H3C MSR 系列路由器

OAA 配置指导(V5)

新华三技术有限公司
http://www.h3c.com

资料版本：20180706-C-1.16
产品版本：MSR-CMW520-R2516

H3C、H3C、H3CS、H3CIE、H3CNE、Aolynk、Aolynk、H^{3}Care、H3care、IRF、NetPilot、Netflow、SecEngine、SecPath、SecCenter、SecBlade、Comware、ITCMM、HUASAN、华三均为新华三技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

H3C MSR 系列路由器 配置指导(V5)共分为十七本手册，介绍了 MSR 系列路由器各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《OAA 配置指导》主要介绍 OAA 架构支持的相关协议如 ACFP、ACSEI 的原理及配置，以及 OAP 单板的配置。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 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 | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。

格　式	意　义
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

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

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 OAP单板

MSR 系列路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	OAP 接口模块	OAA 功能
MSR800	不支持	不支持
MSR 900	不支持	不支持
MSR900-E	不支持	不支持
MSR 930	不支持	不支持
MSR 20-1X	不支持	支持
MSR 20	不支持	不支持
MSR 30	支持	支持
MSR 50	支持（MSR 50-06不支持）	支持（MSR 50-06不支持）
MSR 2600	不支持	不支持
MSR3600-51F	支持	支持

1.1 OAP单板简介

OAA（Open Application Architecture，开放应用架构）是一个开放的软硬件体系。H3C 的 OAA 技术以 H3C 设备为基础，提供了一套完整的软、硬件标准接口。第三方合作厂商可以根据自己的优势生产具有特殊功能的产品，只要这些产品遵循 OAA 标准接口，就可以与 H3C 的设备互相兼容，使单一网络产品的功能得到扩充，为客户创造更大的价值。OAP（Open Application Platform，开放应用平台）是基于 OAA 架构的物理平台。它可以是一台独立的网络设备，也可以是一块插卡，作为设备扩展部件或集成在网络设备中。我们把这种形式的 OAP 称为 OAP 单板。OAP 单板上运行独立的操作系统，客户可根据需要在该操作系统下加载安全、语音等业务软件，为客户提供多样化的服务。同时，OAP 单板插入设备的扩展插槽，通过内部业务接口与设备进行数据交互、状态交互以及控制交互。

1.2 登录OAP单板的操作系统

1.2.1 从设备侧重定向到OAP单板

从设备侧通过以下操作可以重定向连接到单板的操作系统，显示界面将从设备的命令行操作界面切换到 OAP 单板操作系统的操作界面，从而可以对 OAP 单板上的系统及应用软件进行管理。切换以后，可以通过快捷键<Ctrl+k>返回到设备的命令行操作界面。

表1-1 从设备侧重定向到 OAP 单板

操作	命令	说明
从设备侧重定向到OAP单板	**oap connect slot** *slot-number*	必选 该操作在用户视图下执行

1.2.2 通过OAP的管理以太网口以SSH或Telnet方式登录

通过 OAP 单板上的管理以太网口以 SSH 或 Telnet 方式登录 OAP 单板的操作系统，OAP 单板作为 SSH 服务器，配置步骤如下：

(1) 从设备侧重定向到 OAP 单板，开启 OAP 单板的 SSH 或 Telnet 服务器功能，配置可供 SSH 或 Telnet 客户端登录使用的账户。

(2) 用网线将 OAP 单板的管理以太网口接入网络。

(3) 给 OAP 单板的管理以太网口配置 IP 地址，并确保 SSH 或 Telnet 客户端（可以是 H3C 设备或者装有 SSH 或 Telnet 客户端软件的 PC）和管理以太网口之间路由可达。

(4) 建立 SSH 或 Telnet 连接，输入 OAP 管理以太网口的 IP 地址作为 SSH 或 Telnet 服务器地址，连接成功后即可登录单板的操作系统。

1.2.3 通过OAP单板内部以太网口以SSH或Telnet方式登录

OAP 单板安装到设备的扩展插槽后，通过两个内部的业务口与设备进行信息交互。一个是串口，一个是快速以太网口，这种登录方式用到的就是快速以太网口。

通过 OAP 单板内部以太网口以 SSH 或 Telnet 方式登录 OAP 单板的操作系统，OAP 单板作为 SSH 或 Telnet 服务器，配置步骤如下：

(1) 从设备侧重定向到 OAP 单板，开启 OAP 单板的 SSH 或 Telnet 服务器功能，配置可供 SSH 或 Telnet 客户端登录使用的账户。

(2) 给 OAP 单板的快速以太网口配置 IP 地址。

(3) 用网线将 PC 和设备上的以太网口连接起来。

(4) 确保 PC 与内部业务口中的快速以太网口之间路由可达。

(5) 在 PC 上使用 SSH 或 Telnet 客户端功能输入 OAP 单板的快速以太网口的 IP 地址作为 SSH 或 Telnet 服务器地址，连接成功后即可登录单板的操作系统。

