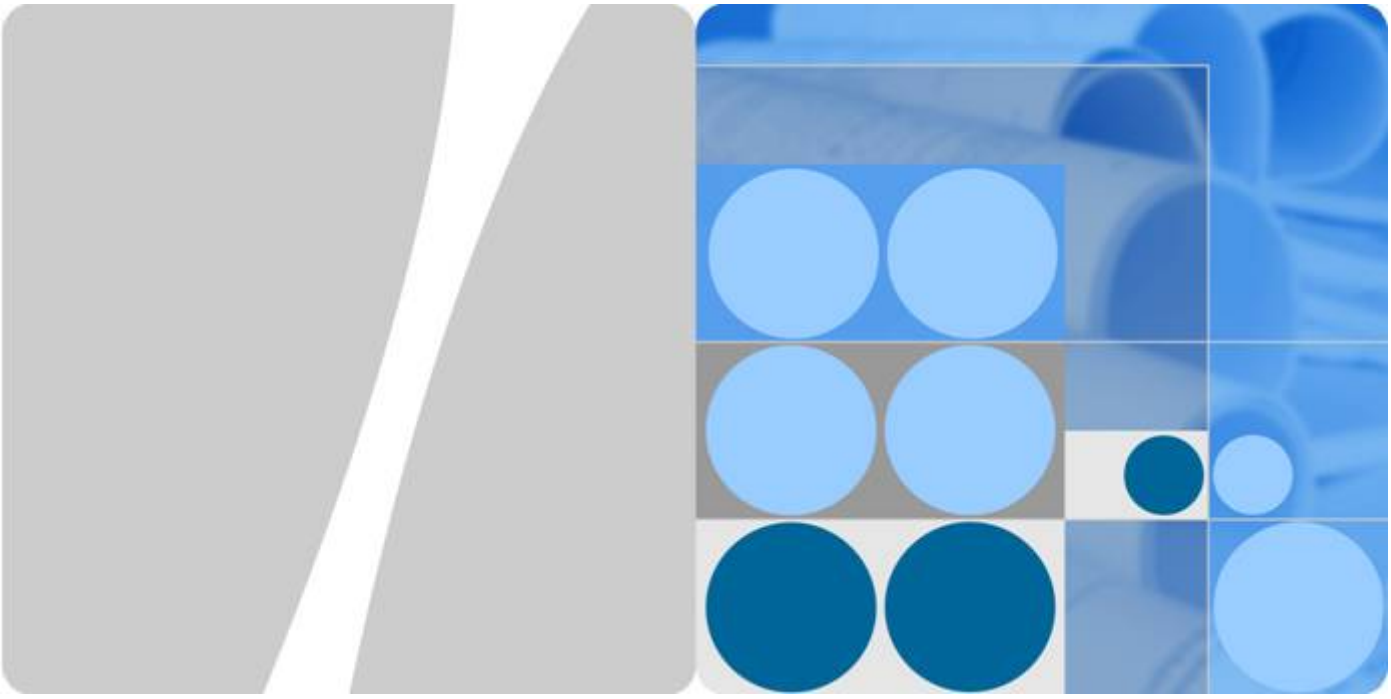


Huawei AR1200 系列企业路由器

V200R002C01

配置指南-安全

文档版本　01

发布日期　2012-04-20

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

本文档介绍了 AR1200 中的安全特性基本概念、在不同应用场景中的配置过程和配置举例。

本文档提供了安全特性的配置方法。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 网络监控工程师
- 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。

接口编号约定

本手册中出现的接口编号仅作示例，并不代表设备上实际具有此编号的接口，实际使用中请以设备上存在的接口编号为准。

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 (2012-04-20)

第一次正式发布。

目 录

1 AAA 配置

关于本章

通过配置认证、授权、计费，可以判断接入用户是否合法并下发相应的权限，保证网络的安全。

1.1 AAA 概述
AAA 是 Authentication（认证）、Authorization（授权）和 Accounting（计费）的简称，提供了认证、授权、计费三种安全功能。

1.2 AR1200 支持的 AAA 特性
AR1200 支持通过 RADIUS 协议和 HWTACACS 协议进行认证、授权、计费，还支持本地认证和授权。

1.3 配置采用本地方式进行认证和授权
配置采用本地方式进行认证和授权后，AR1200 根据本地的用户信息对接入用户进行认证和授权。

1.4 配置采用 RADIUS 方式进行认证、授权和计费
AAA 可以用多种协议来实现，但最常用的是 RADIUS 协议。RADIUS（Remote Authentication Dial-In User Service）是一种客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。

1.5 配置采用 HWTACACS 方式进行认证、授权、计费
HWTACACS 协议与 RADIUS 协议类似，主要是通过客户端/服务器模式与 HWTACACS 服务器通信来实现对接入用户进行认证、授权和计费。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。

1.6 维护 AAA
清除统计信息。

1.7 配置举例
通过示例介绍如何配置 AAA。配置示例中包括组网需求、配置注意事项、配置思路等。

1.1 AAA 概述

AAA 是 Authentication（认证）、Authorization（授权）和 Accounting（计费）的简称，提供了认证、授权、计费三种安全功能。

AAA 提供的安全功能

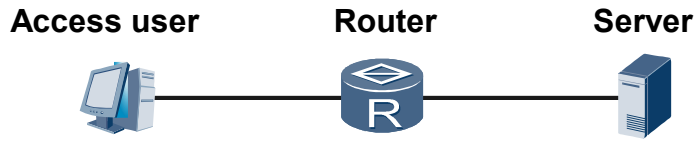
- 认证：确认用户的身份，判断用户是否为合法用户。
- 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。
- 计费：记录用户使用网络服务中的所有操作，包括使用的服务类型、起始时间、数据流量等。

用户可以使用一种或多种安全服务。例如，公司仅仅要求在员工访问某些特定资源的时候进行身份认证，那么只需要配置认证服务器。如果还需要对员工使用网络的情况进行记录，那么还需要配置计费服务器。

AAA 的基本构架

AAA 通常采用“客户端-服务器”结构，如图 1-1 所示。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。

图 1-1 AAA 的基本构架示意图



当用户需要通过 Router 访问网络前，需要先获得访问网络的权限，Router 起到验证用户的作用。Router 负责把用户的认证、授权、计费信息发送给 AAA Server。

1.2 AR1200 支持的 AAA 特性

AR1200 支持通过 RADIUS 协议和 HWTACACS 协议进行认证、授权、计费，还支持本地认证和授权。

RADIUS 方式进行认证、授权、计费

RADIUS 是客户端/服务器结构的信息交互协议，能保护网络不受未授权用户访问的干扰，常应用在既要求较高安全性又要求控制远程用户访问权限的网络环境中。

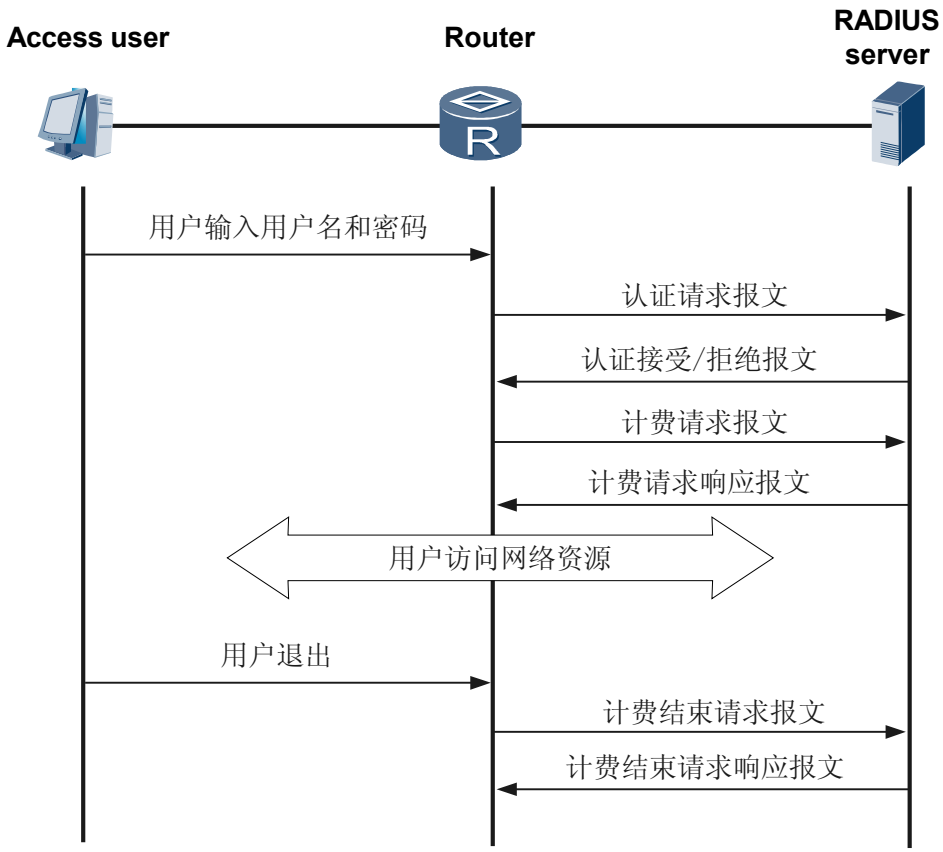
RADIUS 协议采用 UDP 报文来承载数据，通过定时器管理机制、重传机制、备用服务器机制，确保 RADIUS 服务器和客户端之间交互消息正确收发。RADIUS 协议中认证和授权绑定在一起，即认证响应报文中携带了授权信息。

说明

在管理用户采用 RADIUS 方式进行认证时，需检查用户的接入类型是否与 RADIUS 接受报文中下发的属性一致，如果不一致，则返回认证失败。

用户、AR1200 和 RADIUS 服务器之间的交互流程如图 1-2 所示。

图 1-2 RADIUS 方式进行认证、授权、计费的基本交互流程



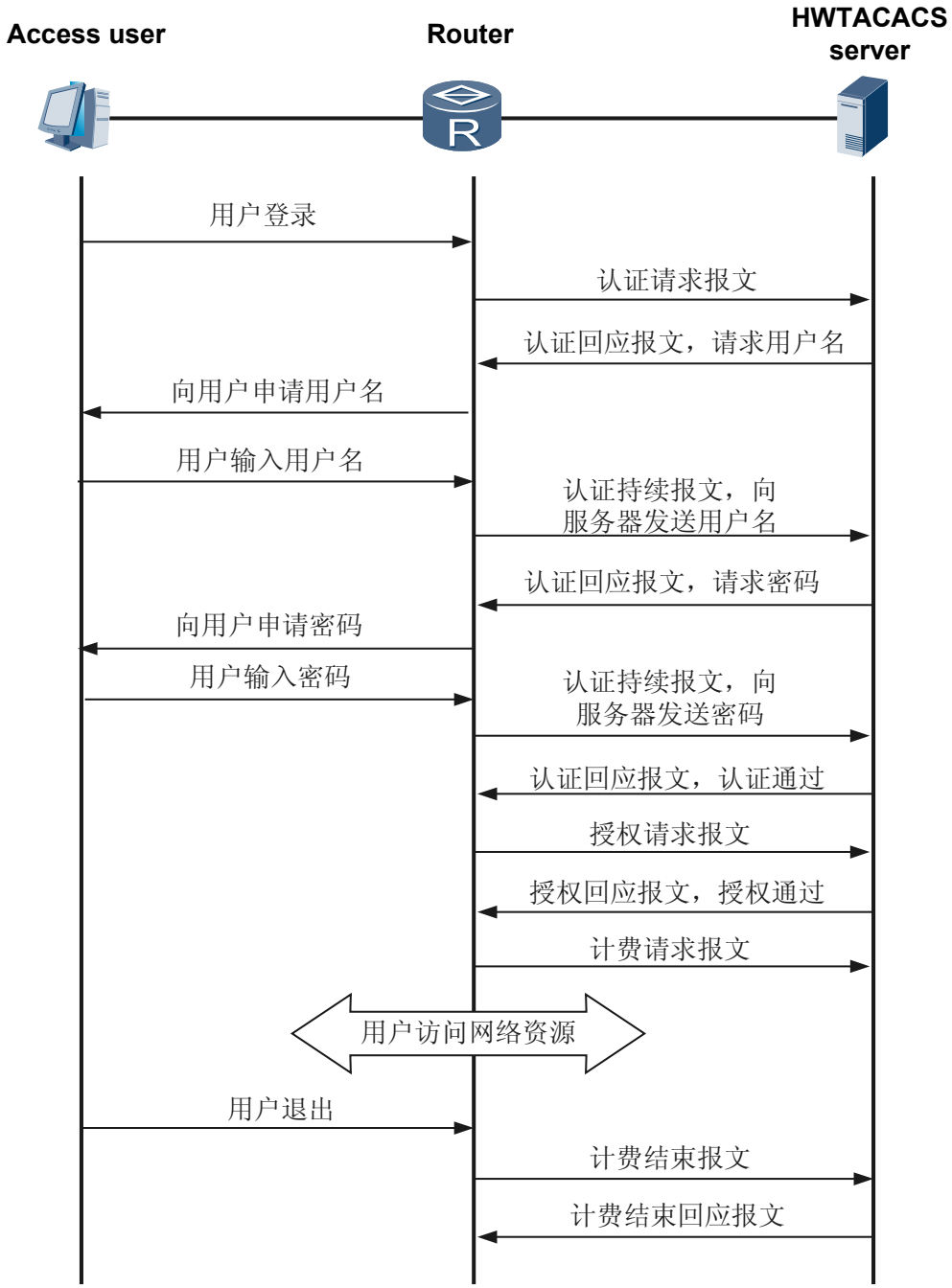
1. 用户发起连接请求，向 AR1200 发送用户名和密码。
2. AR1200 向 RADIUS 服务器发送认证请求报文，其中包含用户的用户名和密码。
3. RADIUS 服务器对用户名和密码进行认证。如果认证成功，RADIUS 服务器向 AR1200 发送认证接受报文；如果认证失败，则返回认证拒绝报文。由于 RADIUS 协议合并了认证和授权的过程，因此认证接受报文中也包含了用户的授权信息。
4. AR1200 根据接收到的认证结果接入/拒绝用户。如果允许用户接入，则 AR1200 向 RADIUS 服务器发送计费开始请求报文。
5. RADIUS 服务器返回计费开始响应报文，并开始计费。
6. 用户开始访问网络资源。
7. 用户请求断开连接，AR1200 向 RADIUS 服务器发送计费停止请求报文。
8. RADIUS 服务器返回计费结束响应报文，并停止计费。

HWTACACS 方式进行认证、授权、计费

HWTACACS 是在 TACACS 协议基础上进行了功能增强的安全协议。HWTACACS 协议与 RADIUS 协议类似，主要是通过客户端/服务器模式与 TACACS 服务器通信来实现对接入用户进行认证、授权和计费。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。

以 Telnet 用户为例，用户、AR1200 和 HWTACACS 服务器之间的交互流程如图 1-3 所示。

图 1-3 HWTACACS 方式进行认证、授权、计费的基本交互流程



1. Telnet 用户请求登录设备。
2. AR1200 收到请求之后，向 HWTACACS 服务器发送认证请求报文。
3. HWTACACS 服务器发送认证回应报文，请求用户名。
4. AR1200 收到回应报文后，向用户询问用户名。
5. 用户输入用户名。
6. AR1200 收到用户名后，向 HWTACACS 服务器发送认证持续报文，其中包括了用户名。
7. HWTACACS 服务器发送认证回应报文，请求登录密码。

8. AR1200 收到回应报文，向用户询问登录密码。
9. 用户输入密码。
10. AR1200 收到密码后，向 HWTACACS 服务器发送认证持续报文，其中包括了密码。
11. HWTACACS 服务器发送认证回应报文，指示用户通过认证。
12. AR1200 向 HWTACACS 服务器发送授权请求报文。
13. HWTACACS 服务器发送授权回应报文，指示用户通过授权。
14. AR1200 收到授权回应成功报文。
15. AR1200 向 HWTACACS 服务器发送计费开始报文。
16. HWTACACS 服务器发送计费回应报文，并且开始计费。
17. 用户开始访问网络资源。
18. 用户请求断开连接，AR1200 向 HWTACACS 服务器发送计费结束报文。
19. HWTACACS 服务器发送计费结束报文，并停止计费。

本地方式进行认证和授权

在本地方式进行认证和授权中，用户信息（包括本地用户的用户名、密码和各种属性）都配置在 AR1200 上。本地方式进行认证和授权的优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。

通常使用本地方式对管理员进行认证和授权。此外，本地认证还常用于 RADIUS 认证和 HWTACACS 认证的备份认证方式，本地授权作为 HWTACACS 授权的备份授权方式。

1.3 配置采用本地方式进行认证和授权

配置采用本地方式进行认证和授权后，AR1200 根据本地的用户信息对接入用户进行认证和授权。

1.3.1 建立配置任务

在配置本地认证和授权前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

如果需要对用户进行认证或授权，但是在网络中没有部署 RADIUS 服务器和 HWTACACS 服务器，那么可以采用本地方式进行认证和授权。本地方式进行认证和授权的优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。

通常使用本地方式对管理员进行认证和授权。本地认证还常用于 RADIUS 认证和 HWTACACS 认证的备份认证方案，本地授权作为 HWTACACS 授权的备份授权方案。

前置任务

在配置本地方式进行认证和授权之前，需完成以下任务：

- 配置接口的物理属性，使接口的物理层状态为 Up。

数据准备

在配置本地用户管理之前，需要准备以下数据。

序号	数据
1	用户名、用户口令
2	（可选）本地用户的优先级别
3	（可选）本地用户的接入类型
4	（可选）本地用户的 FTP 目录名
5	（可选）本地用户的状态
6	（可选）本地用户的接入限制数量
7	认证方案的名称
8	授权方案的名称
9	域的名称

1.3.2 配置本地用户

当采用本地方式进行认证和授权时，需要在 AR1200 上配置用户的认证和授权信息，如用户名、密码、优先级等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **local-user** *user-name* **password** *password*，创建本地用户帐号，并配置本地用户的密码。

说明

如果用户名中带域名分割符（如“@”、“|”、“%”等符号），则认为分割符前面的部分是用户名，后面部分是域名。如果没有分割符，则整个字符串为用户名，默认到 **default** 域认证。

步骤 4 （可选）执行命令 **local-user** *user-name* **privilege level** *level*，配置本地用户的优先级。

缺省情况下，本地用户的优先级由管理模块来决定，例如在用户界面视图下有用户级别的配置，如果没有配置，则为 0 级用户。

步骤 5 （可选）执行命令 **local-user** *user-name* **idle-timeout** *minutes* [*seconds*]，配置指定用户的闲置切断时间。

步骤 6 （可选）执行命令 **local-user** *user-name* **service-type** { **8021x** | **bind** | **ftp** | **http** | **l2tp** | **ppp** | **ssh** | **telnet** | **terminal** | **web** | **x25-pad** } *，配置允许本地用户的接入类型。

缺省情况下，不限制本地用户的接入类型。

步骤 7 （可选）执行命令 **local-user** *user-name* **ftp-directory** *directory*，配置允许 FTP 用户访问的 FTP 目录。

缺省情况下，允许 FTP 用户访问的 FTP 目录为空。

当 AR1200 作为 FTP 服务器时，必须配置允许 FTP 用户访问的 FTP 目录，否则 FTP 用户无法访问 AR1200。

步骤 8 （可选）执行命令 **local-user** *user-name* **state** { **active** | **block** }，配置本地用户的状态。

缺省情况下，本地用户的状态为激活态。

AR1200 对处于激活态和阻塞态用户的处理方式如下：

- 若用户状态为激活态，将接收该用户的认证请求并做进一步处理。
- 若用户状态为阻塞态，将拒绝该用户的认证请求。

步骤 9 （可选）执行命令 **local-user** *user-name* **access-limit** *max-number*，配置指定用户名可建立的连接数目。

缺省情况下，不限制用户可建立的连接数目。

----结束

1.3.3 配置认证和授权方案

如果需要采用本地方式进行认证和授权，需要在认证方案中配置认证模式为本地认证，在授权方案中配置授权模式为本地授权。

背景信息

缺省情况下，AR1200 对用户进行本地认证和授权。

说明

AR1200 不支持本地计费。

操作步骤

- 配置认证方案
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **aaa**，进入 AAA 视图。
  3. 执行命令 **authentication-scheme** *authentication-scheme-name*，创建一个认证方案，并进入认证方案视图或直接进入一个已存在的认证方案视图。

     缺省情况下，AR1200 中有一个认证方案，认证方案名称是 **default**，不能删除，只能修改。
  4. 执行命令 **authentication-mode local**，配置认证模式为本地认证。
  5. (可选)执行命令 **authentication-super** { **hwtacacs** | **super** } * [**none**],在当前认证模板下，配置对用户提升级别进行认证时采用的认证模式。
  6. (可选)执行命令 **quit**，返回 AAA 视图。
  7. (可选)执行命令 **domainname-parse-direction** { **left-to-right** | **right-to-left** }，配置用户名和域名解析的方向，从左向右或从右向左。
- 配置授权方案
  1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **aaa**，进入 AAA 视图。
3. 执行命令 **authorization-scheme** *authorization-scheme-name*，创建授权方案，并进入授权方案视图或直接进入一个已存在的授权方案视图。

   缺省情况下，AR1200 有一个授权方案，授权方案配置名是 **default**，不能删除，只能修改。
4. 执行命令 **authorization-mode local** [**none**]配置授权模式。

----结束

1.3.4 配置域

创建的认证和授权方案，只有在域下应用后才能生效。

背景信息

在配置域之前，需要配置完成认证方案和授权方案。

采用本地方式进行认证和授权时，采用缺省的计费方案，即不计费。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，创建域并进入域视图或进入一个已存在的域视图。

缺省情况下，AR1200 存在两个域：“default”和“default_admin”。“default”用于普通接入用户的域，“default_admin”用于管理员的域。

步骤 4 执行命令 **authentication-scheme** *authentication-scheme-name*，配置域的认证方案。

缺省情况下，域使用配置名为 default 的认证方案。

步骤 5 执行命令 **authorization-scheme** *authorization-scheme-name*，配置域的授权方案。

缺省情况下，域下没有绑定授权方案。

步骤 6（可选）执行命令 **state** { **active** | **block** }，配置域的状态。

当域处于阻塞态时，属于该域的用户不能登录。缺省情况下，域创建后处于激活状态。

步骤 7 执行命令 **quit**，退出域视图。

步骤 8（可选）执行命令 **domain-name-delimiter** *delimiter*，配置域名分隔符。

域名分隔符可以是 \ / : < > | @ ' % 中的某一个。

缺省情况下，域名分隔符为@。

----结束

1.3.5 检查配置结果

前提条件

已完成域的配置。

操作步骤

- 使用命令 **display aaa configuration** 查看 AAA 的概要信息。
- 使用命令 **display authentication-scheme** [*authentication-scheme-name*]查看认证方案的配置信息。
- 使用命令 **display authorization-scheme** [*authorization-scheme-name*]查看授权方案的配置信息。
- 使用命令 **display access-user** [**domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *instance-name*] | **mac-address** *mac-address* | **slot** *slot-id* | **ssid** *ssid-name* | **user-id** *user-number*]查看所有在线用户的概要信息。
- 使用命令 **display domain** [**name** *domain-name*]查看域的配置信息。

----结束

1.4 配置采用 RADIUS 方式进行认证、授权和计费

AAA 可以用多种协议来实现，但最常用的是 RADIUS 协议。RADIUS（Remote Authentication Dial-In User Service）是一种客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。

1.4.1 建立配置任务

在配置 RADIUS 方式进行认证、授权、计费前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

为了防止非法用户对网络的攻击，可以配置认证、授权和计费：

- 认证：确认用户的身份，判断用户是否为合法用户。只有通过认证的合法用户才可以接入网络。
- 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。
- 计费：记录用户使用网络服务中的所有操作，包括使用的服务类型、起始时间、数据流量等。

采用 RADIUS 方式进行认证、授权、计费可以防止非法用户对网络的攻击，常应用在既要求较高安全性又要求控制远程用户访问权限的网络环境中。

前置任务

在配置 RADIUS 方式进行认证、授权、计费之前，需完成以下任务：

- 配置接口的物理属性，使接口的物理层状态为 Up。

数据准备

在配置 RADIUS 方式之前，需要准备以下数据。

序号	数据
1	认证方案的名称
2	计费方案的名称
3	RADIUS 服务器模板名称
4	RADIUS 主认证服务器的 IP 地址，端口号
5	RADIUS 主计费服务器的 IP 地址，端口号
6	（可选）RADIUS 授权服务器的 IP 地址
7	（可选）RADIUS 备认证服务器的 IP 地址，端口号
8	（可选）RADIUS 备计费服务器的 IP 地址，端口号
9	（可选）RADIUS 共享密钥
10	（可选）RADIUS 请求报文的超时重传次数和超时时间

1.4.2 配置 AAA 方案

如果需要采用 RADIUS 方式进行认证、授权和计费，需要在认证方案中配置认证模式为 RADIUS 认证，在计费方案中配置计费模式为 RADIUS 计费。

背景信息

配置认证模式为 RADIUS 认证时还可以配置本地认证或不认证为备份认证。配置备份认证可以避免单一认证模式无响应而造成的认证失败。同理，配置计费模式为 RADIUS 计费时还可以配置不计费模式为备份计费。

操作步骤

- 配置认证方案
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **aaa**，进入 AAA 视图。
  3. 执行命令 **authentication-scheme** *authentication-scheme-name*，创建一个认证方案，并进入认证方案视图或直接进入一个已存在的认证方案视图。

     缺省情况下，AR1200 中有一个认证方案，认证方案名称是 **default**，不能删除，只能修改。
  4. 执行命令 **authentication-mode radius** [**none**]，配置认证模式为 RADIUS 认证。

     缺省情况下，认证模式为本地认证。

     如果配置了本地认证方式为备份认证方式，还需要配置本地认证，请执行命令 **authentication-mode radius local**。

说明

如果在一个认证方案中使用多种认证模式，则认证模式的执行顺序为配置的先后顺序。只有在当前认证模式没有响应的情况下，才会采用下一种认证模式；如果在当前认证模式认证失败，则不会跳转到下一个认证方案进行认证。

5. (可选)执行命令 **authentication-super** { **hwtacacs** | **super** } * [**none**],在当前认证模板下，配置对用户提升级别进行认证时采用的认证模式。
6. (可选)执行命令 **quit**，返回 AAA 视图。
7. (可选)执行命令 **domainname-parse-direction** { **left-to-right** | **right-to-left** }，配置用户名和域名解析的方向，从左向右或从右向左。

- 配置计费方案
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **aaa**，进入 AAA 视图。
  3. 执行命令 **accounting-scheme** *accounting-scheme-name*，创建计费方案，并进入计费方案视图。

     缺省情况下，AR1200 中有一个计费方案，计费方案配置名是 default，不能删除，只能修改。
  4. 执行命令 **accounting-mode radius**，配置计费模式。

     缺省情况下，计费模式采用不计费模式（none）。

     说明

     如果在一个计费方案中使用多种计费模式，则计费模式的执行顺序为配置的先后顺序。只有在当前计费模式没有响应的情况下，才会采用下一种计费模式。
  5. （可选）执行命令 **accounting start-fail** { **online** | **offline** }，配置开始计费失败策略。

     缺省情况下，如果初始计费失败，不允许用户上线。
  6. （可选）执行命令 **accounting realtime** *interval*，使能实时计费并设置计费间隔。

     缺省情况下，实时计费功能未使能。
  7. （可选）执行命令 **accounting interim-fail** [**max-times** *times*] { **online** | **offline** }，配置允许的实时计费请求最大无响应次数，以及实时计费失败后采取的策略。

     使能实时计费功能后，缺省情况下，允许的实时计费请求最大无响应次数为 3 次，实时计费失败后保持付费用户在线。

----结束

1.4.3 配置 RADIUS 服务器模板

配置 RADIUS 服务器模板中的关键步骤是指定服务器的 IP 地址和端口号、RADIUS 共享密钥。其他的步骤如配置 RADIUS 用户名格式、流量单位、RADIUS 请求报文的超时重传次数等都有缺省配置，用户可以根据实际需要进行修改。

背景信息

RADIUS 服务器模板下的配置如 RADIUS 用户名格式、RADIUS 共享密钥等要与 RADIUS 服务器上的配置一致。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **radius-server authorization** *ip-address* { **server-group** *group-name* | **shared-key** { **cipher** | **simple** } *key-string* } * [**ack-reserved-interval** *interval*]，配置 RADIUS 授权服务器。

缺省情况下，没有配置 RADIUS 授权服务器。

步骤 3 执行命令 **radius-server template** *template-name*，进入 RADIUS 服务器模板视图。

步骤 4 执行命令 **radius-server authentication** *ip-address port* [**source** { **loopback** *interface-number* | **ip-address** *ip-address* }]，配置 RADIUS 主用认证服务器。

缺省情况下，RADIUS 主用认证服务器的 IP 地址为 0.0.0.0，端口号为 0。

步骤 5 （可选）执行命令 **radius-server authentication** *ip-address port* [**source** { **loopback** *interface-number* | **ip-address** *ip-address* }] **secondary**，配置 RADIUS 备用认证服务器。

缺省情况下，RADIUS 备用认证服务器的 IP 地址为 0.0.0.0，端口号为 0。

步骤 6 执行命令 **radius-server accounting** *ip-address port* [**source** { **loopback** *interface-number* | **ip-address** *ip-address* }] 配置 RADIUS 主用计费服务器。

缺省情况下，RADIUS 主用计费服务器的 IP 地址为 0.0.0.0，端口号为 0。

步骤 7 （可选）执行命令 **radius-server accounting** *ip-address port* [**source** { **loopback** *interface-number* | **ip-address** *ip-address* }] **secondary** 配置 RADIUS 备用计费服务器。

缺省情况下，RADIUS 备份计费服务器的 IP 地址为 0.0.0.0，端口号为 0。

步骤 8 （可选）执行命令 **radius-server shared-key** { **cipher** | **simple** }*key-string*，配置 RADIUS 共享密钥，采用明文形式显示用户口令。

缺省情况下，RADIUS 共享密钥是 huawei。

步骤 9 （可选）执行命令 **radius-server user-name domain-included**，配置 RADIUS 用户名格式。

缺省情况下，RADIUS 用户名中包含域名，即 AR1200 会把用户名和域名及域名分割符一起发送给 RADIUS 服务器进行认证。

如果 RADIUS 服务器不接受带域名的用户名，可以执行命令 **undo radius-server user-name domain-included**，AR1200 会将用户名中的域名去掉，再发送给 RADIUS 服务器。

步骤 10 （可选）执行命令 **radius-server traffic-unit** { **byte** | **kbyte** | **mbyte** | **gbyte** }，配置 RADIUS 流量单位。

缺省情况下，AR1200 以字节（byte）作为 RADIUS 流量单位。

步骤 11 （可选）执行命令 **radius-server** { **retransmit** *retry-times* | **timeout** *time-value* }*，设置 RADIUS 请求报文的超时重传次数和超时时间。

缺省情况下，RADIUS 请求报文的超时重传次数为 3，超时时间是 5 秒。

步骤 12 （可选）执行命令 **radius-server nas-port-format** { **new** | **old** }，配置 RADIUS 服务器的 NAS 端口形式。

缺省情况下，采用新的 NAS 端口形式。

步骤 13 （可选）执行命令 **radius-server nas-port-id-format** { **new** | **old** }，配置 RADIUS 服务器的 NAS 端口 ID 形式。

缺省情况下，采用新的 NAS 端口 ID 形式。

步骤 14 （可选）执行命令 **radius-attribute nas-ip**，配置设备发送 RADIUS 报文使用的 NAS-IP-Address 属性。

步骤 15 （可选）执行命令 **return**，返回用户视图。

步骤 16 （可选）执行命令 **test-aaa** *user-name user-password* **radius-template** *template-name* [**chap** | **pap**]，测试某个用户是否能够通过 RADIUS 认证。

----结束

1.4.4 配置域

创建的认证方案、计费方案、RADIUS 服务器模板，只有在域下应用后才能生效。

背景信息

在配置域之前，需要完成以下任务：

- 配置认证方案和计费方案。
- 配置 RADIUS 服务器模板。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，创建域并进入域视图。

缺省情况下，AR1200 存在两个域：“default”和“default_admin”。“default”用于普通接入用户的域，“default_admin”用于管理员的域。

步骤 4 执行命令 **authentication-scheme** *authentication-scheme-name*，配置域的认证方案。

缺省情况下，域使用配置名为 default 的认证方案。

步骤 5 （可选）执行命令 **accounting-scheme** *accounting-scheme-name*，配置域的计费方案。

缺省情况下，域使用名为“default”的计费方案。“default”计费方案的策略为：计费模式为不计费，关闭实时计费开关。

步骤 6 （可选）执行命令 **service-scheme** *service-scheme-name*，配置域的业务方案。

缺省情况下，域下没有配置任何业务方案。

步骤 7 执行命令 **radius-server** *template-name*，配置域的 RADIUS 服务器模板。

缺省情况下，域下没有配置 RADIUS 服务器模板。

步骤 8 （可选）执行命令 **state** { **active** | **block** }，配置域的状态。

当域处于阻塞态时，属于该域的用户不能登录。缺省情况下，域创建后处于激活状态。

步骤 9 执行命令 **quit**，退出域视图。

步骤 10 （可选）执行命令 **domain-name-delimiter** *delimiter*，配置域名分隔符。

域名分隔符可以是 \ / : < > | @ ' % 中的某一个。

缺省情况下，域名分隔符为@。

----结束

1.4.5 检查配置结果

前提条件

已经完成采用 RADIUS 方式进行认证、授权和计费的所有配置。

操作步骤

- 使用命令 **display aaa configuration** 查看 AAA 的概要信息。
- 使用命令 **display authentication-scheme** [*authentication-scheme-name*]查看认证方案的配置信息。
- 使用命令 **display accounting-scheme** [*accounting-scheme-name*]查看计费方案的配置信息。
- 使用命令 **display service-scheme** [**name** *name*]查看业务方案的配置信息。
- 使用命令 **display radius-server configuration** [**template** *template-name*]查看 RADIUS 服务器模板的配置信息。
- 使用命令 **display radius-attribute** [**template** *template-name*] **disable** 查看设备禁用的 RADIUS 属性。
- 使用命令 **display radius-attribute** [**template** *template-name*] **translate** 查看 RADIUS 属性转换的配置信息。
- 使用命令 **display domain** [**name** *domain-name*]查看域的配置信息。

----结束

1.5 配置采用 HWTACACS 方式进行认证、授权、计费

HWTACACS 协议与 RADIUS 协议类似，主要是通过客户端/服务器模式与 HWTACACS 服务器通信来实现对接入用户进行认证、授权和计费。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。

1.5.1 建立配置任务

在配置 HWTACACS 方式进行认证、授权、计费前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

为了防止非法用户对网络的攻击，可以配置认证、授权和计费：

- 认证：确认用户的身份，判断用户是否为合法用户。只有通过认证的合法用户才可以接入网络。

- 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。
- 计费：记录用户使用网络服务中的所有操作，包括使用的服务类型、起始时间、数据流量等。

采用 HWTACACS 方式进行认证、授权、计费可以防止非法用户对网络的攻击，HWTACACS 还支持对命令行进行授权，比 RADIUS 更适用于进行安全控制。

前置任务

在配置 HWTACACS 方式进行认证、授权、计费之前，需完成以下任务：

- 配置接口的物理属性，使接口的物理层状态为 Up。

数据准备

在配置本地用户管理之前，需要准备以下数据。

序号	数据
1	认证方案的名称
2	授权方案的名称
3	计费方案的名称
4	HWTACACS 服务器模板名称
5	HWTACACS 主、备认证服务器的 IP 地址，端口号
6	HWTACACS 主、备授权服务器的 IP 地址，端口号
7	（可选）HWTACACS 主、备计费服务器的 IP 地址，端口号
8	（可选）HWTACACS 共享密钥
9	（可选）应答超时时间
10	（可选）HWTACACS 主服务器恢复激活时间
11	（可选）计费结束报文的重传

1.5.2 配置 AAA 方案

如果需要采用 HWTACACS 方式进行认证、授权和计费，需要在认证方案中配置认证模式为 HWTACACS 认证，在授权方案中配置认证模式为 HWTACACS 授权，在计费方案中配置计费模式为 HWTACACS 计费。

背景信息

配置认证模式为 HWTACACS 认证时还可以配置本地认证或不认证为备份认证模式。配置备份认证可以避免单一认证模式无响应而造成的认证失败。同理，配置授权模式为

HWTACACS 授权时还可以配置本地授权或不授权为备份授权模式，配置计费模式为 HWTACACS 计费时还可以配置不计费模式为备份计费。

操作步骤

- 配置认证方案
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **aaa**，进入 AAA 视图。
  3. 执行命令 **authentication-scheme** *authentication-scheme-name*，创建一个认证方案，并进入认证方案视图或直接进入一个已存在的认证方案视图。

     缺省情况下，AR1200 中有一个认证方案，认证方案名称是 **default**，不能删除，只能修改。
  4. 执行命令 **authentication-mode hwtacacs** [**none**]，配置认证模式为 HWTACACS 认证。

     缺省情况下，认证模式为本地认证。

     如果配置了本地认证方式为备份认证方式，还需要配置本地认证，具体配置方法请参考**配置采用本地方式进行认证和授权**。

     说明

     如果在一个认证方案中使用多种认证模式，则认证模式的执行顺序为配置的先后顺序。只有在当前认证模式没有响应的情况下，才会采用下一种认证模式；如果在当前认证模式认证失败，则不会跳转到下一个认证方案进行认证。
  5. (可选)执行命令 **authentication-super** { **hwtacacs** | **super** } * [**none**],在当前认证模板下，配置对用户提升级别进行认证时采用的认证模式。
  6. (可选)执行命令 **quit**，返回 AAA 视图。
  7. (可选)执行命令 **domainname-parse-direction** { **left-to-right** | **right-to-left** }，配置用户名和域名解析的方向，从左向右或从右向左。
- 配置授权方案
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **aaa**，进入 AAA 视图。
  3. 执行命令 **authorization-scheme** *authorization-scheme-name*，创建一个授权方案，并进入授权方案视图或直接进入一个已存在的授权方案视图。

     缺省情况下，AR1200 有一个授权方案，授权方案配置名是 default，不能删除，只能修改。
  4. 执行命令 **authorization-mode** { **hwtacacs** | **local** }* [**none**]配置授权模式。

     缺省情况下，授权模式为本地授权模式。

     如果采用 HWTACACS 授权模式，必须配置 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。

     说明

     如果在一个授权方案中使用多种授权模式，则授权模式的执行顺序为配置的先后顺序。只有在当前授权模式没有响应的情况下，才会采用下一种授权模式；如果当前授权模式失败，则不会采用下一种授权模式进行授权。
  5. （可选）执行命令 **authorization-cmd** *privilege-level* **hwtacacs** [**local**]，配置某级别的用户按命令行授权。

缺省情况下，0 ～ 15 级用户都没有配置按命令行授权。

如果使能按命令行授权功能，必须配置 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。

- 配置计费方案
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **aaa**，进入 AAA 视图。
  3. 执行命令 **accounting-scheme** *accounting-scheme-name*，创建一个计费方案，并进入计费方案视图或直接进入一个已存在的计费方案视图。

     缺省情况下，AR1200 中有一个计费方案，计费方案配置名是 default，不能删除，只能修改。
  4. 执行命令 **accounting-mode hwtacacs**，配置计费模式。

     缺省情况下，计费模式采用不计费模式（none）。

     说明

     如果在一个计费方案中使用多种计费模式，则计费模式的执行顺序为配置的先后顺序。只有在当前计费模式没有响应的情况下，才会采用下一种计费模式。
  5. （可选）执行命令 **accounting start-fail** { **online** | **offline** }，配置开始计费失败策略。

     缺省情况下，如果初始计费失败，不允许用户上线。
  6. （可选）执行命令 **accounting realtime** *interval*，使能实时计费并设置计费间隔。

     缺省情况下，实时计费功能未使能。
  7. （可选）执行命令 **accounting interim-fail** [**max-times** *times*] { **online** | **offline** }，配置允许的实时计费请求最大无响应次数，以及实时计费失败后采取的策略。

     使能实时计费功能后，缺省情况下，允许的实时计费请求最大无响应次数为 3 次，实时计费失败后保持付费用户在线。

----结束

1.5.3 配置 HWTACACS 服务器模板

配置 HWTACACS 服务器模板中的关键步骤是指定服务器的 IP 地址和端口号、HWTACACS 共享密钥。其他的步骤如配置 HWTACACS 用户名格式、流量单位等都有缺省配置，用户可以根据实际需要进行修改。

背景信息

HWTACACS 服务器模板下配置的 HWTACACS 用户名格式、HWTACACS 共享密钥等要与 HWTACACS 服务器上的配置一致。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **hwtacacs enable**，使能 HWTACACS 功能。

步骤 3 执行命令 **hwtacacs-server template** *template-name*，创建 HWTACACS 服务器模板，并进入 HWTACACS 服务器模板视图。

步骤 4 执行命令 **hwtacacs-server authentication** *ip-address* [*port*] [**public-net**| **vpn-instance** *vpn-instance-name*]，配置 HWTACACS 的主用认证服务器 IP 地址。

缺省情况下，HWTACACS 主用认证服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

步骤 5 （可选）执行命令 **hwtacacs-server authentication** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] **secondary**，配置 HWTACACS 的备用认证服务器 IP 地址。

缺省情况下，HWTACACS 备用认证服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

步骤 6 执行命令 **hwtacacs-server authorization** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*]，配置 HWTACACS 的主用授权服务器 IP 地址。

缺省情况下，HWTACACS 主用授权服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

步骤 7 （可选）执行命令 **hwtacacs-server authorization** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] **secondary**，配置 HWTACACS 的备用授权服务器 IP 地址。

缺省情况下，HWTACACS 备用授权服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

步骤 8 执行命令 **hwtacacs-server accounting** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*]，配置 HWTACACS 主用计费服务器。

缺省情况下，HWTACACS 主用计费服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

步骤 9 （可选）执行命令 **hwtacacs-server accounting** *ip-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] **secondary**，配置 HWTACACS 备用计费服务器。

缺省情况下，HWTACACS 备用计费服务器的 IP 地址为 0.0.0.0，端口号是 0，不绑定 VPN 实例。

步骤 10 （可选）执行命令 **hwtacacs-server source-ip** *ip-address*，配置 HWTACACS 的源 IP 地址。

缺省情况下，HWTACACS 的源 IP 地址是 0.0.0.0，此时 AR1200 使用实际出方向的接口的 IP 地址作为 HWTACACS 报文的源 IP 地址。

指定 HWTACACS 的源 IP 地址后，使用该 HWTACACS 模板与服务器通信时，报文的源 IP 地址为指定的 IP 地址。此时，服务器也将使用指定的 IP 地址与 AR1200 通信。

步骤 11 （可选）执行命令 **hwtacacs-server shared-key** [**cipher** | **simple**] *key-string*，配置 HWTACACS 的共享密钥。

缺省情况下，没有配置 HWTACACS 的共享密钥。

步骤 12 （可选）执行命令 **hwtacacs-server user-name domain-included**，配置 HWTACACS 用户名格式。

缺省情况下，HWTACACS 用户名中包含域名，即 AR1200 会把用户名和域名及域名分割符一起发送给 HWTACACS 服务器进行认证。

步骤 13 （可选）执行命令 **hwtacacs-server traffic-unit** { **byte** | **kbyte** | **mbyte** | **gbyte** }，配置 HWTACACS 流量单位。

缺省情况下，AR1200 使用字节（**byte**）作为 HWTACACS 流量单位。

步骤 14 （可选）执行命令 **hwtacacs-server timer response-timeout** *value*，配置 HWTACACS 服务器应答超时时间。

缺省情况下，HWTACACS 应答超时时间为 5 秒。

如果 AR1200 在应答超时时间内，没有收到 HWTACACS 服务器的回复，则认为服务器不可用。此时 AR1200 将尝试使用其他方式进行认证、授权。

步骤 15 （可选）执行命令 **hwtacacs-server timer quiet** *value*，配置 HWTACACS 主服务器恢复激活时间。

缺省情况下，主用服务器恢复激活状态前需要等待 5 分钟。

步骤 16 （可选）执行命令 **quit**，返回系统视图。

步骤 17 （可选）执行命令 **hwtacacs-server accounting-stop-packet resend** { **disable** | **enable** *number* }，配置计费结束报文的重传功能。

可以配置是否启用计费结束报文的重传功能以及报文的重传次数。缺省情况下，AR1200 启用计费结束报文的重传功能，报文的重传次数为 100。

步骤 18 （可选）执行命令 **return**，返回用户视图。

步骤 19 （可选）执行命令 **hwtacacs-user change-password hwtacacs-server** *template-name*，修改用户在 HWTACACS 服务器上保存的用户密码。

----结束

1.5.4 配置域

创建的认证方案、授权方案、计费方案、HWTACACS 服务器模板，只有在域下应用后才能生效。

背景信息

在配置域之前，需要完成以下任务：

- 配置认证方案、授权方案、计费方案。
- 配置 HWTACACS 服务器模板。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **aaa**，进入 AAA 视图。

步骤 3 执行命令 **domain** *domain-name*，创建域并进入域视图或直接进入一个已存在的域视图。

缺省情况下，AR1200 存在两个域：“default”和“default_admin”。“default”用于普通接入用户的域，“default_admin”用于管理员的域。

步骤 4 执行命令 **authentication-scheme** *authentication-scheme-name*，配置域的认证方案。

缺省情况下，域使用配置名为 default 的认证方案。

步骤 5 （可选）执行命令 **authorization-scheme** *authorization-scheme-name*，配置域的授权方案。

缺省情况下，域下没有绑定授权方案。

步骤 6 （可选）执行命令 **accounting-scheme** *accounting-scheme-name*，配置域的计费方案。

缺省情况下，域使用名为“default”的计费方案。“default”计费方案的策略为：计费模式为不计费，关闭实时计费。

步骤 7 （可选）执行命令 **service-scheme** *service-scheme-name*，配置域的业务方案。

缺省情况下，域下没有配置任何业务方案。

步骤 8 执行命令 **hwtacacs-server** *template-name*，配置域的 HWTACACS 服务器模板。

缺省情况下，域下没有配置 HWTACACS 服务器模板。

步骤 9 （可选）执行命令 **state** { **active** | **block** }，配置域的状态。

当域处于阻塞态时，属于该域的用户不能登录。缺省情况下，域创建后处于激活状态。

步骤 10 执行命令 **quit**，退出域视图。

步骤 11 （可选）执行命令 **domain-name-delimiter** *delimiter*，配置域名分隔符。

域名分隔符可以是 \ / : < > | @ ' % 中的某一个。

缺省情况下，域名分隔符为@。

----结束

1.5.5 检查配置结果

前提条件

已经完成采用 RADIUS 方式进行认证、授权和计费的所有配置。

操作步骤

- 使用命令 **display aaa configuration** 查看 AAA 的概要信息。
- 使用命令 **display authentication-scheme** [*authentication-scheme-name*]查看认证方案的配置信息。
- 使用命令 **display authorization-scheme** [*authentication-scheme-name*]查看授权方案的配置信息。
- 使用命令 **display accounting-scheme** [*accounting-scheme-name*]查看计费方案的配置信息。
- 使用命令 **display service-scheme** [**name** *name*]查看业务方案的配置信息。
- 使用命令 **display hwtacacs-server template** [*template-name*]查看 HWTACACS 服务器模板的配置信息。
- 使用命令 **display domain** [**name** *domain-name*]查看域的配置信息。

----结束

1.6 维护 AAA

清除统计信息。

1.6.1 清除统计信息

背景信息

注意

清除统计信息后，以前的统计信息将无法恢复，请务必仔细确认。

在确认需要清除统计信息后,请在用户视图下执行以下命令。

操作步骤

- 使用 **reset hwtacacs-server statistics** { **all** | **accounting** | **authentication** | **authorization** }命令清除 HWTACACS 的统计信息。
- 使用 **reset hwtacacs-server accounting-stop-packet** { **all** | **ip** *ip-address* }命令清除计费停止报文的统计信息。

----结束

1.7 配置举例

通过示例介绍如何配置 AAA。配置示例中包括组网需求、配置注意事项、配置思路等。

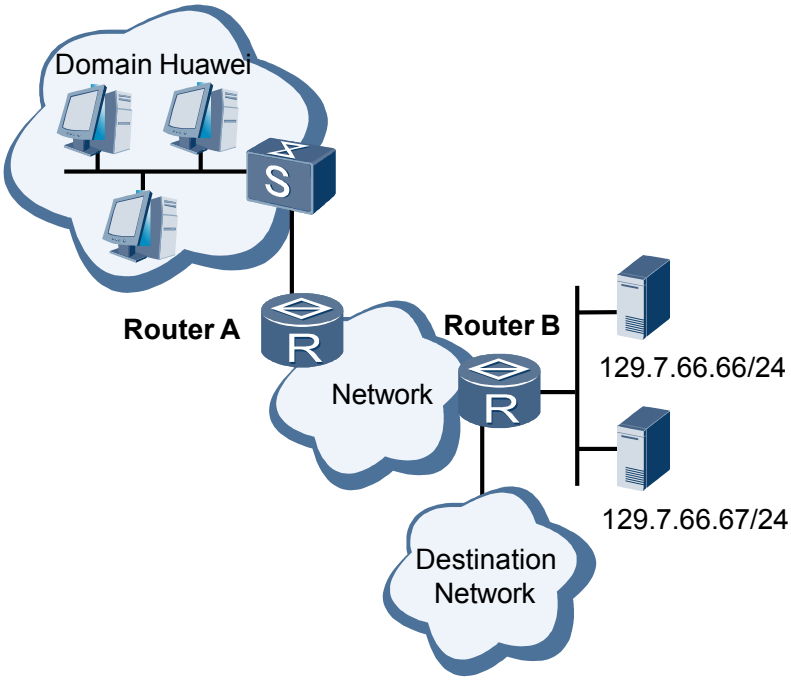
1.7.1 配置采用 RADIUS 协议进行认证、计费和授权示例

组网需求

如图 1-4 所示，用户通过 RouterA 访问网络，用户同处于 huawei 域。RouterB 作为目的网络接入服务器。用户首先需要穿越 RouterA 和 RouterB 所在的网络，然后通过服务器的远端认证才能通过 RouterB 访问目的网络。在 RouterB 上的远端认证方式如下：

- 用 RADIUS 服务器对接入用户进行认证、计费。
- RADIUS 服务器 129.7.66.66/24 作为主用认证服务器和计费服务器，RADIUS 服务器 129.7.66.67/24 作为备用认证服务器和计费服务器，认证端口号缺省为 1812，计费端口号缺省为 1813。

图 1-4 采用 RADIUS 协议对用户进行认证和计费组网图



配置思路

用如下的思路配置采用 RADIUS 协议对用户进行认证和计费。

1. 配置 RADIUS 服务器模板。
2. 配置认证方案、计费方案。
3. 在域下应用 RADIUS 服务器模板、认证方案和计费方案。

数据准备

为完成此配置举例，需要准备如下数据：

- 用户所属的域名
- RADIUS 服务器模板名
- 认证方案名、认证模式、计费方案名、计费模式
- 主用和备用 RADIUS 服务器的 IP 地址、认证端口号、计费端口号
- RADIUS 服务器密钥和重传次数

说明

以下配置均在 RouterB 上进行。

操作步骤

步骤 1 配置接口的 IP 地址和路由，使用户和服务器之间路由可达。

步骤 2 配置 RADIUS 服务器模板

配置 RADIUS 服务器模板 shiva。

```
<Huawei> system-view
[Huawei] radius-server template shiva
```

配置 RADIUS 主用认证服务器和计费服务器的 IP 地址、端口。

```
[Huawei-radius-shiva] radius-server authentication 129.7.66.66 1812
[Huawei-radius-shiva] radius-server accounting 129.7.66.66 1813
```

配置 RADIUS 备用认证服务器和计费服务器的 IP 地址、端口。

```
[Huawei-radius-shiva] radius-server authentication 129.7.66.67 1812 secondary
[Huawei-radius-shiva] radius-server accounting 129.7.66.67 1813 secondary
```

配置 RADIUS 服务器密钥、重传次数。

```
[Huawei-radius-shiva] radius-server shared-key cipher hello
[Huawei-radius-shiva] radius-server retransmit 2
[Huawei-radius-shiva] quit
```

步骤 3 配置认证方案、计费方案

配置认证方案 1，认证模式为 RADIUS。

```
[Huawei] aaa
[Huawei-aaa] authentication-scheme 1
[Huawei-aaa-authen-1] authentication-mode radius
[Huawei-aaa-authen-1] quit
```

配置计费方案 1，计费模式为 RADIUS。

```
[Huawei-aaa] accounting-scheme 1
[Huawei-aaa-accounting-1] accounting-mode radius
[Huawei-aaa-accounting-1] quit
```

步骤 4 配置 huawei 域，在域下应用认证方案 1、计费方案 1、RADIUS 模板 shiva

```
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] authentication-scheme 1
[Huawei-aaa-domain-huawei] accounting-scheme 1
[Huawei-aaa-domain-huawei] radius-server shiva
```

步骤 5 检查配置结果

在 RouterB 上执行命令 **display radius-server configuration template**，可以观察到该 RADIUS 服务器模板的配置与要求一致。

```
<Huawei> display radius-server configuration template shiva

  ------------------------------------------------------------------

Server-template-name              :  shiva
  Protocol-version                :  standard
  Traffic-unit                    :  B
  Shared-secret-key               :  3MQ*TZ,O3KCQ=^Q`MAF4<1!!
  Timeout-interval(in second)     :  5
  Primary-authentication-server   :  129.7.66.66    :1812 :-
                                     LoopBack:NULL   Source-IP:0.0.0.0
  Primary-accounting-server       :  129.7.66.66    :1813 :-
                                     LoopBack:NULL   Source-IP:0.0.0.0
  Secondary-authentication-server :  129.7.66.67    :1812 :-
                                     LoopBack:NULL   Source-IP:0.0.0.0
  Secondary-accounting-server     :  129.7.66.67    :1813 :-
                                     LoopBack:NULL   Source-IP:0.0.0.0
  Retransmission                  :  2
  Domain-included                 :  YES
  NAS-IP-Address                  :  0.0.0.0
  ------------------------------------------------------------------
```

----结束

配置文件

```
#
radius-server template shiva
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 129.7.66.66 1812
 radius-server authentication 129.7.66.67 1812 secondary
 radius-server accounting 129.7.66.66 1813
 radius-server accounting 129.7.66.67 1813 secondary
 radius-server retransmit 2
#
aaa
 authentication-scheme default
 authentication-scheme 1
  authentication-mode radius
 authorization-scheme default
 accounting-scheme default
 accounting-scheme 1
  accounting-mode radius
 domain default
 domain default_admin
 domain huawei
  authentication-scheme 1
  accounting-scheme 1
  radius-server shiva
#
return
```

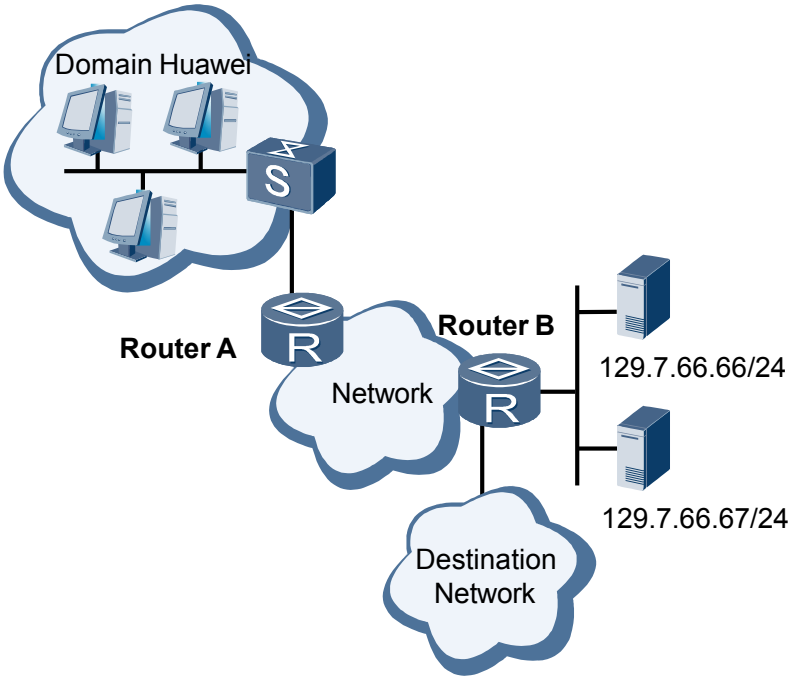
1.7.2 配置采用 HWTACACS 协议进行认证、计费和授权示例

组网需求

如图 1-5 所示，

- Router B 对接入用户先用 HWTACACS 服务器进行认证，如果认证没有响应，再使用本地认证。
- 接入的用户进行用户等级提升时，要求先使用 HWTACACS 对其进行认证，如果 HWTACACS 认证没有响应，再使用本地认证。
- Router B 对接入用户采用 HWTACACS 授权。
- Router B 对接入用户采用 HWTACACS 计费。
- 对用户进行实时计费，计费间隔为 3 分钟。
- HWTACACS 主用服务器为 129.7.66.66/24，备用服务器为 129.7.66.67/24，服务器的认证、授权和计费端口号均为 49。

图 1-5 采用 HWTACACS 协议对用户进行认证、计费和授权组网图



配置思路

采用如下的思路配置对用户使用本地和 HWTACACS 认证、HWTACACS 授权和进行实时计费。

1. 配置 HWTACACS 服务器模板。
2. 配置认证方案、授权方案、计费方案。
3. 在域下应用 HWTACACS 服务器模板、认证方案、授权方案、计费方案。

