配置手册

RG-RAP230 系列无线接入点

RGOS11.1(9)B1P7

文档版本 ：V1.0

版权声明

免责声明

您所购买的产品、服务或特性等应受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，锐捷网络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。锐捷网络保留在没有任何通知或者提示的情况下对文档内容进行修改的权利。

本手册仅作为使用指导。锐捷网络在编写本手册时已尽力保证其内容准确可靠，但并不确保手册内容完全没有错误或遗漏，本手册中的所有信息也不构成任何明示或暗示的担保。

前言

读者对象

本书适合下列人员阅读

- 网络工程师
- 技术推广人员
- 网络管理员

技术支持

- 锐捷网络官方网站：http://www.ruijie.com.cn/
- 锐捷网络在线客服：http://webchat.ruijie.com.cn
- 锐捷网络官方网站服务与支持版块：http://www.ruijie.com.cn/service.aspx
- 7 天无休服务热线：4001-000-078
- 锐捷网络技术论坛：http://ryzj.ruijie.com.cn/forum.php
- 常见问题搜索：http://www.ruijie.com.cn/service/know.aspx
- 锐捷网络技术支持与反馈信箱：4001000078@ruijie.com.cn

本书约定

1. 命令行格式约定

命令行格式意义如下：

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。

//：由双斜杠开始的行表示为注释行。

2. 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：

警告标志。表示用户必须严格遵守的规则。如果忽视此类信息，可能导致人身危险或设备损坏。

注意标志。表示用户必须了解的重要信息。如果忽视此类信息，可能导致功能失效或性能降低。

说明标志。用于提供补充、申明、提示等。如果忽视此类信息，不会导致严重后果。

产品/版本支持情况标志。用于提供产品或版本支持情况的说明。

3. 说明

- 本手册举例说明部分的端口类型同实际可能不符，实际操作中需要按照各产品所支持的端口类型进行配置。
- 本手册部分举例的显示信息中可能含有其它产品系列的内容（如产品型号、描述等），具体显示信息请以实际使用的设备信息为准。
- 本手册中涉及的路由器及路由器产品图标，代表了一般意义下的路由器，以及运行了路由协议的三层交换机。

配置指南-WLAN 基础配置

本分册介绍 WLAN 基础配置配置指南相关内容，包括以下章节：

1. APMG
2. STAMG
3. DATA-PLANE
4. WLOG

1 APMG

1.1 概述

无。

1.2 典型应用

无。

1.3 功能详解

基本概念

AP

AP（Access Point）：无线终端访问有线网络的接入点，相当于无线终端与有线网络通信的桥梁。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置AP胖瘦模式	⚠ 可选配置，根据需要对 AP 的胖瘦模式进行切换	
	switch2fat	AC 设备的 AC 配置模式下，配置指定 AP 切换到胖 AP 模式
	ap-mode	AP 设备的全局配置模式下，配置 AP 的胖瘦模式

1.4.1 配置AP模式

配置效果

- AC 设备上，通过 AC 配置模式下 **switch2fat** 命令可配置在线 AP 切换为胖 AP 模式。
- AP 设备上，全局配置模式下，可通过 **ap-mode** 命令对 AP 进行胖、瘦以及 MACC 模式之间两两相互切换的配置。

注意事项

无。

配置方法

- AP 上通过全局配置模式下 **ap-mode** 命令配置。

【命令格式】 **ap-mode** { **fit** | **fat** [**dhcp**] | **macc** }

【参数说明】 **fit**：切换为瘦 AP 模式

fat：切换为胖 AP 模式

dhcp：**ap-mode fat** 命令携带该选择（即 **ap-mode fat dhcp**），则配置 AP 切换为胖 AP 模式后，AP 缺省使用 DHCP 获取 IP 地址；否则配置 AP 切换为胖 AP 模式后，AP 缺省使用静态 IP 地址；、

macc：切换为 macc 模式

【缺省配置】 无

【命令模式】 AP 的全局配置模式

【使用指导】 在进行模式切换之后，需要重启以保证配置的一致性。

我司 WALL-AP 型号 AP，在 AP 为胖 AP 模式时，后端有线接口（连接 POE 交换设备的有线接口）默认 IP 地址为 192.168.110.1/255.255.255.0，前端有线网络接口（产品正面提供的以太网口）默认 IP 地址为 192.168.111.1/255.255.255.0。

如果配置了 **ap-mode fat dhcp**，那么 AP 切换为胖 AP 模式时，缺省以 DHCP 方式获取地址，同时 AP 在重启之后，如果没有相关配置，同样缺省以 DHCP 方式获取地址，另外需要注意两点：1.如果 WALL-AP 型号 AP 配置了 **ap-mode fat dhcp**，只有后端有线接口缺省使用 DHCP，前端有线网络接口缺省使用静态地址。2.Fit/fat/fat dhcp/macc 两两模式之间切换会删除当前配置，并重启，重启后 AP 加载对应模式的默认配置。

检验方法

- 在 AP 上通过 **show ap-mode** 命令查看 AP 的当前胖瘦模式。

配置举例

AP 上配置 AP 切换到瘦 AP 模式

【配置方法】
- 进入全局配置模式
- 配置 **ap-mode** 命令

AP

```
Ruijie(config)#ap-mode fit
```

【检验方法】 在 AP 上通过 **show ap-mode** 命令查看 AP 的胖瘦模式

AP

```
Ruijie#show ap-mode
current mode: fit
```

常见错误

- 无。

1.5 监视与维护

清除各类信息

- 无。

查看运行情况

作用	命令
查看 AP 胖瘦模式	**show ap-mode**

查看调试信息

- 无。

2 STAMG

2.1 概述

STAMG(Sta Manage，无线用户管理)是对无线用户进行管理的功能，主要包含 STA 接入控制的管理以及 STA 的事件通告，事件通告主要服务于其他模块。STAMG 功能适用于：

- 动态黑名单适用于对安全性要求较高的网络中，避免用户攻击。
- STA 数量限制适用于用户数超过 AP 容量的情况下。
- 负载均衡适用于用户需要均衡的分布到多台 AP 上的场景。
- 关联控制适用于电子书包场景中。

协议规范

- 无。

2.2 典型应用

无。

2.3 功能详解

基本概念

无。

功能特性

功能特性	作用
radio间负载均衡	能够让 STA 均衡地分布在同一 AP 的各 radio 间。
关联控制	能够让从 STA 跟着主 STA 关联到同一组 AP 上。
智能隐藏SSID	当 AP 或者 radio 上的用户数达到上限时，隐藏 SSID。

2.3.1 Radio间负载均衡

Radio 间负载均衡是对 AP 内各个 radio 之间的负载进行的均衡，可以按一定比例进行均衡，目的是避免单一 radio 的负载过大。同样，这里的负载可以是流量，也可以是关联的 STA 个数。

工作原理

Radio 间负载均衡的原理与均衡组负载均衡基本相同，但用户可以分别配置同频 radio(同为 2.4G 或 5G)和不同频 radio 的负载均衡启动门限值和阈值。可以配置 radio 间的负载比例，负载比例即为 radio 的权重的比例，radio 的权重默认为 100，比如把 radio 1 的权重配置为 50，则 radio 1 和 radio 2 的负载比例为 1:2，负载均衡时将尽量按照 1:2 的比例进行负载。

2.3.2 关联控制

关联控制，是控制无线 STA 关联行为的一种方法。通过对 STA 进行分组，定义其中一台 STA 为主 STA，其他 STA 为从 STA，控制从 STA 只能跟随主 STA 的方式，使得从 STA 关联的无线网络必须与主 STA 关联的无线网络相同，从而达到控制。

工作原理

将无线网络需要覆盖的范围划分成若干个关联控制域，在每个关联控制域中部署一台或多台 AP，再对无线终端进行分组，严格控制终端能关联的控制域。比如，学校的电子书包应用，一个学校有很多个教室，每个教室里都安装有无线 AP，无线信号是在空间中传播的，当两个相邻的教室都在用电子书包上课时，理想的状况是，教师机和学生机都关联到本教室的 AP 上，这样，每个教室各上各的课，互不干扰。这就要求一个教室就是一个关联控制域，这个教室里的所有学生机和教师机都关联到本教室的无线 AP 上。

关联控制的目的是为了防止终端在有多个无线网络选择的情况下进行胡乱关联，对于网络配置是有一定前提的。主要包括如下：

- AC 会根据预先配置的关联控制域和终端包信息，将所有终端包中的主 STA 信息都下发到所有关联控制域的 AP 上，并将这些 AP 上生成该主 STA 的白名单信息。
- 由于所有终端包的主 STA 信息已经在 AP 的白名单列表中，应用关联控制功能时，需要主 STA 首先与指定控制域对应的 SSID 进行关联；主 STA 完成关联后，AC 会根据该主 STA 所在的终端包配置，将对应的所有从 STA 下发到该关联控制域的所有 AP 上并生成白名单列表，从而允许从 STA 关联到本控制域中来。
- 当主 STA 解关联下线后，所有对应的从 STA 也都会跟着下线，并从关联控制域的 AP 上的白名单列表中删除。
- 上述的过程可以简单地概括为从 STA 跟着主 STA 走，主 STA 关联到哪个关联控制域的 AP 上，从 STA 也必须跟着关联到这个控制域的某个 AP 上，因为只有在这个关联控制域的 AP 上才有对应从 STA 的白名单列表，其他关联控制域的 AP 上没有，这样就可以保证 STA 不会胡乱关联。

2.3.3 智能隐藏SSID

当 AP 或者 radio 上的用户数达到上限时，不允许新用户上线，但是用户仍然可以扫描到 SSID，并尝试关联。开启智能隐藏 SSID 后，新用户将扫描不到这个信号，也就不会尝试关联，避免用户点击关联，却又关联不上。

工作原理

当 AP 或者 radio 达到用户数上限时，AP 上放出的 beacon 帧不携带 ssid，终端发 probe request，AP 也不应答 probe response。

2.4 配置详解

配置项	配置建议 & 相关命令	
Radio间负载均衡	⚠ 必须配置。用于开启 radio 间负载均衡功能。	
	inter-radio-balance num-balance enable	开启 radio 间数量负载均衡功能
	⚠ 可选配置。用于配置负载均衡参数。	
	inter-radio-balance num-balance dual-band	配置不同频 radio 间数量负载均衡参数
	inter-radio-balance num-balance same-band	配置同频 radio 间数量负载均衡参数
关联控制	⚠ 必须配置。用于开启关联控制功能。	
	package	配置终端包
	primary-sta	配置终端包中的主 STA
	secondary-sta	配置终端包中的从 STA
	control-zone	配置关联控制域
	ap	配置 AP 信息
	assoc-control	开启关联控制
智能隐藏SSID	**hide-ssid sta-reach-limit [radio { 2.4g | 5g }]**	配置智能隐藏 SSID

2.4.1 Radio间负载均衡

配置效果

- 开启 radio 间负载均衡的 AP 上，各 radio 之间的负载将尽可能均衡。
- 配置 radio 间负载比例，radio 之间的负载将尽量可能按比例进行均衡。

注意事项

- 智分场景不适用此功能。由于不同 radio 的信号覆盖不同空间范围，STA 可能只能收到一个或几个 radio 的信号，此时不能开启 radio 间负载均衡功能。
- 负载均衡只对 STA 上线过程进行处理，对于 STA 下线过程不进行处理，因此 STA 下线之后，会存在 AP 间的流量差值或者 STA 数量差值超过阈值的情况。
- 若 STA 意图关联的 radio 与最低负载 radio 类型不同，则仅当 AP 上报 STA 能力为双频时，才进行负载均衡。否则，仅支持 2.4G 的用户可能会在 5G 的 radio 没有用户的情况下，无法关联到 2.4G 的 radio。

- 负载均衡参数的配置区分同频 radio 和不同频 radio，在进行负载均衡时，根据目标 radio 和 STA 关联的 radio 的类型，来决定使用哪个均衡参数，从而决定是否要将 STA 引导到目标 radio 上。
- radio 间负载均衡在 5min 内对同一 STA 最多只会连续拒绝关联 2 次，若 STA 第 3 次仍关联到负载较高的 radio，将允许关联。因此，radio 间负载均衡的实际效果与 STA 的具体行为有关。

配置方法

开启 radio 间数量负载均衡

- 在胖 AP 上配置，必须配置。开启后同一 AP 的不同 radio 之间将尽可能保持用户数均衡。
- 可以针对单个 AP 开启。

【命令格式】 **inter-radio-balance num-balance enable**
【参数说明】 -
【缺省配置】 没有开启 radio 间数量负载均衡
【命令模式】 全局配置模式
【使用指导】 -

调整 radio 间负载均衡参数

- 在胖 AP 上配置，可选配置。进行网络优化时可以按实际需求调整各参数。
- 使用 **inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num* 配置不同频 radio 数量负载均衡的启动门限值和阈值。门限值越低则负载均衡越容易启动，阈值越低则越均衡。
- 使用 **inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num* 配置同频 radio 数量负载均衡的启动门限值和阈值。门限值越低则负载均衡越容易启动，阈值越低则越均衡。

【命令格式】 **inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num*
【参数说明】 en-num：启动门限值，范围 1-100。
thrs-num：负载阈值，范围 1-100。
【缺省配置】 缺省启动门限值为 20，负载阈值为 8
【命令模式】 全局配置模式
【使用指导】 -

【命令格式】 **inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num*
【参数说明】 en-num：启动门限值，范围 1-100。
thrs-num：负载阈值，范围 1-100。
【缺省配置】 缺省启动门限值为 20，负载阈值为 6
【命令模式】 全局配置模式
【使用指导】 -

配置 radio 间的负载比例

- 在胖 AP 上配置，可选配置。配置后同一 AP 的不同 radio 之间将尽可能按照权重比例进行均衡。

- 可以针对单个 AP 开启。

【命令格式】 **inter-radio-balance radio** *radio-id* **weight** *weight-num*
【参数说明】 -
【缺省配置】 Radio 的权重为 100，radio 间按照 1:1 进行负载均衡
【命令模式】 全局配置模式
【使用指导】 -

检验方法

- 数量负载均衡：**show ap-config summary** 查看开启均衡的 AP 下各 radio 的 STA 数的差值是否在阈值范围内。
- 流量负载均衡：**show ac-config client** 查看开启均衡的 AP 下各 radio 的流量差值是否在阈值范围内。

配置举例

- 无。

常见错误

- 无。

2.4.2 关联控制

配置效果

- 从 STA 上线受主 STA 上线影响，跟着主 STA 关联到同一组的 AP 中。

注意事项

- 删除终端包时，所有与该终端包相关的配置都将被清除，而且如果这个时候该终端包中有 STA 在线，则会造成所有这些 STA 下线。
- 一部终端包对应只能配置一个主 STA，如果多次配置不同的主 STA 信息，则以最后一次的配置为准。
- 从一个终端包中删除主 STA 时，则可能会造成该 STA 下线，同时也会造成所有从 STA 下线。
- 从一个终端包中删除一个从 STA 时，可能会造成该 STA 下线。
- 关联控制域不能重名，否则将得出到一个错误提示。另外，删除关联控制域时，所有与该控制域相关的配置将被清除，而且可能会导致关联到该控制域中的终端包对应的 STA 下线。
- 删除一个关联控制域中的 AP 信息时，可能会导致关联在该 AP 上的终端包对应的 STA 下线。

配置方法

配置终端包

- 在胖 AP 上配置，必须配置。
- 配置终端包之后，才能配置主从 STA 信息。

【命令格式】 **package** *pkg-name*
【参数说明】 *pkg-name*：终端包名称，长度：1-32。
【缺省配置】 无配置终端包
【命令模式】 全局配置模式
【使用指导】 -

配置终端包中的主从 STA

- 在胖 AP 上配置，必须配置。
- 使用 **primary-sta** 命令配置主 STA。只能配置一台主 STA，从 STA 会跟随主 STA 关联到同一组 AP 上。
- 使用 **secondary-sta 命**令配置从 STA。配置了从 STA，从 STA 会跟随主 STA 关联到同一组 AP 上。

【命令格式】 **primary-sta** *mac-address*
【参数说明】 *mac-address*：STA 的 MAC 地址。
【缺省配置】 没有配置主 STA
【命令模式】 终端包配置
【使用指导】 -

【命令格式】 **secondary-sta** *mac-address*
【参数说明】 *mac-address*：STA 的 MAC 地址。
【缺省配置】 没有配置从 STA
【命令模式】 终端包配置
【使用指导】 -

配置关联控制域

- 在胖 AP 上配置，必须配置。
- 配置管理控制域。
- 只有配置了关联控制域之后，才能将 AP 加入到关联控制域中。

【命令格式】 **control-zone** *czone-name*
【参数说明】 *czone-name*：关联控制域名称，长度：1-64。
【缺省配置】 无关联控制域配置
【命令模式】 全局配置模式
【使用指导】 -

将 AP 加入关联控制域中

- 在胖 AP 上配置，必须配置。
- 将 AP 加入到关联控制域中。
- 只有加入到关联控制域中的 AP，才能进行关联控制。

【命令格式】 **ap** *WORD*
【参数说明】 *WORD*：AP 名称，长度：1-64。
【缺省配置】 没有 AP 加入到关联控制域中
【命令模式】 关联控制域配置模式
【使用指导】 -

开启关联控制功能

- 在胖 AP 上配置，必须配置。只有使用 **assoc-control** 这个命令才能开启关联控制功能。
- 开启关联控制功能。

【命令格式】 **assoc-control**
【参数说明】 -
【缺省配置】 关联控制功能关闭
【命令模式】 全局配置模式
【使用指导】 -

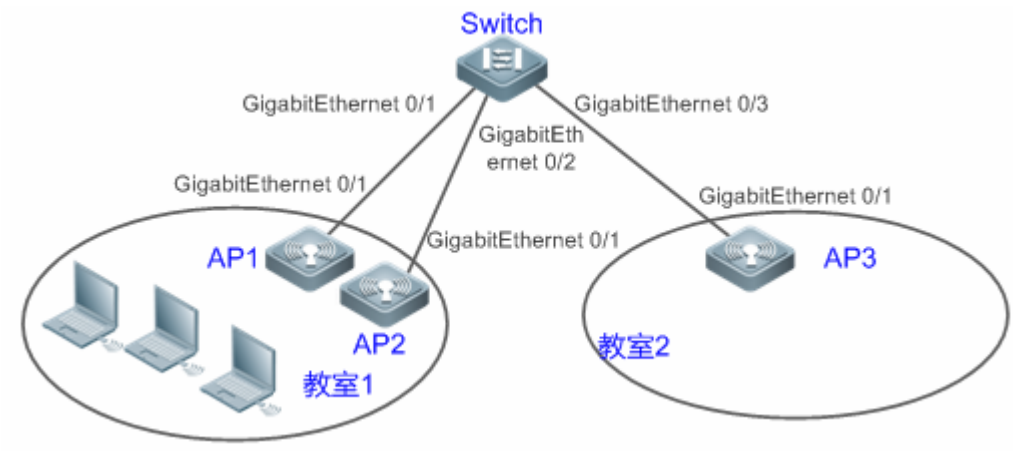
检验方法

- 确认从 STA 能够跟着主 STA 关联到同一组 AP 上。

配置举例

配置胖 AP 架构电子书包

【网络环境】
图 2-1



【配置方法】
- 配置终端包以及对应的主 STA 和从 STA。

- 配置关联控制域以及对应的 AP 信息。
- 开启关联控制功能。

AP1

```
AP1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP1(config)# package 推车 1
AP1(config-package)# primary-sta 00d0.f800.0001
AP1(config-package)# secondary-sta 00d0.f800.0002
AP1(config-package)# secondary-sta 00d0.f800.0003
AP1(config-package)# exit
AP1(config)# control-zone 教室 1
AP1(config-czone)# ap AP1
AP1(config-czone)# exit
AP1(config)# assoc-control
```

AP3

```
AP3# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AP3(config)# package 推车 1
AP3(config-package)# primary-sta 00d0.f800.0001
AP3(config-package)# secondary-sta 00d0.f800.0002
AP3(config-package)# secondary-sta 00d0.f800.0003
AP3(config-package)# exit
AP3(config)# control-zone 教室 2
AP3(config-czone)# ap AP3
AP3(config-czone)# exit
AP3(config)# assoc-control
```

【检验方法】

- 显示验证关联控制运行状态。
- 显示验证终端包配置。
- 显示验证关联控制域配置

AP1

```
AP1# show assoc-control
Association control is enabled.
AP1# show package
total package num : 1
========= 推车 1 =========
primary STA : 00d0.f800.0001
secondary STA num : 2
00d0.f800.0002
00d0.f800.0003
AP1# show control-zone
control zone num : 1
control-zone AP
-------------      ------------------------
```

AP3

```
教室 1                AP1   00d0.f800.889e
AP3# show assoc-control
Association control is enabled.
AP3# show package
total package num : 1
========= 推车 1 =========
primary STA : 00d0.f800.0001
secondary STA num : 2
00d0.f800.0002
00d0.f800.0003
AP3# show control-zone
control zone num : 1
control-zone AP
-------------      ------------------------
教室 2                AP3   00d0.f800.889f
```

常见错误

- 无。

2.4.3 智能隐藏SSID

配置效果

- 当 AP 或者 RADIO 达到用户数上限时，新用户扫描不到 SSID。

注意事项

- 这个功能需要 AC/AP 的版本都支持，功能才会生效。

配置方法

↘ 开启智能隐藏 ssid

- 在胖 AP 上配置，可选配置。
- 开启智能隐藏 ssid。

【命令格式】 **hide-ssid sta-reach-limit [radio { 2.4g | 5g }]**

【参数说明】 radio: 指定命令在特定 radio 上开启此功能，不指定时在所有 radio 上开启

2.4g: 2.4g 的 radio 上开启此功能

5g: 5g 的 radio 上开启此功能

【缺省配置】 未开启智能隐藏 SSID 功能
【命令模式】 全局配置模式
【使用指导】 开启智能隐藏 SSID 功能后，如果一个区域的 AP 都达到用户数上限，新用户在这个区域扫描不到 SSID。

检验方法

- 通过 show running / show ap-config running 检查该配置是否配置成功。

配置举例

无。

2.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看当前的关联控制功能开启情况	**show assoc-control**
查看关联控制域配置	**show control-zone** [**summary** | *czone-name*]
查看终端包配置	**show package** [*pkt-name*]

查看调试信息

无。

3 DATA-PLANE

3.1 概述

data-plane 是一种对广播转发报文的控制功能，它包括广播转发比重控制，广播无线转发控制。

广播转发比重控制，是限定广播转发中不同类型报文的比重，避免某种类型的报文占用所有资源，而影响用户使用。

广播无线转发控制，是仅将必要的报文转发到无线，以避免一些无用的广播报文占用大量的无线射频资源。

- 广播转发比重控制适用于所有需要广播洪泛的报文。
- 广播无线转发控制适用于所有需要发往无线空口的报文。

协议规范

- 无

3.2 典型应用

无。

3.3 功能详解

基本概念

↘ 广播转发比重控制

在网络交换设备中，需要进行广播洪泛的报文可能有广播、组播以及部分单播报文。针对每种类型报文设置广播转发比重，避免某类广播报文将所有广播转发能力耗尽，以提升用户使用网络的体验。

↘ 广播无线转发控制

广播无线转发控制功能只将必需的广播报文转发到无线网络，避免广播报文占用大量的无线空口资源，为 STA 提供更好的网速。

功能特性

功能特性	作用
广播转发比重	限制不同类型报文广播转发中的比重，避免某种类型报文独占广播资源，而影响其他报文的正常转发。
广播无线转发	限制广播报文是否转发到无线网络，避免无用广播报文占用大量无线射频资源。

3.3.1 广播转发比重控制

广播转发比重控制是用来对某种类型的报文进行限制，保证该类型报文在广播转发中不能超过设置的比重。

工作原理

广播转发比重控制先对报文进行分类。

- 报文分类，大致可分为以下几类：单播报文、组播报文、广播报文、未知名组播、未知名单播。
- 为每个报文类分配一个令牌桶，记录这个时刻可以通过的报文个数。
- 在每个单位周期内，会根据配置的广播转发比重，算出每个单位周期内可以通过的报文个数，来增加令牌桶的大小。
- 当有报文到达时，先判断该报文的类型，并查看相应类型的令牌桶是否令牌，若有令牌，则允许报文通过，并将令牌桶减少；若已无令牌，则将报文进行丢弃。

3.3.2 广播无线转发控制

广播无线转发控制是只将部分影响用户的广播报文转发到无线网络，来避免无用的广播报文占用大量的空口资源。

工作原理

由于无线网络的特殊性，在同一个网络的 STA（包括 AP）共享空口资源，而由于无线和有线网络性能上的差异，空口资源往往成为 STA 性能的瓶颈。而对于广播报文，通常是以低速率来进行发送，因此，广播报文的发送会占用更多的空口时间。

从实际应用来看，有部分的广播报文对无线用户来说是无用的，因此，若将这些广播报文转发到无线，将导致用户可用的空口资源变少，影响用户体验。

为了解决这个问题，对广播报文进行分类控制，只将某些特定的广播报文转到无线网络。

3.4 配置详解

配置项	配置建议&相关命令	
广播转发比重控制	⚠ 可选配置。用来设置不同类型广播转发报文的比重。	
	data-plane queue-weight	AP 上，配置不同类型广播转发比重
	data-plane token	AP 上，配置广播转发令牌桶的更新周期和倍数
广播无线转发控制	⚠ 可选配置。用来设置广播无线转发。	

	data-plane wireless-broadcast	AP 上，开启或关闭广播无线转发控制

3.4.1 配置广播转发比重

配置效果

- 用户可根据实际网络情况，限制某种报文广播转发的比重，防止由于过分突发流量所引发的网络拥塞。

注意事项

- 无。

配置方法

↘ 配置广播转发比重

- 可选配置。
- 如果用户需要调整广播报文的转发比重时，可进行配置。

【命令格式】 **data-plane queue-weight** *unicast-packet-weight multicast-packet-weight broadcast-packet-weight unknown-multicast-packet-weight unknown-unicast-packet-weight*

【参数说明】 *unicast-packet-weight：单播报文转发比重，范围为 1-100，缺省值为 16*
multicast-packet-weight：组播报文转发比重，范围为 1-50，缺省值为 4
broadcast-packet-weight：广播报文转发比重，范围为 1-50，缺省值为 2
unknown-multicast-packet-weight：未知名组播报文转发比重，范围为 1-25，缺省值为 1
unknown-unicast-packet-weight：未知名单播报文转发比重，范围为 1-25，缺省值为 1

【缺省配置】 使用默认参数

【命令模式】 全局模式

【使用指导】 -

↘ 配置广播转发令牌桶的更新周期和倍数

- 可选配置。
- 如果用户需要调整广播报文的控制粒度，可进行配置。

【命令格式】 **data-plane token** *token-interval token-base-rate*

【参数说明】 token-interval：广播转发令牌桶的更新周期，缺省值为 1，单位是 10ms
token-base-rate：广播转发令牌桶的倍数，AC 缺省值为 64，AP 缺省值为 5

【缺省配置】 使用默认参数

【命令模式】 全局模式

【使用指导】 设备每秒钟允许的广播报文速率为：报文比重 × (1 秒 / 令牌桶更新周期) × 令牌桶更新倍数

检验方法

- 使用 **show run** 查看相应的配置。

配置举例

无。

常见错误

- 无。

3.4.2 配置广播无线转发

配置效果

- 无用广播报文不会转发向空口。

注意事项

- 无。

配置方法

↘ 广播转发功能

- 可选配置。
- 默认配置会限制网络中的广播报文。
- 如果用户希望对网络中的广播报文不作限制，可进行配置。
- 在全局配置模式下通过 **data-plane wireless-broadcast** 命令配置。

【命令格式】 **data-plane wireless-broadcast**{ **enable** | **disable** }
【参数说明】 **enable**：允许所有广播报文转发到空口。
disable：禁止所有广播报文转发到空口
【缺省配置】 广播无线转发关闭的，即广播报文不会转发到无线网络。
【命令模式】 全局配置模式
【使用指导】 -

检验方法

- 使用 **show run** 查看配置信息

配置举例

无。

常见错误

- 无。

3.5 监视与维护

清除各类信息

无。

查看运行情况

无。

查看调试信息

无。

4 WLOG

4.1 概述

WLOG（Wlan Log，无线日志）称为无线网络与终端状况存储与查看功能，主要针对的是对无线网络在过去一段时间内的网络及终端状况信息掌握的需求。通过收集、存储过去 24 小时的 STA 的信息，然后通过 CLI 命令提供显示给用户，便于用户分析无线网络中出现的状况，定位出现的问题。

因此，WLOG 针对的信息的收集与存储，暂时不支持信息的自动分析、诊断。WLOG 功能致力于让用户通过提供的信息能够对过去 24 小时的终端的状况有较为准确的了解，能够对出现的问题进行分析定位。

协议规范

- 无。

4.2 典型应用

- 无。

4.3 功能详解

基本概念

↘ AP 概况信息包括：

- AP 名称
- AP MAC 地址
- AP IP 地址
- AP 上线时间
- AP 各个有线端口情况：

1、最近 5 分钟输入/输出速率(bits/sec)

2、单播、广播、多播、错帧的输入/输出统计

- 每 radio 概况

1、工作信道

2、发射功率(dBm 绝对值)

3、当前关联成功在线终端数

4、当前 WEB 认证成功在线终端数

5、当前 1X 认证成功在线终端数

6、同频干扰信号强度

7、收到错帧数量

8、报文重传次数

↘ 终端（STA）的概况信息包括：

1、IP 地址

2、信号强度

3、连接速率

4、当前关联的 AP、radio 以及 SSID

↘ STA 的空间信息

- STA 的空间信息主要包含终端的数据帧、管理帧的统计信息，各类型速率的统计信息，具体如下：

1、成功发送（AP 发送给终端）的数据帧数量/流量统计

2、无应答的数据帧数量/流量统计

3、管理帧数量/流量统计

4、各个类型常规速率的帧数统计（常规速率分 8 个档次统计）

档次	0	1	2	3	4	5	6	7
包含速率类型（Mbps）	1/2	5.5/11	6/9	12/18	24/36	48/54	预留	预留

5、各个类型 MIMO 速率的帧数统计（MIMO 速率分 8 个档次统计）

档次	0	1	2	3	4	5	6	7
包含速率类型	mcs0 mcs1	mcs2 mcs3	mcs4 mcs5	mcs6 mcs7	mcs8 mcs9	mcs10 mcs11	mcs12 mcs13	mcs14 mcs15

空间信息主要用于检查 STA 是否处于低速状态、是否有过高比例的无 ACK 帧、是否收发了太多的管理帧，从而进一步分析定位低速节点、管理帧攻击、环境恶劣等导致的网络问题。STA 的空间信息属于实时变化的信息，目前的采集频率为每 5 分钟一次，由于数据量较大，目前只保存在 AP 上。

↘ AP 的行为类型

AP 的行为类型包括：上线、下线、CAPWAP 连接失败。

功能特性

功能特性	作用
开启WLOG功能	开启 WLOG 功能，自动收集 AP、STA 的信息。

4.3.1 开启WLOG功能

开启 WLOG 功能之后，AP 会自动收集 AP、STA 的信息，记录在内存中，让用户通过提供的信息能够对过去 24 小时的无线网络、终端的状况有较为准确的了解，能够对出现的问题进行分析定位。

工作原理

开启 WLOG 功能之后，AP 会自动收集 AP、STA 的信息，记录在内存中。同时接收 AP、STA 的上下线通告，也记录到内存中，供用户查看。

4.4 配置详解

配置项	配置建议 & 相关命令	
配置开启WLOG功能	⚠ 必须配置。开启 WLOG 功能。	
	wlan diag enable	开启 WLOG 功能

4.4.1 配置开启WLOG功能

配置效果

- 打开 WLOG 功能之后， AP 能够自动记录 AP、STA 信息。

注意事项

- 配置 WLOG 功能使能会进行内存的预分配。如果内存不够，则 WLOG 功能将使能失败；WLOG 功能关闭会进行所有存储信息内存与及预分配内存的释放。

配置方法

↘ 开启 WLOG 功能

- 必须配置，使用 wlog diag enable 命令来开启 WLOG 功能。
- 在 AP 设备的配置模式下开启。
- 开启 WLOG 功能之后，会定期收集信息，记录到内存中。

【命令格式】 **wlan diag enable**
【参数说明】 -
【缺省配置】 WLOG 功能缺省关闭
【命令模式】 全局配置模式

【使用指导】 -

检验方法

- 通过 **show wlan diag sta** 检查确认 AP 上能看到 STA 信息。

配置举例

无。

常见错误

- 无。

4.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
在 AP 上查看终端信息	**show wlan diag sta** [**sta-mac** *sta-mac*] [**number** *number*]

查看调试信息

无。

配置指南-WLAN 射频

本分册介绍 WLAN 射频配置指南相关内容，包括以下章节：

1. 射频调度
2. 频谱导航
3. 无线定位

1 射频调度

1.1 概述

本文中的射频资源包括 AP 上的射频和提供接入服务的 WLAN

射频调度是一种能代替用户定时自动管理射频资源的工具。

射频调度用来在用户指定的时间区间内关闭 AP 的射频或者 WLAN，使用射频资源调度可以：

- 减少网络流量，节约有限的网络资源，防止浪费和滥用。
- 减少射频干扰，节约电能、更环保。
- 在“危险”时段关闭接入服务，减少潜在的不安全因素。

射频调度功能适用于那些在固定周期提供无线接入服务的场合。

协议规范

- 无。

1.2 典型应用

无。

1.3 功能详解

基本概念

调度 session

一个调度 session 表示一个射频资源调度配置的时间。简单的调度 session 可能只是某一天的一段时间；复杂的调度时间包含多个时间段，并可以在不同的日期重复。目前，一个调度 session 支持配置 8 个不同（也可以相同）的时间段，每个时间段都可以指定连续重复的日期。

比如，一个调度 session 可以指：周一到周五的 12：00 到 14：00 和 18：00 到第二天的 8：00，周六到周日的 8：00 到 12：00 和 17：00 到第二天 8：00。

功能特性

功能特性	作用
配置调度session	指定调度时间周期

调度WLAN	应用调度 session 到 WLAN，定时打开、关闭 WLAN

1.3.1 配置调度session

指定调度时间周期。

工作原理

首先，调度功能需要用户创建一个调度 session，用来指定射频资源调度的时间。然后才能将该调度 session 应用到 AP 的射频接口或者 WLAN 上。

↘ 配置调度 session

使用调度功能的第一步就是创建一个调度 session，然后指定调度的时间和周期。

比如，前面提到的例子：“某高校的教学楼只在白天上课时间提供无线接入服务”，可以创建一个调度 session，指定周期为每天；指定调度时间为晚间，比如在 21：00 到第二天早上 6：00 之间。“某银行提供给客户的 WLAN 只在工作日的上班时间开启”，可以创建一个调度 session，指定一个调度时间段的周期为每工作日，指定该时间段的调度时间为下班时间，比如在 18：00 到第二天早上 9：00 之间；指定另一个调度时间段为周末，指定该时间段的调度时间为全天。

1.3.2 调度AP的射频

定时打开、关闭 AP 射频。

工作原理

首先，调度功能需要用户创建一个调度 session，用来指定射频资源调度的时间。然后将调度 session 应用到 AP 的射频接口上。

当时间到了该调度 session 的调度时间的开始或结束，系统会发出相应的调度消息。调度消息的处理逻辑会在有应用该调度 session 的 AP，将对应的射频接口关闭或打开。

↘ 应用调度 session 到射频接口

创建调度 session 之后，必须将调度 session 应用到相应的 AP 的射频接口，调度才能在 AP 的射频上生效。

↘ 调度消息的处理

创建调度 session 并指定运行周期和时间之后，系统会运行该调度 session 的定时器，然后会在时间进入、退出该调度 session 所标识的时间段时发出调度信息。调度消息包含的信息有：

- 调度 session ID。
- 消息类型：进入调度状态或退出调度状态。

1.3.3 调度WLAN

定时打开、关闭 WLAN。

工作原理

首先，调度功能需要用户创建一个调度 session，用来指定射频资源调度的时间。然后将调度 session 应用到 WLAN 上。

当时间到了该调度 session 的调度时间的开始或结束，系统会发出相应的调度消息。调度消息的处理逻辑会找到有应用该调度 session 的 WLAN，将其关闭或打开。

↘ 应用调度 session 到射频接口

创建调度 session 之后，必须将调度 session 应用到相应的 WLAN，调度才能在 WLAN 上生效。

指定方式就是在 WLAN 配置模式指定该 WLAN 上应用的调度 session ID。

↘ 调度消息的处理

创建调度 session 并指定运行周期和时间之后，系统会运行该调度 session 的定时器，然后会在时间进入、退出该调度 session 所标识的时间段时发出调度信息。调度消息包含的信息有：

- 调度 session ID。
- 消息类型：进入调度状态或退出调度状态。

调度消息处理会遍历所有的 WLAN，关注 WLAN 上应用的调度 session ID，如果确定某 WLAN 上应用的调度 session ID 和消息中的一致，那么就看消息类型，如果是进入调度状态，那么就关闭该 WLAN；否则，就打开该 WLAN。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置AP射频调度	⚠ 必须配置。用于创建调度 session，指定调度时间和应用到 AP、AP 组。	
	schedule session	创建调度 session
	schedule session time-range	指定调度 session 的调度时间
	schedule session	应用调度 session 到无线接口
配置WLAN调度	⚠ 必须配置。用于创建调度 session 和应用到 WLAN。	
	schedule session	创建调度 session
	schedule session time-range	指定调度 session 的调度时间
	schedule session	应用调度 session 到 WLAN

1.4.1 配置AP射频调度

配置效果

- 创建调度 session，指定调度 session 的调度时间，应用调度 session 到无线接口，实现 AP 射频调度功能。

注意事项

- 无。

配置方法

↘ 创建调度 session

- 必须配置。使用 **schedule session** *sid* 命令可以创建调度 session，参数为调度 session 的 ID，在胖 AP 设备上取值范围[1，8]。
- 使用调度 session 前必须首先创建调度 session。

【命令格式】 **schedule session** *sid*
【参数说明】 *sid*：调度 session ID，胖 AP 设备上取值范围[1，8]。
【缺省配置】 设备上没有调度 session。
【命令模式】 全局模式
【使用指导】 -

↘ 调度 session 的调度时间

- 必须配置。使用 **schedule session** *sid* **time-range** *n* **period** *day1* [**to** *day2*] **time** *hh1:mm1* **to** *hh2:mm2* 命令可以指定调度 session 的调度时间和周期。
- 参数 **session** *sid* 为调度 session 的 ID，在胖 AP 设备上取值范围[1，8]；
- 参数 **time-range** *n* 是调度 session 时间段编号，取值范围[1，8]；
- 参数 **period** *day1* [**to** *day2*]指定调度周期，*day1* 表示调度周期开始日期，*day2* 表示调度周期结束日期。日期有效值 { sun | mon | tue | wed | thu | fri | sat }。**to** *day2* 缺省表示调度时间段的周期只有一天。
- 参数 **time** *hh1:mm1* **to** *hh2:mm2* 指定调度的时间段。*hh1:mm1* 和 *hh2:mm2* 分别是起始时间和结束时间的小时和分钟。小时取值范围[0，23]，分钟取值范围[0，59]。

【命令格式】 **schedule session** *sid* **time-range** *n* **period** *day1* [**to** *day2*] **time** *hh1:mm1* **to** *hh2:mm2*
【参数说明】 *sid*：调度 session ID，胖 AP 设备上取值范围[1，8]。
n：调度 session 时间段编号，取值范围[1，8]。
day1：调度 session 时间段的周期，day1 表示调度周期开始日期。日期有效值 { sun | mon | tue | wed | thu | fri | sat }。
to *day2*：day2 表示调度周期结束日期。缺省表示调度时间段的周期只有一天。

time *hh1:mm1* **to** *hh2:mm2*：调度 session 时间范围：hh1:mm1 和 hh2:mm2 分别是起始时间和结束时间的小时和分钟。小时取值范围[0，23]，分钟取值范围[0，59]。

【缺省配置】 刚创建的调度 session 没有指定任何时间段和周期。

【命令模式】 全局模式

【使用指导】 -

↘ 应用调度 session

- 必须配置。
- 使用 **schedule session** *sid* 命令可以指定单个 AP 上应用的调度 session ID。

【命令格式】 **schedule session** *sid*

【参数说明】 *sid*：调度 session ID，胖 AP 设备上取值范围[1，8]。

【缺省配置】 没有应用任何调度 session。

【命令模式】 WLAN 模式/接口配置模式

【使用指导】 -

检验方法

- 通过 **show running-config** 命令可以查看射频调度相关配置。
- 观察应用调度 session 的 AP 的射频在调度 session 到期后，是否有调度行为。

配置举例

无。

常见错误

- 调度 session 没有创建。
- 调度 session 时间指定错误。
- AP 上调度优先级冲突。
- 应用时指定了 Radio，导致另一个 Radio 没有调度。

1.4.2 配置WLAN调度

配置效果

- 创建调度 session，指定调度 session 的调度时间，应用调度 session 到 WLAN，实现 WLAN 调度功能。

注意事项

- 无。

配置方法

创建调度 session

- 必须配置。使用 **schedule session** *sid* 命令可以指定 WLAN 上应用的调度 session ID。
- 应用调度 session 后，如果有该调度 session 的调度消息，那么指定的 WLAN 将被自动管理，根据调度 session 的消息类型进入或退出调度状态。

【命令格式】 **schedule session** *sid*
【参数说明】 **session** *sid*：调度 session ID，胖 AP 设备上取值范围[1，8]。
【缺省配置】 所有 WLAN 上均没有应用任何调度 session。
【命令模式】 全局模式
【使用指导】 -

调度 session 的调度时间

- 必须配置。

【命令格式】 **schedule session** *sid* **time-range** *n* **period** *day1* [**to** *day2*] **time** *hh1:mm1* **to** *hh2:mm2*
【参数说明】 **session** *sid*：调度 session ID，胖 AP 设备上取值范围[1，8]。
time-range *n*：调度 session 时间段编号，取值范围[1，8]。
period *day1*：调度 session 时间段的周期，day1 表示调度周期开始日期。日期有效值 { sun | mon | tue | wed | thu | fri | sat }。
to *day2*：day2 表示调度周期结束日期。缺省表示调度时间段的周期只有一天。
time *hh1:mm1* **to** *hh2:mm2*：调度 session 时间范围：hh1:mm1 和 hh2:mm2 分别是起始时间和结束时间的小时和分钟。小时取值范围[0，23]，分钟取值范围[0，59]。
【缺省配置】 调度 session 时间段为空
【命令模式】 全局模式
【使用指导】 -

应用调度 session

- 必须配置。

【命令格式】 **schedule session** *sid*
【参数说明】 **session** *sid*：调度 session ID，胖 AP 设备上取值范围[1，8]。
【缺省配置】 调度 session 不存在。
【命令模式】 WLAN 模式/接口配置模式
【使用指导】 -

检验方法

- 通过 **show running-config** 命令可以查看射频调度相关配置。

- 观察应用调度 session 的 WLAN 在调度 session 到期后，是否有调度行为。

配置举例

无。

常见错误

- 调度 session 没有创建。
- 调度 session 时间指定错误。

1.5 监视与维护

清除各类信息

无。

查看运行情况

无。

查看调试信息

无。

2 频谱导航

2.1 概述

频谱导航（Band Select）是一种 WLAN 优化无线用户接入频段分配的技术。

频谱导航使用技术手段，引导使用双频 STA 的无线用户接入容量更高的 5G 频段，从而减轻 2.4G 频段的压力，提升用户体验。

频谱导航，适用于使用双频 AP 做覆盖，AP 两个射频接口分别工作在 2.4G 和 5G 频段；并且 WLAN 映射在 AP 的两个射频接口上，同时在两个频段提供接入服务的场景。

协议规范

- IEEE 802.11

2.2 典型应用

无。

2.3 功能详解

基本概念

IEEE802.11 通讯频段

IEEE802.11 的主要通讯频段分成两段：

- 2.4GHz (2.4 to 2.4835 GHz)，802.11b/g/n 所在频段
- 5GHz (5.15 to 5.35 and 5.725 to 5.825 GHz)，802.11a/n 所在频段

随着 WLAN 的普及，无线用户也越来越多，其中很多的用户使用能同时支持 2.4G 频段和 5G 频段的双频无线客户端(STA)。但是，802.11b/g 比 802.11a 的应用更为广泛，很多双频 STA 都使用 2.4G 频段，会造成 2.4G 频段的拥挤和 5G 频段的浪费。实际上，5G 频段拥有更高的接入容量：2.4G 频段最多只能有 3 个不重叠的通讯信道；而 5G 频段却能提供更多不重叠的通讯信道。

STA 发现 WLAN 的方式

有两种发现方式：被动扫描和主动扫描。

- 被动扫描：STA 在其支持的所有频段的所有信道上监听附近 AP 上发出的信标（Beacon）帧，信标帧包含了提供接入服务的 WLAN 以及附属信息。STA 解析这些信息就能了解周围存在哪些可以接入的 WLAN。

- 主动扫描：STA 首先在其支持的所有频段的所有信道上广播发送探测请求（Probe Request）帧，提供 WLAN 接入服务的 AP 收到探测请求帧，就会发出探测回应（Probe Response）帧，将自己提供的 WLAN 的一些信息发给 STA。

STA 一般会把发现的所有 WLAN 的 SSID 进行汇总，以可接入的 WLAN 列表的方式呈现给用户，供用户选择接入某个 WLAN。

双频 STA

无线用户用来连接 WLAN 的无线网卡，其功能规格描述中会有 a、b、g、n 等，它们表明无线网卡支持的 802.11 协议类型。802.11a 工作在 5G 频段；802.11b/g 工作在 2.4G 频段；802.11n 既可以工作在 5G 频段，也可以工作在 2.4G 频段。

所以，如果网卡功能规格描述中既包含 a，也包含 b 或者 g，那么就说明该网卡同时支持这两个频段，即为双频 STA。双频 STA 既可以接入 5G 频段，也可以接入 2.4G 频段。

双频 AP

双频 AP 即同时具有两个频段接入能力的 AP，所以双频 AP 至少需要两个射频接口，一个工作在 5G，另一个工作在 2.4G。

需要开启频谱导航的 WLAN，必须同时映射到双频 AP 的两个射频接口上，同时提供两个频段的接入服务。

功能特性

功能特性	作用
识别STA类型信息	识别 STA 是否双频 STA。
控制主动扫描过程	控制双频 STA 的主动扫描，防止其发现 2.4G 频段的 WLAN。
拒绝双频STA接入 2.4G频段	拒绝双频 STA 接入 2.4G 频段，提高其接入 5G 频段的几率。

2.3.1 识别STA类型信息

要做到引导双频 STA 接入 5G 频段，第一步要识别 STA 是否双频 STA，就是识别 STA 的频段支持情况。

工作原理

主动扫描是 STA 发现 WLAN 的方式之一，STA 使用主动扫描时，会在 STA 支持的每个信道上发出探测请求帧，如果能得知 STA 发出的探测请求帧的信道信息，那么就能识别 STA 的频段支持情况。

比如，如果 AP 在 1～13 信道上接收到 STA 的探测请求帧，那么该 AP 就能知道该 STA 支持 2.4G 频段；如果 AP 在 149～165 信道上接收到 STA 的探测请求帧，那么该 AP 就能知道该 STA 支持 5G 频段。

因为单频 AP 只能从一个频段接收到探测请求帧，所以只有双频 AP 才能正确识别出 STA 类型。这就是频谱导航要求使用双频 AP 的原因。

STA 分类标准

双频 AP 通过下面的标准将 STA 分类：

- 如果既能从 2.4G 频段收到该 STA 的探测请求，又能从 5G 频段收到该 STA 的探测请求，那么这是一个双频 STA；

- 如果只能从 5G 频段收到该 STA 的探测请求，那么该 AP 为 5G 的 STA；
- 如果只能从 2.4G 频段收到该 STA 的探测请求，那么该 AP 为 2.4G 的 STA；

因为需要等待一段时间以确认不会从另一个频段收到探测请求，识别单频的 STA 比较耗时一些，不过不会影响用户的正常使用。这三种 STA，前两种 STA 在频谱导航功能中称为双频类 STA，简称双频 STA；后面一种称为抑制类 STA，简称抑制 STA。

对双频 STA 的识别，只能依赖等待一段时间(固定两秒)来确认其是否能在 5G 频段发出探测请求，因为 STA 驱动差别，这个时间不可能适用于所有的双频 STA，所以有几率出现刚开始不能正确识别 STA 类型的现象。只要以后双频 STA 能在 5G 频段发出探测请求，识别的 STA 类型就能恢复正确。

STA 信息保存

双频 AP 识别到的 STA 的信息需要保存起来，给后续的回应策略提供依据。

因为 STA 的探测请求是广播报文，一般情况下，AP 都会收到大量的探测请求，把它们都保存起来是没有必要的，因为有些 STA 的距离太远，没有接入到本 AP 的可能。所以频谱导航只保存那些有可能接入的 STA 的信息，选择标准就是 STA 的 RSSI（Received Signal Strength Indication），RSSI 超过一个门限值的才是有可能接入的 STA，识别信息才需要保存。

STA 信息老化

因为某些 STA 的频段支持情况是用户可以配置的，所以会出现在使用过程中，STA 的类型转换的情况。

比如一款支持 802.11agn 的无线网卡，开始使用时是双频 STA。后来用户手动禁用了它的 802.11a 模式或者 5G 频段信道的支持，那么该无线网卡就变成了单频 2.4G 的 STA 了。

针对这种情况，识别的 STA 信息要引入老化机制，一定时间后，丢弃先前识别的 STA 信息，然后重新识别。

2.3.2 控制主动扫描过程

识别了 STA 的频段支持情况后，双频 AP 就能根据 STA 信息，对 STA 的主动扫描过程进行控制，防止双频 STA 发现 2.4G 频段的 WLAN，从而达到引导双频 STA 接入 5G 频段的目的。

工作原理

STA 的主动扫描过程，正常情况下，STA 广播探测请求帧，AP 收到后会马上回应探测响应帧，告诉 STA 本 AP 上可以提供接入服务的 WLAN 信息等。双频 STA 在主动扫描时，在两个频段上都会发送探测请求并等待探测响应。打开频谱导航功能后，AP 要控制主动扫描的回应过程，针对不同的情况采用不同的回应方式。

频谱导航识别 STA 类型前的主动扫描

如果 WLAN 上开启了频谱导航功能，对 STA 的主动扫描回应有所变化。在识别 STA 类型信息之前：

- 2.4G 频段的探测请求不响应。
- 5G 频段的探测请求正常响应。

收到 2.4G 频段的探测请求，不能确定该 STA 是否支持 5G 频段，为了避免其发现 WLAN 在 2.4G 频段提供接入服务，需要等待识别过程结束才能回应。

收到 5G 频段的探测请求，就说明该 STA 支持 5G 频段，所以可以立刻回应探测响应，告诉该 WLAN 在 5G 频段提供接入服务。

↘ 频谱导航识别 STA 类型后的主动扫描

识别 STA 类型信息后，再收到 STA 的探测请求报文，可以根据探测请求报文中的源 MAC 地址找到 AP 上保存的 STA 的类型信息：

- 2.4G 频段的探测请求，如果 STA 类型是双频 STA，那么不回应探测响应；如果 STA 类型是抑制 STA，那么进行消极响应。
- 5G 频段的探测请求正常响应。

对双频 STA 在 2.4G 频段发出的探测请求，不回应探测响应可以避免双频 STA 发现 WLAN 在 2.4G 提供接入服务，让双频 STA 只能发现 WLAN 在 5G 频段提供接入服务，那么用户选择该 WLAN 接入时，双频 STA 就只能选择 5G 频段了。这就起到了引导双频 STA 接入 5G 频段的目的。

抑制 STA 在 2.4G 频段发出的探测请求，则必须进行回应。因为抑制 STA 只能支持 2.4G 频段，如果在 2.4G 频段不回应，那么它就无法发现 WLAN 了。不过回应方式上，可以对抑制 STA 进行抑制，也就是消极的回应。

5G 频段的探测请求，只有双频 STA 才能发出来，这时立刻回应探测响应，告诉该 WLAN 在 5G 频段提供接入服务。

↘ 频谱导航对抑制 STA 的消极回应

频谱导航对 5G 频段的探测请求都是积极回应的，对双频 STA 在 2.4G 频段探测请求都是不回应的，而对抑制 STA 的探测请求则是消极回应的。

消极回应，形象一点说，就是打了折扣的回应。比如连续收到多个探测请求，只回应一个探测响应。

频谱导航对抑制 STA 的消极回应程度，取决于两个参数：STA 探测扫描周期门限和抑制 STA 的探测周期计数值。

STA 探测扫描周期指的是 STA 主动扫描时，扫描完所有支持信道所花费的时间，这个时间取决于 STA 的驱动程序，每种 STA 可能均不相同。STA 探测扫描周期门限是一个用户可配置的值，可以理解成用户限制的 STA 探测扫描周期的最小值，如果某种 STA 的扫描周期小于这个值，那么连续的两个扫描周期会被 AP 认为是一个是扫描周期，这个参数可以正确处理某些 STA 在一个扫描周期内发送多个探测请求报文的情况。

举例说明：假设某 STA 每 150 毫秒扫描完所有信道，在每个信道上连续发送两个探测请求帧；如果 AP 上没有指定 STA 探测扫描周期的最小值，那么 AP 收到两个探测报文后，就无法判断是 STA 在一个扫描周期内发出来的两个还是连续两个扫描周期各发出来一个；如果 AP 上指定 STA 探测扫描周期的最小值为 200 毫秒，那么，因为两个报文的间隔不到 200 毫秒，就被认为是一个扫描周期内发出来的，AP 上该 STA 的探测周期计数就是 1。就例子中的 STA 而言，因为指定的 STA 探测扫描周期的最小值为 200 毫秒和实际扫描周期 150 毫秒不一致，也存在计数上的不一致问题：假设该 STA 连续扫描 3 个周期，那么 AP 上只能计数成 2 个周期，其中前两个周期被认为是同一个周期。不过这问题不会造成用户使用上的不便。

STA 的探测周期计数反映了频谱导航对抑制 STA 的消极回应的程度，这个参数的意思是：抑制 STA 主动扫描多个周期，AP 上才回应一次。比如，这个参数默认值为 2，表示 STA 连续两个扫描周期，AP 上的 WLAN 才回应一个探测响应帧。

2.3.3 拒绝双频STA接入 2.4G频段

⚠ 频谱导航功能只是控制了 STA 的主动扫描过程，还无法防止 STA 通过被动扫描发现 2.4G 频段的 WLAN。所以部分双频 STA 还是能发现 2.4G 频段的 WLAN 并尝试接入。这时频段导航功能就可能失效。

频谱导航可以拒绝双频 STA 在 2.4G 频段的接入请求，以提高双频 STA 接入 5G 频段的几率。

⚠ 拒绝双频 STA 在 2.4G 频段的接入请求，可以提高频谱导航成功的几率，但是不可能达到 100%，频谱导航还是有可能失效的。

工作原理

STA 发现 WLAN 后，用户选择接入时，STA 首先发送链路认证请求帧（Authentication Request）给 AP，然后 AP 回应链路认证响应帧（Authentication Response）允许或拒绝 STA 的认证请求。

频谱导航功能可以处理链路认证请求帧，如果是双频 STA 在 2.4G 频段发出的认证请求，可以选择拒绝其认证请求，直到双频 STA 在 5G 频段发出认证请求才允许接入。这样也能起到引导双频 STA 接入 5G 频段的目的。

一般的双频 STA 接入时，会先在某个频段上发出一个或多个认证请求并等待回应，如果没有回应或者没有成功，就会转而在另一个频段发出认证请求并等待回应。但是也不排除有双频 STA 始终只在 2.4G 频段发出认证请求的情况，为了高可用性，频谱导航可以配置拒绝双频 STA 接入的次数。

假设某款双频 STA 接入时转换一次频段前会连续发送认证请求 M 次；而频谱导航功能的拒绝双频 STA 接入的次数配置成 N 次；那么，如果该双频 STA 首先尝试 5G 频段，那么就能马上接入；反之，如果该双频 STA 首先尝试 2.4G 频段，那么如果 N 大于等于 M，那么 STA 就能接入 5G 频段；反之，STA 将接入 2.4G 频段。不管接入哪个频段，如果双频 STA 首先尝试 2.4G 频段，那么总会有 min（M，N）（M，N 的较小的那个）个链路认证请求被拒绝或忽略，后果就是 STA 接入时间延长，延长的具体时间取决于 STA 的驱动，比如 STA 发送认证请求的间隔是 100 毫秒，有 4 个认证请求被忽略，那么该 STA 的正常接入会延长 400 毫秒。

⚠ 频谱导航决定拒绝双频 STA 的接入请求时，如果其他的接入控制功能模块，比如负载均衡，决定接受该 STA 的接入请求，那么该 STA 是可以接入的。这是因为频谱导航功能只是在 STA 接入过程中起到“引导”作用，相对优先级比较低，当与其他功能相冲突时，以其他功能为优先。

2.4 配置详解

配置项	配置建议 & 相关命令	
配置频谱导航	⚠ 必须配置。用于开启 WLAN 的频谱导航功能。	
	band-select enable	开启频谱导航功能
	⚠ 可选配置。用于配置频谱导航功能的工作参数。	
	band-select acceptable-rssi	配置频谱导航可以接受的 STA 信号强度下限。
	band-select access-denial	配置拒绝双频 STA 接入 2.4G 频段的次数。
	band-select age-out	配置 STA 信息的老化时间。
	band-select probe-count	配置抑制 STA 的探测周期计数值。
	band-select scan-cycle	配置 STA 探测扫描周期门限。

2.4.1 配置频谱导航

配置效果

- 开启 WLAN 的频谱导航功能，引导双频 STA 接入 5G 频段

注意事项

- 无。

配置方法

↘ 开启 WLAN 的频谱导航功能

- 必须配置。
- 若无特殊要求，在胖 AP 上打开。

【命令格式】 **band-select enable**
【参数说明】 **-**
【缺省配置】 关闭频谱导航功能
【命令模式】 WLAN 配置模式
【使用指导】 -

↘ 配置频谱导航可以接受的 STA 信号强度下限

- 可选配置，在需要调整频谱导航覆盖范围时进行配置。
- 若无特殊要求，在胖 AP 上打开。
- 该限值越高，频谱导航的覆盖范围越小；该限值越低，频谱导航的覆盖范围越大；但是，如果超过了可以正常使用的限制，会导致接入的 STA 信号过弱，拖慢整网的连接速率。

【命令格式】 **band-select acceptable-rssi** *value*
【参数说明】 *value*：频谱导航可以接受的 STA RSSI 下限，范围[-100，-50]，单位 dBm。
【缺省配置】 -80 dBm
【命令模式】 全局模式
【使用指导】 -

↘ 配置拒绝双频 STA 接入 2.4G 频段的次数

- 可选配置，在需要拒绝双频 STA 接入 2.4G 频段时配置；如果配置后出现较多双频 STA 接入时间过长或无法接入，要配置较小的值或配置为 0。
- 若无特殊要求，在胖 AP 上打开。

- 拒绝双频 STA 接入 2.4G 频段的次数越大，双频 STA 接入 2.4G 频段越困难，接入 2.4G 频段花费的时间也越长；拒绝双频 STA 接入 2.4G 频段的次数越小，双频 STA 接入 2.4G 频段越容易，接入 2.4G 频段花费的时间也越短。

【命令格式】 **band-select access-denial** *value*
【参数说明】 *value*：拒绝双频 STA 接入 2.4G 频段的次数，范围[0，10]。
【缺省配置】 2
【命令模式】 全局模式
【使用指导】 -

配置 STA 信息的老化时间

- 可选配置，如果环境中没有双频 STA 切换成单频 2.4G STA 的情况，可以配置较大的老化周期，反之，配置较小的老化周期；如果不确定，使用默认配置即可。
- 若无特殊要求，在胖 AP 上打开。
- STA 信息老化时间越大，STA 的信息生命周期越长，AP 对 STA 的频段切换越不敏感。STA 信息老化时间越小，STA 的信息生命周期越短，AP 对 STA 的频段切换越敏感。

【命令格式】 **band-select age-out** { **dual-band** *value* **| suppression** *value* }
【参数说明】 **dual-band** *value*：双频 STA 信息的老化时间，范围[20，120]，单位秒。
suppression *value*：抑制 STA 信息的老化时间，范围[10，60]，单位秒。
【缺省配置】 双频 STA 信息老化时间为 60 秒；抑制 STA 信息老化时间为 20 秒
【命令模式】 全局模式
【使用指导】 推荐双频 STA 的信息老化时间配置为抑制 STA 的信息老化时间的两倍到三倍。

配置抑制 STA 的探测周期计数值

- 可选配置，如果出现单频 2.4G STA 长时间发现不了 WLAN 的情况，那么应该减小该配置。
- 若无特殊要求，在胖 AP 上打开。
- STA 的探测周期计数值越大，频谱导航对抑制 STA 的抑制越大，抑制 STA 越不容易发现 WLAN；STA 的探测周期计数值越小，频谱导航对抑制 STA 的抑制越小，抑制 STA 越容易发现 WLAN。

【命令格式】 **band-select probe-count** *value*
【参数说明】 *value*：抑制 STA 的探测周期计数值，范围[1，10]。
【缺省配置】 2
【命令模式】 全局模式
【使用指导】 -

配置 STA 探测扫描周期门限

- 可选配置，如果出现单频 2.4G STA 长时间发现不了 WLAN 的情况，那么应该减小该配置；如果不确定，使用默认配置即可。
- 若无特殊要求，在胖 AP 上打开。
- STA 探测扫描周期门限值越大，STA 的探测周期计数增加越慢，STA 越不容易发现 WLAN；STA 探测扫描周期门限值越小，STA 的探测周期计数增加越快，STA 越容易发现 WLAN。

【命令格式】 **band-select scan-cycle** *value*
【参数说明】 *value*：STA 探测扫描周期门限，范围[1，1000]，单位毫秒。
【缺省配置】 200 毫秒
【命令模式】 全局模式
【使用指导】 -

检验方法

- 使用 **show band-select configuration** 命令查看设备上的频谱导航参数配置。
- 使用 **show running-config** 命令查看 WLAN 配置是否打开了频谱导航功能。
- 运行一段时间后，使用 **show band-select statistics** 命令查看设备上的运行统计值。
- 抓包确认频谱导航是否控制了主动探测过程。

配置举例

无

常见错误

- 频谱导航运行参数配置不合适。
- 频谱导航功能没有打开。
- 双频 AP 的两个射频接口被关闭了一个。

2.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看频谱导航运行配置。	**show band-select configuration**
查看频谱导航运行统计值。	**show band-select statistics**

查看调试信息

无。

3 无线定位

3.1 概述

锐捷 WLAN 产品的无线定位(Wlan Location，下文简称 WL)功能，是一种利用 802.11 无线信号对终端设备进行定位的功能。可以支持所有标准的 802.11a/b/g/n 设备，如笔记本电脑，移动设备（ Mobile Unit，下文简称 MU ）。通过对这些设备发送的 802.11 无线信号的分析和汇总，可以在服务器控制端软件上实现对物资的定位，并可以通过地图、表格或者报告的形式直观的表示出来。

锐捷 WL 功能同时具有以下特点：

- 支持室内、室外的部署
- 支持 RSSI 与 TDOA 两种定位算法
- 支持 MU（ Mobile Unit ）设备的定位

3.2 典型应用

无。

3.3 功能详解

基本概念

定位系统分为三个部分：需要定位的设备或源、定位信息接收装置和后台定位系统。

↘ 需要定位的设备或源

锐捷 WL 功能可以定位的终端设备有两种：

- AeroScout 公司生产的 Tag，一种轻便、易携带的 RFID 设备，使用中通常放置或粘贴在需要定位的目标上。
- MU（ Mobile Unit，移动设备 ），即任何符合 802.11 技术的无线终端或设备，这些设备的特点是都可以定时向周围发送无线信号。

↘ 定位信息接收装置

定位信息接收装置可以是锐捷的 AP 产品，或者 AeroScout 公司的 Tag 激发器(用于激励 Tag 发送指定无线信号，但不参与定位信息收集 ）。

↘ 后台定位系统

后台定位系统包括：定位服务器、AE 计算软件、各种图形软件等。

功能特性

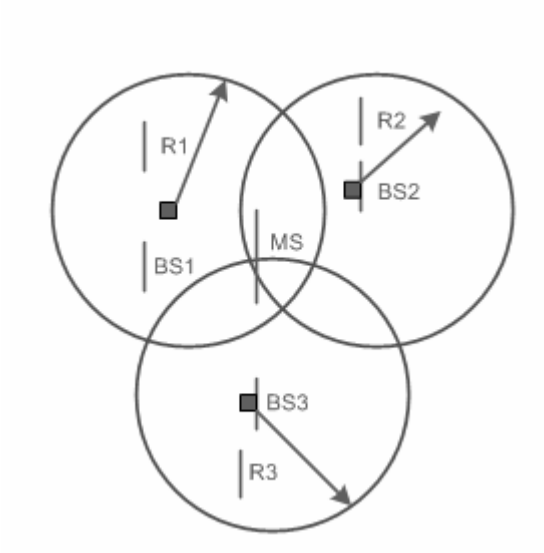
功能特性	作用
无线定位	使能 AP 上的无线定位功能。

3.3.1 无线定位

工作原理

基本原理：通过测量基站收到的来自移动台的信号强度(RSSI)，以及它们之间无线信道的传输模型，可以估计出移动台到基站的大致距离为 d。这样对一个基站 BS(i)来讲，移动台必处于以 BS(i)为圆心，d 为半径的圆上。当采用三个或三个以上的基站对同一个移动台进行测距时，即可以测得该移动站的所在位置，在这种方法中，无线信号传输过程中的多径效应和通过障碍时产生的阴影效应是产生定位误差的主要原因。在开放空间里，若无障碍物的阻隔，可以得到较为精确的定位，而在很多环境下，因为存在各种各样的障碍物导致的多径效应，衰减，散射等等不确定因素，将大大影响其定位精度。

图 3-1



3.4 配置详解

配置项	配置建议 & 相关命令	
配置WL基本功能	⚠ 必须配置。用于使能无线定位功能。	
	wlocation enable	开启指定 AP 的无线定位功能
	wlocation ae-ip	配置指定 AP 上连接的 AE 服务器的 IP 地址
	wlocation ae-port	配置指定 AP 上连接的 AE 服务器的端口号

	wlocation mu enable	打开指定 AP 的 MU 无线定位功能
	可选配置。用于优化无线定位数据的传输。	
	wlocation compound enable	打开无线定位信息聚合传输功能
	wlocation send-mu-time	配置指定 AP 的 MU 定位信息上送间隔时间
	wlocation mu report enable	打开直接发送 MU 定位信息功能
	wlocation mu report reduce enable	打开精简 MU 定位信息功能
	wlocation ignore beacon enable	打开过滤 AP 发出的 beacon 报文功能

3.4.1 配置WL基本功能

配置效果

- 使能 WL 功能，可进行基本的定位服务。

注意事项

- 无。

配置方法

↘ 启动 AP 的 WL 功能

- 必须配置。
- 使用 **wlocation enable** 命令可以启动或关闭 AP 的无线定位功能。
- 同时需要指定支持的无线定位设备，使用的命令为：**wlocation mu enable**，使能 MU 设备。
- 如果没有开启无线定位或者没有指定支持的无线定位设备，则无线定位功能不能使用。
- 若无特殊要求，应在需要定位功能的部署中的每台 AP 上开启。

【命令格式】 **wlocation enable**
【参数说明】 -
【缺省配置】 关闭 WL 功能
【命令模式】 wlocation 模式。
【使用指导】 -

↘ 配置定位服务器 IP 地址和端口号

- 必须配置。
- 端口号有默认值，具体根据定位服务器配置决定。

- AP 的无线定位功能需要配合定位服务器才能工作，因此需要配置无线定位服务器的 IP 地址和端口号，并保证 AP 与定位服务器可以通信。
- 配置 IP 和端口号的命令分别为：**wlocation ae-ip** *ip-address* 和 **wlocation ae-port** *port*。
- 配置正确的 IP 地址和端口号后，AP 才能够正常的启用无线定位的功能。

【命令格式】 **wlocation ae-ip** *ip-address*
【参数说明】 *ip-address*：定位服务器的 IP 地址
【缺省配置】 默认无配置，AE 的 IP 地址为 0.0.0.0
【命令模式】 wlocation 模式。
【使用指导】 -

【命令格式】 **wlocation ae-port** *port*
【参数说明】 *port*：AE 服务器的端口号
【缺省配置】 默认值为 12092
【命令模式】 wlocation 模式。
【使用指导】 -

↘ 开启 MU 定位功能

- 必须配置。
- 如果要使能 AP 上的定位功能，则 MU 定位必须开启。具体根据应用场景和需要定位的终端设备来决定。

【命令格式】 **wlocation mu enable**
【参数说明】 -
【缺省配置】 缺省关闭
【命令模式】 wlocation 模式。
【使用指导】 -

↘ 调整 MU 定位的信息上送间隔时间

- 可选配置。
- 调整定位信息上送的时间。如果没有特殊要求，可以不用调整。
- 在需要定位的终端设备较多的场景下，需要减小发送的时间间隔，避免信息的丢失。（ AP 能够缓存的定位信息在 500-700 条之间 ）

【命令格式】 **wlocation send-mu-time** *interval*
【参数说明】 *interval*：时间间隔，范围 100 –600000ms
【缺省配置】 默认 300ms
【命令模式】 wlocation 模式。
【使用指导】 -

↘ 开启直接发送 MU 定位信息功能

- 可选配置。

- 定位服务器和 AP 未交互，直接发送无线定位 MU 信息的 AP,比如穿越 NAT 网络。如果没有特殊要求，可以不用调整。

【命令格式】 **wlocation mu report enable**
【参数说明】 -
【缺省配置】 缺省关闭
【命令模式】 wlocation 模式。
【使用指导】 开启直接发送 MU 定位信息给功能，在开启 MU 定位，忽略协议的握手环节，穿越 NAT 网络使用。

↘ 开启精简 MU 定位信息功能

- 可选配置。
- 有减少带宽流量需求，且定位系统部署是和我司开发的定位服务器对接。若没有该需求，可以不配置。

【命令格式】 **wlocation mu report reduce enable**
【参数说明】 -
【缺省配置】 缺省关闭
【命令模式】 wlocation 模式。
【使用指导】 开启精简 MU 定位信息功能，以便减少带宽流量，仅在定位部署服务器为我司开发的定位服务器使用。

↘ 开启过滤 AP 发出的 beacon 报文功能

- 可选配置。
- 有减少流浪带宽需求。若没有该需求，可以不配置。

【命令格式】 **wlocation ignore beacon enable**
【参数说明】 -
【缺省配置】 缺省关闭
【命令模式】 wlocation 模式。
【使用指导】 开启过滤 wifi 环境下 AP 发出的 beacon 报文功能，以便减少带宽流量。

检验方法

在部署的网络中开启终端设备，发送无线报文。

- 检查 AP 是否有上送无线定位信息。
- 检查定位服务器是否有收到定位信息。

配置举例

无。

常见错误

无。

3.5 监视与维护

清除各类信息

无。

查看运行情况

无。

查看调试信息

无。

配置指南-WLAN 安全

本分册介绍 WLAN 安全配置指南相关内容，包括以下章节：

1. RSNA
2. WIDS
3. CPP
4. NFPP

1 RSNA

1.1 概述

RSNA（Robust Security Network Architecture，强健安全网络架构）功能实现无线网络安全机制。

由于无线网络使用的是开放性媒介采用公共电磁波作为载体来传输数据信号，通信双方没有线缆连接。如果传输链路未采取适当的加密保护，数据传输的风险就会大大增加。因此，安全机制在 WLAN 中显得尤为重要。

为了增强无线网络安全性，至少需要提供认证和加密两个安全机制：

- 认证机制：认证机制用来对用户的身份进行验证，以限定特定的用户（授权的用户）可以使用网络资源。
- 加密机制：加密机制用来对无线链路的数据进行加密，以保证无线网络数据只被所期望的用户接收和理解。

下文仅介绍 RSNA 的相关内容。

协议规范

- IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements -2007
- WI-FI Protected Access – Enhanced Security Implementation Based On IEEE P802.11i Standard-Aug 2004
- Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—802.11, 1999 IEEE Standard for Local and metropolitan area networks ”Port-Based Network Access Control” 802.1X™- 2004
- 802.11i IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements

1.2 典型应用

典型应用	场景描述
WEP加密	在较为小型且对安全性要求不高的WLAN中，使用静态WEP加密模式保护无线数据通信。
PSK接入认证	对于一些中小型的企业网络或者家庭用户，使用基于预共享密钥的接入认证方式加强无线网络安全。
802.1x接入认证	在对安全性要求较高或者有统一管理需求的场景，使用基于端口的网络接入控制。

1.2.1 WEP加密

应用场景

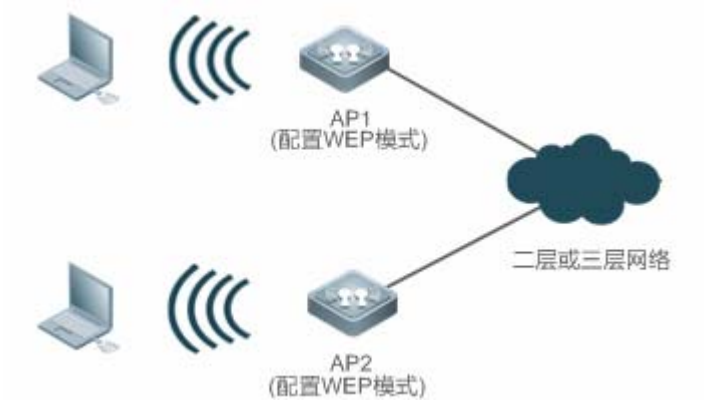
在较为小型且对安全性要求不高的 WLAN 中，可使用 WEP 加密模式。

WEP 加密模式可以分别采用 open-system 或者 shared-key 链路验证方式，两者的主要区别在于：

- 采用 open-system，此时 wep 密钥只用于数据加密，即使密钥配的不一致，用户也是可以上线，但上线后传输的数据会因为密钥不一致被接收端丢弃；
- 采用 shared-key，此时 wep 密钥做链路认证和数据加密，如果密钥不一致，客户端链路验证失败，无法上线。

静态 WEP 加密模式的应用场景如下图所示。

图 1-1



功能部属

- 在 AP（AP1 和 AP2）上配置 WLAN。
- 在 AP（AP1 和 AP2）上的 WLAN 安全模式下配置 WEP 加密模式。

1.2.2 PSK接入认证

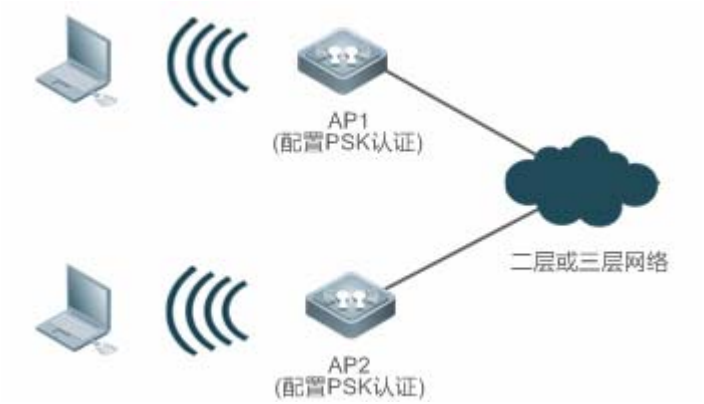
应用场景

对于一些中小型的企业网络或者家庭用户，使用 WPA 或 WPA2 标准加强无线网络安全，最简单的方法就是使用预共享密钥认证(分别称为 WPA-PSK 和 WPA2-PSK)。在这种情况下，WPA 的使用方法同 WEP 相似，但是能够得到 WPA 和 802.11i 带来的更高安全性，包括更强壮的认证和更好的加密算法。

PSK 认证只需为 STA 和接入设备配置相同的预共享密钥即可建立连接和通信，无需额外的认证服务器。

PSK 认证模式的应用场景如下图所示。

图 1-2



功能部属

- 在 AP（AP1 和 AP2）上配置 WLAN。
- 在 AP（AP1 和 AP2）上的 WLAN 安全模式下配置 PSK 认证模式。
- 可配合 WEB 认证一起使用，以支持网络认证及计费功能。

1.2.3 802.1x接入认证

应用场景

在对安全性要求更高的场景，可以使用 802.1x 认证。

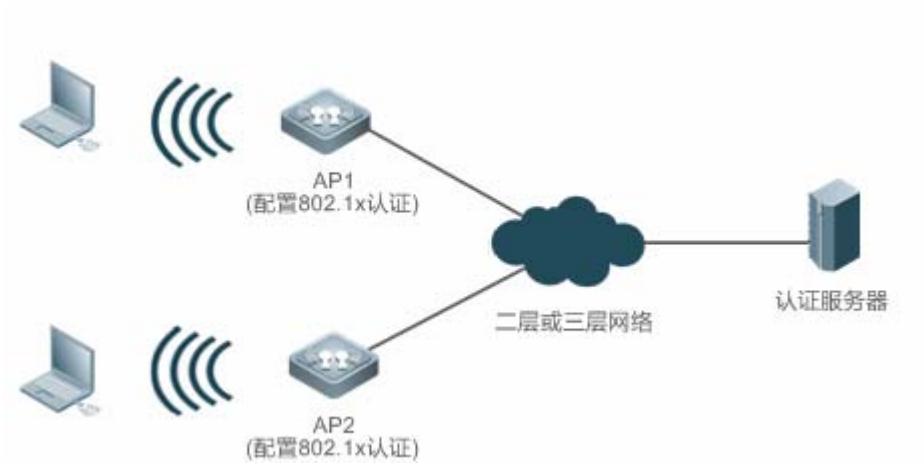
802.1x 协议是一种基于端口的网络接入控制协议。这种认证方式在 WLAN 接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在接口上的用户设备如果能通过认证，就可以访问 WLAN 中的资源；如果不能通过认证，则无法访问 WLAN 中的资源。

802.1X 认证需要终端上安装认证客户端软件。但在某些情况下，这个条件是无法满足的，比如一些无线打印机。出于网络管理和安全考虑，即便这些终端无 802.1X 认证客户端，网络管理员仍然需要控制这些接入设备的合法性。MAC 旁路认证(MAC Authentication Bypass,简称 MAB)为这种应用提供了一种解决方案。

WLAN 上部署了 MAB 功能后，无线设备会自动窥探连接的终端的 MAC 地址，并利用 MAC 地址作为账号向认证服务器发起求。

802.1x 认证模式的应用场景如下图所示。

图 1-3



功能部属

- 在 AP（AP1 和 AP2）上配置 WLAN。
- 在 AP（AP1 和 AP2）上配置认证服务器。
- 在 AP（AP1 和 AP2）上 WLAN 安全模式下配置 802.1x 认证模式。

1.3 功能详解

基本概念

WPA

Wi-Fi Protected Access，WPA 是 Wi-Fi 联盟定义的无线安全草案，IEEE802.11i 标准兼容该草案。

RSN

Robust Security Network，鲁棒性安全网络。IEEE802.11i 标准定义了 RSN 的概念，针对 WEP 加密机制的各种缺陷做了多方面的改进，功能上完全等同于 Wi-Fi 联盟推出的 WPA2。

TKIP

Temporal Key Integrity Protocol，临时密钥完整性协议，是对 WEP 安全性的增强。TKIP 提供每一数据包密钥混合、消息完整性核实和重新生成密钥机制，从而消除 WEP 的隐患。

AES

Advanced Encryption Standard，高级加密算法。AES 是 1997 年 1 月美国国家标准和技术研究所（NIST）发布征集的新加密算法。2000 年 10 月 2 日，由比利时设计者 Joan Daemen 和 Vincent Rijmen 设计的 Rijndael 算法以其优秀的性能和抗攻击能力，最终赢得了胜利，成为新一代的加密标准 AES。

CCMP

Counter CBC-MAC Protocol， 计数器模式密码块链消息完整码协议。CCMP 采用了比 TKIP 更安全的 AES 加密算法。

AKM

Authentication and Key Management，认证与密钥管理，即用户连接 WLAN 的接入认证方式。

功能特性

功能特性	作用
链路验证	STA 关联 WLAN 之前进行的无线链路安全验证。
接入认证	对接入 WLAN 的 STA 进行身份认证。
无线数据加密	实现对加入 WLAN 之后的 STA 通信数据的安全保护。

1.3.1 链路验证

链路验证即 802.11 身份验证，是一种低级的身份验证机制。在 STA 同 AP 进行 802.11 关联时发生，该行为早于接入认证。任何一个 STA 试图连接网络之前，都必须进行 802.11 的身份验证进行身份确认。可以把 802.11 身份验证看作是 STA 连接到网络时的握手过程的起点，是网络连接过程中的第一步。

IEEE 802.11 标准定义了两种链路层的认证：

- 开放系统链路验证
- 共享密钥链路验证

工作原理

开放系统链路验证

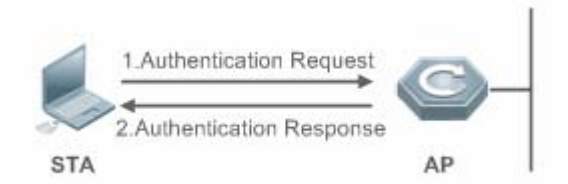
开放系统链路验证允许任何用户接入到无线网络中来。从这个意义上来说，实际上并没有提供对数据的保护，即不认证。也就是说，如果认证类型设置为开放系统认证，则所有请求认证的 STA 都会通过认证。

开放系统链路验证包括两个步骤：

第一步，STA 请求认证。STA 发出认证请求，请求中包含 STA 的 ID（通常为 MAC 地址）。

第二步，AP 返回认证结果。AP 发出认证响应，响应报文中包含表明认证是成功还是失败的消息。如果认证结果为“成功”，那么 STA 和 AP 就通过双向认证。

图 1-4



↘ 共享密钥链路验证

共享密钥链路验证是除开放系统链路验证以外的另外一种认证机制。共享密钥认证需要 STA 和 AP 配置相同的共享密钥。仅静态 WEP 加密模式下可配置共享密钥链路验证方式，其他模式均使用开放系统链路验证方式。

共享密钥链路验证的过程如下：

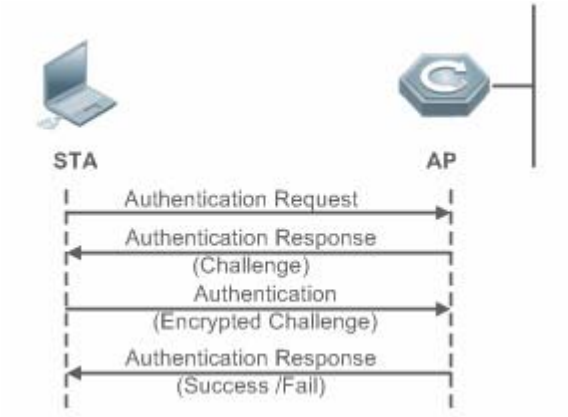
第一步，STA 先向 AP 发送认证请求；

第二步，AP 会随机产生一个 Challenge 包（即一个字符串）发送给 STA；

第三步，STA 会将接收到字符串拷贝到新的消息中，用密钥加密后再发送给 AP；

第四步，AP 接收到该消息后，用密钥将该消息解密，然后对解密后的字符串和最初给 STA 的字符串进行比较。如果相同，则说明 STA 拥有无线设备端相同的共享密钥，即通过了共享密钥认证；否则共享密钥认证失败。

图 1-5



1.3.2 接入认证

接入认证是一种增强 WLAN 安全性的解决方案。

当 STA 同 AP 关联后，是否可以使用无线接入点的服务要取决于接入认证的结果。如果认证通过，则无线接入点为 STA 打开这个逻辑端口，否则不允许用户连接网络。

IEEE 802.11 标准定义了两种接入认证方式：

- PSK接入认证
- 802.1X接入认证

工作原理

↘ PSK 接入认证

PSK（Pre-shared key，预共享密钥）是一种 802.11i 身份验证方式，以预先设定好的静态密钥进行身份验证。该认证方式需要在无线用户端和无线接入设备端配置相同的预共享密钥。如果密钥相同， PSK 接入认证成功；如果密钥不同，PSK 接入认证失败。

↘ 802.1X 接入认证

802.1X 协议是一种基于端口的网络接入控制协议。这种认证方式在 WLAN 接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在接口上的用户设备如果能通过认证，就可以访问 WLAN 中的资源；如果不能通过认证，则无法访问 WLAN 中的资源。

一个具有 802.1x 认证功能的无线网络系统必须具备以下三个要素才能够完成基于端口的访问控制的用户认证和授权：

- 认证客户端

一般安装在用户的工作站上，当用户有上网需求时，激活客户端程序，输入必要的用户名和口令，客户端程序将会送出连接请求。

- 认证者

在无线网络中就是无线接入点 AP 或者具有无线接入点 AP 功能的通信设备。其主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口。

- 认证服务器

通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的服务，并根据认证结果向认证系统发出打开或保持端口关闭的状态。

其中 MAB 认证利用 MAC 地址作为账号向认证服务器发起求，所以终端上可以不安装认证客户端软件。

1.3.3 无线数据加密

相对于有线网络，无线网络存在着更大的数据安全隐患。在一个区域内的所有的 WLAN 设备共享一个传输媒介，任何一个设备可以接收到其他所有设备的数据，这个特性直接威胁到 WLAN 接入数据的安全。

IEEE 802.11i 协议定义了以下三种无线数据加密算法：

- WEP加密
- TKIP加密
- AES加密

工作原理

↘ WEP加密

WEP（Wired Equivalent Privacy，有线等效加密）是原始 IEEE 802.11 标准中指定的数据加密方法，是 WLAN 安全认证和加密的基础，用来保护无线局域网中授权用户所交换的数据的私密性，防止这些数据被窃取。

WEP 使用 RC4 算法来保证数据的保密性，通过共享密钥来实现认证。WEP 没有规定密钥的管理方案，一般手动进行密钥的配置与维护。通常把这种不具密钥分配机制的 WEP 称为手动 WEP 或者静态 WEP。

WEP 加密密钥的长度一般有 64 位和 128 位两种。其中有 24Bit 的 IV（Initialization Vector，初始化向量）是由系统产生的。因此需要在 AP 和 STA 上配置的共享密钥就只有 40 位或 104 位。在实际中，已经广泛使用 104 位密钥的 WEP 来代替 40 位密钥的 WEP，104 位密钥的 WEP 称为 WEP-104。虽然 WEP-104 在一定程度上提高了 WEP 加密的安全性，但是受到 RC4 加密算法以及静态配置密钥的限制，WEP 加密还是存在比较大的安全隐患，无法保证数据的机密性、完整性和对接入用户实现身份认证。

↘ TKIP 加密

TKIP（Temporal Key Integrity Protocol，暂时密钥集成协议） 是 IEEE 802.11 组织为修补 WEP 加密机制而创建的一种临时的过渡方案。TKIP 也和 WEP 加密机制一样使用的是 RC4 算法，但是相比 WEP 加密机制，TKIP 加密机制可以为 WLAN 服务提供更加安全的保护。主要体现在以下几点：

–静态 WEP 的密钥为手工配置，且一个服务区内的所有用户都共享同一把密钥。而 TKIP 的密钥为动态协商生成，每个传输的数据包都有一个与众不同的密钥。

– TKIP 将密钥的长度由 WEP 的 40 位加长到 128 位，初始化向量 IV 的长度由 24 位加长到 48 位，提高了 WEP 加密的安全性。

– TKIP 支持 MIC 认证（Message Integrity Check，信息完整性校验）和防止重放攻击功能。

↘ AES 加密

AES-CCMP（Counter mode with CBC-MAC Protocol，计数器模式搭配 CBC-MAC 协议）是目前为止面向大众的最高级无线安全协议。

IEEE 802.11i 要求使用 CCMP 来提供全部四种安全服务：认证、机密性、完整性和重发保护。CCMP 使用 128 位 AES（Advanced Encryption Standard，高级加密标准）加密算法实现机密性，使用 CBC-MAC（区块密码锁链 - 信息真实性检查码协议）来保证数据的完整性和认证。

作为一种全新的高级加密标准，AES 加密算法采用对称的块加密技术，提供比 WEP/TKIP 中 RC4 算法更高的加密性能，成为取代 WEP 的新一代的加密技术，为无线网络带来更强大的安全防护。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置静态WEP模式	⚠ 必须配置。用于启用静态 WEP 加密模式。	
	security static-wep-key encryption	配置 WLAN 启用静态 WEP 模式，同时配置静态 WEP 密钥。
	⚠ 可选配置。用于配置链路验证方式。	
	security static-wep-key authentication	配置静态 WEP 模式的链路验证方式。
配置WPA认证	⚠ 必须配置。用于启用 WPA 认证模式。	
	security wpa	配置 WLAN 的认证模式为 WPA 认证模式。
	security wpa ciphers	配置 WPA 认证模式的加密方式。
	security wpa akm	配置 WPA 认证模式的接入认证方式。

	可选配置。用于配置 WPA PSK 认证方式的共享密码。	
	security wpa akm psk set-key	配置 WPA PSK 认证方式的共享密码。
配置RSN认证	必须配置。用于启用 RSN 认证模式。	
	security rsn	配置 WLAN 的认证模式为 RSN 认证模式。
	security rsn ciphers	配置 RSN 认证模式的加密方式。
	security rsn akm	配置 RSN 认证模式的接入认证方式。
	可选配置。用于配置 RSN PSK 认证方式的共享密码。	
	security rsn akm psk set-key	配置 RSN PSK 认证方式的共享密码。
配置MAB认证	可选配置。用于配置 MAB 认证模式。	
	dot1x-mab	配置开启 MAB 认证方式。
配置认证参数	可选配置。用于配置密钥交互相关参数及 WEB 认证模式下的防抖时间参数。	
	authtimeout forbidcount	配置四次握手 key 交互失败后，禁止关联的次数。
	authtimeout forbidtime	配置四次握手 key 交互失败后，禁止关联的时间间隔。
	authtimeout groupcount	配置组播密钥协商报文重传次数。
	authtimeout grouptime	配置组播密钥协商报文超时时间。
	authtimeout paircount	配置单播密钥协商报文重传次数。
	authtimeout pairtime	配置单播密钥协商报文超时时间。
	webauth prevent-jitter	配置 WEB 认证防抖时间。

1.4.1 配置静态WEP模式

配置效果

- 启用静态 WEP 加密模式，对 WLAN 中的数据提供 WEP 加密保护。
- 可配置链路验证方式。

注意事项

- 链路验证方式必须在启用静态 WEP 加密模式之后才可以配置。
- 在同一个 WLAN 安全模式下，静态 WEP 加密不可与其他认证加密同时配置。
- 只有 1 个 WLAN 可配置静态 WEP 加密模式。

配置方法

↘ 启用静态 WEP 模式

- 必须配置。
- 在 AP 设备上要启用静态 WEP 加密模式的 WLAN 对应的安全配置模式下配置。

【命令格式】 **security static-wep-key encryption** *key-length* { **ascii** | **hex** } *key-index key*

【参数说明】 *key-length*：密码长度，单位是比特，可以为 40 或 104。

ascii：密码形式为 ASCII 码。

hex：密码形式为 16 进制字符。

key-index：密钥索引号，配置范围是：1--4。

key：密码数据。

【缺省配置】 未启用静态 WEP 模式。

【命令模式】 WLAN 安全配置模式

【使用指导】 这条命令在配置静态 WEP 密钥，同时启用静态 WEP 模式。

这条命令可以重复配置，最后一次配置的命令生效。

密钥数据长度必须与命令中指定的 *key-length* 参数一致。

↘ 配置链路验证方式

- 可选配置。默认链路验证方式为开放系统链路验证，可使用该命令配置为共享密钥链路验证方式。
- 在 AP 设备上启用静态 WEP 加密模式的安全配置模式下配置。
- 必须在启用静态 WEP 模式之后才可以配置链路验证方式。配置共享密钥链路验证方式之后，STA 端也应该将链路验证方式选择为共享式，否则无法加入 WLAN。

【命令格式】 **security static-wep-key authentication** { **open** | **share-key** }

【参数说明】 **open**：配置开放系统链路验证方式。

share-key：配置共享密钥链路验证方式。

【缺省配置】 STA 加入 WLAN 采用开放系统链路验证方式

【命令模式】 WLAN 安全配置模式

【使用指导】 先配置完静态 WEP 密钥后才能配置链路验证方式。

除了静态 WEP 模式之外的其它安全配置模式，无法配置链路验证方式。

检验方法

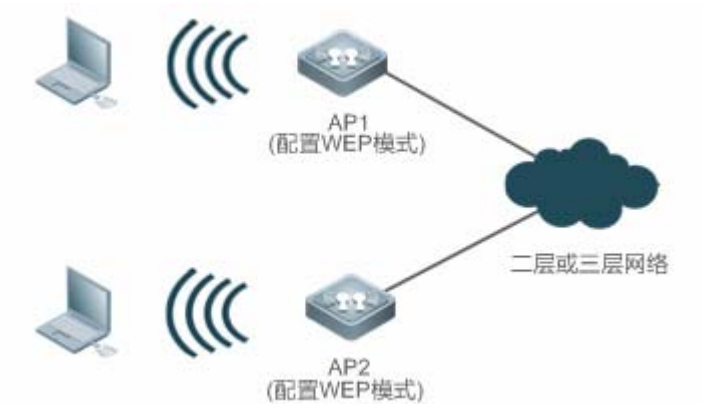
使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

↘ 配置 WLAN 1 为静态 WEP 加密模式，且使用共享密钥链路验证方式

【网络环境】

图 1-6



胖 AP 环境中，在 AP（AP1 或者 AP2）设备上配置 WLAN 1，并配置 WLAN 1 的安全策略为：

1、静态 WEP 加密模式；

2、使用共享密钥链路验证方式。

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用静态 WEP 加密模式及 WEP 密钥。
- 配置链路验证方式为共享密钥链路验证。

AP

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security static-wep-key encryption 40 ascii 1 12345
Ruijie(config-wlansec)#security static-wep-key authentication share-key
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AP

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security static-wep-key encryption 40 ascii 1 12345
 security static-wep-key authentication share-key
!
```

常见错误

- 配置的密码字符数与指定的密码长度不一致。
- 配置多个 WLAN 为静态 WEP 模式。
- 未配置启用静态 WEP 模式就配置链路验证方式。

1.4.2 配置WPA认证

配置效果

- WLAN 启用 WPA 认证模式。

- 指定 WPA 认证模式下的接入认证方式和数据加密方式。

注意事项

- 使用 WPA 认证时，需要配合配置数据加密方式和接入认证方式。
- 如果配置接入认证方式为 PSK，需配置 PSK 密码。
- 在同一个 WLAN 安全模式下，WPA 认证模式不能与 WEP 模式同时配置。

配置方法

↘ 配置 WPA 认证模式

- 必须配置。
- 在 AP 设备上要启用 WPA 认证模式的 WLAN 对应的安全配置模式下配置。

【命令格式】 **security wpa** { **enable** | **disable** }

【参数说明】 **enable**：启用 WPA 认证模式。

disable：关闭 WPA 认证模式。

【缺省配置】 关闭 WPA 认证模式。

【命令模式】 WLAN 安全配置模式

【使用指导】 只有启用了 WPA 认证模式才能在 WPA 模式下对加密方式和接入认证方式的配置，否则是配置是无效。

使用 WPA 认证时，需要配合配置加密方式和接入认证方式。如果只配置了加密方式，或者只配置了接入认证方式，或者两者都未配置，那么无线客户端将无法关联到无线网络。

↘ 配置 WPA 认证模式的数据加密方式

- 必须配置。
- 在 AP 设备上启用 WPA 认证模式的安全配置模式下配置。
- 必须在启用 WPA 认证模式之后才可以配置 WPA 认证模式下的数据加密方式。一个 WLAN 安全配置模式下可同时开启 AES 和 TKIP 两种加密方式。配置 WLAN 的数据加密方式之后，STA 加入 WLAN 之后的通信数据将使用相应的数据加密方式进行保护。

【命令格式】 **security wpa ciphers** { **aes** | **tkip** } { **enable** | **disable** }

【参数说明】 **aes**：配置加密方式为 AES。

tkip：配置加密方式为 TKIP。

enable：开启 WPA 认证模式的加密方式。

disable：关闭 WPA 认证模式的加密方式。

【缺省配置】 未配置数据加密方式

【命令模式】 WLAN 安全配置模式

【使用指导】 这个命令是用来启用 WPA 认证模式下的加密方式，有 AES 和 TKIP 两种加密方式。

一个 WLAN 安全配置模式下可同时开启 AES 和 TKIP 两种加密方式。

↘ 配置 WPA 认证模式的接入认证方式

- 必须配置。
- 在 AP 设备上启用 WPA 认证模式的安全配置模式下配置。
- 必须在启用 WPA 认证模式之后才可以配置 WPA 认证模式下的接入认证方式。一个 WLAN 安全配置模式下只能开启一种接入认证方式。启用接入认证方式的 WLAN，STA 必须通过相应的接入认证才可以加入 WLAN。

【命令格式】 **security wpa akm** { **psk** | **802.1x** } { **enable** | **disable** }

【参数说明】 **psk**：配置接入认证方式为预共享密钥认证。

802.1x：配置接入认证方式为 802.1x 认证。

enable：开启 WPA 认证模式的接入认证方式。

disable：关闭 WPA 认证模式的接入认证方式。

【缺省配置】 未配置接入认证方式。

【命令模式】 WLAN 安全配置模式

【使用指导】 只有启用了 WPA 认证模式才能进行接入认证方式的配置。

一个 WLAN 安全配置模式下只能开启一种接入认证方式。

↘ 配置 WPA 认证模式的共享密码

- 可选配置，启用 WPA PSK 认证方式时必须配置。
- 在 AP 设备上启用 WPA PSK 认证模式的安全配置模式下配置。

【命令格式】 **security wpa akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }

【参数说明】 **ascii**：指定 PSK 密码形式为 ASCII 码。

ascii-key：ASCII 码形式的密码，长度限制为 8--63 个 ASCII 码字符。

hex：指定 PSK 密码形式为十六进制字符。

hex-key：十六进制形式的密码，长度必须为 64 个十六进制字符。

【缺省配置】 无

【命令模式】 WLAN 安全配置模式

【使用指导】 只有开启了 PSK 认证方式时，这个共享密码才有意义。

ASCII 码形式的密码，长度限制为 8--63 个 ASCII 码字符。

十六进制形式的密码，长度必须为 64 个十六进制字符。

检验方法

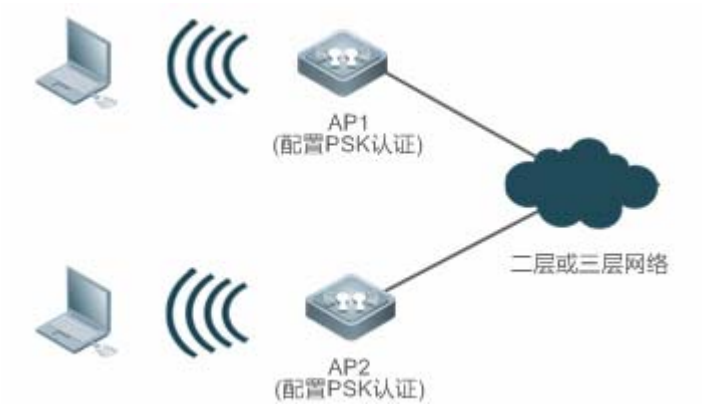
使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

↘ 配置 WLAN 1 为 WPA PSK 认证模式，数据加密方式为 AES，密码为 12345678。

【网络环境】

图 1-7



胖 AP 环境中，在 AP（AP1 或者 AP2）设备上配置 WLAN 1 的安全策略为：

1、配置为 WPA PSK 认证方式；

2、配置数据加密方式为 AES；

3、配置共享密码为 12345678。

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用 WPA 认证模式。
- 配置 WPA 认证模式的数据加密方式为 AES。
- 配置 WPA 认证模式的接入认证方式为 PSK。
- 配置 PSK 密码为 12345678。

AP

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security wpa enable
Ruijie(config-wlansec)#security wpa ciphers aes enable
Ruijie(config-wlansec)#security wpa akm psk enable
Ruijie(config-wlansec)#security wpa akm psk set-key ascii 12345678
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AP

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security wpa enable
 security wpa ciphers aes enable
 security wpa akm psk enable
 security wpa akm psk set-key ascii 12345678
!
```

常见配置错误

- WLAN 已经启用了其他的加密认证方式（如 WEP）。
- WLAN 安全配置模式下未启用 WPA 认证就配置 WPA 加密方式。
- WLAN 安全配置模式下未启用 WPA 认证就配置接入认证方式。

- WLAN 安全配置模式下已经开启了一种接入认证方式，则无法配置另一种接入认证方式。
- 未启用 WPA 认证，就配置 WPA PSK 密码。
- ASCII 码形式的密码长度不足 8 个字符或超过 63 个字符。
- 十六进制形式的密码长度不是 64 个十六进制字符。

1.4.3 配置RSN认证

配置效果

- WLAN 启用 RSN 认证模式。
- 指定 RSN 认证模式下的接入认证方式和数据加密方式。

注意事项

- 使用 RSN 认证时，需要配合配置数据加密方式和接入认证方式。
- 如果配置接入认证方式为 PSK，需配置 PSK 密码。
- 在同一个 WLAN 安全模式下，RSN 认证模式不能与 WEP 模式同时配置。

配置方法

↘ 配置 RSN 认证模式

- 必须配置。
- 在 AP 设备上要启用 RSN 认证模式的 WLAN 对应的安全配置模式下配置。

【命令格式】 **security rsn** { **enable** | **disable** }

【参数说明】 **enable**：启用 RSN 认证模式。

disable：关闭 RSN 认证模式。

【缺省配置】 关闭 RSN 认证模式。

【命令模式】 WLAN 安全配置模式

【使用指导】 只有启用了 RSN 认证模式才能在 RSN 模式下对加密方式和接入认证方式的配置，否则是配置是无效。

使用 RSN 认证时，需要配合配置加密方式和接入认证方式。如果只配置了加密方式，或者只配置了接入认证方式，或者两者都未配置，那么无线客户端将无法关联到无线网络。

↘ 配置 RSN 认证模式的数据加密方式

- 必须配置。
- 在 AP 设备上启用 RSN 认证模式的安全配置模式下配置。

- 必须在启用 RSN 认证模式之后才可以配置 RSN 认证模式下的数据加密方式。一个 WLAN 安全配置模式下可同时开启 AES 和 TKIP 两种加密方式。配置 WLAN 的数据加密方式之后，STA 加入 WLAN 之后的通信数据将使用相应的数据加密方式进行保护。

【命令格式】 **security rsn ciphers** { **aes** | **tkip** } { **enable** | **disable** }

【参数说明】 **aes**：配置加密方式为 AES。

tkip：配置加密方式为 TKIP。

enable：开启 RSN 认证模式的加密方式。

disable：关闭 RSN 认证模式的加密方式。

【缺省配置】 未配置数据加密方式

【命令模式】 WLAN 安全配置模式

【使用指导】 这个命令是用来启用 RSN 认证模式下的加密方式，有 AES 和 TKIP 两种加密方式。

一个 WLAN 安全配置模式下可同时开启 AES 和 TKIP 两种加密方式。

配置 RSN 认证模式的接入认证方式

- 必须配置。
- 在 AP 设备上启用 RSN 认证模式的安全配置模式下配置。
- 必须在启用 RSN 认证模式之后才可以配置 RSN 认证模式下的接入认证方式。一个 WLAN 安全配置模式下只能开启一种接入认证方式。启用接入认证方式的 WLAN，STA 必须通过相应的接入认证才可以加入 WLAN。

【命令格式】 **security rsn akm** { **psk** | **802.1x** } { **enable | disable** }

【参数说明】 **psk**：配置接入认证方式为预共享密钥认证。

802.1x：配置接入认证方式为 802.1x 认证。

enable：开启 RSN 认证模式的接入认证方式。

disable：关闭 RSN 认证模式的接入认证方式。

【缺省配置】 未配置接入认证方式

【命令模式】 WLAN 安全配置模式

【使用指导】 只有启用了 RSN 认证模式才能进行接入认证方式的配置。

一个 WLAN 安全配置模式下只能开启一种接入认证方式。

配置 RSN 认证模式的共享密码

- 可选配置，启用 RSN PSK 认证方式时必须配置。
- 在 AP 设备上启用 RSN PSK 认证模式的安全配置模式下配置。

【命令格式】 **security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }

【参数说明】 **ascii**：指定 PSK 密码形式为 ASCII 码。

ascii-key：ASCII 码形式的密码，长度限制为 8--63 个 ASCII 码字符。

hex：指定 PSK 密码形式为十六进制字符。

hex-key：十六进制形式的密码，长度必须为 64 个十六进制字符。

【缺省配置】 无

【命令模式】 WLAN 安全配置模式

【使用指导】 只有开启了 PSK 认证方式时，这个共享密码才有意义。

ASCII 码形式的密码，长度限制为 8--63 个 ASCII 码字符。
十六进制形式的密码，长度必须为 64 个十六进制字符。

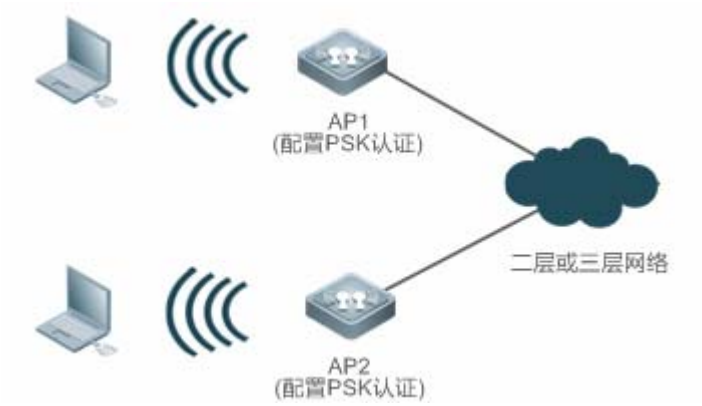
检验方法

使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

↘ 配置 WLAN 1 为 RSN PSK 认证模式，数据加密方式为 AES，密码为 12345678。

【网络环境】
图 1-8



胖 AP 环境中，在 AP（AP1 或者 AP2）设备上配置 WLAN 1 的安全策略为：
1、配置为 RSN PSK 认证方式；
2、配置数据加密方式为 AES；
3、配置共享密码为 12345678。

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用 RSN 认证模式。
- 配置 RSN 认证模式的数据加密方式为 AES。
- 配置 RSN 认证模式的接入认证方式为 PSK。
- 配置 PSK 密码为 12345678。

AP

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security rsn enable
Ruijie(config-wlansec)#security rsn ciphers aes enable
Ruijie(config-wlansec)#security rsn akm psk enable
Ruijie(config-wlansec)#security rsn akm psk set-key ascii 12345678
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AP

