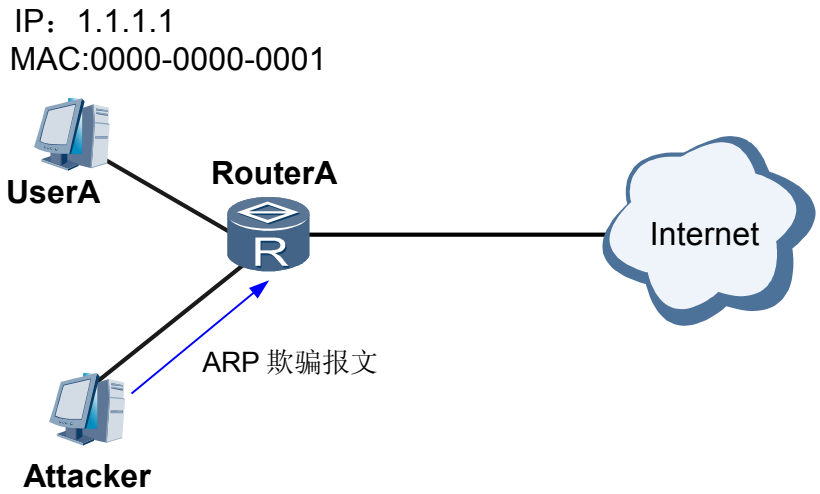
5.5 应用

5.5.1 ARP 表项保护

在企业网中，AR200-S 作为用户网关，用户上线后，在 AR200-S 上生成用户的 ARP 表项。如果此时其中的一个用户 PC 发送 ARP 欺骗报文，就可以修改 AR200-S 上正常用户的 ARP 表项，导致正常用户无法正常转发。

这种情况下，可以在 AR200-S 上配置 ARP 表项保护，防止非法用户修改设备上的 ARP 表项，保护合法用户正常访问网络。

图 5-2 ARP 表项保护



如图 5-2 所示，用户上线后，在 AR200-S 上生成用户的 ARP 表，用户可以正常访问网络，此时攻击者发送 ARP 欺骗报文来修改用户的 ARP 表，由于配置了 ARP 表项保护，AR200-S 上用户的 ARP 表不会被修改。

5.6 术语与缩略语

术语

无。

缩略语

无。

6 AAA 和用户管理

关于本章

6.1 介绍

定义

AAA（Authentication Authorization Accounting）是一种提供认证、授权和计费的技术。

- 认证（Authentication）：验证用户是否可以获得访问权，确定哪些用户可以访问网络。
- 授权（Authorization）：授权用户可以使用哪些服务。
- 计费（Accounting）：记录用户使用网络资源的情况。

说明

目前 AR200-S 不支持本地计费。

AR200-S 支持下列特性：

认证：

- 支持不认证方法。防止存在安全漏洞，不支持管理用户的认证方法为不认证。
- 支持本地认证方法。
- 支持 RADIUS 认证方法。
- 支持 HWTACACS 认证方法。
- 支持多个认证方法组合。当前认证方法无响应的情况下，会尝试用下一个认证方法认证。
- 支持 EAP 终结认证。
- 支持 EAP 透传认证。
- 支持 PAP/CHAP 认证。支持密码为明文、密文两种认证方式。
- 支持管理用户管理级别切换认证。
- 支持通过 HWTACACS 进行管理级别切换认证。
- 支持通过本地进行管理级别切换认证。
- 支持通过不认证进行管理级别切换认证。

授权：

- 支持不授权方法。
- 支持本地授权方法。
- 支持 HWTACACS 授权方法。
- 支持 if-authenticated 授权方法。如果用户认证通过并且认证方法不是不认证，则授权通过，否则授权失败。
- 支持多个授权方法组合。当前授权方法无响应的情况下，会尝试用下一个授权方法授权。
- 支持管理用户的命令行授权。
- 支持通过 HWTACACS 进行命令行授权。
- 支持通过本地进行命令行授权。
- 支持 RADIUS COA。
- 支持 RADIUS DM。

计费：

- 支持不计费。
- 支持 Radius 计费。
- 支持 Hwtacacs 计费。
- 支持按时长计费。
- 支持实时计费。

此外还可以在 AR200-S 上配置计费失败策略:

应用了计费方案之后，如果有用户上线，AR200-S 将向计费服务器发送开始计费请求。正常情况下，计费服务器响应 AR200-S 的请求。由于网络故障的影响，可能造成 AR200-S 没有收到计费服务器的响应而造成计费失败。计费失败后，需要执行相应的策略：

- 为了避免因网络故障导致的计费失败对用户造成影响，可以配置允许用户上线。
- 只要计费失败就停止为用户提供服务，可以配置拒绝用户上线。

目的

提供对用户进行认证、授权和计费三种安全功能。

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
RFC 2093	Generic AAA Architecture	
RFC 2094	AAA Authorization Framework	
RFC 2095	AAA Authorization Application Examples	
RFC 2096	AAA Authorization Requirements	
RFC 2058	Remote Authentication Dial In User Service (RADIUS)	
RFC 2059	RADIUS Accounting	
RFC 2138	Remote Authentication Dial In User Service (RADIUS)	
RFC 2139	RADIUS Accounting	
RFC 2865	Remote Authentication Dial In User Service (RADIUS)	
RFC 2866	RADIUS Accounting	
RFC 2869	RADIUS Extensions	
RFC 0927	TACACS user identification Telnet option	

文档	描述	备注
RFC 1492	An Access Control Protocol, Sometimes Called TACACS	

6.3 可获得性

涉及网元

RADIUS 服务器、HWTACACS 服务器。

License

无须 Licence 支持。

版本支持

产品	最低支持版本
AR200-S	V200R002C00

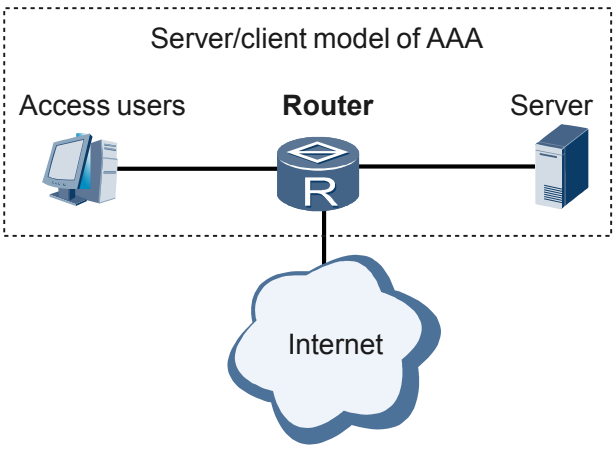
6.4 原理描述

6.4.1 AAA 协议

AAA 的基本构架

AAA 通常采用“客户端—服务器”结构。这种结构既具有良好的可扩展性，又便于集中管理用户信息。如图 6-1 所示。

图 6-1 AAA 的基本构架示意图



认证

AAA 支持以下认证方式：

- 不认证：对用户非常信任，不对其进行合法检查，一般情况下不采用这种方式。

  说明

  管理用户不支持 AAA 的不认证方式。

- 本地认证：将用户信息（包括本地用户的用户名、密码和各种属性）配置在网络接入服务器上。本地认证的优点是速度快，可以为运营降低成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证：将用户信息（包括本地用户的用户名、密码和各种属性）配置在认证服务器上。AAA 支持通过 RADIUS（Remote Authentication Dial In User Service）协议或 HWTACACS （HuaWei Terminal Access Controller Access Control System）协议进行远端认证。网络接入服务器 NAS（Network Access Server）作为客户端，与 RADIUS 服务器或 HWTACACS 服务器通信。

如果在一个认证方案中采用多种认证模式，将按照配置的顺序进行认证。

- 当配置的认证方式是先远端认证后本地认证时

  如果登录的帐号在远端服务器上没有创建，但是在本地是存在的，经过远端认证时，将被认为认证失败，不再转入本地认证。

  只有在远端认证服务器无响应时，才会转入本地认证。
- 如果选用了不认证（none）或本地认证（local），它必须作为最后一种认证模式。

授权

AAA 支持以下授权方式：

- 不授权：不对用户进行授权处理。
- 本地授权：根据网络接入服务器为本地用户账号配置的相关属性进行授权。
- HWTACACS 授权：由 TACACS 服务器对用户进行授权。
- if-authenticated 授权：如果用户通过了认证，而且使用的认证模式不是不认证，则用户授权通过。
- RADIUS 认证成功后授权：RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。

如果在一个授权方案中使用多次授权，授权模式的执行顺序按照配置的先后，只有在当前授权模式没有响应时，才会尝试下一个授权模式，如果授权失败则将不会再进行授权。

计费

AAA 支持以下计费方式：

- 不计费：不对用户计费。
- 远端计费：通过 RADIUS 服务器或 HWTACACS 服务器进行远端计费。

6.4.2 RADIUS 协议

AAA 可以用多种协议来实现，最常用的是 RADIUS 协议。RADIUS 最初用来管理使用串口和调制解调器的大量分散用户，后来广泛应用于网络接入服务器 NAS（Network Access Server）系统。

当用户想要通过某个网络（如电话网络）与 NAS 建立连接从而取得访问其他网络的权利或取得使用某些网络资源的权利时，NAS 起到了认证用户或对应连接的作用。

NAS 负责把用户的认证和计费信息传递给 RADIUS 服务器。RADIUS 协议规定了 NAS 与 RADIUS 服务器之间如何传递用户信息和计费信息以及认证和计费结果，RADIUS 服务器负责接收用户的连接请求，完成认证，并把认证结果和用户所需的配置信息返回给 NAS。

NAS 和 RADIUS 之间的验证信息的传递是通过密钥的参与来完成的，以避免用户的密码在不安全的网络上传输时被窃取。

协议实现

RADIUS 使用 UDP（User Datagram Protocol）作为传输协议，具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。

网络接入服务器作为 RADIUS 协议的客户端，实现以下功能：

- 标准 RADIUS 协议及扩充属性，包括 RFC2865、RFC2866。
- 华为扩展的私有属性。
- 对 RADIUS 服务器状态的主动探测功能：收到 AAA 的认证或计费消息后，如果当前服务器的状态为 DOWN，启动服务器探测处理，将消息转换为报文后向当前服务器发送，该报文作为服务器的探测报文，如果收到 RADIUS 服务器的回应，则认为该服务器重新可用。
- 自动切换 RADIUS 服务器功能：如果当前发送的服务器的状态为不可发送，或者发送次数超过当前服务器的最大重传次数，则需要在配置的服务器组中选择另外的服务器发送报文。

认证和计费

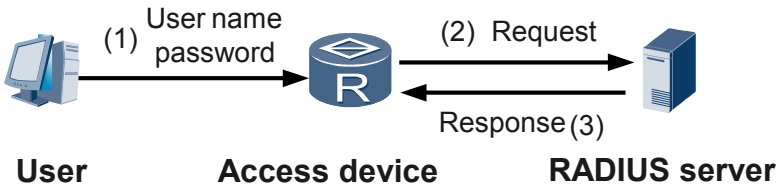
RADIUS 服务器通过建立一个唯一的用户数据库，存储用户名、密码来对用户进行验证。

RADIUS 客户端与服务器间的消息流程如图 6-2 所示。

- 用户登录路由器或接入服务器等网络设备时，会将用户名和密码发送给该网络接入服务器；
- 该网络设备中的 RADIUS 客户端（网络接入服务器）接收用户名和密码，并向 RADIUS 服务器发送认证请求；
- RADIUS 服务器接收到合法的请求后，完成认证，并把所需的用户授权信息返回给客户端；对于非法的请求，RADIUS 服务器返回认证失败的信息给客户端。

客户端和 RADIUS 服务器之间发送的用户密码信息经过加密以后才在网络上传递，以避免用户密码在不安全的网络上被窃取。

图 6-2 RADIUS 客户端与服务器间的消息流程



计费的消息流程和认证/授权的消息流程类似。

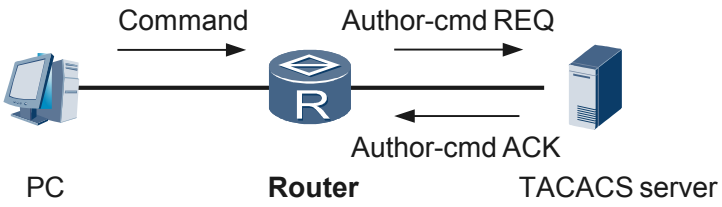
6.4.3 HWTACACS 协议

HWTACACS 是在 TACACS（RFC1492）基础上进行了功能增强的一种安全协议。该协议与 RADIUS 协议类似，主要是通过“客户端—服务器”模式与 HWTACACS 服务器通信来实现多种用户的 AAA 功能，可用于 PPP、VPDN（Virtual Private Dial Network）接入用户的认证、授权和计费。

HWTACACS 协议原理

- 按命令行授权
  - 用户通过 Telnet 或者 SSH 登录到路由器上后，如果需要对该用户输入的命令行进行认证，可以将该级别用户的命令行授权方法设置为 HWTACACS，该用户输入的每一条命令都要通过 HWTACACS 服务器授权。如果授权通过，命令就可以被执行。否则，HWTACACS 服务器输出信息，通知用户该命令的授权失败，命令不能执行。
  - 命令行授权可以使用本地授权的方法作为备选方法，这样，如果因为服务器的问题（服务器 Down、不可达或回应超时）导致命令行授权失败时，可以将命令行授权转入本地授权处理。
  - 如果在用户配置的超时时间内，路由器没有接收到 HWTACACS 服务器的授权结果，则授权超时，该命令不能被执行。
  - HWTACACS 按命令行授权的执行流程如图 6-3 所示。

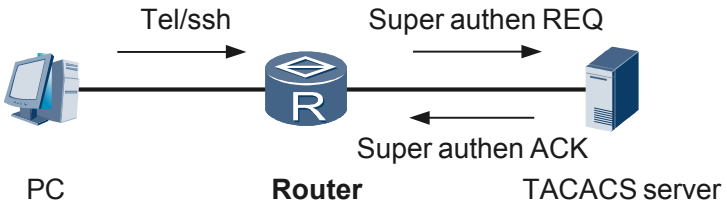
图 6-3 HWTACACS 按命令行授权的执行流程



- 对用户级别提升进行认证
  - 用户通过 Telnet 或者 SSH 登录到路由器后，可以通过在用户模式下使用 **super** 命令来提升自己的级别。这时，路由器对用户的密码进行验证。
  - HWTACACS 可以对用户级别的提升进行认证，其执行流程如图 6-4 所示。路由器将用户的密码发送到 HWTACACS 服务器上进行认证，如果认证通过，用户

的权限就可以得到提升，否则，用户的权限不能提升。特权等级更改的结果只影响本次登录。

图 6-4 HWTACACS 的用户级别提升的执行流程



- 如果在用户配置的超时时间内，路由器没有接收到 HWTACACS 服务器用户级别提升的认证结果，则认证超时，用户不能提升权限。
- 用户级别提升可以使用本地认证作为备选方法，使用设备上的 super 密码验证。这样，如果因为服务器的问题（如，服务器 Down、不可达或回应超时等）导致级别提升失败时，可以将级别提升转入本地处理。

