目 录

1 APR配置

1.1 APR简介

APR（Application Recognition）即应用层协议识别。一些基于应用的业务（例如 QoS，ASPF）在进行报文处理时需要知道报文所属的应用层协议，APR 可以为这样的业务提供应用识别服务，并能够对接口上接收或者发送的某个应用层协议的报文进行数目和速率统计。APR 为了更好地识别报文所属的应用层协议，提供了两种应用识别方法：基于端口的应用识别和基于内容特征的应用识别。

- PBAR（Port Based Application Recognition，基于端口的应用层协议识别）：根据定义的应用层协议端口与应用的映射关系识别报文所属的应用层协议。
- 基于内容特征的应用层协议识别：提取应用报文区别于其它应用报文的特征，通过将报文的内容与特征库中的特征项进行匹配来识别报文所属的应用层协议。这种识别方式目前还不支持。

下文中的应用均指设备可以通过 APR 识别出的应用层协议。应用分为预定义应用和自定义应用两种：预定义应用由系统缺省创建；自定义应用由用户通过配置创建。

1.1.1 PBAR

PBAR（Port Based Application Recognition，基于端口的应用层协议识别）根据预定义的、自定义的端口与应用的映射关系识别出应用层协议。预定义的端口与应用的映射关系由系统预先定义，自定义的端口与应用的映射关系由用户配置进行创建。

PBAR 提供了以下两种映射机制来维护和使用自定义的端口与应用映射关系：

- 通用端口映射：对用户自定义端口号和应用层协议建立映射关系。例如：将 2121 端口映射为 FTP 协议，这样所有目的端口是 2121 的报文将被识别为 FTP 报文。
- 主机端口映射：对去往某些特定范围内主机的报文建立自定义端口号和应用层协议的映射。例如：将目的地址为 10.110.0.0/16 网段的、使用 2121 端口的报文映射为 FTP 报文。主机范围可以通过配置 ACL 或者指定主机地址、网段来确定。

1.1.2 应用组

可以将具有相似特征的应用添加到一个应用组中。一个应用组，就是若干个应用的集合。如果报文被识别为属于某个应用，而该应用又属于某个应用组，则报文相当于被识别为属于某个应用组。基于应用的业务可以对属于同一个应用组的报文做统一处理。

应用组分为预定义和自定义两种：预定义应用组由系统预先定义并包含了指定的预定义应用；自定义应用组由用户通过配置创建。一个自定义应用组中可以包含多个预定义应用和自定义应用。

1.2 配置PBAR

根据与应用层协议进行映射的对象范围的不同，可以将端口映射的配置分为以下四类：

- 通用端口映射：对于所有报文，建立端口号与应用层协议的映射关系；
- 基于 ACL 的主机端口映射：对于匹配指定 ACL 的报文，建立端口号与应用层协议的映射关系；

- 基于网段的主机端口映射：对于目的地址为指定网段的报文，建立端口号与应用层协议的映射关系；
- 基于 IP 地址的主机端口映射：对于目的地址为指定 IP 地址的报文，建立端口号与应用层协议的映射关系。

以上四类端口映射配置对于同一个报文的生效优先级从高到低依次为：基于 IP 地址、基于网段、基于 ACL、通用。而对于其中的每一类，指定传输层协议名称的配置优先级高于不指定传输层协议名称的配置。

表1-1 配置 PBAR

操作	命令	说明
进入系统视图	**system-view**	-
配置通用端口映射	**port-mapping application** *application-name* **port** *port-number* [**protocol** *protocol-name*]	至少选其一 缺省情况下，各应用层协议与其对应的知名端口号映射 配置映射关系时，如果指定的应用不存在就会创建这个应用
配置基于ACL的主机端口映射	**port-mapping application** *application-name* **port** *port-number* [**protocol** *protocol-name*] **acl** *acl-number*	
配置基于网段的主机端口映射	**port-mapping application** *application-name* **port** *port-number* [**protocol** *protocol-name*] **subnet ip** *ipv4-address* { *mask-length* | *mask* }	
配置基于IP地址的主机端口映射	**port-mapping application** *application-name* **port** *port-number* [**protocol** *protocol-name*] **host ip** *start-ip-address* [*end-ip-address*]	

1.3 配置应用组

可以将具有相似特征的应用添加到一个应用组中或将一个应用组中的应用拷贝到另一个组中。设备最多可支持配置 65536 个应用组，每个应用组里最多可以包含 65536 个自定义应用。