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security rsn enable
```

```
security rsn ciphers aes enable
security rsn akm psk enable
security rsn akm psk set-key ascii 12345678
!
```

常见配置错误

- WLAN 已经启用了其他的加密认证方式（如 WEP）。
- WLAN 安全配置模式下未启用 RSN 认证就配置 RSN 加密方式。
- WLAN 安全配置模式下未启用 RSN 认证就配置接入认证方式。
- WLAN 安全配置模式下已经开启了一种接入认证方式，则无法配置另一种接入认证方式。
- 未启用 RSN 认证，就配置 RSN PSK 密码。
- ASCII 码形式的密码长度不足 8 个字符或超过 63 个字符。
- 十六进制形式的密码长度不是 64 个十六进制字符。

1.4.4 配置MAB认证方式

配置效果

- WLAN 启用 MAB 认证模式。

注意事项

- 在同一个 WLAN 安全模式下，MAB 认证模式不能与 802.1x 接入认证模式或 WEP 模式同时配置，但是可以与 PSK 接入认证模式同时配置。

配置方法

↘ 配置 MAB 认证模式

- 必须配置。
- 在 AP 设备上要启用 MAB 认证模式的 WLAN 对应的安全配置模式下配置。
- 使用 **dot1x-mab** 命令可以启用 MAB 认证方式，使用 **no dot1x-mab** 命令关闭 MAB 功能。
- MAB 认证方式可以单独配置使用，无需启用 RSN/WPA 认证模式就可以配置。可以与 PSK 接入认证方式同时使用，但是不能与 802.1x 接入认证同时使用。

【命令格式】 **dot1x-mab**

【参数说明】 **no**：清除 MAB 认证模式。

【缺省配置】 未配置 MAB 认证方式

【命令模式】 WLAN 安全配置模式。

【使用指导】 这个命令是用来启用 MAB 认证模式。可以和 PSK 接入认证方式同时使用，但是不能和 802.1x 接入认证同时使用。

检验方法

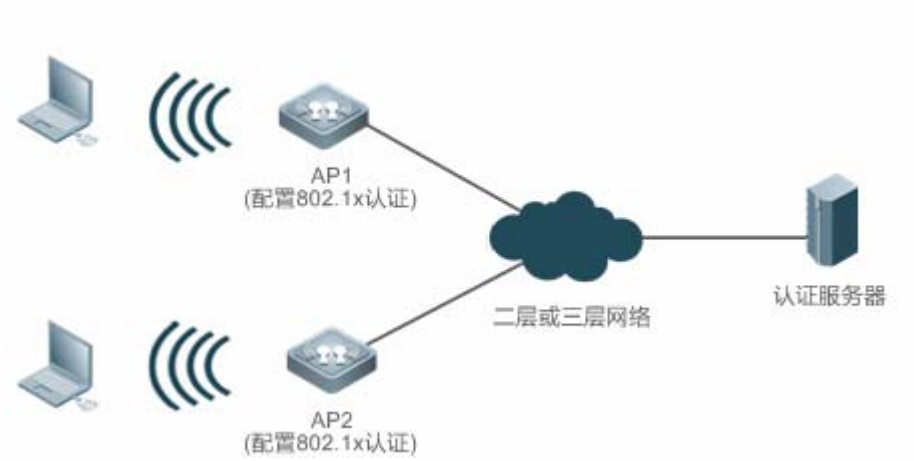
使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

↘ 配置 WLAN 1 为 MAB 认证模式。

【网络环境】

图 1-9



胖 AP 环境中，在 AP（AP1 或者 AP2）设备上配置 WLAN 1 的安全策略为：

1、配置为 MAB 认证方式；

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用 MAB 认证模式。

AP

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#dot1x-mab
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AP

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 dot1x-mab
!
```

常见配置错误

- WLAN 已经启用了其他的加密认证方式（如 WEP）。
- WLAN 安全配置模式下已经开启了 802.1x 接入认证模式，则无法配置。

1.4.5 配置认证参数

配置效果

- 配置密钥交互相关参数。
- 配置 WEB 认证模式下的防抖时间参数。

注意事项

- 密钥交互相关参数在 PSK 认证或 802.1x 认证方式下才生效。
- 必须先启用 WEB 认证，才可以配置 WEB 认证防抖时间参数。

配置方法

↘ 配置密钥交互相关参数

- 可选配置。一般不需要配置，无线网络环境较差的情况下可配置较大的报文重传次数及超时时间。
- 在 AP 设备上启用 PSK 认证或 802.1x 认证方式的安全配置模式下配置。

【命令格式】 **authtimeout** { **forbidcount** *count* | **forbidtime** *time* | **groupcount** *count* | **grouptime** *timeout* | **paircount** *count* | **pairtime** *timeout* }

【参数说明】 **forbidcount** *count*：配置四次握手 key 交互失败后，禁止关联的次数。
forbidtime *time*：配置四次握手 key 交互失败后，禁止关联的时间间隔。
groupcount *count*：配置组播密钥协商报文重传次数。
grouptime *timeout*：配置组播密钥协商报文超时时间。
paircount *count*：配置单播密钥协商报文重传次数。
pairtime *timeout*：配置单播密钥协商报文超时时间。

【缺省配置】 四次握手 key 交互失败后不禁止关联。
组播密钥协商报文重传次数缺省为 4 次
组播密钥协商报文超时时间缺省为 1200ms
单播密钥协商报文重传次数缺省为 4 次
单播密钥协商报文超时时间缺省为 1200ms

【命令模式】 WLAN 安全配置模式

【使用指导】 密钥交互相关参数在 PSK 认证或 802.1x 认证方式下才生效。

↘ 配置 WEB 认证防抖时间参数

- 可选配置。WEB 认证防抖时间默认为 300 秒，用户可根据实际需求配置防抖时间。或者通过配置 WEB 认证防抖时间为 0 秒关闭 WEB 认证防抖功能。
- 在 AP 设备上启用 WEB 认证的安全配置模式下配置。

【命令格式】 **webauth prevent-jitter** *timeout*

【参数说明】 *timeout*：配置 WEB 认证防抖时间，以秒为单位。*timeout* 的取值范围是 0s---86400s（*timeout* 为 0 表示关闭 WEB 认证防抖功能)。

【缺省配置】 WEB 认证防抖时间，缺省值为 300 秒。

【命令模式】 WLAN 安全配置模式

【使用指导】 必须先启用 WEB 认证，才可以配置 WEB 认证防抖时间。

检验方法

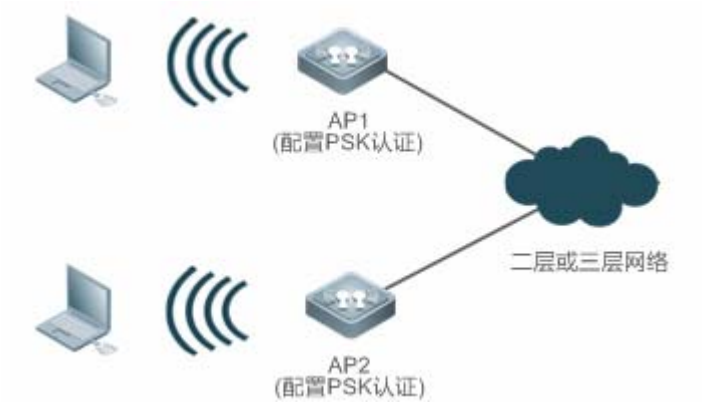
使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

配置举例

↘ 配置 WLAN 1 为 RSN-PSK + WEB 认证模式，配置单播密钥协商报文重传次数为 5 次，配置 WEB 认证防抖时间为 900 秒。

【网络环境】

图 1-10



胖 AP 环境中，在 AP（AP1 或者 AP2）设备上配置 WLAN 1 的安全策略为：

1、配置为 RSN PSK 认证方式；

2、启用 WEB 认证。

【配置方法】

- 进入 WLAN 1 的安全配置模式。
- 配置启用 RSN 认证模式。
- 配置 RSN 认证模式的数据加密方式为 AES。
- 配置 RSN 认证模式的接入认证方式为 PSK。
- 配置 PSK 密码为 12345678。
- 配置单播密钥协商报文重传次数为 5 次。
- 配置 WEB 认证。
- 配置 WEB 认证防抖时间为 900 秒。

AP

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#security rsn enable
Ruijie(config-wlansec)#security rsn ciphers aes enable
Ruijie(config-wlansec)#security rsn akm psk enable
Ruijie(config-wlansec)#security rsn akm psk set-key ascii 12345678
Ruijie(config-wlansec)#authtimeout paircount 5
Ruijie(config-wlansec)#webauth
Ruijie(config-wlansec)#webauth prevent-jitter 900
```

【检验方法】 使用 **show running-config | begin wlansec** *wlan_id* 命令，可以查看配置是否生效。

AP

```
Ruijie#show running-config | begin wlansec 1
wlansec 1
 security rsn enable
 security rsn ciphers aes enable
 security rsn akm psk enable
 security rsn akm psk set-key ascii 12345678
 webauth prevent-jitter 900
 webauth
 authtimeout paircount 5
```

常见配置错误

- 未启用 WEB 认证就配置 WEB 认证防抖时间参数。

1.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
显示 WLAN 的安全配置信息。	**show wlan security** *wlan-id*
查看 STA 的安全配置信息。	**show wclient security** *mac-address*

查看调试信息

无。

2 WIDS

2.1 概述

WLAN 具有安装便捷、使用灵活、经济节约和易于扩展等有线网络无法比拟的优点，因此得到越来越广泛的使用。但由于 WLAN 信道开放的特点，使得无线网络很容易受到各种网络威胁的影响，如冒牌的 AP 设备、Ad-hoc 网络、各种针对无线网络的协议攻击等等，因此安全性成为阻碍 WLAN 发展的重要因素。

WIDS（Wireless Intrusion Detection System，无线入侵检测系统）可以对恶意的用户攻击和入侵行为进行早期检测，帮助网络管理者主动发现网络中的隐患，在第一时间对无线攻击者进行主动防御和预警。

下文仅介绍 WIDS 的相关内容。

协议规范

无。

2.2 典型应用

无。

2.3 功能详解

基本概念

工作模式的分类

工作模式可以分为如下三种：

- normal 模式，仅提供接入服务
- monitor 模式，仅提供监测服务
- hybrid 模式，提供监测服务和接入服务

IDS 攻击检测类型

IDS 攻击检测类型有如下五种：

- DDOS 攻击检测，包含检测 ARP、ICMP 以及 SYN 报文的拒绝服务攻击。
- Flooding 攻击检测，包含检测单用户或者多用户的管理报文泛洪攻击。
- Spoof 攻击检测，表示检测广播解除关联和解除认证攻击。

- Weak IV 攻击检测，表示检测弱向量攻击。

用户隔离模式

用户隔离模式有如下两种：

- 基于 AP 二层用户隔离，同 AP 下的二层用户通讯隔离。
- 基于 AP-SSID 二层用户隔离，同 AP 下相同 WLAN 下的二层用户隔离。

Rogue 设备反制模式

Rogue 设备反制模式有如下四种：

- Adhoc 反制模式，反制 Rogue Ad-hoc 设备。
- Rogue 反制模式，反制信号强度超过阈值的 Rogue 设备。
- SSID 反制模式，反制 SSID 一样的非法设备。
- Config 反制模式，反制与静态攻击列表或者 SSID 黑名单中一样的非法设备。

Rogue 设备模糊反制

- 对 Rogue AP 的 SSID 进行模糊匹配，例如本机的 SSID 为 RUIJIE-WEB,开启模糊反制后能够反制 SSID 名称为 RU1JIE-WEB 的 Rogue AP。

Rogue 设备检测分类

Rogue 设备检测分类如下：

- AP 设备
- Ad-hoc 设备
- 未知名 STA 设备

功能特性

功能特性	作用
帧过滤	通过一定的帧过滤规则判定是否允许指定无线客户端的报文通过，实现了对无线终端用户的接入控制
IDS攻击检测	及时发现并防御 WLAN 网络中恶意或者无意的攻击
用户隔离	控制在无线网络覆盖区域中，无线终端之间的不安全访问，避免私人信息遭到他人窃取。
Rogue设备检测与反制	Rogue 设备检测功能，可以对整个 WLAN 网络中的异常设备进行监视，帮助网络管理者发现网络中的隐患。 Rogue 设备反制是使用攻击列表中的 Rogue 设备的地址发送假的解除认证帧来对 Rogue 设备进行反制。

2.3.1 帧过滤

用于对无线终端用户的接入控制，主要包括：低速用户过滤、白名单列表、静态黑名单列表、动态黑名单列表、基于 SSID 的白名单和基于 SSID 的黑名单。

工作原理

↘ 低速用户过滤

低速用户过滤主要通过低速用户过滤阈值，当阈值大于 0 的时候，表示低速用户过滤功能开启。如果用户的速率低于该阈值，用户的报文将被丢弃，同时用户将被剔除出设备。

↘ 白名单列表

白名单列表中包含了允许接入的无线客户端的 MAC 地址，如果启用了白名单功能，则只有白名单中指定的无线用户可以接入到 WLAN 网络中，其他的无线用户的所有报文都将被 AP 直接丢弃，从而减少非法报文对无线网络的冲击。

↘ 静态黑名单列表

静态黑名单列表中包含了拒绝接入的无线客户端的 MAC 地址，如果启用了静态黑名单功能，则黑名单中指定的无线用户的所有报文都将被 AP 丢弃。

↘ 动态黑名单列表

动态黑名单列表中包含了拒绝接入的无线客户端的 MAC 地址，可以在 WIDS 检测到 IDS 攻击时动态添加动态黑名单。当 WLAN 检测到来自某一终端设备的无线入侵攻击时，可以选择将该设备的 MAC 地址动态加入到黑名单中，禁止接收任何来自于该设备的报文，实现 WLAN 网络的安全保护。

↘ 基于 SSID 的白名单列表

基于 SSID 白名单列表包含了指定 SSID 允许接入的无线客户端的 MAC 地址，用户可以通过命令行进行配置。如果启用了基于 SSID 白名单功能，则在该 SSID 子集内，只有白名单中指定的无线用户可以接入，其他无线用户的所有报文都将被 AP 直接丢弃，从而减少非法报文对无线网络的冲击。

↘ 基于 SSID 的黑名单列表

基于 SSID 黑名单列表包含了指定 SSID 拒绝接入的无线客户端的 MAC 地址，用户可以通过命令行进行配置。如果启用了基于 SSID 黑名单功能，则在该 SSID 子集内，黑名单中指定的无线用户的所有报文都将被 AP 丢弃。

2.3.2 IDS攻击检测

为了及时发现并防御 WLAN 网络中恶意或者无意的攻击，WIDS 支持对多种攻击行为进行检测。当 WIDS 检测到攻击后，会产生告警或者日志信息，提醒网络管理者进行相应处理。根据检测的结果，网络管理员可以及时调整网络的配置，清除 WLAN 网络的不安全因素。

目前设备支持的 IDS 攻击检测有以下五种：

- DDOS 攻击检测（分布式拒绝服务攻击检测）
- Flooding 攻击检测（泛洪攻击检测）
- Spoof 攻击检测（欺骗攻击检测）
- Weak IV 检测（弱初始化向量检测）

工作原理

DDOS 攻击检测

DDOS 攻击是指攻击者在短时间内向目标设备发送大量的攻击报文(目前识别 ARP 报文、ICMP 报文、SYN 报文)，从而影响合法用户关联到被攻击设备。

WIDS 的 DDOS 检测功能通过对攻击者的报文进行统计，通过判断报文的 PPS（每秒报文数）是否超出配置阈值，如果超出会将这个检测结果记录到日志中。如果开启动态黑名单功能，则将攻击者加入动态黑名单链表中。

Flooding 攻击检测

Flooding（泛洪）攻击是指攻击者在短时间内发送大量的同种类型的报文，导致 WLAN 设备被攻击者发送的泛洪报文淹没而无法处理真正正当的用户请求。

WIDS攻击检测通过持续地监控每台设备的流量大小来预防这种泛洪攻击。在规定时间内，当流量超出网络管理者设置的上限时，该设备被认为正在进行网络泛洪攻击从而被锁定。Flooding攻击检测可以和 动态黑名单功能配合使用，当WIDS检测到Flooding攻击时，此时如果开启了动态黑名单功能，则发起攻击的无线客户端将被添加到动态黑名单中，从而保证WLAN系统不会再次被该设备攻击，保障网络安全。

Spoof 攻击检测

Spoof（欺骗）攻击是指攻击者以其他设备的名义发送仿冒报文。例如：一个仿冒的解除认证报文会导致无线客户端下线。

WIDS 通过对广播解除认证和广播解除关联报文进行检测，当接收到这类报文时将立刻被定义为欺骗攻击并被记录到日志中。

Weak IV 攻击检测

Weak IV（Weak Initialization Vector，弱初始化向量）攻击是指在 WLAN 使用 WEP 加密的过程中，攻击者通过截获带有弱初始化向量的报文，破解出共享密钥并最终窃取加密信息的一种攻击行为。

WLAN 使用 WEP 进行加密的时候，对于每一个报文都会产生一个 IV，IV 和共享密钥一起作为输入来生成密钥串。密钥串同明文加密，最终生成密文。当一个 WEP 报文被发送时，用于加密报文的 IV 也作为报文头的一部分被发送。如果使用不安全的方法生成 IV，例如频繁生成重复的 IV 甚至是始终生成相同的 IV，就会轻易暴露共享密钥。如果潜在的攻击者获得了共享的密钥，攻击者将能够控制网络资源，对网络安全造成威胁。

WIDS 通过识别每个 WEP 报文的 IV 来预防这种攻击，当一个带有弱初始化向量的报文被检测到时，WIDS 即判定这是个攻击漏洞，将立刻将这个检测结果记录到日志中。

2.3.3 用户隔离

由于无线用户的流动性和不确定性，在某些场合（特别是在公共场合），用户信息的私密性显得尤为重要，需要限制用户之间直接访问。用户隔离技术可以控制在无线网络覆盖区域中，无线终端之间的不安全访问（例如无线上网用户之间通过网上邻居访问），避免私人信息遭到他人窃取。

用户隔离功能在不影响用户正常上网的情况下对用户进行隔离，使之不能互访，保证了用户业务的安全。用户隔离功能分成以下两种：

- 基于 AP的二层用户隔离
- 基于 AP-SSID 的二层用户隔离

工作原理

↘ 基于 AP 的二层用户隔离

关联到同一个 AP 上的所有二层用户之间不能直接进行通讯。

↘ 基于 AP-SSID 的二层用户隔离

关联到同一 AP 上的同一个 WLAN 下的用户之间不能直接进行通讯。

2.3.4 Rogue设备检测与反制

一般可以把网络中的设备分为两种类型：非法设备（Rogue 设备）和合法设备。Rogue 设备可能存在安全漏洞或被攻击者操纵，因此会对用户网络的安全造成严重威胁或危害。WIDS 的 Rogue 设备检测功能，可以对整个 WLAN 网络中的异常设备进行监视，帮助网络管理者发现网络中的隐患。

Rogue 设备检测可以检测 WLAN 中多种 Rogue 设备：Rogue AP，Rogue Client，Rogue 无线网桥，Ad-hoc 网络等。目前，仅支持对 Rogue AP 和 Ad-hoc 网络的检测以及未知名 STA 的检测。

Rogue 设备反制是使用 Rogue 设备的地址发送假的解除认证帧来对 Rogue 设备进行反制，防止用户接入非法的服务或者非法的用户接入设备。

工作原理

↘ Rogue 设备检测

Rogue 设备检测功能是由工作在监听模式或者混合模式下的 AP 进行检测的。WIDS 通过在无线网络中部署一些 AP 并设置它们工作在监听或者混合模式，捕捉空气介质中的无线报文。通过对监听到的无线报文进行分析统计，AP 就可以获取到 Rogue 设备的信息。同时，网络管理员还可以通过制定非法设备的检测规则，对整个 WLAN 网络中的异常设备进行监视。

↘ 未知名 STA 检测

未知名 STA 检测功能是对网络中非已接入用户的探测请求报文进行监测，同时网络管理员还可以通过配置来指定未知名 STA 信息。

Rogue 设备反制

Rogue 设备反制指的是通过模拟假的广播解除认证报文来反制符合反制模式规则的 Rogue 设备，反制正常用户接入 Rogue 设备的服务。

未知名 STA 反制

未知名 STA 反制指的是直接构造解除认证报文来防止未知名的 STA 的接入。

2.4 配置详解

配置项	配置建议&相关命令	
配置帧过滤功能	可选配置，用于设置帧过滤功能的配置	
	kickout threshold	配置低速用户过滤阈值
	whitelist mac-address	配置白名单列表表项
	whitelist max	配置白名单列表长度
	static-blacklist mac-address	配置静态黑名单列表表项
	static-blacklist max	配置静态黑名单列表长度
	dynamic-blacklist enable	配置动态黑名单功能
	dynamic-blacklist lifetime	配置动态黑名单表项生存时间
	dynamic-blacklist ap-max	配置动态黑名单列表 AP 端长度
	ssid-filter max	配置基于 SSID 的黑、白名单和 SSID 列表长度
	ssid-filter blacklist mac-address	配置基于 SSID 的黑名单列表表项
	ssid-filter blacklist max	配置基于 SSID 的黑名单列表长度，默认 256
	ssid-filter whitelist mac-address	配置基于 SSID 的白名单列表表项
	ssid-filter whitelist max	配置基于 SSID 的白名单列表长度，默认 256
配置IDS攻击检测功能	可选配置，用于配置 IDS 攻击检测配置	
	attack-detection enable	配置 IDS 攻击检测功能的检测类型
	attack-detection ddos	配置 ddos 攻击检测周期时长和指定类型报文的报文检测阈值
	attack-detection flood multi-mac	配置 flood 攻击检测的多用户攻击检测阈值和周期检测时长
	attack-detection flood single-mac	配置 flood 攻击检测的单用户攻击检测阈值和周期检测时长
	attack-detection weak-iv	配置 weak-iv 攻击检测报文阈值和检测周期时长
	attack-detection statistics ap-max	配置 IDS 攻击检测统计列表 AP 端长度
配置用户隔离功能	可选配置，用于设置用户隔离功能功能	

	user-isolation enable	配置使能基于 ap、基于 ap-ssid 二层用户隔离功能模式
	user-isolation permit-mac	配置隔离允许 MAC 列表表项
	user-isolation permit-mac max	配置隔离允许 MAC 列表长度
配置Rogue设备检测与反制	可选择配置，用于设置设备检测与反制功能	
	countermeasures enable	配置使能设备反制功能
	countermeasures ap-max	配置单次反制的设备数量
	countermeasures channel-match	配置使能基于信道反制
	countermeasures interval	配置反制周期时长
	countermeasures mode	配置反制模式
	countermeasures rssi-min	配置反制的信号强度下限
	countermeasures fuzzy-enable	配置开启模糊反制
	device aging duration	配置检测到的设备生存时间
	device attack mac-address	配置静态攻击列表表项
	device attack max	配置静态攻击列表长度
	device black-ssid	配置 SSID 黑名单列表表项
	device max-black-ssid	配置 SSID 黑名单列表长度
	device friendly-flags	配置设备友好标识
	device permit mac-address	配置允许 MAC 列表表项
	device permit mac-address max	配置允许 MAC 列表长度
	device permit ssid	配置允许 SSID 列表表项
	device permit max-ssid	配置允许 SSID 列表长度
	device permit vendor bssid	配置允许产商列表表项
	device permit vendor bssid max	配置允许产商列表长度
	device unknown-sta dynamic-enable	配置使能未知名 STA 功能
	device unknown-sta mac-address	配置未知名 STA 列表表项
	device unknown-sta mac-address max	配置未知名 STA 列表长度
	device detected-ap-max	配置扫描 AP 检测名单最大个数
	hybrid-scan radio	配置指定 radio 的扫描状态
	scan-channels { 802.11a | 802.11b } channels	配置指定 AP 的扫描信道
配置AP工作模式	可选配置，用于设置 AP 工作模式	
	device mode	配置 AP 工作模式

2.4.1 配置帧过滤功能

配置效果

- 配置帧过滤规则，提供报文过滤服务。

注意事项

- 同一个配置信息不能同时在静态黑名单列表和白名单列表中存在。
- 同一个配置信息不能同时在同一个 SSID 的黑名单列表和白名单列表中存在。

配置方法

配置低速用户过滤功能

- 可选配置，使用 **kickout threshold** 命令在 WIDS 配置模式下配置低速用户过滤阈值。配置了低速用户过滤阈值（阈值>0）后，低速用户过滤功能才能够有效运行。

【命令格式】 **kickout threshold** *rate*
【参数说明】 *rate*：低速用户过滤阈值，可配置范围 0~130Mbps
【缺省配置】 默认情况下不过滤低速用户，速率阈值为 0
【命令模式】 WIDS 配置模式
【使用指导】 用户可以根据需要选择不同低速用户过滤阈值。

配置白名单功能

- 可选配置。
- 使用 **whitelist mac-address** 命令在 WIDS 配置模式下配置白名单列表的单个表项信息。配置了有效的白名单表项后，白名单列表过滤功能才能够有效运行。
- 使用 **whitelist max** 命令在 WIDS 配置模式下配置白名单列表的表项个数上限，表示设备上允许配置的白名单表项个数上限。

【命令格式】 **whitelist** { **mac-address** *H.H.H* | **max** *num* }
【参数说明】 **mac-address** *H.H.H*：白名单列表表项 mac 地址
max *num*：白名单列表长度，可配置范围 1~2048。
【缺省配置】 缺省情况下白名单列表为空，白名单列表长度默认为 1024
【命令模式】 WIDS 配置模式
【使用指导】 白名单列表中存在表项时，白名单功能才生效。

配置静态黑名单功能

- 可选配置。
- 使用 **static-blacklist mac-address** 命令在 WIDS 配置模式下配置静态黑名单列表的单个表项信息。配置了有效的静态黑名单表项后，静态黑名单列表过滤功能才能够有效运行。
- 使用 **static-blacklist max** 命令在 WIDS 配置模式下配置静态名单列表的表项个数上限，表项设备上允许的静态黑名单最多配置个数上限。

【命令格式】 **static-blacklist** { **mac-address** *H.H.H* | **max** *num* }

【参数说明】 **mac-address** *H.H.H*：静态黑名单列表表项 mac 地址

max *num*：静态黑名单列表长度，可配置范围 1~2048。

【缺省配置】 缺省情况下静态黑名单列表为空，静态黑名单列表长度默认为 1024

【命令模式】 WIDS 配置模式

【使用指导】 静态黑名单列表中存在表项时，静态黑名单功能才生效。

配置动态黑名单功能

- 可选配置。
- 使用 **dynamic-blacklist enable** 命令在 WIDS 配置模式下配置开启动态态黑名单列表过滤功能。开启了动态黑名单过滤功能后，动态黑名单的表项才会随着 IDS 攻击检测动态生成，同时动态黑名单列表过滤功能才会运行。
- 使用 **dynamic-blacklist lifetime** 命令在 WIDS 配置模式下配置动态态名单列表的生存时长，表示动态生成的动态黑名单表项信息可以在设备在存在多长时间。
- 使用 **dynamic-blacklist ap-max** 命令在 WIDS 配置模式下配置动态黑名单在 AP 端的表项个数上限，表示 AP 端设备最多允许的表项个数上限。
- 使用 **dynamic-blacklist mac-adress** 命令在 WIDS 配置模式下配置动态黑名单表项名单。

【命令格式】 **dynamic-blacklist** { **enable** | **lifetime** *time* | **ap-max** *num* | **mac-address** *H.H.H* }

【参数说明】 **enable**：使能动态黑名单功能

lifetime *time*：动态黑名单列表生存时间，可配置范围 60~86400s。

ap-max *num*：动态黑名单列表 AP 端长度

mac-address *H.H.H*：动态黑名单列表表项 mac 地址

【缺省配置】 缺省情况动态黑名单功能关闭，动态黑名单列表端长度默认为 2048，AP 端长度默认为 2048，动态黑名单生存时间 300s

【命令模式】 WIDS 配置模式

【使用指导】 动态黑名单列表表项在 IDS 攻击检测功能中生成。

配置基于 SSID 的黑名单功能

- 可选配置。
- 使用 **ssid-filter blacklist mac-address** 命令在 WIDS 配置模式下配置基于 ssid 的静态黑名单列表的单个表项信息。配置了有效的静态黑名单表项后，静态黑名单列表过滤功能才能够有效运行。
- 使用 **ssid-filter blacklist max** 命令在 WIDS 配置模式下配置基于 ssid 的静态名单列表的表项个数上限，表项设备上允许的静态黑名单最多配置个数上限。

【命令格式】 **ssid-filter** { **max** *num* | **blacklist mac-address** *H.H.H* **in-ssid** *string* | **blacklist max** *num* }

【参数说明】 **max** *num*：SSID 列表的最大长度，可配置范围 1 ~ 128

blacklist mac-address *H.H.H* **in-ssid** *string*：配置指定 SSID 的黑名单列表表项

blacklist max *num*：配置基于 SSID 的黑名单列长度，可配置范围 1~2048

【缺省配置】 基于 SSID 的黑名单列表为空

【命令模式】 WIDS 配置模式

【使用指导】 基于 SSID 的黑名单列表中存在表项时，功能才生效

↘ 配置基于 SSID 的白名单功能

- 可选配置。
- 使用 **ssid-filter whitelist mac-address** 命令在 WIDS 配置模式下配置基于 ssid 的白名单列表的单个表项信息。配置了有效的白名单表项后，白名单列表过滤功能才能够有效运行。
- 使用 **ssid-filter whitelist max** 命令在 WIDS 配置模式下配置基于 ssid 的白名单列表的表项个数上限，表示设备上允许配置的白名单表项个数上限。

【命令格式】 **ssid-filter** { **whitelist mac-address** *H.H.H* **in-ssid** *string* | **whitelist max** *num* }

【参数说明】 **whitelist mac-address** *H.H.H* **in-ssid** *string*：配置指定 SSID 的白名单列表表项

whitelist max *num*：配置基于 SSID 的白名单列长度，可配置范围 1~2048

【缺省配置】 基于 SSID 的白名单列表为空

【命令模式】 WIDS 配置模式

【使用指导】 基于 SSID 的白名单列表中存在表项时，功能才生效

检验方法

根据相应的帧过滤规则，进行相关的功能验证。

- 检测低速用户过滤功能，报文丢弃，低速用户成功被剔除。
- 检测白名单功能，白名单列表中存在配置时，非白名单列表中的用户无法加入 AP。
- 检测静态黑名单功能，静态黑名单中存在配置时，静态黑名单列表中的用户无法加入 AP。
- 检测动态黑名单功能，动态黑名单功能开启时，动态黑名单列表中的表项能够随着 IDS 攻击检测动态生成，在动态黑名单中的用户不能再次加入 AP。
- 检测基于 SSID 的黑名单功能，基于 SSID 的黑名单存在配置时，基于 SSID 的黑名单列表中的用户无法加入该 SSID 服务。
- 检测基于 SSID 的白名单功能，基于 SSID 的白名单存在配置时，非基于 SSID 的白名单列表中的用户无法加入该 SSID 服务。

配置举例

无。

常见错误

无。

2.4.2 配置IDS攻击检测功能

配置效果

- 通过 IDS 攻击检测功能，可以及时发现并防御 WLAN 网络中恶意或者无意的攻击。

注意事项

- IDS 攻击检测功能需要和动态黑名单功能配置使用，这样可以更有效防止 WLAN 网络的攻击。

配置方法

配置使能 IDS 攻击检测类型

- 可选配置，缺省情况下 IDS 攻击检测类型未开启。

【命令格式】 **attack-detection enable** { **all** | **ddos** | **flood** | **weak-iv** }

【参数说明】 **ddos**：配置 DDOS 攻击检测功能，默认关闭

flood：配置 Flooding 攻击检测功能，默认关闭

weak-iv：配置 Weak IV 攻击检测功能，默认关闭

all：配置开启所有 IDS 攻击检测类型，默认关闭

【缺省配置】 IDS 攻击检测的四种检测类型默认关闭

【命令模式】 WIDS 配置模式

【使用指导】 -

配置 DDOS 攻击检测

- 可选配置。
- 配置 DDOS 攻击检测指定类型报文阈值和周期时长，同上。

【命令格式】 **attack-detection ddos** { **arp-threshold** *num* | **icmp-threshold** *num* | **syn-threshold** *num* | **interval** *time* }

【参数说明】 **arp-threshold** *num*：arp 报文阈值，可配置范围 1～10000pps

icmp-threshold *num*：icmp 报文阈值，可配置范围 1～10000pps

syn-threshold *num*：syn 报文阈值，可配置范围 1～10000pps

interval *time*：ddos 攻击检测周期，可配置范围 10~60s

【缺省配置】 缺省情况下，DDOS 攻击检测周期为 30s，对应的三种 DDOS 攻击检测阈值分别：arp 报文为 50pps，icmp 报文为 100pps，syn 报文为 50pps

【命令模式】 WIDS 配置模式

【使用指导】 -

配置 Flooding 攻击检测

- 可选配置，缺省情况下 Flooding 攻击检测功能未开启。
- 使用 **attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time* 命令在 WIDS 配置模式下配置单用户的 flood 攻击的指定类型报文阈值和周期时长。
- 使用 **attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time* 配置模式下配置多用户的 flood 攻击的指定类型报文阈值和周期时长。

【命令格式】 **attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time*

【参数说明】 **single-mac**：单用户检测

total：全部报文

assoc：关联报文

reassoc：重关联报文

disassoc：解关联报文

probe：探测报文

action：action 报文

auth：认证报文

deauth：解认证报文

null-data：空数据报文

num：报文攻击检测阈值，可配置范围 1~10000

time：报文攻击检测周期，可配置范围 10~60s

【缺省配置】 所有 flood 攻击检测的报文阈值，单用户时默认 300，多用户默认 4800，统计周期默认 10s

【命令模式】 WIDS 配置模式

【使用指导】 -

【命令格式】 **attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time*

【参数说明】 **multi-mac**：多用户检测

assoc：关联报文

reassoc：重关联报文

disassoc：解关联报文

probe：探测报文

action：action 报文

auth：认证报文

deauth：解认证报文

null-data：空数据报文

num：报文攻击检测阈值，可配置范围 1~10000

time：报文攻击检测周期，可配置范围 10~60s

【缺省配置】 所有 flood 攻击检测的报文阈值，单用户时默认 300，多用户默认 4800 统计周期默认 10s。

【命令模式】 WIDS 配置模式

【使用指导】 -

配置 Weak IV 攻击检测

- 可选配置，缺省情况下 Weak IV 攻击检测功能未开启。
- 配置 Weak IV 攻击检测指定类型报文阈值和周期时长，同上。

【命令格式】 **attack-detection weak-iv** { **threshold** *num* | **interval** *time* }

【参数说明】 **threshold** *num*：Weak IV 攻击检测报文阈值，可配置范围 1～10000

interval *time*：Weak IV 攻击检测周期，可配置范围 1～60s

【缺省配置】 Weak IV 的默认检测周期时长为 15s，默认检测阈值为 10

【命令模式】 WIDS 配置模式

【使用指导】 -

检验方法

根据相应的 IDS 攻击检测类型。

- DDOS 攻击检测功能，检测 arp 报文攻击、icmp 报文攻击和 syn 报文攻击。
- Flooding 攻击检测功能，检测多用户泛洪攻击和单用户泛洪攻击。
- Spoof 攻击检测功能，检测广播解关联和解认证报文攻击。
- Weak IV 攻击检测功能，检测弱初始化向量报文攻击。

配置举例

无。

常见错误

无。

2.4.3 配置用户隔离功能

配置效果

- 配置用户隔离功能后，符合用户隔离规则的用户将不能直接通信。

注意事项

- 用户隔离功能仅针对二层用户进行隔离

配置方法

↘ 配置隔离模式

- 可选配置。

【命令格式】 **user-isolation** { **ap** | **ssid-ap** } **enable**

【参数说明】 **ap** :基于 AP 二层用户隔离

ssid-ap :基于 AP-SSID 二层用户隔离

【缺省配置】 默认关闭
【命令模式】 WIDS 配置模式
【使用指导】 -

↘ 配置隔离允许 MAC 列表

- 可选配置。

【命令格式】 **user-isolation permit-mac** { *H.H.H* | **max** *num* }
【参数说明】 *H.H.H*：隔离允许 MAC 列表表项信息
max *num*：隔离允许 MAC 列表长度，可配置范围 1～1024
【缺省配置】 用户隔离允许 MAC 列表为空，默认隔离允许 MAC 列表长度为 1024
【命令模式】 WIDS 配置模式
【使用指导】 -

检验方法

- 根据隔离模式进行相关验证。

配置举例

无。

常见错误

无

2.4.4 配置Rogue设备检测与反制

配置效果

配置 Rogue 设备检测与反制，设备能够提供对非法设备的抑制，维护无线网络的安全。

注意事项

Rogue 设备检测与反制功能需要 AP 工作模式为 hybrid 或者 monitor 才生效。

配置方法

↘ 配置 Rogue 设备反制功能

- 可选配置，使用 **countermeasures enable** 命令在 WIDS 配置模式下配置 Rogue 设备反制功能。

【命令格式】 **countermeasures enable**
【参数说明】 -
【缺省配置】 默认关闭
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 Rogue 设备反制周期

- 可选配置，使用 **countermeasures interval** *time* 命令在 WIDS 配置模式下配置 Rogue 设备的反制周期。

【命令格式】 **countermeasures interval** *time*
【参数说明】 *time*：配置 Rogue 设备反制周期，默认为 1000ms，可配置范围为 100~10000ms
【缺省配置】 默认反制功能的时长为 1000ms
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 Rogue 设备检测、反制规则

- 可选配置，使用 **countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** }命令在 WIDS 配置模式下配置 Rogue 设备的检测、反制规则模式。

【命令格式】 **countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** }
【参数说明】 **adhoc**：配置 adhoc 反制模式，反制对象为 adhoc 检测设备。
config：配置 config 反制模式，反制对象为符合 SSID 黑名单以及静态攻击列表中表项的检测设备。
rogue：配置 rogue 反制模式，反制对象为信号强度大于阈值的检测设备。
ssid：配置 ssid 反制模式，反制对象为不在同一 AC 上的相同 SSID 检测设备。
all：配置 all 反制模式，表示 adhoc、config、rogue 和 ssid 四种模式。
【缺省配置】 Rogue 设备的检测、反制规则为空
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置静态攻击列表

- 可选配置，使用 **device attack mac-address** *H.H.H* 命令在 WIDS 配置模式下配置静态攻击统计列表信息。

【命令格式】 **device attack** { **mac-address** *H.H.H* | **max** *num* }
【参数说明】 **mac-address** *H.H.H*：配置静态攻击列表表项信息，默认为空
max *num*：配置静态攻击列表长度，可配置范围为 1~1024
【缺省配置】 静态攻击列表为空，静态攻击列表长度缺省为 512
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 SSID 黑名单

- 可选配置，使用 **device black-ssid** *ssid* 命令在 WIDS 配置模式下配置 SSID 黑名单列表信息。

【命令格式】 **device { black-ssid** *ssid* | **max-black-ssid** *num* }
【参数说明】 **black-ssid** *ssid*：配置 SSID 黑名单列表表项，默认为空

max-black-ssid *num*：配置 SSID 黑名单列表长度，可配置范围 1~1024

【缺省配置】 SSID 黑名单列表为空，SSID 黑名单列表长度缺省为 512

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置允许 MAC、允许 SSID 和允许产商列表

- 可选配置。
- 使用 **device permit mac-address** *H.H.H* 命令在 WIDS 配置模式下配置允许 MAC 列表表项信息。
- 使用 **device permit ssid** *ssid* 命令在 WIDS 配置模式下配置允许 SSID 列表表项信息。
- 使用 **device permit vendor bssid** *H.H.H* 命令在 WIDS 配置模式下配置允许产商列表表项信息。

【命令格式】 **device permit** { **mac-address** *H.H.H* | **mac-address max** *num* | **ssid** *ssid* | **max-ssid** *num* | **vendor bssid** *H.H.H* | **vendor bssid max** *num* }

【参数说明】 **mac-address** *H.H.H*：配置允许 MAC 列表表项，默认为空

mac-address max *num*：配置允许 MAC 列表长度，默认为 1024，可配置范围 1~2048

ssid *ssid*：配置允许 SSID 列表表项，默认为空

max-ssid *num*：配置允许 SSID 列表长度，默认为 512，可配置范围 1~1024

vendor bssid *H.H.H*：配置允许产商列表表项，默认为空

vendor bssid max *num*：配置允许产商列表长度，默认为 512，可配置范围 1~1024

【缺省配置】 见参数说明

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 Rogue 设备反制数量

- 可选配置，使用 **countermeasures ap-max** *ap-num* 命令在 WIDS 配置模式下配置 Rogue 设备反制数量。

【命令格式】 **countermeasures ap-max** *ap-num*

【参数说明】 *ap-num*：配置每次反制周期反制的设备最大数量，可配置范围 1~256

【缺省配置】 30

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置设备超时时间

- 可选配置，使用 **device aging duration** *time* 命令在 WIDS 配置模式下配置设备超时时间。

【命令格式】 **device aging duration** *time*

【参数说明】 *time*：配置检测设备超时时间，可配置范围 500~5000s

【缺省配置】 1200s

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置设备友好标识

- 可选配置，使用 **device friendly-flags** *value* 命令在 WIDS 配置模式下配置设备友好标识。

【命令格式】 **device friendly-flags** *value*
【参数说明】 *value*：配置设备友好标识，可配置范围 1 ~ 4294967295
【缺省配置】 默认值为 0
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置 Rogue 设备反制信号强度

- 可选配置，使用 **countermeasures rssi-min** *num* 命令在 WIDS 配置模式下配置 Rogue 设备反制信号强度。超过该信号强度的 Rogue 设备将被反制。

【命令格式】 **countermeasures rssi-min** *num*
【参数说明】 *num*：配置 Rogue 设备反制信号强度，可配置范围 0~75(-95~-20)
【缺省配置】 默认反制功能的反制信号强度下限值为 25(-70)
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置基于信道反制

- 可选配置，使用 **countermeasures channel-match** 命令在 WIDS 配置模式下配置基于信道反制功能。基于信道反制可以根据检测的 Rogue 设备所在的信道进行反制。

【命令格式】 **countermeasures channel-match**
【参数说明】 **channel-match**：配置基于信道反制功能
【缺省配置】 默认关闭
【命令模式】 WIDS 配置模式
【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置模糊反制

- 可选配置，使用 **countermeasures fuzzy-enable** 命令在 WIDS 配置模式下配置模糊反制功能。支持对流氓 AP 的 SSID 进行模糊匹配，例如本机的 SSID 为 RUIJIE-WEB,开启模糊反制后能够反制 SSID 名称为 RU1JIE-WEB 的流氓 AP。
- 若无特殊要求，在需要使用模糊反制的 AC 设备上进行配置。

【命令格式】 **countermeasures fuzzy-enable**
【参数说明】
【缺省配置】 默认关闭
【命令模式】 WIDS 配置模式
【使用指导】 反制模式中包含 config 模式时，反制与 SSID 黑名单中（device black-ssid ssidname）名称相似的流氓 AP；反制模式包含 ssid 模式时，反制与本机 SSID 相似的流氓 AP。模糊反制只在 config 和 ssid 两种模式下生效。

配置未知名 STA 检测与反制

- 可选配置。
- 使用 device unknown-sta dynamic-enable 命令在 WIDS 配置模式下配置未知名 STA 检测与反制功能。

- 使 **device unknown-sta mac-address** *H.H.H* 命令在 WIDS 配置模式下配置未知名 STA 列表表项信息。

【命令格式】 **device unknown-sta** { **dynamic-enable** | **mac-address** *H.H.H* | **mac-address max** *num* }

【参数说明】 **dynamic-enable**：配置未知名 STA 检测与反制，默认关闭

mac-address *H.H.H*：配置未知名 STA 列表表项，默认为空

mac-address max *num*：配置未知名 STA 列表长度，可配置范围 1～256

【缺省配置】 默认关闭

【命令模式】 WIDS 配置模式

【使用指导】 AP 工作在 normal 模式时，反制功能无效

配置扫描 AP 检测名单最大个数

- 可选配置，使用 **device detected-ap-max** *num* 命令在 WIDS 配置模式下配置扫描 AP 检测链表最大个数，配置值越小会导致 AP 上检测的数据过少，设备反制功能可能会由于检测数据太少，反制效果不明显，配置值越大，需要占用更多的内存。

【命令格式】 **device detected-ap-max** *num*

【参数说明】 *num*: 表示扫描 AP 检测名单的最大个数，可配置范围 1~4096

【缺省配置】 2048

【命令模式】 WIDS 配置模式

【使用指导】 -

配置指定 radio 扫描状态

- 可选配置，使用 **hybrid-scan radio** *num* **{ disable | enable }**命令在 WIDS 配置模式下配置指定 radio 的扫描状态，如果配置关闭会导致 AP 工作在非 normal 模式时，无设备检测数据。

【命令格式】 **hybrid-scan radio** *num* **{ enable | disable }**

【参数说明】 *num*: 表示指定 radio

【缺省配置】 所有 radio 扫描默认开启

【命令模式】 WIDS 配置模式

【使用指导】 -

配置 AP 的扫描信道

- 可选配置，使用 **scan-channels { 802.11a | 802.11b } channels** *num1 num2…num13* 命令在 WIDS 配置模式下配置扫描信道，如果没有配置扫描信道，结果会导致 AP 工作在非法 normal 时，无设备检测数据。

【命令格式】 **scan-channels { 802.11a | 802.11b } channels** *num1 num2…num13*

【参数说明】 *num*: 表示 AP 的扫描信道

【缺省配置】 扫描信道为空

【命令模式】 WIDS 配置模式

【使用指导】 -

检验方法

- 通过 **show wids detected** 命令查看检测结果

配置举例

无。

常见错误

无。

2.4.5 配置AP工作模式

配置效果

- 根据配置的工作模式，AP 能够提供不同的服务

注意事项

无。

配置方法

↘ 配置 AP 工作模式

- 可选配置。
- 若无特殊要求，应在每台 AP 设备上面配置。

【命令格式】 **device mode** { **hybrid** | **monitor** | **normal** }

【参数说明】 **hybrid**：混合模式，设备提供接入服务和监测服务

monitor：监测模式，设备仅提供监测服务

normal：普通模式，设备仅提供接入服务

【缺省配置】 AP 的工作模式为 normal

【命令模式】 WIDS 配置模式

【使用指导】 -

检验方法

- 通过 **show ap-config running** *ap-name* 命令可以查看该 AP 的当前工作模式

配置举例

无。

常见错误

无。

2.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看攻击列表配置信息	**show wids attack-list**
查看动态和静态黑名单列表配置信息	**show wids blacklist** { **dynamic** | **static** }
查看 SSID 黑名单列表配置信息	**show wids black-ssid**
查看检测到的指定类型设备信息	**show wids detected** { **adhoc** | **all** | **friendly ap** | **interfering ap** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } | **mac-address** *H.H.H* }
查看基于 SSID 的黑白名单列表表项配置信息	**show wids ssid-filter** { **blacklist all** [**in-ssid** *string*] | **ssid all** | **whitelist all** [**in-ssid string**] }
查看允许 MAC、允许 SSID 和允许产商列表表项配置信息	**show wids permitted** { **mac-address** | **ssid** | **vendor** }
查看 IDS 攻击检测信息	**show wids statistics**
查看未知名 STA 列表配置信息	**show wids unknown-sta**
查看用户隔离允许列表表项信息	**show wids user-isolation permit-mac**
查看白名单列表表项信息	**show wids whitelist**
查看 WIDS 其他配置信息	**show running-config**

查看调试信息

无。

3 CPP

3.1 概述

CPP（CPU Protect Policy）是一种 CPU 保护策略。

在网络环境中经常发现一些恶意的攻击，这些攻击通常通过伪造各种大量的管理和协议报文使得设备由于忙于处理这些攻击报文而无暇处理正常管理和协议报文，从而给设备的安全以及网络的稳定带来破坏性的影响。CPP 功能通过报文识别、报文带宽控制实现设备处理器资源保护以及重要报文保障。

下文仅介绍 CPP 的相关内容。

协议规范

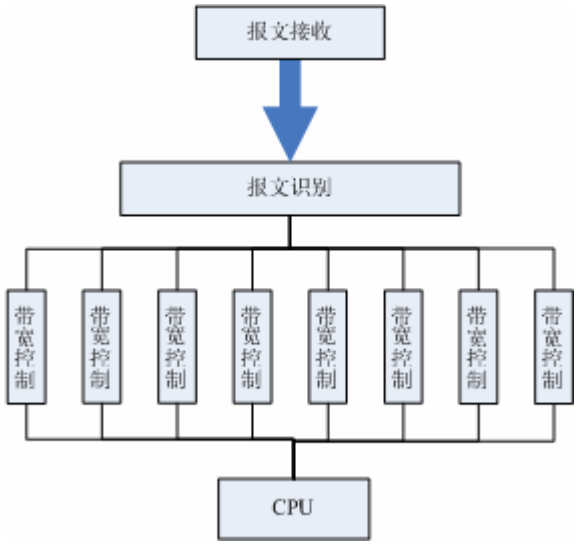
无。

3.2 典型应用

无。

3.3 功能详解

图 3-1 CPP 工作原理



基本概念

报文识别

所有送到 AC/AP 设备进行协议处理的报文首先通过报文识别处理过程将报文进行分类，例如 ARP、BPDU、d1x 等等(各产品的数据分类参照配置详解章节)。

报文带宽控制

管理员可以 配置每种类型报文带宽，通过这种方式可以有效地抑制网络中高速率的攻击报文。

功能特性

功能特性	作用
报文识别	所有送到处理器处理的报文首先通过报文识别过程进行报文分类。
报文带宽控制	通过报文带宽控制可以有效地抑制网络中高速率的攻击报文。

3.3.1 报文识别

所有送到处理器处理的报文首先通过报文识别过程进行报文分类。

工作原理

报文识别

CPP 功能将会对报文进行分类，缺省情况下自动运行报文识别功能。

3.3.2 报文带宽控制

管理员可以配置每种类型报文带宽，通过这种方式可以有效地抑制网络中高速率的攻击报文。

工作原理

报文带宽控制

通过对已经识别分类的报文进行限制，超出带宽限制的报文将被直接丢弃。

3.4 配置详解

配置项	配置建议&相关命令	
配置指定类型报文的带宽限制	⚠ 可选配置，用户设置指定类型报文的带宽限制	
	cpu-protect type	设置指定类型报文的带宽限制

3.4.1 配置指定类型报文的带宽限制

配置效果

- 设置各种类型的带宽。

注意事项

无。

配置方法

↘ 配置指定类型报文的带宽

- 可选配置。
- 若无特殊需求，在每台 AP 设备上都启动 CPP 功能。
- 用户可以根据实际情况调整各种类型报文的默认带宽。

【命令格式】 **cpu-protect type** { **arp** | **bpdu** | **capwap-disc** | **d1x** | **dhcp-option82** | **dhcp-relay-client** | **dhcp-realy-server** | **dhcps** | **igmp** | **ipmc** | **ipv6-nans** | **isis** | **lldp** | **ospf** | **ospfv3** | **pim** | **pppoe** | **rip** | **ripng** | **tcp80** | **tcp443 | vrrp** } **pps** *value*

【参数说明】 **arp**：ARP 协议报文类型。
bpdu：IEEE BPDU 协议报文类型。
capwap-disc：CAPWAP DISCOVER 报文类型。
d1x：802.1x EAPOL 报文类型。
dhcp-option82：DHCP OPTION82 报文类型。
dhcp-relay-client：DHCP RELAY CLIENT 报文类型。
dhcp-relay-server：DHCP RELAY SERVER 报文类型。
dhcps：DHCP SNOOPING 报文类型。
igmp：IGMP 协议报文类型。
ipmc：IPv4 组播协议报文类型。
ipv6-nans：IPv6 邻居发现协议报文类型。
isis：ISIS 协议报文类型。
lldp：LLDP 协议报文类型。
ospf：OSPF 协议报文类型。
ospfv3：OSPF version3 协议报文类型。
pppoe：PPPOE 协议报文类型。
pim：PIM 协议报文类型。
rip：IPv4 RIP 协议报文类型。
ripng：IPv6 RIP 协议报文类型。
tcp80：web 认证重定向报文类型。

tcp443：https 报文类型

vrrp：VRRP 协议报文类型。

pps *value*：每秒报文数上限，可配置范围 0~148810pps。

【缺省配置】 根据不同的产品，提供不同的默认值。

【命令模式】 全局配置模式

【使用指导】 -

检验方法

- 通过命令 **show cpu-protect summary** 查看配置信息

配置举例

无。

常见错误

无。

3.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看各种类型报文的带宽配置信息	**show cpu-protect summary**
查看指定类型报文的统计信息	**show cpu-protect type** { **arp** | **bpdu** | **capwap-disc** | **d1x** | **dhcp-option82** | **dhcp-relay-client** |**dhcp-realy-server** | **dhcps** | **igmp** | **ipmc** | **ipv6-nans** | **isis** | **lldp** | **ospf** | **ospfv3** | **pim** | **pppoe** | **rip** | **ripng** | **tcp80** | **tcp443** | **vrrp** }

查看调试信息

无。

4 NFPP

4.1 概述

网络基础保护策略 (Network Foundation Protection Policy)，简称 NFPP，提供交换机防攻击功能。

在网络环境中经常发现一些恶意的攻击，这些攻击会给交换机带来过重的负担，引起交换机 CPU 利用率过高，导致交换机无法正常运行。这些攻击具体表现在：

拒绝服务攻击可能导致大量消耗交换机内存、表项或者其它资源，使系统无法继续服务。

大量的报文流砸向 CPU，占用了整个送 CPU 的报文的带宽，导致正常的协议流和管理流无法被 CPU 处理, 带来协议震荡或者无法管理，从而导致数据面的转发受影响，并引起整个网络无法正常运行。

大量的报文砸向 CPU 会消耗大量的 CPU 资源，使 CPU 一直处于高负载状态，从而影响管理员对设备进行管理或者设备自身无法运行。

NFPP 可以有效地防止系统受这些攻击的影响。在受攻击情况下，保护系统各种服务的正常运行，以及保持较低的 CPU 负载，从而保障了整个网络的稳定运行。

4.2 典型应用

典型应用	场景描述
攻击检测限速	网络中存在各种的恶意攻击，如 ARP 攻击，IP 扫描攻击等。导致正常的协议流和管理流无法被 CPU 处理, 带来协议震荡或者无法管理。采用 NFPP 的攻击检测限速功能，可限速或隔离攻击流，使网络恢复正常。
集中限速分发	正常业务流量太大，这时给流分处理优先级。当大量的报文砸向CPU，使CPU一直处于高负载状态，出现管理员无法对设备进行管理或者设备自身无法运行的情况。采用集中限速分发功能，提高该部分处理优先级，确保交换机自身稳定运行。

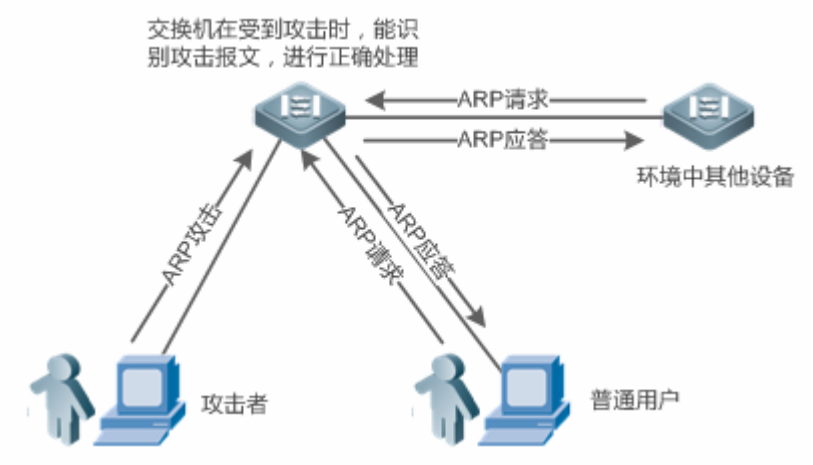
4.2.1 攻击检测限速

应用场景

NFPP 支持对多种报文的攻击检测限速，包括 ARP、ICMP、DHCP 等；同时还支持用户自己定义报文匹配特征，以及对应的攻击检测限速策略。攻击检测限速功能是基于每种报文匹配生效的，这里以 ARP 为例进行应用场景分析。

当存在一个攻击者，进行 ARP 报文攻击，由于 ARP 报文会送 CPU 处理，而 CPU 处理能力有限，因此，该 ARP 会导致 CPU 资源耗费，大量资源用于处理攻击者的ARP报文。若攻击者的ARP报文流量超过了交换机的CPP(CPU Protect Policy，CPU 保护策略)的 ARP 限速带宽，正常的 ARP 报文将出现丢包。针对图中场景，将会导致：普通用户无法上网，交换机与环境中其他设备无法进行正常 ARP 应答。

图 4-1



功能部属

- 在缺省情况下，ARP 攻击检测限速功能打开，且配置了攻击检测限速策略。攻击者的ARP 报文超过限速水线，报文将被丢弃，若超过攻击水线，则另生成监控用户，同时输出提示信息。
- 若攻击者的 ARP 报文流量很大，已超出 CPP 的限速线，影响正常 ARP 应答，用户可开启隔离功能，ACL 丢弃 ARP 攻击报文，网络恢复正常。

针对 CPP 相关配置说明，请参考“CPP”章节。

为了最大限度地利用 NFPP 中抗攻击功能，请根据具体的应用环境修改 CPU Protect Policy 中各种服务的限速值，也可以使用系统提供的推荐配置，这些推荐值可以通过命令 **show cpu-protect summary** 查看。

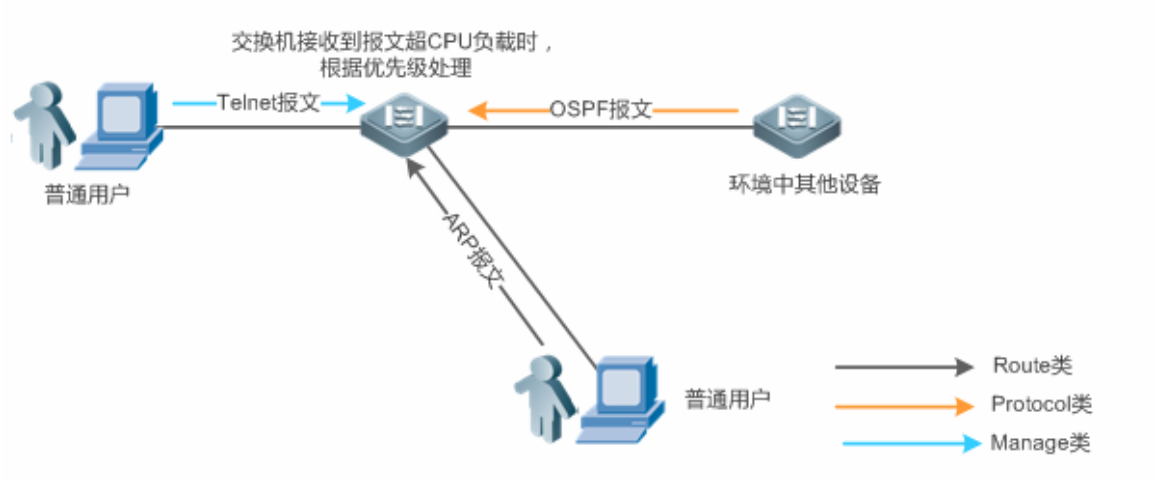
4.2.2 集中限速分发

应用场景

交换机将 CPP 中定义的各种服务按照管理类(Manage)、转发类(Route)和协议类(Protocol)的原则进行的分类，每一类都拥有独立的带宽，不同类别之间的带宽不能共享，超过带宽阈值的流将被丢弃。这样将不同的服务区分类别后，可以保证属于某类的各种服务报文在设备上得到优先处理。

在下图的应用场景中，交换机同时接收到大量的 Telnet 报文、OSPF 报文以及 ARP 报文，由于 CPU 超负载，无法全部处理所有的报文，大量报文积压在队列中，这时将出现用户 Telnet 不时断开、OSPF 协议震荡，用户 ARP 访问异常等情况。

图 4-2



功能部属

- 默认情况下，CPU 集中保护打开，为每种分类分配独立带宽与占宽比。这时 CPU 将优先处理 Telnet 报文，保证用户 Telnet 不断连；其次处理 OSPF 报文，尽量维护 OSPF 协议的稳定；最后处理 ARP 报文。
- 若在缺省配置下仍然出现上述现象，可适当调整分类带宽与占宽比参数。

4.3 功能详解

基本概念

↘ ARP 抗攻击

在局域网中，通过 ARP 协议把 IP 地址转换为 MAC 地址，ARP 协议对网络安全具有重要的意义。通过网络向网关发送大量非法的 ARP 报文，造成网关不能为正常主机提供服务，这就是基于 ARP 的拒绝服务攻击。对于这种攻击，防范措施是一方面对 ARP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

↘ IP 防扫描

众所周知，许多黑客攻击、网络病毒入侵都是从扫描网络内活动的主机开始的。因此大量的扫描报文急剧占用了网络带宽，导致网络通讯无法正常进行。

为此，交换机三层设备提供了防 IP 攻击的功能，用以防止黑客扫描和类似“冲击波”病毒的攻击，还能减少三层设备的 CPU 负担。目前发现的 IP 攻击主要有两种：

- 目的 IP 地址变化的扫描。这种扫描是最危害网络的，不但消耗网络带宽，增加设备的负担，而且更是大部分黑客攻击手段的前奏。
- 向不存在目的 IP 地址高速发送 IP 报文。这种攻击主要是针对设备 CPU 的负担来设计。对三层设备来说，如果目的 IP 地址存在，则报文会被交换芯片直接转发，不会占用设备 CPU 的资源，而如果目的 IP 地址不存在，IP 报文会送到 CPU，

由 CPU 发送 ARP 请求询问目的 IP 地址对应的 MAC 地址，如果送到 CPU 的报文太多，会消耗 CPU 资源。当然，这种攻击的危害比第一种小得多了。

对于“向不存在的目的 IP 地址高速发 IP 报文”这种 IP 攻击，防范措施是一方面对 IP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

↘ ICMP 抗攻击

ICMP 协议作为诊断网络故障的常用手段，它的基本原理是主机发出 ICMP 回应请求报文（ICMP echo request），路由器或者交换机接收到这个请求报文后会回应一个 ICMP 回音应答（ICMP echo reply）报文。在上述这个处理过程中需要设备的 CPU 进行处理，这样就必然需要消耗 CPU 的一部分资源。如果攻击者向目标设备发送大量的 ICMP 回音请求，这样势必会导致设备的 CPU 资源被大量消耗，严重的情况可能导致设备无法正常工作，这种攻击方式也被人们命名为“ICMP 洪水”。对于这种攻击，防范措施是一方面对 ICMP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

↘ DHCP 抗攻击

DHCP 协议被广泛地应用在局域网环境里来动态分配 IP 地址。DHCP 协议对网络安全起着非常重要的意义。目前，存在的最广泛的 DHCP 攻击就是称为“DHCP 耗竭”的攻击，这种攻击通过伪造的 MAC 地址来广播 DHCP 请求的方式进行。目前网络上存在多种这样的攻击工具都可以很容易地实现上述攻击。如果发出的 DHCP 请求足够多的话，网络攻击者就可以在一段时间内耗竭 DHCP 服务器所提供的地址空间，这样当一台合法的主机请求一个 DHCP IP 地址的时候无法成功，从而无法访问网络。对于这种攻击，防范措施是一方面对 DHCP 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

↘ DHCPv6 抗攻击

DHCPv6 协议被广泛地应用在局域网环境里来动态分配 IPv6 地址。和 DHCPv4 协议一样，DHCPv6 协议存在安全问题，对 DHCPv4 协议的攻击方法同样适用于 DHCPv6 协议。网络攻击者可以发出大量 DHCPv6 请求，在一段时间内耗竭 DHCPv6 服务器所提供的地址空间，这样当一台合法的主机请求一个 IPv6 地址的时候无法成功，从而无法访问网络。对于这种攻击，防范措施是一方面对 DHCPv6 报文限速，另一方面检测出攻击源，对攻击源头采取隔离措施。

↘ ND 抗攻击

ND 的全称是 Neighbor Discovery，翻译成汉语是“邻居发现”，在 IPv6 网络中主要负责地址解析、路由器发现、前缀发现和重定向。邻居发现使用 5 类报文：邻居请求、邻居公告、路由器请求、路由器公告和重定向报文，英语名称分别为 Neighbor Solicitation、Neighbor Advertisement、Router Solicitation、Router Advertisement 和 Redirect，前四类报文的英语缩写分别为 NS、NA、RS 和 RA。下文把邻居发现使用的 5 类报文统称为 ND 报文。

ND snooping 通过监听网络中的 ND 报文，过滤非法的 ND 报文，监听网络中的 IPv6 用户，并将监听到的 IPv6 用户绑定到端口，防止 IPv6 地址盗用。ND snooping 要求把 ND 报文送 CPU，如果 ND 报文的速率很高，会造成对 CPU 的攻击，所以需要实现 ND guard，对 ND 报文进行限速。

功能特性

功能特性	作用
主机限速和识别攻击	根据主机限速水线进行限速，并识别网络中的主机用户攻击。
端口限速和识别攻击	根据端口限速水线进行限速，并识别端口攻击。
设置监控时间	在指定时间内，对主机用户攻击者进行软件监控。

设置隔离时间	在指定时间内，对主机用户攻击者或攻击端口进行隔离。
设置信任用户	对某主机用户不进行监控，即对该主机表示信任。
集中限速分发	将报文分类，区分处理优先级。

4.3.1 主机限速和识别攻击

对主机用户攻击报文进行限速，识别主机用户攻击。

识别 ARP 扫描。

识别 IP 扫描。

工作原理

识别主机有源 IP/VLAN ID/端口和链路层源 MAC/VLAN ID/端口两种识别方法。每台主机都有限速水线和攻击阈值（也称为告警水线），限速水线必须低于攻击阈值。当单台主机的攻击报文速度超过限速水线时，将丢弃这些超出限速水线的报文；如果单台主机的攻击报文速度超过攻击阈值，将识别主机用户攻击，记录到日志中，发送 TRAP。

如果在配置时间内收到超过扫描水线的 ARP 报文，链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化，就认为有 ARP 扫描嫌疑。

如果在配置时间内收到超过扫描水线的 IP 报文，源 IP 不变，目的 IP 一直在变化，就认为有 IP 扫描嫌疑。

NFPP 在检测到某种服务的某个具体报文的攻击后，可以向管理员发出告警信息，但是为了防止告警信息频繁出现，如果攻击流持续存在，NFPP 在发出告警后的连续 60 秒时间内不再重复告警。

防止频繁打印日志消耗 CPU 资源，NFPP 把攻击检测的日志信息写到缓冲区，然后以指定速率从缓冲区取出来打印。NFPP 对 TRAP 没有限速。

当前仅 ARP 抗攻击与 IP 防扫描支持防扫描功能。

4.3.2 端口限速和识别攻击

对端口攻击报文进行限速，识别端口攻击。

工作原理

每个端口都有限速水线和攻击阈值，限速水线必须低于攻击阈值。当某个端口的报文速度超过限速水线时，就丢弃报文。如果某个端口的报文速度超过攻击阈值，将记录到日志中，发送 TRAP。

4.3.3 设置监控时间

设置攻击用户的监控时间。

工作原理

监控用户提供当前系统中存在哪些攻击者的信息。如果隔离时间为 0（即不隔离），防攻击模块将自动根据配置的监控时间对攻击者进行软件监控。在监控时间内,用户可以查看到被监控的用户表项.在监控时间老化前,如果又收到该用户的攻击,则重新刷新用户的监控时间,否则监控时间老化为 0 时,该监控用户表项删除.当把隔离时间配置成非零值后，防攻击模块将自动对软件监控的主机采取隔离。

4.3.4 设置隔离时间

设置攻击用户的隔离时间。

工作原理

隔离动作是在检测到攻击后交由抗攻击策略执行的。隔离利用软件 ACL 的过滤功能实现，这样保证该攻击报文不会再被送到 CPU 处理，从而保证了设备正常运行。

隔离功能支持基于主机用户的隔离以及基于端口的隔离。对攻击者进行隔离，会设置一条策略到 ACL 中。但当 ACL 资源耗尽，隔离失败的时候，会打印日志提醒管理员。

4.3.5 设置信任用户

设置不监控的可信主机。

工作原理

如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的指定类型报文将被允许发往 CPU。

4.3.6 集中限速分发

设置管理、转发、协议等三大类报文的限速阈值和百分比。

工作原理

将 CPP 中定义的各种服务按照管理类(Manage) 、转发类(Route)和协议类(Protocol)的原则进行的分类（具体分类如下表所列），每一类都拥有独立的带宽，不同类别之间的带宽不能共享，超过带宽阈值的流将被丢弃。这样将不同的服务区分类别后，可以保证属于某类的各种服务报文在设备上得到优先处理。

NFPP 允许管理员根据实际的网络环境灵活分配三类报文的带宽，从而保障 protocol 类和 manage 类能得到优先处理，protocol 类的优先处理保证了协议的正确运行，而 manage 类的优先处理保证了管理员能够实施正常管理，从而保障了设备的各种重要功能的正常运行，提高设备的抗攻击能力。

经过以上的分类限速后，再将所有的分类流集中一个队列中，这样当某一类服务处理效率较低时，队列上就会堆积该服务对应的报文，并可能最终耗尽该队列资源，NFPP 允许管理员配置该队列中三类所占百分比，当某一类占用的队列长度超过总队列长度和该类所占百分比的乘积时，报文就会被丢弃。这样就有效地解决了某一类独占队列资源的问题。

三种属性分类	CPU Protect Policy 中定义服务类型
Protocol	tp-guard，dot1x，rldp，rerp，slow-packet，bpdu，isis dhcps，gvrp，ripng，dvmrp，igmp，mpls，ospf，pim，pimv6，rip，vrrp，ospf3，dhcp-relay-s，dhcp-relay-c，option82，tunnel-bpdu，tunnel-gvrp
Route	unknown-ipmc，unknown-ipmcv6，ttl1，ttl0，udp-helper，ip4-packet-other，ip6-packet-other，non-ip-packet-other
Manage	ip4-packet-local，ip6-packet-local，arp

服务类型具体含义参见 CPP 配置指南

4.4 配置详解

配置项	配置建议 & 相关命令	
配置ARP抗攻击	必须配置。用于设置全局 ARP 抗攻击功能。	
	arp-guard enable	配置全局攻击检测使能
	arp-guard monitor-period	配置监控时间
	arp-guard monitored-host-limit	配置监控主机最大数目
	arp-guard rate-limit	配置全局限速水线
	arp-guard attack-threshold	配置全局攻击水线
	arp-guard scan-threshold	配置全局主机扫描水线
	可选配置。用于设置 ARP 隔离和端口 ARP 抗攻击功能。	
	arp-guard isolate-period	配置全局隔离时间
	arp-guard trusted-host	配置信任用户
	nfpp arp-guard enable	配置端口攻击检测使能
	nfpp arp-guard policy	配置端口限速水线、攻击水线
	nfpp arp-guard scan-threshold	配置端口逐级扫描水线
	nfpp arp-guard isolate-period	配置端口隔离时间
配置IP防扫描	必须配置。用于设置全局 IP 防扫描功能。	
	ip-guard enable	配置全局攻击检测使能
	ip-guard monitor-period	配置监控时间
	ip-guard monitored-host-limit	配置监控主机最大数目
	ip-guard rate-limit	配置全局限速水线

	ip-guard attack-threshold	配置全局攻击水线
	ip-guard scan-threshold	配置全局主机扫描水线
	可选配置。用于设置 IP 信任用户、IP 隔离和端口 IP 防扫描功能。	
	ip-guard isolate-period	配置全局隔离时间
	ip-guard trusted-host	配置信任用户
	nfpp ip-guard enable	配置端口攻击检测使能
	nfpp ip-guard policy	配置端口限速水线、攻击水线
	nfpp ip-guard scan-threshold	配置端口逐级扫描水线
	nfpp ip-guard isolate-period	配置端口隔离时间
配置ICMP抗攻击	必须配置。用于设置全局 ICMP 抗攻击功能。	
	icmp-guard enable	配置全局攻击检测使能
	icmp-guard monitor-period	配置监控时间
	icmp-guard monitored-host-limit	配置监控主机最大数目
	icmp-guard rate-limit	配置全局限速水线
	icmp-guard attack-threshold	配置全局攻击水线
	可选配置。用于设置 ICMP 信任用户、ICMP 隔离和端口 ICMP 抗攻击功能。	
	icmp-guard isolate-period	配置全局隔离时间
	icmp-guard trusted-host	配置信任用户
	nfpp icmp-guard enable	配置端口攻击检测使能
	nfpp icmp-guard policy	配置端口限速水线、攻击水线
	nfpp icmp-guard isolate-period	配置端口隔离时间
配置DHCP抗攻击	必须配置。用于设置全局 DHCP 抗攻击功能。	
	dhcp-guard enable	配置全局攻击检测使能
	dhcp-guard monitor-period	配置监控时间
	dhcp-guard monitored-host-limit	配置监控主机最大数目
	dhcp-guard rate-limit	配置全局限速水线
	dhcp-guard attack-threshold	配置全局攻击水线
	可选配置。用于设置 DHCP 隔离和端口 DHCP 抗攻击功能。	
	dhcp-guard isolate-period	配置全局隔离时间
	dhcp-guard trusted-host	配置信任用户
	nfpp dhcp-guard enable	配置端口攻击检测使能
	nfpp dhcp-guard policy	配置端口限速水线、攻击水线
	nfpp dhcp-guard isolate-period	配置端口隔离时间
配置DHCPv6 抗攻击	必须配置。用于设置全局 DHCPv6 抗攻击功能。	
	dhcpv6-guard enable	配置全局攻击检测使能
	dhcpv6-guard monitor-period	配置监控时间

	dhcpv6-guard monitored-host-limit	配置监控主机最大数目
	dhcpv6-guard rate-limit	配置全局限速水线
	dhcpv6-guard attack-threshold	配置全局攻击水线
	可选配置。用于设置 DHCPv6 隔离和端口 DHCPv6 抗攻击功能。	
	dhcpv6-guard isolate-period	配置全局隔离时间
	dhcpv6-guard trusted-host	配置信任用户
	nfpp dhcpv6-guard enable	配置端口攻击检测使能
	nfpp dhcpv6-guard policy	配置端口限速水线、攻击水线
	nfpp dhcpv6-guard isolate-period	配置端口隔离时间
配置ND抗攻击	必须配置。用于设置全局 ND 抗攻击功能。	
	nd-guard enable	配置全局攻击检测使能
	nd-guard rate-limit	配置全局限速水线
	nd-guard attack-threshold	配置全局攻击水线
	可选配置。用于设置端口 ND 抗攻击功能。	
	nd-guard trusted-host	配置信任用户
	nfpp nd-guard enable	配置端口攻击检测使能
	nfpp nd-guard policy	配置端口限速水线、攻击水线
配置集中限速分发	必须配置。设置管理、转发、协议等三大类报文的限速阈值和百分比。	
	cpu-protect sub-interface pps	配置每类报文允许的最大带宽
	cpu-protect sub-interface percent	配置每类报文占用队列的最大百分比
NFPP日记信息	必须配置。用于设置日志信息。	
	log-buffer entries	配置 NFPP 日志缓冲区大小
	log-buffer logs	配置从专用日志缓冲区取日志生成系统消息的速率
	可选配置。用于设置记录哪些日志。	
	logging vlan	指定需要记录哪些 VLAN 的日志
	logging interface	指定需要记录哪个端口的日志

4.4.1 配置ARP抗攻击

配置效果

- ARP 攻击识别分为基于主机和基于物理端口两个类别。基于主机又细分为基于源 IP 地址/VLAN ID/物理端口和基于链路层源 MAC 地址/ VLAN ID /物理端口。每种攻击识别都有限速水线和告警水线。当 ARP 报文速率超过限速水线时，超限

报文将被丢弃。当 ARP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

- ARP 抗攻击还能检测出 ARP 扫描。ARP 扫描是指链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化。由于存在误判的可能，对检测出有 ARP 扫描嫌疑的主机不进行隔离，只是提供给管理员参考。

注意事项

- 对于在全局与接口上同时存在配置的命令，接口优先级高于全局。
- 隔离默认关闭，若打开隔离功能，攻击用户将占用安全模块表项。
- ARP 抗攻击只是针对攻击交换机本身的 ARP 拒绝服务攻击，而不是针对 ARP 欺骗或者是解决网络中的 ARP 攻击问题。

配置方法

使能攻击检测

- 必须配置。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当关闭 ARP 抗攻击功能时，系统将自动清除受监控的主机、扫描主机和端口隔离表项。

【命令格式】 **arp-guard enable**
【参数说明】 -
【缺省配置】 默认 ARP 抗攻击功能打开
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp arp-guard enable**
【参数说明】 -
【缺省配置】 端口没有配置 ARP 抗攻击开关，采用全局开关
【命令模式】 接口模式下
【使用指导】 端口的 ARP 抗攻击开关优先于全局 ARP 抗攻击开关。

配置隔离时间

- 可选配置，默认关闭隔离功能。
- 在攻击用户报文流量超过限速带宽时，可配置隔离时间，将报文直接丢弃，避免占用带宽资源。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【命令格式】 **arp-guard isolate-period** [*seconds* | **permanent**]
【参数说明】 *seconds*：隔离时间，单位是秒，取值范围是 0 或者[30, 86400]。

permanent：永久隔离。

【缺省配置】 全局隔离时间的缺省值是 0，即不隔离

【命令模式】 nfpp 模式下

【使用指导】 -

【命令格式】 **nfpp arp-guard isolate-period** [*seconds* | **permanent**]

【参数说明】 *seconds*：隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。

permanent：永久隔离。

【缺省配置】 缺省情况是没有配置局部隔离时间，采用全局隔离时间

【命令模式】 接口模式下

【使用指导】 -

配置监控时间

- 必须配置。
- 在配置了隔离时间时，攻击用户监控时间直接采用隔离时间，配置的监控时间不生效。
- 支持在 AP 设备上进行全局配置。

【命令格式】 **arp-guard monitor-period** *seconds*

【参数说明】 *seconds*： 监控时间，单位是秒，取值范围是[180, 86400]。

【缺省配置】 监控时间的缺省值是 600 秒

【命令模式】 nfpp 模式下

【使用指导】 -

配置监控主机最大数目

- 必须配置。
- 配置监控主机最大数目，随实际监控主机数增加，处理监控用户需占用更多 CPU 资源。
- 支持在 AP 设备上进行全局配置
- 如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR：The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。
- 当受监控主机表满时，打印日志“% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

【命令格式】 **arp-guard monitored-host-limit** *number*

【参数说明】 *number*：支持的最大受监控主机数，取值范围为 1 到 4294967295。

【缺省配置】 最大受监控主机数默认 1000 个

【命令模式】 nfpp 模式下

【使用指导】 -

配置攻击检测水线

- 必须配置。
- 为了使 ARP 抗攻击得到最佳的防攻击效果，建议管理员配置基于主机的限速水线和告警水线时遵循以下原则：基于 IP 地址的限速水线 < 基于 IP 地址的告警水线 < 基于源 MAC 地址的限速水线 < 基于源 MAC 地址的告警水线。。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当管理员配置的限速水线大于攻击阈值时，打印命令提示信息“%ERROR：rate limit is higher than attack threshold 500pps(配置的攻击阈值).”提醒管理员。
- 当管理员配置的攻击阈值小于限速水线时，打印命令提示信息“%ERROR：attack threshold is smaller than rate limit 300pps(配置的限速水线).”提醒管理员。
- 当无法为检测到的攻击者分配内存时，打印日志“%NFPP_ARP_GUARD-4-NO_MEMORY: Failed to alloc memory..”提醒管理员。
- 基于 MAC 地址限速的优先级高于基于 IP 地址限速，而基于 IP 地址限速又高于基于端口限速。
- 在 nfpp 模式下：使用 **arp-guard rate-limit** { **per-src-ip** | **per-src-mac**} *pps* 命令可以配置 IP/VID/端口识别主机与基于链路层源 MAC/VID/端口识别主机的限速水线。
- 在 nfpp 模式下：使用 **arp-guard attack-threshold** { **per-src-ip** | **per-src-mac** } *pps* 命令可以配置 IP/VID/端口识别主机与基于链路层源 MAC/VID/端口识别主机的攻击水线。
- 在接口模式下：使用 **nfpp arp-guard policy** { **per-src-ip | per-src-mac** } *rate-limit-pps attack-threshold-pps* 命令可以配置该端口上 IP/VID/端口识别主机与基于链路层源 MAC/VID/端口识别主机的限速水线和攻击水线。

【命令格式】 **arp-guard rate-limit** { **per-src-ip** | **per-src-mac** | **per-port** } *pps*

【参数说明】 **per-src-ip：**对每个源 IP 地址进行限速。

per-src-mac：对每个源 MAC 地址进行限速。

per-port：对每个端口进行限速。

pps：限速水线值，取值范围是[1,9999]。

【缺省配置】 根据不同的产品，提供不同的默认值。

【命令模式】 nfpp 模式下

【使用指导】 -

【命令格式】 **arp-guard attack-threshold** { **per-src-ip** | **per-src-mac | per-port** } *pps*

【参数说明】 **per-src-ip：**配置每个源 IP 地址的攻击水线

per-src-mac：配置每个源 MAC 地址的攻击水线

per-port：配置每个端口的攻击水线

pps：攻击水线，单位是每秒报文数，取值范围是[1,9999]

【缺省配置】 根据不同的产品，提供不同的默认值。

【命令模式】 nfpp 模式下

【使用指导】 攻击水线不能小于限速水线。

【命令格式】 **nfpp arp-guard policy** { **per-src-ip | per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps*

【参数说明】 **per-src-ip：**配置每个源 IP 地址的限速水线和攻击水线。
per-src-mac：配置每个源 MAC 地址的限速水线和攻击水线。
per-port：配置每个端口的限速水线和攻击水线。
rate-limit-pps： 限速水线，取值范围是 1 到 9999。
attack-threshold-pps：攻击水线，取值范围是 1 到 9999。
【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线
【命令模式】 接口模式下
【使用指导】 攻击水线不能小于限速水线。

配置扫描检测水线

- 必须配置。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- ARP 扫描表只记录最新的 256 条记录。当 ARP 扫描表满了以后，最新记录将覆盖最旧记录。
- 如果 10 秒钟收到的 ARP 报文，链路层源 MAC 地址固定而源 IP 地址变化，或者链路层源 MAC 地址和源 IP 地址固定而目标 IP 地址不断变化，变化次数超过扫描水线，就认为有扫描嫌疑。

【命令格式】 **arp-guard scan-threshold** *pkt-cnt*
【参数说明】 *pkt-cnt*：扫描水线值，取值范围是[1,9999]。
【缺省配置】 缺省扫描水线是 100，时间单位是 10 秒
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp arp-guard scan-threshold** *pkt-cnt*
【参数说明】 *pkt-cnt*：扫描水线值，取值范围是[1,9999]。
【缺省配置】 没配置基于端口的 ARP 扫描阈值，采用全局 ARP 扫描阈值
【命令模式】 接口模式下
【使用指导】 -

配置信任用户

- 可选配置，默认无不监控可信主机。
- ARP 防攻击仅支持配置不进行监控 IP + MAC 方式，最多可配置 500 条。
- 支持在 AP 设备上进行全局配置。
- 当受监控主机表中存在与可信主机相匹配的表项（IP 地址和 MAC 地址相同）时，系统将自动删除此 IP 地址和 MAC 地址对应的表项。
- 当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。
- 当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 1.1.1.1 0000.0000.1111 (配置的可信主机）.”提醒管理员。

- 当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 1.1.1.1 0000.0000.1111（配置的可信主机）.”提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 1.1.1.1 0000.0000.1111（配置的可信主机）has already been configured.”提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 1.1.1.1 0000.0000.1111（配置的可信主机）is not found.”提醒管理员。

【命令格式】 **arp-guard trusted-host** *ip mac*

【参数说明】 *ip*：IP 地址。

mac：MAC 地址。

【缺省配置】 没有设置任何可信主机

【命令模式】 nfpp 模式下

【使用指导】 如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 ARP 报文将被允许发往 CPU，不做任何的限速和告警处理。

检验方法

网络主机往配置了 ARP 攻击检测限速的交换机发送 ARP 攻击报文，需确认该报文可送 CPU。

- 对于不满足信任用户配置的报文，若超过攻击水线或扫描水线，将有攻击信息提示。
- 若攻击报文满足信任用户配置，将无提示信息。

配置举例

通过 ARP 抗攻击保护 CPU

【网络环境】
- 系统中带有 ARP 主机用户攻击，导致部分用户无法正常建立 ARP 连接。
- 系统中存在 ARP 扫描，导致 CPU 利用率很高。
- 系统中，部分主机报文 ARP 报文流量很大，需放行。

【配置方法】
- 配置基于主机的攻击检测水线为 5pps。
- 配置 ARP 扫描检测水线为 10pps。
- 配置隔离时间为 180pps。
- 配置信任用户

```
Ruijie# configure terminal
Ruijie(config)# nfpp
Ruijie (config-nfpp)#arp-guard rate-limit per-src-mac 5
Ruijie (config-nfpp)#arp-guard attack-threshold per-src-mac 10
Ruijie (config-nfpp)#arp-guard isolate-period 180
Ruijie (config-nfpp)#arp-guard trusted-host 1.1.1.1 0000.0000.1111
```

【检验方法】

- 通过 **show nfpp arp-guard summary** 可以查看到配置信息。

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit      Attack-threshold Scan-threshold
Global    Disable 180            4/5/100         8/10/200         15

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

- 通过 **show nfpp arp-guard hosts** 可以查看到监控用户。

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address        MAC address     remain-time(s)
 ----    ---------   ----------        -----------     --------------
 1       Gi0/43      5.5.5.16          -               175
Total: 1 host
```

- 通过 **show nfpp arp-guard scan** 可以查看到扫描用户。

```
VLAN  interface       IP address        MAC address     timestamp
----  ---------       ----------        -----------     ---------
1     Gi0/5           -                 001a.a9c2.4609  2013-4-30 23:50:32
1     Gi0/5           192.168.206.2     001a.a9c2.4609  2013-4-30 23:50:33
1     Gi0/5           -                 001a.a9c2.4609  2013-4-30 23:51:33
1     Gi0/5           192.168.206.2     001a.a9c2.4609  2013-4-30 23:51:34
Total: 4 record(s)
```

- 通过 **show nfpp arp-guard trusted-host** 可以查看不监控信任主机信息。

```
IP address      mac
----------      ----
1.1.1.1         0000.0000.1111
Total: 1 record(s)
```

常见错误

无。

4.4.2 配置IP防扫描

配置效果

- IP 攻击识别分为基于主机和基于物理端口两个类别。基于主机是采用源 IP 地址/VLAN ID/物理端口三者结合识别的。每种攻击识别都有限速水线和告警水线。当 IP 报文速率超过限速水线时，超限报文将被丢弃。当 IP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。
- IP 抗攻击还能检测出 IP 扫描。，IP 防扫描针对的是目的 IP 一直发生变化，源 IP 不变，且目的 IP 地址不是本机 IP 地址的 IP 报文攻击。

- IP 防扫描针对的是目的 IP 地址不是本机 IP 地址的 IP 报文攻击。对于目的 IP 地址是本机 IP 地址的 IP 报文，则由 CPP（CPU Protect Policy）限速。

注意事项

- 对于在全局与接口上同时存在配置的命令，接口优先级高于全局。
- 隔离默认关闭，若打开隔离功能，攻击用户将占用安全模块表项。

配置方法

使能攻击检测

- 必须配置，默认打开。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当关闭 IP 防扫描功能时，系统将自动清除受监控的主机。

【命令格式】 **ip-guard enable**
【参数说明】 -
【缺省配置】 默认 IP 防扫描功能打开
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp ip-guard enable**
【参数说明】 -
【缺省配置】 端口没有配置 IP 防扫描开关，采用全局开关
【命令模式】 接口模式下
【使用指导】 端口的 IP 防扫描开关优先于全局防扫描开关。

配置隔离时间

- 可选配置，默认关闭隔离功能，。
- 在攻击用户报文流量超过 CPP 限速带宽时，可配置隔离时间，将报文直接丢弃，避免占用带宽资源。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【命令格式】 **ip-guard isolate-period** [*seconds* | **permanent**]
【参数说明】 *seconds*：隔离时间，单位是秒，取值范围是 0 或者[30, 86400]。
permanent：永久隔离。
【缺省配置】 全局隔离时间的缺省值是 0，即不隔离
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp ip-guard isolate-period** [*seconds* | **permanent**]
【参数说明】 *seconds*：隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
permanent：永久隔离。
【缺省配置】 缺省情况是没有配置局部隔离时间，采用全局隔离时间
【命令模式】 接口模式下
【使用指导】 -

配置配置监控时间

- 必须配置。
- 在配置了隔离时间时，攻击用户监控时间直接采用隔离时间，配置的监控时间不生效。
- 支持在 AP 设备上进行全局配置。

【命令格式】 **ip-guard monitor-period** *seconds*
【参数说明】 *seconds*：监控时间，单位是秒，取值范围是[180, 86400]。
【缺省配置】 600 秒
【命令模式】 nfpp 模式下
【使用指导】 如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

配置监控主机最大数目

- 必须配置。
- 提高监控主机最大数目，随实际监控主机数增加，处理监控用户需占用更多 CPU 资源。
- 支持在 AP 设备上进行全局配置
- 如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR： The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。
- 当受监控主机表满时，打印日志“% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.” 提醒管理员。

【命令格式】 **ip-guard monitored-host-limit** *number*
【参数说明】 *number*：支持的最大受监控主机数，取值范围为 1 到 4294967295。
【缺省配置】 1000 个
【命令模式】 nfpp 模式下
【使用指导】 -

配置攻击检测水线

- 必须配置。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。

- 当管理员配置的限速水线大于攻击阈值时，打印命令提示信息“%ERROR：rate limit is higher than attack threshold 500pps(配置的攻击阈值).”提醒管理员。
- 当管理员配置的攻击阈值小于限速水线时，打印命令提示信息“%ERROR：attack threshold is smaller than rate limit 300pps(配置的限速水线).”提醒管理员。
- 当无法为检测到的攻击者分配内存时，打印日志“%NFPP_IP_GUARD-4-NO_MEMORY: Failed to alloc memory.”提醒管理员。
- 基于源 IP 地址限速优先级高于基于端口限速。
- 在 nfpp 模式下：通过命令 **ip-guard rate-limit** { **per-src-ip** | **per-port** } *pps* 配置全局限速水线。
- 在 nfpp 模式下：通过命令 **ip-guard attack-threshold** { **per-src-ip** | **per-port** } *pps* 配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。
- 在接口模式下：通过命令 **nfpp ip-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps* 在端口上配置局部的限速水线和攻击水线。

【命令格式】 **ip-guard rate-limit** { **per-src-ip** | **per-port** } *pps*
【参数说明】 **per-src-ip：**对每个源 IP 地址进行限速。
per-port：对每个端口进行限速。
pps： 限速水线值，取值范围是[1,9999]。
【缺省配置】 见产品特性文档
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **ip-guard attack-threshold** { **per-src-ip** | **per-port** } *pps*
【参数说明】 **per-src-ip：**配置每个源 IP 地址的攻击水线。
per-port：配置每个端口的攻击水线。
pps：攻击水线，单位是每秒报文数，取值范围是[1,9999]。
【缺省配置】 见产品特性文档
【命令模式】 nfpp 模式下
【使用指导】 攻击水线不能小于限速水线。

【命令格式】 **nfpp ip-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps*
【参数说明】 **per-src-ip：**配置每个源 IP 地址的攻击水线。
per-port：配置每个端口的攻击水线。
rate-limit-pps：限速水线，取值范围是 1 到 9999。
attack-threshold-pps：攻击水线，取值范围是 1 到 9999。
【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线
【命令模式】 接口模式下
【使用指导】 攻击水线不能小于限速水线。

配置扫描检测水线

- 必须配置。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 如果 10 秒钟收到的 IP 报文，目的 IP 一直发生变化，源 IP 不变，且目的 IP 地址不是本机 IP 地址的 IP 报文，若变化次数超过扫描水线，就认为有扫描嫌疑。

【命令格式】 **ip-guard scan-threshold** *pkt-cnt*
【参数说明】 *pkt-cnt*：扫描水线值，取值范围是[1,9999]。
【缺省配置】 缺省扫描水线是 10 秒 100 个
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp ip-guard scan-threshold** *pkt-cnt*
【参数说明】 *pkt-cnt*：扫描水线值，取值范围是[1,9999]。
【缺省配置】 没配置基于端口的 IP 扫描水线，采用全局 ARP 扫描水线
【命令模式】 接口模式下
【使用指导】 -

配置信任用户

- 可选配置，默认无不监控可信主机。
- IP 防扫描仅支持配置不进行监控 IP，最多可配置 500 条。
- 支持在 AP 设备上进行全局配置。
- 当受监控主机表中存在与可信主机相匹配的表项（IP 地址相同）时，系统将自动删除此 IP 地址对应的表项。
- 当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。
- 当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。
- 当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）has already been configured.”提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）is not found.”提醒管理员。

【命令格式】 **ip-guard trusted-host** *ip mask*
【参数说明】 *ip*：IP 地址。
mask： IP 地址的掩码。
【缺省配置】 没有设置任何可信主机
【命令模式】 nfpp 模式下
【使用指导】 如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 IP 报文将被允许发往 CPU，不做任何的限速和告警处理。

检验方法

网络主机往配置了 IP 攻击检测限速的交换机发送 IP 攻击报文，需确认该报文可送 CPU。

- 对于不满足信任用户配置的报文，若超过攻击水线或扫描水线，将有攻击信息提示。
- 若攻击报文满足信任用户配置，将无提示信息。

配置举例

↘ 通过 IP 防扫描保护 CPU

【网络环境】
- 系统中带有 IP 主机用户攻击，部分用户报文无法正常路由转发。
- 系统中存在 IP 扫描，导致 CPU 利用率很高。
- 系统中，部分主机报文流量很大，需放行

【配置方法】
- 配置基于主机的攻击检测水线。
- 配置 IP 扫描检测水线。
- 配置隔离时间为非 0。
- 配置信任用户

```
Ruijie# configure terminal
Ruijie(config)# nfpp
Ruijie (config-nfpp)#ip-guard rate-limit per-src-ip 20
Ruijie (config-nfpp)#ip-guard attack-threshold per-src-ip 30
Ruijie (config-nfpp)#ip-guard isolate-period 180
Ruijie (config-nfpp)#ip-guard trusted-host 192.168.201.46 255.255.255.255
```

【检验方法】
- 通过 **show nfpp ip-guard summary** 可以查看到配置信息。

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit      Attack-threshold Scan-threshold
Global    Disable 180            20/-/100        30/-/200         100

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

- 通过 **show nfpp ip-guard hosts** 可以查看到监控用户。

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address        Reason    remain-time(s)
 ----    ---------   ----------        ------    --------------
  1      Gi0/5       192.168.201.47    ATTACK    160
Total: 1 host
```

- 通过 **show nfpp ip-guard trusted-host** 可以查看不监控信任主机信息。

```
IP address          mask
```

```
----------          ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

常见错误

无。

4.4.3 配置ICMP抗攻击

配置效果

- ICMP 攻击识别分为基于主机和基于物理端口两个类别。基于主机方式是采用源 IP 地址/虚拟局域网号/端口三者结合来识别的。每种攻击识别都有限速水线和告警水线。当ICMP报文速率超过限速水线时，将被丢弃。当ICMP报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

注意事项

- 对于在全局与接口上同时存在配置的命令，接口优先级高于全局。
- 隔离默认关闭，若打开隔离功能，攻击用户将占用安全模块表项。

配置方法

↘ 使能攻击检测

- 必须配置，默认打开。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当关闭 ICMP 抗攻击功能时，系统将自动清除受监控的主机。

【命令格式】 **icmp-guard enable**
【参数说明】 -
【缺省配置】 默认 ICMP 防攻击功能打开
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp icmp-guard enable**
【参数说明】 -
【缺省配置】 端口没有配置 ICMP 抗攻击开关，采用全局开关
【命令模式】 接口模式下

【使用指导】 端口的 ICMP 抗攻击开关优先于全局 ICMP 抗攻击开关。

配置隔离时间

- 可选配置，默认关闭隔离功能。
- 在攻击用户报文流量超过 CPP 限速带宽时，可配置隔离时间，将报文直接丢弃，避免占用带宽资源。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【命令格式】 **icmp-guard isolate-period** [*seconds* | **permanent**]

【参数说明】 *seconds*：隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
permanent：永久隔离。

【缺省配置】 全局隔离时间的缺省值是 0，即不隔离

【命令模式】 nfpp 模式下

【使用指导】 对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间(即局部隔离时间)。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

【命令格式】 **nfpp icmp-guard isolate-period** [*seconds* | **permanent**]

【参数说明】 *seconds*： 隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
permanent：永久隔离。

【缺省配置】 缺省情况是没有配置局部隔离时间，采用全局隔离时间

【命令模式】 接口模式下

【使用指导】 -

配置配置监控时间

- 必须配置。
- 在配置了隔离时间时，攻击用户监控时间直接采用隔离时间，配置的监控时间不生效。
- 支持在 AP 设备上进行全局配置。

【命令格式】 **icmp-guard monitor-period** *seconds*

【参数说明】 *seconds*：监控时间，单位是秒，取值范围是[180, 86400]。

【缺省配置】 600 秒

【命令模式】 nfpp 模式下

【使用指导】 检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。
如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

配置监控主机最大数目

- 必须配置。
- 提高监控主机最大数目，随实际监控主机数增加，处理监控用户需占用更多 CPU 资源。

- 支持在 AP 设备上进行全局配置
- 如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR： The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。
- 当受监控主机满时，打印日志“% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000(配置的受监控主机数） monitored hosts.”提醒管理员

【命令格式】 **icmp-guard monitored-host-limit** *number*

【参数说明】 *number*：支持的最大受监控主机数，取值范围为 1 到 4294967295。

【缺省配置】 1000 个

【命令模式】 nfpp 模式下

【使用指导】 如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR：The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机满时，打印日志“% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

配置攻击检测水线

- 必须配置。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当管理员配置的限速水线大于攻击阈值时，打印命令提示信息“%ERROR：rate limit is higher than attack threshold 500pps(配置的攻击阈值).”提醒管理员。
- 当管理员配置的攻击阈值小于限速水线时，打印命令提示信息“%ERROR：attack threshold is smaller than rate limit 300pps(配置的限速水线).”提醒管理员。
- 当无法为检测到的攻击者分配内存时，打印日志“%NFPPP_ ICMP_GUARD -4-NO_MEMORY: Failed to alloc memory.”提醒管理员。
- 基于源 IP 地址限速优先级高于基于端口限速。
- 在 nfpp 模式下：通过命令 **icmp-guard rate-limit** { **per-src-ip** | **per-port** } *pps* 配置全局限速水线。
- 在 nfpp 模式下：通过命令 **icmp-guard attack-threshold** { **per-src-ip** | **per-port** } *pps* 配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。
- 在接口模式下：通过命令 **nfpp icmp-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps* 在端口上配置局部的限速水线和攻击水线。

【命令格式】 **icmp-guard rate-limit** { **per-src-ip** | **per-port** } *pps*

【参数说明】 **per-src-ip：**对每个源 IP 地址进行限速。

per-port：对每个端口进行限速。

pps：限速水线值，取值范围是[1,9999]。

【缺省配置】 见产品特性文档

【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **icmp-guard attack-threshold** { **per-src-ip** | **per-port** } *pps*
【参数说明】 **per-src-ip：**配置每个源 IP 地址的攻击水线。
per-port：配置每个端口的攻击水线。
pps：攻击水线，单位是每秒报文数，取值范围是[1,9999]。
【缺省配置】 见产品特性文档
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp icmp-guard policy** { **per-src-ip | per-port** } *rate-limit-pps attack-threshold-pps*
【参数说明】 **per-src-ip：**配置每个源 IP 地址的限速水线和攻击水线。
per-port：配置每个端口的限速水线和攻击水线。
rate-limit-pps：限速水线，取值范围是 1 到 9999。
attack-threshold-pps：攻击水线，取值范围是 1 到 9999。
【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线
【命令模式】 接口模式下
【使用指导】 攻击水线不能小于限速水线。

配置信任用户

- 可选配置，默认无不监控可信主机。
- ICMP 防扫描仅支持配置不进行监控 IP，最多可配置 500 条。
- 支持在 AP 设备上进行全局配置。
- 当受监控主机表中存在与可信主机相匹配的表项（IP 地址相同）时，系统将自动删除此 IP 地址对应的表项。
- 当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。
- 当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。
- 当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0（配置的可信主机）.”提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）has already been configured.”提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 1.1.1.0 255.255.255.0（配置的可信主机）is not found.”提醒管理员。

【命令格式】 **icmp-guard trusted-host** *ip mask*
【参数说明】 *ip*： IP 地址。
mask：: IP 地址的掩码。

【缺省配置】 没有设置任何可信主机

【命令模式】 nfpp 模式下

【使用指导】 如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 ICMP 报文将被允许发往 CPU，不做任何的限速和告警处理。通过配置掩码可以达到对某一个网段的所有主机都不进行监控。

最多支持设置 500 条可信主机。

检验方法

网络主机往配置了 ICMP 攻击检测限速的交换机发送 ICMP 攻击报文，需确认该报文可送 CPU。

- 对于不满足信任用户配置的报文，若超过攻击水线，将有攻击信息提示。
- 若攻击报文满足信任用户配置，将无提示信息。

配置举例

↘ 通过 ICMP 抗攻击保护 CPU

【网络环境】
- 系统中带有 ICMP 主机用户攻击，部分用户无法 ping 通。
- 系统中，部分主机报文流量很大，需放行

【配置方法】
- 配置基于主机的攻击检测水线。
- 配置隔离时间为非 0。
- 配置信任用户

```
Ruijie# configure terminal
Ruijie(config)# nfpp
Ruijie (config-nfpp)#icmp-guard rate-limit per-src-ip 20
Ruijie (config-nfpp)#icmp-guard attack-threshold per-src-ip 30
Ruijie (config-nfpp)#icmp-guard isolate-period 180
Ruijie (config-nfpp)#icmp-guard trusted-host 192.168.201.46 255.255.255.255
```

【检验方法】
- 通过 **show nfpp icmp-guard summary** 可以查看到配置信息。

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit      Attack-threshold
Global    Disable 180            20/-/400        30/-/400

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

- 通过 **show nfpp icmp-guard hosts** 可以查看到监控用户。

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   IP address        remain-time(s)
 ----    ---------   ----------        --------------
```

```
  1       Gi0/5        192.168.201.47     160
Total: 1 host
```

- 通过 **show nfpp icmp-guard trusted-host** 可以查看不监控信任主机信息。

```
IP address          mask
----------          ----
192.168.201.46      255.255.255.255
Total: 1 record(s)
```

常见错误

无。

4.4.4 配置DHCP抗攻击

配置效果

- DHCP 攻击识别分为基于主机和基于物理端口两个类别。基于主机方式是采用链路层源 MAC 地址/虚拟局域网号/端口三者结合来识别的。每种攻击识别都有限速水线和告警水线。当 DHCP 报文速率超过限速水线时，超限的 DHCP 报文将被丢弃。当 DHCP 报文速率超过告警水线时，将打印警告信息，发送 TRAP，基于主机的攻击识别还会对攻击源头采取隔离措施。

注意事项

- 对于在全局与接口上同时存在配置的命令，接口优先级高于全局。
- 隔离默认关闭，若打开隔离功能，攻击用户将占用安全模块表项。

配置方法

↘ 使能攻击检测

- 必须配置，默认打开。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当关闭 DHCP 抗攻击功能时，系统将自动清除受监控的主机。

【命令格式】 **dhcp-guard enable**
【参数说明】 -
【缺省配置】 默认打开
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp dhcp-guard enable**
【参数说明】 -
【缺省配置】 端口没有配置 DHCP 抗攻击开关，采用全局开关
【命令模式】 接口模式下
【使用指导】 端口的 DHCP 抗攻击开关优先于全局 DHCP 抗攻击开关。

配置隔离时间

- 可选配置，默认关闭隔离功能。
- 在攻击用户报文流量超过 CPP 限速带宽时，可配置隔离时间，将报文直接丢弃，避免占用带宽资源。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【命令格式】 **dhcp-guard isolate-period** [*seconds* | **permanent**]
【参数说明】 *seconds*：隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
permanent：永久隔离。
【缺省配置】 全局隔离时间的缺省值是 0，即不隔离
【命令模式】 nfpp 模式下
【使用指导】 对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间(即局部隔离时间)。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

【命令格式】 **nfpp dhcp-guard isolate-period** [*seconds* | **permanent**]
【参数说明】 *seconds*： 隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
permanent：永久隔离。
【缺省配置】 缺省情况是没有配置局部隔离时间，采用全局隔离时间
【命令模式】 接口模式下
【使用指导】 -

配置配置监控时间

- 必须配置。
- 在配置了隔离时间时，攻击用户监控时间直接采用隔离时间，配置的监控时间不生效。
- 支持在 AP 设备上进行全局配置。

【命令格式】 **dhcp-guard monitor-period** *seconds*
【参数说明】 *seconds*：监控时间，单位是秒，取值范围是[180, 86400]。
【缺省配置】 600 秒
【命令模式】 nfpp 模式下
【使用指导】 检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。
如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

配置监控主机最大数目

- 必须配置。
- 提高监控主机最大数目，随实际监控主机数增加，处理监控用户需占用更多 CPU 资源。
- 支持在 AP 设备上进行全局配置
- 如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR： The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。
- 当受监控主机满时，打印日志“% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员。

【命令格式】 **dhcp-guard monitored-host-limit** *number*

【参数说明】 *number*：支持的最大最大受监控主机数，取值范围为 1 到 4294967295。

【缺省配置】 1000 个

【命令模式】 nfpp 模式下

【使用指导】 如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR：The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志“% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置受监控主机数） monitored hosts.”提醒管理员。

配置攻击检测水线

- 必须配置。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当管理员配置的限速水线大于攻击阈值时，打印命令提示信息“%ERROR：rate limit is higher than attack threshold 500pps(配置的攻击阈值).”提醒管理员。
- 当管理员配置的攻击阈值小于限速水线时，打印命令提示信息“%ERROR：attack threshold is smaller than rate limit 300pps(配置的限速水线).”提醒管理员。
- 当无法为检测到的攻击者分配内存时，打印日志“%NFPP_DHCP_GUARD-4-NO_MEMORY: Failed to alloc memory.”提醒管理员。
- 基于链路层源 MAC 地址限速优先于基于端口限速处理。
- 在 nfpp 模式下：通过命令 **dhcp-guard rate-limit** { **per-src-mac** | **per-port** } *pps* 配置全局限速水线。
- 在 nfpp 模式下：通过命令 **dhcp-guard attack-threshold** { **per-src-mac** | **per-port** } *pps* 配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。
- 在接口模式下：通过命令 **nfpp dhcp-guard policy** { **per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps* 在端口上配置局部的限速水线和攻击水线。

【命令格式】 **dhcp-guard rate-limit** { **per-src-mac** | **per-port** } *pps*

【参数说明】 **per-src-mac：**对每个源 MAC 地址进行限速。
per-port：对每个端口进行限速。
pps：限速水线值，取值范围是[1,9999]。
【缺省配置】 根据不同的 AC 产品，提供不同的默认值。
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **dhcp-guard attack-threshold** { **per-src-mac** | **per-port** } *pps*
【参数说明】 **per-src-mac：**配置每个源 MAC 地址的攻击水线。
per-port：配置每个端口的攻击水线。
pps：攻击水线，单位是每秒报文数，取值范围是[1,9999]。
【缺省配置】 根据不同的 AC 产品，提供不同的默认值。
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp dhcp-guard policy** { **per-src-mac | per-port** } *rate-limit-pps attack-threshold-pps*
【参数说明】 **per-src-mac：**配置每个源 MAC 地址的限速水线和攻击水线。
per-port：配置每个端口的限速水线和攻击水线。
rate-limit-pps：限速水线，取值范围是 1 到 9999。
attack-threshold-pps：攻击水线，取值范围是 1 到 9999。
【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线
【命令模式】 接口模式下
【使用指导】 攻击水线不能小于限速水线。

配置信任用户

- 可选配置，默认无不监控可信主机。
- DHCP 防攻击仅支持配置不进行监控 MAC，最多可配置 500 条。
- 支持在 AP 设备上进行全局配置。
- 当受监控主机表中存在与可信主机相匹配的表项（MAC 地址相同）时，系统将自动删除此 MAC 地址对应的表项。
- 当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。
- 当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 0000.0000.1111（配置的可信主机）.”提醒管理员。
- 当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 0000.0000.1111（配置的可信主机）.”提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 0000.0000.1111（配置的可信主机）has already been configured.”提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 0000.0000.1111（配置的可信主机）is not found.”提醒管理员。

【命令格式】 **dhcp-guard trusted-host** *mac*

【参数说明】 *mac*： MAC 地址。

【缺省配置】 没有设置任何可信主机

【命令模式】 nfpp 模式下

【使用指导】 如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 DHCP 报文将被允许发往 CPU，不做任何的限速和告警处理。

检验方法

网络主机往配置了 DHCP 攻击检测限速的交换机发送 DHCP 攻击报文，需确认该报文可送 CPU。

- 对于不满足信任用户配置的报文，若超过攻击水线或扫描水线，将有攻击信息提示。
- 若攻击报文满足信任用户配置，将无提示信息。

配置举例

↘ 通过 DHCP 抗攻击保护 CPU

【网络环境】 系统中带有 DHCP 主机用户攻击，部分用户地址申请失败。
系统中，部分主机的 DHCP 报文流量很大，需放行。

【配置方法】
- 配置基于主机的攻击检测水线。
- 配置隔离时间为非 0。
- 配置信任用户。