HWTACACS 协议和 RADIUS 协议的比较

与 RADIUS 相比，HWTACACS 具有更加可靠的传输和加密特性，更加适合于安全控制。HWTACACS 协议与 RADIUS 协议的主要区别如表 6-1 所示。

表 6-1 HWTACACS 协议与 RADIUS 协议的比较

HWTACACS	RADIUS
使用 TCP，网络传输更可靠	使用 UDP
除了标准的 HWTACACS 报文头，对报文主体全部进行加密	只是对认证报文中的密码字段进行加密
认证与授权分离	认证与授权一起处理
适于进行安全控制	适于进行计费
支持对路由器上的配置命令进行授权使用	不支持

6.4.4 基于域的用户管理

在目前 AAA 的实现中，所有用户都属于某个域。用户属于哪个域是由用户名中带的“@”后的字符串来决定的，比如“user@hua”，就属于“hua”域；如果用户名中没有带“@”，对于普通用户，属于系统缺省的 default 域，对于管理用户，属于系统缺省的 default_admin 域。

路由器对接入用户的管理

路由器通过域来进行用户管理，域下可以进行缺省授权配置、RADIUS/HWTACACS 模板配置、认证和计费方案的配置等。

所有对于接入用户的认证、授权、计费都是在域视图下应用认证方案、授权方案、计费方案来实现的，为此必须先在 AAA 视图下分别配置相应的认证方案、授权方案、计费方案。

AAA 有缺省的认证方案、授权方案、计费方案，分别采用本地认证、本地授权、不计费。如果新创建一个域，没有在域下应用认证方案、授权方案、计费方案，那么 AAA 对该域将采用缺省的认证方案和计费方案。新创建域默认不绑定授权方案。此外，如果要对用户采用 RADIUS/HWTACACS 方案，必须预先在系统视图下配置 RADIUS/HWTACACS 服务器模板，然后在用户所属域的视图下应用该服务器模板。

当域和域下的用户同时配置了某一属性时，基于用户的配置优先级高于域的配置优先级。

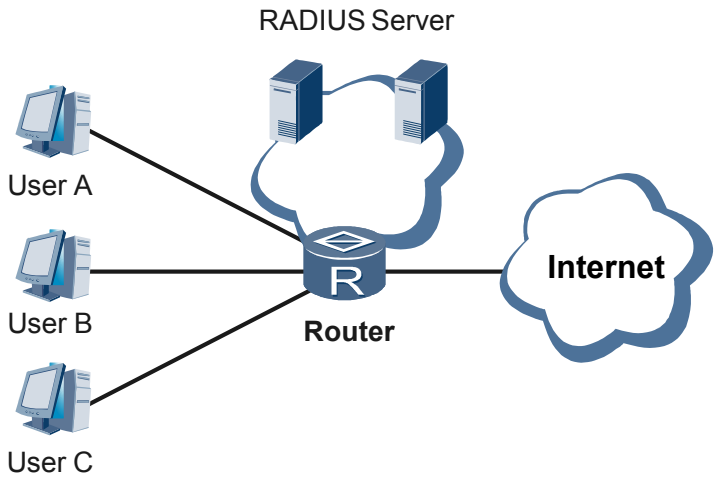
域下配置的授权信息较 AAA 服务器的授权信息优先级低，即，优先使用 AAA 服务器下发的授权属性，在 AAA 服务器无该项授权或不支持该项授权时，域的授权属性生效。这样处理的优点是：可以凭借域管理灵活增加业务，而不必受限于 AAA 服务器提供的属性。

6.5 应用

6.5.1 使用 RADIUS 对接入用户进行管理

使用 RADIUS 对接入用户进行管理，如图 6-5 所示。用户 A、B、C 都属于某个域下的用户，通过 Router 接入 Internet。设备根据用户所属的域，选择具体的 RADIUS 服务器对其进行认证，如果认证通过，用户就可以访问 Internet。

图 6-5 使用 RADIUS 对接入用户进行管理

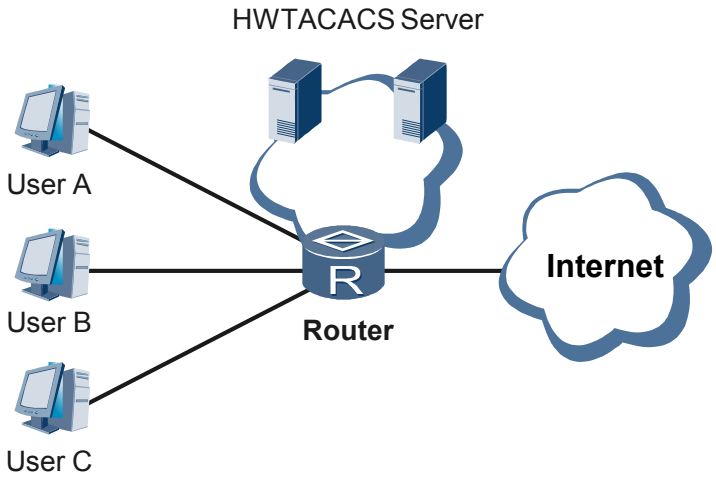


6.5.2 使用 HWTACACS 对接入用户进行管理

使用 HWTACACS 对接入用户进行管理，如图 6-6 所示。用户 A、C 属于某个域下的用户，通过 Router 接入 Internet。Router 根据用户所属的域，选择具体的 HWTACACS 服务器对其进行认证，如果认证通过，用户 A、C 就可以访问 Internet。

用户 B 是管理用户，需要登录设备对其进行配置。使用 HWTACACS 对其进行管理，对用户 B 在设备上配置的每一条命令进行授权，以获得较高的安全性。

图 6-6 使用 HWTACACS 对接入用户进行管理



6.6 术语与缩略语

缩略语

缩略语	英文全称	中文全称
AAA	Authentication、Authorization、Accounting	认证、授权、计费
RADIUS	Remote Authentication Dial in User Service	远端用户拨入认证服务
HWTACACS	HUAWEI Terminal Access Controller Access Control System	华为终端访问控制器控制系统协议

7 NAC

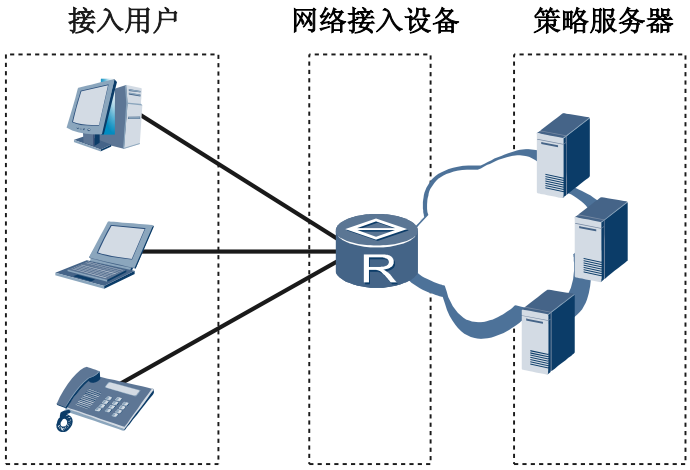
关于本章

7.1 介绍

定义

NAC（Network Access Control）称为网络接入控制，是一种安全接入的框架。其理念就是安全是“端到端”的概念。

图 7-1 NAC 的基本构架示意图



如图 7-1 所示，NAC 作为解决网络安全接入控制的一种方案，主要包括以下几个部分：

- 接入用户：需要对其进行认证。如果采用 802.1x 认证，用户还需要安装客户端软件。
- 网络接入设备：对接入用户进行认证和授权。一般需要和 AAA 服务器配合使用，防止非法终端接入，降低不安全终端的威胁；防止合法终端越权访问，保护核心资源。
- 策略服务器：主要对接入用户进行安全检查与策略管理。

目的

对用户的接入进行安全控制。

7.2 参考标准和协议

与 NAC 特性相关的参考资料清单如下：

文档	描述	备注
RFC3748	Extensible Authentication Protocol (EAP)	-

文档	描述	备注
Portal	Portal 协议标准	-

7.3 可获得性

涉及网元

用户终端软件、AAA 服务器。

License 支持

无需 License 支持。

版本支持

产品	最低支持版本
AR200-S	V200R002C00

7.4 原理描述

7.4.1 802.1X 认证

802.1x 认证，又称 EAPOE 认证，主要目的是为了解决局域网用户的接入认证问题。

IEEE 802.1x 标准（以下简称 802.1x）的主要内容是一种基于端口的网络接入控制（Port Based Network Access Control）协议。“基于端口的网络接入控制”是指在局域网接入控制设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

802.1x 协议仅关注接入端口的状态。当合法用户（根据帐号和密码）接入时，该端口打开；当非法用户接入或没有用户接入时，该端口处于关闭状态。认证的结果在于端口状态的改变，而不涉及通常认证技术必须考虑的 IP 地址协商和分配问题，是各种认证技术中最简化的实现方案。

802.1x 支持的认证模式

- 基于端口模式：当采用基于端口方式时，只要该端口下的第一个用户认证成功后，其他接入用户无须认证就可使用网络资源。但是当第一个用户下线后，其他用户也会被拒绝使用网络。
- 基于 MAC 模式：当采用基于 MAC 地址方式时，该端口下的所有接入用户均需要单独认证。

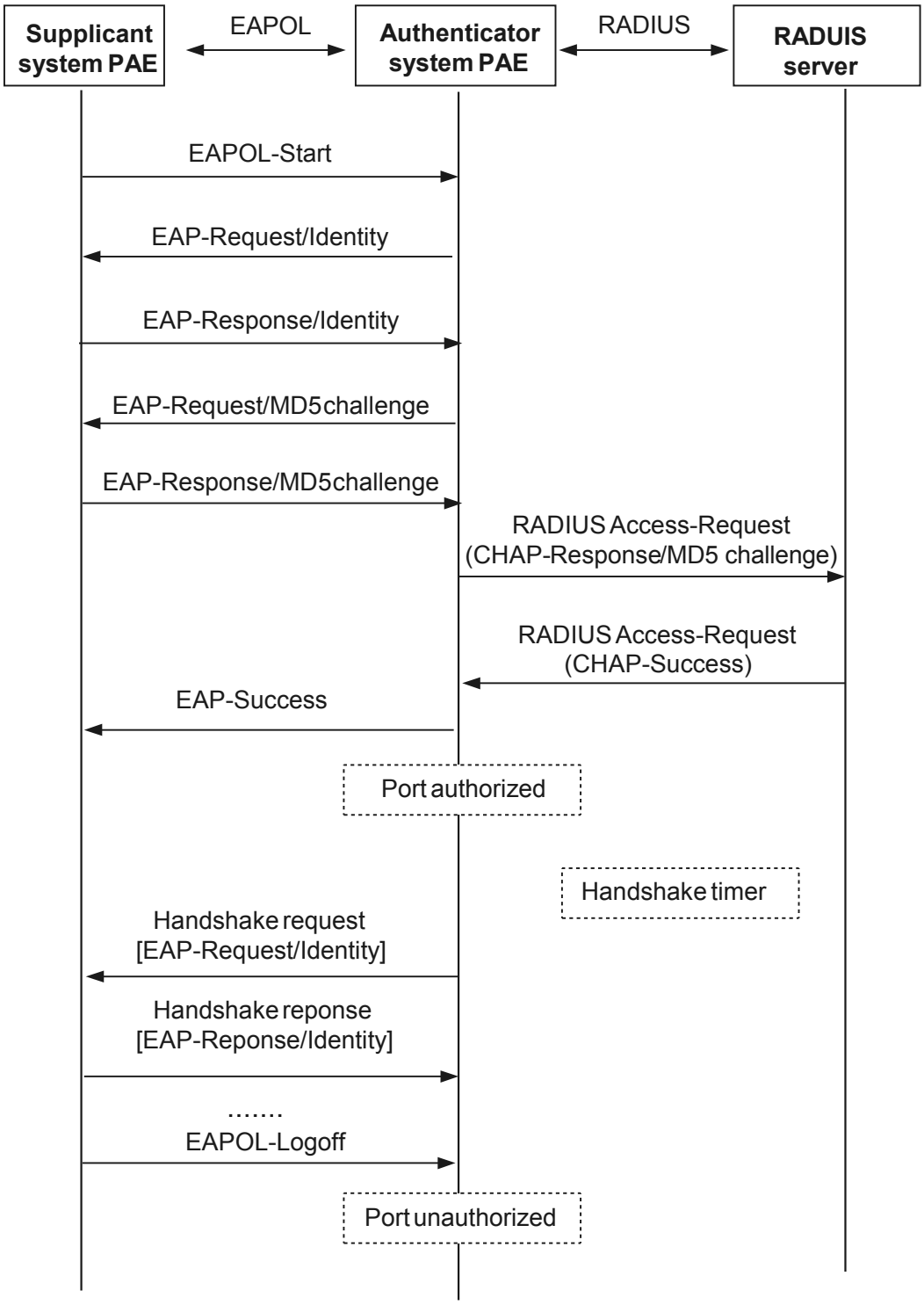
802.1x 支持的端口控制方式

- 自动识别模式：端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果认证流程通过，则端口切换到授权状态，允许用户访问网络资源。
- 强制授权模式；端口始终处于授权状态，允许用户不经认证授权即可访问网络资源。
- 强制非授权模式；端口始终处于非授权状态，不允许用户访问网络资源。