1.3 复位OAP单板系统

在操作系统出现故障或其他异常情况下，如不响应用户操作，可以通过下面的命令复位 OAP 单板系统，使得 OAP 单板再次上电启动。该操作相当于使用 OAP 单板上的复位按钮进行硬件复位 OAP 单板。

OAP 单板有独立的 CPU 系统，复位 OAP 单板系统，设备侧仍然可以对 OAP 单板进行识别和控制。

表1-2 复位 OAP 单板系统

操作	命令	说明
复位OAP单板系统	**oap reboot slot** *slot-number*	必选 该操作在用户视图下执行

注意

执行复位操作前，请先对 OAP 单板操作系统执行关机操作（poweroff），以免硬盘数据丢失。

目 录

1 ACFP

MSR 系列路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR800	ACFP	不支持
MSR 900		支持
MSR900-E		不支持
MSR 930		不支持
MSR 20-1X		支持
MSR 20		不支持
MSR 30		支持（仅MSR30-11、MSR30-11E和MSR30-11F不支持）
MSR 50		支持（仅MSR 50-06不支持）
MSR 2600		不支持
MSR3600-51F		不支持

1.1 ACFP简介

数据通信的基础网络主要由路由器和交换机组成，由这些设备完成数据报文的转发。随着数据网络的逐步发展，数据网络上运行的业务越来越多，但是传统的路由器、交换机并不适合处理很多新兴业务，因此产生了一些专门处理某些业务的产品，如防火墙、IDS（Intrusion Detection System，入侵检测系统）、IPS（Intrusion Prevention System，入侵防御系统）等安全产品及语音、无线等产品。

为了更好地支撑新兴业务，传统网络设备（这里指路由器、交换机）生产厂家纷纷推出多种专用业务板（卡），或者提供一套软硬件接口，允许其他厂家提供板（卡）或者设备的硬件或软件，插入或连接到传统网络设备上，协作处理这些业务，从而能发挥各厂家在各自领域的优势，更有效地支撑新兴业务，同时减少用户投资。OAA（Open Application Architecture，开放应用架构）就是基于该思想而提出的开放业务架构，它能够让众多不同厂商生产的设备和软件集成在一起，象一台设备那样工作，为客户提供一体化的解决方案。

ACFP（Application Control Forwarding Protocol，应用控制转发协议）是基于 OAA 架构设计的应用控制转发协议。例如，联动的 IPS/IDS 卡或者 IPS/IDS 设备作为 ACFP 客户端，上面运行其他厂家的软件，支撑 IPS/IDS 业务。路由器或交换机收到 IP 报文后，通过匹配 ACFP 的联动策略规则，将报文镜像或重定向给 ACFP 客户端，ACFP 客户端上的软件对报文做监控、检测等业务处理，然后根据监控、检测的结果，再通过联动 MIB（Management Information Base，管理信息库）反馈给路由器或交换机，指示路由器或交换机做出相应处理（如过滤某些报文）。

1.1.1 ACFP体系结构

图1-1 ACFP 体系结构示意图

如 图 1-1 所示，ACFP体系可以分成三部分：

- 路由交换部件：是路由器和交换机的主体部分，这部分有着完整的路由器或交换机的功能，也是用户管理控制的核心，此部分称为 ACFP server；
- 独立业务部件：是可以开放给第三方合作开发的主体，主要用来提供各种独特的业务服务功能，此部分称为 ACFP client；
- 接口连接部件：是路由交换部件和独立业务部件的接口连接体，通过这个部件将两个不同厂商的设备连接在一起，以形成一个整体。

1.1.2 ACFP联动

ACFP 联动就是指独立业务部件可以向路由交换部件发指令，改变路由交换部件的功能。联动功能主要是通过 SNMP 协议实现的：独立业务部件仿照网管系统的功能，向路由交换部件发送各种 SNMP 命令；而路由交换部件上支持 SNMP Agent 功能，可以执行收到的这些命令。在这个过程中，联系双方的关键就是联动的 MIB。

1.1.3 ACFP管理

ACFP 联动提供了一套机制，使得 ACFP client 能够控制 ACFP server 上的流量，包括：

- 将 ACFP server 上的流量镜像、重定向到 ACFP client；
- 允许、拒绝 ACFP server 上的流量通过；
- 对 ACFP server 上的流量进行限速；
- 在报文中携带上下文 ID，通过上下文 ID 使得 ACFP server 和 ACFP client 能互通报文上下文环境。具体过程如下：ACFP server 中维护一个上下文表，通过上下文 ID 查询上下文表，每个上下文 ID 对应一个 ACFP 联动策略（联动策略的内容包括报文入接口、报文出接口、联动规则等信息）。当 ACFP server 收到的报文由于匹配某个联动规则而被重定向或镜像到 ACFP client 时，报文中会携带该联动规则所在联动策略对应的上下文 ID；当被重定向的报文从 ACFP client 返回时，报文中也会携带该上下文 ID，通过上下文 ID，ACFP server 就知道该报文是重定向返回的报文，然后进行正常的转发处理。