```
Ruijie# configure terminal
Ruijie(config)# nfpp
Ruijie (config-nfpp)#dhcp-guard rate-limit per-src-mac 8
Ruijie (config-nfpp)#dhcp-guard attack-threshold per-src-mac 16
Ruijie (config-nfpp)#dhcp-guard isolate-period 180
Ruijie (config-nfpp)#dhcp-guard trusted-host 0000.0000.1111
```

【检验方法】
- 通过 **show nfpp dhcp-guard summary** 可以查看到配置信息。

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit      Attack-threshold
Global    Disable 180            -/8/150         -/16/300

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

- 通过 **show nfpp dhcp-guard hosts** 可以查看到监控用户。

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   MAC address     remain-time(s)
 ----    ---------   -----------     --------------
```

```
 *1        Gi0/5       001a.a9c2.4609   160
Total: 1 host
```

- 通过 **show nfpp dhcp-guard trusted-host** 可以查看不监控信任主机信息。

```
mac
----
0000.0000.1111
Total: 1 record(s)
```

常见错误

无。

4.4.5 配置DHCPv6 抗攻击

配置效果

- DHCPv6 攻击识别分为基于主机和基于物理端口两个类别。基于主机方式是采用链路层源 MAC 地址/虚拟局域网号/端口三者结合来识别的。每种攻击识别都有限速水线和告警水线。当 DHCP 报文速率超过限速水线时，超限的 DHCPv6 报文将被丢弃。当 DHCPv6 报文速率超过告警水线时，将打印警告信息，发送 TRAP。
- 基于主机的攻击识别还会对攻击源头采取隔离措施。

注意事项

- 对于在全局与接口上同时存在配置的命令，接口优先级高于全局。
- 隔离默认关闭，若打开隔离功能，攻击用户将占用安全模块表项。

配置方法

↘ 使能攻击检测

- 必须配置，默认打开。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当关闭 DHCPv6 抗攻击功能时，系统将自动清除受监控的主机。

【命令格式】 **dhcpv6-guard enable**
【参数说明】 -
【缺省配置】 默认打开
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp dhcpv6-guard enable**
【参数说明】 -
【缺省配置】 端口没有配置 DHCPv6 抗攻击开关，采用全局开关
【命令模式】 接口模式下
【使用指导】 端口的 DHCPv6 抗攻击开关优先于全局 DHCP 抗攻击开关。

配置隔离时间

- 可选配置，默认关闭隔离功能。
- 在攻击用户报文流量超过 CPP 限速带宽时，可配置隔离时间，将报文直接丢弃，避免占用带宽资源。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

【命令格式】 **dhcpv6-guard isolate-period** [*seconds* | **permanent**]
【参数说明】 *seconds*：隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
permanent：永久隔离。
【缺省配置】 全局隔离时间的缺省值是 0，即不隔离
【命令模式】 nfpp 模式下
【使用指导】 对攻击者的隔离时间分为全局隔离时间和基于端口的隔离时间(即局部隔离时间)。对于某个端口，如果没有配置基于端口的隔离时间，那么采用全局隔离时间；否则，采用基于端口的隔离时间。

【命令格式】 **nfpp dhcpv6-guard isolate-period** [*seconds* | **permanent**]
【参数说明】 *seconds*：隔离时间，单位是秒，取值范围是 0 或者[30, 86400]，0 表示不隔离。
permanent：永久隔离。
【缺省配置】 缺省情况是没有配置局部隔离时间，采用全局隔离时间
【命令模式】 接口模式下
【使用指导】 -

配置配置监控时间

- 必须配置。
- 在配置了隔离时间时，攻击用户监控时间直接采用隔离时间，配置的监控时间不生效。
- 支持在 AP 设备上进行全局配置。

【命令格式】 **dhcpv6-guard monitor-period** *seconds*
【参数说明】 *seconds*：监控时间，单位是秒，取值范围是[180, 86400]。
【缺省配置】 600 秒
【命令模式】 nfpp 模式下
【使用指导】 检测出攻击者的时候，如果隔离时间为 0，将对攻击者进行软件监控，超时为监控时间。在软件监控过程中，当隔离时间被配置为非零值时，将自动对软件监控的攻击者采取隔离，并且把超时设置为隔离时间。监控时间在隔离时间为 0 的情况下才有意义。
如果把隔离时间从非零值改成零，将直接把相关端口的攻击者删除，而不是进行软件监控。

配置监控主机最大数目

- 必须配置。
- 提高监控主机最大数目，随实际监控主机数增加，处理监控用户需占用更多 CPU 资源。
- 支持在 AP 设备上进行全局配置
- 如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR： The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。
- 当受监控主机满时，打印日志“% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置的受监控主机数） monitored hosts.”提醒管理员

【命令格式】 **dhcpv6-guard monitored-host-limit** *number*

【参数说明】 *number*：支持的最大最大受监控主机数，取值范围为 1 到 4294967295。

【缺省配置】 1000 个

【命令模式】 nfpp 模式下

【使用指导】 如果受监控主机数已经达到默认的 1000 个，此时管理员把受监控主机的最大数目设置成小于 1000，不会删除已有的受监控主机，而是打印信息“%ERROR：The value that you configured is smaller than current monitored hosts 1000（配置的受监控主机数），please clear a part of monitored hosts.”来提醒管理员配置没有生效，需要删除部分已经被监控的主机。

当受监控主机表满时，打印日志“% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000（配置受监控主机数） monitored hosts.”提醒管理员。

配置攻击检测水线

- 必须配置。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当管理员配置的限速水线大于攻击阈值时，打印命令提示信息“%ERROR：rate limit is higher than attack threshold 500pps(配置的攻击阈值).”提醒管理员。
- 当管理员配置的攻击阈值小于限速水线时，打印命令提示信息“%ERROR：attack threshold is smaller than rate limit 300pps(配置的限速水线).”提醒管理员。
- 当无法为检测到的攻击者分配内存时，打印日志“%NFPP_DHCPV6_GUARD-4-NO_MEMORY: Failed to alloc memory..”提醒管理员。
- 基于链路层源 MAC 地址限速优先于基于端口限速处理。
- 在 nfpp 模式下：通过命令 **dhcpv6-guard rate-limit** { **per-src-mac** | **per-port** } *pps* 配置全局限速水线。
- 在 nfpp 模式下：通过命令 **dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port** } *pps* 配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。
- 在接口模式下：通过命令 **nfpp dhcpv6-guard policy** { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps* 在端口上配置局部的限速水线和攻击水线。

【命令格式】 **dhcpv6-guard rate-limit** { **per-src-mac** | **per-port** } *pps*

【参数说明】 **per-src-mac：**对每个源 MAC 地址进行限速。
per-port：对每个端口进行限速。
pps：限速水线值，取值范围是[1,9999]。
【缺省配置】 根据不同的 AC 产品，提供不同的默认值。
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **dhcpv6-guard attack-threshold** { **per-src-mac** | **per-port** } *pps*
【参数说明】 **per-src-mac：**配置每个源 MAC 地址的攻击水线。
per-port：配置每个端口的攻击水线。
pps：攻击水线，单位是每秒报文数，取值范围是[1,9999]。
【缺省配置】 根据不同的 AC 产品，提供不同的默认值。
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp dhcpv6-guard policy** { **per-src-mac** | **per-port** } *rate-limit-pps attack-threshold-pps*
【参数说明】 **per-src-mac：**配置每个源 MAC 地址的限速水线和攻击水线。
per-port：配置每个端口的限速水线和攻击水线。
rate-limit-pps：限速水线，取值范围是 1 到 9999。
attack-threshold-pps：攻击水线，取值范围是 1 到 9999。
【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和限速水线
【命令模式】 接口模式下
【使用指导】 攻击水线不能小于限速水线。

配置信任用户

- 可选配置，默认无不监控可信主机。
- DHCPv6 防攻击仅支持配置不进行监控 MAC，最多可配置 500 条。
- 支持在 AP 设备上进行全局配置。
- 当受监控主机表中存在与可信主机相匹配的表项（MAC 地址相同）时，系统将自动删除此 MAC 地址对应的表项。
- 当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。
- 当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 0000.0000.1111（配置的可信主机）.”提醒管理员。
- 当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 0000.0000.1111（配置的可信主机）.”提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 0000.0000.1111（配置的可信主机）has already been configured.”提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 0000.0000.1111（配置的可信主机）is not found.”提醒管理员。

【命令格式】 **dhcpv6-guard trusted-host** *mac*

【参数说明】 *mac*： MAC 地址。

【缺省配置】 没有设置任何可信主机

【命令模式】 nfpp 模式下

【使用指导】 如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 DCHPv6 报文将被允许发往 CPU，不做任何的限速和告警处理。

检验方法

网络主机往配置了 DHCPv6 攻击检测限速的交换机发送 DHCPv6 攻击报文，需确认该报文可送 CPU。

- 对于不满足信任用户配置的报文，若超过攻击水线或扫描水线，将有攻击信息提示。
- 若攻击用户需生成隔离标项，将有用户隔离信息提示。

配置举例

↘ 通过 DHCPv6 抗攻击保护 CPU

【网络环境】 系统中带有 DHCPv6 主机用户攻击，部分 DHCPv6 邻居发现失败。
系统中，部分主机的 DHCPv6 报文流量很大，需放行。

【配置方法】
- 配置基于主机的攻击检测水线。
- 配置隔离时间为非 0。
- 配置信任用户。

```
Ruijie# configure terminal
Ruijie(config)# nfpp
Ruijie (config-nfpp)#dhcpv6-guard rate-limit per-src-mac 8
Ruijie (config-nfpp)#dhcpv6-guard attack-threshold per-src-mac 16
Ruijie (config-nfpp)#dhcpv6-guard isolate-period 180
Ruijie (config-nfpp)#dhcpv6-guard trusted-host 0000.0000.1111
```

【检验方法】
- 通过 **show nfpp dhcpv6-guard summary** 可以查看到配置信息。

```
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status  Isolate-period Rate-limit      Attack-threshold
Global    Disable 180            -/8/150         -/16/300

Maximum count of monitored hosts: 1000
Monitor period: 600s
```

- 通过 **show nfpp dhcpv6-guard hosts** 可以查看到监控用户。

```
If col_filter 1 shows '*', it means "hardware do not isolate host".
 VLAN    interface   MAC address     remain-time(s)
 ----    ---------   -----------     --------------
```

```
 *1        Gi0/5       001a.a9c2.4609   160
Total: 1 host
```

- 通过 **show nfpp dhcpv6-guard trusted-host** 可以查看不监控信任主机信息。

```
mac
----
0000.0000.1111
Total: 1 record(s)
```

常见错误

无。

4.4.6 配置ND抗攻击

配置效果

- AR ND guard 按用途把 ND 报文分成 3 类：邻居请求和邻居公告为第一类，路由器请求为第二类，路由器公告和重定向报文为第三类。第一类报文用于地址解析；第二类报文用于主机发现网关；路由器公告用于通告网关和前缀，重定向报文用于通告更优的下一跳，都和路由有关系。所以划分到第三类。
- 目前仅实现基于物理端口识别 ND 报文攻击。可以对三类报文分别配置限速水线和告警水线。当 ND 报文速率超过限速水线时，超限的 ND 报文将被丢弃。当 ND 报文速率超过告警水线时，将打印警告信息，发送 TRAP。。

注意事项

- 对于在全局与接口上同时存在配置的命令，接口优先级高于全局。
- 隔离默认关闭，若打开隔离功能，攻击用户将占用安全模块表项。

配置方法

↘ 使能攻击检测

- 必须配置，默认打开。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。

【命令格式】 **nd-guard enable**
【参数说明】 -
【缺省配置】 ND 抗攻击功能打开
【命令模式】 nfpp 模式下
【使用指导】 -

【命令格式】 **nfpp nd-guard enable**

【参数说明】 -

【缺省配置】 端口没有配置 ND 抗攻击开关，采用全局开关

【命令模式】 接口模式下

【使用指导】 端口的 ND 抗攻击开关优先于全局开关。

配置攻击检测水线

- 必须配置。
- 支持在 AP 设备上进行全局配置以及单端口独立配置。
- 当管理员配置的限速水线大于攻击阈值时，打印命令提示信息“%ERROR：rate limit is higher than attack threshold 500pps(配置的攻击阈值).”提醒管理员。
- 当管理员配置的攻击阈值小于限速水线时，打印命令提示信息“%ERROR：attack threshold is smaller than rate limit 300pps(配置的限速水线).”提醒管理员。
- 当无法为检测到的攻击者分配内存时，打印日志“%NFPP_ND_GUARD-4-NO_MEMORY: Failed to alloc memory..”提醒管理员。
- 在 nfpp 模式下：通过命令 **nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps* 配置全局限速水线。
- 在 nfpp 模式下：通过命令 **nd-guard attack-threshold per-port** [**ns-na** | **rs** | **ra-redirect**] *pps* 配置全局攻击水线，即当报文速度超过攻击水线的时候，认为存在攻击行为。
- 在接口模式下：通过命令 **nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps* 在端口上配置局部的限速水线和攻击水线。

【命令格式】 **nd-guard rate-limit per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*

【参数说明】 **ns-na：**邻居请求和邻居公告。

rs：路由器请求。

ra-redirect：路由器公告和重定向报文。

pps：限速水线值，取值范围是[1,9999]。

【缺省配置】 每个端口邻居请求/公告的缺省限速水线是每秒 15 个，路由器请求的缺省攻击水线是每秒 15 个，路由器公告/重定向报文的缺省攻击水线是每秒 15 个。

【命令模式】 nfpp 模式下

【使用指导】 -

【命令格式】 **nd-guard attack-threshold per-port** [**ns-na** | **rs** | **ra-redirect**] *pps*

【参数说明】 **ns-na：**邻居请求和邻居公告。

rs：路由器请求。

ra-redirect：路由器公告和重定向报文。

pps：攻击水线，单位是每秒报文数，取值范围是[1,9999]。

【缺省配置】 每个端口邻居请求/公告的缺省限速水线是每秒 30 个，路由器请求的缺省限速水线是每秒 30 个，路由器公告/重定向报文的缺省限速水线是每秒 30 个

【命令模式】 nfpp 模式下

【使用指导】 攻击水线不能小于限速水线。

【命令格式】 **nfpp nd-guard policy per-port** [**ns-na** | **rs** | **ra-redirect**] *rate-limit-pps attack-threshold-pps*

【参数说明】 **ns-na：**邻居请求和邻居公告。

rs：路由器请求。

ra-redirect：路由器公告和重定向报文。

rate-limit-pps：限速水线，取值范围是 1 到 9999。

attack-threshold-pps：攻击水线，取值范围是 1 到 9999。

【缺省配置】 端口没有自己的限速水线和攻击水线，采用全局的限速水线和攻击水线

【命令模式】 接口模式下

【使用指导】 攻击水线不能小于限速水线。

ND snooping 把端口划分为非信任端口和信任端口，非信任端口连接主机，信任端口连接网关。由于通常信任端口的流量大于非信任端口的流量，所以信任端口的限速水线应该高于非信任端口的限速水线，开启 ND snooping 功能时，对于信任端口，ND snooping 将通告 ND guard 把端口的三类报文限速水线都设置成每秒 800 个，把攻击水线都设置成每秒 900 个。

ND guard 同等对待 ND snooping 设置的限速水线和管理员配置的限速水线，后配置的值覆盖先配置的值，并且保存到配置文件中。ND snooping 设置的攻击水线类似。

配置信任用户

- 可选配置，默认无不监控可信主机。
- ND 防攻击仅支持配置不进行监控 MAC，最多可配置 500 条。
- 支持在 AP 设备上进行全局配置。
- 当不监控的可信主机表满时，打印提示信息“%ERROR: Attempt to exceed limit of 500 trusted hosts.”提醒管理员。
- 当删除可信主机失败时，打印提示信息“%ERROR: Failed to delete trusted host 0000.0000.1111（配置的可信主机）.”提醒管理员。
- 当添加可信主机失败时，打印提示信息“%ERROR: Failed to add trusted host 0000.0000.1111（配置的可信主机）.”提醒管理员。
- 当添加的可信主机已经存在时，打印提示信息“%ERROR: Trusted host 0000.0000.1111（配置的可信主机）has already been configured.”提醒管理员。
- 当要删除的可信主机不存在时，打印提示信息“%ERROR: Trusted host 0000.0000.1111（配置的可信主机）is not found.”提醒管理员。

【命令格式】 **nd-guard trusted-host** *mac*

【参数说明】 *mac*： MAC 地址。

【缺省配置】 没有设置任何可信主机

【命令模式】 nfpp 模式下

【使用指导】 如果管理员希望对某台主机不进行监控，即对该主机表示信任，则可以通过该命令配置。该可信主机发往 CPU 的 ND 报文将被允许发往 CPU，不做任何的限速和告警处理。

检验方法

网络主机往配置了 ND 攻击检测限速的交换机发送 ND 攻击报文，需确认该报文可送 CPU。

- 对于不满足信任用户配置的报文，若超过端口攻击水线，将有攻击信息提示。
- 若攻击报文满足信任用户配置，将无提示信息。

配置举例

↘ 通过 ND 抗攻击保护 CPU

【网络环境】 系统中带有 ND 主机用户攻击，部分用户邻居发现失败。
系统中，部分主机的 ND 报文流量很大，需放行。

【配置方法】
- 配置基于主机的攻击检测水线。

```
Ruijie# configure terminal
Ruijie(config)# nfpp
Ruijie (config-nfpp)# nd-guard rate-limit per-port ns-na 30
Ruijie (config-nfpp)# nd-guard attack-threshold per-port ns-na 50
Ruijie (config-nfpp)#nd-guard trusted-host 0000.0000.1111
```

【检验方法】
- 通过 **show nfpp nd-guard summary** 可以查看到配置信息。

```
(Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA-REDIRECT.)
Interface Status  Rate-limit       Attack-threshold
Global    Disable 30/15/15
```

- 通过 **show nfpp nd-guard trusted-host** 可以查看不监控信任主机信息。

```
mac
----
0000.0000.1111
Total: 1 record(s)
```

常见错误

无。

4.4.7 配置集中限速分发

配置效果

通过配置集中限速分发，解决网络忙情况下管理报文和协议报文优先处理问题。

注意事项

配置某类型所占百分比的有效值区间，必须小于等于百分之百减去其它两种类型百分比之和的差值。

配置方法

↘ 配置每类报文允许的最大带宽

必须配置，管理类(Manage)、转发类(Route)、协议类(Protocol)的缺省流量带宽是一样的，具体数值参见产品特性文档。

支持在 AP 设备上进行全局配置。

【命令格式】 **cpu-protect sub-interface** { **manage** | **protocol** | **route** } **pps** *pps_vaule*

【参数说明】 **manage** ：指定管理类

protocol ：指定协议类

route ：指定转发类

pps_vaule ：限速水线，取值范围是 1-100000。

【缺省配置】 -

【命令模式】 在全局模式下

【使用指导】 -

↘ 配置每类报文占用队列的最大百分比

必须配置，默认情况下管理类(Manage)占用 30%，转发类(Route)占用 25%、协议类(Protocol)占用 45%。

支持在 AP 设备上进行全局配置。

【命令格式】 **cpu-protect sub-interface** { **manage** | **protocol** | **route** } **percent** *percent_vaule*

【参数说明】 **manage** ：指定管理类

protocol ：指定协议类

route ：指定转发类

percent_vaule：百分比，取值范围是 1 到 100。

【缺省配置】 见产品特性文档

【配置模式】 在全局模式下

【使用指导】 配置某类型所占百分比的有效值区间，必须小于等于百分之百减去其它两种类型百分比之和的差值。

检验方法

略。

配置举例

↘ 通过集中配置分发，为送 CPU 报文分优先级

【网络环境】

- 网络中存在多种大流量报文，分属不同集中分类。

【配置方法】
- 配置每类报文允许的最大带宽。
- 配置每类报文占用队列的最大百分比

```
Ruijie# configure terminal
Ruijie(config)# cpu-protect sub-interface manage pps 5000
Ruijie(config)# cpu-protect sub-interface manage percent 25
```

【检验方法】 略

常见错误

无。

4.4.8 NFPP日志信息

配置效果

NFPP 以一定速率从专用缓冲区取出日志，生成系统消息，并且从专用日志缓冲区清除这条日志。

注意事项

记录在缓冲区中日志会持续打出，即使这时攻击已停止。

配置方法

↘ 配置日志缓冲区容量

- 必须配置。
- 若缓冲区已满，新生成日志将丢弃，并有信息提示。
- 当日志缓冲区溢出时，后续的日志将被丢弃，同时在日志缓冲区中显示一条所有属性都为"-"的表项。管理员需要增加日志缓冲区容量或者提高生成系统消息的速率。
- 支持在 AP 设备上进行全局配置。

【命令格式】 **log-buffer entries** *number*
【参数说明】 *umber*： 缓冲区大小，单位是日志条数，取值范围是[0,1024]。
【缺省配置】 默认缓冲区大小为 256
【命令模式】 nfpp 模式下
【使用指导】 -

↘ 配置生成系统消息的速率

- 必须配置。
- 由两参数决定：时间段长度以及该时间段内生成系统消息个数。
- 若两参数均为 0，表示日志立即生成系统消息，不入缓冲区。
- 支持在 AP 设备上进行全局配置。

【命令格式】 **log-buffer logs** *number_of_message* **interval** *length_in_seconds*

【参数说明】 *number_of_message*：范围为 0-1024，0 表示日志全部记录在专用缓冲区，不生成系统消息。
length_in_seconds：范围为 0-86400（1 天），0 表示不把日志写到缓冲区，而是立即生成系统消息。。
number_of_message 和 *length_in_seconds* 都为 0 表示不把日志写到缓冲区，而是立即生成系统消息。
number_of_message /length_in_second 表示取日志生成系统消息的速率。

【缺省配置】 number_of_message 缺省为 1，length_in_seconds 缺省值为 30

【命令模式】 nfpp 模式下

【使用指导】

↘ 配置日志过滤

- 可选配置，默认情况下不做过滤。
- 支持基于端口的过滤规则以及基于 vlan 的过滤规则。
- 若配置过滤，不符合过滤规则的日志丢弃。
- 支持在 AP 设备上进行全局配置。

【命令格式】 **logging vlan** *vlan-range*

【参数说明】 *vlan-range*：需要记录指定 VLAN 范围内的日志信息，输入格式如“1-3,5。

【缺省配置】 所有日志都记录

【命令模式】 nfpp 模式

【使用指导】 通过该命令可以对日志进行过滤，只记录指定 VLAN 范围的日志信息。与端口范围日志过滤配置是或的关系，即只需要满足其中一条日志过滤规则，就应该记录到日志缓冲区中。

【命令格式】 **logging interface** *interface-id*

【参数说明】 *interface-id*：需要记录指定端口的日志信息。

【缺省配置】 所有日志都记录

【命令模式】 nfpp 模式

【使用指导】 通过该命令可以对日志进行过滤，只记录指定端口的日志信息。与 vlan 范围日志过滤配置是或的关系，即只需要满足其中一条日志过滤规则，就应该记录到日志缓冲区中。

检验方法

略。

配置举例

↘ 通过 ND 抗攻击保护 CPU

【网络环境】
- 当攻击用户过多时，日志打印影响用户界面使用，需进行限制

【配置方法】
- 配置日志缓冲区容量。
- 配置生成系统消息的速率
- 配置日志基于 vlan 过滤

```
Ruijie# configure terminal
Ruijie(config)# nfpp
Ruijie (config-nfpp)#log-buffer entries 1024
Ruijie (config-nfpp)#log-buffer logs 3 interval 5
Ruijie (config-nfpp)#logging interface vlan 1
```

【检验方法】
- 通过 **show nfpp logsummary** 可以查看到配置信息。

```
Total log buffer size : 1024
Syslog rate : 3 entry per 5 seconds
Logging:
    VLAN 1
```

- 通过 **show nfpp log buffer** 查看缓冲区中日志信息

```
Protocol VLAN Interface  IP address       MAC address      Reason          Timestamp
-------- ---- ---------  -----------      -----------      ------          ---------
ARP      1    Gi0/5      192.168.206.2    001a.a9c2.4609   SCAN            2013-5-1 5:4:24
```

常见错误

无。

4.5 监视与维护

清除各类信息

作用	命令
清除 arp-guard 扫描表。	**clear nfpp arp-guard scan**
清除 arp-guard 抗攻击受监控主机。	**clear nfpp arp-guard hosts**
清除 ip-guard 抗攻击受监控主机。	**clear nfpp ip-guard hosts**
清除 icmp-guard 抗攻击受监控主机。	**clear nfpp icmp-guard hosts**
清除 dhcp-guard 抗攻击受监控主机。	**clear nfpp dhcp-guard hosts**
清除 dhcpv6-guard 抗攻击受监控主机。	**clear nfpp dhcpv6-guard hosts**
清除日志。	**clear nfpp log**

查看运行情况

作用	命令
查看 arp-guard 抗攻击的配置参数。	**show nfpp arp-guard summary**
查看 arp-guard 受监控主机的信息	**show nfpp arp-guard hosts**
查看 arp-guard 扫描表信息	**show nfpp arp-guard scan**
查看 arp-guard 信任用户	**show nfpp arp-guard trusted-host**
查看 ip-guard 抗攻击的配置参数。	**show nfpp ip-guard summary**
查看 ip-guard 受监控主机的信息	**show nfpp ip-guard hosts**
查看 ip-guard 信任用户	**show nfpp ip-guard trusted-host**
查看 icmp-guard 抗攻击的配置参数。	**show nfpp icmp-guard summary**
查看 icmp-guard 受监控主机的信息	**show nfpp icmp-guard hosts**
查看 icmp-guard 信任用户	**show nfpp icmp-guard trusted-host**
查看 dhcp-guard 抗攻击的配置参数。	**show nfpp dhcp-guard summary**
查看 dhcp-guard 受监控主机的信息	**show nfpp dhcp-guard hosts**
查看 dhcp-guard 信任用户	**show nfpp dhcp-guard trusted-host**
查看 dhcpv6-guard 抗攻击的配置参数。	**show nfpp dhcpv6-guard summary**
查看 dhcpv6-guard 受监控主机的信息	**show nfpp dhcpv6-guard hosts**
查看 dhcpv6-guard 信任用户	**show nfpp dhcpv6-guard trusted-host**
查看 nd-guard 抗攻击的配置参数。	**show nfpp nd-guard summary**
查看 nd-guard 信任用户	**show nfpp nd-guard trusted-host**
查看 NFPP 日志信息配置	**show nfpp log summary**
显示 NFPP 的日志缓冲区	**show nfpp log buffer** [**statistics**]

配置指南-WLAN QOS

本分册介绍 WLAN QOS 配置指南相关内容，包括以下章节：

1. WQOS

1 WQOS

1.1 概述

WQOS（WLAN QoS，无线带宽控制）是一种无线的带宽控制功能，它包括流量限速，公平调度。

流量限速，是用来对 AP、WLAN、STA 的数据流量进行限制，避免流量超过一定范围。流量限速适用于某些 STA 占用过多带宽挤占其它 STA 带宽的场景。

公平调度通过将时间均分，解决不同设备占用空口时间不一样，导致低速节点可能长期占用空口时间。公平调度适用于所有无线网络。

协议规范

- IEEE 802.11e-2005：Amendment 8：Medium Access Control (MAC) QualityofServiceEnhancements, IEEE Computer Society
- Wi-Fi：WMM Specification version 1.1

1.2 典型应用

无。

1.3 功能详解

基本概念

↘ 流量限速

为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，设备需要支持流量限速功能。当数据流量符合承诺速率时，允许数据包通过；数据流量不符合承诺速率时，丢弃数据包。

评估流量的参数如下：

- 平均速率（average-data-rate），即允许的流的平均速度，也叫承诺信息速率。
- 突发速率（burst-data-rate），即每次突发所允许的最大的流量，也叫承诺突发尺寸。设置的突发尺寸必须大于最大报文长度。这里指单个周期 10ms 里允许发送的最大速率(计算时，通过单个周期的最大流量除以 10ms 计算出速率值 KBps）

↘ 公平调度

公平调度功能允许关联到同一个 AP 上同一个频段的 STA 共享 AP 提供的无线网络资源，公平的分享无线网络的带宽。使用公平调度功能可以防止低速 STA 拖慢整个无线网络的吞吐量，而且能够为 STA 提供更加平滑的网速体验。另外，公平调度功能

还能够智能地监控每个 STA 的网络流量的变化，动态地调整每个 STA 的所占用的无线带宽比例，为用户带来更好的无线网络体验。在 10.4(1T19)p1 版本之后，允许在公平调度中，对 STA 设置不同的优先级，达到让特定用户能够优先占用无线带宽的目的。

功能特性

功能特性	作用
流量限速	针对 AP、WLAN、STA 进行流量限速，使得流量不会超过限速值。
公平调度	对关联到同一 AP 上同一个频段的 STA 共享 AP 提供的无线网络资源，公平的分享无线网络的带宽。

1.3.1 流量限速

流量限速是用来对某个 AP、某个 WLAN、或者某台 STA 的流量进行限制，保证流量不能超过一定的范围。

工作原理

流量限速是根据令牌桶算法来实现的。

- 记录这个时刻可以通过的报文字节数，通常称为令牌桶。
- 在每个单位周期内，会根据配置的平均速率和突发速率，算出每个单位周期内可以通过的报文字节数，来增加令牌桶的大小。
- 当有报文到达时，会判断报文字节数与令牌桶的大小。如果报文字节数小于令牌桶大小，则允许报文通过，并将令牌桶减少；当报文字节数大于令牌桶大小时，缓存报文，等到令牌桶允许通告之后，再继续发送，通常称为流量整形。流量整形算法，使得流量比较平稳，波动小。
- 目前 AP 上，AP、STA、WLAN 的限速使用流量整形进行处理

1.3.2 公平调度

公平调度是通过将时间均分，解决不同设备占用空口时间不一样，导致低速节点可能长期占用空口时间。

工作原理

由于无线网络的特殊性，在同一个网络的 STA（包括 AP）共享空口资源，而由于无线和有线网络性能上的差异，空口资源往往成为 STA 性能的瓶颈。传统的报文调度采用 FIFO 的方式，同一个无线网络中，每个需要传输的 STA 都希望尽可能的占用空口资源。大量的低速报文的传送造成空口被长时间占用，从而队列长时间被占用，导致报文被丢，使得整体性能低下。

然而在实际无线应用场景中，STA 之间存在差别（类型不一样、能力不一样等）是十分常见的，这时往往导致了某些 STA 总是得不到空口资源，获取网络资源响应慢，极端情况下甚至关联不到网络，严重影响用户的体验。

为了解决这个问题，保证每一个 STA 都能够得到空口资源，就需要让 STA 公平地获得资源，这里的公平指的是每个需要传输的 STA 占用空口的时间是公平的。通过获取 STA 相关信息（协商速率、聚合类型等）、对应报文有效字节数来预测每个 STA

流量，并转换成单个 STA 可发送的报文个数，通过调整 STA 可发送报文数对 STA 空口带宽分配以及流量整形，从而实现无线链路的公平占用。在公平调度的协调下，STA 占用空口的时间较为平均，有效避免了出现某个 STA 性能特别差的情况，提升用户体验。

1.4 配置详解

配置项	配置建议&相关命令	
配置流量限速	⚠ 必须配置。用来开启流量限速。	
	wlan-based	AC 上，配置基于 WLAN 的流量限速
	wlan-qos ap-based	AP 上，配置基于 AP 的流量限速
	wlan-qos netuser	AP 上，配置基于 STA 的流量限速
	wlan-qos wlan-based	AP 上，配置基于 WLAN 的流量限速
配置公平调度	⚠ 必须配置。用来开启公平调度功能。	
	fair-schedule	开启公平调度功能
	⚠ 可选配置。用来调整公平调度过程中 STA 的优先级。	
	sta-fair	设置 STA 的公平调度优先级

1.4.1 配置流量限速

配置效果

- 用户可根据实际网络情况，限制某个流只能得到承诺分配给它的那部分资源，防止由于过分突发流量所引发的网络拥塞。

注意事项

- 胖 AP 上的 CLI 命令是在全局模式下配置的。

配置方法

↘ 配置基于 AP 的流量限速

- 必须配置。
- 胖 AP 上，在全局配置模式下，使用 **wlan-qos ap-based** 命令配置基于 AP 的限速。

【命令格式】 **wlan-qos ap-based** { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

wlan-qos ap-based total-user-limit { **down-streams** | **up-streams** } **intelligent**

【参数说明】 **per-user-limit**：对 AP 上的每个用户进行限速。
total-user-limit：对整个 AP 进行限速。
intelligent：表示是否对 total 进行智能限速。
down-streams：表示设置 AP 的下行流量限速。
up-streams：表示设置 AP 的上行流量限速。
average-data-rate：表示设置平均速率限制，单位为 8Kbps，范围为 8-261120。
burst-data-rate：表示设置突发速率限制，单位为 8Kbps，范围为 8-261120。

【缺省配置】 缺省为无流量限速。配置了 total-user-limit 缺省不开启智能限速

【命令模式】 全局配置模式

【使用指导】 -

配置基于 STA 的流量限速

- 必须配置。
- 胖 AP 下，在全局配置模式下，使用 **wlan-qosnetuser** 命令进行配置。

【命令格式】 **wlan-qos netuser** *mac-address* { **inbound** | **outbound** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*

【参数说明】 *mac-address*：表示需要设置的用户 MAC 地址。
inbound：表示设置用户的上行流量限速。
outbound：表示设置用户的下行流量限速。
average-data-rate：表示设置平均速率限制，单位为 8Kbps，范围为 8-261120。
burst-data-rate：表示设置突发速率限制，单位为 8Kbps，范围为 8-261120。

【缺省配置】 缺省为无流量限速

【命令模式】 全局配置模式

【使用指导】 -

配置基于 WLAN 的流量限速

- 必须配置。
- 胖 AP 下，在全局配置模式下，使用 **wlan-qos wlan-based** 命令进行配置。

【命令格式】 **wlan-qos wlan-based** { *wlan-id* | *ssid* } { **per-user-limit** | **total-user-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
wlan-qos wlan-based { *wlan-id* | *ssid* } **total-user-limit** { **down-streams** | **up-streams** } **intelligent**

【参数说明】 **per-user-limit**：对 WLAN 上的每个用户进行限速。
total-user-limit：对整个 WLAN 进行限速。
intelligent：表示是否对 total 进行智能限速。
per-ap-limit：对每个 AP 各自做 WLAN TOTAL 限速。
down-streams：表示设置 WLAN 的下行流量限速参数。
up-streams：表示设置 WLAN 的上行流量限速参数。
average-data-rate：表示设置平均速率限制，单位为 8Kbps，范围为 8-261120。
burst-data-rate：表示设置突发速率限制，单位为 8Kbps，范围为 8-261120。

【缺省配置】 缺省为无流量限速。
【命令模式】 全局配置模式
【使用指导】 -

检验方法

无。

配置举例

无。

常见错误

- 无。

1.4.2 配置公平调度

配置效果

- 用公平调度功能可以防止低速 STA 拖慢整个无线网络的吞吐量，而且能够为 STA 提供更加平滑的网速体验。

注意事项

- 在胖 AP 上，配置公平调度的命令位于全局配置模式下，使用 **show running-config** 查看配置。

配置方法

↘ 开启公平调度功能

- 必须配置。
- 胖 AP 上，在全局配置模式下通过 **fair-schedule** 配置。
- 开启公平调度功能，使得可以时间公平的给 STA 分配时间。

【命令格式】 **fair-schedule**
【参数说明】 -
【缺省配置】 公平调度功能开启
【命令模式】 全局配置模式
【使用指导】 -

↘ 配置公平调度优先级

- 可选配置。如果需要提高某一 STA 的优先级的话，必须配置。
- 胖 AP 上，在全局配置模式下通过 **sta-fair** 命令配置。

【命令格式】 **sta-fair** *mac-address* **priority** *priority*

【参数说明】 *mac-address*：表示需要设置的用户 MAC 地址。

priority：优先级别，范围：1 到 6

【缺省配置】 缺省所有的 STA 优先级为 1。数值越大代表优先级越高，优先级越高，分配给 STA 的空口时间越多。

【命令模式】 全局配置模式

【使用指导】 -

检验方法

- 使用 **show ap-config run** 查看配置信息

配置举例

无。

常见错误

- 无。

1.5 监视与维护

清除各类信息

无。

查看运行情况

无。

查看调试信息

无。

配置指南-WLAN 组网

本分册介绍 WLAN 组网配置指南相关内容，包括以下章节：

1. 配置胖 AP
2. WDS

1 配置胖 AP

1.1 概述

AP（Access Point，无线接入点）是一种控制和管理无线客户端的无线设备。

帧在无线客户端和 LAN 之间传输需要经过无线到有线以及有线到无线的转换，而 AP 在这个过程中起到了桥梁的作用。

AP 有两种模式：FAT-AP（Fat Access Point，胖 AP）、FIT-AP（Fit Access Point，瘦 AP）。

- FAT-AP 适用于家庭和小型网络，功能比较全，一般一台设备就能实现接入、认证、路由、VPN、地址翻译、甚至防火墙功能。
- FIT-AP 适用于大规模无线部署，需要专用无线控制器统一管理，通过无线控制器下发配置才能用，本身不能进行相关配置。

下文仅介绍 FAT-AP 的相关内容。

协议规范

- IEEE Std 802.11-2012：Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

1.2 典型应用

典型应用	场景描述
单一BSS	最简单的 WLAN 可以由一个 BSS 建立，所有的无线客户端都在同一个 BSS 内。
多ESS	网络中存在多个逻辑管理域（即 ESS）的情况。当一个移动用户加入到某个 FAT-AP，它可以加入一个可用的 ESS。
单一ESS多BSS（多重射频情况）	FAT-AP 在单一逻辑管理时有超过一个频段的应用。所有的频段支持相同的服务集（在同一个 ESS 内），但由于属于不同的 BSS 所以逻辑上的覆盖范围是不同的。

1.2.1 单一BSS

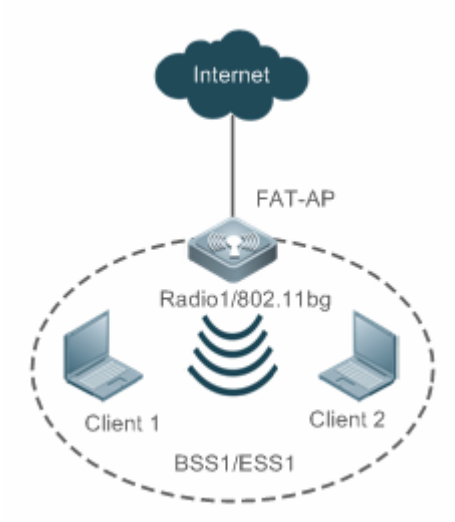
应用场景

一个 AP 所覆盖的范围被称为 BSS（Basic Service Set，基本服务集）。每一个 BSS 由 BSSID 来标识。最简单的 WLAN 可以由一个 BSS 建立，所有的无线客户端都在同一个 BSS 内。如果这些客户端都得到了同样的授权，那么他们就可以互相通信。这些客户端可以互相访问，也可以访问网络中的主机。属于同一 BSS 的客户端之间的通信由 FAT-AP 实现。

以下图为例，Client1 和 Client2 都连接到 2.4GHz 频段；Client1 和 Client2 都在 BSS1 内。

- Client1 和 Client2 可以互相访问，也可以访问网络中的主机。

图 1-1



【注释】 Radio1 为 FAT-AP 的第一个射频口。
Client1、Client2 为无线客户端。
FAT-AP、Client1、Client2 共同构成 BSS1，BSS1 归属 ESS1。

功能部属

- 在 FAT-AP、Client1、Client2 中运行 IEEE802.11 协议，实现无线客户端的接入、认证。
- 在 FAT-AP 上实现胖 AP 的配置管理。
- 在 FAT-AP 上只有 Radio1，只能选择运行 802.11a 协议或 802.11b 协议。
- 在 FAT-AP 上只创建一个 WLAN，即 ESS1；ESS1 只能映射到 Radio1，即 BSS1。

1.2.2 多ESS

应用场景

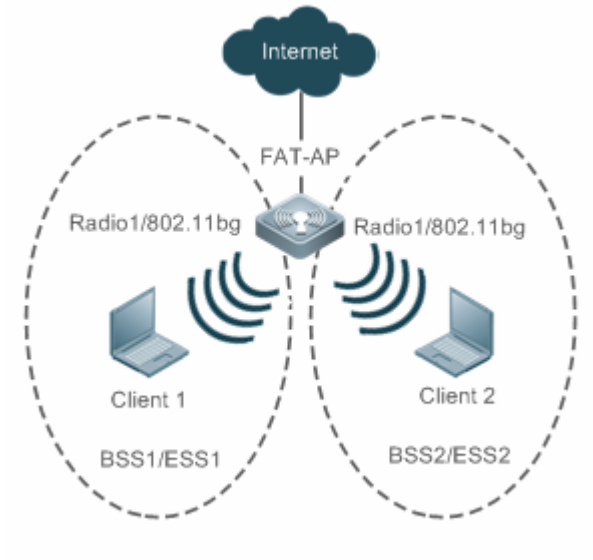
多 ESS 拓扑结构用于网络中存在多个逻辑管理域（即 ESS）的情况。当一个移动用户加入到某个 FAT-AP，它可以加入一个可用的 ESS。

通常，FAT-AP 可以同时提供多个逻辑 ESS。FAT-AP 中的 ESS 的配置主要通过发送信标或探查响应帧，在网络中广播这些 ESS 的当前信息，客户端可以根据情况选择加入的 ESS。

在 FAT-AP 上，可以配置不同的 ESS 域，并可以配置当这些域中的用户通过身份认证后，允许 FAT-AP 通告并接受这些用户。

以下图为例，Client1 和 Client2 都连接到 2.4GHz 频段；Client1 属于 ESS1，而 Client2 属于 ESS2；Client1 属于 BSS1，而 Client2 属于 BSS2。

图 1-2



【注释】 Radio1 为 FAT-AP 的第一个射频口。
Client1、Client2 为无线客户端。
FAT-AP、Client1 共同构成 BSS1，BSS1 归属 ESS1。
FAT-AP、Client2 共同构成 BSS2，BSS2 归属 ESS2。

功能部属

- 在 FAT-AP、Client1、Client2 中运行 IEEE802.11 协议，实现无线客户端的接入、认证。
- 在 FAT-AP 上实现胖 AP 的配置管理。
- 在 FAT-AP 上只有 Radio1，只能选择运行 802.11a 协议或 802.11b 协议。
- 在 FAT-AP 上创建两个 WLAN，即 ESS1 和 ESS2；两个 WLAN 都映射到 Radio1，即 BSS1 和 BSS2。

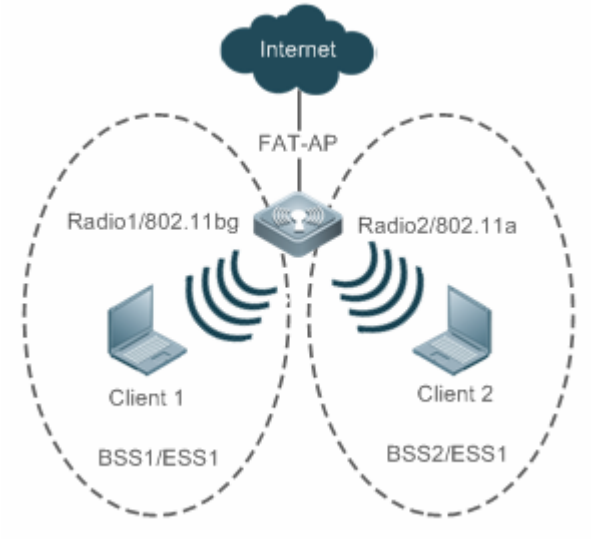
1.2.3 单一ESS多BSS（多重射频情况）

应用场景

FAT-AP 在单一逻辑管理域有超过一个频段的应用，所有的频段支持相同的服务集（在同一个 ESS 内）；但是因为属于不同的 BSS，所以物理上的覆盖范围是不同的。这种组网也应用于需要共同支持 802.11a 和 802.11b/g 的情形。

以下图为例，Client1 连接到 2.4GHz 频段，Client2 连接到 5GHz 频段；Client1 和 Client2 都属于相同 ESS1，但是 Client1 属于 BSS1，而 Client2 属于 BSS2。

图 1-3



【注释】 Radio1 为 FAT-AP 的第一个射频口。
Radio2 为 FAT-AP 的第二个射频口。
Client1、Client2 为无线客户端。
FAT-AP、Client1 共同构成 BSS1，BSS1 归属 ESS1。
FAT-AP、Client2 共同构成 BSS2，BSS2 同样归属 ESS1。

功能部属

- 在 FAT-AP、Client1、Client2 中运行 IEEE802.11 协议，实现无线客户端的接入、认证。
- 在 FAT-AP 上实现胖 AP 的配置管理。
- 在 FAT-AP 上有两个 Radio，即 Radio1 和 Radio2；Radio1 运行 802.11b 协议，Radio2 运行 802.11a 协议。
- 在 FAT-AP 上创建两个 WLAN，即 ESS1 和 ESS2；ESS1 映射到 Radio1，即 BSS1；ESS2 映射到 Radio2，即 BSS2。

1.3 功能详解

基本概念

WLAN

WLAN（Wireless Local Area Network，无线局域网）是通过无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。

AC

AC（Access Category）：访问类型。AC 是通用的 EDCA 参数集合的标签。不同 AC 因 EDCA 参数不同，而有不同的访问媒介的优先级。

AP

AP（Access Point）：无线终端访问有线网络的接入点，相当于无线终端与有线网络通信的桥梁。

STA

无线用户：使用无线终端上网的用户。

BSS

指一个 AP 所覆盖的范围。每一个 BSS 由 BSSID 来标识，最简单的 WLAN 可以由一个 BSS 建立，所有的无线客户端都在同一个 BSS 内。如果这些客户端都得到了同样的授权，那么他们就可以互相通信。

ESS

ESS（Extended Service Set，扩展服务集），由相同逻辑管理域下的所有客户端组成。一个 ESS 可能包含多个 BSS。

SSID

SSID（Service Set Identifier，服务集标识），也可以写为 ESSID。用于区分不同的网络，即标识一个 ESS。SSID 最多可以有 32 个字符。无线网卡设置了不同的 SSID 就可以进入不同网络，SSID 通常由 AP 或无线路由器广播出来，通过 XP 自带的扫描功能可以查看当前区域内的 SSID。出于安全考虑可以不广播 SSID，此时用户就要手工设置 SSID 才能进入相应的网络。简单说，SSID 就是一个局域网的名称，只有设置为名称相同 SSID 的值的电脑才能互相通信。

功能特性

功能特性	作用
建立WLAN	建立 WLAN 网络、并关联到 SSID。
映射WLAN到无线设备	指定 WLAN 网络使用的虚拟的无线设备。
网络部署与优化	设置无线设备的射频参数进行无线网络部署、优化等。
电子书包参数设置	实现对 AP 及其 Radio 相关的电子书包参数设置。
链路完整性检测	开启或关闭链路完整性检测功能。
一键WLAN配置	在空配置的设备上，为了实现快速配置，提供一键配置 WLAN 的功能。

1.3.1 建立WLAN

FAT-AP 要向无线客户端提供无线接入服务，第一步就是要建立 WLAN 网络。

工作原理

划分 WLAN 子网

在无线网络中，用户可以通过创建 WLAN 将网络划分成多个 WLAN 子网，并在 WLAN 配置模式下配置指定 WLAN 的功能属性，实现为无线用户提供不同的网络服务。

关联到 SSID

在创建 WLAN 的同时必须关联一个 SSID，SSID 仅是一个网络服务域的名称，一个 SSID 可以对应一个或多个 WLAN。

广播 SSID

在 WLAN 网络中，AP 会定期广播 SSID 信息，向外通告无线网络的存在，无线用户使用无线网卡搜索 SSID 发现网络。为避免无线网络被非法用户通过 SSID 广播搜索到，并建立非法连接，可以将 SSID 广播禁用。

组播速率

在 WLAN 网络中，AP 向 STA 发送多播报文时采用的速率。组播速率越高，网络性能越高，但是对信噪比的要求也就越高，远距离无线终端的组播丢包率越高；相反地，组播速率越低，网络性能越低，但是对信噪比的要求也就越低，远距离无线终端的组播丢包率越低。

1.3.2 映射WLAN到无线设备

建立了 WLAN 网络后，这个 WLAN 网络要使用无线设备进行无线传输。

工作原理

dot11radio 子接口

dot11radio 子接口是一个虚拟的无线设备，其功能与实体的无线设备基本没有差别。

dot11radio 子接口封装的 VLAN

无线设备的无线报文在有线网络进行转发时需要 VLAN 属性。

映射 WLAN ID 到 dot11radio 子接口

指定 WLAN 网络使用的虚拟的无线设备，以进行无线传输。

1.3.3 网络部署与优化

映射 WLAN 网络到无线设备后，要设置无线设备的射频参数进行网络部署与优化等。

工作原理

DTIM 周期

DTIM（Delivery Traffic indication Map，延迟传输指示讯息）是 Beacon 帧内的一个标志位，用来定时 AP 发送广播帧或多播帧的时间间隔。当无线终端处于休眠状态时，AP 会自动为其暂存 DTIM 时间间隔内需要接收的数据。待 DTIM 超时，AP 将这些缓存数据发送给无线终端。

DTIM 是以发送的 Beacon 数为周期，假设设置的 DTIM 周期时间为 3，即每发送 3 个 Beacon 帧后，AP 才会发送广播帧或多播帧。

U-APSD 节电模式

U-APSD 是对原有节电模式的改进。客户端在关联时可以指定某些 AC 具有触发属性，某些 AC 具有发送属性，以及触发后最多允许发送的数据报文数量。触发和发送属性还可以在通过连接准入控制创建流的时候进行更改。客户端休眠后，发往客户端的属于具有发送属性 AC 的数据报文将被缓存在发送缓存队列中，客户端需要发送属于具有触发属性 AC 的报文以获取发送缓存队列中的报文。AP 收到触发报文后，按照接入时确定的发送报文数量，发送属于发送队列的报文。没有发送属性的 AC 仍然使用 802.11 定义的传统方式存储和传送。

A-MPDU 聚合

802.11n 标准中采用 A-MPDU 聚合帧格式，即将多个 MPDU 聚合为一个 A-MPDU，只保留一个 PHY 头，删除其余 MPDU 的 PHY 头，减少了传输每个 MPDU 的 PHY 头的附加信息，同时也减少了 ACK 帧的数目，从而降低了协议的负荷，有效的提高网络吞吐量。

传输标准

802.11 是 IEEE 为无线局域网定义的一个无线网络通信的工业标准，此后这一标准又不断得到补充和完善，形成 802.11X 的标准系列。其中，主要的传输标准为 802.11b\a\g\n，具体说明如下：

1、802.11b

其工作频段为 2.4GHZ，最大数据传输速率可达到 11Mb/s，根据实际需要，传输速率可降低为 5.5、2 或 1Mb/s。

2、802.11a

其工作频段为 5GHZ，最大数据传输速率可达到 54Mb/s，根据实际需要，传输速率可降低为 48，36，24，18，12，9 或 6Mb/s。

3、802.11g

其工作频段为 2.4GHZ，最大数据传输速率可达到 54Mb/s，根据实际需要，传输速率可降低为 48，36，24，18，12，9 或 6Mb/s,支持 802.11g 的设备可向后兼容 802.11b。

4、802.11n

支持 2.4GHZ 和 5GHZ 两个工作频段，最大数据传输速率可达到 600Mb/s，支持 802.11n 的设备可向后兼容 802.11a/b/g。

MCS

802.11n 射频速率的配置通过 MCS（Modulation and Coding Scheme，调制与编码策略）索引值实现。MCS 调制编码表是 802.11n 为表征 WLAN 的通讯速率而提出的一种表示形式。MCS 将所关注的影响通讯速率的因素作为表的列，将 MCS 索引作为行，形成一张速率表。所以，每一个 MCS 索引其实对应了一组参数下的物理传输速率，全部 MCS 速率表的描述可参见“IEEE P802.11n D2.00”。

接入 AP 的无线用户范围

无线用户搜索 AP 的方式主要通过主动扫描或被动扫描。

- 主动扫描：即无线用户发送 Probe Request 帧请求接入 AP，AP 确认后发送 Probe Response 帧响应；
- 被动扫描：即 AP 定期向外广播 Beacon 帧，无线用户侦听到 Beacon 帧试图连接。

为控制 AP 的网络覆盖范围，提高无线信号传输质量，可以通过限制接入的无线用户。首先，可以通过控制 AP 广播 Beacon 帧的范围，减少远距离的无线用户接入；其次，可以通过限制无线用户接入时的 RSSI（接收信号强度指示）的最小值，当接收到无线用户的请求帧的 RSSI 小于这个值，则不允许该无线用户接入；再次，可以通过限制无线用户数据传输时的 RSSI 的最小值，当接收到无线用户的数据帧的 RSSI 小于这个值，则踢掉该无线用户，帮助其接入到无线信号更好的 AP 上。

无线用户老化

每个无线用户加入 WLAN 网络，系统自动为其设置老化时间，如果在该时间内，没有收到无线用户发来的信息，将默认该无线用户离开 WLAN 网络，系统将其从网络中删除。

无线信道

无线信道（Channel）是 AP 与无线用户之间传输射频介质的通道。不同的国家以及不同的频段支持的信道也不同。在中国，2.4GHZ 的频段可以配置的信道有 13 个（channel 1、2、3...13），5GHZ 的频段可以配置的信道有 24 个（Channel 36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、 149、153、157、161、165） 。在 2.4GHZ 的频段中，互相重叠的信道会产生干扰，为避免无线信号冲突，建议将其配置为不重叠的信道（例如 Channel 1、6、11）；而 5GHZ 的频段，这 24 个信道不会互相重叠，也不会产生干扰。

报文分片

为了提高传输成功率，IEEE 802.11 MAC 协议允许将报文分成若干小片段进行传输。根据分片阈值，对报文进行分片，可降低受干扰机率，且即使重传也可减少所重传浪费的带宽。

RTS/CTS

为了避免信道冲突，而导致数据传输失败，IEEE 802.11 MAC 协议提供了一个 RTS/CTS(Request To Send/Clear To Send)握手协议，即请求发送/允许发送协议。假设工作站 A 需要向工作站 B 发送数据，首先会发送一个 RTS 请求帧，如果工作站 B 允许工作站 A 发送，就会回复一个 CTS 允许帧，工作站 A 收到后便开始发送数据。如果存在多个工作站向同一个工作站发送 RTS 以示请求发送数据，则只有收到 CTS 的工作站可以发送数据，没有收到 CTS 的工作站默认信道冲突，则等待一定时间后再发送 RTS 请求。

如果每个工作站每次发送数据前都要执行 RTS/CTS 握手，将导致过多的 RTS 帧占用信道带宽，用户可以设置 RTS Threshold 来指定发送数据的帧长度，如果工作站发送数据的帧长度小于 RTS Threshold 设置的门限，将不执行 RST/CTS 握手。。

Beacon

在 WLAN 网络中，AP 会定期向外发送 Beacon（即信标帧），Beacon 包含了该 AP 的相关信息，无线用户通过接收 Beacon 来发现 WLAN 网络。

前导码类型

前导码（Preamble）是数据报文头部的一组 Bit 位，用于同步发送端与接收端的传输信号，用户可以配置指定 AP 支持的前导码类型（long 或 short），长前导码的数据帧传输时间长，短前导码的数据帧传输时间短。

时隙类型

在 WLAN 网络中，为避免多个工作站发送数据引起信道竞争，工作站在发送数据之前需要检测信道是否空闲。如果检测到信道处于空闲状态，工作站并不立即发送数据，而是等待一个退避时间(Backoff Time)。退避时间是时隙时间(Slot Time，MAC

协议中的一个操作时间单元）的随机整数倍，假设随机值为 3，则每经过一个时隙时间，系统自动将数值减 1，待数值减为零时，工作站开始发送数据。因此，降低时隙时间可以减少总体退避时间，从而增加网络的吞吐量。

信道带宽

802.11n 通过将两个 20MHz 的带宽绑定在一起组成一个 40MHz 通讯带宽，在实际工作时可以作为两个 20MHz 的带宽使用（一个为主带宽， 一个为次带宽， 收发数据时既可以以 40MHz 的带宽工作，也可以以单个 20MHz 带宽工作），这样可将速率提高一倍，提高无线网络的吞吐量。

防护间隔

802.11n 提供了缩短防护时间的机制，使能短防护间隔机制，防护时间由 0.8us 降低为 0.4us。

国家代码

国家代码是用来识别使用射频所在的国家，不同的国家代码规定的射频频段、信道、功率将有所不同。在配置 AP 前，需要先明确该 AP 所支持的国家代码，如果配置的国家代码发生变化，对应的射频频段、信道、功率值也会有所变化。

天线收发类型

AP 发射与接受使用不同数量的天线，可以使得 AP 在 802.11n 模式下采用双空间流模式或者三空间流模式来发射信号，提升 AP 数据传输的性能。

内置天线与外置天线

内置天线是集成到 AP 设备壳体内的天线。外置天线是可以通过 AP 设备预留的硬件接口进行外接的天线。相同传输功率下，外置天线比内置天线的传输距离更远。

AP 的 radio 与无线传输对端之间允许的最远距离

无线信号以光速在空间传播。AP 的 radio 与无线传输对端之间的距离越远，无线报文在空间传输所需的时间越长；相应地，AP 等待接收 ACK 帧、CTS 帧所需的超时时间就越长。因此，有必要根据 AP 的 radio 与无线传输对端之间的距离长短适当地调整超时时间；否则将无法进行无线数据传输。但是，超时时间也不能过度地加长；否则当 AP 没有接收到 ACK 帧、CTS 帧时，过度的超时时间会造成空口资源浪费。

mcell

mcell 功能通过关闭 radio 的 LNA（Low Noise Amplifier）器件达到降低接收灵敏度/增加密集部署环境下空口并发的效果。

1.3.4 电子书包参数设置

实现对 AP 及其 Radio 相关的电子书包参数设置。

工作原理

在电子书包场景中，经常需要配置一些命令，来达到更好的体验效果。一键配置电子书包网优命令可以用于快速配置。

AMPDU

即 A-MPDU 聚合。

LDPC

LDPC 码是一种易实现和系统复杂度低的优秀的线性纠错码。它是一种前向错误修正(Forward Error Correction, FEC)编码技术，可提高编码的可靠性与编码增益。此技术于 1960 年初期开始发展，可在具有大量背景或内容损坏的噪杂频率中传送讯息。在受到严重噪杂干扰的频率中使用此技术，可大幅降低资料遗失的风险，但是存在极少量终端在兼容 LDPC 上具备一定问题，表现为丢包。

STBC

无线通信技术中一种在不同时刻、不同天线上发射数据的多个副本，从而利用时间和空间分集以提高数据传输可靠性的编码，这种 STBC 编码的最大优势在于，采用简单的最大似然译码准则，可以获得完全的天线增益。但是可能存在部分终端无法有效兼容该编码方式。

AMPDU 软件重传次数

配置 AMPDU 软件重传次数作用在于在无线中可能存在子帧丢失情况，因此可以通过软件重传来避免子帧丢失，重传的次数越大，子帧丢失的可能性越低，但是重传次数过多可能造成空口负担增大，造成空气中其他报文的实时性下降，如果需要在子帧丢失概率较大的干扰下确保报文尽可能避免丢失，可以将数值调大。

AMPDU-RTS

AMPDU 的 RTS 保护能够避免因为隐藏节点问题导致 AMPDU 报文在空口碰撞，造成空口资源浪费，但是同时由于 RTS 交互会造成一定的空口消耗，在大多数应用场景中，会对空口造成一定副作用，因此默认情况下处于关闭状态。只有隐藏节点问题造成的空口资源浪费大于 RTS 交互造成的空口资源浪费时，才开启 AMPDU 的 RTS 保护。

1.3.5 链路完整性检测

AP 设备作为无线接入设备，本身的作用相当于物理层和 MAC 的一部分，一般不具备交换功能。从硬件结构看，不管是胖 AP 或者瘦 AP，一般只有单条上链有线链路，这条链路是所有接入用户的数据通道。如果这条上链有线链路由于故障断开，那么所有接入这台 AP 的无线用户都无法连接到外部网络。

问题在于，一旦出现上述问题，无线用户无法立刻感知而采取相应的对策，导致无线用户的网络长时间无法恢复正常连接。

链路完整性检测旨在解决这个问题。

工作原理

链路完整性检测功能，在 AP 上持续检测 AP 上链有线链路；在链路断开时，立刻关闭该 AP 上的射频口，暂停 AP 的接入服务，强制关联此 AP 的无线用户下线，迫使无线用户选择周围其他正常工作的 AP 重新接入网络。

在 AP 上链有线链路恢复正常后，链路完整性检测功能再重新打开 AP 的射频口，恢复 AP 的无线接入服务。

链路完整性检测的必要性在于，当 AP 的唯一上行链路断开后，AP 无法再给无线用户提供接入功能，与其让无线用户继续关联，不如关闭 AP 的射频口，强制无线用户下线，让无线用户选择其他的 AP 重新接入。

1.3.6 一键WLAN配置

在空配置的设备上，为了实现快速配置，提供一键配置 WLAN 的功能。

工作原理

autowifi

在 AP 上配置：

（1）vlan 划分：AP 上使用 vlan 10 作为 STA 的 vlan。

（2）地址池：FAT AP 上使用 192.168.110.0 网段作为 STA 地址池，bvi 1 的 IP 地址为 192.168.110.1。

（3）wlan 配置：使用 autowifi_XXXX，后面 4 个字符为设备 MAC 的后 4 位；使用 wlan-id 1。

（4）安全：默认使用 WPA2 加密，密码为 autowifi。

（5）wlan-vlan 映射：AP 上，在无线口上封装 vlan 10，配置 wlan-id 1。

（6）服务：开启 DHCP 服务。

1.3.7 取消供电限制功能配置

针对需要 POE+供电的 AP，如果该 AP 和 POE+供电设备不能协商到 POE+的情况下，取消供电限制，AP 可以按最大能力值使用。

工作原理

供电协商为 15.4W 供电限制情况下，通过配置该命令可以取消供电限制。

该命令使用的时候请确保对应的供电设备支持对应 AP 的最大能力功耗要求，否则易出现重启情况，请注意配置该命令的风险。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置WLAN	必须配置。用于配置 SSID。	
	ssid	配置 SSID
	可选配置。用于配置是否广播 SSID。	
	broadcast-ssid	配置是否广播 SSID
	可选配置。用于配置组播速率。	

	mcast-rate	配置组播速率
配置dot11radio子接口	⚠ 必须配置。用于创建 dot11radio 子接口、配置 dot11radio 子接口的属性。	
	encapsulation	配置 dot11radio 子接口封装的 VLAN
	wlan-id	配置映射到 dot11radio 子接口的 WLAN ID
配置无线射频参数	⚠ 可选配置。用于配置无线射频参数。	
	beacon dtim-period	配置 DTIM 周期
	apsd	配置启用/禁用 U-APSD 节电模式
	ampdu	配置启用/禁用 A-MPDU 聚合方式
	rate-set 11a	配置 11a 速率集
	rate-set 11b	配置 11b 速率集
	rate-set 11g	配置 11g 速率集
	rate-set 11n	配置 11n 速率集
	rate-set 11ac	配置 11ac 速率集
	mcast-rate	配置组播速率
	power local	配置发送功率
	sta-limit	配置基于射频口的 STA 数量限制
	11asupport	配置是否支持 11a
	11bsupport	配置是否支持 11b
	11gsupport	配置是否支持 11g
	11nsupport	配置是否支持 11n
	11acsupport	配置是否支持 11ac
	response-rssi	配置无线用户接入最小 RSSI
	assoc-rssi	配置无线用户保持接入的最小 RSSI
	coverage-area-control	配置管理帧发送功率
	sta-idle-timeout	配置 STA 空闲时间
	channel	配置信道
	fragment-threshold	配置分片阈值
	rts threshold	配置 RTS 阈值
	beacon period	配置 Beacon 帧周期
	short-preamble	配置启用/禁用短前导
	slottime	配置启用/禁用短时隙
	chan-width	配置信道带宽
	short-gi	配置启用/禁用短防护间隔
	radio-type	配置无线模式 a/b
	country-code	配置国家代码
	antenna receive	配置天线接收方式
	antenna transmit	配置天线发送方式
	external-antenna enable	配置启用外置天线，并禁用内置天线
	peer-distance	配置 AP 与无线传输对端之间允许的最远距离

	mcell	配置启用/禁用 mcell 功能
配置电子书包参数	⚠ 可选配置，用于设置电子书包参数	
	ampdu-retries	配置 AMPDU 软件重传次数
	ampdu-rts	配置是否开启 AMPDU 聚合报文的 RTS 保护机制
	eth-schd	配置 AP 以太网单次收包数
	ldpc	配置是否支持低密度奇偶校验编码
	stbc	配置是否使能接收发送空时分组码
	ebag	一键配置电子书包网优
配置链路完整性检测功能	⚠ 必须配置。用于开启链路完整性检测功能。	
	link-check enable	打开链路完整性检测功能
一键WLAN配置	⚠ 可选配置，用于一键配置 WLAN	
	autowifi	一键配置 WLAN
配置整机用户数限制	⚠ 可选配置，用于配置整个胖 AP 上的用户数限制	
	sta-limit	配置整机用户数限制
配置取消供电限制功能	⚠ 可选配置，用于取消供电限制	
	poe-unlimit	配置取消供电限制

1.4.1 配置WLAN

配置效果

- 创建 WLAN。
- 配置 WLAN 属性。

注意事项

- 胖 AP 产品支持。

配置方法

↘ 创建 WLAN

- 必须配置，FAT-AP 才能提供 WLAN 服务，使用 **dot11 wlan** 命令可以创建或删除 WLAN。
- 若无特殊要求，应在 AP 设备的全局配置模式下配置。

【命令格式】 **dot11 wlan** *wlan-id*
【参数说明】 *wlan-id*：指定 WLAN ID。
【缺省配置】 -
【命令模式】 全局配置模式
【使用指导】 -

配置 SSID

- 必须配置，FAT-AP 才能提供 WLAN 服务，使用 **ssid** 命令可以配置指定 WLAN 的 SSID。
- 若无特殊要求，应在 AP 设备的 WLAN 配置模式下配置。

【命令格式】 **ssid** *ssid-string*
【参数说明】 *ssid-string*：指定 SSID 字符串。
【缺省配置】 -
【命令模式】 WLAN 配置模式
【使用指导】 -

配置是否广播 SSID

- 可选配置。
- 若无特殊要求，应在 AP 设备的 WLAN 配置模式下配置。
- 如果广播 SSID，AP 会定期广播 SSID 信息，无线用户使用无线网卡搜索 SSID 发现网络。如果不广播 SSID，AP 不会定期广播 SSID 信息，无线用户使用无线网卡无法搜索到 SSID，此时无线用户就要手工设置 SSID 才能进入相应的网络。

【命令格式】 **broadcast-ssid**
no broadcast-ssid
【参数说明】 **no**：指的是不广播 SSID。
【缺省配置】 广播 SSID
【命令模式】 WLAN 配置模式
【使用指导】 -

配置组播速率

- 可选配置。
- 若无特殊要求，应在 AP 设备的 WLAN 配置模式下配置。
- 组播速率越高，网络性能越高，但是对信噪比的要求也就越高，远距离无线终端的组播丢包率越高；相反地，组播速率越低，网络性能越低，但是对信噪比的要求也就越低，远距离无线终端的组播丢包率越低。

【命令格式】 **mcast-rate** *mcas-num*
【参数说明】 *mcast-num*：WLAN 组播速率，用户可配置的组播速率为 1 Mbps、6 Mbps、11 Mbps、24 Mbps、54 Mbps。
【缺省配置】 24Mbps
【命令模式】 WLAN 配置模式
【使用指导】 组播速率仅在当前 AP 频段支持下生效，在当前频段不支持该速率情况下，使用缺省速率。

配置 WLAN 下的用户数限制

- 可选配置。
- 应在 AP 设备的 WLAN 配置模式下配置。
- 默认无限制。当 WLAN 上关联的用户数达到限制时，新用户将不能接入该 WLAN。

【命令格式】 **sta-limit** *num*
no sta-limit
【参数说明】 *num* 该 WLAN 下允许接入的最大用户数
【缺省配置】 无限制
【命令模式】 WLAN 配置模式
【使用指导】 -

检验方法

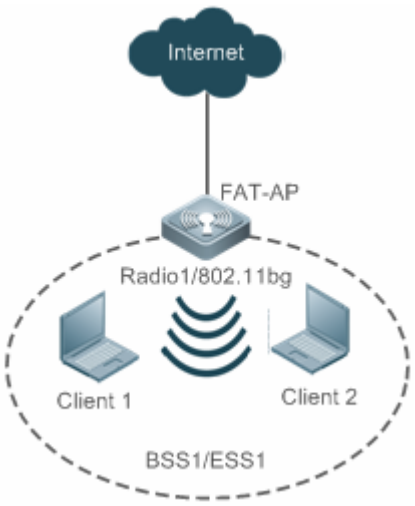
- 通过 **show running-config** 命令可以查看 WLAN 的配置信息。

配置举例

以下配置举例，仅介绍与 WLAN 相关的配置。

配置 WLAN

【网络环境】
图 1-4



【配置方法】
- 在 AP 设备上创建 WLAN ID 为 1 的 WLAN；
- 在 AP 设备上配置 WLAN 1 的 SSID 为 fat_ap；
- 在 AP 设备上配置 WLAN 1 广播 SSID。
- 在 AP 设备上配置 WLAN 1 组播速率为 6Mbps。

FAT-AP

```
Ruijie#config
```

```
Ruijie(config)#dot11 wlan 1
Ruijie(dot11-wlan-config)#ssid fat_ap
Ruijie(dot11-wlan-config)#broadcast-ssid
Ruijie(dot11-wlan-config)#mcast-rate 6
```

【检验方法】 用户配置 WLAN 后，通过显示 WLAN 配置信息进行检验。

- 通过 **show running-config** 命令可以查看 WLAN 的配置信息。

```
Ruijie#show running-config
!
dot11 wlan 1
 mcast-rate 6
 broadcast-ssid
 ssid fat_ap
!
```

常见错误

无。

1.4.2 配置dot11radio子接口

配置效果

- 创建 dot11radio 子接口。
- 配置 dot11radio 子接口属性。

注意事项

- 胖 AP 产品支持。

配置方法

↘ 创建 dot11radio 子接口

- 必须配置，FAT-AP 才能提供 WLAN 服务，使用 **interface dot11radio** 命令可以创建或删除 dot11radio 子接口。
- 若无特殊要求，应在 AP 设备的全局配置模式下配置。

【命令格式】 **interface dot11radio** *interface-num*

【参数说明】 *interface-num*：指定 dot11radio 子接口编号。

【缺省配置】 -

【命令模式】 全局配置模式
【使用指导】 -

配置 dot11radio 子接口封装的 VLAN

- 必须配置。
- 必须配置 dot11radio 子接口封装的 VLAN 属性，FAT-AP 才能正常转发数据；否则，可能导致无线用户可以接入，却无法进行正常通信。使用 **encapsulation dot1Q** 命令可以配置指定 dot11radio 子接口的 VLAN 属性。
- 若无特殊要求，应在 AP 设备的 dot11radio 子接口配置模式下配置。

【命令格式】 **encapsulation dot1Q** *vlan-id*
【参数说明】 *vlan-id*：指定 VLAN ID，或者 VLAN GROUP ID。
【缺省配置】 -
【命令模式】 dot11radio 子接口配置模式
【使用指导】 -

配置映射到 dot11radio 子接口的 WLAN ID

- 必须配置，映射到 dot11radio 子接口的 WLAN ID，FAT-AP 才能提供 WLAN 服务。使用 **broadcast-ssid** 命令可以配置是否广播 SSID。
- 若无特殊要求，应在 AP 设备的 dot11radio 子接口配置模式下配置。

【命令格式】 **wlan-id** *wlan-id*
【参数说明】 *wlan-id*：指定 WLAN ID。
【缺省配置】 -
【命令模式】 dot11radio 子接口配置模式
【使用指导】 -

检验方法

- 通过 **show running-config** 命令可以查看 WLAN 的配置信息。

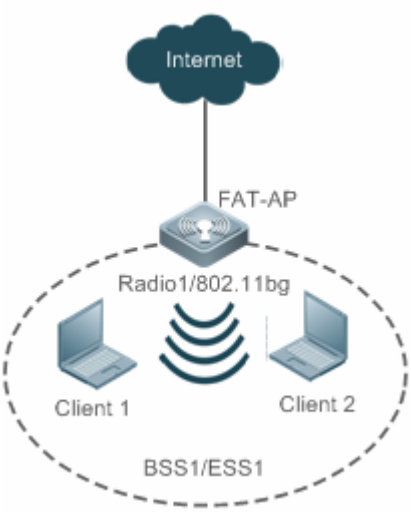
配置举例

以下配置举例，仅介绍与 dot11radio 子接口相关的配置。

配置 dot11radio 子接口

【网络环境】

图 1-5



【配置方法】

- 在 AP 设备上创建编号为 1/0.1 的 dot11radio 子接口；
- 在 AP 设备上配置 dot11radio 1/0.1 封装的 VLAN ID 为 1；
- 在 AP 设备上映射 WLAN 1 到 dot11radio 1/0.1。

FAT-AP

```
Ruijie#config
Ruijie(config)#interface dot11radio 1/0.1
Ruijie(config-subif)#encapsulation dot1Q 1
Ruijie(config-subif)#wlan-id 1
```

【检验方法】 用户配置 dot11radio 子接口后，通过显示 dot11radio 子接口配置信息进行检验。

- 通过 **show running-config** 命令可以查看 dot11radio 子接口的配置信息。

```
Ruijie#show running-config
!
interface Dot11radio 1/0.1
 encapsulation dot1Q 1
 mcast-rate 54
 wlan-id 1
!
```

常见错误

无。

1.4.3 配置无线射频参数

配置效果

- 配置无线射频参数。

注意事项

- 胖 AP 产品支持。

配置方法

配置 DTIM 周期

- 可选配置，使用 **beacon dtim-period** 命令可以配置 DTIM 周期，取值范围为：1~255。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- DTIM 周期越大，节电效果越好，但是下行的多播报文延时越大。

【命令格式】 **beacon dtim-period** *num*
【参数说明】 *num*：指定 DTIM 周期，单位为 1 个 Beacon 帧周期，取值范围 1~255。
【缺省配置】 DTIM 周期为 1 个 Beacon 帧周期间隔
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置启用/禁用 U-APSD 节电模式

- 可选配置，使用 **apsd** 命令可以配置启用/禁用 U-APSD 节电模式。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 启用 U-APSD 节电模式，可以减小实时性要求高的业务在电源管理过程中的延迟，通过关闭大多时候的无线信号的发射，延长了电池的使用时间。

【命令格式】 **apsd** { **enable | disable** }
【参数说明】 **enable**：指定启用 U-APSD 节电模式。
disable：指定禁用 U-APSD 节电模式。
【缺省配置】 启用 U-APSD 节电模式
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置启用/禁用 A-MPDU 聚合方式

- 可选配置，使用 **ampdu** 命令可以配置启用/禁用 A-MPDU 聚合方式。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 启用 A-MPDU 聚合方式，将多个帧聚合到一个帧中传输，从而减少了帧头和帧间隙的数量；另外，由于帧数量的减少，也在总体上降低了冲突的几率。

【命令格式】 **ampdu** { **enable | disable** }
【参数说明】 **enable**：指定启用 A-MPDU 聚合方式。
disable：指定禁用 A-MPDU 聚合方式。

【缺省配置】 启用 A-MPDU 聚合方式
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置 11a 速率集

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 禁用一个速率，将使这个速率不可用；禁用全部速率，将导致无线用户无法接入。

【命令格式】 **rate-set 11a** { **mandatory | support | disable** *speed* }
【参数说明】 **mandatory**：指定是否强制速率。
support：指定是否支持速率。
disable：指定是否禁用速率。
speed：指定速率。
【缺省配置】 6 Mbps、9 Mbps、12 Mbps 是强制速率，其他均为支持速率
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置 11b 速率集

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 禁用一个速率，将使这个速率不可用；禁用全部速率，将导致 11b 的无线用户无法接入。

【命令格式】 **rate-set 11b** { **mandatory** | **support** | **disable** *speed* }
【参数说明】 **mandatory**：指定是否强制速率。
support：指定是否支持速率。
disable：指定是否禁用速率。
speed：指定速率。
【缺省配置】 1 Mbps，2 Mbps，5.5 Mbps，11 Mbps 均为强制速率
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置 11g 速率集

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 禁用一个速率，将使这个速率不可用；禁用全部速率，将导致 11g 的无线用户无法接入。

【命令格式】 **rate-set 11g** { **mandatory** | **support** | **disable** *speed* }
【参数说明】 **mandatory**：指定是否强制速率。
support：指定是否支持速率。
disable：指定是否禁用速率。
speed：指定速率。

【缺省配置】 1 Mbps，2 Mbps，5.5 Mbps，11 Mbps 是强制速率，其他均为支持速率
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置 11n 速率集

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 支持 mcs 越大，可用的速率越高。

【命令格式】 **rate-set 11n** { **mcs-mandatory** | **mcs-support** *index* }
【参数说明】 **mcs-mandatory**：指定是否强制 mcs 速率。
mcs-support：指定是否支持 mcs 速率。
index：指定 mcs 速率。
【缺省配置】 一条流的支持 mcs 为 7、两条流的支持 mcs 为 15、三条流的支持 mcs 为 23，强制 mcs 均为 0
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置 11ac 速率集

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 支持 mcs 越大，可用的速率越高。

【命令格式】 **rate-set 11ac** { **mcs-mandatory** | **mcs-support** *index* }
【参数说明】 **mcs-mandatory**：指定是否强制 mcs 速率。
mcs-support：指定是否支持 mcs 速率。
index：指定 mcs 速率。
【缺省配置】 一条流的支持 mcs 为 9、两条流的支持 mcs 为 19、三条流的支持 mcs 为 29，强制 mcs 均为 0
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置组播速率

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 组播速率越大，发送多播报文的速率越快、占用信道时间越短、信道利用率越高，但是在信道质量不好时发送成功率越低。

【命令格式】 **mcast-rate** {**1** | **6** | **11** | **24** | **54**}
【参数说明】 **1**：指定组播速率为 1Mbps
6：指定组播速率为 6Mbps
11：指定组播速率为 11Mbps
24：指定组播速率为 24Mbps
54：指定组播速率为 54Mbps

【缺省配置】 24Mbps
【命令模式】 dot11radio 接口配置模式
【使用指导】 -

配置发送功率

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 发送功率越大，无线信号的覆盖范围越大，STA 接收到的信号质量越好，但是 FAT-AP 越耗电，不同信道之间的干扰越大。

【命令格式】 **power local** *power-value*
【参数说明】 *power-value*：指定发送功率，单位：%，范围：1~100。
【缺省配置】 100%
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置基于射频口的 STA 数量限制

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 基于射频口的 STA 数量限制越大，可以接入的 STA 越多。

【命令格式】 **sta-limit** *client-num*
【参数说明】 *client-num*：指定 STA 数量，范围：1~128。
【缺省配置】 基于射频口的 STA 数量限制为 32
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置是否支持 11a

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 如果支持 11a，11a 的 STA 可以接入，否则不允许 11a 的 STA 接入。

【命令格式】 **11asupport enable**
no 11asupport enable
【参数说明】 **no**：指定不支持 11a。
【缺省配置】 支持 11a 的 STA 接入
【命令模式】 dot11radio 主接口配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 5G 下生效

配置是否支持 11b

- 可选配置。

- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 如果支持 11b，11b 的 STA 可以接入，否则不允许 11b 的 STA 接入。

【命令格式】 **11bsupport enable**

no 11bsupport enable

【参数说明】 **no**：指定不支持 11b。

【缺省配置】 支持 11b 的 STA 接入

【命令模式】 dot11radio 主接口配置模式

【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效

配置是否支持 11g

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 如果支持 11g，11g 的 STA 可以接入，否则不允许 11g 的 STA 接入。

【命令格式】 **11gsupport enable**

no 11gsupport enable

【参数说明】 **no**：指定不支持 11g。

【缺省配置】 支持 11g 的 STA 接入

【命令模式】 dot11radio 主接口配置模式

【使用指导】 配置仅在 AP 的 Radio 工作在 2.4G 下生效

配置是否支持 11n

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 如果支持 11n，11n 的 STA 可以接入，否则不允许 11n 的 STA 接入。

【命令格式】 **11nsupport enable**

no 11nsupport enable

【参数说明】 **no**：指定不支持 11n。

【缺省配置】 支持 11n 的 STA 接入

【命令模式】 dot11radio 主接口配置模式

【使用指导】 -

配置是否支持 11ac

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 如果支持 11ac，11ac 的 STA 可以接入，否则不允许 11ac 的 STA 接入。

【命令格式】 **11acsupport enable**

no 11acsupport enable

【参数说明】 **no**：指定不支持 11ac。

【缺省配置】 当 Radio 具有 11ac 能力时，默认支持 11ac 的 STA 接入
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置无线用户接入最小 RSSI

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 无线用户接入的 RSSI 越小，可以允许接入的无线用户的 RSSI 就越小，往往表示允许接入的无线用户距离 FAT-AP 的距离就越远。

【命令格式】 **response-rssi** *rssi-value*
【参数说明】 *rssi-value*：指定无线用户接入最小 RSSI，单位：dB，范围为 0~100。
【缺省配置】 无线用户接入最小 RSSI 为 0，即不管无线用户的 RSSI 大小都允许接入
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置无线用户保持接入的最小 RSSI

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 无线用户保持接入的 RSSI 越小，可以保持接入的无线用户的 RSSI 就越小，往往表示允许接入的无线用户距离 FAT-AP 的距离就越远。

【命令格式】 **assoc-rssi** *rssi-value*
【参数说明】 *rssi-value*：指定无线用户保持接入最小 RSSI，单位：dB，范围为 0~100。
【缺省配置】 无线用户保持接入的最小 RSSI 为 0，即不管无线用户的 RSSI 大小都保持接入
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置管理帧发送功率

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 管理帧发送功率越大（0 除外），FAT-AP 的无线用户范围越大，往往表示允许接入的无线用户距离 FAT-AP 的距离就越远。

【命令格式】 **coverage-area-control** *power-value*
【参数说明】 *power-value*：指定管理帧发送功率，单位：dBm，范围 0~32。
【缺省配置】 管理帧发送功率为 0，即不配置管理帧发送功率
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置 STA 空闲时间

- 可选配置。

- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- STA 空闲时间越短，无线用户越容易因为低流量离开无线网络。

【命令格式】 **sta-idle-timeout** *seconds*
【参数说明】 *seconds*：指定 STA 空闲时间，单位：秒，范围：60~86400。
【缺省配置】 STA 空闲时间为 300 秒
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置信道

- 可选配置，使用 **channel** 命令可以配置信道。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 在 2.4GHz 频段中，互相重叠的信道会产生干扰，为避免无线信号冲突，建议将其配置为不重叠的信道(Channel 1、6、11 ）；而 5GHz 频段的 24 个信道（ Channel 36、40、44、48、52、56、60、64、100、104、108、112、116、120、124、128、132、136、140、 149、153、157、161、165 ）在 HT20 下不会互相重叠，也不会产生干扰。

【命令格式】 **channel** *channel-num*
【参数说明】 *channel-num*：指定工作信道。
【缺省配置】 2.4GHz 使用 1 信道，5.8GHz 使用 149 信道
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置分片阈值

- 可选配置，使用 **fragment-threshold** 命令可以配置分片阈值，分片阈值必须为偶数。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 来自较上层的封包以及某些较大型的管理帧可能必须经过分片，无线信道才有办法加以传送。当干扰存在时，分片封包也有助于提升可靠性。利用帧的分片，无线局域网工作站可让干扰只影响较小的帧片段，而非较大的帧。通过降低可能被干扰的数据量，帧分片可以提高整体的有效吞吐量。当干扰存在时，分片阈值越小，抗干扰能力越强。

【命令格式】 **fragment-threshold** *threshold-value*
【参数说明】 *threshold-value*：指定分片阈值，单位：字节，范围：256~2346。
【缺省配置】 分片阈值为 2346 字节
【命令模式】 dot11radio 主接口配置模式
【使用指导】 分片阈值必须为偶数

配置 RTS 阈值

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 当同频干扰存在时，RTS 阈值越小，抗干扰能力越强；但是 RTS/CTS 报文越多，即控制报文的信道占用率越多，无线用户可用的信道带宽越少。

【命令格式】 **rts threshold** *threshold-value*

【参数说明】 *threshold-value*：指定 RTS 阈值，单位：字节，范围：257-2347。
【缺省配置】 RTS 阈值为 2347 字节
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置 Beacon 帧周期

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- Beacon 帧周期越小，发送 Beacon 帧越频繁，无线用户搜索到无线网络的速度越快；但是 Beacon 帧越多，即管理报文的信道占用率越多，无线用户可用的信道带宽越少。Beacon 帧周期不能太大，否则可能导致用户频繁掉线或探测。

【命令格式】 **beacon period** *milliseconds*
【参数说明】 *milliseconds*：指定 Beacon 帧周期，单位：ms，范围：20~1000。
【缺省配置】 Beacon 帧周期为 100 毫秒
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置启用/禁用短前导

- 可选配置。
- 启用短前导可以缩短数据帧的传输时间，从而增加网络的吞吐量。前导码配置仅当 AP 工作在 2.4G 下生效，5G 下默认为长前导，且不允许配置前导码。

【命令格式】 **short-preamble**
no short-preambl
【参数说明】 **no**：指定禁用短前导。
【缺省配置】 禁用短前导
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置启用/禁用短时隙

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 启用短时隙可以减少总体退避时间，从而增加网络的吞吐量。时隙配置仅当 AP 工作在 2.4GHz 下且非 11b 网络下生效，5GHz 下默认为短时隙。

【命令格式】 **slottime** { **long** | **short** }
【参数说明】 **long**：指定使用长时隙。
short：指定使用短时隙。
【缺省配置】 启用短时隙
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置信道带宽

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 信道带宽越大，无线用户可用的信道带宽就越多；但是可配置的信道越少，相邻信道互相干扰的概率越大。

【命令格式】 **chan-width** { **20** | **40** | **80** }
【参数说明】 **20**：指定使用 20MHz 信道带宽。
40：指定使用 40MHz 信道带宽。
80：指定使用 80MHz 信道带宽。
【缺省配置】 信道带宽为 20MHz
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置启用/禁用短防护间隔

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 启用短防护间隔，防护时间由 0.8us 降低为 0.4us，从而增加网络的吞吐量。

【命令格式】 **short-gi enable chan-width** {**20** | **40** | **80**}
no short-gi enable chan-width {**20** | **40** | **80**}
【参数说明】 **no**：指定禁用短防护间隔。
20：指定在 20MHz 信道带宽的情况下启用/禁用短防护间隔。
40：指定在 40MHz 信道带宽的情况下启用/禁用短防护间隔。
80：指定在 80MHz 信道带宽的情况下启用/禁用短防护间隔。
【缺省配置】 20MHz 信道带宽启用短防护间隔，40MHz 信道带宽启用短防护间隔，80MHz 信道带宽禁用短防护间隔
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置无线模式 a/b

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- AP 可支持 2.4GHz 和 5GHz 两个频段的射频传输，用户可以指定 AP 的工作频段。

【命令格式】 **radio-type** { **802.11a** | **802.11b** }
【参数说明】 **802.11a**：指定无线模式为 5GHz。
802.11b：指定无线模式为 2.4GHz。
【缺省配置】 单频 AP（即 Radio 1）支持 2.4GHz 频段，双频 AP 的 Radio 1 支持 2.4GHz，Radio 2 支持 5GHz，三频 AP 的 Radio 1 支持 2.4GHz，Radio 2 支持 5GHz，Radio 3 支持 5GHz
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置国家代码

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 国家代码是用来识别使用射频所在的国家，不同的国家代码规定的射频频段、信道、功率将有所不同。在配置 AP 前，需要先明确该 AP 所支持的国家代码；如果配置的国家代码发生变化，对应的射频频段、信道、功率值也会有所变化。

【命令格式】 **country-code** *country-code*

【参数说明】 *country-code*：指定国家代码。

【缺省配置】 国家代码为“CN”，即中国

【命令模式】 dot11radio 主接口配置模式

【使用指导】 1. 当前可选支持的国家代码有：

国家码	国家
CN	China
US	United States
JP	Japan
ID	Indonesia
IN	India
KR	Korea ROC
MY	Malaysia
RU	Russia
SG	Singapore
HK	Hong Kong
MO	Macau
AU	Australia
TH	Thailand
PK	Pakistan
PH	Philippines
VN	Vietnam
DE	Germany
TR	Turkey
AE	United Arab Emirates

2.4G 的信道 14 只允许在 802.11b 模式下设置。

配置天线接收方式

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- AP 接收使用不同数量的天线，可以使得 AP 在 802.11n 模式下采用双空间流模式或者三空间流模式来接收信号，提升 AP 数据传输的性能。

【命令格式】 **antenna receive** *chain-mask*

【参数说明】 *chain-mask*：指定天线选择掩码，范围：1~7。

【缺省配置】 不同产品型号具有不同天线数目，其缺省天线选择掩码也不同，具体视各产品型号而定
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置天线发送方式

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- AP 发射使用不同数量的天线，可以使得 AP 在 802.11n 模式下采用双空间流模式或者三空间流模式来发射信号，提升 AP 数据传输的性能。

【命令格式】 **antenna transmit** *chain-mask*
【参数说明】 *chain-mask*：指定天线选择掩码，范围：1~7。
【缺省配置】 不同产品型号具有不同天线数目，其缺省天线选择掩码也不同，具体视各产品型号而定
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置启用外置天线

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 相同传输功率下，外置天线比内置天线的传输距离更远。

【命令格式】 **external-antenna enable**
【参数说明】 -
【缺省配置】 启用内置天线，并禁用外置天线
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置 AP 与无线传输对端之间允许的最远距离

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 根据 AP 的 radio 与无线传输对端之间的距离长短适当地调整超时时间；否则将无法进行无线数据传输。但是，超时时间也不能过度地加长；否则当 AP 没有接收到 ACK 帧、CTS 帧时，过度的超时时间会造成空口资源浪费。

【命令格式】 **peer-distance** *val*
【参数说明】 *val*：要配置 AP 允许的最远距离，取值范围为 1000~25000，单位：m
【缺省配置】 1000m
【命令模式】 dot11radio 主接口配置模式
【使用指导】 不支持对所有 AP 进行配置。仅当 AP 与无线传输对端的最远距离大于 1000m 时才需要配置。配置的距离可以偏大但不得小于实际距离。

配置启用/禁用 mcell 功能

- 可选配置。

- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 启用 mcell 功能，接收灵敏度会降低。

【命令格式】 **mcell enable**
no mcell enable
【参数说明】 **no**：关闭 mcell 功能
【缺省配置】 mcell 关闭
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

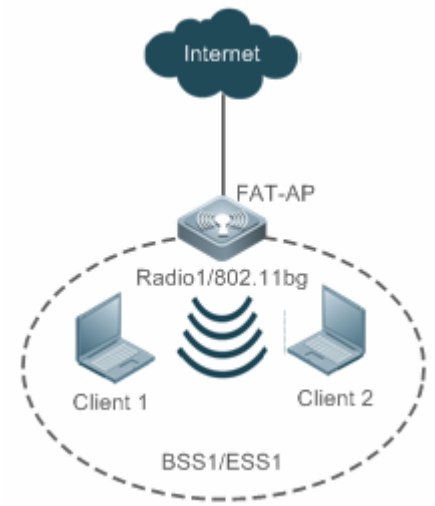
检验方法

- 通过 **show running-config** 命令可以查看射频参数的配置信息。

配置举例

↘ 配置射频参数。

【网络环境】
图 1-6



【配置方法】 ● 在 AP 设备上配置 dot11radio 主接口。

FAT-AP

```
Ruijie#config
Ruijie(config)#interface Dot11radio 1/0
Ruijie(config-if-Dot11radio 1/0)#beacon dtim-period 3
Ruijie(config-if-Dot11radio 1/0)#apsd enable
Ruijie(config-if-Dot11radio 1/0)#ampdu enable
Ruijie(config-if-Dot11radio 1/0)#rate-set 11a mandatory 24
Ruijie(config-if-Dot11radio 1/0)#rate-set 11a support 54
Ruijie(config-if-Dot11radio 1/0)#rate-set 11b disable 1
Ruijie(config-if-Dot11radio 1/0)#rate-set 11b disable 2
```

```
Ruijie(config-if-Dot11radio 1/0)#rate-set 11g disable 1
Ruijie(config-if-Dot11radio 1/0)#rate-set 11g disable 2
Ruijie(config-if-Dot11radio 1/0)#rate-set 11n mcs-mandatory 3
Ruijie(config-if-Dot11radio 1/0)#rate-set 11n mcs-support 15
Ruijie(config-if-Dot11radio 1/0)#mcast-rate 24
Ruijie(config-if-Dot11radio 1/0)#power local 50
Ruijie(config-if-Dot11radio 1/0)#sta-limit 12
Ruijie(config-if-Dot11radio 1/0)#11asupport enable
Ruijie(config-if-Dot11radio 1/0)#11bsupport enable
Ruijie(config-if-Dot11radio 1/0)#11gsupport enable
Ruijie(config-if-Dot11radio 1/0)#11nsupport enable
Ruijie(config-if-Dot11radio 1/0)#11acsupport enable
Ruijie(config-if-Dot11radio 1/0)#response-rssi 20
Ruijie(config-if-Dot11radio 1/0)#assoc-rssi 15
Ruijie(config-if-Dot11radio 1/0)#coverage-area-control 12
Ruijie(config-if-Dot11radio 1/0)#sta-idle-timeout 900
Ruijie(config-if-Dot11radio 1/0)#radio-type 802.11b
Ruijie(config-if-Dot11radio 1/0)#channel 11
Ruijie(config-if-Dot11radio 1/0)#fragment-threshold 1500
Ruijie(config-if-Dot11radio 1/0)#rts threshold 1000
Ruijie(config-if-Dot11radio 1/0)#beacon period 300
Ruijie(config-if-Dot11radio 1/0)#short-preamble
Ruijie(config-if-Dot11radio 1/0)#slottime long
Ruijie(config-if-Dot11radio 1/0)#chan-width 40
Ruijie(config-if-Dot11radio 1/0)#short-gi enable chan-width 20
Ruijie(config-if-Dot11radio 1/0)#short-gi enable chan-width 40
Ruijie(config-if-Dot11radio 1/0)#country-code CNI
Ruijie(config-if-Dot11radio 1/0)#antenna receive 3
Ruijie(config-if-Dot11radio 1/0)#antenna transmit 3
Ruijie(config-if-Dot11radio 1/0)#external-antenna enable
Ruijie(config-if-Dot11radio 1/0)#restries long 4
Ruijie(config-if-Dot11radio 1/0)#restries short 7
Ruijie(config-if-Dot11radio 1/0)#peer-distance 3000
```

【检验方法】 用户配置射频参数后，通过显示 dot11radio 主接口配置信息进行检验。

- 通过 **show running-config** 命令可以查看 dot11radio 主接口的配置信息。

```
Ruijie#show running-config
!
interface Dot11radio 1/0
 ip proxy-arp
 rate-set 11b mandatory 5 11
```

```
rate-set 11b disable 1 2
rate-set 11g mandatory 5 11
rate-set 11g support 6 9 12 18 24 36 48 54
rate-set 11g disable 1 2
rate-set 11a mandatory 6 12 24
rate-set 11a support 9 18 36 48 54
rate-set 11n mcs-support 15
rate-set 11n mcs-mandatory 3
station-role root-ap
beacon period 300
beacon dtim-period 3
slottime long
rts threshold 1000
sta-limit 12
sta-idle-timeout 900
chan-width 40
radio-type 802.11b
antenna receive 3
antenna transmit 3
external-antenna enable
coverage-area-control 12
response-rssi 20
assoc-rssi 15
country-code CNI
power local 50
channel 11
mcast-rate 24
coverage-rssi 10
peer-distance 3000
!
```

常见错误

无。

1.4.4 配置电子书包参数

配置效果

- 可以实现对 AP 及其 Radio 相关电子书包参数设置，方便管理员进行配置管理。

注意事项

- 无。

配置方法

配置 AMPDU 软件重传次数

- 可选配置。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 重传的次数越大，子帧丢失的可能性越低，但是重传次数过多可能造成空口负担增大，造成空气中其他报文的实时性下降，如果需要在子帧丢失概率较大的干扰下确保报文尽可能避免丢失，可以将数值调大。

【命令格式】 **ampdu-retries** *times*
【参数说明】 *times*：软件重传次数，取值范围 1-10
【缺省配置】 重传次数为 4
【命令模式】 dot11radio 主接口配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式下生效。

配置是否开启 AMPDU 聚合报文的 RTS 保护机制

- 可选配置，缺省情况下关闭 AMPDU 聚合报文的 RTS 保护机制。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 只有隐藏节点问题造成的空口资源浪费大于 RTS 交互造成的空口资源浪费时，才开启 AMPDU 的 RTS 保护。

【命令格式】 **ampdu-rts**
【参数说明】 -
【缺省配置】 不开启
【命令模式】 dot11radio 主接口配置模式
【使用指导】 配置仅在 AP 的 Radio 工作在 11N 模式下生效。

配置 AP 以太网单次收包数

- 可选配置，缺省情况下所有不同 AP 的取值是不同的。
- 若无特殊要求，应在 AP 设备的全局配置模式下配置。
- 以太网单次收包数调高能够确保整网性能提升，但是有可能会降低 AP 对关键报文处理的实时性，例如在电子书包等对性能要求不高同时要求多用户并发且对报文实时性要求高的场景下，可以降低以太网单次收包数，此时的建议值为 25。

【命令格式】 **eth-schd** *limit*
【参数说明】 *limit*：以太网单次收包数，范围 1~256
【缺省配置】 -
【命令模式】 全局配置模式
【使用指导】 -

配置是否支持低密度奇偶校验编码

- 可选配置，缺省情况下支持低密度奇偶校验编码。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 如果支持低密度奇偶校验编码，可提高编码的可靠性与编码增益。在受到严重噪杂干扰的频率中使用此技术，可大幅降低资料遗失的风险，但是存在极少量终端在兼容 LDPC 上具备一定问题，表现为丢包。
- 配置 ldpc 表示开启，no ldpc 表示关闭该功能。

【命令格式】 **ldpc**
【参数说明】 -
【缺省配置】 *默认开启*
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

配置是否使能接收发送空时分组码

- 可选配置，缺省情况下使能接收发送空时分组码。
- 若无特殊要求，应在 AP 设备的 dot11radio 主接口配置模式下配置。
- 如果使能接收发送空时分组码，可以提高数据传输的可靠性；但是可能存在部分终端无法有效兼容该编码方式。
- 配置 stbc 表示开启，no stbc 表示关闭该功能。

【命令格式】 **stbc**
【参数说明】 -
【缺省配置】 *默认开启*
【命令模式】 dot11radio 主接口配置模式
【使用指导】 -

一键配置电子书包网优

- 可选配置，没有缺省配置。
- 若无特殊要求，应在 AP 设备的全局配置模式下配置。
- AP320/AP330/AP3220 等产品的优化项是：
- （1）有线口报文处理优化：eth-schd 25
- （2）无线聚合报文重传优化：ampdu-retries 2
- （3）关闭 wifox
- AP530 的优化项是：
- （1）radio 1、2 使用默认的 sta-idle-time 1800
- （2）radio 1 优化：11b/11g 禁用强制速率 1 2 5M，11g 强制速率 11 24M，开启 ampdu-rts
- 配置 ebag 表示开启，no ebag 表示关闭该功能。

【命令格式】 **ebag**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 一般用于电子书包场景中，其他场景慎用！

检验方法

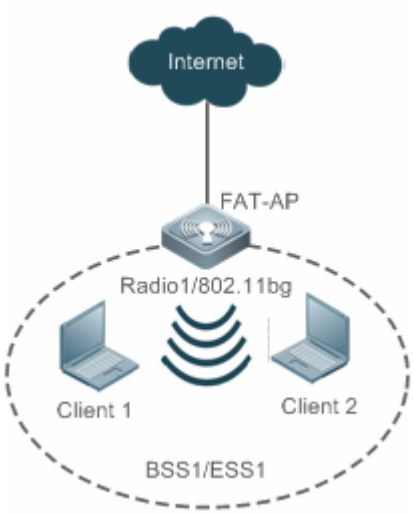
- 通过 **show running-config** 命令可以查看设置的电子书包参数配置。

配置举例

↘ 配置电子书包参数

【网络环境】

图 1-7



假设胖 AP 环境中，在 AP 设备上有以下电子书包参数配置要求：

1、 在 Radio 1 上配置 AMPDU 软件重传次数为 3；

2、 在 Radio 1 上配置开启 AMPDU 聚合报文的 RTS 保护机制；

3、 在 AP 上配置以太网单次收包数为 100；

4、 在 Radio 1 上配置不支持低密度奇偶校验编码；

5、 在 Radio 1 上配置禁用接收发送空时分组码。

【配置方法】

- 在 AP 设备上面配置电子书包参数如下

FAT-AP

```
Ruijie# configure terminal
Ruijie(config)# eth-schd 100
Ruijie(config)# interface dot11radio 1/0
Ruijie(config-if-Dot11radio 1/0)# ampdu-retries 3
Ruijie(config-if-Dot11radio 1/0)# ampdu-rts
Ruijie(config-if-Dot11radio 1/0)# no ldpc
Ruijie(config-if-Dot11radio 1/0)# no stbc
```

【检验方法】

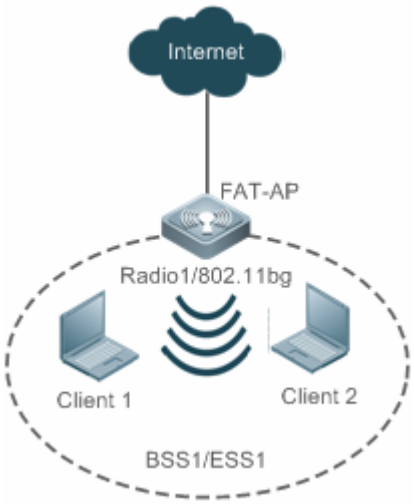
- 通过 **show running-config** 命令可以查看 AP 的电子书包参数配置。

```
Ruijie(config)# show running-config
!
eth-schd 100
!
interface Dot11radio 1/0
 ampdu-retries 3
 ampdu-rts
 no stbc
 no ldpc
!
```

一键配置电子书包网优

【网络环境】

图 1-8



假设胖 AP 环境中，AP 设备工作在电子书包场景。在 AP 设备上有一键配置电子书包网优的要求。

【配置方法】

- 在 AP 设备上一键配置电子书包网优参数如下

FAT-AP

```
Ruijie# configure terminal
Ruijie(config)# ebag
```

【检验方法】

- 通过 **show running-config** 命令可以查看指定 AP 的电子书包参数配置。

```
Ruijie(config)# show running-config
!
eth-schd 25
!
```

```
interface Dot11radio 1/0
 ampdu-retries 2
 no ampdu-rts
!
interface Dot11radio 2/0
 ampdu-retries 2
 no ampdu-rts
!
```

常见错误

- 无。

1.4.5 配置链路完整性检测功能

配置效果

- 开启链路完整性检测功能。

注意事项

- 无。

配置方法

↘ 开启链路完整性检测功能

- 必须配置，使用 **link-check enable** 命令可以打开链路完整性检测功能。

【命令格式】 **link-check enable**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 默认情况下，链路完整性检测功能关闭。

检验方法

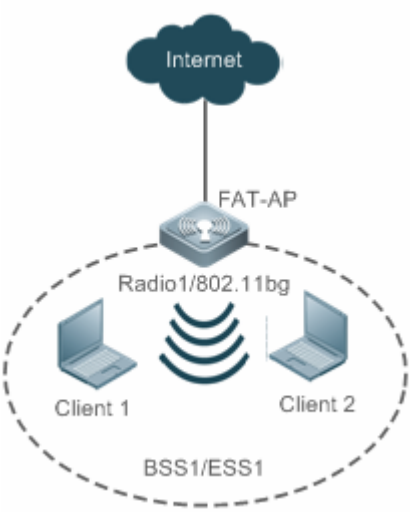
- 通过 **show running-config** 命令可以查看链路完整性检测功能配置状态。