数据准备

为完成此配置举例，需要准备如下数据：

- 用户所属的域名
- HWTACACS 服务器模板名
- 认证方案名、认证模式、授权方案名、授权模式、计费方案名、计费模式
- 主用和备用 HWTACACS 服务器的 IP 地址、认证端口号、授权端口号、计费端口号
- HWTACACS 服务器密钥

说明

以下配置均在 RouterB 上进行。

操作步骤

步骤 1 配置 HWTACACS 服务器模板

配置 HWTACACS 服务器模板 ht。

```
<Huawei> system-view
[Huawei] hwtacacs-server template ht
```

配置 HWTACACS 主用认证、授权、计费服务器的 IP 地址和端口。

```
[Huawei-hwtacacs-ht] hwtacacs-server authentication 129.7.66.66 49
[Huawei-hwtacacs-ht] hwtacacs-server authorization 129.7.66.66 49
[Huawei-hwtacacs-ht] hwtacacs-server accounting 129.7.66.66 49
```

配置 HWTACACS 备用认证、授权、计费服务器的 IP 地址和端口。

```
[Huawei-hwtacacs-ht] hwtacacs-server authentication 129.7.66.67 49 secondary
[Huawei-hwtacacs-ht] hwtacacs-server authorization 129.7.66.67 49 secondary
[Huawei-hwtacacs-ht] hwtacacs-server accounting 129.7.66.67 49 secondary
```

配置 TACACS 服务器密钥。

```
[Huawei-hwtacacs-ht] hwtacacs-server shared-key cipher hello
[Huawei-hwtacacs-ht] quit
```

步骤 2 配置认证方案、授权方案、计费方案

配置认证方案 l-h，认证方法为先进行 HWTACACS 认证，后进行本地认证。用户级别提升认证方法为先进行 HWTACACS 认证，后进行本地认证。

```
[Huawei] aaa
[Huawei-aaa] authentication-scheme l-h
[Huawei-aaa-authen-l-h] authentication-mode hwtacacs local
[Huawei-aaa-authen-l-h] authentication-super hwtacacs super
[Huawei-aaa-authen-l-h] quit
```

配置授权方案 hwtacacs，授权方法为 HWTACACS。

```
[Huawei-aaa] authorization-scheme hwtacacs
[Huawei-aaa-author-hwtacacs] authorization-mode hwtacacs
[Huawei-aaa-author-hwtacacs] quit
```

配置计费方案 hwtacacs，计费方法为 HWTACACS。

```
[Huawei-aaa] accounting-scheme hwtacacs
[Huawei-aaa-accounting-hwtacacs] accounting-mode hwtacacs
```

配置实时计费间隔为 3 分钟。

```
[Huawei-aaa-accounting-hwtacacs] accounting realtime 3
[Huawei-aaa-accounting-hwtacacs] quit
```

步骤 3 配置 huawei 域，在域下采用 l-h 认证方案、HWTACACS 授权方案、HWTACACS 计费方案、ht 的 HWTACACS 模板

```
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] authentication-scheme l-h
[Huawei-aaa-domain-huawei] authorization-scheme hwtacacs
[Huawei-aaa-domain-huawei] accounting-scheme hwtacacs
[Huawei-aaa-domain-huawei] hwtacacs-server ht
[Huawei-aaa-domain-huawei] quit
[Huawei-aaa] quit
```

步骤 4 检查配置结果

在 RouterB 上执行命令 **display hwtacacs-server template**，可以观察到该 HWTACACS 服务器模板的配置与要求一致。

```
<Huawei> display hwtacacs-server template ht
  ------------------------------------------------------------------------------
  HWTACACS-server template name   : ht
  Primary-authentication-server   : 129.7.66.66:49:-
  Primary-authorization-server    : 129.7.66.66:49:-
  Primary-accounting-server       : 129.7.66.66:49:-
```

```
  Secondary-authentication-server : 129.7.66.67:49:-
  Secondary-authorization-server  : 129.7.66.67:49:-
  Secondary-accounting-server     : 129.7.66.67:49:-
  Current-authentication-server   : 129.7.66.66:49:-
  Current-authorization-server    : 129.7.66.66:49:-
  Current-accounting-server       : 129.7.66.66:49:-
  Source-IP-address               : 0.0.0.0
  Shared-key                      : ****************
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : Yes
  Traffic-unit                    : B
  -----------------------------------------------------------------------------
```

同时在 RouterB 上执行命令 **display domain**，可以观察到该域的配置与要求一致。

```
<Huawei> display domain name huawei

  Domain-name                     : huawei
  Domain-state                    : Active
  Authentication-scheme-name      : l-h
  Accounting-scheme-name          : hwtacacs
  Authorization-scheme-name       : hwtacacs
  Service-scheme-name             : -
  RADIUS-server-group             : -
  HWTACACS-server-template        : ht
```

----结束

配置文件

```
#
hwtacacs-server template ht
 hwtacacs-server authentication 129.7.66.66
 hwtacacs-server authentication 129.7.66.67 secondary
 hwtacacs-server authorization 129.7.66.66
 hwtacacs-server authorization 129.7.66.67 secondary
 hwtacacs-server accounting 129.7.66.66
 hwtacacs-server accounting 129.7.66.67 secondary
 hwtacacs-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
#
aaa
 authentication-scheme default
 authentication-scheme l-h
  authentication-mode hwtacacs local
  authentication-super hwtacacs super
 authorization-scheme default
 authorization-scheme hwtacacs
  authorization-mode  hwtacacs
 accounting-scheme default
 accounting-scheme hwtacacs
  accounting-mode hwtacacs
  accounting realtime 3
 domain default
 domain default_admin
 domain huawei
  authentication-scheme l-h
  accounting-scheme hwtacacs
  authorization-scheme hwtacacs
  hwtacacs-server ht
#
return
```

2 HTTPS 配置

关于本章

安全超文本传输协议 HTTPS（Hypertext Transfer Protocol Secure）通过 SSL 提供的数据加密、身份验证和消息完整性验证等安全机制，为 Web 访问提供安全性保证。

2.1 HTTPS 概述
HTTPS 是基于 SSL 安全连接的 HTTP 协议。

2.2 AR1200 支持的 HTTPS 特性
AR1200 支持 HTTPS 服务器功能。

2.3 配置 HTTPS 服务器
在 AR1200 上配置 HTTPS 服务器功能后，用户可以利用 Web 页面安全访问远程的 AR1200。

2.4 配置举例
介绍 HTTPS 的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

2.1 HTTPS 概述

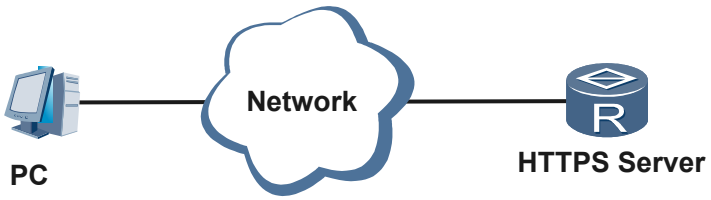
HTTPS 是基于 SSL 安全连接的 HTTP 协议。

HTTPS 将 HTTP 和 SSL 结合，通过 SSL 对客户端和服务器进行身份验证，对传输的数据进行加密，从而实现了对设备的安全管理。

对于支持 Web 网管功能的设备，开启 HTTP 服务后，设备可以作为 Web 服务器，允许用户通过 HTTP 协议登录，并利用 Web 页面实现对设备的访问和控制。但是 HTTP 协议本身不能对 Web 服务器的身份进行验证，也不能保证数据传输的私密性，无法提供安全性保证。为此，可在设备上部署 HTTPS 功能，将 HTTP 和 SSL 结合，通过 SSL 对客户端和服务器进行身份验证，对传输的数据进行加密，从而实现了对设备的安全管理。

如图 2-1 所示，在作为 HTTP 服务器的设备上部署 SSL 策略，并使能 HTTPS 服务器功能后，用户可以在终端通过浏览器登录 HTTPS 服务器，利用 Web 页面安全管理远程设备。

图 2-1 通过浏览器登录 HTTPS 服务器



2.2 AR1200 支持的 HTTPS 特性

AR1200 支持 HTTPS 服务器功能。

在 AR1200 上配置 HTTPS 服务器功能后，AR1200 将作为 HTTPS 服务器，利用 SSL 协议的数据加密、身份验证和消息完整性验证机制，保证用户和 AR1200 之间数据传输的安全性，这样用户可以利用 Web 页面安全访问远程的 AR1200。

AR1200 的 HTTPS 服务器功能可以作为配置某些业务的前提和基础，比如安全 Web 网管和 SSL VPN 业务。

说明

HTTPS 功能使用 License 授权，缺省情况下，设备的 HTTPS 功能受限无法使用。如果需要使用 HTTPS 功能，请联系华为办事处申请并购买如下 License，

- AR1200 安全业务增值包

2.3 配置 HTTPS 服务器

在 AR1200 上配置 HTTPS 服务器功能后，用户可以利用 Web 页面安全访问远程的 AR1200。

应用环境

用户通过 Web 页面远程访问作为 HTTP 服务器的 AR1200 时，传统的 HTTP 会出现以下问题：

- 传统的 HTTP 不能使用户对 AR1200 进行身份验证。
- 传统的 HTTP 不能保证用户和 AR1200 之间数据传输的私密性。
- 传统的 HTTP 不能保证用户和 AR1200 之间数据传输的完整性，数据可能会被修改。

由于传统的 HTTP 存在安全方面的缺陷，AR1200 可以作为 HTTPS 服务器，利用 SSL 协议的数据加密、身份验证和消息完整性验证机制，保证用户和 AR1200 之间数据传输的安全性，这样用户可以利用 Web 页面安全访问远程的 AR1200。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 配置服务器型 SSL 策略。参见**配置服务器型 SSL 策略**。

步骤 3 执行命令 **http secure-server ssl-policy** *ssl-policy*，配置 HTTPS 服务器关联 SSL 策略。

缺省情况下，AR1200 没有配置 HTTPS 服务器关联 SSL 策略。

步骤 4 （可选）执行命令 **http secure-server port** *port*，修改 HTTPS 服务的端口号。

缺省情况下，HTTPS 服务的端口号是 443。

步骤 5 执行命令 **http secure-server enable**，使能 AR1200 的 HTTPS 服务器功能。

缺省情况下，不使能 AR1200 的 HTTPS 服务器功能。

----结束

任务示例

执行命令 **display current-configuration**，查看 HTTPS 服务器的配置信息。

```
<Huawei> display current-configuration | include http secure-server
 http secure-server port 1026
 http secure-server ssl-policy user
 http secure-server enable
```

2.4 配置举例

介绍 HTTPS 的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

2.4.1 配置 HTTPS 服务器示例

本例以企业 A 的管理员远程登录网关设备为例，介绍 HTTPS 服务器的配置过程。

组网环境

企业 A 的管理员与该公司的研发部位于不同的城市，管理员希望安全地远程登录到研发部的网关设备，实现对网关设备的管理。

如图 2-2 所示，要满足企业需求，可以在作为网关设备的 Router 上配置 HTTPS 服务器功能，从而实现：

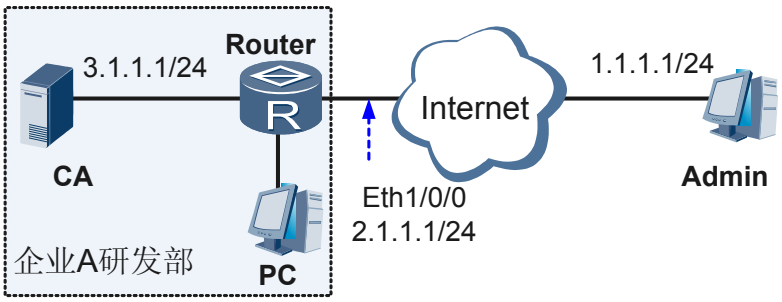
- 管理员通过主机 Admin 与网关设备 Router 建立 HTTPS 连接，通过 Web 页面实现对 Router 的管理。

- 利用 SSL 的安全机制对 HTTPS 服务器 Router 进行身份验证，提高了远程登录的安全性。

说明

为了实现基于证书的身份验证，还需要 CA 服务器。CA 服务器的具体配置略。

图 2-2 配置 HTTPS 服务器组网图



配置思路

采用如下的配置思路：

1. 配置 PKI。
2. 配置服务器型 SSL 策略。
3. 配置 HTTPS 服务器。

数据准备

为完成此配置举例，需要准备如下数据：

- Router 连接 Internet 的接口:Ethernet1/0/0
- 接口 Ethernet1/0/0 的 IP 地址：2.1.1.1/24
- CA 的 IP 地址：3.1.1.1/24
- PKI 参数:

配置项	数据
PKI 实体	PKI 实体名：admin ● 实体通用名：hello ● 国家代码：CN
PKI 域名	PKI 域名：admin ● 信任的 CA：ca_root ● 注册证书的 URL：http://3.1.1.1:8080/certsrv/mscep/mscep.dll ● 绑定的实体:admin ● CA 的指纹：采用安全散列算法 指纹值：17A34D94624B1C1BCBF6D763C4A67035D5B578EAF

- SSL 策略参数：

策略名称	保存会话的最大数目	保存会话的最大时长
adminserver	40 个	7200 秒

- HTTPS 服务的端口号：1278

说明

进行下面的配置之前，需要确保 Router、Admin、CA 之间路由可达。

操作步骤

步骤 1 配置 PKI

配置 PKI 实体

```
<Huawei> system-view
[Huawei] sysname Router
[Router] pki entity admin
[Router-pki-entity-admin] common-name hello
[Router-pki-entity-admin] country CN
[Router-pki-entity-admin] quit
```

配置 PKI 域

```
[Router] pki realm admin
[Router-pki-realm-admin] entity admin
[Router-pki-realm-admin] ca id ca_root
[Router-pki-realm-admin] enrollment-url http://3.1.1.1:8080/certsrv/mscep/mscep.dll ra
[Router-pki-realm-admin] fingerprint sha1 7A34D94624B1C1BCBF6D763C4A67035D5B578EAF
[Router-pki-realm-admin] quit
```

手工注册证书

```
[Router] pki enroll-certificate admin
 Info: Start certificate enrollment ...
 Create a challenge password. You will need to verbally provide this password to
 the CA Administrator in order to revoke your certificate.
 For security reasons your password will not be saved in the configuration. Plea
se make a note of it.
 Choice no password ,please enter the enter-key.
 Please enter Password:
 Start certificate enrollment ...
 Cert enrolling now,It will take a few minutes or more.
 Please waiting...
[Router]
 The certificate enroll successful.
```

说明

证书注册过程中会提示输入密码，如果没有密码，按回车键继续。

步骤 2 配置服务器型 SSL 策略

配置 SSL 策略使用 PKI 域 admin，以便 Router 可以基于该 PKI 域从认证机构 CA 获取数字证书

```
[Router] ssl policy adminserver type server
[Router-ssl-policy-adminserver] pki-realm admin
```

配置保存会话的最大数目和最大时长

```
[Router-ssl-policy-adminserver] session cachesize 40 timeout 7200
[Router-ssl-policy-adminserver] quit
```

步骤 3 配置 HTTPS 服务器

配置 HTTPS 服务器关联的 SSL 策略为 adminserver

```
[Router] http secure-server ssl-policy adminserver
```

配置 HTTPS 服务的端口号

```
[Router] http secure-server port 1278
```

使能 Router 的 HTTPS 服务器功能

```
[Router] http secure-server enable
```

步骤 4 检查配置结果

执行命令 **display ssl policy** *policy-name*，查看 SSL 策略 adminserver 的配置信息。

```
<Router> display ssl policy adminserver
 ------------------------------------------------------------------------------
  Policy name                    :   adminserver
  Policy ID                      :   1
  Policy type                    :   Server
  Cache number                   :   40
  Time out(second)               :   7200
  Server certificate load status  :   loaded
  Bind number                    :   1
  SSL connection number          :   1
  ------------------------------------------------------------------------------
```

管理员在主机 admin 打开浏览器，输入网址“https://2.1.1.1:1278”，主机 admin 将以 HTTPS 的方式访问 Web 网管页面，管理员后续可以利用 Web 网管页面安全访问和管理 Router。

----结束

配置文件

Router 的配置文件

```
#
 sysname Router
#
interface Ethernet 1/0/0
 ip address 2.1.1.1 255.255.255.0
#
pki entity admin
 common-name hello
 country CN
#
pki realm admin
 entity admin
 ca id ca_root
 enrollment-url http://3.1.1.1:8080/certsrv/mscep/mscep.dll ra
 fingerprint sha1 7A34D94624B1C1BCBF6D763C4A67035D5B578EAF
#
ssl policy adminserver type server
 pki-realm admin
 session cachesize 40 timeout 7200
#
 http secure-server ssl-policy adminserver
```

```
 http secure-server enable
 http secure-server port 1278
#
return
```

3 防火墙配置

关于本章

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，用防火墙作为这个网络边防产品。

3.1 防火墙概述
防火墙可以用来在组织网络内部保护大型机和重要的资源,将需要禁止的数据包丢掉。

3.2 AR1200 支持的防火墙特性
AR1200 支持的防火墙特性包括：ACL/包过滤防火墙、黑名单、白名单、ASPF、端口映射、虚拟防火墙、攻击防范、流量统计和监控及日志输出。

3.3 配置安全域
在防火墙中，所有的安全策略都基于安全区域实施。

3.4 配置包过滤防火墙
包过滤防火墙通过配置 ACL 实施数据包的过滤。

3.5 配置黑名单
黑名单可以手工配置，也可以由 AR1200 在使能攻击防范模块的 IP 地址扫描和端口扫描后，当实际针对某个 IP 地址或端口的连接速率超过设置的值时，AR1200 认为发生了扫描攻击，动态地将该源 IP 地址加入黑名单表项，以屏蔽该源 IP 地址发送来的报文。

3.6 配置白名单
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。

3.7 配置 ASPF
ASPF 能够检测试图通过防火墙的应用层协议会话信息，阻止不符合规则的数据报文穿过防火墙。同时，还可以使某些无法穿越防火墙的应用协议正常使用。

3.8 配置端口映射
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，使服务器更少地受到针对某种服务的恶意攻击。

3.9 配置防火墙会话表老化时间

3.10 配置攻击防范

攻击防范主要防止攻击报文对 CPU 的攻击，保证服务器在遭受攻击的情况下仍然正常运行。

3.11 配置流量统计和监控
AR1200 支持针对系统级、安全区域和 IP 的流量统计和监控。

3.12 配置日志输出
防火墙日志包括流日志、统计日志、攻击日志和黑名单日志。

3.13 维护防火墙

3.14 配置示例
介绍使用放火墙提高网络安全性的各种示例。

3.1 防火墙概述

防火墙可以用来在组织网络内部保护大型机和重要的资源,将需要禁止的数据包丢掉。

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：防止因特网的危险传播到私有网络。

在网络边界处，防火墙一方面阻止来自因特网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因特网进行 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。

防火墙不单用于私有网络对因特网的连接，也可以用来在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因特网的权限控制关口，如允许组织内特定的人访问因特网。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。

AR1200 的防火墙包括：

- ACL/包过滤防火墙：通过配置 ACL 实施数据包的过滤。
- ASPF：针对应用层的包过滤。
- 黑名单：根据报文的源 IP 地址进行过滤的一种方式。
- 白名单：根据报文的源 IP 地址进行过滤，防止特定的 IP 地址被加入黑名单。
- 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，使服务器更少地受到针对某种服务的恶意攻击。
- 攻击防范：基于防火墙的攻击防范功能可以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。
- 流量统计和监控：对数据流量进行监控，并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。

3.2 AR1200 支持的防火墙特性

AR1200 支持的防火墙特性包括：ACL/包过滤防火墙、黑名单、白名单、ASPF、端口映射、虚拟防火墙、攻击防范、流量统计和监控及日志输出。

安全区域

在防火墙中，安全区域（Security Zone），或者简称为区域（zone），是一个基本概念，所有的安全策略都基于安全区域实施。

一个安全区域是一个或多个接口的组合，这些接口所包含的用户具有相同的安全属性。每个安全区域具有全局唯一的安全优先级，即不存在两个具有相同优先级的安全区域。

AR1200 认为在同一安全区域内部发生的数据流动是可信的，不需要实施任何安全策略。只有当不同安全区域之间发生数据流动时，才会触发防火墙的安全检查，并实施相应的安全策略。

安全域间

任何两个安全区域都构成一个安全域间（Interzone），并具有单独的安全域间视图，大部分的防火墙配置都在安全域间视图下配置。

例如：配置了安全区域 zone1 和 zone2，则在 zone1 和 zone2 的安全域间视图中，可以配置 ACL 包过滤功能，表示对 zone1 和 zone2 之间发生的数据流动实施 ACL 包过滤。

方向

安全域间的数据流动具有方向性，包括入方向（inbound）和出方向（outbound）。

- 入方向：数据由低优先级的安全区域向高优先级的安全区域传输。
- 出方向：数据由高优先级的安全区域向低优先级的安全区域传输。

ACL 包过滤防火墙

基本的 ACL 包过滤针对需要转发的数据包，分析其五元组（源/目的 IP 地址、源/目的端口号、IP 协议号）信息，与设定的 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。

同时 AR1200 支持针对 IP 分片报文的过滤处理，防止攻击者使用非首片的分片报文实施攻击。

ASPF

ASPF 是针对应用层的包过滤，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，阻止不符合规则的数据报文穿过防火墙。

AR1200 支持针对 FTP（File Transfer Protocol）、HTTP（Hyper Text Transport Protocol）等应用层协议实施 ASPF。

黑名单

黑名单是指根据报文的源 IP 地址进行过滤的一种方式。同 ACL 相比，由于进行匹配的字段非常简单，可以以很高的速度实现包过滤，从而有效的将特定 IP 地址发送来的报文屏蔽。

黑名单最主要的一个特色是可以由防火墙动态地进行添加，当防火墙根据报文的行为特征发现特定 IP 地址的攻击企图之后，可以主动修改黑名单列表，将这个 IP 地址发送过来的报文过滤掉。

白名单

白名单是根据报文的源 IP 地址进行过滤，防止特定的 IP 地址被加入黑名单。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。

AR1200 的白名单表项只能手工添加。

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，使服务器更少地受到针对某种服务的恶意攻击。

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。

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。

AR1200 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。对于网络运营商，应用这种技术可向外出租网络安全保障服务。

每个虚拟防火墙都是 VPN（Virtual Private Network）实例（VPN-Instance）和安全实例的综合体。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。其中：

- 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地址绑定、黑名单、地址转换、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。

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。

防火墙日志包括流日志、流量统计日志、攻击日志和黑名单日志。

- 流日志生成后立即向日志服务器输出。
- 黑名单日志生成后立即向信息中心输出。
- 攻击日志和流量统计日志会由系统整理后，定时向信息中心输出。

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。

流量统计和监控

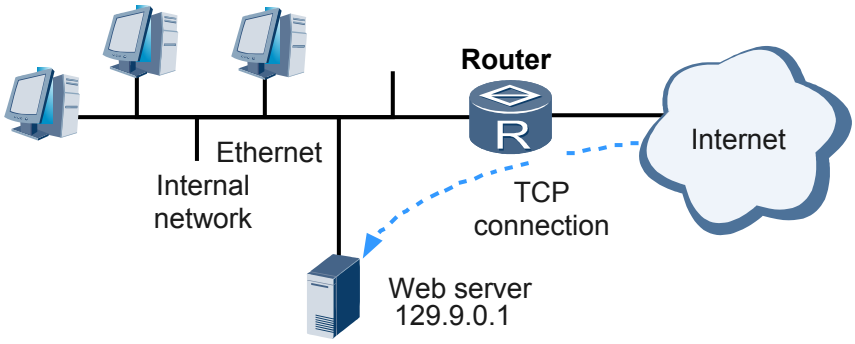
防火墙不仅要对数据流量进行监控，还要对内外部网络之间的连接发起情况进行检测，进行大量的统计计算与分析。防火墙的统计分析一方面可以通过专门的分析软件对日志信息进行事后分析，另一方面，防火墙系统本身可以完成一部分分析功能，具有一定的实时性。

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。

又比如，通过分析发现系统的总连接数超过阈值，则可以加快系统的连接老化速度，以保证新连接能够正常建立，防止因系统太忙而导致拒绝服务情况的发生。

图 3-1 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 129.9.0.1 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 3-1 防火墙拒绝外部网络向服务器发起过多的连接



攻击防范

在 AR1200 中，基于防火墙的攻击防范功能可以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。

网络攻击可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报文攻击系统，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路由器。

- 扫描窥探攻击

  扫描窥探攻击是利用 ping 扫描（包括 ICMP 和 TCP）来标识网络上存在的系统，从而准确的指出潜在的目标。利用 TCP 端口扫描，就能检测出操作系统和监听着的潜在服务。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 报文时会出现崩溃，给目标系统带来损失。主要的畸形报文攻击有 Ping of Death、Teardrop 等。

Land 攻击

所谓 Land 攻击，就是把 TCP SYN 报文的源地址和目标地址都设置成受害者的 IP 地址。这将导致受害者向它自己的地址发送 SYN-ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时。各种受害者对 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。方法是发 ICMP 应答请求，该请求报文的目标地址设置为受害网络的广播地址，这样该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，这比 ping 大报文的流量高出一或两个数量级。

高级的 Smurf 攻击，主要用来攻击目标主机。方法是将上述 ICMP 应答请求报文的源地址改为受害主机的地址，最终导致受害主机雪崩。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，网络的主机越多，攻击的效果越明显。Smurf 攻击的另一个变体为 Fraggle 攻击。

WinNuke 攻击

WinNuke 攻击通常向装有 Windows 系统的特定目标的 NetBIOS 端口（139）发送 OOB（out-of-band）数据报文，引起一个 NetBIOS 片断重叠，致使目标主机崩溃。还有一种是 IGMP（Internet Group Management Protocol）分片报文，一般情况下，IGMP 报文是不会分片的，所以，不少系统对 IGMP 分片报文的处理有问题。如果收到 IGMP 分片报文，则基本可判定受到了攻击。

SYN Flood 攻击

由于资源的限制，TCP/IP 栈的实现只能允许有限个 TCP 连接。而 SYN Flood 攻击正是利用这一点，它伪造一个 SYN 报文，其源地址是伪造的、或者一个不存在的地址，向服务器发起连接，服务器在收到报文后用 SYN-ACK 应答，而此应答发出去后，不会收到 ACK 报文，造成一个半连接。如果攻击者发送大量这样的报文，会在被攻击主机上出现大量的半连接，消耗尽其资源，使正常的用户无法访问。直到半连接超时。在一些创建连接不受限制的实现里，SYN Flood 具有类似的影响，它会消耗掉系统的内存等资源。

ICMP 和 UDP Flood 攻击

短时间内用大量的 ICMP 消息（如 ping）和 UDP 报文向特定目标不断请求回应，致使目标系统负担过重而不能处理合法的任务。

地址扫描与端口扫描攻击

运用扫描工具探测目标地址和端口，对此作出响应的表示其存在，用来确定哪些目标系统确实存在并且连接在目标网络上，这些主机使用哪些端口提供服务。

Ping of Death 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。对于有些路由器或系统，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。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。

ICMP-Redirect 和 ICMP-Unreachable 攻击

网络设备向同一个子网的主机发送 ICMP 重定向报文，请求主机改变路由。一些恶意的攻击可能跨越网段向另外一个网络的主机发送虚假的重定向报文，以期改变主机的路由表，干扰主机正常的 IP 报文转发。

有的系统在收到网络（代码为 0）或主机（代码为 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，好像切断了目的地与主机的连接，造成攻击。

Teardrop 攻击

IP 报文通过 MF（More Fragment）位、Offset 字段、Length 字段指示该分段所包含的是原报文的哪一段，某些 TCP/IP 在收到含有重叠偏移的伪造分段时会崩溃。Teardrop 攻击就是利用了一些实现不检测分片信息的合法性的漏洞来进行攻击。

Fraggle 攻击

UDP 端口 7（ECHO）和端口 19（Chargen）在收到 UDP 报文后，都会产生回应。在 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；而 UDP 的 19 号端口在收到报文后，会产生一串字符流。就象 ICMP 一样，这两个 UDP 端口都会产生大量无用的应答报文，占满网络带宽。

攻击者可以向攻击目标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 或 19。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的崩溃；子网上没有启动这些功能的系统将产生一个 ICMP 不可达消息，因而仍然消耗带宽。也可将源端口改为 Chargen，目的端口为 ECHO，这样会自动不停地产生回应报文，其危害性更大。

IP-Fragment 攻击

IP 报文中有几个字段和标志位与分片有关，包括 Fragment Offset、Length 字段以及 DF（Don’t Fragment）、MF 标志位。

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。

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，它可以窥探网络的结构。

3.3 配置安全域

在防火墙中，所有的安全策略都基于安全区域实施。

3.3.1 建立配置任务

在配置安全域之前，了解其应用环境，以及配置安全域需要提前完成的任务和准备的数据。

应用环境

在配置任何防火墙功能之前，都必须配置安全区域，才能针对安全区域或者安全域间配置防火墙功能。

前置任务

在配置安全域之前，需要完成以下任务。

- 配置需要加入安全区域的接口。

数据准备

在配置安全域之前，需要准备以下数据。

序号	数据
1	安全区域的名称
2	安全区域的优先级
3	需要加入安全域的接口

3.3.2 创建安全域

当需要配置防火墙业务时，必须先创建相关的安全区域，根据不同安全区域间的优先级关系来确定安全业务的部署。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall zone** *zone-name*，创建安全区域。

AR1200 最多可配置 255 个安全区域，没有缺省的安全区域。

步骤 3 执行命令 **priority** *security-priority*，配置安全区域优先级。

安全区域必须指定优先级，且指定后不能修改，否则不能进行其他配置。所有安全区域的优先级都不能相同，值越大，则该区域的优先级越高。

----结束

3.3.3 配置接口加入安全域

将接口加入指定的安全区域。

前提条件

已通过执行 **firewall zone** 命令创建相应的安全区域。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 执行命令 **zone** *zone-name*，将接口加入安全区域。

----结束

3.3.4 创建安全域间

要配置防火墙在指定的安全域间按照要求对各种非法报文或应用层服务进行过滤，必须先创建安全域间。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall interzone** *zone-name1 zone-name2*，创建安全域间。

创建安全域间必须指定两个已存在的安全区域。

----结束

3.3.5 在安全域间使能防火墙功能

只有在安全域间使能防火墙功能后，所配置的所有防火墙功能才能生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall interzone** *zone-name1 zone-name2*，进入安全域间视图。

zone-name1 和 *zone-name2* 已经通过 **firewall zone** 命令创建完成。

步骤 3 执行命令 **firewall enable**，使能防火墙功能。

缺省情况下，安全域间的防火墙功能未使能。

----结束

3.3.6 检查配置结果

配置安全域和安全域间之后，可以查看安全域和安全域间的相关信息。

操作步骤

- 执行 **display firewall zone** [*zone-name*] [**interface** | **priority**]命令查看安全域的相关信息。
- 执行 **display firewall interzone** [*zone-name1 zone-name2*]命令查看安全域间的相关信息。

----结束

3.4 配置包过滤防火墙

包过滤防火墙通过配置 ACL 实施数据包的过滤。

3.4.1 建立配置任务

在配置 ACL 包过滤防火墙之前，了解其应用环境，以及配置 ACL 包过滤防火墙需要提前完成的任务和准备的数据。

应用环境

ACL 包过滤可以在两个安全区域之间发生数据流动时，根据 ACL 规则实施过滤策略。在 ACL 包过滤中可以使用的 ACL 包括基本 ACL、高级 ACL。

前置任务

在配置 ACL 包过滤之前，需要完成以下任务。

- 配置安全区域，并将接口加入安全区域。
- 配置安全域间，并在安全域间使能防火墙功能。
- 创建基本 ACL 或高级 ACL 并配置规则。

数据准备

在配置 ACL 包过滤之前，需要准备以下数据。

序号	数据
1	实施 ACL 包过滤的高优先级安全区域名称和低优先级安全区域名称
2	实施 ACL 包过滤使用的 ACL 编号
3	实施 ACL 包过滤的方向

3.4.2 在安全域间配置 ACL 包过滤

通过配置 ACL 实施数据包的过滤。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **acl** [**number**] *acl-number* [**match-order** { **config** |**auto** }]，创建一个访问控制列表并进入其视图。

步骤 3 执行命令 **rule**，在 ACL 视图下，配置访问控制规则。

步骤 4 执行命令 **quit**，返回系统视图。

步骤 5 执行命令 **firewall interzone** *zone-name1 zone-name2*，进入安全域间视图。

步骤 6 执行命令 **packet-filter** *acl-number* { **inbound** | **outbound** }，配置 ACL 包过滤。

在安全域间配置 ACL 包过滤时，可针对出方向和入方向分别配置。

步骤 7 （可选）执行命令 **packet-filter default** { **deny** | **permit** } { **inbound** | **outbound** }，设置包过滤的缺省过滤方式。

缺省情况下，Outbound 方向为允许任何报文通过，Inbound 方向为拒绝任何报文通过。

如果域间出或入方向配置了 ACL 过滤规则，则按照 ACL 规则进行报文过滤，如果报文不能匹配 ACL，则按照默认的规则进行。

说明

更改防火墙安全域间的过滤配置后，建议使用 **reset firewall session all** 命令清除现有的防火墙会话表项，否则由于更改期间的规则更新，可能会导致部分会话不能按照过滤规则执行正确的过滤动作。

----结束

3.4.3 检查配置结果

配置 ACL 包过滤防火墙后，可以查看 ACL 包过滤的相关信息。

操作步骤

- 执行 **display firewall interzone** [*zone-name1 zone-name2*]命令查看包过滤的相关信息。
- 执行 **display acl** *acl-number* 命令查看配置的 ACL 信息。

----结束

3.5 配置黑名单

黑名单可以手工配置，也可以由 AR1200 在使能攻击防范模块的 IP 地址扫描和端口扫描后，当实际针对某个 IP 地址或端口的连接速率超过设置的值时，AR1200 认为发生了扫描攻击，动态地将该源 IP 地址加入黑名单表项，以屏蔽该源 IP 地址发送来的报文。

3.5.1 建立配置任务

在配置黑名单之前，了解黑名单的应用环境，以及配置黑名单需要提前完成的任务和准备的数据。

应用环境

使用黑名单功能可以将特定 IP 地址发送到安全区域的报文屏蔽。黑名单列表可以通过命令行手工添加，也可以由防火墙自动添加。

使能防火墙的地址扫描和端口扫描攻击防范后，防火墙根据报文的行为特征，判断出特定 IP 地址的攻击企图，可以自动将该 IP 地址加入到黑名单中，从而屏蔽该 IP 地址发送的报文。

前置任务

在配置黑名单之前，需要完成以下任务。

- 配置安全区域，并将接口加入安全区域。
- 配置安全域间，并在安全域间使能防火墙功能。
- 如果使用攻击防范功能自动添加黑名单，需要使能地址扫描或端口扫描攻击防范。

数据准备

在配置黑名单之前，需要准备以下数据。

序号	数据
1	需要加入黑名单的 IP 地址
2	（可选）黑名单表项的老化时间

3.5.2 使能黑名单

必须先使能黑名单功能，创建的黑名单表项才会生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall blacklist enable**，使能黑名单功能。

缺省情况下，防火墙黑名单功能未使能。

----结束

3.5.3 配置黑名单表项（手工单条配置）

将某个 IP 地址加入到防火墙黑名单后，在黑名单表项的有效时间内，防火墙将会过滤从该地址发来的报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall blacklist** *ip-address* [**vpn-instance** *vpn-instance-name*] [**expire-time** *minutes*]，添加黑名单表项。

添加黑名单表项时可以指定 IP 地址、老化时间和 VPN 实例。其中老化时间是指 IP 地址添加到黑名单后生效的时间，当 IP 地址加入黑名单的时间超过老化时间后，该 IP 地址从黑名单中释放。如果不指定老化时间，则表示该黑名单表项永远有效。

黑名单表项的添加操作不依赖于黑名单功能是否使能，即使黑名单功能不使能，依然可以添加黑名单表项，只是不会生效。

最多可以手工添加 32 个。

说明

不指定老化时间的黑名单表项会被写入配置文件。指定老化时间的黑名单表项不会被写入配置文件，但可以通过 **display firewall blacklist** 命令查看。

----结束

后续处理

执行命令 **firewall black-white-list save** 可将设备上的黑白名单保存至指定的配置文件，以便于下次加载。

3.5.4 加载配置文件批量配置黑白名单

通过加载黑白名单配置文件，可以实现快速批量配置黑白名单功能。

前提条件

需要预先配置好黑白名单配置文件。

背景信息

黑白名单配置文件只支持文本格式，格式要求如下：

```
[FirewallBlacklist]  #标识此条目是黑名单
IPAddress =                #黑名单的IP地址，点分十进制格式
VPNName =                  #黑名单所属的VPN实例名称，可选配置，不配置即不填。
[FirewallWhitelist]        #标识此条目是白名单
IPAddress =                #白名单的IP地址，点分十进制格式
VPNName =                  #白名单所属的VPN实例名称，可选配置，不配置即不填。
```

支持多条配置，但必须逐行进行编辑(行与行之间允许空行)，示例如下：

```
[FirewallBlacklist]
IPAddress = 210.10.10.1
VPNName = vpna
[FirewallBlacklist]
IPAddress = 220.10.10.2
VPNName =

[FirewallWhitelist]
IPAddress = 10.10.10.1
VPNName = vpnb
[FirewallWhitelist]
IPAddress =20.20.20.1
VPNName =
```

说明

配置文件最多可支持配置 50K 行。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall black-white-list load configuration-file** *configuration-file-name*，加载黑白名单配置文件。

同执行 firewall blacklist 命令单条配置黑名单一样，仍需要执行 firewall blacklist enable 命令使能后，黑名单功能才会生效。

白名单配置不需要使能，配置的白名单表项直接生效。

黑名单最多支持创建 32 个，白名单最多可以创建 32 个。

----结束

后续处理

执行命令 **firewall black-white-list save** 将设备上的黑白名单保存至指定的配置文件，以便于下次加载。

3.5.5 检查配置结果

配置黑名单之后，可以查看黑名单的相关信息。

操作步骤

- 执行 **display firewall blacklist** 命令查看黑名单的相关信息。

----结束

任务示例

执行命令 **display firewall blacklist**，可以查看黑名单的信息，例如：

```
<Huawei> display firewall blacklist all
Firewall blacklist items :
------------------------------------------------------------------------------
IP-Address      Reason       Expire-Time(m)    VPN-Instance
------------------------------------------------------------------------------
10.1.1.1        Manual       100
------------------------------------------------------------------------------
 Total number is : 1
```

3.6 配置白名单

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。

3.6.1 建立配置任务

在配置白名单之前，了解白名单的应用环境，以及配置白名单需要提前完成的任务和准备的数据。

应用环境

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。

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 地址加入黑名单中。

前置任务

在配置白名单之前，需要完成以下任务。

- 配置安全区域，并将接口加入安全区域。

- 配置安全域间，并在安全域间使能防火墙功能。

数据准备

在配置白名单之前，需要准备以下数据。

序号	数据
1	需要加入白名单的 IP 地址
2	（可选）白名单表项的老化时间

3.6.2 配置白名单表项（单条配置）

白名单配置不需要使能，配置的白名单表项直接生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall whitelist** *ip-address* [**vpn-instance** *vpn-instance-name*] [**expire-time** *minutes*]，添加白名单表项。

本步骤用于手工添加白名单表项，添加时可以指定 IP 地址、老化时间和 VPN 实例。其中老化时间是指 IP 地址添加到白名单后生效的时间，当 IP 地址加入白名单的时间超过老化时间后，该 IP 地址从白名单中释放。如果不指定老化时间，则表示该白名单表项永远有效。

在白名单中最多可以创建 32 条表项。

----结束

后续处理

执行命令 **firewall black-white-list save** 可将设备上的黑白名单保存至指定的配置文件，以便于下次加载。

3.6.3 加载配置文件批量配置黑白名单

通过加载黑白名单配置文件，可以实现快速批量配置黑白名单功能。

前提条件

需要预先配置好黑白名单配置文件。

背景信息

黑白名单配置文件只支持文本格式，格式要求如下：

```
[FirewallBlacklist]  #标识此条目是黑名单
IPAddress =                #黑名单的IP地址，点分十进制格式
VPNName =                  #黑名单所属的VPN实例名称，可选配置，不配置即不填。
[FirewallWhitelist]        #标识此条目是白名单
IPAddress =                #白名单的IP地址，点分十进制格式
VPNName =                  #白名单所属的VPN实例名称，可选配置，不配置即不填。
```

支持多条配置，但必须逐行进行编辑(行与行之间允许空行)，示例如下：

```
[FirewallBlacklist]
IPAddress = 210.10.10.1
VPNName = vpna
[FirewallBlacklist]
IPAddress = 220.10.10.2
VPNName =

[FirewallWhitelist]
IPAddress = 10.10.10.1
VPNName = vpnb
[FirewallWhitelist]
IPAddress =20.20.20.1
VPNName =
```

说明

配置文件最多可支持配置 50K 行。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall black-white-list load configuration-file** *configuration-file-name*，加载黑白名单配置文件。

同执行 firewall blacklist 命令单条配置黑名单一样，仍需要执行 firewall blacklist enable 命令使能后，黑名单功能才会生效。

白名单配置不需要使能，配置的白名单表项直接生效。

黑名单最多支持创建 32 个，白名单最多可以创建 32 个。

----结束

后续处理

执行命令 **firewall black-white-list save** 将设备上的黑白名单保存至指定的配置文件，以便于下次加载。

3.6.4 检查配置结果

配置白名单之后，可以查看白名单的相关信息。

操作步骤

- 执行 **display firewall whitelist** { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **vpn-instance** *vpn-instance-name* }命令查看白名单的相关信息。

----结束

任务示例

执行命令 **display firewall whitelist** { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **vpn-instance** *vpn-instance-name* }，可以查看白名单的信息，例如：

```
<Huawei> display firewall whitelist all
Firewall whitelist items  :
------------------------------------------------------------------------
IP-Address     Expire-Time(m)  Vpn-Instance
------------------------------------------------------------------------
1.1.1.1         3              vpn1
```

```
1.1.1.2         Permanent      vpn2
1.1.1.3         6
 --------------------------------------------------------------------------
 Total number is : 3
```

3.7 配置 ASPF

ASPF 能够检测试图通过防火墙的应用层协议会话信息，阻止不符合规则的数据报文穿过防火墙。同时，还可以使某些无法穿越防火墙的应用协议正常使用。

3.7.1 建立配置任务

在配置 ASPF 之前，了解其应用环境，以及配置 ASPF 需要提前完成的任务和准备的数据。

应用环境

ASPF 可以在两个安全区域之间发生数据流动时，实施应用层的状态检查，丢弃不符合应用层状态的报文。

前置任务

在配置 ASPF 之前，需要完成以下任务。

- 配置安全区域，并将接口加入安全区域。
- 配置安全域间，并在安全域间使能防火墙功能。

数据准备

在配置 ASPF 之前，需要准备以下数据。

序号	数据
1	实施 ASPF 的高优先级安全区域名称和低优先级安全区域名称
2	实施 ASPF 的应用层协议类型
3	各种应用层协议会话表的老化时间（可选）

3.7.2 配置 ASPF 检测功能

ASPF 可以检测过滤应用层的 FTP、HTTP、SIP 和 RTSP 报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall interzone** *zone-name1 zone-name2*，进入安全域间视图。

步骤 3 执行命令 **detect aspf** { **all** | **ftp** | **http** [**activex-blocking** | **java-blocking**] | **rtsp** | **sip** }，配置 ASPF。

应用层协议基本都具有双向交互过程，因此在配置 ASPF 时，无需配置方向，AR1200 自动对双向的数据报文都进行状态检查。

缺省情况下，安全域间未配置 ASPF。

----结束

3.7.3 检查配置结果

配置 ASPF 之后，可以查看 ASPF 的相关信息。

操作步骤

- 执行 **display firewall interzone** [*zone-name1 zone-name2*]命令查看安全域间 ASPF 的相关信息。

----结束

任务示例

执行命令 **display firewall interzone** [*zone-name1 zone-name2*]，可以查看安全域间 ASPF 的相关信息，例如：

```
<Huawei> display firewall interzone
interzone zone2 zone1
 firewall enable
 packet-filter default permit outbound
 packet-filter default permit inbound
 session-log 2006 inbound
 detect aspf ftp
 detect aspf sip
 detect aspf rtsp
 detect aspf http
 detect aspf http java-blocking
 detect aspf http activex-blocking

 total number is : 1
```

3.8 配置端口映射

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，使服务器更少地受到针对某种服务的恶意攻击。

3.8.1 建立配置任务

在配置端口映射之前，了解端口映射的应用环境，以及配置端口映射需要提前完成的任务和准备的数据。

应用环境

通过端口映射，防火墙可以识别使用非知名端口的应用层协议报文，用于 ASPF 等应用层敏感的特性。端口映射支持的应用层协议包括 FTP、DNS、HTTP、SIP 和 RTSP。

端口映射基于 ACL 进行，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。

说明

端口映射功能只对安全域间的数据流生效，因此在配置端口映射时，也必须配置安全区域和安全域间。

前置任务

在配置端口映射之前，需要完成以下任务。

- 配置安全区域，并将接口加入安全区域。
- 配置安全域间，并在安全域间使能防火墙功能。
- 创建基本 ACL 并配置规则。

数据准备

在配置端口映射之前，需要准备以下数据。

序号	数据
1	应用层协议类型
2	映射的自定义端口
3	基本 ACL 的编号

3.8.2 配置端口映射

端口映射支持基于基本 ACL 的协议端口映射。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **port-mapping** { **dns** | **ftp** | **http** | **sip** | **rtsp** } **port** *port-number* **acl** *acl-number*，配置端口映射。

配置端口映射时，一个协议可以配置多个映射端口；一个端口可以映射为多个协议，但是必须通过 ACL 进行区分，匹配不同 ACL 的报文使用不同的映射关系。

说明

端口映射实际上是针对访问某个特定 IP 地址（例如 WWW 服务器）的报文进行协议识别，因此在匹配基本 ACL 规则时，使用报文的目的地址去匹配 ACL 规则中定义的源 IP 地址。

----结束

3.8.3 检查配置结果

配置端口映射之后，可以查看端口映射的相关信息。

操作步骤

- 执行 **display port-mapping [dns | ftp | http | rtsp | sip | port** *port-number* **]**命令查看端口映射的相关信息。

----结束

任务示例

执行命令 **display port-mapping [dns | ftp | http | rtsp | sip | port** *port-number* **]**，可以查看端口映射的信息，例如：

```
<Huawei> display port-mapping dns
 ------------------------------------------------
  Service    Port       Acl        Type
 ------------------------------------------------
 dns          53                 system defined
 ------------------------------------------------
 Total number is : 1
```

3.9 配置防火墙会话表老化时间

3.9.1 建立配置任务

在配置防火墙会话表老化时间之前，了解防火墙会话表老化时间的应用环境，以及配置防火墙会话表老化时间需要提前完成的任务和准备的数据。

应用环境

AR1200 对于通过防火墙的 TCP、UDP、ICMP 等协议的数据流都会建立会话表，用于记录协议的连接状态。会话表中含有老化时间，当其中某条记录长时间未被后续报文命中（超过老化时间）时，该会话表项将会被删除。

如果需要修改某协议会话的老化时间时，可以进行防火墙会话表老化时间的配置。

数据准备

在配置防火墙会话表老化时间之前，需要准备以下数据。

序号	数据
1	各种应用层协议会话表的老化时间

3.9.2 配置防火墙会话表老化时间

若在设定的时间内未使用某条会话表项，则这条会话将失效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall-nat session** { **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** } **aging-time** *time-value*，配置防火墙会话表老化时间。

缺省情况下，各协议的老化时间为：DNS（120 秒），ftp（120 秒），ftp-data（120 秒），HTTP（120 秒），icmp（20 秒），tcp（600 秒），tcp-proxy（10 秒），udp（40 秒），sip（1800 秒），sip-media（120 秒）,rtsp（60 秒），rtsp-media（120 秒）。

说明

通常情况下，不需要改动会话表的老化时间。

----结束

3.9.3 检查配置结果

配置防火墙会话表老化时间之后，可以查看防火墙会话表老化时间的相关信息。

操作步骤

- 执行 **display firewall-nat session aging-time** 命令查看防火墙会话表老化时间的相关信息。

----结束

任务示例

执行命令 **display firewall-nat session aging-time**，可以查看防火墙会话表老化时间的信息，例如：

```
<Huawei> display firewall-nat session aging-time
------------------------------------------
  tcp protocol timeout          : 60    (s)
  tcp-proxy timeout             : 60    (s)
  udp protocol timeout          : 40    (s)
  icmp protocol timeout         : 20    (s)
  dns protocol timeout          : 120   (s)
  http protocol timeout         : 120   (s)
  ftp protocol timeout          : 120   (s)
  ftp-data protocol timeout     : 120   (s)
  rtsp protocol timeout         : 60    (s)
  rtsp-media protocol timeout   : 120   (s)
  sip protocol timeout          : 1800  (s)
  sip-media protocol timeout    : 120   (s)
------------------------------------------
```

3.10 配置攻击防范

攻击防范主要防止攻击报文对 CPU 的攻击，保证服务器在遭受攻击的情况下仍然正常运行。

3.10.1 建立配置任务

在配置攻击防范之前，了解其应用环境，以及配置攻击防范需要提前完成的任务和准备的数据。

应用环境

在 AR1200 中，可以针对某个需要保护的区域配置攻击防范功能。需要保护的区域可以是某些安全区域或者指定的 IP 地址。

前置任务

在配置攻击防范之前，需要完成以下任务。

- 配置安全区域，并将接口加入安全区域。
- 配置安全域间，并在安全域间使能防火墙功能。

数据准备

在配置攻击防范之前，需要准备以下数据。

序号	数据
1	需要防范的攻击类型，可选择某种具体的攻击类型或所有类型
2	对于 Flood 类攻击（ICMP Flood、SYN Flood、UDP Flood），可指定需要进行攻击防范的安全区域或者 IP 地址，指定最大连接速率
3	对于 SYN Flood 攻击，还可以指定 TCP-Proxy 的启用原则，可选择始终启用、始终关闭或者自动启用（当连接数超过最大连接速率时启用）
4	对于扫描类攻击（地址扫描、端口扫描），可指定黑名单超时时间和最大连接速率
5	对于超大 ICMP 报文攻击，可配置报文的最大长度

3.10.2 使能攻击防范

背景信息

以下步骤 2 ～步骤 19 是并列可选的关系，用户可以根据需要选择使能不同类型的攻击防范。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall defend all enable**，使能所有类型的攻击防范。

步骤 3 执行命令 **firewall defend fraggle enable**，使能 Fraggle 攻击防范。

步骤 4 执行命令 **firewall defend icmp-flood enable**，使能 ICMP Flood 攻击防范。

配置 ICMP Flood 攻击防范参数后，必须使能 ICMP Flood 攻击防范，AR1200 才会检测，然后采取相应的攻击防范措施。

步骤 5 执行命令 **firewall defend icmp-redirect enable**，使能 ICMP Redirect 攻击防范。

步骤 6 执行命令 **firewall defend icmp-unreachable enable**，使能 ICMP 不可达攻击防范。

步骤 7 执行命令 **firewall defend ip-fragment enable**，使能 IP-Fragment 攻击防范。

步骤 8 执行命令 **firewall defend ip-sweep enable**，使能地址扫描攻击防范。

配置 IP 地址扫描后，必须使能地址扫描攻击防范，AR1200 才会检测，然后采取相应的攻击防范措施。

步骤 9 执行命令 **firewall defend land enable**，使能 Land 攻击防范。

步骤 10 执行命令 **firewall defend large-icmp enable**，使能超大 ICMP 报文攻击防范。

配置超大 ICMP 报文长度后，必须使能超大 ICMP 报文攻击防范，AR1200 才会检测，然后采取相应的攻击防范措施。

步骤 11 执行命令 **firewall defend ping-of-death enable**，使能 Ping of Death 攻击防范。

步骤 12 执行命令 **firewall defend port-scan enable**，使能端口扫描攻击防范。

配置端口扫描后，必须使能端口扫描攻击防范，AR1200 才会检测，然后采取相应的攻击防范措施。

步骤 13 执行命令 **firewall defend smurf enable**，使能 Smurf 攻击防范。

步骤 14 执行命令 **firewall defend syn-flood enable**，使能 SYN Flood 攻击防范。

配置 SYN Flood 攻击防范参数后，必须使能 SYN Flood 攻击防范，AR1200 才会检测，然后采取相应的攻击防范措施。

步骤 15 执行命令 **firewall defend tcp-flag enable**，使能 TCP 标志攻击防范。

步骤 16 执行命令 **firewall defend teardrop enable**，使能 Teardrop 攻击防范。

步骤 17 执行命令 **firewall defend tracert enable**，使能 Tracert 攻击防范。

步骤 18 执行命令 **firewall defend udp-flood enable**，使能 UDP Flood 攻击防范。

配置 UDP Flood 攻击防范参数后，必须使能 UDP Flood 攻击防范，AR1200 才会检测，然后采取相应的攻击防范措施。

步骤 19 执行命令 **firewall defend winnuke enable**，使能 WinNuke 攻击防范。

缺省情况下，未使能任何类型的攻击防范。

----结束

3.10.3 配置 flood 类攻击防范参数

背景信息

以下步骤 2 ～步骤 4 是并列可选的关系，用户可以根据需要配置不同类型的 Flood 类攻击防范参数。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall defend icmp-flood** { **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **zone** *zone-name* } [**max-rate** *rate-value*]，配置 ICMP Flood 攻击防范参数。

步骤 3 执行命令 **firewall defend syn-flood** { **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **zone** *zone-name* } [**max-rate** *rate-value*] | [**tcp-proxy** { **auto** | **off** | **on** }]，配置 SYN Flood 攻击防范参数。

步骤 4 执行命令 **firewall defend udp-flood** { **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **zone** *zone-name* } [**max-rate** *rate-value*]，配置 UDP Flood 攻击防范参数。

对于 Flood 类攻击防范，需要指定防范的安全区域或者 IP 地址，否则防范不能生效。同时还可以指定最大连接速率，当实际的连接速率超过该值时，AR1200 认为发生了攻击，自动采取攻击防范措施。

对于 Flood 类攻击防范，针对 IP 地址配置的优先级高于针对安全区域配置的优先级。如果对指定 IP 地址配置了 Flood 攻击防范功能，同时也对该 IP 地址所在安全区域配置了 Flood 攻击防范功能，则以 IP 地址所配置的参数为准；如果此时取消针对 IP 地址的配置，则再以安全区域所配置的参数为准。

缺省情况下，Flood 类攻击防范的最大连接速率均为 1000pps，SYN Flood 攻击防范中的 TCP 代理功能自动启用。

Flood 类攻击防范功能最多能够同时配置对 32 个 IP 地址进行保护。

----结束

3.10.4 配置对超大 ICMP 报文的攻击防范

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall defend large-icmp max-length** *length*，配置超大 ICMP 报文攻击防范参数。

对于超大 ICMP 报文攻击防范参数只有一个，即 ICMP 报文的最大长度。当实际 ICMP 报文的长度超过该值时，AR1200 认为发生了超大 ICMP 报文攻击，将丢弃该报文。

缺省情况下，ICMP 报文的最大长度为 4000 字节。

----结束

3.10.5 配置扫描类攻击防范参数

背景信息

以下步骤 2 ～步骤 3 是并列可选的关系，用户可以根据需要配置不同类型的扫描类攻击防范参数。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall defend ip-sweep** { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }，配置地址扫描攻击防范参数。

步骤 3 执行命令 **firewall defend port-scan** { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }，配置端口扫描攻击防范参数。

对于扫描类攻击防范，有两个参数：

- 最大连接速率：当实际针对某个 IP 地址或端口的连接速率超过该值时，AR1200 认为发生了扫描攻击，将该 IP 地址加入黑名单，禁止建立新连接。
- 黑名单超时时间：黑名单具有超时时间，当 IP 地址进入黑名单的时间超过超时时间后，AR1200 将其从黑名单中释放，允许建立新连接。

缺省情况下，地址扫描和端口扫描的最大连接速率均为 4000 pps，黑名单超时时间均为 20 分钟。

----结束

3.10.6 检查配置结果

配置攻击防范之后，可以查看攻击防范的相关信息。

操作步骤

- 执行 **display firewall defend** { **flag** | { **icmp-flood** | **syn-flood** | **udp-flood** } [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]] | *other-attack-type* } 命令查看攻击防范的相关信息。

----结束

任务示例

执行命令 **display firewall defend** { **flag** | { **icmp-flood** | **syn-flood** | **udp-flood** } [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]] | *other-attack-type* }，可以查看攻击防范的信息，例如：

显示当前设备上各种攻击防范功能的使能状态。

```
<Huawei> display firewall defend flag
--------------------------------
  Type                   Flag
--------------------------------
  land                 : disable
  smurf                : disable
  fraggle              : disable
  winnuke              : disable
  syn-flood            : disable
  udp-flood            : disable
  icmp-flood           : disable
  icmp-redirect        : disable
  icmp-unreachable     : disable
  ip-sweep             : disable
  port-scan            : disable
  tracert              : disable
  ping-of-death        : disable
  teardrop             : disable
  tcp-flag             : disable
  ip-fragment          : disable
  large-icmp           : disable
--------------------------------
```

显示当前设备上 ip-sweep 攻击防范的配置信息。

```
<Huawei> display firewall defend ip-sweep

  defend-flag          : disable
  max-rate             : 4000  (pps)
  blacklist-expire-time : 20    (m)
```