802.1x 支持的认证方式

- EAP 终结认证：由网络接入设备终结用户的 EAP 报文，解析出用户名和密码，并对密码进行加密，再发送到 AAA 服务器进行认证。

图 7-2 EAP 终结认证



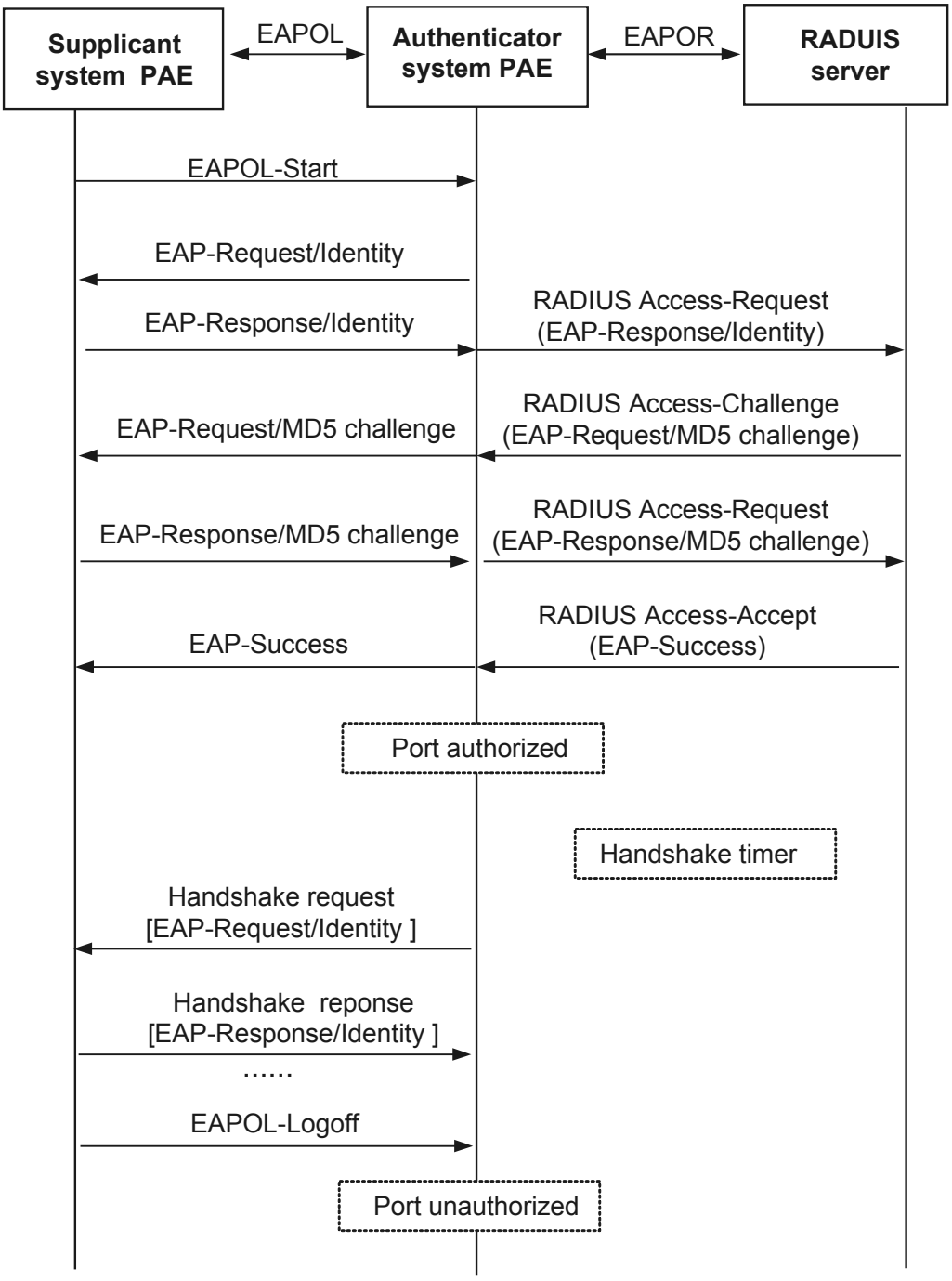
EAP 终结认证过程如下（设备指的是网络接入设备）：

1. EAP 客户端发送 EAP-Start 报文给设备。
2. 设备发送 EAP-Request/Identity 报文给客户端。

3. 客户端回应 EAP-Response/Identity 报文，报文携带用户名信息。
4. 设备发送 EAP-Request/MD5-Challenge 报文给客户端。
5. 客户端回应 EAP-Response /MD5-Challenge 报文，设备获取客户端的密码信息。
6. 设备携带用户账户信息，到 AAA 系统进行认证。
7. 认证通过后设备通知客户端认证成功，端口打开。
8. 设备通过 EAP 探测判断 EAP 客户端是否维持在线。

- EAP 透传认证：也叫 EAP 中继认证，由网络接入设备直接把 802.1x 用户的认证信息以及 EAP 报文直接封装到 RADIUS 报文的属性字段中，发送给 RADIUS 服务器，而无须将 EAP 报文转换成标准的 RADIUS 报文后再发给 RADIUS 服务器来完成认证。

图 7-3 EAP 透传认证



EAP 透传认证的过程如下（设备指的是网络接入设备）：

1. EAP 客户端发送 EAP-Start 报文给设备。
2. 设备发送 EAP-Request/Identity 报文给客户端。
3. 客户端回应 EAP-Response/Identity 报文，设备透传报文给 RADIUS 服务器。
4. 设备收到 RADIUS 挑战报文后，发送 EAP 挑战报文 EAP-Request/MD5-Challenge 给客户端。

5. 客户端回应 EAP-Response/MD5-Challenge 报文，设备透传报文给 RADIUS 服务器。
6. 设备认证成功后，通知客户端认证成功，端口打开。
7. 客户端在线过程中，设备通过 EAP 握手报文进行探测客户端是否保持在线。

Guest VLAN

在配置 802.1x 认证时，可以配置 Guest VLAN 功能，并在 Guest VLAN 中配置常用的服务器，如补丁服务器、防病毒服务器等。当认证终端不响应 802.1x 认证请求时，例如没有安装客户端软件，AR200-S 将与认证终端连接的接口加入到 Guest VLAN 中，这样用户就可以访问 Guest VLAN 中的资源。从而满足未认证的用户进行更新病毒库、下载补丁等操作。

Restrict VLAN

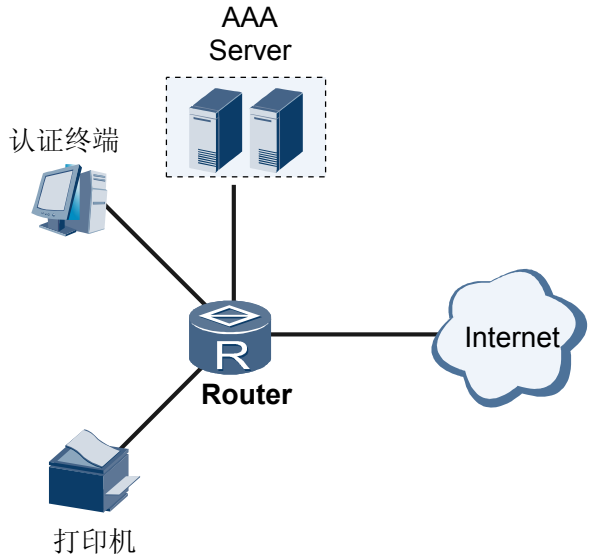
在配置 802.1x 认证时，可以配置 Restrict VLAN 功能。当用户认证失败后，例如输入了错误的用户名和密码，AR200-S 将与认证终端连接的接口加入到 Restrict VLAN 中。Restrict VLAN 和 Guest VLAN 的功能相似，都是满足用户在通过认证前可以访问有限的网络资源。通常在 Restrict VLAN 中部署的网络资源比 Guest VLAN 中更少，从而更严格的限制没有通过认证的用户。

7.5 应用

7.5.1 802.1x 认证的应用

如图 7-4 所示，认证终端安装终端软件后，认证终端发起认证申请，Router 和认证终端交互信息后，把用户信息发送到 ASC 进行认证。认证通过后，Router 打开与该认证终端相连的端口，允许终端访问网络。

图 7-4 802.1x 认证的应用



在此应用场景下，认证的结果在于端口状态的改变，而不涉及通常认证技术必须考虑的IP 地址协商和分配问题，是各种认证技术中最简化的实现方案。但是需要安装终端软件。

7.6 术语与缩略语

缩略语

缩略语	英文全称	中文全称
AAA	Authentication、Authorization、Accounting	认证、授权、计费
EAP	Extensible Authentication Protocol	可扩展认证协议

8 防火墙

关于本章

8.1 介绍

防火墙的引入

目前，Internet 网络上常见的安全威胁大致分为以下几类：

- 非法使用：资源被未授权的用户（也称为非法用户）或以未授权方式（非法权限）使用。例如，攻击者通过猜测帐号和密码的组合，从而进入计算机系统非法使用资源。
- 拒绝服务：服务器拒绝合法用户正常访问信息或资源的请求。例如，攻击者短时间内使用大量数据包或畸形报文向服务器不断发起连接或请求回应，致使服务器负荷过重而不能处理合法任务。
- 信息盗窃：攻击者并不直接入侵目标系统，而是通过窃听网络来获取重要数据或信息。
- 数据篡改：攻击者对系统数据或消息流进行有选择的修改、删除、延误、重排序及插入虚假消息等操作，而使数据的一致性被破坏。

一般而言，安全防范体系具体实施的基本内容就是在内部网和外部网之间构筑一道防线，以抵御来自外部的绝大多数攻击。通常，我们用防火墙作为内外部网之间的安全“防线”。

防火墙分为包过滤防火墙、代理防火墙和状态防火墙三种，AR200-S 提供包过滤防火墙和状态防火墙功能。

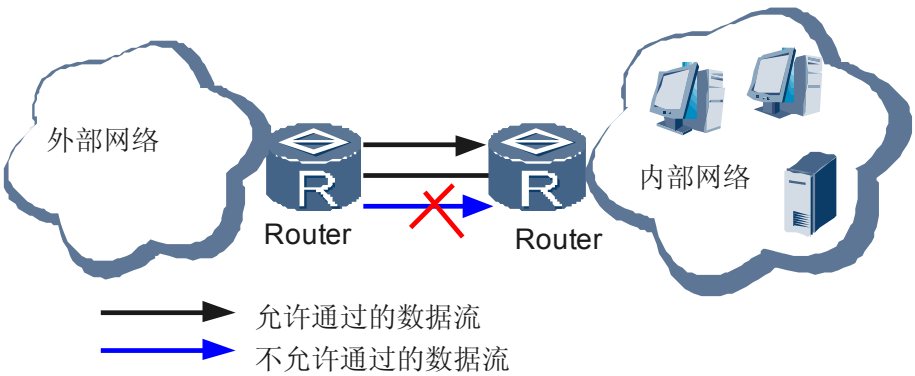
防火墙的作用

在大厦构造中，防火墙被设计用来防止火从大厦的一部分传播到另一部分。网络中的防火墙有类似的作用：防止 Internet 的危险传播到私有网络，或者在企业私有网络中保护重要的设备。

在网络边界处，防火墙一方面阻止来自 Internet 对受保护网络的未授权或未验证的访问，另一方面允许内部网络的用户对 Internet 进行 WEB 访问或收发 E-mail 等。

当外部网络的用户访问内部网络资源时，要经过防火墙；而内部网络的用户访问外部网络资源时，也会经过防火墙。这样，防火墙就起到了一个“警卫”的作用，可以将需要禁止的数据包在这里丢掉，如图 8-1 所示：

图 8-1 防火墙示意图



防火墙不单用于私有网络对 Internet 的连接，也可以用来在组织网络内部保护大型机和重要的资源（如数据）。对受保护数据的访问都必须经过防火墙的过滤，即使网络内部用户要访问受保护的资源，也要经过防火墙。

防火墙还可以作为一个访问 Internet 的权限控制关口，如允许组织内特定的人访问 Internet。现在的许多防火墙同时还具有其他一些功能，如进行身份认证、对信息进行安全（加密）处理等等。

防火墙的局限性

防火墙具有以下局限性：

- 防火墙难于防内。它无法防范来自防火墙内部的攻击。
- 防火墙的执行效率会随着防火墙上应用规则的增多而降低。配置的匹配项目越多，效率越低。

8.2 参考标准和协议

本特性的参考资料清单如下：

文档	描述
RFC 791	Internet Protocol
RFC 792	Internet Control Message Protocol
RFC 793	Transmission Control Protocol

8.3 可获得性

涉及网元

无需其他网元的配合。

License 支持

无需获得 License 许可，即可获得该特性的服务。

版本支持

表 8-1 版本支持

产品	最低支持版本
AR200-S	V200R001C00

特性依赖

不依赖其他特性。

硬件要求

对硬件无特殊要求。

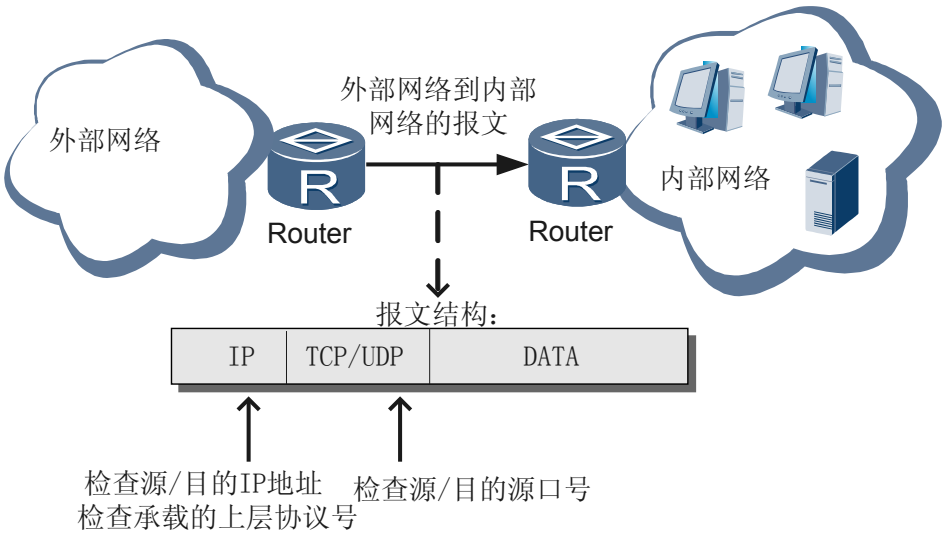
8.4 原理描述

8.4.1 包过滤防火墙

包过滤防火墙的基本原理是：通过配置 ACL 实施数据包的过滤。实施过滤主要是基于数据包中的 IP 层所承载的上层协议的协议号、源/目的 IP 地址、源/目的端口号和报文传递的方向等信息。

包过滤应用在 AR200-S 的防火墙中，对 AR200-S 需要转发的数据包，先获取数据包的包头信息，然后和设定的 ACL 规则进行比较，根据比较的结果决定对数据包进行转发或者丢弃。如图 8-2 所示。

图 8-2 包过滤防火墙



AR200-S 对包过滤防火墙的支持

- 普通 IP 报文过滤：防火墙基于访问控制列表 ACL 对报文进行检查和过滤。防火墙检查报文的源/目的 IP 地址、源/目的端口号、协议类型号，根据访问控制列表允许符合条件的报文通过，拒绝不符合匹配条件的报文。防火墙所检查的信息来源于 IP、TCP 或 UDP 包头。
- 分片报文过滤：包过滤提供了对分片报文进行检测过滤的支持。包过滤防火墙将识别报文类型，如：非分片报文、首片分片报文、后续分片报文，对所有类型的报文都做过滤。

  对于首片分片报文，AR200-S 根据报文的三层信息及四层信息，与 ACL 规则进行匹配，如果允许通过，则记录首片分片报文的状态信息，建立后续分片的匹配信息

表。当后续分片报文到达时，防火墙不再进行 ACL 规则的匹配，而是根据首片分片报文的 ACL 匹配结果进行转发。

另外，对于不匹配 ACL 规则的报文，防火墙还可以配置缺省处理方式。

8.4.2 状态防火墙

状态防火墙是包过滤防火墙的扩展，它不仅仅把数据包作为独立单元进行 ACL 检查和过滤，同时也考虑前后数据包的应用层关联性。

状态防火墙使用各种状态表来监控 TCP/UDP 会话，由 ACL 表来决定哪些会话允许建立，只有与被允许会话相关联的数据包才被转发。同时状态防火墙针对 TCP/UDP 会话，分析数据包的应用层状态信息，过滤不符合当前应用层状态的数据包。

状态防火墙结合了包过滤防火墙和代理防火墙的优点，不仅速度快，而且安全性高。

ASPF

ASPF（Application Specific Packet Filter）是针对应用层的报文过滤，即基于状态的报文过滤。它能够检测试图通过防火墙的应用层协议会话信息，通过维护会话的状态和检查会话报文的协议和端口号等信息，阻止不符合规则的数据报文穿过防火墙。对于所有连接，每一个连接状态信息都将被 ASPF 维护并用于动态的决定数据包是否被允许通过防火墙或丢弃。同时，ASPF 可以对各种应用层协议的流量进行监测。