配置举例

↘ 配置链路完整性检测功能

【网络环境】

图 1-9



假设如图胖 AP 环境中，需要打开链路完整性检测功能。

1、打开链路完整性检测功能

【配置方法】

- 在 AP 设备上面配置链路完整性检测功能

FAT-AP

```
Ruijie# configure terminal
Ruijie(config)# link-check enable
```

【检验方法】

- 通过 **show running-config** 命令可以查看。

```
Ruijie(config)# show running-config
.....
link-check enable
.....
```

常见错误

- 无。

1.4.6 一键WLAN配置

配置效果

- 在空配置的设备上，可以快速配置 WLAN 的功能；方便地勘人员快速配置，提高操作效率；方便渠道快速配置 WLAN 来进行性能测试等。

注意事项

- 无。

配置方法

一键配置 WLAN

- 可选配置。
- 在 config 配置模式下使用 **autowifi** 命令一键配置 WLAN，来实现快速配置无线网络。一般用于地勘人员快速配置，提高操作效率；方便渠道快速配置 WLAN 来进行性能测试等。

【命令格式】 **autowifi**

【参数说明】 -

【缺省配置】 -

【命令模式】 AP 的全局配置模式

【使用指导】 在空配置的设备上，为了实现快速配置，提供一键配置 WLAN 的功能。

一般用于地勘人员快速配置，提高操作效率；

方便渠道快速配置 WLAN 来进行性能测试等。

检验方法

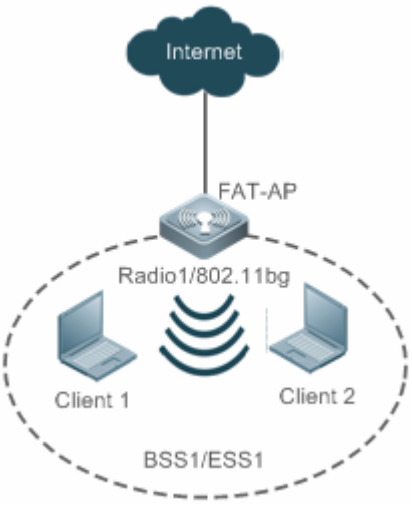
- 通过 **show running-config** 命令可以查看一键 WLAN 配置。

配置举例

一键配置 WLAN

【网络环境】

图 1-10



假设胖 AP 环境中，在 AP 设备上有一键配置 WLAN 的要求。

【配置方法】

- 在 AP 设备上面一键配置 WLAN 如下

FAT-AP

```
Ruijie# configure terminal
Ruijie(config)# autowifi
```

【检验方法】

- 通过 **show running-config** 命令可以查看一键 WLAN 配置。

```
Ruijie#show running-config

fair-schedule
!
spectral
!
cwmp
!
service dhcp
!
ip dhcp pool web_sta_pool_1
 network 192.168.110.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.110.1
!
no service password-encryption
!
dot11 wlan 1
!
link-check disable
!
nfpp
!
wids
!
wlocation
!
vlan 1
!
vlan 10
!
interface GigabitEthernet 0/1
 encapsulation dot1Q 1
!
```

```
interface Dot11radio 1/0
 encapsulation dot1Q 10
 chan-width 20
 country-code CN
 radio-type 802.11b
 channel 1
 antenna receive 3
 antenna transmit 3
 rate-set 11b mandatory 1 2 5 11
 rate-set 11g mandatory 1 2 5 11
 rate-set 11g support 6 9 12 18 24 36 48 54
 rate-set 11n mcs-support 15
 no ampdu-rts
 wlan-id 1
 station-role root-ap
!
interface Dot11radio 2/0
 encapsulation dot1Q 10
 chan-width 20
 country-code CN
 no short-preamble
 radio-type 802.11a
 channel 149
 antenna receive 3
 antenna transmit 3
 rate-set 11a mandatory 6 12 24
 rate-set 11a support 9 18 36 48 54
 rate-set 11n mcs-support 15
 no ampdu-rts
 wlan-id 1
 station-role root-ap
!
interface BVI 1
 ip address 192.168.110.1 255.255.255.0
!
wlansec 1
 security rsn enable
 security rsn ciphers aes enable
 security rsn akm psk enable
 security rsn akm psk set-key ascii autowifi
!
```

```
no offline-detect
!
line console 0
 login
 password admin
line vty 0 4
 privilege level 15
 login
 password admin
!
end
```

1.4.7 配置整机用户数限制

配置效果

- 配置整个胖 AP 允许接入的用户数上限。

注意事项

- 胖 AP 产品支持。

配置方法

↘ 配置整机用户数限制

- 可选配置。

【命令格式】 **sta-limit** *num*

【参数说明】 *num*：AP 整机允许接入的最大用户数。

【缺省配置】 不限制。

【命令模式】 全局配置模式

【使用指导】 应注意整机用户数限制与每个射频口的用户数限制是分开判断的，整机用户数限制并不等于各射频口限制之和。当一个终端接入时，无论整机还是射频口用户数达到限制，都会拒绝接入。

检验方法

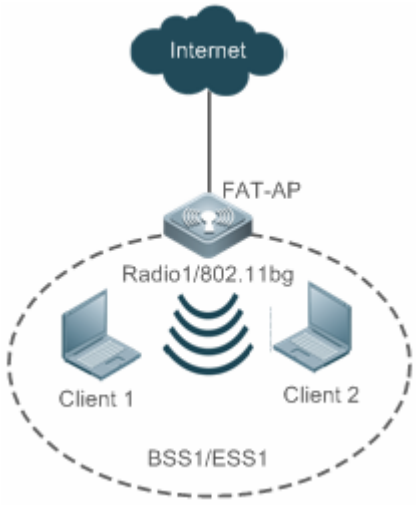
- 通过 **show running-config** 命令可以查看配置信息。

配置举例

↘ 配置整机用户数限制

【网络环境】

图 1-11



【配置方法】

- 配置整机用户数限制为 128 个

FAT-AP

```
Ruijie#config
Ruijie(config)#sta-limit 128
```

【检验方法】

- 通过 **show running-config** 命令可以查看整机用户数限制。

```
Ruijie#show running-config
!
sta-limit 128
!
```

常见错误

在扩大胖 AP 的用户数限制时，可能出现只修改了各射频口的用户数限制、并未修改整机用户数限制的情况，导致仍然无法达到预期的用户数。

1.4.8 配置取消供电限制功能

配置效果

- 供电协商为 15.4W 供电限制情况下，通过配置该命令可以取消供电限制。

注意事项

- 配置这条命令，如果 AP 的功耗大于供电设备输出的功耗，AP 会自动重启。

配置方法

配置 poe-unlimit

- 可选配置。
- 在 config 配置模式下可以取消指定频段射频口的供电限制。
- 在 dot11 radio 主接口配置模式下可以取消指定 radio 的供电限制。

【命令格式】 **poe-unlimit** [**radio-type** { **802.11b** | **802.11a** }]

【参数说明】 在全局配置模式下，需要加 radio-type，在 dot11 radio 主接口配置模式不需要 radio-type

802.11b:表示工作在 2GHz 频段的射频

802.11a:表示工作在 5GHz 频段的射频

【缺省配置】 不限制。

【命令模式】 全局配置模式或 dot11 radio 主接口配置模式

【使用指导】 配置该命令后，如果供电设备输出功耗小于 AP 所需功耗，AP 会重启。

检验方法

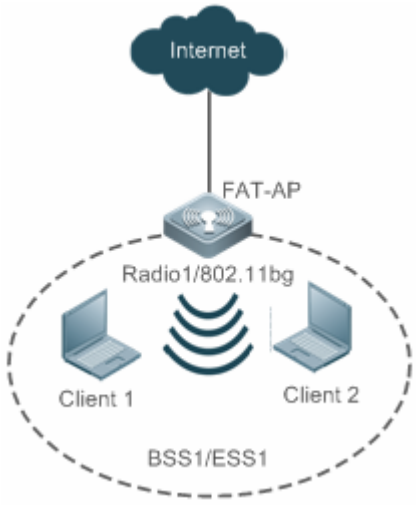
- 通过 **show running-config** 命令可以查看配置信息。

配置举例

配置取消供电限制功能

【网络环境】

图 1-12



【配置方法】

- 配置整机取消供电策略

FAT-AP

```
Ruijie#config
Ruijie(config)# interface dot11radio 2/0
```

```
Ruijie(config-if-Dot11radio 2/0)#poe-unlimit
```

【检验方法】

- 通过 **show running-config** 命令可以查看整机用户数限制。

```
Ruijie#show running-config
!
!
interface Dot11radio 2/0
poe-unlimit
!
```

常见错误

无。

1.4.9 配置启用或禁用供电能力

配置效果

- 配置该命令可以禁用或启用 AP 对外的供电能力。

注意事项

- 胖 AP 支持，且仅限于部分 AP 型号。

配置方法

↘ 配置 poeout

- 可选配置。
- 在 config 配置模式通过该命令禁用或启用 AP 对外的供电能力。

【命令格式】 **poeout { enable | disable | default }**

【参数说明】 **enable:**表示启用 AP 供电能力

disable:表示禁用 AP 供电能力

default:表示使用设备的默认对外供电能力设定

【缺省配置】 使用设备的默认对外供电能力设定

【命令模式】 全局配置模式

【使用指导】 该命令无需使用 write 命令保存，配置后就会保存。该命令不支持 no 和 default 前缀。poeout default 配置后会被转化为设备默认设定的 poeout enable 或 poeout disable。

检验方法

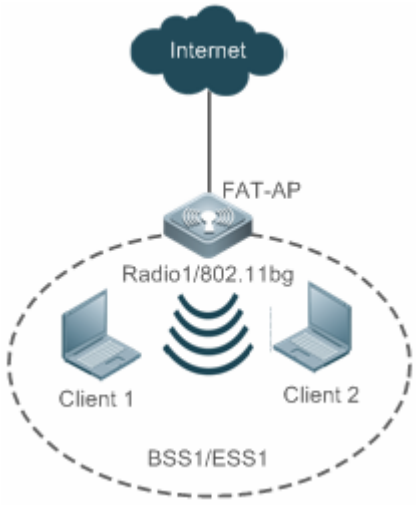
- 通过 **show running-config** 命令可以查看配置信息。

配置举例

↘ 配置启用对外供电能力

【网络环境】

图 1-13



【配置方法】

- 配置整机启用对外供电能力

FAT-AP

```
Ruijie#config
Ruijie(config)#poeout enable
```

【检验方法】

- 通过 **show running-config** 命令可以查看配置的命令

```
Ruijie#show running-config
...
poeout enable
...
```

常见错误

无。

1.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看胖 AP 配置。	**show running-config**
查看无线网卡相关无线信息和配置	**show dot11 wireless** *interface-num*
查看无线网卡连接信息	**show dot11 associations** *H.H.H interface-name*
查看无线网卡连接的所有用户信息	**show dot11 associations all-client**
查看已创建的 BSS 列表	**show dot11 mbssid**
查看所有射频口的在线状态和能力信息	**show dot11 radio-status**
查看所有射频口的速率集信息	**show dot11 rate-set**
查看 WLAN 相关无线信息和配置	**show dot11 wlan** *wlan-id*
查看无线网卡支持的工作信道信息	**show dot11 channels active** *interface-name*
查看无线网卡支持的所有工作信道信息	**show dot11 channels all** *interface-name*
查看电子书包相关无线信息和配置	**show ebag**

查看调试信息

无。

2 WDS

2.1 概述

WDS（Wireless Distribution System，无线分布式系统）是把多个 AP 通过无线桥接或中继的方式相连，从而达到连接分布网络和扩展无线信号的作用。

WDS 有两种工作模式：ROOT-BRIDGE、NONROOT-BRIDGE。

- ROOT-BRIDGE 的有线接口可以连接有线网络；无线接口作为无线网桥，可以连接 Non-root Bridge。
- NONROOT-BRIDGE 的有线接口可以连接有线网络；无线接口作为无线网桥，可以连接 Root Bridge。

协议规范

无。

2.2 典型应用

2.3 功能详解

基本概念

↘ ROOT-BRIDGE

ROOT-BRIDGE 是 WDS 桥接的根节点，ROOT-BRIDGE 允许 NONROOT-BRIDGE 接入建立 WDS 桥接。

↘ NONROOT-BRIDGE

NONROOT-BRIDGE 是 WDS 桥接的非根节点，它会根据用户配置主动接入 ROOT-BRIDGE 建立 WDS 桥接。

功能特性

功能特性	作用
WDS桥接的建立	建立 WDS 桥接
WDS MAC帧地址结构	WDS 桥接，ROOT 端跟 NONROOT 端交互报文的 MAC 帧地址结构

2.3.1 WDS桥接的建立

建立 WDS 桥接

工作原理

每台 AP 相当于一个 BSS（基本服务集），每个 BSS 对应一个 BSSID（通常是该 AP 的 MAC 地址）。AP 定期广播带有 SSID（即无线局域网的名称）和 BSSID 的 beacon 帧，STA 通过扫描监听 Beacon 帧，如果该 Beacon 帧的 SSID 与自己预设的网络名相同，就可以通过接入这个 AP 加入该网络。如果 STA 监听到多个 AP 发送的 Beacon 帧，就选择其中一个 AP 接入。STA 接入 AP 的过程是通过识别该 AP 的 BSSID，并与其进行关联。

而对于 WDS 来说，ROOT-BRIDGE 端会指定一个 BSS 用于 NONROOT-BRIDGE 接入建立桥接使用。该 BSS 就不允许进行普通 STA 用户接入。当这个 BSS 存在时候，就相当于 ROOT-BRIDGE 可以接受 NONROOT-BRIDGE 的接入请求了。接入过程中，ROOT 端会有机制进行判断，该 NONROOT 是否是一个可以接入的 NONROOT-BRIDGE。

对于 NONROOT-BRIDGE 端，会根据用户的配置的 BSSID 或者 SSID 寻找可以接入的 ROOT-BRIDGE，寻找过程会有一个判断机制，指定的 BSSID 或者 SSID 是否是一个可以接入的 ROOT-BRIDGE。判断通过后，就会进行接入处理。处理成功后，WDS 桥接就建立了。

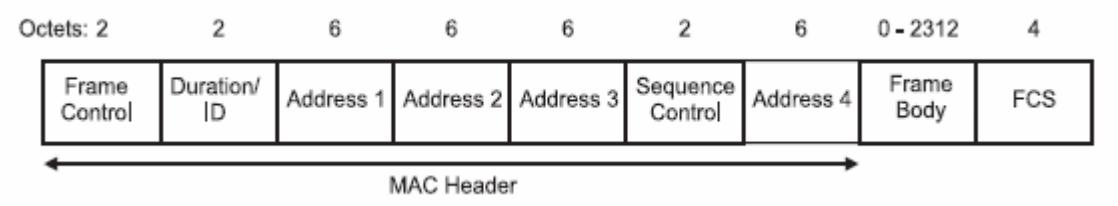
2.3.2 WDS MAC帧地址结构

WDS 桥接，ROOT 端跟 NONROOT 端交互报文的 MAC 帧地址结构。

工作原理

在 IEEE 802.11 标准中，为无线技术定义了一种 MAC 帧格式。其中，MAC 帧头部包含有四个地址字段，如下图所示：

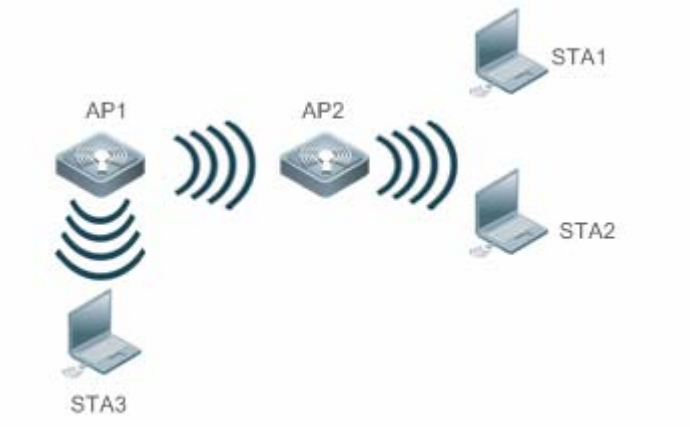
图 2-1



根据 802.11 MAC 帧的传输方式，可以将 MAC 帧的地址结构分为三地址结构和四地址结构。其中，AP 与 STA 之间传输的 MAC 帧采用三地址结构，AP 与 AP 之间传输的 MAC 帧采用四地址结构。

如下图所示，如果 STA 1 与 STA 2 通信，STA 1 发送三地址结构的 MAC 帧给 AP 2，三个地址字段依次填充 AP2、STA 1、STA 2 的 MAC 地址信息（参见表 STA 1->AP 2），AP 2 收到后转发给 STA 2，三个地址字段依次修改为 STA 2、AP 2、STA 1 的 MAC 地址信息（参见表 AP 2->STA 2）；如果 STA 1 与 STA 3 通信，AP 2 收到 STA 1 的 MAC 帧后需要转发给 AP 1，便将三地址结构修改为四地址结构，四个地址字段依次填充为 AP 2、AP 1、STA 3、STA 1 的 MAC 地址信息（参见图 1-4），AP 1 收到后转发给 STA 3，又将四地址结构修改为三地址结构。

图 2-2



传输方式	Address 1	Address 2	Address 3	Address 4
STA 1 -> AP2	RA = AP 2	TA = STA 1	DA = STA 2	N/A
AP 2 -> STA 2	RA = STA 2	TA = AP 2	SA = STA 1	N/A
AP 2 -> AP 1	RA = AP 1	TA = AP 2	DA = STA 3	SA = STA 1

2.4 配置详解

配置项	配置建议&相关命令	
配置WDS基本功能	⚠ 必须配置。用于建立 WDS 桥接。	
	station-role root-bridge bridge-wlan	配置 ROOT-BRIDGE
	station-role non-root-bridge	配置 NONROOT-BRIDGE
	parent	NONROOT 配置要接入的 ROOT 端信息
	⚠ 若 NONROOT 工作在 fit 模式下，必须配置。用于 WDS 预配置。	
	wds pre-config	nonroot 预配置命令

2.4.1 配置WDS基本功能

配置效果

- 配置 WDS 桥接

注意事项

- WDS 应用环境，必须开启 MSTP 功能，防止可能出现的网络环路
- WDS 应用环境，必须关闭 ARP 代理功能
- WDS 配置命令只能建立桥接，必须配合其他命令完成测试环境的搭建，例如创建 BSS，例如有线口配置等等。

配置方法

配置 ROOT-BRIDGE

- 必须配置。
- 胖 AP 在 AP 上配置
- 使用 **station-role root-bridge bridge-wlan** *wlan-id* 命令可以配置 AP 工作在 WDS 桥接 ROOT-BRIDGE 模式下
- 指定的 wlan 是作为桥接 BSS 的 wlan，若该 wlan，用户未创建，则 WDS 桥接未开始工作

【命令格式】 **station-role root-bridge bridge-wlan** *wlan-id*
【参数说明】 **bridge-wlan** *wlan-id*：指定桥接用的 WLAN。
【缺省配置】 root-ap 模式，即普通 AP 模式
【命令模式】 接口配置模式
【使用指导】 -

配置 NONROOT-BRIDGE

- 必须配置。
- 胖 AP 在 AP 上配置
- NONROOT 端必须指定 RADIO 工作在桥接的 NONROOT-BRIDGE 模式下。
- 使用 **station-role non-root-bridge** 命令可以配置 AP 工作在 WDS 桥接 NONROOT-BRIDGE 模式下。
- 必须要指定要接入的 ROOT 端的信息，NONROOT 才会开始开始 WDS 桥接接入处理，才能最终建立桥接

【命令格式】 **station-role non-root-bridge**
【参数说明】 **-**
【缺省配置】 root-ap 模式，即普通 AP 模式
【命令模式】 接口配置模式
【使用指导】 在 NONROOT 模式的 with-client 下，该射频口能够创建的 WLAN 数量视不同的产品而定。

NONROOT 配置要接入的 ROOT 端信息

- 必须配置。
- 胖 AP 在 AP 上配置
- 指定要接入的 ROOT 端有 2 个方式：指定要接入的 ROOT 端的 BSSID、指定要接入的 ROOT 端的 SSID。两个方式任选一个。
- 指定 ROOT 端的 BSSID：适用于固定连接的 ROOT 端。
- 指定 ROOT 端的 SSID：会开启 NONROOT 漫游功能，会选择信号最好的 ROOT 端，进行接入。

- 使用 **parent** { **mac-address** *HHHH.HHHH.HHHH* | **ssid** *ssid* }命令可以指定 NONROOT 要接入的 ROOT 端的 BSSID 或者 SSID。

【命令格式】 **parent** { **mac-address** *HHHH.HHHH.HHHH* | **ssid** *ssid* }

【参数说明】 **mac-address** *HHHH.HHHH.HHHH*：指定要接入的 ROOT 端的 BSSID，定点接入

ssid *ssid*：指定要接入的 ROOT 端的 SSID，会在符合条件的 ROOT 端漫游

【缺省配置】 缺省不配置

【命令模式】 接口配置模式

【使用指导】 NONROOT 端通过该条命令开始寻找 ROOT 端。如果需要使用 WDS 桥接功能，NONROOT 端一定要配置 parent 相关信息。

NONROOT FIT 预配置

- 可选配置。
- 当 NONROOT 需要工作在 FIT 模式下时候，必须在胖 AP 上进行预配置。
- 首先先配置需要的 nonroot 配置（包括配置工作模式为 NONROOT-BRIDGE，指定要接入的 ROOT 端信息等）。
- **show run** 确认配置正确后，执行 **wds pre-config create**，进行预配置创建，然后切换 AP 至瘦模式。

【命令格式】 **wds pre-config** [**create** | **delete**]

【参数说明】 **create**：仅在 AP 上配置的选项，胖 AP 下创建预配置

delete：删除预配置

【缺省配置】 -

【命令模式】 接口配置模式

【使用指导】 若 NONROOT 需要工作在 FIT 模式下时候，必须进行预配置；

首先先配置需要的 nonroot 配置（包括配置工作模式为 NONROOT-BRIDGE，指定要接入的 ROOT 端信息等）；

show run 确认配置正确后，执行 **wds pre-config create**，进行预配置创建，然后切换 AP 至瘦模式; 反过来，如果要退出桥接模式，需要配置 wds pre-config delete 将预配置时创建的 nonroot 配置删除

检验方法

在 AP 上使用 show running-config/ show dot11 wds-bridge-info/show wds-mode 命令可以查看 WDS 信息。

配置举例

无。

常见错误

无

2.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
AP 上查看 WDS 连接信息	**show dot11 wds-bridge-info** *interface-name*

查看调试信息

无

配置指南-接入服务

本分册介绍接入服务配置指南相关内容，包括以下章节：

1. 接口
2. MAC 地址
3. VLAN
4. VLAN-GROUP
5. LLDP
6. PPPOE-CLIENT

1 接口

1.1 概述

接口是网络设备上能够实现数据交换功能的重要部件。我司网络设备上支持两种类型的接口：物理接口和逻辑接口。物理接口意味着该接口在设备上有对应的、实际存在的硬件接口，如：百兆以太网接口、千兆以太网接口等。逻辑接口意味着该接口在路由器上没有对应的、实际存在的硬件接口，逻辑接口可以与物理接口关联，也可以独立于物理接口存在，如：Loopback 接口和 Tunnel 接口等等。实际上对于网络协议而言，无论是物理接口还是逻辑接口，都是一样对待的。

下文仅介绍接口的相关内容。

协议规范

- 无。

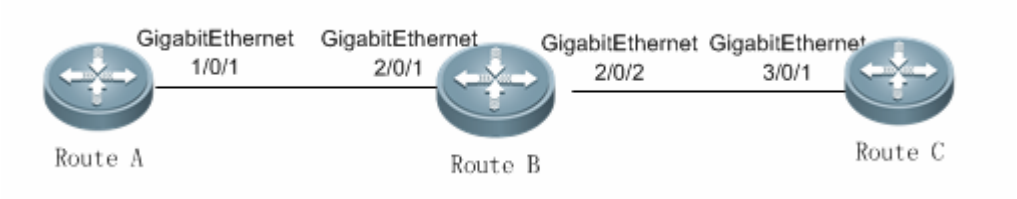
1.2 典型应用

典型应用	场景描述
以太网物理接口路由通信	通过以太网物理接口实现网络设备的三层数据通信。

1.2.1 以太网物理接口路由通信

应用场景

图 1-1



上图中，三台路由器设备 Route A、Route B 和 Route C 组成了一个简单的路由数据通信网络。

【注释】 -

功能部属

- Route A 和 Route B 分别通过千兆以太网物理接口 GigabitEthernet 1/0/1 和 GigabitEthernet 2/0/1 进行相连。

- Route B 和 Route C 分别通过千兆以太网物理接口 GigabitEthernet 2/0/2 和 GigabitEthernet 3/0/1 进行相连。
- 分别给 GigabitEthernet 1/0/1 和 GigabitEthernet 2/0/1 配置相同网段的 IP 地址，其中，GigabitEthernet 1/0/1 的 IP 地址配置为 192.168.1.1/24，GigabitEthernet 2/0/1 的 IP 地址配置为 192.168.1.2/24。
- 分别给 GigabitEthernet 2/0/2 和 GigabitEthernet 3/0/1 配置相同网段的 IP 地址，其中，GigabitEthernet 2/0/2 的 IP 地址配置为 192.168.2.1/24，GigabitEthernet 3/0/1 的 IP 地址配置为 192.168.2.2/24。
- 在 Route C 上配置一条静态路由表项使其能够直通 192.168.1.0/24 网段。
- 在 Route A 和 Route C 上分别执行 ping 192.168.2.2 和 ping 192.168.1.1 操作，可以实现设备 B 上的路由通信功能。

1.3 功能详解

基本概念

↘ 接口类型分类

锐捷 AP 设备的接口类型可分为以下两大类：

- LAN(Local Area Network，局域网)接口
- 逻辑接口

1. 常见的 LAN 接口可分为以下几种类型：

- 以太网端口(FastEthernet、GigabitEthernet)

2. 常见的逻辑接口可分为以下几种类型：

- 子接口
- Loopback 口
- NULL 口
- Tunnel 接口

↘ 以太网端口

以太网端口由设备上的单个物理端口构成，主要用于与局域网内设备通讯。以太网接口有 10M 以太网口和 10M/100M 快速以太网口两种，分别符合 10Base - T，100Base-TX。10Base-T 以太网口工作速率 10Mbits/s，有全双工和半双工两种类型。100Base-TX 兼容于 10Base-T 接口，可以在 10Mbits/s 和 100Mbits/s 的情形下同时工作，同样有全双工和半双工两种类型，并且具有自动协商的特性，可以自动识别其它设备的以太网接口

↘ 子接口

子接口是从单个物理接口上衍生出来并依附于该物理接口的逻辑接口，允许在单个物理接口上配置多个子接口，并为应用提供了高度灵活性。子接口是在一个物理接口上衍生出来的多个逻辑接口，即将多个逻辑接口与一个物理接口建立关联关系，同属于一个物理接口的若干个逻辑接口在工作时共用物理接口的物理配置参数，但又有各自的链路层与网络层配置参数。

Loopback 口

Loopback 接口是完全软件模拟的本地三层逻辑接口，它永远都处于 UP 状态。发往 Loopback 接口的数据包将会在设备本地处理，包括路由信息。Loopback 接口的 IP 地址可以用来作为 OSPF 路由协议的设备标识、实施发向 Telnet 或者作为远程 Telnet 访问的网络接口等等。配置一个 Loopback 接口类似于配置一个以太网接口，可以把它看作一个虚拟的以太网接口。

NULL 口

NULL 口是一个的虚拟接口。该虚拟接口仅仅相当于一个可用的系统设备。NULL(空)永远都处于 UP 状态并且永远不会主动发送或者接受网络数据，任何发往 NULL 接口的数据包都会被丢弃，在 NULL 接口上任何链路层协议封装的企图都不会成功。在 NULL 接口上不能配置任何命令（不包括每一个接口都有的命令 **help** 与 **exit**）。

NULL 接口更多地用于网络数据流的过滤。如果使用空接口，可以通过将不希望处理的网络数据流路由给 NULL 接口而不必使用访问列表。

Tunnel 口

Tunnel 接口来实现隧道功能，允许利用传输协议(如 IP)来传送任意协议的网络数据包。同其它逻辑接口一样，Tunnel 接口也是系统虚拟的接口。Tunnel 接口并不特别指定传输协议或者负载协议，它提供的是一个用来实现标准的点对点的传输模式。由于 Tunnel 实现的是点对点的传输链路，所以对于每一个单独的链路都必须设置一个 Tunnel 接口。

功能特性

功能特性	作用
接口配置命令的使用	进入接口配置模式，在接口配置模式下用户可配置接口的相关属性。对于逻辑口，用户进入接口模式时，如果该接口不存在，将会首先创建出该接口。
接口的描述和管理状态	用户可以为一个接口起一个专门的名字来标识这个接口，有助于用户记住一个接口的功能；用户可以设置接口的管理状态。
接口的MTU	用户可以通过设置端口的 MTU 来控制该端口允许收发的最大帧长。
接口的LinkTrap策略	在设备中可以基于接口配置是否发送该接口的 LinkTrap 信息。
接口索引永久化功能	接口索引永久化功能，即设备重启后接口索引不变。
配置接口带宽	用户可以基于接口配置接口的带宽。
配置接口的Load-interval	用户可以指定每隔多少时间计算报文输入输出的负载情况。
配置接口载波时延	用户可以调整接口的载波时延来调整接口状态从 Down 状态到 Up 状态或者从 Up 状态到 Down 状态的时间延时。
配置VLAN封装标识	用户可以在以太网口或以太网子接口上配置 VLAN 封装标识，接口发报文会封装上用户指定的 VLAN TAG，以便接口能与 VLAN 内设备进行通讯。
接口的速率、双工	用户可以调整接口的速率，双工模式。
模块自动检测	在配置接口速率为自动协商模式的情况下，能够根据插入的模块类型自动调节接口的速率。

1.3.1 接口配置命令的使用

用户可在全局配置模式下使用 **interface** 命令进入接口配置模式。在接口配置模式下用户可配置接口的相关属性。

工作原理

在全局配置模式下输入 **interface** 命令，进入接口配置模式。对于逻辑口，用户进入接口模式时，如果该接口不存在，将会首先创建出该接口。用户也可以在全局配置模式下使用 **interface range** 或 **interface range macro** 命令创建、配置一定范围的接口（接口的编号）。但是定义在一个范围内的接口必须是相同类型和具有相同特性的。

对于逻辑口，可以在全局配置模式下通过执行 **no interface** 或者 **no interface range** 命令删除指定的逻辑接口。

↘ 接口编号规则

对于物理端口，在单机模式下编号由两部分组成：插槽号和端口在插槽上的编号，例如端口所在的插槽编号为 2，端口在插槽上的编号为 3，则端口对应的接口编号为 2/3；在 VSU 模式或者堆叠模式下编号由三部分组成：设备号，插槽号和端口在插槽上的编号，例如设备号为 1，端口所在的插槽编号为 2，端口在插槽上的编号为 3，则端口对应的接口编号为 1/2/3。

设备号是从 1 到支持的成员设备的最大数量。

插槽的编号规则：静态插槽的编号固定为 0，动态插槽（可插拔模块或线卡）的编号是从 1 - 插槽的个数。动态插槽的编号规则是：面对设备的面板，插槽按照从前至后，从左至右，从上至下的顺序一次排列，对应的插槽号从 1 开始依次增加。

插槽上的端口编号是从 1 - 插槽上的端口数，编号顺序是从左到右。

↘ 配置一定范围的接口

用户可以使用全局配置模式下的**interface range**命令同时配置多个接口。当进入**interface range**配置模式时，此时设置的属性适用于所选范围内的所有接口。
输入一定范围的接口。
interface range 命令可以指定若干范围段。
macro 参数可以使用范围段的宏定义，参见配置和使用端口范围的宏定义。
每个范围段可以使用逗号（,）隔开。

同一条命令中的所有范围段中的接口必须属于相同类型。

当使用 **interface range** 命令时，请注意 range 参数的格式：

常见的有效的接口范围格式：

- **FastEthernet** device/slot/{第一个 port} - {最后一个 port}；
- **GigabitEthernet** device/slot/{第一个 port} - {最后一个 port}；
- **Loopback** loopback-ID-loopback-ID，范围是 1～设备支持的最大 Loopback 端口范围；
- **Tunnel tunnel**-ID-tunnel-ID，范围是 1～设备支持的最大 Loopback 端口范围。

在一个 **interface range** 中的接口必须是相同类型的，即或者全是 FastEthernet、GigabitEthernet，或者全是 Loopback 接口等。

配置和使用端口范围的宏定义

用户可以自行定义一些宏来取代端口范围的输入。但在用户使用 **interface range** 命令中的 **macro** 关键字之前，必须先在全局配置模式下使用 **define interface-range** 命令定义这些宏。

在全局配置模式下使用 **no define interface-range** *macro_name* 命令来删除设置的宏定义。

相关配置

配置接口

使用 **interface** 命令可以进入接口配置模式。

配置接口范围

用户可以使用全局配置模式下的 **interface range** 命令同时配置多个接口，这些接口必须是同一类型的接口，比如都是百兆口，或者都是千兆口等。

配置和使用端口范围的宏定义

用户可以自行定义一些宏来取代端口范围的输入，方便用户记忆和区分。在用户使用 **interface range** 命令中的 **macro** 关键字之前，必须先在全局配置模式下使用 **define interface-range** 命令定义这些宏，缺省情况下，没有此项定义。

配置 Loopback 口

缺省情况下，Loopback 口没有被创建。

用户可以在全局配置模式下，使用 **interface** *loopback loopback-interface-number* 命令创建出一个指定的 Loopback 口，其中 *loopback-interface-number* 值范围为 1 到设备支持的最大 Loopback 口数。创建成功后进入该 Loopback 口的接口配置模式。使用 **no interface** *loopback loopback-interface-number* 命令删除一个指定的 Loopback 口。

配置 Tunnel 口

缺省情况下，Tunnel 口没有被创建。

用户可以在全局配置模式下，使用 **interface tunnel** *tunnel-number* 创建出一个指定的 Tunnel 口，其中 tunnel-number 值范围为 1 到设备支持的最大 Tunnel 口数。创建成功后进入该 Tunnel 口的接口配置模式。使用 **no interface** *tunnel tunnel-number* 命令删除一个指定的 Tunnel 口。

1.3.2 接口的描述和管理状态

用户可以为一个接口起一个专门的名字来标识这个接口，有助于用户记住一个接口的功能。

用户可以进入接口模式对接口进行关闭和打开管理。

工作原理

接口的描述

用户可以根据要表达的含义来设置接口的具体名称，比如，用户想将GigabitEthernet 0/1分配给用户A专门使用，用户就可以将这个接口的描述设置为“Port for User A”。

接口的管理状态

在某些情况下，用户可能需要禁用某个接口。用户可以通过设置接口的管理状态来直接关闭一个接口。如果关闭一个接口，则这个接口上将不会接收和发送任何帧，这个接口将丧失这个接口对应的所有功能。用户也可以通过设置管理状态来重新打开一个已经关闭的接口。接口的管理状态有两种：Up 和 Down，当端口被关闭时，端口的管理状态为 Down，否则为 Up。

相关配置

配置接口的描述

缺省情况下，是没有对接口进行描述的。

用户可根据接口的功能对接口进行描述。在接口模式下使用 **description** *string* 命令可以对接口进行描述。

设置接口的管理状态

缺省情况下，接口的管理状态是 Up 的。

用户可根据需要对设置接口的管理状态。在接口模式下使用 **shutdown** 命令可以关闭一个接口，此时接口的管理状态变为 Down 的。使用 **no shutdown** 可以重新打开一个已经关闭的接口。

1.3.3 接口的MTU

用户可以通过设置端口的 MTU 来控制该端口允许收发的最大帧长。

工作原理

当端口进行大吞吐量数据交换时，可能会遇到大于以太网标准帧长度的帧，这种帧被称为 jumbo 帧。MTU 是指帧中有效数据段的长度，不包括以太网封装的开销。

端口收到或者转发的帧，如果长度超过设置的 MTU 将被丢弃。

此配置命令只对物理端口有效。

相关配置

配置接口的 MTU

缺省情况下，接口的 MTU 值一般为 1500 字节。

在接口模式下使用 **mtu** *num* 命令可以设置端口的 MTU。

1.3.4 接口的LinkTrap策略

在设备中，用户可以基于接口配置选择是否发送该接口的 LinkTrap 状态变化信息。

工作原理

当接口的 LinkTrap 发送功能打开时，如果该接口的 Link 状态变化，SNMP 将发出 LinkTrap 信息，反之则不发。

相关配置

↘ 配置接口的 LinkTrap 策略

缺省情况下，该功能打开。

在接口模式下，使用[**no**] **snmp trap link-status** 命令可以打开或者关闭发送该接口 LinkTrap 功能。

1.3.5 接口索引永久化功能

和接口的名字一样，接口索引也可以用于标识一个接口，接口索引是一个接口的“身份 ID”，每个接口创建时，系统会自动为每个接口分配不重复的接口索引值，而当设备重启后，一个接口的索引值可能会和重启前的不一致。接口索引永久化功能，即设备重启后接口索引不变。

工作原理

当配置了该功能，设备重启后相同接口的接口索引值和设备重启前该接口的接口索引值保持不变。

相关配置

↘ 配置接口索引永久化功能

缺省情况下，该功能关闭。

在全局模式下，使用 **snmp-server if-index persist** 命令可以开启接口索引永久化功能。

1.3.6 配置接口带宽

工作原理

主要用于一些路由协议(如 OSPF 路由协议)计算路由量度和 RSVP 计算保留带宽。修改接口带宽不会影响物理接口的数据传输速率。

接口的带宽命令不能实际影响某个接口的带宽，它只是个路由参数，不会影响物理链路的接口的真正带宽。

相关配置

配置接口带宽

缺省情况下，接口带宽值一般和接口类型相匹配，比如对于千兆以太网物理端口，该接口的缺省带宽值为 1000000，万兆以太网物理端口则为 10000000。

在接口配置模式下使用 **bandwidth** *kilobits* 命令来设置接口的带宽，其中 kilobits 为每秒钟带宽，以每秒 K 比特为单位，可配置的范围为 1 到我司设备目前支持的最大以太网速率能力值，比如目前支持最大速率能力值的以太网物理端口为 40G 的物理端口，则带宽参数的最大值为 40000000。使用本命令的 **no bandwidth** 形式来恢复带宽参数的缺省值。

1.3.7 配置接口的Load-interval

工作原理

接口的 load-interval 可以指定每隔多少时间计算报文输入输出的负载情况，一般是每隔 10 秒钟计算一次每秒中输入输出的报文数和比特数。

相关配置

配置接口的 load-interval

缺省情况下，接口的 load-interval 值为 10 秒。

在接口配置模式下使用 **load-interval** *seconds* 命令来设置接口的 load-interval 值，其中 seconds 以秒为单位，可配置的范围为 5 到 600 秒，注意必须是 5 的整数倍。使用本命令的 **no load-interval** 形式来恢复带宽参数的缺省值。

1.3.8 配置接口载波时延

工作原理

接口的载波时延 Carry-delay 是指接口链路的载波检测信号 DCD 从 Down 状态到 Up 状态或者从 Up 状态到 Down 状态的时间延时，如果 DCD 在延时之内发生变化，那么系统将忽略这种状态的变化而不至于上层的数据链路层重新协商。如果参数设置的比较大，那么几乎每次瞬间的 DCD 变化将无法被检测到；相反，如果参数设置成 0，那么每次微小的 DCD 信号的跳变都将被系统检测到，这样系统也就将增加不稳定性。

如果 DCD 载波中断时间比较长，那么将该参数设长些，可以尽快加速拓扑收敛和路由汇聚，以便网络拓扑或者路由表可以较快的收敛。如果相反，DCD 载波中断时间小于网络拓扑或者路由汇聚所花的时间，那么应该将该参数设置相对的大些，以免造成没有必要的网络拓扑振荡或者路由振荡。

相关配置

↘ 配置接口载波时延

缺省情况下，接口的 Carry-delay 值为 2 秒。

在接口配置模式下使用 **carrier-delay** *seconds* 命令来设置接口的 Carry-delay 值，其中 *seconds* 以秒为单位，可配置的范围为 0 到 60。使用本命令的 **no carrier-delay** 形式来恢复接口的 Carry-delay 缺省值。

1.3.9 配置VLAN封装标识

工作原理

VLAN（Virtual Local Area Network）即虚拟局域网，它是在一个物理网络上划分出来的逻辑网络，这个网络对应于 ISO 模型的第二层网络。IEEE 于 1999 年颁布了用以标准化 VLAN 实现方案的 802.1Q 协议标准草案。

VLAN 技术允许网络管理者将一个物理的 LAN 逻辑划分成不同的广播域（或称虚拟 LAN，即 VLAN），每一个 VLAN 都包含一组有着相同需求的计算机工作站，与物理上形成的 LAN 有着相同的属性。但由于它是逻辑划分而不是物理划分，所以同一个 VLAN 内的各个工作站无须被放置在同一个物理空间里，即这些工作站不一定属于同一个物理 LAN 网段。一个 VLAN 内部的广播和单播流量都不会转发到其他 VLAN 中，从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

VLAN 是为解决以太网的广播问题和安全性而提出的一种协议，它在以太网帧的基础上增加了 VLAN 头，用 VLAN ID 把用户划分为更小的工作组，限制不同工作组间的用户二层互访，每个工作组就是一个虚拟局域网。虚拟局域网的好处是可以限制广播范围，并能够形成虚拟工作组，动态管理网络。

为了能与某个 VLAN 内主机进行通讯，用户可以在以太网接口或以太网子接口上配置 802.1Q（VLAN 协议规范）VLAN 封装标志，以太网口在发包的时候，就会封装上相应的 VLAN 头部，在收包的时候，剥离报文的 VLAN 头部。

相关配置

↘ 配置接口的 VLAN 封装标识

缺省情况下，接口没有开启 802.1Q 封装协议。

在接口模式下使用 **encapsulation dot1Q** *VlanID* 命令可以指定接口封装 802.1Q，VlanID 为指定封装的 VLAN 号。

1.3.10 接口的速率、双工

对于以太网物理接口和 AP 口，用户可以配置管理接口的速率、双工。

工作原理

↘ 接口的速率

通常情况下，以太网物理接口速率是通过和对端设备自协商决定的。协商得到的速率可以是接口速率能力范围内的任意一个速率。用户也可以通过配置接口能力范围内的任意一个具体速率值让以太网物理接口工作在该指定速率值上。

对于 AP 口，当用户设置 AP 口的速率时，实际上是生效到该 AP 口的所有成员口上(这些成员口都是以太网物理接口)的。

接口的双工

以太网物理接口和 AP 口的双工模式时存在三种情况：

- 可以将接口设置为全双工属性实现接口在发送数据包的同时可以接收数据包；
- 可以将接口设置为半双工属性控制接口同一时刻只能发送数据包或接收数据包时；
- 当设置接口的双工属性为自协商模式时，接口的双工状态由本接口和对端接口自动协商而定。

对于 AP 口，当用户设置 AP 口的双工模式时，实际上是生效到该 AP 口的所有成员口上(这些成员口都是以太网物理接口)的。

相关配置

设置接口的速率

缺省情况下，接口的速率是自协商模式，即接口的速率配置缺省为 auto 模式。

在接口配置模式下使用 speed { 10 | 100 | 1000 | auto }命令，对接口的速率进行配置。可配置的速率范围为该接口的速率能力范围值，也可以将接口的速率配置为 auto 模式。

设置接口的双工

缺省情况下，接口的双工是自协商模式，即接口的双工配置缺省为 auto 模式。

在接口配置模式下使用 **duplex** { **full** | **half** | **auto** }命令，对接口的双工进行配置。

1.3.11 模块自动检测

在配置接口速率为自动协商模式的情况下，能够根据插入的模块类型自动调节接口的速率。

工作原理

目前支持的模块有 SFP 和 SFP+两种模块，其中 SFP 为千兆模块，SFP+为万兆模块，若插入的是 SFP 模块，则接口工作在千兆模式，若插入的是 SFP+模块，则接口工作在万兆模式。

模块的自动检测功能只在速率配置为自动协商时才能生效。

相关配置

接口速率为自动协商模式

缺省情况下，接口速率为自动协商模式的，模块的自动检测功能也是开启的。但接口速率被设置为任意数值之和，模块的自动检测功能便关闭。

1.4 配置详解

配置项	配置建议 & 相关命令	
接口配置管理	可选配置。主要用于进行接口的创建、删除、接口描述管理等管理配置。	
	interface	创建一个接口（包括子接口），并进入指定接口配置模式，或者直接进入该接口的接口配置模式。
	interface range	输入一定范围的接口，当这些接口未被创建时，同时进行接口创建，并进入接口批量配置模式。
	define interface-range	将批量操作的接口定义成宏定义形式。
	snmp-server if-index persist	开启接口索引永久化功能，即设备重启后接口索引不变。
	description	在接口配置模式下，使用该命令设置接口的描述，最多 32 字符。
	snmp trap link-status	基于接口配置是否发送该接口的 LinkTrap 信息。
	shutdown	在接口配置模式下，使用该命令关闭接口。
配置接口属性	可选配置。主要用于进行接口的属性等管理配置。	
	bandwidth	在接口配置模式下，使用该命令设置接口的带宽参数。
	carrier-delay	在接口配置模式下，使用该命令设置接口载波时延。
	load-interval	在接口配置模式下，使用该命令设置接口的负载计算的间隔时间
	duplex	设置接口的双工模式。
	mtu	设置接口的 MTU。
	speed	设置接口的速率。
	encapsulation dot1Q	设置接口 VLAN 封装标识。

1.4.1 接口配置管理

配置效果

- 能够创建出指定的单个逻辑口，并进入接口的配置模式，或者对于已经存在的物接口或者逻辑接口，可以进入接口的配置模式。
- 能够批量创建出指定的逻辑口，并进入接口批量操作的配置模式，或者对于已经存在的物接口或者逻辑接口，可以进入接口批量操作的配置模式。
- 能够实现相同接口在设备重启前后接口索引保持不变。
- 设置接口的描述符，对该接口直观、形象化的理解。

- 能够启用或者关闭接口的 LinkTrap 功能。
- 配置接口管理状态，关闭或者打开接口。

注意事项

- 无。

配置方法

配置单个指定的接口

- 可选配置。该命令在全局配置模式下配置。
- 可以用于需要创建某个不存在的逻辑接口或者进入已经存在的物理接口和逻辑接口的接口配置模式以进行接口相关的配置时，需要配置该命令。
- 对于逻辑接口，可以使用该命令的 **no** 命令形式进行删除接口，但不可以使用该命令的 **no** 命令形式删除指定的物理接口。
- 可以使用该命令的 **default** 命令形式将指定物理接口或者逻辑接口在接口模式下的相关配置恢复到缺省配置。

配置一定范围的接口

- 可选配置，如果需要设置此功能，则应该执行此配置项。
- 该命令在全局配置模式下配置。
- 可以用于需要批量创建不存在的逻辑接口或者进入已经存在的物理接口和逻辑接口的接口批量配置模式以进行接口相关的配置时，需要配置该命令。
- 对于逻辑接口，可以使用该命令的 **no** 命令形式进行指定范围接口的批量删除，但不可以使用该命令的 **no** 命令形式批量删除指定范围的物理接口。
- 可以使用该命令的 **default** 命令形式将指定范围的接口在接口模式下的相关配置恢复到缺省配置。

配置接口的索引永久化

- 如果需要设置此功能，则应该执行此配置项。
- 该命令在全局配置模式下配置。
- 可以使用该命令的 **no** 命令或者 **default** 命令形式关闭该功能。

配置接口的描述符

- 如果需要设置接口的描述符，则应该执行此配置项。
- 该命令在接口配置模式下配置。
- 可以使用该命令的 **no** 命令或者 **default** 命令形式取消配置接口的描述符。

配置接口的 LinkTrap

- 如果需要设置此功能，则应该执行此配置项。
- 该命令在接口配置模式下配置。
- 可以使用该命令的 **no** 命令或者 **default** 命令形式关闭该功能。

配置接口的管理状态

- 如果需要关闭接口，则应该执行此配置项。
- 该命令在接口配置模式下配置。
- 可以使用该命令的 **no** 命令或者 **default** 命令形式重新打开该接口。

检验方法

配置单个指定的接口

- 执行 **interface** 操作，如果能够正常进入接口模式，即说明配置是成功的。
- 对于逻辑接口，如果是执行 **no interface** 操作，也可以通过 **show running** 命令查看对应的接口是否存在，如果不存在，则该逻辑接口是被正常删除的。
- 执行 **default interface** 操作，通过 **show running** 命令查看对应的接口下的配置是否都恢复到了缺省配置，如果是，则说明该操作是成功的。

配置一定范围的接口

- 执行 **interface range** 操作，如果能够正常进入接口批量配置模式，即说明配置是成功的。
- 对于逻辑接口，如果是执行 **no interface range** 操作，也可以通过 **show running** 命令查看对应的接口是否存在，如果不存在，则这些逻辑接口是被正常删除的。
- 执行 **default interface range** 操作，通过 **show running** 命令查看对应的接口下的配置是否都恢复到了缺省配置，如果是，则说明该操作是成功的。

配置接口索引永久化

- 配置完该命令后，执行 **write** 保存配置操作，重启设备后，通过 **show interface** 命令查看接口的接口索引值，如果对于同一个接口的索引值在设备重启后保持一致，那么说明接口的索引永久化功能是正常的。

配置接口的 LinkTrap

- 选择一个物理端口，进行网线插拔，同时打开 SNMP 服务器，如果在网线插拔的时候，SNMP 服务器能够正常收到该接口的 Link 状态变化的 Trap 信息，则说明该功能是正常的。
- 执行 **no** 命令形式操作，如果验证到在一个物理端口，进行网线插拔，同时打开 SNMP 服务器，如果在网线插拔的时候，SNMP 服务器无法收到该接口的 Link 状态变化的 Trap 信息，则说明已经正常关闭了接口的 LinkTrap 功能。

配置接口的管理状态

- 选择一个物理端口，插上网线，让端口 Up 起来，对该端口执行 **shutdown** 关闭接口的操作，用户在控制台上能够看到端口状态变成管理 Down 的 Syslog 信息，同时该端口上的指示灯灭掉，则关闭端口的功能是正常的。在此基础上，执行 **no**

shutdown 重新打开该接口，用户在控制台上能够看到端口 Up 的 Syslog 信息，同时该端口上的指示灯重新亮起来，则打开端口的功能是正常的。

相关命令

配置单个接口

【命令格式】 **interface** *interface-type interface-number*

【参数说明】 *interface-type interface-number*：即接口的类型和接口编号，可以是以太网物理接口、Loopback 口等。

【命令模式】 全局配置模式

【使用指导】
- 对于逻辑接口，如果该接口未被创建，则首先创建出该接口并进入接口的配置模式。
- 对于物理接口或者已经创建的逻辑接口，直接进入该接口的配置模式。
- 使用 **no** 命令形式删除指定的逻辑接口。
- 使用 **default** 命令形式将该接口的接口模式下配置恢复到缺省配置。

配置一定范围接口

【命令格式】 **interface range** { *port-range* | **macro** *macro_name* }

【参数说明】 *port-range*：即批量操作的接口类型和接口编号范围，可以是以太网物理接口、Loopback 口等。
macro_name：即一定范围接口类型的宏定义名。

【命令模式】 全局配置模式

【使用指导】
- 对于逻辑接口，如果接口未被创建，则首先创建出接口然后再进入接口的批量配置模式。
- 对于物理接口或者已经创建的逻辑接口，直接进入接口的批量配置模式。
- 使用 **no** 命令形式批量删除指定的逻辑接口。
- 使用 **default** 命令形式批量将接口模式下配置恢复到缺省配置。
- 使用宏定义的时候，需要在全局配置模式下，先将一定范围的接口类型通过 **define interface-range** 命令进行宏定义成 *macro_name*，然后再通过 **interface range macro** *macro_name* 进行接口的批量配置管理。

接口索引永久化

【命令格式】 **snmp-server if-index persist**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 执行该命令后，保存配置时将会把当前所有接口的索引保存起来，重启后接口使用重启前分配的接口索引。

配置 LinkTrap 策略

【命令格式】 **snmp trap link-status**

【参数说明】 -

【命令模式】 接口配置模式

【使用指导】 该命令配置是否发送该接口的 LinkTrap，当功能打开时，如果接口的 Link 状态变化，SNMP 将发出 LinkTrap，反之则不发。

配置接口描述符

【命令格式】 **description** *string*

【参数说明】 *string* ：接口别名字符串

【命令模式】 接口配置模式

【使用指导】 该命令进入接口配置模式，下一步就可以修改接口的配置。

配置接口管理状态

【命令格式】 **shutdown**

【参数说明】 -

【命令模式】 接口配置模式

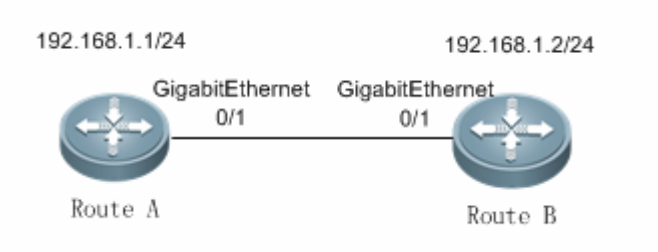
【使用指导】 对接口执行 **shutdown** 操作时，即关闭该接口，执行 **no shutdown** 操作将重新打开该接口。注意有些情况下，不允许将端口执行 **no shutdown** 操作，比如该端口处于端口违例状态，那么该端口将无法执行 **no shutdown** 操作。

配置举例

接口配置管理

【网络环境】

图 1-2



【配置方法】

- 将 2 台设备通过以太网端口进行连接。
- 分别给 2 台设备配置相同网段的 IP 地址。
- 在 2 台设备上分别配置接口索引永久化。
- 在 2 台设备上分别启用 LinkTrap 功能。
- 在两台设备上配置接口管理状态。

A

```
A# configure terminal
A(config)# snmp-server if-index persist
A(config)# interface gigabitethernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 192.168.1.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# snmp trap link-status
A(config-if-GigabitEthernet 0/1)# shutdown
A(config-if-GigabitEthernet 0/1)# end
A# write
```

B

```
B# configure terminal
B(config)# snmp-server if-index persist
B(config)# interface gigabitethernet 0/1
B(config-if-GigabitEthernet 0/1)# ip address 192.168.1.2 255.255.255.0
```

```
B(config-if-GigabitEthernet 0/1)# snmp trap link-status
B(config-if-GigabitEthernet 0/1)# shutdown
B(config-if-GigabitEthernet 0/1)# end
B# write
```

【检验方法】 在 A、B 设备上分别进行如下检验：

- 检查设备上的 GigabitEthern 0/1 在接口 shutdown 操作后的接口状态是否正确
- 检查接口 GigabitEthern 0/1 shutdown 操作后，是否有发出该接口 Link Down 的 Trap 信息
- 重启设备后，接口 GigabitEthern 0/1 的接口索引值是否和重启前的一致

A

```
A# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is administratively down  , line protocol is DOWN
  Hardware is PQ3 TSEC GIGABIT ETHERNET CONTROLLER GigabitEthernet, address is 0a0b.0c0d.0e0e (bia
0a0b.0c0d.0e0e)
  Interface address is: 192.168.1.1/24
  ARP type: ARPA,ARP Timeout: 3600 seconds
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Ethernet attributes:
    Medium-type is Copper
    Last link state change time: 2013-12-20 13:55:20
    Time duration since last link state change: 5 days,  5 hours, 17 minutes, 36 seconds
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
   Rxload is 1/255, Txload is 1/255
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
    4 packets input, 408 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 408 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

B

```
B# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is administratively down  , line protocol is DOWN
```

```
  Hardware is PQ3 TSEC GIGABIT ETHERNET CONTROLLER GigabitEthernet, address is  00d0.f8fb.5945 (bia
00d0.f8fb.5945)
  Interface address is: 192.168.1.2/24
  ARP type: ARPA,ARP Timeout: 3600 seconds
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Ethernet attributes:
    Medium-type is Copper
    Last link state change time: 2013-12-20 13:55:20
    Time duration since last link state change: 5 days,  5 hours, 17 minutes, 36 seconds
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
   Rxload is 1/255, Txload is 1/255
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
    4 packets input, 408 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 408 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

常见错误

- 无。

1.4.2 配置接口属性

配置效果

- 将设备通过路由端口进行连接和数据通信。
- 在设备上分别调整各种接口属性。

注意事项

- 无。

配置方法

配置接口速率

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 接口速率缺省为 auto 模式。

配置接口双工模式

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 接口双工缺省为 auto 模式。

配置接口 MTU

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 一般情况下，接口的 MTU 缺省值为 1500。

配置接口带宽

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 一般情况下，接口的带宽值和接口支持的速率值相同。

配置接口载波时延

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 接口的载波时延缺省值为 2 秒。

配置接口 Load-interval

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 接口的 Load-interval 缺省值为 10 秒。

配置接口 VLAN 封装标识

- 可选配置。如果需要设置此功能，则应该在接口模式下执行此配置项。
- 接口的 VLAN 封装协议默认关闭。

检验方法

- 可以通过 **show interfaces** 命令查看接口的属性配置是否正常。

相关命令

配置接口 MTU

【命令格式】 **mtu** *num*

【参数说明】 *num*：64 - ?(不同产品的最大值不同，由芯片决定)

【命令模式】 接口模式

【使用指导】 设置接口所支持的 MTU，即链路层数据部分的最大长度。目前只支持设置物理端口和包含成员口的 AP 口的 MTU。

配置接口速率

【命令格式】 **speed** [**10** | **100** | **1000** | **auto**]

【参数说明】 **10**：表示接口的速率为 10Mbps。

100：表示接口的速率为 100Mbps。

1000：表示接口的速率为 1000Mbps。

auto：表示接口的速率为自适应的。

【命令模式】 接口模式

【使用指导】 如果接口是聚合端口的成员，则该接口的速率由聚合端口的速率决定。接口退出聚合端口时使用自己的速率设置。使用 **show interfaces** 命令查看设置。接口类型不同，允许设置的速率类型也会有所不同，如 SFP 类型的接口就不允许把速率设为 10M。

配置接口的双工模式

【命令格式】 **duplex** { **auto** | **full** | **half** }

【参数说明】 **auto**：表示全双工和半双工自适应。

full：表示全双工。

half：表示半双工。

【命令模式】 接口模式

【使用指导】 接口的双工属性与接口的类型有关。可以使用 **show interfaces** 命令查看接口双工的设置。

配置接口的载波时延

【命令格式】 **carrier-delay** *seconds*

【参数说明】 *seconds*：以秒为单位，范围 0～60 秒。

【命令模式】 接口配置模式

【使用指导】 -

配置接口的 Load-interval

【命令格式】 **load-interval** *seconds*

【参数说明】 *seconds*：以秒为单位，范围 5-600 秒。

【命令模式】 接口配置模式

【使用指导】 -

配置接口的带宽

【命令格式】 **bandwidth** *kilobits*

【参数说明】 *kilobits*：以以每秒 K 比特为单位，范围为 1 到我司设备目前支持的最大以太网速率能力值。

【命令模式】 接口配置模式

【使用指导】 -

配置接口 VLAN 封装标识

【命令格式】 **encapsulation dot1Q** *VlanID*

【参数说明】 *VlanID*：VLAN ID，范围是 1-4094。

【命令模式】 接口配置模式

【使用指导】 -

配置举例

配置接口属性

【网络环境】

图 1-3

【配置方法】

- 在 Switch A 上配置 GigabitEthernet 0/1 为 Trunk 模式交换端口，配置 SVI 2，并为 SVI2 配置 IP 以及到 Switch B 的路由。
- 在 Route A 上配置 GigabitEthernet 0/1.1 封装 VLAN 标识，VLAN ID 为 2，并配置 IP 地址，配置 Serial 1/0 封装帧中继，并配置另一网段 IP，配置 RIP 路由协议，使其能生成到 Switch B 的路由。
- 在 Route B 上配置 GigabitEthernet 0/1.1 封装 VLAN 标识，VLAN ID 为 2，并配置 IP 地址，配置 Serial 1/0 封装帧中继，并配置另一网段 IP，配置 RIP 路由协议，使其能生成到 Switch A 的路由。
- 在在 Switch B 上配置 GigabitEthernet 0/1 为 Trunk 模式交换端口，配置 SVI 2，并为 SVI2 配置 IP 以及到 Switch A 的路由。

Switch A

```
SA# configure terminal
SA(config)# interface GigabitEthernet 0/1
SA(config-if)# switchport mode trunk
SA(config-if)# exit
SA(config)# interface vlan 2
SA(config-if)# ip address 192.168.1.2 255.255.255.0
SA(config-if)# exit
SA(config)# ip route 0.0.0.0 255.255.255.0 VLAN 1 192.168.1.1
```

Route A

```
RA# configure terminal
RA(config)# interface GigabitEthernet 0/1.1
RA(config-if)# encapsulation dot1Q 2
RA(config-if)# ip address 192.168.1.1 255.255.255.0
RA(config-if)# exit
RA(config)# interface Serial 1/0
RA(config-if)# encapsulation frame-relay
```

```
RA(config-if)# ip address 172.16.1.1 255.255.255.0
RA(config-if)# exit
RA(config)# router rip
RA(config-router)# network 192.168.1.0
RA(config-router)# network 17.16.1.0
RA(config-router)# exit
```

Route B

```
RB# configure terminal
RB(config)# interface GigabitEthernet 0/1.1
RB(config-if)# encapsulation dot1Q 2
RB(config-if)# ip address 192.168.2.1 255.255.255.0
RB(config-if)# exit
RB(config)# interface Serial 1/0
RB(config-if)# encapsulation frame-relay
RB(config-if)# ip address 172.16.1.2 255.255.255.0
RB(config-if)# exit
RB(config)# router rip
RB(config-router)# network 192.168.2.0
RB(config-router)# network 17.16.1.0
RB(config-router)# exit
```

Switch B

```
SB# configure terminal
SB(config)# interface GigabitEthernet 0/1
SB(config-if)# switchport mode trunk
SB(config-if)# exit
SB(config)# interface vlan 2
SB(config-if)# ip address 192.168.2.2 255.255.255.0
SB(config-if)# exit
SB(config)# ip route 0.0.0.0 255.255.255.0 VLAN 1 192.168.2.1
```

【检验方法】 在 Switch A、Switch B、Route A、Route B 四台设备上分别进行如下检验：

- Switch A Ping 其它 3 台设备的接口 IP，两两之间可以相互访问。
- Route A 和 Route B 互 Ping 能通。
- 检查接口状态是否正确。

Switch A

```
SA# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
```

```
  Rxload is 1/255, Txload is 1/255
  Queue     Transmitted packets      Transmitted bytes       Dropped packets         Dropped bytes
      0                       0                       0                     0                     0
      1                       0                       0                     0                     0
      2                       0                       0                     0                     0
      3                       0                       0                     0                     0
      4                       0                       0                     0                     0
      5                       0                       0                     0                     0
      6                       0                       0                     0                     0
      7                     363                   85164                     0                     0
  Switchport attributes:
    interface's description:""
    admin medium-type is Copper, oper medium-type is Copper
    lastchange time:0 Day: 0 Hour: 1 Minute: 9 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Full
    admin speed is AUTO, oper speed is 100M
    flow control admin status is OFF, flow control oper status is OFF
    admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Port-type: trunk
    Native vlan: 1
    Allowed vlan lists: 1-4094
    Active vlan lists: 1-5
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 67 bits/sec, 0 packets/sec
    362 packets input, 87760 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    363 packets output, 82260 bytes, 0 underruns , 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

Route A

```
RA# show interfaces gigabitEthernet 0/1.1
Index(dec):10 (hex):10
GigabitEthernet 0/1 is UP  , line protocol is UP
  Hardware is OCTEON-SGMII GigabitEthernet, address is  00d0.f8fb.5945 (bia  00d0.f8fb.5945)
  Interface address is: 192.168.1.1/24
  ARP type: ARPA,ARP Timeout: 3600 seconds
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is 802.1Q Virtual LAN,Vlan ID 2
```

```
RA# show interface serial 1/0
Index(dec):1 (hex):1
Serial 1/0 is UP , line protocol is UP
  Hardware is Infineon DSCC4 PEB20534 H-10 serial
  Interface address is: 172.16.1.1/24
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is frame-relay, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Queueing strategy: WFQ
  Rxload is 1/255,Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    235 packets input, 434532 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    35 packets output, 36545 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
```

Route B

```
RB# show interfaces gigabitEthernet 0/1.1
Index(dec):10 (hex):10
GigabitEthernet 0/1 is UP  , line protocol is UP
  Hardware is OCTEON-SGMII GigabitEthernet, address is  00d0.f8fb.5946 (bia  00d0.f8fb.5946)
  Interface address is: 192.168.2.1/24
  ARP type: ARPA,ARP Timeout: 3600 seconds
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is 802.1Q Virtual LAN,Vlan ID 2
RB# show interface serial 1/0
Index(dec):1 (hex):1
Serial 1/0 is UP , line protocol is UP
```

```
  Hardware is Infineon DSCC4 PEB20534 H-10 serial
  Interface address is: 172.16.1.1/24
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 2000 Kbit
  Encapsulation protocol is frame-relay, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Queueing strategy: WFQ
  Rxload is 1/255,Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    235 packets input, 434532 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    35 packets output, 36545 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
```

Switch B

```
SB# show interfaces gigabitEthernet 0/1
Index(dec):1 (hex):1
GigabitEthernet 0/1 is UP  , line protocol is UP
Hardware is GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 100000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  Rxload is 1/255, Txload is 1/255
  Queue     Transmitted packets      Transmitted bytes       Dropped packets         Dropped bytes
      0                       0                       0                     0                     0
      1                       0                       0                     0                     0
      2                       0                       0                     0                     0
      3                       0                       0                     0                     0
      4                       0                       0                     0                     0
      5                       0                       0                     0                     0
      6                       0                       0                     0                     0
      7                     363                   85164                     0                     0
```

```
Switchport attributes:
  interface's description:""
  admin medium-type is Copper, oper medium-type is Copper
  lastchange time:0 Day: 0 Hour: 1 Minute: 9 Second
  Priority is 0
  admin duplex mode is AUTO, oper duplex is Full
  admin speed is AUTO, oper speed is 100M
  flow control admin status is OFF, flow control oper status is OFF
  admin negotiation mode is OFF, oper negotiation state is ON
  Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Port-type: trunk
  Native vlan: 1
  Allowed vlan lists: 1-4094
  Active vlan lists: 1-5
 10 seconds input rate 0 bits/sec, 0 packets/sec
 10 seconds output rate 67 bits/sec, 0 packets/sec
  362 packets input, 87760 bytes, 0 no buffer, 0 dropped
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
  363 packets output, 82260 bytes, 0 underruns , 0 dropped
  0 output errors, 0 collisions, 0 interface resets
```

常见错误

无。

1.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除接口的统计值。	**clear counters** [*interface-type interface-number*]
接口硬件复位。	**clearinterface** *interface-type interface-number*

查看运行情况

↘ 显示接口配置和状态

作用	命令

显示指定接口的全部状态和配置信息。	**show interfaces** [*interface-type interface-number*]
查看端口链路状态变化时间和次数。	**show interfaces** [*interface-type interface-number*] **link-state-change statistics**
显示指定接口的描述配置和接口状态。	**show interfaces** [*interface-type interface-number*] **description**
显示指定端口的统计值信息，其中速率显示可能有 0.5%内的误差。	**show interfaces** [*interface-type interface-number*] **counters**
显示上一个采样时间间隔内增加的报文统计值。	**show interfaces** [*interface-type interface-number*] **counters increment**
显示错误报文统计值。	**show interfaces** [*interface-type interface-number*] **counters error**
显示接口报文收发速率	**show interfaces** [*interface-type interface-number*] **counters rate**
显示接口简要统计值	**show interfaces** [*interface-type interface-number*] **counters summary**
显示接口带宽利用率	**show interfaces** [*interface-type interface-number*] **usage**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

无

2 MAC 地址

2.1 概述

MAC 地址表记录了与该设备相连的设备的 MAC 地址、接口号以及所属的 VLAN ID。

设备在转发报文时通过报文的目的 MAC 地址以及报文所属的 VLAN ID 的信息在 MAC 地址表中查找相应的转发输出端口。

根据 mac 地址查找到转发出口后就可以采取单播、组播或广播的方式转发报文。

本文只涉及动态地址、静态地址与过滤地址的管理，组播地址的管理不在本文内描述，请参看《IGMP Snooping 配置指南》。

协议规范

- IEEE 802.3：Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications
- IEEE 802.1Q：Virtual Bridged Local Area Networks

2.2 典型应用

典型应用	场景描述
动态地址学习	通过动态地址学习，实现报文单播转发
MAC地址变化通知	通过 MAC 地址添加删除通知，监控网络设备下用户变化。

2.2.1 动态地址学习

应用场景

通常情况下 MAC 地址表的维护都是通过动态地址学习的方式进行，其工作原理如下：

设备的 MAC 地址表为空的情况下，UserA 要与 UserB 进行通讯，UserA 首先发送报文到交换机的端口 GigabitEthernet 0/2，此时设备将 UserA 的 MAC 地址学习到 MAC 地址表中。

由于地址表中没有 UserB 的源 MAC 地址，因此设备以广播的方式将报文发送到除了 UserA 以外的所有端口，包括 User B 与 User C 的端口，此时 UserC 能够收到 UserA 所发出的不属于它的报文。

图 2-1 动态地址学习步骤一

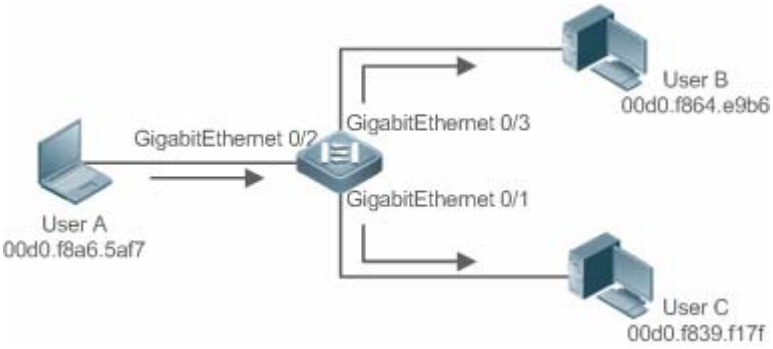


图 2-2 以太网交换 MAC 地址表一

Status	VLAN	MAC地址	端口
动态	1	00d0.f8a6.5af7	GigabitEthernet 0/2

UserB 收到报文后将回应报文通过设备的端口 GigabitEthernet 0/3 发送 UserA，此时设备的 MAC 地址表中已存在 UserA 的 MAC 地址，所以报文被以单播的方式转发到 GigabitEthernet 0/2 端口，同时设备将学习 UserB 的 MAC 地址，与步骤 1 中所不同的是 UserC 此时接收不到 UserB 发送给 UserA 的报文。

图 2-3 动态地址学习步骤二

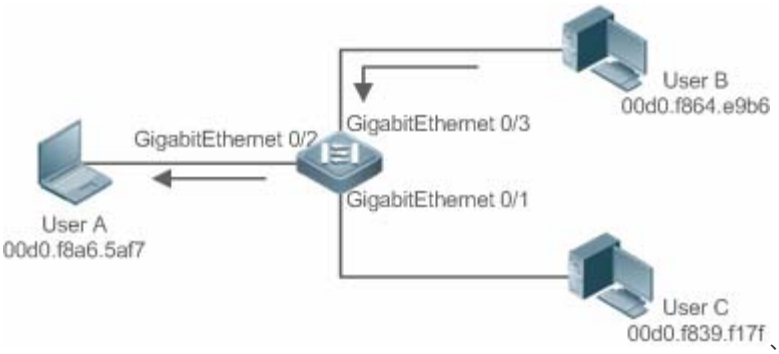


图 2-4 设备 MAC 地址表二

Status	VLAN	MAC地址	端口
动态	1	00d0.f8a6.5af7	GigabitEthernet 0/2
动态	1	00d0.f864.e9b6	GigabitEthernet 0/3

通过 UserA 与 UserB 的一次交互过程后，设备学习到了 UserA 与 UserB 的源 MAC 地址，之后 UserA 与 UserB 之间的报文交互则采用单播的方式进行转发，此后 UserC 将不再接收到 UserA 与 UserB 之间的交互报文。

功能部属

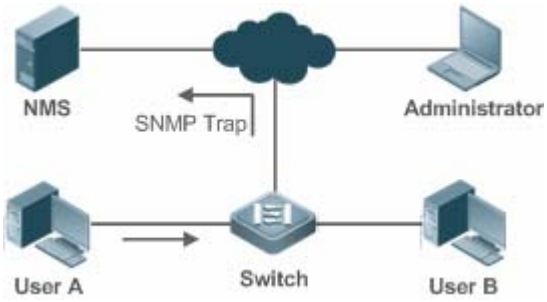
- 二层交换设备通过动态地址学习，实现报文单播转发，减少广播报文，减轻网络不必要的负荷。

2.2.2 MAC地址变化通知

设备的 MAC 地址通知功能通过与网络管理工作站（NMS）的协作为网络管理提供了监控网络设备下用户变化的机制。

应用场景

图 2-5 MAC 地址通知



打开 MAC 地址通知的功能后，当设备学习到一个新的 MAC 地址或老化掉一个已学习到的 MAC 地址时，一个反映 MAC 地址变化的通知信息就会产生，并以 SNMP Trap 的方式将通知信息发送给指定的 NMS(网络管理工作站)。

当一个 MAC 地址增加的通知产生，就可以知道一个由此 MAC 地址标识的新用户开始使用网络，当一个 MAC 地址删除的通知产生，则表示一个用户在地址老化时间内没有新的报文发送，通常可以认为此用户已经停止使用网络了。

当使用设备下接的用户较多时，可能会出现在短时间内会有大量的 MAC 地址变化产生，导致网络流量增加。为了减轻网络负担，可以设置发送 MAC 地址通知的时间间隔。在达到配置的时间间隔之后，系统将这个时间内的所有通知信息进行打包封装，此时在每条地址通知信息中，包含了若干个 MAC 地址变化的信息，从而可以会有效地减少网络流量。

当 MAC 地址通知产生时，通知信息同时会记录到 MAC 地址通知历史记录表中。此时即便没有配置接收 Trap 的 NMS，管理员也可以通过查看 MAC 地址通知历史记录表来了解最近 MAC 地址变化的消息。

MAC 地址通知仅对动态地址有效，对于配置的静态地址与过滤地址的变化将不会产生通知信息。

功能部属

- 二层交换设备开启 MAC 地址变化通知，实现监控网络设备下的用户变化。

2.3 功能详解

基本概念

动态地址

通过设备的自动地址学习过程产生的 MAC 地址表项被称为动态地址。

地址老化

设备的 MAC 地址表是有容量限制的，设备采用地址表老化机制进行不活跃的地址表项淘汰。

设备在学习到一个新的地址的同时启动该地址的老化记时，在达到老化记时前，如果设备没有再一次收到以该地址为源 MAC 地址的报文，那该地址在达到老化时间后会从 MAC 地址表中删除。

单播转发

设备能够在 MAC 地址表中查到与报文的目的 MAC 地址和 VLAN ID 相对应的表项并且表项中的输出端口是唯一的，报文直接从表项对应的端口输出。

广播转发

设备收到目的地址为 ffff.ffff.ffff 的报文或者在 MAC 地址表中查找不到对应的表项时，报文被送到所属的 VLAN 中除报文输入端口外的其他所有端口输出。

2.4 配置详解

配置项	配置建议 & 相关命令	
配置动态地址	⚠ 可选配置。用于实现动态地址学习。	
	mac-address-table aging-time	配置动态地址老化时间
配置静态地址	⚠ 可选配置。用于绑定设备下接的网络设备的 MAC 地址与端口关系。	
	mac-address-table static	配置静态地址
配置过滤地址	⚠ 可选配置。用于过滤报文。	
	mac-address-table filtering	配置过滤地址
配置MAC地址变化通知	⚠ 可选配置。用于监控网络设备下的用户变化。	
	mac-address-table notification	配置全局 MAC 地址变化通知功能
	snmp trap mac-notification	配置接口 MAC 地址变化通知功能

2.4.1 配置动态地址

配置效果

实现动态地址学习，报文正常单播转发。

配置方法

配置动态地址老化时间

- 可选配置。
- 如果需要修改动态地址老化时间，则应该执行此配置项。

【命令格式】 **mac-address-table aging-time** *value*

【参数说明】 *value*：老化时间。取值范围{ 0 | 10 - 1000000 }，缺省值 300 秒。

【缺省配置】 缺省值是 300 秒

【命令模式】 全局模式

【使用指导】 当设置该值为 0 时，地址老化功能将被关闭，学习到的地址将不会被老化。

地址表的实际老化时间会与设定值存在一定偏差，但不会超过设定值的 2 倍。

检验方法

- 检查设备是否能正常学习动态地址。
- 通过 **show mac-address-table dynamic** 命令查看动态地址信息。
- 通过 **show mac-address-table aging-time** 命令查看动态地址老化时间。

【命令格式】 **show mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

【参数说明】 **address** *mac-address*：查看设备上特定动态 MAC 地址信息。

interface *interface-id*：指定的物理接口或是 Aggregate Port。

vlan *vlan-id*：查看特定的 VLAN 中的动态地址。

【命令模式】 特权模式，全局模式，接口模式

【使用指导】 -

【命令展示】

```
Ruijie# show mac-address-table dynamic
Vlan     MAC Address       Type        Interface
----    ------------     ------    ------------------
1      0000.0000.0001      DYNAMIC  GigabitEthernet 1/1
1      0001.960c.a740      DYNAMIC  GigabitEthernet 1/1
1      0007.95c7.dff9      DYNAMIC  GigabitEthernet 1/1
1      0007.95cf.eee0      DYNAMIC  GigabitEthernet 1/1
1      0007.95cf.f41f      DYNAMIC  GigabitEthernet 1/1
1      0009.b715.d400      DYNAMIC  GigabitEthernet 1/1
1      0050.bade.63c4      DYNAMIC  GigabitEthernet 1/1
```

字段解释：

字段	说明
Vlan	MAC 地址所在的 VLAN
MAC Address	MAC 地址
Type	MAC 地址类型
Interface	MAC 地址所在的接口

【命令格式】 **show mac-address-table aging-time**

【参数说明】 -

【命令模式】 特权模式，全局模式，接口模式

【使用指导】 -

【命令展示】

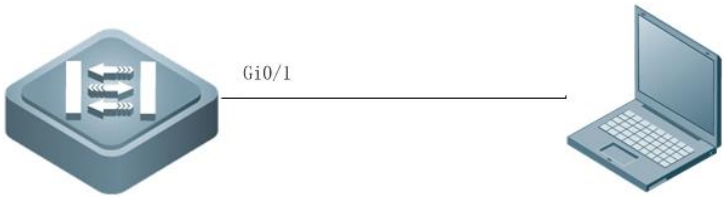
```
Ruijie# show mac-address-table aging-time
Aging time    : 300
```

配置举例

配置动态地址

【网络环境】

图 2-6



【配置方法】

- 配置动态地址老化时间为 180 秒
- 删除接口 GigabitEthernet 0/1 下 VLAN 1 中的所有动态地址

```
Ruijie# configure terminal
Ruijie(config)# mac aging-time 180
Ruijie# clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
```

【检验方法】

- 查看接口 MAC 地址学习能力
- 查询动态地址老化时间
- 查看接口 GigabitEthernet 0/1 下 VLAN 1 中的所有动态地址

```
Ruijie# show mac-address-learning
GigabitEthernet 0/1      learning ability: enable
Ruijie# show mac aging-time
Aging time    : 180 seconds
Ruijie# show mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
Vlan          MAC Address           Type      Interface
----------  -------------------- -------- --------------------
1           00d0.f800.1001       STATIC    GigabitEthernet 1/1
```

常见错误

配置接口地址学习能力时，接口没有先配置成二层接口，包括交换口、AP 口。

2.4.2 配置静态地址

配置效果

- 配置静态地址，绑定设备下接的网络设备的 MAC 地址与端口关系。

配置方法

配置静态地址

- 可选配置。。
- 如果需要绑定设备下接的网络设备的 MAC 地址与端口关系，则应该执行此配置项。

【命令格式】 **mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*

【参数说明】 **address** *mac-address*：指定要删除的 MAC 地址

vlan *vlan-id*：指定要删除的 MAC 地址所在的 VLAN。

interface *interface-id*：指定的物理接口或是 Aggregate Port。

【缺省配置】 缺省没有设置任何静态地址

【命令模式】 全局模式

【使用指导】 当设备在 vlan-id 指定的 VLAN 上接收到以 mac- address 为目的地址的报文时，这个报文将被转发到 interface-id 所指定的接口上。

检验方法

- 通过命令 **show mac-address-table static** 显示静态地址信息是否正确。

【命令格式】 **show mac-address-table static** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

【参数说明】 **address** *mac-address*：查看设备上特定静态 MAC 地址信息。

interface *interface-id*：指定的物理接口或是 Aggregate Port。

vlan *vlan-id*：查看特定的 VLAN 中的静态地址。

【命令模式】 特权模式，全局模式，接口模式

【使用指导】 -

【命令展示】

```
Ruijie# show mac-address-table static
Vlan    MAC Address      Type         Interface
-----  -----------    --------  ------------------
1    00d0.f800.1001    STATIC   GigabitEthernet 1/1
1    00d0.f800.1002    STATIC   GigabitEthernet 1/1
1    00d0.f800.1003    STATIC   GigabitEthernet 1/1
```

配置举例

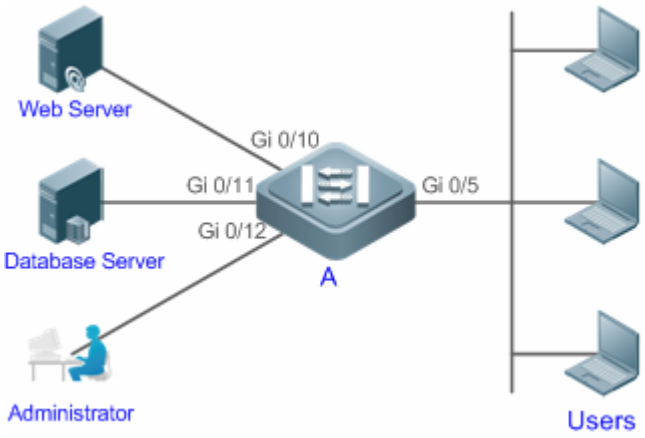
配置静态地址

本例的 MAC 地址同 VLAN、接口对应关系如下表所示：

角色	MAC 地址	VLAN ID	接口 ID
Web 服务器	00d0.3232.0001	VLAN2	Gi0/10
信息服务器	00d0.3232.0002	VLAN2	Gi0/11
网络管理员	00d0.3232.1000	VLAN2	Gi0/12

【网络环境】

图 2-7



【配置方法】

- 指定表项对应的目的 MAC 地址（Mac-address）
- 指定该地址所属的 VLAN（vlan-id）
- 接口 ID（Interface-id）

A

```
A# configure terminal
A(config)# mac-address-table static 00d0.f800.3232.0001 vlan 2 interface gigabitEthernet 0/10
A(config)# mac-address-table static 00d0.f800.3232.0002 vlan 2 interface gigabitEthernet 0/11
A(config)# mac-address-table static 00d0.f800.3232.1000 vlan 2 interface gigabitEthernet 0/12
```

【检验方法】 在交换机上查看配置的静态 MAC 地址

A

```
A# show mac-address-table static
Vlan        MAC Address          Type     Interface
----------  -------------------- -------- ------------------
   2        00d0.f800.3232.0001  STATIC   GigabitEthernet 0/10
   2        00d0.f800.3232.0002  STATIC   GigabitEthernet 0/11
   2        00d0.f800.3232.1000  STATIC   GigabitEthernet 0/12
```

常见错误

- 配置静态地址时，指定接口没有先配置成二层接口，包括交换口、AP 口。

2.4.3 配置过滤地址

配置效果

- 配置过滤地址，当在对应 VLAN 中接收到源 MAC 或目的 MAC 为过滤地址的报文时，将丢弃此报文。

配置方法

配置过滤地址

- 可选配置。。
- 如果需要过滤报文，则应该执行此配置项。

【命令格式】 **mac-address-table filtering** *mac-address* **vlan** *vlan-id*

【参数说明】 **address** *mac-address*：指定要删除的 MAC 地址

vlan *vlan-id*：指定要删除的 MAC 地址所在的 VLAN。

【缺省配置】 缺省没有设置任何过滤地址

【命令模式】 全局模式

【使用指导】 当设备在 vlan-id 指定的 VLAN 上接收到以 mac-address 指定的地址为源地址或目的地址的报文将被丢弃。

检验方法

- 通过命令 **show mac-address-table filter** 显示过滤地址信息。

【命令格式】 **show mac-address-table filter** [**address** *mac-address*] [**vlan** *vlan-id*]

【参数说明】 **address** *mac-address*：查看设备上特定过滤 MAC 地址信息。

vlan *vlan-id*：查看特定的 VLAN 中的过滤地址。

【命令模式】 特权模式，全局模式，接口模式

【使用指导】 -

【命令展示】

```
Ruijie# show mac-address-table filtering
Vlan        MAC Address          Type     Interface
------  -------------------- -------- -----------
1       0000.2222.2222           FILTER
```

配置举例

配置过滤地址

【配置方法】
- 指定过滤地址对应的目的 MAC 地址（Mac-address）
- 指定过滤地址所属的 VLAN（vlan-id）

```
Ruijie# configure terminal
Ruijie(config)# mac-address-table static 00d0.f800.3232.0001 vlan 1
```

【检验方法】 在交换机上查看配置的过滤 MAC 地址

```
Ruijie# show mac-address-table filter
Vlan        MAC Address          Type     Interface
----------  -------------------- -------- --------------------
   1        00d0.f800.3232.0001  FILTER
```

常见错误

无。

2.4.4 配置MAC地址变化通知

配置效果

- 配置 MAC 地址变化通知，监控网络设备下的用户变化。

配置方法

配置接收 MAC 地址通知的 NMS

- 可选配置。
- 如果需要接收 MAC 地址通知，则应该执行此配置项。

【命令格式】 **snmp-server host** *host-addr* **traps** [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*

【参数说明】 **host** *host-addr*：指明接收者的 IP。

version { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }：指明发送哪种版本的 snmp trap 报文，对 v3 版本还可以指定是否认证以及安全等级参数。

community-string：认证名

【缺省配置】 缺省不需要配置

【命令模式】 全局模式

【使用指导】 -

配置使能发送 Trap 功能

- 可选配置。
- 如果需要发送 Trap，则应该执行此配置项。

【命令格式】 **snmp-server enable traps**

【参数说明】 **-**

【缺省配置】 缺省不需要配置

【命令模式】 全局模式

【使用指导】 -

配置全局 MAC 地址通知开关

- 可选配置。
- 全局开关被关闭，所有接口的 MAC 地址通知功能也均被关闭。

【命令格式】 **mac-address-table notification**
【参数说明】 **-**
【缺省配置】 缺省全局 MAC 地址变化通知开关关闭
【命令模式】 全局模式
【使用指导】 -

配置接口 MAC 地址通知开关

- 可选配置
- 如果需要接收接口 MAC 地址变化通知，则应该执行此配置项。

【命令格式】 **snmp trap mac-notification** { **added** | **removed** }
【参数说明】 **added**：当地址增加时通知。
removed：当地址被删除时通知。
【缺省配置】 缺省接口 MAC 地址变化通知开关关闭
【命令模式】 接口模式
【使用指导】 -

配置 MAC 地址通知的时间间隔与历史记录容量

- 可选配置。
- 如果需要修改 MAC 地址通知的时间间隔或历史记录容量，则应该执行此配置项。

【命令格式】 **mac-address-table notification** { **interval** *value* | **history-size** *value* }
【参数说明】 **interval** *value* ：设置产生 MAC 地址通知的时间间隔(可选)。时间间隔的单位为秒，范围为 1 - 3600，缺省为 1 秒。
history-size *value* ：MAC 通知历史记录表中记录的最大个数，范围 1 - 200，缺省为 50。
【缺省配置】 时间间隔缺省为 1 秒，表项默认通告的最大通告个数为 50。
【命令模式】 全局模式
【使用指导】 -

检验方法

- 通过命令 **show mac-address-table notification** 检查 NMS 是否能正常接收 MAC 地址变化通知。

【命令格式】 **show mac-address-table notification** [**interface** [*interface-id*] **| history**]
【参数说明】 **interface :** 显示全部接口上的 MAC 通知功能设置。
interface-id ：查看接口的 MAC 地址变化通知的使能状况。
history：查看 MAC 地址变化通知信息的历史记录表。
【命令模式】 特权模式，全局模式，接口模式

【使用指导】 -

【使用指导】 1、查看 MAC 地址通告功能的全局配置信息

```
Ruijie#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

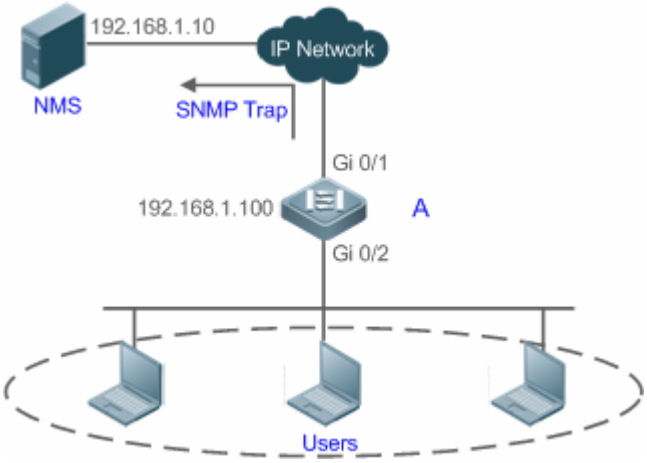
字段解释：

字段	说明
Interval(Sec)	通告 MAC 地址的时间间隔
Maximum History Size	MAC 地址通告历史记录表的最大表项个数
Current History Size	当前记录条目数

配置举例

【网络环境】

图 2-8



图为某企业内部网络示意图。下联用户通过 Gi0/2 口连接到交换机。

为了便于管理员对下联用户使用网络情况信息的掌控，希望通过配置达到以下目的：

- 当交换机下联用户的接口学习到一个新的 MAC 地址或老化掉一个已学习到的地址时，将地址变化信息记录到 MAC 地址通知历史记录表中，供管理员了解最近的 MAC 地址变化信息。
- 同时，交换机能将 MAC 地址变化通知以 SNMP Trap 的方式将通知信息发送给指定的 NMS(网络管理工作站)
- 当交换机下联用户较多时，能尽量避免短时间内产生大量的 MAC 地址变化信息，减轻网络的负担。

【配置方法】

- 打开交换机全局 MAC 地址通知开关，在 Gi0/2 接口上配置 MAC 地址通知功能。
- 配置 NMS 主机地址，使能交换机主动发送 SNMP Trap 通知。交换机到 NMS（网络管理工作站）的路由可达。
- 设置交换机发送 MAC 地址通知的时间间隔为 300 秒（默认时间间隔为 1 秒）。

A

```
Ruijie# configure terminal
```

```
Ruijie(config)# mac-address-table notification
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added
Ruijie(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed
Ruijie(config-if-GigabitEthernet 0/2)# exit
Ruijie(config)# snmp-server host 192.168.1.10 traps version 2c comefrom2
Ruijie(config)# snmp-server enable traps
Ruijie(config)# mac-address-table notification interval 300
```

【检验方法】

- 查看 MAC 地址通知功能的全局配置信息。
- 查看接口的 MAC 地址变化通知的使能状况。
- 查看接口 MAC 地址表，并使用使用 **clear mac-address-table dynamic** 命令模拟动态地址的老化。
- 查看 MAC 地址通知功能的全局配置信息。
- 查看 MAC 地址变化通知信息的历史记录表。

A

```
Ruijie# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
Ruijie# show mac-address-table notification interface GigabitEthernet 0/2
Interface               MAC Added Trap     MAC Removed Trap
-----------             --------------     --------------
GigabitEthernet 0/2    Enabled            Enabled
Ruijie# show mac-address-table interface GigabitEthernet 0/2
Vlan        MAC Address          Type     Interface
----------  -------------------- -------- --------------------
   1        00d0.3232.0001       DYNAMIC  GigabitEthernet 0/2
Ruijie# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 1
Ruijie# show mac-address-table notification history
History Index : 0
Entry Timestamp: 221683
MAC Changed Message :
Operation:DEL Vlan:1 MAC Addr: 00d0.3232.0003 GigabitEthernet 0/2
```

常见错误

无。

2.5 监视与维护

清除各类信息

在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除动态地址表项。	**clear mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

查看运行情况

作用	命令
查看 MAC 地址表。	**show mac-address-table** { **dynamic** | **static** | **filter** } [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
查看动态地址老化时间	**show mac-address-table aging-time**
查看地址变化通知配置及历史记录表	**show mac-address-table notification** [**interface** [*interface-id*] **| history**]

查看调试信息

输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 MAC 运行情况的调试开关。	**debug bridge mac**

3 VLAN

3.1 概述

VLAN 是虚拟局域网(Virtual Local Area Network)的简称，它是在一个物理网络上划分出来的逻辑网络。这个网络对应于 ISO 模型的第二层网络。

VLAN 有着和普通物理网络同样的属性，除了没有物理位置的限制，它和普通局域网一样。第二层的单播、广播和多播帧在一个 VLAN 内转发、扩散，而不会直接进入其他的 VLAN 之中。

可以把一个端口定义为一个 VLAN 的成员，所有连接到这个特定端口的终端都是虚拟网络的一部分，并且整个网络可以支持多个 VLAN。当在 VLAN 中增加、删除和修改用户的时候，不必从物理上调整网络配置。VLAN 之间的通讯必须通过三层设备，

协议规范

- IEEE 802.1Q

3.2 典型应用

无。

3.3 功能详解

基本概念

VLAN

VLAN 是虚拟局域网（Virtual Local Area Network）的简称，它是在一个物理网络上划分出来的逻辑网络。VLAN 有着和普通物理网络同样的属性，除了没有物理位置的限制，它和普通局域网一样。第二层的单播、广播和多播帧在一个 VLAN 内转发、扩散，而不会直接进入其他的 VLAN 之中。

产品支持的 VLAN 遵循 IEEE802.1Q 标准，最多支持 4094 个 VLAN(VLAN ID 1-4094)，其中 VLAN 1 是不可删除的默认 VLAN。

许可配置的 VLAN ID 范围为 1-4094。

当硬件资源不足的情况下，系统将返回创建 VLAN 失败信息。

3.4 配置详解

配置项	配置建议 & 相关命令	
配置基本VLAN	⚠ 必选配置。 用于创建 VLAN，加入 ACCESS 模式接口。	
	vlan	输入一个 VLAN ID。
	⚠ 可选配置，用于 VLAN 重命名。	
	name	为 VLAN 取一个名字。

3.4.1 配置基本VLAN

配置效果

- 一个 VLAN 是以 VLAN ID 来标识的。在设备中，您可以添加、删除、修改 VLAN 2-4094，而 VLAN 1 是由设备自动创建，并且不可被删除。可以在接口配置模式下配置一个端口的 VLAN 成员类型或加入、移出一个 VLAN。

注意事项

- 无

配置方法

↘ 创建、修改一个 vlan

- 必须配置。
- 当硬件资源不足的情况下，系统将返回创建 VLAN 失败信息。
- 使用 **vlan** *vlan-id* 命令添加一个新的 VLAN 或者进入 VLAN 模式。

【命令格式】 **vlan** *vlan-id*

【参数说明】 *vlan-id*: VLAN vid，范围为 1-4094

【缺省配置】 VLAN 1 由设备自动创建，并且不可被删除

【命令模式】 全局配置模式

【使用指导】 如果输入的是一个新的 VLAN ID，则设备会创建一个 VLAN，如果输入的是已经存在的 VLAN ID，则修改相应的 VLAN。使用 **no vlan** *vlan-id* 命令可以删除 vlan，其中不允许删除的 VLAN 有：默认 VLAN1、配置 SVI 的 VLAN、SUBVLAN 等。

↘ vlan 重命名

- 可选配置。
- 用户不能将 VLAN 重命名为其他 VLAN 的缺省名字。

【命令格式】 **name** *vlan-name*

【参数说明】 *vlan-name*：要重新命令的 VLAN 名字

【缺省配置】 缺省情况下，VLAN 的名称为该 VLAN 的 VLAN ID。比如，VLAN 0004 就是 VLAN 4 的缺省名字。

【命令模式】 VLAN 配置模式

【使用指导】 如果想把 VLAN 的名字改回缺省名字，只需输入 **no name** 命令即可

检验方法

- 使用命令 **show vlan 和 show interface switchport** 查看配置显示是否生效。

【命令格式】 **show vlan** [**id** *vlan-id*]

【参数说明】 *vlan-id* ：VLAN ID 号

【命令模式】 所有模式

【使用指导】 -

【命令展示】

```
Ruijie(config-vlan)#show vlan id 20
VLAN Name                              Status    Ports
---- --------------------------------- --------- ----------------------------------
  20 VLAN0020                          STATIC    Gi0/1
```

配置举例

基本 VLAN 配置

以下配置举例，仅介绍 VLAN 相关的配置。

【配置方法】

- 创建一个新 VLAN，并且重命名

```
Ruijie# configure terminal
Ruijie(config)# vlan 888
Ruijie(config-vlan)# name test888
```

【检验方法】 **show** 显示是否正确

```
Ruijie(config-vlan)#show vlan
VLAN Name                              Status    Ports
---- --------------------------------- --------- ----------------------------------
   1 VLAN0001                          STATIC
  20 VLAN0020                          STATIC    Gi0/3
 888 test888                           STATIC
```

3.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 VLAN 配置	**show vlan**

查看调试信息

输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 VLAN 的调试开关。	**debug bridge vlan**

4 VLAN-GROUP

4.1 概述

VLAN-Group 功能，指每个 VLAN-Group 中包含多个 VLAN，将 WLAN 与 VLAN- Group 进行关联，实现 WLAN 与 VLAN 的 1:N 映射，为接入 WLAN 的 STA 进行灵活的 VLAN 分配。

VLAN 分配模式，主要如下：

- STA 通过 802.1x 认证后，由认证服务器为 STA 分配相应的 VLAN。

本文只介绍 VLAN-Group 相关的内容。

协议规范

- 无

4.2 典型应用

无。

4.3 功能详解

基本概念

VLAN-Group

将多个 VLAN 加入同一 VLAN-Group 中，当 STA 接入 WLAN 时，根据当前 WLAN 映射 VLAN-Group 的 VLAN 分配模式，为 STA 进行 VLAN 分配。

VLAN 分配模式

每个 VLAN-Group 进行 VLAN 分配的方式，可以根据 802.1x 下发 VLAN 进行分配。

功能特性

功能特性	作用
VLAN-Group通过 802.1X下发VLAN	用户可规划 STA 通过 802.1X 认证后，分配的 VLAN

4.3.1 VLAN-Group通过 802.1X下发VLAN

工作原理

用户认证通过前，用户所属 VLAN 为当前接入 WLAN 对应 VLAN-Group 的默认 VLAN。

STA 在默认 VLAN 中进行认证，认证通过后，由认证服务器进行 VLAN 下发，如果认证服务器有下发 VLAN，该 STA 后续发出的报文，将被自动跳转到下发 VLAN 中，如果认证服务器没有下发 VLAN，该 STA 后续发出的报文，在 VLAN-Group 的默认 VLAN 中传输。

相关配置

↘ 配置 VLAN 分配模式为 802.1X

缺省情况下，VLAN-Group 的 VLAN 没有分配模式。

使用 **vlan-assign-mode dot1x** 命令配置 VLAN 分配模式为 802.1x 模式。

↘ 配置 VLAN-Group 的默认 vlan

使用 **default-vlan XX** 命令配置 VLAN-Group 的默认 vlan 为 XX。

4.4 配置详解

配置项	配置建议 & 相关命令	
配置VLAN-Group	⚠ 必须配置。用于创建 VLAN_Group、配置 VLAN-LIST、VLAN 分配模式、创建 Default VLAN。	
	vlan-group group-id	创建 vlan-Group
	vlan-list vlan-list	配置 VLAN-Group 的 VLAN 集合
	vlan-assign-mode XX	配置 VLAN-Group 的 VLAN 分配模式
	default-vlan XX	配置 VLAN-Group 的 default vlan
配置WLAN与VLAN-Group映射	⚠ 必须配置。用于 WLAN 和 VLAN-GROUP 映射。	
	dot11 wlan wlan-id **vlan-group group-id**	AP 上配置 WLAN 和 VLAN-Group 关联

4.4.1 配置VLAN-Group

配置效果

- 创建 VLAN-Group 以及实现 VLAN-Group 下的相关配置。

配置方法

创建 vlan-Group

- 必须配置。

配置 VLAN-Group 的 VLAN 集合

- 必须配置，确保 VLAN 以及创建。

配置 VLAN-Group 的 VLAN 分配模式

- 必须配置，确保 VLAN-Group 分配 VLAN 的策略。

配置 VLAN-Group 的 default vlan

- 802.1X 模式下必须配置。
- 配置的 default vlan，确保已经在 VLAN-Group 的 vlan 集合中。

检验方法

- 查看 VLAN-Group 的表项配置。

相关命令

无

配置举例

配置 VLAN-Group

【配置方法】
- 创建 VLAN-Group 10
- 配置 VLAN 分配模式为 dot1X 模式
- 配置 VLAN 集合为 1-10
- 配置 default vlan 为 1

```
Ruijie# configure terminal
Ruijie(config)# vlan-group 10
Ruijie(config-vlan-group)# vlan-assign-mode dot1x
Ruijie(config-vlan-group)# vlan-list 1-10
Ruijie(config-vlan-group)# default-vlan 1
Ruijie(config-vlan-group)# end
```

【检验方法】
- 查看 VLAN-Group 10 的配置是否正确

```
Ruijie#show vlan-group 10
vlan-group id       mode        default-vlan vlan-list
```

```
------------ ----------------- ------------ --------------------------
10           dot1x             1            1-10
```

常见错误

- 配置的 VLAN 集合的 VLAN 没有创建。
- 配置的 default　vlan 没在 VLAN 集合中。

⚠ VLAN-Group 的创建范围为：[1～128]。

⚠ VLAN-Group 支持最大 VLAN 成员数量为 128。

4.4.2 配置WLAN与VLAN-Group映射

配置效果

- WLAN 和 VLAN-Group 关联，STA 可以关联 WLAN。

配置方法

↘ 配置 WLAN 和 VLAN-Group 映射

- 必须配置。

检验方法

- 检查 WLAN 和 VLAN-Group 映射是否正确。

相关命令

无

配置举例

↘ 配置 WLAN 和 VLAN-Group 关联

【配置方法】
- 创建 WLAN
- 配置当前 WLAN 与 VLAN-Group 的映射关系
- 为无线子接口配置 VLAN-Group 封装

```
Ruijie(config)# dot11 wlan 100
Ruijie(dot11-wlan-config)# vlan-group-id 100
```

```
Ruijie(dot11-wlan-config)# end
Ruijie(config)# interface dot11radio 1/0.1
Ruijie(config-subif)# encapsulation dot1Q group 10
Ruijie(config-subif)# end
Ruijie(config)# interface dot11radio 1/0
Ruijie(config-if-Dot11radio 1/0)# wlan-id 100
```

【检验方法】 ● show runing 查看配置是否正确

常见错误

- 无。

4.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 VLAN-Group 信息	**show vlan-group** [*group-id*]

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 VLAN-Group 运行情况的调试开关	**debug bridge vgoup**

5 LLDP

5.1 概述

LLDP（Link Layer Discovery Protocol，链路层发现协议）是由 IEEE 802.1AB 定义的一种链路层发现协议。通过 LLDP 协议能够进行拓扑的发现及掌握拓扑的变化情况。LLDP 将设备的本地信息组织成 TLV 的格式(Type/Length/Value，类型/长度/值）封装在 LLDPDU（LLDP data unit，链路层发现协议数据单元）中发送给邻居设备，同时它将邻居设备发送的 LLDPDU 以 MIB（Management Information Base，管理信息库）的形式存储起来，提供给网络管理系统访问。

通过 LLDP，网络管理系统可以掌握拓扑的连接情况，比如设备的哪些端口与其它设备相连接，链路连接两端的端口的速率、双工是否匹配等，管理员可以根据这些信息快速地定位及排查故障。

一台支持 LLDP 协议的锐捷交换机产品，当对端设备是支持 LLDP 协议的锐捷交换机产品，或支持 LLDP-MED 协议的终端设备的时候，该产品可以发现邻居信息。

- 支持 LLDP 协议的锐捷交换机产品。
- 支持 LLDP-MED 协议的终端设备。

协议规范

- IEEE 802.1AB 2005：Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057：Link Layer Discovery Protocol for Media Endpoint Devices

5.2 典型应用

典型应用	场景描述
利用LLDP查看拓扑连接情况	网络拓扑中有若干交换机设备、MED 设备、NMS 设备。
利用LLDP进行错误检测	网络拓扑中有直连的两台交换机设备，错误配置信息将显示。

5.2.1 利用LLDP查看拓扑连接情况

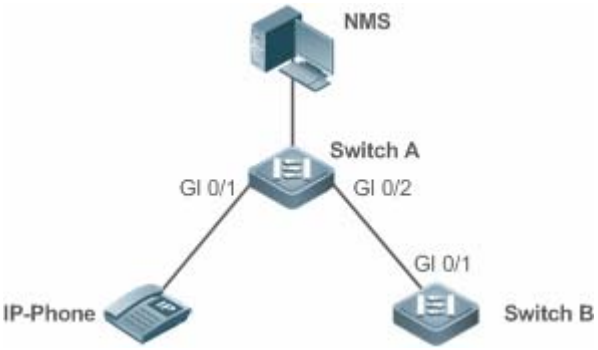
应用场景

网络拓扑中有若干交换机设备、MED 设备、NMS 设备。

以下图为例，LLDP 功能默认打开，不需要再进行配置。

- Switch A 和 Switch B 可以互相发现对方是自己的邻居设备。
- Switch A 在端口 Gi 0/1 上可以发现邻居 MED 设备 IP-Phone。
- NMS（Network Management System，网络管理系统）能够访问 Switch A 的邻居设备信息。

图 5-1



【注释】 锐捷交换机产品 Switch A 和 Switch B、IP-Phone 都支持 LLDP 和 LLDP-MED。
交换机端口上 LLDP 的工作模式为 TxRx。
LLDP 报文的发送时间参数采用缺省值，即发送时间间隔为 30 秒、传输 LLDP 报文的延迟时间为 2 秒。

功能部属

- 在交换机中运行 LLDP 协议，实现邻居发现。
- 在交换机中运行 SNMP 协议，实现网络管理系统获取和设置交换机中的 LLDP 相关信息。

5.2.2 利用LLDP进行错误检测

应用场景

网络拓扑中有直连的两台交换机设备，错误配置信息将显示。

以下图为例，LLDP 功能默认打开，LLDP 错误检测功能缺省打开，不需要再进行配置。

- 管理员在对 Switch A 进行 VLAN 配置、端口速率双工配置、聚合端口配置和端口 MTU 配置时，如果配置的信息与相连接的邻居设备 Switch B 的配置不匹配，将提示相应的错误信息。反之亦然。