3.11 配置流量统计和监控

AR1200 支持针对系统级、安全区域和 IP 的流量统计和监控。

3.11.1 建立配置任务

在配置流量统计和监控之前，了解其应用环境，以及配置流量统计和监控需要提前完成的任务和准备的数据。

应用环境

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 AR1200 会统计所有安全域间的 ICMP、TCP、TCP-Proxy、UDP 等连接数。当连接数超过配置阈值时，AR1200 采取限制连接措施，直至连接数降至阈值以下。

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 AR1200 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。当连接总数超过配置的阈值时，AR1200 采取限制连接数措施，直至连接数降至阈值以下。安全区域的流量统计和监控功能，可以按入方向和出方向分别配置。入方向是指统计和监控本安全区域为源端的连接；出方向是指统计和监控本安全区域为目的端的连接。

IP 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。当单个 IP 地址建立的 TCP/UDP 连接数超过配置的阈值时，AR1200 采取限制连接数措施，直至连接数降至阈值以下。IP 流量统计和监控功能，可以按入方向和出方向分别配置。入方向是指统计和监控本安全区域中的 IP 地址为源端的连接；出方向是指统计和监控本安全区域中的 IP 地址为目的端的连接。

前置任务

在配置流量统计和监控之前，需要完成以下任务。

- 配置安全区域，并将接口加入安全区域。
- 配置安全域间，并在安全域间使能防火墙功能。

数据准备

在配置流量统计和监控之前，需要准备以下数据。

序号	数据
1	流量统计和监控的类型，可以选择 TCP、UDP 等
2	流量统计和监控的连接数阈值
3	安全区域流量统计和监控的方向

3.11.2 使能流量统计和监控功能

可根据实际应用使能系统级、安全区域和 IP 的流量统计和监控功能。

操作步骤

- 使能系统流量统计和监控：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **firewall statistics system enable**，使能系统流量统计和监控。

     缺省情况下，防火墙的系统流量统计功能未使能。
- 使能安全区域流量统计和监控：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **firewall zone** *zone-name*，进入安全区域视图。
  3. 执行命令 **statistics zone enable** { **inzone** | **outzone** }，使能安全区域流量统计和监控。

     缺省情况下，设备未使能对安全区域的流量统计功能。
- 使能 IP 流量统计和监控：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **firewall zone** *zone-name*，进入安全区域视图。
  3. 执行命令 **statistics ip enable** { **inzone** | **outzone** }，使能 IP 流量统计和监控。

     缺省情况下，设备未使能对安全区域的 IP 流量统计功能。

----结束

3.11.3 配置流量统计和监控的会话数阈值

可根据实际应用配置系统级、安全区域和 IP 流量统计和监控的阈值。

操作步骤

- 配置系统流量统计和监控的阈值：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **firewall statistics system enable**，使能系统流量统计和监控。

     缺省情况下，防火墙的系统流量统计功能未使能。
  3. 执行命令 **firewall statistics system connect-number** { **frag** | **icmp** | **tcp** | **tcp-proxy** | **udp** } **high** *high-threshold* **low** *low-threshold*，配置系统流量统计和监控的阈值。

     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 的连接数阈值设置为 15000 时，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，AR1200 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。

缺省情况下，防火墙对各协议报文的连接数的上限阈值为 16384、下限阈值为 12288。

- 配置安全区域流量统计和监控的阈值：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **firewall zone** *zone-name*，进入安全区域视图。
  3. 执行命令 **statistics zone enable** { **inzone** | **outzone** }，使能安全区域流量统计和监控。

     缺省情况下，设备未使能对安全区域的流量统计功能。
  4. 执行命令 **statistics connect-number zone** { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** } **high** *high-threshold* **low** *low-threshold*，配置安全区域流量统计和监控的阈值。

     安全区域的流量统计功能可以针对 TCP/UDP 连接，在入和出两个方向配置其阈值。例如当入方向 TCP 连接数阈值为 15000 时，当本区域向其他区域发起的 TCP 连接总数超过 15000，AR1200 将拒绝本区域向其他区域发起新的 TCP 连接请求。

     缺省情况下，防火墙对各协议报文的连接数的上限阈值为 16384、下限阈值为 12288。
- 配置 IP 流量统计和监控的阈值：
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **firewall zone** *zone-name*，进入安全区域视图。
  3. 执行命令 **statistics ip enable** { **inzone** | **outzone** }，使能 IP 流量统计和监控。

     缺省情况下，设备未使能对安全区域的 IP 流量统计功能。
  4. 执行命令 **statistics connect-number ip** { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** } **high** *high-threshold* **low** *low-threshold*，配置安全区域 IP 流量统计和监控的阈值。

     IP 流量统计功能可以针对 TCP/UDP 连接，在入和出两个方向配置其阈值。例如当入方向 TCP 连接数阈值为 10000 时，当本区域中某个 IP 地址向其他区域发起的 TCP 连接总数超过 10000，AR1200 将拒绝该 IP 地址向其他区域发起新的 TCP 连接请求。

     缺省情况下，防火墙对各协议报文的连接数的上限阈值为 16384、下限阈值为 12288。

----结束

3.11.4 检查配置结果

配置流量统计和监控之后，可以查看流量统计和监控的相关信息。

操作步骤

- 执行 **display firewall statistics system** 命令查看系统流量统计和监控的相关信息。
- 执行 **system-view** 命令，进入系统视图。执行 **display firewall statistics zone** *zone-name* { **inzone** | **outzone** } **all** 命令查看安全区域流量统计和监控间的相关信息。
- 执行 **display firewall statistics zone-ip** *zone-name* 命令查看安全区域 IP 流量统计和监控间的相关信息。

----结束

3.12 配置日志输出

防火墙日志包括流日志、统计日志、攻击日志和黑名单日志。

3.12.1 建立配置任务

在配置防火墙日志之前，了解防火墙日志的应用环境，以及配置防火墙日志需要提前完成的任务和准备的数据。

应用环境

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。

前置任务

在配置防火墙日志之前，需要完成以下任务。

- 配置安全区域，并将接口加入安全区域。
- 配置安全域间，并在安全域间使能防火墙功能。
- 创建基本 ACL 或高级 ACL 并配置规则。

数据准备

在配置防火墙日志之前，需要准备以下数据。

序号	数据
1	防火墙日志的类型
2	流日志主机的 IP 地址、端口号，AR1200 和流日志主机通讯用的源 IP 地址、源端口
3	配置记录流日志的条件，包括 ACL 编号和方向
4	攻击日志和统计日志的输出时间（可选）

3.12.2 使能防火墙日志功能

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall log** { **all** | **blacklist** | **defend** | **session** | **statistics** } **enable**，使能防火墙日志功能。

防火墙日志功能可以按类别分别使能，也可以使用 **all** 参数全部使能。

缺省情况下，防火墙日志功能未使能。

步骤 3 执行命令 **firewall log session nat enable**，使能 NAT 类型的流日志功能。

必须先执行 **firewall log session enable** 命令，使能 NAT 类型的流日志功能才能生效。

缺省情况下，NAT 类型的流日志功能未使能。

----结束

3.12.3 配置日志其他参数

配置流日志主机、记录流日志的条件和日志的输出时间间隔。

背景信息

流日志实时向日志主机输出，因此首先需要配置日志主机。包括日志主机的 IP 地址、端口号，以及 AR1200 和日志主机通讯所使用的源 IP 地址和源端口号。

在安全域间可以根据 ACL 来设置记录流日志的条件，同时可以针对出方向和入方向分别配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **firewall log binary-log host** *host-ip-address host-port* **source** *source-ip-address source-port* [**vpn-instance** *vpn-instance-name*]，配置流日志主机。

缺省情况下，流日志主机未配置。

步骤 3 （可选）执行命令 **firewall log** { **blacklist** | **defend** | **session** | **statistics** } **log-interval** *time*，配置日志输出时间间隔。

缺省情况下，设备定时输出日志的时间间隔为 30 秒。

步骤 4 执行命令 **firewall interzone** *zone-name1 zone-name2*，进入安全域间视图。

步骤 5 执行命令 **session-log** *acl-number* { **inbound** | **outbound** }，配置记录流日志的条件。

缺省情况下，安全域间没有配置记录流日志的条件。

----结束

3.12.4 检查配置结果

配置防火墙日志之后，可以查看防火墙日志的相关信息。

操作步骤

- 执行 **display firewall log configuration** 命令查看防火墙日志的相关信息。

----结束

任务示例

执行命令 **display firewall log configuration**，可以查看防火墙日志的信息，例如：

```
<Huawei> display firewall log configuration
defend log :
  status : enabled
  log-interval : 30 s
statistics log :
  status : enabled
  log-interval : 30 s
blacklist log :
  status : enabled
  log-interval : 30 s
session log :
  status : enabled
  log-interval : 30 s
  nat-session : disabled
binary-log host :
  host                  source                VPN instance-name
  ----:--               ----:--               ---
```

3.13 维护防火墙

3.13.1 显示防火墙配置

操作步骤

- 执行命令 **display firewall zone** [*zone-name*] | [**interface** | **priority**]查看全部或指定安全区域的配置信息。
- 执行命令 **display firewall interzone** [*zone-name1 zone-name2*]查看安全域间的信息。
- 执行命令 **display firewall blacklist configuration** 查看防火墙黑名单功能是否使能。
- 执行命令 **display firewall blacklist** { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **dynamic** | **static** | **vpn-instance** *vpn-instance-name* }查看防火墙黑名单表项的内容。
- 执行命令 **display firewall whitelist** { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **vpn-instance** *vpn-instance-name* }查看白名单表项的信息。
- 执行命令 **display firewall statistics system** 查看防火墙的系统流量统计信息。
- 执行命令 **display firewall statistics zone** *zone-name* { **inzone** | **outzone** } **all** 查看安全区域的流量统计和监控信息。
- 执行命令 **display firewall statistics zone-ip** *zone-name* 显示指定域下域的流量监控使能情况与各种协议配置的监控阈值。
- 执行命令 **display firewall-nat session aging-time** 查看防火墙设备上会话表项的超时时间。
- 执行命令 **display port-mapping** [**dns** | **ftp** | **http** | **rtsp** | **sip** | **port** *port-number*]查看指定的应用层协议和端口的映射关系。
- 执行命令 **display firewall defend** { **flag** | { **icmp-flood** | **syn-flood** | **udp-flood** } [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]] | *other-attack-type* }查看各种攻击防范功能的使能状态和配置信息。
- 执行命令 **display firewall log configuration** 用来查看防火墙日志的全局配置信息。
- 执行命令 **display firewall session** 用来查看 Firewall 的流表信息。

----结束

3.13.2 清除防火墙统计信息

背景信息

为了能够清楚地查看某一时间段内设备正常通信的报文，可以执行下面的命令先清空之前的报文统计数。

步骤 2、步骤 3 是并列可选的关系，用户可以根据需要选择清空不同的报文统计数。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **clear firewall statistics system normal**，清空系统正常报文的报文统计数。

步骤 3 执行命令 **clear firewall statistics zone** *zone-name*，清空安全区域正常报文的报文统计数。

----结束

3.14 配置示例

介绍使用放火墙提高网络安全性的各种示例。

3.14.1 配置 ACL 包过滤防火墙典型示例

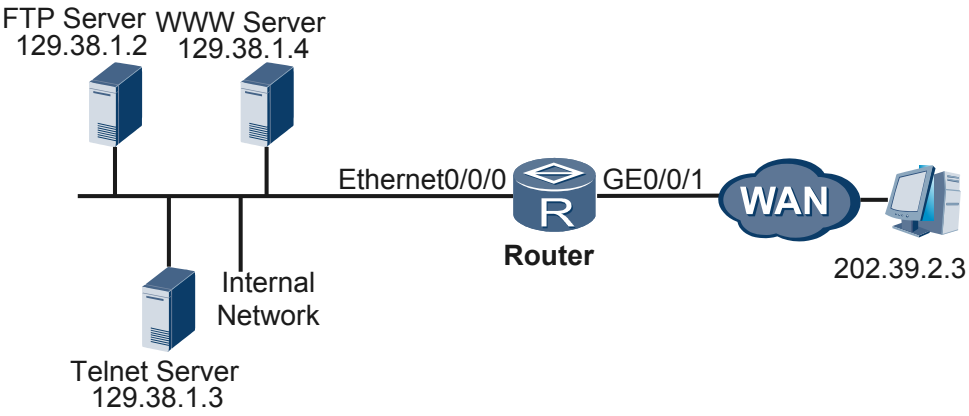
ACL 包过滤防火墙在具体组网中的应用。根据数据流的源、目的 IP 地址，源、目的端口号，协议类型五元组过滤数据流，提高数据流的安全性。

组网需求

如图 3-2 所示，Router 的接口 Ethernet0/0/0 连接一个高安全优先级的内部网络，接口 GE0/0/1 连接低安全优先级的外部网络，需要对内部网络和外部网络之间的通信实施包过滤。具体要求如下：

- 外部特定主机（202.39.2.3）允许访问内部网络中的服务器。
- 其余的访问均不允许。

图 3-2 配置 ACL 包过滤组网图



配置思路

采用如下思路配置 ACL 包过滤防火墙：

1. 配置安全区域和安全域间。
2. 将接口加入安全区域。
3. 配置 ACL。
4. 在安全域间配置基于 ACL 的包过滤。

操作步骤

步骤 1 在 Router 上配置安全区域和安全域间。

```
<Huawei> system-view
[Huawei] firewall zone trust
[Huawei-zone-trust] priority 15
[Huawei-zone-trust] quit
[Huawei] firewall zone untrust
[Huawei-zone-untrust] priority 1
[Huawei-zone-untrust] quit
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] firewall enable
[Huawei-interzone-trust-untrust] quit
```

步骤 2 在 Router 上将接口加入安全区域。

```
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 129.38.1.1 24
[Huawei-Vlanif100] quit
[Huawei] interface Ethernet 0/0/0
[Huawei-Ethernet0/0/0] port link-type access
[Huawei-Ethernet0/0/0] port default vlan 100
[Huawei-Ethernet0/0/0] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] zone trust
[Huawei-Vlanif100] quit
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ip address 202.39.2.1 24
[Huawei-GigabitEthernet0/0/1] zone untrust
[Huawei-GigabitEthernet0/0/1] quit
```

步骤 3 在 Router 上配置 ACL。

```
[Huawei] acl 3102
[Huawei-acl-adv-3102] rule permit tcp source 202.39.2.3 0.0.0.0 destination 129.38.1.2 0.0.0.0
[Huawei-acl-adv-3102] rule permit tcp source 202.39.2.3 0.0.0.0 destination 129.38.1.3 0.0.0.0
[Huawei-acl-adv-3102] rule permit tcp source 202.39.2.3 0.0.0.0 destination 129.38.1.4 0.0.0.0
[Huawei-acl-adv-3102] rule deny ip
[Huawei-acl-adv-3102] quit
```

步骤 4 在 Router 上配置包过滤。

```
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] packet-filter 3102 inbound
[Huawei-interzone-trust-untrust] quit
```

步骤 5 检查配置结果。

配置成功后，仅特定主机（202.39.2.3）可以访问内部服务器。

在 Router 上执行 **display firewall interzone** [*zone-name1 zone-name2*]操作，结果如下。

```
[Huawei] display firewall interzone trust untrust
interzone trust untrust
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3102 inbound
```

----结束

配置文件

```
#
 vlan 100
#
acl number 3102
 rule 5 permit tcp source 202.39.2.3 0 destination 129.38.1.2 0
 rule 10 permit tcp source 202.39.2.3 0 destination 129.38.1.3 0
 rule 15 permit tcp source 202.39.2.3 0 destination 129.38.1.4 0
 rule 20 deny ip
#
interface Vlanif100
 ip address 129.38.1.1 255.255.255.0
zone trust
#
firewall zone trust
 priority 15
#
firewall zone untrust
 priority 1
#
firewall interzone trust untrust
 firewall enable
 packet-filter 3102 inbound
#
interface Ethernet0/0/0
 port link-type access
 port default vlan 100
#
interface
GigabitEthernet0/0/1
 ip address 202.39.2.1 255.255.255.0
 zone untrust
#
return
```

3.14.2 配置 ASPF 和端口映射示例

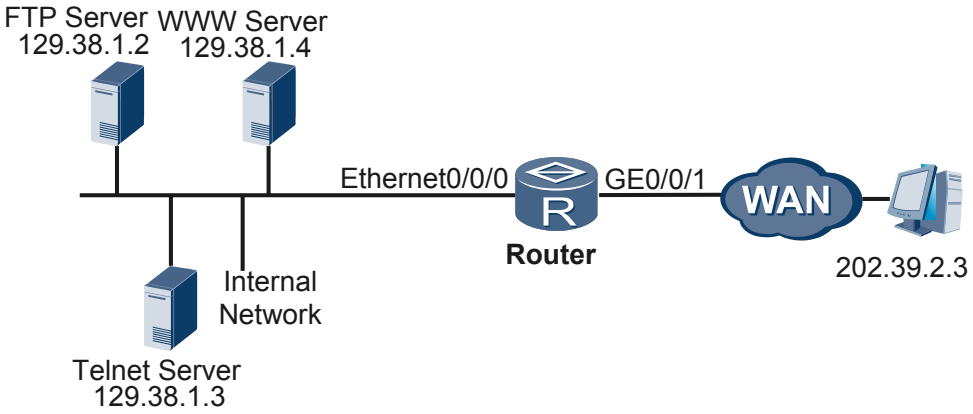
ASPF 和端口映射在具体组网中的应用。检测指定的应用层协议报文，过滤掉不符合规则的应用层数据报文。

组网需求

如图 3-3 的接口 Ethernet0/0/0 连接一个高安全优先级的内部网络，接口 GE0/0/1 连接低安全优先级的外部网络，需要对内部网络和外部网络之间的通信实施包过滤和 ASPF 检查。具体要求如下：

- 外部特定主机（202.39.2.3）允许访问内部网络中的服务器。
- 其余的访问均不允许。
- 对上述访问的连接进行 FTP 状态检查，过滤不符合状态的报文。
- 对于外部主机访问 FTP 服务器的报文，识别 2121 端口为 FTP 协议。

图 3-3 配置 ASPF 和端口映射组网图



配置思路

采用如下思路配置 ASPF 和端口映射：

1. 配置安全区域和安全域间。
2. 将接口加入安全区域。
3. 配置 ACL。
4. 在安全域间配置基于 ACL 的包过滤。
5. 在安全域间配置 ASPF。
6. 配置端口映射，将 2121 端口映射为 FTP 协议通信端口。

操作步骤

步骤 1 在 Router 上配置安全区域和安全域间。

```
<Huawei> system-view
[Huawei] firewall zone trust
[Huawei-zone-trust] priority 15
[Huawei-zone-trust] quit
[Huawei] firewall zone untrust
[Huawei-zone-untrust] priority 1
[Huawei-zone-untrust] quit
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] firewall enable
[Huawei-interzone-trust-untrust] quit
```

步骤 2 在 Router 上将接口加入安全区域。

```
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 129.38.1.1 24
[Huawei-Vlanif100] quit
[Huawei] interface Ethernet 0/0/0
[Huawei-Ethernet0/0/0] port link-type access
[Huawei-Ethernet0/0/0] port default vlan 100
[Huawei-Ethernet0/0/0] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] zone trust
[Huawei-Vlanif100] quit
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ip address 202.39.2.1 24
```

```
[Huawei-GigabitEthernet0/0/1] zone untrust
[Huawei-GigabitEthernet0/0/1] quit
```

步骤 3 在 Router 上配置 ACL。

```
[Huawei] acl 2102
[Huawei-acl-basic-2102] rule permit source 129.38.1.2 0.0.0.0
[Huawei-acl-basic-2102] quit
[Huawei] acl 3102
[Huawei-acl-adv-3102] rule permit tcp source 202.39.2.3 0.0.0.0 destination 129.38.1.2 0.0.0.0
[Huawei-acl-adv-3102] rule permit tcp source 202.39.2.3 0.0.0.0 destination 129.38.1.3 0.0.0.0
[Huawei-acl-adv-3102] rule permit tcp source 202.39.2.3 0.0.0.0 destination 129.38.1.4 0.0.0.0
[Huawei-acl-adv-3102] rule deny ip
[Huawei-acl-adv-3102] quit
```

步骤 4 在 Router 上配置包过滤。

```
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] packet-filter 3102 inbound
[Huawei-interzone-trust-untrust] quit
```

步骤 5 在 Router 上配置 ASPF。

```
[Huawei-interzone-trust-untrust] detect aspf ftp
[Huawei-interzone-trust-untrust] quit
```

步骤 6 在 Router 上配置端口映射。

```
[Huawei] port-mapping ftp port 2121 acl 2102
```

步骤 7 检查配置结果。

在 Router 上执行 **display firewall interzone** *zone-name1 zone-name2* 操作，结果如下。

```
[Huawei] display firewall interzone trust untrust
 interzone trust untrust
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3102 inbound
 detect aspf ftp
```

在 Router 上执行 **display port-mapping ftp** 操作，结果如下。

```
[Huawei] display port-mapping ftp
  ------------------------------------------------
  Service    Port       Acl        Type
 ------------------------------------------------
  ftp          21                   system defined
  ftp        2121      2102        user   defined
 ------------------------------------------------
 Total number is : 2
```

----结束

配置文件

```
#
 vlan 100
 #
acl number 2102
rule 5 permit source 129.38.1.2 0
#
acl number 3102
 rule 5 permit tcp source 202.39.2.3 0 destination 129.38.1.2 0
 rule 10 permit tcp source 202.39.2.3 0 destination 129.38.1.3 0
 rule 15 permit tcp source 202.39.2.3 0 destination 129.38.1.4 0
 rule 20 deny ip
#
port-mapping ftp port 2121 acl 2102
#
```

```
interface Vlanif100
 ip address 129.38.1.1 255.255.255.0
zone trust
#
firewall zone trust
priority 15
#
firewall zone untrust
priority 1
#
firewall interzone trust untrust
firewall enable
packet-filter 3102 inbound
detect aspf ftp
#
interface Ethernet0/0/0
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/1
ip address 202.39.2.1 255.255.255.0
zone untrust
#
return
```

3.14.3 配置黑名单示例

黑名单在具体组网中的应用。防止特定 IP 地址的攻击。

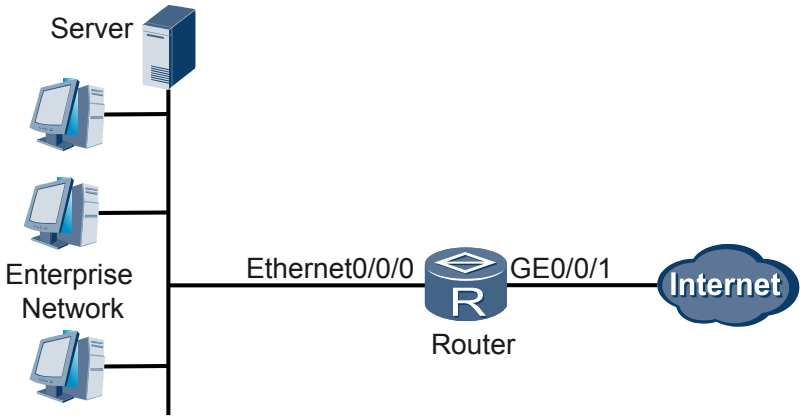
组网需求

如图 3-4 所示，Router 的接口 Ethernet0/0/0 连接一个高安全优先级的内部网络，接口 GE0/0/1 连接低安全优先级的外部网络。

需要对互联网访问企业网的流量配置 IP 地址扫描攻击防范和黑名单功能，一旦发现某个 IP 地址对企业网发起了 IP 地址扫描攻击，则自动把该 IP 地址加入黑名单。其中最大连接速率为 5000 pps，黑名单超时时间为 30 分钟。

另外，由于发现 IP 地址 202.39.1.2 多次企图对企业网发起攻击，因此将其手工加入黑名单，永久有效。

图 3-4 配置黑名单组网图



配置思路

采用如下思路配置黑名单：

1. 配置安全区域和安全域间。
2. 将接口加入安全区域。
3. 使能防火墙黑名单功能。
4. 添加黑名单表项。
5. 使能地址扫描或端口扫描攻击功能。
6. 配置地址扫描或端口扫描攻击的 max-rate 及动态黑名单老化时间。

操作步骤

步骤 1 在 Router 上配置安全区域和安全域间。

```
[Huawei] firewall zone trust
[Huawei-zone-trust] priority 15
[Huawei-zone-trust] quit
[Huawei] firewall zone untrust
[Huawei-zone-untrust] priority 1
[Huawei-zone-untrust] quit
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] firewall enable
[Huawei-interzone-trust-untrust] quit
```

步骤 2 在 Router 上将接口加入安全区域。

```
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 129.38.1.1 24
[Huawei-Vlanif100] quit
[Huawei] interface Ethernet 0/0/0
[Huawei-Ethernet0/0/0] port link-type access
[Huawei-Ethernet0/0/0] port default vlan 100
[Huawei-Ethernet0/0/0] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] zone trust
[Huawei-Vlanif100] quit
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ip address 202.39.2.1 24
[Huawei-GigabitEthernet0/0/1] zone untrust
[Huawei-GigabitEthernet0/0/1] quit
```

步骤 3 使能黑名单功能。

```
[Huawei] firewall blacklist enable
```

步骤 4 添加黑名单表项。

```
[Huawei] firewall blacklist 202.39.1.2
```

步骤 5 使能 IP 地址和端口扫描攻击防范。

```
[Huawei] firewall defend ip-sweep enable
[Huawei] firewall defend port-scan enable
```

步骤 6 配置地址扫描或端口扫描攻击的 max-rate 及动态黑名单老化时间。

```
[Huawei] firewall defend ip-sweep max-rate 5000
[Huawei] firewall defend ip-sweep blacklist-expire-time 30
[Huawei] firewall defend port-scan max-rate 5000
[Huawei] firewall defend port-scan blacklist-expire-time 30
```

步骤 7 检查配置结果。

在 Router 上执行 **display firewall interzone** [*zone-name1 zone-name2*]操作，结果如下。

```
[Huawei] display firewall interzone trust untrust
 interzone trust untrust
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
```

在 Router 上执行 **display firewall blacklist all** 操作，结果如下。

```
[Huawei] display firewall blacklist all
Firewall Blacklist Items :
------------------------------------------------------------------------------
IP-Address      Reason       Expire-Time(m) VPN-Instance
------------------------------------------------------------------------------
202.39.1.2      Manual       Permanent
------------------------------------------------------------------------------
 total number is : 1
```

在 Router 上执行 **display firewall defend** 查看地址扫描或端口扫描的配置结果，如下。

```
[Huawei] display firewall defend port-scan
  defend-flag               : enable
  max-rate                  : 5000  (pps)
  blacklist-expire-time     : 30    (m)

[Huawei] display firewall defend ip-sweep
  defend-flag               : enable
  max-rate                  : 5000  (pps)
  blacklist-expire-time     : 30    (m)
```

----结束

配置文件

```
#
 firewall defend ip-sweep enable
 firewall defend port-scan enable
 firewall defend ip-sweep max-rate 5000
 firewall defend ip-sweep blacklist-expire-time 30
 firewall defend port-scan max-rate 5000
 firewall defend port-scan blacklist-expire-time 30
#
 firewall blacklist enable
 firewall blacklist 202.39.1.2
#
 vlan
100
#
interface Vlanif100
ip address 129.38.1.1 255.255.255.0
zone trust
#
firewall zone trust
priority 15
#
firewall zone untrust
priority 1
#
firewall interzone trust untrust
firewall enable
#
interface Ethernet0/0/0
 port link-type access
 port default vlan 100
#
interface GigabitEthernet0/0/1
ip address 202.39.2.1 255.255.255.0
```

```
zone untrust
#
```

4 流量抑制配置

关于本章

介绍流量抑制的基本原理、配置方法和配置举例。

4.1 流量抑制概述
简单介绍流量抑制的基本原理。

4.2 AR1200 支持的流量抑制特性
介绍 AR1200 支持的流量抑制特性。

4.3 配置流量抑制
介绍在指定接口下配置流量抑制的方法。

4.4 配置举例
介绍流量抑制的配置举例。

4.1 流量抑制概述

简单介绍流量抑制的基本原理。

进入 AR1200 的广播报文会在该 VLAN 的所有端口被转发，组播报文也会在该组播组的端口被转发。而未知单播报文进入后，AR1200 将会向该 VLAN 的所有端口广播该报文。可以看到，这三类报文会大量占用系统资源，降低系统的可用带宽，影响正常的转发能力和处理能力。

流量抑制功能可以限制进入端口的这些类型的流量。保障 AR1200 免受这三种流量的冲击，在网络流量异常的情况下，保证设备的可用带宽和处理能力。

4.2 AR1200 支持的流量抑制特性

介绍 AR1200 支持的流量抑制特性。

AR1200 支持在以太接口下配置流量抑制功能，包括对广播、组播和未知单播报文按照字节模式或包模式的方式在接口下进行流量抑制。

4.3 配置流量抑制

介绍在指定接口下配置流量抑制的方法。

4.3.1 建立配置任务

在配置流量抑制前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

当 AR1200 收到未知单播、组播或广播报文时，由于根据报文的目的 MAC 地址并不能明确指定出接口，AR1200 会向 VLAN 内除了接收接口之外的所有接口转发这些流量，这样可能导致广播风暴，降低 AR1200 的转发性能。因此需要限制进入接口的广播、组播或未知单播类型报文的速率，避免设备受到大的流量冲击，使得流量激增时可以保证 AR1200 依然能进行正常的单播转发，此时可以在该接口上配置对应类型的流量抑制功能。

前置任务

在配置流量抑制之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置流量抑制之前，需要准备以下数据。

序号	数据
1	需要配置流量抑制的接口类型和编号
2	需要抑制的流量类型（广播、组播或未知单播）
3	基于何种方式来抑制流量（字节模式或包模式） **说明** 只有 AR1220 主控板上 LAN 侧的 8 个固定 Ethernet 接口支持以字节模式进行流量抑制。
4	限制的速率值（承诺信息速率值或包模式速率值） **说明** 只有 AR1220 主控板上 LAN 侧的 8 个固定 Ethernet 接口支持以承诺信息速率值进行流量抑制。

4.3.2 配置接口的流量抑制

介绍接口流量抑制功能的配置。

背景信息

在需要进行流量抑制的 AR1200 上进行如下配置。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

步骤 3 配置接口的流量抑制，方式如下：

- 以字节模式进行流量抑制的配置。
  - 执行命令 **broadcast-suppression cir** *cir-value*，以字节模式对广播报文的流量抑制进行配置。
  - 执行命令 **multicast-suppression cir** *cir-value*，以字节模式对组播报文的流量抑制进行配置。
  - 执行命令 **unicast-suppression cir** *cir-value*，以字节模式对未知单播报文的流量抑制进行配置。

  说明

  AR1220 主控板 LAN 侧的 8 个固定 Ethernet 接口支持以字节模式进行流量抑制。
- 以包模式进行流量抑制的配置。
  - 执行命令 **broadcast-suppression packets** *packets-per-second*，以包模式对广播报文的流量抑制进行配置。
  - 执行命令 **multicast-suppression packets** *packets-per-second*，以包模式对组播报文的流量抑制进行配置。
  - 执行命令 **unicast-suppression packets** *packets-per-second*，以包模式对未知单播报文的流量抑制进行配置。

说明

AR1200 主控板不支持包模式的流量抑制功能，接口板上 LAN 侧的 GE 接口、Ethernet 接口支持以包模式进行流量抑制。

----结束

4.3.3 检查配置结果

检查流量抑制的配置结果。

前提条件

已完成流量抑制配置。

操作步骤

- 使用命令 **display flow-suppression interface** *interface-type interface-number* 查看流量抑制配置信息。

----结束

任务示例

执行命令 **display flow-suppression interface** *interface-type interface-number* 可以查看指定接口下的流量抑制配置。

```
<AR1200> display flow-suppression interface ethernet 2/0/1
  storm type         rate mode   set rate value
-------------------------------------------------------------------------------
 unknown-unicast     pps         packets: 1260(packets per second)
 multicast           pps         packets: 2520(packets per second)
 broadcast           pps         packets: 1260(packets per second)
-------------------------------------------------------------------------------
```

4.4 配置举例

介绍流量抑制的配置举例。

4.4.1 配置以字节模式进行流量抑制示例

介绍以字节模式进行流量抑制的基本配置过程。

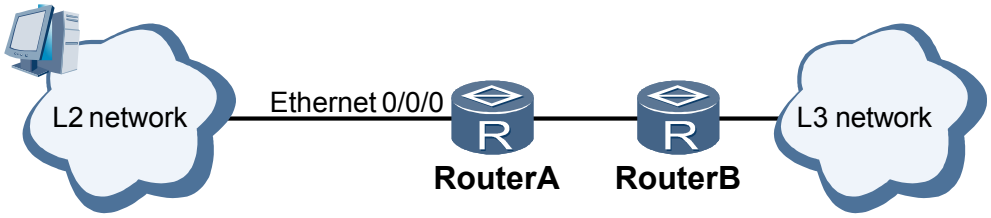
组网需求

如图 4-1 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 Ethernet 0/0/0 接口上配置按字节模式进行流量抑制来实现。

说明

图 4-1 中的 RouterA 是指 AR1200 设备，RouterB 是指汇聚路由器。只有 AR1200 主控板上 LAN 侧的固定 Ethernet 接口支持以字节模式进行流量抑制。

图 4-1 配置以字节模式进行流量抑制组网图



配置思路

采用如下的思路:

- 直接在 Ethernet 0/0/0 接口视图下配置以字节模式进行流量抑制的功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 配置流量抑制的接口名称为 Ethernet 0/0/0。
- 流量抑制后的广播、未知单播报文的承诺信息速率为 100kbit/s，组播报文的承诺信息速率为 200kbit/s。

操作步骤

步骤 1 进入接口视图

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface ethernet 0/0/0
```

步骤 2 配置广播报文以字节模式进行流量抑制

```
[RouterA-Ethernet0/0/0] broadcast-suppression cir 100
```

步骤 3 配置组播报文以字节模式进行流量抑制

```
[RouterA-Ethernet0/0/0] multicast-suppression cir 200
```

步骤 4 配置未知单播报文以字节模式进行流量抑制

```
[RouterA-Ethernet0/0/0] unicast-suppression cir 100
```

步骤 5 验证配置结果

执行命令 **display flow-suppression interface** 查看 Ethernet 0/0/0 接口下的流量抑制配置情况。

```
[RouterA] display flow-suppression interface Ethernet 0/0/0
 storm type         rate mode    set rate value
-------------------------------------------------------------------------------
 unknown-unicast    bps          cir: 100(kbit/s)
 multicast          bps          cir: 200(kbit/s)
 broadcast          bps          cir: 100(kbit/s)
-------------------------------------------------------------------------------
```

----结束

配置文件

```
#
```

```
 sysname RouterA
#
interface Ethernet 0/0/0
 unicast-suppression cir 100
 multicast-suppression cir 200
 broadcast-suppression cir 100
#
return
```

4.4.2 配置以包模式进行流量抑制示例

介绍以包模式进行流量抑制的基本配置过程。

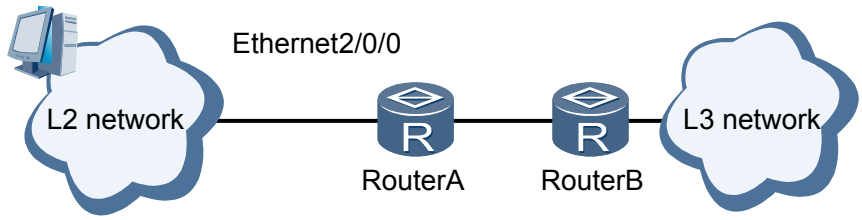
组网需求

如图 4-2 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 Ethernet 2/0/0 接口上配置以包模式进行流量抑制来实现。

说明

图 4-2 中的 RouterA 是指企业路由器，RouterB 是指汇聚路由器。

图 4-2 配置以包模式进行流量抑制组网图



配置思路

采用如下的思路：

- 直接在 Ethernet 2/0/0 接口视图下配置以包模式进行流量抑制的功能。

数据准备

为完成此配置举例，需要准备如下数据：

- 配置流量抑制的接口名称为 Ethernet 2/0/0。
- 广播、组播和未知单播以包模式进行流量抑制。
- 流量抑制后的广播、未知单播报文的包模式的速率值为 12600pps，组播报文的包模式的速率值为 25200pps。

操作步骤

步骤 1 进入接口视图

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface ethernet 2/0/0
```

步骤 2 配置广播报文以包模式进行流量抑制

```
[RouterA-Ethernet2/0/0] broadcast-suppression packets 12600
```

步骤 3 配置组播报文以包模式进行流量抑制

```
[RouterA-Ethernet2/0/0] multicast-suppression packets 25200
```

步骤 4 配置未知单播报文以包模式进行流量抑制

```
[RouterA-Ethernet2/0/0] unicast-suppression packets 12600
```

步骤 5 验证配置结果

执行命令 **display flow-suppression interface** 查看 Ethernet 2/0/0 接口下的流量抑制配置情况。

```
[RouterA] display flow-suppression interface Ethernet 2/0/0
 storm type         rate mode   set rate value
-------------------------------------------------------------------------------
 unknown-unicast    pps         pps: 12600(packet/s)
 multicast          pps         pps: 25200(packet/s)
 broadcast          pps         pps: 12600(packet/s)
-------------------------------------------------------------------------------
```

----结束

配置文件

```
#
 sysname RouterA
#
interface Ethernet 2/0/0
 unicast-suppression packets 12600
 multicast-suppression packets 25200
 broadcast-suppression packets 12600
#
return
```

5 NAC 配置

关于本章

介绍了 NAC 的体系结构，基本原理和常用认证方式。

5.1 NAC 概述
网络接入控制 NAC（Network Access Control），是一种“端到端”的安全结构，包括 web 认证、802.1x 认证、MAC 认证。

5.2 AR1200 支持的 NAC 特性
AR1200 支持多种认证和控制方式，以实现对用户权限和访问区域的控制。

5.3 配置 802.1x 认证
配置 802.1x 认证可以实现基于接口的网络接入控制，即在接入控制设备的接口对所接入的设备进行认证和控制。

5.4 配置 MAC 认证
配置 MAC 认证后，AR1200 使用用户的 MAC 地址作为用户名和密码对用户进行认证。

5.5 维护 NAC
清除认证统计信息、调试 NAC。

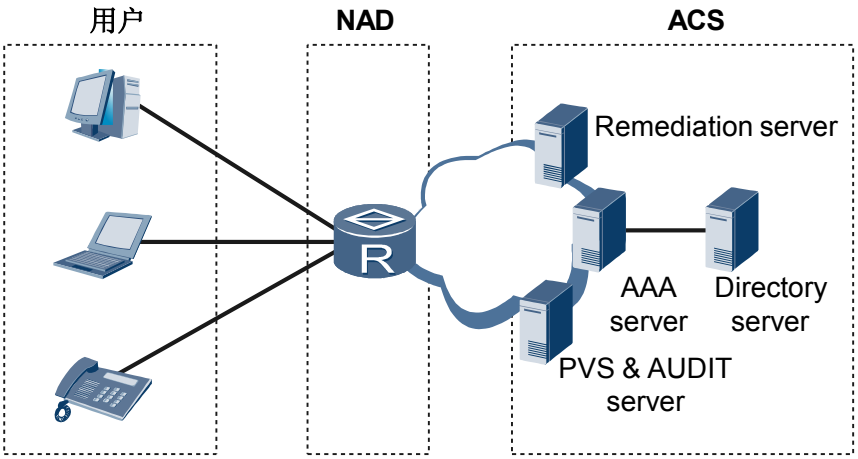
5.6 配置举例
通过示例介绍如何应用 NAC。配置示例中包括组网需求、配置注意事项、配置思路等。

5.1 NAC 概述

网络接入控制 NAC（Network Access Control），是一种“端到端”的安全结构，包括 web 认证、802.1x 认证、MAC 认证。

传统的网络安全技术只考虑了外部计算机对网络的威胁，而没有考虑到内部计算机对网络的威胁，而且现有的网络设备难以有效防止内部设备对网络的威胁。NAC 从用户终端考虑内部网络安全，提供“端到端”的安全保证。

图 5-1 NAC 典型组网图



如图 5-1 所示，NAC 作为网络安全接入的一种控制方案，主要包括以下几部分：

- 用户：接入用户，需要对其进行认证。如果采用 802.1x 认证，用户需要安装客户端软件。
- NAD：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。
- ACS：接入控制服务器，主要进行终端安全健康性检查与策略管理；用户行为管理与违规审计，强化行为审计，防止恶意终端破坏。

5.2 AR1200 支持的 NAC 特性

AR1200 支持多种认证和控制方式，以实现对用户权限和访问区域的控制。

AR1200 作为 NAC 方案中的 NAD，支持 802.1x 认证、MAC 认证、Web 认证。

802.1x 认证

IEEE 802.1x 标准（以下简称 802.1x）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。

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。

认证方式

- EAP 终结认证：由 AR1200 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。EAP 终结认证还包括 PAP（Password Authentication Protocol）认证和 CHAP（Challenge Handshake Authentication Protocol）认证。
  - PAP 是一种两次握手认证协议，采用明文交互密码，安全性不高。
  - CHAP 是一种三次握手认证协议，采用密文交互密码，安全性比 PAP 高。
- EAP 中继认证：也叫 EAP 透传认证，由 AR1200 直接把 802.1x 用户的认证信息以及 EAP 报文直接封装到 RADIUS 报文或 HWTACACS 报文的属性字段中，发送给 AAA 服务器。

Guest VLAN 功能

在某些情况下，需要保证没有通过 802.1x 认证的用户仍然可以获得某些网络资源，例如下载 802.1x 客户端，更新病毒库等。配置 Guest VLAN 后，没有通过 802.1x 认证的用户将被加入到 Guest VLAN 中，这部分用户就可以获取 Guest VLAN 中的资源。

MAC 旁路认证

对于某些特殊终端，例如打印机等，无法使用和安装 802.1x 认证软件，可以通过 MAC 旁路认证方式进行认证。配置 MAC 旁路认证后，当 AR1200 发起 802.1x 认证而没有收到终端的响应时，AR1200 就将该终端的 MAC 地址作为用户名和密码上送认证服务器进行认证。

MAC 认证

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件，用户名和密码都是用户设备的 MAC 地址。AR1200 在首次检测到用户的 MAC 地址以后，即启动对该用户的认证。

NAC 特性的应用范围

在 AR1220 的所有接口板上的 LAN 侧 Ethernet 和 GigabitEthernet 接口上都可以配置 802.1x 认证和 MAC 认证。但是在 AR1220 的主控板上仅可以在 LAN 侧 Ethernet 和 GigabitEthernet 接口上配置 802.1x 认证，不可以配置 MAC 认证。

5.3 配置 802.1x 认证

配置 802.1x 认证可以实现基于接口的网络接入控制，即在接入控制设备的接口对所接入的设备进行认证和控制。

5.3.1 建立配置任务

在配置 802.1x 认证前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

802.1x 协议作为局域网接口的一个接入控制机制应用于以太网中，在局域网接入控制设备的接口对接入的设备进行认证和控制，用于解决以太网内认证和安全方面的问题。

前置任务

无

数据准备

在配置 802.1x 之前，需要准备以下数据。

序号	数据
1	使能 802.1x 地址认证的接口
2	（可选）接口下允许接入的最大用户数量
3	（可选）向用户发送认证请求的最大次数
4	（可选）使能 MAC 旁路认证的接口

5.3.2 使能全局 802.1x 认证功能

只有全局使能 802.1x 认证功能后，802.1x 认证的其他相关配置才会生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x enable**，使能全局 802.1x 认证功能。

缺省情况下，未使能全局 802.1x 认证功能。

----结束

5.3.3 使能接口 802.1x 认证功能

如果需要对某个用户进行 802.1x 认证，就必须在和此用户连接的接口上使能 802.1x 认证功能。

背景信息

如果接口使能了 802.1x 认证功能，则禁止在该接口上使能 MAC 地址认证功能；反之，如果接口使能了 MAC 地址认证功能，则不能使能该接口的 802.1x 认证功能。

在系统视图和接口视图下都可以使能接口的 802.1x 认证功能。

操作步骤

- 系统视图下使能接口的 802.1x 认证功能

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dot1x enable interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，使能接口的 802.1x 认证功能。

   缺省情况下，没有使能接口的 802.1x 认证功能。

- 接口视图下使能接口的 802.1x 认证功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x enable**，在接口下使能 802.1x 认证功能。

  缺省情况下，没有使能接口的 802.1x 认证功能。

----结束

5.3.4 （可选）使能 MAC 旁路认证功能

对于某些特殊终端，例如打印机等，无法使用和安装 802.1x 认证软件，可以通过 MAC 旁路认证方式进行认证。配置 MAC 旁路认证后，当 AR1200 发起 802.1x 认证而没有收到终端的响应时，AR1200 就将该终端的 MAC 地址作为用户名和密码上送认证服务器进行认证。

背景信息

如果接口下没有使能 802.1x 认证功能，执行 **dot1x mac-bypass** 命令后，802.1x 认证功能也同时被使能。

如果接口下原来已经使能 802.1x 认证功能，执行本命令后，覆盖原来的配置。

系统视图和接口视图都可以配置 MAC 旁路认证。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x mac-bypass interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，使能接口 MAC 旁路认证功能。

     缺省情况下，没有使能接口的 MAC 旁路认证功能。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x mac-bypass**，在接口下使能 MAC 旁路认证功能。

  缺省情况下，没有使能接口的 MAC 旁路认证功能。

----结束

5.3.5 （可选）配置 802.1x 的认证方式

AR1200 支持的认证方式包括：CHAP 认证、PAP 认证、EAP 中继认证。

背景信息

PAP（Password Authentication Protocol）是一种两次握手认证协议，采用明文交互密码，安全性不高。

CHAP（Challenge Handshake Authentication Protocol）是一种三次握手认证协议，采用密文交互密码，安全性比 PAP 高。

EAP（Extensible Authentication Protocol），是一个支持多种认证机制的通用协议。采用 EAP，AR1200 不关心认证的过程，而直接将 EAP 认证 request 报文和 response 报文透传给认证服务器。AR1200 只要判断认证服务器返回的认证结果就可以决定是否允许该用户接入。

注意

当采用本地认证时，不能配置对 802.1x 用户采用 EAP 方式进行认证。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x authentication-method** { **chap** | **eap** | **pap** }，配置 802.1x 的认证方式。

缺省情况下，AR1200 对 802.1x 用户采用 CHAP 方式进行认证。

----结束

5.3.6 （可选）配置接口接入控制方式

AR1200 支持的接入控制方式为基于端口方式和基于 MAC 方式。

背景信息

基于 MAC 方式：接口下的所有 802.1x 用户均需要单独认证。

基于端口方式：只要该接口下的第一个用户认证成功后，其他 802.1x 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。

在系统视图和接口视图下都可以配置接口的接入控制方式。

注意

当某个接口下有 802.1x 用户在线时，不允许更改此接口的接入控制方式。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x port-method** { **mac** | **port** } **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口的接入控制方式。

缺省情况下，接口的接入控制方式为基于 MAC 地址。

- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x port-method** { **mac** | **port** }，配置接口的接入控制方式。

  缺省情况下，接口的接入控制方式为基于 MAC 地址。

----结束

5.3.7 （可选）配置接口授权状态

AR1200 支持的接口授权状态为：自动识别模式、强制授权模式、强制非授权模式。

背景信息

自动识别模式（**auto**）：接口初始状态为非授权状态，仅允许收发 EAPoL 报文，不允许用户访问网络资源；如果认证通过，则接口切换到授权状态，允许用户访问网络资源。

强制授权模式（**authorized-force**）：接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（**unauthorized-force**）：接口始终处于非授权状态，不允许用户访问网络资源。

在系统视图和接口视图下都可以配置接口的授权状态。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x port-control** { **auto** | **authorized-force** | **unauthorized-force** } **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口的授权状态。

     缺省情况下，接口的授权状态为 **auto**，即自动识别模式。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x port-control** { **auto** | **authorized-force** | **unauthorized-force** }，配置接口的授权状态。

  缺省情况下，接口的授权状态为 **auto**，即自动识别模式。

----结束

5.3.8 （可选）配置接口允许接入的最大用户数量

配置接口允许接入的最大用户数量后，当接口下接入的用户数达到最大数量时，AR1200 将不会再对之后接入的用户进行认证，这些用户也就无法正常访问网络。

背景信息

AR1200 整机允许接入的 NAC 用户的最大数为 128。

说明

如果在配置接口允许接入的最大用户数量时，该接口下的在线用户数量已经超过此最大值，不会影响在线用户，只会影响后接入的用户。

在系统视图和接口视图下都可以配置接口允许接入的最大用户数量。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x max-user** *user-number* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口允许接入的最大用户数量。

     缺省情况下，接口允许同时接入用户的最大数为 128。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **dot1x max-user** *user-number*，配置接口可以同时接入的最大用户数量。

  缺省情况下，每个接口可以同时接入用户的最大数为 128。

----结束

5.3.9 （可选）配置允许 DHCP 报文触发认证

配置允许 DHCP 报文触发认证后，AR1200 在接入用户运行 DHCP 申请动态 IP 地址时就触发对其进行 802.1x 认证。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x dhcp-trigger**，配置允许 DHCP 报文触发 802.1x 认证。

缺省情况下，DHCP 报文不触发 802.1x 认证。

----结束

5.3.10 （可选）配置 802.1x 定时器

AR1200 支持配置的 802.1x 定时器包括：客户端认证超时定时器、AR1200 与 802.1x 客户端握手时间间隔、静默定时器、重认证周期、认证服务器超时定时器、发送认证请求的时间间隔。

背景信息

配置定时器的时长前请确认该定时器是否使能。

一般情况下，建议保持这些定时器的缺省值。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令，**dot1x timer** { **client-timeout** *client-timeout-value* | **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **reauthenticate-period** *reauthenticate-period-value* | **server-timeout** *server-timeout-value* | **tx-period** *tx-period-value* }，配置 802.1x 认证的各项定时器参数。

各定时器的缺省值：

- **client-timeout**：客户端认证超时定时器。缺省值是 30 秒。
- **handshake-period**：AR1200 与 802.1x 客户端握手时间间隔。缺省值是 60 秒。
- **quiet-period**：静默定时器时长。缺省值是 60 秒。
- **reauthenticate-period**：重认证周期。缺省值是 3600 秒。
- **server-timeout**：认证服务器超时定时器。缺省值是 30 秒。
- **tx-period**：发送认证请求的时间间隔。缺省值是 30 秒。

这里只是配置定时器的时长，具体到每个定时器是否使能，要进行相应配置或采取系统默认配置。

----结束

5.3.11 （可选）配置定时静默功能

开启静默定时器功能后，当 802.1x 用户认证失败以后，AR1200 会将该用户静默一段时间，在这段时间内不对用户的认证请求进行处理。这样可以防止频繁认证对系统造成冲击。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x quiet-period**，使能静默定时器功能。

缺省情况下，未使能静默定时器功能。

步骤 3 （可选）执行命令 **dot1x timer quiet-period** *quiet-period-value*，静默定时器的时长。

使能静默定时器功能后，缺省情况下，静默定时器时长是 60 秒。

步骤 4 （可选）执行命令 **dot1x quiet-times** *fail-times*，配置 802.1x 用户被静默前 60 秒内允许认证失败的次数。

使能静默定时器功能后，缺省情况下，802.1x 用户在 60 秒内认证失败 3 次被静默。

----结束

5.3.12 （可选）配置 802.1x 重认证

在进行 802.1x 认证时，AR1200 可以每隔一段时间对已认证成功的用户进行重认证，以确保用户的合法性。

背景信息

在系统视图和接口视图下都可以配置 802.1x 重认证功能。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x reauthenticate interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，使能接口的重认证功能。

     缺省情况下，未使能接口的 802.1x 重认证功能。
  3. （可选）执行命令 **dot1x timer reauthenticate-period** *reauthenticate-period-value*，配置重认证周期。

     使能接口的 802.1x 重认证功能后，缺省情况下，重认证周期为 3600 秒。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **dot1x timer reauthenticate-period** *reauthenticate-period-value*，配置重认证周期。

     使能接口的 802.1x 重认证功能后，缺省情况下，重认证周期为 3600 秒。
  3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  4. 执行命令 **dot1x reauthenticate**，使能接口的重认证功能。

     缺省情况下，未使能接口的 802.1x 重认证功能。

----结束

5.3.13 （可选）配置 802.1x 认证的 Guest VLAN

背景信息

当 Guest VLAN 功能开启后，如果 AR1200 向所有开启 802.1x 功能的端口广播主动认证报文，如果达到最大重认证次数后，仍有端口上未返回响应报文，则 AR1200 将该端口加入到 Guest VLAN 中。该 Guest VLAN 中的用户访问该 Guest VLAN 中的资源时，不需要进行 802.1x 认证，但访问外部的资源时仍需要进行认证。

说明

配置的 Guest VLAN 不能是接口的缺省 VLAN。

Super VLAN 不能作为 Guest VLAN。

接口下配置 Guest VLAN 以后，不能再配置将该接口加入该 VLAN，也不能直接删除该 VLAN，相同 VLAN 的用户可以和 Guest VLAN 用户可以互通。

在系统视图和接口视图下都可以配置 Guest VLAN。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **dot1x guest-vlan** *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口的 Guest VLAN。

     缺省情况下，接口下未配置 Guest VLAN。
- 接口视图下

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **dot1x guest-vlan** *vlan-id*，配置接口的 Guest VLAN。

缺省情况下，接口下未配置 Guest VLAN。

----结束

5.3.14 （可选）配置 802.1x 认证的 Restrict VLAN

在某些情况下，需要保证没有通过 802.1x 认证的用户仍然可以获得某些网络资源，例如更新病毒库等。配置 Restrict VLAN 后，没有通过 802.1x 认证的用户将被加入到 Restrict VLAN 中，这部分用户就可以获取 Restrict VLAN 中的资源。

背景信息

当 Restrict VLAN 功能开启后，如果用户认证失败，则 AR1200 将该端口加入到 Restrict VLAN 中。之后属于该 Restrict VLAN 中的用户访问该 Restrict VLAN 中的资源时，不需要进行 802.1x 认证，但访问外部的资源时仍需要进行认证。

说明

配置的 Restrict VLAN 不能是接口的缺省 VLAN。

Super VLAN 不能作为 Restrict VLAN。

接口下配置 Restrict VLAN 以后，不能再配置将该接口加入该 VLAN，也不能直接删除该 VLAN，相同 VLAN 的用户可以和 Restrict VLAN 用户可以互通。

在系统视图和接口视图下都可以配置 Restrict VLAN。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **dot1x restrict-vlan fail-times** *fail-times*，配置允许用户认证失败的最大次数。

     缺省情况下，允许用户认证失败的最大次数为 3 次。
  3. 执行命令 **dot1x restrict-vlan** *vlan-id* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口的 Restrict VLAN。

     缺省情况下，接口下未配置 Restrict VLAN。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. （可选）执行命令 **dot1x restrict-vlan fail-times** *fail-times*，配置允许用户认证失败的最大次数。

     缺省情况下，允许用户认证失败的最大次数为 3 次。
  3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  4. 执行命令 **dot1x restrict-vlan** *vlan-id*，配置接口的 Restrict VLAN。

  缺省情况下，接口下未配置 Restrict VLAN。

----结束

5.3.15 （可选）配置在线用户握手功能

配置在线用户握手功能后，AR1200 向客户端定期发送握手报文来探测用户是否在线。

背景信息

对于不支持握手功能的客户端，在握手周期内 AR1200 不会收到握手回应报文。因此为了防止 AR1200 错误地认为用户下线，需要将在线用户握手功能关闭。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x handshake**，使能 AR1200 与在线用户握手功能。

缺省情况下，AR1200 使能与在线用户握手功能。

步骤 3 （可选）执行命令 **dot1x timer handshake-period** *handshake-period-value*，配置 AR1200 与 802.1x 客户端握手时间间隔。

缺省情况下，AR1200 与 802.1x 客户端握手时间间隔 60 秒。

----结束

5.3.16 （可选）配置向用户发送认证请求的最大次数

为了避免由于网络不稳定而造成的丢包引起用户没有响应认证请求，可以配置向用户发送认证请求的最大次数。

背景信息

AR1200 初次向用户发送认证请求帧后，在规定的时间里没有收到用户的响应，AR1200 将再次向用户发送该认证请求。当发送次数达到最大次数后仍没有收到响应，AR1200 不再重复向用户发送该认证请求。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **dot1x retry** *max-retry-value*，配置 AR1200 向用户发送认证请求的最大次数。

缺省情况下，AR1200 可以重复向接入用户发送认证请求帧的最大次数为 2 次。

----结束

5.3.17 检查配置结果

操作步骤

- 使用命令 **display dot1x** [**statistics**] [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]或 **display dot1x global** 查看 802.1x 的配置信息。
- 使用命令 **display mac-address authen** [**vlan** *vlan-id*]查看通过 802.1x 认证的 MAC 地址信息。

----结束

5.4 配置 MAC 认证

配置 MAC 认证后，AR1200 使用用户的 MAC 地址作为用户名和密码对用户进行认证。

5.4.1 建立配置任务

在配置 MAC 认证前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以帮助您快速、准确地完成配置任务。

应用环境

对无法安装客户端软件的终端，如传真机、打印机等设备，当需要对其进行认证时，可以配置 MAC 地址认证。

前置任务

无

数据准备

在配置 MAC 地址认证前，需要准备以下数据。

序号	数据
1	使能 MAC 地址认证的接口
2	（可选）MAC 认证的域
3	（可选）MAC 认证用户的最大数量

5.4.2 使能全局 MAC 认证功能

只有使能全局 MAC 认证功能后，MAC 认证的其他相关配置才会生效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-authen**，使能全局 MAC 认证功能。