ASPF 和普通的包过滤防火墙协同工作，以便于实施内部网络的安全策略。

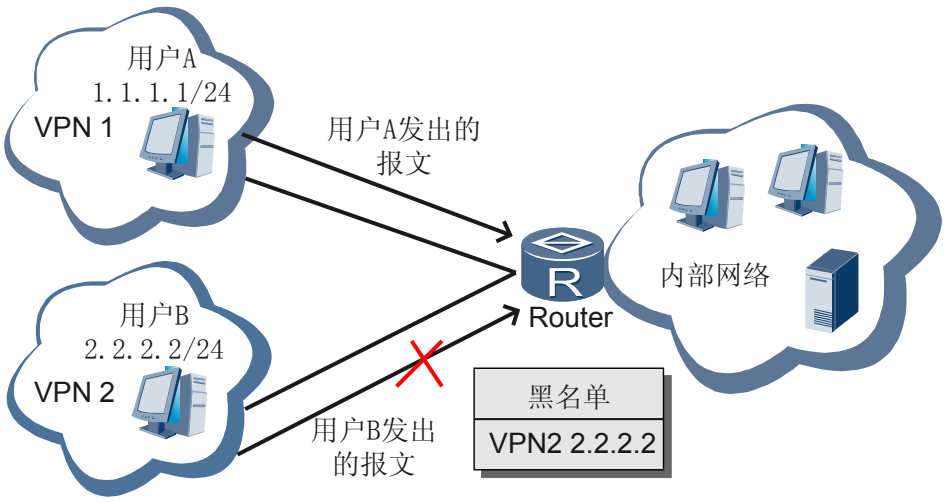
AR200-S 支持针对 FTP（File Transfer Protocol）、HTTP（Hyper Text Transport Protocol）、SIP（Session Initiation Protocol）、RTSP（Real-Time Streaming Protocol）等应用层协议实施 ASPF，支持 Java Blocking 和 ActiveX Blocking。

8.4.3 黑名单

黑名单，指根据报文的源 VPN 和源 IP 地址进行过滤的一种方式。同 ACL 相比，由于进行匹配的域非常简单，可以以很高的速度实现报文的过滤，从而有效地将特定 IP 地址发送来的报文屏蔽，同时支持用户静态配置黑名单和防火墙动态生成黑名单。

如图 8-3 所示，用户 B 的 IP 地址已经在黑名单中，从用户 B 发出的所有报文都会被防火墙丢弃。

图 8-3 黑名单



AR200-S 对黑名单的支持

除了用户可以静态配置黑名单外，当 AR200-S 发现特定 IP 地址在进行 IP 扫描攻击或端口扫描攻击时，会将发起攻击的 IP 主动插入到黑名单中。如果黑名单已使能的话，在此后的一定时间内，来自这个 IP 地址的任何报文，都可以被黑名单过滤掉。

用户可以配置静态和动态黑名单的老化时间。

无论命中了黑名单的数据包是否为 ACL 规则允许的访问，防火墙对此类数据包予以丢弃。

用户可以将黑名单配置信息导出到文件中，也可以通过文件导入黑名单配置。

8.4.4 白名单

在防火墙上加入白名单的主机不会再被加入动态和静态黑名单，使用源 VPN 和 IP 地址来表示一个白名单项。

白名单主要用在网络上的特定设备发出的合法业务报文具备 IP 扫描攻击和端口扫描攻击特性的场合，防止该特定设备被防火墙加入黑名单。

白名单只有静态的。

白名单的特点

如果用户将某个主机的 VPN 和 IP 地址加入防火墙白名单，防火墙就不会对该主机发出的报文进行 IP 扫描攻击和端口扫描攻击检查，也不会将其 IP 地址生成动态黑名单，也不允许用户将白名单主机添加到静态黑名单中。

AR200-S 对白名单的支持

当 AR200-S 收到一个报文后，就会检查是否是来自于白名单项的报文。如果是，AR200-S 对该报文就不会进行 IP 扫描攻击和端口扫描攻击检查，也不会将源 IP 生成动态黑名单，但是其他安全过滤功能，比如 ACL 包过滤、ASPF、流量统计和监控等，还是要进行，以达到防火墙的最大安全过滤效果。

用户可以配置白名单的老化时间。

用户可以将白名单配置信息导出到文件中，也可以通过文件导入白名单配置。

8.4.5 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。

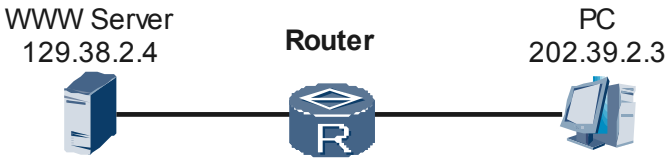
端口映射只有和 ASPF、NAT 等针对业务敏感的特性联合使用的时候才具有实际意义。例如在一个企业私网中，内部 FTP 服务器 10.10.10.10 通过 2121 端口提供 FTP 服务。用户通过 NAT 服务器访问 FTP 服务器时，只能使用 2121 做为端口号。由于默认情况下 FTP 报文的端口号是 21，这时 FTP 服务器无法将 21 端口的报文识别为 FTP 应用。在这样的场合则需要使用端口映射功能把 2121 端口映射成 FTP 协议，则 NAT 服务器就把 2121 端口的报文识别为 FTP 协议报文转发给 FTP 服务器，实现用户对 FTP 服务器的访问。

AR200-S 对端口映射的支持

AR200-S 对端口映射的支持都是通过 ACL 来实现的，只有匹配某条 ACL 的报文，才会实施端口映射。端口映射使用基本 ACL（编号 2000 ～ 2999）。端口映射在使用 ACL 过滤报文时，使用报文的目的 IP 地址去匹配基本 ACL 规则中配置的 IP 地址。

如图 8-4 所示，外部 PC 通过 AR200-S 访问内部 WWW 服务器（端口号为 8080），在外部 PC 的报文通过 AR200-S 时，命中 ACL 的报文会进行端口映射，只有目的地址是 129.38.2.4 的报文才可以通过 AR200-S 进行端口映射访问 WWW 服务器。

图 8-4 端口映射示意图



8.4.6 攻击防范

网络攻击的种类

网络攻击一般分为拒绝服务型攻击、扫描窥探攻击和畸形报文攻击三大类：

- 拒绝服务型攻击

  拒绝服务型 DoS（Denial of Service）攻击是使用大量的数据包攻击系统，使系统无法接受正常用户的请求，或者主机挂起不能正常的工作。主要 DoS 攻击有 SYN Flood、Fraggle 等。

  拒绝服务攻击和其他类型的攻击不同之处在于：攻击者并不是去寻找进入内部网络的入口，而是阻止合法用户访问资源或防火墙。

- 扫描窥探攻击

  扫描窥探攻击是利用 ping 扫描（包括 ICMP 和 TCP）来标识网络上存活着的系统，从而准确地指出潜在的目标。利用 TCP 和 UDP 等进行端口扫描，就能检测出操作系统的种类和潜在的服务种类。

  攻击者通过扫描窥探就能大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入系统做好准备。

- 畸形报文攻击

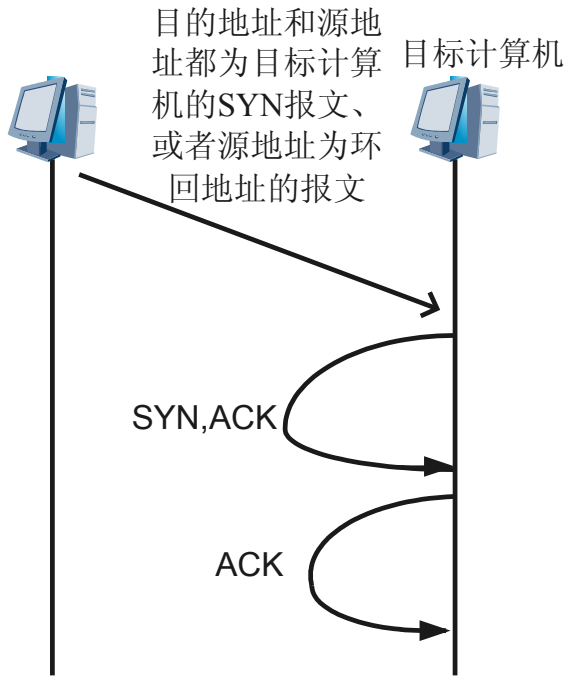
  畸形报文攻击是通过向目标系统发送有缺陷的 IP 报文，使得目标系统在处理这样的 IP 包时会出现崩溃，给目标系统带来损失。主要的畸形报文攻击有 Ping of Death、Teardrop 等。

AR200-S 对攻击防范的支持：

Land 攻击

Land 攻击，就是把 TCP 的 SYN 包的源地址和目的地址都设置为目标计算机的 IP 地址。这将导致目标计算机向它自己发送 SYN-ACK 报文，目标计算机又向自己发回 ACK 报文并创建一个空连接，每一个这样的连接都将保留直到超时。如图 8-5 所示。

图 8-5 Land 攻击示意图

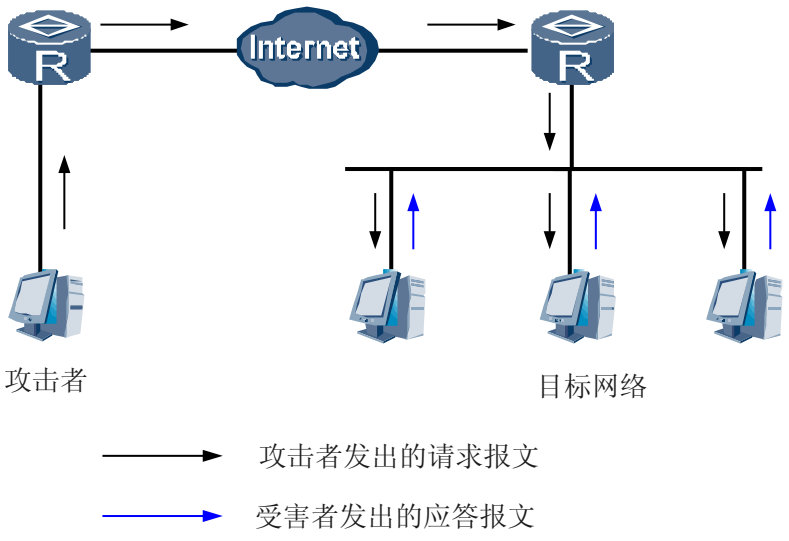


各种类型的主机对 Land 攻击反应不同，许多 UNIX 主机将崩溃，Windows NT 主机会变得极其缓慢。

Smurf 攻击

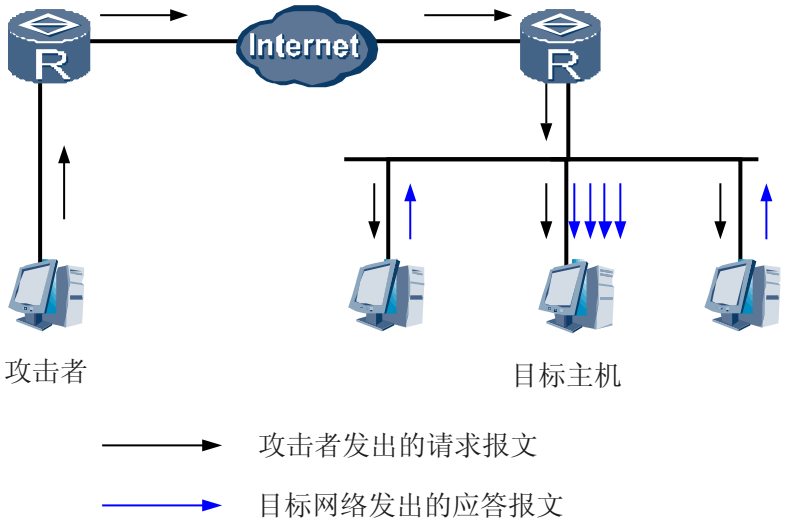
简单的 Smurf 攻击，用来攻击一个网络。攻击者向目标网络发送 ICMP 应答请求报文，该报文的目标地址设置为目标网络的广播地址，这样，目标网络的所有主机都对此 ICMP 应答请求作出答复，导致网络阻塞。如图 8-6 所示。

图 8-6 简单 Smurf 攻击示意图



高级的 Smurf 攻击，主要用来攻击目标主机。攻击者向目标主机所在的网络发送 ICMP 应答请求报文，该报文的源地址设置为目标主机的地址，这样，所有的应答报文都将发送给目标主机。最终导致目标主机处理速度缓慢，甚至崩溃。如图 8-7 所示。

图 8-7 高级 Smurf 攻击示意图



Smurf 攻击报文的发送需要一定的流量和持续时间，才能真正构成攻击。理论上讲，目标网络的主机越多，攻击的效果越明显。

WinNuke 攻击

NetBIOS 作为一种基本的网络资源访问接口，广泛的应用于文件共享，打印共享，进程间通信（IPC），以及不同操作系统之间的数据交换。一般情况下，NetBIOS 是运行在 LLC2 链路协议之上的，是一种基于组播的网络访问接口。为了在 TCP/IP 协议栈上实现 NetBIOS，RFC 规定了一系列交互标准，以及几个常用的 TCP/UDP 端口，如下。

- 139：NetBIOS 会话服务的 TCP 端口。
- 137：NetBIOS 名字服务的 UDP 端口。
- 136：NetBIOS 数据报服务的 UDP 端口。

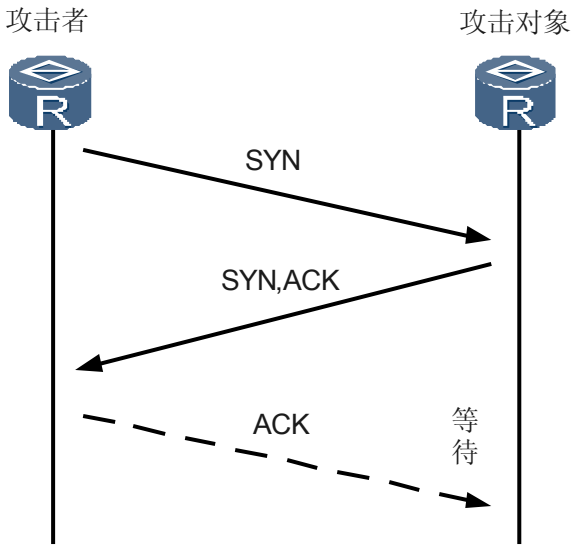
Windows 操作系统实现了 NetBIOS over TCP/IP 功能，并开放了 139 端口。

WinNuke 攻击就是利用了 Windows 操作系统的一个漏洞，向这个 139 端口发送一些携带 TCP 带外（OOB）数据报文，但这些攻击报文与正常携带 OOB 数据报文不同的是，其指针字段与数据的实际位置不符，即存在重叠，Windows 操作系统在处理这些数据的时候，就会崩溃。