图 5-2

【注释】 两台锐捷交换机产品 Switch A 和 Switch B 都支持 LLDP 协议。
交换机端口上 LLDP 的工作模式为 TxRx。
LLDP 报文的发送时间参数采用缺省值，即发送时间间隔为 30 秒、传输 LLDP 报文的延迟时间为 2 秒。

功能部属

- 在交换机中运行 LLDP 协议，实现邻居发现，并检测两端的交换机直接接口的配置信息是否错误。

5.3 功能详解

基本概念

LLDPDU

LLDPDU 是指封装在 LLDP 报文中的协议数据单元，它由一系列的 TLV 封装而成。这些 TLV 集合包括了三个固定的 TLV 加上一系列可选的 TLVs 和一个 End Of TLV 组成。LLDPDU 的具体格式如图所示：

图 5-3 LLDPDU 格式

其中：

- M 表示是固定的 TLV。
- 在 LLDPDU 中，Chassis ID TLV、Port ID TLV、Time To Live TLV 和 End Of LLDPDU TLV 是必须携带的，而其它类型的 TLV 是可选携带。

LLDP 报文封装格式

LLDP 报文支持两种封装格式：Ethernet II 和 SNAP（Subnetwork Access Protocols，子网访问协议）。

其中 Ethernet II 格式封装的 LLDP 报文如图所示：

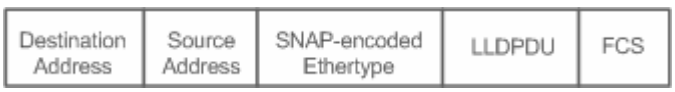
图 5-4 Ethernet II 格式封装的 LLDP 报文

其中：

- Destination Address：目的 MAC 地址，为 LLDP 的组播地址 01-80-C2-00-00-0E。
- Source Address：源 MAC 地址，为设备的端口 MAC 地址。
- Ethertype：以太网类型，为 0x88CC。
- LLDPDU：LLDP 协议数据单元。
- FCS：帧校验序列。

SNAP 格式封装的 LLDP 报文如图所示：

图 5-5 SNAP 格式封装的 LLDP 报文



其中：

- Destination Address：目的 MAC 地址，为 LLDP 的组播地址 01-80-C2-00-00-0E。

- Source Address：源 MAC 地址，为设备的端口 MAC 地址。
- SNAP-encoded Ethertype：SNAP 封装的以太网类型，为 AA-AA-03-00-00-00-88-CC.。
- LLDPDU：LLDP 协议数据单元。
- FCS：帧校验序列。

TLV

LLDPDU 中封装的 TLV 可以分成二个大类：

- 基本管理 TLV
- 组织定义 TLV

基本管理 TLV 是一组用于网络管理的基础 TLV 集合。组织定义 TLV 是由标准组织和其它机构定义的 TLV，比如 IEEE 802.1 组织、IEEE 802.3 组织分别定义了各自的 TLV 集合。

1. 基本管理 TLV

基本管理 TLV 集合包含了两种类型的 TLV：固定 TLV 和可选 TLV。固定 TLV 是指该 TLV 信息必须包含在 LLDPDU 中发布，可选 TLV 是指根据需要确定 TLV 是否包含在 LLDPDU 中发布。

基本管理 TLV 的内容见表：

TLV 类型	TLV 说明	在 LLDPDU 中用法
End Of LLDPDU TLV	LLDPDU 的结束标志，占用 2 个字节	固定
Chassis ID TLV	用于标识设备，通常用 MAC 地址表示	固定
Port ID TLV	用于标识发送 LLDPDU 的端口	固定
Time To Live TLV	本地信息在邻居设备上的存活时间，当收到 TTL 为 0 的 TLV 时，此时需要删除掉对应的邻居信息。	固定
Port Description TLV	发送 LLDPDU 的端口描述符	可选
System Name TLV	描述设备的名称	可选
System Description TLV	设备描述信息，包括硬件/软件版本、操作系统等信息	可选
System Capabilities TLV	描述设备的主要功能，例如桥接、路由、中继等功能	可选
Management Address TLV	管理地址 ,同时包含了接口号和 OID(Object Identifier，对象标识)。	可选

锐捷交换机系列产品 LLDP 协议支持基本管理 TLV 的发布。

2. 组织定义 TLV

不同的组织 (例如 IEEE 802.1、IEEE 802.3、IETF 或者设备供应商) 定义特定的 TLV 信息去通告设备的特定信息。TLV 格式中通过 OUI（Organizationally Unique Identifier，组织唯一标识符）字段来区分不同的组织。

- 组织定义 TLV 属于可选的 TLV 集合，根据用户的实际需要在 LLDPDU 中发布。目前比较常见的组织定义 TLV 有以下三种： IEEE 802.1 组织定义的 TLV

IEEE 802.1 组织定义的 TLV 见表：

TLV 类型	TLV 说明
Port VLAN ID TLV	端口的 VLAN 标识符
Port And Protocol VLAN ID TLV	端口的协议 VLAN 标识符
VLAN Name TLV	端口的 VLAN 名称
Protocol Identity TLV	端口支持的协议类型

锐捷交换机系列产品 LLDP 协议，不支持发送 Protocol Identity TLV，但支持接收该类型的 TLV。

- IEEE 802.3 组织定义的 TLV

IEEE 802.3 组织定义的 TLV 见表：

TLV 类型	TLV 说明
MAC/PHY Configuration//Status TLV	端口的速率双工状态、是否支持并使能自动协商功能
Power Via MDI TLV	端口的供电能力
Link Aggregation TLV	端口的链路聚合能力及当前的聚合状态
Maximum Frame Size TLV	端口所能传输的最大的帧的大小

锐捷交换机系列产品 LLDP 协议支持 IEEE 802.3 组织定义的 TLV 的发布。

- LLDP-MED TLV

LLDP-MED 以 IEEE 802.1AB LLDP 协议为基础，它扩展了 LLDP，使用户能够更方便地部署 VoIP（Voice Over IP，基于 IP 的语音传输）网络及进行故障检测。它提供了网络配置策略、设备发现、以太网供电管理和目录管理等应用，满足了节约成本、有效地管理和易于部署方面的需求，简化了语音设备地部署。

LLDP-MED 定义的 TLV 见表：

TLV 类型	TLV 说明
LLDP-MED Capabilities TLV	设备是否支持 LLDP-MED、LLDPDU 中封装的 LLDP-MED TLV 类型以及当前设备的类型（网络连接设备或终端）
Network Policy TLV	通告端口的 VLAN 的配置、支持的应用类型（如语音或视频）、二层的优先级信息等
Location Identification TLV	定位标识终端设备。在网络拓扑收集等应用中能够精确地定位出终端设备
Extended Power-via-MDI TLV	提供了更高级的供电管理
Inventory – Hardware Revision TLV	MED 设备的硬件版本
Inventory – Firmware Revision TLV	MED 设备的固件版本
Inventory – Software Revision TLV	MED 设备的软件版本
Inventory – Serial Number TLV	MED 设备的序列号
Inventory – Manufacturer Name TLV	MED 设备的制造商的名称
Inventory – Model Name TLV	MED 设备的模块名称
Inventory – Asset ID TLV	MED 设备的资产标识符，用于目录管理和资产跟踪

锐捷交换机系列产品 LLDP 协议支持 LLDP-MED 定义的 TLV 的发布。

功能特性

功能特性	作用
LLDP工作模式	配置 LLDP 报文收发的模式。
LLDP报文的传输机制	直连支持 LLDP 协议的交换机设备可发送 LLDP 报文给对方。
LLDP报文的接收机制	直连支持 LLDP 协议的交换机设备可接收对方发送的 LLDP 报文。

5.3.1 LLDP工作模式

配置 LLDP 工作模式，能够使交换机收发 LLDP 报文的方式发生变化。

工作原理

LLDP 提供了三种工作模式：

- TxRx：既发送也接收 LLDPDU。
- Rx Only：只接收不发送 LLDPDU。
- Tx Only：只发送不接收 LLDPDU。

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作，通过配置端口初始化的延迟时间，可以避免由于工作模式频繁改变而导致端口不断地进行初始化操作。

相关配置

↘ 配置 LLDP 工作模式

缺省情况下，接口上的工作模式为 TxRx。

使用 **lldp mode** 命令可以改变接口上的工作模式。

必须在接口上配置工作模式为 TxRx 才能使 LLDP 协议报文收发功能正常。若接口工作模式配置为 Rx Only，那么设备只能接收 LLDP 报文，但无法发送 LLDP 报文；若接口工作模式配置为 Tx Only，那么设备只能发送 LLDP 报文，但无法接收 LLDP 报文；若借口工作模式关闭，将不再收发 LLDP 报文。

5.3.2 LLDP报文的传输机制

LLDP 报文的传输能让对端设备发现其邻居设备的存在，当取消 LLDP 传输模式或端口被管理 Shutdown 的时候，能够通告给对端设备其邻居信息不再有效。

工作原理

LLDP 工作在 TxRx 或 Tx Only 模式时，会周期性的发送 LLDP 报文。当本地设备的信息发生变化时，会立即发送 LLDP 报文。为了避免本地信息的频繁变化引起的频繁发送 LLDP 报文，在发送完一个 LLDP 报文后需要延迟一定的时间后再发往下一个 LLDP 报文。该延迟时间可以手工配置。

LLDP 提供了两种报文类型：

- 标准 LLDP 报文：包含了本地设备的管理和配置信息。
- Shutdown 通告报文：当取消了 LLDP 的传输模式或者端口被管理 Shutdown 时，将触发 LLDP Shutdown 通告报文的发送。Shutdown 通告报文由 Chassis ID TLV、Port ID TLV、Time To Live TLV 和 End OF LLDP TLV 组成。其中 Time To Live TLV 中 TTL 等于 0。当设备收到 LLDP Shutdown 通告报文时，将认为邻居信息已经不再有效并立即删除邻居信息。

当 LLDP 工作模式由关闭或 Rx 转变为 TxRx 或 Tx，或者发现新邻居时(即收到新的 LLDP 报文且本地尚未保存该邻居信息)，为了让邻居设备尽快学习到本设备的信息，将启动快速发送机制。快速发送机制调整 LLDP 报文的发送周期为 1 秒，并连续发送一定数量的 LLDP 报文。

相关配置

配置 LLDP 工作模式

缺省情况下，接口上的工作模式为 TxRx。

使用 **lldp mode txrx** 和 **lldp mode tx** 命令可以使 LLDP 报文传输功能打开，使用 **lldp mode rx** 和 **no lldp mode** 命令可以使 LLDP 报文传输功能关闭。

必须在接口上配置工作模式为 TxRx 或 Tx Only 才能使 LLDP 的报文传输功能正常。若接口工作模式配置为 Rx Only，那么设备只能接收 LLDP 报文，但无法发送 LLDP 报文。

配置 LLDP 报文的发送延迟时间

缺省情况下，LLDP 报文的发送延迟时间为 2 秒。

使用 **lldp timer tx-delay** 命令可以修改 LLDP 报文的发送延迟时间。

延迟时间配置过小，本地信息的频繁变化引起的频繁发送 LLDP 报文；配置值太大，本地信息的变化可能不能使发送 LLDP 报文。

配置 LLDP 报文的发送时间间隔

缺省情况下，LLDP 报文的发送时间间隔为 30 秒。

使用 **lldp timer tx-interval** 命令可以修改 LLDP 报文的发送时间间隔。

配置值太小，则会使 LLDP 发送频率过高；配置值太大，则可能会使对端设备不能及时发现本地设备。

配置允许发布的 TLV 类型

缺省情况下，接口上允许发布除 Location Identification TLV 之外的所有类型的 TLV。

使用 **lldp tlv-enable** 命令可以改变允许发布的 TLV 类型。

增加或减少发送的 LLDP 报文中 LLDPDU 的对应 TLV 字段。

配置 LLDP 快速发送报文的个数

缺省情况下，LLDP 快速发送报文的个数为 3 个。

使用 **lldp fast-count** 命令可以改变 LLDP 快速发送报文的个数。

改变快速发送机制下快速发送报文的个数。

5.3.3 LLDP报文的接收机制

LLDP 报文的接收能够发现邻居设备的存在以及何时应该老化邻居信息。

工作原理

LLDP 工作在 TxRx 或 RxOnly 模式时，能够接收 LLDP 报文。当设备收到 LLDP 报文时，会进行有效性检查。通过报文校验后，判断是新的邻居信息还是已经存在的邻居信息更新，并将邻居信息保存在本地设备。同时根据报文中 TTL TLV 的值设置邻居信息在本地设备的存活时间。如果收到 TTL TLV 的值为 0，表示需要立即老化掉该邻居信息。

相关配置

↘ 配置 LLDP 工作模式

缺省情况下，接口上的工作模式为 TxRx。

使用 **lldp mode txrx** 和 **lldp mode rx** 命令可以使 LLDP 报文接收功能打开，使用 **lldp mode tx** 和 **no lldp mode** 命令可以使 LLDP 报文接收功能关闭。

必须在接口上配置工作模式为 TxRx 或 Rx Only 才能使 LLDP 的报文接收功能正常。若接口工作模式配置为 Tx Only 或关闭，那么设备只能发送 LLDP 报文，但无法接收 LLDP 报文。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置LLDP功能	⚠ 可选配置。用于打开或关闭全局和接口的 LLDP 功能。	
	lldp enable	打开 LLDP 功能
	no lldp enable	关闭 LLDP 功能
配置LLDP工作模式	⚠ 可选配置。用于配置 LLDP 报文收发模式。	
	lldp mode {rx | tx | txrx }	配置 LLDP 工作模式
	no lldp mode	关闭 LLDP 工作模式
配置允许发布的TLV类型	⚠ 可选配置。用于配置允许发布的 TLV 类型。	
	lldp tlv-enable	配置允许发布的 TLV 类型
	no lldp tlv-enable	取消发布指定的 TLV 类型

配置LLDP报文中发布管理地址	可选配置。用于配置 LLDP 报文中发布。	
	lldp management-address-tlv [*ip-address*]	配置 LLDP 报文中发布管理地址
	no lldp management-address-tlv	取消管理地址的发布
配置快速发送LLDP报文的个数	可选配置。用于配置快速发送 LLDP 报文的个数。	
	lldp fast-count *value*	配置快速发送 LLDP 报文的个数
	no lldp fast-count	恢复缺省快速发送 LLDP 报文个数
配置TTL乘数和LLDP报文发送时间间隔	可选配置。用于配置 TTL 乘数和 LLDP 报文发送时间间隔。	
	lldp hold-multiplier *value*	配置 TTL 乘数
	no lldp hold-multiplier	恢复缺省 TTL 乘数
	lldp timer tx-interval *seconds*	配置 LLDP 报文发送时间间隔
	no lldp timer tx-interval	恢复缺省 LLDP 报文发送时间间隔
配置LLDP报文的发送延迟时间	可选配置。用于配置 LLDP 报文的发送延迟时间。	
	lldp timer tx-delay *seconds*	配置 LLDP 报文的发送延迟时间
	no lldp timer tx-delay	恢复缺省 LLDP 报文的发送延迟时间
配置端口初始化的延迟时间	可选配置。用于配置端口初始化的延迟时间。	
	lldp timer reinit-delay *seconds*	配置端口初始化的延迟时间
	no lldp timer reinit-delay	恢复缺省端口初始化的延迟时间
配置LLDP Trap功能	可选配置。用于配置 LLDP Trap 功能。	
	lldp notification remote-change enable	打开 LLDP Trap 功能
	no lldp notification remote-change enable	关闭 LLDP Trap 功能
	lldp timer notification-interval	配置发送 LLDP Trap 信息的时间间隔
	no lldp timer notification-interval	恢复缺省发送 LLDP Trap 信息的时间间隔
配置LLDP错误检测功能	可选配置。用于配置 LLDP 错误检测功能。	
	lldp error-detect	打开 LLDP 错误检测功能
	no lldp error-detect	关闭 LLDP 错误检测功能
配置LLDP报文封装格式	可选配置。用于配置 LLDP 报文封装格式。	
	lldp encapsulation snap	配置 LLDP 报文的封装格式为 SNAP
	no lldp encapsulation snap	配置 LLDP 报文的封装格式为 Ethernet II
配置LLDP Network Policy策略	可选配置。用于配置 LLDP Network Policy 策略。	
	lldp network-policy profile *profile-num*	配置 LLDP Network Profile 策略
	no lldp network-policy profile *profile-num*	删除 LLDP Network Profile 策略
配置设备的普通地址信息	可选配置。用于配置设备的普通地址信息。	

	{ **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** } *ca-word*	配置设备的普通地址信息
	no { **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** } *ca-word*	删除设备的普通地址信息
配置设备的紧急电话号码信息	⚠ 可选配置。用于配置设备的紧急电话号码信息。	
	lldp location elin identifier *id* **elin-location** *tel-number*	配置设备的紧急电话号码信息
	no lldp location elin identifier *id*	删除设备的紧急电话号码信息

5.4.1 配置LLDP功能

配置效果

- 打开或关闭 LLDP 的功能。

注意事项

- 如果要求接口上 LLDP 功能生效，则要同时开启全局和该接口上的 LLDP 功能。

配置方法

- 可选配置。
- 可对全局或接口下配置 LLDP 功能。

检验方法

显示 LLDP 的状态信息。

- 检查全局 LLDP 功能是否开启。
- 检查接口下 LLDP 功能是否开启。

相关命令

打开 LLDP 功能

【命令格式】 **lldp enable**
【参数说明】 -
【命令模式】 全局模式、接口模式
【使用指导】 需要全局打开 LLDP 开关，接口的 LLDP 功能才生效。

关闭 LLDP 功能

【命令格式】 **no lldp enable**
【参数说明】 -
【命令模式】 全局模式、接口模式
【使用指导】 -

配置举例

关闭 LLDP 功能

【配置方法】 关闭全局 LLDP 功能。

	Ruijie(config)#no lldp enable

【检验方法】 显示 LLDP 全局状态信息。

	Ruijie(config)#show lldp status Global status of LLDP: Disable

常见错误

- 接口已开启 LLDP 功能，但是全局没有开启 LLDP 功能，此时接口下的 LLDP 功能还是不能生效。
- 端口学习到的邻居个数限制在 5 个，即端口最多只能学习到 5 个邻居。
- 如果邻居设备不支持 LLDP，但是邻居设备下连的设备支持 LLDP，由于邻居设备可能会转发 LLDP 的报文，这样，端口可能会学习到非直连的设备的信息。

5.4.2 配置LLDP工作模式

配置效果

- 配置接口的 LLDP 的工作模式为 TxRx，则该接口可发送和接收报文。
- 配置接口的 LLDP 的工作模式为 Tx，则该接口只能发送报文，不能接收报文。
- 配置接口的 LLDP 的工作模式为 Rx，则该接口只能接收报文，不能发送报文。
- 关闭接口的 LLDP 工作模式，则该接口不能接收和发送报文。

注意事项

- LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。

配置方法

- 可选配置。
- 用户可根据实际需要将工作模式修改为 Tx 或 Rx 模式。

检验方法

显示接口下 LLDP 的状态信息。

- 检查接口下 LLDP 的工作模式是否和配置的相同。

相关命令

↘ 配置 LLDP 工作模式

【命令格式】 **lldp mode** { **rx | tx | txrx** }

【参数说明】 rx：表示只接收不发送 LLDPDU

tx：表示只发送不接收 LLDPDU

txrx：表示即发送又接收 LLDPDU

【命令模式】 接口模式

【使用指导】 接口 LLDP 功能生效的前提是全局使能了 LLDP 且接口 LLDP 的工作模式处于 tx、rx 或 txrx。

↘ 关闭 LLDP 工作模式

【命令格式】 **no lldp mode**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 关闭接口的 LLDP 工作模式，此时接口不再发送和接收 LLDP 报文。

配置举例

↘ 配置 LLDP 工作模式

【配置方法】 接口下配置 LLDP 的工作模式为 Tx 模式。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp mode tx
```

【检验方法】 显示 LLDP 在接口下的状态信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : TxOnly
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

常见配置错误

-

5.4.3 配置允许发布的TLV类型

配置效果

- 用户可以通过配置运行发布的 TLV 类型，使发送 LLDP 报文中 LLDPDU 的内容改变。

注意事项

- 配置基本管理 TLV、IEEE 802.1 组织定义 TLV、IEEE 802.3 组织定义 TLV 时，如果指定 **all** 参数，将发布该类型的所有可选 TLV。
- 配置 LLDP-MED TLV 时，如果指定 **all** 参数，将发布除 Location Identification TLV 之外的所有类型的 LLDP-MED TLV。
- 配置允许发布 LLDP-MED Capability TLV 时，需要先配置允许发布 LLDP 802.3 MAC/PHY TLV；取消发布 LLDP 802.3 MAC/PHY TLV 时，需要先取消发布 LLDP-MED Capability TLV

- 配置 LLDP-MED TLV 时，必须配置允许发布 LLDP-MED Capability TLV，才可以配置允许发布 LLDP-MED 其它类型的 TLV。取消发布 LLDP-MED TLV，必须先取消发布 LLDP-MED 其它类型的 TLV，才允许取消发布 LLDP-MED Capability TLV。当设备下联 IP 电话，若 IP 电话支持 LLDP-MED，则可以通过配置 network policy TLV 下发策略给 IP 电话
- 如果设备缺省支持 DCBX 功能，缺省情况下端口上不允许发布 IEEE 802.3 TLV 及 LLDP-MED TLV

配置方法

- 可选配置。
- 用户可根据实际需要在某接口下配置允许发布的 TLV 类型。

检验方法

显示端口上可发布的 TLV 配置信息。

- 检查接口下允许发布的 TLV 是否和配置的一致。

相关命令

配置 LLDP 允许发布的 TLV

【命令格式】 **lldp tlv-enable** { **basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **|dot1-tlv** { **all | port-vlan-id | protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] } **|dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [*profile-num*] **| power-over-ethernet** } }

【参数说明】 **basic-tlv**：基本管理 TLV

port-description：表示 Port Description TLV

system-capability：表示 System Capabilities TLV

system-description：表示 System Description TLV

system-name：表示 System Name TLV

dot1-tlv：802.1 组织定义的 TLV

port-vlan-id：表示 Port VLAN ID TLV

protocol-vlan-id：表示 Port And Protocol VLAN ID TLV

vlan-id：表示端口协议 VLAN ID，配置范围为：1-4094

vlan-name：表示 VLAN Name TLV

vlan-id：表示指定 VLAN 名称对应的 VLAN ID，配置范围为：1-4094

dot3-tlv：802.3 组织定义的 TLV

link-aggregation：表示 Link Aggregation TLV

mac-physic：表示 MAC/PHY Configuratioin/Status TLV

max-frame-size：表示 Maximum Frame Size TLV

power：表示 Power Via MDI TLV

med-tlv：LLDP MED TLV

capability：表示 LLDP-MED Capabilities TLV

inventory：表示目录管理 TLV，包括硬件版本、固件版本、软件版本、序列号、制造产商名称、模块名称和资产标识符等

location：表示 Location Identification TLV

civic-location：表示封装网络连接设备的普通地址信息

elin：表示封装紧急电话号码信息

id：表示配置的策略 ID，配置范围为：1-1024

network-policy：表示 Network Policy TLV

profile-num：Network Policy 策略 ID，配置范围为：1-1024

power-over-ethernet：表示 Extended Power-via-MDI TLV

【命令模式】 接口模式

【使用指导】

取消发布指定的 TLV 类型

【命令格式】 **no lldp tlv-enable {basic-tlv** { **all | port-description | system-capability | system-description | system-name** } **| dot1-tlv** { **all | port-vlan-id | protocol-vlan-id | vlan-name** } **| dot3-tlv** { **all | link-aggregation | mac-physic | max-frame-size | power** } **| med-tlv { all | capability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [*profile-num*] **| power-over-ethernet** } }

【参数说明】 **basic-tlv**：基本管理 TLV

port-description：表示 Port Description TLV

system-capability：表示 System Capabilities TLV

system-description：表示 System Description TLV

system-name：表示 System Name TLV

dot1-tlv：802.1 组织定义的 TLV

port-vlan-id：表示 Port VLAN ID TLV

protocol-vlan-id：表示 Port And Protocol VLAN ID TLV

vlan-name：表示 VLAN Name TLV

dot3-tlv：802.3 组织定义的 TLV

link-aggregation：表示 Link Aggregation TLV

mac-physic：表示 MAC/PHY Configuratioin/Status TLV

max-frame-size：表示 Maximum Frame Size TLV

power：表示 Power Via MDI TLV

med-tlv：LLDP MED TLV

capability：表示 LLDP-MED Capabilities TLV

inventory：表示目录管理 TLV，包括硬件版本、固件版本、软件版本、序列号、制造产商名称、模块名称和资产标识符等

location：表示 Location Identification TLV

civic-location：表示封装网络连接设备的普通地址信息

elin：表示封装紧急电话号码信息

id：表示配置的策略 ID，配置范围为：1-1024

network-policy：表示 Network Policy TLV

profile-num：Network Policy 策略 ID，配置范围为：1-1024

power-over-ethernet：表示 Extended Power-via-MDI TLV

【命令模式】 接口模式

【使用指导】

配置举例

配置 LLDP 允许发布的 TLV

【配置方法】 配置取消发布 IEEE 802.1 组织定义的 Port And Protocol VLAN ID TLV

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id
```

【检验方法】 显示 LLDP 在接口下的 TLV 配置信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp tlv-config interface gigabitethernet 0/1
LLDP tlv-config of port [GigabitEthernet 0/1]
               NAME                  STATUS DEFAULT
------------------------------ ------ -------
Basic optional TLV:
Port Description TLV              YES    YES
System Name TLV                    YES    YES
System Description TLV            YES    YES
System Capabilities TLV           YES    YES
Management Address TLV            YES    YES

IEEE 802.1 extend TLV:
Port VLAN ID TLV                   YES    YES
Port And Protocol VLAN ID TLV    NO     YES
VLAN Name TLV                       YES    YES

IEEE 802.3 extend TLV:
MAC-Physic TLV                      YES    YES
Power via MDI TLV                  YES    YES
Link Aggregation TLV               YES    YES
Maximum Frame Size TLV             YES    YES

LLDP-MED extend TLV:
Capabilities TLV                    YES    YES
Network Policy TLV                  YES    YES
```

```
Location Identification TLV       NO      NO
Extended Power via MDI TLV        YES     YES
Inventory TLV                        YES     YES
```

常见配置错误

-

5.4.4 配置LLDP报文中发布管理地址

配置效果

- 配置接口下 LLDP 报文中的发布管理地址，可使管理地址 TLV 发生改变。
- 取消管理地址发布将使 LLDP 报文中的管理地址按缺省情况下选取。

注意事项

- LLDP 运行在实际的物理接口上（对于 AP 口，则实际是运行在 AP 成员口上）。堆叠口，VSL 口不支持 LLDP。

配置方法

- 可选配置。
- 在接口下配置 LLDP 报文发布的管理地址。

检验方法

显示本地设备接口下的 LLDP 信息。

- 检查本地设备接口下的 LLDP 信息是否和配置的相同。

相关命令

↘ 配置 LLDP 报文中发布的管理地址

【命令格式】 **lldp management-address-tlv** [*ip-address*]

【参数说明】 ip-address：LLDP 报文中发布的管理地址

【命令模式】 接口模式

【使用指导】 缺省情况下，LLDP 报文发布管理地址。发布的管理地址为端口允许通过的最小 VLAN 的 IPv4 地址，如果该 VLAN 未配置 IPv4 地址，则继续查找下一个允许通过的最小 VLAN，直到找到 IPv4 地址为止。
如果未找到 IPv4 地址，则查找端口允许通过的最小 VLAN 的 IPv6 地址。

如果仍未找到 IPv6 地址，则采用本机地址 127.0.0.1 作为管理地址发布。

取消管理地址的发布

【命令格式】 **no lldp management-address-tlv**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 缺省情况下，LLDP 报文发布管理地址。发布的管理地址为端口允许通过的最小 VLAN 的 IPv4 地址，如果该 VLAN 未配置 IPv4 地址，则继续查找下一个允许通过的最小 VLAN，直到找到 IPv4 地址为止。
如果未找到 IPv4 地址，则查找端口允许通过的最小 VLAN 的 IPv6 地址。
如果仍未找到 IPv6 地址，则采用本机地址 127.0.0.1 作为管理地址发布。

配置举例

配置 LLDP 报文中发布的管理地址

【配置方法】 在接口下配置 LLDP 报文发布的管理地址为 192.168.1.1

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1
```

【检验方法】 查看对应接口下相应的配置信息

```
Ruijie(config-if-GigabitEthernet 0/1)#show  lldp local-information interface GigabitEthernet 0/1
Lldp local-information of port [GigabitEthernet 0/1]
  Port ID type                      : Interface name
  Port id                           : GigabitEthernet 0/1
  Port description                  : GigabitEthernet 0/1

  Management address subtype        : ipv4
  Management address                : 192.168.1.1
  Interface numbering subtype       : ifIndex
  Interface number                  : 1
  Object identifier                 :

  802.1 organizationally information
  Port VLAN ID                      : 1
  Port and protocol VLAN ID(PPVID)  : 1
      PPVID Supported               : YES
      PPVID Enabled                 : NO
  VLAN name of VLAN 1               : VLAN0001
  Protocol Identity                 :

  802.3 organizationally information
  Auto-negotiation supported        : YES
```

```
  Auto-negotiation enabled          : YES
  PMD auto-negotiation advertised   : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode,
100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode
  Operational MAU type              : speed(100)/duplex(Full)
  PoE support                       : NO
  Link aggregation supported        : YES
  Link aggregation enabled          : NO
  Aggregation port ID               : 0
  Maximum frame Size                : 1500

  LLDP-MED organizationally information
  Power-via-MDI device type         : PD
  Power-via-MDI power source        : Local
  Power-via-MDI power priority      :
  Power-via-MDI power value         :
  Model name                        : Model name
```

常见配置错误

-

5.4.5 配置快速发送LLDP报文的个数

配置效果

- 改变快速发送机制下 LLDP 报文发送的个数。

注意事项

- -

配置方法

- 可选配置。
- 在全局配置模式下配置快速发送 LLDP 报文个数。

检验方法

显示全局 LLDP 的状态信息。

- 检查 LLDP 快速发送个数是否和配置的相同。

相关命令

配置快速发送 LLDP 报文的个数

【命令格式】 **lldp fast-count** *value*

【参数说明】 value：LLDP 快速发送报文的个数，缺省为 3 个，可配置的范围为 1-10

【命令模式】 全局模式

【使用指导】 -

恢复缺省快速发送 LLDP 报文个数

【命令格式】 **no lldp fast-count**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 -

配置举例

配置快速发送 LLDP 报文的个数

【配置方法】 全局配置模式下配置快速发送 LLDP 报文的个数为 5 个

```
Ruijie(config)#lldp fast-count 5
```

【检验方法】 显示全局 LLDP 的状态信息。

```
Ruijie(config)#show lldp status
Global status of LLDP                  : Enable
Neighbor information last changed time :
Transmit interval                      : 30s
Hold multiplier                        : 4
Reinit delay                           : 2s
Transmit delay                         : 2s
Notification interval                  : 5s
Fast start counts                      : 5
```

常见配置错误

-

5.4.6 配置TTL乘数和LLDP报文发送时间间隔

配置效果

- 改变 TTL 乘数的值。
- 改变 LLDP 报文发送时间间隔。

注意事项

-

配置方法

- 可选配置。
- 全局配置模式下进行配置。

检验方法

显示接口下 LLDP 的状态信息。

- 检查接口下 LLDP 的工作模式是否和配置的相同。

相关命令

↘ 配置 TTL 乘数

【命令格式】 **lldp hold-multiplier** *value*

【参数说明】 value：TTL 乘数，缺省为 4，配置范围为 2-10

【命令模式】 全局模式

【使用指导】 LLDP 报文中 Time To Live TLV 的值=TTL 乘数×报文发送时间间隔+1。因此，通过调整 TTL 乘数可以控制本设备信息在邻居设备的存活时间。

↘ 恢复缺省 TTL 乘数

【命令格式】 **no lldp hold-multiplier**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 LLDP 报文中 Time To Live TLV 的值=TTL 乘数×报文发送时间间隔+1。因此，通过调整 TTL 乘数可以控制本设备信息在邻居设备的存活时间。

↘ 配置 LLDP 报文发送时间间隔

【命令格式】 **lldp timer tx-interval** *seconds*
【参数说明】 seconds：LLDP 报文的发送时间间隔，可配置范围为 5-32768
【命令模式】 全局模式
【使用指导】 -

↘ 恢复缺省 LLDP 报文发送时间间隔

【命令格式】 **no lldp timer tx-interval**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

配置举例

↘ 配置 LLDP 工作模式

【配置方法】 配置 TTL 乘数为 3，LLDP 报文的发送间隔为 20 秒，此时，本地设备信息在邻居设备的存活时间为 61 秒

```
Ruijie(config)#lldp hold-multiplier 3
Ruijie(config)#lldp timer tx-interval 20
```

【检验方法】 显示全局 LLDP 状态信息。

```
Ruijie(config)#lldp hold-multiplier 3
Ruijie(config)#lldp timer tx-interval 20
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 20s
Hold multiplier                       : 3
Reinit delay                          : 2s
Transmit delay                        : 2s
Notification interval                 : 5s
Fast start counts                     : 3
```

常见配置错误

-

5.4.7 配置LLDP报文的发送延迟时间

配置效果

- 改变 LLDP 报文的发送延迟时间。

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要在全局配置模式下进行配置。

检验方法

显示全局 LLDP 的状态信息。

- 检查 LLDP 报文的发送延迟时间是否和配置的相同。

相关命令

配置 LLDP 报文的发送延迟时间

【命令格式】 **lldp timer tx-delay** *seconds*

【参数说明】 seconds：LLDP 报文的发送延迟时间，可配置范围为 1-8192

【命令模式】 全局模式

【使用指导】 当本地信息发生变化时，会立即向邻居设备发送 LLDP 报文。为了避免本地信息频繁变化引起的频繁地发送 LLDP 报文，可以配置 LLDP 报文的发送延迟时间来限制 LLDP 报文的频繁发送。

恢复缺省的 LLDP 报文的发送延迟时间

【命令格式】 **no lldp timer tx-delay**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 当本地信息发生变化时，会立即向邻居设备发送 LLDP 报文。为了避免本地信息频繁变化引起的频繁地发送 LLDP 报文，可以配置 LLDP 报文的发送延迟时间来限制 LLDP 报文的频繁发送。

配置举例

配置 LLDP 报文的发送延迟时间

【配置方法】 配置发送 LLDP 报文的延迟时间为 3 秒

```
Ruijie(config)#lldp timer tx-delay 3
```

【检验方法】 查看全局 LLDP 状态信息

```
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 2s
Transmit delay                        : 3s
Notification interval                 : 5s
Fast start counts                     : 3
```

常见配置错误

-

5.4.8 配置端口初始化的延迟时间

配置效果

- 改变端口初始化的延迟时间。

注意事项

- -

配置方法

- 可选配置。
- 用户可根据实际需要对端口状态机初始化的延迟时间进行配置。

检验方法

显示全局 LLDP 的状态信息。

- 检查全局 LLDP 的端口初始化的延迟时间是否和配置的相同。

相关命令

↘ 配置端口初始化的延迟时间

【命令格式】 **lldp timer reinit-delay** *seconds*

【参数说明】 seconds：端口初始化的延迟时间，配置范围为 1-10 秒

【命令模式】 全局模式

【使用指导】 为了避免端口的工作模式的频繁变化引起的频繁地初始化状态机，可以配置端口初始化的延迟时间。

恢复缺省端口初始化的延迟时间

【命令格式】 **no lldp timer reinit-delay**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 为了避免端口的工作模式的频繁变化引起的频繁地初始化状态机，可以配置端口初始化的延迟时间。

配置举例

配置端口初始化的延迟时间

【配置方法】 配置端口初始化的延迟时间为 3 秒，并显示 LLDP 的状态信息。

```
Ruijie(config)#lldp timer reinit-delay 3
```

【检验方法】 显示全局 LLDP 的状态信息。

```
Ruijie(config)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 3s
Transmit delay                        : 2s
Notification interval                 : 5s
Fast start counts                     : 3
```

常见配置错误

-

5.4.9 配置LLDP Trap功能

配置效果

- 改变发送 LLDP Trap 信息的时间间隔。

注意事项

-

配置方法

打开 LLDP Trap 功能

- 可选配置。
- 接口配置模式下进行配置。

配置发送 LLDP Trap 信息的时间间隔

- 可选配置。
- 全局配置模式下进行配置。

检验方法

显示 LLDP 的状态信息。

- 检查 LLDP Trap 功能是否打开。
- 检查发送 LLDP Trap 信息的时间间隔和配置的相同。

相关命令

打开 LLDP Trap 功能

【命令格式】 **lldp notification remote-change enable**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 通过配置 Trap 功能，可以将本地设备的 LLDP 信息（例如发现新邻居、检测到与邻居的通信链路故障等信息）发送给网管服务器，管理员可以根据此信息监控网络的运行状况。

关闭 LLDP Trap 功能

【命令格式】 **no lldp notification remote-change enable**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 通过配置 Trap 功能，可以将本地设备的 LLDP 信息（例如发现新邻居、检测到与邻居的通信链路故障等信息）发送给网管服务器，管理员可以根据此信息监控网络的运行状况。

配置发送 LLDP Trap 信息的时间间隔

【命令格式】 **lldp timer notification-interval** *seconds*

【参数说明】 *seconds*：配置发送 LLDP Trap 信息的时间间隔，缺省的时间间隔是 5 秒，可配置的范围是 5-3600

【命令模式】 全局模式

【使用指导】 为了防止 LLDP Trap 信息的频繁发送，可以配置发送 LLDP Trap 的时间间隔。在这段时间间隔内，检测到 LLDP 信息变化，将发送 Trap 给网管服务器。

恢复缺省的发送 LLDP Trap 信息的时间间隔

【命令格式】 **no lldp timer notification-interval**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 为了防止 LLDP Trap 信息的频繁发送 ,可以配置发送 LLDP Trap 的时间间隔。在这段时间间隔内 检测到 LLDP 信息变化，将发送 Trap 给网管服务器。

配置举例

打开 LLDP Trap 功能及配置发送 LLDP Trap 信息的时间间隔

【配置方法】 使能 LLDP Trap 功能，并配置 LLDP Trap 信息的发送时间间隔为 10 秒。

```
Ruijie(config)#lldp timer notification-interval 10
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
```

【检验方法】 显示 LLDP 的状态信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status
Global status of LLDP                 : Enable
Neighbor information last changed time :
Transmit interval                     : 30s
Hold multiplier                       : 4
Reinit delay                          : 2s
Transmit delay                        : 2s
Notification interval                 : 10s
Fast start counts                     : 3
------------------------------------------------------------
Port [GigabitEthernet 0/1]
------------------------------------------------------------
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : RxAndTx
Notification enable             : YES
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

常见配置错误

-

5.4.10 配置LLDP错误检测功能

配置效果

- LLDP 错误检测功能打开，当 LLDP 检测到错误时，将打印 LOG 信息提示管理员。
- 配置 LLDP 错误检测功能，错误检测包括链路两端的 VLAN 配置检测、端口状态检测、端口聚合配置检测、MTU 配置检测及环路检测

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要在接口模式下进行配置，打开或关闭 LLDP 错误检测功能。

检验方法

显示接口下 LLDP 的状态信息。

- 检查接口下 LLDP 错误检测功能是打开还是关闭，与实际配置是否一致。

相关命令

↘ 打开 LLDP 错误检测功能

【命令格式】 **lldp error-detect**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 LLDP 错误检测功能是依靠链路两端的设备交互 LLDP 报文中的特定的 TLV 信息进行的 ,为了保证检测功能的正确运行，需要设备发布正确的 TLV 信息。

↘ 关闭 LLDP 错误检测功能

【命令格式】 **no lldp error-detect**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 LLDP 错误检测功能是依靠链路两端的设备交互 LLDP 报文中的特定的 TLV 信息进行的 ,为了保证检测功能的正确运行，需要设备发布正确的 TLV 信息。

配置举例

↘ 打开 LLDP 错误检测功能

【配置方法】 打开 LLDP 在接口 GI 0/1 下的错误检测功能。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp error-detect
```

【检验方法】 显示 LLDP 在接口下的状态信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Ethernet II
Operational mode                : RxAndTx
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

常见配置错误

-

5.4.11 配置LLDP报文封装格式

配置效果

- 改变 LLDP 报文的封装格式。

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要在接口下改变 LLDP 报文的封装格式。

检验方法

显示接口下 LLDP 的状态信息。

- 检查接口下 LLDP 报文封装格式是否和配置的相同。

相关命令

配置 LLDP 报文的封装格式为 SNAP

【命令格式】 **lldp encapsulation snap**

【参数说明】 -

【命令模式】 接口模式

【使用指导】

⚠ 为了保证本地设备和邻居设备的正常通信，需要将 LLDP 报文配置成相同的封装格式。

恢复缺省的 LLDP 报文的封装格式，即为 Ethernet II

【命令格式】 **no lldp encapsulation snap**

【参数说明】 -

【命令模式】 接口模式

【使用指导】

⚠ 为了保证本地设备和邻居设备的正常通信，需要将 LLDP 报文配置成相同的封装格式。

配置举例

配置 LLDP 报文的封装格式为 SNAP

【配置方法】 配置 LLDP 报文的封装格式为 SNAP。

```
Ruijie(config)#interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#lldp encapsulation snap
```

【检验方法】 显示 LLDP 在接口下的状态信息。

```
Ruijie(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1
Port [GigabitEthernet 0/1]
Port status of LLDP             : Enable
Port state                      : UP
Port encapsulation              : Snap
Operational mode                : RxAndTx
Notification enable             : NO
Error detect enable             : YES
Number of neighbors             : 0
Number of MED neighbors         : 0
```

常见配置错误

-

5.4.12 配置LLDP Network Policy策略

配置效果

- 改变 LLDP Network Policy 策略。
- 当设备下联 IP 电话，若 IP 电话支持 LLDP-MED，则可以通过配置 Network Policy TLV 下发策略给 IP 电话，由 IP 电话修改语音流 Tag 和 QOS。在设备上，除配置上述策外，还需要配置步骤为：1.使能 Voice VLAN 功能，把连接 IP 电话的端口静态加入 Voice VLAN；2.把连接 IP 电话的端口配置为 QOS 信任口（推荐使用信任 DSCP 模式）；3.如果在此端口上同时开启了 1X 认证，则还需要配置一条安全通道，允许 Voice VLAN 内的报文通过。若 IP 电话不支持 LLDP-MED，则必须使能 Voice VLAN 功能，并将话机 MAC 地址手动配置到 Voice VLAN OUI 列表中。
- QOS 信任模式的配置方法请参见《IP QOS》章节；Voice VLAN 的配置方法请参见《Voice VLAN》章节；安全通道的配置方法请参见《ACL》章节。

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要配置 LLDP Network Policy 策略。

检验方法

显示本地设备的 LLDP network-policy 配置策略信息。

- 检查 LLDP Network Policy 策略是否和配置的相同。

相关命令

↘ 配置 LLDP Network Profile 策略

【命令格式】 **lldp network-policy profile** *profile-num*

【参数说明】 *profile-num*：LLDP network-policy 策略的标识，范围为：1-1024

【命令模式】 全局模式

【使用指导】 使用此命令进入 LLDP network-policy 配置模式，使用此命令时需要指定策略 ID。
进入 LLDP network-policy 配置模式后，可使用{ voice | voice-signaling } vlan 命令配置具体的 network-policy 策略。

删除 LLDP Network Profile 策略

【命令格式】 **no lldp network-policy profile** *profile-num*
【参数说明】 *profile-num*：LLDP network-policy 策略的标识，范围为：1-1024
【命令模式】 接口模式
【使用指导】 使用此命令进入 LLDP network-policy 配置模式，使用此命令时需要指定策略 ID。
进入 LLDP network-policy 配置模式后，可使用{ voice | voice-signaling } vlan 命令配置具体的 network-policy 策略。

配置举例

配置 LLDP Network Profile 策略

【配置方法】 配置接口 1 发布的 LLDP 报文中 Network Policy TLV 策略为 1：voice 应用类型 vlan id 是 3，cos 是 4，dscp 是 6。

```
Ruijie#config
Ruijie(config)#lldp network-policy profile 1
Ruijie(config-lldp-network-policy)# voice vlan 3 cos 4
Ruijie(config-lldp-network-policy)# voice vlan 3 dscp 6
Ruijie(config-lldp-network-policy)#exit
Ruijie(config)# interface gigabitethernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1
```

【检验方法】 显示本地设备的 LLDP network-policy 配置策略信息。

```
network-policy information:
---------------------------
network policy profile :1
voice vlan 3 cos 4
voice vlan 3 dscp 6
```

常见配置错误

-

5.4.13 配置设备的普通地址信息

配置效果

- 设备的地址信息发生变化。

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要配置设备的普通地址信息。

检验方法

显示本地设备的 LLDP 普通地址信息。

- 检查 LLDP 普通地址信息是否和配置的相同。

相关命令

↘ 配置设备的普通地址信息

【命令格式】 配置 LLDP 普通地址信息。用户可以使用 no 选项删除地址信息。

{ **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** } *ca-word*

【参数说明】 **country**：国家代码，2 个字符。china：CH

state：地址信息 CA 类型为 1

county：CA 类型为 2

city：CA 类型为 3

division：CA 类型为 4

neighborhood：CA 类型为 5

street-group：CA 类型为 6

leading-street-dir：CA 类型为 16

trailing-street-suffix：CA 类型为 17

street-suffix：CA 类型为 18

number：CA 类型为 19

street-number-suffix：CA 类型为 20

landmark：CA 类型为 21

additional-location-information：CA 类型为 22

name：CA 类型为 23

postal-code： CA 类型为 24

building：CA 类型为 25
unit：CA 类型为 26
floor：CA 类型为 27
room：CA 类型为 28
type-of-place：CA 类型为 29
postal-community-name：CA 类型为 30
post-office-box：CA 类型为 31
additional-code：CA 类型为 32
ca-word：地址信息

【命令模式】 LLDP Civic Address 配置模式

【使用指导】 进入 LLDP Civic Address 配置模式后，配置 LLDP 普通地址信息。

删除设备的普通地址信息

【命令格式】 **no** { **country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code** }

【参数说明】 -

【命令模式】 LLDP Civic Address 配置模式

【使用指导】 进入 LLDP Civic Address 配置模式后，配置 LLDP 普通地址信息。

配置设备类型信息

【命令格式】 **device-type** *device-type*

【参数说明】 *device-type*：设备类型，缺省为 1，取值范围为 0-2
0 表示设备类型为 DHCP Server
1 表示设备类型为 Switch
2 表示设备类型为 LLDP MED 终端

【命令模式】 LLDP Civic Address 配置模式

【使用指导】 进入 LLDP Civic Address 配置模式后，配置 LLDP 普通地址中设备类型信息。

恢复设备类型信息

【命令格式】 **no device-type**

【参数说明】 -

【命令模式】 LLDP Civic Address 配置模式

【使用指导】 进入 LLDP Civic Address 配置模式后，恢复 LLDP 普通地址中设备类型信息为缺省值。

配置举例

配置设备的普通地址信息

【配置方法】 配置设备接口 1 的地址为：交换机设备，地址是国家：CH，城市：Fuzhou，邮编：350000。

```
Ruijie#config
```

```
Ruijie(config)#lldp location civic-location identifier 1
Ruijie(config-lldp-civic)# country CH
Ruijie(config-lldp-civic)# city Fuzhou
Ruijie(config-lldp-civic)# postal-code 350000
```

【检验方法】 显示设备接口 1 的 LLDP 普通地址信息。

```
civic location information:
---------------------------
Identifier            :1
country               :CH
device type           :1
city                  :Fuzhou
postal-code           :350000
```

常见配置错误

-

5.4.14 配置设备的紧急电话号码信息

配置效果

- 更改设备的紧急电话号码信息。

注意事项

-

配置方法

- 可选配置。
- 用户可根据实际需要配置设备的紧急电话号码信息。

检验方法

显示本地设备的紧急电话号码信息。

- 检查本地设备的紧急电话号码信息是否和配置的相同。

相关命令

配置设备的紧急电话号码信息

【命令格式】 **lldp location elin identifier** *id* **elin-location** *tel-number*

【参数说明】 *id*：表示紧急电话号码信息的配置标识号，范围为：1-1024

tel-number：表示紧急电话号码，范围：10 – 25 字节

【命令模式】 全局模式

【使用指导】 使用此命令来配置紧急电话号码信息。

删除设备的紧急电话号码信息

【命令格式】 **no lldp location elin identifier** *id*

【参数说明】 *id*：表示紧急电话号码信息的配置标识号，范围为：1-1024

【命令模式】 全局模式

【使用指导】 -

配置举例

配置设备的紧急电话号码信息

【配置方法】 配置设备接口 1 的紧急电话号码为：085285555556。

```
Ruijie#config
Ruijie(config)#lldp location elin identifier 1 elin-location 085283671111
```

【检验方法】 显示设备接口 1 的紧急电话号码信息。

```
elin location information:
-------------------------
Identifier          :1
elin number         :085283671111
```

常见配置错误

-

5.5 监视与维护

清除各类信息

在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除 LLDP 的统计信息。	**clear lldp statistics** [**interface** *interface-name*]
清除 LLDP 的邻居信息。	**clear lldp table** [**interface** *interface-name*]

查看运行情况

作用	命令
显示本地设备的 LLDP 信息 ,这些信息将被组织成 TLV 发送给邻居设备。	**show lldp local-information** [**global** | **interface** interface-name]
显示本地设备的 LLDP 普通地址信息或者紧急电话号码信息。	**show lldp location** { **civic-location | elin-location** } { **identifier** *id* **| interface** *interface-name* **| static** }
显示邻居设备的 LLDP 信息。	**show lldp neighbors [interface** *interface-name*] [**detail**]
显示本地设备的 LLDP network-policy 配置策略信息	**show lldp network-policy** { **profile** [*profile-num*] | **interface** *interface-name* }
显示 LLDP 的统计信息。	**show lldp statistics** [**global | interface** *interface-name*]
显示 LLDP 的状态信息。	**show lldp status** [**interface** *interface-name*]
显示端口上可发布的 TLV 配置信息。	**show lldp tlv-config** [**interface** *interface-name*]

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 LLDP 错误处理的调试开关。	**debug lldp error**
打开 LLDP 事件处理的调试开关。	**debug lldp event**
打开 LLDP 热备份处理的调试开关。	**debug lldp ha**
打开 LLDP 报文接收的调试开关。	**debug lldp packet**
打开 LLDP 状态机相关的调试开关。	**debug lldp stm**

6 PPPOE-CLIENT

6.1 概述

PPPoE（Point-to-point Protocol Over Ethernet）即，基于以太网的点对点协议。

锐捷产品支持在以太网口上运行 PPPoE 客户端，使产品具有了通过简单的桥接访问设备到远程访问集中器来连接主机网络的能力。通过 PPPoE 协议，PPPoE 服务器能够实现对每个接入客户端的控制和计费。

锐捷产品支持两种模式的拨号：按需拨号(DDR，有数据通信则刺激拨号，空闲指定时间以后，自动挂断线路)、自动拨号(no DDR，永远在线)。

- PPPOE-CLIENT 适用于通过 ADSL 上网的场景。

下文仅介绍 PPPOE-CLIENT 的相关内容。

协议规范

- RFC2516：A Method for Transmitting PPP Over Ethernet (PPPoE)
- RFC1661：The Point-to-Point Protocol (PPP)

6.2 典型应用

典型应用	场景描述
ADSL场景	在使用 ADSL 上网的场景中，提供拨号和报文转发功能。

6.2.1 ADSL场景

应用场景

在使用 ADSL 上网的场景中，提供拨号和报文转发功能。

以下图为例，讲述设备拨号上网场景。

- 设备启动拨号功能，通过 ADSL 线路，连接到远端 ISP 并获得上网的能力。
- 内网 PC 通过设备上网。

图 6-1

功能部属

- 设备启用拨号功能，通过 ADSL 线路，拨号上网。

6.3 功能详解

基本概念

ISP

ISP(Internet Service Provider) 互联网服务提供商，即向广大用户综合提供互联网接入业务、信息业务和增值业务的网络运营商。

ADSL

ADSL（Asymmetric Digital Subscriber Line）即，非对称数字用户环路，也就是拨号上网线路。

数据流

设备仅对其起转发作用的报文流。

兴趣流

由用户在配置中定义的特定的报文类，这类报文可以刺激设备开始拨号。

功能特性

功能特性	作用
拨号上网	在使用 ADSL 上网的场景中，提供拨号和报文转发功能。

6.3.1 拨号上网

拨号完成之后，设备获得了上网的能力，所以，内网中的主机也都获得了上网的能力。

工作原理

拨号、上网分别对应协商和报文转发两个过程。

其中，协商又可分为：协议协商、协议保活、协议终止三部分。

↘ 协议协商

协议协商分为 PPPoE 协商和 PPP 协商两部分。

在 PPPoE 协商中，协商双方会确认唯一的对方、记录对方 MAC 信息、建立唯一的会话 ID。

在 PPP 协商中，服务器会校验客户端的认证信息。如果校验通过，服务器就会为客户端分配 IP（如果客户端配置了 IP，且符合服务器的要求，服务器会同意这个 IP 为客户端的 IP）。

在两个协议都 UP 之后，设备就获得了上网的能力，也准备好了封装数据流报文所需的二层头。

↘ 协议保活

在 PPP 协议 UP 之后，双方会定期互发 LCP 心跳报文。如果一端在一定时间内没有收到对方回复的心跳报文，这一端就会主动终止协议。

↘ 协议终止

协议双方在一定情况下会主动终止协议。

主动终止协议方会发送 PPP 协议终止报文来结束这个 PPP 会话，然后发送 PPPoE 协议终止报文来结束这个 PPPoE 会话。

被动终止协议方在收到 PPP 协议终止报文后，会发送同意结束 PPP 会话的报文；在收到 PPPoE 协议终止报文后，会发送同意结束 PPPoE 会话的报文。

双方一旦接收到 PPPoE 协议终止报文，即使之前没有收到 PPP 协议终止报文，PPP 和 PPPoE 会话也即刻终止。

↘ 报文转发

报文发送流程：数据流路由到 dialer 口时，设备用已经准备好的二层头信息来封装数据流报文，并最终通过物理口发送出去。

报文接收流程：物理口收到报文之后，设备将报文的三层头位置标好，然后执行下一个业务，并最终发往内网的主机。

相关配置

↘ 配置以太网口

缺省情况下，以下几项都关闭，且没有默认值。

使用 **pppoe enable** 命令可以启用接口上的 PPPoE client 功能。

使用 **no pppoe enable** 命令可以关闭接口上的 PPPoE client 功能。

使用 **pppoe-client dial-pool-number** *pool-number* **dial-on-demand** 将以太网口绑定到指定的逻辑拨号池 (实现按需拨号的功能，有报文刺激才拨号 pppoe 服务器)。

使用 **no pppoe-client dial-pool-number** *pool-number* 将以太网口从指定的逻辑拨号池中解除绑定。

↘ 配置逻辑接口

缺省情况下，以下几项都关闭。

使用 **interface dialer** *dialer-number* 添加并进入指定逻辑接口。

使用 **no interface dialer** *dialer-number* 删除指定逻辑接口。

使用 **ip address negotiate** 配置 IP 地址由协商获得。

使用 **no ip address negotiate** 取消配置。

使用 **dialer pool** *number* 关联拨号池，与以太网口中拨号池一一对应。

使用 **no dialer pool** *number* 解除与拨号池的关联。

使用 **encapsulation ppp** 配置封装 PPP 协议，PPPoE 是建立在 PPP 基础上的。

使用 **no encapsulatio** 取消封装协议的配置。

使用 **mtu** *1488* 配置最大传输单元的大小为 1488。

使用 **no mtu** 取消 mtu 的配置。

使用 **dialer-group** *dialer-group-number* 关联刺激拨号的规则，与 dialer-list 对应。

使用 **no dialer-group** 取消刺激拨号的规则的配置

使用 **ppp chap hostname** *username* 配置 CHAP 认证使用的用户名。

使用 **no ppp chap hostname** 取消 CHAP 认证使用的用户名。

使用 **ppp chap password** *password* 配置 CHAP 认证使用的密码。

使用 **no ppp chap password** 取消 CHAP 认证使用的密码。

使用 **ppp pap sent-username** *username* **password** *password* 配置 PAP 认证使用的用户名和密码。

使用 **no ppp pap sent-username** 取消 PAP 认证使用的用户名和密码。

↘ 配置必要的全局参数

缺省情况下，以下几项都关闭，要根据实际情况配置以下几项。如果要与其他功能模块合用的话，还要配置其他全局参数。

使用 **dialer-list number protocol** *protocol-name* { **permit** | **deny** | **list** *access-list-number* }定义刺激拨号的规则。
使用 **no dialer-list number** 删除刺激拨号的规则。
使用 **ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* [**permanent**]配置路由，permanent 选项使路由一直有效，即使逻辑接口在线路无线时间（enable-timeout）内，此时逻辑接口处于 down 状态。

使用 no **ip route** *0.0.0.0 0.0.0.0* **dialer** *dialer-number* 取消这条路由。

6.4 配置详解

配置项	配置建议 & 相关命令	
配置PPPoE client基本功能	⚠ 必须配置。	
	pppoe enable	启动 PPPoE client 功能
	pppoe-client dial-pool-number *number* { **dial-on-demand** | **no-ddr** }	绑定逻辑拨号池与指定拨号模式
	interface dialer *dialer-number*	添加并进入指定逻辑接口
	ip address { **negotiate** | *ip-addr subnet-mask* }	配置 IP 地址由获得方式
	dialer pool *number*	关联拨号池
	encapsulation ppp	配置封装 PPP 协议
	mtu *1488*	配置最大传输单元的大小为 1488
	dialer-group *dialer-group-number*	关联刺激拨号的规则
	ppp chap hostname *username*	配置 CHAP 认证使用的用户名
	ppp chap password *password*	配置 CHAP 认证使用的密码
	ppp pap sent-username *username* **password** *password*	配置 PAP 认证使用的用户名和密码
	dialer-list number protocol *protocol-name* { **permit** | **deny** | **list** *access-list-number* }	定义刺激拨号的规则

6.4.1 配置PPPoE client基本功能

配置效果

- 设备主动发起 PPPoE 协商，并完成：协商过程、协议保活、协议终止。
- 协商完成之后，获得上网能力，开始转发路由到 dialer 口的数据流。

注意事项

- 内核模块卸载后，用户依然可以继续配置管理，但是将无法完成协商和数据流转发。

配置方法

↘ 启用 PPPoE client 功能

- 必须配置。
- 在以太口上配置。

- 启用 PPPoE client 功能。

绑定逻辑拨号池与指定拨号模式

- 必须配置。
- 在以太口上配置。
- 将以太网口绑定到指定的逻辑拨号池，并指定拨号模式。

添加并进入指定逻辑接口

- 必须配置。
- 在全局模式配置。
- 添加并进入指定逻辑接口的配置模式。

配置逻辑口 IP 获得方式

- 必须配置。
- 在逻辑口上配置。
- 配置逻辑口 IP 获得方式。

关联拨号池

- 必须配置。
- 在逻辑口上配置。
- 将逻辑接口与特定拨号池关联起来。

配置封装协议

- 必须配置。
- 在逻辑口上配置。
- 为逻辑接口配置 PPP 封装协议。

配置逻辑口 MTU

- 必须配置。
- 在逻辑口上配置。
- 配置逻辑接口的 MTU 为 1488。

关联刺激拨号规则

- 必须配置。
- 在逻辑口上配置。
- 关联刺激拨号的规则。

配置 CHAP 认证使用的用户名

- 必须配置。
- 在逻辑口上配置。
- 配置 CHAP 认证使用的用户名。

配置 CHAP 认证使用的密码

- 必须配置。
- 在逻辑口上配置。
- 配置 CHAP 认证使用的密码。

配置 PAP 认证使用的用户名和密码

- 必须配置。
- 在逻辑口上配置。
- 配置 PAP 认证使用的用户名和密码。

定义刺激拨号规则

- 必须配置。
- 在全局模式配置
- 定义刺激拨号的规则。

检验方法

- 检查 dialer 口是否获取到了 IP。
- 检查设备上是否建立了正确的 dialer 口路由表项。

相关命令

启用 PPPoE client 功能

【命令格式】 **pppoe enable**
【参数说明】 **-**
【命令模式】 接口模式
【使用指导】 启用 PPPoE client 接口必须是 WAN 属性的以太口。

绑定逻辑拨号池与指定拨号模式

【命令格式】 **pppoe-client dial-pool-number** *number* { **dial-on-demand** | **no-ddr** }
【参数说明】 *number* ：拨号池编号
【命令模式】 接口模式
【使用指导】 接口必须先启用 PPPoE client 功能。

添加并进入指定逻辑接口

【命令格式】 **interface dialer** *dialer-number*
【参数说明】 *dialer-number*：接口编号。
【命令模式】 全局模式
【使用指导】 -

配置逻辑口 IP 获得方式

【命令格式】 **ip address** { **negotiate** | *ip-addr subnet-mask* }
【参数说明】 *ip-addr*：手动配置 IP。
subnet-mask：手动配置子网掩码。
【命令模式】 接口模式
【使用指导】 如果选择 negotiate，那么 dialer 口的 IP 将协商获得。
如果手动指定 dialer 口的 IP，需要在协商中得到对端同意，才能正常工作。

关联拨号池

【命令格式】 **dialer pool** *number*
【参数说明】 *number*：拨号池编号。
【命令模式】 接口模式
【使用指导】 dialer 口将从这个拨号池中选择以太口进行拨号。

配置封装协议

【命令格式】 **encapsulation ppp**
【参数说明】 **-**
【命令模式】 接口模式
【使用指导】 -

配置逻辑口 MTU

【命令格式】 **mtu** *1488*
【参数说明】 **-**
【命令模式】 接口模式
【使用指导】 因为通过 PPPoE 协议上网，报文的二层头比普通以太报文要长。

关联刺激拨号规则

【命令格式】 **dialer-group** *dialer-group-number*
【参数说明】 *dialer-group-number*: 刺激拨号规则的编号
【命令模式】 接口模式
【使用指导】 如果配置的是 DDR 模式，只有规则内的报文路由到 dialer 口才会刺激设备拨号。
如果配置的是 no-ddr 模式，则这行配置没有作用。

配置 CHAP 认证使用的用户名

【命令格式】 **ppp chap hostname** *username*

【参数说明】 *username*：用户名
【命令模式】 接口模式
【使用指导】 -

配置 CHAP 认证使用的密码

【命令格式】 **ppp chap password** *password*

【参数说明】 *password*：密码
【命令模式】 接口模式
【使用指导】 -

配置 PAP 认证使用的用户名和密码

【命令格式】 **ppp pap sent-username** *username* **password** *password*
【参数说明】 *username*：用户名
password：密码
【命令模式】 接口模式
【使用指导】 -

定义刺激拨号的规则

【命令格式】 **dialer-list number protocol** *protocol-name* { **permit** | **deny** | **list** *access-list-number* }
【参数说明】 *protocol-name*：协议名称
access-list-number：ACL 编号
【命令模式】 全局模式
【使用指导】 -

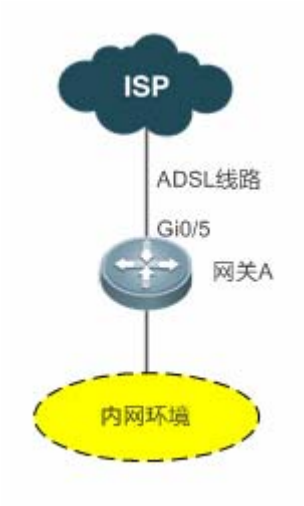
配置举例

以下配置举例，仅介绍与 PPPoE client 相关的配置。

在 ADSL 场景下，启用 PPPoE client 功能，并通过 ADSL 线路上网。

【网络环境】

图 6-2



【配置方法】 ● 在设备上启用 PPPoE client 功能，将 Gi0/5 口放入拨号池。

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/5
A(config-if)# pppoe enable
A(config-if)# pppoe-client dial-pool-number 1 dial-on-demand
A(config-if)# exit
A(config)# interface dialer 1
A(config-if)# ip address negotiate
A(config-if)# mtu 1488
A(config-if)# encapsulation ppp
A(config-if)# ip nat outside
A(config-if)# dialer pool 1
A(config-if)# dialer-group 1
A(config-if)# ppp chap hostname pppoe
A(config-if)# ppp chap password pppoe
A(config-if)# ppp pap sent-username pppoe password pppoe
A(config-if)# exit
A(config)# access-list 1 permit any
A(config)# dialer-list 1 protocol ip permit
A(config)# ip nat inside source list 1 interface dialer 1
A(config)# ip route 0.0.0.0 0.0.0.0 dialer 1
A(config)# end
A#
```

【检验方法】 使用 **show ip interface brief | in dialer** *1* 查看 dialer 口是否获取到 IP。

使用 **show ip route** 查看是否建立了正确的 dialer 口路由表项。

```
A# show ip interface brief | in dialer 1
```

```
dialer 1                        49.1.1.127/32        YES       UP
A# show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*   0.0.0.0/0 is directly connected, dialer 1
C    10.10.3.0/24 is directly connected, GigabitEthernet 0/0
C    10.10.3.1/32 is local host.
C    10.202.172.1/32 is directly connected, dialer 1
C    49.1.1.127/32 is local host.
```

常见错误

- 用户名、密码不对导致无法协商成功。
- NAT 配置不正确导致内网主机无法上网。
- 路由配置不正确导致内网主机无法上网。

6.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear pppoe tunnel** 命令，会清除隧道而导致报文转发中断。

作用	命令
清除进行 DDR 拨号接口的统计信息。	**clear dialer** [*interface-type interface-number*]
清除隧道。	**clear pppoe tunnel**

查看运行情况

作用	命令
查看 DDR 拨号的相关信息。	**show dialer** [**interface** type number] [**maps**] [**pools**]
查看 PPPoE 状态信息。	**show pppoe** { **ref** | **session** | **tunnel** }

查看调试信息

输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开按需拨号（DDR）的调试开关。	**debug dialer** { **pkt** | **mlp|callback|event** }
打开 PPP 协商的调试开关。	**debug ppp** [**authentication** | **error** | **event** | **negotiation** | **packet**]
打开 PPPoE 协商的调试开关。	**debug pppoe** [**datas** | **errors** | **events** | **packets**]

配置指南-IP 地址及应用

本分册介绍 IP 地址及应用配置指南相关内容，包括以下章节：

1. IP 地址与服务
2. ARP
3. IPv6
4. DHCP
5. DNS
6. 网络连通性测试工具
7. TCP
8. 软件 IPv4/v6 快转
9. NAT

1 IP 地址与服务

1.1 概述

因特网协议（Internet Protocol，IP）使用逻辑虚拟的地址将数据包从源方发送到目的方，即 IP 地址。在网络层，路由设备使用 IP 地址完成数据包转发。

以下仅针对 IPv4 地址进行介绍。

协议规范

- RFC 1918：Address Allocation for Private Internets
- RFC 1166：Internet Numbers

1.2 典型应用

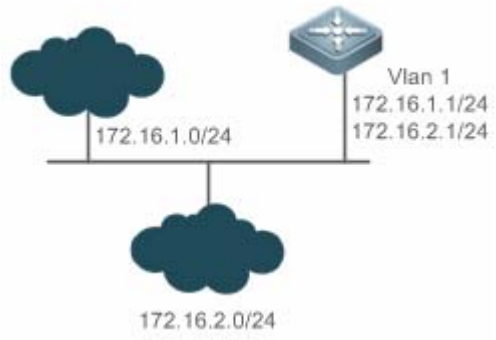
典型应用	场景描述
配置IP地址通信	两个网络使用同一个交换机接口进行通信

1.2.1 配置IP地址通信

应用场景

交换机连接一个局域网，局域网分为两个网段：172.16.1.0/24 和 172.16.2.0/24。要求两个网段的计算机都可以通过交换机和因特网通信，并且两个网段的计算机之间可以互相通信。

图 1-1 IP 地址配置范例



功能部属

- 在 vlan1 口上配置两个 ip 地址，一个主 ip 地址，一个从 ip 地址。
- 在 172.16.1.0/24 网段中的主机上配置网关为 172.16.1.1，在 172.16.2.0/24 网段中的主机上配置网关为 172.16.2.1。

1.3 功能详解

基本概念

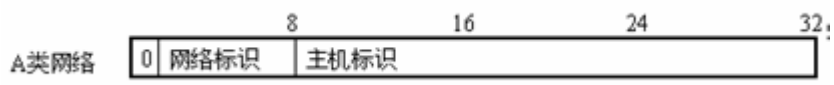
IP 地址

IP 地址由 32 位二进制组成，为了书写和描述方便，一般用十进制表示。十进制表示时，分为四组，每组 8 位，范围从 0~255，组之间用“.”号隔开，比如“192.168.1.1”就是用十进制表示的 IP 地址。

IP 地址顾名思义，自然是 IP 层协议的互连地址。32 位的 IP 地址由两个部分组成：1）网络部分；2）本地地址部分。根据网络部分的头几个比特位的值，目前使用中的 IP 地址可以划分成四大类。

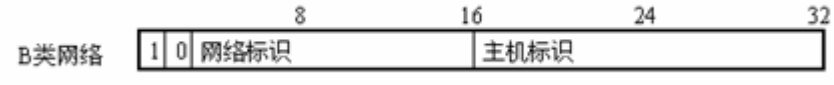
A 类地址，最高比特位为“0”，有 7 个比特位表示网络号，24 个比特位表示本地地址。这样总共有 128 个 A 类网络。

图 1-2



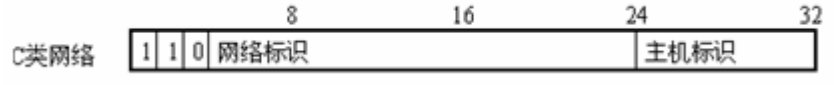
B 类地址，前两个最高比特位为“10”，有 14 个比特位表示网络号，16 个比特位表示本地地址。这样总共有 16,348 个 B 类网络。

图 1-3



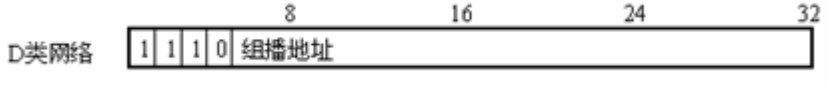
C 类地址，前三个最高比特位为“110”，有 21 个比特位表示网络号，8 个比特位表示本地地址。这样总共有 2,097,152 个 C 类网络。

图 1-4



D 类地址，前四个最高比特位为“1110”，其余比特位为组播地址。

图 1-5



前四个最高比特位为“1111”的地址是不允许分配的，这些地址称为 E 类地址，属于保留地址。

在建设网络过程中，进行 IP 地址规划时，一定要根据建设网络的性质进行 IP 地址分配。如果建设的网络需要与互联网连接，则需要到相应的机构申请分配 IP 地址。中国地区可以向中国互联网信息中心（CNNIC）申请，负责 IP 地址分配的最终机构为国际互联网名字与编号分配公司（ICANN, Internet Corporation for Assigned Names and Numbers）。如果建设的网络为内部私有网络，就不需要申请 IP 地址，但是也不能随便分配，最好分配专门的私有网络地址。

下表为保留与可用的地址列表：

类别	地址空间	状态
A 类网络	0.0.0.0~0.255.255.255	保留
	1.0.0.0~126.255.255.255	可用
	127.0.0.0~127.255.255.255	保留
B 类网络	128.0.0.0~191.254.255.255	可用
	191.255.0.0~191.255.255.255	保留
C 类网络	192.0.0.0~192.0.0.255	保留
	192.0.1.0~223.255.254.255	可用
	223.255.255.0~223.255.255.255	保留
D 类网络	224.0.0.0~239.255.255.255	组播地址
E 类网络	240.0.0.0~255.255.255.254	保留
	255.255.255.255	广播地址

其中专门有三个地址块提供给私有网络，这些地址是不会在互联网中使用的，如果分配了这些地址的网络需要连接互联网，则需要将这些 IP 地址转换成有效的互联网地址。下表为私有网络地址空间，私有网络地址由 RFC 1918 文档定义：

类别	地址空间	状态
A 类网络	10.0.0.0~10.255.255.255	1 个 A 类网络
B 类网络	172.16.0.0~172.31.255.255	16 个 B 类网络
C 类网络	192.168.0.0~192.168.255.255	256 个 C 类网络

关于 IP 地址、TCP/UDP 端口及其它编码的分配情况，请参考 RFC 1166 文档。

↘ 子网掩码

网络掩码也是一个 32 比特的数值，标识着该 IP 地址的哪几个比特为网络部分。网络掩码中，值为“1”的比特对应的 IP 地址比特位就是网络部分，值为“0”的比特对应的 IP 地址比特位就是主机地址部分。如 A 类网络对应的网络掩码为“255.0.0.0”。您可以利用网络掩码对一个网络进行子网划分，子网划分就是将主机地址部分的一些比特位也作为网络部分，缩小主机容量，增加网络的数量，这时的网络掩码就称为子网掩码。

↘ 广播报文

广播报文是指目标地址为某个物理网络上所有主机的数据包。锐捷产品支持两种类型广播报文：1）定向广播，是指数据包接收者为一个指定网络的所有主机，目标地址的主机部分全为“1”；2）淹没广播，是指数据包接收者为所有网络的主机，目标地址 32 比特位全为“1”。

↘ ICMP 报文

ICMP 是（Internet Control Message Protocol）Internet 控制报文协议。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、网络设备之间传递控制消息，主要用于网络出现异常的时候通知相应设备。

TTL

TTL（Time-To-Live），生存时间。指定 数据包被 路由器丢弃之前允许通过的网段数量。它是IP协议报文中的一个值，它告诉网络，数据包在网络中的时间是否太长而应被丢弃。

功能特性

功能特性	作用
IP地址	用于配置接口 IP 地址，该接口才允许运行 IP 协议。
广播报文处理	设置 IP 广播地址，转发处理定向广播报文。
发送ICMP报文	控制 ICMP 协议报文的收发。
控制ICMP差错报文的发送速率	防止拒绝服务攻击。
IP MTU	用于配置接口 IP 报文的最大传输单元。
IP TTL	用于配置单播报文和广播报文的 TTL。
IP源路由	用于对接收报文的源路由进行检查。

1.3.1 IP地址

接口获取 IP 地址有以下方式：

(1) 手工配置 IP 地址。

(2) 利用 DHCP 协议获取 IP 地址。

(3) 通过 PPP 协商获得 IP 地址。

(4) 借用其它接口的 IP 地址。

这几种方式是互斥的，配置新的获取 IP 地址方式时会覆盖通过原有方式获取的 IP 地址。

利用 DHCP 协议获取 IP 地址请参见“DHCP”章节，以下仅介绍其他三种获取 IP 地址的方式。

配置接口 IP 地址

一个设备只有配置了 IP 地址，才可以接收和发送 IP 数据包，接口配置了 IP 地址，说明该接口允许运行 IP 协议。

接口配置多个 IP 地址

锐捷产品可以支持一个接口配置多个 IP 地址，其中一个为主 IP 地址，其余全部为次 IP 地址。次 IP 地址的配置理论上没有数目限制，但是次 IP 地址与主 IP 以及次 IP 地址之间必须属于不同网络。在网络建设中，会经常使用到次 IP 地址，通常在以下情况下应该考虑使用次 IP 地址：

- 一个网络没有足够多的主机地址。例如，现在一般局域网需要一个 C 类网络，可分配 254 台主机。但是当局域网主机超过 254 台时，一个 C 类网络将不够分配，有必要分配另一个 C 类网络地址。这样设备就需要连接两个网络，所以就需要配置多个 IP 地址。

- 许多旧的网络是基于第二层的桥接网络，没有进行子网的划分。次 IP 地址的使用可以使该网络很容易升级到基于 IP 层的路由网络。对于每个子网，设备都配置一个 IP 地址。
- 一个网络的两个子网被另外一个网络隔离开，可以创建一个被隔离网络的子网，通过配置次 IP 地址的方式，将隔离的子网连接起来。一个子网不能在设备的两个或两个以上接口出现。

配置次 IP 地址之前，需要确定已经配置了主 IP 地址。如果网络上的一台设备配置了次 IP 地址，则其它设备也必须配置同一网络的次 IP 地址。当然如果其它设备原先没有分配 IP 地址，可以配置为主地址。

配置通过 PPP 协商获取 IP 地址

本命令只在点对点接口上支持。

通过此配置，点对点接口可以通过 PPP 协商接受对端为自己分配的 IP 地址。

配置接口借用 IP 地址

所谓“借用 IP 地址”，是指一个接口上没有配置 IP 地址，但为了使该接口能正常使用，就向同一设备上其它有 IP 地址的接口借用一个 IP 地址。

以太网接口、隧道接口和环回接口的 IP 地址可以被其它接口借用，但它们不能借用其它接口的 IP 地址。

被借用接口的 IP 地址不能是借用其它接口的 IP 地址。

如果被借用接口有多个 IP 地址，只有主 IP 地址被借用。

一个接口的 IP 地址可以借给多个接口。

借用接口的 IP 地址始终和被借用接口的 IP 地址保持一致，随着被借用接口的 IP 地址变化而变化。

相关配置

配置接口一个或多个 IP 地址

- 缺省情况接口没有配置 IP 地址。
- 通过 **ip address** 命令配置接口 IP 地址。
- 配置后根据冲突检测即可使用该 IP 地址进行通信。
- 通过 **ip address** *ip-address mask* **secondary** 可以配置多个次 IP 地址。

配置通过 PPP 协商获取 IP 地址

- 缺省情况接口没有配置通过 PPP 协商获取 ip 地址。
- 通过 **ip address negotiate** 命令配置为点对点接口协商 IP 地址。

配置接口借用 IP 地址

- 缺省情况接口没有配置 IP 地址。
- 通过 **ip unnumbered** 命令可以向其他接口借用 IP 地址。

1.3.2 广播报文处理

工作原理

广播分两种，全广播，即IP地址为 255.255.255.255，由于会被 路由器禁止传输，所以也叫本地网络广播。另一种是所有的主机位都为 1 的广播，例如：192.168.1.255/24，这种广播，通过配置是可以被转发的。

如果 IP 网络设备转发淹没广播（一般指目标 IP 地址为全“1”的广播报文），可能会引起网络的超负载，严重影响网络的运行，这种情况称为广播风暴。设备提供了一些办法能够将广播风暴限制在本地网络，阻止其继续扩张。但对于桥和交换机等基于二层网络设备，将转发和传播广播风暴。

解决广播风暴最好的办法就是给每个网络指定一个广播地址，这就是定向广播，这要求使用广播报文的 IP 协议尽可能应用定向广播而不是淹没广播进行数据传播。

关于广播问题的详细描述，请参见 RFC 919 和 RFC 922。

IP 定向广播报文是指目标地址为某个 IP 子网广播地址的 IP 报文，如目标地址为 172.16.16.255 的报文就称为定向广播报文。但是产生该报文的节点又不是目标子网的成员。

没有与目标子网直连的设备接收到 IP 定向广播报文，跟转发单播报文一样处理定向广播报文。当定向广播报文到达直连该子网的设备后，设备将把定向广播报文转换为淹没广播报文（一般指目标 IP 地址为全“1”的广播报文），然后以链路层广播方式发送给目标子网上的所有主机。

相关配置

配置 IP 广播地址

- 缺省情况下接口 IP 广播地址为 255.255.255.255。
- 如果需要定义其它地址的广播报文，可以在接口下配置 **ip broadcast-address** 命令。

允许转发定向广播

- 缺省情况接口不允许转发定向广播。
- 用户可以在指定的接口上，通过 **ip directed-broadcast** 命令配置接口允许转发定向广播，这样该接口就可以转发到直连网络的定向广播了。该命令只影响定向广播报文在目标子网的传输，而不影响其它定向广播报文的正常转发。
- 在接口上，用户还可以通过定义访问控制列表来控制转发某些定向广播。当定义了访问列表时，只有符合访问列表中定义的定向广播才会被转发。

1.3.3 发送ICMP报文

工作原理

ICMP 协议不可达消息

当设备接收到目标为自己的非广播报文，但是该数据包中采用了设备不能处理的 IP 协议，设备就向源地址发送 ICMP 协议不可达消息。另外，如果设备由于不知道路由而不能转发数据包时，也会发送 ICMP 主机不可达消息。

↘ ICMP 重定向消息

路由有时会不够优化，使得设备从一个接口接收到的数据包，还要从该接口发送出去。如果设备将数据包从接收接口重新发送出去，设备就会给数据源发送一个 ICMP 重定向消息，告诉数据源到该目标地址的网关为同一子网上的另外一台设备。这样数据源就会将后续的数据包按照最佳的路径进行发送。

↘ ICMP 掩码应答消息

网络设备有时需要知道互联网上某个子网的子网掩码，为了获取该信息，网络设备可以发送 ICMP 掩码请求消息，接收到 ICMP 掩码请求消息的网络设备就会发送掩码应答消息。

相关配置

↘ 启用 ICMP 协议不可达消息

- 缺省情况接口启用 ICMP 协议不可达消息功能。
- 可通过[**no**] **ip unreachables** 命令关闭或启用该功能。

↘ 启用 ICMP 重定向消息

- 缺省情况接口启用 ICMP 协议重定向消息功能。
- 可通过[**no**] **ip redirects** 命令关闭或启用该功能。

↘ 启用 ICMP 掩码应答消息

- 缺省情况接口启用 ICMP 掩码应答消息功能。
- 可通过[**no**] **ip mask-reply** 命令关闭或启用该功能。

1.3.4 控制ICMP差错报文的发送速率

工作原理

为了防止拒绝服务攻击，对 ICMP 差错报文的发送速率进行限制，采用令牌桶算法。

如果 IP 报文需要分片，但是 IP 首部的不可分片位被设置了，设备会向源 IP 地址发送编号为 4 的 ICMP 目的不可达报文，这种 ICMP 差错报文的主要用途是路径 MTU 发现。为了防止其它 ICMP 差错报文太多导致发不出编号为 4 的 ICMP 目的不可达报文，从而导致路径 MTU 发现功能失效，对编号为 4 的 ICMP 目的不可达报文和其它 ICMP 差错报文分别限速。

相关配置

↘ 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 **ip icmp error-interval DF** 配置发送速率。

配置其它 ICMP 差错报文的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 **ip icmp error-interval** 配置发送速率。

1.3.5 IP MTU

工作原理

如果一个 IP 报文超过 IP MTU 的大小， RGOS 软件就会对报文进行拆分。所有在同一物理网段上的设备，其互联接口的 IP MTU 一定要一致。锐捷产品允许调整接口的链路 MTU 值，而且接口的链路 MTU 的变化会引起接口的 IP MTU 的变化，接口的 IP MTU 会自动与接口的链路 MTU 保持一致。但是反之不行，如果调整了接口的 IP MTU 值，接口的链路 MTU 不会跟着改变。

相关配置

设置 IP MTU

- 缺省情况接口 IP MTU 为 1500。
- 可通过 **ip mtu** 设置 IP 包最大传输单元(MTU)。

1.3.6 IP TTL

工作原理

IP 数据包从源地址向目的地址经过路由器间传播，设置一个 TTL 数值，每过一个路由器 TTL 值就减一，当减到零的时候，路由器就把这个包丢掉，这样可以防止无用的包在网络上无限传播下去，浪费网络带宽。

相关配置

设置 IP TTL

- 缺省情况接口 IP TTL 为 64。
- 可通过 **ip ttl** 设置接口的 IP TTL 值。

1.3.7 IP源路由

工作原理

锐捷产品支持IP源路由。当设备接收到IP数据包时，会对IP报头的严格源路由、宽松源路由和记录路由等选项进行检查，这些选项在 RFC 791 中有详细描述。如果检测到该数据包启用了其中一个选项，就会执行响应的动作；如果检测到无效的选项，就会给数据源发送一个 ICMP 参数问题消息，然后丢弃该数据包。

开启 IP 源路由，在 IP 数据报选项中增加源路由选项，可用于测试某特定网络的吞吐率，也可以是数据报绕开出错的网络。然而，可能会导致诸如源地址欺骗(Source Address Spoofing)、IP 欺骗(IP Spoofing)等的网络攻击。

相关配置

↘ 配置 IP 源路由

- 缺省情况开启 IP 源路由功能。
- 可通过 **ip source-route** 开启或关闭该功能。

1.3.8 IP地址池

工作原理

点对点接口可以通过 PPP 协商为对端分配 IP 地址。在 PPP 协商过程中，服务器会校验客户端的认证信息，如果校验通过，服务器就会为客户端分配 IP（如果客户端配置了 IP，且符合服务器的要求，服务器会同意这个 IP 为客户端的 IP），配置可以直接指定对端 IP 地址也可以从地址池获取空闲地址进行分配。

相关配置

↘ 使能地址池功能

- 缺省情况已使能地址池功能。
- 可通过 **ip address-pool local** 开启或关闭该功能。

↘ 创建地址池

- 缺省情况未配置 IP 地址池。
- 可通过 **ip local pool** 命令创建删除地址池。

↘ 配置为 PPP 协商分配 IP 地址给对端

- 缺省情况接口不为对端分配 IP 地址。

- 可通过 **peer default ip address** 命令为对端分配 ip 地址。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置接口IP地址	⚠ 必须配置。用于配置 ip 地址，允许接口运行 IP 协议。	
	ip address	手工配置接口 IP 地址
	ip address negotiate	配置通过 PPP 协商获取 ip 地址
	ip unnumbered	配置接口借用 IP 地址
配置广播报文处理方式	⚠ 可选配置。用于设置 IP 广播地址，允许转发定向广播报文。	
	ip broadcast-address	配置 IP 广播地址
	ip directed-broadcast	允许转发定向广播
配置发送ICMP报文	⚠ 可选配置。用于控制 ICMP 协议报文的收发。	
	ip unreachables	启用 ICMP 协议不可达和主机不可达消息
	ip redirects	启用 ICMP 重定向消息
	ip mask-reply	启用掩码应答消息
配置ICMP差错报文的发送速率	⚠ 可选配置。	
	ip icmp error-interval DF	配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率
	ip icmp error-interval	配置其它 ICMP 差错报文和 ICMP 重定向报文的发送速率
设置IP MTU	⚠ 可选配置。用于配置接口 IP 报文的最大传输单元。	
	ip mtu	设置 MTU 值
设置IP TTL	⚠ 可选配置。用于配置单播报文和广播报文的 TTL。	
	ip ttl	设置 TTL 值
配置IP源路由	⚠ 可选配置。用于配置对接收报文的源路由进行检查。	
	ip source-route	启用 IP 源路由

1.4.1 配置接口IP地址

配置效果

通过配置接口 IP 地址实现 IP 网络通信。

注意事项

-

配置方法

↘ 手工配置接口 IP 地址

- 必须配置。
- 在三层接口模式下配置。

↘ 配置通过 PPP 协商获取接口 IP 地址

- 可选配置。
- 如果点对点接口上没有配置 IP 地址，且需要通过 PPP 协商获取 IP 地址时配置。
- 在三层接口模式下配置。

↘ 配置接口借用 IP 地址

- 可选配置。
- 如果接口上没有配置 IP 地址，且需要向其它接口借用 IP 地址时配置。
- 在三层接口模式下配置。

检验方法

通过 **show ip interface** 可以看到配置的地址生效

相关命令

↘ 手工配置接口 IP 地址

【命令格式】 **ip address** *ip-address network-mask* [**secondary**]

【参数说明】 *ip-addr0065ss*：32 个比特位 IP 地址，8 位一组，以十进制方式表示，组之间用点隔开。

network-mask：32 个比特位网络掩码，“1”表示掩码位，“0”表示主机位。每 8 位一组，以十进制方式表示，组之间用点隔开。

secondary：表示配置的次 IP 地址。

【命令模式】 接口模式

【使用指导】 -

↘ 配置通过 PPP 协商获取接口 IP 地址

【命令格式】 **ip address negotiate**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 只有点对点接口才支持通过 PPP 协商获取 IP 地址，在接口上配置了 **ip address negotiate** 后，对端需要配置 **peer default ip address**。

配置接口借用 IP 地址

【命令格式】 **ip unnumbered** *interface-type interface-number*

【参数说明】 *interface-type*：关联接口类型。

interface-number：关联接口编号。

【命令模式】 接口模式

【使用指导】 无编号接口就是只在接口启动 IP 协议，但是不分配 IP 地址，无编号接口需要关联一个具有 IP 地址的接口。无编号接口产生的 IP 数据包，该数据包的源 IP 地址为关联接口的 IP 地址。另外路由协议进程也根据关联接口的 IP 地址，决定是否往无编号接口发送路由更新报文。应用无编号接口，需要注意以下限制：

以太网接口不能配置成无编号接口。

当串行口封装 SLIP、HDLC、PPP、LAPB、Frame-relay 时，可以配置成无编号接口。但是封装帧中继时，只有点到点子接口才允许配置无编号接口。X.25 封装是不允许配置无编号接口的。

不能用 ping 命令来检测无编号接口是否工作正常，因为无编号接口没有 IP 地址。但是通过 SNMP 可以远程监测到无编号接口状态。

不能通过无编号接口进行网络启动。

配置举例

给接口配置 IP 地址

【配置方法】 在接口 GigabitEthernet 0/0 配置 ip 地址 192.168.23.110 255.255.255.0

```
Ruijie#configure terminal
Ruijie(config)#interface gigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)# no switchport
Ruijie(config-if-GigabitEthernet 0/0)#ip address 192.168.23.110 255.255.255.0
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/0 添加地址成功

```
Ruijie# show ip interface gigabitEthernet 0/0
GigabitEthernet 0/0
  IP interface state is: UP
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    192.168.23.110/24 (primary)
```

给点对点接口配置通过 PPP 协商获取 IP 地址

【配置方法】 在接口点对点接口上配置通过协商获取 ip 地址

```
Ruijie(config)#int virtual-ppp 1
```

```
Ruijie(config-if-Virtual-ppp 1)#ip address negotiate
```

【检验方法】 使用 **show run** 可以看到点对点接口相关配置

```
Ruijie#show run interface virtual-ppp 1

Building configuration...
Current configuration: 48 bytes

interface Virtual-ppp 1
 ip address negotiate
```

1.4.2 配置广播报文处理方式

配置效果

配置接口广播地址为 0.0.0.0，并允许转发定向广播报文。

注意事项

-

配置方法

↘ 配置 IP 广播地址

- 可选配置，有些老的主机可能只认 0.0.0.0 的广播地址，此时需要配置接口的广播地址为 0.0.0.0。
- 在三层接口模式下配置。

↘ 允许转发定向广播

- 可选配置，向处在一个广播域的全部主机发送广播，但是发送者并不处在这个广播域内，此时需要配置允许转发定向广播。
- 在三层接口模式下配置。

检验方法

通过 **show running-config interface** 可以看到配置生效

相关命令

↘ 配置 IP 广播地址

【命令格式】 **ip broadcast-address** *ip-address*

【参数说明】 *ip-address*：IP 网络的广播地址。

【命令模式】 接口模式

【使用指导】 目前IP广播报文的目标地址一般为全“1”，表示为255.255.255.255。RGOS软件可以通过定义产生其它IP地址的广播报文，而且可以同时接收全“1”以及自己定义的广播包。

↘ 允许转发定向广播

【命令格式】 **ip directed-broadcast** [*access-list-number*]

【参数说明】 *access-list-number*：访问列表号，范围从 1-199，1300 - 2699。如果定义了访问列表号，只有匹配该访问列表的 IP 定向广播报文才转换。

【命令模式】 接口模式

【使用指导】 如果在接口上配置了 **no ip directed-broadcast**，RGOS 将丢弃接收到的直连网络的定向广播报文。

配置举例

【配置方法】 在设备端口 gigabitEthernet 0/1 配置 IP 广播报文的目标地址为 0.0.0.0，启用定向广播的转发。

```
Ruijie#configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)# ip broadcast-address  0.0.0.0
Ruijie(config-if-GigabitEthernet 0/1)# ip directed-broadcast
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/1 配置成功

```
Ruijie#show running-config interface gigabitEthernet 0/1
ip directed-broadcast
ip broadcast-address 0.0.0.0
```

1.4.3 配置发送ICMP报文

配置效果

启用接口 ICMP 协议不可达消息，ICMP 重定向消息以及掩码应答消息。

注意事项

-

配置方法

↘ 启用 ICMP 协议不可达消息

- 缺省开启 ICMP 协议不可达消息。
- 可选配置，通过 **no ip unreachables** 禁止该功能。
- 在三层接口模式下配置。

启用 ICMP 重定向消息

- 缺省开启 ICMP 重定向消息。
- 可选配置，通过 **no ip redirects** 禁止该功能。
- 在三层接口模式下配置。

启用 ICMP 掩码应答消息

- 缺省开启 ICMP 掩码应答消息。
- 可选配置，通过 **no ip mask-reply** 禁止该功能。
- 在三层接口模式下配置。

检验方法

通过 **show ip interface** 可以看到配置生效。

相关命令

启用 ICMP 协议不可达消息

【命令格式】 **ip unreachables**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 -

启用 ICMP 重定向消息

【命令格式】 **ip redirects**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 -

启用 ICMP 掩码应答消息

【命令格式】 **ip mask-reply**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 -

配置举例

【配置方法】 在设备端口 gigabitEthernet 0/1 启用 ICMP 协议不可达消息，ICMP 重定向消息以及 ICMP 掩码应答消息功能。

```
Ruijie#configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)# ip unreachables
Ruijie(config-if-GigabitEthernet 0/1)# ip redirects
Ruijie(config-if-GigabitEthernet 0/1)# ip mask-reply
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/1 配置成功

```
Ruijie#show ip interface gigabitEthernet 0/1
GigabitEthernet 0/1
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachabled is: ON
```

1.4.4 配置ICMP报文差错报文的发送速率

配置效果

配置 ICMP 差错报文的发送速率。

注意事项

-

配置方法

↘ 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率

- 可选配置。
- 在全局模式下配置。

↘ 配置其它 ICMP 差错报文的发送速率

- 可选配置。
- 在全局模式下配置。

检验方法

执行 **show running-config** 可以看到配置生效。

相关命令

配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率

【命令格式】 **ip icmp error-interval DF** *milliseconds* [*bucket-size*]

【参数说明】 *milliseconds*：令牌桶的刷新周期，取值范围 0~2147483647，缺省值为 100，单位为毫秒。取值为 0 时，表示不限制 ICMP 差错报文的发送速率。

bucket-size：令牌桶中容纳的令牌数，取值范围 1~200，缺省值为 10。

【命令模式】 全局模式

【使用指导】 为了防止拒绝服务攻击，对 ICMP 差错报文的发送速率进行限制，采用令牌桶算法。

如果 IP 报文需要分片，但是 IP 首部的不可分片位被设置了，设备会向源 IP 地址发送编号为 4 的 ICMP 目的不可达报文，这种 ICMP 差错报文的主要用途是路径 MTU 发现。为了防止其它 ICMP 差错报文太多导致发不出编号为 4 的 ICMP 目的不可达报文，从而导致路径 MTU 发现功能失效，对编号为 4 的 ICMP 目的不可达报文和其它 ICMP 差错报文分别限速。

因为定时器的精度是 10 毫秒，建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于,0 小于 10，实际生效的刷新周期是 10 毫秒，例如配置 5 毫秒 1 个，实际效果是 10 毫秒 2 个；如果令牌桶的刷新周期不是 10 毫秒的整数倍，实际生效的刷新周期自动换算成 10 毫秒的整数倍，例如配置 15 毫秒 3 个，实际效果是 10 毫秒 2 个。

配置其它 ICMP 差错报文的发送速率

【命令格式】 **ip icmp error-interval** *milliseconds* [*bucket-size*]

【参数说明】 *milliseconds*：令牌桶的刷新周期，取值范围 0~2147483647，缺省值为 100，单位为毫秒。取值为 0 时，表示不限制 ICMP 差错报文的发送速率。

bucket-size：令牌桶中容纳的令牌数，取值范围 1~200，缺省值为 10。

【命令模式】 全局模式

【使用指导】 为了防止拒绝服务攻击，对 ICMP 差错报文的发送速率进行限制，采用令牌桶算法。

因为定时器的精度是 10 毫秒，建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于,0 小于 10，实际生效的刷新周期是 10 毫秒，例如配置 5 毫秒 1 个，实际效果是 10 毫秒 2 个；如果令牌桶的刷新周期不是 10 毫秒的整数倍，实际生效的刷新周期自动换算成 10 毫秒的整数倍，例如配置 15 毫秒 3 个，实际效果是 10 毫秒 2 个。

配置举例

【配置方法】 配置 IP 首部不可分片位触发的 ICMP 目的不可达报文的发送速率为 1 秒 100 个，配置其它 ICMP 差错报文的发送速率为 1 秒 10 个。

```
Ruijie(config)# ip icmp error-interval DF 1000 100
Ruijie(config)# ip icmp error-interval 1000 10
```

【检验方法】 执行 **show running-config** 可以看到配置生效

```
Ruijie#show running-config | include ip icmp error-interval
ip icmp error-interval 1000 10
ip icmp error-interval DF 1000 100
```

1.4.5 配置IP MTU

配置效果

调整 IP 包最大传输单元。

注意事项

-

配置方法

- 可选配置，所有在同一物理网段上的设备，当互联接口的 IP MTU 不一致时需要配置为一致。
- 在三层接口模式下配置。

检验方法

通过 **show ip interface** 可以看到配置生效

相关命令

↘ 配置 IP MTU

【命令格式】 **ip mtu** *bytes*

【参数说明】 *bytes*：IP 包最大传输单元，以字节为单位，范围 68~1500。

【命令模式】 接口模式

【使用指导】 -

配置举例

【配置方法】 将 gigabitEthernet 0/1 接口的 IP MTU 值设为 512 字节

```
Ruijie#configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# no switchport
Ruijie(config-if-GigabitEthernet 0/1)# ip mtu 512
```

【检验方法】 使用 **show ip interface** 可以看到接口 GigabitEthernet 0/1 配置成功

```
Ruijie# show ip interface gigabitEthernet 0/1
IP interface MTU is: 512
```

1.4.6 配置IP TTL

配置效果

修改接口的 IP TTL 值。

注意事项

-

配置方法

- 可选配置。
- 在三层接口模式下配置。

检验方法

通过 **show run-config** 可以看到配置生效

相关命令

↘ 配置 IP TTL

【命令格式】 **ip ttl** *value*

【参数说明】 *value*：TTL 值，取值范围是 0~255。

【命令模式】 全局模式

【使用指导】 -

配置举例

【配置方法】 配置本机发送的单播报文的缺省 TTL 值为 100。

```
Ruijie#configure terminal
Ruijie(config)#ip ttl 100
```

【检验方法】 通过 **show run-config** 可以看到配置生效

```
Ruijie#show running-config
ip ttl 100
```

1.4.7 配置IP源路由

配置效果

开启或关闭 IP 源路由信息的处理功能。

注意事项

-

配置方法

- 缺省情况下开启 IP 源路由功能。
- 可选配置，通过 **no ip source-route** 可关闭 IP 源路由功能。

检验方法

通过 **show run-config** 可以看到配置生效。

相关命令

↘ 配置 IP 源路由

【命令格式】 **ip source-route**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

配置举例

【配置方法】 关闭了 IP 源路由信息的处理功能。

```
Ruijie#configure terminal
Ruijie(config)# no ip source-route
```

【检验方法】 通过 **show run-config** 可以看到配置生效

```
Ruijie#show running-config
no ip source-route
```

1.4.8 配置IP地址池

配置效果

PPP 协议为客户端分配 IP 地址。

注意事项

-

配置方法

↘ 使能 IP 地址池功能

- 可选配置。
- 在全局配置模式下配置。

↘ 创建 IP 地址池

- 可选配置。
- 在使能 IP 地址池功能后才能配置，关闭 IP 地址池功能后会自动删除已创建的地址池。
- 在全局模式下配置。

↘ 配置 PPP 协商分配 IP 地址给对端

- 可选配置。
- 在三层接口模式下配置。

检验方法

通过 **show run-config** 可以看到配置生效。

相关命令

↘ 配置使能 IP 地址池

【命令格式】 **ip address-pool local**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 缺省情况下，IP 地址池功能开启，用户可以配置 IP 地址池，PPP 用户可以用 IP 地址池分配对端的 IP 地址。
如果想关闭 IP 地址池功能，可以使用 no ip address-pool local 命令，此时会删除所有之前配置的 IP 地址池。

配置创建 IP 地址池

【命令格式】 **ip local pool** *pool-name low-ip-address* [*high-ip-address*]

【参数说明】 *pool-name*：指定本地 IP 地址池的名字，**default** 为默认地址池名字。

low-ip-address：IP 地址池中最小的 IP 地址。

high-ip-address：可选，IP 地址池中最大的 IP 地址。如果未指定最大的 IP 地址，则 IP 地址池中只有一个地址，即是 *low-ip-address*

【命令模式】 全局配置模式

【使用指导】 可以用该命令创建一个或多个 IP 地址池，供 PPP 分配 IP 地址给连接的用户。

配置 PPP 协商分配 IP 地址给对端

【命令格式】 **peer default ip address** {*ip-address* | **pool** [*pool-name*] }

【参数说明】 *ip-address*：指定为对端分配的 IP 地址。

pool-name：可选， 指定分配 IP 地址的地址池名字，若未配置该参数，则在 default 地址池中分配 IP 地址。

【命令模式】 接口模式

【使用指导】 当对端接口还未配置 IP 地址而本端设备已经有 IP 地址时，可配置本端设备为对端接口分配 IP 地址。这时，需要在对端设备上配置 **ip address negotiate** 命令，在本端设备上配置 **peer default ip address** 命令，使对端接口接受由 PPP 协商分配的 IP 地址。

该命令仅支持封装 PPP 或 SLIP 协议的点对点接口下配置。

peer default ip address pool 命令，是从 IP 地址池里分配出一个 IP 地址给对端， 这个 IP 地址池是通过 ip local pool 命令配置的地址池。

peer default ip address *ip-address* 命令，直接给对端指定一个 IP 地址，该命令不能在虚拟模板接口及异步口上配置。

配置举例

【配置方法】 配置接口 dialer1 从地址池 quark 为对端分配分配 IP 地址

```
Ruijie#configure terminal
Ruijie(config)# ip address-pool local
Ruijie(config)# ip local pool quark 172.16.23.2 172.16.23.255
Ruijie(config)# interface dialer 1
Ruijie(config-if-dialer 1)# peer default ip address pool quark
```

【检验方法】 通过 **show run-config** 可以看到配置生效