缺省情况下，未使能全局 MAC 认证功能。

----结束

5.4.3 使能接口的 MAC 认证功能

如果需要对某个用户进行 MAC 认证，就需要在和此用户连接的接口上使能 MAC 认证功能。

背景信息

如果接口使能了 MAC 地址认证功能，则禁止在该接口上使能 802.1x 功能；反之，如果接口使能了 802.1x 功能，则不能使能该接口的 MAC 地址认证功能。

在接口视图和全局视图下都可以使能接口的 MAC 认证功能。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **mac-authen interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，使能接口的 MAC 地址认证功能。

     缺省情况下，没有使能接口的 MAC 认证功能。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **mac-authen**，在接口下使能 MAC 地址认证功能。

  缺省情况下，没有使能接口的 MAC 认证功能。

----结束

5.4.4 （可选）配置 MAC 认证的用户名格式

MAC 认证的用户名形式可以采用固定用户名形式或 MAC 地址形式。

背景信息

当 MAC 认证的用户名形式为 MAC 地址形式时，用户使用 MAC 地址作为用户名进行认证，同时该 MAC 地址也作为认证密码。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-authen username macaddress [format** { **with-hyphen** | **without-hyphen** }]，配置 MAC 认证用户名的形式。

缺省情况下，MAC 认证的用户名和密码为不带分隔符“-”的 MAC 地址。

----结束

5.4.5 （可选）配置 MAC 认证的域

如果没有配置认证域，MAC 地址认证用户使用 **default** 域认证。

背景信息

配置 MAC 地址认证用户所使用的认证域前，需要已经创建该域。

在接口视图和系统视图下都可以配置 MAC 认证的域。如果在系统视图和接口视图下都配置了 MAC 认证的域，接口视图下配置的优先级更高。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **mac-authen domain** *domain-name*，配置 MAC 地址认证用户所使用的认证域的域名。

  缺省情况下，认证域使用系统缺省的“default”域。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **mac-authen domain** *domain-name*，配置 MAC 地址认证用户所使用的认证域的域名。

  缺省情况下，认证域使用系统缺省的“default”域。

----结束

5.4.6 （可选）配置 MAC 认证定时器

AR1200 支持配置的 MAC 认证定时器包括：重认证周期、下线检测定时器、静默定时器、认证服务器超时定时器。

背景信息

MAC 认证的定时器都有缺省值，一般情况下不需要修改 MAC 认证定时器的值。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-authen timer** { **guest-vlan reauthenticate-period** *interval* | **offline-detect** *offline-detect-value* | **quiet-period** *quiet-value* | **server-timeout** *server-timeout-value* }，配置 MAC 地址认证的各项定时器参数。

- **guest-vlan reauthenticate-period**：Guest VLAN 内的用户进行重认证的时间间隔。缺省值是 60 秒。
- **offline-detect**：下线检测定时器，用来设置 AR1200 检查用户是否已经下线的时间间隔。缺省值是 300 秒。
- **quiet-period**：静默定时器，对用户认证失败以后，AR1200 需要静默一段时间后再处理用户认证请求，在静默期间，AR1200 不处理该用户的认证请求。缺省值是 60 秒。
- **server-timeout**：服务器超时定时器，在用户的认证过程中，如果 AR1200 同认证服务器的连接超时，则此次认证失败。缺省值是 30 秒。

----结束

5.4.7 （可选）配置 MAC 认证用户的最大数量

当接入用户到达配置的最大数量时，AR1200 将不会再对之后接入的用户进行认证触发动作，这些用户也就无法正常访问网络。

背景信息

在接口视图和系统视图下都可以配置 MAC 认证用户的最大数量。

操作步骤

- 系统视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **mac-authen max-user** *user-number* **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>，配置接口可以接入的 MAC 地址认证用户的最大数量。

     缺省情况下，AR1200 接口允许接入的 MAC 地址认证用户的最大数量为 128 个。
- 接口视图下
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **mac-authen max-user** *user-number*，配置接口可以接入的 MAC 地址认证用户的最大数量。

  缺省情况下，AR1200 接口允许接入的 MAC 地址认证用户的最大数量为 128 个。

----结束

5.4.8 （可选）对指定 MAC 地址进行重认证

系统可以对某个已经通过 MAC 认证的用户进行一次重认证，如果重认证成功则对用户重新进行授权，否则使该用户下线。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **mac-authen reauthenticate mac-address** *mac-address*，配置对某个已经通过认证的 MAC 地址进行重认证。

缺省情况下，不对 MAC 地址进行重认证。

----结束

5.4.9 检查配置结果

操作步骤

- 使用命令 **display mac-authen** [**global** | **interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]查看 MAC 认证的配置信息。

- 使用命令 **display mac-address authen** [**vlan** *vlan-id*]查看通过 MAC 认证的 MAC 地址信息。

----结束

5.5 维护 NAC

清除认证统计信息、调试 NAC。

5.5.1 清除 802.1x 认证的统计信息

使用 reset 命令清除 802.1x 认证的统计信息，以便重新统计。

背景信息

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除统计信息后，请在用户视图下执行以下命令。

操作步骤

- 使用 **reset dot1x statistics** [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]命令清除 802.1x 认证的统计信息。

----结束

5.5.2 清除 MAC 认证的统计信息

使用 reset 命令清除 MAC 认证的统计信息，以便重新统计。

背景信息

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除统计信息后，请在用户视图下执行以下命令。

操作步骤

- 使用 **reset mac-authen statistics** [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]命令清除 MAC 地址认证的统计信息。

----结束

5.6 配置举例

通过示例介绍如何应用 NAC。配置示例中包括组网需求、配置注意事项、配置思路等。

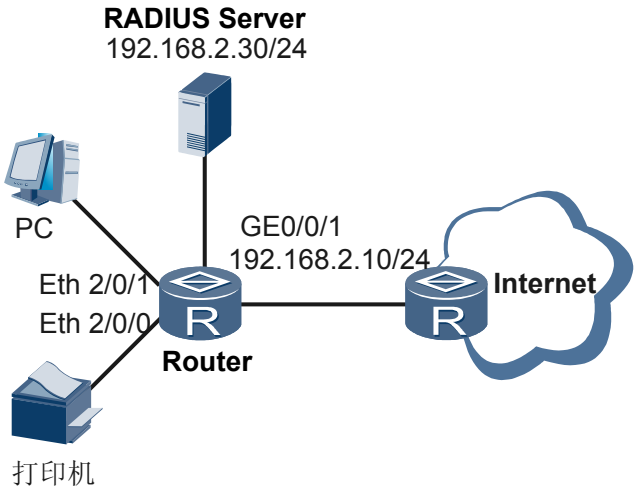
5.6.1 配置 802.1x 认证示例

通过配置 802.1x 认证，未认证用户在接入网络前必须先通过 802.1x 认证，否则只能访问有限的资源，从而保证网络的安全。

组网需求

如图 5-2 所示，用户通过 Router 访问网络。为了保证网络的安全性，要求在用户接入网络时进行认证。认证成功后可以正常访问网络，认证失败的用户只可以访问 VLAN 10 中的资源。

图 5-2 配置 802.1x 认证组网图



配置思路

用如下的思路配置 802.1x 认证。

1. 配置 AAA 认证，用来将 802.1x 用户的用户名和密码发送到 RADIUS 服务器进行认证。
2. 配置 802.1x 认证，用来对接口 Ethernet2/0/0 下的用户进行认证。
3. 配置 GUEST VLAN，保证认证失败的用户仍然可以访问 VLAN 10 中的资源。
4. 配置 MAC 旁路认证，用来完成对接口 Ethernet2/0/1 下的打印机进行认证。

数据准备

为完成此配置举例，需要准备如下数据：

- RADIUS 服务器 IP 地址为 192.168.2.30，认证端口号为 1812。

- RADIUS 服务器密钥为 dot1x-isp，重传次数为 2。
- AAA 认证方案 scheme1。
- RADIUS 服务器模版 temp1。
- 域 isp1。

说明

本案例只包括 Router 上的配置，RADIUS 服务器上的配置这里不做具体介绍。

操作步骤

步骤 1 配置 RADIUS 服务器模板

配置 RADIUS 服务器模板 temp1。

```
[Huawei] radius-server template temp1
```

配置 RADIUS 主用认证服务器的 IP 地址、端口。

```
[Huawei-radius-temp1] radius-server authentication 192.168.2.30 1812
```

配置 RADIUS 服务器密钥、重传次数。

```
[Huawei-radius-temp1] radius-server shared-key cipher dot1x-isp
[Huawei-radius-temp1] radius-server retransmit 2
[Huawei-radius-temp1] quit
```

步骤 2 配置认证方案，认证方案 scheme1，认证方法为 RADIUS

```
[Huawei] aaa
[Huawei-aaa] authentication-scheme scheme1
[Huawei-aaa-scheme1] authentication-mode radius
[Huawei-aaa-scheme1] quit
```

步骤 3 配置 isp1 域，绑定认证方式和 RADIUS 服务器模板

```
[Huawei-aaa] domain isp1
[Huawei-aaa-domain-isp1] authentication-scheme scheme1
[Huawei-aaa-domain-isp1] radius-server temp1
[Huawei-aaa-domain-isp1] quit
[Huawei-aaa] quit
```

步骤 4 配置 802.1x 认证

在全局和接口下使能 802.1x 认证。

```
[Huawei] dot1x enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dot1x enable
[Huawei-Ethernet2/0/0] quit
```

配置 GUEST VLAN。

```
[Huawei] vlan batch 10
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dot1x guest-vlan 10
[Huawei-Ethernet2/0/0] quit
```

步骤 5 配置 MAC 旁路认证

```
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] dot1x mac-bypass
```

步骤 6 检查配置结果

在 Router 执行命令 **display dot1x interface**，可以看到 802.1x 配置信息和统计信息。

```
<Huawei> display dot1x interface ethernet 2/0/0
 Ethernet2/0/0 status: UP  802.1x protocol is enabled.
```

```
  Port control type is auto.
  Authentication method is MAC-based.
  Reauthentication is disabled.
  Maximum users: 128
  Current users: 1
  Port PVID : 1
  Port configured PVID : 1
  Guest VLAN : 10
  Restrict VLAN : 0

  Authentication success: 4
  Authentication failure: 0
  EAPOL Packets: TX     : 10         RX     : 0
  Sent      EAPOL Request/Identity Packets  : 4
            EAPOL Request/Challenge Packets : 4
            Multicast Trigger Packets       : 0
            EAPOL Success Packets           : 4
            EAPOL Failure Packets           : 0
  Received  EAPOL Start Packets             : 4
            EAPOL LogOff Packets            : 3
            EAPOL Response/Identity Packets : 4
            EAPOL Response/Challenge Packets: 4
<Huawei> display dot1x interface ethernet 2/0/1
Ethernet 2/0/1 status: UP  802.1x protocol is Enabled[mac-bypass]
  Port control type is Auto.
  Authentication method is MAC-based.
  Reauthentication is disabled.
  Maximum users: 128
  Current users: 1
  Port PVID : 1
  Port configured PVID : 1
  Guest VLAN : 0
  Restrict VLAN : 0

  Authentication success: 4
  Authentication failure: 0
  EAPOL Packets: TX     : 10         RX     : 0
  Sent      EAPOL Request/Identity Packets  : 4
            EAPOL Request/Challenge Packets : 4
            Multicast Trigger Packets       : 0
            EAPOL Success Packets           : 4
            EAPOL Failure Packets           : 0
  Received  EAPOL Start Packets             : 4
            EAPOL LogOff Packets            : 3
            EAPOL Response/Identity Packets : 4
            EAPOL Response/Challenge Packets: 4
```

----结束

配置文件

```
#
 vlan batch 10 20
#
dot1x enable
#
radius-server template temp1
 radius-server shared-key cipher #%I/SW5&ABHRID9_LGZK@1!!
 radius-server authentication 192.168.2.30 1812
 radius-server retransmit 2
#
aaa
 authentication-scheme scheme1
  authentication-mode radius
 domain isp1
  authentication-scheme scheme1
  radius-server temp1
#
```

```
interface Ethernet2/0/0
 dot1x enable
 dot1x guest-vlan 10
#
interface Ethernet2/0/1
 dot1x mac-bypass
#
interface GigabitEthernet0/0/1
 ip address 192.168.2.10 255.255.255.0
#
return
```

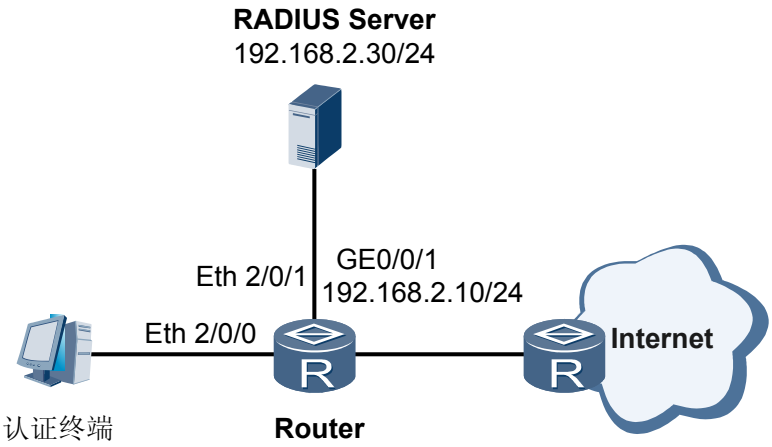
5.6.2 配置 MAC 认证示例

通过配置 MAC 认证，未认证用户在接入网络前必须先通过 MAC 认证才能访问网络资源，从而保证网络的安全。

组网需求

如图 5-3 所示，用户通过 Router 访问网络。为了保证网络的安全性，要求在用户接入网络时进行 MAC 认证。

图 5-3 配置 MAC 认证组网图



配置思路

用如下的思路配置 MAC 认证。

1. 配置 AAA 认证，用来用户名和密码发送到 RADIUS 服务器进行认证。
2. 配置 MAC 认证，用来对接口 Ethernet2/0/0 下的用户进行认证。

数据准备

为完成此配置举例，需要准备如下数据：

- RADIUS 服务器 IP 地址为 192.168.2.30，认证端口号为 1812。
- RADIUS 服务器密钥为 mac-default，重传次数为 3。
- AAA 认证方案 scheme1。

- RADIUS 服务器模版 temp1。

说明

本案例只包括 Router 的配置，RADIUS 服务器的配置这里不做相关说明。

操作步骤

步骤 1 配置 RADIUS 服务器模板

配置 RADIUS 服务器模板 temp1。

```
[Huawei] radius-server template temp1
```

配置 RADIUS 主用认证服务器的 IP 地址、端口。

```
[Huawei-radius-temp1] radius-server authentication 192.168.2.30 1812
```

配置 RADIUS 服务器密钥、重传次数。

```
[Huawei-radius-temp1] radius-server shared-key cipher mac-default
[Huawei-radius-temp1] radius-server retransmit 3
[Huawei-radius-temp1] quit
```

步骤 2 配置认证方案，认证方案 scheme1，认证方法为 RADIUS

```
[Huawei] aaa
[Huawei-aaa] authentication-scheme scheme1
[Huawei-aaa-scheme1] authentication-mode radius
[Huawei-aaa-scheme1] quit
```

步骤 3 配置 default 域，绑定认证方式和 RADIUS 服务器模板

```
[Huawei-aaa] domain default
[Huawei-aaa-domain-default] authentication-scheme scheme1
[Huawei-aaa-domain-default] radius-server temp1
[Huawei-aaa-domain-default] quit
[Huawei-aaa-domain] quit
```

步骤 4 配置 MAC 认证

在全局和接口下使能 MAC 认证。

```
[Huawei] mac-authen
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mac-authen
```

步骤 5 检查配置结果

在 Router 执行命令 **display mac-authen interface**，可以看到 MAC 认证配置信息。

```
<Huawei> display mac-authen interface ethernet 2/0/0
 Ethernet2/0/0 state: UP.  MAC address authentication is enabled
  Maximum users: 128
  Current users: 1
  Authentication success: 1
  Authentication failure: 0
```

----结束

配置文件

```
#
mac-authen
#
radius-server template temp1
 radius-server shared-key cipher 3MQ*TZ,O3KCQ=^Q`MAF4<1!!
 radius-server authentication 192.168.2.30 1812
```

```
#
aaa
 authentication-scheme scheme1
  authentication-mode radius
 domain default
  authentication-scheme scheme1
  radius-server temp1
#
interface GigabitEthernet0/0/1
 ip address 192.168.2.10 255.255.255.0
#
interface Ethernet2/0/0
 mac-authen
#
interface Ethernet2/0/1
 port hybrid pvid vlan 20
#
return
```

6 ARP 安全配置

关于本章

ARP 安全通过过滤不信任的 ARP 报文、检查 ARP 报文绑定表和防止 ARP 网关冲突等方法来保证网络设备的安全性和健壮性。

6.1 ARP 安全概述
简要介绍 ARP 安全原理。

6.2 AR1200 支持的 ARP 安全特性
AR1200 支持的 ARP 安全特性包括 ARP 表项限制、防止 ARP 地址欺骗、防止 ARP 网关冲突、ARP 报文源抑制、ARP Miss 消息源抑制和 ARP 报文速率限制功能。

6.3 配置 ARP 表项限制
介绍 ARP 表项限制的配置过程。

6.4 配置 ARP 防攻击
通过配置 ARP 防攻击，可以防止仿冒用户主机，仿冒网关，以及中间人攻击的产生。

6.5 配置 ARP 抑制
大量 ARP 攻击报文会造成 ARP 表项溢出或者 CPU 资源占用过高，AR1200 可以针对不同的报文类型进行丢弃、限速等操作防范此类攻击。

6.6 维护 ARP 安全
查看、清除 ARP 报文的统计信息，清除 ARP 丢弃报文计数以及调试 ARP 报文。

6.7 配置举例
介绍 ARP 安全功能的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

6.1 ARP 安全概述

简要介绍 ARP 安全原理。

ARP 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

ARP 安全

ARP 安全通过过滤不信任的 ARP 报文、检查 ARP 报文绑定表和防止 ARP 网关冲突等方法来保证网络设备的安全性和健壮性。

6.2 AR1200 支持的 ARP 安全特性

AR1200 支持的 ARP 安全特性包括 ARP 表项限制、防止 ARP 地址欺骗、防止 ARP 网关冲突、ARP 报文源抑制、ARP Miss 消息源抑制和 ARP 报文速率限制功能。

ARP 表项限制

可以配置严格学习 ARP 表项，使 AR1200 只学习自己发送的 ARP 请求的回应报文。

可以配置接口可以学习到的最大动态 ARP 表项数目，以防止恶意用户占用 ARP 表项资源造成 AR1200 无法学习合法用户的 ARP 表项。

防止 ARP 地址欺骗

ARP 地址欺骗指的是攻击者通过伪造其他用户发出的 ARP 报文，篡改设备上的用户 ARP 表项，造成其他合法用户的网络中断。

AR1200 可以通过以下两种方法防御此类攻击。

- 固定 MAC 地址：AR1200 第一次学习到 ARP 表项之后不再允许通过 ARP 学习来修改 MAC 地址，直到此 ARP 表项老化之后才允许更新，以保护合法用户的 ARP 表项不被修改。

固定 MAC 地址有两种方式：Fixed-mac 和 Fixed-all。Fixed-mac 方式下，不允许修改 MAC 地址，但是允许修改 VLAN 和接口信息；Fixed-all 方式下，MAC、VLAN 和接口信息都不允许修改。

- 主动确认：AR1200 收到一个涉及表项中 MAC 地址信息修改的 ARP 报文时，不会立即修改 ARP 表项，而是先对原 ARP 表中与此 MAC 地址对应的用户发一个单播确认，根据确认结果再决定是否修改。

防止 ARP 网关冲突

ARP 网关冲突指攻击者仿冒网关地址，在局域网内部发送源 IP 地址是网关地址的免费 ARP 报文。主机接收到该报文后，会修改自己原来的网关地址为攻击者的地址，最终导致局域网内部所有主机无法访问网络。

AR1200 收到与网关地址冲突的 ARP 报文时，如果存在下列情况之一：

- ARP 报文的源 IP 与报文入接口的 IP 地址相同；
- VRRP（Virtual Router Redundancy Protocol）虚 MAC 方式时，ARP 报文的源 IP 是入接口的虚拟 IP 地址，但 ARP 报文源 MAC 不是 VRRP 虚 MAC。

则系统生成 ARP 防攻击表项，在后续一段时间（默认 3 分钟）内直接丢弃该报文，这样可以防止与网关地址冲突的 ARP 报文在 VLAN 内广播。

为了防止网络中主机的报文不能被正常转发到网关或者被恶意攻击者窃听，AR1200 支持主动发送免费 ARP 报文的功能，定时更新主机 ARP 表项中的网关地址为正确的网关地址。

ARP 报文源抑制

某个源 IP 地址发送大量 ARP 报文，浪费设备的 CPU 资源和给 ARP 报文上送预留的有限带宽。

AR1200 具有针对源 IP 地址的 ARP 报文速率抑制的功能。在一段时间内，如果 AR1200 收到某一源 IP 地址的 ARP 报文数目超过设定阈值，则不处理超出阈值部分的 ARP 请求报文。

ARP Miss 消息源抑制

主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备。

对此类攻击，AR1200 提供对 ARP Miss 消息基于源 IP 地址的抑制。如果一个源 IP 地址向 AR1200 发送了目标 IP 地址不能解析的 IP 报文，就会触发 ARP Miss 消息，AR1200 对上报的 ARP Miss 消息进行统计。如果一个源 IP 地址在一定时间内不断触发 ARP Miss，而且其触发速率超过了设定的阈值，则认为此 IP 地址在进行攻击。

当设备检测到这种攻击后，可以通过对这个用户进行 ARP Miss 消息源抑制来保护设备的 CPU 资源，保证 CPU 可以正常处理业务。

ARP 报文和 ARP Miss 消息速率限制

基于全局、接口或 VLAN 对 ARP 报文以及基于全局对 ARP Miss 消息进行限速，防止上送安全模块检查的 ARP 报文或 ARP Miss 消息过多，对系统性能造成影响。

6.3 配置 ARP 表项限制

介绍 ARP 表项限制的配置过程。

6.3.1 建立配置任务

在配置 ARP 表项限制之前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

使能 ARP 严格学习功能，使 AR1200 只学习自己发送的 ARP 请求报文的应答报文。

配置基于接口的 ARP 表项限制，限制接口学习的动态 ARP 表项数目。

前置任务

在配置 ARP 表项限制之前，需要完成以下任务：

- 配置接口的链路层协议参数，使接口的链路层协议状态为 Up。

数据准备

在配置 ARP 表项限制之前，需要准备以下数据。

序号	数据
1	限制 ARP 表项学习的接口类型和接口编号

6.3.2 配置严格学习 ARP 表项

通过配置 AR1200 只学习自己发送的 ARP 请求报文的应答报文，可以防止攻击者仿冒用户欺骗网关设备。

操作步骤

- 配置全局严格学习 ARP 表项
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **arp learning strict**，配置严格学习 ARP 表项。

     缺省情况下，严格学习 ARP 表项功能处于去使能状态。
- 配置接口严格学习 ARP 表项功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     AR1200 支持严格学习 ARP 表项功能的接口包括三层的 Ethernet 接口及其子接口、三层 GE 接口及其子接口和三层 Eth-Trunk 接口及其子接口以及 VLANIF 接口。
  3. 执行命令 **arp learning strict** { **force-enable** | **force-disable** | **trust** }，配置接口的 ARP 严格学习功能。
     - **force-enable** 表示使能接口的 ARP 严格学习功能。
     - **force-disable** 表示去使能接口的 ARP 严格学习功能。

- **trust** 表示接口的 ARP 严格学习功能与全局配置保持一致。

缺省情况下，接口的 ARP 严格学习功能和全局配置保持一致。

----结束

6.3.3 配置基于接口的 ARP 表项限制

为了防止攻击者占用大量 ARP 表项资源，造成 AR1200 学习不到合法用户的 ARP 表项，可以配置接口能够学习到的最大动态 ARP 表项数目。

操作步骤

- 配置接口的 ARP 表项限制
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **arp-limit** [**vlan** *vlan-id1* [**to** *vlan-id2*]] **maximum** *maximum*，配置基于接口的 ARP 表项限制。

     参数 **vlan** 只能在二层接口视图下配置。
- 配置子接口的 ARP 表项限制
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number.subnumber*，进入子接口视图。

     AR1200 支持 ARP 表项限制的子接口包括 GE 子接口、Ethernet 子接口和 Eth-Trunk 子接口。
  3. 执行命令 **arp-limit maximum** *maximum*，配置基于子接口的 ARP 表项限制。

----结束

6.3.4 检查配置结果

完成 ARP 表项限制配置以后，检查配置结果。

操作步骤

- 执行命令 **display arp learning strict**，查看 ARP 表项严格学习限制。
- 执行命令 **display arp-limit** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]，查看接口或 VLAN 下配置的 ARP 表项限制数目。

----结束

任务示例

查看所有接口的 ARP 严格学习情况。

```
<Huawei> display arp learning strict
 The global configuration:arp learning strict
 Interface                         LearningStrictState
------------------------------------------------------------
 GigabitEthernet1/0/0              force-enable
 Vlanif1                           force-enable
------------------------------------------------------------
 Total:2
 Force-enable:2
 Force-disable:0
```

查询整机配置限制数目。

```
<Huawei> display arp-limit
 interface                     LimitNum   VlanID     LearnedNum(Mainboard)
-------------------------------------------------------------------------
 GigabitEthernet1/0/0          10         0          0
 Ethernet0/0/0                 10         10         0
-------------------------------------------------------------------------
  Total:2
```

6.4 配置 ARP 防攻击

通过配置 ARP 防攻击，可以防止仿冒用户主机，仿冒网关，以及中间人攻击的产生。

6.4.1 建立配置任务

在配置 ARP 防攻击之前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

在企业网中，存在着很多针对 ARP 表项的攻击，因此需要在网络的接入层配置防止对 ARP 表项的攻击，以保护网络的安全性。

- 为防止攻击者通过伪造其他用户发出的 ARP 报文，篡改网关设备上的用户 ARP 表项，可以配置 ARP 防地址欺骗功能。
- 为防止攻击者仿冒网关地址，在局域网内部发送源 IP 地址是网关地址的免费 ARP 报文，从而使主机修改网关地址为攻击者的地址，可以配置 ARP 防网关冲突功能以及发送 ARP 免费报文功能。
- 为防止非法用户的 ARP 报文任意通过 AR1200 访问外部网络，对合法用户的业务造成影响，可以配置 ARP 报文检查功能。

前置任务

在配置 ARP 防攻击功能之前，需要完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。

数据准备

在配置 ARP 防攻击功能之前，需要准备以下数据。

序号	数据
1	ARP 报文检查项
2	（可选）ARP 报文检查不匹配丢弃报文告警阈值
3	（可选）发送免费 ARP 报文的时间间隔

6.4.2 配置防止 ARP 地址欺骗

介绍防止 ARP 地址欺骗的配置方法。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp anti-attack entry-check** { **fixed-mac** | **fixed-all** | **send-ack** } **enable**，使能 ARP 地址防欺骗功能。

只能同时使能一种 ARP 地址防欺骗方式。如果原来使能了某一种方式，则新配置的方式将覆盖原来配置的方式。

缺省情况下，AR1200 未使能 ARP 地址防欺骗功能。

----结束

6.4.3 配置检查 ARP 报文合法性

通过检查 ARP 报文合法性，可以丢弃非法的 ARP 报文，防止非法的 ARP 报文对 AR1200 造成攻击。

背景信息

缺省情况下，检查 ARP 报文合法性的检查项包括：

- ARP 报文长度
- 以太报文头的源 MAC 和目的 MAC 的合法性
- VLAN Tag
- ARP 报文的类型（类型值只能为 1 或 2）
- 硬件地址长度
- 协议地址长度
- ARP 报文帧格式是否为以太类型

其中，对于以太报文头的源 MAC 或目的 MAC 全为 0 的情形，AR1200 默认会对收到的每个 ARP 报文进行检查，如果是源 MAC 或目的 MAC 全为 0，则丢弃该 ARP 报文，不再继续处理。

在大多数情况下，ARP 报文的以太报文头和 ARP 报文头的源 MAC 地址一致。当出现两者不一致的情况时，该 ARP 报文很可能是攻击报文。AR1200 支持检查 ARP 报文的以太报文头和 ARP 报文头的源 MAC 地址是否一致，并丢弃不一致的 ARP 报文，以防止可能的 ARP 攻击。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp anti-attack packet-check sender-mac**，检查 ARP 报文的以太报文头和 ARP 报文头的源 MAC 地址是否一致。

缺省情况下，AR1200 不检查 ARP 报文的以太报文头和 ARP 报文头的源 MAC 地址是否一致。

----结束

6.4.4 配置防止 ARP 网关冲突

为了防止攻击者发送虚假 ARP 报文仿冒网关，造成 VLAN 内的用户网关 ARP 表被修改为错误的 ARP，可以配置防止 ARP 网关冲突功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp anti-attack gateway-duplicate enable**，使能 ARP 网关冲突防攻击功能。

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。

----结束

6.4.5 配置发送免费 ARP 报文

通过配置发送免费 ARP 报文，防止用户的报文不能正常的转发到网关或者被恶意攻击者窃听。

背景信息

该报文使用网关的 IP 地址作为目标地址发送 ARP 请求，定时更新用户 ARP 表项的网关 MAC 地址，防止用户的报文不能正常的转发到网关或者被恶意攻击者窃听。

当 AR1200 作为网关时，可以在全局或接口下发送免费 ARP 报文。当全局和接口下都使能发送免费 ARP 功能时，接口下的配置优先生效。

操作步骤

- 配置全局发送免费 ARP 报文。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **arp gratuitous-arp send enable**，使能发送免费 ARP 报文的功能。

     缺省情况下，发送免费 ARP 报文的功能未使能。
  3. （可选）执行命令 **arp gratuitous-arp send interval** *interval-time*，配置发送免费 ARP 报文的时间间隔。

     缺省情况下，系统发送免费 ARP 报文的时间间隔为 90 秒。
- 配置接口发送免费 ARP 报文。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
  3. 执行命令 **arp gratuitous-arp send enable**，使能发送免费 ARP 报文的功能。

     缺省情况下，发送免费 ARP 报文的功能未使能。
  4. （可选）执行命令 **arp gratuitous-arp send interval** *interval-time*，配置发送免费 ARP 报文的时间间隔。

缺省情况下，系统发送免费 ARP 报文的时间间隔为 90 秒。

----结束

6.4.6 检查配置结果

介绍检查 ARP 防攻击的结果的配置方法。

操作步骤

- 执行命令 **display arp anti-attack configuration { arp-rate-limit | arpmiss-rate-limit | arp-speed-limit | arpmiss-speed-limit | entry-check | gateway-duplicate | log-trap-timer | all }**，查看当前 ARP 防攻击配置。
- 执行命令 **display arp anti-attack gateway-duplicate item**，查看当前网络中存在的网关地址冲突攻击信息。

----结束

任务示例

执行命令 **display arp anti-attack configuration all**，查看全部 ARP 防攻击配置。

```
<Huawei> display arp anti-attack configuration all
 ARP anti-attack packet-check function: enable

 ARP anti-attack entry-check mode: disabled

 ARP gateway-duplicate anti-attack function: disabled

 ARP rate-limit configuration:
------------------------------------------------------------------------------
 Global configuration:
    arp anti-attack rate-limit enable
    arp packet drop count = 0
 Interface configuration:
------------------------------------------------------------------------------

 ARP miss rate-limit configuration:
------------------------------------------------------------------------------
 Global configuration:
    arp-miss anti-attack rate-limit enable
------------------------------------------------------------------------------

 ARP speed-limit for source-MAC configuration:
 MAC-address          suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
 0000-0000-0001       200
 Others               100
------------------------------------------------------------------------------
 1 specified MAC addresses are configured, spec is 256 items.

 ARP speed-limit for source-IP configuration:
 IP-address           suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
 10.0.0.1             512
 Others               126
------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 128 items.

 ARP miss speed-limit for source-IP configuration:
 IP-address           suppress-rate(pps)(rate=0 means function disabled)
------------------------------------------------------------------------------
 10.134.23.6          400
 Others               500
```

```
-------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 128 items.
```

查看 ARP 防网关冲突攻击表项。

```
<Huawei> display arp anti-attack gateway-duplicate item
 interface         IP address       MAC address     VLANID   aging time
-------------------------------------------------------------------------------
 GigabitEthernet1/0/0          2.1.1.1          0000-0000-0002    2         150
-------------------------------------------------------------------------------
There are 1 records in gateway conflict table
```

6.5 配置 ARP 抑制

大量 ARP 攻击报文会造成 ARP 表项溢出或者 CPU 资源占用过高，AR1200 可以针对不同的报文类型进行丢弃、限速等操作防范此类攻击。

6.5.1 建立配置任务

在配置 ARP 抑制之前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

在网络中，存在着很多针对 ARP 表项的攻击，因此需要在网络的接入层配置防止对 ARP 表项的攻击，以保护网络的安全性。

- 为防止大量的 ARP 报文增加 CPU 的负荷，以及占用大量的 ARP 表项，可以配置 ARP 报文速率抑制，将上送主控板处理的 ARP 报文速率限制在一个合理的范围内。
- 为防止主机发送大量目标 IP 地址不能解析的 IP 报文来攻击设备，可以配置 ARP Miss 源抑制功能，对攻击者的报文进行丢弃处理。
- 接口下使能 ARP 报文检查功能后，经过接口的 ARP 报文上送安全模块进行检查，为防止大量 ARP 报文对安全模块的冲击，可以配置 ARP 报文速率抑制，对超过速率限制的报文做丢弃处理。

前置任务

在配置 ARP 速率抑制功能之前，需要完成以下任务：

- 配置接口的链路层协议参数和 IP 地址，使接口的链路协议状态为 Up。

数据准备

在配置 ARP 速率抑制功能之前，需要准备以下数据。

序号	数据
1	ARP 报文源抑制的目标速率值
2	ARP-Miss 源抑制的目标速率值
3	ARP 报文上送检查的限速时间和限速值 （可选）ARP 报文因超过速率限制丢弃告警阈值

序号	数据
4	ARP Miss 消息上送检查的限速时间和限速值 （可选）ARP Miss 消息因超过速率限制丢弃告警阈值
5	Super VLAN 的 VLANIF 接口下 ARP Request 报文的广播发送限制速率

6.5.2 配置 ARP 报文源 IP 抑制

考虑到某些特定的用户有特别的需求，在对 ARP 报文进行源 IP 抑制时，可以针对该用户的 IP 地址配置不同于其他 IP 地址的 ARP 报文抑制速率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp speed-limit source-ip maximum** *maximum*，配置 ARP 报文源 IP 抑制速率。

步骤 3 （可选）执行命令 **arp speed-limit source-ip** *ip-address* **maximum** *maximum*，配置指定 **source-ip** 用户的 ARP 报文源 IP 抑制速率。

对指定了 **source-ip** 的用户，ARP 报文源 IP 抑制速率为步骤 3 中配置的 *maximum* 值；其他 IP 地址的 ARP 报文源 IP 抑制速率为步骤 2 中配置的 *maximum* 值。

----结束

6.5.3 配置 ARP 报文速率抑制

介绍 ARP 报文速率抑制的配置。

操作步骤

- 系统视图下配置 ARP 报文速率抑制功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **arp anti-attack rate-limit enable**，全局使能 ARP 报文速率抑制功能。

     缺省情况下，全局未使能 ARP 报文速率抑制功能。
  3. 执行命令 **arp anti-attack rate-limit** *packet-number* [*interval-value*]，在系统视图下配置 ARP 报文的限速时间和限速值。

     配置了 ARP 报文的限速时间和限速值，在限速时间内超过限速值的 ARP 报文将被丢弃。缺省情况下，ARP 报文的限速值是 100，限速时间是 1 秒。
  4. （可选）执行命令 **arp anti-attack rate-limit alarm enable**，全局使能 ARP 报文限速丢弃告警功能。

     缺省情况下，未使能 ARP 报文限速丢弃告警功能。
  5. （可选）执行命令 **arp anti-attack rate-limit alarm threshold** *threshold*，在系统视图下配置 ARP 报文限速丢弃告警阈值。

缺省情况下，ARP 报文限速丢弃告警阈值为 100。

- 接口视图下配置 ARP 报文速率抑制功能
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     接口类型包括 Ethernet 接口、GE 接口和 Eth-Trunk 接口。
  3. 执行命令 **arp anti-attack rate-limit enable**，在接口视图下使能 ARP 报文速率抑制功能。

     缺省情况下，接口视图下未使能 ARP 报文速率抑制功能。
  4. 执行命令 **arp anti-attack rate-limit** *packet-number* [*interval-value*]，在接口视图下配置 ARP 报文的限速时间和限速值。

     配置了 ARP 报文的限速时间和限速值，在限速时间内超过限速值的 ARP 报文将被丢弃。缺省情况下，ARP 报文的限速值是 100，限速时间是 1 秒。
  5. （可选）执行命令 **arp anti-attack rate-limit alarm enable**，在接口视图下使能 ARP 报文限速丢弃告警功能。

     缺省情况下，未使能 ARP 报文限速丢弃告警功能。
  6. （可选）执行命令 **arp anti-attack rate-limit alarm threshold** *threshold*，在接口视图下配置 ARP 报文限速丢弃告警阈值。

     缺省情况下，ARP 报文限速丢弃告警阈值为 100。

----结束

6.5.4 配置 ARP Miss 消息源 IP 抑制

考虑到某些特定的用户有特别的需求，对于该用户的 IP 地址可以配置不同于其他 IP 地址的 ARP Miss 抑制速率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp-miss speed-limit source-ip maximum** *maximum*，配置 ARP Miss 消息源 IP 抑制速率。

步骤 3 （可选）执行命令 **arp-miss speed-limit source-ip** *ip-address* **maximum** *maximum*，配置指定 **source-ip** 用户的 ARP Miss 源 IP 抑制速率。

完成上述配置后，对指定了 **source-ip** 的用户，ARP Miss 源 IP 抑制速率为步骤 3 中配置的 *maximum* 值；其他 IP 地址的 ARP Miss 源 IP 抑制速率为步骤 2 中配置的 *maximum* 值。

如果将速率配置为 0，则表示不作 ARP Miss 源 IP 抑制。缺省情况下，所有 IP 地址的 ARP Miss 源 IP 抑制速率为 5pps。

----结束

6.5.5 配置 ARP Miss 消息速率抑制

介绍 ARP Miss 消息速率抑制的配置。

背景信息

如果在一定时间内不断上报 ARP Miss 消息，使得设备由于忙于发送广播 ARP 请求而性能下降。ARP Miss 消息的抑制功能是对上报的 ARP Miss 消息进行统计，并将超过限速值的 ARP Miss 消息丢弃的过程。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp-miss anti-attack rate-limit enable**，全局使能 ARP Miss 消息速率抑制功能。

缺省情况下，全局未使能 ARP Miss 消息速率抑制功能。

步骤 3 执行命令 **arp-miss anti-attack rate-limit** *packet-number* [*interval-value*]，配置 ARP Miss 消息的限速时间和限速值。

配置了 ARP Miss 消息的限速时间和限速值，在限速时间内超过限速值的 ARP Miss 消息将被丢弃。缺省情况下，ARP Miss 消息的限速值是 100，限速时间是 1 秒。

步骤 4 （可选）执行命令 **arp-miss anti-attack rate-limit alarm enable**，全局使能 ARP Miss 消息限速丢弃告警功能。

缺省情况下，未使能 ARP Miss 消息限速丢弃告警功能。

步骤 5 （可选）执行命令 **arp-miss anti-attack rate-limit alarm threshold** *threshold*，配置 ARP Miss 消息限速丢弃告警阈值。

缺省情况下，ARP Miss 消息限速丢弃告警阈值为 100。

----结束

6.5.6 配置 ARP 报文源 MAC 抑制

考虑到某些特定的用户有特别的需求，在对 ARP 报文进行源 MAC 抑制时，可以针对该用户的 MAC 地址配置不同于其他 MAC 地址的 ARP 报文抑制速率。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp speed-limit source-mac maximum** *maximum*，配置 ARP 报文源 MAC 抑制速率。

步骤 3 （可选）执行命令 **arp speed-limit source-mac** *mac-address* **maximum** *maximum*，配置指定 **source-mac** 用户的 ARP 报文源 MAC 抑制速率。

对指定了 **source-mac** 的用户，ARP 报文源 MAC 抑制速率为步骤 3 中配置的 *maximum* 值；其他 MAC 地址的 ARP 报文源 MAC 抑制速率为步骤 2 中配置的 *maximum* 值。

----结束

6.5.7 配置临时 ARP 表项的老化时间

通过设置临时 ARP 表项的老化超时时间，可以控制 ARP Miss 消息向上层软件发送的频率，从而减小对系统的攻击。

背景信息

临时 ARP 表项的老化时间配置成功后，在老化时间内，相同的 ARP Miss 信息只发送一次。老化时间超时后，临时 ARP 表项被清除，设备转发时如果匹配不到对应的 ARP 表项，重新生成 ARP Miss 消息进行上报，设备再次生成临时 ARP 表项发送给设备。直到设备生成正确的 ARP 表项替换掉临时 ARP 表项。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

接口类型包括 Ethernet、GigabitEthernet、Eth-Trunk 和 VLANIF。

步骤 3 执行命令 **arp-fake expire-time** *expire-time*，配置临时 ARP 表项的老化时间。

缺省情况下，临时 ARP 表项的老化时间是 1 秒。

----结束

6.5.8 （可选）配置 Super VLAN 的 VLANIF 接口下 ARP 报文速率抑制

通过在 Super VLAN 的 VLANIF 接口下配置 ARP Request 报文的速率抑制，系统可以将超过速率限制值的 ARP Request 报文丢弃，防止 CPU 忙于处理大量 ARP Request 报文。

背景信息

以下 2 种情况会触发 Super VLAN 的 VLANIF 接口进行 ARP 学习。

- VLANIF 接口接收到未知单播报文。
- 在 VLANIF 接口上启用 ARP 代理功能之后接收到 ARP Request 报文。

Super VLAN 的 VLANIF 接口进行 ARP 学习时会将 ARP Request 报文在每个 Sub VLAN 下复制，当该 Super VLAN 下配置大量 Sub VLAN 时，设备将产生大量的 ARP Request 报文，使得 CPU 忙于处理 ARP Request 报文，影响其他特性功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **arp speed-limit flood-rate** *rate*，配置 Super VLAN 的 VLANIF 接口下 ARP Request 报文的广播发送限制速率。

缺省情况下，Super VLAN 的 VLANIF 接口下 ARP Request 报文的广播发送限制速率为 1000pps。

----结束

6.5.9 检查配置结果

介绍检查 ARP 抑制的配置结果。

操作步骤

- 执行命令 **display arp anti-attack configuration** { **arp-rate-limit** | **arpmiss-rate-limit** }，查看当前 ARP 速率抑制配置。
- 执行命令 **display arp anti-attack configuration** { **arp-speed-limit** | **arpmiss-speed-limit** }，查看当前 ARP 源抑制配置。
- 执行命令 **display arp flood statistics**，查看所有 Super VLAN 的 VLANIF 接口下 ARP Request 报文的发送统计信息。

----结束

任务示例

查看 ARP 报文源抑制的抑制速率。

```
<Huawei> display arp anti-attack configuration arp-speed-limit
 ARP speed-limit for source-MAC configuration:
 MAC-address         suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 0000-0000-0001      150
 Others              200
-------------------------------------------------------------------------------
 1 specified MAC addresses are configured, spec is 256 items.

 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 10.0.0.20           50
 Others              100
-------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 512 items.
```

执行命令 **display arp flood statistics**，查看所有 Super VLAN 的 VLANIF 接口下 ARP Request 报文的发送统计信息。

```
<Huawei> display arp flood statistics
ARP request packets statistics on supervlan:
Total ARP request packets number :  5100
Sent ARP request packets number :  4000
Droped ARP request packets number:  1100
```

6.6 维护 ARP 安全

查看、清除 ARP 报文的统计信息，清除 ARP 丢弃报文计数以及调试 ARP 报文。

6.6.1 查看 ARP 报文统计信息

介绍查看 ARP 报文的统计信息。

操作步骤

- 使用命令 **display arp packet statistics**，查看 ARP 报文的统计信息。

----结束

任务示例

查询所有 ARP 统计情况。

```
<Huawei> display arp packet statistics
ARP Pkt Received:   sum  199992
ARP Learnt Count:   sum      4
ARP Pkt Discard For Limit:   sum      0
ARP Pkt Discard For SpeedLimit:   sum      0
ARP Pkt Discard For Proxy Suppress:   sum      0
ARP Pkt Discard For Other:   sum  18220
```

6.6.2 清除 ARP 报文统计信息

介绍清除 ARP 报文统计信息。

背景信息

注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除运行信息后，请在用户视图下执行下列命令。

操作步骤

- 执行命令 **reset arp packet statistics**，清除 ARP 报文的统计信息。
- 执行命令 **reset arp flood statistics**，清除所有 Super VLAN 的 VLANIF 接口下 ARP Request 报文的发送统计信息。

----结束

6.6.3 清除 ARP 丢弃报文计数

介绍清除 ARP 丢弃报文计数。

背景信息

注意

清除统计信息后，以前的统计信息将无法恢复，务必仔细确认。

在确认需要清除运行信息后，请在用户视图下执行下列命令。

操作步骤

- 执行命令 **reset arp anti-attack statistics rate-limit** { **global** | **interface** *interface-type interface-number* }，清除由于 ARP 报文速率超过限制阈值造成的丢弃计数。

----结束

6.7 配置举例

介绍 ARP 安全功能的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

6.7.1 配置 ARP 安全功能示例

介绍 ARP 安全功能的基本配置过程。

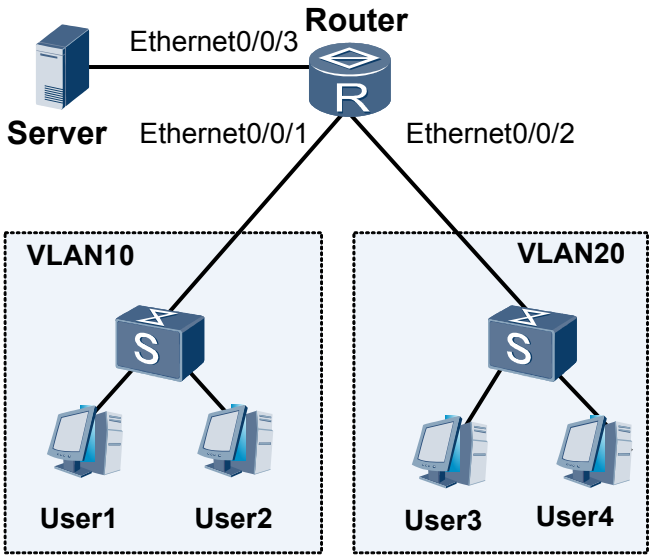
组网需求

如图 6-1 所示，Router 通过 Ethernet0/0/3 接口连接一台服务器，通过 Ethernet0/0/1 和 Ethernet0/0/2 接口连接 VLAN10 和 VLAN20 下的用户，且 Ethernet0/0/3 接口加入 VLAN30。网络中存在的 ARP 威胁是：

- 服务器可能会发出一些目的 IP 地址不可达的报文，而且这种报文相对其他普通用户的报文要多。
- 用户 User1 中病毒后，会发出大量 ARP 攻击报文，部分 ARP 报文的源 IP 地址在本网段内不停变化，部分 ARP 报文的源 IP 地址和网关 IP 地址相同。
- 用户 User3 构造大量源 IP 地址固定的 ARP 报文对网络进行攻击。
- 用户 User4 发送大量目的 IP 不可达的 IP 报文对网络进行攻击。

要求在 Router 配置 ARP 的安全功能，能够防止以上的攻击。需要配置服务器的 ARP Miss 源 IP 抑制的速率比其他用户大。

图 6-1 配置 ARP 安全功能组网图



配置思路

采用如下思路配置 ARP 的安全功能：

1. 配置严格学习 ARP 表项。
2. 配置基于接口的 ARP 表项限制。
3. 配置防止 ARP 地址欺骗攻击。
4. 配置防止 ARP 网关冲突攻击。
5. 配置 ARP 报文源 IP 抑制。

6. 配置 ARP Miss 源 IP 抑制。
7. 配置对潜在的攻击行为写日志和发送告警。

数据准备

为完成此配置举例，需要准备如下数据：

- 接口的 ARP 表项限制：20 个。
- 防止 User1 发起的 ARP 地址欺骗攻击方式为 **fixed-mac**。
- VLANIF10、VLANIF20 和 VLANIF30 的 IP 地址：2.2.1.10/24、2.2.4.10/24 和 2.2.2.10/24。
- 服务器 IP 地址：2.2.2.2/24。
- 发出大量 ARP 报文的 User4 的地址：2.2.4.2/24。
- ARP 报文速率源 IP 抑制阈值：User4 为 10pps，其他用户为 15pps。
- ARP Miss 源 IP 抑制阈值：普通用户为 20pps，对 Server 为 50pps。
- 对潜在的攻击行为写日志和发送告警的时间间隔为 300 秒。

操作步骤

步骤 1 创建 VLAN，配置接口加入 VLAN，配置相应 VLANIF 接口的 IP 地址（具体配置请参考配置文件）

步骤 2 配置严格学习 ARP 表项

```
<Huawei> system-view
[Huawei] sysname Router
[Router] arp learning strict
```

步骤 3 配置基于接口的 ARP 表项限制

配置接口 Ethernet0/0/1、Ethernet0/0/2 和 Ethernet0/0/3 的 ARP 表项限制为 20，以 Ethernet0/0/1 为例。

```
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] arp-limit vlan 10 maximum 20
[Router-Ethernet0/0/1] quit
```

步骤 4 配置防止 ARP 地址欺骗攻击

配置 ARP 地址欺骗防攻击方式为 **fixed-mac** 方式，防止 User1 发起的 ARP 地址欺骗攻击。

```
[Router] arp anti-attack entry-check fixed-mac enable
```

步骤 5 配置防止 ARP 网关冲突攻击

使能 ARP 网关冲突防攻击功能，防止 User1 发起的伪造网关地址攻击。

```
[Router] arp anti-attack gateway-duplicate enable
```

步骤 6 配置 ARP 报文源 IP 抑制

配置 User4 发送的 ARP 报文速率抑制阈值为 10pps。为防止所有用户误发过多 ARP 报文，配置系统的 ARP 报文速率抑制阈值为 15pps。

```
[Router] arp speed-limit source-ip maximum 15
[Router] arp speed-limit source-ip 2.2.4.2 maximum 10
```

步骤 7 配置 ARP Miss 源 IP 抑制

配置系统的 ARP Miss 源 IP 抑制阈值为 20pps，以防止较大流量目的 IP 地址不可达的 IP 报文的攻击。

```
[Router] arp-miss speed-limit source-ip maximum 20
```

配置 Server 的 ARP Miss 源 IP 抑制阈值为 50pps，这样既防止 Server 无意发起大流量目的 IP 地址不可达的 IP 报文的攻击；又防止在其发送的目的 IP 地址不可达的 IP 报文速率并非特别大的时候，就阻止了它的网络通信。

```
[Router] arp-miss speed-limit source-ip 2.2.2.2 maximum 50
```

步骤 8 验证配置结果

配置完成后，可以使用命令 **display arp learning strict**，查看 ARP 严格学习情况。

```
<Router> display arp learning strict
 The global configuration:arp learning strict
 interface                          LearningStrictState
------------------------------------------------------------
------------------------------------------------------------
 Total:0
 force-enable:0
 force-disable:0
```

可以使用命令 **display arp-limit** 查看接口可以学习 ARP 数目的最大值。以 Ethernet0/0/1 接口为例。

```
<Router> display arp-limit interface ethernet 0/0/1
 interface                    LimitNum   VlanID     LearnedNum(Mainboard)
------------------------------------------------------------------------
 Ethernet0/0/1                  20         10          0
------------------------------------------------------------------------
 Total:1
```

可以使用命令 **display arp anti-attack configuration all** 查看当前 ARP 防攻击配置情况。

```
<Router> display arp anti-attack configuration all
 ARP anti-attack packet-check function: disabled

 ARP anti-attack entry-check mode: fixed-MAC

 ARP gateway-duplicate anti-attack function: enabled

 ARP rate-limit configuration:
-------------------------------------------------------------------------------
 Global configuration:
 Interface configuration:
-------------------------------------------------------------------------------

 ARP miss rate-limit configuration:
-------------------------------------------------------------------------------
 Global configuration:
-------------------------------------------------------------------------------

 ARP speed-limit for source-MAC configuration:
 MAC-address         suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 All                 0
-------------------------------------------------------------------------------
 0 specified MAC addresses are configured, spec is 256 items.


 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 ------------------------------------------------------------------------
 2.2.4.2             10
```

```
 Others              15
 ------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 128 items.

 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 ------------------------------------------------------------------------------
 2.2.2.2             50
 Others              20
 ------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 128 items.
```

可以使用命令 **display arp packet statistics** 查看丢弃的 ARP 报文数目和学习到的 ARP 表项。

```
<Router> display arp packet statistics
ARP Pkt Received:   sum    167
ARP Learnt Count:   sum      8
ARP Pkt Discard For Limit:   sum      5
ARP Pkt Discard For SpeedLimit:   sum      0
ARP Pkt Discard For Proxy Suppress:   sum      0
ARP Pkt Discard For Other:   sum      3
```

同时，还可以通过 **display arp anti-attack gateway-duplicate item** 命令查看当前网络中存在的网关地址冲突攻击信息。

```
<Router> display arp anti-attack gateway-duplicate item
 interface               IP address       MAC address     VLANID   aging time
--------------------------------------------------------------------------------
 Ethernet0/0/1           2.2.1.10         0000-0000-0002    10         153
 Ethernet0/0/2           2.2.4.10         0000-0000-0004    20         179
--------------------------------------------------------------------------------
There are 2 records in gateway conflict table
```

----结束

配置文件

```
#
 sysname Router
#
vlan batch 10 20 30
#
 arp speed-limit source-ip maximum 15
 arp-miss speed-limit source-ip maximum 20
 arp learning strict
#
 arp anti-attack entry-check fixed-mac enable
 arp anti-attack gateway-duplicate enable
 arp-miss speed-limit source-ip 2.2.2.2 maximum 50
 arp speed-limit source-ip 2.2.4.2 maximum 10
#
interface Ethernet0/0/1
 port hybrid pvid vlan 10
 port hybrid tagged vlan 10
 arp-limit vlan 10 maximum 20
#
interface Ethernet0/0/2
 port hybrid pvid vlan 20
 port hybrid tagged vlan 20
 arp-limit vlan 20 maximum 20
#
interface Ethernet0/0/3
 port hybrid pvid vlan 30
 port hybrid tagged vlan 30
 arp-limit vlan 30 maximum 20
#
```

```
interface Vlanif 10
 ip address 2.2.1.10 255.255.255.0
#
interface Vlanif 20
 ip address 2.2.4.10 255.255.255.0
#
interface Vlanif 30
 ip address 2.2.2.10 255.255.255.0
#
return
```

7 ICMP 安全配置

关于本章

介绍 ICMP 安全的基本原理、配置方法和配置举例。

7.1 ICMP 安全概述
简要介绍 ICMP 安全原理。

7.2 AR1200 支持的 ICMP 安全特性
AR1200 支持的 ICMP 安全特性包括 ICMP 报文限速、合法性检查和丢弃 ICMP 报文以及不响应目的不可达报文。

7.3 配置 ICMP 报文限速
介绍 ICMP 报文限速的配置过程。

7.4 配置丢弃 ICMP 报文
介绍设备丢弃 ICMP 报文的配置。

7.5 配置不响应目的不可达报文
介绍不响应目的不可达报文功能的配置过程。

7.6 维护 ICMP 安全
介绍了使用 display 命令监控 ICMP 运行状况。

7.7 配置举例
介绍 ICMP 安全的配置举例。

7.1 ICMP 安全概述

简要介绍 ICMP 安全原理。

ICMP（Internet Control Message Protocol）是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。

设备会收到来自网络的大量 ICMP 报文，对设备 CPU 造成冲击，因此需要对 ICMP 报文做一些合法性检查、丢弃 ICMP 报文和速率限制来保证设备的安全。

7.2 AR1200 支持的 ICMP 安全特性

AR1200 支持的 ICMP 安全特性包括 ICMP 报文限速、合法性检查和丢弃 ICMP 报文以及不响应目的不可达报文。

ICMP 报文限速

网络中设备会收到大量的 ICMP 报文，对设备 CPU 造成冲击，设备可以对收到的 ICMP 报文进行速率限制，从而减轻 CPU 的负担，保证业务的正常运行。

AR1200 支持基于全局和接口对 ICMP 报文进行速率限制。

合法性检查和丢弃 ICMP 报文

对于一些不合法的 ICMP 报文，比如 TTL=0 的 ICMP 报文、类型为 15、16、17 的 ICMP 报文，AR1200 默认将直接丢弃，以保护 CPU 资源。

AR1200 支持配置丢弃某些不常用或基本不使用的 ICMP 报文，包括 TTL=1 的 ICMP 报文、带选项的 ICMP 报文、目的不可达的 ICMP 报文，减轻设备处理 ICMP 报文的压力，保护 CPU 资源。

不响应目的不可达报文

AR1200 支持配置不响应目的不可达报文，包括主机不可达报文和端口不可达报文。这样，当攻击者通过发送大量目的不可达报文攻击 AR1200 时，AR1200 将不响应并直接丢弃这些目的不可达报文，以保护 CPU 资源。