为便于 ACFP client 更好地控制流量，联动内容中设置联动策略与联动规则两级组织，基于策略管理匹配规则的流量，达到一种弹性管理的目的。

为有效支撑 Client/Server 这种联动模式，细粒度、弹性地设置各种规则，联动内容分成四块组织：ACFP server 信息、ACFP client 信息、ACFP 联动策略、ACFP 联动规则。这四块内容存储在 ACFP server 中。

由于一个 ACFP server 可以支持多个 ACFP client，因此，ACFP client 信息、ACFP 联动策略、ACFP 联动规则都是以表的形式组织的。

ACFP server 信息由 ACFP server 自己生成，ACFP client 信息、ACFP 联动策略、ACFP 联动规则都是由 ACFP client 生成并通过联动 MIB 或联动协议发送到 ACFP server。

1.1.4 ACFP信息概述

1. ACFP server信息

ACFP server 信息包含的内容及其含义如下：

- 所能支持的工作模式：分为主机、穿透、镜像和重定向四种。ACFP server 可以同时支持其中的多种工作模式。只有当 ACFP server 所支持的工作模式包含 ACFP client 的工作模式时，这两个主体才能进行联动。
- 联动策略的最长有效期：说明了 ACFP server 的联动策略所能存活的最长时间。
- 联动策略存储的持久性：说明了 ACFP server 是否具备永久保存联动策略的能力，主要指 ACFP server 重新启动后还能否保有原来的联动策略。
- 当前所支持的上下文 ID 的类型为 VLANID-context（使用 VLAN ID 作为上下文 ID），不同的 ACFP server 中，上下文 ID 在报文中所处的位置可能不同。

上述这些信息表明了一个 ACFP server 的联动能力，各 ACFP client 可通过联动协议、联动 MIB 的途径来获取这些信息。

2. ACFP client信息

ACFP client 信息包含的内容及其含义如下：

- ACFP client ID：ACFP client 的标识，可以通过联动协议由 ACFP server 分配，也可以由网络管理员指定，目的都是要确保各 ACFP client 在 ACFP server 中 client ID 的唯一性。
- 描述：ACFP client 的描述信息。
- 硬件版本：ACFP client 的硬件类别及版本号等信息。
- 操作系统版本：ACFP client 的系统名称及版本号等信息。
- 应用软件版本：ACFP client 的应用软件类别名称及其版本号等信息。
- IP 地址：ACFP client 的 IP 地址。
- 支持的工作模式：ACFP client 当前所能支持的工作模式，指主机、穿透、镜像、重定向这些模式的组合。

3. ACFP联动策略

ACFP 联动策略指 ACFP client 发送给 ACFP server 所要实施的联动策略，策略信息包含的内容及其含义如下：

- ACFP client ID：ACFP client 的标识。
- 策略号：策略的标识。
- 策略入接口：报文进入 ACFP server 的接口。
- 策略出接口：报文被正常转发的出接口。
- 策略目的接口：ACFP server 连接该 ACFP client 的接口。

- 报文上下文 ID：会在镜像或重定向报文给 ACFP client 时用到。当发送的策略指定了连接 ACFP client 的接口时，由 ACFP server 为该策略分配一个全局的序号，即报文上下文 ID，每个上下文 ID 对应一个 ACFP 联动策略。
- 策略管理状态：表示该策略是否允许生效。
- 策略有效期：表示该策略有效的期限，借此来控制策略下的所有规则有效期限。
- 策略开始时间：表示该策略生效的起始时间，单位为每天的时、分、秒，借此来控制策略下的所有规则。
- 策略结束时间：表示该策略生效的结束时间，单位为每天的时、分、秒，借此来控制策略下的所有规则。
- 策略目的接口 down 时，该策略下所有规则处理动作：对于转发优先设备，在目的接口 down 后希望重定向和镜像的报文继续转发，此时选择 delete 动作；对于安全优先设备，在目的接口 down 后希望重定向和镜像的报文直接丢弃，此时选择 reserve 动作。
- 策略优先级：表示该策略的优先级，用数字 1～8 表示，数字越大，优先级越高。

4. ACFP联动规则

ACFP 联动规则指 ACFP client 发送给 ACFP server 所要实施的联动规则，联动规则可以分为 3 类：

- 监控规则：即将哪些报文递给 ACFP client 做监控分析及业务处理。该规则对应的动作类型目前有重定向、镜像。
- 过滤规则：即明确哪些报文被丢弃、哪些报文允许通过。该规则对应的动作类型有丢弃、通过。
- 限制规则：即明确哪些报文将被限速。该规则对应的动作类型为限速。

规则信息包含的内容及其含义如下：

- ACFP client ID：ACFP client 的标识；
- 策略号：策略的标识；
- 规则号：规则的标识；
- 规则操作状态：表示规则是否应用成功；
- 动作类型：包括镜像、重定向、丢弃、通过和限速 5 种动作；
- 是否匹配所有报文：表示该规则是否要匹配所有的报文，如果是的话，则不需要进行下面的匹配；
- 源 MAC 地址；
- 目的 MAC 地址；
- 起始 VLAN ID；
- 结束 VLAN ID；
- IP 中的协议号；
- 源 IP 地址；
- 源 IP 地址的通配符掩码；
- 源端口号操作符：类型为等于、不等于、大于、小于、之间，只有类型为之间时，下面的结束源端口号才有意义，标识所匹配的报文的源端口应该大于起始源端口号而小于结束源端口号；
- 起始源端口号；