```
Ruijie#show running-config
ip local pool quark 172.16.23.2 172.16.23.255
!
interface dialer 1
 peer default ip address pool quark
```

1.5 监视与维护

清除各类信息

-

查看运行情况

作用	命令
显示接口 IP 信息	**show ip interface** [*interface-type interface-number* | **brief**]
显示 IP 报文统计值	**show ip packet statistics** [**total |** *interface-name*]
显示地址池统计情况	**show ip pool [***pool-name***]**

查看调试信息

-

2 ARP

2.1 概述

在局域网中，每个 IP 网络设备都有两个地址：1) 本地地址，由于它包含在数据链路层的帧头中，更准确地说应该是数据链路层地址，但实际上对本地地址进行处理的是数据链路层中的 MAC 子层，因此习惯上称为 MAC 地址，MAC 地址在局域网上代表着 IP 网络设备；2) 网络地址，在互联网上代表着 IP 网络设备，同时它也说明了该设备所属的网络。

局域网上两台 IP 设备之间需要通信，必须要知道对方的 48 比特的 MAC 地址。根据 IP 地址来获知 MAC 地址的过程称为地址解析。地址解析的方式有两类：1) 地址解析协议 (ARP) ；2) 代理地址解析协议 (Proxy ARP) 。关于 ARP 、Proxy ARP，分别在 RFC 826，RFC 1027 文档中描述。

ARP(Address Resolution Protocol，地址解析协议)是用来绑定 MAC 地址和 IP 地址的，以 IP 地址作为输入，ARP 能够知道其关联的 MAC 地址。一旦知道了 MAC 地址，IP 地址与 MAC 地址对应关系就会保存在设备的 ARP 缓存中。有了 MAC 地址，IP 设备就可以封装链路层的帧，然后将数据帧发送到局域网上去。缺省配置下，以太网上 IP 和 ARP 的封装为 Ethernet II 类型。

协议规范

- RFC826：An Ethernet Address Resolution Protocol
- RFC1027：Using ARP to implement transparent subnet gateways

2.2 典型应用

典型应用	场景描述
在局域网内提供地址解析协议服务	在同一网段中，主机学习其他设备的 MAC 地址，需要用到地址解析协议。
使用代理ARP实现透明的子网网关	通过代理地址解析服务，允许主机在不知道另一个网络是否存在的情况下和另一网络内的主机直接通讯。

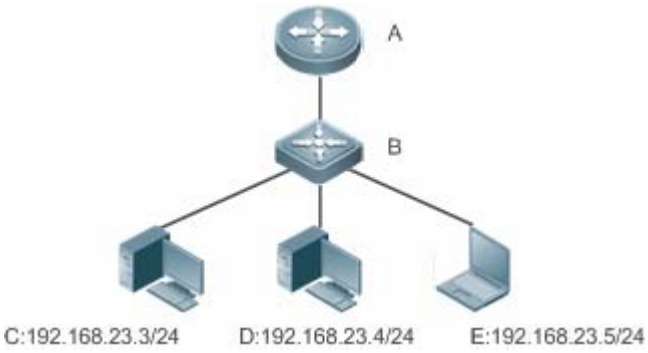
2.2.1 在局域网内提供地址解析协议服务

应用场景

在所有 IPv4 局域网内，都需要用到 ARP 协议。

- 主机需要通过 ARP 协议来学习其他设备的 MAC 地址，只有学到 MAC 地址后，主机才可以和其他设备通信。

图 2-1



【注释】 A 为路由器
B 为交换机，作为用户主机网段的网关。
C、D、E 为用户主机

功能部属

- 在局域网内运行 ARP 协议，实现 IP 地址和 MAC 地址的映射。

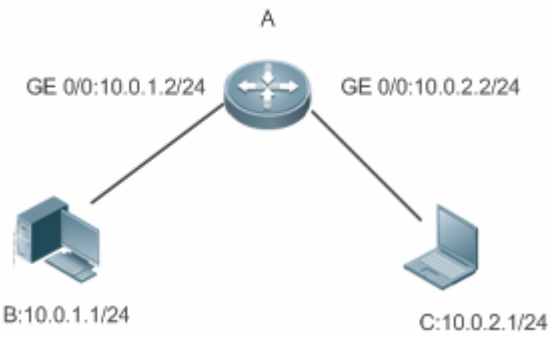
2.2.2 使用代理ARP实现透明的子网网关

应用场景

在不同的 IPv4 局域网内，实现透明的子网网关。

- 通过在设备上配置代理 ARP 的功能，实现不同网段内主机的直接通讯。

图 2-2



【注释】 A 为路由器，连接两个局域网
B、C 为用户主机，不配置默认网关，在不同的子网

功能部属

- 在子网网关上运行代理 ARP 功能，可以帮助没有路由信息的主机获得其它子网 IP 地址的 MAC 地址。

2.3 功能详解

功能特性

功能特性	作用
静态ARP	用户手工指定 IP 地址和 MAC 地址的映射，防止设备学到错误的 ARP 表项而影响网络。
ARP属性设置	用户指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、未解析 ARP 表项数上限。
免费ARP	检测 IP 地址冲突，以及让外围设备更新本机的 ARP。
代理ARP	代理应答请求其他设备的 ARP 请求。
ARP可信检测	通过 NDU（邻居不可达探测），保证学习的 ARP 表项正确。
关闭动态ARP学习	关闭动态 ARP 学习功能后，接口不再进行动态 ARP 的学习。

2.3.1 静态ARP

静态 ARP 包括手工配置的静态 ARP 和认证下发的静态 ARP。手工配置的静态 ARP 优先级大于认证下发的静态 ARP。静态 ARP 能够防止设备学到错误的 ARP 表项而影响网络。

工作原理

静态 ARP，设备不会再去主动更新 ARP 表项，并且永久存在。

设备转发三层报文时，以太头部的目的 MAC 地址将采用静态配置的 MAC 地址来封装。

相关配置

↘ 配置静态 ARP

手工配置的静态 ARP，在全局模式下，使用 **arp** *ip-address mac-address type* 命令配置静态 ARP 表项。缺省情况下用户没有配置任何静态 ARP 表项。ARP 封装只支持 Ethernet II 类型，用 arpa 表示。

2.3.2 ARP属性设置

用户指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、未解析 ARP 表项数上限、接口 ARP 学习数量限制、单板 ARP 学习数量限制。

工作原理

↘ ARP 超时设置

ARP 超时设置只对动态学习到的 IP 地址和 MAC 地址映射起作用。当一个 ARP 表项超时后，设备会发送单播 ARP 请求报文探测对方是否在线，假如能收到对方的 ARP 应答，则说明对方仍在线，该 ARP 表项不会删除，否则会删除该 ARP 表项。

超时时间设置得越短，ARP 缓冲中保存的映射表就越真实，但是 ARP 消耗网络带宽也越多。

ARP 请求重传时间间隔和次数

IP 地址解析成 MAC 地址时连续发送 ARP 请求的时间间隔和次数。时间间隔越短，解析速率更快。次数越多，解析成功率更大，但是 ARP 消耗网络带宽也越多。

未解析 ARP 表项的数量限制

在局域网中可能存在对网关的攻击，扫描网段，使网关生成大量未解析的ARP表项，从而使网关无法正常学习主机的MAC地址。为了防止这种攻击，用户可以配置未解析 ARP 表项的数量限制。

接口 ARP 学习数量限制

改成通过配置指定接口的用户 ARP 表项个数，灵活控制 ARP 表项资源的按需分配，防止表项资源浪费。

单板 ARP 学习数量限制

通过配置指定槽数的 ARP 学习数量，可以限制不同槽数的 ARP 能力，灵活控制 ARP 表项的按槽分配和按需分配。

相关配置

ARP 超时设置

在接口模式下，使用命令 **arp timeout** *seconds* 配置 ARP 的超时时间。默认情况下超时时间为 3600 秒，用户可以根据实际情况重新调整。

ARP 请求重传时间间隔和次数

- 在全局模式下，使用命令 **arp retry interval** *seconds* 配置 ARP 的重传时间间隔。默认情况下超时时间为 1 秒，用户可以根据实际情况重新调整。
- 在全局模式下，使用命令 **arp retry times** *number* 配置 ARP 的重传次数。默认情况下可以连续发送 5 次，用户可以根据实际情况重新调整。

未解析 ARP 表项的数量限制

在全局模式下，使用命令 **arp unresolve** *number* 配置 ARP 的未解析表项数。默认为 arp 容量的最大值，用户可以根据实际情况重新调整。

接口 ARP 学习数量限制

在接口模式下，使用命令 **arp cache interface-limit** *limit* 配置接口 ARP 的学习数量限制。默认不限制接口上 ARP 学习的数量，用户可以根据实际情况重新调整。此数量限制包含静态 ARP。

2.3.3 免费ARP

工作原理

免费 ARP 报文是一种特殊的 ARP 报文，该报文的发送端 IP 地址和目标 IP 地址都是本机 IP 地址。免费 ARP 的主要用途有：

1. IP 地址冲突检测。当设备收到免费 ARP 报文后，如果发现报文中的 IP 地址和自己的 IP 地址相同，向发送免费 ARP 报文的设备返回一个 ARP 应答，告诉该设备 IP 地址冲突。
2. 当接口的 MAC 地址变化时，发送免费 ARP 通知其它设备更新 ARP 表项。

设备具有免费 ARP 报文学习功能。当设备收到免费 ARP 报文时，设备判断是否存在和免费 ARP 报文源 IP 地址对应的动态 ARP 表项，如果存在，根据免费 ARP 报文中携带的信息更新 ARP 表项。

相关配置

↘ 配置免费 ARP

接口模式下，使用命令 **arp gratuitous-send interval** *seconds* [*number*]允许接口定时发送免费 ARP 请求报文。缺省情况下接口上该功能是关闭的。一般在该接口充当下联设备网关时，需要开启这个功能，定时更新使下联设备的网关 mac，防止他人冒充网关。

2.3.4 代理ARP

工作原理

设备的代理 ARP 功能可以帮助没有路由信息的主机，获得其它子网 IP 地址的 MAC 地址。比如设备接收到一个 ARP 请求，ARP 请求的发送者 IP 地址与目标 IP 地址不属于同一网段，而设备又知道所请求 IP 地址的路由，设备就会发送 ARP 响应，响应的 MAC 地址为设备自身的以太网 MAC 地址，这个过程就是代理 ARP 的功能。

相关配置

↘ 配置代理 ARP

- 接口模式下，使用命令 **ip proxy-arp** 开启代理 ARP 功能。
- 缺省情况下开启了代理 ARP 功能。

2.3.5 ARP可信检测

工作原理

该命令用于防止 arp 欺骗导致无用的 arp 表项过多占用设备资源。在三层接口开启 arp 可信检测功能后，从该接口上收到 arp 请求报文：

1. 如果对应表项不存在，则创建动态 arp 表项，并经过 1 到 5 秒的一个随机时间后进入 NUD（邻居不可达探测），即将新学习的 arp 表项设置为老化状态并单播 arp 请求，在老化时间内收到对端 arp 更新，则保存表项，否则直接删除该表项。
2. 如果对应 arp 表项已经存在，则不进行 NUD 探测逻辑。
3. 如果已有的动态 arp 表项的 MAC 地址被更新，也走 NUD 探测逻辑。

该功能由于在 ARP 学习过程中增加了一个严格确认的过程，所以开启该功能会影响到 ARP 的学习性能。

关闭该功能后，arp 表项的学习和更新不再走 NUD 逻辑。

相关配置

↘ 配置 ARP 可信检测

接口模式下，使用命令 **arp trust-monitor enable** 命令开启 ARP 可信检查功能，缺省情况下没有开启该功能。

2.3.6 关闭动态ARP学习

工作原理

配置关闭动态 ARP 学习后，接口上禁止学习动态 ARP。

相关配置

↘ 配置关闭动态 ARP 学习

- 缺省情况下接口使能动态 arp 的学习。
- 在接口模式下，使用命令 **no arp-learning enable** 命令关闭动态 ARP 学习功能。

2.4 配置详解

配置项	配置建议 & 相关命令	
配置静态ARP	⚠ 可选配置，用于 IP 地址和 MAC 地址的静态绑定。	
	arp	定义静态 ARP
配置ARP属性	⚠ 可选配置，用于指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、未解析 ARP 表项数上限、接口 ARP 学习数量限制、单板 ARP 学习数量限制。	
	arp timeout	配置 ARP 超时时间
	arp retry interval	配置 ARP 请求重传时间间隔
	arp unresolve	配置未解析 ARP 表项的数量限制

	arp cache interface-limit	配置接口 ARP 学习数量限制
配置免费ARP	⚠ 可选配置，用于检测 IP 地址冲突，以及让外围设备更新本机的 ARP。	
	arp gratuitous-send interval	开启定时发送免费 ARP 的功能
配置代理ARP	⚠ 可选配置，用于代理应答请求不同子网内其他设备的 ARP 请求。	
	ip proxy-arp	开启代理 ARP 功能。
配置 ARP可信检测	⚠ 可选配置，用于发送单播 ARP 请求确认，以保证学习 ARP 表项正确性。	
	arp trusted-monitor enable	开启 ARP 可信检测功能
配置关闭动态ARP学习	⚠ 可选配置，用于禁止接口上的动态 ARP 学习。	
	no arp-learning enable	关闭接口的动态 ARP 学习功能

2.4.1 配置静态ARP

配置效果

用户手工指定 IP 地址和 MAC 地址的映射，防止设备学到错误的 ARP 表项而影响网络。

注意事项

对于三层设备，配置完静态 ARP 表项后，设备必须在学习到该静态 ARP 表项的 MAC 地址对应的物理端口后才能进行正常的三层路由。

配置方法

↘ 配置静态 ARP

- 可选配置
- 在汇聚设备上，可以通过静态绑定上联设备的 IP 和 MAC 地址的映射，防止设备因受到 ARP 攻击而更改掉上联设备的 ARP 表项的 MAC 地址，导致网络异常。
- 在全局模式下配置

检验方法

使用命令 **show running-config** 查看命令是否生效，或使用命令 **show arp static** 查看是否成功创建了静态 ARP 缓存表。

相关命令

配置静态 ARP

【命令格式】 **arp** *ip-address mac-address type*

【参数说明】 *ip-address*：与 MAC 地址对应的 IP 地址，分为四组十进制表示的数值，组之间用点隔开。

mac-address：数据链路层地址，48 个比特位组成。

type：ARP 封装类型。对于以太网接口，关键字为 arpa。

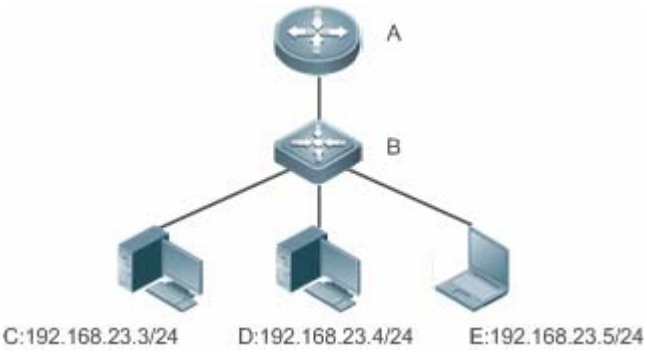
【命令模式】 全局模式

【使用指导】 RGOS 使用 ARP 缓冲表，根据 32 个比特位 IP 地址查找 48 个比特位的 MAC 地址。

由于大多数主机支持动态 ARP 解析，所以通常不需要配置静态 ARP 映射。利用 **clear arp-cache** 命令可以删除动态学习到的 ARP 映射。

配置举例

【网络环境】



【注释】 A 为路由器

B 为交换机，作为用户主机网段的网关。

C、D、E 为用户主机

【配置方法】 在设备 B 上配置静态 ARP 表项，静态绑定设备 A 的 IP 和 MAC 地址映射。

```
Ruijie(config)#arp 192.168.23.1 00D0.F822.334B arpa
```

【检验方法】 通过 **show arp static** 命令可查看静态 ARP 表项：

```
Ruijie(config)#show arp static
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.23.1     <static>  00D0.F822.334B  arpa
 1  static arp entries exist.
```

常见配置错误

- 静态绑定的 MAC 地址错误。

2.4.2 配置ARP属性

配置效果

用户指定 ARP 表项的超时时间、ARP 请求重传次数和间隔、未解析 ARP 表项数上限、接口 ARP 学习数量限制、单板 ARP 学习数量限制。

注意事项

无

配置方法

ARP 超时设置

- 可选配置
- 局域网中如果用户上下线较频繁，则可以将 ARP 超时时间设置小一点，可以将无效的 ARP 表项尽早删除。
- 在接口模式下配置

ARP 请求重传时间间隔和次数

- 可选配置
- 在网络带宽资源不足时，可以将重传时间间隔配大，次数配小，以减少网络带宽的消耗。
- 在全局模式下配置

未解析 ARP 表项的数量限制

- 可选配置
- 在网络带宽资源不足时，可以将未解析 ARP 表项的数量配小，以减少网络带宽的消耗。
- 在全局模式下配置

接口 ARP 学习数量限制

- 可选配置
- 在接口模式下配置

单板 ARP 学习数量限制

- 可选配置
- 在全局模式下配置

检验方法

使用命令 **show arp timeout** 可以查看所有接口的老化超时时间。

使用命令 **show running-config** 查看 ARP 请求重传时间间隔和次数、未解析 ARP 表项是数量限制、接口 ARP 学习数量限制、单板 ARP 学习数量限制命令是否生效。

相关命令

ARP 超时设置

【命令格式】 **arp timeout** *seconds*

【参数说明】 *seconds*：超时时间，以秒为计算单位，默认值为 3600，范围 0-2147483。

【命令模式】 接口模式

【使用指导】 ARP 超时设置只对动态学习到的 IP 地址和 MAC 地址映射起作用。超时时间设置得越短，ARP 缓存中保存的映射表就越真实，但是 ARP 消耗网络带宽也越多，所以需要权衡利弊。除非有特别的需要，否则一般不需要配置 ARP 超时时间。

ARP 请求重传时间间隔和次数

【命令格式】 **arp retry interval** *seconds*

【参数说明】 *seconds*：<1-3600>,ARP 请求的重传时间可以设置为 1~3600 秒，默认值为 1 秒。

【配置模式】 全局模式

【使用指导】 当发现本设备有频繁的向外发送 ARP 请求，引起网络繁忙等其它问题时，可以将 ARP 请求的重传时间设置长一点，一般不要超过动态 ARP 表项的老化时间。

未解析 ARP 表项的数量限制

【命令格式】 **arp unresolve** *number*

【参数说明】 *number*：未解析 ARP 表项的最大个数，取值范围为< 1-8192 >。默认值为 8192。

【配置模式】 全局模式

【使用指导】 当发现 ARP 缓存表中出现大量未解析表项，并且一段时间后还没有消失时，可以用此命令限制未解析表项的个数。

接口 ARP 学习数量限制

【命令格式】 **arp cache interface-limit** *limit*

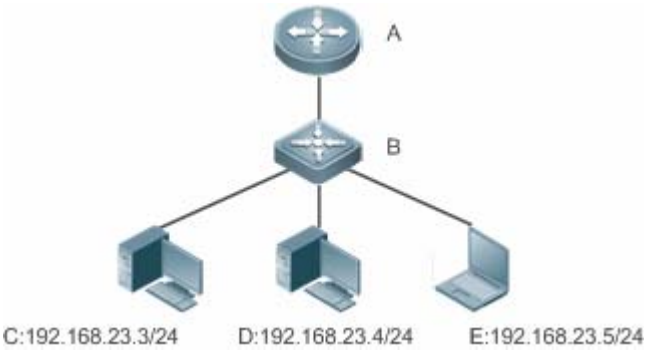
【参数说明】 *limit*：指定接口所能学习的 ARP 数量最大限制，包括静态配置和动态学习的 ARP，取值范围为 0-设备支持的 ARP 表项容量，0 表示不限制接口 ARP 学习数量。

【配置模式】 接口模式

【使用指导】 限制接口的 ARP 学习数量，可防止恶意的 ARP 攻击，让设备生成大量的 ARP 表项，占用过多的表项资源。配置的值必须不小于当前接口已经学习到的 ARP 表项数量，否则配置不生效。该限制受限于设备支持的 ARP 容量。

配置举例

【网络环境】



【注释】 A 为路由器

B 为交换机，作为用户主机网段的网关。

C、D、E 为用户主机

【配置方法】

- 配置接口 GigabitEthernet 0/1 下的 ARP 超时时间为 60 秒
- 配置接口 GigabitEthernet 0/1 下的 ARP 学习数量限制为 300
- 配置 ARP 请求重传时间间隔为 3 秒
- 配置 ARP 请求重传次数为 4 次
- 配置未解析 ARP 表项数量限制为 4096

```
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#arp timeout 60
Ruijie(config-if-GigabitEthernet 0/1)#arp cache interface-limit 300
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#arp retry interval 3
Ruijie(config)#arp retry times 4
Ruijie(config)#arp unresolve 4096
```

【检验方法】

- 通过 **show arp timeout** 查看接口的老化时间
- 通过 **show running-config** 查看 ARP 请求重传时间间隔和次数、未解析 ARP 表项是数量限制、接口 ARP 学习数量限制、单板 ARP 学习数量限制

```
Ruijie#show arp timeout
Interface               arp timeout(sec)
----------------------  ----------------
GigabitEthernet 0/1     60
GigabitEthernet 0/2     3600
GigabitEthernet 0/4     3600
GigabitEthernet 0/5     3600
GigabitEthernet 0/7     3600
VLAN 100                3600
VLAN 111                3600
Mgmt 0                  3600

Ruijie(config)# show running-config
arp unresolve 4096
```

```
arp retry times 4
arp retry interval 3
!
interface GigabitEthernet 0/1
 arp cache interface-limit 300
```

常见配置错误

无

2.4.3 配置免费ARP

配置效果

接口定时发送免费 ARP 报文。

注意事项

无

配置方法

- 可选配置
- 设备做用户网关时，为了防止因为 ARP 欺骗导致其他用户学习到错误的网关 MAC 后会一直上不了网，需要在接口上开启免费 ARP 功能。
- 在接口模式下配置

检验方法

使用 **show running-config interface** [*name*]查看是否配置成功。

相关命令

↘ 开启定时发送免费 ARP 的功能

【命令格式】 **arp gratuitous-send interval** *seconds* [*number*]

【参数说明】 *seconds*：发送免费 ARP 请求的时间间隔，单位秒，取值范围<1-3600>。

number：发送免费 ARP 请求的数量，缺省值是 1，取值范围<1-100>。

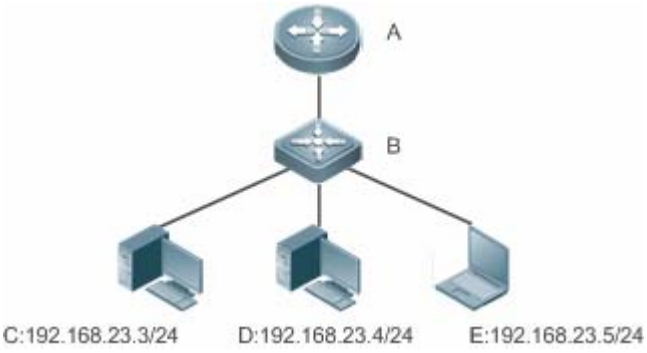
【命令模式】 接口模式

【使用指导】 当设备的网络接口作为下联设备的网关时，如果下联设备中有冒充网关的行为，则可以在此接口配置定时发

送免费 ARP 请求，公告自己才是真正的网关。

配置举例

【网络环境】



【注释】 A 为路由器

B 为交换机，作为用户主机网段的网关。

C、D、E 为用户主机

【配置方法】 配置 GigabitEthernet 0/0 口发送免费 ARP 功能，频率为每 5 秒发送一个免费 ARP 请求报文。

```
Ruijie(config-if-GigabitEthernet 0/0)#arp gratuitous-send interval 5
```

【检验方法】 使用 **show running-config interface** 命令查看配置是否生效

```
Ruijie#sh running-config interface gigabitEthernet 0/0

Building configuration...
Current configuration : 127 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 arp gratuitous-send interval 5
```

常见配置错误

无

2.4.4 配置代理ARP

配置效果

设备代理应答非本机的 ARP 请求报文。

注意事项

缺省关闭代理 ARP 功能。

配置方法

- 可选配置。
- 没有路由信息的主机需要获得其它子网 IP 地址的 MAC 地址，设备需要开启代理 ARP 功能，代理应答 ARP。
- 在接口模式下配置

检验方法

使用 **show ip interface** [*name*]命令查看是否配置成功。

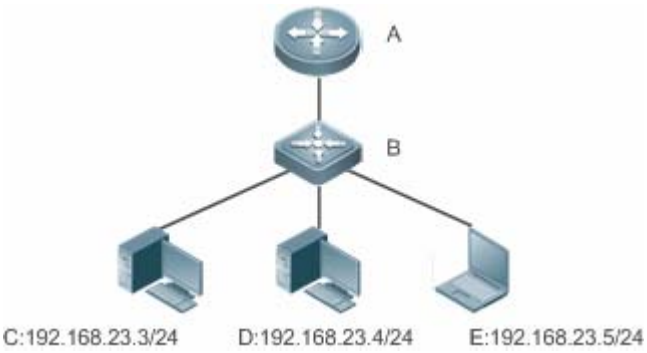
相关命令

↘ 开启代理 ARP 功能

【命令格式】 **ip proxy-arp**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 -

配置举例

【网络环境】



【注释】 A 为路由器
B 为交换机，作为用户主机网段的网关。
C、D、E 为用户主机

【配置方法】 配置 GigabitEthernet 0/0 口开启代理 ARP 功能

```
Ruijie(config-if-GigabitEthernet 0/0)#ip proxy-arp
```

【检验方法】 使用 **show ip interface** 命令查看是否配置成功

```
Ruijie#show ip interface gigabitEthernet 0/0
GigabitEthernet 0/0
  IP interface state is: DOWN
  IP interface type is: BROADCAST
  IP interface MTU is: 1500
  IP address is:
    No address configured
  IP address negotiate is: OFF
  Forward direct-broadcast is: OFF
  ICMP mask reply is: ON
  Send ICMP redirect is: ON
  Send ICMP unreachable is: ON
  DHCP relay is: OFF
  Fast switch is: ON
  Help address is: 0.0.0.0
  Proxy ARP is: ON
ARP packet input number: 0
  Request packet     : 0
  Reply packet       : 0
  Unknown packet     : 0
TTL invalid packet number: 0
ICMP packet input number: 0
 Echo request       : 0
 Echo reply         : 0
 Unreachable        : 0
 Source quench      : 0
 Routing redirect   : 0
```

常见配置错误

无

2.4.5 配置ARP可信检测

配置效果

开启 arp 可信检测功能，在收到 arp 请求报文后，如果对应表项不存在，进入 NUD（邻居不可达探测）。如果已有的动态 arp 表项的 MAC 地址被更新，马上走 NUD 探测逻辑，起到防止 arp 攻击的作用。

注意事项

该功能由于在 ARP 学习过程中增加了一个严格确认的过程，所以开启该功能会影响到 ARP 的学习性能。

配置方法

- 可选配置。
- 如果有要求严格学习 ARP 表项的需求时，设备上可以开启 arp 可信功能，设备在收到 arp 请求报文后，如果之前不存在对应 arp 表项，则需要发送单播 ARP 请求报文，在确认对端真实存在后才学习 ARP 表项，否则不学习 ARP 表项。在 arp 表项的 mac 地址发生了变化后，马上走 NUD 探测，防止 arp 欺骗。
- 在接口模式下配置

检验方法

使用 **show running-config interface** [*name*] 查看是否配置成功。

相关命令

开启 ARP 可信检测功能

【命令格式】 **arp trust-monitor enable**

【参数说明】 -

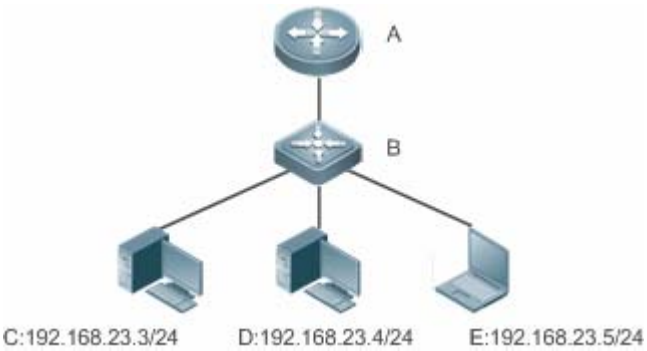
【命令模式】 接口模式

【使用指导】

- 开启该功能，如果对应 arp 表项已经存在，且 mac 地址没发生更新，则不进行 NUD 探测逻辑。
- 开启该功能，如果已有的动态 arp 表项的 mac 地址被更新，则马上走 NUD 探测逻辑。
- 关闭该功能后，arp 表项的学习和更新不需要 NUD 过程。

配置举例

【网络环境】



【注释】 A 为路由器
B 为交换机，作为用户主机网段的网关。
C、D、E 为用户主机

【配置方法】 配置 GigabitEthernet 0/0 口开启 ARP 可信检测功能

```
Ruijie(config-if-GigabitEthernet 0/0)#arp trust-monitor enable
```

【检验方法】 使用 **show running-config interface** 查看是否配置是否生效

```
Ruijie#show running-config interface gigabitEthernet 0/0

Building configuration...
Current configuration : 184 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 arp trust-monitor enable
```

常见配置错误

无

2.4.6 配置关闭动态ARP学习功能

配置效果

在接口上关闭动态 ARP 的学习功能后，接口将不能进行动态 ARP 学习。

注意事项

无

配置方法

- 可选配置
- 在接口模式下配置

检验方法

使用 **show running-config interface** [*name*] 查看是否配置成功。

相关命令

↘ 关闭动态 ARP 学习的功能

【命令格式】 **no arp-learning enable**

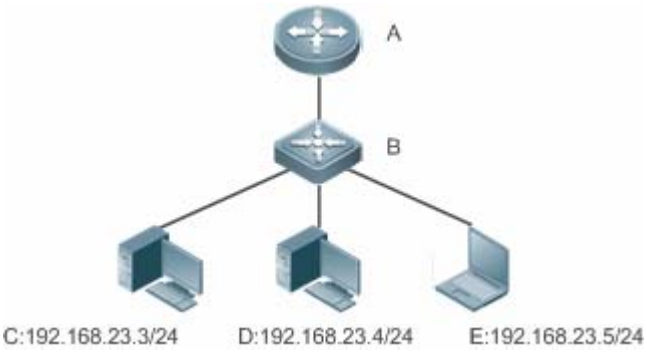
【参数说明】 -

【命令模式】 接口模式

【使用指导】 如果确认设备已经学习到需要学习的动态 ARP 表项，通过 web 将动态 ARP 转化为静态 ARP 后，建议开启该功能，否则不建议开启该功能。开启动态 ARP 不学习功能后，存在动态 ARP 表项的话，如果用户需要将动态 ARP 表项转化为静态 ARP 表项，可以通过 web 配置，如果用户需要清除掉该动态 ARP 表项，不允许某一用户上网，则可以通过 clear arp 命令，否则动态 ARP 表项进行正常老化，在老化时间到后，该动态 ARP 表项被清除掉。开启接口停止动态 ARP 学习功能后，则 AnyIP 功能、ARP 可信检测功能失效。

配置举例

【网络环境】



【注释】 A 为路由器
B 为交换机，作为用户主机网段的网关。
C、D、E 为用户主机

【配置方法】 配置 GigabitEthernet 0/0 口禁止动态 ARP 学习功能。

```
Ruijie(config-if-GigabitEthernet 0/0)#no arp-learning enable
```

【检验方法】 使用 **show running-config interface** 命令查看配置是否生效

```
Ruijie#sh running-config interface gigabitEthernet 0/0

Building configuration...
Current configuration : 127 bytes
!
interface GigabitEthernet 0/0
 duplex auto
 speed auto
 ip address 30.1.1.1 255.255.255.0
 no arp-learning enable
```

常见配置错误

无

2.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除动态 ARP 表项。在网关认证模式下，不会删除认证 VLAN 下的动态 ARP 表项。	**clear arp-cache**

查看运行情况

作用	命令
显示 ARP 表	**show ip arp**
显示 ARP 表项相应计数	**show arp counter**
显示动态 ARP 表项的老化时间	**show arp timeout**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
显示 ARP 报文的收发情况	**debug arp**
显示 ARP 表项的创建删除情况	**debug arp event**

3 IPv6

3.1 概述

随着 Internet 的迅速增长以及 IPv4 地址空间的逐渐耗尽，IPv4 的局限性就越来越明显。对新一代互联网络协议（Internet Protocol Next Generation - IPng）的研究和实践已经成为热点，Internet 工程任务工作小组(IETF)的 IPng 工作组确定了 IPng 的协议规范，并称之为"IP 版本 6"（IPv6），该协议的规范在 RFC2460 中有详细的描述。

IPv6 的主要特点

更大的地址空间

地址长度由 IPv4 的 32 位扩展到 128 位，约有 2^128 个地址，IPv6 采用分级地址模式，支持从 Internet 核心主干网到企业内部子网等多级子网地址分配方式。

简化了报头格式

新 IPv6 报文头的设计原则是力图将报文头开销降到最低，因此将一些非关键性字段和可选字段从报文头中移出，放到扩展的报文头中，虽然 IPv6 地址长度是 IPv4 的四倍，但报头仅为基本 IPv4 首部的两倍。改进的 IPv6 报文头在设备转发时拥有更高的效率，例如 IPv6 报文头中没有校验和，IPv6 设备在转发中不需要去处理分片(分片由发起者完成)。

高效的层次寻址及路由结构

IPv6 采用聚合机制，定义非常灵活的层次寻址及路由结构，同一层次上的多个网络在上层设备中表示为一个统一的网络前缀，这样可以显著减少设备必须维护的路由表项，这也大大降低了设备的选路和存储开销。

简单的管理：即插即用

通过实现一系列的自动发现和自动配置功能，简化网络节点的管理和维护。比如邻接节点发现（Neighbor Discovery）、最大传输单元发现（MTU Discovery）、路由器通告（Router Advertisement）、路由器请求（Router Solicitation）、节点自动配置（Auto-configuration）等技术就为即插即用提供了相关的服务。特别要提到的是 IPv6 支持全状态和无状态两种地址配置方式，在 IPv4 中，动态主机配置协议 DHCP 实现了主机 IP 地址及其相关配置的自动设置，IPv6 承继 IPv4 的这种自动配置服务，并将其称为全状态自动配置(Stateful Autoconfiguration)（参见 DHCPv6）。除了全状态自动配置，IPv6 还采用了一种被称为无状态自动配置（Stateless Autoconfiguration）的自动配置服务。在无状态自动配置过程中，主机自动获得链路本地地址、本地设备的地址前缀以及其它一些相关的配置信息。

安全性

IPSec 是 IPv4 的一个可选扩展协议，但是在 IPv6 中它是 IPv6 的一个组成部分，用于提供 IPv6 的安全性。目前，IPv6 实现了认证头（Authentication Header，AH）和封装安全载荷（Encapsulated Security Payload，ESP）两种机制。前者实现数据的完整性及对 IP 包来源的认证，保证分组确实来自源地址所标记的节点；后者提供数据加密功能，实现端到端的加密。

更好的 QoS 支持

IPv6 包头的新字段定义了数据流如何识别和处理。IPv6 包头中的流标识（Flow Label）字段用于识别数据流身份，利用该字段，IPv6 允许用户对通信质量提出要求。设备可以根据该字段标识出同属于某一特定数据流的所有包，并按需对这些包提供特定的处理。

↘ 用于邻居节点交互的新协议

IPv6 的邻居发现协议（Neighbor Discovery Protocol）使用一系列 IPv6 控制信息报文（ICMPv6）来实现相邻节点（同一链路上的节点）的交互管理。邻居发现协议以及高效的组播和单播邻居发现报文替代了以往基于广播的地址解析协议 ARP、ICMPv4 路由器发现等报文。

↘ 可扩展性

IPv6 特性具有很强的可扩展性，新特性可以添加在 IPv6 包头之后的扩展包头中。不像 IPv4，包头最多只能支持 40 字节的可选项，IPv6 扩展包头的大小仅受到整个 IPv6 包最大字节数的限制。

协议规范

- RFC4291 - IP Version 6 Addressing Architecture.
- RFC2460 - Internet Protocol, Version 6 (IPv6) Specification
- RFC4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC4861 - Neighbor Discovery for IP version 6 (IPv6)
- RFC4862 - IPv6 Stateless Address Autoconfiguration
- RFC5059 - Deprecation of Type 0 Routing Headers in IPv6

3.2 典型应用

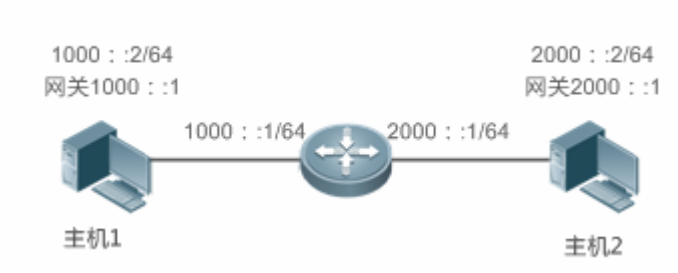
典型应用	场景描述
IPv6 地址通讯	两台 PC 使用 IPv6 地址进行通信

3.2.1 IPv6 地址通讯

应用场景

如下图所示，主机 1 和主机 2 可以通过 IPv6 地址进行通信。

图 3-1



功能部属

主机可以使用无状态地址自动配置也可以使用 DHCPv6 分配地址，配置完地址后，即可以使用 IPv6 地址进行通讯。

3.3 功能详解

功能特性

功能特性	作用
IPv6 地址格式	IPv6 的地址格式使其具有更大的地址空间，及灵活的表示方法。
IPv6 地址类型	IPv6 通过地址标识来区分其网络应用。
IPv6 包头结构	IPv6 通过简化固定报头、扩展选项报头，提高了设备处理数据包的速度，也提高了其转发性能。
IPv6 路径MTU发现	主机动态的发现并调整发送数据路径上的 MTU 的大小，节省了路由器的资源，提高了 IPv6 网络的效率。
IPv6 邻居发现	完成路由器发现、前缀发现、参数发现、地址自动配置、地址解析（相当于 ARP）、确定下一跳、邻居不可达检测、地址冲突检测和重定向。
IPv6 源路由	用来指定报文经过哪些中间节点到达目的地址，类似于 IPv4 的宽松源路由选项和宽松记录路。
控制ICMPv6 差错报文的发送速率	防止拒绝服务攻击。
IPv6 HOP-LIMIT	防止无用的单播报文在网络上无限传播下去，浪费网络带宽

3.3.1 IPv6 地址格式

IPv6 地址格式 IPv6 地址的基本表达方式是 X：X：X：X：X：X：X：X，其中 X 是一个 4 位十六进制整数(16 位)。每一个数字包含 4 个比特，每个整数包含 4 个十六进制数字，每个地址包括 8 个整数，一共 128 位。下面是一些合法的 IPv6 地址：

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800：0：0：0：0：0：0：1

1080：0：0：0：8：800：200C：417A

这些整数是十六进制整数，其中 A 到 F 表示的是 10 到 15。地址中的每个整数都必须表示出来，但起始的 0 可以不必表示。某些 IPv6 地址中可能包含一长串的 0 (就像上面的第二和第三个例子一样)。当出现这种情况时，允许用“：：”来表示这一长串的 0。即地址 800 : 0 : 0 : 0 : 0 : 0 : 0 : 1 可以被表示为：800 :: 1

这两个冒号表示该地址可以扩展到一个完整的 128 位地址。在这种方法中，只有当 16 位组全部为 0 时才会被两个冒号取代，且两个冒号在地址中只能出现一次。

在 IPv4 和 IPv6 的混合环境中还有一种混合的表示方法。IPv6 地址中的最低 32 位可以用于表示 IPv4 地址，该地址可以按照一种混合方式表达，即 X : X : X : X : X : X : d . d . d . d，其中 X 表示一个 1 6 位整数，而 d 表示一个 8 位的十进制整数。例如，地址 0：0：0：0：0：0：192 .168 ． 20 .1 就是一个合法的 IPv6 地址。使用简写的表达方式后，该地址也可以表示为：：192 .168 ． 20 ． 1。典型代表是 IPv4 兼容 IPv6 地址和 IPv4 映射 IPv6 地址，IPv4 兼容 IPv6 地址前 96 比特是 0，表示法为“**::**A.B.C.D”，例如“**::**1.1.1.1”，目前 IPv4 兼容地址已被废除；IPv4 映射 IPv6 地址表示法为“**::FFFF:**A.B.C.D”，用于把 IPv4 地址表示为 IPv6 地址，如把 IPv4 地址“1.1.1.1”映射到 IPv6 地址“**::FFFF:**1.1.1.1”。

由于 IPv6 地址被分成两个部分：子网前缀和接口标识符，因此可以按照类似 CIDR 地址的方式被表示为一个带额外数值的地址，其中该数值指出了地址中有多少位是代表网络部分(网络前缀)，即 IPv6 节点地址中指出了前缀长度，该长度与 IPv6 地址间以斜杠区分，例如：12AB::CD30:0:0:0:0/60，这个地址中用于选路的前缀长度为 60 位。

相关配置

配置 IPv6 地址

- 缺省情况接口没有配置 IPv6 地址。
- 可通过 **ipv6 address** 命令配置接口 IPv6 地址。
- 配置后根据冲突检测即可使用该 IPv6 地址进行通信。

3.3.2 IPv6 地址类型

RFC4291 定义了三种 IPv6 地址类型：

- 单播(Unicast)：单个接口的标识符。送往一个单播地址的包将被传送至该地址标识的接口上。
- 组播(Multicast)：一组接口(一般属于不同节点)的标识符。送往一个组播地址的包将被传送至加入该组播地址的所有接口上。
- 泛播(Anycast)：一组接口的标识符。送往一个泛播地址的包将被传送至该地址标识的接口之一(根据选路协议选择“最近”的一个)。

⚠ 在 IPv6 中已经没有定义广播地址。

下面逐一介绍这几类地址：

单播地址 (Unicast Addresses)

单播地址分为未指定地址、环回地址、链路本地地址、站点本地地址和全球单播地址。目前，站点本地地址被废除了，除了未指定地址、环回地址和链路本地地址以外的单播地址，都是全球单播地址。

- 未指定地址

未指定地址是 0:0:0:0:0:0:0:0，通常简写为**::**，常见的两个用途是：

1. 若主机启动时没有单播地址，则以未指定地址作为源地址，发送路由器请求，从网关获取前缀信息，从而自动生成单播地址。
2. 给主机配置 IPv6 地址时，检测地址是否和同网段其它主机的地址冲突，则以未指定地址作为源地址发送邻居请求（相当于免费 ARP）。

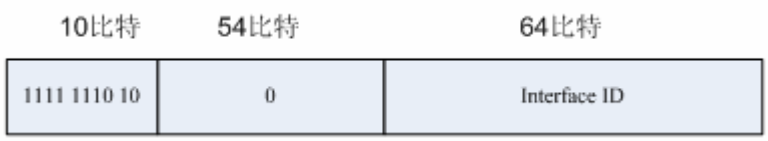
- 环回地址

环回地址是 0:0:0:0:0:0:0:1，通常简写为**::**1，相当于 IPv4 地址 127.0.0.1，一般在节点给自身发报文时使用。

- 链路本地地址

链路本地地址的格式如下：

图 3-2

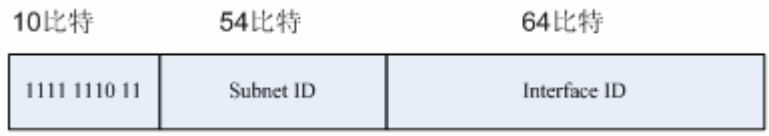


链路本地地址用于单个网络链路上给主机编号。前缀的前 10 位标识的地址即链路本地地址。设备永远不会转发源地址或者目的地址带有链路本地地址的报文。该地址的中间 54 位置成 0。后 64 位表示接口标识符，地址空间的这部分允许单个网络连接多达（2 的 64 次方减 1）个主机。

- 站点本地地址

站点本地地址的格式如下：

图 3-3



站点本地地址可以用在站点内传送数据，设备不会将源地址或者目的地址带有站点本地地址的报文转发到 Internet 上，即这样的包只能在站点内转发，而不能把包转发到站点外去。站点可以理解为一个公司的局域网，这种地址类似于 IPv4 的私有地址，如 192.168.0.0/16。RFC3879 已经废除了站点本地地址。对于新的实现，不再支持该前缀，统一视为全球单播地址；对于已经实现和部署的，可以继续用这个前缀。

- 全球单播地址

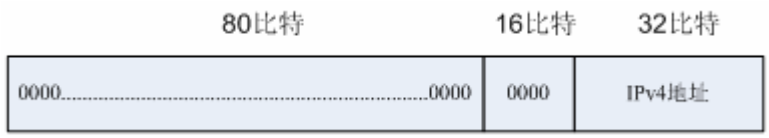
全球单播地址格式如下：

图 3-4

全球单播地址中有一类地址是嵌入 IPv4 地址的 IPv6 地址，用于 IPv4 节点和 IPv6 节点互通，分为 IPv4 兼容 IPv6 地址和 IPv4 映射 IPv6 地址两种。

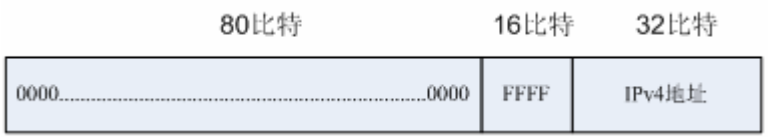
IPv4 兼容 IPv6 地址格式（IPv4-compatible IPv6 address）

图 3-5



IPv4 映射 IPv6 地址格式（IPv4-mapped IPv6 address）

图 3-6



IPv4 兼容 IPv6 地址主要是用在自动隧道上，这类节点既支持 IPv4 也支持 IPv6，IPv4 兼容 IPv6 地址通过 IPv4 设备以隧道方式传送 IPv6 报文，目前 IPv4 兼容 IPv6 地址已被废除。而 IPv4 映射 IPv6 地址则被 IP6 节点用于访问只支持 IPv4 的节点，例如当一个 IPv4/IPv6 主机的 IPv6 应用程序请求解析一个主机名字(该主机只支持 IPv4)时，那么名字服务器内部将动态生成 IPv4 映射的 IPv6 地址返回给 IPv6 应用程序。

↘ 组播地址（Multicast Addresses）

IPv6 组播的地址格式如下：

```
|    8     |  4 |  4 |                   112 bits                   |
+--------+----+----+----------------------------------------------+
|11111111|flgs|scop|                    group ID                    |
+--------+----+----+----------------------------------------------+
```

地址格式中的第 1 个字节为全“1”代表是一个组播地址。

- 标志字段：

由 4 个比特位组成。目前只指定了第 4 位，该位用来表示该地址是由 Internet 编号机构指定的知名的组播地址，还是特定场合使用的临时组播地址。如果该标志位为“0”，表示该地址为知名组播地址；如果该位为“1”，表示该地址为临时地址。其他 3 个标志位保留将来用。

- 范围字段：

由 4 个比特位组成，用来表示组播的范围。即组播组是包括本地节点、本地链路、本地站点，还包括 IPv6 全球地址空间中任何位置的节点。

- 组标识符字段：

长 112 位，用于标识组播组。根据组播地址是临时的还是知名的以及地址的范围，同一个组播标识符可以表示不同的组。

IPv6 的组播地址是以 FF00::/8 为前缀的这类地址。一个 IPv6 的组播地址通常标识一系列不同节点的接口。当一个报文发送到一个组播地址上时，那么该报文将分发到标识有该组播地址的每个节点的接口上。一个节点(主机或者设备)必须加入下列的组播：

3. 本地链路所有节点组播地址 FF02::1

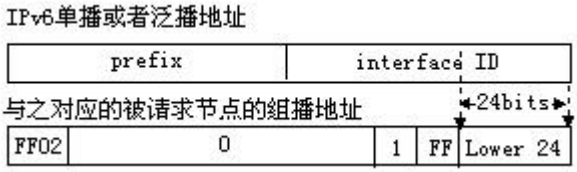
4. 被请求节点的组播地址， 前缀为 FF02:0:0:0:0:1:FF00:0000/104

如果是设备那么还必须加入本地链路所有设备的组播地址 FF02::2。

被请求节点的组播地址是对应于 IPv6 单播(unicast)和泛播(anycast)地址的，IPv6 节点必须为配置的每个单播地址和泛播地址加入其相应的被请求节点的组播地址。被请求节点的组播地址的前缀为 FF02:0:0:0:0:1:FF00:0000/104，另外 24 位由单播地址或者泛播地址的低 24 比特组成，例如对应于单播地址 FE80::2AA:FF:FE21:1234 的被请求节点的组播地址是 FF02::1:FF21:1234 ，

被请求节点组播地址通常用于邻居请求(NS)报文中，被请求节点组播地址的格式如下：

图 3-7



泛播地址（Anycast Addresses）

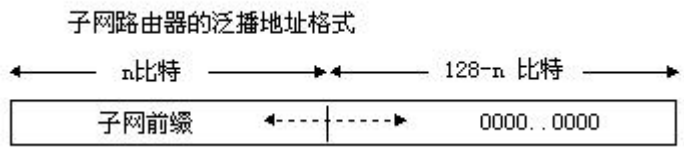
泛播地址与组播地址类似，同样是多个节点共享一个泛播地址，不同的是只有一个节点期待接收给泛播地址的数据包而组播地址成员的所有节点均期待着接收发给该地址的所有包。泛播地址被分配在正常的 IPv6 单播地址空间，因此泛播地址在形式上与单播地址无法区分开，一个泛播地址的每个成员，必须显式地加以配置，以便识别是泛播地址。

⚠ 泛播地址只能分配给设备，不能分配给主机，并且泛播地址不能作为报文的源地址。

在 RFC2373 中预定义了一个泛播地址，称之为子网路由器的泛播地址。下图显示了子网路由器的泛播地址格式，这类地址由子网前缀后面跟着一系列的 0(作为接口标识符)组成。

其中子网前缀标识了一个指定的链路(子网)，送给子网路由器泛播地址的报文将被分发到在该子网上的一个设备。子网路由器的泛播地址通常是被用于一个节点上的应用程序需要和远程子网的一个设备通信而使用。

图 3-8



相关配置

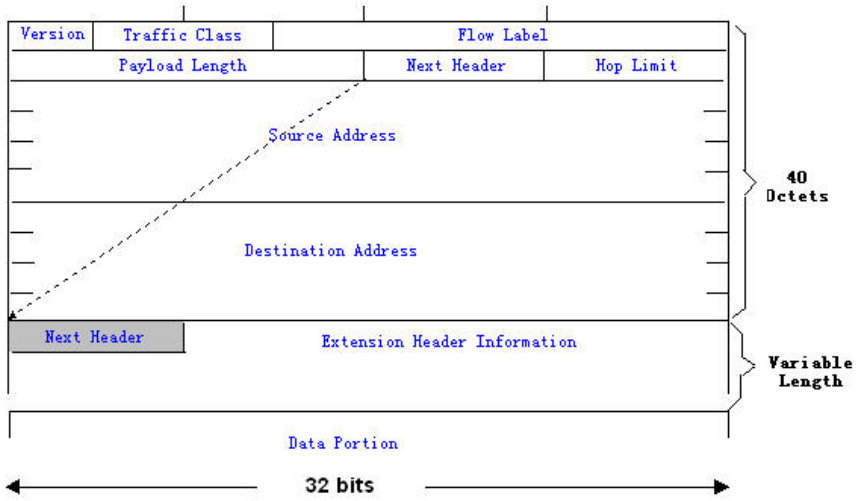
配置 IPv6 地址

- 缺省情况接口没有配置 IPv6 地址。
- 可通过 **ipv6 address** 命令配置接口 IPv6 单播地址和泛播地址。
- 接口 up 之后将会自动加入相应的组播组。

3.3.3 IPv6 包头结构

IPv6 包头格式如下图：

图 3-9



在 IPv4 中，所有包头以 4 字节为单位。在 IPv6 中，包头以 8 字节为单位，包头的总长度是 40 字节。IPv6 包头定义了以下字段：

- 版本(Version)：

长度为 4 位，对于 IPv6 该字段必须为 6。

- 类别(Traffic Class)：

长度为 8 位，指明为该包提供了某种服务，相当于 IPv4 中的“TOS”。

- 流标签(Flow Label)：

长度为 20 位，用于标识属于同一业务流的包，一个节点可以同时作为多个业务流的发送源，流标签和源节点地址唯一标识了一个业务流。

- 净荷长度(Payload Length)：

长度为 16 位，其中包括包净荷的字节长度，同时也包含了各个 IPv6 扩展选项的长度(如果存在)，换句话说就是包含了除 IPv6 头本身外的 IPv6 包的长度。

- 下一个头(Next Header)：

这个字段指出了 IPv6 头后所跟的头字段中的协议类型。与 IPv4 协议字段类似，下一个头字段可以用来指出高层是 TCP 还是 UDP，它也可以用来指明 IPv6 扩展头的存在。

- 跳数(Hop Limit)：

长度为 8 位。每当设备对包进行一次转发之后，这个字段就会被减 1，如果该字段达到 0，这个包就将被丢弃。它与 IPv4 包头中的生存期字段类似。

- 源地址(Source Address)：

长度为 128 位，指出了 IPv6 包的发送方地址。

- 目的地址(Destination Address)：

长度为 128 位，指出了 IPv6 包的接收方地址。

IPv6 的扩展头，目前 IPv6 定义了下列的扩展头：

- 逐跳选项头(Hop-by-Hop Options)：

此扩展头必须紧随在 IPv6 头之后，它包含包所经过的路径上的每个节点都必须检查的选项数据。

- 路由选项头（Routing （Type 0））：

此扩展头指明包在到达目的地途中将经过哪些节点，它包含包沿途经过的各节点的地址列表。IPv6 头的最初目的地址是选路头的一系列地址中的第一个地址，而不是包的最终目的地址。IPv6 头部目的地址对应的节点接收到该包之后，对 IPv6 头和选路头进行处理，并把包发送到选路头列表中的第二个地址，如此继续，直到包到达其最终目的地。

- 分片头（Fragment）：

此扩展头用于源节点对长度超出源节点和目的节点路径 MTU 的包进行分片。

- 目的地选项头（Destination Options）：

此扩展头代替了 IPv4 选项字段，目前唯一定义的目的地选项是在需要时把选项填充为 6 4 位（8 字节）的整数倍，此扩展头可以用来携带由目的地节点检查的信息。

- 上层扩展头(Upper-layer header)：

指明了上层传输数据的协议，如 TCP(6)、UDP(17)。

此外还有身份验证头(Authentication)和封装安全性净荷(Encapsulating Security Payload)的扩展头，这将放到 IPSec 章节描述。

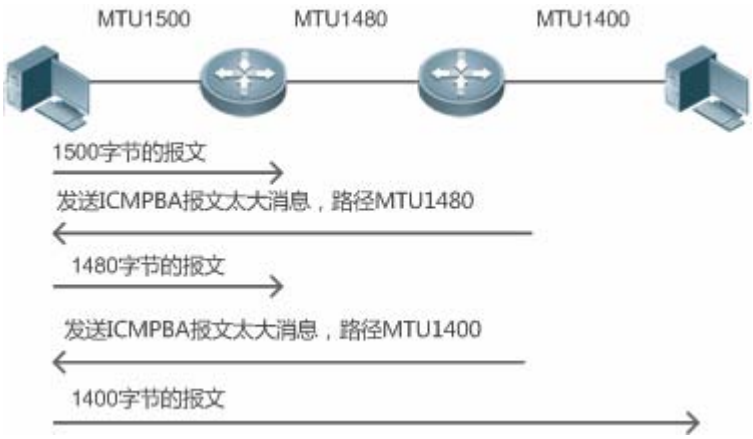
相关配置

无

3.3.4 IPv6 路径MTU发现

和IPv4的路径MTU发现类似，IPv6的路径MTU发现允许一台主机动态的发现并调整发送数据路径上的MTU的大小。另外，当主机要发送的数据包的大小如果比发送数据路径上的 MTU 大时，那么将由主机自行负责分片。这种由主机分片的行为使得设备无需处理分片从而节省了 IPv6 设备的资源，同时也提高了 IPv6 网络的效率。

图 3-10



如上图，当主机要发送的报文的长度比路径 MTU 大时，路由器丢弃报文，并且向主机发送一个 ICMP“报文太大”消息，把MTU告诉主机，然后主机根据新的路径MTU对报文进行分片。这种由主机分片的行为使得路由器不需要对报文进行分片从而节省了路由器的资源，同时也提高了 IPv6 网络的效率。

相关配置

↘ 配置接口 IPv6 MTU

- 默认以太网 IPv6 MTU 是 1500
- 为减少报文被丢弃带来的额外流量开销，需要根据实际组网环境设置合适的接口 MTU 值。可通过 **ipv6 mtu** 命令修改接口的 IPv6 MTU 大小

3.3.5 IPv6 邻居发现

邻居发现协议是 IPv6 协议的一个基本的组成部分，它的主要功能有路由器发现、前缀发现、参数发现、地址自动配置、地址解析（相当于 ARP）、确定下一跳、邻居不可达检测、地址冲突检测和重定向。邻居发现定义了 5 种 ICMP 报文：“路由器请求， ICMP 类型为 133；路由器公告， ICMP 类型为 134；邻居请求，相当于 ARP 请求，ICMP 类型为 135；邻居公告，相当于 ARP 应答，ICMP 类型为 136；ICMP 重定向报文，ICMP 类型为 137”。

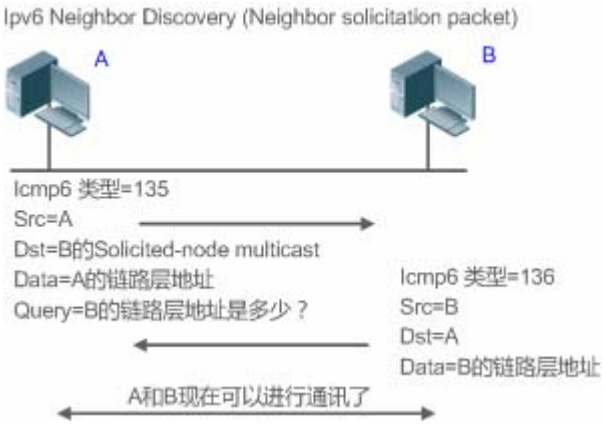
上述五种ICMP报文都会携带一个或者多个的选项，这些选项在某些情况下是可选，事实上，有些情况下选项实际上就是报文的全部意义所在，邻居发现主要定义五种选项：“源链路层地址选项”，类型=1；“目标链路层地址选项”，类型=2；“前缀信息选项”，类型=3；“重定向的首部选项”，类型=4；“MTU 选项”类型=5；

地址解析

当一个节点要与另外一个节点通信时，那么该节点必须获取对方的链路层地址，此时就要向该节点发送邻居请求(NS)报文,报文的目的地址是对应于目的节点的 IPv6 地址的被请求多播地址，发送的 NS 报文同时也包含了自身的链路层地址。当对应的节点收到该邻居请求后发回一个响应的报文称之为邻居公告报文(NA)，其目的地址是邻居请求的源地址，内容为被请求的节点的链路层的地址。当源节点收到该应答报文后就可以和目的节点进行通讯了。

下图是地址解析的过程：

图 3-11



邻居不可达检测

当一个邻居被认为可到达的时间到期以后，如果有 IPv6 单播报文需要发送给这个邻居，将执行邻居不可达检测 (Neighbor Unreachability Detection)。

邻居不可达检测和向邻居发送 IPv6 报文可以同时进行，在检测过程中，继续向该邻居转发 IPv6 报文。

地址冲突检测

当给主机配置 IPv6 地址以后，想知道这个 IPv6 地址在链路上是不是唯一的，需要执行地址冲突检测，发送源 IPv6 地址是未指定地址的邻居请求。

如果设备检测到地址冲突，该地址将被设置为冲突状态，设备将不能接收目的地址为该地址的 ipv6 报文，同时设备会为该冲突的地址起一个定时器，定时进行地址冲突检测，如果重新检测没有冲突，该地址将可以正常使用。

路由器，前缀和参数发现

路由器公告报文(RA)在设备上是定期被发往链路本地所有节点的。

路由器公告报文发送如下图：

图 3-12

路由器公告报文中通常包含如下内容：

- 一个或者多个 IPv6 地址前缀（用于 on-link 确定，或无状态地址自动配置）
- IPv6 地址前缀的有效期。
- 主机自动配置使用的方式(有状态还是无状态)。
- 作为缺省设备的信息(即决定本设备是否要作为缺省设备，如果是那么还宣布自己充当缺省设备的时间)。
- 提供给主机配置的一些其它信息如跳数限制、MTU、邻居请求重传间隔时间等。

路由器公告报文同时也用来应答主机发出的路由器请求(RS)报文，路由器请求报文允许主机一旦启动后可以立即获得自动配置的信息而无需等待设备发出的路由器公告报文(RA)。当主机刚启动时如果没有单播地址，那么主机发出的路由器请求报文将使用未指定地址(0:0:0:0:0:0:0:0)作为请求报文的源地址，否则使用已有的单播地址作为源地址，路由器请求报文使用本地链路所有设备组播地址(FF02::2)作为目的地址。作为应答路由器请求(RS)报文的路由器公告(RA)报文将使用请求报文的源地址作为目的地址(如果源地址是未指定地址那么将使用本地链路所有节点组播地址 FF02::1)。

在路由器公告报文中下列参数是可以被配置的：

- Ra-interval 路由器公告报文的发送间隔。
- Ra-lifetime 路由器生存期，即设备是否充当本地链路的缺省路由器以及充当该角色的时间。
- Prefix 本地链路的 IPv6 地址前缀，用于 on-link 确定，或无状态地址自动配置，包括前缀的其它参数配置 。
- Ns-initerval 邻居请求报文重传的时间间隔。
- Reachabletime 检测到邻居可到达事件后认为邻居是可到达的所维持的时间。
- Ra-hoplimit 路由器公告(RA)报文跳数的值，用于设置主机发送单播报文的 hop-limit
- Ra-mtu 路由器公告(RA)报文的 MTU 字段的值
- Maneged-config-flag 决定了收到该路由器公告的主机是否要使用全状态自动配置来获取地址
- Other-config-flag 决定了收到该路由器公告的主机是否将使用 dhcpv6 来获取除 IPv6 地址以外的其他信息进行自动配置。

以上这些参数在 IPv6 接口属性中进行配置。

↘ 重定向

当路由器收到 IPv6 报文以后，发现存在更优的下一跳，就发送 ICMP 重定向报文把更优的下一跳告诉主机，下一次主机直接把 IPv6 报文发给更优的下一跳。

未解析的邻居表项的最大数量

- 为防止恶意扫描网段，生成大量的未解析邻居表项，占用过多的内存，可配置限制未解析的邻居表项的最大数量

处理 ND 选项最大数量

- 为防止伪造 ND 报文携带无穷的 ND 选项，设备处理占用过多的 CPU，可配置限制 ND 选项最大数量

接口邻居学习表项数量

- 为防止邻居学习攻击，占用设备邻居表项，占用内存且影响转发性能，可配置限制接口邻居学习表项数量

相关配置

配置 IPv6 重定向

- 缺省情况 IPV6 的接口上允许发送 ICMPv6 重定向报文
- 可以使用接口配置模式命令“**no ipv6 redirects**”禁止接口发送重定向报文

配置 IPv6 地址冲突检测

- 缺省情况接口上为 IPV6 地址执行地址冲突检测时会发送的 1 个邻居请求(NS)报文
- 可以使用接口配置模式命令“**ipv6 nd dad attempts** *value*”配置 DAD 连续发送的 NS 报文个数，0 表示阻止为该接口上的 Ipv6 地址启动地址冲突检测
- 使用“**no ipv6 nd dad attempts**”恢复默认配置
- 缺省情况设备对已经冲突 IPv6 地址会定时执行地址冲突检测，时间间隔为 60s
- 可以使用全局配置模式命令“**ipv6 nd dad retry** value”配置重复地址冲突检测的时间间隔，0 表示关闭设备进行重复冲突地址检测功能。
- 使用“**no ipv6 nd dad retry**”恢复默认配置

配置邻居可达时间

- 缺省情况 IPv6 邻居默认可达时间为 30s
- 可以使用接口配置模式命令“**ipv6 nd reachable-time** *milliseconds*”修改可达时间

配置邻居 stale 状态时间

- 缺省情况 IPv6 邻居默认 stale 状态持续时间 1h，到期后将进行邻居不可达检测
- 可以使用接口配置模式命令“**ipv6 nd stale-time** *seconds*”修改 stale 状态持续时间

配置前缀信息

- 缺省情况 RA 公告的前缀是在该接口上通过 **ipv6 address** 命令配置的前缀
- 可以使用接口配置模式命令“**ipv6 nd prefix**”添加或删除可公告的前缀及前缀参数

配置 RA 抑制功能

- 缺省情况 IPv6 的接口上不会发送路由器公告报文
- 可以使用接口配置模式命令“**no ipv6 nd suppress-ra**”关闭 RA 抑制功能

配置未解析的邻居表项的最大数量

- 默认值为 0，表示不限制，即受限于设备支持的 ND 表项容量
- 使用全局配置模式下命令 **ipv6 nd unresolved** *number* 限制未解析邻居数量，表项超过该限制后，将不为后续报文进行主动解析

配置接口可学习邻居表项的数量

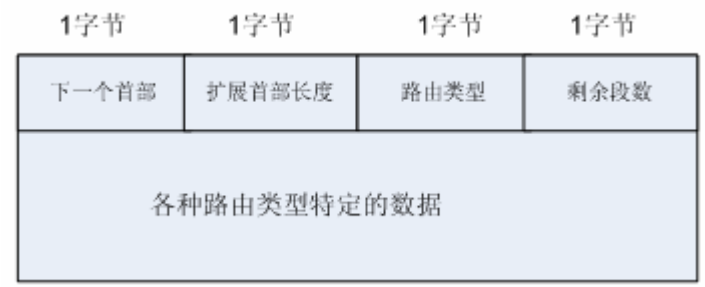
- 使用接口配置模式下命令 **ipv6 nd cache interface-limit** *value* 限制接口可学习的邻居数量，默认值为 0，表示不限制

3.3.6 IPv6 源路由

工作原理

IPv6 报文通过路由首部被发送者用来指定报文经过哪些中间节点到达目的地址，类似于 IPv4 的宽松源路由选项和宽松记录路由选项，格式为：

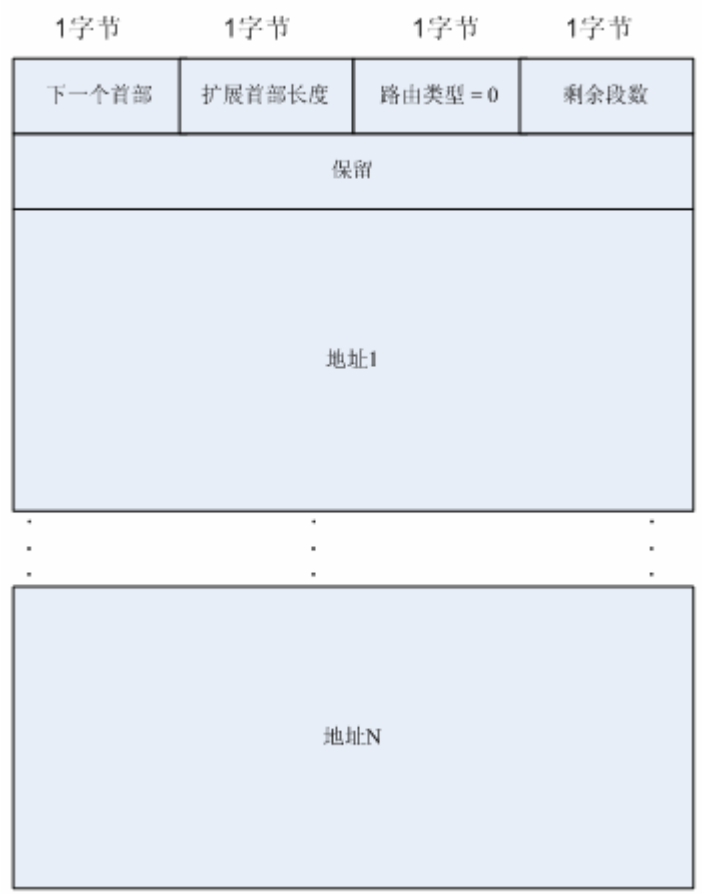
图 3-13



其中剩余段数用来指明报文从当前节点到最终目的地址，还需要经过多少个路由首部指明的中间节点，不包括路由首部没有列出的中间节点。

目前定义了两种路由类型：0 和 2。类型 2 路由首部用于移动通信。RFC2460 定义了类型 0 路由首部（类似于 IPv4 的宽松源路由选项），格式如下图所示。

图 3-14



下面举例说明类型 0 路由首部的应用，如 图 3-15 所示。

图 3-15

主机 1 发报文给主机 2，指明要经过路由器 2 和 3，转发过程中报文 IPv6 首部和路由首部的相关字段变化如下表所示：

传输节点	IPv6 首部的相关字段	类型 0 路由首部的相关字段
主机 1	源地址=1000::2 目的地址=1001::1（路由器 2 的地址）	剩余段数=2 地址 1=1002::1（路由器 3 的地址） 地址 2=1003::2（主机 2 的地址）
路由器 1	无变化	
路由器 2	源地址=1000::2 目的地址=1002::1（路由器 3 的地址）	剩余段数=1 地址 1=1001::1（路由器 2 的地址） 地址 2=1003::2（主机 2 的地址）
路由器 3	源地址=1000::2 目的地址=1003::2（主机 2 的地址）	剩余段数=0 地址 1=1001::1（路由器 2 的地址）

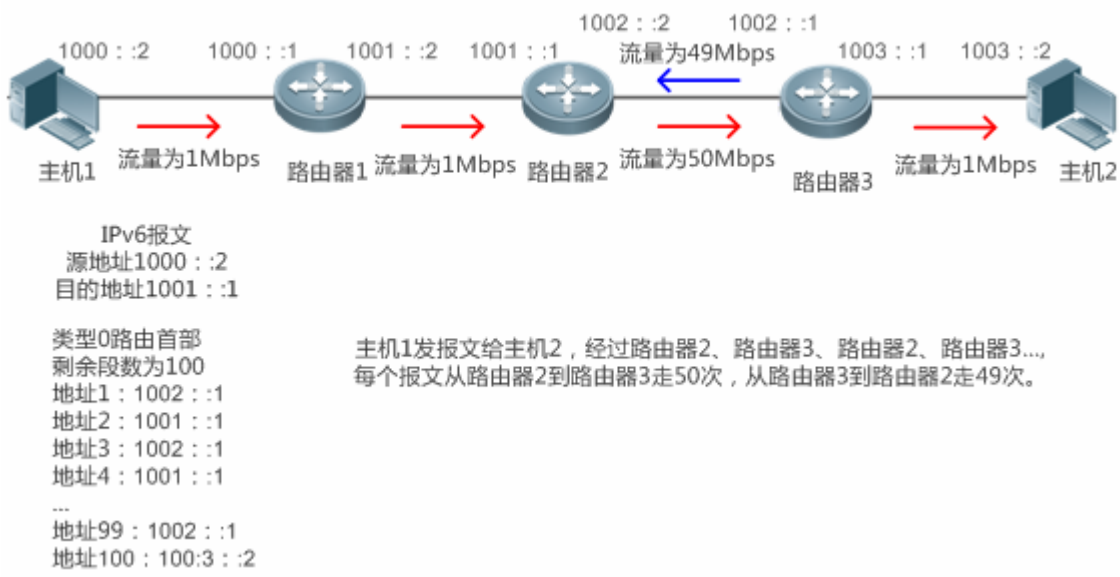
		地址 2=1002::1（路由器 3 的地址）
主机 2	无变化	

具体过程如下：

5. 主机 1 发出报文，目的地址是路由器 2 的地址 1001::1，在类型 0 路由首部中填上路由器 3 的地址 1002::1 和主机 2 的地址 1003::2，剩余段数是 2。
6. 路由器 1 只是简单地把报文转发给路由器 2。
7. 路由器 2 把 IPv6 首部的目的地址和路由首部的地址 1 交换，即现在目的地址是路由器 3 的地址 1002::1，路由首部的地址 1 是路由器 2 的地址 1001::1，剩余段数是 1。修改完以后，路由器 2 把报文转发给路由器 3。
8. 路由器 3 把 IPv6 首部的目的地址和路由首部的地址 2 交换，即现在目的地址是主机 2 的地址 1003::2，路由首部的地址 2 是路由器 3 的地址 1002::1，剩余段数是 0。修改完以后，路由器 3 把报文转发给主机 2。

类型 0 路由首部有可能被利用进行拒绝服务攻击，如下图所示，主机 1 以 1Mbps 的速度向主机 2 发报文，故意构造一个路由首部，使报文在路由器 2 和路由器 3 之间多次往返，从路由器 2 到路由器 3 走 50 次，从路由器 3 到路由器 2 走 49 次，这时路由首部产生流量放大效应：“路由器 2 到路由器 3 方向的流量为 50Mbps，路由器 3 到路由器 2 方向的流量为 49Mbps”。由于存在这个安全问题，RFC5095 废除了类型 0 路由首部。

图 3-16



相关配置

配置 IPv6 源路由

- 缺省情况不支持类型 0 路由首部
- 可以使用全局配置模式命令“**ipv6 source-route**”打开这项功能

3.3.7 控制ICMPv6 差错报文的发送速率

工作原理

ICMPv6 差错报文是由目标节点或者中间路由器发送，用于报告在转发和传送 IPv6 数据包过程中出现的错误。主要包括下面四种类型的差错报文：目标不可达（Destination unreachable）、报文太大（Packet too big）、超时（Time exceeded）、参数问题（Parameter problem）。

往设备发送非法 IPv6 报文，设备会丢弃这些报文，并向源 IPv6 地址发送相应的 ICMPv6 差错报文。如果受到 IPv6 非法报文攻击，可能出现设备一直在应答 ICMPv6 差错报文而耗尽设备资源，这样设备将不能正常提供服务，针对这种攻击，可以对 ICMPv6 差错报文的发送速率进行限制。

如果转发的 IPv6 报文的长度超过出口的 IPv6 MTU，路由器会丢弃 IPv6 报文，并且向源 IPv6 地址发送 ICMPv6 报文太大消息，这种 ICMPv6 差错报文的主要用途是 IPv6 路径 MTU 发现。为了防止其它 ICMPv6 差错报文太多而将 ICMPv6 报文太大消息限速过滤掉，从而导致 IPv6 路径 MTU 发现功能失效，对 ICMPv6 报文太大消息和其它 ICMPv6 差错报文分别限速。

ICMPv6 重定向报文不属于 ICMPv6 差错报文，我司把 ICMPv6 重定向报文和其它 ICMPv6 差错报一起限速。

相关配置

↘ 配置 ICMPv6 报文太大消息的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 **ipv6 icmp error-interval too-big** 配置发送速率。

↘ 配置其它 ICMPv6 差错报文的发送速率

- 缺省速率是 100 毫秒 10 个。
- 可通过 **ipv6 icmp error-interval** 配置发送速率。

3.3.8 IPv6 HOP-LIMIT

工作原理

IPv6 数据包从源地址向目的地址经过路由器间传播，设置一个 hop-limit 数值，每过一个路由器 hop-limit 值就减一，当减到零的时候，路由器就把这个包丢掉，这样可以防止无用的包在网络上无限传播下去，浪费网络带宽。其功能类似于 IPv4 的 TTL。

相关配置

↘ 设置 IPv6 hop-limit

- 缺省情况设备 IPv6 HOP-LIMIT 为 64。

- 可通过 **ipv6 hop-limit** 设置设备的 IPv6 HOP-LIMIT 值。

3.4 配置详解

配置项	配置建议 & 相关命令	
配置IPv6 地址	⚠ 必须配置，用于配置 ipv6 地址，启用 IPv6 协议。	
	ipv6 enable	打开接口的 IPv6 协议
	ipv6 address	配置接口 IPv6 的单播地址
配置IPv6 邻居发现	⚠ 可选配置，用于限制接口 IPv6 重定向功能。	
	ipv6 redirects	打开该接口的 IPv6 重定向功能
	⚠ 可选配置，用于设置 DAD 检测。	
	ipv6 nd dad attempts	配置冲突检测时要连续发送的邻居请求(NS)报文的数量。
	⚠ 可选配置，用于设置邻居发现的各种参数。	
	ipv6 nd reachable-time	设置邻居被认为可到达的时间
	ipv6 nd prefix	设置路由器公告(RA)报文中所要公告的地址前缀
	ipv6 nd suppress-ra	设置是否在该接口上阻止路由器公告（RA）报文发送
	⚠ 可选配置，用于设置未解析邻居的最大数量。	
	ipv6 nd unresolved	设置未解析邻居的最大数量
	⚠ 可选配置，用于限制接口可学习的邻居数量	
	ipv6 nd cache interface-limit	设置接口可学习邻居数量
配置接口IPv6 MTU	⚠ 可选配置，用于限制接口发送 IPv6 报文的 mtu。	
	ipv6 mtu	设置 IPv6 MTU 值
配置IPv6 源路由	⚠ 可选配置，用于开启支持 IPv6 源路由功能。	
	ipv6 source-route	配置设备转发带有路由首部的 IPv6 报文。
配置ICMPv6 差错报文的发送速率	⚠ 可选配置。	
	ipv6 icmp error-interval too-big	配置 ICMPv6 报文太大消息的发送速率。
	ipv6 icmp error-interval	配置其它 ICMPv6 差错报文和 ICMPv6 重定向报文的发送速率。
配置设备IPv6 HOP-LIMIT	⚠ 可选配置，用于限制接口发送 IPv6 单播报文的可转发跳数。	
	ipv6 hop-limit	设置 IPv6 HOP-LIMIT 值。

3.4.1 配置IPv6 地址

配置效果

通过配置接口 IPv6 地址实现 IPv6 网络通信。

注意事项

无

配置方法

↘ 打开接口的 IPv6 协议

- 可选配置，若不想通过配置 IPv6 地址来开启接口 IPv6 协议，则必须配置 **ipv6 enable** 来开启接口 IPv6 功能。

↘ 配置接口 IPv6 的单播地址

- 必须配置。

检验方法

通过 **show ipv6 interface** 可以看到配置的地址生效

相关命令

↘ 打开接口的 IPv6 协议

【命令格式】 **ipv6 enable**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 有 2 种方式可以打开接口上的 IPv6 功能，一是在接口下配置 **ipv6 enable** 命令，二是直接在接口下配置了 IPv6 地址。

如果在接口上配置了 IPv6 地址那么接口的 IPv6 功能就会自动打开，即使使用 **no ipv6 enable** 也不能关闭 IPV6 功能。

↘ 配置接口 IPv6 的单播地址

【命令格式】 **ipv6 address** *ipv6-address* / *prefix-length*

ipv6 address *ipv6-prefix* / *prefix-length* **eui-64**

ipv6 address *prefix-name sub-bits* / *prefix-length* [**eui-64**]

【参数说明】 *ipv6-address*：IPV6 地址，必须遵循 RFC4291 定义的地址形式，每个地址域之间用冒号隔开，每个域占 16 比特，用十六进制数表示.

ipv6-prefix：IPV6 地址前缀，必须遵循 RFC4291 定义的地址形式，每个地址域之间用冒号隔开，每个域占 16 比特，用十六进制数表示.

prefix-length：IPV6 前缀的长度即 IPV6 地址中代表网络的部分。

prefix-name：通用前缀的名字。使用这个指定的通用前缀生成接口地址。

sub-bits：子前缀比特与主机比特的值。这个值与通用前缀中的前缀合并生成接口地址。这个值的表示法要遵循 RFC4291 描述的冒号表示法。

eui-64：表示生成的 IPV6 地址由配置的地址前缀和 64 比特的接口 ID 标识符组成。

【命令模式】 接口模式

【使用指导】 当一个 IPV6 接口被创建并且链路状态为 UP 时那么系统将为该接口自动生成链路本地地址。

接口的 IPv6 地址也可以使用通用前缀机制生成。其机制就是 IPv6 地址=“通用前缀”+“子前缀”+“主机比特”。通用前缀可以使用 **ipv6 general-prefix** 命令配置，也可能通过 DHCPv6 客户端的 PD(前缀发现)功能学习到(参见 DHCPv6 配置指南)。“子前缀”+“主机比特”就是使用本命令的 *sub-bits/prefix-length* 参数配置。

使用 **no ipv6 address** 如果不指定删除具体的地址，那么将删除所有手工配置的地址。

使用 **no ipv6 address** *ipv6-prefix/prefix-length* **eui-64** 可以删除使用命令 **ipv6 address** *ipv6-prefix/prefix-length* **eui-64** 配置的地址。

配置举例

给接口配置 IPv6 地址

【配置方法】 在接口 GigabitEthernet 0/0 开启 IPv6 协议，并添加 ipv6 地址 2000::1

```
Ruijie(config)#interface gigabitEthernet 0/0
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 enable
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 address 2000::1/64
```

【检验方法】 使用 **show ipv6 interface** 可以看到接口 GigabitEthernet 0/0 添加地址成功

```
Ruijie(config-if-GigabitEthernet 0/0)#show ipv6 interface gigabitEthernet 0/0


interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:00:00:00:00:00
    INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/64
    INET6: 2000::1 [ TENTATIVE ], subnet is 2000::/64
  Joined group address(es):
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
```

```
ND router advertisements are sent every 200 seconds<160--240>
ND router advertisements live for 1800 seconds
```

常见错误

无

3.4.2 配置IPv6 邻居发现

配置效果

配置 ND 协议相关属性，比如配置 ipv6 重定向功能，配置 DAD 检测等。

注意事项

接口默认是抑制发送 RA 报文，要设备能够发送 RA 报文必须在接口模式下配置 no ipv6 nd suppress-ra。

配置方法

↘ 打开该接口的 IPv6 重定向功能

- 可选配置，缺省已开启。
- 当需要关闭接口 IPv6 重定向功能时，使用“**no ipv6 redirects**”。

↘ 配置冲突检测时要连续发送的邻居请求(NS)报文的数量

- 可选配置。
- 如果需要阻止为该接口上的 Ipv6 地址启动地址冲突检测或者修订 DAD 连续发送邻居请求(NS)报文个数，可使用该配置。

↘ 设置邻居被认为可到达的时间

- 可选配置。
- 如果需要修改邻接可达时间，可使用该配置。

↘ 设置路由器公告(RA)报文中所要公告的地址前缀

- 缺省情况 RA 公告的前缀是在该接口上通过 ipv6 address 命令配置的前缀
- 可选配置，可使用“**ipv6 nd prefix**”手工添加或删除可公告的前缀及前缀参数

↘ 设置是否在该接口上阻止路由器公告（RA）报文发送

- 可选配置。

- 如果需要设备能发送路由器公告，可使用该命令来配置。

配置未解析的邻居表项的最大数量

- 可选配置。
- 如果设备受到扫描攻击而创建大量未解析邻居表项，消耗表项资源，可以使用该命令限制未解析邻居的数量。

配置处理 ND 选项最大数量

- 可选配置
- 如果环境要求设备能够处理更多的选项内容，可使用该命令来配置。

配置接口可学习邻居表项的数量

- 可选配置
- 如果环境中 IPv6 主机数可控制，可以使用该功能限制接口的学习邻居个数，防止网络中进行 ND 学习攻击，使得设备学习表项占用内存影响性能。

检验方法

通过以下命令查看配置是否正确：

- **show ipv6 interface** *interface-type interface-num* 可查看接口重定向功能，邻居可达时间、邻居请求发送间隔等信息是否配置生效
- **show ipv6 interface** *interface-type interface-num* **ra-inifo** 可查看路由器公告配置的前缀及其他信息是否正确
- **show run**

相关命令

打开该接口的 IPv6 重定向功能

【命令格式】 **ipv6 redirects**
【参数说明】 -
【命令模式】 接口模式
【使用指导】 所有 ICMPv6 的错误报文的数据包传输速率是有限制的，缺省每秒钟最多可以发送 10 个错误 ICMPv6 错误报文(10pps)。

配置冲突检测时要连续发送的邻居请求(NS)报文的数量

【命令格式】 **ipv6 nd dad attempts** *value*
【参数说明】 *value*：邻居请求(NS)报文的数量
【命令模式】 接口模式
【使用指导】 当在接口上配置一个新的 IPV6 地址前要为它启动地址冲突检测，此时该地址处于"tentative"(试验)的状态。地址冲突过程执行完了，如果没有检测到冲突，那么该地址就可以被正确使用，如果检测到冲突了，并且该地址所使用的接口标识符是使用 EUI-64 的标识符，那么表明在该链路上存在链路层地址出现重复，那么此时

系统会自动关闭该接口（即阻止在该接口上进行 IPV6 的相关操作），此时必须手工去修改并配置新的地址，并通过再次 down/up 接口重新启动地址冲突检测。任何情况下当一个接口从 down 状态变为 up 状态时都会为该接口上的地址重新启动地址冲突检测。

↘ 设置邻居被认为可到达的时间

【命令格式】 **ipv6 nd reachable-time** *milliseconds*

【参数说明】 *milliseconds*：邻居被认为可到达的时间，以毫秒为单位，范围： 0-3600000。缺省为 30 秒。

【命令模式】 接口模式

【使用指导】 设备通过该配置的时间来检测不可用的邻居，所设置的时间越短意味着可以更快的检测到邻居失效，但是将浪费更多的网络带宽、消耗设备更多的资源。因此不建议将该时间配置的过小。

配置的值将在路由器公告报文(RA)中被发布出去，同时该值也被设备自身使用。如果设置的值为 0 表示设备未指定该时间，即使用缺省值。

↘ 设置路由器公告(RA)报文中所要公告的地址前缀

【命令格式】 **ipv6 nd prefix {***ipv6-prefix*/*prefix-length* | **default**} [[*valid-lifetime* { **infinite** | *preferred-lifetime* }] | [**at** *valid-date preferred-date*] | [**infinite** {**infinite** | *preferred-lifetime*}]] [**no-advertise**] | [[**off-link**] [**no-autoconfig**]]

【参数说明】 *ipv6-prefix*：IPV6 的网络号，必须遵循 RFC4291 的地址表示形式。

prefix-length：IPV6 前缀的长度，注意前面必须加上’ /’ 。

valid-lifetime：主机收到路由器公告的前缀后认为有效的时间，取值范围 0-4294967295。缺省 30 天。

preferred-lifetime：主机收到路由器公告的前缀后认为首选有效的时间，取值范围 0-4294967295，缺省 7 天。

at *valid-date preferred-date*：设置公告前缀有效和首选有效的截止时间，截止时间是以 日、月、年、小时、分钟表示的。

infinite：表示永远都有效。

default：设置要使用的缺省参数配置。

no-advertise：表示该前缀不被路由器公告。

off-link：主机在发送 IPV6 报文时如果目的地址的前缀匹配前缀那么认为该目的地是在同一链路(on-link)上是可直接到达的。设置了该选项表示该前缀不用来做 on-link 的判断。

no-autoconfig：该选项指示主机收到该路由器公告中的前缀不能用于地址自动配置。

【命令模式】 接口模式

【使用指导】 通过该命令可以分别配置每一个前缀的各个参数，包括是否要公告该前缀，缺省情况下路由器公告报文中(RA)公告的前缀是在该接口上通过 **ipv6 address** 命令配置的前缀，如果要增加其它前缀可以使用该命令进行配置。

ipv6 nd prefix default 设置该接口上使用的缺省配置参数，即新增加一个前缀时，如果没有指定任何参数，那么将使用 **ipv6 nd prefix default** 所设置的参数做为配置的前缀的参数。注意一旦为该前缀指定了某个参数以后将不再认为使用缺省参数配置。即以后使用 **ipv6 nd prefix default** 改变缺省参数配置时不会去修改该前缀的配置，而只修改完全使用缺省参数配置的前缀。

at *valid-date preferred-date* 前缀的有效时间有 2 种指定方式：一种是在公告报文中每个前缀指定一个固定的时间；另外一种是指定截止时间，使用该方式那么每次发出去的公告报文中的前缀的有效时间将采用递减的方式，直到值为 0。

设置是否在该接口上阻止路由器公告（RA）报文发送

【命令格式】 **ipv6 nd suppress-ra**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 当要在一个接口上抑制路由器公告报文发送时可以使用 ipv6 suppress-ra 命令

设置未解析的邻居表项的最大数量

【命令格式】 **ipv6 nd unresolved** *number*

【参数说明】 *number*：表示未解析邻居表项限制数

【命令模式】 全局模式

【使用指导】 为了防止恶意扫描攻击导致生成大量未解析的 ND 表项，占用表项资源，可以通过配置限制未解析的 ND 表项的个数。

设置接口可学习邻居表项数量

【命令格式】 **ipv6 nd cache interface-limit** *value*

【参数说明】 value：接口所能学习的邻居最大限制

【命令模式】 接口模式

【使用指导】 限制接口的邻居学习数量，可防止恶意的邻居攻击，让设备生成大量的邻居表项，占用过多的内存。配置的值必须不小于当前接口已经学习到的邻居数，否则配置不生效。该限制受限于设备支持 ND 容量。

配置举例

打开接口的 IPv6 重定向功能

【配置方法】 开启接口 IPv6 重定向功能。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 redirects
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie#show ipv6 interface gigabitEthernet 0/0


interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:00:00:00:00:00
    INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/64
  Joined group address(es):
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
```

【配置方法】 开启接口 IPv6 重定向功能。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 redirects
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
```

配置 IPv6 地址冲突检测

【配置方法】 配置 DAD 检测要连续发送 3 个 NS 报文。

```
Ruijie(config-if-GigabitEthernet 0/0)# ipv6 nd dad attempts 3
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie#show ipv6 interface gigabitEthernet 0/0


interface GigabitEthernet 0/0 is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:00:00:00:00:00
    INET6: FE80::200:FF:FE00:1 [ TENTATIVE ], subnet is FE80::/64
  Joined group address(es):
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 3
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
  ND router advertisements live for 1800 seconds
Ruijie(config-if-GigabitEthernet 0/0)#
```

手工配置路由器公告的前缀信息

【配置方法】 为接口添加一个前缀 1234::/64。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/6
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie#show ipv6 interface gigabitEthernet 0/0 ra-info


GigabitEthernet 0/0: DOWN (RA is suppressed)
  RA timer is stopped
  waits: 0, initcount: 0
  statistics: RA(out/in/inconsistent): 0/0/0, RS(input): 0
  Link-layer address: 00:00:00:00:00:00
```

【配置方法】 为接口添加一个前缀 1234::/64。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 nd prefix 1234::/6
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
  Physical MTU: 1500
  ND router advertisements live for 1800 seconds
  ND router advertisements are sent every 200 seconds<160--240>
  Flags: !M!O, Adv MTU: 1500
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit time is 0 milliseconds
  ND advertised CurHopLimit is 64
  Prefixes: <total: 1>
    1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)
```

配置路由器公告的前缀从前缀池获取

【配置方法】 配置路由器公告的前缀从前缀池“ra-pool”获取

```
Ruijie(config-if-GigabitEthernet 0/0)#peel default ipv6 pool ra-pool
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0

Building configuration...
Current configuration : 125 bytes

interface GigabitEthernet 0/0
 ipv6 enable
 no ipv6 nd suppress-ra
 peel default ipv6 pool ra-pool
!
```

配置关闭路由器公告抑制功能

【配置方法】 关闭接口抑制路由器公告功能

```
Ruijie(config-if-GigabitEthernet 0/0)# no ipv6 nd suppress-ra
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie(config-if-GigabitEthernet 0/0)#show run interface gigabitEthernet 0/0

Building configuration...
Current configuration : 125 bytes

interface GigabitEthernet 0/0
 ipv6 enable
 no ipv6 nd suppress-ra
!
```

↘ 配置未解析的邻居表项的最大数量

【配置方法】 配置未解析的邻居表项的最大数量为 200

```
Ruijie(config)# ipv6 nd unresolved 200
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie#show run

ipv6 nd unresolved 200
!
```

↘ 配置接口可学习邻居表项数量

【配置方法】 配置接口可学习邻居表项数量 100

```
Ruijie(config-if-GigabitEthernet 0/1)# ipv6 nd cache interface-limit 100
```

【检验方法】 通过 **show run** 查看配置是否生效。

```
Ruijie#show run
!
interface GigabitEthernet 0/1
 ipv6 nd cache interface-limit 100
!
```

常见配置错误

无

3.4.3 配置接口IPv6 MTU

配置效果

根据实现网络环境修改接口 IPv6 MTU 值，避免报文被丢弃。

注意事项

IPv6 mtu 配置范围受接口 mtu 限制，一般为 1280-1500.

配置方法

↘ 设置 IPv6 MTU 值

- 可选配置。

- 当网络路径上的最小 MTU 比接口 IPv6 MTU 小时，为减少报文被丢弃带来的额外流量开销，可使用该配置调整合适的接口 MTU 值。

检验方法

- 通过 **show run**、**show ipv6 interface** 命令查看配置是否正确。
- 本地发送 ipv6 大包（大于接口 IPv6 mtu），抓包可以看到根据接口 IPv6 mtu 大小进行分配。

相关命令

设置 IPv6 MTU 值

【命令格式】 **ipv6 mtu** *bytes*

【参数说明】 *bytes*：IPv6 包最大传输单元，以字节为单位，范围 1280~1500。

【命令模式】 接口模式

【使用指导】 -

配置举例

配置接口 IPv6 mtu

【配置方法】 修改接口 IPv6 MTU 为 1300。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
Ruijie(config-if-GigabitEthernet 0/0)#show ipv6 interface


interface GigabitEthernet 0/ is Down, ifindex: 1, vrf_id 0
  address(es):
    Mac Address: 00:d0:f8:22:33:47
    INET6: FE80::2D0:F8FF:FE22:3347 [ TENTATIVE ], subnet is FE80::/64
    INET6: 1020::1 [ TENTATIVE ], subnet is 1020::/64
    INET6: 1023::1 [ TENTATIVE ], subnet is 1023::/64
  Joined group address(es):
  MTU is 1300 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds<160--240>
```

【配置方法】 修改接口 IPv6 MTU 为 1300。

```
Ruijie(config-if-GigabitEthernet 0/0)#ipv6 mtu 1300
```

【检验方法】 通过 **show ipv6 interface** 查看配置是否生效。

```
  ND router advertisements live for 1800 seconds
```

常见配置错误

无

3.4.4 配置IPv6 源路由

配置效果

RFC5095 废除了类型 0 路由首部。锐捷的解决方法是缺省情况不支持类型 0 路由首部，管理员可以使用全局配置模式命令“ipv6 source-route”打开这项功能。

注意事项

无

配置方法

↘ 配置设备转发带有路由首部的 IPv6 报文

- 可选配置。
- 如果需要开启 IPv6 源路由功能，可使用该配置。

检验方法

向设备发送带有 0 路由首部的报文，设备能够正常转发。

相关命令

↘ 配置设备转发带有路由首部的 IPv6 报文

【命令格式】 **ipv6 source-route**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 因为类型 0 路由首部有安全隐患：使设备很容易遭受拒绝服务攻击，所以在缺省情况下禁止转发带有路由首部的 IPv6 报文，但是仍然处理最终目的地址是本机的带有类型 0 路由首部的 IPv6 报文。

配置举例

配置支持 IPv6 类型 0 路由。

【配置方法】 开启支持 IPv6 类型 0 路由功能。

```
Ruijie(config)#ipv6 source-route
```

【检验方法】 使用 **show run** 查看配置是否生效。

```
Ruijie#show run | inc ipv6 source-route
ipv6 source-route
```

常见配置错误

无

3.4.5 配置ICMPv6 差错报文的发送速率

配置效果

配置 ICMPv6 差错报文的发送速率。

注意事项

-

配置方法

配置 ICMPv6 报文太大消息的发送速率

- 可选配置。
- 如果设备收到大量 IPv6 报文的长度超过出口的 IPv6 MTU，并因发送 ICMPv6 报文太大消息而消耗较大 CPU 的情况，可以使用该配置限制该差错报文的发送。

配置其它 ICMPv6 差错报文的发送速率

- 可选配置。
- 如果设备收到大量非法 IPv6 报文，并因此而产生大量 ICMPv6 差错报文时，可以使用该配置限制差错报文发送速率（该命令不会影响 ICMPv6 报文太大差错报文的发送速率）

检验方法

执行 **show running-config** 可以看到配置生效。

相关命令

配置 ICMPv6 报文太大消息的发送速率

【命令格式】 **ipv6 icmp error-interval too-big** *milliseconds* [*bucket-size*]

【参数说明】 *milliseconds*：令牌桶的刷新周期，取值范围 0~2147483647，缺省值为 100，单位为毫秒。取值为 0 时，表示不限制 ICMPv6 差错报文的发送速率。

bucket-size：令牌桶中容纳的令牌数，取值范围 1~200，缺省值为 10。

【命令模式】 全局模式

【使用指导】 为了防止拒绝服务攻击，对 ICMPv6 差错报文的发送速率进行限制，采用令牌桶算法。

如果转发的 IPv6 报文的长度超过出口的 IPv6 MTU，路由器会丢弃 IPv6 报文，并且向源 IPv6 地址发送 ICMPv6 报文太大消息，这种 ICMPv6 差错报文的主要用途是 IPv6 路径 MTU 发现。为了防止其它 ICMPv6 差错报文太多导致发不出 ICMPv6 报文太大消息，从而导致 IPv6 路径 MTU 发现功能失效，对 ICMPv6 报文太大消息和其它 ICMPv6 差错报文分别限速。

因为定时器的精度是 10 毫秒，建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于,0 小于 10，实际生效的刷新周期是 10 毫秒，例如配置 5 毫秒 1 个，实际效果是 10 毫秒 2 个；如果令牌桶的刷新周期不是 10 毫秒的整数倍，实际生效的刷新周期自动换算成 10 毫秒的整数倍，例如配置 15 毫秒 3 个，实际效果是 10 毫秒 2 个。

配置其它 ICMPv6 差错报文的发送速率

【命令格式】 **ipv6 icmp error-interval** *milliseconds* [*bucket-size*]

【参数说明】 *milliseconds*：令牌桶的刷新周期，取值范围 0~2147483647，缺省值为 100，单位为毫秒。取值为 0 时，表示不限制 ICMPv6 差错报文的发送速率。

bucket-size：令牌桶中容纳的令牌数，取值范围 1~200，缺省值为 10。

【命令模式】 全局模式

【使用指导】 为了防止拒绝服务攻击，对 ICMPv6 差错报文的发送速率进行限制，采用令牌桶算法。

因为定时器的精度是 10 毫秒，建议用户把令牌桶的刷新周期配置成 10 毫秒的整数倍。如果令牌桶的刷新周期大于,0 小于 10，实际生效的刷新周期是 10 毫秒，例如配置 5 毫秒 1 个，实际效果是 10 毫秒 2 个；如果令牌桶的刷新周期不是 10 毫秒的整数倍，实际生效的刷新周期自动换算成 10 毫秒的整数倍，例如配置 15 毫秒 3 个，实际效果是 10 毫秒 2 个。

配置举例

配置 ICMPv6 差错报文的发送速率

【配置方法】 配置 ICMPv6 报文太大消息的发送速率为 1 秒 100 个，配置其它 ICMPv6 差错报文的发送速率为 1 秒 10 个。

```
Ruijie(config)#ipv6 icmp error-interval too-big 1000 100
Ruijie(config)#ipv6 icmp error-interval 1000 10
```

【检验方法】 执行 **show running-config** 可以看到配置生效。

```
Ruijie#show running-config | include ipv6 icmp error-interval
ipv6 icmp error-interval 1000 10
ipv6 icmp error-interval too-big 1000 100
```

常见配置错误

无

3.4.6 配置IPv6 HOP-LIMIT

配置效果

配置发送单播报文的跳数，避免报文在网络上无限传播下去。

注意事项

-

配置方法

↘ 设置 IPv6 HOP-LIMIT 值

- 可选配置
- 如果需要修订单播报文的转发跳数，可以使用该配置

检验方法

- 通过 **show running-config** 命令查看配置是否正确。
- 本地发送 ipv6 单播报文，抓包可以看到 ipv6 首部的 hop-limit 字段值与配置的一致。

相关命令

↘ 设置 IPv6 HOP-LIMIT 值

【命令格式】 **ipv6 hop-limit value**
【参数说明】 *value*：设备发送单播报文的跳数值，范围 1~255。
【命令模式】 全局模式
【使用指导】 -

配置举例

配置 IPv6 HOP-LIMIT

【配置方法】 修改设备 IPv6 HOP-LIMIT 为 250。

```
Ruijie(config)#ipv6 hop-limit 250
```

【检验方法】 通过 **show running-config** 查看配置是否生效。

```
Ruijie#show running-config
ipv6 hop-limit 254
```

常见配置错误

无

3.5 监视与维护

清除各类信息

在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除动态学习到的邻居。	**clrear ipv6 neighbors** [*interface-id*]

查看运行情况

作用	命令
显示接口上关于 IPv6 的信息	**show ipv6 interface** [[*interface-id*] [ra-info]] [brief [*interface-id*]]
显示邻居的信息	**show ipv6 neighbors** [**verbose**] [*interface-id*] [*ipv6-address*] [**static**]

查看调试信息

输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
查看 ND 学习情况	**debug ipv6 nd**

4 DHCP

4.1 概述

DHCP（Dynamic Host Configuration Protocol，动态主机设置协议）是一个 局域网的 网络协议，使用UDP协议工作，被广泛用来动态分配可重用的网络资源，如IP地址。

DHCP 是基于 Client/Server 工作模式，DHCP 客户端通过发送请求消息向 DHCP 服务器获取 IP 地址，等其他配置信息。当 DHCP 客户端与服务器不在同一个子网上，必须有 DHCP 中继代理（DHCP Relay）来转发 DHCP 请求和应答消息。

协议规范

- RFC2131：Dynamic Host Configuration Protocol
- RFC2132：DHCP Options and BOOTP Vendor Extensions
- RFC3046：DHCP Relay Agent Information Option

4.2 典型应用

典型应用	场景描述
在局域网内提供DHCP服务	为局域网内下游用户分配地址。
设备启动DHCP Client功能	局域网内下游多设备启动 DHCP Client 功能。
无线场景中DHCP Relay典型应用	无线场景中跨网段的用户申请 IP 上网。
使用外部获取DNS服务器地址	无线场景，DHPC Server 优先使用外部获取的 DNS 服务器地址

4.2.1 在局域网内提供DHCP服务

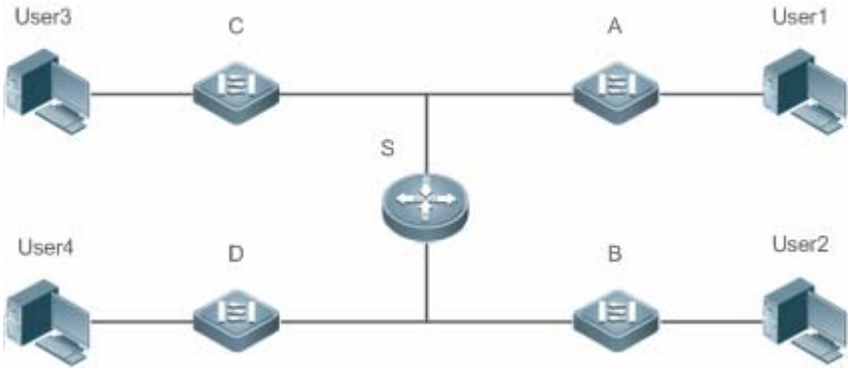
应用场景

在一个局域网内，为四个用户分配 IP 地址。

以下图为例，为 User1、User2、User3 、User4 分配 IP 地址。

- User1、User2、User3 、User4 通过 A、B、C、D 与 Server 相连

图 4-1



【注释】 S 为出口网关设备，作 DHCP-Server。
A、B、C、D 为接入交换机，作二层透传
User1、User2、User3 、User4 为用户

功能部属

- Server(S)上运行 DHCP-Server 服务
- 在 A、B、C、D 上实行二层 VLAN 透传功能
- User1、User2、User3 、User4 上主动发起 DHCP-Client 请求

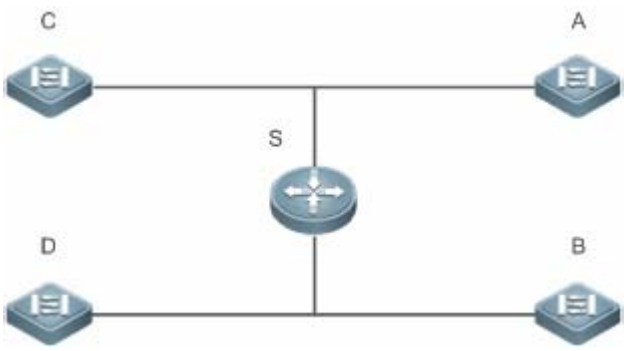
4.2.2 设备启动DHCP Client功能

应用场景

在一个局域网内，A、B、C、D 四个接入设备向 S 请求地址

以下图为例，A、B、C、D 接口上开启 DHCP-Client 功能，请求 IP 地址。

图 4-2



【注释】 S 为出口网关设备，作 DHCP-Server。
A、B、C、D 为接入交换机，接口启动 DHCP-Client 功能

功能部属

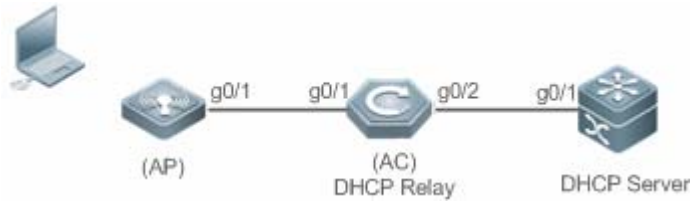
- Server(S)上运行 DHCP-Server 服务
- 在 A、B、C、D 在接口上开启 DHCP-Client 功能

4.2.3 无线场景中DHCP Relay典型应用

应用场景

无线跨网段的用户申请 IP 上网，要求无线用户跨网段可以获取 IP 地址进行正常上网。

图 4-6DHCP Relay 组网拓扑图



【注释】 AP 为无线接入点设备。
AC 为无线管理点设备，同时作为 DHCP Relay 设备，负责无线用户跨网段报文中继。
核心设备为 Server 服务器，负责为用户分配地址。

功能部属

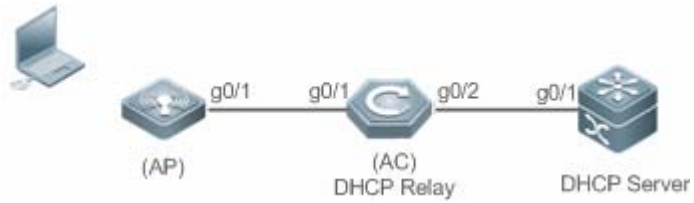
- 配置无线接入点（AP 设备）接入到无线管理设备（AC 设备）中。
- 配置无线管理设备（AC 设备）中启动 DHCP Relay 功能。
- 配置核心设备中启动 DHCP Server 功能。

4.2.4 无线场景中DHCP Server优先使用外部获取的DNS服务器地址

应用场景

无线胖 AP 的 WAN 口工作在 PPPoE 或 DHCP Client 场景下，可自动从外部获取到 DNS 地址，设置到本机的 DHCP 服务器上，避免用户必须进行 DNS 配置。当胖 AP 作为 DHCP Server 给用户分配地址时，优先使用从外部获取到 DNS 地址。

图 4-3 DHCP Server 组网拓扑图



【注释】 AP 工作模式为胖 AP，其中 WAN 口工作在 PPPoE 或者 DHCP Client 模式，从外部获取 IP 地址和 DNS 服务器地址。同时 AP 也作为 DHCP Server 给 STA 分配地址。

功能部属

- 配置 AP 为胖 AP 模式，AP 的 WAN 口上面开启 PPPoE 或者 DHCP Client 功能。
- AP 上面启动 DHCP Server 功能，为 STA 分配地址。
- DHCP Server 给 STA 分配地址时 ,分配给用户的 DNS 地址优先使用 PPPoE 或者 DHCP Client 模块从外部获取到的 DNS 地址。

4.3 功能详解

基本概念

DHCP 服务器

锐捷产品的 DHCP 服务器完全根据 RFC 2131 来实现的，主要功能就是为主机分配和管理 IP 地址。

DHCP 客户端

DHCP 客户端可以让设备自动地从 DHCP 服务器获得 IP 地址以及其它配置参数。

DHCP 中继

当 DHCP 客户端与服务器不在同一个子网上，就必须有 DHCP 中继代理来转发 DHCP 请求和应答消息。

租约

租约是客户机可使用指派的 IP 地址期间 DHCP 服务器指定的时间长度。租用给客户时，租约是活动的。在租约过期之前，客户机一般需要通过服务器更新其地址租约时间。当租约期满或在服务器上删除时，租约是非活动的。租约期限决定租约何时期满以及客户需要用服务器更新它的次数。

排除地址

排除地址是指从 DHCP 服务器中排除指定的一些 IP 地址序列，排除地址作用是为了确保在这些地址都不会是由 DHCP 服务器提供给 DHCP 客户机。

地址池

地址池是指 DHCP 服务器可分配给用户的地址集合，所有分配给用户的地址都从管理员配置的池中取出的。

选项类型

选项类型是 DHCP 服务器在向 DHCP 客户机提供租约服务时指派的配置参数。例如，某些公用选项包括默认网关（路由器）、WINS 服务器和 DNS 服务器的 IP 地址。DHCP-Server 还允许配置其它选项。虽然大多数选项都是在 RFC 2132 中预定义的，但若需要的话，可添加自定义选项类型。

功能特性

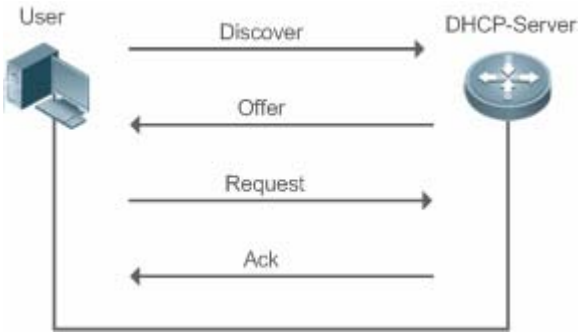
功能特性	作用
DHCP服务器	设备启用 DHCP Server 功能，可以为主机动态分配 IP 地址和提供主机配置参数。
DHCP中继	设备启用 DHCP Relayr 功能，可以在不同网段之间转发 DHCP 请求和应答消息。
DHCP客户端	设备启用 DHCP Client 功能，可以自动从 DHCP 服务器获取 IP 地址以及其它配置参数。
AM规则	用于规划不同 vlan + port/vlan 上来的 DHCP 客户端请求的 IP 范围

4.3.1 DHCP服务器

工作原理

DHCP 工作的基本流程

图 4-8



DHCP 请求 IP 地址的过程如下：

1. 主机发送 DHCPDISCOVER 广播包在网络上寻找 DHCP 服务器；
2. DHCP 服务器向主机发送 DHCPOFFER 单播/广播(依据主机报文相关属性确定)数据包，包含 IP 地址、MAC 地址、域名信息以及地址租期；
3. 主机发送 DHCPREQUEST 广播包，正式向服务器请求分配已提供的 IP 地址；
4. DHCP 服务器向主机发送 DHCPACK 单播包，确认主机的请求。

DHCP 客户端可以接收到多个 DHCP 服务器的 DHCPOFFER 数据包，然后可能接受任何一个 DHCPOFFER 数据包，但客户端通常只接受收到的第一个 DHCPOFFER 数据包。另外，DHCP 服务器 DHCPOFFER 中指定的地址不一定为最终分配的地址，通常情况下，DHCP 服务器会保留该地址直到客户端发出正式请求。