7.3 配置 ICMP 报文限速

介绍 ICMP 报文限速的配置过程。

应用环境

网络中设备会收到大量的 ICMP 报文，对设备 CPU 造成冲击，设备可以对收到的 ICMP 报文进行速率限制，将超过限速阈值的报文丢弃，从而减轻 CPU 的负担，保证业务的正常运行。

说明

配置该功能后，会影响 AR1200 对 PING 报文的响应。

操作步骤

- 配置基于全局的 ICMP 报文限速。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **icmp rate-limit enable**，使能全局 ICMP 报文的限速功能。

     缺省情况下，全局 ICMP 报文的限速功能不使能。
  3. （可选）执行命令 **icmp rate-limit threshold** *threshold-value*，配置基于全局的 ICMP 报文限速的阈值。

     缺省情况下，全局的 ICMP 报文的限速阈值为 100pps。
- 配置基于接口的 ICMP 报文限速。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

     AR1200 支持 ICMP 报文限速功能的接口包括 GE 接口、Ethernet 接口和 Eth-Trunk 接口。
  3. 执行命令 **icmp rate-limit enable**，使能接口 ICMP 报文的限速功能。

     缺省情况下，接口 ICMP 报文的限速功能不使能。
  4. （可选）执行命令 **icmp rate-limit threshold** *threshold-value*，配置基于接口的 ICMP 报文限速的阈值。

     缺省情况下，接口的 ICMP 报文的限速阈值为 100pps。

     如果需要配置多个接口的 ICMP 报文限速阈值，可以反复执行此步骤。

----结束

检查配置结果

执行命令 **display current-configuration | include icmp**，查看 ICMP 报文限速的配置信息。

```
<Huawei> display current-configuration | include icmp
 icmp rate-limit enable
 icmp rate-limit threshold 120
```

7.4 配置丢弃 ICMP 报文

介绍设备丢弃 ICMP 报文的配置。

7.4.1 建立配置任务

在配置丢弃 ICMP 报文前了解此特性的应用环境、前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

设备会收到来自网络的大量 ICMP 报文，对设备 CPU 造成冲击，AR1200 支持配置丢弃某些不常用或基本不使用的 ICMP 报文，包括 TTL=1 的 ICMP 报文、带选项的 ICMP 报文、目的不可达的 ICMP 报文，减轻设备处理 ICMP 报文的压力，保护 CPU 资源。

前置任务

在配置 ICMP 报文限速之前，需要完成以下任务：

- 配置接口的网络层协议参数，使接口的路由协议状态为 Up

数据准备

无

7.4.2 配置丢弃 TTL=1 的 ICMP 报文

介绍丢弃 TTL=1 的 ICMP 报文的配置过程。

背景信息

网络中 ICMP 流量过大，会对 CPU 造成冲击，为了防御这种攻击，AR1200 支持配置丢弃 TTL=1 的 ICMP 报文，以减轻设备处理 ICMP 报文的压力，保护 CPU 资源。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **icmp ttl-exceeded drop**，使能全局丢弃 TTL=1 的 ICMP 报文功能。

缺省情况下，不使能全局丢弃 TTL=1 的 ICMP 报文功能。

----结束

7.4.3 配置丢弃带选项的 ICMP 报文

介绍丢弃带选项的 ICMP 报文的配置过程。

背景信息

ICMP 报文的 IP 头带有选项，会使设备忙于进行这些选项所要求的操作（如计算经过的路由总跳数），而影响对正常业务的处理。

当网络中 ICMP 流量过大时，会对 CPU 造成冲击。为了防御这种攻击，AR1200 支持丢弃带选项的 ICMP 报文功能，以减轻设备处理 ICMP 报文的压力，保护 CPU 资源。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **icmp with-options drop**，使能全局丢弃带选项的 ICMP 报文功能。

缺省情况下，不使能丢弃带选项的 ICMP 报文功能。

----结束

7.4.4 配置丢弃目的不可达的 ICMP 报文

介绍丢弃目的不可达的 ICMP 报文的配置过程。

背景信息

网络中 ICMP 流量过大，会对 CPU 造成冲击，为了防御这种攻击，AR1200 支持丢弃目的不可达的 ICMP 报文功能，以减轻设备处理 ICMP 报文的压力，保护 CPU 资源。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **icmp unreachable drop**，使能丢弃目的不可达 ICMP 报文功能。

缺省情况下，不使能丢弃目的不可达 ICMP 报文功能。

----结束

7.4.5 检查配置结果

可以查看丢弃 ICMP 报文的配置信息。

操作步骤

- 执行命令 **display current-configuration**，查看丢弃 ICMP 报文的配置信息。

----结束

任务示例

执行命令 **display current-configuration | include icmp**，查看丢弃 ICMP 报文的配置信息。

```
<Huawei> display current-configuration | include icmp
 icmp unreachable drop
 icmp ttl-exceeded drop
 icmp with-options drop
```

7.5 配置不响应目的不可达报文

介绍不响应目的不可达报文功能的配置过程。

应用环境

AR1200 支持不响应目的不可达报文，包括主机不可达报文和端口不可达报文。这样，当攻击者通过发送大量目的不可达报文攻击 AR1200 时，AR1200 不响应并直接丢弃这些不可达报文，以保护 CPU 资源。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **undo icmp port-unreachable send**，去使能设备的端口不可达 ICMP 报文的发送功能。

缺省情况下，AR1200 使能端口不可达 ICMP 报文的发送功能。

步骤 3 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 不支持在二层接口下配置主机不可达 ICMP 报文的发送功能。

步骤 4 执行命令 **undo icmp host-unreachable send**，在接口上去使能主机不可达 ICMP 报文的发送功能。

缺省情况下，AR1200 使能主机不可达 ICMP 报文的发送功能。

----结束

检查配置结果

执行命令 **display current-configuration | include icmp**，查看 ICMP 报文发送功能的配置信息。

```
<Huawei> display current-configuration | include icmp
 undo icmp port-unreachable send
 undo icmp host-unreachable send
```

7.6 维护 ICMP 安全

介绍了使用 display 命令监控 ICMP 运行状况。

操作步骤

- 执行命令 **display icmp statistics**，查看 ICMP 流量统计信息。

----结束

任务示例

执行命令 **display icmp statistics**，查看 ICMP 流量统计信息。

```
<Huawei> display icmp statistics
  Input: bad formats       0      bad checksum               0
         echo              0      destination unreachable    0
         source quench     0      redirects                  0
         echo reply        0      parameter problem          0
         timestamp         0      information request        0
         mask requests     0      mask replies               0
         time exceeded     0
         Mping request     0      Mping reply                0
  Output:echo              0      destination unreachable    0
         source quench     0      redirects                  0
         echo reply        0      parameter problem          0
         timestamp         0      information reply          0
         mask requests     0      mask replies               0
         time exceeded     0
         Mping request     0      Mping reply                0
```

7.7 配置举例

介绍 ICMP 安全的配置举例。

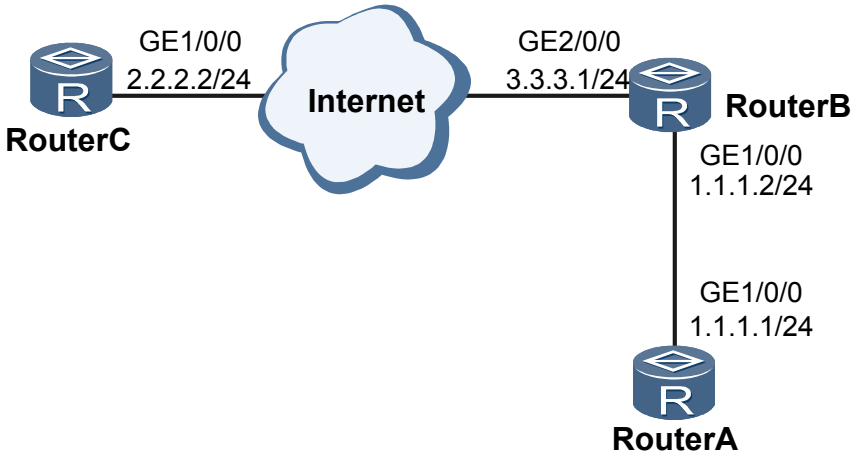
7.7.1 配置不响应主机不可达报文示例

介绍配置不响应主机不可达报文功能的配置过程。

组网需求

如图 7-1 所示，为测试主机不可达 ICMP 报文的发送功能需要 RouterA、RouterB、RouterC 三台设备，并且这三台设备通过各自的三层接口相连。

图 7-1 配置不响应主机不可达报文组网图



配置思路

配置不响应主机不可达报文的思路如下：

1. 在各设备上的相应接口上配置 IP 地址。
2. 配置 RouterA 到 RouterC 的静态路由。
3. 在 RouterA 和 RouterC 接口上使能发送主机不可达 ICMP 报文的功能。

   说明

   缺省情况下，接口视图下的主机不可达 ICMP 报文功能处于使能状态。如果没有关闭接口的主机不可达 ICMP 报文功能，则不需要配置这一步。
4. 在 RouterB 的接口 GE1/0/0 上关闭发送主机不可达 ICMP 报文的功能，这样，RouterB 将不响应接口 GE1/0/0 收到的主机不可达报文。

数据准备

完成此配置，需准备如下的数据：

- RouterA 到达 RouterC 的静态路由
- 各接口的 IP 地址

操作步骤

步骤 1 配置 RouterA

在 RouterA 上配置静态路由。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
```

配置接口 GE1/0/0 的 IP 地址。

```
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 1.1.1.1 24
[RouterA-GigabitEthernet1/0/0] quit
```

步骤 2 配置 RouterC

在 RouterC 上配置接口 GE1/0/0 的 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterC
[RouterC] interface gigabitethernet 1/0/0
[RouterC-GigabitEthernet1/0/0] ip address 2.2.2.2 24
[RouterC-GigabitEthernet1/0/0] quit
```

步骤 3 配置 RouterB

在 RouterB 的接口 GE1/0/0 上取消主机不可达 ICMP 报文的发送功能，并配置接口 GE1/0/0 的 IP 地址。

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface gigabitethernet 1/0/0
[RouterB-GigabitEthernet1/0/0] undo icmp host-unreachable send
[RouterB-GigabitEthernet1/0/0] ip address 1.1.1.2 24
[RouterB-GigabitEthernet1/0/0] quit
[RouterB] quit
```

步骤 4 验证配置结果。

打开 RouterB 的 ICMP 报文调试开关。

```
<RouterB> debugging ip icmp
<RouterB> terminal monitor
<RouterB> terminal debugging
```

在 RouterA 上运行 **ping 2.2.2.2**，可以看到 RouterB 不发送主机不可达 ICMP 报文。

由于 RouterB 到 RouterC 的路由不可达，正常情况下 RouterB 应该响应来自 RouterA 的 PING 报文，并给 RouterA 发送一个主机不可达 ICMP 报文。由于 RouterB 接口上关闭主机不可达 ICMP 报文的发送功能，所以 RouterB 不响应来自 RouterA 的 PING 报文。

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet 1/0/0
 ip address 1.1.1.1 255.255.255.0
#
 ip route-static 2.2.2.0 255.255.255.0 1.1.1.2
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet 1/0/0
 ip address 1.1.1.2 255.255.255.0
 undo icmp host-unreachable send
#
```

```
return
```

- RouterC 的配置文件

```
#
 sysname RouterC
#
interface GigabitEthernet 1/0/0
 ip address 2.2.2.2 255.255.255.0
#
return
```

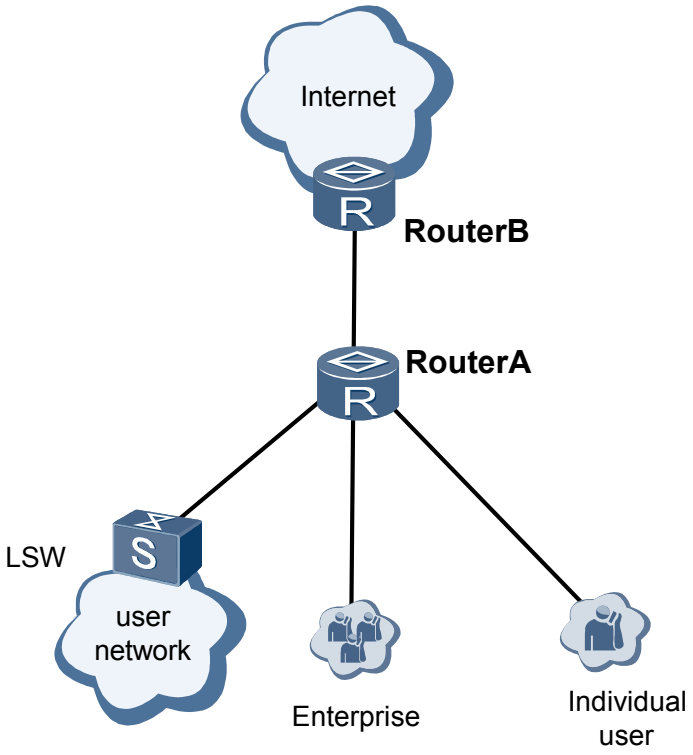
7.7.2 通过丢弃某种 ICMP 报文优化系统性能示例

介绍通过丢弃某种 ICMP 报文优化系统性能示例的配置过程。

组网需求

如图 7-2 所示，RouterA 作为企业网接入设备，下挂企业、个人用户、以及本地交换机设备连接的用户网络，上接汇聚路由器设备接入 Internet。要求在 RouterA 上配置丢弃 TTL 为 1、带选项、目的不可达的 ICMP 报文，减轻设备处理大量 ICMP 报文的压力。

图 7-2 配置 ICMP 安全功能组网图



配置思路

直接在 RouterA 的系统视图下配置：

- 配置丢弃 TTL 为 1 的 ICMP 报文。
- 配置丢弃带选项的 ICMP 报文。

- 配置丢弃目的不可达 ICMP 报文。

数据准备

无

操作步骤

步骤 1 配置丢弃某些 ICMP 报文。

配置丢弃 TTL 为 1 的所有 ICMP 报文。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] icmp ttl-exceeded drop
```

配置丢弃带选项的所有 ICMP 报文。

```
[RouterA] icmp with-options drop
```

配置丢弃目的不可达的所有 ICMP 报文。

```
[RouterA] icmp unreachable drop
```

步骤 2 验证配置结果。

在用户视图下执行命令 **display current-configuration**，可以看到 ICMP 安全配置。

```
<RouterA> display current-configuration | include icmp
 icmp unreachable drop
 icmp ttl-exceeded drop
 icmp with-options drop
```

----结束

配置文件

```
#
 sysname RouterA
#
 icmp unreachable drop
 icmp ttl-exceeded drop
 icmp with-options drop
#
return
```

8 IP 源防攻击配置

关于本章

针对网络中利用报文的源 IP 地址对合法用户进行攻击的行为，本章介绍了应对的原理和方法。

8.1 IP 源防攻击概述
IP 源防攻击可以防范针对源 IP 地址进行欺骗的攻击行为。

8.2 AR1200 支持的 IP 源防攻击特性
介绍 IP 源防攻击特性在 AR1200 中的支持情况。

8.3 配置 URPF
介绍配置 URPF 功能的应用环境、操作步骤。

8.4 配置举例
介绍 IP 源防攻击的配置举例。

8.1 IP 源防攻击概述

IP 源防攻击可以防范针对源 IP 地址进行欺骗的攻击行为。

随着网络规模的扩大，基于源 IP 地址欺骗发起的网络攻击，已经成为一种普遍的攻击形式。攻击者向基于 IP 地址验证的服务器发送带有合法用户 IP 地址的报文，使自己以合法用户的身份获得访问应用服务器的权限，导致合法用户不能正常获得网络服务，或者造成合法用户的信息泄露。针对此类攻击，AR1200 支持 URPF（Unicast Reverse Path Forwarding）功能。

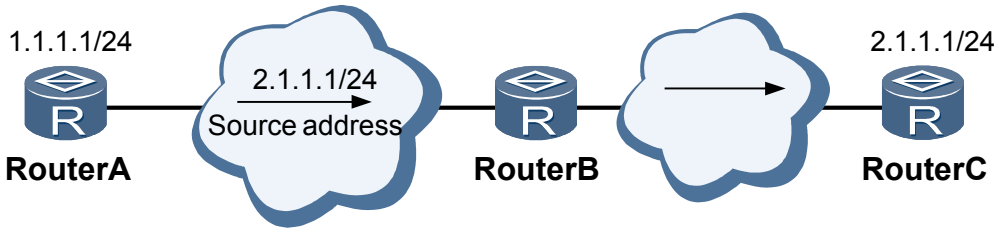
URPF

一般情况下，AR1200 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出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。

如图 8-1 所示，RouterA 转发伪造的源地址为 2.1.1.1 的报文，向 RouterB 发起请求。RouterB 响应请求时将向真正的“2.1.1.1”发送报文。这种非法报文对 RouterB 和 RouterC 都造成了攻击。

如果在 RouterB 的接口上启用 URPF 功能，RouterB 在收到源地址为 2.1.1.1 的非法报文时，会检查到该报文不应该从 RouterA 方向的接口进入，则该非法报文被 RouterB 丢弃。

图 8-1 URPF 功能示意图



8.2 AR1200 支持的 IP 源防攻击特性

介绍 IP 源防攻击特性在 AR1200 中的支持情况。

URPF

URPF 只在 AR1200 的三层入接口起作用。当在相应的接口使能了 URPF 功能，URPF 将对经过这个接口的入报文进行相应的检查。

AR1200 支持两种 URPF 检查方式：严格检查和松散检查。

- 严格检查：报文的源地址必须在 AR1200 的 FIB 表存在，而且其相应的出接口必须和报文的入接口相一致，才能被转发。否则将不能通过检查，被丢弃。

- 松散检查：报文的源地址在 AR1200 的 FIB 中存在，不管其相应的出接口和报文的入接口是否一致，都将通过检查，进行正常的转发。

8.3 配置 URPF

介绍配置 URPF 功能的应用环境、操作步骤。

应用环境

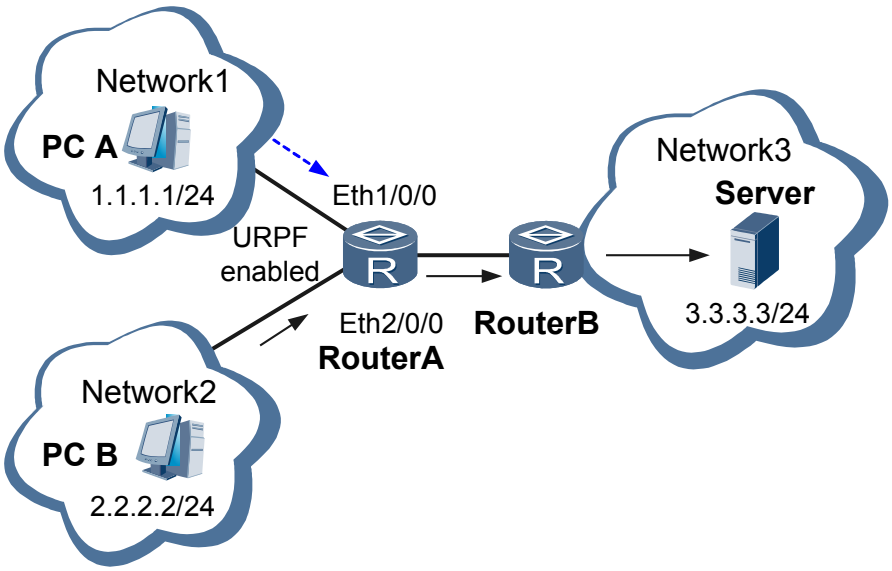
企业网用户获取外部基于 IP 地址验证的应用时，经常会受到来自不同网段非法用户的攻击。攻击者向服务器发送带有合法用户 IP 地址的报文，使自己以合法用户的身份获得访问应用服务器的权限，导致企业网内部合法用户不能正常获得服务器提供的应用，或者造成企业网内部合法用户的信息泄露。为了防止此类攻击，可以在 AR1200 上配置 URPF 功能。

如图 8-2 所示，Network1 和 NetWork2 分别通过 GE1/0/0 接口和 GE2/0/0 接口与 RouterA 连接，在 RouterA 的 GE1/0/0 接口和 GE2/0/0 接口上配置 URPF 严格检查功能。

如果 Network1 中的主机 PC A 伪造了一个源地址为 2.2.2.2 的报文，向 NetWork3 中的 Server 发送请求。RouterA 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 GE2/0/0 接口进入，而不应该从 GE1/0/0 接口进入，则 RouterA 认为该报文源地址是伪造的，直接丢弃该伪造报文。这样，保护 NetWork2 的 PC B 免受来自 PC A 的源 IP 地址欺骗攻击。

从 NetWork2 发向 Server 的正常报文，检查通过后，可以正常转发。

图 8-2 URPF 应用环境示意图



操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface** *interface-type interface-number*，进入接口视图。

AR1200 不支持在二层接口配置 URPF 检查功能。

步骤 3 配置对接口的报文进行 URPF 检查。

- 配置对接口的 IPv4 报文进行 URPF 检查的模式。

  执行命令 **urpf** { **loose** | **strict** } [**allow-default-route**]，配置对接口的 IPv4 报文进行 URPF 检查的模式。

- 配置对接口的 IPv6 报文进行 URPF 检查的模式。

  执行命令 **ipv6 urpf** { **loose** | **strict** } [**allow-default-route**]，配置对接口的 IPv6 报文进行 URPF 检查的模式。

  说明

  如果需要配置对接口的 IPv6 报文进行 URPF 检查的功能，需要先使能接口的 IPv6 功能。请先在系统视图下执行命令 **ipv6**，然后在接口视图下执行命令 **ipv6 enable**。

----结束

检查配置结果

完成配置后，在接口视图下执行命令 **display this**，查看接口下 URPF 功能的配置情况。

```
[Huawei-GigabitEthernet1/0/0] display this
#
interface GigabitEthernet 1/0/0
 urpf strict allow-default-route
 ipv6 urpf strict allow-default-route
#
return
```

8.4 配置举例

介绍 IP 源防攻击的配置举例。

8.4.1 配置 URPF 功能示例

介绍 URPF 功能的配置示例。

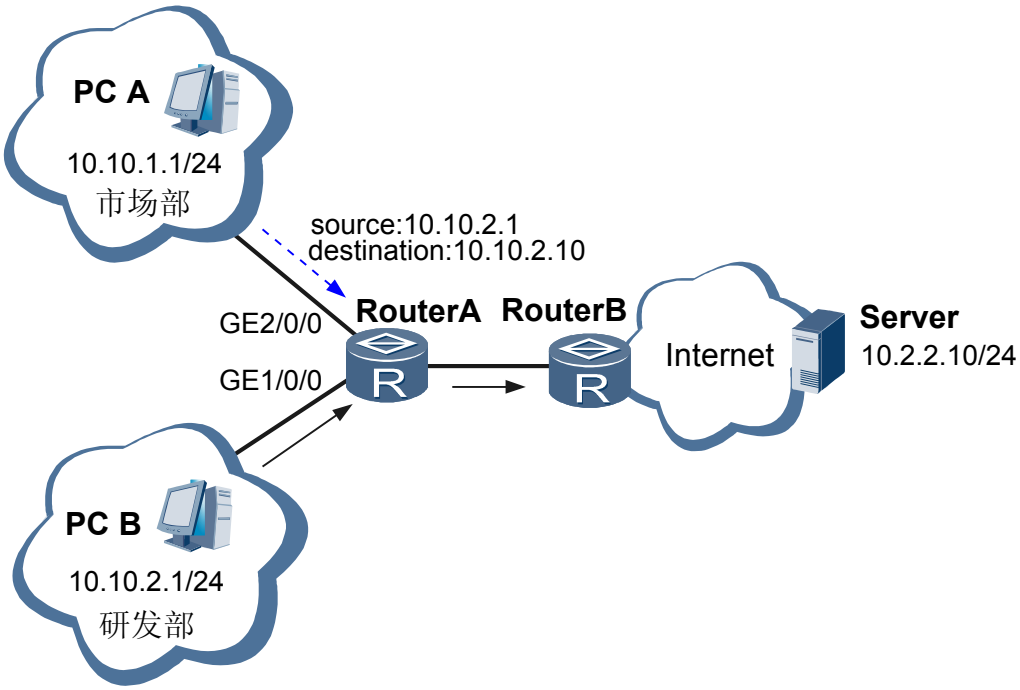
组网需求

如图 8-3 所示，某企业研发部和市场部通过接口 GE1/0/0 和接口 GE2/0/0 与 RouterA 连接，RouterA 与外部的某个 Server 之间路由可达，研发部员工和市场部员工都可以通过 RouterA 访问该 Server。公司希望在 RouterA 上进行配置，防止不同部门的员工利用源 IP 地址欺骗的方法超越权限，非法获取 Server 的服务。

说明

图 8-3 中的 RouterA 是指企业路由器，RouterB 是指汇聚路由器。

图 8-3 配置 URPF 组网图



配置思路

该组网的配置思路如下：

在接口 GE1/0/0 和接口 GE2/0/0 配置 URPF 功能，并允许对缺省路由进行特殊处理。

数据准备

- URPF 检查模式：严格检查。

  说明

  本例组网是路由对称的环境，因此使用严格检查模式。
- 研发部网段：10.10.2.0/24。
- 市场部网段：10.10.1.0/24。
- Server 的 IP 地址：10.2.2.10/24。

操作步骤

步骤 1 配置接口的 URPF 检查模式。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] urpf strict allow-default-route
[RouterA] interface gigabitethernet 2/0/0
[RouterA-GigabitEthernet2/0/0] urpf strict allow-default-route
```

步骤 2 验证配置结果。

在 GE1/0/0 接口视图下执行命令 **display this** 查看 URPF 配置。

```
[RouterA-GigabitEthernet1/0/0] display this
#
interface GigabitEthernet 1/0/0
 urpf strict allow-default-route
#
return
```

在 GE2/0/0 接口视图下执行命令 **display this** 查看 URPF 配置。

```
[RouterA-GigabitEthernet2/0/0] display this
#
interface GigabitEthernet 2/0/0
 urpf strict allow-default-route
#
return
```

----结束

配置文件

```
#
sysname RouterA
#
interface GigabitEthernet 1/0/0
 urpf strict allow-default-route
#
interface GigabitEthernet 2/0/0
 urpf strict allow-default-route
#
return
```

9 本机防攻击配置

关于本章

介绍本机防攻击的基本原理、配置方法和配置举例。

9.1 本机防攻击概述
简单介绍本机防攻击的概念和作用。

9.2 AR1200 支持的本机防攻击特性
介绍 AR1200 支持的本机防攻击特性。

9.3 配置攻击溯源
配置攻击溯源，分析上送 CPU 的报文是否会对 CPU 造成攻击，对可能造成攻击的报文进行写日志或告警提醒网络管理员。

9.4 配置 CPU 防攻击
配置 CPU 防攻击功能，可以限制上送 CPU 的报文，保护 CPU 的性能，保证 CPU 对正常业务的处理。

9.5 维护防攻击策略
包括清除上送 CPU 报文统计信息、清除攻击源信息。

9.6 配置举例
介绍本地防攻击的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

9.1 本机防攻击概述

简单介绍本机防攻击的概念和作用。

在网络中，存在着大量针对 CPU 的恶意攻击报文或者正常的需要上送 CPU 的报文，针对 CPU 的恶意攻击报文会引发其他业务的断续甚至系统的中断，大量正常的报文也会导致 CPU 占用率过高，性能下降，从而影响正常的业务。

为保护 CPU，保持 CPU 对正常业务的处理和响应，AR1200 提供了本机防攻击功能。本机防攻击针对的是上送 CPU 的报文，主要用于保护设备自身安全、保证已有业务在发生攻击时的正常运转、屏蔽遭受攻击时各业务的相互影响。

9.2 AR1200 支持的本机防攻击特性

介绍 AR1200 支持的本机防攻击特性。

AR1200 支持的防攻击策略

AR1200 支持名称为 **default** 的缺省防攻击策略，**default** 策略对速率限制、协议优先级和统一限速功能进行缺省配置，并且默认应用到所有单板，不允许删除，也不允许修改参数。

AR1200 支持用户自己创建防攻击策略。如果用户创建新的防攻击策略，则在防攻击策略视图下，用户可以按照自己的需要进行配置，此配置将覆盖 **default** 策略的缺省配置；对于用户没有进行的配置，新的防攻击策略将使用 **default** 策略的缺省配置。

说明

防攻击策略对于从 3G Cellular 接口上送到主控板 CPU 的协议报文不生效。

说明

对于 AR1220 设备，防攻击策略对于从 LAN 接口板上送到主控板 CPU 的三层协议报文不生效。

AR1200 支持的防攻击功能

AR1200 支持在同一个防攻击策略中配置攻击溯源和 CPU 防攻击。

攻击溯源提供了一种防攻击手段，通过分析上送 CPU 的报文是否会对 CPU 造成攻击，将可能造成攻击的报文的情况，以日志或告警的方式通知网络管理员，这样网络管理员可以对可能的攻击源进行防御部署，比如，将可能的攻击源列入黑名单中。攻击溯源包括以下功能：

- 攻击溯源检查功能

  使能攻击溯源功能后，网络管理员可以配置攻击溯源检查阈值，当可能的攻击源在单位时间内发送某种协议类型的报文超过此阈值时，设备开始溯源，并将攻击源记录到日志中，通过日志方式提醒网络管理员。

- 攻击溯源告警功能

  使能攻击溯源告警功能后，网络管理员可以配置攻击溯源告警阈值，当可能的攻击源在单位时间内发送某种协议类型的报文超过此阈值时，设备以告警的方式通知网络管理员。

CPU 防攻击对上送 CPU 的报文进行限制和约束，使单位时间内上送 CPU 报文的数量限制在一定的范围之内，从而保护 CPU 的安全，保证 CPU 对正常业务的处理。CPU 防攻击包括以下功能：

- 黑名单

  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 AR1200 后均会被丢弃。

- 速率限制

  速率限制将限制报文上送 CPU 的速率。AR1200 可以通过对不同类型的报文设置不同的限制速率，也可以对报文设置为丢弃，从而减少上送 CPU 的报文数量，降低不同类型报文的相互影响，达到保护 CPU 的目的。

- 协议优先级

  AR1200 支持对上送 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。

- 统一限速

  AR1200 支持对所有上送 CPU 的报文进行统一限速，使所有上送 CPU 的报文的整体速率限制在一个范围之内，保证 CPU 可以正常处理其他业务。

- 动态链路保护

  AR1200 通过动态链路保护特性保护基于会话的应用层数据，包括 HTTP Session 数据、FTP Session 数据以及 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 AR1200 检测到 HTTP Session、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。

9.3 配置攻击溯源

配置攻击溯源，分析上送 CPU 的报文是否会对 CPU 造成攻击，对可能造成攻击的报文进行写日志或告警提醒网络管理员。

应用环境

网络上可能会出现大量攻击报文攻击网络节点设备的 CPU。攻击溯源提供了一种防攻击手段，通过分析上送 CPU 的报文是否会对 CPU 造成攻击，对可能造成攻击的报文进行以日志或告警的方式通知网络管理员，这样网络管理员可以对可能的攻击源进行防御部署。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，创建防攻击策略并进入防攻击策略视图。

AR1200 最多支持 19 个防攻击策略。其中名称为 **default** 的策略为系统自动生成的缺省策略，**default** 策略默认应用到所有单板，不允许删除，也不允许修改参数；其余 18 个允许用户创建和删除。

步骤 3 （可选）执行命令 **description** *text*，配置防攻击策略的描述信息。

步骤 4 执行命令 **auto-defend enable**，使能攻击溯源功能。

缺省情况下，攻击溯源功能未使能。

步骤 5 （可选）执行命令 **auto-defend protocol** { **all** | { **arp** | **dhcp** | **icmp** | **igmp** | **tcp** | **telnet** | **ttl-expired** } * }，配置攻击溯源防范的报文类型。

缺省情况下，攻击溯源防范的报文类型为 ARP、DHCP、ICMP、IGMP、TCP、Telnet 和 TTL-expired。

步骤 6 （可选）执行命令 **auto-defend trace-type** { **source-ip** | **source-mac** | **source-portvlan** } *，配置攻击溯源的溯源模式。

缺省情况下，攻击溯源的溯源模式为 **source-ip**、**source-mac** 和 **source-portvlan**。

步骤 7 （可选）执行命令 **auto-defend threshold** *threshold*，配置攻击溯源检查阈值。

缺省情况下，攻击溯源检查阈值为 128pps。

步骤 8 （可选）执行命令 **auto-defend action deny** [**timer** *time-length*]，配置对检测到的攻击源进行惩罚。

缺省情况下，AR1200 不对检测到的攻击源进行惩罚。

步骤 9 （可选）配置攻击溯源告警功能

1. 执行命令 **auto-defend alarm enable**，使能攻击溯源告警功能。

   缺省情况下，攻击溯源告警功能未使能。

2. （可选）执行命令 **auto-defend alarm threshold** *threshold*，配置攻击溯源告警阈值。

步骤 10 在系统试图下执行命令 **cpu-defend-policy** *policy-name* [**global** | **slot** *slot-id*]，应用防攻击策略。

执行此命令时，不带参数 **global** 和 **slot**，则防攻击策略应用到主控板；带参数 **global**，则防攻击策略应用到所有接口板；带参数 **slot**，则防攻击策略应用到指定槽位的接口板上。

如果应用在接口板，防攻击策略只对上送接口板 CPU 的报文有效；如果应用在主控板，防攻击策略只对上送主控板 CPU 的报文有效。

说明

在防攻击策略中配置攻击溯源功能，在主控板上应用该防攻击策略时，攻击溯源功能才可以生效。

----结束

检查配置结果

- 执行命令 **display auto-defend attack-source**，查看主控板的攻击源信息。
- 执行命令 **display auto-defend configuration**，查看防攻击策略的攻击溯源配置信息。
- 执行命令 **display cpu-defend policy**，查看防攻击策略的信息。

9.4 配置 CPU 防攻击

配置 CPU 防攻击功能，可以限制上送 CPU 的报文，保护 CPU 的性能，保证 CPU 对正常业务的处理。

9.4.1 建立配置任务

在配置 CPU 防攻击前了解此特性的应用环境、配置此特性的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

当 AR1200 接入大量用户时，容易遭受针对 CPU 的报文攻击或需要处理大量上送 CPU 的报文。CPU 防攻击对上送 CPU 的报文进行限制和约束，使单位时间内上送 CPU 报文的数量限制在一定的范围之内，从而保护 CPU 的安全，保证 CPU 对正常业务的处理。

CPU 防攻击通过以下策略实现对 AR1200 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。

动态链路保护功能保护基于会话的应用层数据，包括 HTTP Session 数据、FTP Session 数据以及 BGP Session 数据，从而保证这些业务在攻击发生时可以正常运行。

前置任务

在配置 CPU 防攻击之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置防攻击策略之前，需要准备以下数据。

序号	数据
1	防攻击策略的名称
2	（可选）防攻击策略的描述信息
3	（可选）黑名单的 ACL 的规则及编号
4	（可选）上送 CPU 报文的限制速率
5	（可选）协议优先级
6	（可选）统一限速值
7	（可选）动态链路保护功能限速值
8	应用防攻击策略的接口板编号

9.4.2 创建防攻击策略

用户需要先创建防攻击策略，然后在创建的防攻击策略中配置 CPU 防攻击功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，创建防攻击策略并进入防攻击策略视图。

AR1200 最多支持 19 个防攻击策略。其中名称为 **default** 的策略为系统自动生成的缺省策略，**default** 策略默认应用到所有单板，不允许删除，也不允许修改参数；其余 18 个允许用户创建和删除。

步骤 3 （可选）执行命令 **description** *text*，配置防攻击策略的描述信息。

----结束

9.4.3 （可选）配置黑名单

黑名单指非法用户的集合，匹配黑名单特征的用户发送的报文将被设备丢弃。

背景信息

针对来自特定用户恶意报文的攻击，AR1200 通过 ACL 把符合特定特征的用户纳入到黑名单中，丢弃列入黑名单用户上送的报文。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **blacklist** *blacklist-id* **acl** *acl-number*，创建黑名单。

AR1200 的一个防攻击策略中最多可以配置 8 条黑名单。

黑名单应用的 ACL 可以是基本 ACL、高级 ACL 或二层 ACL。

缺省情况下，AR1200 中没有配置黑名单。

----结束

9.4.4 （可选）配置速率限制

AR1200 可以通过对不同类型的报文设置不同的限制速率，也可以对报文设置为丢弃，从而减少上送 CPU 的报文数量，降低不同类型报文的相互影响，达到保护 CPU 的目的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 配置速率限制。

- 执行命令 **packet-type** *packet-type* **rate-limit** *rate-value*，对上送 CPU 的报文进行限速，并设置速率阈值。超过此速率限制的报文将会被丢弃。
- 执行命令 **deny packet-type** *packet-type*，配置对上送 CPU 的报文进行丢弃。丢弃报文相当于将该类型报文的限速的阈值设置为 0。

缺省情况下，AR1200 对上送 CPU 的报文按照 **default** 策略缺省的限速值进行限速。

----结束

9.4.5 （可选）配置协议优先级

创建防攻击策略后，可以在防攻击策略中对上送 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。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **packet-type** *packet-type* **priority** *priority-level*，配置上送 CPU 报文的协议类型的优先级。

缺省情况下，使用 **default** 策略的缺省配置对上送 CPU 报文的协议类型区分优先级。

----结束

9.4.6 （可选）配置统一限速

创建防攻击策略后，可以在防攻击策略中配置对所有上送 CPU 的报文进行统一限速。AR1200 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。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **rate-limit all-packets pps** *pps-value*，配置对所有上送 CPU 的报文进行统一限速。

AR1200 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。

----结束

9.4.7 （可选）配置动态链路保护功能限制速率

用户可以在防攻击策略中配置动态链路保护功能的限制速率，以改变系统配置的缺省值。

背景信息

动态链路保护功能保护基于会话的应用层数据，包括 HTTP Session 数据、FTP Session 数据以及 BGP Session 数据，保证这些业务在攻击发生时可以正常运行。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **cpu-defend policy** *policy-name*，进入防攻击策略视图。

步骤 3 执行命令 **application-apperceive packet-type** { **bgp** | **ftp** | **http** } **rate-limit** *rate-value*，配置 HTTP 报文、BGP 报文或 FTP 报文的动态链路保护功能的限制速率。

说明

当 HTTP、FTP 或 BGP 协议连接建立时，如果用户没有配置 **application-apperceive** 的限制速率，那么 HTTP、FTP 或 BGP 协议报文使用 **application-apperceive** 命令缺省的限制速率上送。

缺省情况下，HTTP 报文的动态链路保护功能的限制速率是 512pps，FTP 报文的动态链路保护功能的限制速率是 1024pps，BGP 报文的动态链路保护功能的限制速率是 512pps。

----结束

9.4.8 应用防攻击策略

只有将防攻击策略应用在单板上后，防攻击策略才能生效。

前提条件

为了保护基于会话的应用层数据，包括 HTTP Session 数据、FTP Session 数据和 BGP Session 数据，保证这些业务在攻击发生时可以正常运行，可以在应用防攻击策略之前使能动态链路保护功能。

背景信息

防攻击策略可以在系统视图下应用到主控板或所有 LAN 接口板，也可以应用到指定 LAN 接口板。

说明

如果应用在 LAN 接口板，防攻击策略只对上送 LAN 接口板 CPU 的报文有效；如果应用在主控板，防攻击策略只对上送主控板 CPU 的报文有效。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 （可选）执行命令 **cpu-defend application-apperceive** [**bgp** | **ftp** | **http**] **enable**，使能动态链路保护功能。

说明

缺省情况下，对于 FTP 协议和 HTTP 协议，使能动态链路保护功能；对于 BGP 协议，不使能动态链路保护功能。

步骤 3 执行命令 **cpu-defend-policy** *policy-name* [**global** | **slot** *slot-id*]，应用防攻击策略。

执行此命令时，不带参数 **global** 和 **slot**，则防攻击策略应用到主控板；带参数 **global**，则防攻击策略应用到所有 LAN 接口板；带参数 **slot**，则防攻击策略应用到指定槽位的 LAN 接口板上。

----结束

9.4.9 检查配置结果

检查 CPU 防攻击的配置结果。

操作步骤

- 使用命令 **display cpu-defend policy** [*policy-name*]，查看防攻击策略信息。
- 使用命令 **display cpu-defend statistics** [**packet-type** *packet-type*]，查看上送 CPU 报文的统计信息。
- 使用命令 **display cpu-defend configuration** [**packet-type** *packet-type*] { **all** | **slot** *slot-id* | **sru** }，查看对上送 CPU 报文限速的配置信息。

----结束

9.5 维护防攻击策略

包括清除上送 CPU 报文统计信息、清除攻击源信息。

9.5.1 清除上送 CPU 报文的统计信息

介绍清除上送 CPU 报文的统计信息功能。

操作步骤

- 执行命令 **reset cpu-defend statistics** [**packet-type** *packet-type*]，清除上送 CPU 报文的统计信息。

----结束

9.5.2 清除攻击源信息

介绍清除攻击源信息功能。

操作步骤

- 执行命令 **reset auto-defend attack-source**，清除攻击源信息。

----结束

9.6 配置举例

介绍本地防攻击的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

9.6.1 配置本机防攻击示例

介绍本机防攻击的基本配置过程。

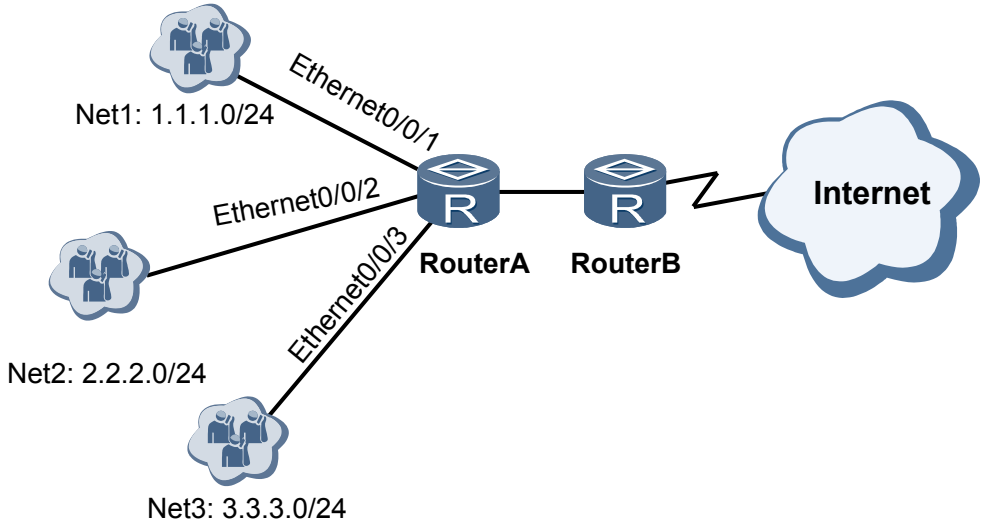
组网需求

如图 9-1 所示，位于不同局域网的用户通过 RouterA 访问 Internet。为分析 RouterA 受攻击情况，需要配置攻击溯源检查功能记录攻击源信息。管理员发现存在以下现象：

- 通过攻击溯源检查功能分析可知，Net1 网段中的某个用户经常会发生攻击行为。
- 攻击者发送大量的 ARP Request 报文，影响 CPU 的正常工作。
- 管理员需要以 FTP 方式上传文件到 RouterA，此时需要建立管理员主机与 RouterA 之间的数据连接。
- 大多数局域网用户通过 DHCP 方式动态获取 IP 地址，但 RouterA 不优先处理上送 CPU 的 DHCP Client 报文。
- RouterA 不应用 Telnet Server 功能，但经常收到大量的 Telnet 报文。

管理员希望通过在 RouterA 进行配置，以便解决上述问题。

图 9-1 配置防攻击策略组网图



配置思路

采用如下的思路配置本机防攻击：

1. 配置黑名单，将 Net1 网段中的攻击者列入黑名单，阻止其接入网络。
2. 配置 ARP Request 报文上送 CPU 的速率限制，使 ARP Request 报文限制在一个较小的速率范围内，减少对 CPU 处理正常业务的影响。
3. 配置 FTP 协议的动态链路保护功能，保证文件数据可以在管理员主机与 RouterA 之间正常传输。
4. 配置协议优先级，对 DHCP Client 报文设置较高的优先级，保证 RouterA 优先处理上送 CPU 的 DHCP Client 报文。
5. 配置 Telnet 的应用层联动功能，使 RouterA 丢弃收到的 Telnet 报文。

数据准备

为完成此配置举例，需要准备如下数据：

- 防攻击策略名称：devicesafety。
- 攻击溯源检查阈值：50pps。

- 攻击者的 MAC 地址：0001-c0a8-0102。
- ACL 规则的编号：4001。
- 黑名单的编号：1。
- ARP Request 报文上送 CPU 报文的速率限制值：64pps。
- FTP 协议动态链路保护功能速率限制值：2000pps。
- DHCP Client 报文的优先级：3。

说明

以下仅给出本机防攻击特性的配置步骤，关于路由的配置请参见《Huawei AR1200 系列企业路由器 配置指南-IP 路由》。

操作步骤

步骤 1 配置黑名单使用的 ACL

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] acl number 4001
[RouterA-acl-L2-4001] rule 5 permit source-mac 0001-c0a8-0102
[RouterA-acl-L2-4001] quit
```

步骤 2 创建防攻击策略

```
[RouterA] cpu-defend policy devicesafety
```

步骤 3 配置攻击溯源检查功能

```
[RouterA-cpu-defend-policy-devicesafety] auto-defend enable
[RouterA-cpu-defend-policy-devicesafety] auto-defend threshold 50
```

步骤 4 配置黑名单

```
[RouterA-cpu-defend-policy-devicesafety] blacklist 1 acl 4001
```

步骤 5 配置 ARP Request 报文上送 CPU 的速率限制

```
[RouterA-cpu-defend-policy-devicesafety] packet-type arp-request rate-limit 64
```

步骤 6 配置 FTP 协议动态链路保护功能的速率限制值

```
[RouterA-cpu-defend-policy-devicesafety] application-apperceive packet-type ftp rate-limit 2000
```

步骤 7 配置 DHCP Client 报文的优先级

```
[RouterA-cpu-defend-policy-devicesafety] packet-type dhcp-client priority 3
[RouterA-cpu-defend-policy-devicesafety] quit
```

步骤 8 应用防攻击策略

使能 FTP 协议动态链路保护功能

```
[RouterA] cpu-defend application-apperceive ftp enable
```

应用防攻击策略到主控板

```
[RouterA] cpu-defend-policy devicesafety
```

步骤 9 配置 Telnet 的应用层联动功能。

```
[RouterA] undo telnet server enable
```

步骤 10 验证配置结果

查看配置的防攻击策略的信息

```
[RouterA] display cpu-defend policy devicesafety
 Related slot : <0>
 BlackList Status :
```

```
  Slot<0> : Success
Configuration :
  Blacklist 1 ACL number : 4001
  Packet-type arp-request rate-limit : 64(pps)
  Packet-type dhcp-client priority : 3
  Rate-limit all-packets : 2000(pps)(default)
  Application-apperceive packet-type ftp : 2000(pps)
  Application-apperceive packet-type tftp : 2000(pps)
```

查看主控板上配置的限速信息，显示结果表明，Telnet 的应用层联动、对 arp-request 报文的限制速率和 dhcp-client 报文优先级的配置成功。

```
<Huawei> display cpu-defend configuration sru
Rate configurations on main board.
-------------------------------------------------------------------
Packet-type             Status        Rate-limit(PPS)  Priority
-------------------------------------------------------------------
8021X                    Disabled          160              2
arp-miss                 Enabled            64             2
arp-reply                Enabled           128             2
arp-request              Enabled            64             2
bfd                      Disabled          512             4
bgp                      Enabled           256             3
bgp4plus                 Enabled           256             3
dhcp-client              Enabled           128             3
dhcp-server              Enabled           128             2
dhcpv6-reply             Enabled           128             2
dhcpv6-request           Enabled           128             2
dlsw                     Enabled          4096             2
dns                      Enabled           256             2
fib-hit                  Enabled           256             2
fr                       Enabled           128             3
ftp-client               Disabled          256             2
ftp-server               Enabled           256             2
fw-dns                   Enabled           128             2
fw-ftp                   Enabled           128             2
fw-http                  Enabled           128             2
fw-rtsp                  Enabled           128             2
fw-sip                   Enabled           128             2
gre-keepalive            Enabled           128             3
gvrp                     Enabled            48             3
hdlc                     Enabled           128             3
http-client              Enabled           256             4
http-server              Enabled           256             4
hw-tacacs                Enabled           128             2
icmp                     Enabled           256             2
icmpv6                   Enabled           256             2
igmp                     Enabled           256             2
ip-option                Enabled           256             2
ipsec-ike                Enabled           128             2
ipsec-isa                Enabled           128             2
ipsec-osa                Enabled           128             2
isis                     Enabled           256             3
isisv6                   Enabled           256             3
l2tp                     Enabled           256             2
lacp                     Enabled           320             3
lldp                     Enabled            48             3
nd                       Enabled           128             5
nd-miss                  Enabled            64             5
nhrp                     Enabled           256             3
ntp                      Enabled           128             4
ospf                     Enabled           256             3
ospfv3                   Enabled           256             3
pim                      Disabled          256             3
ppp                      Enabled           512             2
pppoe                    Enabled           512             2
radius                   Enabled           128             2
rip                      Enabled           128             3
ripng                    Enabled           256             3
snmp                     Enabled           256             4
```

```
ssh-client                Enabled          128            4
ssh-server                Enabled          128            4
sslvpn                    Enabled         4096            3
stp                       Enabled           96            3
tcp                       Enabled          128            2
telnet-client             Enabled          128            4
telnet-server             Enabled          128            4
ttl-expired               Enabled          256            1
udp-helper                Disabled          32            2
unknown-multicast         Enabled          128            1
unknown-packet            Enabled          256            1
voice                     Enabled          256            4
vrrp                      Disabled         256            3
------------------------------------------------------------------
```

配置攻击溯源检查功能后，对 Net1 网段中的攻击者进行溯源的日志信息显示，攻击溯源检查功能生效。

```
Dec 18 2010 09:55:50-05:13 AR1200 %%01SECE/4/USER_ATTACK(l)[0]:User attack
occurred.(Slot=MPU, SourceAttackInterface=Ethernet0/0/1, OuterVlan/
InnerVlan=0/0, UserMacAddress=0001-c0a8-0102, AttackPackets=48 packets per
second)
```

查看上送到主控板的报文的统计信息，丢弃的报文表明设备对 arp-request 进行了速率限制。

```
<Huawei> display cpu-defend statistics
------------------------------------------------------------------------
Packet Type                Pass Packets        Drop Packets
------------------------------------------------------------------------
8021X                                 0                   0
arp-miss                              5                   0
arp-reply                          8090                   0
arp-request                     1446576              127773
bfd                                   0                   0
bgp                                   0                   0
bgp4plus                              0                   0
dhcp-client                         879                   0
dhcp-server                           0                   0
dhcpv6-reply                          0                   0
dhcpv6-request                        0                   0
dns                                   4                   0
fib-hit                               0                   0
fr                                    0                   0
ftp-client                            0                   0
ftp-server                            0                   0
fw-dns                                0                   0
fw-ftp                                0                   0
fw-http                               0                   0
fw-rtsp                               0                   0
fw-sip                                0                   0
gre-keepalive                         0                   0
gvrp                                  0                   0
hdlc                                  0                   0
http-client                           0                   0
http-server                           0                   0
hw-tacacs                             0                   0
icmp                                 59                   0
icmpv6                              224                   0
igmp                                539                   0
ip-option                             0                   0
ipsec-ike                             0                   0
ipsec-isa                             0                   0
ipsec-osa                             0                   0
isis                              70252                   0
isisv6                                0                   0
l2tp                                  0                   0
lacp                                  0                   0
lldp                                  0                   0
```

```
nd                                  358                 0
nd-miss                               0                 0
nhrp                                  0                 0
ntp                                   0                 0
ospf                                  0                 0
ospfv3                                0                 0
pim                                   0                 0
ppp                                   0                 0
pppoe                                 0                 0
radius                                0                 0
rip                               11306                 0
ripng                              7385                 0
snmp                                  0                 0
ssh-client                            0                 0
ssh-server                            0                 0
sslvpn                                0                 0
stp                                   0                 0
tcp                                  15                 0
telnet-client                     81476                 0
telnet-server                         0                 0
ttl-expired                           0                 0
udp-helper                            0                 0
unknown-multicast                     0                 0
unknown-packet                    66146                 0
voice                                 0                 0
vrrp                                  0                 0
------------------------------------------------------------------------------
```

----结束

配置文件