SYN Flood 攻击

SYN Flood 攻击利用 TCP 三次握手的一个漏洞向目标计算机发动攻击。攻击者向目标计算机发送 TCP 连接请求（SYN 报文），然后对于目标返回的 SYN-ACK 报文不作回应。目标计算机如果没有收到攻击者的 ACK 回应，就会一直等待，形成半连接，直到连接超时才释放。如图 8-8 所示。

图 8-8 半连接示意图



攻击者利用这种方式发送大量 TCP SYN 报文，让目标计算机上生成大量的半连接，迫使其大量资源浪费在这些半连接上。目标计算机一旦资源耗尽，就会出现速度极慢、正常的用户不能接入等情况。

攻击者还可以伪造 SYN 报文，其源地址是伪造的或者不存在的地址，向目标计算机发起攻击。

ICMP Flood 攻击

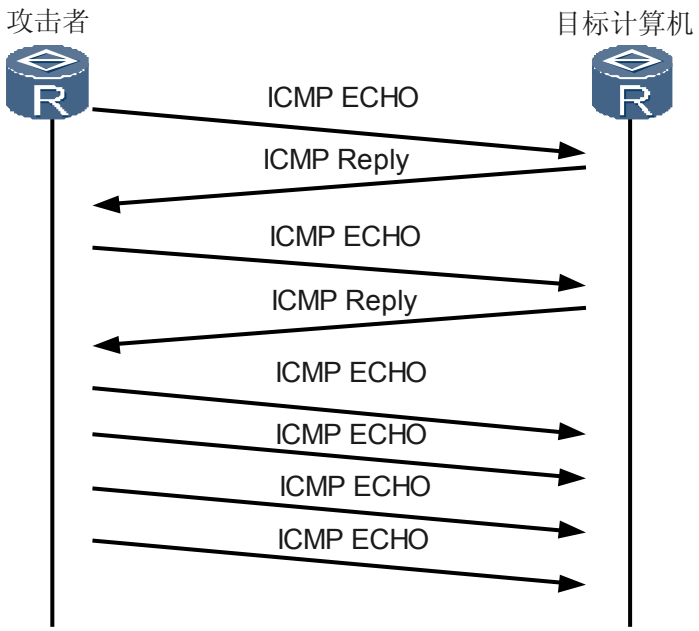
通常情况下，网络管理员会用 PING 程序对网络进行监控和故障排除，大概过程如下：

1. 源计算机向接收计算机发出 ICMP 响应请求报文（ICMP ECHO）。
2. 接收计算机接收到 ICMP 响应请求报文后，会向源计算机回应一个 ICMP 应答报文（ECHO Reply）。

这个过程是需要 CPU 处理的，在有些情况下还可能消耗掉大量的资源。

如果攻击者向目标计算机发送大量的 ICMP ECHO 报文（产生 ICMP 洪水），则目标计算机会忙于处理这些 ECHO 报文，而无法继续处理其它的数据报文。如图 8-9 所示。

图 8-9 ICMP Flood 攻击示意图



UDP Flood 攻击

UDP Flood 攻击的原理与 ICMP Flood 攻击类似，攻击者通过发送大量的 UDP 报文给目标计算机，导致目标计算机忙于处理这些 UDP 报文而无法继续处理正常的报文。

地址扫描与端口扫描攻击

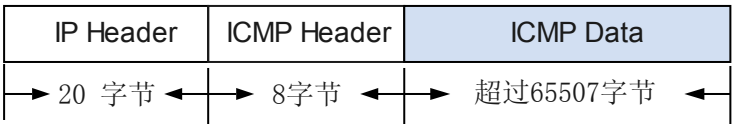
攻击者运用扫描工具探测目标地址和端口，目标地址会对这些探测作出响应，攻击者根据这些响应用来确定哪些目标系统是存活着并且连接在网络上、目标主机开放或者关闭了哪些端口。

Ping of Death 攻击

所谓 Ping of Death，就是利用一些尺寸超大的 ICMP 报文对系统进行的一种攻击。

IP 报文的长度字段为 16 位，这表明一个 IP 报文的最大长度为 65535。对于 ICMP 回应请求报文，如果数据长度大于 65507，就会使 ICMP 数据＋ IP 头长度（20）＋ ICMP 头长度（8）＞65535。对于有些防火墙或系统，在接收到一个这样的报文后，由于处理不当，会造成系统崩溃、死机或重启。如图 8-10 所示。

图 8-10 ICMP 超大报文示意图



Large-ICMP 攻击

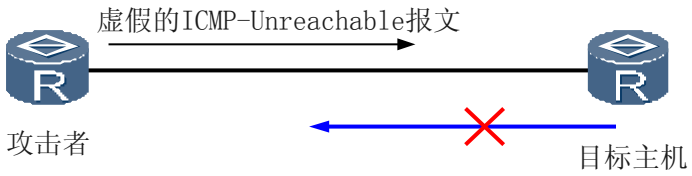
同 ping of death 类似,Large-ICMP 也是利用一些大尺寸的 ICMP 报文对系统进行的一种攻击,与 ping of death 不同的是，Large-ICMP 报文的长度不会超过 IP 报文的最大长度 65535，但是对一些操作系统也会造成破坏。

需要在防火墙上配置允许通过的 ICMP 报文的最大长度。

ICMP-Unreachable 攻击

某些系统在收到网络（报文类型字段为 3，代码字段为 0）或主机（报文类型字段为 3，代码字段为 1）不可达的 ICMP 报文后，对于后续发往此目的地的报文直接认为不可达。如图 8-11 所示。

图 8-11 ICMP-Unreachable 攻击示意图



攻击者利用这种机制，向目标主机发送虚假的 ICMP-Unreachable 报文，干扰了目标主机的路由信息，影响了报文发送。

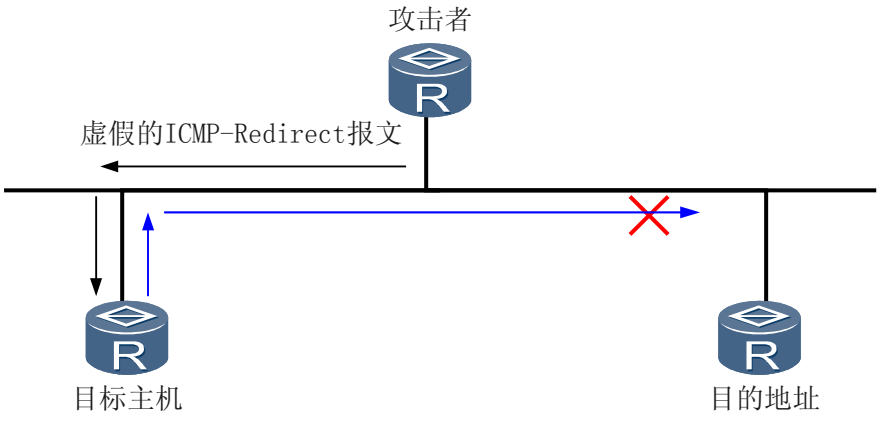
ICMP-Redirect 攻击

ICMP-Redirect 攻击和 ICMP-Unreachable 攻击类似。

网络设备可以向同一个子网的主机发送 ICMP 重定向报文，请求主机修改路由。

攻击者利用这个原理，跨越网段向另外一个网络的目标主机发送虚假的重定向报文，以改变目标主机的路由表。这种攻击干扰了目标主机的路由信息，影响了报文发送。如图 8-12 所示。

图 8-12 ICMP-Redirect 攻击示意图



IP-fragment 攻击

IP 报文中有几个字段与分片有关：DF（Don’t Fragmentate）位、MF 位、Fragment Offset、Length。

如果上述字段的值出现矛盾，而设备处理不当，会对设备造成一定的影响，甚至瘫痪。矛盾的情况有：

- DF 位被置位，而 MF 位同时被置位或 Fragment Offset 不为 0。
- DF 位为 0，而 Fragment Offset + Length > 65535。

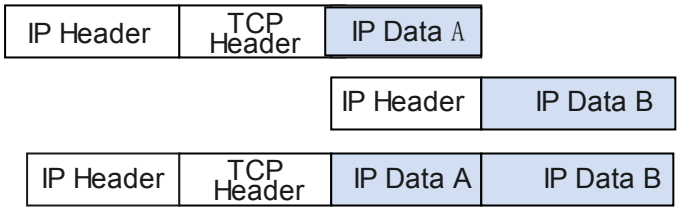
另外，由于分片报文可以增加目的设备缓冲和重组的负担，应直接丢弃目的地址为设备本身的分片报文。

Teardrop 攻击

在网络传输的过程中，如果 IP 报文的长度超过链路层的 MTU（最大传输单元），就会进行分片。在 IP 报头中有一个偏移字段（OFFSET）和一个分片标志（MF），如果 MF 标志设置为 1，则表明这个 IP 报文是一个大 IP 包的分片，其中偏移字段指出了这个片断在整个 IP 包中的位置。接收端可以根据报文头中的这些信息还原该 IP 包。

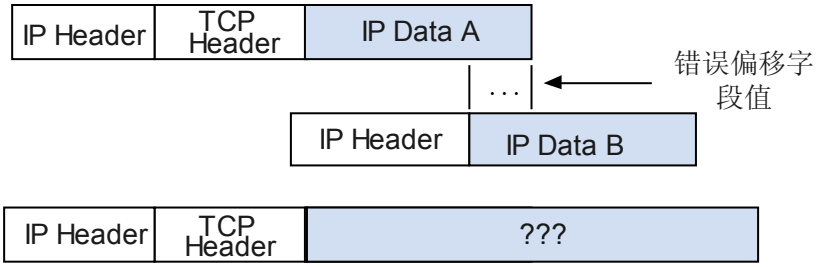
比如，一个较大的报文在 MTU 较小的链路上传输的时候，被分成了两个 IP 报文，这两个 IP 报文将在目的端进行组装，还原为原始的 IP 报文。如图 8-13 所示。

图 8-13 正常的分片组装示意图



如果一个攻击者打破这种正常情况，把偏移字段设置成不正确的值，即可能出现重合或断开的情况。某些 TCP/IP 协议栈在收到类似这种含有重叠偏移的伪造分段时会崩溃，这就是所谓的 Teardrop 攻击。如图 8-14 所示。

图 8-14 Teardrop 攻击示意图



Fraggle 攻击

Fraggle 攻击的原理与 Smurf 攻击的原理类似，不过，Fraggle 攻击发送的是 UDP 报文而非 ICMP 报文。因为发送的是 UDP 报文，Fraggle 攻击可以穿过一些阻止 ICMP 报文进入的防火墙。

Fraggle 攻击利用的原理是：UDP 端口 7（ECHO）和端口 19（Chargen）在收到 UDP 报文后，都会产生回应。如下：

- UDP 的 7 号端口收到报文后，会象 ICMP Echo Reply 一样回应收到的内容。
- UDP 的 19 号端口在收到报文后，会产生一串字符流。

这两个 UDP 端口都会产生大量应答报文，挤占网络带宽。

攻击者可以向目标主机所在的网络发送源地址为被攻击主机、而目的地址为其所在子网的广播地址或子网网络地址的 UDP 报文，目的端口号为 7（ECHO）或 19（Chargen）。子网中启用了此功能的每个系统都会向受害主机发送回应报文，从而产生大量的流量，导致受害网络的阻塞或受害主机崩溃。

如果目标主机所在网络上的主机没有启动这些功能，这些主机将产生一个 ICMP 不可达消息，仍然消耗带宽。也可将源端口改为端口 19（Chargen），目的端口为 7（ECHO），这样会自动不停地产生回应报文，其危害性更大。

Tracert 攻击

Tracert 是利用 TTL（Time To Live）为 0 时返回的 ICMP 超时报文，和达到目的地时返回的 ICMP 端口不可达报文来发现报文到达目的地所经过的路径。

攻击者可以利用 Tracert 窥探网络的结构。对网络造成潜在的危险。

畸形 TCP 报文攻击

畸形 TCP 报文是通过故意错误设置 TCP 头中的 6 个标记位，造成接收方 TCP 协议栈的处理错误，达到攻击的目的。

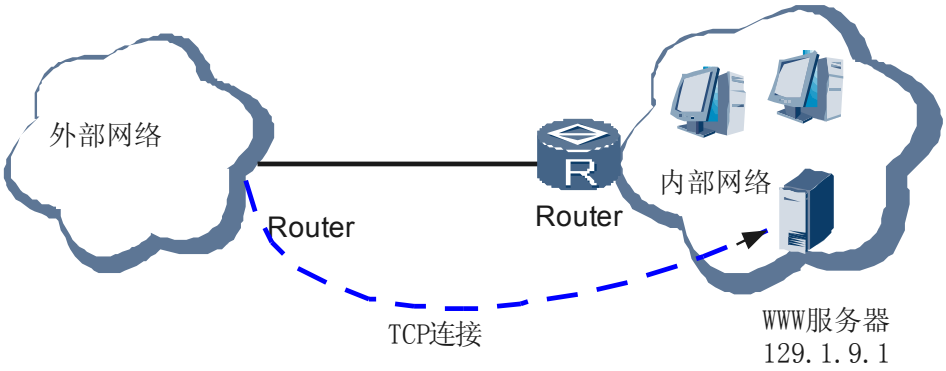
8.4.7 流量统计及监控

防火墙不仅要对数据流量进行监控，还要对内外部网络之间的连接发起情况进行检测，进行大量的统计计算与分析。防火墙的统计分析一方面可以通过专门的分析软件对日志信息进行事后分析，另一方面，防火墙系统本身可以完成一部分分析功能，具有一定的实时性。

比如，通过分析外部网络向内部网络发起的 TCP/UDP 连接数是否超过设定阈值，可以确定是否需要限制该方向发起新连接，或者限制向内部网络某一 IP 地址发起新连接。

图 8-15 是防火墙的一个典型应用示例，当启动了外部网络到内部网络的基于 IP 地址的统计分析功能时，如果外部网络对 Web 服务器 129.1.9.1 发起的 TCP 连接数超过了设定的阈值，将限制外部网络向该服务器发起新连接，直到连接数降到正常范围。

图 8-15 TCP 连接数超限示意图



AR200-S 支持的流量统计及监控方法如下。

系统级的流量统计和监控

系统级的流量统计和监控，对系统中所有启用了防火墙功能的安全域间的数据流生效，即 AR200-S 单板会统计所有安全域间的 ICMP、TCP、UDP 等连接数。当连接数超过配置阈值时，AR200-S 单板采取限制连接措施，直至连接数降至阈值以下。

系统级的流量统计功能可以针对不同的连接类型配置其阈值。例如当 TCP 的连接数上限阈值设置为 15000，下限阈值设置为 12000 时，则当所有安全域间建立的 TCP 连接总数超过 15000 时，AR200-S 单板将拒绝所有安全域间的新的 TCP 连接请求，并会产生流量告警，输出到信息中心。流量恢复到下限阈值 12000 以下时，会产生流量恢复日志，输出到信息中心。

基于安全区域的流量统计和监控

基于安全区域的流量统计和监控，对本安全区域和其他安全区域之间的数据流生效，即 AR200-S 单板会统计本安全区域和其他所有安全域间建立的 TCP、UDP 等连接总数。当本安全区域和其他所有安全域间建立的连接总数或者某个方向的连接总数超过配置的阈值时，AR200-S 单板采取限制连接数措施，直至连接数降至阈值以下。