- 结束源端口号；
- 目的 IP 地址；
- 目的 IP 地址的通配符掩码；
- 目的端口号操作符：类型为等于、不等于、大于、小于、之间，只有类型为之间时，下面的结束目的端口号才有意义，标识所匹配的报文的目的端口应该大于起始目的端口号而小于结束目的端口号；
- 起始目的端口号；
- 结束目的端口号；
- 报文的协议类型：包括 GRE、ICMP、IGMP、OSPF、TCP、UDP、IP 等；
- IP 优先级：报文优先级，用数字表示，取值范围为 0～7；
- IP ToS：IP 报文的服务类型；
- IP DSCP：IP 报文的差分服务编码点；
- TCP 标志：表示关心 TCP 六个标志位（URG、ACK、PSH、RST、SYN 和 FIN）中的某些位；
- IP 分片：是否是 IP 分片报文；
- 限制速率。

联动规则隶属于联动策略，通过联动策略可以管理策略下的规则。

1.1.5 ACFP使用说明

- ACFP 策略在 GRE 隧道环境中应用时只能配置在 Tunnel 口上。
- ACFP 不支持策略路由业务和 Netstream 业务。
- ACFP 重定向的报文处理和部分 QoS 处理（FR-DE 匹配、ATM-CLP 匹配、入接口匹配、QoS local-id 及本地优先级等）互斥，重定向到 ACFP client 后返回的报文不进行上述 QoS 处理。
- ACFP 重定向或镜像的报文在目的接口仅支持二层 QoS 处理（包括队列、WRED 等），不支持其它业务处理（包括非二层的 QoS 处理及非 QoS 业务的处理）。
- ACFP 不支持将同一个流镜像或重定向到多个 ACFP client。
- ACFP 不能处理本地发出的报文。

1.2 ACFP配置任务简介

表1-1 ACFP 配置任务简介

配置任务	说明	详细配置
配置ACFP server	必选	1.3
配置ACFP client	必选	1.4
开启ACFP Trap功能	可选	1.5

1.3 配置ACFP server

表1-2 配置 ACFP server

操作	命令	说明
进入系统视图	**system-view**	-
使能ACFP server功能	**acfp server enable**	必选 缺省情况下，ACFP server功能处于关闭状态

1.4 配置ACFP client

用户需通过 MIB Browser 配置 ACFP client 上的 ACFP 联动策略和规则，具体配置方式与 ACFP client 所使用的业务软件有关。

说明

在关闭 ACSEI 功能或者改变内联口（即 ACFP server 与 ACFP client 相连的接口）的连接模式时，建议先在 ACFP client 上操作，再在 ACFP server 上操作，这样可以有效避免操作过程对流量产生的影响。

1.5 开启ACFP Trap功能

为确保 ACFP 功能正常运行，必须允许设备发送 ACFP 模块的 Trap 报文。

开启ACFP模块的Trap功能后，该模块会生成Trap报文，用于报告该模块的重要事件。ACFP Trap 报文对应的级别如 表 1-3 所示。

表1-3 ACFP Trap 报文对应的级别

Trap 报文	级别
上下文ID类型改变	notifications
ACFP client注册	notifications
ACFP client注销	notifications
ACSEI协议检测到ACFP client没有响应	warnings
ACFP server不支持ACFP client的工作模式	errors
ACFP联动策略的有效期改变	notifications
ACFP联动规则创建	informational
ACFP联动规则删除	informational
ACFP联动规则发生错误	errors
ACFP联动策略的有效期超时	notifications

生成的 Trap 报文将被发送到设备的信息中心，通过设置信息中心的参数，最终决定 Trap 报文的输出规则（即是否允许输出以及输出方向）。有关信息中心各参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。

表1-4 开启 ACFP Trap 功能

操作	命令	说明
进入系统视图	**system-view**	-
开启ACFP模块的Trap功能	**snmp-agent trap enable acfp** [**client** | **policy** | **rule** | **server**]	可选 缺省情况下，ACFP模块的Trap功能处于开启状态


说明

有关 **snmp-agent trap enable** 命令的详细介绍，请参见“网络管理和监控命令参考”中的“SNMP”。

1.6 ACFP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 ACFP 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 ACFP 规则缓存信息。