```
#
sysname RouterA
#
acl number 4001
 rule 5 permit source-mac 0001-c0a8-0102
#
cpu-defend policy devicesafety
 blacklist 1 acl 4001
 packet-type arp-request rate-limit 64
 packet-type dhcp-client priority 3
 application-apperceive packet-type ftp rate-limit 2000
 auto-defend enable
 auto-defend threshold 50
 auto-defend trace-type source-mac source-ip source-portvlan
 auto-defend protocol all
#
 cpu-defend-policy devicesafety
#
 undo telnet server enable
#
return
```

10 ACL 配置

关于本章

AR1200 为了过滤报文，需要配置一系列的规则，以决定什么样的报文能够通过，这些规则就是通过访问控制列表 ACL（Access Control List）定义的。

10.1 ACL 概述
介绍 ACL 基本概念。

10.2 AR1200 支持的 ACL 特性

10.3 配置基本 ACL
当用户仅需要根据源 IP 地址、分片标记或时间段等信息对 IPv4 报文进行过滤时，可以使用基本 ACL。

10.4 配置高级 ACL
当用户需要使用源 IP 地址、目的 IP 地址、源端口号、目的端口号、优先级、时间段等信息对 IPv4 报文进行过滤时，可以使用高级 ACL。

10.5 配置二层 ACL
当用户需要使用源 MAC 地址、目的 MAC 地址、MAC 承载的协议类型等信息对二层报文（以太协议类型为 Ethernet_II）进行过滤时，可以使用二层 ACL。

10.6 配置举例
介绍 ACL 的配置举例。配置示例中包括组网需求、配置思路、操作步骤等。

10.1 ACL 概述

介绍 ACL 基本概念。

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规则的集合，它通过匹配报文的信息实现对报文的分类。AR1200 根据 ACL 定义的规则判断哪些报文可以接收，哪些报文需要拒绝，从而实现对报文的过滤。

ACL 可以应用在 AR1200 的一些业务和功能中，比如路由策略、流分类、防火墙、IPSec 等。

说明

ACL 本身只是一组规则，只能区分某一类报文，无法实现过滤报文的功能。对这类报文的处理方法，需要由引用 ACL 的具体功能来决定。

10.2 AR1200 支持的 ACL 特性

AR1200 支持的 ACL 分类

根据不同的划分规则，AR1200 支持的 ACL 可以有不同的类型，如表 10-1 所示。

表 10-1 ACL 分类

划分规则	分类	功能介绍	说明
根据定义规则的信息	基本 ACL	基本 ACL 根据报文的源 IP 地址、分片标记和时间段等信息定义规则。	编号范围为 2000 ～ 2999。
	高级 ACL	高级 ACL 根据报文的源 IP 地址、目的 IP 地址、源端口号、目的端口号、优先级、时间段等信息定义规则。	编号范围为 3000 ～ 3999。
	二层 ACL	二层 ACL 根据报文的源 MAC 地址、目的 MAC 地址、MAC 承载的协议类型等信息定义规则。	编号范围为 4000 ～ 4999。
按照命名方式	编号型 ACL	传统的 ACL 标识方法。用户在创建 ACL 时，可以为该 ACL 指定一个唯一的编号，后续可以通过这个唯一的编号对该 ACL 进行相关操作。	-

划分规则	分类	功能介绍	说明
	命名型 ACL	名称相对编号更为直观，具备较好的记忆效果。用户在创建 ACL 时，可以为该 ACL 指定一个唯一的名称，后续可以通过这个唯一的名称对该 ACL 进行相关操作。	AR1200 提供了灵活的 ACL 命名方式：在配置命名型 ACL 的同时，也可以同时为该命名型 ACL 指定编号。如果用户没有为该命名型 ACL 指定编号，则系统会自动分配一个编号给该命名型 ACL。

基本 ACL、高级 ACL 和二层 ACL 支持的定义规则的信息如**表 10-2** 所示。其中，高级 ACL 根据 IP 版本信息和 IP 承载的协议类型（gre、igmp、ipinip、ospf、tcp、udp、icmp）可以进一步细分。

表 10-2 不同类型的 ACL 定义规则的信息

定义规则的信息		基本 ACL	高级 ACL					二层 ACL
			ip	gre、igmp、ipinip、ospf	tcp	udp	icmp	
三层报文信息	源 IP 地址	Yes	Yes	Yes	Yes	Yes	Yes	No
	目的 IP 地址	No	Yes	Yes	Yes	Yes	Yes	No
	区分服务代码点	No	Yes	Yes	Yes	Yes	Yes	No
	优先级	No	Yes	Yes	Yes	Yes	Yes	No
	分片标记	Yes	Yes	Yes	Yes	Yes	Yes	No
	服务类型	No	Yes	Yes	Yes	Yes	Yes	No
	ICMP 报文的类型和消息码	No	No	No	No	No	Yes	No
四层报文	源端口号	No	No	No	Yes	Yes	No	No

定义规则的信息		基本ACL	高级 ACL					二层 ACL
			ip	gre、igmp、ipinip、ospf	tcp	udp	icmp	
信息	目的端口号	No	No	No	Yes	Yes	No	No
	SYN Flag 类型	No	No	No	Yes	No	No	No
二层报文信息	源 MAC 地址	No	No	No	No	No	No	Yes
	目的 MAC 地址	No	No	No	No	No	No	Yes
	MAC 承载的协议类型	No	No	No	No	No	No	Yes
	VLAN 编号	No	No	No	No	No	No	Yes
	802.1p 优先级	No	No	No	No	No	No	Yes
其他信息	时间段	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	VPN 实例	Yes	Yes	Yes	Yes	Yes	Yes	No

AR1200 支持的其他 ACL 特性

AR1200 支持配置 ACL 步长、ACL 描述信息以及 ACL 规则的描述信息。

- 通过设置 ACL 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。
- ACL 的描述信息可以描述 ACL 的用途或使用场景，方便用户区分或识别不同的 ACL。
- ACL 规则的描述信息用来描述 ACL 规则的用途或使用场景，方便用户区分或识别 ACL 的不同规则。
- 通过配置时间段，可以在 ACL 规则中引用已配置的时间段信息，限制规则生效的时间范围。引用 ACL 的业务或功能需要限制在一定的时间范围内启动，比如，在流量高峰期时启动设备的 QoS 功能。用户可以为 ACL 创建生效时间段，通过在规

则中引用时间段信息限制 ACL 生效的时间范围，从而实现该业务或功能在一定的时间范围内启动的目的。

说明

设备的固定 LAN 接口上，配置的 ACL 对 LAN 到 LAN 的二层流量不生效

10.3 配置基本 ACL

当用户仅需要根据源 IP 地址、分片标记或时间段等信息对 IPv4 报文进行过滤时，可以使用基本 ACL。

10.3.1 建立配置任务

在配置基本 ACL 前了解此特性的应用环境以及配置的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

基本 ACL 可以用于很多业务和功能，比如路由策略、流分类等。AR1200 通过基本 ACL 定义的规则对不同类别的报文进行不同的处理。

基本 ACL 的作用对象是网络层及其上层的所有 IPv4 报文。针对这些报文，基本 ACL 根据报文自身的源 IP 地址、分片标记信息，以及时间段、VPN 实例信息对报文进行分类。

前置任务

在基本 ACL 之前，需要完成以下任务：

- 配置接口的链路层协议参数，使接口的链路层协议状态为 Up。

数据准备

在配置基本 ACL 之前，需准备以下数据。

序号	数据
1	（可选）生效时间段名称以及生效时间
2	基本 ACL 的编号或名称
3	源 IP 地址、分片标记或 VPN 实例信息
4	（可选）基本 ACL 的描述内容
5	（可选）基本 ACL 规则的描述内容
6	（可选）基本 ACL 的步长

10.3.2 （可选）创建基本 ACL 的生效时间段

用户可以为基本 ACL 创建生效时间段，通过在规则中引用时间段信息限制该规则生效的时间范围。如果配置规则时不指定时间段，则该规则不受时间范围限制，除非删除该规则或删除该 ACL。

背景信息

某些引用基本 ACL 的业务或功能需要限制在一定的时间范围内生效，比如，在流量高峰期时启动设备的 QoS 功能。用户可以为基本 ACL 创建生效时间段，通过在规则中引用时间段信息限制基本 ACL 生效的时间范围，从而实现该业务或功能在一定的时间范围内生效的目的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **time-range** *time-name* { *start-time* **to** *end-time days* | **from** *time1 date1* [**to** *time2 date2*] }，创建一个时间段。

AR1200 支持具有相同 *time-name* 的多个时间段共同描述某个时间范围，此时可以使用相同的 *time-name* 反复执行本步骤。

说明

可以为多个时间段范围配置相同的 *time-name*，共同来描述某个特殊时间。例如：时间段“test”配置了三个生效时段

- 从 2010 年 1 月 1 日 00:00 起到 2010 年 12 月 31 日 23:59 生效，这是一个绝对时间段。
- 在周一到周五每天 8:00 到 18:00 生效，这是一个周期时间段。
- 在周六、周日下午 14:00 到 18:00 生效，这是一个周期时间段。

则时间段“test”最终描述的时间范围为：2010 年的周一到周五每天 8:00 到 18:00 以及周六和周日下午 14:00 到 18:00。

----结束

后续处理

在配置基本 ACL 规则时，用户可以通过参数 **time-range** 在规则中引用已配置的时间段信息，限制规则生效的时间范围。

10.3.3 创建基本 ACL

使用基本 ACL 前，必须先创建基本 ACL。用户可以使用编号或名称来创建基本 ACL。

前提条件

使用 **display acl all** 命令查看所有已配置的 ACL，避免重复配置基本 ACL。

操作步骤

- 使用编号创建基本 ACL。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号创建一个基本 ACL，并进入基本 ACL 视图。

基本 ACL 编号 *acl-number* 的范围是 2000 ～ 2999。

match-order 指定了基本 ACL 规则的匹配顺序。

- **auto** 表示匹配规则时系统自动排序（按“深度优先”的顺序）。
- **config** 表示匹配规则时按用户的配置顺序。

3. （可选）执行命令 **description** *text*，配置基本 ACL 描述信息。

   ACL 的描述信息可以描述 ACL 的用途或使用场景，方便用户区分或识别不同的 ACL。

   缺省情况下，不配置 ACL 描述信息。

- 使用名称创建基本 ACL。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl name** *acl-name* { **basic** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个基本 ACL，进入基本 ACL 视图。

     基本 ACL 编号 *acl-number* 的范围是 2000 ～ 2999。

     match-order 指定了基本 ACL 规则的匹配顺序。

     - **auto** 表示匹配规则时系统自动排序（按“深度优先”的顺序）。
     - **config** 表示匹配规则时按用户的配置顺序。

  3. （可选）执行命令 **description** *text*，配置基本 ACL 描述信息。

     ACL 的描述信息可以描述 ACL 的用途或使用场景，方便用户区分或识别不同的 ACL。

     缺省情况下，不配置 ACL 描述信息。

----结束

后续处理

在基本 ACL 视图下配置该 ACL 的规则。

10.3.4 配置基本 ACL 的规则

基本 ACL 是一系列有顺序规则的集合，通过规则来匹配报文的信息，实现对报文的分类。

前提条件

已经创建基本 ACL 并进入基本 ACL 视图。

使用命令 **display acl** { *acl-number* | **name** *acl-name* }命令查看该 ACL 已配置的所有规则，避免新规则覆盖已配置的规则。

背景信息

基本 ACL 通过规则匹配报文的信息，从而实现对报文的分类，因此创建基本 ACL 以后，需要配置基本 ACL 的规则。

以下操作是在基本 ACL 视图下进行的。

操作步骤

步骤 1 （可选）执行命令 **step** *step-value*，配置 ACL 步长。

缺省情况下，基本 ACL 步长值为 5。

步骤 2 执行命令 **rule** { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**fragment** | **none-first-fragment**]] *，配置基本 ACL 的规则。

如果基本 ACL 需要配置多个规则，可以反复执行本步骤。

说明

本步骤中，**rule** 命令没有选择参数 *rule-id*，这种情况下，步长值作为规则的起始编号，并作为步长间隔。

配置规则时，如果不同的规则之间存在矛盾或包含的关系，请注意规则的匹配顺序，防止出现错误配置。

步骤 3 （可选）执行 **rule** *rule-id* **description** *text*，配置基本 ACL 规则的描述信息。

基本 ACL 规则的描述信息用来描述 ACL 规则的用途或使用场景，方便用户区分或识别 ACL 的不同规则。

----结束

后续处理

配置基本 ACL 规则后，通常有以下的后续处理步骤：

- 用户需要调整规则的步长时，可以执行 **step** 命令，重新设置步长值。
- 当匹配方式为 config 时，用户需要在规则之间插入新的规则，可以执行 **rule** 命令并选择参数 *rule-id*。

10.3.5 应用基本 ACL

基本 ACL 可以应用在某些业务或功能中，实现对报文的过滤。

前提条件

已经创建基本 ACL，并完成基本 ACL 规则的配置。

背景信息

基本 ACL 可以应用在以下业务和功能：

- 流分类
- 本机防攻击特性中的黑名单功能
- 路由过滤
- OSPF 特性中对发送的 LSA 进行过滤功能
- IP 组播
- 限制对 FTP 或 TFTP 服务器访问
- 防火墙
- NAT

- 在接口上根据 ACL 对报文流进行过滤

操作步骤

- 流分类

  对于进入设备的各种流量，可以根据报文的信息对不同的业务提供差别服务，此时需要配置流分类。AR1200 支持基于基本 ACL 定义流分类中的匹配规则。参见配置流分类。

- 本机防攻击特性中的黑名单功能

  黑名单指非法用户的集合，通过基本 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 AR1200 后均会被丢弃。参见**配置黑名单**。

- 路由过滤

  对于 RIP、OSPF、IS-IS、BGP 或 MBGP 协议，可以配置路由过滤功能，对这些协议的路由信息设置过滤条件，没有通过过滤的路由不会被添加进路由表，也不会对外发布出去。AR1200 支持使用基本 ACL 设置过滤条件，实现路由过滤功能。参见 IP 路由配置。

- OSPF 特性中对发送的 LSA 进行过滤功能

  某些特殊的网络环境中，需要配置 OSPF 的一些特性功能，并需要对 OSPF 网络的性能进行调整和优化。当两台路由器之间存在多条链路时，通过对出方向的 LSA 进行过滤可以在某些链路上过滤 LSA 的传送，减少不必要的重传，节省带宽资源。AR1200 支持使用基本 ACL 对出方向的 LSA 进行过滤。参见调整优化 OSPF 网络。

- IP 组播

  组播业务中的 IGMP 协议、PIM-SM 协议或 PIM-DM 协议的配置，部分功能需要使用基本 ACL。参见组播配置。

- 限制对 FTP 或 TFTP 服务器访问

  当路由器作为 FTP 或 TFTP 服务器时，为提高安全性，可以通过配置基本 ACL 实现只允许满足匹配条件的客户端访问服务器。参见（可选）配置 FTP 访问控制。

- 防火墙

  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，用防火墙作为这个网络边防产品。其中，包过滤防火墙通过配置 ACL 实施数据包的过滤。AR1200 支持通过基本 ACL 配置包过滤防火墙。参见**配置包过滤防火墙**。

- NAT

  NAT（Network Address Translation）又称为网络地址转换，用于实现私有网络和公有网络之间的互访。NAT 地址池是一组公网 IP 地址集合，当内部数据包通过地址转换到达外部网络时，将会选择 NAT 地址池中的某个公网地址作为转换后的源地址。AR1200 支持使用基本 ACL 对 NAT 地址池中的 IP 地址进行分类，将匹配基本 ACL 规则的数据报文的源地址进行地址转换。参见配置 ACL 和地址池关联。

- 在接口上根据 ACL 对报文流进行过滤

  AR1200 支持在接口上根据 ACL 对报文流进行过滤。这样，AR1200 将会过滤符合 ACL 规则的报文：

  - 当报文命中的规则的动作为 **deny**，则直接丢掉该报文。

- 当报文命中的规则的动作为 **permit**，则允许该报文通过。

下面介绍在接口上根据 ACL 对报文流进行过滤的配置步骤。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **traffic-filter** { **inbound** | **outbound** } **acl** { *acl-number* | **name** *acl-name* }，配置根据 ACL 对报文流进行过滤。

----结束

10.3.6 检查配置结果

基本 ACL 配置完成以后，查看基本 ACL 规则和时间段信息。

前提条件

已经完成了基本 ACL 的配置。

操作步骤

- 执行命令 **display acl** *acl-number*，查看以编号创建的基本 ACL 规则。
- 执行命令 **display acl name** *acl-name*，查看以名称创建的基本 ACL 规则。
- 执行命令 **display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

任务示例

执行命令 **display acl** *acl-number*，可以看到基本 ACL 的编号、规则数量、步长和规则的具体内容。

```
<Huawei> display acl 2009
Basic ACL 2009, 1 rule
Acl's step is 5
 rule 5 deny source 10.1.1.1 0
```

执行命令 **display acl name** *acl-name*，可以看到基本 ACL 的名称、编号、规则数量、步长和规则的具体内容。

```
<Huawei> display acl name qos1
Basic ACL qos1 2999, 1 rule
Acl's step is 5
 rule 5 permit source 202.114.24.56 0.0.0.255
```

执行命令 **display time-range all**，可以看到当前时间段的配置和状态。

```
<Huawei> display time-range all
Current time is 09:13:37 12-27-2010 Thursday

Time-range : test1 ( Inactive )
 13:00 to 18:00 working-day
 13:00 to 18:00 off-day
```

10.4 配置高级 ACL

当用户需要使用源 IP 地址、目的 IP 地址、源端口号、目的端口号、优先级、时间段等信息对 IPv4 报文进行过滤时，可以使用高级 ACL。

10.4.1 建立配置任务

在配置高级 ACL 前了解此特性的应用环境以及配置的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

高级 ACL 可以用于很多业务和功能，比如流分类、组播等。AR1200 通过高级 ACL 定义的规则对不同类别的报文进行不同的处理。

高级 ACL 的作用对象分为两种情况：

- 高级 ACL 作用对象为网络层及其上层的所有 IPv4 报文。针对这些报文，高级 ACL 根据报文自身的源 IP 地址、目的 IP 地址、优先级、分片标记等信息，以及时间段、VPN 实例信息对 IPv4 报文进行分类。

  说明

  这种情况下，高级 ACL 和基本 ACL 类似，只是提供了比基本 ACL 更为丰富的限制信息。

- 高级 ACL 作用对象为特定的某种报文，包括：GRE 报文、IGMP 报文、IPinIP 报文、OSPF 报文、ICMP 报文、UDP 报文和 TCP 报文。
  - 针对 GRE 报文、IGMP 报文、IPinIP 报文和 OSPF 报文，高级 ACL 根据报文自身的源 IP 地址、目的 IP 地址、优先级、分片标记等信息，以及时间段、VPN 实例信息对该种类型的报文进行分类。
  - 针对 ICMP 报文，高级 ACL 根据报文自身的源 IP 地址、目的 IP 地址、优先级、分片标记、ICMP 报文的类型和消息码等信息，以及时间段、VPN 实例信息对 ICMP 报文进行分类。
  - 针对 UDP 报文，高级 ACL 根据报文自身的源 IP 地址、目的 IP 地址、源端口号、目的端口号、优先级、分片标记等信息，以及时间段、VPN 实例信息对 UDP 报文进行分类。
  - 针对 TCP 报文，高级 ACL 根据报文自身的源 IP 地址、目的 IP 地址、源端口号、目的端口号、SYN Flag 类型、优先级、分片标记等信息，以及时间段、VPN 实例信息对 TCP 报文进行分类。

前置任务

在高级 ACL 之前，需要完成以下任务：

- 配置接口的链路层协议参数，使接口的链路层协议状态为 Up。

数据准备

在配置高级 ACL 之前，需准备以下数据。

序号	数据
1	（可选）生效时间段名称以及生效时间
2	高级 ACL 的编号或名称
3	协议类型
4	源 IP 地址及端口、目的 IP 地址及端口、源 IP 地址是否分片、ICMP 类型和编码、优先级、tos 值和生效时间等
5	（可选）高级 ACL 的描述内容
6	（可选）高级 ACL 的规则的描述内容
7	（可选）高级 ACL 的步长

10.4.2 （可选）创建高级 ACL 生效时间段

用户可以为基本 ACL 创建生效时间段，通过在规则中引用时间段信息限制该规则生效的时间范围。如果配置规则时不指定时间段，则该规则不受时间范围限制，除非删除该规则或删除该 ACL。

背景信息

某些引用高级 ACL 的业务或功能需要限制在一定的时间范围内生效，比如，在流量高峰期时启动设备的 QoS 功能。用户可以为高级 ACL 创建生效时间段，通过在规则中引用时间段信息限制高级 ACL 生效的时间范围，从而实现该业务或功能在一定的时间范围内生效的目的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **time-range** *time-name* { *start-time* **to** *end-time days* | **from** *time1 date1* [**to** *time2 date2*] }，创建一个时间段。

AR1200 支持具有相同 *time-name* 的多个时间段共同描述某个时间范围，此时可以使用相同的 *time-name* 反复执行本步骤。

说明

可以为多个时间段范围配置相同的 *time-name*，共同来描述某个特殊时间。例如：时间段“test”配置了三个生效时段

- 从 2010 年 1 月 1 日 00:00 起到 2010 年 12 月 31 日 23:59 生效，这是一个绝对时间段。
- 在周一到周五每天 8:00 到 18:00 生效，这是一个周期时间段。
- 在周六、周日下午 14:00 到 18:00 生效，这是一个周期时间段。

则时间段“test”最终描述的时间范围为：2010 年的周一到周五每天 8:00 到 18:00 以及周六和周日下午 14:00 到 18:00。

----结束

后续处理

在配置高级 ACL 规则时，用户可以通过参数 **time-range** 在规则中引用已配置的时间段信息，限制规则生效的时间范围。

10.4.3 创建高级 ACL

使用高级 ACL 前，必须先创建高级 ACL。用户可以使用编号或名称来创建高级 ACL。

前提条件

使用 **display acl all** 命令查看所有已配置的 ACL，避免重复配置高级 ACL。

操作步骤

- 使用编号创建高级 ACL。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号创建一个高级 ACL，并进入高级 ACL 视图。

     高级 ACL 编号 *acl-number* 的范围是 3000 ～ 3999。

     match-order 指定了高级 ACL 规则的匹配顺序。

     - **auto** 表示匹配规则时系统自动排序（按“深度优先”的顺序）。
     - **config** 表示匹配规则时按用户的配置顺序。
  3. （可选）执行命令 **description** *text*，配置高级 ACL 描述信息。

     ACL 的描述信息可以描述 ACL 的用途或使用场景，方便用户区分或识别不同的 ACL。

     缺省情况下，不配置 ACL 描述信息。
- 使用名称创建高级 ACL。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl name** *acl-name* [**advance** | *acl-number*] [**match-order** { **auto** | **config** }]，使用名称创建一个高级 ACL，进入高级 ACL 视图。

     高级 ACL 编号 *acl-number* 的范围是 3000 ～ 3999。

     match-order 指定了高级 ACL 规则的匹配顺序。

     - **auto** 表示匹配规则时系统自动排序（按“深度优先”的顺序）。
     - **config** 表示匹配规则时按用户的配置顺序。
  3. （可选）执行命令 **description** *text*，配置高级 ACL 描述信息。

     ACL 的描述信息可以描述 ACL 的用途或使用场景，方便用户区分或识别不同的 ACL。

     缺省情况下，不配置 ACL 描述信息。

----结束

后续处理

在高级 ACL 视图下配置该 ACL 的规则。

10.4.4 配置高级 ACL 的规则

高级 ACL 是一系列有顺序规则的集合，通过规则来匹配报文的信息，实现对报文的分类。

前提条件

已经创建高级 ACL 并进入高级 ACL 视图。

使用命令 **display acl** { *acl-number* | **name** *acl-name* }命令查看该 ACL 已配置的所有规则，避免新规则覆盖已配置的规则。

背景信息

高级 ACL 通过规则匹配报文的信息，从而实现对报文的分类，因此创建高级 ACL 以后，需要配置高级 ACL 的规则。

以下操作是在高级 ACL 视图下进行的。

操作步骤

步骤 1 （可选）执行命令 **step** *step-value*，配置 ACL 步长。

缺省情况下，高级 ACL 步长值为 5。

步骤 2 根据报文的 IP 协议版本或 IP 承载的协议类型配置高级 ACL 规则。

- 根据 IP 协议版本配置高级 ACL 规则。当 IP 协议版本为 IPv4 时，高级访问控制列表的命令格式为：

  rule { **deny** | **permit** } **ip** [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**]] *

- 根据报文中 IP 承载的协议类型配置高级 ACL 规则。
  - 当 IP 承载的协议类型为 ICMP 时，高级访问控制列表的命令格式为：

    rule { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**]] *

  - 当 IP 承载的协议类型为 TCP 时，高级访问控制列表的命令格式为：

    rule { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** | **gt** | **lt** | **range** } *port* | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** | **gt** | **lt** | **range** } *port* | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**]] *

  - 当 IP 承载的协议类型为 UDP 时，高级访问控制列表的命令格式为：

    rule { **deny** | **permit** }{ *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** | **gt** | **lt** | **range** } *port* | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** | **gt** | **lt** | **range** } *port* | **time-**

range *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**]] *

- 当 IP 承载的协议类型为 GRE、IGMP、IPINIP、OSPF 时，高级访问控制列表的命令格式为：

  rule { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**]] *

如果高级 ACL 需要配置多个规则，可以反复执行本步骤。

说明

本步骤中，**rule** 命令没有选择参数 *rule-id*，这种情况下，步长值作为规则的起始编号，并作为步长间隔。

配置规则时，如果不同的规则之间存在矛盾或包含的关系，请注意规则的匹配顺序，防止出现错误配置。

步骤 3 （可选）执行 **rule** *rule-id* **description** *text*，配置高级 ACL 规则的描述信息。

高级 ACL 规则的描述信息用来描述 ACL 规则的用途或使用场景，方便用户区分或识别 ACL 的不同规则。

----结束

后续处理

配置高级 ACL 规则后，通常有以下的后续处理步骤：

- 用户需要调整规则的步长时，可以执行 **step** 命令，重新设置步长值。
- 当匹配方式为 config 时，用户需要在规则之间插入新的规则，可以执行 **rule** 命令并选择参数 *rule-id*。

10.4.5 应用高级 ACL

高级 ACL 可以应用在某些业务或功能中，实现对报文的过滤。

前提条件

已经创建高级 ACL，并完成高级 ACL 规则的配置。

背景信息

高级 ACL 可以应用在以下业务和功能：

- 流分类
- 本机防攻击特性中的黑名单功能
- IP 组播
- IPSec
- 防火墙
- NAT
- 在接口上根据 ACL 对报文流进行过滤

操作步骤

- 流分类

  对于进入设备的各种流量，可以根据报文的信息对不同的业务提供差别服务，此时需要配置流分类。AR1200 支持基于高级 ACL 定义流分类中的匹配规则。参见配置流分类。

- 本机防攻击特性中的黑名单功能

  黑名单指非法用户的集合，通过高级 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 AR1200 后均会被丢弃。参见**配置黑名单**。

- IP 组播

  组播业务中的 IGMP 协议、PIM-SM 协议或 PIM-DM 协议的配置，部分功能需要使用高级 ACL。参见组播配置。

- IPSec

  IPSec 协议族是 IETF（Internet Engineering Task Force）制定的一系列协议，它为 IP 数据报提供了高质量的、可互操作的、基于密码学的安全性。通过 IPSec，对等体之间（指 IPSec 对等体）能够对不同的数据流实施不同的安全保护（认证、加密或两者同时使用）。AR1200 支持通过配置高级 ACL 来区分数据流，从而定义被保护的数据流。参见 IPSec 配置

- 防火墙

  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，用防火墙作为这个网络边防产品。其中，包过滤防火墙通过配置 ACL 实施数据包的过滤。AR1200 支持通过高级 ACL 配置包过滤防火墙。参见**配置包过滤防火墙**。

- NAT

  NAT（Network Address Translation）又称为网络地址转换，用于实现私有网络和公有网络之间的互访。NAT 地址池是一组公网 IP 地址集合，当内部数据包通过地址转换到达外部网络时，将会选择 NAT 地址池中的某个公网地址作为转换后的源地址。AR1200 支持使用高级 ACL 对 NAT 地址池中的 IP 地址进行分类，将匹配高级 ACL 规则的数据报文的源地址进行地址转换。参见配置 ACL 和地址池关联。

- 在接口上根据 ACL 对报文流进行过滤

  AR1200 支持在接口上根据 ACL 对报文流进行过滤。这样，AR1200 将会过滤匹配 ACL 规则的报文：

  - 当报文命中的规则的动作为 **deny**，则直接丢掉该报文。
  - 当报文命中的规则的动作为 **permit**，则允许该报文通过。

  下面介绍在接口上根据 ACL 对报文流进行过滤的配置步骤。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
  3. 执行命令 **traffic-filter** { **inbound** | **outbound** } **acl** { *acl-number* | **name** *acl-name* }，配置根据 ACL 对报文流进行过滤。

----结束

10.4.6 检查配置结果

高级 ACL 配置完成以后，查看高级 ACL 规则和时间段信息。

前提条件

已经完成了高级 ACL 的配置。

操作步骤

- 执行命令 **display acl** *acl-number*，查看以编号创建的高级 ACL 规则。
- 执行命令 **display acl name** *acl-name*，查看以名称创建的高级 ACL 规则。
- 执行命令 **display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

任务示例

执行命令 **display acl** *acl-number*，可以看到高级 ACL 的编号、规则数量、步长和规则的具体内容。

```
<Huawei> display acl 3000
Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.1.1.1 0
```

执行命令 **display acl name** *acl-name*，可以看到高级 ACL 的名称、编号、规则数量、步长和规则的具体内容。

```
<Huawei> display acl name qos1
Advanced ACL qos1 3999, 1 rule
Acl's step is 5
 rule 5 permit tcp
```

执行命令 **display time-range all**，可以看到当前时间段的配置和状态。

```
<Huawei> display time-range all
Current time is 09:13:37 12-27-2010 Thursday

Time-range : test1 ( Inactive )
 13:00 to 18:00 working-day
 13:00 to 18:00 off-day
```

10.5 配置二层 ACL

当用户需要使用源 MAC 地址、目的 MAC 地址、MAC 承载的协议类型等信息对二层报文（以太协议类型为 Ethernet_II）进行过滤时，可以使用二层 ACL。

10.5.1 建立配置任务

在配置二层 ACL 前了解此特性的应用环境以及配置的前置任务和数据准备，可以更快速、准确地完成配置任务。

应用环境

二层 ACL 可以用于很多业务中，比如流分类。AR1200 通过二层 ACL 定义的规则对不同类别的报文进行不同的处理。

二层 ACL 的作用对象为二层报文（以太协议类型为 Ethernet_II）。针对这些报文，二层 ACL 根据报文自身的源 MAC 地址、目的 MAC 地址、MAC 承载的协议类型、VLAN 编号或 802.1p 优先级信息，以及时间段信息对二层报文进行分类。

前置任务

在二层 ACL 之前，需要完成以下任务：

- 连接接口并配置接口的物理参数，使接口的物理层状态为 Up。

数据准备

在配置二层 ACL 之前，需准备以下数据。

序号	数据
1	（可选）生效时间段名称以及生效时间
2	二层 ACL 的编号或名称
3	源 MAC 地址、目的 MAC 地址、MAC 承载的协议类型、VLAN 编号或 802.1p 优先级信息
4	（可选）二层 ACL 的描述内容
5	（可选）二层 ACL 规则的描述内容
6	（可选）二层 ACL 的步长

10.5.2 （可选）创建二层 ACL 生效时间段

用户可以为二层 ACL 创建生效时间段，通过在规则中引用时间段信息限制该规则生效的时间范围。如果配置规则时不指定时间段，则该规则不受时间范围限制，除非删除该规则或删除该 ACL。

背景信息

某些引用二层 ACL 的业务或功能需要限制在一定的时间范围内生效，比如，在流量高峰期时启动设备的 QoS 功能。用户可以为二层 ACL 创建生效时间段，通过在规则中引用时间段信息限制二层 ACL 生效的时间范围，从而实现该业务或功能在一定的时间范围内生效的目的。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **time-range** *time-name* { *start-time* **to** *end-time days* | **from** *time1 date1* [**to** *time2 date2*] }，创建一个时间段。

AR1200 支持具有相同 *time-name* 的多个时间段共同描述某个时间范围，此时可以使用相同的 *time-name* 反复执行本步骤。

说明

可以为多个时间段范围配置相同的 *time-name*，共同来描述某个特殊时间。例如：时间段“test”配置了三个生效时段

- 从 2010 年 1 月 1 日 00:00 起到 2010 年 12 月 31 日 23:59 生效，这是一个绝对时间段。
- 在周一到周五每天 8:00 到 18:00 生效，这是一个周期时间段。
- 在周六、周日下午 14:00 到 18:00 生效，这是一个周期时间段。

则时间段“test”最终描述的时间范围为：2010 年的周一到周五每天 8:00 到 18:00 以及周六和周日下午 14:00 到 18:00。

----结束

后续处理

在配置二层 ACL 规则时，用户可以通过参数 **time-range** 在规则中引用已配置的时间段信息，限制规则生效的时间范围。

10.5.3 创建二层 ACL

使用二层 ACL 前，必须先创建二层 ACL。用户可以使用编号或名称来创建二层 ACL。

前提条件

使用 **display acl all** 命令查看所有已配置的 ACL，避免重复配置二层 ACL。

操作步骤

- 使用编号创建二层 ACL。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号创建一个二层 ACL，并进入二层 ACL 视图。

     二层 ACL 编号 *acl-number* 的范围是 4000 ～ 4999。

     match-order 指定了二层 ACL 规则的匹配顺序。

     - **auto** 表示匹配规则时系统自动排序（按“深度优先”的顺序）。
     - **config** 表示匹配规则时按用户的配置顺序。
  3. （可选）执行命令 **description** *text*，配置二层 ACL 描述信息。

     ACL 的描述信息可以描述 ACL 的用途或使用场景，方便用户区分或识别不同的 ACL。

     缺省情况下，不配置 ACL 描述信息。
- 使用名称创建二层 ACL。
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **acl name** *acl-name* { **link** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个二层 ACL，进入二层 ACL 视图。

     二层 ACL 编号 *acl-number* 的范围是 4000 ～ 4999。

match-order 指定了二层 ACL 规则的匹配顺序。

- **auto** 表示匹配规则时系统自动排序（按“深度优先”的顺序）。
- **config** 表示匹配规则时按用户的配置顺序。

3. （可选）执行命令 **description** *text*，配置二层 ACL 描述信息。

   ACL 的描述信息可以描述 ACL 的用途或使用场景，方便用户区分或识别不同的 ACL。

   缺省情况下，不配置 ACL 描述信息。

----结束

后续处理

在二层 ACL 视图下配置该 ACL 的规则。

10.5.4 配置二层 ACL 的规则

二层 ACL 是一系列有顺序规则的集合，通过规则来匹配报文的信息，实现对报文的分类。

前提条件

已经创建二层 ACL 并进入二层 ACL 视图。

使用命令 **display acl** { *acl-number* | **name** *acl-name* }命令查看该 ACL 已配置的所有规则，避免新规则覆盖已配置的规则。

背景信息

二层 ACL 通过规则匹配报文的信息，从而实现对报文的分类，因此创建二层 ACL 以后，需要配置二层 ACL 的规则。

以下操作是在二层 ACL 视图下进行的。

操作步骤

步骤 1 （可选）执行命令 **step** *step-value*，配置 ACL 步长。

缺省情况下，二层 ACL 步长值为 5。

步骤 2 执行命令 **rule** { **permit** | **deny** } [**l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | [**time-range** *time-range-name*]] *

如果二层 ACL 需要配置多个规则，可以反复执行本步骤。

说明

本步骤中，**rule** 命令没有选择参数 *rule-id*，这种情况下，步长值作为规则的起始编号，并作为步长间隔。

配置规则时，如果不同的规则之间存在矛盾或包含的关系，请注意规则的匹配顺序，防止出现错误配置。

步骤 3 （可选）执行 **rule** *rule-id* **description** *text*，配置二层 ACL 规则的描述信息。

二层 ACL 规则的描述信息用来描述 ACL 规则的用途或使用场景，方便用户区分或识别 ACL 的不同规则。

----结束

后续处理

配置二层 ACL 规则后，通常有以下的后续处理步骤：

- 用户需要调整规则的步长时，可以执行 **step** 命令，重新设置步长值。
- 当匹配方式为 config 时，用户需要在规则之间插入新的规则，可以执行 **rule** 命令并选择参数 *rule-id*。

10.5.5 应用二层 ACL

二层 ACL 可以应用在某些业务或功能中，实现对报文的过滤。

前提条件

已经创建二层 ACL，并完成二层 ACL 规则的配置。

背景信息

二层 ACL 可以应用在以下业务和功能：

- 流分类
- 本机防攻击特性中的黑名单功能
- 在接口上根据 ACL 对报文流进行过滤

操作步骤

- 流分类

  对于进入设备的各种流量，可以根据报文的信息对不同的业务提供差别服务，此时需要配置流分类。AR1200 支持基于二层 ACL 定义流分类中的匹配规则。参见配置流分类。

- 本机防攻击特性中的黑名单功能

  黑名单指非法用户的集合，通过二层 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 AR1200 后均会被丢弃。参见**配置黑名单**。

- 在接口上根据 ACL 对报文流进行过滤

  AR1200 支持在接口上根据 ACL 对报文流进行过滤。这样，AR1200 将会过滤匹配 ACL 规则的报文：

  - 当报文命中的规则的动作为 **deny**，则直接丢掉该报文。
  - 当报文命中的规则的动作为 **permit**，则允许该报文通过。

  下面介绍在接口上根据 ACL 对报文流进行过滤的配置步骤。

  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

3. 执行命令 **traffic-filter** { **inbound** | **outbound** } **acl** { *acl-number* | **name** *acl-name* }，配置根据 ACL 对报文流进行过滤。

----结束

10.5.6 检查配置结果

二层 ACL 配置完成以后，查看二层 ACL 规则和时间段信息。

前提条件

已经完成了二层 ACL 的配置。

操作步骤

- 执行命令 **display acl** *acl-number*，查看以编号创建的 ACL 规则。
- 执行命令 **display acl name** *acl-name*，查看以名称创建的 ACL 规则。
- 执行命令 **display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

任务示例

执行命令 **display acl** *acl-number*，可以看到二层 ACL 的编号、规则数量、步长和规则的具体内容。

```
<Huawei> display acl 4001
L2 ACL 4001, 1 rule
Acl's step is 5
  rule 5 permit l2-protocol ip destination-mac 0000-0000-0001 source-mac 0000-0000-0002
```

执行命令 **display acl name** *acl-name*，可以看到二层 ACL 的名称、编号、规则数量、步长和规则的具体内容。

```
<Huawei> display acl name test
L2 ACL test 4999, 1 rule
Acl's step is 5
 rule 5 deny destination-mac 00e0-fc01-0304
```

执行命令 **display time-range**，可以看到当前时间段的配置和状态。

```
<Huawei> display time-range all
Current time is 09:13:37 12-27-2010 Thursday

Time-range : test1 ( Inactive )
 13:00 to 18:00 working-day
 13:00 to 18:00 off-day
```

10.6 配置举例

介绍 ACL 的配置举例。配置示例中包括组网需求、配置思路、操作步骤等。

10.6.1 应用基本 ACL 配置 FTP 服务器访问权限示例

在本示例中，通过应用基本 ACL，实现 FTP 服务器对客户端访问权限的设置。

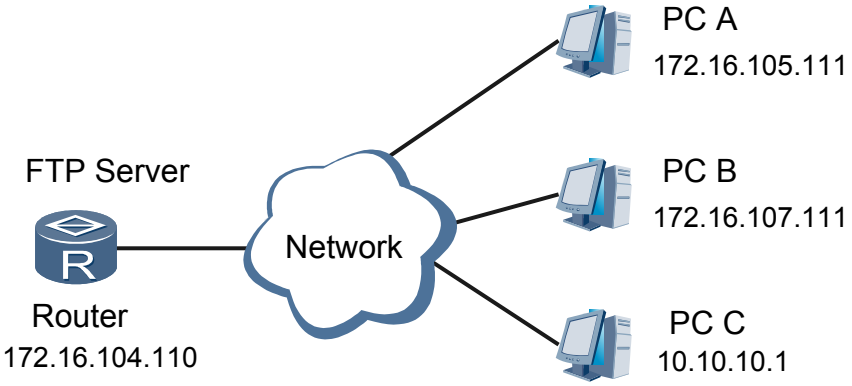
组网需求

如图 10-1 所示，Router 作为 FTP 服务器（172.16.104.110/24）为网络中的不同用户设置不同的访问权限：

- 子网 1（172.16.105.0/23）的所有用户在任意时间都可以访问 FTP 服务器。
- 子网 2（172.16.107.0/23）的所有用户只能在某一个时间范围内访问 FTP 服务器。
- 其他用户不可以访问 FTP 服务器。

已知 Router 与各个子网之间路由可达，要求在 Router 上进行配置，实现 FTP 服务器对客户端访问权限的设置。

图 10-1 应用基本 ACL 配置 FTP 服务器访问权限组网图



配置思路

采用如下的配置思路：

- 在 Router 上创建基本 ACL，并通过配置基本 ACL 规则对网络中不同用户进行分类。
- 在 Router 上配置 FTP 基本功能。
- 在 Router 应用基本 ACL 为网络中的不同用户设置不同的访问权限。

数据准备

为完成配置举例，需准备如下的数据：

- 基本 ACl 编号：2001。
- 子网 2 访问 FTP 服务器的时间段名称：ftp-access。
- ftp-access 描述的时间范围：2009 年到 2011 年周六、周日下午 14:00 到 18:00。

操作步骤

步骤 1 配置时间段

```
<Huawei> system-view
[Huawei] sysname Router
[Router] time-range ftp-access from 0:0 2009/1/1 to 23:59 2011/12/31
[Router] time-range ftp-access 14:00 to 18:00 off-day
```

步骤 2 配置基本 ACL

```
[Router] acl number 2001
[Router-acl-basic-2001] rule permit source 172.16.105.0 0.0.1.255
[Router-acl-basic-2001] rule permit source 172.16.107.0 0.0.1.255 time-range ftp-access
[Router-acl-basic-2001] quit
```

步骤 3 配置 FTP 基本功能（略）

步骤 4 配置 FTP 服务器访问权限

```
[Router] ftp acl 2001
```

步骤 5 验证配置结果

在子网 1 的 PC A（172.16.105.111/24）上执行 **ftp 172.16.104.110** 命令，可以连接 FTP 服务器。

2010 年某个周一在子网 2 的 PC B（172.16.107.111/24）上执行 **ftp 172.16.104.110** 命令，不能连接 FTP 服务器；2010 年某个周六下午 15:00 在子网 2 的 PC B（172.16.107.111/24）上执行 **ftp 172.16.104.110** 命令，可以连接 FTP 服务器。

在 PC C（10.10.10.1/24）上执行 **ftp 172.16.104.110** 命令，不能连接 FTP 服务器。

----结束

配置文件

Router 的配置文件

```
#
sysname Router
#
ftp server enable
ftp acl 2001
#
time-range ftp-access from 0:0 2009/1/1 to 23:59 2011/12/31
time-range ftp-access 14:00 to 18:00 off-day
#
acl number 2001
 rule 5 permit source 172.16.104.0 0.0.1.255
 rule 10 permit source 172.16.106.0 0.0.1.255 time-range ftp-access
#
return
```

10.6.2 应用高级 ACL 配置防火墙示例

在本示例中，通过应用高级 ACL，实现企业内部网络与外部网络之间包过滤防火墙的配置。

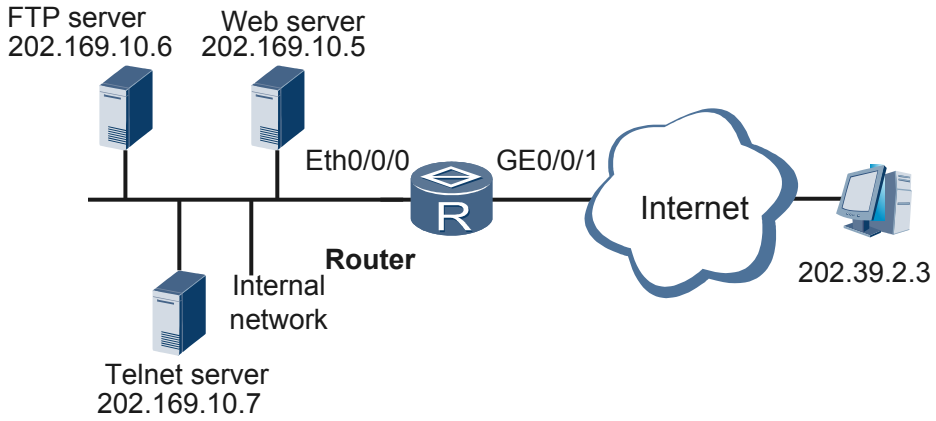
组网需求

如图 10-2 所示，某个对外提供 WWW、FTP 和 Telnet 服务的企业通过 Router 的接口 GE0/0/1 访问外部网络，通过 Router 的接口 Ethernet0/0/0 加入 VLAN。

已知企业的网段为 202.169.10.0/24，企业内部的 WWW 服务器、FTP 服务器和 Telnet 服务器 IP 地址分别为 202.169.10.5/24、202.169.10.6/24 和 202.169.10.7/24。

为了实现内部网络具备较高的安全性，企业希望在 Router 上配置防火墙功能，使外部网络只有特定用户可以访问内部服务器，企业内只有内部服务器可以访问外部网络。

图 10-2 应用高级 ACL 配置防火墙组网图



配置思路

采用如下的配置思路：

- 为企业内部网络和外部网络配置不同的安全区域。
- 配置安全域间，在安全域间使能防火墙功能。
- 配置不同的高级 ACL，对可以访问内部服务器的外部网络用户以及可以访问外部网络的内部服务器进行分类。
- 在安全域间配置基于高级 ACL 的包过滤。

数据准备

为完成配置举例，需准备如下的数据：

- 表示企业内部网络的安全区域名称：company。
- 安全区域 company 的优先级：12。
- 表示外部网络的安全区域名称：external。
- 安全区域 external 的优先级：5。
- 企业加入的 VLAN ID：100。
- 接口 VLANIF100 的 IP 地址：202.169.10.1/24。
- 接口 GE0/0/1 的 IP 地址：129.39.10.8/24
- 从外部网络可以访问内部服务器的特定用户的 IP 地址：202.39.2.3/24。
- 为该特定用户进行分类的高级 ACL 编号：3001。
- 为内部服务器进行分类的高级 ACL 编号：3002。

操作步骤

步骤 1 配置安全区域。

为企业内部网络配置安全区域。

```
<Huawei> system-view
[Huawei] sysname Router
```

```
[Router] firewall zone company
[Router-zone-company] priority 12
[Router-zone-company] quit
```

将接口 VLANIF100 加入安全区域 company。

```
[Router] interface vlanif 100
[Router-Vlanif100] zone company
[Router-Vlanif100] quit
```

为外部网络配置安全区域。

```
[Router] firewall zone external
[Router-zone-external] priority 5
[Router-zone-external] quit
```

将接口 GE0/0/1 加入安全区域 external。

```
[Router] interface gigabitEthernet 0/0/1
[Router-gigabitEthernet0/0/1] zone external
[Router-gigabitEthernet0/0/1] quit
```

步骤 2 配置安全域间。

```
[Router] firewall interzone company external
[Router-interzone-company-external] firewall enable
[Router-interzone-company-external] quit
```

步骤 3 配置 ACL3001。

创建 ACL3001。

```
[Router] acl 3001
```

配置允许特定用户从外部网络可以访问内部服务器。

```
[Router-acl-adv-3001] rule permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.5 0.0.0.0
[Router-acl-adv-3001] rule permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.6 0.0.0.0
[Router-acl-adv-3001] rule permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.7 0.0.0.0
```

配置其他用户不能从外部网络访问企业内部的任何主机。

```
[Router-acl-adv-3001] rule deny ip
[Router-acl-adv-3001] quit
```

步骤 4 配置 ACL3002。

创建 ACL3002。

```
[Router] acl 3002
```

配置允许内部服务器访问外部网络。

```
[Router-acl-adv-3002] rule permit ip source 202.169.10.5 0.0.0.0
[Router-acl-adv-3002] rule permit ip source 202.169.10.6 0.0.0.0
[Router-acl-adv-3002] rule permit ip source 202.169.10.7 0.0.0.0
```

配置网络内部的其他用户不能访问外部网络。

```
[Router-acl-adv-3002] rule deny ip
[Router-acl-adv-3002] quit
```

步骤 5 在安全域间配置基于高级 ACL 的包过滤。

```
[Router] firewall interzone company external
[Router-interzone-company-external] packet-filter 3001 inbound
[Router-interzone-company-external] packet-filter 3002 outbound
[Router-interzone-company-external] quit
```

步骤 6 检查配置结果。

配置成功后，仅特定主机（202.39.2.3）可以访问内部服务器，仅内部服务器可以访问外部网络。

在 Router 上执行 **display firewall interzone** [*zone-name1 zone-name2*]操作，结果如下。

```
[Router] display firewall interzone company external
interzone company external
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3001 inbound
 packet-filter 3002 outbound
```

----结束

配置文件

Router 的配置文件

```
#
 sysname Router
#
 vlan batch 100
#
acl number 3001
 rule 5 permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.5 0.0.0.0
 rule 10 permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.6 0.0.0.0
 rule 15 permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.7 0.0.0.0
 rule 20 deny ip
#
acl number 3002
 rule 5 permit ip source 202.169.10.5 0.0.0.0
 rule 10 permit ip source 202.169.10.6 0.0.0.0
 rule 15 permit ip source 202.169.10.7 0.0.0.0
 rule 20 deny ip
#
interface Vlanif100
 ip address 202.169.10.1 255.255.255.0
 zone company
#
firewall zone company
 priority 12
#
firewall zone external
 priority 5
#
firewall interzone company external
 firewall enable
 packet-filter 3001 inbound
 packet-filter 3002 outbound
#
interface Ethernet0/0/0
 port link-type access
 port default vlan 100
#
interface
GigabitEthernet0/0/1
 ip address 129.39.10.8 255.255.255.0
 zone external
#
return
```

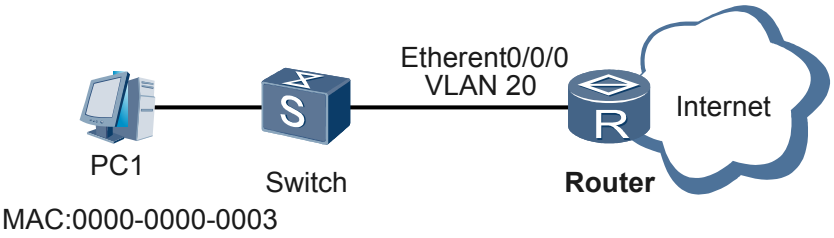
10.6.3 应用二层 ACL（命名型）配置流分类示例

在本示例中，通过应用二层 ACL 配置流分类，实现对特定源 MAC 的报文进行流量统计。

组网需求

如图 10-3 所示，PC1 的 MAC 地址为 0000-0000-0003，它通过交换机连接在 Router 的 Ethernet0/0/0 端口上。要求 Router 对源 MAC 为 0000-0000-0003 的报文进行流量统计。

图 10-3 应用二层 ACL 配置流分类示例组网图



配置思路

采用如下的思路配置基于流分类的流量统计：

1. 配置二层 ACL 规则，匹配源 MAC 为 0000-0000-0003 的报文。
2. 根据二层 ACL 配置流分类。
3. 配置流行为，对分类后的报文进行流量统计。
4. 配置流策略，绑定上述流分类和流行为。

数据准备

为完成此配置示例，需准备如下的数据：

- Router 与 Switch 相连的接口所属 VLAN 编号：20。
- 二层 ACL 名称：layer2。
- 流分类的名称：c1。
- 流行为的名称：b1。
- 流策略的名称：p1。

操作步骤

步骤 1 创建 VLAN 并配置各接口

创建 VLAN20。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan 20
[Router-vlan20] quit
```

配置接口 Ethernet0/0/0 为 Trunk 类型端口，并将 Ethernet0/0/0 加入 VLAN20。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] port link-type trunk
[Router-Ethernet0/0/0] port trunk allow-pass vlan 20
[Router-Ethernet0/0/0] quit
```

说明

请配置 Switch 与 Router 对接的接口为 Trunk 类型接口，并加入 VLAN20，本例不再描述。

请配置 Switch 与 PC1 对接的接口为 Access 类型接口，并加入 VLAN20，本例不再描述。

步骤 2 配置 ACL 规则

在 Router 上创建名称为 layer2 的二层 ACL，匹配源 MAC 为 0000-0000-0003 的报文。

```
[Router] acl name layer2 link
[Router-acl-L2-layer2] rule permit source-mac 0000-0000-0003 ffff-ffff-ffff
[Router-acl-L2-layer2] quit
```

步骤 3 配置流分类

在 Router 上创建流分类 c1，匹配的 ACL 的名称为 layer2。

```
[Router] traffic classifier c1
[Router-classifier-c1] if-match acl layer2
[Router-classifier-c1] quit
```

步骤 4 配置流行为

在 Router 上创建流行为 b1，并配置流量统计动作。

```
[Router] traffic behavior b1
[Router-behavior-b1] statistic enable
[Router-behavior-b1] quit
```

步骤 5 配置流策略并应用到接口上

在 Router 上创建流策略 p1，将流分类和对应的流行为进行绑定。

```
[Router] traffic policy p1
[Router-trafficpolicy-p1] classifier c1 behavior b1
[Router-trafficpolicy-p1] quit
```

将流策略 p1 应用到接口 Ethernet0/0/0。

```
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] traffic-policy p1 inbound
[Router-Ethernet0/0/0] quit
[Router] quit
```

步骤 6 验证配置结果

查看 ACL 规则的配置信息。

```
<Router> display acl name layer2
L2 ACL layer2 4999, 1 rule
Acl's step is 5
 rule 5 permit source-mac 0000-0000-0003
```

查看流分类的配置信息。

```
<Router> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c1
    Operator: OR
    Rule(s) : if-match acl name layer2
```

查看流策略的配置信息。

```
<Router> display traffic policy user-defined p1
  User Defined Traffic Policy Information:
```

```
Policy: p1
 Classifier: c1
  Operator: OR
   Behavior: b1
    statistic: enable
```

----结束

配置文件

- Router 的配置文件

```
#
 sysname Router
#
 vlan batch 20
#
acl name layer2 4999
 rule 5 permit source-mac 0000-0000-0003
#
traffic classifier c1 operator or
 if-match acl layer2
#
traffic behavior b1
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1
#
interface Ethernet0/0/0
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p1 inbound
#
return
```

11 SSL 配置

关于本章

安全套接层 SSL（Secure Sockets Layer）协议是在 Internet 基础上提供的一种保证私密性的安全协议。

11.1 SSL 概述
SSL 利用数据加密、身份验证和消息完整性验证机制，为基于 TCP 可靠连接的应用层协议提供安全性保证。

11.2 AR1200 支持的 SSL 特性
AR1200 支持配置两种类型的 SSL 策略：服务器型 SSL 策略和客户端型 SSL 策略。

11.3 配置服务器型 SSL 策略
服务器型 SSL 策略包含 SSL 握手过程中使用的 SSL 参数，比如 PKI 域（必选）、保存会话的最大数目（可选）、保存会话的最大时长（可选）和加密套件（可选）。

11.4 配置客户端型 SSL 策略
客户端型 SSL 策略包含 SSL 握手过程中使用的参数，比如 PKI 域、SSL 协议版本和加密套件。

11.5 配置举例
介绍 SSL 的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

11.1 SSL 概述

SSL 利用数据加密、身份验证和消息完整性验证机制，为基于 TCP 可靠连接的应用层协议提供安全性保证。

概述

SSL 协议是在 Internet 基础上提供的一种保证私密性的安全协议。它能使客户端与服务器之间的通信不被攻击者窃听，并且始终对服务器进行认证，还可选择对客户端进行认证。目前，SSL 协议广泛应用于电子商务、网上银行等领域。SSL 具有以下优点：

- 提供较高的安全性保证。SSL 利用数据加密、身份验证和消息完整性验证机制，保证网络上数据传输的安全性。
- 支持各种应用层协议。虽然 SSL 设计的初衷是为了解决万维网安全性问题，但是由于 SSL 位于应用层和传输层之间，它可以为任何基于 TCP 可靠连接的应用层协议提供安全性保证。
- 部署简单。目前 SSL 已经成为网络中用来鉴别网站和网页浏览者身份，在浏览器使用者及 Web 服务器之间进行加密通信的全球化标准。

SSL 从以下几方面提高了设备的安全性：

- 通过 SSL 协议保证合法客户端可以安全地访问服务器，禁止非法的客户端访问服务器。
- 客户端与服务器之间交互的数据需要经过加密和摘要，加密保证了传输的安全性，摘要保证了数据的完整性，从而实现了对设备的安全管理。
- 为设备制定基于证书属性的访问控制策略，对客户端的访问权限进行控制，进一步避免了非法客户对设备进行攻击。

基本概念

- CA（Certificate Authority）

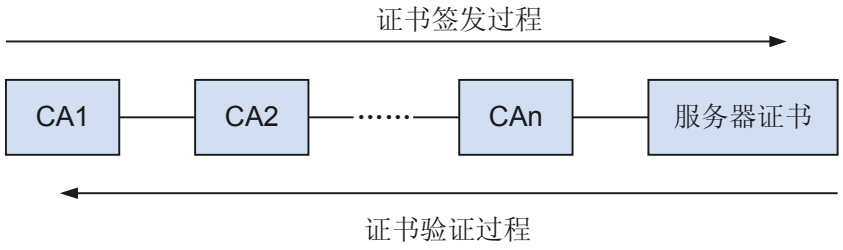
  CA 是发放、管理、废除数字证书的机构。CA 的作用是检查数字证书持有者身份的合法性，并签发数字证书（在证书上签字），以防证书被伪造或篡改，以及对证书和密钥进行管理。国际上被广泛信任的 CA，被称之为根 CA。根 CA 可授权其它 CA 为其下级 CA。CA 的身份也需要证明，而证明信息在信任证书机构文件中描述。

  例如：CA1 作为最上级 CA 也叫根证书，签发下一级 CA2 证书，CA2 又可以给它的下一级 CA3 签发证书，以此下去，最终由 CAn 签发服务器的证书。

  如果服务器端的证书由 CA3 签发，则在客户端验证证书的过程从服务器端的证书有效性验证开始。先由 CA3 证书验证服务器端证书的有效性，如果通过则再由 CA2 证书验证 CA3 证书的有效性，最后由最上级 CA1 证书验证 CA2 证书的有效性。只有通过最上级 CA 证书即根证书的验证，服务器证书才会验证成功。

  证书签发过程与证书验证过程如图 11-1 所示。

图 11-1 证书签发过程与证书验证过程示意图



- 数字证书

  数字证书实际上是存于计算机上的一个记录，是由 CA 签发的一个声明，证明证书主体（证书申请者拥有了证书后即成为证书主体）与证书中所包含的公钥的惟一对应关系。数字证书中包括证书申请者的名称及相关信息、申请者的公钥、签发数字证书的 CA 的数字签名及数字证书的有效期等内容。数字证书的作用使网上通信双方的身份得到了互相验证，提高了通信的可靠性。

  用户必须事先获取信息发送者的公钥证书，以便对信息进行解码认证，同时还需要 CA 发送给发送者的证书，以便用户验证发送者的身份。

- 证书撤销列表 CRL（Certificate Revocation List）

  CRL 由 CA 发布，它指定了一套证书发布者认为无效的证书。

  数字证书的寿命是有限的，但 CA 可通过证书撤销过程缩短证书的寿命。CRL 指定的寿命通常比数字证书指定的寿命要短。由 CA 撤销数字证书，意味着 CA 在数字证书正常到期之前撤销允许使用密钥对的有关声明。在撤销证书到期后，CRL 中的有关数据被删除，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。

协议安全机制

- 连接的私密性

  SSL 利用对称加密算法对传输数据进行加密，并利用密钥交换算法—RSA（Rivest Shamir and Adleman，非对称密钥算法的一种）加密传输对称密钥算法中使用的密钥。

- 身份验证机制

  基于证书利用数字签名方法对服务器和客户端进行身份验证。SSL 服务器和客户端通过 PKI（Public Key Infrastructure，公钥基础设施）提供的机制从 CA（Certificate Authority，认证机构）获取证书。

- 内容的可靠性

  消息传输过程中使用基于密钥的 MAC（Message Authentication Code，消息验证码）来检验消息的完整性。

  MAC 算法是将密钥和任意长度的数据转换为固定长度数据的一种算法。

  - 发送端在密钥参与下，利用 MAC 算法计算出消息的 MAC 值，并将其加在消息之后发送给接收端。
  - 接收端利用同样的密钥和 MAC 算法计算出消息的 MAC 值，并与接收到的 MAC 值比较。

如果二者相同，则报文没有改变。否则，报文在传输过程中被修改，接收端将丢弃该报文。

11.2 AR1200 支持的 SSL 特性

AR1200 支持配置两种类型的 SSL 策略：服务器型 SSL 策略和客户端型 SSL 策略。

服务器型 SSL 策略

服务器型 SSL 策略包含 SSL 握手过程中使用的 SSL 参数，比如 PKI 域、保存会话的最大数、保存会话的最大时长和加密套件。

管理员在 AR1200 配置服务器型 SSL 策略后，AR1200 可以作为 SSL 服务器。在 SSL 握手过程中，AR1200 使用服务器型 SSL 策略所设置的 SSL 参数与 SSL 客户端之间协商会话参数，并建立会话。

应用层协议（如 HTTP 协议）可以关联服务器型 SSL 策略，使应用层协议与 SSL 结合，从而为应用层协议提供安全连接。目前，服务器型 SSL 策略可以应用在 HTTPS 业务中。

客户端型 SSL 策略

客户端型 SSL 策略包含 SSL 握手过程中使用的参数，比如 PKI 域、SSL 协议版本和加密套件。

管理员在 AR1200 上配置客户端型 SSL 策略后，AR1200 可以作为 SSL 客户端。在 SSL 握手过程中，AR1200 使用客户端型 SSL 策略所设置的 SSL 参数与 SSL 服务器之间协商会话参数，并建立会话。

应用层协议（如 CWMP 协议）可以关联客户端型 SSL 策略，使应用层协议与 SSL 结合，从而为应用层协议提供安全连接。目前，客户端型 SSL 策略可以应用在 CWMP 业务中。

11.3 配置服务器型 SSL 策略

服务器型 SSL 策略包含 SSL 握手过程中使用的 SSL 参数，比如 PKI 域（必选）、保存会话的最大数目（可选）、保存会话的最大时长（可选）和加密套件（可选）。

前提条件

PKI 域已成功配置。

应用环境

SSL 利用数据加密、身份验证和消息完整性验证机制，为基于 TCP 可靠连接的应用层协议提供安全性保证。应用层协议（如 HTTP 协议）可以关联服务器型 SSL 策略，使应用层协议与 SSL 结合，从而为应用层协议提供安全连接。

图 11-2 AR1200 作为 SSL 服务器示意图

如图 11-2 所示，管理员在 AR1200 配置服务器型 SSL 策略后，AR1200 可以作为 SSL 服务器。在 SSL 握手过程中，AR1200 使用服务器型 SSL 策略所设置的 SSL 参数与 SSL 客户端之间协商会话参数，并建立会话。

AR1200 作为 SSL 服务器时，允许 SSL 客户端对其进行身份验证，但它不具备对 SSL 客户端进行身份验证的功能。

说明

AR1200 作为 SSL 服务器时，可以与 SSL3.0、TLS1.0 和 TLS 1.1 版本的 SSL 客户端通信。AR1200 确定本次通信采用的 SSL 协议版本（SSL3.0、TLS1.0 或 TLS1.1 版本），并通过 Server Hello 消息通知给 SSL 客户端。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssl policy** *policy-name* **type server**，创建服务器型 SSL 策略。

步骤 3 执行命令 **pki-realm** *realm-name*，配置服务器型 SSL 策略所使用的 PKI 域。

缺省情况下，AR1200 没有配置服务器型 SSL 策略所使用的 PKI 域。

说明

作为 SSL 服务器的 AR1200 基于 PKI 域从认证机构 CA 获取数字证书，以便 SSL 客户端可以根据数字证书对 AR1200 进行身份验证。

步骤 4 （可选）执行命令 **session** { **cachesize** *size* | **timeout** *time* } *，配置保存会话的最大数目和最大时长。

缺省情况下，保存会话的最大数目为 128 个，保存会话的最大时长为 3600 秒。

步骤 5 （可选）执行命令 **ciphersuite** { **rsa_aes_128_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** } *，配置服务器型 SSL 策略支持的加密套件。

缺省情况下，服务器型 SSL 策略支持的加密套件为 rsa_aes_128_cbc_sha、rsa_des_cbc_sha、rsa_rc4_128_md5 和 rsa_rc4_128_sha。

----结束

任务示例

执行命令 **display ssl policy** *policy-name*，查看 SSL 策略 server-users 的配置信息。