例如当入方向 TCP 连接数阈值为 15000 时，如果本区域向其他区域发起的 TCP 连接总数超过 15000，AR200-S 单板将拒绝本区域向其他区域发起新的 TCP 连接请求。

基于 IP 地址的流量统计和监控

基于 IP 地址的流量统计和监控，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。AR200-S 单板通过分析源 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。

8.4.8 防火墙日志

防火墙可以实时记录防火墙的动作和状态（例如实施了某种防火墙措施、检测到某种网络攻击等），并将信息记录到日志中。

对日志内容的分析和归档，能够使管理员检查防火墙的安全漏洞、何时何人试图违背安全策略、网络攻击的类型，实时的日志记录还可以用来检测正在进行的入侵。

当需要对防火墙的动作和状态进行记录，以便检查防火墙的安全漏洞、检测网络攻击和入侵等，可以配置防火墙日志功能。

AR200-S 对防火墙日志的支持

AR200-S 支持以下防火墙日志：

- 黑名单日志

  AR200-S 在发现有地址扫瞄、端口扫瞄等攻击的时候，在黑名单使能的情况下会动态生成黑名单日志。

  手动加入的黑名单同样也会生成黑名单日志。

动态生成的黑名单、手动加入的静态黑名单到老化时间之后，会生成解除黑名单日志。

- 攻击日志

  设备发现各种攻击类型后，会生成攻击日志，记录攻击类型和参数。

- 流量监控日志

  当系统全局、区域出入的会话数超过所配置的连接数阈值上限时，设备会生成流量监控日志，当会话数低于所配置的连接数阈值下限时，设备会生成流量恢复日志。

- 流日志

  AR200-S 的流日志是在会话表老化的情况下，封装流日志信息，发送到日志服务器，由于流日志信息量大，流日志采用二进制格式，发送到二进制日志服务器。

黑名单日志、攻击日志、流量监控日志采用文本格式。日志生成时发送到信息中心，信息中心可以配置输出目的地为 SYSLOG 服务器、本地 CF 卡等。

8.4.9 虚拟防火墙

近年来小型私有网络不断增加，这些网络一般对应小型企业。此类用户有如下特点：

- 有较强的安全防范需求。
- 经济上无法负担一台专有安全设备。

AR200-S 支持从逻辑上划分为多台虚拟防火墙，分别为多个小型私有网络提供独立的安全保障。

每台虚拟防火墙都是 VPN（Virtual Private Network）实例（VPN-Instance）、安全实例的综合体。它能够为虚拟防火墙用户提供私有的路由转发平面、安全服务。

VPN 实例

VPN 实例为虚拟防火墙用户提供相互隔离的 VPN 路由，与虚拟防火墙一一对应。这些 VPN 路由将为各虚拟防火墙接收的报文提供路由支持。

安全实例

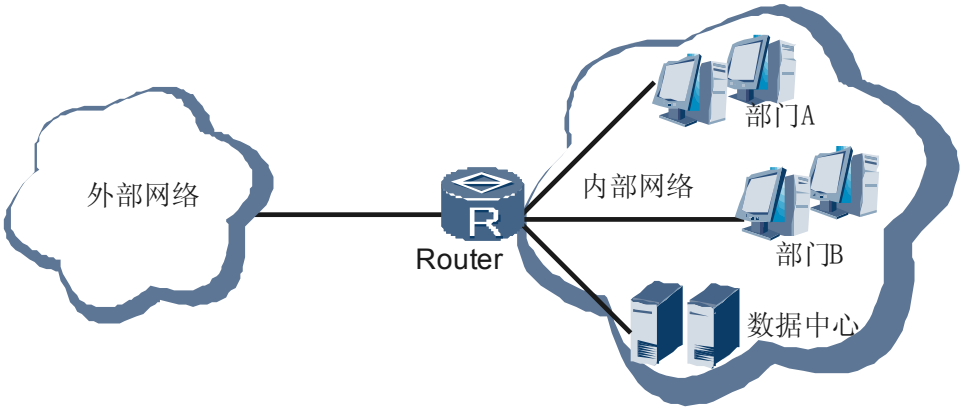
安全实例为虚拟防火墙用户提供相互隔离的安全服务，与虚拟防火墙一一对应。这些安全实例具备私有的接口、安全区域、安全域间、ACL 和 NAT 规则，并能为虚拟防火墙用户提供黑名单、包过滤、流量统计和监控、攻击防范、ASPF 和 NAT 等私有的安全服务。

8.5 应用

8.5.1 防火墙应用在内外网之间

如图 8-16 所示，防火墙用在内外网络边缘处，防止外部网络对内部网络的入侵。对于使用私有地址的内部网络，可以通过 NAT、ALG 技术和防火墙技术结合，实现更进一步的安全防护。

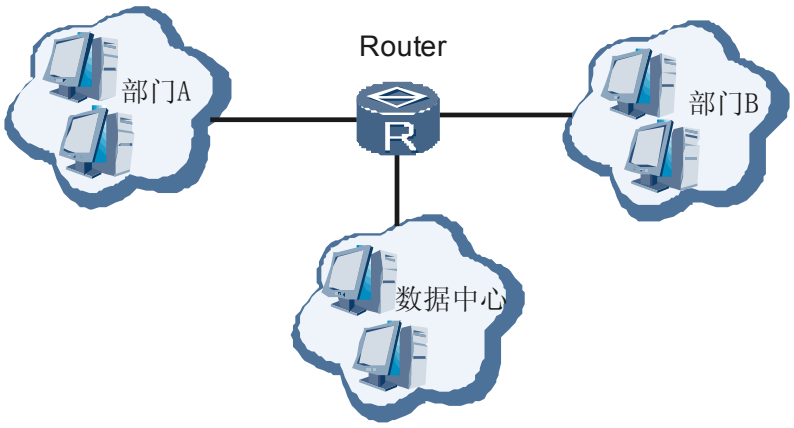
图 8-16 防火墙应用在内外网之间的示意图



8.5.2 防火墙在内部网络中的应用

如图 8-17 所示，防火墙用于内部网络中，主要是为了防止发自内部的攻击，保障重要数据的安全性。数据中心存储了大量的公司机密。这时，防火墙就需要配置严谨的策略以保护数据中心。

图 8-17 防火墙应用在内部网络的示意图



8.5.3 防火墙工作模式

为了增加防火墙组网的灵活性，AR200-S 不再定义整个设备的工作模式，而是定义接口的工作模式，接口的工作模式如下：

- 路由模式

  如果 AR200-S 接口为第三层对外连接，接口具有 IP 地址，则认为该接口工作在路由模式下。

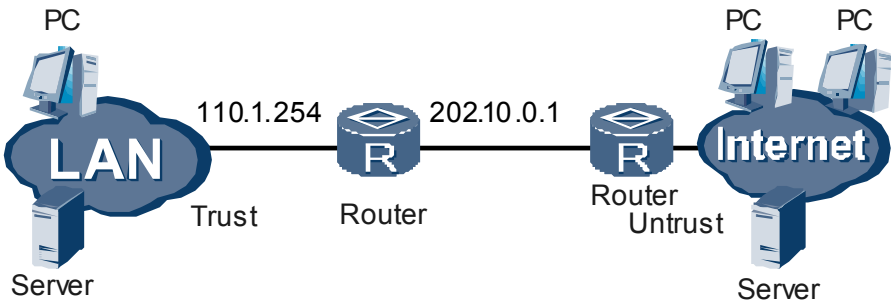
路由模式

当 AR200-S 位于内部网络和外部网络之间，同时要将其与内部网络、外部网络以及 DMZ（Demilitarized Zone）三个区域相连的接口分别配置成不同网段的 IP 地址，并重新规划原有的网络拓扑结构。此时的 AR200-S 相当于一台路由器。

如图 8-18 所示，AR200-S 的 Trust 区域接口与公司内部网络相连，Untrust 区域接口与外部网络相连。

需要注意的是，Trust 区域接口和 Untrust 区域接口分别处于两个不同的子网中。

图 8-18 路由模式组网图



采用路由模式时，可以完成 ACL（Access Control List）包过滤、ASPF 动态过滤、NAT 转换等功能。然而，路由模式需要对网络拓扑结构进行修改，例如，内部网络用户需要更改网关，路由器需要更改路由配置等。进行网络改造前，请权衡利弊。

路由模式工作过程

AR200-S 的接口工作在路由模式下时，接口需要配置 IP 地址，各接口所在的安全区域是三层区域，不同三层区域相关的接口连接的外部用户属于不同的子网。

当报文在三层区域的接口间进行转发时，根据报文的 IP 地址来查找路由表。此时 AR200-S 表现为一个路由器。但是，AR200-S 与路由器不同，AR200-S 转发的 IP 报文还需要进行过滤等相关处理，通过检查会话表或 ACL 规则以确定是否允许该报文通过。除此之外，AR200-S 还需要完成其它攻击防范检查。

8.6 术语与缩略语

术语

术语	解释
A	
ASPF	针对应用层的包过滤协议，能够检测试图通过防火墙的应用层协议会话信息，通过维护会话的状态和检查会话报文的协议和端口号等信息，阻止不符合规则的数据报文穿过防火墙。
F	
防火墙	一个或一组实施访问控制策略的系统，它监控可信任网络（相当于内部网络）和不可信任网络（相当于外部网络）之间的访问通道，以防止外部网络的危险蔓延到内部网络上。

术语	解释
非法使用	资源被未授权的用户（也可以称为非法用户）或以未授权方式（非法权限）使用。
G	
攻击防范	防火墙的一项功能，检测出多种类型的网络攻击，并能采取相应的措施保护内部网络免受恶意攻击，保证内部网络及系统的正常运行。
H	
黑名单	根据报文的源 IP 地址进行报文过滤的一种方式。
J	
拒绝服务	服务器拒绝合法用户正常访问信息或资源的请求。
S	
数据篡改	攻击者对系统数据或消息流进行有选择的修改、删除、延误、重排序及插入虚假消息等操作，而使数据的一致性被破坏。
W	
网络安全服务	针对各种安全威胁而采取的安全防护措施
X	
信息盗窃	攻击者并不直接入侵目标系统，而是通过窃听网络来获取重要数据或信息。
Y	
验证	在访问网络前或网络提供服务前来鉴别用户身份的合法性。

缩略语

缩略语	英文全称	中文全称
A		

缩略语	英文全称	中文全称
ACL	Access Control List	访问控制列表
ALG	Application Layer Gateway	应用层网关
ASPF	Application Specific Packet Filter	应用层级包过滤防火墙
D		
DoS	Deny of Service	拒绝服务
F		
FTP	File Transfer Protocol	文件传输协议
H		
HTTP	Hyper Text Transport Protocol	超文本传送协议
I		
ICMP	Internet Control Message Protocol	互联网控制报文协议
IGMP	Internet Group Management Protocol	互联网组管理协议
IP	Internet Protocol	互联网协议
M		
MAC	Media Access Control	媒体访问控制
MPLS	Multiprotocol Label Switching	多协议标签交换
N		
NetBIOS	Network Basic Input/Output System	网络基本输入输出系统
NGN	Next Generation Network	下一代网络
NMS	Network Management System	网络管理系统
P		
PC	Personal Computer	个人计算机
PDU	Protocol Data Unit	协议数据单元

缩略语	英文全称	中文全称
S		
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
T		
TCP	Transmission Control Protocol	传输控制协议
TTL	Time to Live	生存时间
U		
UDP	User Datagram Protocol	用户数据包协议
V		
VPN	Virtual Private Network	虚拟私有网
W		
WWW	World Wide Web	万维网

9 PKI

关于本章

9.1 介绍

定义

PKI（Public Key Infrastructure，公钥基础设施）是通过使用公钥技术和数字证书来提供系统信息安全服务，并负责验证数字证书持有者身份的一种体系。PKI 基础设施采用证书管理公钥，通过第三方的可信任机构认证中心，把用户的公钥和用户的其他身份信息捆绑在一起，它是一个具有通用性的安全基础设施，是一个系统或服务体系。

PKI 的功能是通过签发数字证书来绑定证书持有者的身份和相关的公开密钥，为用户获取证书、访问证书和撤销证书提供了方便的途径。同时利用数字证书及相关的各种服务（证书发布、黑名单发布等）实现通信过程中各实体的身份认证，保证了通信数据的机密性、完整性、不可否认性和认证性。

- 数据的机密性是指数据在传输过程中，不能被非授权者偷看。
- 数据的完整性是指数据在传输过程中不能被非法篡改。
- 数据的不可否认性是指发送者不能否认已发送的信息。
- 数据的认证性是指确认通信实体的真实身份。

PKI 支持在不安全的网络上传输安全信息，也支持在公司内网这样私有网络上传输信息。不仅如此，PKI 还可以被用来在用户间安全地传输密钥等等。

目的

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。作为一种基础设施，PKI 的应用范围非常广泛，并且在不断发展之中，下面给出几个常见的应用场景。

1. 虚拟专用网络（VPN，Virtual Private Network）

   VPN 是一种构建在公用通信基础设施上的专用数据通信网络，利用网络层安全协议（如 IPSec）和建立在 PKI 上的加密与数字签名技术来获得机密性保护。

2. 安全电子邮件

   电子邮件的安全也要求机密、完整、认证和不可否认，而这些都可以利用 PKI 技术来实现。目前发展很快的安全电子邮件协议 S/MIME(Secure/Multipurpose Internet Mail Extensions，安全/多用途 Internet 邮件扩充协议)，是一个允许发送加密和有签名邮件的协议。该协议的实现需要依赖于 PKI 技术。

3. Web 安全

   为了透明地解决 Web 的安全问题，在两个实体进行通信之前，先要建立 SSL（Secure Sockets Layer，安全套接字层）连接，以此实现对应用层透明的安全通信。利用 PKI 技术，SSL 协议允许在浏览器和服务器之间进行加密通信。此外，服务器端和浏览器端通信时双方可以通过数字证书确认对方的身份。

受益

- 用户受益
  - 通过 PKI 证书认证技术，用户可以验证接入设备的合法性，从而可以保证用户接入安全、合法的网络中。
  - 通过 PKI 加密技术，可以保证网络中传输的用户数据的安全性，用户数据不会被篡改和窥探。

- 通过 PKI 签名技术，可以保证用户数据的私密性，未授权的设备和用户无法查看数据。
- 通过 PKI 技术，可以在用户和网络设备之间建立安全的数据传输通道。

- 企业受益
  - 企业可以防止非法用户接入企业网络中。
  - 企业分支之间可以建立安全通道，保证企业数据的安全性。

9.2 参考标准和协议

文档	描述
PKCS#1	RSA 加密算法 V2.1(RFC 3447)
PKCS#7	加密消息语法 V1.5(RFC 2315)
PKCS#8	私钥信息语法 V1.2(RFC 5208)
PKCS#9	可选对象类和属性类型 V2.0(RFC 2985)
PKCS#10	证书请求语法说明 V1.7(RFC 2986)
PKCS#12	个人信息交换语法标准 V1.0
RFC 2511	X.509 证书请求消息格式
RFC 2560	在线证书状态协议(OCSP)
RFC 2585	PKI 操作协议：FTP 和 HTTP
RFC 3279	X.509PKI 证书和 CRL 的算法和标识
RFC 3280	X.509 证书 V3 格式和 CRL V2 格式
draft-nourse-scep-20	简单证书注册协议(SCEP)
X.208	抽象语法描述语言 ASN.1
X.209	基本编码规则 BER
X.609	可识别编码规则 DER
X.509	数字证书标准
PEM	隐私增强邮件（RFC 1421-1424）