正式请求 DHCP 服务器分配地址 DHCPREQUEST 采用广播包，是为了让其它所有发送 DHCPOFFER 数据包的 DHCP 服务器也能够接收到该数据包，然后释放已经 OFFER（预分配）给客户端的 IP 地址。

如果发送给 DHCP 客户端的 DHCPOFFER 信息包中包含无效的配置参数，客户端会向服务器发送 DHCPDECLINE 信息包拒绝接受已经分配的配置信息。

在协商过程中，如果 DHCP 客户端没有及时响应 DHCPOFFER 信息包，DHCP 服务器会发送 DHCPNAK 消息给 DHCP 客户端，导致客户端重新发起地址请求过程。

在网络建设中，应用锐捷产品 DHCP 服务器，可以带来以下好处：

- 降低网络接入成本。一般采用静态地址分配的接入费用比较昂贵，应用动态地址分配的接入成本较低。
- 简化配置任务，降低网络建设成本。采用动态地址分配，大大简化了设备配置，对于在没有专业技术人员的地方部署设备，更是降低了部署成本。
- 集中化管理。在对多个子网进行配置管理时，有任何配置参数的变动，只需要修改和更新 DHCP 服务器的配置即可。

↘ 地址池

Server 收到来自 Client 请求报文，首先选择出一个合法有效地址池，并在该池中通过 PING 机制确认一个可用的地址，接着下发该池相关配置信息与地址至客户端，同时本地保存该租约信息在，以供该客户续租时检查有效性使用；由此完成整个租约分配流程。

地址池中可以带有各种配置参数，以下列举几个常用的：

- 地址池范围，可以分配给用户的地址范围
- 网关地址，通告用户网关地址，最多可以有八个
- DNS 地址，通告用户 DNS 地址，最多可以有八个
- 租约周期，通告用户地址何时老化，用户何时该请求续租

↘ VRRP 监控功能

在 VRRP (Virtual Router Redundancy Protocol，虚拟路由冗余协议)应用场景下，DHCP 提供配置命令来决定是否监控当前接口的 VRRP 状态。对于配置了 VRRP 地址的接口，当配置监控 VRRP 状态后，DHCP 服务器仅对处于 Master 状态的设备接口上来的 DHCP 客户端请求报文进行处理，处于备份(Backup)状态的接口请求报文将被丢弃。而对于没配置 VRRP 地址的接口，DHCP 服务器不再监控 VRRP 状态，所有 DHCP 请求报文都会得到处理。VRRP 监控命令只能在三层口上配置，默认情况下 VRRP 监控功能关闭，即只有主机处理 DHCP 业务备机不处理。

↘ 基于 vlan+端口+ip-range 地址分配功能

在布署地址池的环境下，为每个 vlan+端口号来分配指定 ip-range 的地址功能(在满足正常动态地址分配逻辑后，才能从本配置中选择有效地址)。主要有三种应用场景：1.只有全局默认配置；2.只有基于 vlan+端口+ip-range 的配置；3.上述两种配置均有；场景 1 有全局配置,默认分配全局配置的区间地址；场景 2 来自指定 vlan+端口的用户分配指定区间的地址，其余则用户无地址分配；场景 3 满足场景 2 的分配指定区间地址，其余用户分配全局默认配置地址。

↘ 添加可信 ARP 功能

可信 ARP 用于防止针对网关的 ARP 欺骗。DHCP 提供配置命令来决定分配地址时是否下发可信 ARP。当配置了添加可信 ARP 后，DHCP 服务器在分配地址时，会添加可信 ARP，从而有效防止 ARP 欺骗。

基于 ARP 检测用户下线

DHCP 提供配置命令来决定是否基于 ARP 检测用户下线。当配置了基于 ARP 检测用户下线时，用户下线后，DHCP 服务器会收到 ARP 老化通告，开始回收地址。如果一段时间内（默认 5 分钟），用户没有重新上线，DHCP 服务器就回收该地址，分配给新用户；如果在该段时间内重新上线，用户可以继续使用该地址。

添加伪服务器检测功能

如果网络中私自部署 DHCP 服务器，当客户端申请地址时，会与这台服务器进行交互，导致客户端分配到错误的 IP 地址。这台服务器称为伪服务器。DHCP 提供配置命令来决定是否开启伪服务器检测功能。当配置伪服务器检测功能时，DHCP 会检查接收到的 DHCP 报文中是否携带 Option 54（Server Identifier Option，服务器标识选项）。如果携带该选项，并且选项内容与真实 DHCP 服务器标识不相符，则记录此伪服务器的 IP 地址和接收到报文的端口信息。伪服务器检测只是一种事后检测的安全功能，并不能预防非法 DHCP 服务器给客户端分配地址。

相关配置

全局启动 DHCP-Server 服务

- 缺省情况下，该服务关闭。
- 全局使用 **service dhcp** 开启该服务。
- 必须在全局使用 **service dhcp** 功能，才能进行 DHCP 服务。

配置地址池

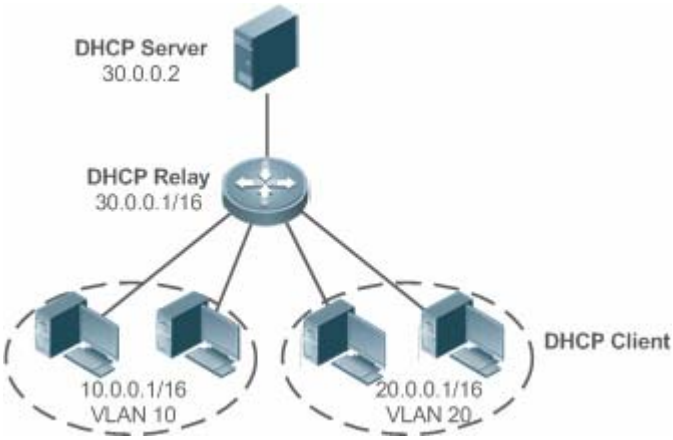
- 缺省情况下，无地址池。
- 使用 **ip dhcp pool** 命令可以进入到地址池配置模式，进行地址范围、网关地址、DNS 等信息配置。
- 不配置地址池范围将无地址可分配，无法下发任何地址。

4.3.2 DHCP中继代理

工作原理

DHCP 请求报文的目的 IP 地址为 255.255.255.255，这种类型报文的转发局限于子网内。为了实现跨网段的动态 IP 地址分配，DHCP 中继就产生了。DHCP 中继将收到的 DHCP 请求报文以单播方式转发给 DHCP 服务器，同时将收到的 DHCP 响应报文转发给 DHCP 客户端。DHCP 中继相当于一个转发站，负责沟通位于不同网段的 DHCP 客户端和 DHCP 服务器，即转发客户端 DHCP 请求报文、转发服务端 DHCP 应答报文。这样就实现了只要安装一个 DHCP 服务器，就可以实现对多个网段的动态 IP 管理，即 Client—Relay—Server 模式的 DHCP 动态 IP 管理。如图所示：

图 4-9 DHCP Relay 应用场景



VLAN 10 和 VLAN 20 分别对应 10.0.0.1/16 和 20.0.0.1/16 的网络，而 DHCP 服务器在 30.0.0.1/16 的网络上，30.0.0.2 的 DHCP 服务器要对 10.0.0.1/16 和 20.0.0.1/16 的网络进行动态 IP 管理，只要在作为网关的设备上打开 DHCP 中继功能，并配置 30.0.0.2 为 DHCP 服务器的 IP 地址。

↘ DHCP Relay Agent Information(option 82)

根据 RFC3046 的定义，中继设备进行 DHCP Relay 时，可以通过添加 option 的方式来详细的标明 DHCP 客户端的一些网络信息，从而使服务器可以根据更精确的信息给用户分配不同权限的 IP，根据 RFC3046 的定义，所使用 option 选项的选项号为 82，故也被称作 option 82。锐捷实现的 Relay agent information 目前存在以下应用方案：

1. Relay agent information option82：此种 option 的应用不需要结合其他协议模块的运行。DHCP 中继根据接收 DHCP 请求报文的实体端口，以及设备自身的物理地址信息，组合构成 option82 选项。选项格式如下图所示：

图 4-11 Agent Circuit ID

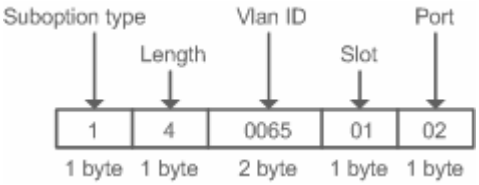
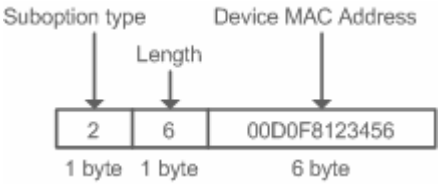


图 4-4 Agent Remote ID



↘ DHCP Relay Check Server-id 功能

在 DHCP 应用环境中，通常会为每一个网络配备多个 DHCP 服务器，从而进行备份，防止因为一台服务器的工作不正常影响网络的正常使用。在 DHCP 获取的四个交互过程中，当 DHCP 客户端在发送 DHCP REQUEST 时已经选定了服务器，此时会在请求的报文中携带一个 server-id 的 option 选项，在某些特定的应用环境中为了减轻网络服务器压力，需要我们 Relay 能够

使能此选项，只把请求报文发给此选项里的 DHCP 服务器，而不是发送给每一个配置的 DHCP 服务器，上述就是 DHCP Relay check server-id 功能 。

DHCP Relay suppression 功能

在指定接口上配置命令 ip DHCP Relay suppression 后，将屏蔽该接口上收到的 DHCP 请求报文；而对于其他接口上收到的 DHCP 请求报文，则正常转发。

相关配置

启动设备上的 DHCP Relay 功能

- 缺省情况下，设备上的 DHCP Relay 功能关闭。
- 使用 **service dhcp** 命令可以启动设备上的 DHCP Relay 功能。
- 必须在设备上启用 DHCP Relay 功能，DHCP Relay 才能正常工作。

配置 DHCP 服务器的 IP 地址

- 缺省情况下，无 DHCP 服务器的 IP 地址表项。
- 使用 **ip helper-address** 命令可以添加 DHCP 服务器地址表项，DHCP 服务器地址全局配置最多可以配置 20 个 DHCP 服务器地址。

启动 DHCP option 82 功能

- 缺省情况下，设备上的 DHCP option 82 功能关闭。
- 使用 **ip dhcp relay information option82** 命令可以启动设备上的 DHCP option 82 功能。

启动 DHCP Relay check server-id 功能

- 缺省情况下，设备上的 DHCP Relay check server-id 功能关闭。
- 使用 **ip dhcp relay check server-id** 命令可以启动设备上的 DHCP Relay check server-id 功能。

启动 DHCP Relay suppression 功能

- 缺省情况下，所有接口上 DHCP Relay suppression 功能关闭。
- 使用 **ip dhcp relay suppression** 命令可以启动对应接口上的 DHCP Relay suppression 功能。

4.3.3 DHCP客户端

工作原理

Client 状态机进入 Init 状态，主动发出广播 Discover 报文，之后 Client 有可能收到多份 Offer，进入 Offer 选择阶段选择一份最优的 Offer 后给予该服务器响应，此后在地址的老化 1/2、4/5 周期内还会发出续租等报文请求对地址的继续使用。

相关配置

↘ 接口上启动 DHCP-Client 功能

- 缺省情况下，该服务关闭。
- 接口模式下使用 **ip address dhcp** 开启功能。
- 必须开启客户端功能，才能进行 DHCP 服务。
- 该功能只在三层接口上有效，如 SVI、Rourter Port 等；

4.3.4 AM规则

工作原理

AM 规则用于规划不同 vlan + port/vlan 上来的 DHCP 客户端请求的 IP 范围，可快速定位出问题的 DHCP 客户端所属的 vlan + port/vlan，也可以更有效地分配地址池的地址。使用 AM 规则后，所有来自配置 vlan + port/vlan 的 DHCP 客户端能够正常获得地址；反之，若 DHCP 客户端来源未配置 vlan + port/vlan 时：如果配置了缺省 AM 规则， DHCP 客户端将获得缺省区间中的地址，如果未配置缺省 AM 规则， DHCP 客户端无法获得地址。

相关配置

↘ 在全局配置模式下进入 AM 规则配置模式

- 全局配置模式下使用 **address-manage** 进入 AM 配置模式；
- 使用 match ip default 命令配置缺省 AM 规则；
- 使用 match ip 命令配置基于 vlan+port/vlan 的 AM 规则；

4.4 配置详解

↘ 配置 DHCP 服务器

配置项	配置建议 & 相关命令	
配置DHCP服务器动态分配IP地址	⚠ 必须配置，用于启用 DHCP 服务器实现动态 IP 址分配。	
	service dhcp	启动 DHCP-SERVER 功能
	ip dhcp pool	配置地址池
	network	配置 DHCP 地址池的网络号和掩码
	⚠ 可选配置，用于设置地址池相关属性。	
	default-router	配置客户端缺省网关
	lease	配置地址租期
	next-server	配置客户端启动的下载服务器地址
	bootfile	配置客户端启动文件
	domain-name	配置客户端的域名

	dns-server	配置域名服务器
	netbios-name-server	配置 NetBIOS WINS 服务器
	netbios-node-type	配置客户端 NetBIOS 节点类型
	lease-threshold	配置地址池告警门限值
	option	配置自定义选项
	pool-status	配置地址池启用或关闭
	update arp	配置从地址池分配地址时添加可信 ARP
配置DHCP服务器手工地址绑定	⚠ 可选配置，用于为客户静态配置 IP 地址。	
	ip dhcp pool	配置地址池名并进入地址池配置模式
	host	配置客户端主机的 IP 地址和网络掩码
	hardware-address	配置客户端的硬件地址
	client-identifier	配置客户端的唯一标识
	client-name	配置客户端的名字
配置基于vlan / port地址分配	⚠ 可选配置，用于规划不同 vlan + port/vlan 上来的 DHCP 客户端请求的 IP 范围	
	address-manage	进入 AM 配置模式
	match ip default	配置缺省 AM 规则
	match ip	配置基于 vlan+port/vlan 的 AM 规则
配置DHCP服务器全局属性	⚠ 可选配置，用于设置 DHCP 服务器相关属性。	
	ip dhcp excluded-address	配置排除地址
	ip dhcp force-send-nak	配置 DHCP 服务器强制回复 NAK
	ip dhcp monitor-vrrp-state	配置监控 VRRP 状态
	ip dhcp ping packets	配置 Ping 包次数
	ip dhcp ping timeout	配置 Ping 包超时时间
	ip dhcp refresh arp	配置 DHCP 服务器重新下发可信 ARP
	ip dhcp server arp-detect	配置 DHCP 服务器检测用户下线
	ip dhcp server detect	配置伪服务器检测

↘ 配置 DHCP 中继代理

配置项	配置建议 & 相关命令	
配置DHCP Relay基本功能	⚠ 必须配置。用于建立 DHCP Relay 服务。	
	service dhcp	启动 DHCP Relay 功能
	ip helper-address	配置 DHCP 服务器的 IP 地址
配置DHCP Relay option 82 功能	⚠ 可选配置。结合设备自身物理接口信息，给用户分配不同权限 IP。	
	ip dhcp relay information option82	启用 DHCP option82 功能

配置DHCP Relay check server-id 功能	⚠ 可选配置。DHCP Relay 仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。	
	ip dhcp relay check server-id	启用 DHCP Relay check server-di 功能
配置DHCP Relay suppression功能	⚠ 可选配置。屏蔽对应接口地址上 DHCP 请求报文。	
	ip dhcp relay suppression	启用 DHCP Relay suppression 功能

配置 DHCP 客户端

配置项	配置建议 & 相关命令	
配置DHCP客户端	⚠ 必须配置，用于启用 DHCP 客户端	
	ip address dhcp	使得以太网或者 PPP、HDLC、FR 封装的接口能够通过 DHCP 获得 IP 地址信息

4.4.1 配置DHCP服务器动态分配IP地址

配置效果

向所有 dhcp-client 提供 dhcp 服务，包括地址、网关等信息下发

注意事项

DHCP 服务器和 DHCP 中继共用 **service dhcp** 这条命令，但是这两个功能是互斥的，两者之间的切换依赖于是否配置了 DHCP 地址池。

配置方法

启动 DHCP-SERVER 功能

- 实现动态分配地址功能，为必选配置。
- 在配置模式下执行 **service dhcp** 命令。

配置地址池

- 创建地址池，为必选配置。
- 在配置模式下执行 **ip dhcp pool** 命令。

配置 DHCP 地址池的网络号和掩码

- 动态分配地址范围，为必选配置。
- 在地址池模式下执行 **network** 命令。

配置客户端缺省网关

- 用于通告客户端网关地址，为可选配置。
- 在地址池模式下执行 **default-router** 命令。

配置地址租期

- 用于通告客户端租约老化周期，默认值为 24h，为可选配置。
- 在地址池模式下执行 **lease** 命令。

配置客户端启动的下载服务器地址

- 用于通告客户端 TFTP 服务器地址，为可选配置。
- 在地址池模式下执行 **next-server** 命令。

配置客户端的域名

- 用于通告客户端的域名，为可选配置。
- 在地址池模式下执行 **domain-name** 命令。

配置域名服务器

- 用于通告客户客户端 dns 地址，为可选配置。
- 在地址池模式下执行 **dns** 命令。

配置 NetBIOS WINS 服务器

- 用于通告 windows 客户端 dns 地址，为可选配置。
- 在地址池模式下执行 **netbios-name-server** 命令。

配置客户端 NetBIOS 节点类型

- 用于通告 windows 客户端节点类型，为可选配置。
- 在地址池模式下执行 **netbios-name-type** 命令。

配置地址池告警门限值

- 用于管理租约数量，达到限制时打印警告，默认为 90%，为可选配置。
- 在地址池模式下执行 **lease-threshold** 命令。

配置自定义选项

- 用于通告客户端相当配置信息，为可选配置。
- 在地址池模式下执行 **option** 命令。

配置地址池启用或关闭

- 用于配置地址池是否可用，默认为开启，为可选配置。
- 在地址池模式下执行 **pool-status** 命令。

配置添加可信 ARP

- 用于配置分配地址时添加可信 ARP，默认为关闭，为可选配置。
- 在地址池模式下执行 **update arp** 命令。

检验方法

利用 DHCP 客户端与 DHCP 服务器进行连接

- 检查客户端是否能取到服务器上配置的相关信息

相关命令

启动 DHCP-SERVER 功能

【命令格式】 **service dhcp**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 启用 DHCP 服务器和 DHCP 中继代理功能，DHCP 服务器和 DHCP 中继共用 **service dhcp** 这条命令，两功能可以同时存在，但是报文是通过 Relay 转发还是直接由 Server 处理，取决于设备上是否配置了合法有效的地址池，如果存在地址池则由 Server 处理，不存在由 Relay 转发。

配置地址池

【命令格式】 **ip dhcp pool** *dhcp-pool*

【参数说明】 *pool-name*：地址池名称

【命令模式】 全局模式

【使用指导】 要给用户下发地址，首先要配置地址池名并进入地址池配置模式

配置 DHCP 地址池的网络号和掩码

【命令格式】 **network** *network-number mask* [*low-ip-address high-ip-address*]

【参数说明】 *network-number:* DHCP 地址池的 IP 地址网络号

mask: DHCP 地址池的 IP 地址网络掩码。如果没有定义掩码，缺省为自然网络掩码

【命令模式】 DHCP 地址池配置模式

【使用指导】 进行动态地址绑定的配置，必须配置新建地址池的子网及其掩码，为 DHCP 服务器提供了一个可分配给客户端的地址空间。DHCP 在分配地址池中的地址，是按顺序进行的，如果该地址已经在 DHCP 绑定表中或者检测到该地址已经在该网段中存在，就检查下一个地址，直到分配一个有效的地址。

锐捷无线产品中新增了可以配置地址池的网段范围，指明可以分配的网段中的起始地址和终止地址，该配置为可选配置。在不指明起始地址和终止地址的情况下，地址池的可分配的 IP 地址范围为该网段内的所有 IP 地址

锐捷产品的 DHCP 动态地址池中，地址的分配是以客户端的物理地址和客户端 ID 为索引的，这就意味着 DHCP 动态地址池中不可能存在相同客户端的两份租约；如果客户端和服务器之间的网络拓扑存在路径上的冗余[客户端可以通过直连路径，同时也可以通过中继路径到达服务器]，就会导致服务器分配地址出现问题，可能导致地址分配失败；

因此，为了避免上述问题，要求网络管理员在构建网络的时候，通过其它的方式，如调整物理链路或者网络

路径，来避免这种客户端到服务器的路径冗余

配置客户端缺省网关

【命令格式】 **default-router** *address* [*address2…address8*]

【参数说明】 *address*：定义客户端默认网关的 IP 地址。要求至少配置一个

ip-address2…ip-address8：（可选）最多可以配置 8 个网关

【命令模式】 DHCP 地址池配置模式

【使用指导】 配置客户端默认网关，这个将作为服务器分配给客户端的默认网关参数。缺省网关的 IP 地址必须与 DHCP 客户端的 IP 地址在同一网络

配置地址租期

【命令格式】 **lease** {*days* [*hours]* [*minutes*] | **infinite**}

【参数说明】 *days*：定义租期的时间，以天为单位

hours: （可选）定义租期的时间，以小时为单位。定义小时数前必须定义天数

minutes: （可选）定义租期的时间，以分钟为单位。定义分钟前必须定义天数和小时数

infinite: 定义没有限制的租期

【命令模式】 DHCP 地址池配置模式

【使用指导】 DHCP 服务器给客户端分配的地址，缺省情况下租期为 1 天。当租期快到时客户端需要请求续租，否则过期后就不能使用该地址

配置客户端启动文件

【命令格式】 **bootfile** *filename*

【参数说明】 *file-name*：定义用于启动的文件名

【命令模式】 DHCP 地址池配置模式

【使用指导】 客户端启动文件是客户端启动时要用到的启动映像文件。启动映像文件通常是 DHCP 客户端需要下载的操作系统

配置客户端的域名

【命令格式】 **domain-name** *domain*

【参数说明】 *domain-name:* 定义 DHCP 客户端的后缀域名字符串

【命令模式】 DHCP 地址池配置模式

【使用指导】 可以指定客户端的域名，这样当客户端通过主机名访问网络资源时，不完整的主机名会自动加上域名后缀形成完整的主机名

配置域名服务器

【命令格式】 **dns-server** *ip-address* [*ip-address2…ip-address8*]

【参数说明】 *ip-address:* 定义 DNS 服务器的 IP 地址。要求至少配置一个

ip-address2…ip-address8: （可选）最多可以配置 8 个 DNS 服务器

【命令模式】 DHCP 地址池配置模式

【使用指导】 当客户端通过主机名访问网络资源时，需要指定 DNS 服务器进行域名解析。要配置 DHCP 客户端可使用的域名服务器

配置 NetBIOS WINS 服务器

【命令格式】 **netbios-name-server** *address* [*address2…address8*]

【参数说明】 *address:* 定义 WINS 服务器的 IP 地址。要求至少配置一个

ip-address2…ip-address8: （可选）最多可以配置 8 个 WINS 服务器

【命令模式】 DHCP 地址池配置模式

【使用指导】 WINS 是微软 TCP/IP 网络解析 NetNBIOS 名字到 IP 地址的一种域名解析服务。WINS 服务器是一个运行在 Windows NT 下的服务器。当 WINS 服务器启动后，会接收从 WINS 客户端发送的注册请求，WINS 客户端关闭时，会向 WINS 服务器发送名字释放消息，这样 WINS 数据库中与网络上可用的计算机就可以保持一致了

配置客户端 NetBIOS 节点类型

【命令格式】 **netbios-node-type** *type*

【参数说明】 type: 定义 NetBIOS 节点类型，有两种方式

数字定义，范围从 0~FF，十六进制数，但只能取以下值：

- 代表 b-node
- 代表 p-node
- 代表 m-node
- 8，代表 h-node

字符串定义：

- b-node，广播型节点
- p-node，对等型节点
- m-node，混合型节点
- h-node，复合型节点

【命令模式】 DHCP 地址池配置模式

【使用指导】 微软 DHCP 客户端 NetBIOS 节点类型有四种：1）Broadcast，广播型节点，通过广播方式进行 NetBIOS 名字解析；2）Peer-to-peer，对等型节点，通过直接请求 WINS 服务器进行 NetBIOS 名字解析；3）Mixed，混合型节点，先通过广播方式请求名字解析，后通过与 WINS 服务器连接进行名字解析；4）Hybrid，复合型节点，首先直接请求 WINS 服务器进行 NetBIOS 名字解析，如果没有得到应答，就通过广播方式进行 NetBIOS 名字解析。

缺省情况下，微软操作系统的节点类型为广播型或者复合型。如果没有配置 WINS 服务器，就为广播型节点；如果配置了 WINS 服务器，就为复合型节点

配置自定义选项

【命令格式】 **option** *code* { **ascii** *string* | **hex** *string* | **ip** *ip-address* }

【参数说明】 *code:* 定义 DHCP 选项代码

ascii *string:* 定义一个 ASCII 字符串

hex *string:* 定义十六进制字符串

ip *ip-address:* 定义 IP 地址列表

【命令模式】 DHCP 地址池配置模式

【使用指导】 DHCP 提供了一个机制，允许在 TCP/IP 网络中将配置信息传送给主机。DHCP 报文专门有 option 字段，该部分内容为可变化内容，用户可以根据实际情况进行定义，DHCP 客户端必须能够接收携带至少 312 字节 option 信息的 DHCP 报文。另外 DHCP 报文中的固定数据字段也称为一个选项

在 WLAN 无线应用环境中，AP 上的 DHCP 客户端会动态申请获取 AC 的 IP 地址列表，可以通过在 DHCP 服务器上配置自定义选项携带 AC 的 IP 地址列表来实现

配置地址池启用或关闭

【命令格式】 **pool-status** {**enable | disable**}

【参数说明】 **enable**：启用地址池

disable：关闭地址池

默认为开启

【命令模式】 DHCP 地址池配置模式

【使用指导】 在锐捷无线产品中新增了可配置 DHCP 地址池是否启用命令，通过配置命令可以启用或关闭对应地址池服务

配置添加可信 ARP

【命令格式】 **update arp**

【参数说明】 -

【命令模式】 DHCP 地址池配置模式

【使用指导】 配置 **update arp** 后，DHCP 从地址池分配地址时添加可信 ARP。可信 ARP 用于防止 ARP 欺骗。

配置举例

配置地址池

【配置方法】

- 定义了一个地址池 net172
- 地址池网段为 172.16.1.0/24
- 缺省网关为 172.16.1.254
- 地址租期为 1 天
- 排除 172.16.1.2~172.16.1.100 地址

```
Ruijie(config)# ip dhcp excluded-address 172.16.1.2 172.16.1.100
Ruijie(dhcp-config)# ip dhcp pool net172
Ruijie(dhcp-config)# network 172.16.1.0 255.255.255.0
Ruijie(dhcp-config)# default-router 172.16.1.254
Ruijie(dhcp-config)# lease 1
```

【检验方法】 1.**show run** 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp excluded-address 172.16.1.2 172.16.1.100
ip dhcp pool net172
network 172.16.1.0 255.255.255.0default-router 172.16.1.254
lease 1
```

4.4.2 配置DHCP服务器手工地址绑定

配置效果

向某些特定的 dhcp-client 下发特定的 ip 地址及其它配置信息

注意事项

无

配置方法

配置地址池名并进入地址池配置模式

- 创建地址池，为必选配置。
- 在配置模式下执行 **ip dhcp pool** 命令。

配置客户端主机的 IP 地址和网络掩码

- 配置静态 ip 地址及网络掩码，必选配置。
- 在地址池模式下执行 **host** 命令。

配置客户端的硬件地址

- 配置静态 mac 地址，可选配置。
- 在地址池模式下执行 **hardware** 命令。

配置客户端的唯一标识

- 配置静态用户 uid，可选配置。
- 在地址池配置下执行 **client-identifier** 命令。

配置客户端的名字

- 配置静态用户名字，可选配置。
- 在地址池模式下执行 **host-name** 命令。

检验方法

对应的用户上线，判断是否能取到相应地址。

相关命令

配置地址池

【命令格式】 **ip dhcp pool** *dhcp-pool*

【参数说明】 *pool-name*：地址池名称

【命令模式】 全局模式

【使用指导】 要给用户下发地址，首先要配置地址池名并进入地址池配置模式

手工地址绑定

【命令格式】 **host** *ip-address* [*netmask*]

client-identifier *unique-identifier*

client-name *name*

【参数说明】 **i***p-address:* 定义 DHCP 客户端主机的 IP 地址

netmask: 定义 DHCP 客户端主机的网络掩码

unique-identifier : 定义客户端硬件地址，如 aabb.bbbb.bb88;定义客户端的标识，如 01aa.bbbb.bbbb.88

name: （可选）用标准的 ASCII 字符定义客户端的名字，名字不要包括域名。如定义 mary 主机名，不可定义成 mary.rg.com

【命令模式】 DHCP 地址池配置模式

【使用指导】 地址绑定是指 IP 地址和客户端 MAC 地址的映射关系。地址绑定有两种：1）手工绑定，就是在 DHCP 服务器数据库中，通过手工定义将 IP 地址和 MAC 地址进行静态映射，手工绑定其实是一个特殊地址池；2）动态绑定，DHCP 服务器接收到 DHCP 请求时，动态地从地址池中分配 IP 地址给客户端，而形成的 IP 地址和 MAC 地址映射。

要定义手工地址绑定，首先需要为每一个手动绑定定义一个主机地址池，然后定义 DHCP 客户端的 IP 地址和硬件地址或客户端标识。硬件地址就是 MAC 地址。客户端标识，微软客户端一般定义客户端标识，而不定义 MAC 地址，客户端标识包含了网络媒介类型和 MAC 地址。关于媒介类型的编码，请参见 RFC 1700 中关于“Address Resolution Protocol Parameters”部分内容。以太网类型为“01”

配置举例

动态地址池

【配置方法】

- 地址池 vlan1 20.1.1.0 255.255.255.0
- 缺省网关为 20.1.1.1
- 租约时间为 1 天

```
Ruijie(config)# ip dhcp pool vlan1
Ruijie(dhcp-config)# network 20.1.1.0 255.255.255.0
Ruijie(dhcp-config)# default-router 20.1.1.1
Ruijie(dhcp-config)# lease 1 0 0
```

【检验方法】 1. show run 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp pool vlan1
network 20.1.1.0 255.255.255.0
default-router 20.1.1.1
lease 1 0 0
```

↘ 手工绑定配置

【配置方法】

- 主机地址 172.16.1.101，掩码为 255.255.255.0
- 主机名 Billy.rg.com
- 缺省网关为 172.16.16.254
- MAC 地址为 00d0.df34.32a3

```
Ruijie(config)# ip dhcp pool Billy
Ruijie(dhcp-config)# host 172.16.1.101 255.255.255.0
Ruijie(dhcp-config)# client-name Billy
Ruijie(dhcp-config)# hardware-address 00d0.df34.32a3 ethernet
Ruijie(dhcp-config)# default-router 172.16.1.254
```

【检验方法】 1.**show run** 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp pool Billy
host 172.16.1.101 255.255.255.0
client-name Billy
hardware-address 00d0.df34.32a3 ethernet
default-router 172.16.1.254
```

4.4.3 配置基于vlan / port地址分配

配置效果

配置该命令后，可依据端口+VLAN 按区间进行地址分配

注意事项

锐捷产品目前版本支持以太网接口、千兆口以及 FR、PPP、HDLC 接口上的配置。

配置方法

在 config 模式下执行 address-manage

在 address-manage 模式下执行 match ip 命令

检验方法

查看不同 vlan、端口下的用户是否取到有效地址

相关命令

配置缺省区间

【命令格式】 **match ip default** *ip-address netmask*

【参数说明】 *ip-address:* 网络地址

netmask: 地址掩码

【命令模式】 address-manage 模式下

【使用指导】 配置该命令后所有来自未配置 vlan + port 的 DHCP 客户端将取得缺省区间内的地址，如果无该配置命令同时也无任何其它 vlan + port 配置，则按正常流程分配地址。

配置基于 vlan/port 规则下的动态地址分配

【命令格式】 **match ip** *ip-address netmask interface* [**add**/**remove**] **vlan** *vlan-list*

【参数说明】 *ip-address:* 网络地址

netmask: 地址掩码

interface: 接口名称

add/remove: 添加或删除指定 vlan

vlan-list: vlan 索引

【命令模式】 address-manage 模式下

【使用指导】 配置该命令后来自指定 vlan + port 的 DHCP 客户端将取得配置间内地址。

配置基于 vlan 规则下的静态地址分配

【命令格式】 **match ip** *ip-address netmask* [**add**/**remove**] **vlan** *vlan-list*

【参数说明】 *ip-address:* 网络地址

netmask: 地址掩码

add/remove: 添加或删除指定 vlan

vlan-list: vlan 索引

【命令模式】 address-manage 模式下

【使用指导】 在 supervlan 场景下，满足 Dhcp 静态地址池配置的用户，无论在哪个 subvlan 下都只分配该静态地址；此时 AM 无需基于所有 subvlan/port 对该地址进行配置，只需要配置该地址在对应的 vlan 区间生效即可。该规则当前只对静态地址分配生效，动态地址不生效。

配置举例

AM 规则配置

【配置方法】

- 配置缺省规则规则
- 配置指定 vlan+port+地址区间规则
- 配置指定 vlan+地址区间规则

```
Ruijie(config)# address-manage
Ruijie(config-address-manage)# match ip default 172.50.128.0 255.255.128.0
Ruijie(config-address-manage)# match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005
Ruijie(config-address-manage)# match ip 10.1.6.0 255.255.255.0 vlan 1006
```

【检验方法】 1：**show run** 查看

```
address-manage
 match ip default 172.50.128.0 255.255.128.0
 match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005
```

```
match ip 10.1.6.0 255.255.255.0 vlan 1006
```

4.4.4 配置DHCP服务器全局属性

配置效果

开启服务器一些特定的功能，如 ping 机制、强制 nak 等。

注意事项

Nak 命令的配置可能引起网络中其它服务器的功能异常。

配置方法

配置排除地址

- 配置某些地址或地址段不可用，为可选配置。
- 在配置模式下执行 **ip dhcp excluded-address** 命令

配置 DHCP 服务器强制回复 NAK

- 针对某些用户的错误地址请求，服务器回复 nak 报文，可选配置。
- 在配置模式下执行 **ip dhcp force-send-nak** 命令。

配置监控 VRRP 状态

- 启动该功能后，主机 server 处理 DHCP 相关报文，备机 server 则不处理 DHCP 相关报文，可选配置。
- 在配置模式下执行 **ip dhcp monitor-vrrp-state** 命令。

配置 Ping 包次数

- 检查地址的可达性，执行 **ping** 操作，默认值为 2，可选配置。
- 在配置模式下执行 **ip dhcp ping packet** 命令。

配置 Ping 包超时时间

- 检查地址的可达性，设置 **ping** 返回时长，默认值为 500ms， 可选配置。
- 在配置模式下执行 **ip dhcp ping timeout** 命令。

配置 DHCP 服务器重新下发可信 ARP

- 用于配置 DHCP 服务器重新下发可信 ARP。只根据从配置有 **update arp** 的地址池上分配出去的地址重新下发可信 ARP。
- 在配置模式下执行 **ip dhcp refresh arp** 命令。

配置 DHCP 服务器检测用户下线

- 用于配置 DHCP 服务器是否检测用户下线。如果用户下线后一段时间内没有重新上线，则回收分配给该用户的地址。
- 在配置模式下执行 **ip dhcp server arp-detect** 命令。

配置伪服务器检测

- 启动该功能后，网络中存在伪服务器，会记录在日志中，可选配置。
- 在配置模式下执行 **ip dhcp server detect** 命令。

检验方法

启动 **dhcp-server** 下发地址过程中可检验。

相关命令

配置排除地址

【命令格式】 **ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]

【参数说明】 *low-ip-address:* 排斥 IP 地址范围的起始 IP 地址

high-ip-address : 排斥地址范围的结束 IP 地址

【命令模式】 全局模式

【使用指导】 如果没有特别配置，DHCP 服务器会试图将在地址池中定义的所有子网地址分配给 DHCP 客户端。因此，如果想保留一些地址不分配，比如已经分配给服务器或者设备了，必须明确定义这些地址是不允许分配给客户端的；配置 DHCP 服务器，一个好的习惯是将所有已明确分配的地址全部不允许 DHCP 分配，这样可以带来两个好处：1）不会发生地址冲突；2）DHCP 分配地址时，减少了检测时间，从而提高 DHCP 分配效率

配置 DHCP 服务器强制回复 NAK

【命令格式】 **ip dhcp force-send-nak**

【参数说明】 **-**

【命令模式】 全局配置模式

【使用指导】 在无线应用中，DHCP 客户端的移动性较大，DHCP 客户端会经常性的从一个网络移动到另一个网络中。当 DHCP 服务器在收到客户端的 Request 续租报文时，发现客户端的网段发生更改或者是租约超时时会给予回复 NAK，要求客户端重新获取 IP 地址，避免客户端不断发送 Request 报文直至超时后重新获取 IP 地址，延长 IP 地址获取时间。

但是，DHCP 服务器发送 NAK 报文的前提是该 DHCP 客户端在自己的管理范围之内，也就是可以查找到对应的租约记录信息。当 DHCP 客户端从另一个网络环境中移入时，DHCP 服务器将无法在本地查找到对应的租约记录信息，不予回复 NAK，此时 DHCP 客户端需要不断发送 Request 报文直至超时后重新获取 IP 地址，导致 IP 地址获取时间变长。在 DHCP 服务器重启时丢失客户端租约，而客户端要求续租时也会遇到类似情况。在这种情况下，可以通过配置命令强制让 DHCP 服务器在查找不到租约记录时也给予回复 NAK 报文，触发客户端快速获取到 IP 地址，注意：默认情况下该条命令关闭；在开启该命令的时候，在同一广播域内，不允许开启多台 DHCP 服务器

配置 Ping 包次数

【命令格式】 **ip dhcp ping packets** [*number*]

【参数说明】 *Number*：（可选）范围从 0 到 10，0 表示关闭 ping 操作。缺省 ping 两个包

【命令模式】 全局配置模式

【使用指导】 缺省情况，当 DHCP 服务器试图从地址池中分配一个 IP 地址时，会对该地址执行两次 Ping 命令(一次一个数据包)。如果 Ping 没有应答，DHCP 服务器认为该地址为空闲地址，就将该地址分配给 DHCP 客户端；如果 Ping 有应答，DHCP 服务器认为该地址已经在使用，就试图分配另外一个地址给 DHCP 客户端，直到分配成功

配置 Ping 包超时时间

【命令格式】 **ip dhcp ping timeout** *milliseconds*

【参数说明】 *milli-seconds*：DHCP 服务器等待 ping 应答的时间（以毫秒计）。取值范围为 100 到 10000

【命令模式】 全局配置模式

【使用指导】 缺省情况下，DHCP 服务器 Ping 操作如果 500 毫秒没有应答，就认为没有该 IP 地址主机存在。可以通过调整 Ping 包超时时间，改变服务器 Ping 等待应答的时间

配置重新下发可信 ARP

【命令格式】 **ip dhcp refresh arp**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 缺省情况下，如果 DHCP 地址池上配置 **update arp**，DHCP 服务器在分配地址时会下发可信 ARP。如果用户清除掉可信 ARP 后，DHCP 服务器不会主动重新下发可信 ARP。配置该命令后，DHCP 服务器可以根据配置有 **update arp** 的地址池上分配出去的地址重新下发可信 ARP。

配置基于 ARP 检测用户下线

【命令格式】 **ip dhcp server arp-detect**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 缺省情况下，DHCP 服务器不会基于 ARP 检测用户下线。配置该命令后，DHCP 服务器可以检测用户的下线。如果用户在一段时间内（默认 5 分钟）未重新上线，DHCP 服务器就回收分配给该用户的地址。

配置伪服务器检测

【命令格式】 **ip dhcp server detect**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 缺省情况下，DHCP 服务器是关闭伪服务器检测功能。配置该命令后，DHCP 服务器可以检测网络中存在的伪服务器。

配置举例

配置 ping 机制

【配置方法】

- 配置 ping 次数为 5

- 配置 ping 超时时长为 800ms

```
Ruijie(config)# ip dhcp ping packet 5
Ruijie(config)# ip dhcp ping timeout 800
```

【检验方法】 1.**show run** 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp ping packet 5
ip dhcp ping timeout 800
```

↘ 配置排除地址

【配置方法】

- 排除 192.168.0.0 – 192.168.255.255 的所有地址

```
Ruijie(config)# ip dhcp excluded-address 192.168.0.0 192.168.255.255
```

【检验方法】 1.**show run** 查看

```
Ruijie(config)#show run | begin ip dhcp
ip dhcp excluded-address 192.168.0.0 192.168.255.255
```

4.4.5 配置DHCP Relay基本功能

配置效果

- 建立 Client—Relay—Server 模式的 DHCP 动态 IP 管理，解决 DHCP 客户端与 DHCP 服务器不在同一网段时 DHCP 客户端与在其他网段的 DHCP 服务器通讯问题。

注意事项

- DHCP Relay 需要借助网络中现有的单播路由。因此，网络中必须配置 IPv4 单播路由。

配置方法

↘ 启动 DHCP Relay 功能

- 必须配置。
- 若无特殊要求，应在设备上启动 DHCP Relay 功能。

↘ 配置 DHCP 服务器的 IP 地址

- 必须配置。
- 应在设备上启动 DHCP 服务器的 IP 地址。

检验方法

- 检查用户主机能否通过 DHCP Relay 成功获取到 IP 地址。

相关命令

启动 DHCP Relay 功能

【命令格式】 **service dhcp**

【参数说明】 **-**

【命令模式】 全局模式

【使用指导】 -

配置 DHCP 服务器的 IP 地址

【命令格式】 **ip helper-address { cycle-mode |** *A.B.C.D* **}**

【参数说明】 *cycle-mode* ：开启 dhcp 请求报文转发所有 dhcp 服务器

A.B.C.D: Server 的 ip 地址

【命令模式】 全局模式

【使用指导】 -

配置举例

以下配置举例，仅介绍与 DHCP Relay 相关的配置。

有线场景中 DHCP Relay 配置

【网络环境】

图 4-5

【配置方法】

- 用户设备启动通过 DHCP 获取地址的功能。
- 在作为 DHCP Relay Agent 的网络设备中启动 DHCP Relay 功能。
- 配置 DHCP Server。

A 用户设备启动 DHCP 获取地址的功能。

B # 启用 DHCP 中继代理

```
Ruijie(config)# service dhcp
```

添加一个全局的 DHCP 服务器的地址

```
Ruijie(config)# ip helper-address 172.2.2.1
```

配置与用户设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if)# ip address 192.1.1.1 255.255.255.0
```

配置与 Server 设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 0/2
Ruijie(config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0
```

C

启用 DHCP SERVER 功能

```
Ruijie(config)# service dhcp
```

添加一个客户端地址池

```
Ruijie(config)# ip dhcp pool relay
Ruijie (dhcp-config)#network 192.1.1.0 255.255.255.0
Ruijie (dhcp-config)#default-router 192.1.1.1
```

配置与 relay 设备连接的端口的 IP 地址

```
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/2)# ip address 172.2.2.1 255.255.255.0
```

【检验方法】 查看用户是否能获取到 IP 地址。

- 检查用户设备是否能获取到 IP 地址。
- 检查 DHCP Relay 配置是否正确。

A 用户设备能获取到 IP 地址

B 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置

```
Ruijie# show running-config
service dhcp
ip helper-address 172.2.2.1
!
interface GigabitEthernet 0/1
ip address 192.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
ip address 172.2.2.2 255.255.255.0
!
```

常见错误

- IPv4 单播路由配置错误。
- 没有启动 DHCP Relay 功能。
- 没有配置 DHCP Relay 与 DHCP Service 之间的路由。
- 没有配置 DHCP 服务器 IP 地址。

4.4.6 配置DHCP Relay option 82 功能

配置效果

- 中继设备进行 DHCP Relay 时，可以通过添加 option 的方式来详细的标明 DHCP 客户端的一些网络信息，从而使服务器可以根据更精确的信息给用户分配不同权限的 IP。

注意事项

- 必须配置 DHCP Relay 基本功能。

配置方法

启动 DHCP Relay 基本功能

- 必须配置。
- 若无特殊要求，应在设备上启动 DHCP Relay 基本功能。

启动 DHCP option82 功能

- 缺省情况下，设备上的 DHCP option 82 功能关闭。
- 使用 **ip dhcp relay information option82** 命令可以启动或关闭设备上的 DHCP option 82 功能。

检验方法

- 检查客户端获取到的 IP 地址，是否是根据 option 82 规则分配。。

相关命令

配置 DHCP option82 功能

【命令格式】 **ip dhcp relay information option82**
【参数说明】 **-**
【命令模式】 全局模式
【使用指导】 -

配置举例

启动 DHCP option 82 功能。

【配置方法】
- 启动 DHCP option 82 功能

```
Ruijie(config)# ip dhcp relay information option82
```

【检验方法】 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置。

```
Ruijie#show ru | incl ip dhcp relay
ip dhcp relay information option82
```

常见配置错误

- DHCP Relay 基本功能没有配置，或配置失败。

4.4.7 配置DHCP Relay check server-id功能

配置效果

- 当配置命令 **ip dhcp relay check server-id** 后，DHCP Relay 仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。如果没有配置该命令，则向所有配置的 DHCP 服务器转发 DHCP 请求报文。

注意事项

- 必须配置 DHCP Relay 基本功能。

配置方法

↘ 启动 DHCP Relay check server-id 功能

- 缺省情况下，设备上的 DHCP Relay check server-id 功能关闭。
- 使用 **ip dhcp relay check server-id** 命令可以启动设备上的 DHCP Relay check server-id 功能。

检验方法

DHCP Relay 是否仅将 DHCP 请求报文转发到 option server-id 中指定的服务器。

相关命令

↘ 配置 DHCP Relay check server-id 功能

【命令格式】 **ip dhcp relay check server-id**
【参数说明】 **-**
【命令模式】 全局模式
【使用指导】 -

配置举例

↘ 配置 DHCP Relay check server-id 功能。

【配置方法】
- 配置 DHCP Relay 基本功能。略
- 在对应接口上配置 DHCP Relay check server-id 功能。

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp relay check server-id
```

【检验方法】 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置。

```
Ruijie# show running-config | include check server-id
ip dhcp relay check server-id
Ruijie#
```

常见配置错误

- DHCP Relay 基本功能没有配置，或配置失败。

4.4.8 配置DHCP Relay suppression功能

配置效果

- 在指定接口上配置命令 **ip dhcp relay suppression** 后，将屏蔽该接口上收到的 DHCP 请求报文；而对于其他接口上收到的 DHCP 请求报文，则正常转发。

注意事项

- 必须配置 DHCP Relay 基本功能。

配置方法

↘ 启动 DHCP Relay suppression 功能

缺省情况下，设备上所有接口的 DHCP Relay suppression 功能关闭。

使用 **ip dhcp relay suppression** 命令可以启动设备上的 DHCP Relay suppression 功能。

检验方法

- 接口上收到的 DHCP 请求报文是否被过滤。

相关命令

↘ 配置 DHCP Relay suppression 功能

【命令格式】 **ip dhcp relay suppression**
【参数说明】 **-**
【命令模式】 接口模式
【使用指导】 -

配置举例

配置 DHCP Relay suppression 功能。

【配置方法】
- 配置 DHCP Relay 基本功能。略
- 在对应接口上配置 DHCP Relay suppression 功能。

```
Ruijie# configure terminal
Ruijie(config)# interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip dhcp relay suppression
Ruijie(config-if-GigabitEthernet 0/1)#end
Ruijie#
```

【检验方法】 登录到 DHCP Relay Agent 设备后在特权模式下用 **show running-config** 命令显示 DHCP Relay 配置。

```
Ruijie# show running-config | include relay suppression
ip dhcp relay suppression
Ruijie#
```

常见配置错误

DHCP Relay 基本功能没有配置，或配置失败。

4.4.9 配置DHCP客户端

配置效果

设备启动 dhcp-client，可动态取得地址及其它需求配置。

注意事项

锐捷产品目前版本支持以太网接口以及 FR、PPP、HDLC 接口上的 DHCP 客户端。

配置方法

在接口上执行 **ip address dhcp** 命令

检验方法

查看接口是否取到 ip 地址

相关命令

配置 DHCP 客户端

【命令格式】 **ip address dhcp**

【参数说明】 -

【命令模式】 接口配置模式

【使用指导】
- 锐捷产品支持以太网端口通过 DHCP 获得动态分配的 IP 地址
- 锐捷产品支持 ppp 封装的端口通过 DHCP 获得动态分配的 IP 地址
- 锐捷产品支持 FR 封装的端口通过 DHCP 获得动态分配的 IP 地址
- 锐捷产品支持 HDLC 封装的端口通过 DHCP 获得动态分配的 IP 地址

配置举例

DHCP 客户端配置

【配置方法】 1：为设备接口 FastEthernet 0/0 配置 DHCP 自动分配地址

```
Ruijie(config)# interface FastEthernet0/0
Ruijie(config-if-FastEthernet 0/0)#ip address dhcp
```

【检验方法】 1：**show run** 查看

```
Ruijie(config)#show run | begin ip address dhcp
ip address dhcp
```

4.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除 DHCP 地址绑定	**clear ip dhcp binding** { *address* | *}
清除 DHCP 地址冲突	**clear ip dhcp conflict** { *address* | *}
清除 DHCP 服务器统计状态	**clear ip dhcp server statistics**
清除 DHCP 中继统计状态	**clear ip dhcp relay statistics**
清除 DHCP 服务器性能统计信息	**clear ip dhcp server rate**
清除 DHCP 伪服务器信息	**clear ip dhcp server detect**

查看运行情况

作用	命令
显示 DHCP 租约信息	**show dhcp lease**
显示手工配置的地址	**show dhcp manual**
显示 dhcp 用的套接字	**show ip dhcp socket**
显示已经分配的地址	**show ip dhcp binding**
显示创建的地址池	**show ip dhcp pool**
显示 dhcp-server 统计信息	**show ip dhcp server statistic**
显示 dhcp-relay 统计信息	**show ip dhcp relay-statistic**
显示冲突地址	**show ip dhcp conflict**
显示 DHCP 伪服务器信息	**show ip dhcp server detect**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
DHCPagent 调试开关	**debug ip dhcp server agent**
DHCP 热备调试开关	**debug ip dhcp server ha**
DHCP 地址池调试开关	**debug ip dhcp server pool**
DHCP VRRP 调试开关	**debug ip dhcp server vrrp**
DHCP 打开所有调试开关	**debug ip dhcp server all**
DHCP 报文调试开关	**debug ip dhcp client**
DHCP Relay 事件调试开关。	**debug ip dhcp relay**

5 DNS

5.1 概述

DNS（Domain Name System，域名系统），因特网上作为域名和IP地址相互映射的一个 分布式数据库，能够使用户更方便的访问 互联网，而不用去记住能够被机器直接读取的IP数串。通过主机名，最终得到该主机名对应的IP地址的过程叫做域名解析（或主机名解析）。

下文仅介绍 DNS 的相关内容。

协议规范

- RFC1034：DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035：DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

5.2 典型应用

典型应用	场景描述
静态域名解析	直接在本设备上根据预设的域名/IP 对应表进行域名解析
动态域名解析	从网络上的 DNS 服务器动态获取域名对应的地址

5.2.1 静态域名解析

应用场景

- 在设备上预设置域名和 IP 的对应表
- 设备上的一些应用（比如 Ping，Telnet 等）进行域名操作时，直接在设备上就能解析到预设的 IP，无需连到网络上的服务器。

功能部属

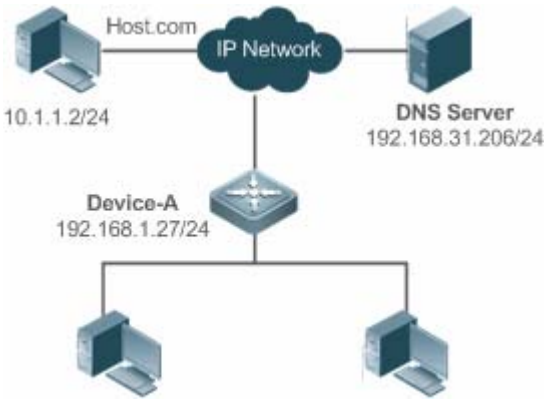
- 在设备上预设置域名和 IP 的对应关系

5.2.2 动态域名解析

应用场景

- “DNS Server”部署在网络上，对外提供域名服务
- “host.com”部署在网络上，使用域名(host.com)对外提供服务
- “Device-A"设备指定“DNS Server”作为 DNS 服务器，从“DNS Server”上获取到“host.com"的地址

图 5-1 动态域名解析配置组网图



功能部属

- 将 DNS Server 部署为"Device-A"的 DNS 服务器

5.3 功能详解

基本概念

↘ DNS

DNS 由解析器和域名服务器组成。域名服务器是指保存有网络中所有主机的域名和 IP 地址的对应关系，并提供将域名和 IP 互转的服务器。DNS 的 TCP 和 UDP 端口号都是 53，通常使用 UDP。

功能特性

功能特性	作用
域名解析	根据域名从域名服务器或本地数据库获取对应的 IP 地址

5.3.1 域名解析

工作原理

↘ 静态域名解析

静态域名解析，就是用户在设备上预先设置好域名和IP的对应关系，当用户使用某些应用(比如Ping、Telnet等等)进行域名操作时，系统从本设备上解析出域名对应的 IP，而不需要到网络上的 DNS 服务器获取域名对应的 IP。

动态域名解析

动态域名解析，就是当用户使用某些应用进行域名操作时，系统DNS解析器查询外部的DNS服务器，获取到域名对应的IP。

动态域名解析过程：

2. 用户应用(Ping、Telnet 等)向系统 DNS 解析器请求域名对应的 IP
3. 系统 DNS 解析器先查找动态缓存，如果动态缓存的域名未过期则返回给应用程序
4. 如果不存在未过期的域名，DNS 解析器向外部的 DNS 服务器发起域名转 IP 的请求
5. DNS 解析器接收到 DNS 服务器的应答，缓存并转发给应用程序

相关配置

开启域名解析功能

- 缺省情况下，设备是开启域名解析功能。
- 通过 **ip domain-lookup** 命令开启或关闭域名解析功能。

配置静态域名对应的 IP

- 缺省情况下，没有域名/IP 的静态配置。
- 通过 **ip host** 命令指定域名对应的 IPv4 地址
- 通过 **ipv6 host** 命令配置域名对应的 IPv6 地址

配置域名服务器

- 缺省情况下，未配置域名服务器。
- 通过 **ip name-server** 命令配置域名服务器。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置静态域名解析	可选配置	
	ip domain-lookup	开启域名解析功能
	ip host	配置域名对应的 IPv4 地址
	ipv6 host	配置域名对应的 IPv6 地址
配置动态域名解析	可选配置	

	ip domain-lookup	开启域名解析功能
	ip name-server	配置域名服务器

5.4.1 配置静态域名解析

配置效果

系统解析器从设备本地解析域名对应的 IP

配置方法

↘ 开启域名解析功能

- 缺省已开启域名解析功能
- 如果关闭该功能，静态域名解析不生效。

↘ 配置静态域名对应的 IPv4 或 IPv6 地址

- 必须配置，用户使用到的域名必须配置对应的 IP。

检验方法

- 通过 **show run** 查看配置信息。
- 通过 **show hosts** 当前的域名和 IP 对应关系

相关命令

↘ 配置域名对应的 IPv4 地址

【命令格式】 **ip host** *host-name ip-address*
【参数说明】 *host-name*：域名
ip-address：对应的 IPv4 地址
【命令模式】 全局模式
【使用指导】 -

↘ 配置域名对应的 IPv6 地址

【命令格式】 **ipv6 host** *host-name ipv6-address*
【参数说明】 *host-name*：域名
ipv6-address：对应的 IPv6 地址
【命令模式】 全局模式
【使用指导】 -

配置举例

配置静态域名解析

【配置方法】
- 在设备上静态配置域名 www.test.com 的 IP 地址为 192.168.1.1
- 在设备上静态配置域名 www.testv6.com 的 IP 地址为 2001::1

```
Ruijie#configure terminal
Ruijie(config)# ip host www.test.com 192.168.1.1
Ruijie(config)# ipv6 host www.testv6.com 2001::1
Ruijie(config)# exit
```

【检验方法】 通过 **show hosts** 查看是否有所配置的静态域名表项

```
Ruijie#show hosts
Name servers are:

Host                      type     Address           TTL(sec)
www.test.com              static   192.168.1.1         ---
www.testv6.com            static   2001::1             ---
```

5.4.2 配置动态域名解析

配置效果

系统解析器从 DNS 服务器解析域名对应的 IP

配置方法

开启域名解析功能

- 缺省已开启域名解析功能
- 如果关闭该功能，动态域名解析不生效。

配置 DNS 服务器

- 必须配置，使用动态域名解析必须配置外部的 DNS 服务器。

检验方法

- 通过 **show run** 查看配置信息

相关命令

配置域名服务器

【命令格式】 **ip name-server** { *ip-address* | *ipv6-address* }

【参数说明】 *ip-address*：DNS 服务器的 IPv4 地址

ipv6-address：DNS 服务器的 IPv6 地址

【命令模式】 全局模式

【使用指导】 -

配置举例

↘ 配置动态域名解析

【网络环境】

图 5-2

DEVICE：从网络上的 DNS 服务器(192.168.10.1)解析域名

【配置方法】 在设备上配置 DNS 服务器地址为 192.168.10.1

```
DEVICE#configure terminal
DEVICE(config)# ip name-server 192.168.10.1
DEVICE(config)# exit
```

【检验方法】 通过 **show hosts** 查看是否配置指定 DNS 服务器

```
Ruijie(config)#show hosts
Name servers are:
192.168.10.1 static

Host          type     Address                                  TTL(sec)
```

5.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除动态主机名缓存表。	**clear host** [*host-name*]

查看运行情况

作用	命令
查看 DNS 的相关参数	**show hosts** [*host-name*]

查看调试信息

输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开调试功能	**debug ip dns**

6 网络通信检测工具

6.1 概述

网络通信检测工具可以用于检查网络是否能够连通，用好网络通信监测工具可以很好地帮助我们分析判定网络故障。网络通信检测工具包括 PING（Packet Internet Groper，因特网包探索器）和 Traceroute（路由侦测）。PING 工具主要用于检测网络通与不通，以及网路的时延，时延值越大，则表示网络速度越慢。Traceroute 工具则可以帮助用户了解网络的物理与逻辑连接的拓扑情况以及数据传输的效率。在网络设备上，这两个工具所对应的命令为 ping 和 traceroute。

协议规范

- RFC792：Internet Control Message Protocol
- RFC4443：Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification

6.2 典型应用

典型应用	场景描述
端对端连通性检查	网络设备与目标主机都连接在 IP 网络上，都配置有 IP 地址。
主机路由检查	网络设备与目标主机都连接在 IP 网络上，都配置有 IP 地址。

6.2.1 端对端连通性检查

应用场景

图 6-1 网络设备 A 与目标主机 B 都连接在 IP 网络上。

网络设备与目标主机都连接在 IP 网络上，端对端连通性检查就是判定 IP 报文能否在二者之间传输。目标主机可以是网络设备本身，这种情况一般用于检查设备自身网络接口和 TCP/IP 协议配置的正确性。

功能部属

通过在网络设备上运行 Ping 功能。

6.2.2 主机路由检查

应用场景

图 6-2 网络设备 A 与目标主机 B 都连接在 IP 网络上。

网络设备与目标主机都连接在 IP 网络上，主机路由检查就是判定 IP 报文在二者之间传输，究竟需要经过多少网关(路由器)。目标主机通常不是网络设备本身，并且通常与网络设备不在同一个 IP 网段。

功能部属

通过在网络设备上运行 Traceroute 功能。

6.3 功能详解

功能特性

功能特性	作用
Ping连通性测试	检测指定 IPv4/v6 地址是否可达，并输出相关信息。
Traceroute连通性测试	显示 IPv4/v6 数据包从源地址到目的地址所经过的网关。

6.3.1 Ping 连通性测试

工作原理

PING 工具向目标 IP 地址发送一个 ICMP 请求（ICMP Request）数据包，要求对方返回一个 ICMP 回声（ICMP Echo）数据包，来确定两台网络机器是否连接相通，时延是多少。

相关配置

- 通过 **ping** 命令进行配置

6.3.2 Traceroute 连通性测试

工作原理

Traceroute 工具利用 ICMP 及 IP 报文头部的 TTL（Time To Live）字段。首先，网络设备的 Traceroute 工具送出一个 TTL 是 1 的 ICMP Request 到目的主机，当路径上的第一个路由器收到这个报文时，它将 TTL 减 1。此时 TTL 变为 0 了，所以该路由器会将此报文丢弃，并送回一个 ICMP 超时（ICMP time exceeded）消息，Traceroute 工具收到这个消息后，便知道这个路由器存在于这个路径上，接着再送出另一个 TTL 是 2 的报文，发现第 2 个路由器。Traceroute 工具每次将送出的报文的 TTL 加 1 来发现另一个路由器，这个重复的动作一直持续到某个数据报文到达目的主机。当报文到达目的主机后，该主机不会送回 ICMP time exceeded 消息，而是送回 ICMP Echo，Traceroute 工具结束探测并显示从网络设备到目的主机的路径信息。

相关配置

- 通过 **traceroute** 命令进行配置

6.4 配置详解

配置项	配置建议 & 相关命令	
Ping连通性测试	⚠ 可选配置，用于检测 IPv4/v6 地址是否可达。	
	ping	运行 Ping 功能。
Traceroute连通性测试	⚠ 可选配置，显示 IPv4/v6 数据包从源地址到目的地址所经过的网关。	
	traceroute	运行 Traceroute 功能。

6.4.1 Ping 连通性测试

配置效果

在网络设备上采用 Ping 连通性测试，可以得知该网络设备和目的主机之间是否保持连通，报文是否可以在网络设备和目的主机之间传输。

注意事项

执行 PING 操作的网络设备本身需要配置 IP 地址。

配置方法

- 如果需要检测 IPv4 地址是否可达，可通过 Ping IPv4 命令。

- 如果需要检测 IPv6 地址是否可达，可通过 Ping IPv6 命令。

检验方法

输入 **ping** 命令，即可在 CLI 界面显示相关信息。

相关命令

Ping IPv4

【命令格式】 **ping** [**ip**] [*address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**df-bit**] [**validate**] [**detail**]]

【参数说明】 *address*：指定目的 IPv4 地址或域名。

length：指定发送数据包数据填充段的长度，范围：36~18024，默认填充长度为 100。

times：指定发送数据包的个数，范围：1~ 4294967295。

seconds：指定超时的时间，范围：1~10（秒）。

data：指定报文填充数据，格式为 1-255 长度的字符串，默认填充为 abcd。

source：指定报文源 IPv4 地址或源接口。其中，环回接口地址（例如 127.0.0.1）不允许作为源地址。

df-bit：设置 IP 的 DF 标识位，当 DF 位被设置为 1 时，表示不对数据包进行分段处理，默认 DF 位为 0。

validate：设置是否校验响应报文。

detail:设置回显是否显示详细信息，默认只显示‘!’和‘.’。

【命令模式】 在普通用户模式下，只能运行基本的 **ping** 功能；在特权用户模式下，还可以运行 **ping** 的扩展功能。

在其他模式下，可以通过 do 命令执行 **ping** 的扩展功能，具体配置请参考 do 命令说明。

【使用指导】 运行 **ping** 功能，如果有应答，则显示出应答的相关信息，最后输出一个统计信息。在扩展 **ping** 中，可以指定发送数据包的个数、长度、超时的时间等等，和基本的 **ping** 功能一样，最后也输出一个统计信息。

要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

Ping IPv6

【命令格式】 **ping** [**ipv6**] [*address* [**length** *length*] [**ntimes** *times*] [**timeout** *seconds*] [**data** *data*] [**source** *source*] [**detail**]]

【参数说明】 *address*：指定目的 IPv6 地址或域名。

length：指定发送数据包的长度，范围：16~18024，默认填充长度为 100。

times：指定发送数据包的个数，范围：1~ 4294967295。

seconds：指定超时的时间，范围：1~10（秒）。

data：指定报文填充数据，格式为 1-255 长度的字符串。

source：指定报文源 IPv6 地址或源接口。其中，环回接口地址（例如::1）不允许作为源地址。

detail:设置回显是否显示详细信息，默认只显示‘!’和‘.’。

【命令模式】 在普通用户模式下，只能运行基本的 **ping ipv6** 功能；在特权用户模式下，还可以运行 **ping ipv6** 的扩展功能。

在其他模式下，可以通过 do 命令执行 **ping** 的扩展功能，具体配置请参考 do 命令说明。

【使用指导】 运行 **ping ipv6** 功能，如果有应答，则显示出应答的相关信息，最后输出一个统计信息。

在扩展 **ping ipv6** 中，可以指定发送数据包的个数、长度、超时的时间等等，和基本的 **ping ipv6** 功能一样，

最后也输出一个统计信息。

要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

配置举例

运行普通 Ping 功能

【配置方法】 在特权模式下输入 Ping IPv4 地址 192.168.21.26

```
常规 ping
Ruijie# ping 192.168.21.26
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
显示 detail 的 ping
Ruijie#ping 192.168.21.26 detail
Sending 5, 100-byte ICMP Echoes to 192.168.21.26, timeout is 2 seconds:
  < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=100 time=4ms TTL=64
Reply from 192.168.21.26: bytes=100 time=3ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64
Reply from 192.168.21.26: bytes=100 time=1ms TTL=64

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms.
```

【检验方法】 缺省将 5 个数据段长度为 100Byte 的数据包发送到指定的 IP 地址，在指定的时间（缺省为 2 秒）内，显示相应的探测信息，最后输出一个统计信息。

运行扩展 Ping 功能

【配置方法】 在特权模式下输入 Ping IPv4 地址 192.168.21.26，并指定发送数据包的长度、个数、超时的时间等。

```
常规 ping
Ruijie# ping 192.168.21.26 length 1500 ntimes 100 data ffff source 192.168.21.99 timeout 3
Sending 100, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
显示 detail 的 ping
ping 192.168.21.26 length 1500 ntimes 20 data ffff source 192.168.21.99 timeout 3 detail
Sending 20, 1500-byte ICMP Echoes to 192.168.21.26, timeout is 3 seconds:
  < press Ctrl+C to break >
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
```

```
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=2ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=3ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64
Reply from 192.168.21.26: bytes=1500 time=1ms TTL=64

Success rate is 100 percent (20/20), round-trip min/avg/max = 1/1/3 ms.
```

【检验方法】 将 20 个长度为 1500Byte 的数据包发送到指定的 IP 地址，在指定的时间（3 秒）内，如果有应答，显示相应的探测信息，最后输出一个统计信息。

↘ 运行普通 Ping IPv6 功能

【配置方法】 在特权模式下输入 Ping IPv6 地址 2001::1

常规 ping

```
Ruijie# ping ipv6 2001::1
Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

显示 detail 的 ping

```
Ruijie#ping 2001::1 detail
Sending 5, 100-byte ICMP Echoes to 2001::1, timeout is 2 seconds:
  < press Ctrl+C to break >
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms
```

```
Reply from 2001::1: bytes=100 time=1ms
Reply from 2001::1: bytes=100 time=1ms

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

【检验方法】 缺省将 5 个数据段长度为 100Byte 的数据包发送到指定的 IP 地址，在指定的时间（缺省为 2 秒）内，显示相应的探测信息，最后输出一个统计信息。

↘ 运行扩展 Ping IPv6 功能

【配置方法】 在特权模式下输入 Ping IPv6 地址 2001::5，并指定发送数据包的长度、个数、超时的时间等。

常规 ping

```
Ruijie# ping ipv6 2001::5  length 1500 ntimes 100 data ffff source 2001::9 timeout 3
Sending 100, 1500-byte ICMP Echoes to 2000::1, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

显示 detail 的 ping

```
Ruijie#ping 2001::5 length 1500 ntimes 10 data ffff source 2001::9 timeout 3
Sending 10, 1500-byte ICMP Echoes to 2001::5, timeout is 3 seconds:
  < press Ctrl+C to break >
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms
Reply from 2001::5: bytes=1500 time=1ms

Success rate is 100 percent (10/10), round-trip min/avg/max = 1/1/1 ms.
```

【检验方法】 将 100 个长度为 1500Byte 的数据包发送到指定的 IPv6 地址，指定的时间(3 秒)内，显示相应的探测信息，最后输出一个统计信息。

6.4.2 Traceroute 连通性测试

配置效果

在网络设备上采用 Traceroute 连通性测试，可以得知该网络设备和目的主机之间的路由拓扑信息，报文从网络设备到目的主机经过了多少个网关。

注意事项

执行 Traceroute 操作的网络设备本身需要配置 IP 地址。

配置方法

- 如果需要跟踪 IPv4 数据包到达目的主机经过哪些网关，可通过配置 Traceroute IPv4 命令。
- 如果需要跟踪 IPv6 数据包到达目的主机经过哪些网关，可通过配置 Traceroute IPv6 命令。

检验方法

输入 **traceroute** 命令，即可在 CLI 界面显示相关信息。

相关命令

Traceroute IPv4

【命令格式】 **traceroute** [**ip**] [*adress* [**probe** *number*] [**source** *source*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]

【参数说明】 *address*：指定目的 IPv4 地址或域名。

number：指定发送的探测的数量，范围：1~255。

source：指定报文源 IPv4 地址或源接口。其中，环回接口地址（例如 127.0.0.1）不允许作为源地址

seconds：指定超时的时间，范围：1~10（秒）。

minimum maximum：指定最小和最大 TTL 值，范围：1~255。

【命令模式】 在普通用户模式下，只能运行基本的 **traceroute** 功能；在特权用户模式下，还可以运行 **traceroute** 的扩展功能。

【使用指导】 **Traceroute** 命令主要用于检查网络的连通性，并在网络故障发生时，准确的定位故障发生的位置。要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

Traceroute IPv6

【命令格式】 **traceroute** [**ipv6**] [*address* [**probe** *number*] [**timeout** *seconds*] [**ttl** *minimum maximum*]]

【参数说明】 *address*：指定目的 IPv6 地址或域名。

number：指定发送的探测的数量，范围：1~255。

seconds：指定超时时间，范围：1~10（秒）。

minimum maximum：指定最小和最大 TTL 值，范围：1~255。

【配置模式】 在普通用户模式下，只能运行基本的 **traceroute ipv6** 功能；在特权用户模式下，还可以运行 **traceroute ipv6** 的扩展功能。

【使用指导】 **Traceroute ipv6** 命令主要用于检查网络的连通性，并在网络故障发生时，准确的定位故障发生的位置。要使用域名功能，则要先配置域名服务器，具体配置请参考 DNS 配置部分。

配置举例

网络畅通的 Traceroute 举例

【配置方法】 在特权模式下，输入 Traceroute IPv4 地址 61.154.22.36。

```
Ruijie# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36
1       192.168.12.1         0 msec  0 msec  0 msec
2       192.168.9.2          4 msec  4 msec 4 msec
3       192.168.9.1          8 msec  8 msec  4 msec
4       192.168.0.10         4 msec  28 msec  12 msec
5       202.101.143.130     4 msec  16 msec  8 msec
6       202.101.143.154    12 msec  8 msec  24 msec
7       61.154.22.36         12 msec  8 msec  22 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 61.154.22.36 的主机，网络数据包都经过了哪些网关（1 - 6），同时给出了到达该网关所花费的时间。

网络中某些网关不通的 Traceroute 举例

【配置方法】 在特权模式下，输入 Traceroute IPv4 地址 202.108.37.42。

```
Ruijie# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1       192.168.12.1         0 msec  0 msec  0 msec
2       192.168.9.2          0 msec  4 msec 4 msec
3       192.168.110.1       16 msec  12 msec  16 msec
4       *  *  *
5       61.154.8.129         12 msec  28 msec  12 msec
6       61.154.8.17           8 msec  12 msec  16 msec
7       61.154.8.250         12 msec  12 msec  12 msec
8       218.85.157.222       12 msec  12 msec  12 msec
9       218.85.157.130       16 msec  16 msec  16 msec
10      218.85.157.77        16 msec  48 msec  16 msec
11      202.97.40.65         76 msec  24 msec  24 msec
12      202.97.37.65         32 msec  24 msec  24 msec
13      202.97.38.162        52 msec  52 msec  224 msec
14      202.96.12.38         84 msec  52 msec  52 msec
15      202.106.192.226      88 msec  52 msec  52 msec
16      202.106.192.174      52 msec  52 msec  88 msec
17      210.74.176.158      100 msec  52 msec  84 msec
18      202.108.37.42         48 msec  48 msec  52 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 202.108.37.42 的主机，网络数据包都经过了哪些网关（1 - 17），并且网关 4 出现了故障。

网络畅通的 Traceroute ipv6 举例

【配置方法】 在特权模式下，输入 Traceroute IPv6 地址 3004::1。

```
Ruijie# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1       3000::1          0 msec  0 msec  0 msec
2       3001::1          4 msec  4 msec 4 msec
3       3002::1          8 msec  8 msec  4 msec
4       3004::1          4 msec  28 msec  12 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 *3004::1* 的主机，网络数据包都经过了哪些网关(1 - 4)，同时给出了到达该网关所花费的时间。

网络中某些网关不通的 Traceroute IPv6 举例

【配置方法】 在特权模式下，输入 Traceroute IPv6 地址 3004::1。

```
Ruijie# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1       3000::1          0 msec  0 msec  0 msec
2       3001::1          4 msec  4 msec 4 msec
3       3002::1          8 msec  8 msec  4 msec
4       * * *
5       3004::1          4 msec  28 msec  12 msec
```

从上面的结果可以清楚地看到，从源地址要访问 IP 地址为 *3004::1* 的主机，网络数据包都经过了哪些网关(1 - 5)，并且网关 4 出现了故障。

7 TCP

7.1 概述

TCP 协议为应用层提供了一个可靠的、有连接的基于 IP 的传输层协议。

应用层向 TCP 层发送用于网间传输的、用 8 位字节表示的数据流，然后 TCP 把数据流分割成适当长度的报文段，最大分段大小（MSS）通常受该计算机连接的网络的数据链路层的最大传送单元（MTU）限制。之后 TCP 把报文传给 IP 层，由它来通过网络将报文传送给接收端实体的 TCP 层。

TCP 为了保证不发生丢包，就给每个字节一个序号，同时序号也保证了传送到接收端实体的包的按序接收。然后接收端实体对已成功收到的字节发回一个相应的确认(ACK)；如果发送端实体在合理的往返时延(RTT)内未收到确认，那么对应的数据(假设丢失了) 将会被重传。

- 在数据正确性与合法性上，TCP 用一个校验和函数来检验数据是否有错误，在发送和接收时都要计算校验和；同时可以使用 MD5 认证对数据进行校验。
- 在保证可靠性上，采用超时重传和捎带确认机制。
- 在流量控制上，采用滑动窗口协议，协议中规定，对于窗口内未经确认的分组需要重传。

协议规范

- RFC 793：Transmission Control Protocol
- RFC 1122：Requirements for Internet Hosts -- Communication Layers
- RFC 1191：Path MTU Discovery
- RFC 1213：Management Information Base for Network Management of TCP/IP-based internets:MIB-II
- RFC 2385：Protection of BGP Sessions via the TCP MD5 Signature Option
- RFC 4022：Management Information Base for the Transmission Control Protocol (TCP)

7.2 典型应用

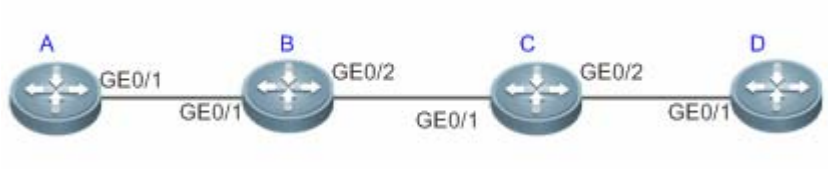
典型应用	场景描述
TCP性能优化	TCP 传输路径上某一段链路的 MTU 比较小，为了避免 TCP 报文分片，可以开启 TCP 的路径 MTU 发现功能。
TCP连接异常检测	TCP 探测对端是否还在正常工作。

7.2.1 TCP 性能优化

应用场景

以下图为例，A 和 D 建立 TCP 连接，A 和 B 之间链路的 MTU 是 1500 字节，B 和 C 之间链路的 MTU 是 1300 字节，C 和 D 之间链路的 MTU 是 1500 字节，为了使 TCP 传输性能达到最优，需要避免 TCP 报文在设备 B 和设备 C 上分片。

图 7-1



【注释】 A、B、C 和 D 为路由器。

功能部署

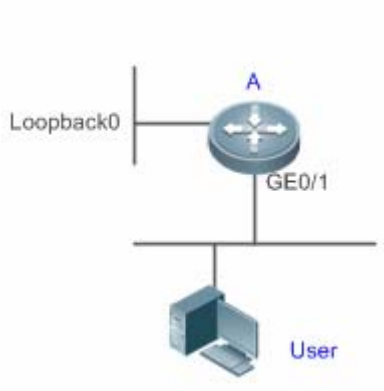
- 在 A 和 D 上开启 TCP 的路径 MTU 发现功能。

7.2.2 TCP 连接异常检测

应用场景

以下图为例，用户远程登陆到设备 A，用户异常关机，如果设备 A 等待 TCP 重传超时，会导致用户的 TCP 连接残留比较长的一段时间，可以利用 TCP 保活功能快速检测出用户的 TCP 连接异常。

图 7-2



【注释】 A 是路由器。

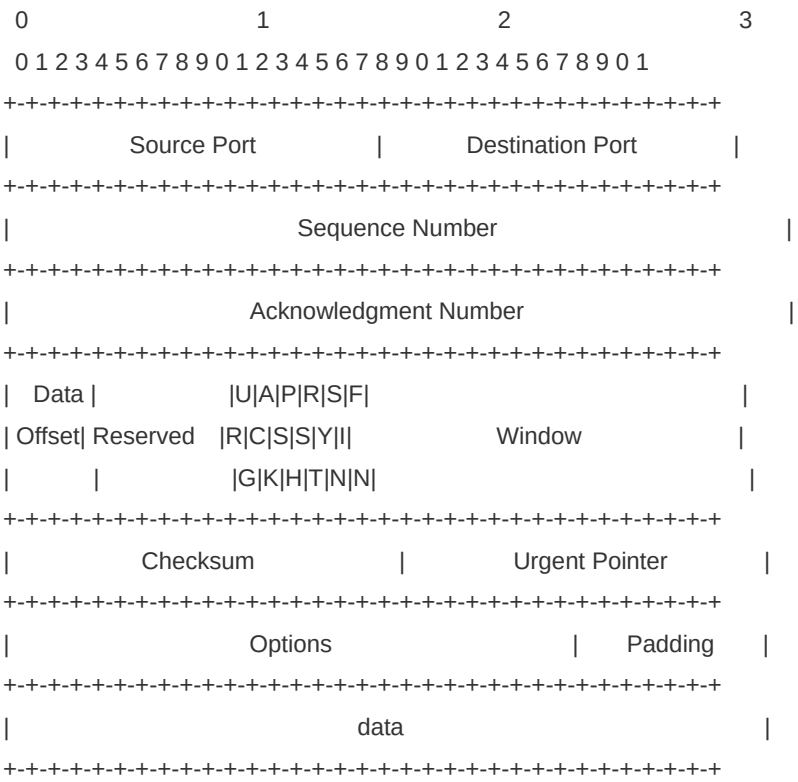
功能部署

- 在设备 A 上开启 TCP 保活功能。

7.3 功能详解

基本概念

TCP 首部格式



- Source Port 是源端口，16 位。
- Destination Port 是目的端口，16 位。
- Sequence Number 是序列号，32 位。
- Acknowledgment Number 是确认序列号，32 位。
- Data Offset 是数据偏移，4 位，该字段的值是 TCP 首部（包括选项）长度除以 4。
- 标志位： 6 位，URG 表示 Urgent Pointer 字段有意义，ACK 表示 Acknowledgment Number 字段有意义，PSH 表示 Push 功能，RST 表示复位 TCP 连接，SYN 表示 SYN 报文（在建立 TCP 连接的时候使用），FIN 表示发送方没有数据需要发送了（在关闭 TCP 连接的时候使用）。

- Window 表示接收缓冲区的空闲空间，16 位，用来告诉 TCP 连接对端自己能够接收的最大数据长度。
- Checksum 是校验和，16 位。
- Urgent Pointers 是紧急指针，16 位，只有 URG 标志位被设置时该字段才有意义，表示紧急数据相对序列号（Sequence Number 字段的值）的偏移。

↘ TCP 三次握手

- TCP 三次握手的过程如下：

(1) 客户端发送 SYN 报文给服务器端。

(2) 服务器端收到 SYN 报文，回应一个 SYN ACK 报文。

(3) 客户端收到服务器端的 SYN 报文，回应一个 ACK 报文。

- 三次握手完成，TCP 客户端和服务器端成功地建立连接，可以开始传输数据了。

功能特性

功能特性	作用
配置SYN超时	配置 TCP 发送 SYN 报文或者 SYN ACK 报文后等待应答报文的超时
配置窗口大小	配置窗口大小
配置端口不可达时是否发送reset报文	配置在收到端口不可达的 TCP 报文时是否发送 reset 报文
配置 MSS	配置 TCP 连接的 MSS
配置转发的SYN报文的MSS选项值	把转发的 SYN 报文中的 MSS 选项值修改为配置的 MSS
路径MTU发现功能	探测 TCP 传输路径上的最小 MTU，根据最小 MTU 调整发送的 TCP 报文的大小，避免分片
TCP保活功能	探测 TCP 连接对端是否还在正常工作

7.3.1 配置 SYN 超时

工作原理

建立 TCP 连接需要经过三次握手：发起方先发送 SYN 报文，响应方回应 SYN+ACK 报文，然后发起方再回应 ACK。

- 在发起方发送 SYN 报文后，如果响应方一直不回应 SYN+ACK 报文，发起方会不断的重传 SYN 报文直到超过一定的重传次数或超时时间。
- 在发起方发送 SYN 报文后，响应方回应 SYN+ACK 报文，但发起方不再回复 ACK，响应方也会一直重传直到超过一定的重传次数或超时时间。（SYN 报文攻击会出现这种情况。）

相关配置

设置 TCP SYN 超时时间

- TCP SYN 超时时间的缺省值是 20 秒。
- 用户可以在全局配置模式下使用“**ip tcp synwait-time** *seconds*”命令设置 SYN 超时时间，取值范围是 5 到 300，单位是秒。
- 如果网络中存在 SYN 攻击，减少 SYN 超时时间可以防止一些资源消耗，但对连续的 SYN 攻击达不到效果。在设备主动与外界请求建立连接时，减少 SYN 超时时间可以减少用户等待时间，如 telnet。如果网络比较差也可以适当增加超时时间。

11.0 版本废弃了 10.x 版本的配置命令“ip tcp syntime-out”被废弃，但兼容 10.x 版本，如果执行了 10.x 版本的配置命令，将自动转换成 11.0 版本的配置命令。

10.x 版本该命令只对 IPv4 TCP 生效，从 11.0 版本开始该命令对 IPv4 TCP 和 IPv6 TCP 都生效。

7.3.2 配置窗口大小

工作原理

TCP 的接收缓冲区用来缓存从对端接收到的数据，这些数据后续会被应用程序读取。一般情况下，TCP 的窗口值反映接收缓冲区的空闲空间的大小。对于带宽比较大、有大批量数据的连接，增大窗口可以显著提高 TCP 传输性能。

相关配置

设置窗口大小

- 用户可以在全局配置模式下使用“**ip tcp window-size** *size*”命令设置窗口大小，单位是字节，取值范围是 128 到 (65535<< 14)，缺省值是 65535。如果窗口大于 65535 字节，自动开启窗口扩大功能。
- 实际通告给对端的窗口大小是从配置的窗口大小和接收缓冲区的剩余空间取较小值。

10.x 版本只对 IPv4 TCP 生效，从 11.0 版本开始对 IPv4 TCP 和 IPv6 TCP 都生效。

7.3.3 配置端口不可达时是否发送 reset 报文

工作原理

TCP 协议在分发 TCP 报文给应用程序时，如果找不到该报文所属的 TCP 连接会主动回复一个 reset 报文以终止对端的 TCP 连接。攻击者可能利用大量的端口不可达的 TCP 报文对设备进行攻击。

相关配置

配置端口不可达时是否发送 reset 报文

收到端口不可达的 TCP 报文时，默认发送 reset 报文。

用户可以在全局配置模式下使用“**no ip tcp send-reset**”命令禁止发送 reset 报文。

如果允许发送 reset 报文，攻击者可能利用大量的端口不可达的 TCP 报文对设备进行攻击。

11.0 版本废弃了 10.x 版本的配置命令“ip tcp not-send-rst”，并且兼容 10.x 版本，如果执行了 10.x 版本的配置命令，将自动转换成 11.0 版本的配置命令。

10.x 版本只对 IPv4 TCP 生效，从 11.0 版本开始对 IPv4 TCP 和 IPv6 TCP 都生效。

7.3.4 配置 MSS

工作原理

最大分段大小（Maxitum Segment Size，MSS），指一个 TCP 报文的数据载荷的最大长度，不包括 TCP 选项。

在 TCP 建立连接的三次握手中需要进行 MSS 协商，连接的双方都在 SYN 报文中增加 MSS 选项，其选项值表示本端最大能接收的段大小，即对端最大能发送的段大小。连接的双方取本端发送的MSS值和接收对端的MSS值的较小者作为本连接最大传输段大小。

发送 SYN 报文时 MSS 选项值的计算方法如下：

- IPv4 TCP：MSS = 对端 IP 地址对应的出口的 IP MTU - 20 字节 IP 首部 - 20 字节 TCP 首部。
- IPv6 TCP：MSS = 对端 IPv6 地址对应的路径 MTU - 40 字节 IPv6 首部 - 20 字节 TCP 首部。

10.x 版本只对 IPv4 TCP 生效，从 11.0 版本开始对 IPv4 TCP 和 IPv6 TCP 都生效。

实际生效的 MSS 是从根据 MTU 计算得到的 MSS 和用户配置的 MSS 取较小值。

如果该连接支持某些选项，那么 MSS 还要减去选项 4 字节对齐后的长度值。如 MD5 选项要减去 20 字节，MD5 选项长度 18 字节，对齐后 20 字节。

相关配置

设置 MSS

- 用户可以在全局配置模式下使用“**ip tcp mss** *max-segment-size*”命令设置 TCP 连接的 MSS，单位是字节，取值范围是 68 到 10000，默认使用根据 MTU 计算得到的 MSS。如果用户配置了 MSS，实际生效的 MSS 是从根据 MTU 计算得到的 MSS 和用户配置的 MSS 取较小值。
- MSS 太小会降低传输性能，增加 MSS 可以提高传输性能，但不是越大越好，选择 MSS 值可以参考接口的 MTU，如果 MSS 大于接口的 MTU，TCP 报文需要分片重组，会降低传输性能。

7.3.5 配置转发的 SYN 报文的 MSS 选项值

工作原理

当客户端发起一个 TCP 连接时，它通过 TCP SYN 报文中的 MSS 选项字段协商 TCP 报文数据载荷的最大值，客户端 SYN 报文的 MSS 值表示后续服务器端发送 TCP 报文数据载荷的最大值，反之同理。

如下图所示，PC 与 HTTP 服务器端建立的连接协商的 MSS 是 1460，但数据长度为 1460 字节的 TCP 报文无法直接通过 R1 和 R2，需要分片，因为 R1 和 R2 用隧道相连，隧道的 MTU 小于 1500。这时可以通过在 R2 的（1）口和（2）口上修改 SYN 报文中的 MSS 选项值，从而修改经过（1）口和（2）口的 TCP 连接协商的 MSS 值。

图 7-3

相关配置

设置转发的 TCPv4 SYN 报文的 MSS 选项值

- 缺省配置是不修改转发的 TCPv4 SYN 报文的选项值。
- 用户可以在接口配置模式下使用“**ip tcp adjust-mss** *max-segment-size*”命令设置转发的 TCPv4 SYN 报文的 MSS 选项值，取值范围是 500 到 1460，单位是字节。
- 如果 TCPv4 报文传输路径中两台设备之间链路的 MTU 比较小，为了避免 TCP 报文分片，用户可以在该设备上设置转发的 TCPv4 SYN 报文的 MSS 选项值，该设备收到 TCPv4 SYN 报文时将会修改 MSS 选项值。用户选择 MSS 值时可以参考接口的 IP MTU。

该配置对于已经存在的 TCP 连接无效，只对新的 TCP 连接有效。

设置转发的 TCPv6 SYN 报文的 MSS 选项值

- 缺省配置是不修改转发的 TCPv6 SYN 报文的选项值。
- 用户可以在接口配置模式下使用“**ipv6 tcp adjust-mss** *max-segment-size*”命令设置转发的 TCPv6 SYN 报文的 MSS 选项值，取值范围是 1220 到 1440，单位是字节。
- 如果 TCPv6 报文传输路径中两台设备之间链路的 MTU 比较小，为了避免 TCPv6 报文分片，用户可以在该设备上设置转发的 TCPv6 SYN 报文的 MSS 选项值，该设备收到 TCPv6 SYN 报文时将会修改 MSS 选项值。用户选择 MSS 值时可以参考接口的 IPv6 MTU。

该配置对于已经存在的 TCPv6 连接无效，只对新的 TCPv6 连接有效。

7.3.6 路径 MTU 发现功能

工作原理

RFC1191 规定的 TCP 连接的路径 MTU 发现功能，用来发现 TCP 报文传输路径的最小 MTU，避免分片重组，可以提高网络带宽的利用率。IPv4 TCP 路径 MTU 发现的过程如下：

(1) TCP 源端将发送的 TCP 报文的外层 IP 首部设置不可分片标志位。

(2) 如果 TCP 路径上某路由器的出口 MTU 值小于该 IP 报文长度，则会丢弃报文，并向 TCP 源端发送 ICMP 差错报文，报文中会携带该出口 MTU 值。

(3) TCP 源端通过解析该 ICMP 差错报文，可知 TCP 路径上当前最小的 MTU 值，即路径 MTU。

(4) 后续 TCP 源端发送数据段的长度不超过 MSS，MSS = 路径 MTU - IP 头部长度 - TCP 头部长度。

相关配置

↘ 启用路径 MTU 发现功能

TCP 缺省关闭路径 MTU 发现功能。

用户可以在全局配置模式下使用“**ip tcp path-mtu-discovery**”命令开启路径 MTU 发现功能。

10.x 版本对 IPv4 TCP 和 IPv6 TCP 都生效。从 11.0 版本开始只对 IPv4 TCP 生效，IPv6 TCP 总是开启路径 MTU 发现功能，并且不能关闭。

7.3.7 TCP 保活功能

工作原理

如果 TCP 希望知道对端是否还在正常工作，可以开启保活功能。当 TCP 对端在一段时间内（称为空闲时间）没有发送过报文给本端，本端开始发送保活报文，连续发送若干次，如果没有收到一个应答报文，就认为对端异常，关闭 TCP 连接。

相关配置

↘ 启用保活功能

- TCP 缺省关闭保活功能。
- 用户可以在全局配置模式下使用“**ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]”命令开启保活功能。interval 是时间间隔，默认值是 75 秒；times 是发送保活报文的最大次数，默认值是 6 次；idle-period 是空闲时间，默认值是 15 分钟。

10.x 版本只对 IPv4 TCP 生效，从 11.0 版本开始对 IPv4 TCP 和 IPv6 TCP 都生效。

10.x 版本提供全局配置模式的配置命令“**service tcp-keepalives-in**”用来开启 TCP 服务器端的保活功能，11.0 版本废弃该命令，该命令隐藏，如果用户执行该命令，将转换成新的配置命令保存。

10.x 版本提供全局配置模式的配置命令“**service tcp-keepalives-out**”用来开启 TCP 客户端的保活功能，11.0 版本废弃该命令，该命令隐藏，如果用户执行该命令，将转换成新的配置命令保存。

该命令不再区分服务器端和客户端，对所有的 TCP 连接都生效。

7.4 配置详解

配置项	配置建议 & 相关命令	
TCP性能优化	可选配置，用于优化 TCP 连接的性能。	
	ip tcp synwait-time	配置建立 TCP 连接的超时时间。
	ip tcp window-size	配置 TCP 窗口大小。
	ip tcp send-reset	配置收到端口不可达的 TCP 报文时是否发送 reset 报文。
	ip tcp mss	配置 TCP 连接的 MSS。
	ip tcp adjust-mss	配置转发的 TCPv4 SYN 报文的 MSS 选项值。
	ipv6 tcp adjust-mss	配置转发的 TCPv6 SYN 报文的 MSS 选项值。
	ip tcp path-mtu-discovery	开启路径 MTU 发现功能。
TCP连接异常检测	可选配置，用于检测 TCP 对端是否正常工作。	
	ip tcp keepalive	开启 TCP 保活功能。

7.4.1 TCP 性能优化

配置效果

- TCP 连接的传输性能达到最优，避免分片。

注意事项

-

配置方法

配置 SYN 超时

- 可选配置。
- 在 TCP 连接的两端配置。

配置 TCP 窗口大小

- 可选配置。
- 在 TCP 连接的两端配置。

配置端口不可达时是否发送 reset 报文

- 可选配置。
- 在 TCP 连接的两端配置。

配置 MSS

- 可选配置。
- 在 TCP 连接的两端配置。

配置转发的 TCPv4 SYN 报文的 MSS 选项值

- 可选配置。
- 如果 TCP 传输路径中两台路由器之间的 MTU 比较小，可以在路由器上配置。

配置转发的 TCPv6 SYN 报文的 MSS 选项值

- 可选配置。
- 如果 TCPv6 传输路径中两台路由器之间的 MTU 比较小，可以在路由器上配置。

配置 TCP 的路径 MTU 发现功能

- 可选配置。
- 在 TCP 连接的两端配置。

检验方法

-

相关命令

配置 SYN 超时

【命令格式】 **ip tcp synwait-time** *seconds*
【参数说明】 *seconds*：SYN 报文超时时间。单位为秒，取值范围是 5 到 300，缺省值是 20。
【命令模式】 全局模式
【使用指导】 如果网络中存在 SYN 攻击，减少 SYN 超时时间可以防止一些资源消耗，但对连续的 SYN 攻击达不到效果。

在设备主动与外界请求建立连接时，减少 SYN 超时时间可以减少用户等待时间，如 telnet。如果网络比较差也可以适当增加超时时间。

配置 TCP 窗口大小

【命令格式】 **ip tcp window-size** *size*
【参数说明】 *size*：单位是字节，取值范围是 128 到(65535 << 14)，缺省值是 65535。
【命令模式】 全局模式
【使用指导】 -

配置端口不可达时是否发送 reset 报文

【命令格式】 **ip tcp send-reset**
【参数说明】 **-**
【命令模式】 全局模式
【使用指导】 收到端口不可达的 TCP 报文时，默认发送 reset 报文。

配置 MSS

【命令格式】 **ip tcp mss** *max-segment-size*
【参数说明】 *max-segment-size*：MSS 的上限值。单位为字节，取值范围是 68 到 10000，默认使用根据 MTU 计算得到的 MSS。
【命令模式】 全局模式
【使用指导】 **ip tcp mss** 的作用就是限制即将建立的 TCP 连接的 MSS 的最大值。任何新建立的连接协商的 MSS 值不能超过配置的值。如果要减小连接的最大 MSS 值，可以配置该命令，一般情况下不需要配置。

配置转发的 TCPv4 SYN 报文的 MSS 选项值

【命令格式】 **ip tcp adjust-mss** *max-segment-size*
【参数说明】 *max-segment-size*：最大数据段大小，单位为字节，取值范围是 500 到 1460。
【命令模式】 接口模式
【使用指导】 **-**

配置转发的 TCPv6 SYN 报文的 MSS 选项值

【命令格式】 **ipv6 tcp adjust-mss** *max-segment-size*
【参数说明】 *max-segment-size*：最大数据段大小，单位为字节，取值范围是 1220 到 1440。
【命令模式】 接口模式
【使用指导】 **-**

配置路径 MTU 发现功能

【命令格式】 **ip tcp path-mtu-discovery** [**age-timer** *minutes* **| age-timer infinite**]
【参数说明】 **age-timer** *minutes*：TCP 在发现路径 MTU 后，重新进行探测的时间间隔。单位是分钟，取值范围是 10 到 30。缺省值是 10。
age-timer infinite：TCP 在发现路径 MTU 后，不重新探测。
【命令模式】 全局模式

【使用指导】 TCP 的路径 MTU 发现功能是按 RFC1191 实现的，这个功能可以提高网络带宽的利用率。当用户使用 TCP 来批量传输大块数据时，该功能可以使传输性能得到明显提升。

按 RFC1191 的描述，TCP 在发现路径 MTU 后，隔一段时间可以使用更大的 MSS 来探测新的路径 MTU。这个时间间隔就是使用参数 **age-timer** 来指定。当设备发现的路径 MTU 比 TCP 连接两端协商出来的 MSS 小时，设备就会按上述配置时间间隔，去尝试发现更大的路径 MTU。直到路径 MTU 达到 MSS 的值，或者用户停止这个定时器，这个探测过程才会停止。停止这个定时器，使用 **age-timer infinite** 参数。

配置举例

↘ 开启 TCP 的路径 MTU 发现功能。

【配置方法】 在设备上开启 TCP 的路径 MTU 发现功能，重新探测的时间间隔取缺省值。

```
Ruijie# configure terminal
Ruijie(config)# ip tcp path-mtu-discovery
Ruijie(config)# end
```

【检验方法】 用户可以执行命令 **show tcp pmtu** 查看 IPv4 TCP 连接的路径 MTU。

```
Ruijie# show tcp pmtu

Number  Local Address           Foreign Address         PMTU

1       192.168.195.212.23      192.168.195.112.13560   1440
```

用户可以执行命令 **show ipv6 tcp pmtu** 查看 IPv6 TCP 连接的路径 MTU。

```
Ruijie# show ipv6 tcp pmtu

Number  Local Address           Foreign Address         PMTU

1       1000::1:23              1000::2.13560           1440
```

常见错误

-

7.4.2 TCP 连接异常检测

配置效果

- TCP 探测对端是否还在正常工作。

注意事项

-

配置方法

开启保活功能

- 可选配置。

检验方法

-

相关命令

开启保活功能

【命令格式】 **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]

【参数说明】 **interval** *num1*：发送保活报文的时间间隔，单位是秒，取值范围是 1 到 120，缺省值是 75 秒。

times *num2*：发送保活报文的最大次数，取值范围是 1 到 10，缺省值是 6。

idle-period *num3*：空闲时间，即对端没有向本端发送过报文的时间长度，单位是秒，取值范围是 60 到 1800，缺省值是 15 分钟。

【命令模式】 全局模式

【使用指导】 如果 TCP 希望知道对端是否还在正常工作，可以开启保活功能，默认关闭。

假设用户开启保活功能，时间间隔，次数和空闲时间都使用缺省值，TCP 在 15 分钟内没有收到过对端发送的报文，开始发送保活报文，每隔 75 秒发送一次，连续发送 6 次，如果没有收到对方发送的任何 TCP 报文，就认为 TCP 连接无效，自动释放 TCP 连接。

配置举例

开启 TCP 保活功能。

【配置方法】 在设备上开启 TCP 保活功能，空闲时间是 3 分钟，发送保活报文的时间间隔是 60 秒，如果连续发送 4 次保活报文，没有收到对方发送的任何 TCP 报文，就认为 TCP 连接无效。

```
Ruijie# configure terminal
Ruijie(config)# ip tcp keepalive interval 60 times 4 idle-period 180
Ruijie(config)# end
```

【检验方法】 用户远程登录到设备，然后用户异常关机，在设备上执行 show tcp connect 观察用户的 IPv4 TCP 连接被删除的时间。

常见错误

-

7.5 监视与维护

清除各类信息

-

查看运行情况

作用	命令
显示 IPv4 TCP 连接的基本信息	**show tcp connect** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
显示 IPv4 TCP 连接的统计信息	**show tcp connect statistics**
显示 IPv4 TCP 路径 MTU 的信息	**show tcp pmtu** [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]
显示 IPv4 TCP 端口使用情况	**show tcp port** [*num*]
显示 IPv6 TCP 连接的基本信息	**show ipv6 tcp connect** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
显示 IPv6 TCP 连接的统计信息	**show ipv6 tcp connect statistics**
显示 IPv6 TCP 路径 MTU 的信息	**show ipv6 tcp pmtu** [**local-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-ipv6** *X:X:X:X::X*] [**peer-port** *num*]
显示 IPv6 TCP 端口使用情况	**show ipv6 tcp port** [*num*]

查看调试信息

输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
查看 IPv4 TCP 报文的调试信息	**debug ip tcp packet** [**in** | **out**] [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**global**] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
查看 IPv4 TCP 连接的调试信息	**debug ip tcp transactions** [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**local-port** *num*] [**peer-port** *num*]
查看 IPv6 TCP 报文的调试信息	**debug ipv6 tcp packet** [**in** | **out**] [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**global**] [**local-port** *num*] [**peer-port** *num*] [**deeply**]
查看 IPv6 TCP 连接的调试信息	**debug ipv6 tcp transactions** [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-port** *num*]

8 软件 IPv4/v6 快转

8.1 概述

在不支持硬件转发的产品上，由软件转发 IPv4/v6 报文，为了使软件转发性能达到最优，我司实现了软件 IPv4/v6 快转。

快转主要维护两张表：转发表和邻接表。转发表用来存放路由；邻接表用来存放下一跳的链路层信息，相当于 ARP 表和 IPv6 邻居表。

快转可以主动解析下一跳，还可以实现流量负载均衡。

下文仅介绍软件 IPv4/v6 的相关内容。

协议规范

-

8.2 典型应用

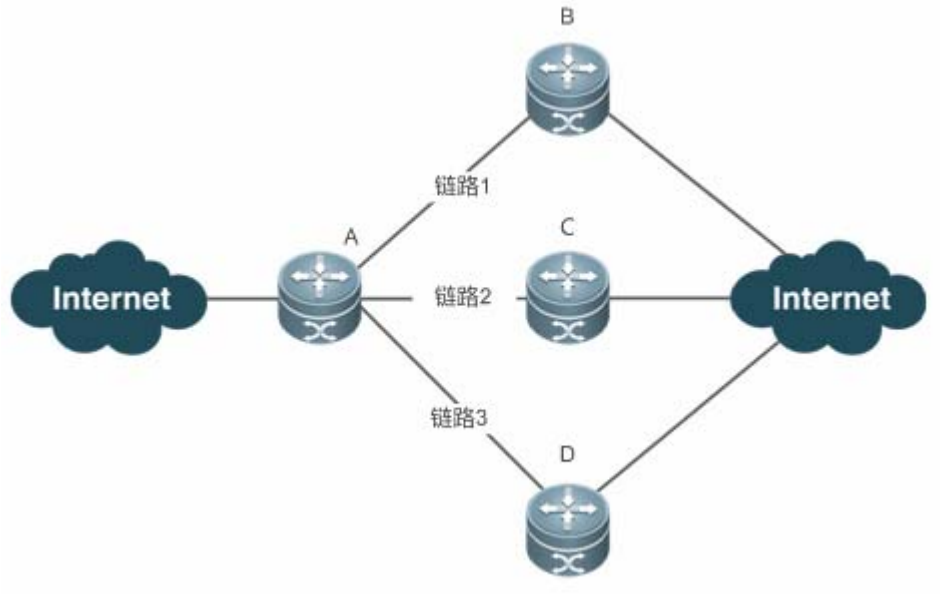
典型应用	场景描述
流量负载均衡	在网络路由中，当路由前缀关联到多个下一跳时，快转可以在多个下一跳中实现流量负载均衡。

8.2.1 流量负载均衡

应用场景

以下图为例，路由器 A 上，对于某条路由前缀关联 3 个下一跳，即链路 1、链路 2 和链路 3。缺省情况下，快转使用目的 IP 地址进行负载均衡，还可以根据源 IP 地址和目的 IP 地址进行负载均衡。

图 8-1



【注释】 A 为运行软件快转的路由器。
B、C、D 可以为其它转发设备。

功能部属

- 路由器 A 上运行软件快转。

8.3 功能详解

基本概念

IPv4/v6 快转主要涉及以下基本概念：

↘ 路由表

IPv4/v6 路由表中存储着指向特定网络地址的路径，同时含有网络周边的拓扑信息。在报文转发的过程中 IPv4/v6 快转根据路由表选择报文的传输路径。

↘ 邻接节点

邻接节点包含了被路由报文的输出接口信息。例如下一跳列表、下一个处理部件、链路层输出封装等信息。当报文与该邻接节点匹配时，直接对报文进行封装，而后调用该节点的发送函数即可实现转发。为了便于检索和更新，邻接节点构成的表一般组织成哈希表的形式；为了支持路由负载均衡，邻接节点的下一条列表信息被组织为负载均衡表的形式；邻接节点中也可以不包含下一跳信息，也可以包含下一个处理部件的索引号（例如其它线卡，多业务卡）。

↘ 主动解析

快转支持主动解析下一跳。对于以太网接口上的下一跳，如果不知道MAC地址，快转将主动解析下一跳。IPv4快转请求ARP模块解析下一跳；IPv6 快转请求 ND 模块解析下一跳。

↘ 报文转发路径

报文的路由转发是根据报文的 IPv4/v6 地址，所以如果指定了报文源 IPv4/v6 地址和目的 IPv4/v6 地址，则该报文的转发路径将是确定的。

8.3.1 快转负载均衡策略

快转负载均衡就是利用多个网络设备通道均衡分担流量。

工作原理

快转支持报文的负载均衡处理，目前实现两种基于 IP 地址的负载均衡策略。在快转模型中，当路由前缀关联到多个下一跳时，即多径路由，该路由将关联到一个负载均衡表，并依路由权重实现负载均衡。当 IPv4/v6 报文依最长前缀匹配到该均衡表时，快转根据报文的 IPv4/v6 地址进行散列，选中其中的一条路径转发报文。

IPv4/v6 快转支持两种负载均衡模式，分别是根据报文的目的 IP 地址进行均衡、根据报文的源 IP 和目的 IP 地址进行均衡。

相关配置

↘ 配置 IPv4 源 IP 地址 + 目的 IP 地址负载均衡算法

- 缺省根据 IPv4 报文的目的 IP 地址进行均衡。
- 可以根据 **ip ref load-sharing original** 配置该负载均衡算法。
- 配置后根据 IPv4 报文的目的 IP 地址和源 IP 地址进行均衡。

↘ 配置 IPv6 源 IP 地址 + 目的 IP 地址负载均衡算法

- 缺省根据 IPv6 报文的目的地址进行均衡。
- 根据 **ipv6 ref load-sharing original** 配置该负载均衡算法。
- 配置后根据 IPv6 报文的目的 IP 地址和源 IP 地址进行均衡。

8.4 配置详解

配置项	配置建议 & 相关命令	
配置快转负载均衡策略	⚠ 可选配置。	
	ip ref load-sharing original	启动 IPv4 源 IP 地址 + 目的 IP 地址负载均衡算法
	ipv6 ref load-sharing original	启动 Ipv6 源 IP 地址 + 目的 IP 地址负载均衡算法

8.4.1 配置快转负载均衡策略

配置效果

路由快转支持的两种选路策略如下：

- 按 IPv4/v6 报文的目的 IPv4/v6 地址进行均衡，对报文的目标地址进行散列，权重大的路径被选中的机率大。缺省采用此策略。
- 按 IPv4/v6 报文的目的 IPv4/v6 地址和源 IPv4/v6 地址进行均衡，对报文的目的 IPv4/v6 地址和源 IPv4/v6 地址进行散列，权重大的路径被选中的机率大。

注意事项

-

配置方法

- 可选配置。
- 在 IPv4/v6 环境下，如果需要根据源 IP 地址+目的 IP 地址进行流量均衡，可采用此配置。
- 在连接多条链路的路由设备上配置。

检验方法

使用 **show ip ref adjacency statistic** 命令可以查看 IPv4 快转的负载均衡策略；使用 **show ipv6 ref adjacency statistic** 命令可以查看 IPv6 快转的负载均衡策略。

相关命令

↘ 配置 IPv4 源 IP 地址 + 目的 IP 地址负载均衡算法

【命令格式】 **ip ref load-sharing original**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

↘ -配置 IPv6 源 IP 地址 + 目的 IP 地址负载均衡算法

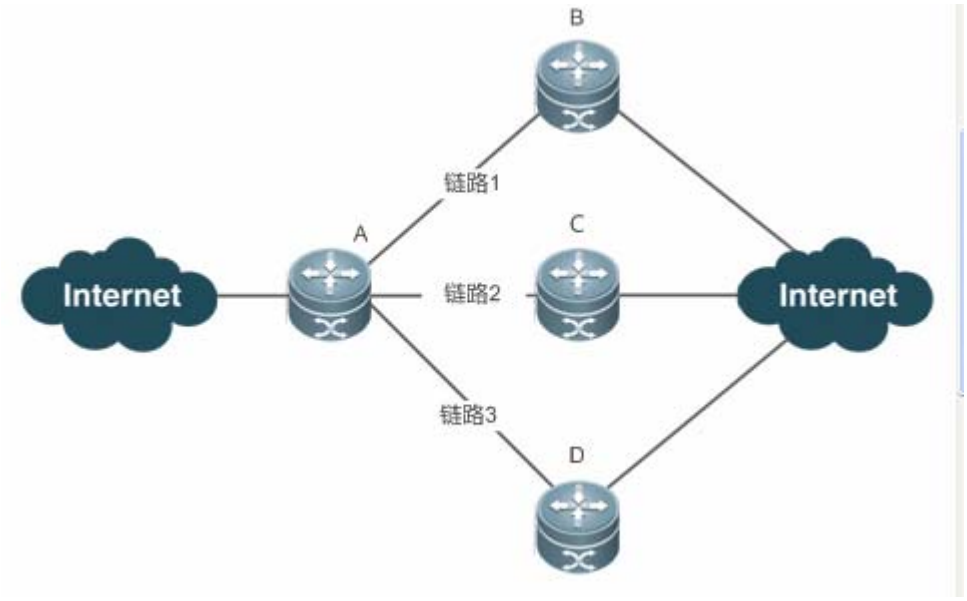
【命令格式】 **ipv6 ref load-sharing original**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 -

配置举例

↘ 配置基于 IPv4 源 IP 地址 + 目的 IP 地址负载均衡

【网络环境】

图 8-2



在路由器 A 上，对于某条路由前缀关联 3 个下一跳，即链路 1、链路 2 和链路 3。

【配置方法】 在路由器 A 上配置 IPv4 源 IP 地址 + 目的 IP 地址负载均衡

A