```
<Huawei> display ssl policy server-users
------------------------------------------------------------------------------
  Policy name                    :   server-users
  Policy ID                      :   1
  Policy type                    :   Server
  Cache number                   :   128
  Time out(second)               :   3600
  Server certificate load status :   loaded
  Bind number                    :   1
  SSL connection number          :   1
------------------------------------------------------------------------------
```

11.4 配置客户端型 SSL 策略

客户端型 SSL 策略包含 SSL 握手过程中使用的参数，比如 PKI 域、SSL 协议版本和加密套件。

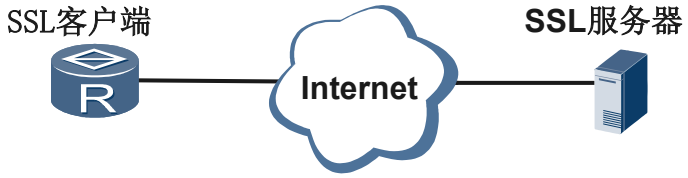
前提条件

PKI 域已成功配置。

应用环境

SSL 利用数据加密、身份验证和消息完整性验证机制，为基于 TCP 可靠连接的应用层协议提供安全性保证。应用层协议（如 CWMP 协议）可以关联客户端型 SSL 策略，使应用层协议与 SSL 结合，从而为应用层协议提供安全连接。

图 11-3 AR1200 作为 SSL 客户端示意图



如图 11-3 所示，管理员在 AR1200 上配置客户端型 SSL 策略后，AR1200 可以作为 SSL 客户端。在 SSL 握手过程中，AR1200 使用客户端型 SSL 策略所设置的 SSL 参数与 SSL 服务器之间协商会话参数，并建立会话。

AR1200 作为 SSL 客户端时，不允许 SSL 服务器对其进行身份验证，但可以选择对 SSL 服务器进行身份验证。为了保证通信安全，当 AR1200 作为 SSL 客户端时，请使能基于证书的 SSL 服务器身份验证。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **ssl policy** *policy-name* **type client**，创建客户端型 SSL 策略。

步骤 3 执行命令 **server-verify enable**，使能基于证书的 SSL 服务器身份验证。

缺省情况下，不使能进行基于证书的 SSL 服务器身份验证。

步骤 4 执行命令 **pki-realm** *realm-name*，配置客户端型 SSL 策略所使用的 PKI 域。

缺省情况下，AR1200 没有配置客户端型 SSL 策略所使用的 PKI 域。

说明

作为 SSL 客户端的 AR1200 基于 PKI 域从认证机构 CA 获取 CA 证书链，以便 AR1200 可以根据 CA 证书链对 SSL 服务器进行身份验证。

步骤 5 （可选）执行命令 **version** { **ssl3.0** | **tls1.0** | **tls1.1** }，配置客户端型 SSL 策略使用的 SSL 协议版本。

缺省情况下，客户端型 SSL 策略使用的 SSL 协议版本为 TLS1.0。

说明

本步骤所配置的 SSL 协议版本必须包含在 SSL 服务器支持的协议版本中。若配置本步骤，请确认 SSL 服务器支持的协议版本。

步骤 6 （可选）执行命令 **prefer-ciphersuite** { **rsa_aes_128_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** }，配置客户端型 SSL 策略使用的加密套件。

缺省情况下，客户端型 SSL 策略使用的加密套件为 rsa_aes_128_cbc_sha、rsa_des_cbc_sha、rsa_rc4_128_md5 和 rsa_rc4_128_sha。

说明

本步骤所配置的加密套件必须包含在 SSL 服务器支持的加密套件中。若配置本步骤，请确认 SSL 服务器支持的加密套件。

----结束

任务示例

执行命令 **display ssl policy** *policy-name*，查看 SSL 策略 client-users 的配置信息。

```
<Huawei> display ssl policy client-users
------------------------------------------------------------------------------
Policy name                     :   client-users
Policy ID                       :   3
Policy type                     :   Client
Server verify                   :   1
CA certificate load status      :   loaded
CA certificate num              :   1
Bind number                     :   1
SSL connection number           :   1
------------------------------------------------------------------------------
```

11.5 配置举例

介绍 SSL 的配置举例。配置举例中包括组网需求、配置思路、操作步骤等。

11.5.1 配置服务器型 SSL 策略示例

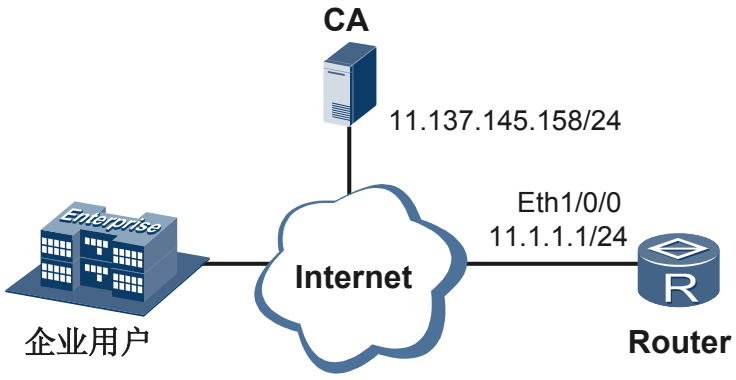
本例以 HTTPS 特性为例，通过在作为 HTTPS 服务器的 AR1200 上关联服务器型 SSL 策略，实现用户利用 Web 页面安全访问和管理 Router。

组网环境

如图 11-4 所示，某企业用户可以利用 Web 页面访问 Router。为了防止传输的数据不被窃听和篡改，实现对设备的安全管理，网络管理员要求用户以 HTTPS 的方式安全访问 Router。

为了满足上述需求，需要把 Router 配置成为 HTTPS 服务器，并且该 HTTPS 服务器关联服务器型 SSL 策略，以便用户可以利用 Web 页面安全访问和管理 Router。

图 11-4 配置服务器型 SSL 策略示意图



配置思路

采用如下的配置思路：

1. 配置 PKI，包括 PKI 实体和 PKI 域。
2. 配置服务器型 SSL 策略。
3. 配置 HTTPS 服务器。

数据准备

为完成此配置举例，需要准备如下数据：

- Router 连接 Internet 的接口:Ethernet1/0/0
- 接口 Ethernet1/0/0 的 IP 地址：11.1.1.1/24
- CA 的 IP 地址：11.137.145.158/24
- PKI 参数:

配置项	数据
PKI 实体	PKI 实体名：users ● 实体通用名：hello ● 国家代码：CN ● 所在的州或者省：jiangsu ● 所在的组织：huawei ● 所在的组织部门：info
PKI 域名	PKI 域名：users ● 信任的 CA：ca_root ● 注册证书的 URL：http://11.137.145.158:8080/certsrv/mscep/mscep.dll ra ● 绑定的实体: users ● CA 的指纹：采用安全散列算法 指纹值：7bb05ada0482273388ed4ec228d79f77309ea3f4

- SSL 策略参数：

策略名称	保存会话的最大数目	保存会话的最大时长
sslserver	40 个	7200 秒

- HTTPS 服务的端口号：1278

说明

进行下面的配置之前，需要确保 Router、Host、CA 之间路由可达。

操作步骤

步骤 1 配置 PKI。

配置 PKI 实体。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] pki entity users
[Router-pki-entity-users] common-name hello
[Router-pki-entity-users] country cn
[Router-pki-entity-users] state jiangsu
[Router-pki-entity-users] organization huawei
[Router-pki-entity-users] organization-unit info
[Router-pki-entity-users] quit
```

说明

实体名和实体通用名如果没有配置为设备的 IP 地址，11.1.1.1，使用 HTTPS 打开网页的时候会提示“证书不合法”，但这不会影响正常使用。

配置 PKI 域，并使能证书自动注册和更新功能。

```
[Router] pki realm users
[Router-pki-realm-users] ca id ca_root
[Router-pki-realm-users] enrollment-url http://11.137.145.158:8080/certsrv/mscep/mscep.dll ra
[Router-pki-realm-users] entity users
[Router-pki-realm-users] auto-enroll regenerate
[Router-pki-realm-users] fingerprint sha1 7bb05ada0482273388ed4ec228d79f77309ea3f4
[Router-pki-realm-users] quit
```

步骤 2 配置服务器型 SSL 策略。

配置 SSL 策略使用 PKI 域 users，以便 Router 可以基于该 PKI 域从认证机构 CA 获取数字证书。

```
[Router] ssl policy sslserver type server
[Router-ssl-policy-sslserver] pki-realm users
```

配置保存会话的最大数目和最大时长。

```
[Router-ssl-policy-sslserver] session cachesize 40 timeout 7200
[Router-ssl-policy-sslserver] quit
```

步骤 3 配置 HTTPS 服务器。

配置 HTTPS 服务器关联的 SSL 策略为 sslserver。

```
[Router] http secure-server ssl-policy sslserver
```

使能 Router 的 HTTPS 服务器功能。

```
[Router] http secure-server enable
```

配置 HTTPS 服务的端口号。

```
[Router] http secure-server port 1278
```

步骤 4 检查配置结果。

执行命令 **display ssl policy**，查看 SSL 策略 sslserver 的配置信息。

```
<Router> display ssl policy sslserver
-------------------------------------------------------------------------------
  Policy name                    :   sslserver
```

```
  Policy ID                      :   1
  Policy type                    :   Server
  Cache number                   :   40
  Time out(second)               :   7200
  Server certificate load status :   loaded
  Bind number                    :   1
  SSL connection number          :   1
  ------------------------------------------------------------------------
```

用户在终端（比如 PC）打开浏览器，输入网址“https://11.1.1.1:1278”，终端将以 HTTPS 的方式访问 Web 网管页面，用户后续可以利用 Web 网管页面安全访问和管理 Router。

----结束

任务示例

Router 的配置文件。

```
#
 sysname Router
#
interface Ethernet 1/0/0
 ip address 11.1.1.1 255.255.255.0
#
pki entity users
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
#
pki realm users
 ca id ca_root
 enrollment-url http://11.137.145.158:8080/certsrv/mscep/mscep.dll ra
 entity users
 auto-enroll regenerate
 fingerprint sha1 7bb05ada0482273388ed4ec228d79f77309ea3f4
#
ssl policy sslserver type server
 pki-realm users
 session cachesize 40 timeout 7200
#
 http secure-server ssl-policy sslserver
 http secure-server enable
 http secure-server port 1278
#
return
```

11.5.2 配置客户端型 SSL 策略示例

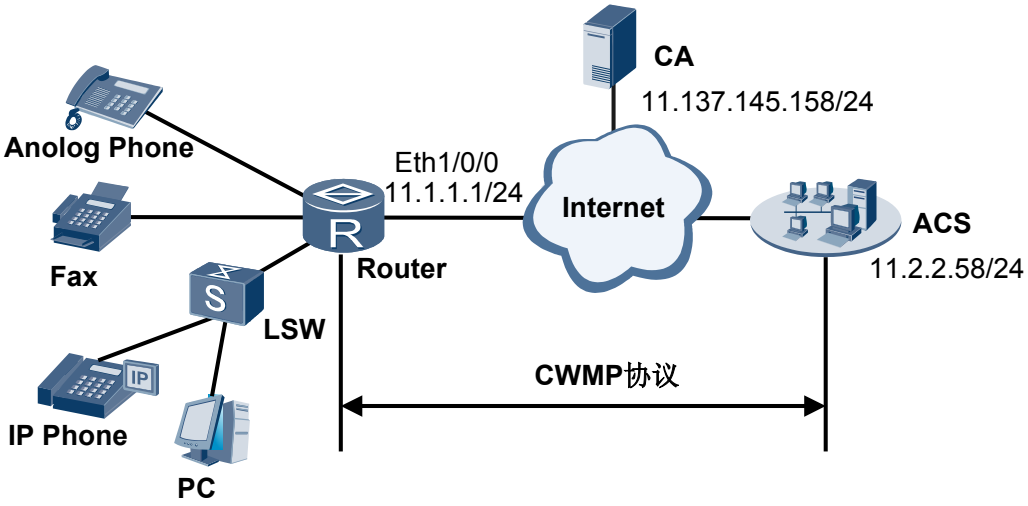
本例以 CWMP 特性为例，通过在作为 CPE 设备的 AR1200 上配置客户端型 SSL 策略，实现 AR1200 对 ACS 的身份验证以及两者之间的安全通信。

组网环境

如图 11-5 所示，Router 作为 CPE 设备，连接电话、传真和交换机。ACS 通过 CWMP 协议完成对 Router 的控制和管理。

已知 ACS 作为 SSL 服务器从 CA 获取数字证书，用户要求在 Router 进行配置，实现 Router 对 ACS 的身份验证，并保证 Router 和 ACS 之间通信的保密性和数据完整性。

图 11-5 配置客户端型 SSL 策略示意图



配置思路

采用如下的配置思路：

1. 在 Router 配置 PKI，包括 PKI 实体和 PKI 域。
2. 在 Router 上配置 SSL 客户端策略，该策略使能基于证书的 SSL 服务器身份验证。
3. 在 Router 上配置 CWMP 的 SSL 功能，其中，配置 CPE 关联 SSL 客户端策略，实现 Router 对 ACS 的身份验证，并保证 Router 和 ACS 之间通信的保密性和数据完整性。
4. 在 Router 上配置 CWMP 的其他功能，包括配置 CWMP 自动连接功能和 CWMP 连接参数，保证 ACS 可以通过 CWMP 协议完成对 Router 的控制和管理。

数据准备

为完成此配置举例，需要准备如下数据：

- PKI 域名：cwmp0
- SSL 客户端策略名称：sslclient
- CA 的 IP 地址：11.137.145.158/24
- ACS 的 URL 地址：https://www.acs.com:80/acs
- PKI 参数:

配置项	数据
PKI 实体	PKI 实体名：cwmp0 ● 实体通用名：hello ● 国家代码：CN ● 所在的州或者省：jiangsu ● 所在的组织：huawei ● 所在的组织部门：info

配置项	数据
PKI 域名	PKI 域名：cwmp0 ● 信任的 CA：ca_root ● 注册证书的 URL：http://11.137.145.158:8080/certsrv/mscep/mscep.dll ra ● 绑定的实体:cwmp0 ● CA 的指纹：采用安全散列算法 指纹值：7bb05ada0482273388ed4ec228d79f77309ea3f4

说明

进行下面的配置之前，需要确保 Router、ACS、CA 之间路由可达。

操作步骤

步骤 1 配置 PKI

配置 PKI 实体

```
<Huawei> system-view
[Huawei] pki entity cwmp0
[Huawei-pki-entity-cwmp0] common-name hello
[Huawei-pki-entity-cwmp0] country cn
[Huawei-pki-entity-cwmp0] state jiangsu
[Huawei-pki-entity-cwmp0] organization huawei
[Huawei-pki-entity-cwmp0] organization-unit info
[Huawei-pki-entity-cwmp0] quit
```

配置 PKI 域，并使能证书自动注册和更新功能

```
[Router] pki realm cwmp0
[Router-pki-realm-cwmp0] entity cwmp0
[Router-pki-realm-cwmp0] ca id ca_root
[Router-pki-realm-cwmp0] enrollment-url http://11.137.145.158:8080/certsrv/mscep/mscep.dll ra
[Router-pki-realm-cwmp0] fingerprint sha1 7bb05ada0482273388ed4ec228d79f77309ea3f4
[Router-pki-realm-cwmp0] auto-enroll regenerate
[Router-pki-realm-cwmp0] quit
```

步骤 2 配置 SSL 客户端策略

使能基于证书的 SSL 服务器身份验证

```
[Router] ssl policy sslclient type client
[Router-ssl-policy-sslclient] server-verify enable
```

配置 SSL 策略使用 PKI 域 cwmp0

```
[Router-ssl-policy-sslclient] pki-realm cwmp0
[Router-ssl-policy-sslclient] quit
```

步骤 3 使能 Router 的 CWMP 功能

```
[Router] cwmp
[Router-cwmp] cwmp enable
```

步骤 4 配置 CWMP 的 SSL 功能

```
[Router-cwmp] cwmp ssl-client ssl-policy sslclient
```

步骤 5 配置 Router 的 CWMP 自动连接功能

配置 Router 连接到 ACS 的 URL

```
[Router-cwmp] cwmp acs url https://www.acs.com:80/acs
```

使能 Router 发送 Inform 报文功能

```
[Router-cwmp] cwmp cpe inform interval enable
```

配置 Router 发送 Inform 报文的时间间隔为 1000 秒

```
[Router-cwmp] cwmp cpe inform interval 1000
```

配置 Router 定时发送 Inform 报文的日期和时间为 2011－01－01 20:00:00

```
[Router-cwmp] cwmp cpe inform time 2011-01-01T20:00:00
```

步骤 6 配置 Router 的 CWMP 连接参数

配置 Router 连接 ACS 的接口

```
[Router-cwmp] cwmp cpe connect interface Ethernet 1/0/0
```

配置 ACS 对 Router 的认证

```
[Router-cwmp] cwmp acs username newacsname
[Router-cwmp] cwmp acs password cipher newacspsw
```

配置 Router 对 ACS 的认证

```
[Router-cwmp] cwmp cpe username newcpename
[Router-cwmp] cwmp cpe password cipher newcpepsw
```

配置 Router 向 ACS 请求连接失败时的重连接次数为 5 次

```
[Router-cwmp] cwmp cpe connect retry 5
```

配置 Router 无数据传输超时时间为 100 秒

```
[Router-cwmp] cwmp cpe wait timeout 100
```

步骤 7 验证配置结果

执行命令 **display current-configuration**，可以看到 CWMP 的 SSL 功能已在 Router 上成功配置。

```
<Router> display current-configuration
...
cwmp
 cwmp cpe inform interval enable
 cwmp acs url https://www.acs.com:80/acs
 cwmp acs username newacsname
 cwmp acs password cipher %$%$"\~.1[)4MGN=d\4zy`$,"ne\%$%
$
 cwmp cpe username newcpename
 cwmp cpe password cipher %$%$"\~.1[)4MGN=d\4zy`$,"ne\%$%
$
 cwmp cpe inform interval 1000
 cwmp cpe connect retry 5
 cwmp cpe wait timeout 100
 cwmp cpe connect interface Ethernet 1/0/0
 cwmp ssl-client ssl-policy sslclient
...
```

执行命令 **display cwmp configuration** 查看 Router 的 CWMP 配置信息，可以看到 CWMP 功能和周期发送 Inform 报文功能都处于 enabled 状态。

```
<Router> display cwmp configuration
  CWMP is enabled
  ACS URL:                              https://www.acs.com:80/acs
  ACS username:                         newacsname
  ACS password:                         %$%$"\~.1[)4MGN=d\4zy`$,"ne\%$%$
  Inform enable status:                 enabled
  Inform interval:                      1000s
  Inform time:                          2011-01-01T20:00:00
  Wait timeout:                         100s
  Reconnection times:                   5
```

执行 **display cwmp status** 查看 Router 的 CWMP 状态信息，可以看到 CWMP 功能处于 enabled 状态，并且 Router 与 ACS 的连接状态为“connected”。

```
<Router> display cwmp status
 CWMP is enabled
 ACS URL:                               https://www.acs.com:80/acs
 Acs information is set by:             user
 ACS username:                          newacsname
 ACS password:                          %$%$.h(P;/FO7%q"9H6D1]/O"90'%$%$
 Connection status:                     connected
 Time of last successful connection:    2010-12-01T20:00:00
```

----结束

任务示例

Router 的配置文件

```
#
 sysname Router
#
interface Ethernet 1/0/0
 ip address 11.1.1.1 255.255.255.0
#
cwmp
 cwmp cpe inform interval enable
 cwmp acs url https://www.acs.com:80/acs
 cwmp acs username newacsname
 cwmp acs password cipher %$%$"\~.1[)4MGN=d\4zy`$,"ne\%$%
$
 cwmp cpe username newcpename
 cwmp cpe password cipher %$%$"\~.1[)4MGN=d\4zy`$,"ne\%$%
$
 cwmp cpe inform interval 1000
 cwmp cpe connect retry 5
 cwmp cpe wait timeout 100
 cwmp cpe connect interface Ethernet 1/0/0
 cwmp ssl-client ssl-policy sslclient
#
pki entity cwmp0
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
#
pki realm cwmp0
 ca id ca_root
 enrollment-url http://11.137.145.158:8080/certsrv/mscep/mscep.dll ra
 entity cwmp0
 auto-enroll regenerate
```

```
 fingerprint sha1 7bb05ada0482273388ed4ec228d79f77309ea3f4
#
ssl policy sslclient type client
 server-verify enable
 pki-realm cwmp0
#
return
```

12 PKI 配置

关于本章

12.1 PKI 概述
PKI（Public Key Infrastructure，公钥基础设施）是一个利用公共密钥理论和技术来实现并提供信息安全服务的具有通用性的安全基础设施。PKI 特性可以为安全协议 IPSec、SSL 提供证书管理机制。

12.2 AR1200 支持的 PKI 特性
AR1200 支持配置 PKI 实体、PKI 域、手工或者自动注册证书、验证证书合法性，同时还支持证书管理，如证书导入导出、删除过期无用的证书。

12.3 配置 PKI 实体
一份证书是一个公开密钥与一个身份的绑定，而身份必须与一个特定的 PKI 实体相关联。PKI 实体标识了一个证书的申请者。

12.4 配置 PKI 域
实体在进行 PKI 证书申请前需要配置一些注册信息来配合完成申请，这些信息的集合就是一个实体的 PKI 域。

12.5 配置证书注册
证书注册就是实体向 CA 自我介绍的过程。实体向 CA 提供身份信息，以及相应的公开密钥，这些信息将成为颁发给该实体证书的主要组成部分。

12.6 配置证书验证
在使用每一个证书之前，必须对证书进行验证。

12.7 管理证书
证书的管理包括证书的删除，证书的导入、导出，配置证书的缺省保存路径等。

12.8 配置举例

12.1 PKI 概述

PKI（Public Key Infrastructure，公钥基础设施）是一个利用公共密钥理论和技术来实现并提供信息安全服务的具有通用性的安全基础设施。PKI 特性可以为安全协议 IPSec、SSL 提供证书管理机制。

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。

数字证书

数字证书是一个经 CA（Certificate Authority，证书机构）签名的、包含公开密钥及相关的用户身份信息的文件，它建立了用户身份信息与用户公钥的关联。CA 对数字证书的签名保证了证书的合法性和权威性。数字证书的格式遵循 ITU-T X.509 国际标准，目前最常用的为 X.509 V3 标准。一个数字证书中包含多个字段，包括证书签发者的名称、主体的公钥信息、CA 对证书的数字签名、证书的有效期等。

本节中涉及三类证书：本地（local）证书、CA（Certificate Authority）证书和设备自签名证书。

- 本地证书：CA 签发给用户的数字证书。
- CA 证书：CA 自身的证书。

  若 PKI 系统中存在多个 CA，则会形成一个 CA 层次结构，最上层的 CA 是根 CA，它拥有一个 CA“自签名”的证书。
- 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。

证书废除列表（CRL，Certificate Revocation List）

由于用户姓名的改变、私钥泄漏或业务中止等原因，需要存在一种方法将现行的证书撤消，即撤消公开密钥及相关的用户身份信息的绑定关系。在 PKI 中，所使用的这种方法为证书废除列表。任何一个证书被废除以后，CA 就要发布 CRL 来声明该证书是无效的，并列出所有被废除的证书的序列号。CRL 提供了一种检验证书有效性的方式。

当一个 CRL 的撤消信息过多时会导致 CRL 的发布规模变得非常庞大，且随着 CRL 大小的增加，网络资源的使用性能也会随之下降。为了避免这种情况，允许一个 CA 的撤消信息通过多个 CRL 发布出来，并且使用 CRL 发布点 CDP（CRL Distribution Point，证书发布点）来指出这些小 CRL 的位置。

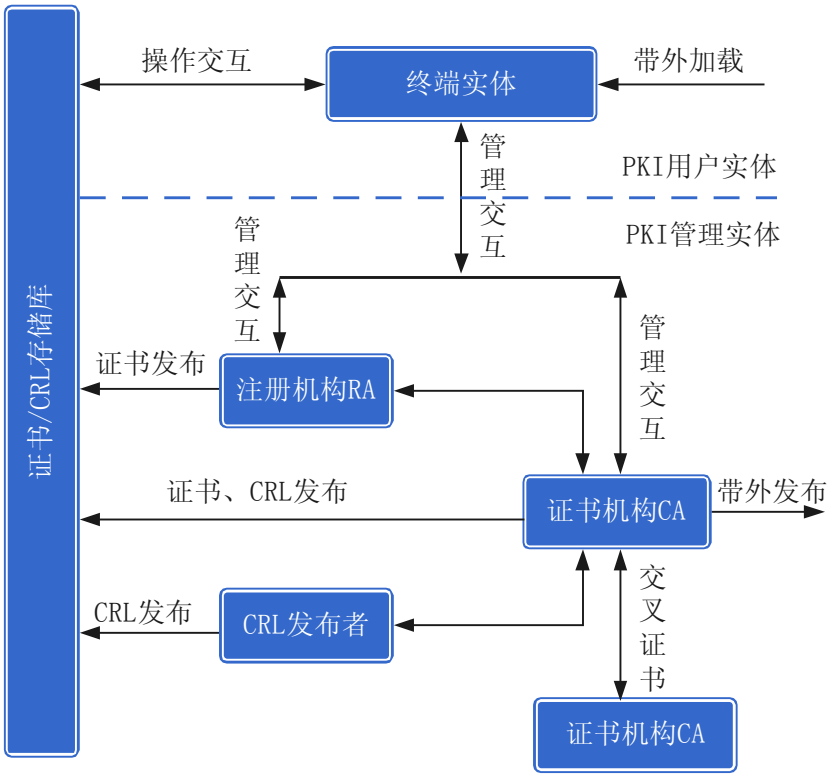
12.2 AR1200 支持的 PKI 特性

AR1200 支持配置 PKI 实体、PKI 域、手工或者自动注册证书、验证证书合法性，同时还支持证书管理，如证书导入导出、删除过期无用的证书。

PKI 架构

PKI 的体系架构如图 12-1。

图 12-1 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。

PKI 工作过程

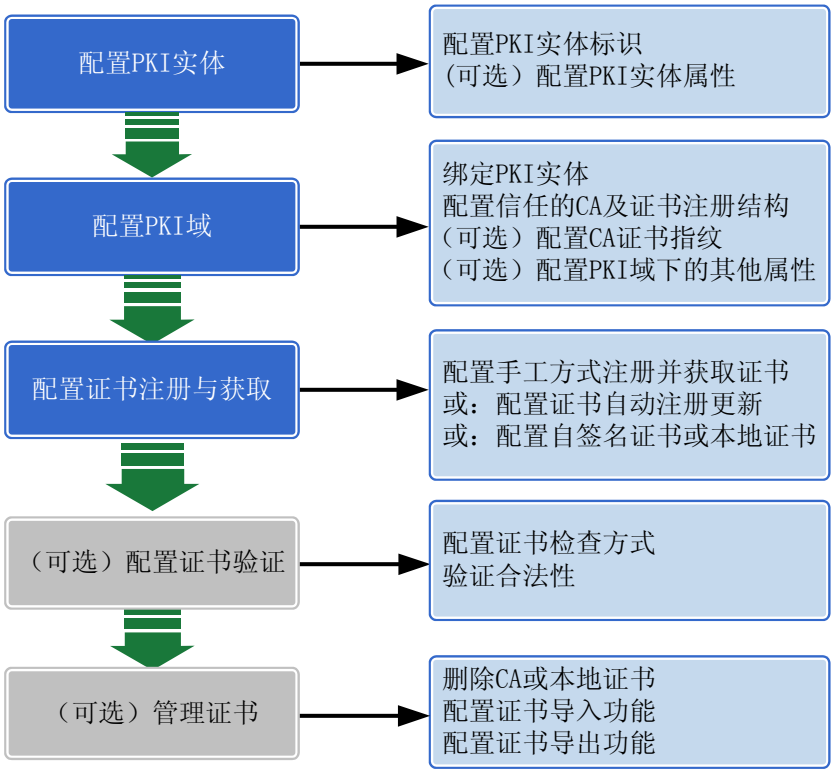
针对一个使用 PKI 的网络，配置 PKI 的目的就是为指定的实体向 CA 申请一个本地证书，并由设备对证书的有效性进行验证。PKI 的工作过程如下：

1. 实体向注册机构 RA 提出证书申请。
2. RA 审核实体身份，将实体身份信息和公开密钥以数字签名的方式发送给 CA。
3. CA 验证数字签名，同意实体的申请，颁发证书。
4. RA 接收 CA 返回的证书，通知实体证书发行成功。
5. 实体获取证书，利用该证书可以与其它实体使用加密、数字签名进行安全通信。
6. 实体希望撤消自己的证书时，向 CA 提交申请。CA 批准实体撤消证书，并更新 CRL。

PKI 配置思路

简要的配置思路如图 12-2 所示：

图 12-2 PKI 配置思路



License 支持

PKI 功能使用 License 授权，缺省情况下，设备的 PKI 功能受限无法使用。如果需要使用 PKI 功能，请联系华为办事处申请并购买如下 License，

- AR1200 安全业务增值包

12.3 配置 PKI 实体

一份证书是一个公开密钥与一个身份的绑定，而身份必须与一个特定的 PKI 实体相关联。PKI 实体标识了一个证书的申请者。

12.3.1 建立配置任务

在配置前了解配置 PKI 实体的应用环境、前置任务和数据准备。

应用环境

一份证书是一个公开密钥与一个身份的绑定，而身份必须与一个特定的 PKI 实体相关联。实体 DN（Distinguished Name，可识别名称）的参数是实体的身份信息，CA 根据实体提供的身份信息来唯一标识证书申请者。

前置任务

无

数据准备

在配置 PKI 实体之前，需准备以下数据。

序号	数据
1	PKI 实体的通用名称、FQDN（Fully Qualified Domain Name，合格域名），两者都唯一标识了一个 PKI 实体，可任配其一，也可两者都配
2	（可选）PKI 实体的国家代码、所属的州、所在的组织名称、部门名称、实体的 IP 地址

12.3.2 配置 PKI 实体标识

配置 PKI 实体的通用名称、FQDN（Fully Qualified Domain Name，合格域名），两者都唯一标识了一个 PKI 实体，可任配其一，也可两者都配。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki entity** *entity-name*，进入 PKI 实体视图。

缺省情况下，AR1200 没有配置 PKI 实体。

步骤 3 执行如下命令，配置 PKI 实体标识。

- 执行命令 **common-name** *common-name*，配置 PKI 实体通用名。

  缺省情况下，AR1200 没有配置通用名。
- 执行命令 **fqdn** *fqdn-name*，配置 PKI 实体合格域名。

  缺省情况下，AR1200 没有配置合格域名。

common-name 和 *fqdn-name* 两者都唯一标识了一个 PKI 实体。两者是或的关系，为了在网络中唯一标识一个 PKI 实体，至少需要配置一个。

----结束

12.3.3 （可选）配置 PKI 实体属性

除了配置通用名或者合格域名外，PKI 特性还支持配置 PKI 实体的国家代码、所在的州或者省、所在的组织、部门名称等，对实体的身份进行补充说明。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki entity** *entity-name*，进入 PKI 实体视图。

步骤 3 执行命令 **country** *country-code*，配置 PKI 实体的国家代码。

缺省情况下，AR1200 没有配置国家代码。

步骤 4 执行命令 **state** *state-name*，配置 PKI 实体所在的州或者省。

缺省情况下，AR1200 没有配置 PKI 实体所属的州或者省。

步骤 5 执行命令 **organization** *organization-name*，配置实体所在的组织。

缺省情况下，AR1200 没有配置 PKI 实体的组织名称。

步骤 6 执行命令 **organization-unit** *organization-unit-name*，配置实体所在的部门。

缺省情况下，AR1200 没有配置 PKI 实体的部门名称。

步骤 7 执行命令 **ip-address** *ip-address*，配置实体的 IP 地址。

缺省情况下，AR1200 没有配置 PKI 实体的 IP 地址。

----结束

12.3.4 检查配置结果

配置完 PKI 实体后，查看配置的 PKI 实体信息。

操作步骤

- 执行命令 **display pki entity** [*entity-name*]，查看 PKI 实体信息。

----结束

12.4 配置 PKI 域

实体在进行 PKI 证书申请前需要配置一些注册信息来配合完成申请，这些信息的集合就是一个实体的 PKI 域。

12.4.1 建立配置任务

在配置前了解配置 PKI 域的应用环境、前置任务和数据准备。

应用环境

PKI 域是 PKI 实体注册证书所需信息的集合。PKI 域是一个本地概念，创建 PKI 域的目的是便于其它应用引用 PKI 的配置，比如 IKE、SSL 等。一个设备上配置的 PKI 域对 CA 和其它设备是不可见的，每一个 PKI 域有单独的域参数配置信息。

前置任务

已经完成 PKI 实体的创建。

数据准备

在配置 PKI 域之前，需准备以下数据。

序号	数据
1	PKI 域名
2	绑定的 PKI 实体名称
3	信任的 CA 名称、注册证书的 URL
4	（可选）CA 证书指纹
5	（可选）证书吊销时使用的密码、RSA 密钥长度、建立 TCP 连接使用的源 IP 地址

12.4.2 创建 PKI 域

PKI 域是实体注册证书所需信息的集合，创建 PKI 域后便于其它应用引用 PKI 的配置，比如 IKE、SSL 等。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki realm** *realm-name*，创建 PKI 域。

缺省情况下，AR1200 没有创建 PKI 域。

----结束

12.4.3 配置申请证书的 PKI 实体

PKI 域下需要指定申请证书的 PKI 实体，且只能绑定一个 PKI 实体。

背景信息

向 CA 发送证书申请请求时，必须指定所使用的实体名，以向 CA 表明自己的身份。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki realm** *realm-name*，配置 PKI 域。

缺省情况下，AR1200 没有配置 PKI 域。

步骤 3 执行命令 **entity** *entity-name*，指定申请证书的 PKI 实体。

缺省情况下，AR1200 没有指定 PKI 实体。

----结束

12.4.4 配置设备信任的 CA 及证书注册机构

在申请证书时，是通过一个可信实体认证机构，来完成实体证书的注册颁发功能的，因此必须指定一个信任的 CA 名称和注册证书的 URL。

背景信息

证书申请的受理一般由一个独立的注册机构（即 RA）来承担，它接收用户的注册申请，审查用户的申请资格，并决定是否同意 CA 给其签发数字证书。注册机构并不给用户签发证书，而只是对用户进行资格审查。有时 PKI 把注册管理的职能交给 CA 来完成，而不设立独立运行的 RA，但这并不是取消了 PKI 的注册功能，而只是将其作为 CA 的一项功能而已。

证书申请之前必须指定注册服务器的 URL，随后实体可通过 SCEP（Simple Certificate Enrollment Protocol，简单证书注册协议）向该服务器提出证书申请，SCEP 是专门用于与认证机构进行通信的协议。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki realm** *realm-name*，配置 PKI 域。

缺省情况下，AR1200 没有配置 PKI 域。

步骤 3 执行命令 **ca id** *ca-name*，配置 PKI 域信任的 CA。

缺省情况下，AR1200 没有配置 PKI 域信任的 CA。

步骤 4 执行命令 **enrollment-url** *url* [**interval** *minutes*] [**times** *count*] [**ra**]，配置证书注册服务器的 URL。

缺省情况下，AR1200 没有指定注册服务器的 URL。

----结束

12.4.5 （可选）配置 CA 证书指纹

当设备从 CA 获得根证书时，需要验证 CA 根证书的指纹，即根证书内容的散列值，该值对于每一个证书都是唯一的。如果 CA 根证书的指纹与在 PKI 域中配置的指纹不同，则设备将拒绝接收根证书。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki realm** *realm-name*，配置 PKI 域。

缺省情况下，AR1200 没有配置 PKI 域。

步骤 3 执行命令 **fingerprint** { **md5** | **sha1** } *fingerprint*，配置对 CA 证书进行认证时使用的 CA 证书指纹。

CA 证书指纹通过带外方式（如 email 等）发送给设备。缺省情况下，AR1200 没有配置指纹。

----结束

12.4.6 （可选）配置证书吊销密码

在吊销证书时设置密码，防止用户误吊销证书，提高了用户操作的安全性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki realm** *realm-name*，配置 PKI 域。

缺省情况下，AR1200 没有配置 PKI 域。

步骤 3 执行命令 **password** [**cipher**] *password*，配置证书吊销时使用的密码。

缺省情况下，AR1200 没有配置密码。

----结束

12.4.7 （可选）配置设备证书的 RSA 密钥长度

配置 PKI 设备证书的 RSA 密钥长度后，在申请设备证书时，将生成指定长度的 RSA 密钥为证书密钥。

背景信息

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。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki realm** *realm-name*，配置 PKI 域。

缺省情况下，AR1200 没有配置 PKI 域。

步骤 3 执行命令 **rsa-key-size** *size*，配置 PKI 设备证书的 RSA 密钥长度。

缺省情况下，AR1200 的 RSA 密钥长度为 1024。

----结束

12.4.8 （可选）配置 TCP 连接使用的源接口

配置建立 TCP 连接使用的源接口，该接口的 IP 地址作为设备与 SCEP、OCSP 服务器建立 TCP 连接的源 IP 地址。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki realm** *realm-name*，配置 PKI 域。

缺省情况下，AR1200 没有配置 PKI 域。

步骤 3 执行命令 **source interface** *interface-name*，配置建立 TCP 连接使用的源 IP 地址。

缺省情况下，AR1200 使用出接口的 IP 地址作为 TCP 连接的源 IP 地址。

----结束

12.4.9 检查配置结果

配置完 PKI 域后，查看 PKI 域的相关信息。

操作步骤

- 执行命令 **display pki realm** [*pki-realm-name*]，查看 PKI 域的相关信息。

----结束

12.5 配置证书注册

证书注册就是实体向 CA 自我介绍的过程。实体向 CA 提供身份信息，以及相应的公开密钥，这些信息将成为颁发给该实体证书的主要组成部分。

12.5.1 建立配置任务

在配置前了解证书注册的应用环境、前置任务和数据准备。

应用环境

证书注册申请有如下几种方式：

- 手工注册申请：手工触发设备去 CA 服务器注册证书。
- 自动注册更新：证书注册需要的配置信息齐全并且本地没有证书时，将自动触发设备通过 SCEP 协议去 CA 服务器申请证书。
- 设备自身创建：PKI 设备为自己颁发的自签名证书。

前置任务

- PKI 实体已经创建完成。
- PKI 域已经创建完成。

数据准备

在配置证书注册前，需准备以下数据。

序号	数据
1	申请证书的 PKI 域名、（可选）证书申请信息保存的文件名称（PKCS#10 格式）
2	（可选）证书有效期的百分比
3	自签名证书文件的名称

12.5.2 配置手工方式注册证书

手工方式向 CA 注册证书分为在线申请和离线申请两种。离线申请方式下，CA 允许申请方通过带外方式（如电话、磁盘、电子邮件等）向 CA 提供申请信息。

前提条件

PKI 域已经创建并配置完成，具体请参见 **12.4 配置 PKI 域**。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki enroll-certificate** *pki-realm-name* [**pkcs10** [**filename** *filename*]]，配置手工触发设备注册证书。

配置 **pkcs10** 表示离线方式下的证书申请，即用户以 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。

不配置 **pkcs10** 表示在线申请证书。

步骤 3 （可选）执行命令 **pki get-certificate** { **ca** | **local** } *pki-realm-name*，获取证书。

手工注册证书时，CA 证书和设备证书会被自动下载保存在设备缺省路径下。如果用户误操作删除了 CA 证书或设备证书，可以通过本命令从 CA 服务器重新获取证书。

----结束

12.5.3 配置证书自动注册和更新

配置证书自动注册功能，如果证书注册需要的配置信息齐全并且本地没有证书时，将自动触发设备通过 SCEP 协议申请证书；或者当证书即将过期、已经过期、已到达指定百分比时，自动触发设备通过 SCEP 协议申请并更新证书。

前提条件

PKI 域已经创建并配置完成，具体请参见 **12.4 配置 PKI 域**。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki realm** *realm-name*，配置 PKI 域。

缺省情况下，AR1200 没有配置 PKI 域。

步骤 3 执行命令 **auto-enroll** [*percent*] [**regenerate**]，使能实体证书自动注册和更新功能。

配置证书自动注册和更新功能后，则不需要手工下载证书。当有外部应用需要 CA 证书或者设备证书时，将自动触发下载 CA 证书和设备证书。

----结束

12.5.4 配置设备创建自签名证书或本地证书

用户通过 PKI 设备生成自签名证书或设备本地证书，实现简单的证书颁发功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki create-certificate** [**self-signed**] { **filename** *file-name* }，配置自签名证书或设备本地证书。

----结束

12.5.5 检查配置结果

从 CA 服务器获取证书到本地后，或者用户创建完自签名证书或本地证书，查看证书信息。

操作步骤

- 执行命令 **display pki certificate** { **local** | **ca** } *pki-realm-name* [**verbose**]，查看本地或 CA 证书信息。
- 执行命令 **display pki certificate enroll-status** *pki-realm-name*，查看证书的注册状态。

----结束

12.6 配置证书验证

在使用每一个证书之前，必须对证书进行验证。

12.6.1 建立配置任务

在配置前了解证书验证的应用环境、前置任务和数据准备。

应用环境

在使用每一个证书之前，必须对证书进行验证。证书验证包括对签发时间、签发者信息以及证书的有效性几方面进行验证。证书验证的核心是检查 CA 在证书上的签名，并确定证书仍在有效期内，而且未被废除。

证书验证有三种方式：

- CRL 方式：通过 CRL（Certificate Revocation List，证书吊销列表）检查证书的有效性。
- OCSP 方式：通过 OCSP（Online Certificate Status Protocol，在线证书状态协议）服务器检查证书的有效性。
- None 方式：不检查对端证书状态。

前置任务

已经完成证书注册与获取。

数据准备

在配置证书验证之前，需准备以下数据。

序号	数据
1	证书验证的 PKI 域名

序号	数据
2	（可选）cdp-url、PKI 实体从 CRL 存储服务器下载 CRL 的时间间隔
3	（可选）OCSP 服务器的 URL

12.6.2 配置证书状态检查方式

证书状态检查方式有 3 种：CRL 方式、OCSP 方式及不检查，用户可根据情况配置相应的检查方式。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki realm** *realm-name*，配置 PKI 域。

缺省情况下，AR1200 没有配置 PKI 域。

步骤 3 执行命令 **certificate-check** { **crl** | **none** | **ocsp** }，配置验证证书状态的检查方式。

缺省情况下，AR1200 采用 CRL 检查方式。

- 配置 CRL 方式检查，则每次证书验证时都会自动从 CA 服务器下载 CRL：
  - 执行命令 **cdp-url** *cdp-url*，配置获取 CA 发布的 CRL 文件的 HTTP URL 地址。

    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。PKI 实体利用 CDP 中指定的机制来下载 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，PKI 实体使用配置的 URL 来获取 CRL。
  - 执行命令 **crl cache**，表示可以使用缓存的 CRL，不需要每次都去 CA 服务器下载 CRL。
  - 执行命令 **crl update-period** *hours*，配置 PKI 实体从 CRL 存储服务器下载 CRL 的时间间隔。
  - 执行命令 **quit**，返回系统视图。
  - 如果用户怀疑本地缓存的 CRL 内容过期，执行命令 **pki get-crl** *pki-realm-name*，手工下载 CA 服务器上最新的 CRL，并替换原来的 CRL。
- 配置 OCSP 方式检查
  - 执行命令 **ocsp-url** *ocsp-url*，配置 OCSP 服务器的 URL。

    该 URL 地址将覆盖证书中携带的 OCSP 服务器的地址。

----结束

12.6.3 配置检查证书的合法性

配置完证书状态检查方式后，验证证书的合法性。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki validate-certificate** { **ca** | **local** } *pki-realm-name*，检查 CA 证书或本地证书的有效性。

----结束

12.6.4 检查配置结果

验证完证书状态后，查看验证结果。

操作步骤

- 执行命令 **display pki certificate enroll-status** *pki-realm-name*，查看证书的注册状态。
- 执行命令 **display pki crl** *pki-realm-name*，查看存储在本地的 CRL 内容。

----结束

12.7 管理证书

证书的管理包括证书的删除，证书的导入、导出，配置证书的缺省保存路径等。

12.7.1 删除证书

证书过期或希望重新申请证书时，可以删除已经存在的证书。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki delete-certificate** { **ca** | **local** | **ocsp** } *pki-realm-name*，删除保存的证书。

----结束

12.7.2 配置证书导入功能

用户想通过带外方式把外部证书拷贝到设备存储器中，然后导入供设备使用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki import-certificate** { **ca** | **local** | **ocsp** } *pki-realm-name* { **der** | **pkcs12** | **pem** }，将外部证书导入到设备中。

----结束

12.7.3 配置证书导出功能

用户如果需要把证书导出供其他设备使用时，配置证书导出功能。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki export-certificate** { **ca** | **local** | **ocsp** } *pki-realm-name* { **der** | **pkcs12** | **pem** }，将证书导出保存到其他文件中。

----结束

12.7.4 配置证书缺省保存路径

配置缺省情况下，证书文件的保存路径。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **pki credential-storage** *local-dir*，配置保存 CA 证书、设备证书和私钥的缺省位置和目录。

缺省情况下，保存在 flash：/目录下。

----结束

12.8 配置举例

12.8.1 配置 PKI 实体手工注册证书的示例

组网需求

配置 PKI 实体 Router 向 CA 服务器申请设备证书。

图 12-3 PKI 实体向 CA 申请证书组网图

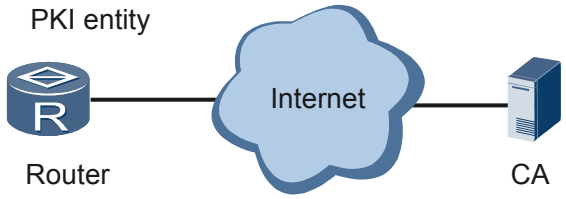


表 12-1 数据规划表

配置项	数据
PKI 实体	PKI 实体名：user01 ● 实体通用名：hello ● 国家代码：CN ● 所在的州或者省：jiangsu ● 所在的组织：huawei ● 所在的组织部门：info
PKI 域名	PKI 域名：test ● 信任的 CA：ca_root ● 注册证书的 URL：http://10.137.145.158:8080/certsrv/mscep/mscep.dll ● 绑定的实体:user01 ● CA 的指纹：采用安全散列算法 指纹值：17A34D94624B1C1BCBF6D763C4A67035D5B578EAF

配置思路

1. 配置 PKI 实体，标识一个申请证书的实体的身份。
2. 配置 PKI 域，通过 PKI 域的形式，把 PKI 实体进行证书注册需要配置的一些注册信息组织起来，包括信任的 CA、绑定的实体、证书注册的 URL 及 CA 证书的指纹等。
3. 手工注册证书。

操作步骤

步骤 1 配置接口的 IP 地址和路由，使得 PKI 实体和 CA 服务器之间路由可达。

步骤 2 配置 PKI 实体，标识申请证书实体的身份信息。

配置实体为 user01。

```
<Huawei> system-view
[Huawei] pki entity user01
[Huawei-pki-entity-user01] common-name hello
[Huawei-pki-entity-user01] country cn
[Huawei-pki-entity-user01] state jiangsu
[Huawei-pki-entity-user01] organization huawei
[Huawei-pki-entity-user01] organization-unit info
[Huawei-pki-entity-user01] quit
```

步骤 3 配置 PKI 域，配置证书注册需要的信息。

配置信任的 CA、绑定的实体、注册证书的 URL、CA 证书指纹

```
[Huawei] pki realm test
[Huawei-pki-realm-test] ca id ca_root
[Huawei-pki-realm-test] entity user01
```

```
[Huawei-pki-realm-test] enrollment-url http://10.137.145.158:8080/certsrv/mscep/mscep.dll ra
[Huawei-pki-realm-test] fingerprint sha1 7A34D94624B1C1BCBF6D763C4A67035D5B578EAF
[Huawei-pki-realm-test] quit
```

步骤 4 手工注册证书。

```
[Huawei] pki enroll-certificate test
 Create a challenge password. You will need to verbally provide this password to
 the CA Administrator in order to revoke your certificate.
 For security reasons your password will not be saved in the configuration. Plea
se make a note of it.
 Choice no password ,please enter the enter-key.
 Please enter Password:
 Start certificate enrollment ...
 Certificate is enrolling now,It will take a few minutes or more.
 Please waiting...
 The certificate enroll successful.
```

证书注册过程中会提示输入密码，如果不配置密码，按回车键继续。

步骤 5 验证配置结果

此时，在 CA 服务器上会看到颁发给实体的证书。在证书的常规信息中，“颁发给”字段值为实体通用名 *hello*。

在申请证书的实体上，执行命令 **display pki certificate** { **local** | **ca** } *pki-realm-name* [**verbose**]，查看获取的设备证书。

```
<Huawei> display pki certificate local test
Certificate
  Status : Available
  Version: 3
  Serial Number:
    19 36 41 af 00 00 00 00 02 ba
  Subject:
    C=CN
    ST=jiangsu
    O=huawei
    OU=info
    CN=hello

  Associated Pki Realm : test

Total Number: 1
```

----结束

配置文件

```
#
pki entity user01
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
#
pki realm test
 ca id ca_root
 enrollment-url http://10.137.145.158:8080/certsrv/mscep/mscep.dll ra
 entity user01
 fingerprint sha1 7a34d94624b1c1bcbf6d763c4a67035d5b578eaf
#
return
```

12.8.2 配置 IPSec 应用 PKI 的示例

组网需求

如图 12-4 所示，两个子网通过各自的网关设备与外部网络互联，希望通过 IPsec 隧道建立数据流的安全通道，具体需求如下：

- 在网关设备之间建立一个 IPsec 安全隧道，对子网 Group 1（10.1.1.0/24）与子网 Group 2（11.1.1.0/24）之间的数据流进行安全保护。
- 在网关设备之间使用 IKE 自动协商建立安全通道，IKE 自动协商采用基于 PKI 证书的身份认证方式。

图 12-4 配置 IPSec 应用 PKI 的组网图

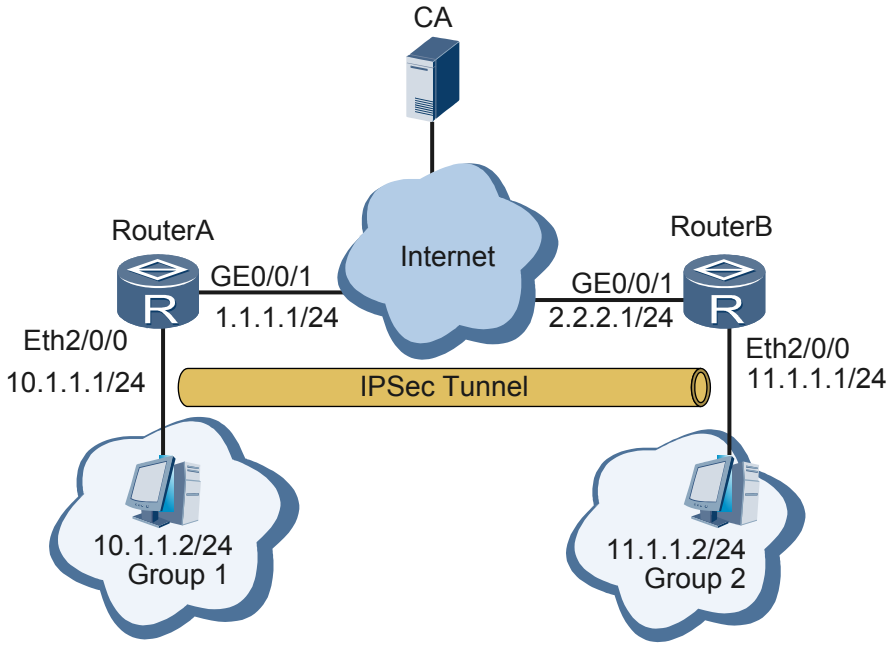


表 12-2 RouterA 数据规划表

配置项	数据
PKI 实体	PKI 实体名：routera ● 实体通用名：helloa ● 国家代码：CN ● 所在的州或者省：jiangsu ● 所在的组织：huawei ● 所在的组织部门：info

配置项	数据
PKI 域名	PKI 域名：testa ● 信任的 CA：ca_root ● 注册证书的 URL：http://10.137.145.158:8080/certsrv/mscep/mscep.dll ● 绑定的实体:routera ● CA 的指纹：采用安全散列算法 指纹值：17A34D94624B1C1BCBF6D763C4A67035D5B578EAF
IKE 安全提议	● 加密算法：3des-cbc ● 认证算法：sha1 ● 认证模式：rsa-signature
IKE Peer	● IKE Peer 名：routera ● 本地 Peer 的 ID 类型：IP ● 本端地址：1.1.1.1 ● 远端地址：2.2.2.1 ● 协商模式：主模式
IPSec 安全提议	● 传输协议：esp ● 认证算法：sha1 ● 加密算法：3des ● 封装模式：隧道模式
IPSec 安全策略	SA 触发模式：自动

表 12-3 RouterB 数据规划表

配置项	数据
PKI 实体	PKI 实体名：routerb ● 实体通用名：hellob ● 国家代码：CN ● 所在的州或者省：jiangsu ● 所在的组织：huawei ● 所在的组织部门：marketing

配置项	数据
PKI 域名	PKI 域名：testb ● 信任的 CA：ca_root ● 注册证书的 URL：http://10.137.145.158:8080/certsrv/mscep/mscep.dll ● 绑定的实体:routerb ● CA 的指纹：采用安全散列算法 指纹值：17A34D94624B1C1BCBF6D763C4A67035D5B578EAF
IKE 安全提议	● 加密算法：3des-cbc ● 认证模式：rsa-signature ● 认证算法：sha1
IKE Peer	● IKE Peer 名：routerb ● 协商模式：主模式 ● 本地 Peer 的 ID 类型：IP ● 本端地址：2.2.2.1 ● 远端地址：1.1.1.1
IPSec 安全提议	● 传输协议：esp ● 认证算法：sha1 ● 加密算法：3des ● 封装模式：隧道模式
IPSec 安全策略	SA 触发模式：自动

配置思路

1. 配置 PKI 实体，标识实体的身份信息。
2. 配置 PKI 域，配置证书注册需要的信息。
3. 配置 IKE，使用数字签名进行身份认证。
4. 配置 IPSec，对两个子网之间的数据流进行保护。
5. 申请证书，并将证书下载到本地，以供 IKE 协商时使用。

操作步骤

步骤 1 配置接口 IP 地址和路由，使得 IPSec 对等体、CA 服务器之间路由可达。

步骤 2 配置 PKI 实体，分别在 RouterA 和 RouterB 上进行如下配置。

#RouterA 的配置。

```
<Huawei> system-view
[Huawei] pki entity routera
[Huawei-pki-entity-routera] common-name helloa
```

```
[Huawei-pki-entity-routera] country cn
[Huawei-pki-entity-routera] state jiangsu
[Huawei-pki-entity-routera] organization huawei
[Huawei-pki-entity-routera] organization-unit info
[Huawei-pki-entity-routera] quit
```