9.3 可获得性

涉及网元

网元	描述
End Entity	终端实体，是证书的请求者，AR200-S 角色即为终端实体。
CA	证书机构，证书的颁发者。
RA	注册机构，负责审核证书请求者的身份信息。
SCEP Server	简单证书注册服务器，负责处理 SCEP 客户端的证书请求和 CRL 请求。
OCSP Server	在线证书状态协议，负责处理 OCSP 客户端的证书状态请求。
CRL Issuer	CRL 发布者，负责发布 CRL。
Cert/CRL Repository	证书和 CRL 存储库，负责证书和 CRL 的存储和查询。

License 支持

无需获得 License 许可，即可获得该特性的服务。

版本支持

表 9-1 版本支持

产品	最低支持版本
AR200-S	V200R002C00

特性依赖

不依赖其他特性。

硬件要求

对硬件无特殊要求。

9.4 原理描述

9.4.1 PKI 基本概念

对称加密算法

对称加密算法，又叫单钥加密算法，或私钥加密算法，是指加密密钥和解密密钥为同一密钥的密码算法。因此，信息的发送者和信息的接收者在进行信息的传输与处理时，必须共同持有该共享密钥。

单钥加密算法简便高效，密钥简短，破译极其困难。由于系统的保密性主要取决于密钥的安全性，所以，在公开的计算机网络上安全地传送和保管密钥是一个严峻的问题。

非对称加密算法

非对称加密算法，又叫双钥加密算法，或公钥加密算法，是指加密密钥和解密密钥为两个不同密钥的密码算法。公钥密码算法不同于单钥密码算法，它使用了一对密钥：一个用于加密信息，另一个则用于解密信息，其中加密密钥公之于众，称为公钥；解密密钥由解密人私密保存，称为私钥。用其中任一个密钥加密的信息只能用另一个密钥进行解密。

数字指纹

数字指纹是指通过某种算法对数据信息进行综合计算得到的一个固定长度的数字序列，这个序列有时也称信息摘要，常采用单向哈希算法对原始数据进行散列计算得出数字指纹。

数字签名

数字签名是指用户用自己的私钥对原始数据的数字指纹（即散列后的信息摘要）进行加密后所得的数据。即用户首先使用单向哈希算法计算出原始数据的数字指纹，然后对数字指纹进行私钥加密，生成数字签名。

信息接收者使用信息发送者的公钥对附在原始信息后的数字签名进行解密后，获得数字指纹，然后与自己对原始数据计算生成的数据指纹进行匹配，根据匹配结果，便可确定原始信息是否被篡改，这样就保证了数据传输的不可否认性。

数字信封

数字信封的功能类似于普通信封，数字信封采用密码技术保证只有指定的接收人才能阅读信息的内容。

数字信封中采用了对称密码算法和非对称密码算法。信息发送者首先利用随机产生或预先配置的对称密码加密信息，再利用接收方的公钥加密对称密码，被公钥加密后的对称密码被称之为数字信封。

信息接收方要解密信息时，必须先用自己的私钥解密数字信封，得到对称密码，然后利用对称密码解密所得到的信息，这样就保证了数据传输的真实性和不可窥探性。

数字证书

数字证书简称为证书，它是由证书机构签发的电子数据，是 PKI 技术的基础。数字证书是网络上实体的身份证明，证明某一实体身份和公钥的合法性以及实体与公钥的匹配关系。证书是公钥的载体，证书上的公钥与唯一实体身份绑定。

证书格式及证书内容遵循 X.509 标准，主要内容包括：序列号、用户公钥、用户实体信息、签证机构的信息、签证机构的签名、证书有效期等。

用来生成用户公钥信息的常用算法为：RSA、DSA、Diffie-Hellman（DH）、KEA（Key Exchange Algorithm，密钥交换算法）、ECDSA、ECDH（Elliptic Curve Diffie Hellman）等。

证书吊销列表

由于用户身份、用户信息或者用户公钥的改变、用户私钥泄漏、CA 私钥泄漏、从属关系改变或用户业务中止等原因，需要存在一种方法提前将现行的证书撤消，即撤消公钥及相关用户身份信息的绑定关系。在 PKI 中，使用的方法为 CRL（Certificate Revocation List，证书吊销列表），即证书黑名单。

通常证书具有一定的有效期，但 CA 可通过证书吊销的过程来缩短这一有效期。CA 发布一个证书吊销列表，列出被认为不能再使用的证书的序列号。CRL 指定的寿命通常比证书指定的寿命短得多。CA 也可以在 CRL 中加入证书被吊销的理由。在吊销的证书到期之后，CRL 中的有关条目被删除，以缩短 CRL 列表的大小。

任何一个证书被废除以后，证书机构 CA 就要发布 CRL 来声明该证书是无效的，并列出所有被废除证书的签发者和序列号、CRL 的签发日期、证书被撤销的日期、CRL 下次发布时间等信息。

CRL 提供了一种检验证书有效性的方式，当终端实体需要验证对端证书合法性时，通常需要检查对端证书的 CRL，判断该证书是否被撤销。

CRL 发布点

CDP（CRL Distribution Point，CRL 发布点），包含在数字证书中的信息，描述如何获取证书的 CRL 列表。最常用的 CDP 是 HTTP URL 和 LDAP URL（Lightweight Directory Access Protocol，轻量级目录访问协议），也可以是其他类型的 URL 或 LDAP 目录说明。一个 CDP 包含一个 URL 或目录说明。

证书注册

证书注册，即证书申请，就是实体向 CA 自我介绍并获取证书的过程。实体向 CA 提供身份信息，以及相应的公钥，这些信息将成为颁发给该实体证书的主要组成部分。

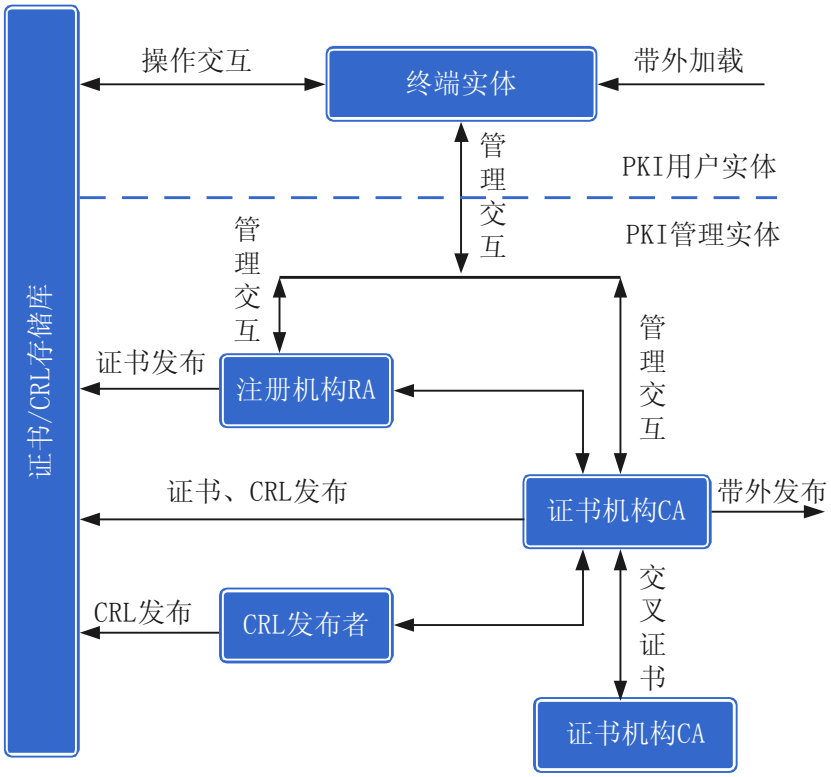
实体向 CA 提出证书申请，有离线和在线两种方式。离线申请方式下，CA 允许申请者通过带外方式（如电话、磁盘、电子邮件等）向 CA 提供申请信息。在线证书申请有手工发起和自动发起两种方式。

9.4.2 PKI 体系架构

PKI 架构

PKI 的体系架构如图 9-1。

图 9-1 PKI 体系架构



PKI 的体系架构主要由以下几个组件构成：

- PKI 实体

  PKI 包括 PKI 用户实体和 PKI 管理实体。

  - PKI 用户实体指数字证书请求者和使用者，即终端实体。
  - PKI 管理实体指数字证书的签发者和管理者，包括证书机构 CA、注册机构 RA、CRL 发布者，有时 CRL 发布者由 AA（Attribute Authority，属性机构）代理实现。

- PKI 存储库

  PKI 存储库负责证书和 CRL 的存储、管理、查询等。

- PKI 协议族

  PKI 协议族包含 PKIX（Public Key Infrastructure And X.509，X.509 和公钥基础设施）和 PKCS（Public-Key Cryptography Standards，公钥加密标准）两大协议族。

  在 IETF 的安全领域中，其中一个工作组负责公钥基础设施及 X.509 标准的制定，通常称为 PKIX 工作组。通常用 PKIX 来指代 PKI 领域的一系列标准和协议。

  PKIX 制定了 PKI 实体之间、PKI 实体与 PKI 存储库之间进行操作交互和管理交互的一系列规范和操作协议、数字证书的格式和内容、CRL 的格式和内容、PKI 使用的系列加密和签名算法、PKI 实施架构策略、PKI 存储库协议、数字证书管理协议等。

  PKCS 制定了公钥密码系统的互操作性，由 RSA 实验室与其他机构合作开发的。PKCS 涉及不断发展的 PKI 格式标准、算法和应用程序接口、描述 PKI 对象的抽象语法描述语言和基本编码规则。PKCS 标准提供了基本的数据格式定义和算法定义，它是所有 PKI 实现的基础。

其中 RSA 算法是 PKI 标准最常用的公钥算法之一，PKCS 系列标准中的 PKCS#1 定义了 RSA 加密算法标准（RSA Cryptography Specifications），该标准描述了 RSA 公钥函数的基本格式，定义数字签名，包括数字签名如何计算、待签名数据和签名本身的格式；它也描述了 RSA 公钥和私钥的语法。

- 其他协议族

  还有一些其他标准，例如 ASN.1（抽象语法描述标准）、DER 编码规则、BER 编码规则、BASE64 编码规则等，虽然不属于 PKCS 协议族，但 PKCS 协议族在描述其对象数据时使用了这些编码规则。

  其中 ASN.1（Abstract Syntax Notation One，或 X.208）定义了一系列的编码规则，用于描述对象的结构，描述了对对象进行表示、编码、传输和解码的数据格式，它是最基础的编码规则。

证书机构

- 证书机构层次

  证书机构是 PKI 体系的核心，通常采用多层次的分级结构，根据证书颁发机构的层次，可以划分为根 CA 和从属 CA。上级证书机构负责签发和管理下级证书机构的证书，最下一级的证书机构直接面向用户。每一份数字证书都与上一级的数字签名证书相关联，最终通过证书链追溯到一个根证书机构，根 CA 通常持有一个自签名证书。

  - 根 CA 是公钥体系中第一个证书颁发机构，它是信任的起源。根 CA 可以为其它 CA 颁发证书，也可以为其它计算机、用户、服务颁发证书。对大多数基于证书的应用程序来说，使用证书的认证都可以通过证书链跟踪到根。
  - 从属 CA 必须从根 CA 或者从一个已由根 CA 授权可颁发从属 CA 证书的从属 CA 处获取证书，从属 CA 可直接颁发证书。

  在建立 CA 时，从属 CA 要通过上级 CA 获得自己的 CA 证书，而根 CA 则是创建自签名的证书。

- 证书机构类型

  证书机构 CA 的类型包括以下三种：

  - 自签名 CA：在自签名 CA 中，证书中的公钥和用于验证证书签名的公钥是相同的。
  - 从属 CA：在从属 CA 中，证书中的公钥和用于验证证书签名的公钥是不同的。
  - 根 CA：根 CA 是一种特殊的 CA，它受到客户无条件地信任，位于证书层次结构的最高层。所有证书链均终止于根 CA。根 CA 必须对它自己的证书签名，因为在证书层次结构中再也没有更高的认证机构了。

- 证书机构功能

  CA 的核心功能就是发放和管理数字证书，包括：证书的颁发、证书的更新、证书的撤销、证书的查询、证书的归档、CRL 的发布等。具体描述如下：

  - 证书申请处理：接收、验证用户数字证书的申请。
  - 证书审批处理：确定是否接受用户数字证书的申请。
  - 证书颁发处理：向申请者颁发或拒绝颁发数字证书。
  - 证书更新处理：接收、处理用户的数字证书更新请求。
  - 证书查询和撤销处理：接收用户数字证书的查询、撤销。
  - 发布 CRL：产生和发布证书吊销列表（CRL）。
  - 证书的归档：数字证书的归档。
  - 密钥的备份和恢复。

- 历史数据归档。

注册机构

RA 是数字证书注册审批机构，RA 是 CA 面对用户的窗口，是 CA 的证书发放、管理功能的延伸，它负责接受用户的证书注册和吊销申请，对用户的身份信息进行审查，并决定是否向 CA 提交签发或吊销数字证书的申请。

RA 作为 CA 功能的一部分，实际应用中，通常 RA 并不一定独立存在，而是和 CA 合并在一起。当然 RA 也可以独立出来，分担 CA 的一部分功能，减轻 CA 的压力，增强 CA 系统的安全性。

9.4.3 PKI 工作原理

证书链验证

公共密钥加密的安全性依赖于人们已经知道相应私钥持有者正确的公共密钥。如果 A 错误地以为自己拿到了 B 的公共密钥，而实际上这个公共密钥属于 C，那么 A 会相信由 C 数字签名的消息实际来自 B（这得以让 C 伪装成 B）。

为验证一个用户的数字证书，需要获得签发这个用户证书的 CA 的公钥，才能检查用户证书上 CA 的私钥签名。一个 CA 可以让另一个更高层次的 CA 来证明其数字证书的合法性，这样顺着证书链，验证数字证书变成了一个叠代过程，最终这个链必须在某个“信任点”（信任点，也叫信任锚，一般是持有自签名证书的根 CA 或者是信任的中间 CA）处结束。

所谓的证书链，是从终端实体证书到根证书的一系列可信任证书构成的证书序列。任何终端实体，如果它们共享相同的根 CA 或子 CA，并且已获取 CA 证书，都可以验证对端证书。一般情况下，当验证对端证书链时，验证过程在碰到第一个可信任的证书或 CA 机构时结束。

证书链的验证过程是一个从目标证书（待验证的实体证书）到信任点证书逐层验证的循环过程。

证书注册

PKI 实体获取证书的途径和方法有多种：

- SCEP 方式（在线注册/下载方式）

  通过简单证书注册协议，利用 HTTP 协议与 CA 或 RA 通信，发送证书注册请求或证书下载请求消息，下载 CA/RA 证书、设备证书，或者申请设备证书。SCEP 方式是最常用的证书自动注册方式。