表1-5 ACFP 显示和维护

操作	命令
查看ACFP server信息	**display acfp server-info** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看ACFP client信息	**display acfp client-info** [*client-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看ACFP策略信息	**display acfp policy-info** [**client** *client-id* [*policy-index*] | **dest-interface** *interface-type interface-number* | **in-interface** *interface-type interface-number* | **out-interface** *interface-type interface-number*] [**active** | **inactive**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看ACFP规则信息	**display acfp rule-info** { **in-interface** [*interface-type interface-number*] | **out-interface** [*interface-type interface-number*] | **policy** [*client-id policy-index*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看ACFP规则缓存信息	**display acfp rule-cache** [**in-interface** *interface-type interface-number* | **out-interface** *interface-type interface-number*] * [**|** { **begin** | **exclude** | **include** } *regular-expression*]
查看ACFP Trap的配置情况	**display snmp-agent trap-list** [**|** { **begin** | **exclude** | **include** } *regular-expression*]
清除ACFP规则缓存信息	**reset acfp rule-cache** [**in-interface** *interface-type interface-number* | **out-interface** *interface-type interface-number*] *

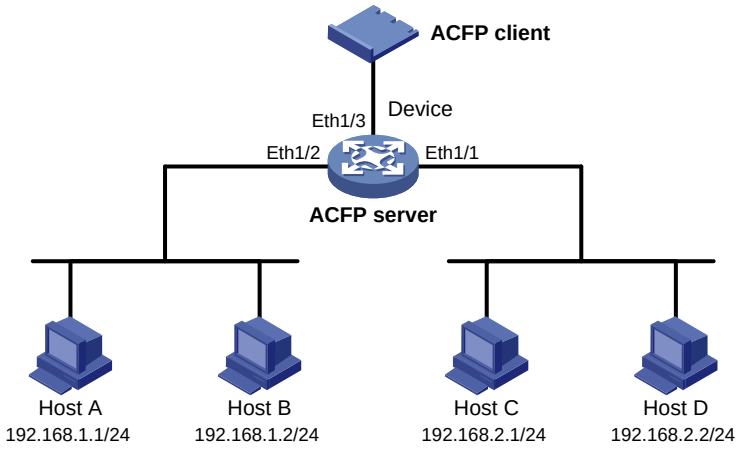
1.7 ACFP典型配置举例

1. 组网需求

- 某企业网通过 Device 实现各部门的互连，该 Device 为 ACFP server；
- ACFP client 与 Device 相连并控制 Device 上的流量，分析入接口为 Ethernet1/2 的流量。ACFP client 经过分析后，允许入接口为 Ethernet1/2、源 IP 为 192.168.1.1/24 的所有报文通过，并拒绝入接口为 Ethernet1/2、源 IP 为 192.168.1.2/24 的所有报文通过。

2. 组网图

图1-2 ACFP 典型配置组网图



3. 配置步骤

(1) 配置 Device

使能 ACFP server 和 ACSEI server 功能。

```
<Device> system-view
[Device] acfp server enable
[Device] acsei server enable
```

(2) 通过 MIB Browser 配置 ACFP client 的联动策略和监控规则

通过将 hh3cAcfpClientRowStatus 节点的值配置为 4，创建一个索引为 1 的 ACFP client；通过将 hh3cAcfpClientMode 节点的值配置为 1，使该 client 的工作模式为重定向。

通过将 hh3cAcfpPolicyRowStatus 节点的值配置为 4，创建一个索引为 1.1 的 ACPF 策略；通过配置 hh3cAcfpPolicyInIfIndex 和 hh3cAcfpPolicyDestIfIndex 节点，分别将该策略的入接口和目的接口设置为 Ethernet1/2 和 Ethernet1/3。

通过将 hh3cAcfpRuleRowStatus 节点的值配置为 4，创建一个索引为 1.1.1 的 ACPF 规则；通过将 hh3cAcfpRuleAction 节点的值配置为 3，使该规则的动作类型为重定向。

(3) 通过 MIB Browser 配置 ACFP client 的联动策略和过滤规则

通过将 hh3cAcfpPolicyRowStatus 节点的值配置为 4，创建一个索引为 1.2 的 ACPF 策略；通过配置 hh3cAcfpPolicyInIfIndex 节点，将该策略的入接口设置为 Ethernet1/2。

通过将 hh3cAcfpRuleRowStatus 节点的值配置为 4，创建一个索引为 1.2.1 的 ACPF 规则；通过将 hh3cAcfpRuleAction 节点的值配置为 1，使该规则的动作类型为允许通过；通过配置

hh3cAcfpRuleSrcIP 和 hh3cAcfpRuleSrcIPMask 节点，分别将该规则所匹配报文的源 IP 地址及其通配符掩码设置为 192.168.1.1 和 0.0.0.255。

通过将 hh3cAcfpRuleRowStatus 节点的值配置为 4，创建一个索引为 1.2.2 的 ACPF 规则；通过将 hh3cAcfpRuleAction 节点的值配置为 2，使该规则的动作类型为拒绝通过；通过配置 hh3cAcfpRuleSrcIP 和 hh3cAcfpRuleSrcIPMask 节点，分别将该规则所匹配报文的源 IP 地址及其通配符掩码设置为 192.168.1.2 和 0.0.0.255。


说明

- 有关 MIB 的详细介绍请参见 “网络管理和监控配置指导”中的 “SNMP”。
- 有关上述 MIB 节点的详情，可通过 MIB Browser 来查看各 MIB 节点属性中的描述字段。