表1-2 配置 APR 应用组

操作	命令	说明
进入系统视图	**system-view**	-
创建应用组，并进入应用组视图	**app-group** *group-name*	缺省情况下，系统中存在若干预定义应用组，可通过**display app-group pre-defined**命令查看 预定义的应用组不允许修改和删除
（可选）为自定义的应用组设置描述信息	**description** *group-description*	缺省情况下，自定义应用组的描述信息为“User-defined application group”

操作	命令	说明
在应用组中添加应用	**include application** *application-name*	缺省情况下，自定义应用组中不包含任何应用 可以通过多次执行本命令添加多个应用 添加应用时，如果对应的应用不存在就会创建这个应用
在应用组中拷贝另一个应用组中的所有应用	**copy app-group** *group-name*	可以通过多次执行本命令拷贝多个应用组里的应用

1.4 配置接口的应用统计功能

提示

接口的应用统计功能会消耗大量系统内存。当系统出现内存告警时，请关闭接口的应用统计功能。

在接口上开启应用统计功能之后，设备能够对接口上收到或者发送的报文的数目、速率按照应用层协议分别进行统计，生成的统计信息可以通过 **display application statistics** 命令查看。

表1-3 配置接口的应用统计功能

操作	命令	说明
进入系统视图	**system-view**	-
进入三层接口视图	**interface** *interface-type interface-number*	-
开启接口的应用统计功能	**application statistics enable** [**inbound** | **outbound**]	缺省情况下，接口的应用统计功能处于关闭状态 可以同时开启接口两个方向上的应用统计功能

1.5 APR显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 APR 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 APR 的统计信息。

表1-4 APR 显示和维护

操作	命令
显示应用信息	**display application** [**name** *application-name* | **pre-defined** | **user-defined**]
显示应用组信息	**display app-group** [**name** *group-name* | **pre-defined** | **user-defined**]

操作	命令
显示接口上的应用统计信息	**display application statistics** [**direction** { **inbound** | **outbound** } | **interface** *interface-type interface-number* | **name** *application-name*] *
按指定类型的统计排名显示接口应用统计信息	**display application statistics top** *number* { **bps** | **bytes** | **packets** | **pps** } **interface** *interface-type interface-number*
显示预定义的端口映射信息	**display port-mapping pre-defined**
显示自定义的端口映射信息	**display port-mapping user-defined** [**application** *application-name* | **port** *port-number*]
清除指定接口或所有接口的应用统计信息	**reset application statistics** [**interface** *interface-type interface-number*]

1.6 APR典型配置举例

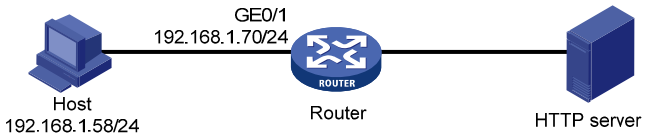
1.6.1 APR典型配置举例

1. 组网需求

主机通过 Router 与外网相连，通过配置 Router 实现丢弃主机向外部网络发送的目的端口为 8080 的 HTTP 连接报文。

2. 组网图

图1-1 APR 典型配置组网图



3. 配置步骤

创建应用组 group1，并进入应用组视图。

```
<Router> system-view
[Router] app-group group1
```

添加 HTTP 应用。

```
[Router-app-group-group1] include application http
[Router-app-group-group1] quit
```

配置 HTTP 应用层协议与 TCP 协议、端口 8080 之间的映射。

```
[Router] port-mapping application http port 8080 protocol tcp
```

定义类 classifier_1，匹配应用组 group1。

```
[Router] traffic classifier classifier_1
[Router-classifier-classifier_1] if-match app-group group1
[Router-classifier-classifier_1] quit
```

定义流行为 bdeny，动作为流量过滤（**deny**），对数据包进行丢弃。

```
[Router] traffic behavior bdeny
```

```
[Router-behavior-bdeny] filter deny
[Router-behavior-bdeny] quit
```

定义策略 1，为类 classifier_1 指定流行为 bdeny。

```
[Router] qos policy 1
[Router-qospolicy-1] classifier classifier_1 behavior bdeny
[Router-qospolicy-1] quit
```

在 GigabitEthernet0/1 入方向上应用 QoS 策略。

```
[Router] interface gigabitethernet 0/1
[Router-GigabitEthernet0/1] qos apply policy 1 inbound
[Router-GigabitEthernet0/1] quit
```

4. 验证配置

以上配置完成后，主机将不能与外部网络建立 HTTP 连接。