- PKCS#12/PEM/DER 方式（证书导入方式）

  通过带外方式（如 FTP、磁盘、电子邮件等）取得 PKCS#12、PEM、DER 格式的 CA/RA 证书文件、设备证书文件，然后将其文件导入本地。

- PKCS#10 方式（离线注册方式）

  当无法通过 SCEP 协议向 CA 在线申请证书时，可以使用 PKCS#10 格式打印出本地的证书申请信息。用户以 PKCS#10 格式保存证书申请信息到文件中，并通过带外方式发送给 CA 进行证书申请。

- 自签名证书

  PKI 设备为自己颁发一个自签名证书，即证书签发者和证书主题相同。

证书更新

AR200-S 在证书即将过期前，先申请一个证书作为“影子证书”，在当前证书过期后，影子证书成为当前证书，完成证书更新功能。

申请“影子证书”的过程，实质上是一个新的证书注册的过程。

证书更新功能需要 CA 服务器的支持，即 CA 服务器必须支持证书更新功能。

证书撤销

由于用户身份、用户信息或者用户公钥的改变、用户私钥泄漏或用户业务中止等原因，用户需要将自己的数字证书撤消，即撤消公钥与用户身份信息的绑定关系。在 PKI 中，CA 撤销证书使用的方法为证书吊销列表 CRL，终端实体撤销自己的证书是通过带外方式申请的。

为了撤销自己的证书，终端实体必须采用带外方式（电话、E-mail 等方式）通知 CA 服务器管理员。

管理员要求终端实体提供自己的 Challenge Password（Challenge Password 在证书注册时已作为 PKCS10 证书请求的属性发给了 CA)。

如果终端实体提供的 Challenge Password 与 CA 服务器保存的一致，CA 发布 CRL 来撤销证书。

证书状态检查

当终端实体验证对端证书时，经常需要检查对端证书是否有效，例如对端证书是否过期、是否被加入证书黑名单中，即检查证书的状态。通常终端实体检查证书状态的方式有三种：CRL 方式、OCSP 方式、None 方式。

- CRL 方式

  如果 CA 支持 CDP，那么当 CA 签发证书时，在证书中会包含 CDP（CRL distribution point）信息，描述了获取该证书 CRL 的途径和方式。终端实体利用 CDP 中指定的机制和地址来定位和下载 CRL。

  如果 PKI 域下配置了 CDP 的 URL 地址，该地址将覆盖证书中携带的 CDP 信息，终端实体使用配置的 URL 来获取 CRL。

  - 如果证书中包含 CDP 或者本地配置了 CDP，那么该证书的 CRL 必须通过 CDP 中指定的机制获取。
  - 如果 CA 不支持 CDP，本地又没有配置 CDP 的 URL 地址，那么 AR200-S 使用 SCEP 协议获取 CRL。

    SCEP 消息中包含证书发布者名字和证书序列号。虽然 SCEP 方式是获取 CRL 的缺省方式，但对于大批量 CRL 的获取推荐使用 HTTP 方式。
- OCSP（Online Certificate Status Protocol，在线证书状态协议）方式

  如果 CA 不支持 CDP，即证书中没有指定 CDP，并且 PKI 域下也没有配置 CRL 的 URL 地址，终端实体可以使用 OCSP 协议检查证书状态。
- None 方式

  如果终端实体没有可用的 CRL 和 OCSP 服务器，或者不需要检查对端证书状态，可以采用 None 方式，即不检查证书是否被撤销。

证书验证

终端实体获取对端证书后，当需要对对端进行证书认证时，例如需要与对端建立安全隧道或安全连接，通常需要验证对端证书的合法性。如果证书签发者的证书无效或过期，

则由该 CA 签发的所有证书都不再有效。但在 CA 证书过期前，设备会自动更新 CA/RA 证书，异常情况下才会出现 CA 证书过期现象。

为完成证书验证，除了需要对端证书外，本地设备需要下面的信息：信任的 CA 证书、CRL、本端数字证书及其私钥、证书认证相关配置信息。

证书验证的主要过程如下：

1. 使用 CA 证书的公钥验证证书机构的签名是否正确。
2. 根据证书的有效期，验证证书是否过期。
3. 检查证书的状态，即通过 CRL、OCSP、None 等方式检查证书是否被撤销。
4. 检查证书是否符合本地的 CA 策略。

证书下载

证书下载是指终端实体通过 SCEP 协议，向 CA 服务器查询并下载已颁发的证书，或者通过 CDP 指定机制和地址，下载已颁发的证书。该证书可以是自己的证书，也可以是 CA 证书，或其他终端实体的证书。

CRL 下载

CA/RA 不会主动把 CRL 发布给终端实体，而是由终端实体主动发起 CRL 查询。有两种下载 CRL 的方法：CDP 方式、SCEP 方式。

CA 如果支持 CDP，在为终端实体颁发证书时，把 CRL 发布点的 URL 地址编码成 CDP 属性封装在证书中，终端实体根据 CDP 来下载 CRL。

如果证书中未携带 CDP 信息，并且设备本地也没有配置 CDP 的 URL 地址，则设备通过 SCEP 协议向 CA 服务器请求 CRL。终端实体通过 SCEP 协议获取证书时，以证书签发者名字和证书序列号作为查询关键字。

9.4.4 RSA 密钥对

概述

RSA 公钥算法是 70 年代末，由美国斯坦福大学几位学者发明的，以他们的名字(Rivest、Shamir、Adelman)命名为 RSA 算法。RSA 算法既能用于数据加密，又能用于数字签名。

RSA 密钥对包括一个 RSA 公钥和一个 RSA 私钥，当终端主机 A 申请证书时，证书请求中必须包含公钥信息。当终端主机 A 被授予证书后，证书中已包含了公钥信息，对端主机 B 可以使用终端主机 A 的公钥加密发送给终端主机 A 的信息。私钥由终端主机 A 自己保存，用来解密对端主机 B 发送过来的数据、或对自己发送的数据进行数字签名。

RSA 密钥对的模数，即 RSA 密钥的长度（单位 bit）。模数越大，密钥越安全，当然生成密钥、加密、解密花费的时间也越长。

私钥保护

私钥由用户私密保存，常用来进行数字签名，如果私钥泄漏或被人获取，攻击者就可以冒充他人身份，与其他设备建立安全连接，给网络带来安全隐患。

为了保护私钥，设备提供私钥加密功能，生成的私钥不在内存中保存，进行 3DES 加密后以文件形式保存，使用时再从文件中读取。

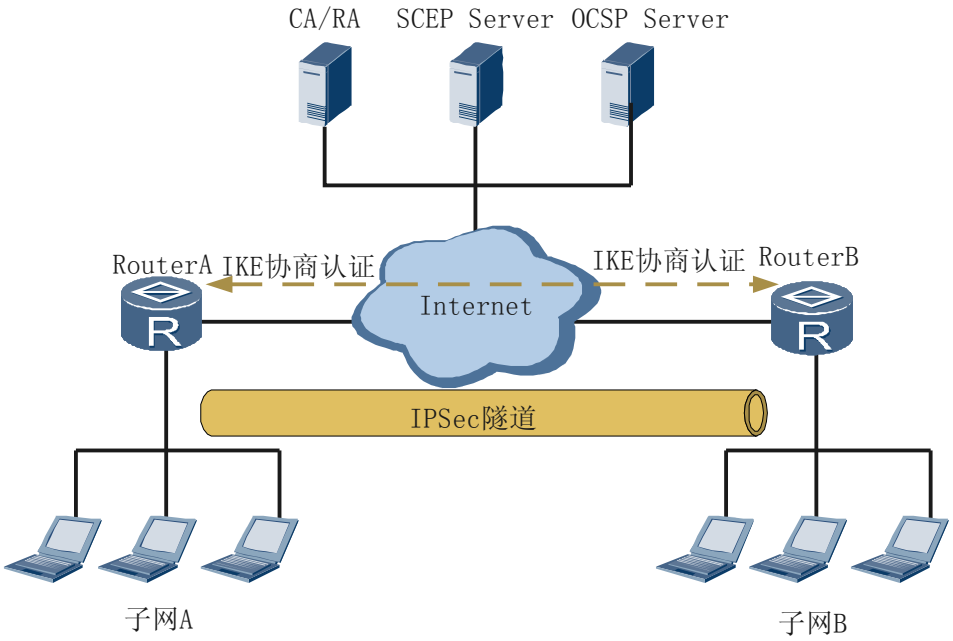
私钥加密是指使用对称加密算法 3DES 进行加密和解密，加密后的私钥仍然可以使用建立新的安全连接。

9.5 应用

9.5.1 IPSec VPN 应用

IPSec VPN 应用组网如图 9-2 所示。

图 9-2 IPSec VPN 应用组网图



子网 A 和子网 B 内的用户通过公网进行相互通信，AR200-S 作为网络 A 和 B 的出口网关。因为公网是不安全的网络，为了保护用户数据的安全性，AR200-S 采用 IPSec 技术，与对端设备建立 IPSec 通道，保护用户数据的安全性。

IPSec 通道使用的 SA（Security Association，安全联盟），可以手工配置，或者使用 IKE 协议进行动态协商。为了简化 IPSec 的使用和管理，通过 IKE（Internet Key Exchange，因特网密钥交换协议）为 IPSec 提供自动协商交换密钥、建立和维护安全联盟的服务。

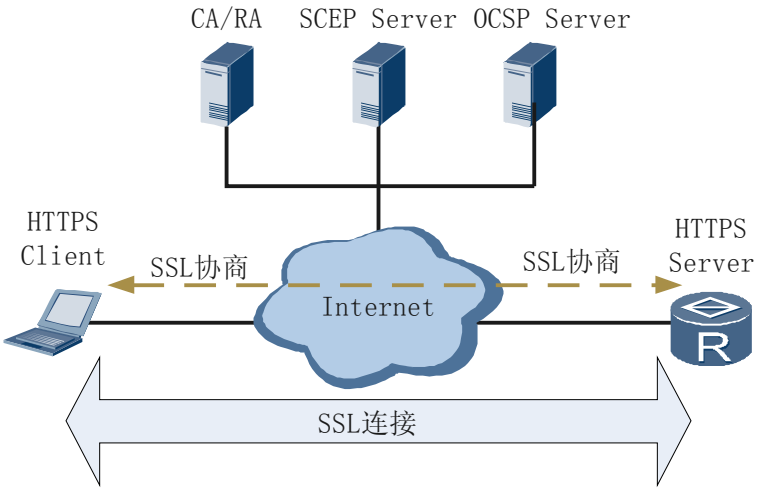
IKE 为了保证在不安全的网络上安全地分发密钥、建立 IPSec SA，需要对通信双方进行身份认证，IKE 通过协议交互，相互交换双方的数字证书，并验证证书合法性，即利用基于 PKI 的数字证书认证完成 IPSec 隧道的建立。

IPSec 在进行 IKE 协商过程，IKE 对等体之间需要互相交换和验证双方的证书，其中证书申请、证书更新和证书验证功能由 PKI 特性完成。

9.5.2 SSL 应用

SSL 组网应用如图 9-3 所示。

图 9-3 SSL 应用组网图



SSL（Secure Sockets Layer，安全套接层）是一个安全协议，为基于 TCP 的应用层协议提供安全连接，如 SSL 可以为 HTTP 协议提供安全连接。SSL 协议广泛应用于电子商务、网上银行等领域，为网络上数据的传输提供安全性保证。

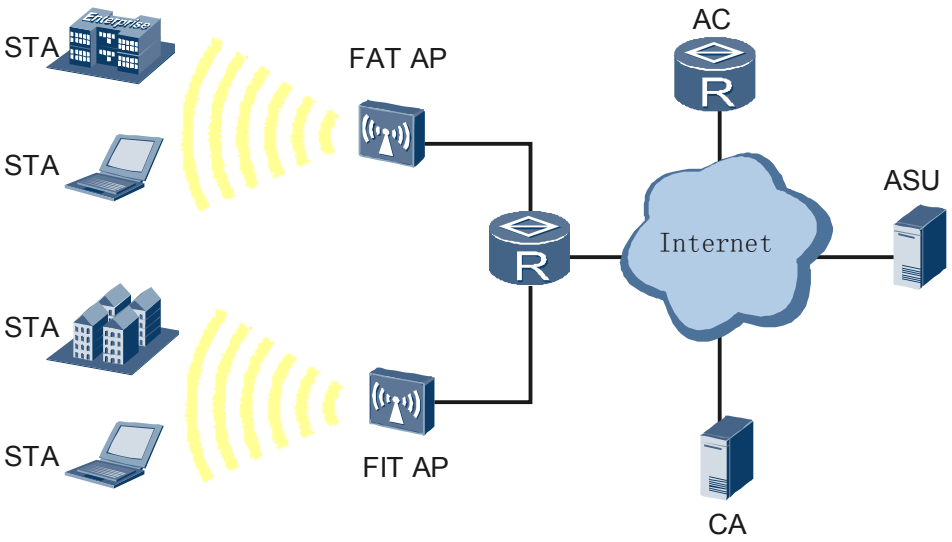
SSL 在建立安全连接的过程中，需要完成基于证书的身份认证和对称密钥协商过程。

SSL 在连接建立的过程中，HTTPS 客户端和 HTTPS 服务器可能需要互相交换和验证双方的证书，其中证书申请、证书更新和证书验证功能由 PKI 特性完成。

9.5.3 WAPI 应用

WAPI 组网应用如图 9-4 所示。

图 9-4 WAPI 应用组网图



WLAN 用户 STA 通过 WAPI-CERT 方式进行 WLAN 认证接入网络中，认证服务器为 ASU，CA 为证书机构，一般情况下 ASU 和 CA 合二为一。

WAPI-CERT 认证，是基于证书的双向认证方式，它是基于 WLAN 用户和 WLAN 设备双方的证书所进行的认证。认证前 WLAN 用户和 WLAN 设备必须预先拥有各自的证书，然后通过 ASU（Authentication Service Unit：鉴别服务单元）对双方的身份进行认证。

WLAN 设备本身不需要验证证书，它只需要将 WLAN 设备和 STA 的证书通过 WAPI 协议报文发送给 ASU，由 ASU 服务器负责验证证书。

WAPI 应用需要的证书加载功能，即从设备存储器中读取证书文件并加载到内存中的功能由 PKI 特性完成。

9.6 术语与缩略语

缩略语	英文名	中文解释
ASN	Abstract Syntax Notation One	抽象语法描述语言
BER	Basic Encoding Rules	基本编码规则
CA	Certificate Authority	证书机构
CDP	CRL Distribution Point	证书发布点
CRL	Certificate Revocation List	证书吊销列表
DER	Distinguished Encoding Rules	可识别编码规则
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
OCSP	Online Certificate Status Protocol	在线证书状态协议
PKCS	Public-Key Cryptography Standards	公钥加密标准
PKI	Public Key Infrastructure	公钥基础设施
PKIX	Public Key Infrastructure And X.509	X.509 和公钥基础设施
RSA	Rivest、Shamir、Adelman	一种加密算法
RA	Registration Authority	注册机构
SCEP	Simple Certificate Enrollment Protocol	简单证书注册协议