---

(4) 验证配置效果

使用 **ping** 命令验证 Host A 与 Host C、以及 Host B 与 Host C 的连通性。测试结果表明：Host A 与 Host C 可以互通，Host B 与 Host C 则无法互通。

目 录

1 ACSEI

MSR 系列路由器各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR800	ACSEI	不支持
MSR 900		支持
MSR900-E		不支持
MSR 930		不支持
MSR 20-1X		支持
MSR 20		不支持
MSR 30		支持（仅MSR 30-11、MSR30-11E和MSR 30-11F不支持）
MSR 50		支持（仅MSR 50-06不支持）
MSR 2600		不支持
MSR3600-51F		不支持

1.1 ACSEI简介

ACSEI（ACFP Client and Server Exchange Information，ACFP 客户端和服务器端信息交互协议）是 H3C 私有协议，是 ACFP（Application Control Forwarding Protocol，应用控制转发协议）运行的基础：它为 ACFPclient 和 server 提供了一种交互信息的方法，为联动提供很好的支撑。

作为 ACFP 的支撑协议，ACSEI 也包括 server 和 client 两种实体。ACSEI server 和 ACFP server 一起运行，ACSEI client 和 ACFP client 一起运行。

- ACSEI server 集成在设备软件系统（Comware）中，是设备支持的一项功能。
- ACSEI client 有两种实现方式：一种是集成在设备的系统软件（Comware）中，作为设备支持的一项功能；一种是集成在 OAP 单板的软件系统当中，是 OAP 单板支持的一项功能。这两种实现方式所需的硬件条件不同，配置方式也不一样，本文将分别进行介绍。

说明

- ACFP 是基于 OAA（Open Application Architecture，开放应用架构）架构设计的应用控制转发协议，联动的 IDS（Intrusion Detection System，入侵检测系统）卡或者 IDS 设备作为 ACFP 客户端，上面运行其他厂家的软件，支撑 IPS（Intrusion Prevention System，入侵防御系统）/IDS 业务。有关 ACFP 的详细介绍请参见“OAA 配置指导”中的“ACFP”。
- OAP（Open Application Platform，开放应用平台）是针对新兴业务提供的一个开放式应用平台。OAP 单板上运行操作系统，根据客户需要可加载安全、语音等业务软件，为客户提供多样化的服务。有关 OAP 单板的详细介绍请参见“OAA 配置指导”中的“OAP 单板”。

1.1.1 ACSEI的功能

ACSEI 协议主要功能如下：

- ACFP client 向 ACFP server 注册、注销；
- ACFP server 给 ACFP client 分配 ID，用于保证各 ACSEI client 的唯一性与清晰性；
- ACFP client 与 ACFP server 之间的互相监控、互相感知；
- ACFP server 与 ACFP client 之间的信息交互（包括时钟同步等）；
- 通过 ACFP server 对 ACFP client 实施简单的控制，例如，关闭 ACFP client、重启 ACFP client。

ACFP server 与 ACFP client 为一对多的关系，一个 ACFP server 允许注册的 ACFP client 个数对于 MSR 系列路由器各款型有所不同，详细差异信息如下：

型号	特性	描述
MSR 900	一个ACSEI server允许注册的ACSEI client个数	1
MSR 20-1X		1
MSR 30		1 (30-16) 6 (MSR 30-10、30-20、30-40、30-60)
MSR 50		6

1.1.2 ACSEI定时器

ACSEI server 用到两个定时器，分别是时钟同步定时器和监控定时器。

- 时钟同步定时器用来定时触发 ACSEI server 向 ACSEI client 发送时钟同步信息通告报文，用户可以通过命令行设置定时器的值。
- 监控定时器用来定时触发 ACSEI server 向 ACSEI client 发送监控请求报文，用户可以通过命令行设置定时器的值。

ACSEI client 启动两个定时器，分别为注册定时器和监控定时器。

- 注册定时器用来定时触发 ACSEI client 以组播方式（组播 MAC 地址为 010F-E200-0021）发送注册请求报文，用户不能设置定时器的值。
- 监控定时器用来定时触发 ACSEI client 向 ACSEI server 发送监控请求报文，用户不能设置定时器的值。

1.1.3 ACSEI的启动和运行过程

ACSEI 启动和运行的整个过程可描述如下：

(1) 运行 ACSEI client 可执行程序，使能 ACSEI client 功能。

(2) 启动设备，使能 ACSEI server 功能。

(3) ACSEI client 以组播方式发送注册请求。

(4) ACSEI server 收到合法的注册请求后，与 ACSEI client 协商参数，协商通过后建立连接。

(5) 连接建立后相互监控连接的情况。

(6) 当ACSEI server检测到ACSEI client连接中断，ACFP server会将对应ACFP client的配置、策略等删除。

1.2 配置ACSEI server

1.2.1 使能ACSEI server

表1-1 使能 ACSEI server

操作	命令	说明
进入系统视图	**system-view**	-
使能ACSEI server功能	**acsei server enable**	必选 缺省情况下，ACSEI server功能处于关闭状态