#RouterB 的配置。

```
<Huawei> system-view
[Huawei] pki entity routerb
[Huawei-pki-entity-routerb] common-name hellob
[Huawei-pki-entity-routerb] country cn
[Huawei-pki-entity-routerb] state jiangsu
[Huawei-pki-entity-routerb] organization huawei
[Huawei-pki-entity-routerb] organization-unit marketing
[Huawei-pki-entity-routerb] quit
```

步骤 3 配置 PKI 域，分别在 RouterA 和 RouterB 上进行如下配置。

#RouterA 的配置。

```
[Huawei] pki realm testa
[Huawei-pki-realm-testa] ca id ca_root
[Huawei-pki-realm-testa] entity routera
[Huawei-pki-realm-testa] enrollment-url http://10.137.145.158:8080/certsrv/mscep/mscep.dll ra
[Huawei-pki-realm-testa] fingerprint sha1 7A34D94624B1C1BCBF6D763C4A67035D5B578EAF
[Huawei-pki-realm-testa] certificate-check none
[Huawei-pki-realm-testa] quit
```

#RouterB 的配置。

```
[Huawei] pki realm testb
[Huawei-pki-realm-testb] ca id ca_root
[Huawei-pki-realm-testb] entity routerb
[Huawei-pki-realm-testb] enrollment-url http://10.137.145.158:8080/certsrv/mscep/mscep.dll ra
[Huawei-pki-realm-testb] fingerprint sha1 7A34D94624B1C1BCBF6D763C4A67035D5B578EAF
[Huawei-pki-realm-testb] certificate-check none
[Huawei-pki-realm-testb] quit
```

步骤 4 配置 IKE，使用数字签名进行身份认证。分别在 RouterA 和 RouterB 上进行如下配置。

#RouterA 的配置。

```
[Huawei] ike proposal 1
[Huawei-ike-proposal-1] encryption-algorithm 3des-cbc
[Huawei-ike-proposal-1] authentication-method rsa-signature
[Huawei-ike-proposal-1] authentication-algorithm sha1
[Huawei-ike-proposal-1] quit
[Huawei] ike peer routera v2
[Huawei-ike-peer-routera] ike-proposal 1
[Huawei-ike-peer-routera] local-address 1.1.1.1
[Huawei-ike-peer-routera] remote-address 2.2.2.1
[Huawei-ike-peer-routera] pki realm testa
```

#RouterB 的配置。

```
[Huawei] ike proposal 1
[Huawei-ike-proposal-1] encryption-algorithm 3des-cbc
[Huawei-ike-proposal-1] authentication-method rsa-signature
[Huawei-ike-proposal-1] authentication-algorithm sha1
[Huawei-ike-proposal-1] quit
[Huawei] ike peer routerb v2
[Huawei-ike-peer-routerb] ike-proposal 1
[Huawei-ike-peer-routerb] local-address 2.2.2.1
[Huawei-ike-peer-routerb] remote-address 1.1.1.1
[Huawei-ike-peer-routerb] pki realm testb
```

步骤 5 配置 ACL，定义受保护的数据流。分别在 RouterA 和 RouterB 上进行如下配置。

#RouterA 的配置。

```
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 5 permit ip source 1.1.1.1 0 destination 2.2.2.1 0
[Huawei-acl-adv-3000] rule 15 permit ip source 10.1.1.1 0 destination 11.1.1.1 0
[Huawei-acl-adv-3000] quit
```

#RouterB 的配置。

```
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 5 permit ip source 2.2.2.1 0 destination 1.1.1.1 0
[Huawei-acl-adv-3000] rule 10 permit ip source 11.1.1.1 0 destination 10.1.1.1 0
[Huawei-acl-adv-3000] quit
```

步骤 6 配置 IPSec，对两个子网之间的数据流进行保护。分别在 RouterA 和 RouterB 上进行如下配置。

#RouterA 的配置。

```
[Huawei] ipsec proposal routera
[Huawei-ipsec-proposal-routera] transform esp
[Huawei-ipsec-proposal-routera] esp authentication-algorithm sha1
[Huawei-ipsec-proposal-routera] esp encryption-algorithm 3des
[Huawei-ipsec-proposal-routera] quit
[Huawei] ipsec policy routera 1 isakmp
[Huawei-ipsec-policy-isakmp-routera-1] security acl 3000
[Huawei-ipsec-policy-isakmp-routera-1] ike-peer routera
[Huawei-ipsec-policy-isakmp-routera-1] proposal routera
[Huawei-ipsec-policy-isakmp-routera-1] quit
```

#RouterB 的配置。

```
[Huawei] ipsec proposal routerb
[Huawei-ipsec-proposal-routerb] transform esp
[Huawei-ipsec-proposal-routerb] esp authentication-algorithm sha1
[Huawei-ipsec-proposal-routerb] esp encryption-algorithm 3des
[Huawei-ipsec-proposal-routerb] quit
[Huawei] ipsec policy routerb 1 isakmp
[Huawei-ipsec-policy-isakmp-routerb-1] security acl 3000
[Huawei-ipsec-policy-isakmp-routerb-1] ike-peer routerb
[Huawei-ipsec-policy-isakmp-routerb-1] proposal routerb
[Huawei-ipsec-policy-isakmp-routerb-1] quit
```

步骤 7 在接口下绑定 IPSec 策略，分别在 RouterA 和 RouterB 上进行如下配置。

#RouterA 的配置。

```
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ipsec policy routera
[Huawei-GigabitEthernet0/0/1] quit
```

#RouterB 的配置。

```
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ipsec policy routerb
[Huawei-GigabitEthernet0/0/1] quit
```

步骤 8 申请证书，并将证书下载到本地，以供 IKE 协商时使用。分别在 RouterA 和 RouterB 上进行如下配置。

#RouterA 的配置。

```
[Huawei] pki enroll-certificate testa
 Create a challenge password. You will need to verbally provide this password to
 the CA Administrator in order to revoke your certificate.
 For security reasons your password will not be saved in the configuration. Plea
se make a note of it.
 Choice no password ,please enter the enter-key.
 Please enter Password:
```

```
 Start certificate enrollment ...
 Certificate is enrolling now,It will take a few minutes or more.
 Please waiting...
 The certificate enroll successful.
```

#RouterB 的配置。

```
[Huawei] pki enroll-certificate testb
 Create a challenge password. You will need to verbally provide this password to
  the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration. Plea
se make a note of it.
 Choice no password ,please enter the enter-key.
 Please enter Password:
 Start certificate enrollment ...
 Certificate is enrolling now,It will take a few minutes or more.
 Please waiting...
 The certificate enroll successful.
```

步骤 9 验证配置结果。

在 RouterA 和 RouterB 上查看 IKE SA，发现已经成功建立 IKE SA，并且可以 ping 通对端。

RouterA 上的结果如下：

```
[Huawei] display ike sa v2
    Conn-ID  Peer            VPN   Flag(s)                 Phase
  -----------------------------------------------------------------
       898    2.2.2.1         0     RD|ST                   2
       895    2.2.2.1         0     RD|ST                   1

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP

[Huawei]
```

RouterB 上的结果如下：

```
[Huawei] display ike sa v2
    Conn-ID  Peer            VPN   Flag(s)                 Phase
  -----------------------------------------------------------------
       874    1.1.1.1         0     RD                      2
       873    1.1.1.1         0     RD                      1

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
```

在 RouterA 上 ping 对端 Peer，能够 ping 通。

```
[Huawei] ping 2.2.2.1
  PING 2.2.2.1: 56  data bytes, press CTRL_C to break
    Reply from 2.2.2.1: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 2.2.2.1: bytes=56 Sequence=2 ttl=255 time=2 ms
    Reply from 2.2.2.1: bytes=56 Sequence=3 ttl=255 time=2 ms
    Reply from 2.2.2.1: bytes=56 Sequence=4 ttl=255 time=2 ms
    Reply from 2.2.2.1: bytes=56 Sequence=5 ttl=255 time=2 ms

  --- 2.2.2.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/3 ms
```

说明

IKE 协商的时候，如果 RouterA 和 RouterB 还未获得 CA 证书和本地证书，则会出现 IKE 初次协商失败的情况。

----结束

配置文件

RouterA 的配置

```
#
router id 1.1.1.1
#
acl number 3000
 rule 5 permit ip source 1.1.1.1 0 destination 2.2.2.1 0
 rule 15 permit ip source 10.1.1.1 0 destination 11.1.1.1 0
#
ipsec proposal routera
 esp authentication-algorithm sha1
 esp encryption-algorithm
3des
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-method rsa-signature
#
ike peer routera v2
 ike-proposal 1
 local-address 1.1.1.1
 remote-address 2.2.2.1
 pki realm testa
#
ipsec policy routera 1 isakmp
 security acl 3000
 ike-peer routera
 proposal routera
#
interface Ethernet2/0/0
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 1.1.1.1 255.255.255.0
 ipsec policy routera
#
ospf 1
 area 0.0.0.0
  network 1.1.1.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
#
pki entity routera
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name helloa
#
pki realm testa
 ca id ca_root
 enrollment-url http://10.137.145.158:8080/certsrv/mscep/mscep.dll ra
 entity routera
 fingerprint sha1 7a34d94624b1c1bcbf6d763c4a67035d5b578eaf
 certificate-check none
#
return
```

RouterB 的配置

```
#
router id 3.3.3.3
#
acl number 3000
 rule 5 permit ip source 2.2.2.1 0 destination 1.1.1.1 0
 rule 10 permit ip source 11.1.1.1 0 destination 10.1.1.1 0
#
ipsec proposal routerb
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ike proposal 1
 encryption-algorithm 3des-cbc
 authentication-method rsa-signature
#
ike peer routerb v2
 ike-proposal 1
 local-address 2.2.2.1
 remote-address 1.1.1.1
 pki realm testb
#
ipsec policy routerb 1 isakmp
 security acl 3000
 ike-peer routerb
 proposal routerb
#
interface Ethernet2/0/0
 ip address 11.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 2.2.2.1 255.255.255.0
 ipsec policy routerb
#
ospf 1
 area 0.0.0.0
  network 2.2.2.0 0.0.0.255
  network 11.1.1.0 0.0.0.255
#
pki entity routerb
 country CN
 state jiangsu
 organization huawei
 organization-unit marketing
 common-name hellob
#
pki realm testb
 ca id ca_root
 enrollment-url http://10.137.145.158:8080/certsrv/mscep/mscep.dll ra
 entity routerb
 fingerprint sha1 7a34d94624b1c1bcbf6d763c4a67035d5b578eaf
 certificate-check none
#
return
```

13 Keychain 配置

关于本章

Keychain 在不中断连接的情况下，通过动态改变路由器之间认证加密的密钥和加密算法，提高控制层面的安全可靠性。

13.1 Keychain 概述

13.2 AR1200 支持的 Keychain 特性

13.3 配置 Keychain 的基本功能
本节介绍 Keychain 基本功能的配置方法。

13.4 配置 TCP 认证参数
本节介绍在 Keychain 模块中如何配置 TCP 认证的参数。

13.5 配置举例

13.1 Keychain 概述

Keychain 提供对所有应用层协议的认证，并且 keychain 能够在不丢包的情况下，动态更改密码链。

为了安全，在网络上需要不断对应用层的认证信息进行更改。通过认证算法和共享安全密钥共同决定信息在不安全的网络上进行传输时是否被篡改。这种认证方式对数据进行认证时，需要数据发送者和接收者之间共享安全密钥和认证算法，并且密钥不能在网络上进行传输。

如果每个应用层协议维护一套认证规则（包括认证算法和密钥），将会有大量的应用程序采用相同的认证方式。这将导致认证信息被复制和更改。同样，如果每个应用程序都采用一个固定的认证密钥，每次更改需要网络管理员手工修改。手工更改密钥或认证算法将是非常复杂和烦琐的，要想实现更改所有路由器的密码而不丢包将是非常困难的。

因此，需要系统能够集中管理所有的认证处理和更改认证算法和密钥，避免过多的人工干预。Keychain 就实现了这个功能。

13.2 AR1200 支持的 Keychain 特性

AR1200 支持以下 Keychain 特性:

- 对应用层协议认证

  应用 Keychain 实现对应用层协议的认证。一个 Keychain 可以配置一个或多个 key-id。key-id 由认证算法和密钥组成。每一个 key-id 关联一个发送和接收的生命周期，生命周期用来定义 Keychain 发送和接收的活跃时间段。key-id 需要发送和接收的两端都是活跃的。管理员在配置 key-id 时，需要保证发送和接收端在通信时不丢包。

- 配置接收容忍时间

  如果发送端路由器的 key-id 发生变更，接收端路由器的 key-id 也需要变更。由于时钟不同步，在接收者和发送者变更 key-id 时有可能存在时间延迟。在延迟的时间范围内会造成数据丢失，因为发送端和接收端的 key-id 不一致。为了实现两端 key-id 变更时不丢包，需要配置容忍时间，在该时间范围内两端的 key-id 都可以使用。这个时间段被称为接收容忍时间，接收容忍时间只对接收端的 Key 有效。接收容忍时间将导致接收起始和终止的时间延长。

- 配置缺省 send-key-id

  如果在某个时间段管理员没有配置 key-id，此时将没有活跃的 key-id 发送。在该时间段，应用程序将没有认证的交互。为了避免这种情况，使用缺省的 send-key-id，该 id 始终处于活跃状态。任何存在的 key-id 都可以被指定为 send-key-id。在一个 Keychain 中只能有一个 send-key-id。在活跃的 key-id 状态变为不活跃，并且不存在其他活跃的 key-id 时，应用程序将使用缺省的 send-key-id。

- 配置 TCP-kind 和 TCP algorithm-id

  TCP 应用程序之间通过 TCP 认证建立连接。对于 TCP 的认证交互，TCP 使用增强的 TCP 认证选项。目前，不同的厂商使用不同的 kind-value 值代表增强的 TCP 认证选项。为了实现不同厂商设备之间的交互，kind-value 必须是可配置的，能根据对端设备的 TCP 类型进行调整。同样，在 TCP 的增强认证选项中存在一个 algorithm-id 字段，该字段用来表示认证算法的类型。由于 algorithm-id 不是 IANA 统一定义的，不同的厂商之间使用不同的 algorithm-id 来代表认证算法。为了实现

不同厂商之间的互通，用户必须根据对端配置的算法类型，配置 TCP algorithm-id，以保持两端算法的一致。

13.3 配置 Keychain 的基本功能

本节介绍 Keychain 基本功能的配置方法。

13.3.1 建立配置任务

应用环境

应用 Keychain 实现对应用层协议的认证。一个 Keychain 可以配置一个或多个 key-id。key-id 由认证算法和密钥组成。每一个 key-id 关联一个发送和接收的生命周期，生命周期用来定义 keychain 发送和接收的活跃时间段。key-id 需要发送和接收的两端都是活跃的。当 key-id 两端都是活跃时，进行正常的认证交互。当 key-id 发送端活跃时，用来发送认证报文，接收端必须用活跃的 key-id 接收认证报文。管理员在配置 key-id 时，需要保证发送和接收端在通信时不丢包。

前置任务

在配置 Keychain 任务之前，需要提前完成以下任务：

- 配置完成 NTP，保证发送端和接收端时间一致。

数据准备

为完成 Keychain 特性的配置，需要准备以下数据。

No.	Data
1	Keychain 名称
2	key-id
3	key-string
4	key-id 的认证算法
5	key-id 的接收和发送时间
6	接收容忍时间

13.3.2 创建 Keychain

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **keychain** *keychain-name* [**mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } }]，创建 Keychain 并进入 Keychain 视图。

说明

创建 Keychain 时，时间模式是必选的。Keychain 创建成功后，进入 Keychain 视图，时间模式可以不用指定。

----结束

13.3.3 配置 Keychain 的接收容忍时间

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **keychain** *keychain-name*，进入 Keychain 视图。

步骤 3 执行命令 **receive-tolerance** { *value* | **infinite** }，配置 Keychain 的接收容忍时间。

说明

配置容忍时间分为以下两种方式:

- 指定一个具体的时间，单位是分钟，最大值是 14400 分钟（10 天）。
- 配置 infinite，容忍所有的时间延迟。

----结束

13.3.4 配置 key-id

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **keychain** *keychain-name*，进入 Keychain 视图。

步骤 3 执行命令 **key-id** *key-id*，创建 key-id，并进入 key-id 视图。

说明

同一个 Keychain 内的 key-id 必须唯一，整数形式，取值范围是 0 ~ 63。

----结束

13.3.5 配置 key-id 的密码字

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **keychain** *keychain-name*，进入 Keychain 视图。

步骤 3 执行命令 **key-id** *key-id*，进入 key-id 视图。

步骤 4 执行命令 **key-string** { **plain** *plain-text* | [**cipher**] *cipher-text* }，配置 Keychain 的密码字。

在发送和接收数据的过程中，key-string 作为密码验证字。使用 **plain** 时，密钥以明文形式显示。使用 **cipher** 时，密钥以密文形式显示。

说明

key-string 不配置时，key-id 处于非活跃状态。

----结束

13.3.6 配置 key-id 的认证算法

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **keychain** *keychain-name*，进入 Keychain 视图。

步骤 3 执行命令 **key-id** *key-id*，进入 key-id 视图。

步骤 4 执行命令 **algorithm** { **hmac-md5** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **simple** }，配置 key-id 的认证算法。

说明

认证算法没有配置时，key-id 处于非活跃状态。

----结束

13.3.7 配置缺省发送 key-id

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **keychain** *keychain-name*，进入 Keychain 视图。

步骤 3 执行命令 **key-id** *key-id*，进入 key-id 视图。

步骤 4 执行命令 **default send-key-id**，配置缺省发送 key-id。

说明

在 Keychain 中，只能有一个 key-id 配置为缺省发送 key-id。

----结束

13.3.8 配置 key-id 的发送时间

背景信息

根据 Keychain 的配置模式不同，对应的 key-id 发送时间模式也不同。

操作步骤

- 绝对时间模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **keychain** *keychain-name* **mode absolute**，创建绝对时间模式 Keychain，并进入 Keychain 视图。
  3. 执行命令 **key-id** *key-id*，进入 key-id 视图。

4. 执行命令 **send-time utc** *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } }，配置 key-id 的发送时间。

- 日周期模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **keychain** *keychain-name* **mode periodic daily**，创建日模式 Keychain，并进入 Keychain 视图。
  3. 执行命令 **key-id** *key-id*，进入 key-id 视图。
  4. 执行命令 **send-time daily** *start-time* **to** *end-time*，配置 key-id 的发送时间。
- 周周期模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **keychain** *keychain-name* **mode periodic weekly**，创建周模式 Keychain，并进入 Keychain 视图。
  3. 执行命令 **key-id** *key-id*，进入 key-id 视图。
  4. 执行命令 **send-time day** { { *start-day-name* } &<1-7> } [*to end-day-name*]，配置 key-id 的发送时间。
- 月周期模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **keychain** *keychain-name* **mode periodic monthly**，创建月模式 Keychain，并进入 Keychain 视图。
  3. 执行命令 **key-id** *key-id*，进入 key-id 视图。
  4. 执行命令 **send-time date** { { *start-date-value* } &<1-31> } [**to** *end-date-value*]，配置 key-id 的发送时间。
- 年周期模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **keychain** *keychain-name* **mode periodic yearly**，创建年模式 Keychain，并进入 Keychain 视图。
  3. 执行命令 **key-id** *key-id*，进入 key-id 视图。
  4. 执行命令 **send-time month** { { *start-month-name* } &<1-12> } [**to** *end-month-name*]，配置 key-id 的发送时间。

  说明

  key-id 的发送时间根据 Keychain 的时间模式进行配置。在一个 Keychain 中，同时只能有一个发送时间生效。同一个 Keychain 中，不同 key-id 对应的发送时间不能有时间重叠。

  在重新配置发送时间之前，需要先删除已经配置的发送时间。

----结束

13.3.9 配置 key-id 的接收时间

背景信息

根据 Keychain 的配置模式不同，对应的 key-id 接收时间模式也不同。

操作步骤

- 绝对时间模式

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **keychain** *keychain-name* **mode absolute**，创建绝对时间模式 Keychain，并进入 Keychain 视图。
3. 执行命令 **key-id** *key-id*，进入 key-id 视图。
4. 执行命令 **receive-time utc** *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date*}，

- 日周期模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **keychain** *keychain-name* **mode periodic daily**，创建日模式 Keychain，并进入 Keychain 视图。
  3. 执行命令 **key-id** *key-id*，进入 key-id 视图。
  4. 执行命令 **receive-time daily** *start-time* **to** *end-time*，配置 key-id 的接收时间。
- 周周期模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **keychain** *keychain-name* **mode periodic weekly**，创建周模式 Keychain，并进入 Keychain 视图。
  3. 执行命令 **key-id** *key-id*，进入 key-id 视图。
  4. 执行命令 **receive-time day** { { *start-day-name* } &<1-7> } [*to end-day-name*]，配置 key-id 的接收时间。
- 月周期模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **keychain** *keychain-name* **mode periodic monthly**，创建月模式 Keychain，并进入 Keychain 视图。
  3. 执行命令 **key-id** *key-id*，进入 key-id 视图。
  4. 执行命令 **receive-time date** { { *start-date-value* } &<1-31> } [**to** *end-date-value*]，配置 key-id 的接收时间。
- 年周期模式
  1. 执行命令 **system-view**，进入系统视图。
  2. 执行命令 **keychain** *keychain-name* **mode periodic yearly**，创建年模式 Keychain，并进入 Keychain 视图。
  3. 执行命令 **key-id** *key-id*，进入 key-id 视图。
  4. 执行命令 **receive-time month** { { *start-month-name* } &<1-12> } [**to** *end-month-name*]，配置 key-id 的接收时间。

     说明

     key-id 的接收时间根据 Keychain 的时间模式进行配置。在一个 Keychain 中，同时只能有一个接收时间生效。同一个 Keychain 中，不同 key-id 对应的接收时间不能有时间重叠。

     在重新配置接收时间之前，需要先删除已经配置的接收时间。

----结束

13.3.10 检查配置结果

前提条件

已完成 Keychain 的配置。

操作步骤

- 执行 **display keychain** *keychain-name* 命令查看 Keychain 的当前配置。
- 执行 **display keychain** *keychain-name* **key-id** *key-id* 命令查看 key-id 的当前配置。

----结束

任务示例

完成 Keychain 的配置后，可以执行命令 **display keychain** *keychain-name* 命令查看 Keychain 的当前配置，如下所示：

```
<Huawei> display keychain earth
 Keychain Information:
 ---------------------
 Keychain Name             : earth
   Timer Mode              : Absolute
   Receive Tolerance(min)  : 0
   TCP Kind                : 254
   TCP Algorithm IDs       :
     HMAC-MD5              : 5
     HMAC-SHA1-12          : 2
     HMAC-SHA1-20          : 6
     MD5                   : 3
     SHA1                  : 4
 Number of Key IDs         : 0
 Active Send Key ID        : None
 Active Receive Key IDs    : None
 Default send Key ID       : Not configured
```

完成 Keychain 的配置后，可以执行命令 **display keychain** *keychain-name* **key-id** *key-id* 查看 key-id 的当前配置，如下所示：

```
<Huawei> display keychain earth key-id 1
 Keychain Information:
 ---------------------
 Keychain Name             : earth
   Timer Mode              : Absolute
   Receive Tolerance(min)  : 100
   TCP Kind                : 182
   TCP Algorithm IDs       :
     HMAC-MD5              : 5
     HMAC-SHA1-12          : 2
     HMAC-SHA1-20          : 6
     MD5                   : 17
     SHA1                  : 4

 Key ID Information:
 -------------------
 Key ID                    : 1
   Key string              : hello (plain)
   Algorithm               : MD5
   SEND TIMER              :
     Start time            : 2012-03-14 00:00
     End time              : 2012-08-08 23:59
     Status                : Active
   RECEIVE TIMER           :
     Start time            : 2012-03-14 00:00
     End time              : 2012-08-08 23:59
     Status                : Active
```

```
DEFAULT SEND KEY ID INFORMATION
  Default               : Not configured
```

13.4 配置 TCP 认证参数

本节介绍在 Keychain 模块中如何配置 TCP 认证的参数。

13.4.1 建立配置任务

应用环境

Keychain 对所有需要认证的应用程序提供认证支持。TCP 两端需要进行 TCP 认证交互。不同设备商之间基于 TCP 协议的应用程序可以通过建立 TCP 认证连接实现互通。

对于 TCP 的认证交互，TCP 使用增强的 TCP 认证选项。目前，不同的设备商使用不同的 kind-value 代表增强的 TCP 认证选项类型。为了实现不同厂商设备之间的交互，kind-value 是必须配置的。并且，在 TCP 的增强认证选项中存在一个 algorithm-id 字段，该字段用来表示认证算法的类型。由于 algorithm-id 不是 IANA（Internet Assigned Numbers Authority，因特网地址分配组织）统一定义的，不同的厂商之间使用不同的 algorithm-id 来代表认证算法。

为了实现不同厂商之间的互通，用户必须根据对端配置的算法类型，配置 TCP algorithm-id，以保持两端算法的一致。

前置任务

在配置 Keychain TCP 认证之前，需要提前完成以下任务：

- 配置 NTP，确保认证两端的时间一致。

数据准备

为完成 Keychain TCP 认证的配置，需要准备以下数据。

No.	Data
1	Keychain 名称
2	TCP 类型值
3	TCP 认证算法 ID

13.4.2 配置 Keychain 的 TCP 类型

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **keychain** *keychain-name*，进入 Keychain 视图。

步骤 3 执行命令 **tcp-kind** *kind-value*，配置 Keychain 认证的 TCP 类型。

kind-value 是整数形式，取值范围是 28 ～ 255。

说明

TCP 使用 TCP 增强认证选项进行认证的交互，TCP 类型值用于体现 Keychain 认证中使用的 TCP 认证类型。

----结束

13.4.3 配置 Keychain 的 TCP 认证算法 ID

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **keychain** *keychain-name*，进入 Keychain 视图。

步骤 3 执行命令 **tcp-algorithm-id** { **md5** | **sha-1** | **hmac-md5** | **hmac-sha1-12** | **hmac-sha1-20** } *algorithm-id*，配置 TCP 认证算法 ID。

TCP algorithm-id 是整数形式，取值范围是 1 ～ 63。

说明

TCP algorithm-id 用来表示 TCP 认证中采用的算法类型。

----结束

13.4.4 检查配置结果

前提条件

已完成 Keychain 的配置。

操作步骤

- 执行 **display keychain** *keychain-name* 命令查看 Keychain 的当前配置。
- 执行 **display keychain** *keychain-name* **key-id** *key-id* 命令查看 key-id 的当前配置。

----结束

任务示例

完成 Keychain 的配置后，可以执行命令 **display keychain** *keychain-name* 命令查看 Keychain 的当前配置，如下所示：

```
<Huawei> display keychain earth
 Keychain Information:
 ----------------------
 Keychain Name             : earth
   Timer Mode              : Absolute
   Receive Tolerance(min)  : 0
   TCP Kind                : 254
   TCP Algorithm IDs       :
```

```
    HMAC-MD5              : 5
    HMAC-SHA1-12          : 2
    HMAC-SHA1-20          : 6
    MD5                   : 3
    SHA1                  : 4
Number of Key IDs         : 0
Active Send Key ID        : None
Active Receive Key IDs    : None
Default send Key ID       : Not configured
```

完成 Keychain 的配置后，可以执行命令 **display keychain** *keychain-name* **key-id** *key-id* 查看 key-id 的当前配置，如下所示：

```
<Huawei> display keychain earth key-id 1
 Keychain Information:
 ---------------------
 Keychain Name             : earth
   Timer Mode              : Absolute
   Receive Tolerance(min)  : 100
   TCP Kind                : 182
   TCP Algorithm IDs       :
     HMAC-MD5              : 5
     HMAC-SHA1-12          : 2
     HMAC-SHA1-20          : 6
     MD5                   : 17
     SHA1                  : 4

 Key ID Information:
 -------------------
 Key ID                    : 1
   Key string              : hello (plain)
   Algorithm               : MD5
   SEND TIMER              :
     Start time            : 2012-03-14 00:00
     End time              : 2012-08-08 23:59
     Status                : Active
   RECEIVE TIMER           :
     Start time            : 2012-03-14 00:00
     End time              : 2012-08-08 23:59
     Status                : Active
   DEFAULT SEND KEY ID INFORMATION
     Default               : Not configured
```

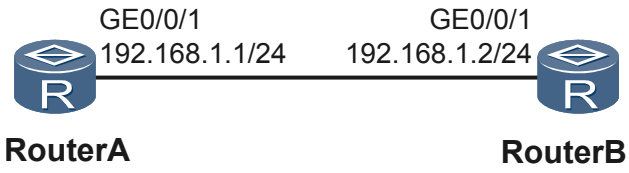
13.5 配置举例

13.5.1 配置非 TCP 应用的 Keychain 认证示例

组网需求

如图 13-1 所示，需要在 RouterA 和 RouterB 的所有接口上配置 RIP 和 Keychain 认证。两台 Router 通过 RIP-2 进行交互。

图 13-1 Keychain 组网图



配置思路

采用如下思路配置 Keychain:

1. 配置 Keychain 的基本功能。
2. 配置 RIP 基本功能。

数据准备

为完成此配置例，需要准备以下数据：

- Keychain 名称
- key-id
- 认证算法和密码验证字
- 发送和接收时间
- 接收容忍时间

操作步骤

步骤 1 配置 RouterA

配置 Keychain 认证。

```
<RouterA> system-view
[RouterA] keychain huawei mode absolute
[RouterA-keychain] receive-tolerance 100
[RouterA-keychain] key-id 1
[RouterA-keychain-keyid-1] algorithm md5
[RouterA-keychain-keyid-1] key-string abcdef
[RouterA-keychain-keyid-1] send-time utc 14:40 2008-10-10 to 14:50 2008-10-10
[RouterA-keychain-keyid-1] receive-time utc 14:30 2008-10-10 to 14:50 2008-10-10
[RouterA-keychain-keyid-1] quit
```

配置 RIP 基本功能。

```
[RouterA] interface gigabitethernet 0/0/1
[RouterA-GigabitEthernet0/0/1] ip address 192.168.1.1 24
[RouterA-GigabitEthernet0/0/1] rip authentication-mode md5 nonstandard keychain huawei
[RouterA-GigabitEthernet0/0/1] quit
```

步骤 2 配置 RouterB

配置 Keychain 认证。

```
[RouterB] keychain huawei mode absolute
[RouterB-keychain] receive-tolerance 100
[RouterB-keychain] key-id 1
[RouterB-keychain-keyid-1] algorithm md5
[RouterB-keychain-keyid-1] key-string abcdef
[RouterB-keychain-keyid-1] send-time utc 14:40 2008-10-10 to 14:50 2008-10-10
[RouterB-keychain-keyid-1] receive-time utc 14:30 2008-10-10 to 14:50 2008-10-10
[RouterB-keychain-keyid-1] quit
```

配置 RIP 基本功能。

```
[RouterB] interface gigabitethernet 0/0/1
[RouterB-GigabitEthernet0/0/1] ip address 192.168.1.2 24
[RouterB-GigabitEthernet0/0/1] rip authentication-mode md5 nonstandard keychain huawei
[RouterB-GigabitEthernet0/0/1] quit
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet0/0/1
ip address  192.168.1.1 255.255.255.0
rip authentication-mode md5 nonstandard keychain huawei
#
keychain huawei mode absolute
receive-tolerance 100
 key-id 1
  algorithm md5
  key-string cipher b{br9\zi%X+/Y@:Y>Lw(L\v#
  send-time utc 14:40 2008-10-10 to 14:50 2008-10-10
  receive-time utc 14:30 2008-10-10 to 14:50 2008-10-10
#
return
```

- RouterB 的配置文件

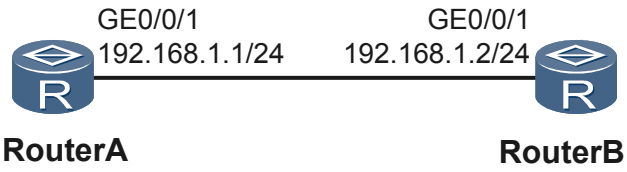
```
#
 sysname RouterB
#
interface GigabitEthernet0/0/1
ip address 192.168.1.2 255.255.255.0
rip authentication-mode md5 nonstandard keychain huawei
#
keychain huawei mode absolute
receive-tolerance 100
 key-id 1
  algorithm md5
  key-string cipher b{br9\zi%X+/Y@:Y>Lw(L\v#
  send-time utc 14:40 2008-10-10 to 14:50 2008-10-10
  receive-time utc 14:30 2008-10-10 to 14:50 2008-10-10
#
return
```

13.5.2 配置 TCP 应用程序的 Keychain 认证示例

组网需求

如图 13-2 所示，在 RouterA 和 RouterB 上配置 BGP 和 Keychain 认证。Router 之间采用 BGP。

图 13-2 Keychain 组网图



配置思路

采用如下思路配置 Keychain 认证：

1. 配置 Keychain 的基本功能。
2. 配置 Router 采用 Keychain 认证 BGP。

数据准备

为完成此配置例，需准备如下数据：

- Keychain 名称
- key-id
- 算法和认证字符串
- 发送和接收时间
- 接收容忍时间
- TCP 类型值和 tcp-algorithm-id

操作步骤

步骤 1 配置 RouterA。

配置 keychain。

```
<RouterA> system-view
[RouterA] keychain huawei mode absolute
[RouterA-keychain] tcp-kind 182
[RouterA-keychain] tcp-algorithm-id md5 17
[RouterA-keychain] receive-tolerance 100
[RouterA-keychain] key-id 1
[RouterA-keychain-keyid-1] algorithm md5
[RouterA-keychain-keyid-1] key-string hello
[RouterA-keychain-keyid-1] send-time utc 14:40 2008-10-10 to 14:50 2008-10-10
[RouterA-keychain-keyid-1] receive-time utc 14:30 2008-10-10 to 14:50 2008-10-10
[RouterA-keychain-keyid-1] quit
[RouterA-keychain] quit
```

配置 Keychain 认证。

```
[RouterA] interface gigabitethernet 0/0/1
[RouterA-GigabitEthernet0/0/1] ip address 192.168.1.1 24
[RouterA-GigabitEthernet0/0/1] quit
[RouterA] bgp 1
[RouterA-bgp] router-id 1.1.1.1
[RouterA-bgp] peer 192.168.1.2 as-number 1
[RouterA-bgp] peer 192.168.1.2 keychain huawei
[RouterA-bgp] quit
```

步骤 2 配置 RouterB。

配置 Keychain。

```
<RouterB> system-view
[RouterB] keychain huawei mode absolute
[RouterB-keychain] tcp-kind 182
[RouterB-keychain] tcp-algorithm-id md5 17
[RouterB-keychain] receive-tolerance 100
[RouterB-keychain] key-id 1
[RouterB-keychain-keyid-1] algorithm md5
[RouterB-keychain-keyid-1] key-string hello
[RouterB-keychain-keyid-1] send-time utc 14:40 2008-10-10 to 14:50 2008-10-10
[RouterB-keychain-keyid-1] receive-time utc 14:30 2008-10-10 to 14:50 2008-10-10
[RouterB-keychain-keyid-1] quit
[RouterB-keychain] quit
```

配置 Keychain 认证。

```
[RouterB] interface gigabitethernet 0/0/1
[RouterB-GigabitEthernet0/0/1] ip address 192.168.1.2 24
[RouterB-GigabitEthernet0/0/1] quit
[RouterB] bgp 1
```

```
[RouterB-bgp] router-id 2.2.2.2
[RouterB-bgp] peer 192.168.1.1 as-number 1
[RouterB-bgp] peer 192.168.1.1 keychain huawei
[RouterB-bgp] quit
```

----结束

配置文件

- # RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet0/0/1
ip address .192.168.1.1 255.255.255.0
#
bgp 1
 router-id 1.1.1.1
 peer 192.168.1.2 as-number 1
 peer 192.168.1.2 keychain huawei
#
keychain huawei mode absolute
tcp-kind 182
tcp-algorithm-id md5 17
receive-tolerance 100
 key-id 1
  algorithm md5
  key-string cipher Hb(c;\@iU'@X,k6.E\Z,*.S#
  send-time utc 14:40 2008-10-10 to 14:50 2008-10-10
  receive-time utc 14:30 2008-10-10 to 14:50 2008-10-10
#
return
```

- #Router B 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet0/0/1
ip address 192.168.1.2 255.255.255.0
#
bgp 1
 router-id 2.2.2.2
 peer 192.168.1.1 as-number 1
 peer 192.168.1.1 keychain huawei
#
keychain huawei mode absolute
tcp-kind 182
tcp-algorithm-id md5 17
receive-tolerance 100
 key-id 1
  algorithm md5
  key-string cipher Hb(c;\@iU'@X,k6.E\Z,*.S#
  send-time utc 14:40 2008-10-10 to 14:50 2008-10-10
  receive-time utc 14:30 2008-10-10 to 14:50 2008-10-10
#
return
```

14 攻击防范和应用层联动配置

关于本章

攻击防范和应用层联动主要防止攻击报文对 CPU 的攻击，保证设备在遭受攻击的情况下仍然正常运行。

14.1 攻击防范和应用层联动简介
TCP/IP 网络的攻击日益增多，特别是对网络设备的攻击，将会导致网络瘫痪或者不可用。

14.2 配置畸形报文攻击防范
畸形报文攻击防范主要防止没有 IP 载荷的泛洪攻击、IGMP 空报文攻击、LAND 攻击、Smurf 攻击、TCP 标志位非法攻击。

14.3 配置分片报文攻击防范
分片报文攻击防范主要包括分片数量巨大、Tear Drop 攻击、Syndrop 攻击、Nesta 攻击、Fawx 攻击、NewTear 攻击、Bonk 攻击、Rose 攻击、巨大 Offset 攻击、死亡之 ping 攻击、Jolt 攻击、重复分片攻击。

14.4 配置泛洪攻击防范
防洪攻击防范主要防止 SYS Flood 攻击、UDP Flood 攻击和 ICMP Flood 攻击。

14.5 配置应用层联动
应用层联动主要通过应用层协议开关控制协议报文的转发和丢弃，达到防攻击目的。

14.6 维护攻击防范和应用层联动
清除攻击防范的统计信息。

14.7 配置举例
介绍使用攻击防范提高设备安全性的各种示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

14.1 攻击防范和应用层联动简介

TCP/IP 网络的攻击日益增多，特别是对网络设备的攻击，将会导致网络瘫痪或者不可用。

14.1.1 攻击防范和应用层联动概述

增强设备对拒绝服务型攻击、扫描窥探攻击和畸形报文攻击三类攻击的防范能力，可以增强系统的安全性，满足这些组网情况下的业务开展需求。

TCP/IP 攻击防范

目前，基于 TCP/IP 网络的攻击日益增多，TCP/IP 协议本身的缺陷以及实现过程的不严谨，导致网络攻击造成的影响越来越大。特别是对网络设备的攻击，将会导致网络瘫痪或者不可用。

对于 TCP/IP 的攻击主要可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，或者资源耗尽不能正常的工作。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路由器。

- 扫描窥探攻击

  扫描窥探攻击是利用 ping 扫射（包括 ICMP 和 TCP）来标识网络上运行的系统，从而准确的找出潜在的目标。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。

应用层联动

路由器可能同时启用多种服务，例如二层业务 STP、MSTP、RRPP，路由业务 OSPF、BGP，MPLS 业务 LDP、RSVP，系统服务 FTP Server、TFTP Server，诊断功能 Ping、Tracert 等。

在这种情况下，攻击者可以发送各种类型的报文攻击路由器，如果是多播协议报文，或者目的地址是路由器自身接口（包括 Loopback 口）IP 地址时，路由器就会直接将报文上送 CPU。这样就会耗费路由器的 CPU 和系统资源，造成 DoS 攻击。

为了避免这种攻击，可以将部分业务和协议实现开关控制，如果开关打开，即协议使能，则上送这种协议报文。开关关闭，即协议去使能，则直接丢弃这种协议报文，完成协议报文的控制，即应用层联动。

对于某些协议可以支持白名单，应用层联动模块检测上送的协议报文，对匹配白名单的协议报文，允许其以大带宽和高速率上送。

14.1.2 AR1200 支持的攻击防范和应用层联动

AR1200 支持的攻击防范包括：畸形报文攻击防范、分片报文攻击防范、泛洪攻击防范，提供应用层联动模块实现应用层联动，实现应用层报文过滤。

AR1200 支持的攻击防范

AR1200 主要支持以下几类 TCP/IP 攻击防范：

- 畸形报文攻击防范

  防止路由器处理畸形报文占用资源过多，导致系统崩溃、网络瘫痪，因此 AR1200 检测到这些畸形报文后直接将其丢弃。针对以下几种畸形报文的攻击防范，AR1200 具体操作如下：

  - 没有 IP 载荷的泛洪攻击，如果发现只有 IP 头部，没有携带任何高层数据 IP 报文，认为是没有作用的，直接丢弃。
  - IGMP 空报文攻击，如果 IGMP 报文长度小于 28 字节，认为是畸形报文直接丢弃。
  - LAND 攻击，检测 TCP syn 报文中的源地址和目的地址、源端口和目的端口是否一致，如果完全一致认为是畸形报文直接丢弃。
  - Smurf 攻击，对于目的地址为广播地址或者子网广播地址的 ICMP echo request 报文，直接认为是畸形报文丢弃。
  - TCP 标志位非法攻击，检查 TCP 报文的各个标志位，若出现 URG、ACK、PSH、RST、SYN、FIN6 个标志位全部为“1”或“0”，或者 SYN 和 FIN 位同时为 1，直接将其丢弃。

- 分片报文攻击防范

  - Teardrop 类攻击主要是利用分片报文的 Offset 可能重叠，系统对分片报文重组时占用资源过高，导致网络中断。AR1200 在处理 Teardrop 类攻击时，丢弃重组有重叠的报文，保证系统对分片报文重组正确。
  - 巨大 Offset 类攻击是利用分片报文 Offset 长度大于 65515，导致系统重组报文时占用资源过高，导致网络服务中断。AR1200 在处理巨大 Offset 类攻击时，判断 Offset 的总长度是否会超过 65515，超过即丢弃。
  - 重复分片类攻击是指将相同的分片报文发送多次，包括相同的分片重传；Offset 相同，但是并不是相同分片，导致系统重组报文失败，CPU 占用资源过高。对于重复分片类报文的攻击，AR1200 在接口板上对分片报文进行限速处理，保证不对 CPU 造成攻击，速度 Car 大小可配置。

- 泛洪攻击防范

  泛洪攻击主要包括 TCP SYN Flood 攻击、UDP Flood 攻击（包括 Fraggle 攻击、UDP 诊断端口攻击）、ICMP Flood 攻击。AR1200 针对 TCP SYN Flood 攻击和 ICMP Flood 攻击主要采用速率限制，防止 CPU 占用资源过高，针对 UDP Flood 攻击，AR1200 检测 UDP 报文的端口号，对于端口号为 7，13，19 的报文，认为是攻击报文，直接丢弃。

说明

攻击防范的相关配置只对设备的主控板生效。

AR1200 支持的应用层联动

AR1200 支持应用层联动功能。通过应用层联动功能，AR1200 可以控制部分协议和业务的报文。

- 当协议开关关闭时，AR1200 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，AR1200 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。

应用层联动模块支持的协议包括 SNMP、HW-TACACS、NTP、SSH、BGP、DHCP、802.1x 和 PIM 协议，支持的业务包括 HTTP Server、Telnet Server、STelnet Server、FTP Server、SFTP Server、BFD、UDP Helper 和 VRRP。

说明

根据需要，用户可以为不同的协议和业务配置应用层联动功能，具体内容请参考相关章节。

14.2 配置畸形报文攻击防范

畸形报文攻击防范主要防止没有 IP 载荷的泛洪攻击、IGMP 空报文攻击、LAND 攻击、Smurf 攻击、TCP 标志位非法攻击。

14.2.1 建立配置任务

在配置畸形报文攻击防范之前，了解其应用环境，以及配置畸形报文攻击需要提前完成的任务和准备的数据。

应用环境

在网络环境中，经常存在着不同类型的网络攻击，导致网络设备资源使用率过高，甚至瘫痪，影响网络服务。

为了避免网络设备被畸形报文攻击的情况下瘫痪，保证正常的网络服务，需要配置畸形报文攻击防范。

前置任务

在畸形报文攻击防范之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up

数据准备

无

14.2.2 使能畸形报文攻击防范

对畸形报文攻击防范的主要措施是判断是否是几种畸形攻击报文类型之一，对畸形报文直接丢弃。

背景信息

请在路由器上进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **anti-attack abnormal enable**，使能畸形报文攻击防范。

缺省情况下，畸形报文攻击防范功能处于使能状态，不需要配置该命令。如果之前将畸形报文攻击防范功能去使能了，重新打开时，需要执行该命令。

----结束

14.2.3 检查配置结果

配置畸形报文攻击防范之后，可以查看接口板上畸形报文防攻击的统计数据。

前提条件

已完成畸形报文攻击防范的所有配置。

操作步骤

步骤 1 执行 **display anti-attck statistics abnormal** 命令查看畸形报文防攻击的统计数据。

----结束

14.3 配置分片报文攻击防范

分片报文攻击防范主要包括分片数量巨大、Tear Drop 攻击、Syndrop 攻击、Nesta 攻击、Fawx 攻击、NewTear 攻击、Bonk 攻击、Rose 攻击、巨大 Offset 攻击、死亡之 ping 攻击、Jolt 攻击、重复分片攻击。

14.3.1 建立配置任务

在配置分片报文攻击防范之前，了解其应用环境，以及配置分片报文攻击防范需要提前完成的任务和准备的数据。

应用环境

在网络环境中，经常存在着不同类型的网络攻击，导致网络设备资源使用率过高，甚至瘫痪，影响网络服务。

为了避免网络设备被分片报文攻击的情况下瘫痪，保证正常的网络服务，需要配置分片报文攻击防范。

前置任务

在分片报文攻击防范之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up

数据准备

在配置分片报文攻击防范之前，需要准备以下数据。

序号	数据
1	分片报文限制的速率

14.3.2 配置分片报文攻击防范

对分片报文攻击防范的主要措施是进行速率限制，防止大量的分片报文造成 CPU 繁忙，保证 CPU 在造成攻击的情况下正常运行。

背景信息

请在路由器上进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **anti-attack fragment enable**，使能分片报文攻击防范。

缺省情况下，分片报文攻击防范功能处于使能状态，不需要配置该命令，只配置限制速率即可。如果之前将分片报文攻击防范功能去使能了，重新打开时，需要执行该命令。

步骤 3 执行命令 **anti-attack fragment car cir** *cir*，限制分片报文发送的速率。

----结束

14.3.3 检查配置结果

配置分片报文攻击防范完成之后，可以查看接口板上分片报文防攻击的统计数据。

前提条件

已完成分片报文攻击防范的所有配置。

操作步骤

步骤 1 执行 **display anti-attck statistics fragment** 命令查看接口板上分片报文防攻击的统计数据。

----结束

14.4 配置泛洪攻击防范

防洪攻击防范主要防止 SYS Flood 攻击、UDP Flood 攻击和 ICMP Flood 攻击。

14.4.1 建立配置任务

在配置泛洪攻击防范之前，了解其应用环境，以及配置泛红攻击防范需要提前完成的任务和需要准备的数据。

应用环境

在网络环境中，经常存在着不同类型的网络攻击，导致网络设备资源使用率过高，甚至瘫痪，影响网络服务。

为了避免网络设备被泛洪攻击的情况下瘫痪，保证正常的网络服务，需要配置泛洪攻击防范。

前置任务

在泛洪攻击防范之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up

数据准备

在配置泛洪攻击防范之前，需要准备以下数据。

序号	数据
1	TCP-syn 报文限制的速率、ICMP Flood 报文限制的速率

14.4.2 配置 SYN Flood 攻击防范

对 SYN Flood 攻击防范的主要措施是限制 TCP SYN 报文的速率。

背景信息

请在路由器上进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **anti-attack tcp-syn enable**，使能 Syn Flood 攻击防范。

缺省情况下，Syn Flood 攻击防范功能处于使能状态，不需要配置该命令，只配置限制速率即可。如果之前将 Syn Flood 攻击防范功能去使能了，重新打开时，需要执行该命令。

步骤 3 执行命令 **anti-attack tcp-syn car cir** *cir*，限制 TCP-syn 报文发送的速率。

----结束

14.4.3 配置 UDP Flood 攻击防范

对 UDP Flood 攻击防范的主要措施是限制 UDP 报文的速率。

背景信息

请在路由器上进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **anti-attack udp-flood enable**，使能 UDP Flood 攻击防范。

缺省情况下，UDP Flood 攻击防范功能处于使能状态，不需要配置该命令。如果之前将 UDP Flood 攻击防范功能去使能了，重新打开时，需要执行该命令。

----结束

14.4.4 配置 ICMP Flood 攻击防范

对 ICMP Flood 攻击防范的主要措施是限制 ICMP 报文的速率。

背景信息

请在路由器上进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **anti-attack icmp-flood enable**，使能 ICMP Flood 攻击防范。

缺省情况下，ICMP Flood 攻击防范功能处于使能状态，不需要配置该命令，只配置限制速率即可。如果之前将 ICMP Flood 攻击防范功能去使能了，重新打开时，需要执行该命令。

步骤 3 执行命令 **anti-attack icmp-flood car cir** *cir*，限制 ICMP flood 报文发送的速率。

----结束

14.4.5 检查配置结果

配置泛洪攻击防范之后，可以查看接口板上泛洪防攻击的统计数据。

前提条件

已完成泛洪攻击防范的所有配置。

操作步骤

步骤 1 执行 **display anti-attck statistics [tcp-syn | udp-flood | icmp-flood]**命令查看泛洪防攻击的统计数据。

----结束

14.5 配置应用层联动

应用层联动主要通过应用层协议开关控制协议报文的转发和丢弃，达到防攻击目的。

14.5.1 建立配置任务

在配置应用层联动模块之前，了解其应用环境，以及配置应用层联动模块需要提前完成的任务和准备的数据。

应用环境

为了避免网络设备被不使用的协议报文攻击，导致网络繁忙，CPU 占用率过高，造成 DoS 攻击，需要配置应用层联动，关闭该协议模块，使该协议模块报文不上送 CPU，直接丢弃，保证 CPU 的正常工作。

前置任务

在配置应用层联动之前，需完成以下任务：

- 配置接口的链路层协议参数（和 IP 地址），使接口的链路协议状态为 Up

数据准备

在配置应用层联动之前，需要准备以下数据。

序号	数据
1	确定使能和去使能的协议
2	确定不匹配应用层联动模块的报文策略

14.5.2 配置应用层联动

应用层联动模块的使能是通过各协议的使能开关控制。对于不匹配应用层联动模块的报文，可以通过配置决定转发和丢弃。

背景信息

应用层联动模块采用协议的使能开关，控制应用层联动功能是否使能。如果协议使能，则上送这种协议报文；协议去使能，则直接丢弃这种协议报文。

因此，为了避免不必要的协议报文攻击，就需要将该协议模块的开关关闭。协议开关处于打开状态，不能起到非法报文过滤的作用，只能通过产品的限速功能限制报文的上送速率，避免对 CPU 的攻击。

请在路由器上进行如下配置：

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 对应用层联动模块匹配的协议和功能，使能其中需要应用的协议，去使能其中闲置的协议，实现防攻击。

步骤 3 （可选）执行命令 **application-apperceive default drop**，设置在查找不到应用层联动策略时，将报文丢弃。

----结束

14.6 维护攻击防范和应用层联动

清除攻击防范的统计信息。

14.6.1 清除攻击防范和应用层联动统计信息

在确认需要清除攻击防范的统计信息时，可以执行命令清除攻击防范的统计信息。

背景信息

清除信息后，以前的信息将无法恢复，务必仔细确认。

操作步骤

步骤 1 在确认需要清除的信息后，执行 **reset anti-attack statistics [abnormal | fragment | tcp-syn | udp-flood | icmp-flood]**命令清除攻击防范的报文统计信息。

----结束

14.7 配置举例

介绍使用攻击防范提高设备安全性的各种示例。请结合配置流程图了解配置过程。配置示例中包括组网需求、配置注意事项和配置思路等。

14.7.1 配置攻击防范示例

攻击防范在具体组网中的应用，包括畸形报文攻击防范、分片报文攻击防范和泛洪攻击防范。

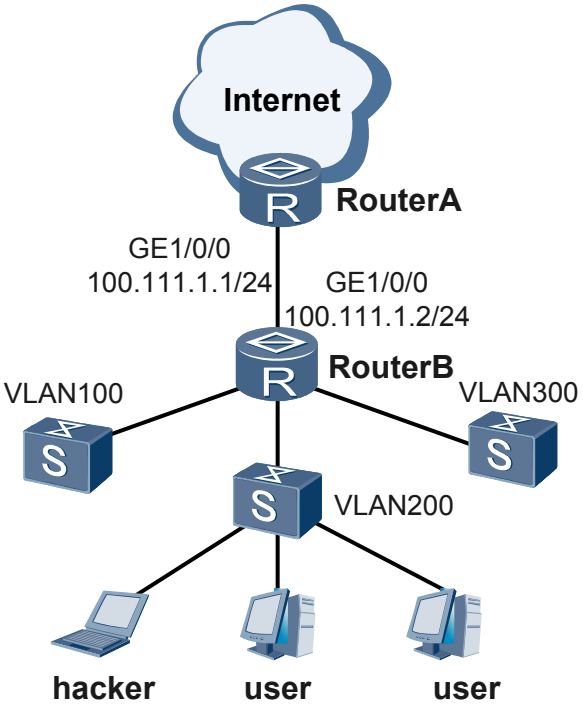
组网需求

如图 14-1 所示，客户端路由器 RouterB 与公网路由器 RouterA 直连，为了防止局域网内部的 Hacker 发送各种 TCP/IP 攻击报文对 RouterA 进行攻击，造成 RouterA 瘫痪，需要在 RouterA 上部署如下各种攻击防范措施：

- 使能畸形报文攻击防范，防止畸形报文攻击；
- 使能分片报文攻击防范，限制分片报文的速率为 15000bit/s，防止分片报文对 CPU 造成攻击，占用过多 CPU 和系统资源；
- 使能泛洪攻击，具体如下：

- 使能 Syn Flood 攻击防范，限制 TCP-syn 报文的上送速率为 15000bit/s，防止 CPU 处理 TCP-syn 报文占用过多资源；
- 使能 UDP Flood 攻击防范，对特定端口发送的 UDP 报文直接丢弃；
- 使能 ICMP Flood 攻击防范，限制 ICMP-Flood 报文的上送速率为 15000bit/s，防止 CPU 处理 ICMP-Flood 报文占用过多资源。

图 14-1 配置攻击防范组网图



配置思路

采用如下思路配置攻击防范：

1. 配置接口地址和路由，保证网络互通。
2. 在路由器 RouterA 上使能畸形报文攻击防范，避免畸形报文攻击。
3. 在路由器 RouterA 上使能分片报文攻击防范，避免分片报文攻击。
4. 在路由器 RouterA 上使能泛洪攻击防范，避免泛洪攻击。

数据准备

为完成该配置例，需要准备如下数据：

- 各接口的 IP 地址
- 限制报文上送 CPU 的速率

操作步骤

步骤 1 配置各接口的 IP 地址和路由，保证网络互通（略）。

步骤 2 在 RouterA 上使能畸形报文攻击防范。

```
<RouterA> system-view
[RouterA] anti-attack abnormal enable
```

步骤 3 # 在 RouterA 上使能分片报文攻击防范，并限制分片报文的速率为 15000bit/s。

```
[RouterA] anti-attack fragment enable
[RouterA] anti-attack fragment car cir 15000
```

步骤 4 # 在 RouterA 上使能 Syn Flood 报文攻击防范，并限制 TCP-syn 报文的上送速率为 15000bit/s。

```
[RouterA] anti-attack tcp-syn enable
[RouterA] anti-attack tcp-syn car cir 15000
```

在 RouterA 上使能 UDP Flood 攻击防范，对特定端口发送的 UDP 报文直接丢弃。

```
[RouterA] anti-attack udp-flood enable
```

在 RouterA 上使能 ICMP Flood 报文攻击防范，并限制 ICMP-Flood 报文的上送速率为 15000bit/s。

```
[RouterA] anti-attack icmp-flood enable
[RouterA] anti-attack icmp-flood car cir 15000
```

步骤 5 验证配置结果

配置完成后，可以通过执行命令 **display anti-attack statistics [abnormal | fragment | tcp-syn | udp-flood | icmp-flood]**查看报文攻击防范的统计数据：

```
<RouterA> display anti-attck statistics
Packets Statistic Information:
-------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum        DropPacketNum         PassPacketNum
             (H)        (L)        (H)        (L)        (H)        (L)
-------------------------------------------------------------------------------
URPF         0          0          0          0          0          0
Abnormal     0          0          0          0          0          0
Fragment     0          0          0          0          0          0
Tcp-syn      0          30         0          0          0          30
Udp-flood    0          0          0          0          0          0
Icmp-flood   0          40         0          0          0          40
-------------------------------------------------------------------------------
```

----结束

配置文件

- RouterA 的配置文件

```
#
 sysname RouterA
#
interface GigabitEthernet1/0/0
 ip address 100.111.1.1 255.255.255.252
#
anti-attack fragment car cir 15000
anti-attack tcp-syn car cir 15000
anti-attack icmp-flood car cir 15000
#
return
```

- RouterB 的配置文件

```
#
 sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 100.111.1.2 255.255.255.252
```

```
#
return
```