1.2.2 配置时钟同步定时器

表1-2 配置时钟同步定时器

操作	命令	说明
进入系统视图	**system-view**	-
使能ACSEI server功能	**acsei server enable**	必选
进入ACSEI视图	**acsei server**	-
配置ACSEI server到ACSEI client的时钟同步定时器的值	**acsei timer clock-sync** *minutes*	可选 缺省情况下，ACSEI server到ACSEI client的时钟同步定时器的值为5分钟

1.2.3 配置监控定时器

表1-3 配置监控定时器

操作	命令	说明
进入系统视图	**system-view**	-
使能ACSEI server功能	**acsei server enable**	必选
进入ACSEI视图	**acsei server**	-
配置ACSEI server对ACSEI client的监控定时器的值	**acsei timer monitor** *seconds*	可选 缺省情况下，ACSEI server对ACSEI client的监控定时器的值为5秒

1.2.4 关闭ACSEI client

表1-4 关闭 ACSEI client

操作	命令	说明
进入系统视图	**system-view**	-
使能ACSEI server功能	**acsei server enable**	必选
进入ACSEI视图	**acsei server**	-
关闭指定的ACSEI client	**acsei client close** *client-id*	必选

注意

本特性仅支持运行 Linux 系统的 ACSEI client。

1.2.5 重新启动ACSEI client

表1-5 重新启动 ACSEI client

操作	命令	说明
进入系统视图	**system-view**	-
使能ACSEI server功能	**acsei server enable**	必选
进入ACSEI视图	**acsei server**	-
重新启动ACSEI client	**acsei client reboot** *client-id*	必选

1.2.6 ACSEI server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 ACSEI server 系统的运行情况，通过查看显示信息验证配置的效果。

表1-6 ACSEI server 显示和维护

配置	命令
显示ACSEI client摘要信息	**display acsei client summary** [*client-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示ACSEI client信息	**display acsei client info** [*client-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.3 配置ACSEI client（OAP单板支持）

OAP 单板是插在设备上的一块单板，主要用于扩展设备的功能。ACSEI client 就作为 OAP 单板的一项功能，集成在 OAP 单板的操作系统上。根据 OAP 单板上安装的操作系统不同，ACSEI client 的配置步骤也不一样，分为两大步：

(1) 登录 OAP 单板的操作系统，请参见“OAA 配置指导”中的“OAP 单板”。

(2) 配置 ACSEI client 功能（OAP 单板缺省已经安装）。当安装的操作系统是 Linux 系统时，请参照以下步骤进行配置。

1.3.1 安装ACSEI client

首先，下载ACSEI client的可执行程序（rpm包）到OAP板上，然后使用Linux命令安装ACSEI client，具体命令行如下：

表1-7 安装 ACSEI client

操作	命令	说明
查询是否已经安装ACSEI client rpm包	**rpm -ql acsei-client**	可选 该操作在OAP单板的Linux系统下执行
卸载已经安装的ACSEI client rpm包	**rpm -e acsei-client**	可选 该操作在OAP单板的Linux系统下执行
安装ACSEI client rpm包	**rpm -ivh** *filename*	可选 缺省情况下，OAP单板上已经安装了ACSEI client程序 该操作在OAP单板的Linux系统下执行
查询ACSEI client版本信息	**rpm -q acsei-client -i**	可选 该操作在OAP单板的Linux系统下执行

说明

- *filename* 为 ACSEI client 对外发布的 rpm 包的名称，如 acsei-client-1.0-0.i386.rpm，其中 1.0-0 为版本号。
- 以上 **rpm** 命令是 Linux 操作系统的命令，请遵循 Linux 命令使用规范，本文档不作详细介绍。

1.3.2 配置默认启动ACSEI client

ACSEI client 在安装后，就已经使能，并且每次单板系统启动后，默认自动引导 ACSEI client 启动，当然用户也可以通过以下的命令行来修改默认配置。

1. 通过命令行修改默认配置

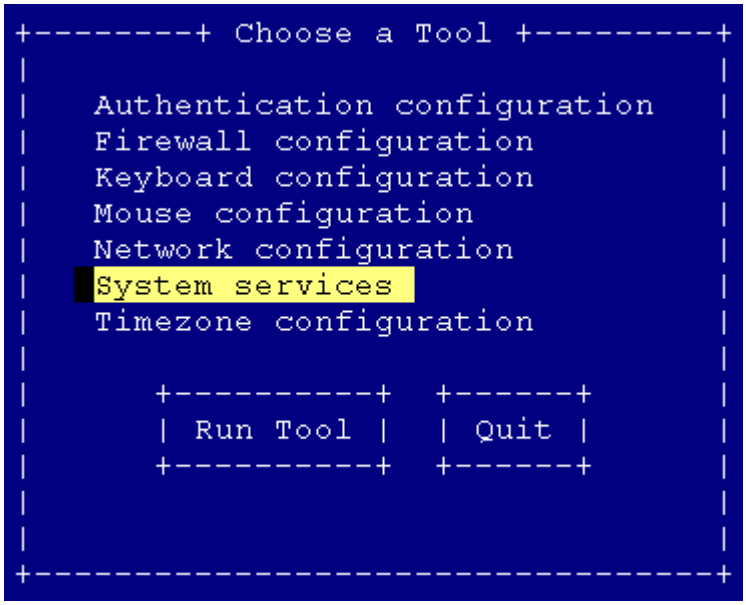
表1-8 配置默认启动 ACSEI client

操作	命令	说明
配置默认不启动ACSEI client	**chkconfig acseid off**	可选 缺省情况下，OAP单板上安装的ACSEI client是默认启动的 该操作在OAP单板的Linux系统下执行
配置默认启动ACSEI client	**chkconfig acseid on**	可选 缺省情况下，OAP单板上安装的ACSEI client是默认启动的 该操作在OAP单板的Linux系统下执行

2. 通过图形界面修改默认配置

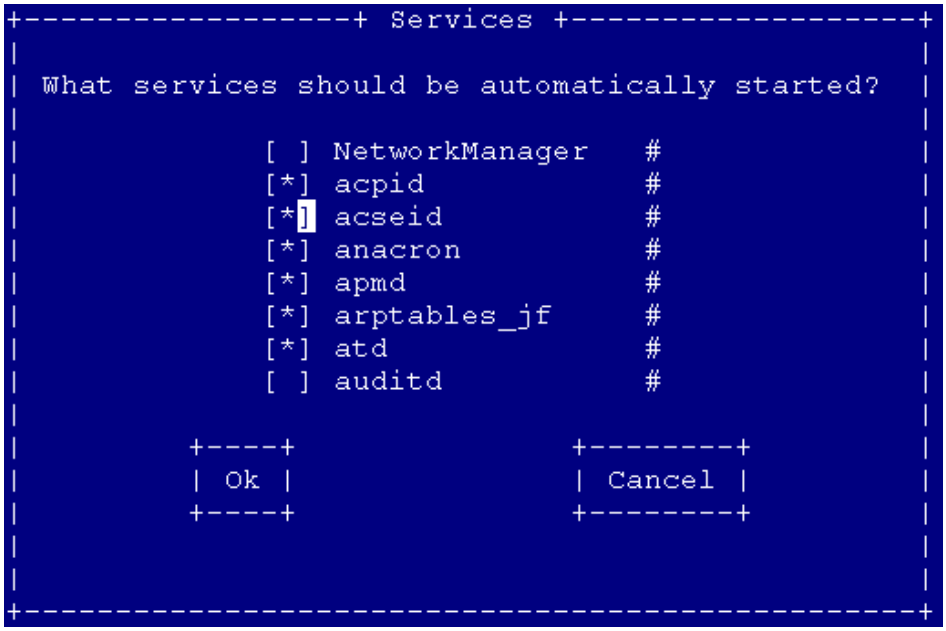
(1) 登录 OAP 单板的 Linux 系统后，在 Linux 系统下执行 setup 命令，出现如下视图：

图1-1 ACSEI client 默认启动配置 setup 界面



(2) 选择 System services，键入<Enter>键，出现如下视图：

图1-2 ACSEI client 默认启动配置 service 界面



(3) 将光标移至 acseid，使用<Space>空格键进行选择，

- [*]表示系统启动时，引导 ACSEI client 启动；
- [ ]表示系统启动时，不引导 ACSEI client 启动。

(4) 确认选项后，使用<Tab>键将光标移至 OK，键入<Enter>，回到上一个视图，再选择 Quit，退出 Setup 界面。

1.3.3 控制ACSEI client

表1-9 控制 ACSEI client

操作	命令	说明
启动ACSEI client	**service acseid start**	可选 缺省情况下，OAP单板上安装的ACSEI client是开启的 该操作在OAP单板的Linux系统下执行
装载ACSEI client配置文件	**service acseid reload**	可选 该操作在OAP单板的Linux系统下执行
重启ACSEI client	**service acseid restart**	可选 该操作在OAP单板的Linux系统下执行
有条件重启ACSEI client	**service acseid condrestart**	可选 该操作在OAP单板的Linux系统下执行
关闭ACSEI client	**service acseid stop**	可选

操作	命令	说明
		该操作在OAP单板的Linux系统下执行

注意

- 当有条件重启 ACSEI client 进程时，如果 ACSEI client 正在运行则关闭进程后，启动该进程；如果 ACSEI client 没有运行，则该命令不执行。
- 请不要在 5 秒内反复重启/关闭 ACSEI client，否则可能会造成其他应用程序无法感知到 ACSEI client 的变化。

1.3.4 ACSEI client显示和维护

在完成上述配置后，在 OAP 单板的 Linux 系统下执行以下命令可以显示配置后 ACSEI client 的运行情况，通过查看显示信息验证配置的效果。

表1-10 ACSEI client 显示和维护

操作	命令
查询ACSEI client的运行状态	**service acseid status**
打开ACSEI client的调试开关	**acsei-client debug enable**
显示ACSEI client的调试信息	**acsei-client debug show**
关闭ACSEI client的调试开关	**acsei-client debug disable**