```
A#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
A(config)#ip ref load-sharing original
```

【检验方法】

```
A #show ip ref adjacency statistics
adjacency balance table statistic:
    source-dest-address load-sharing
    balance: 0

adjacency node table statistic:
    total  : 3
    local  : 1
    glean  : 0
    forward: 0
    discard: 0
    mcast  : 1
    punt   : 1
    bcast  : 0
```

常见配置错误

-

8.5 监视与维护

统计快转报文信息

快转报文统计信息即快转所处理的报文统计信息，包括了转发的报文数目，以及各种原因丢弃的报文数目等。快转提供配置信息查看和清除当前的统计信息，以供判断报文的转发行为是否和预期相同。

命令	作用
show ip ref packet statistics	显示 IPv4 快转当前的报文统计信息
clear ip ref packet statistics	清除 IPv4 快转当前的报文统计信息
show ipv6 ref packet statistics	显示 IPv6 快转当前的报文统计信息
clear ipv6 ref packet statistics	清除 IPv6 快转当前的报文统计信息

查看邻接信息

用户可以通过以下命令来查看当前的邻接信息：

命令	作用
show ip ref adjacency [**glean** | **local** | *ip-address* | {**interface** *interface_type interface_number)* **| discard | statistics**]	可以指定显示 IPv4 快转的集合邻接、本地邻接、指定 IP 对应邻接、指定接口关联邻接及所有邻接节点相关信息。
show ipv6 ref adjacency [glean | local | *ipv6-address* **| (interface** *interface_type interface_number*) **| discard | statistics**]	可以指定显示 IPv6 快转的集合邻接、本地邻接、指定 IPv6 地址对应邻接、指定接口关联邻接及所有邻接节点相关信息。

查看主动解析信息

用户可以通过以下命令来查看需要主动解析的下一跳：

命令	作用
show ip ref resolve-list	查看 IPv4 快转主动解析的下一跳。
show ipv6 ref resolve-list	查看 IPv6 快转主动解析的下一跳。

查看报文转发路径信息

报文的路由转发是根据报文的 IPv4/v6 地址，所以如果指定了报文源 IPv4/v6 地址和目的 IPv4/v6 地址，则该报文的转发路径将是确定的。执行下面的命令，并指定报文的源 IPv4/v6 地址与目的 IPv4/v6 地址，将会显示该报文的实际转发路径，比如报文丢弃、提交 CPU 或转发，进一步还可以知道从哪个接口转发等等。

命令	作用
show ip ref exact-route *source-ipaddress dest_ipaddress*	显示某特定报文的实际转发路径。

show ipv6 ref exact-route *src-ipv6-address dst-ipv6-address*	显示某特定 IPv6 报文的实际转发路径。

查看快转表路由信息

通过下面的命令可以查看快转表的路由信息：

命令	作用
show ip ref route [**default** | {*ip mask*}| **statistics**]	显示当前 IPv4 快转表中的路由信息，参数 default 表示显示缺省路由。
show ipv6 ref route [**default** | **statistics** | *prefix/len*]	显示当前 IPv6 快转表中的路由信息，参数 default 表示显示缺省路由。

9 NAT

9.1 概述

NAT（Network Address Translation，网络地址转换）是将 IP 数据包头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要用于实现私有网络访问公共网络的功能。这种通过使用少量的公有 IP 地址代表较多的私有 IP 地址的方式，将有助于减缓可用 IP 地址空间的枯竭。

下文仅介绍 NAT 的相关内容。

协议规范

- RFC 1631：The IP Network Address Translator (NAT)
- RFC 2663：IP Network Address Translator (NAT) Terminology and Considerations
- RFC 2391：Load Sharing using IP Network Address Translation (LSNAT)
- RFC 4008：Definitions of Managed Objects for Network Address Translators (NAT)

9.2 典型应用

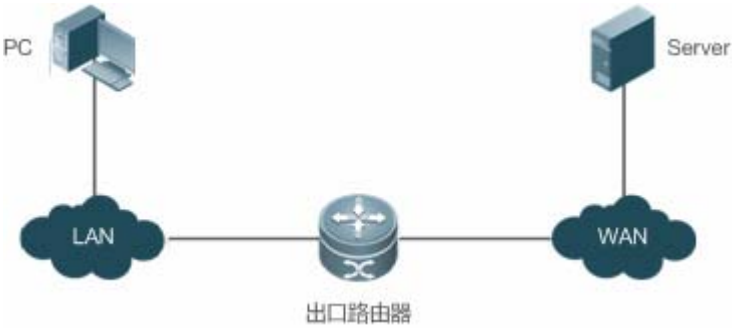
典型应用	场景描述
内网用户访问互联网服务	当内部网络需要与互联网网络通讯时，需要配置 NAT，将内部私有 IP 地址转换成全局唯一 IP 地址。
外部用户访问内网服务器	利用设备将一个或者多个内部主机映射成网络服务器，从而使得外部网络上的网络用户可以获得对应的服务。
内部用户源目的地址转换	两个需要互联的私有网络分配了同样 IP 地址，或者一个私有网络和公有网络分配了同样的全局 IP 地址，两个重叠地址的网络主机之间是不可能通信的，配置了重叠地址 NAT，外部网络主机地址在内部网络表现为另一个网络主机地址，反之一样。
内网服务器负载均衡	当内部网络某台主机 TCP 流量负载过重时，可用多台主机进行 TCP 业务的均衡负载。这时，可以考虑用 NAT 来实现 TCP 流量的负载均衡。

9.2.1 内网用户访问互联网服务

应用场景

以下图为例，PC 位于内网，某服务器位于外网。但由于 IP 地址即将耗尽的问题，整个园区网只分配了一个或者几个外网 IP 地址。出口路由器属于内网，用于连接外网。内网 PC 要访问到外网服务器，需要在出口路由器上开启基本 NAT 功能。

图 9-1



【注释】 出口路由器分别与内网和外网相连

功能部属

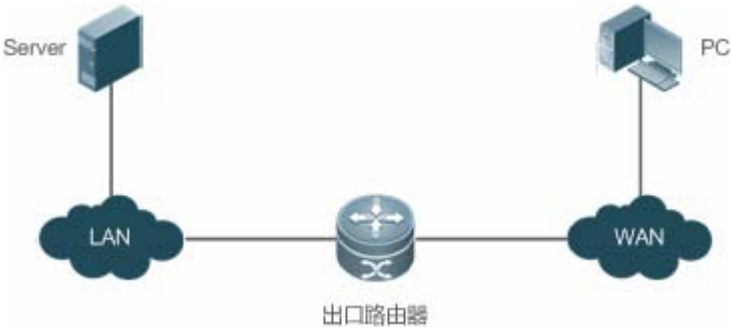
- 在内外网口配置 NAT 接口
- 出口网关上配置内部源地址静态地址转换

9.2.2 外部用户访问内网服务器

应用场景

以下图为例，PC 位于外网，某服务器(如 web 服务器)位于内网。但由于 IP 地址即将耗尽的问题，整个园区网只分配了一个外网 IP 地址。出口路由器属于内网，用于连接外网。PC 要访问到内网的服务器，需要在出口路由器上开启 NAPT 功能，即针对 web 服务提供的端口进行的端口映射。

图 9-2



【注释】 出口路由器分别与内网和外网相连
内网部署服务器

功能部属

- 在内外网口配置 NAT 接口
- 出口网关上配置服务器端口地址转换规则

9.2.3 内部用户源目的地址转换

应用场景

以下图为例，PC1 位于私网 1，PC2 位于私网 2。由于 2 个私网以前是单独管理，所以，2 个私网的 IP 地址网段发生了地址重叠，如 PC1 和 PC2 都配置成在 192.168.1.0/24 网段。出口路由器位于私网 1 和私网 2 之间。PC1 和 PC2 要实现实现互访，需要在出口路由器上开启重叠地址 NAT 功能。

图 9-3

【注释】 出口路由器分别与私网 1 和私网 2 相连

功能部属

- 在内外网口配置 NAT 接口
- 出口网关上配置内部源地址动态地址转换
- 出口网关上配置外部源地址动态地址转换

9.2.4 内网服务器负载均衡

应用场景

以下图为例，服务器 1 和服务器 2 位于内网，2 台服务器形成集群。PC 位于外网。但由于 IP 地址即将耗尽的问题，整个园区网只分配了一个外网 IP 地址。出口路由器属于内网，用于连接外网。出口路由器要将外网访问服务器的流量分担在 2 台服务器上，需要在出口路由器上开启 NAT 负载均衡功能。

图 9-4

【注释】 出口路由器分别与内网和外网相连
内网部署服务器

功能部属

- 在内外网口配置 NAT 接口
- 出口网关上配置 TCP 负载均衡地址转换

9.3 功能详解

基本概念

私有网络地址和公有网络地址

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

A 类私有地址：10.0.0.0~10.255.255.255

B 类私有地址：172.16.0.0~172.31.255.255

C 类私有地址：192.168.0.0~192.168.255.255

NAT 最初的设计目的是用于实现私有网络访问公共网络的功能，后扩展到实现任意两个网络间进行访问时的地址转换应用，本文中将这两个网络分别称为内部网络（内网）和外部网络（外网），通常私网为内部网络，公网为外部网络。

静态 NAT

静态 NAT 是建立内部本地地址和内部全局地址的一对一永久映射。当外部网络需要通过固定的全局可路由地址访问内部主机，静态 NAT 就显得十分重要。

动态 NAT

动态 NAT，是建立内部本地地址和内部全局地址池的临时映射关系，过一段时间没有用就会删除映射关系。当内部网络只访问外网服务，不提供信息服务的主机，内部网络主机数大于全局 IP 地址数时，可以配置动态 NAT。

功能特性

功能特性	作用
基本NAT	内部私有地址转换成公网可以识别的地址，实现互通
NAPT	可以将多个内部本地地址映射到一个内部全局地址，解决 IP 地址枯竭问题
重叠地址NAT	重叠私有网络的互相访问
TCP负载均衡	该功能可以解决某台主机 TCP 流量过载的问题
构建本地服务器	构建本地服务器，以供外部网络的访问
ALG	由于 NAT 只会修改 IP 报文头部，不会去修改应用协议的载荷，引入 ALG，用于支持应用层协议

9.3.1 基本 NAT

当内部网络需要与外部网络通讯时，需要配置 NAT，将内部私有 IP 地址转换成全局唯一 IP 地址。可以配置静态或动态的 NAT 来实现互联互通的目的，或者需要同时配置静态和动态的 NAT。

工作原理

6. 内网用户主机（192.168.1.2）向外网服务器（8.8.8.8）发送的 IP 报文通过 NAT 设备。
7. NAT 设备查看报头内容，发现该报文是发往外网的，将其源 IP 地址字段的的私网地址 192.168.1.2 转换成一个可在 Internet 上选路的公网地址 30.1.1.1，并将该报文发送给外网服务器，同时在 NAT 设备的网络地址转换表中记录这一映射。
8. 外网服务器给内网用户发送的应答报文(其初始目的 IP 地址为 30.1.1.1)到达 NAT 设备后，NAT 设备再次查看报头内容，然后查找当前网络地址转换表的记录，用内网私有地址 192.168.1.2 替换初始的目的 IP 地址。

上述的 NAT 过程对终端（如图中的 Host 和 Server）来说是透明的。对外网服务器而言，它认为内网用户主机的 IP 地址就是 30.1.1.1，并不知道有 192.168.1.2 这个地址。因此，NAT “隐藏” 了企业的私有网络。

基本 NAT 包括静态 NAT、动态 NAT。

相关配置

↘ 配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat** { **inside | outside** }命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

↘ 配置静态 NAT

- 缺省情况下，没配置静态 NAT 信息。

- 使用 **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*] 命令可以配置静态一对一 NAT 映射。

配置动态 NAT

- 缺省情况下，没配置动态 NAT 信息。
- 使用 **ip nat inside source list** *access-list-number* **pool** *address-pool* 命令可以配置动态 NAT 映射。

9.3.2 NAPT

传统的 NAT 一般是指一对一的地址映射，不能同时满足所有的内部网络主机与外部网络通讯的需要。比如内网缺乏全局 IP 地址，甚至没有专门申请全局 IP 地址，只有一个连接 ISP 的全局 IP 地址，内网要求上网的主机数很多的场景下，需要使用 NAPT。

使用 NAPT(网络地址端口转换)，可以将多个内部本地地址映射到一个内部全局地址。

工作原理

NATP,也称之为" 多对一地址转换"，它允许多个内部地址映射到同一个公有地址上。NAPT 同时映射 IP 地址和端口号：来自不同内部地址的数据报文的源地址可以映射到同一外部地址，但它们的端口号被转换为该地址的不同端口号，因而仍然能够共享同一地址，也就是“私网 IP 地址＋端口号”与“公网 IP 地址＋端口号”之间的转换。

静态 NAPT

静态 NAPT 一般应用在将内部网指定主机的指定端口映射到全局地址的指定端口上。而前一小节提及的静态 NAT，是将内部主机映射成全局地址。静态 NAPT 适用于内网有提供信息服务的主机，它提供是永久的一对一 “IP 地址+端口” 映射关系。

动态 NAPT

动态 NAPT 适用于内网只访问外网服务，不提供信息服务的主机。它提供的是临时的一对一"IP 地址+端口"映射关系。

相关配置

配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat** { **inside | outside** }命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAPT

- 缺省情况下，没配置静态 NAPT 信息。
- 使用 **ip nat inside source static** *local-ip* **interface** *interface* [**permit-inside**]命令可以配置静态一对一 NAPT 映射。

配置动态 NAPT

- 缺省情况下，没配置动态 NAPT 信息。
- 使用 **ip nat inside source list** *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload** 命令可以配置动态 NAT 映射。 对于 NAPT，一般地址池就定义一个 IP 地址，一个地址最多可以提供 64512 个 NAT 地址转换。如果地址不够，地址池可以多定义几个地址。

9.3.3 重叠地址 NAT

两个需要互联的私有网络分配了同样 IP 地址，或者一个私有网络和公有网络分配了同样的全局 IP 地址，这种情况称为地址重叠。两个重叠地址的网络主机之间是不可能通信的，因为它们相互认为对方的主机在本地网络。重叠地址 NAT 就是专门针对重叠地址网络之间通信的问题，配置了重叠地址 NAT，外部网络主机地址在内部网络表现为另一个网络主机地址，反之一样。

工作原理

内部网络和外部网络重叠 IP 地址互访，NAT 必须将内部地址转换成唯一的外部地址，同时还需要将与内部重叠的外部地址转换成内部唯一地址，从而实现互访。

相关配置

配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat** { **inside | outside** }命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置内部源地址转换

- 缺省情况下，没配置内部源地址转换。
- 内部源地址转换，可以使用静态/动态基本 NAT 或者静态/动态 NAPT，详细见“基本 NAT”和“NAPT”章节。

配置外部源静态地址转换

- 缺省情况下，没配置外部源地址转换信息。
- 使用 **ip nat outside source static** *global-address local-address* 命令可以配置外部源地址静态 NAT 转换。

配置外部源动态地址转换

- 缺省情况下，没配置外部源动态转换信息。
- 使用 **ip nat outside source list** *access-list-number* **pool** *address-pool* 命令可以外部源地址动态 NAT 转换。

配置访问控制列表

- 缺省情况下，无访问控制列表的配置。
- 使用 **ip access-list {extended | standard}** **{***id* | *name***}**或者 **access-list** 命令配置合适的访问控制列表。

配置静态路由

- 必须配置。
- 使用 **ip route** *network net-mask* { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent | track** *object-number*] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**] [**global**]命令配置静态路由，用于指定内部目的地址转换后网络的出口。

9.3.4 TCP 负载均衡

当内部网络某台主机 TCP 流量负载过重时，可用多台主机进行 TCP 业务的均衡负载。这时，可以考虑用 NAT 来实现 TCP 流量的负载均衡。

工作原理

NAT 创建了一台虚拟主机提供 TCP 服务，该虚拟主机对应内部多台实际的主机，然后对目标地址进行轮询置换，达到负载分流的目的。

相关配置

配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat** { **inside | outside** }命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置地址池

- 缺省情况下，没配置地址池。
- 使用 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }配置转换的 IP 地址池。

配置 ACL

- 缺省情况下，没配置 ACL。
- 使用 **access-list** *access-list-number* **permit** *ip-address wildcard* 命令可以配置目标 IP 的扩展 ACL。注意 ACL 必须配置为匹配目标 IP 的扩展 ACL。

配置内部目的地址转换

- 缺省情况下，没配置内部目的地址转换。
- 使用 **ip nat inside destination list** *access-list-number* **pool** *address-pool* 命令可以配置内部目的地址转换。上述配置，只对 TCP 流量产生作用，对其它流量保持不变，除非有另外的 NAT 配置。

9.3.5 构建本地服务器

用户在内部网内设置了三台服务器(FTP 服务器、WEB 服务器以及 E-MAIL 服务器)，希望广域网上的网络主机能够访问这三个服务器。同时内部网的普通用户可以把网关设置成设备来访问 Internet。

工作原理

把内部一个或者多个内部主机映射成网络服务器，从而使得广域网上的网络用户可以获得对应的服务。

相关配置

配置 NAT 接口

- 缺省情况下，接口上未执行为 NAT 接口。
- 使用 **ip nat** { **inside | outside** }命令指定一对 NAT 接口。
- 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置内部地址端口转换

- 缺省情况下，没配置内部地址端口转换。
- 使用 **ip nat inside source static** { **udp** | **tcp** } **local-address port global-address port** [**permit-inside**]转换内部特定地址和端口，用专属的端口提供对应的服务，比如用 tcp 协议的 20，21 端口构建 ftp 服务器，用 tcp 协议的 80 端口构建 web 服务等

9.3.6 ALG

普通 NAT 实现了对 UDP 或 TCP 报文头中的的 IP 地址及端口转换功能，但对应用层数据载荷中的字段无能为力，在许多应用层协议中，比如多媒体协议(H.323 等)、FTP、SQLNET 等，TCP/UDP 载荷中带有地址或者端口信息，这些内容不能被 NAT 进行有效的转换，就可能导致问题。

工作原理

ALG（Application Level Gateway，应用层网关）技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的 IP 地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。NAT 默认开启所有 ALG。当前支持的 ALG 的协议有：dns、ftp、h323、pptp、tftp、rtsp。

相关配置

开启关闭 ALG

- 缺省情况下，开启所有 ALG。
- 使用 **no ip nat translation dns** 命令关闭 DNS ALG。
- 使用 **no ip nat translation ftp** 命令关闭 FTP ALG。
- 使用 **no ip nat translation h323** 命令关闭 H323 ALG。
- 使用 **no ip nat translation pptp** 命令关闭 PPTP ALG。
- 使用 **no ip nat translation tftp** 命令关闭 TFTP ALG。
- 使用 **no ip nat translation rtsp** 命令关闭 RTSP ALG。

9.4 配置详解

配置项	配置建议 & 相关命令	
配置基本NAT	⚠ 必须配置。用于内部 PC 连接大网的一对一 NAT 转换	
	ip nat inside	定义该接口连接内部网络
	ip nat inside	定义该接口连接外部网络
	⚠ 可选配置。用于静态 NAT 地址转换	
	ip nat inside source static *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** interface]	定义内部源地址静态转换关系。
	⚠ 可选配置。用于动态 NAP 地址转换。	
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* } 或者 **ip nat pool** *pool-name* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**] **address** *start-ip end-ip* [**match interface** *interface*]	定义全局 IP 地址池，对于 NAT，一般就定义一个多个 IP 地址，多于内网用户数，根据内网用户数定义地址池个数。

	access-list *ccess-list-number* **permit** *ip-address wildcard*	定义访问列表，只有匹配该列表的地址才转换。
	ip nat inside source list *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload**	定义源地址动态转换关系，overload 有和没有是一样的效果，仅是兼容主流厂商的配置。
配置NAPT	⚠ 必须配置。用于实现 NAPT	
	ip nat inside	定义该接口连接内部网络
	ip nat outside	定义该接口连接外部网络
	⚠ 可选配置。用于静态 NAPT 地址转换。	
	ip nat inside source static { **UDP** *local-address port* | **TCP** *local-address port* } *global-address port* [**permit-inside**]	定义内部源地址静态转换关系。
	⚠ 可选配置。用于动态 NAPT 地址转换。	
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	定义全局 IP 地址池，对于 NAPT，一般就定义一个 IP 地址。
	access-list *ccess-list-number* **permit** *ip-address wildcard*	定义访问列表，只有匹配该列表的地址才转换。
	ip nat inside source list *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload**	定义源地址动态转换关系，overload 有和没有是一样的效果，仅是兼容主流厂商的配置。
配置重叠地址NAT	必须配置。用于配置重叠地址 NAT。	
	ip nat inside	定义该接口连接内部网络
	ip nat outside	定义该接口连接外部网络
	ip nat inside source static *local-address global-address*	内部源地址转换配置
	⚠ 可选配置。用于静态地址转换	
	ip nat outside source static *global-address local-address*	静态 NAT 配置
	⚠ 可选配置。用于动态地址转换。	
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	定义全局 IP 地址池。
	access-list *ccess-list-number* **permit** *ip-address wildcard*	定义访问列表，只有匹配该列表的地址才转换。

	ip nat outside source list *access-list-number* **pool** *address-pool*	定义源地址动态转换关系，overload 有和没有是一样的效果，仅是兼容主流厂商的配置。
配置TCP负载均衡	⚠ 必须配置。用于实现目标地址的轮询转换	
	ip nat inside	定义该接口连接内部网络
	ip nat outside	定义该接口连接外部网络
	ip nat pool *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }	定义 IP 地址池，包含所有实际主机地址。
	access-list *access-list-number* **permit** *ip-address wildcard*	定义访问列表，只匹配虚拟主机地址。 ⚠ 注意应该使用匹配目标IP的扩展ACL。
	ip nat inside destination list *access-list-number* **pool** *address-pool*	定义内部目标地址动态转换关系。
配置ALG	⚠ 可选配置。用于实现相关协议的 ALG	
	ip nat translation { **dns** [**ttl** *ttl_time*] **| ftp** [**port** *port_num*] **| tftp | pptp | h323 | rtsp** }	定义相关协议的 ALG
配置NAT特殊应用	⚠ 可选配置。用于实现 NAT 特殊应用	
	ip nat application source list *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }	定义 NAT 特殊应用规则
配置NAT发送免费ARP间隔	⚠ 可选配置。发送 NAT 本机地址免费 arp 报文的间隔	
	ip nat keepalive [*keealive_out*]	定义发送 NAT 本机地址免费 arp 报文的间隔

9.4.1 配置基本 NAT

配置效果

当内部网络需要与外部网络通讯时，需要配置 NAT，将内部私有 IP 地址转换成全局唯一 IP 地址。用户可以配置静态或动态的 NAT 来实现互联互通的目的，或者需要同时配置静态和动态的 NAT。

注意事项

- 配置基本 NAT，必须配置至少一个 inside 接口和一个 outside 接口。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的 lan 接口下配置为 NAT inside 口。

配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的 wan 接口下配置为 NAT outside 口。

配置静态 NAT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，，应在全局配置模式下配置静态 NAT 地址转换。

配置动态 NAT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络，应在全局配置模式下配置动态 NAT 地址转换。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAT 地址转换

【命令格式】 **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*]

【参数说明】 *local-address*：内部地址

global-address：外部地址

permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机

netmask *mask*：网段到网段地址

match *interface*：指定出接口

【命令模式】 全局配置模式

【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 -

配置动态 NAT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* **pool** *address-pool*

【参数说明】 *access-list-number*：acl 号。

pool *address-pool*：地址池名字。

【命令模式】 全局模式

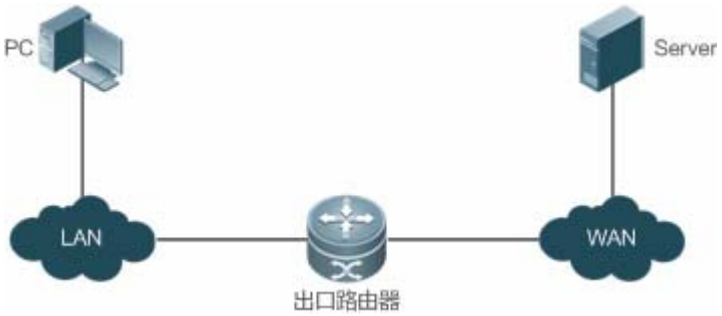
【使用指导】 -

配置举例

内网用户访问外网服务器

【网络环境】

图 9-5



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 nat 转换规则

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
```

```
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。

9.4.2 配置 NAPT

配置效果

传统的 NAT 一般是指一对一的地址映射，不能同时满足所有的内部网络主机与外部网络通讯的需要。比如内网缺乏全局 IP 地址，甚至没有专门申请全局 IP 地址，只有一个连接 ISP 的全局 IP 地址，内网要求上网的主机数很多的场景下，需要使用 NAPT。

使用 NAPT(网络地址端口转换)，可以将多个内部本地地址映射到一个内部全局地址。

注意事项

- 配置 NAPT，必须配置至少一个 inside 接口和一个 outside 接口。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

↘ 配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的接口下配置为 NAT inside 口。

配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的接口下配置为 NAT outside 口。

配置静态 NAPT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，应在全局配置模式下配置静态 NAPT 地址转换。

配置动态 NAPT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络时，应在全局配置模式下配置动态 NAPT 地址转换。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAPT 地址转换

【命令格式】 **ip nat inside source static** { **udp** *local-address port* | **tcp** *local-address port* } *global-address port* [**permit-inside**]

【参数说明】 **udp**：udp 协议

tcp：tcp 协议

local-address：内部本地地址

port：内部本地端口

global-address：外部全局地址

port：外部全局端口

permit-inside：允许内网用户以 global-ip 访问 local-ip 的主机。

【命令模式】 全局配置模式

【使用指导】 该命令是用来架设内部服务器，用于外部公网访问内部服务器，除非配置 **permit-inside**，才允许内部以 *global-address* 访问该服务器,否则内网只能以 *local-address* 访问该服务器

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 -

配置动态 NAPT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* { [**pool** *address-pool*] | [**interface** *interface-type interface-number*] } **overload**

【参数说明】 *access-list-number*：acl 号。

pool *address-pool*：地址池名字。

interface *interface-type interface-number*：利用 outside 接口的全局地址做 NAPT。

overload: pool 中的每个全局地址都可以复用转换，就是做 NAPT。目前没有配置这个参数，全局地址也是复用。之所以添加这个参数是为了跟 cisco 的命令兼容。

【命令模式】 全局配置模式

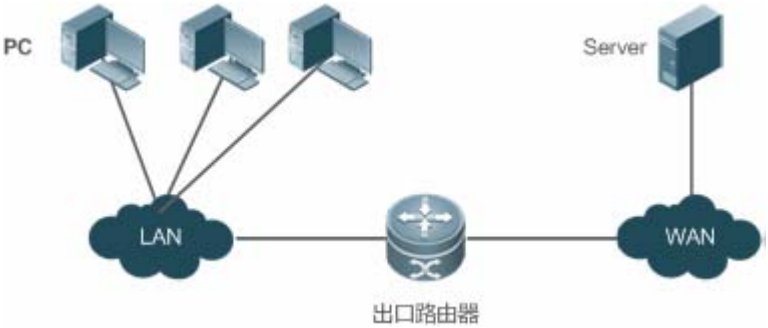
【使用指导】 -

配置举例

内网用户通过 NAPT 访问外网服务器

【网络环境】

图 9-6



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 NAPT 转换规则

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0
```

```
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool net200 200.168.12.1 200.168.12.1 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat inside source static tcp 192.168.12.3 80 200.198.12.1 80
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
icmp 200.168.12.200:2064 192.168.12.66:2063 168.168.12.1:23 168.168.12.1:23
udp 200.168.12.200:2065 192.168.12.67:2063 168.168.12.1:23 168.168.12.1:23
tcp 200.168.12.200:2066 192.168.12.68:2063 168.168.12.1:23 168.168.12.1:23
tcp 200.168.12.200:2067 192.168.12.69:2063 168.168.12.1:23 168.168.12.1:23
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。

9.4.3 配置重叠地址 NAT

配置效果

两个需要互联的私有网络分配了同样 IP 地址，或者一个私有网络和公有网络分配了同样的全局 IP 地址，这种情况称为地址重叠。两个重叠地址的网络主机之间是不可能通信的，因为它们相互认为对方的主机在本地网络。重叠地址 NAT 就是专门针对重叠地址网络之间通信的问题，配置了重叠地址 NAT，外部网络主机地址在内部网络表现为另一个网络主机地址，反之一样。

注意事项

- 配置重叠地址 NAT，必须先配置内部源地址 NAT 转换。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的接口下配置为 NAT inside 口。

配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的接口下配置为 NAT outside 口。

配置静态外部源地址转换

- 可选配置。
- 若外部网络存在少量用户需要访问内部网络时，应在全局配置模式下配置静态外部源地址转换。

配置动态外部源地址转换

- 可选配置。
- 若外部网络存在大量用户需要访问内部网络时，应在全局配置模式下配置动态外部源地址转换。

配置访问控制列表

- 使用动态源地址映射时必选。
- 该配置为限制内网需要通过源地址转换用户的范围。

配置静态路由

- 必须配置。
- 用于指定内部目的地址转换后网络的出口。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由

器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态外部源地址转换

【命令格式】 **ip nat outside source static** *global-address local-address*

【参数说明】 *global-address*：外部全局地址

local-address：内部本地**地**址

【命令模式】 全局配置模式

【使用指导】 -

配置静态外部源地址端口转换

【命令格式】 **ip nat outside source static** { **tcp** *global-address global-port* **| udp** *global-address global-port* } *local-iaddress local-port*

【参数说明】 *protocol*：协议号

global-address：外部全局地址

global-port：外部全局端口

local-address：内部本地地址

local-port：内部本地端口

【命令模式】 全局配置模式

【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 --

配置动态外部源地址转换

【命令格式】 **ip nat outside source list** *access-list-number* **pool** *pool-name*

【参数说明】 *access-list-number*：acl 号。

pool *pool-name*：地址池名字。

【命令模式】 全局配置模式

【使用指导】 -

配置举例

以下配置举例，仅介绍静态外部源地址转换相关的配置。

↘ 静态外部源地址转换

【网络环境】

图 9-7

【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态内部源地址 nat 转换规则
- 配置静态外部源地址 nat 转换规则

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat outside source static 192.168.12.3 172.16.10.1
A(config)# ip route 172.16.10.0 255.255.255.0 200.198.12.2
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 172.16.10.1:23 168.168.12.3:23
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。
- 未配置静态路由或者在 outside 接口配置 ip 地址，使得路由器不知道地址转换后该往哪个接口收发数据包。

9.4.4 配置 TCP 负载均衡

配置效果

当内部网络某台主机 TCP 流量负载过重时，可用多台主机进行 TCP 业务的均衡负载。这时，可以考虑用 NAT 来实现 TCP 流量的负载均衡。在以下的配置中，定义了一个虚拟主机地址，所有来自外部网络访问该虚拟主机的 TCP 连接，将被路由器分配到多台实际主机上，从而实现负载分流的目标。

注意事项

新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

↘ 配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的接口下配置为 NAT inside 口。

↘ 配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的接口下配置为 NAT outside 口。

↘ 配置动态内部目的地址转换

- 必须配置。
- 若需要 TCP 负载均衡访问，应在全局配置模式下配置动态内部目的地址转换。

检验方法

无

相关命令

↘ 配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }
【参数说明】 **inside**：内网口
outside：外网口
【命令模式】 接口模式
【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由

器必须配置至少一个 inside 接口和一个 outside 接口。

配置地址池

【命令格式】 **ip nat pool** *pool-name start-ip end-ip* { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

type rotary：NAT 地址池的类型。rotary 为轮转型，每个地址分配的概率相等。有没有配 rotary 都是轮转型。之所以引入 rotary 参数是与 cisco 命令兼容

【命令模式】 全局配置模式

【使用指导】 -

配置动态内部目的址转换

【命令格式】 **ip nat inside destination list** *access-list-number* **pool** *address-pool*

【参数说明】 *access-list-number*：acl 号。

pool *pool-name*：地址池名字。

【命令模式】 全局配置模式

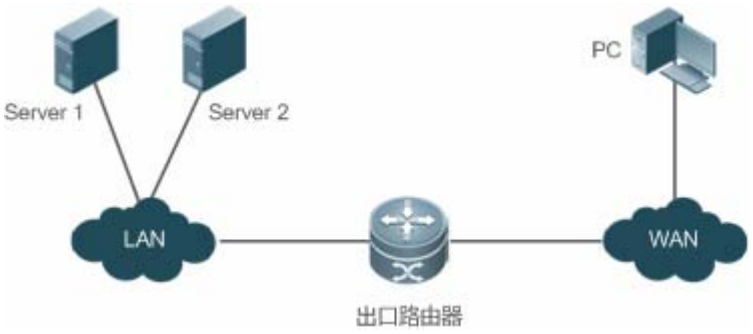
【使用指导】 -

配置举例

外网用户访问内网服务器

【网络环境】

图 9-8



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置内部动态目的地址转换规则

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 10.10.10.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
```

```
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.198.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool realhosts 10.10.10.2 10.10.10.3 netmask 255.255.255.0 type rotary
A(config)# ip nat inside destination list 100 pool realhosts
A(config)# access-list 100 permit ip any host 10.10.10.100
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global   Inside local    Outside local           Outside global
tcp 10.10.10.100:23 10.10.10.2:23   100.100.100.100:1178 100.100.100.100:1178
tcp 10.10.10.100:23 10.10.10.3:23   200.200.200.200:1024 200.200.200.200:1024
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。注意 ACL 必须配置为匹配目标 IP 的扩展 ACL。
- 以上配置，只对 TCP 流量产生作用，对其它流量保持不变，除非有另外的 NAT 配置

9.4.5 配置 ALG

配置效果

通常情况下，NAT 只对报文头中的 IP 地址和端口信息进行转换，不对应用层数据载荷中的字段进行分析。然而一些特殊协议，比如 ftp/dns/tftp 等，它们报文的数据载荷中可能包含 IP 地址或端口信息，这些内容不能被 NAT 进行有效的转换，就可能导致问题。而 NAT ALG 技术能对多通道协议进行应用层报文信息的解析和地址转换，将载荷中需要进行地址转换的 IP 地址和端口或者需特殊处理的字段进行相应的转换和处理，从而保证应用层通信的正确性。

注意事项

- 配置 ALG，必须配置至少一个 inside 接口和一个 outside 接口。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

↘ 配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的 lan 接口下配置为 NAT inside 口。

配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的 wan 接口下配置为 NAT outside 口。

配置静态 NAT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，，应在全局配置模式下配置静态 NAT 地址转换。

配置动态 NAT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络，应在全局配置模式下配置动态 NAT 地址转换。

配置 ALG

- 可选配置。
- 若环境中存在 dns、ftp、tftp、pptp、h323、rtsp 协议需要穿透 NAT 进行通信，则需要配置。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAT 地址转换

【命令格式】 **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*]

【参数说明】 *local-address*：内部地址

global-address：外部地址

permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机

netmask *mask*：网段到网段地址

match *interface*：指定出接口

【命令模式】 全局配置模式

【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 -

配置动态 NAT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* **pool** *address-pool*

【参数说明】 *access-list-number*：acl 号。

pool *address-pool*：地址池名字。

【命令模式】 全局模式

【使用指导】 -

配置 ALG

【命令格式】 **ip nat translation** { **dns** [**ttl** *ttl_time*] **| ftp** [**port** *port_num*] **| tftp | pptp | h323 | rtsp** }

【参数说明】 ttl：定义 DNS 应用的 UDP 连接转换记录的超时时间。默认是 0。

port_num：定义支持 ftp 应用的端口号，默认是 21。

【命令模式】 全局模式

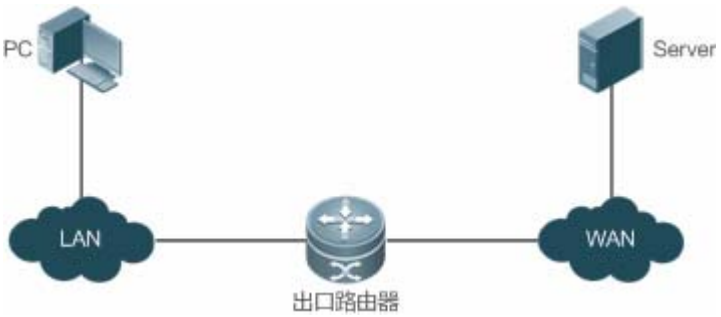
【使用指导】 -

配置举例

内网用户访问外网服务器

【网络环境】

图 9-9



【配置方法】
- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 nat 转换规则
- 配置 ALG

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.100 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat translation ftp 23
```

【检验方法】 显示检验。

A

```
Ruijie# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
tcp 200.168.12.200:2063 192.168.12.65:2063 168.168.12.1:23 168.168.12.1:23
```

常见错误

- Inside/outside 口没配置。
- acl 配置不对。

9.4.6 配置 NAT 特殊应用

配置效果

在一些 NAT 的高级应用场合，需要修改一些特定的 IP 报文源地址或者目的地址。

注意事项

- 配置 NAT 特殊应用，必须配置至少一个 inside 接口和一个 outside 接口。
- 新配置的 NAT 规则，只影响新流，对旧流不影响。

配置方法

配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的 lan 接口下配置为 NAT inside 口。

配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的 wan 接口下配置为 NAT outside 口。

配置静态 NAT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，，应在全局配置模式下配置静态 NAT 地址转换。

配置动态 NAT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络，应在全局配置模式下配置动态 NAT 地址转换。

配置 NAT 特殊应用

- 可选配置。
- 若某些应用需要做特殊的地址转换才能进行通信，则需要配置。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAT 地址转换

【命令格式】 **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*]

[**match** *interface*]

【参数说明】 *local-address*：内部地址

global-address：外部地址

permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机

netmask *mask*：网段到网段地址

match *interface*：指定出接口

【命令模式】 全局配置模式

【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 -

配置动态 NAT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* **pool** *address-pool*

【参数说明】 *access-list-number*：acl 号。

pool *address-pool*：地址池名字。

【命令模式】 全局模式

【使用指导】 -

配置 NAT 特殊应用

【命令格式】 **ip nat application source list** *list-num* **destination** *dest-ip* { **dest-change** *ip-addr* | **src-change** *ip-addr* }

【参数说明】 *local-address*：内部地址

global-address：外部地址

permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机

netmask *mask*：网段到网段地址

match *interface*：指定出接口

【命令模式】 全局配置模式

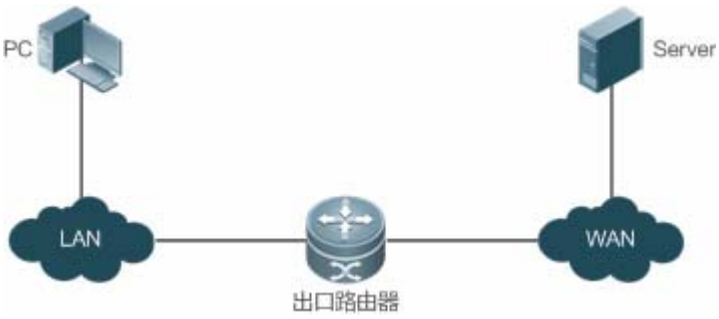
【使用指导】 -

配置举例

实现域名解析中继服务

【网络环境】

图 9-10



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 nat 转换规则
- 配置 NAT 特殊应用

A

```
A#configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1.)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat application source list 1 destination udp 192.168.1.1 53 dest-change 202.101.98.55
53
A(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

【检验方法】 -

常见错误

- Inside/outside 口没配置。

9.4.7 配置 NAT 发送免费 ARP 间隔

配置效果

开启 NAT 地址池中的地址发送免费 ARP 报文的间隔，以防止地址冲突

注意事项

NAT 发送免费 ARP 功能默认关闭。

免费 ARP 的发送仅向外网口方向发送。

配置方法

↘ 配置 NAT inside 口

- 必须配置。
- 若无特殊要求，应在连接内网的 lan 接口下配置为 NAT inside 口。

↘ 配置 NAT outside 口

- 必须配置。
- 若无特殊要求，应在连接外网的 wan 接口下配置为 NAT outside 口。

↘ 配置静态 NAT 地址转换

- 可选配置。
- 若内部网络存在少量固定用户访问外部网络时，，应在全局配置模式下配置静态 NAT 地址转换。

↘ 配置动态 NAT 地址转换

- 可选配置。
- 若内部网络存在大量用户需要访问外部网络，应在全局配置模式下配置动态 NAT 地址转换。

↘ 配置 NAT 发送免费 ARP 间隔

- 可选配置。
- NAT 需要对部分配置规则内的地址当成本机地址，为了防止地址冲突，则需要配置。

检验方法

无

相关命令

配置 NAT 内外网口

【命令格式】 **ip nat** { **inside | outside** }

【参数说明】 **inside**：内网口

outside：外网口

【命令模式】 接口模式

【使用指导】 数据包只有在 outside 接口和 inside 接口之间路由时，并且符合一定规则的，才会进行 NAT 转换。因此路由器必须配置至少一个 inside 接口和一个 outside 接口。

配置静态 NAT 地址转换

【命令格式】 **ip nat inside source static** *local-address global-address* [**permit-inside**] [**netmask** *mask*] [**match** *interface*]

【参数说明】 *local-address*：内部地址

global-address：外部地址

permit-inside：用于允许内网用户以 global-ip 访问 local-ip 的主机

netmask *mask*：网段到网段地址

match *interface*：指定出接口

【命令模式】 全局配置模式

【使用指导】 -

配置地址池

【命令格式】 **ip nat pool** *address-pool start-address end-address* { **netmask** *mask* | **prefix-length** *prefix-length* }

【参数说明】 *address-pool*：地址池名字

start-address：起始 IP 地址

end-address：结束 IP 地址

netmask *mask*：地址网络掩码

prefix-length *prefix-length*：地址网络掩码长度

【命令模式】 全局配置模式

【使用指导】 -

配置动态 NAT 地址转换

【命令格式】 **ip nat inside source list** *access-list-number* **pool** *address-pool*

【参数说明】 *access-list-number*：acl 号。

pool *address-pool*：地址池名字。

【命令模式】 全局模式

【使用指导】 -

配置 NAT 发送免费 ARP 间隔

【命令格式】 **ip nat keepalive** [*keealive_out*]

【参数说明】 *keealive_out*：发送 nat 本机地址免费 arp 报文的间隔

【命令模式】 全局配置模式

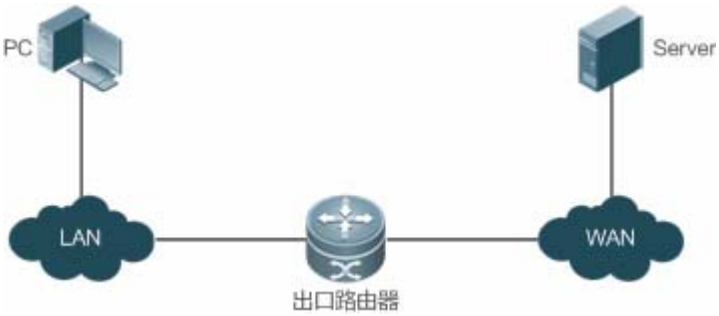
【使用指导】 -

配置举例

实现发送免费 ARP 间隔

【网络环境】

图 9-11



【配置方法】

- 在内网口配置 ip nat inside
- 在外网口配置 ip nat outside
- 配置动态 nat 转换规则
- 配置定时发送免费 ARP

A

```
A#configure terminal
A(config)# interface GigabitEthernet 0/0
A(config-if-GigabitEthernet 0/0)# ip address 192.168.1.1 255.255.255.0
A(config-if-GigabitEthernet 0/0)# ip nat inside
A(config-if-GigabitEthernet 0/0)# exit
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 200.168.12.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# ip nat outside
A(config-if-GigabitEthernet 0/1.)# exit
A(config)# ip nat pool net200 200.168.12.2 200.168.12.10 netmask 255.255.255.0
A(config)# ip nat inside source list 1 pool net200
A(config)# access-list 1 permit 192.168.12.0 0.0.0.255
A(config)# ip nat keepalive 10
```

【检验方法】 -

常见错误

- Inside/outside 口没配置。
- 未配置正确的 NAT 转换规则。

9.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 NAT 转换记录	**show ip nat translations** [*dv_id*] [*slot_id*] [*acl_num*] [**icmp** | **tcp** | **udp**] [**verbose**]

查看调试信息

无

配置指南-IP 路由

本分册介绍 IP 路由配置指南相关内容，包括以下章节：

1. 路由管理
2. FPM

1 路由管理

1.1 概述

路由管理负责管理路由表，整合各种路由协议下发的路由，进行优选，并下发给转发表。路由表中保存了各种路由协议发现的路由，根据来源不同，通常分为以下三类：

- 直连路由：链路层协议发现的路由，也称为接口路由。
- 静态路由：网络管理员手工配置的。静态路由配置方便，对系统要求低，适用于拓扑结构简单并且稳定的小型网络。其缺点是每当网络拓扑结构发生变化，都需要手工重新配置，不能自动适应。
- 动态路由：动态路由协议发现的路由。

下文仅介绍路由表管理和静态路由的相关内容。

协议规范

无

1.2 典型应用

典型应用	场景描述
静态路由基本功能	手工方式配置路由
静态浮动路由	多路径情况下，配置备份路由
静态负载分担路由	多路径情况下，配置负载分担

1.2.1 静态路由基本功能

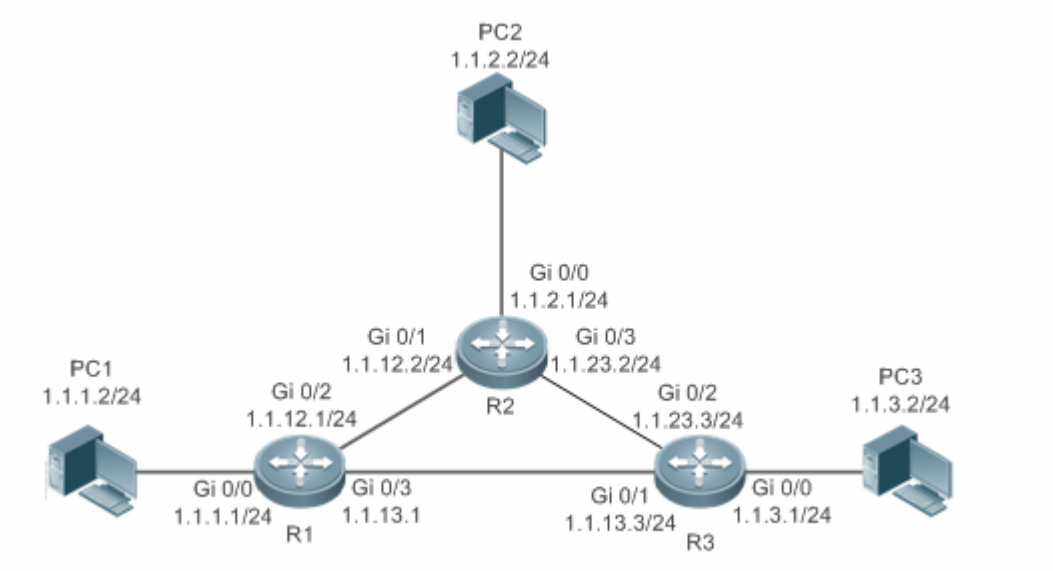
应用场景

在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。

以下图为例，为了使得 PC1，PC2，PC3 互通，可以在 R1，R2，R3 上配置静态路由。

- 在 R1 上配置到达 PC2 网段的路由走 R2，配置到达 PC3 网段的路由走 R3
- 在 R2 上配置到达 PC1 网段的路由走 R1，配置到达 PC3 网段的路由走 R3
- 在 R3 上配置到达 PC1 网段的路由走 R1，配置到达 PC2 网段的路由走 R2

图 1-1



功能部属

- 配置各接口的地址和掩码。
- 在 R1，R2，R3 上配置静态路由。

1.2.2 静态浮动路由

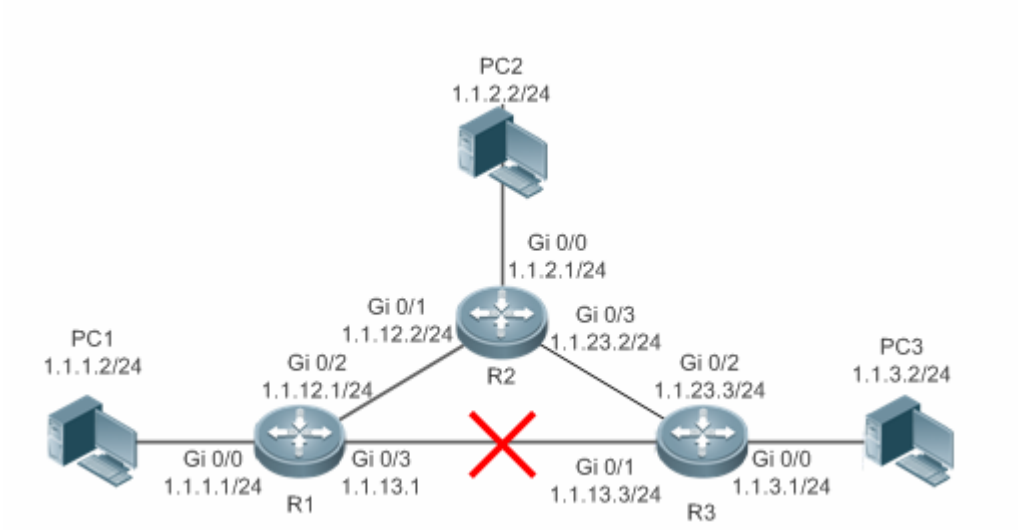
应用场景

在没有配置动态路由协议的情况下，为了避免网络线路故障导致的通信中断，可以配置静态浮动路由，实现路由的动态切换。

以下图为例，为避免 R1 与 R3 间线路故障导致的通信中断，可以在 R1 和 R3 上配置静态浮动路由。正常情况下，报文走管理距离（distance）小的路径，当该路由的链路出现故障 down 掉时，路由自动切换到管理距离大的路径。

- R1 上配置 2 条到达 PC3 网段的路由，一条走 R3（默认 distance=1），另一条走 R2（distance=2）。
- R3 上配置 2 条到达 PC1 网段的路由，一条走 R1（默认 distance=1），另一条走 R2（distance=2）。。

图 1-2



功能部属

- 配置各接口的地址和掩码。
- 在 R1，R2，R3 上配置静态路由。

1.2.3 静态负载分担路由

应用场景

在存在多条路径到达同一个目的的情况下，可以配置负载分担路由。与浮动路由不同的是，多条路由的管理距离（distance）相同。报文根据均衡转发策略在多条路由间分流。

以下图为例，在 R1，R3 上配置负载分担路由，使得到达 PC3 和 PC1 网段的报文，在 R2，R4 两条路径间均衡。

- 在 R1 上配置 2 条到达 PC3 网段的路由，一条走 R2，一条走 R4
- 在 R3 上配置 2 条到达 PC1 网段的路由，一条走 R2，一条走 R4

图 1-3

功能部属

- 配置各接口的地址和掩码。
- 在 R1，R2，R3，R4 上配置静态路由。
- 在 R1，R3 上配置负载分担策略。

1.3 功能详解

功能特性	作用
路由计算	在设备上产生可效的路由。
路由优选	在设备选择最优路由，以供报文转发。
缺省路由	使所有报文得以转发，且有助于缩小路由表规模。

1.3.1 路由计算

路由功能

路由功能分 IPv4 路由功能和 IPv6 路由功能。若关闭了路由功能，则设备相当于一台主机，不具备路由转发功能。

动态路由

动态路由协议以邻居间交换路由的方式学习远方的路由、并保持动态更新。如果邻居失效，则下一跳为此邻居的路由随之失效。

静态路由

在组网结构比较简单的网络中，只需配置静态路由就可以实现网络互通。恰当地设置和使用静态路由可以改善网络的性能，并可为重要的网络应用保证带宽。

静态路由根据本地接口的状态计算路由的活动性。当静态路由的出口处于三层 up 状态（链路状态为 up，且配置有 IP 地址）时，该路由为活动的，可以指导转发。

1.3.2 路由优选

管理距离

当多个路由协议产生了到达同一个目的地址的路由时，根据管理距离判断这些路由的优先级。管理距离越小，优先级越高。

等价路由

到达同一个目的地址，下一跳不同，管理距离相同的多条路由，则形成等价路由。报文根据均衡转发策略在多条路由间分流，从而实现负载分担。

具体设备上，对等价路由中包括的路由条目数是有限制的，超出限制的路由不会参与转发。

浮动路由

到达同一目的地址，下一跳不同，管理距离不同的多条路由，形成浮动路由。管理距离小的优先被选择参与转发，若管理距离小的路由失效，则管理距离大的路由替代管理距离小的路由参与转发，从而达到避免网络线路故障导致的通信中断。

1.3.3 缺省路由

在转发路由表中，目的网段 0.0.0.0 掩码 0.0.0.0 的路由，就是缺省路由。无法被其他路由转发的报文，可以被缺省路由转发出去。缺省路由可以静态配置，也可以由动态路由协议生成。

静态缺省路由

三层设备通过配置网段 0.0.0.0 掩码 0.0.0.0 的静态路由来生成缺省路由。

缺省网络

配置缺省网络的目的是为了产生缺省路由，当在设备上使用 **ip default-network** 指定一个网络(必须为 A 类，B 类，C 类的有类网络) 时，这个网络如果在路由表中存在，则路由设备会将该网络作为缺省网络，该网络的下一跳成为缺省网关。因为 **ip default-network** 是有类的，如果使用该命令标记一个主类网络的某个子网，路由设备会自动生成一条主类网络的静态路由而不会产生任何缺省路由。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置静态路由	⚠ 必须配置。用于配置静态路由条目。	
	ip route	配置静态 IPv4 路由
	ipv6 route	配置静态 IPv6 路由
配置缺省路由	⚠ 可选配置。用于配置缺省网关。	
	ip default gateway	二层设备配置 IPv4 缺省网关
	ipv6 default gateway	二层设备配置 IPv6 缺省网关
	ip route 0.0.0.0 0.0.0.0 *gateway*	三层设备配置 IPv4 缺省网关
	ipv6 route ::/0 *ipv6-gateway*	三层设备配置 IPv6 缺省网关
	ip default network	三层设备配置 IPv4 缺省网络
配置路由限制	⚠ 可选配置。用于限制等价路由的条数，静态路由的条数和限制路由。	
	maximum-paths	配置等价路由条数限制
	ip static route-limit	配置静态 IPv4 路由限制
	ipv6 static route-limit	配置静态 IPv6 路由限制
	no ip routing	配置禁止 IPv4 路由
	no ipv6 unicast-routing	配置禁止 IPv6 路由

1.4.1 配置静态路由

配置效果

路由表中生成一条静态路由。使用静态路由，转发去远端网络的报文。

注意事项

- 三层设备若配置了 **no ip routing**，则不能配置 IPv4 静态路由，之前已经存在的 IPv4 静态路由也会被删除。在未重启的情况下，重新配置 **ip routing**，可以恢复被清空的 IPv4 静态路由。重启过后，则无法恢复这些 IPv4 静态路由。
- 三层设备若配置了 **no ipv6 unicast- routing**，则不能配置 IPv6 静态路由，之前已经存在的 IPv6 静态路由也会被删除。在未重启的情况下，重新配置 **ipv6 unicast- routing**，可以恢复被清空的 IPv6 静态路由。重启过后，则无法恢复这些 IPv6 静态路由。

配置方法

↘ 配置 IPv4 静态路由

在支持 IPv4 的设备上，配置如下命令。

【命令格式】 **ip route** *network net-mask* { *ip-address* | *interface* [*ip-address*] **} [** *distance*] [**tag** *tag*] [**permanent**] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**] [**global**]

【参数说明】

network	目标网络的网络地址
net-mask	目标网络的掩码
ip-address	（可选）静态路由的下一跳地址。ip-address 和 interface 至少要指定一个，或者两者都指定。当未指定 ip-address 时，表示配置静态直连路由。
interface	（可选）静态路由的下一跳出口。ip-address 和 interface 至少要指定一个，或者两者都指定。当未指定 interface 时，表示配置静态递归路由，出口由下一跳在路由表中选路获得。
distance	（可选）静态路由的管理距离，缺省为 1。
tag	（可选）静态路由的 Tag 值，缺省为 0。
permanent	（可选）永久路由标识，缺省为非永久路由。
weight *number*	（可选）静态路由的权重值，缺省为 1。
description *description-text*	（可选）静态路由描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符串。
disabled/enabled	（可选）静态路由的使能标识，缺省为 enabled。
global	（可选）显示指定下一跳属于全局路由表，缺省下一跳也是属于全局路由表。

【缺省配置】 没配置静态路由

【命令模式】 全局模式

【使用指导】 此命令的最简配置：**ip route** *network net-mask ip-address*

↘ 配置 IPv6 静态路由

在支持 IPv6 的设备上，配置如下命令。

【命令格式】 **ipv6 route** *ipv6-prefix* / *prefix-length* { *ipv6-address*] | *interface* [*ipv6-address*]] } [*distance*] [**weight** *number*] [**description** *description-text*]

【参数说明】

ipv6-prefix	IPv6 前缀，必须遵循 RFC4291 的地址表示形式。
prefix-length	IPv6 前缀的长度，注意前面必须加上'/'
Ipv6-address	（可选）静态路由的下一跳地址。ipv6-address 和 interface 至少要指定一个，或者两者都指定。当未指定 ipv6-address 时，表示配置静态直连路由。
interface	（可选）静态路由的下一跳出口。ipv6-address 和 interface 至少要指定一个，或者两者都指定。当未指定 interface 时，表示配置静态递归路由，出口由下一跳在路由表中选路获得。
distance	（可选）静态路由的管理距离，缺省为 1。
weight *number*	（可选）静态路由的权重值，在配置等价路径时指明该路径的权重。配置范围：1-8，一条路由的所有等价路径的权重之和不能超过该条路由所能配置的最大等价路径条目数，同一条路由的等价路径之间的权重比指明了这些路径之间的流量比率关系。缺省为 1。
description *description-text*	（可选）静态路由描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符串。

【缺省配置】 没配置静态路由

【命令模式】 全局模式

【使用指导】 此命令的最简配置：**ipv6 route** *ipv6-prefix* / *prefix-length ipv6-address*

检验方法

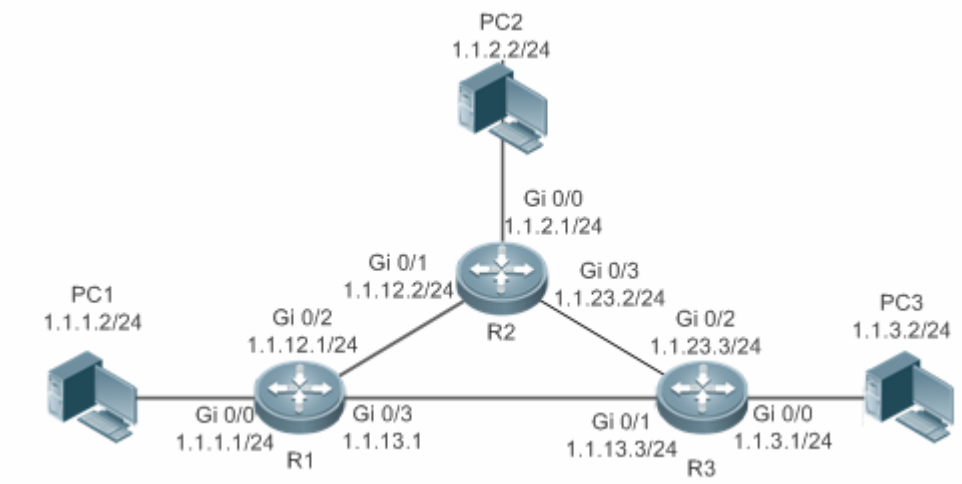
- 使用 **show ip route** 命令查看 IPv4 路由表，检查之前配置的 IPv4 静态路由是否生效。
- 使用 **show ipv6 route** 命令查看 IPv6 路由表，检查之前配置的 IPv6 静态路由是否生效。

配置举例

↘ 在 IPv4 网络上，配置静态路由使网络联通

【网络环境】

图 1-4



【配置方法】

- 在设备各接口上配置地址

R1

```
R1# configure terminal
R1(config)#interface gigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/2
R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/3
R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0
```

R2

```
R2# configure terminal
R2(config)#interface gigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)#interface gigabitEthernet 0/1
R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)#interface gigabitEthernet 0/3
R2(config-if-GigabitEthernet 0/3)# ip address 1.1.23.2 255.255.255.0
```

R3

```
R3# configure terminal
```

```
R3(config)#interface gigabitEthernet 0/0
R3(config-if-GigabitEthernet 0/0)# ip address 1.1.3.1 255.255.255.0
R3(config-if-GigabitEthernet 0/0)# exit
R3(config)#interface gigabitEthernet 0/1
R3(config-if-GigabitEthernet 0/1)# ip address 1.1.13.3 255.255.255.0
R3(config-if-GigabitEthernet 0/0)# exit
R3(config)#interface gigabitEthernet 0/2
R3(config-if-GigabitEthernet 0/2)# ip address 1.1.23.3 255.255.255.0
```

- 在设备上配置静态路由

R1

```
R1# configure terminal
R1(config)# ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.12.2
R1(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3
```

R2

```
R2# configure terminal
R2(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.1
R2(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.23.3
```

R3

```
R3# configure terminal
R3(config)# ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.23.2
R3(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.13.1
```

【检验方法】 显示路由表

R1

```
R1# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is no set
C     1.1.1.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.1.1/32 is local host.
S     1.1.2.0/24 [1/0] via 1.1.12.2, GigabitEthernet 0/2
S     1.1.3.0/24 [1/0] via 1.1.13.3, GigabitEthernet 0/2
C     1.1.12.0/24 is directly connected, GigabitEthernet 0/2
C     1.1.12.1/32 is local host.
C     1.1.13.0/24 is directly connected, GigabitEthernet 0/3
C     1.1.13.1/32 is local host.
```

R2

```
R2# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is no set
S     1.1.1.0/24 [1/0] via 1.1.12.1, GigabitEthernet 0/0
C     1.1.2.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.2.1/32 is local host.
S     1.1.3.0/24 [1/0] via 1.1.23.3, GigabitEthernet 0/3
C     1.1.12.0/24 is directly connected, GigabitEthernet 0/1
C     1.1.12.2/32 is local host.
C     1.1.23.0/24 is directly connected, GigabitEthernet 0/3
C     1.1.23.2/32 is local host.
```

R3

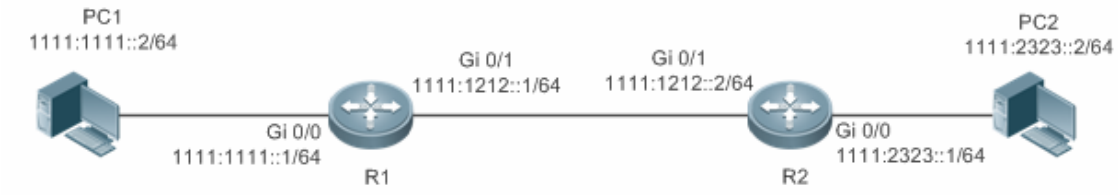
```
R3# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is no set
S     1.1.1.0/24 [1/0] via 1.1.13.1, GigabitEthernet 0/2
S     1.1.2.0/24 [1/0] via 1.1.23.2, GigabitEthernet 0/2
C     1.1.3.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.3.1/32 is local host.
C     1.1.13.0/24 is directly connected, GigabitEthernet 0/1
C     1.1.13.3/32 is local host.
C     1.1.23.0/24 is directly connected, GigabitEthernet 0/2
C     1.1.23.3/32 is local host.
```

↘ 在 IPv6 网络上，配置静态路由使网络联通

【网络环境】

图 1-5



【配置方法】

- 在设备各接口上配置地址

R1

```
R1# configure terminal
```

```
R1(config)#interface gigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)# ipv6 address 1111:1111::1/64
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/1
R1(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::1/64
```

R2

```
R2# configure terminal
R2(config)#interface gigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)#ipv6 address 1111:2323::1/64
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)#interface gigabitEthernet 0/1
R2(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::2/64
```

- 在设备上配置静态路由

R1

```
R1# configure terminal
R1(config)# ipv6 route 1111:2323::0/64 gigabitEthernet 0/1
```

R2

```
R2# configure terminal
R2(config)# ipv6 route 1111:1111::0/64 gigabitEthernet 0/1
```

【检验方法】 显示路由表

R1

```
R1# show ipv6 route

IPv6 routing table name - Default - 10 entries
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

C       1111:1111::/64 via GigabitEthernet 0/0, directly connected
L       1111:1111::1/128 via GigabitEthernet 0/0, local host
C       1111:1212::/64 via GigabitEthernet 0/1, directly connected
L       1111:1212::1/128 via GigabitEthernet 0/1, local host
S       1111:2323::/64 [1/0] via GigabitEthernet 0/1, directly connected
C       FE80::/10 via ::1, Null0
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host
C       FE80::/64 via GigabitEthernet 0/1, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
```

R2

```
R2# show ipv6 route

IPv6 routing table name - Default - 10 entries
```

```
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area

C       1111:2323::/64 via GigabitEthernet 0/0, directly connected
L       1111:2323::1/128 via GigabitEthernet 0/0, local host
C       1111:1212::/64 via GigabitEthernet 0/1, directly connected
L       1111:1212::1/128 via GigabitEthernet 0/1, local host
S       1111:1111::/64 [1/0] via GigabitEthernet 0/1, directly connected
C       FE80::/10 via ::1, Null0
C       FE80::/64 via GigabitEthernet 0/0, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host
C       FE80::/64 via GigabitEthernet 0/1, directly connected
L       FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
```

常见错误

- 接口链路没有 up
- 接口没有配置地址

1.4.2 静态配置缺省路由

配置效果

路由表中生成一条缺省路由。不能被其他路由转发的报文，使用缺省路由转发。

注意事项

- 三层设备可以通过 **ip route** 0.0.0.0 0.0.0.0 *gateway* 和 **ipv6 route** ::/0 *ipv6-gateway* 命令配置网关。

配置方法

↘ 三层设备配置 IPv4 缺省网关

【命令格式】 **ip route 0.0.0.0 0.0.0.0** { *ip-address* | *interface* [*ip-address*] } [*distance*] [**tag** *tag*] [**permanent**] [**weight** *number*] [**description** *description-text*] [**disabled** | **enabled**] [**global**]

【参数说明】		
	0.0.0.0	目标网络的网络地址

0.0.0.0	目标网络的掩码
ip-address	（可选）静态路由的下一跳地址。ip-address 和 interface 至少要指定一个，或者两者都指定。当未指定 ip-address 时，表示配置静态直连路由。
interface	（可选）静态路由的下一跳出口。ip-address 和 interface 至少要指定一个，或者两者都指定。当未指定 interface 时，表示配置静态递归路由，出口由下一跳在路由表中选路获得。
distance	（可选）静态路由的管理距离，缺省为 1。
tag	（可选）静态路由的 Tag 值，缺省为 0。
permanent	（可选）永久路由标识，缺省为非永久路由。
weight *number*	（可选）静态路由的权重值，缺省为 1。
description *description-text*	（可选）静态路由描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符串。
disabled / enabled	（可选）静态路由的使能标识，缺省为 enabled。
global	（可选）显示指定下一跳属于全局路由表，缺省下一跳也是属于全局路由表。

【缺省配置】 无静态缺省路由

【命令模式】 全局模式

【使用指导】 此命令的最简配置：**ip route 0.0.0.0 0.0.0.0** *ip-address*

三层设备配置 IPv6 缺省网关

【命令格式】 **ipv6 route ::/0** { *ipv6-address*] | *interface* [*ipv6-address*]] } [*distance*] [**weight** *number*] [**description** *description-text*]

【参数说明】

::	IPv6 前缀，必须遵循 RFC4291 的地址表示形式。
0	IPv6 前缀的长度，注意前面必须加上'/'
Ipv6-address	（可选）静态路由的下一跳地址。ipv6-address 和 interface 至少要指定一个，或者两者都指定。当未指定 ipv6-address 时，表示配置静态直连路由。
interface	（可选）静态路由的下一跳出口。ipv6-address 和 interface 至少要指定一个，或者两者都指定。当未指定 interface 时，表示配置静态递归路由，出口由下一跳在路由表中选路获得。
distance	（可选）静态路由的管理距离，缺省为 1。
weight *number*	（可选）静态路由的权重值，在配置等价路径时指明该路径的权重。配置范围：1-8，一条路由的所有等价路径的权重之和不能超过该条路由所能配置的最大等价路径条目数，同一条路由的等价路径之间的权重比指明了这些路径之间的流量比率关系。缺省为 1。
description *description-text*	（可选）静态路由描述信息，缺省无描述信息，*description-text* 为 1～60 个字符的字符串。

【缺省配置】 无静态缺省路由

【命令模式】 全局模式

【使用指导】 此命令的最简配置：**ipv6 route** ::/0 *ipv6-gateway*

三层设备配置 IPv4 缺省网络

【命令格式】 **ip default-network** *network*

【参数说明】 *network* | 网络地址（必须为 A 类，B 类，C 类的有类网络）

【缺省配置】 无缺省网络

【命令模式】 全局模式

【使用指导】 如果 **ip default-network** 指定的网络在路由表中存在，则生成一条缺省路由，以到达该网络的下一跳为缺省网关。否则不产生缺省路由。

检验方法

- 在（未关闭路由功能的）三层设备上，使用 **show ip route、show ipv6 route** 命令查看缺省路由。

配置举例

↘ 三层设备，配置 IPv4 缺省路由，使网络连通

【网络环境】

图 1-6

【配置方法】 ● 在三层设备上配置 IP 地址

R1

```
R1# configure terminal
R1(config)#interface gigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/1
R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
```

R2

```
R2# configure terminal
R2(config)#interface gigabitEthernet 0/0
R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# exit
R2(config)#interface gigabitEthernet 0/1
R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0
R2(config-if-GigabitEthernet 0/0)# exit
```

R1 ● 在三层设备 R1 上配置缺省网关

```
R1# configure terminal
R1(config)# ip route 0.0.0.0 0.0.0.0  GigabitEthernet 0/1 1.1.12.2
R2# configure terminal
```

R2

```
R2(config)# ip route 0.0.0.0 0.0.0.0  GigabitEthernet 0/1 1.1.12.1
```

【检验方法】 显示路由表

R1

```
R1# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default

Gateway of last resort is 1.1.12.2
S*    0.0.0.0/0 [1/0] via 1.1.12.2, GigabitEthernet 0/1
C     1.1.1.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.1.1/32 is local host.
C     1.1.12.0/24 is directly connected, GigabitEthernet 0/1
C     1.1.12.1/32 is local host.
```

1.4.3 配置路由限制

配置效果

限制等价路由的条数，静态路由的条数或限制路由转发

注意事项

-

配置方法

↘ 配置等价路由的条数

【命令格式】 **maximum-paths** *number*

【参数说明】 *number* | 等价路由条数，范围 1-64，实际支持范围与具体设备型号相关。

【缺省配置】 实际缺省值与具体设备型号相关。

【命令模式】 全局模式

【使用指导】 通过该命令限制等价路由中下一跳的数目。配置等价路由条数后，在负载均衡模式下，负载均衡的分路数不会超过配置的等价路由数。

↘ 配置静态 IPv4 路由限制

【命令格式】 **ip static route-limit** *number*

【参数说明】 *number* | 路由上限，范围 1-10000，缺省值 1024
【缺省配置】 允许配置的静态路由条数最大值为 IP 路由 1024 条
【命令模式】 全局模式
【使用指导】 使用此命令配置 IPV4 静态路由最大条数。超过了最大条数值后，IPV4 静态路由配置不成功。

配置静态 IPv6 路由限制

【命令格式】 **ipv6 static route-limit** *number*
【参数说明】 *number* | 路由上限，范围 1-10000，缺省值 1000
【缺省配置】 允许配置的静态路由条数最大值为 IPv6 路由 1000 条
【命令模式】 全局模式
【使用指导】 使用此命令配置 IPV6 静态路由最大条数。超过了最大条数值后，IPV6 静态路由配置不成功。

配置禁止 IPv4 路由转发

【命令格式】 **no ip routing**
【参数说明】 **-**
【缺省配置】 IP 路由功能开启
【命令模式】 全局模式
【使用指导】 使用此命令关闭 IPv6 路由。当设备只作为桥接设备，或者只作为 VOIP 网关设备时，可以不需要 RGOS 软件的 IPv4 路由转发功能。这时可以关闭 RGOS 的 IPv4 路由功能。

配置禁止 IPv6 路由

【命令格式】 **no ipv6 unicast-routing**
【参数说明】 **-**
【缺省配置】 IPv6 路由功能开启
【命令模式】 全局模式
【使用指导】 使用此命令关闭 IPv6 路由。当设备只作为桥接设备，或者只作为 VOIP 网关设备时，可以不需要 RGOS 软件的 IPv6 路由转发功能。这时可以关闭 RGOS 的 IPv6 路由功能。

检验方法

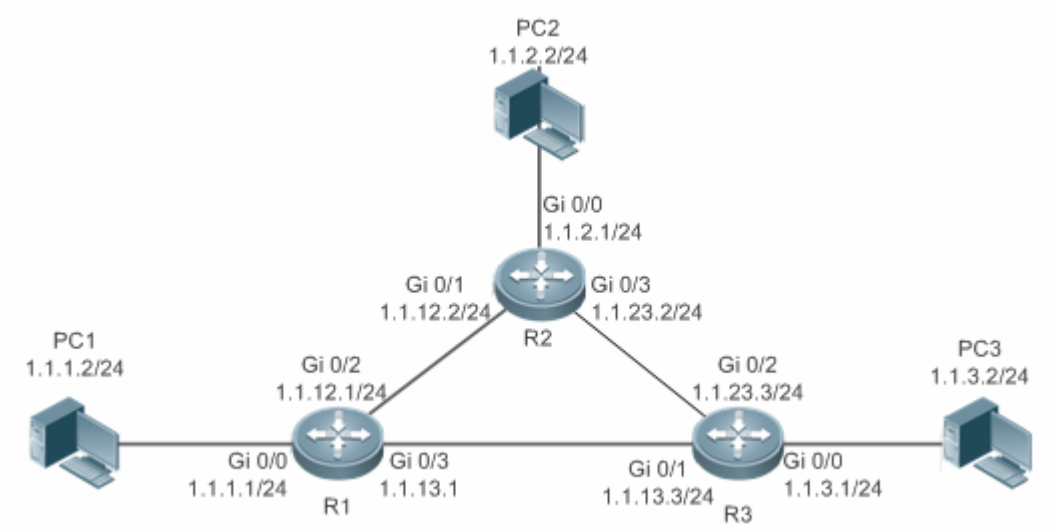
使用 **show run** 命令查看配置文件，确认存在以上配置命令。

配置举例

配置静态路由限制，不超过 2 条

【网络环境】

图 1-7



【配置方法】 在设备 R1 上配置 ip 地址、静态路由、静态路由数量限制。

```
R1# configure terminal
R1(config)#interface gigabitEthernet 0/0
R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/2
R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0
R1(config-if-GigabitEthernet 0/0)# exit
R1(config)#interface gigabitEthernet 0/3
R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0
R1(config-if-GigabitEthernet 0/3)# exit
R1(config)#ip route 1.1.3.0 255.255.255.0 1.1.13.3
R1(config)#ip route 1.1.4.0 255.255.255.0 1.1.12.2
R1(config)#ip route 1.1.5.0 255.255.255.0 1.1.12.2
R1(config)# ip static route-limit 2
% Exceeding maximum static routes limit.
```

【检验方法】 查看路由表中实际生效的静态路由。

```
R1(config)# show ip route
Codes:  C - Connected, L - Local, S - Static
        R - RIP, O - OSPF, B - BGP, I - IS-IS
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        IA - Inter area, * - candidate default
```

```
Gateway of last resort is no set
C     1.1.1.0/24 is directly connected, GigabitEthernet 0/0
C     1.1.1.1/32 is local host.
S     1.1.3.0/24 [1/0] via 1.1.13.3
S     1.1.4.0/24 [1/0] via 1.1.12.2
C     1.1.12.0/24 is directly connected, GigabitEthernet 0/2
C     1.1.12.1/32 is local host.
C     1.1.13.0/24 is directly connected, GigabitEthernet 0/3
C     1.1.13.1/32 is local host.
```

常见错误

-

1.5 监视与维护

查看运行情况

作用	命令
查看 IPv4 路由表。	**show ip route**
查看 IPv6 路由表。	**show ipv6 route**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 v4 路由管理的调试开关	**debug nsm kernel ucast- v4**
打开 v6 路由管理的调试开关	**debug nsm kernel ucast-v6**
打开缺省网络管理的调试开关	**debug nsm kernel default-network**
打开路由管理内部事件调试开关	**debug nsm events**
打开路由管理与路由协议消息发送开关	**debug nsm packet send**
打开路由管理与路由协议消息接收开关	**debug nsm packet recv**

2 FPM

2.1 概述

FPM(Flow Platform)是报文业务处理的加速平台。由于 ip 报文具有流的属性，在业务处理 ip 报文之前，FPM 为业务提供报文的流属性识别，加速业务的处理效率。FPM 是基础平台，系统启机即加载。为了实现配置和管理 FPM，特提供了本配置命令。一般情况下，FPM 的默认配置可以满足实际需求。

下文仅介绍 FPM 的相关内容。

协议规范

无

2.2 典型应用

典型应用	场景描述
配置报文接收水线	单机作为网关设备转发报文
宽松 tcp 状态检查	AS 环境，做主备切换

2.2.1 配置报文接收水线

应用场景

在一个局域网内，当设备收到大量相同 tcp 连接请求报文，这些报文由于收不到对端的响应握手报文，而不能建立合法连接，可能是存在攻击行为。通过 FPM 配置可以限制 TCP 请求连接的报文数量，有效抵抗攻击行为。

功能部属

- 在转发设备上打开严格报文状态追踪
- 配置较小的 tcp-syn-sent 状态报文水线数

2.2.2 宽松tcp状态检查

应用场景

在设备做主备切换时，为了防止期间断流，需要配置宽松 tcp 状态检查。在配置之后，一方单发 ack 报文即可以建立连接并转发报文，使切换期间连接不断开。

功能部署

- 在备份设备上配置宽松 tcp 状态检查

2.3 基本概念

↘ 流表项

流表项是设备识别和管理所有 ip 会话连接的物理资源，在其中会记录当前 ip 会话的基本信息。主要对应的协议类型是 icmp，tcp，udp，rawip 等。

2.4 功能详解

功能特性

功能特性	作用
满流时不建流直接透传	在满流时保证不断流
流老化	回收不再有效的流表项
流允许通过报文数	防止 ip 报文洪水攻击
tcp 状态跟踪	过滤 tcp 非法连接报文
严格报文状态追踪	是否做报文水线数的检查
宽松 tcp 状态检查	是否允许 ack 报文直接建立连接

2.4.1 满流时不建流直接透传

工作原理

当前的 ip 业务做加速处理时，加速逻辑依赖于流表，流表资源是依据当前产品的硬件水平做配置的，一般情况下可以满足环境的应用需求，但是在某些极端环境下，可能会出现流表资源耗尽，不能建流的情况。为了保证业务不断流，在流表满的时候，无线产品上面会不建流，直接透传报文，业务选择执行不做加速处理的逻辑。

2.4.2 流老化

工作原理

流表项的老化是指流表项在一段时间内没有数据交换，需要主动撤消该流表项。流表老化是为了避免异常会话攻击导致系统表项爆满，正常会话无法建立而实现的。不同数据类型的流表项将根据业务的实际情况设定其老化时间；不同的业务数据类型流在其处于不同状态的情况下将设置不同的老化时间。如 TCP SYN 状态流，TCP ESTABLISH 状态流的老化时间是不同的。例如网络中存在端口扫描攻击时，会占用系统比较多的流表资源，依据这些连接建立的流的状态配置合理的老化时间，可以有效回收流表，避免断流。总之配置合理的流老化时间，使得系统流表项中减少“垃圾”表项，满足业务数据流的交换。

2.4.3 流允许通过报文数

工作原理

每个流当前状态下已处理多少报文，会有一个计数，配置相应的流状态允许通过的报文数，可以有效地解决在一种报文的大流量攻击情况下，其他报文无法及时得到处理的问题，满足业务数据流的交换。

2.4.4 tcp状态变迁检查

工作原理

一个 tcp 链接的建立需要有完整的握手过程，否则就是非法连接或者攻击报文。为了能区别对待不同状态的 tcp 会话链接建立的流及判断是否是合法链接，FPM 需要对 tcp 连接进行状态跟踪。但是在一些特殊场景下，比如非对称路由，会导致不能正常做 tcp 链接的状态跟踪，需要关闭这个功能。

2.4.5 流状态报文水线检查

工作原理

当连接建立的流处于某个状态时，一个合法的连接可能通过的报文数会有一个上限，如果通过的报文数超过这个限制，可能是存在有洪水攻击，会占用系统转发资源，所以可以通过配置流状态报文水线检查，有效防御这类攻击。

2.4.6 宽松tcp状态变迁检查

工作原理

一个合法 tcp 连接的建立需要有完整的握手过程，不过在有些情况下，比如热备的切换或者其它场景下，有可能当前的 tcp 连接已经经过握手，只是当前未有对应信息，为了应对这样的情况，需要允许 ack 报文通过，所以 FPM 提供了宽松 tcp 状态检查的命令。

2.5 配置详解

配置项	配置建议 & 相关命令	
配置FPM的功能	⚠ 可选配置。用于管理 FPM 的功能	
	Ip session direct-trans-disable	配置满流时不建流不能直接透传报文
	ip session timeout	配置流的老化时间
	ip session threshold	配置流状态允许接收报文水线数
	ip session tcp_state-inspection-enable	配置做 tcp 的状态变迁检查
	ip session track-state-strictly	配置是否做流状态报文水线检查
	ip session tcp-loose	配置是否做宽松 tcp 的状态变迁检查

2.5.1 配置满流时不建流不能直接透传报文

配置效果

- 应对在无线产品上面开启某些特殊业务时，如 nat，其要求流平台不建流不能直接透传报文

注意事项

- 本项功能目前只在无线产品上面提供
- 系统默认满流时可以不建流直接透传报文

配置方法

- 可选配置
- 缺省情况下，是允许满流时可以不建流直接透传报文， 通过 **ip session direct-trans-disable** 关闭

【命令格式】 **ip session direct-trans-disable**
【参数说明】
【缺省配置】 缺省允许满流时可以不建流直接透传报文
【命令模式】 全局模式
【使用指导】 恢复开启状态，在相应的配置命令前加 **no** 即可

检验方法

- 通过 **show run** 查看，是否有 **ip session direct-trans-disable** 项配置，如果未有对应配置，则为系统默认的开启状态

配置举例

【网络环境】 如果需要在当前无线设备上面开启 nat 业务，nat 业务要求不建流不能直接透传 ip 报文，则需要关闭这项功能。

【配置方法】 设置设备上面关闭满流时可以不建流直接透传报文

```
Ruijie# configure terminal
Ruijie(config)# ip session direct-trans-disable
```

【检验方法】 通过 **show run** 查看，配置信息有此项 **ip session direct-trans-disable**

常见错误

-

2.5.2 配置流的老化时间

配置效果

- 可以合理利用系统流表资源，使系统流表项中减少“垃圾”表项，满足业务数据流的交换。

注意事项

- 系统初始化会有一个默认的老化时间，基本可以满足多数场景的需求，所以本配置不是必须的
- 因为系统检测到对应的流会有一定的耗时，所以实际老化时间会稍迟于配置的时间

配置方法

↘ 配置老化时间

- 可选配置
- 缺省情况下，流是按照默认时间来进行老化的，当默认的老化时间不能满足需求的时候，可以使用 **ip session timeout** 来更改对应流的老化时间，时间越大，当前流的存活时间越长。
- 在对应的转发设备上配置。

【命令格式】 **ip session timeout {icmp-closed | icmp-connected | icmp-started | rawip-closed | rawip-connected |**

rawip-established | rawip-started | tcp-close-wait | tcp-closed | tcp-established | tcp-fin-wait1 | tcp-fin-wait2 | tcp-syn-receive | tcp-syn-sent | tcp-syn-sent2 | tcp-time-wait | udp-closed | udp-started | udp-connected | udp-established} { *num* }

【参数说明】 **icmp-closed：**设置协议为 ICMP 状态为关闭的流的消亡时间，默认 10s，取值范围 5 – 60

icmp-connected：设置协议为 ICMP 状态为连接的流的消亡时间，默认 10s，取值范围 5-120

icmp-started：设置协议为 ICMP 状态为开始的流的消亡时间默认 10s，取值范围 5-120

rawip-closed：设置协议为其他 ip 协议状态为连接的流的消亡时间，默认 10s，取值范围 5 - 60

rawip-connected：设置协议为其他 ip 协议状态为连接的流的消亡时间默认 300s，取值范围 10-300

rawip-established：设置协议为其他 ip 协议状态为建立的流的消亡时间默认 300s，取值范围 10-600

rawip-started：设置协议为其他 ip 协议状态为开始的流的消亡时间默认 300s，取值范围 10-300

tcp-close-wait：设置协议为 TCP 状态为 tcp-close-wait 的流的消亡时间默认 60s，取值范围 10-120

tcp-closed：设置协议为 TCP 状态为 tcp-closed 的流的消亡时间默认 10s，取值范围 5-20

tcp-established：设置协议为 TCP 状态为 tcp-established 的流的消亡时间默认 1800s，取值范围 300-604800

tcp-fin-wait1：设置协议为 TCP 状态为 tcp-fin-wait1 的流的消亡时间默认 60s，取值范围 10-120

tcp-fin-wait2：设置协议为 TCP 状态为 tcp-fin-wait2 的流的消亡时间默认 60s，取值范围 10-120

tcp-syn-sent：设置协议为 TCP 状态为 tcp-syn-sent 的流的消亡时间默认 10s，取值范围 5-30

tcp-syn_sent2：设置协议为 TCP 状态为 tcp-syn_sent2 的流的消亡时间默认 10s，取值范围 5-30

tcp-syn-receive：设置协议为 TCP 状态为 tcp-syn-receive 的流的消亡时间默认 10s，取值范围 5-30

tcp-time-wait：设置协议为 TCP 状态为 tcp-time-wait 的流的消亡时间默认 10s，取值范围 5-60

udp-closed：设置协议为 UDP 状态为关闭的流的消亡时间，默认 10s，取值范围 5 - 60

udp-connected：设置协议为 UDP 状态为连接的流的消亡时间默认 30s，取值范围 10-300

udp-established：设置协议为 UDP 状态为建立的流的消亡时间默认 600s，取值范围 120-600

udp-started：设置协议为 UDP 状态为开始的流的消亡时间默认 10s，取值范围 10-300

num：设置的消亡时间

【缺省配置】 缺省使用默认值。

【命令模式】 全局模式

【使用指导】 恢复默认时间，在相应的配置命令前加 **no** 即可

检验方法

- 通过 **show run** 查看，是否有 **ip session timeout** 配置，如果未有对应配置，则为系统默认的老化时间

配置举例

【网络环境】 如果发现当前的转发设备上面有很多 udp established 状态的流占用大量流表，可以通过减小此状态的流的老化时间，提供老化效率。

【配置方法】 设置其 udp established 状态的流消亡时间为 120s

```
Ruijie# configure terminal
Ruijie(config)# ip session timeout udp-established 120
```

【检验方法】 检查设备上面的 udp established 状态的流的消亡时间约为 120s

通过 **show run** 查看，配置有此项：

```
ip session 1 2 timeout udp-established 120
```

则相应的状态老化时间为 120s

常见错误

-

2.5.3 配置流允许通过报文数

配置效果

- 可以有效地解决在一种报文的大流量攻击情况下，其他报文无法及时得到处理的问题，满足业务数据流的交换。

注意事项

- 系统初始化会有一个默认的允许报文数，基本可以满足多数场景的需求，所以本配置不是必须的
- 本项检查默认不开启，如果需要开启检查，需要系统有配置流状态报文水线检查

配置方法

- 可选配置。
- 缺省情况下，流是按照默认允许数来进行判断的，当默认允许通过报文数不能满足需求的时候，可以使用 **ip session threshold** 来更改对应流的允许通过报文数，数值越大，允许通过的报文越多。
- 在每台需要配置的转发设备上做相应配置。

【命令格式】 **ip session threshold** {icmp-closed | **icmp-started** | rawip-closed | **tcp-syn-sent | tcp-syn-receive** | **tcp-closed | udp-closed** } { *num* }

【参数说明】 **icmp-closed** ：设置协议为 ICMP 状态为关闭的流的报文通过数，默认 10，取值范围 1 - 2000000000

icmp-started：设置协议为 ICMP 状态为开始的流的报文通过数，默认 300，取值范围 5-2000000000

rawip-closed：**设置协议为其它 ip 协议状态为关闭的流的报文通过数，默认 10，**取值范围 1 - 2000000000

tcp-syn-sent：设置协议为 TCP 状态为 syn-send 的流的报文通过数，默认 10，取值范围 5-2000000000

tcp-syn-receive： 设置协议为 TCP 状态为 syn-receive 的流的报文通过数，默认 20，取值范围 5-2000000000

tcp-closed：设置协议为 TCP 状态为 closed 的流的报文通过数，默认 20，取值范围 5-2000000000

udp-closed：**设置协议为 UDP 状态为关闭的流的报文通过数，默认 10**，取值范围 **1 - 2000000000**

num：设置的报文通过数

【命令模式】 全局模式

【使用指导】 恢复默认允许通过报文数，在相应的配置命令前加 **no** 即可

检验方法

- **通过 show run** 查看，是否有 **ip session threshold** 配置，如果未有对应配置，则为系统默认允许通过报文数

配置举例

【网络环境】 如果网络中存在有大量的 ping 报文洪水攻击，可以配置降低 icmp-start 状态通过的报文水线数，以拒绝这类报文大量通过。

【配置方法】 设置其 **icmp-started** 状态的流报文通过数为 10

```
Ruijie# configure terminal
Ruijie(config)# ip session 1 2 threshold icmp-started 10
```

【检验方法】 检查设备上面的 icmp startd 状态的流报文允许通过数为 10

通过 **show run** 查看，配置有此项：

```
ip session  threshold icmp-started 10
```

则相应状态允许通过报文数为 10

常见错误

-

2.5.4 配置开启tcp状态变迁检查

配置效果

- 应对无线产品需要开启 tcp 状态跟踪的需求。

注意事项

- 无线产品默认关闭 tcp 状态变迁检查。

配置方法

- 可选配置
- 缺省情况下，是关闭 tcp 状态追踪的， 通过 **ip session tcp-state-inspection-enable** 开启

【命令格式】 **ip session tcp-state-inspection-enable**

【参数说明】

【缺省配置】 缺省关闭 TCP 状态跟踪

【命令模式】 全局模式

【使用指导】 恢复关闭状态，在相应的配置命令前加 **no** 即可

检验方法

- 通过 **show run** 查看，是否有 **ip session tcp-state-inspection-enable** 项配置，如果未有对应配置，则为系统默认的关闭状态

配置举例

【网络环境】 如果当前无线转发设备需要开启 tcp 状态变迁检查的功能。

【配置方法】 设置设备上面开启 tcp 的状态跟踪

```
Ruijie# configure terminal
Ruijie(config)# ip session tcp-state-inspection-enable
```

【检验方法】 通过 **show run** 查看，配置信息有此项 **ip session tcp-state-inspection-enable**

常见错误

-

2.5.5 配置流状态报文水线检查

配置效果

- 本配置主要是使能报文水线的检查及在报文不可达时关闭当前流

注意事项

-

配置方法

- 可选配置
- 可以通过 **ip session track-state-strictly** 开启严格报文状态追踪
- 如果场景需要开启报文的水线检查，例如当前存在某种报文的攻击，需要在每台转发设备上做相应配置。

【命令格式】 **ip session track-state-strictly**

【参数说明】 -

【缺省配置】 关闭严格报文状态追踪
【命令模式】 全局模式
【使用指导】 恢复默认配置，在相应的配置命令前加 no 即可

检验方法

- 通过 **show run** 查看，是否有 **ip session track-state-strictly** 项配置，如果未有对应配置，则为系统默认的关闭状态

配置举例

【网络环境】 如果当前网络环境中存在有 icmp 洪水攻击，需要做报文水线检查，则打开本配置。
【配置方法】 设置在当前转发设备上面严格报文状态追踪

```
Ruijie# configure terminal
Ruijie(config)# ip session track-state-strictly
```

【检验方法】 通过 **show run** 查看，配置信息有此项 **ip session track-state-strictly**

常见错误

-

2.5.6 配置宽松tcp状态变迁检查

配置效果

- 可以允许 ack 报文可以直接建流。

注意事项

- 默认是允许 ack 报文直接建流。
- 当前配置非必须。

配置方法

- 可选配置。
- 缺省情况下，打开宽松 tcp 状态检查的
- 如果场景需要配置，例如系统在做热备切换，需要在备机上开启本配置。

【命令格式】 **ip session tcp-loose**
【参数说明】 -

【命令模式】 全局模式

【使用指导】 恢复默认配置，在相应的配置命令前加 no 即可

检验方法

- 通过 **show run** 查看，是否有此项配置 **ip session tcp-loose**，如果未有对应配置，则为非宽松状态

配置举例

【网络环境】 当前环境需要做主备切换，需要在备份设备上面打开这项配置。

【配置方法】 设置设备上面的宽松 tcp 状态检查

```
Ruijie# configure terminal
Ruijie(config)# ip session tcp-loose
```

【检验方法】 通过 **show run** 查看，配置信息有此项 **ip session tcp-loose**

常见错误

-

2.6 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除 FPM 处理 ipv4 报文丢包计数	**clear ip fpm counters**
清除 FPM 处理 ipv6 报文丢包计数	**clear ip v6fpm counters**

查看运行情况

作用	命令
查看 FPM 处理 ipv4 报文丢包计数	**show ip fpm counters**
查看 FPM 处理 ipv6 报文丢包计数	**show ip v6fpm counters**
查看 ipv4 报文的流信息	**show ip fpm flows**
筛选查看 ipv4 报文的流信息	**show ip fpm flows filter**
查看 ipv6 报文的流信息	**show ip v6fpm flows**
筛选查看 ipv6 报文的流信息	**show ip v6fpm flows filter**
查看 ipv4 流统计信息	**show ip fpm statistics**

查看 ipv6 流统计信息	**show ip v6fpm statistics**

配置指南-安全

本分册介绍安全配置指南相关内容，包括以下章节：

1. Web 认证
2. AAA
3. RADIUS
4. 802.1x
5. ARP Check
6. 防网关 APR 欺骗
7. 全局 IP+MAC 绑定
8. DHCP Snooping
9. IP Source Guard
10. DNS SNOOPING
11. IGMP Snooping
12. ACL
13. SCC
14. PASSWORD-POLICY
15. SSH

1 Web 认证

1.1 概述

1.1.1 Web认证概述

Web 认证是一种对用户访问网络的权限进行控制的身份认证方法，这种认证方法不需要用户安装专用的客户端认证软件，使用普通的浏览器软件就可以进行身份认证。

未认证用户使用浏览器上网时，网络设备会强制浏览器访问特定站点，也就是 Web 认证服务器，通常称为 Portal 服务器。用户无需认证即可访问 Portal 服务器上的服务，比如下载安全补丁、阅读公告信息等。当用户需要访问认证服务器以外的其它网络资源时，就必须通过浏览器在 Portal 服务器上进行身份认证，只有认证通过后才可以使用网络资源。

除了认证上的便利性之外，由于 Portal 服务器和用户的浏览器有页面交互，可以利用这个特性在 Portal 服务器页面放置一些广告、通知、业务链接等个性化的服务。

锐捷 Web 认证概述

锐捷 web 认证有 3 个版本，不同版本的 Web 认证流程不同，我们将其分别称为锐捷一代 Web 认证、锐捷二代 Web 认证、锐捷内置 Portal Web 认证。细节详见功能详解章节。

⚠ 由于三个版本的 Web 证存在较大差异，配置参数也差别很大，因此在配置 Web 认证相关功能前必须仔细阅读对应章节内容，避免配置错误。

⚠ 二代Web认证和内置Portal Web认证均支持设备的本地帐号认证，但是由于RADIUS认证在实际网络部署中更为常见，因此应用举例中使用了 RADIUS 认证。

⚠ 不同产品端口的概念不一样，比如交换机的端口表示具体的物理端口，路由器则有可能是子接口，无线则可能是一个WLAN，本文统一采用术语端口，使用具体产品时再依据产品的概念找到对应的配置位置。

⚠ Web 认证支持低流量检测用户下线，具体参考 SCC 组件的配置手册。

⚠ Web认证支持域认证，也就是帐号采用"用户名@域名"的形式，该功能需要AAA开启域认证功能，详细参考AAA的配置手册。

ℹ 下文仅介绍 Web 认证的相关内容。

协议规范

- HTTP：RFC1945 RFC2068
- HTTPS：RFC2818
- SNMP： RFC1157 RFC 2578

- RADIUS： RFC2865 RFC2866 RFC3576
- 与 MAC 短信认证相关的规范参照《中国移动无线局域网（WLAN）设备接口规范 V3.1.0_20130901（MAC 认证扩展）.doc》，《浙江移动 WLAN 快速认证方案-接口规范 V1.1-2011.3.22.doc》，《基于 MAC+短信的 WLAN 快速认证方案 V1.1-2011.3.21.doc》

1.2 典型应用

典型应用	场景描述
web认证基本场景	常见的二层基本认证场景，设备、portal 服务器、RADIUS 服务器组成认证体系，用户通过二层网络连接设备

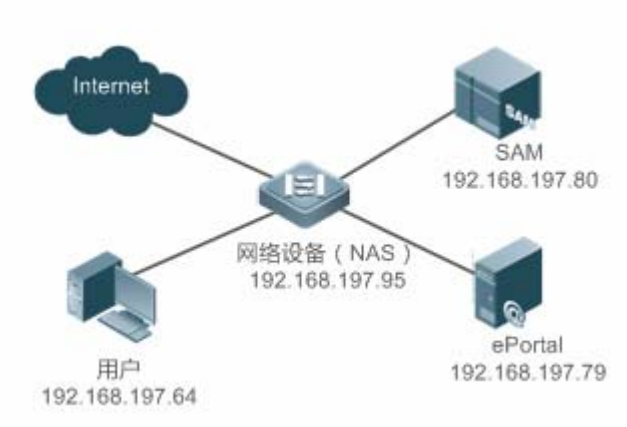
1.2.1 Web认证基本场景

应用场景

如 图 1-1 所示

- 在网络设备上部署 Web 认证方案
- 下联用户需要通过 Web 认证才能访问 internet

图 1-1 Web 认证方案网络拓扑图



【注释】 Web 认证方案可以用于二三层网络。相比于二层网络，三层网络的特点是报文经过了路由后 mac 地址和 vid 信息变了，此时对终端的唯一性识别只有ip，因此在三层设备上，web认证的绑定策略只能用仅ip模式。此处以二层接入设备为例。
RADIUS 服务器安装了锐捷 SAM 服务器软件， Portal 服务器安装了锐捷 ePortal 服务器软件。

功能部属

- 在 NAS 上用户所在端口或者全局开启 Web 认证受控(EG 设备上为全局开启)。
- 在 NAS 上配置 Web 认证服务器信息和通信加密密钥(仅一代认证和二代认证)。
- 在 NAS 上配置 Web 认证服务器 SNMP 通信参数(仅一代认证和二代认证)。
- 在 Portal 服务器和 SAM 服务器上配置两个服务器间相匹配的通信参数(仅一代 Web 认证)。
- 在 SAM 服务器上配置开通用户账户。
- 在 NAS 上配置 AAA 功能和方法列表(仅二代认证和内置认证)。
- 在 NAS 上配置 RADIUS 服务器地址(仅二代认证和内置认证)。
- 在 NAS 上配置 Web 认证方法列表名(仅二代认证和内置认证)。

1.3 功能详解

基本概念

↘ 一代 Web 认证方案

一代 Web 认证方案需要锐捷专有 ePortal 服务器软件的配合，用户通过 ePortal 软件提供的认证页面提交认证信息， ePortal 服务器直接向相应的 RADIUS 服务器请求认证，认证通过后将用户信息通过 SNMP 协议通告设备，由设备完成用户的准入控制。一代 Web 认证通过私有 SNMP 节点进行认证通信，认证记账功能由 ePortal 服务器承载，减轻了设备的业务压力。

↘ 二代 Web 认证方案

二代 Web 认证方案兼容中国移动 Portal 协议规范。Portal 服务器单纯负责用户页面交互部分，较为简单；而 RADIUS 服务器认证交互部分由设备来实现；Portal 服务器和设备间的交互遵循《中移动 portal 协议规范》。用户通过 Portal 服务器提供的认证页面提交认证信息， Portal 服务器将用户信息通过 Portal 协议告知网络设备，网络设备利用该身份信息完成 RADIUS 服务器认证，对合法用户进行准入，同时将结果信息回应给 Portal 服务器。

二代 Web 认证方案由于主要流程都是在设备上完成，对设备的要求比较高，处理能力压力大；但是 Portal 服务器得到了简化，同时使用业界支持度较高的中国移动 Portal 规范进行交互，使得各设备厂商和服务器厂商能够开发出兼容的产品。

↘ 锐捷内置 Portal Web 认证

内置 Portal Web 认证由设备集成页面交互功能，以及 RADISU 服务器认证交互部分的功能。设备默认预置了页面包，用户也可以按照配置手册中介绍的页面包定制规范制作自己的页面包并下载到设备的存储介质上生效。

↘ 锐捷各类 Web 认证的对比

认证角色：

- 客户端：功能一样。
- 网络设备：锐捷一代 Web 认证里面，设备只做重定向，以及和 Portal 服务器交互用户的上下网通知。锐捷二代 Web 认证里面，设备需要负责重定向、用户的认证、通告 Portal 服务器认证是否成功。内置 Portal Web 认证里面，设备集成重定向、页面交互、以及用户的认证等功能。

- Portal 服务器：锐捷一代 Web 认证里面，Portal 服务器负责和客户端的页面交互、用户的认证、通告网络设备用户认证是否可上网。锐捷二代 Web 认证里面，Portal 服务器负责和客户端的页面交互、通告网络设备用户的认证信息、接收网络设备通告的用户是否认证成功。锐捷内置 Web 认证中，Portal 服务器由设备内置实现，功能较为简单，主要负责页面交互过程。
- Radius 服务器：功能一样。

认证流程：

- 锐捷二代 Web 认证将认证记账从 Portal 服务器迁移到网络设备。
- 锐捷二代 Web 认证由于认证在网络设备上，因此就无需等待来自 Portal 服务器发送的用户是否可上网的通告。
- 锐捷内置 Web 认证将一二代中 Portal 服务器功能简化，并移到设备上进行支持。

下线流程

- 锐捷一代 Web 认证中，下线动作可能来自 Portal 服务器的通告或者本机的流量检测、端口状态检测。锐捷二代 Web 认证中，下线动作可能来自 Portal 服务器的通告、RADIUS 服务器的踢线通告、或者本机的流量检测、端口状态检测。锐捷内置 Portal Web 认证中，下线动作可能来自用户主动点击页面的下线按钮、RADIUS 服务器的踢线通告、或者本机的流量检测、端口状态检测。
- 锐捷一代 Web 认证中，计费结束报文是 Portal 服务器发起的。锐捷二代 Web 认证中，计费结束报文是设备发起的。锐捷内置 Portal Web 认证中，计费报文也是由设备发起。

实际网络中是部署一代 Web 认证，还是部署二代 Web 认证或内置 Web 认证，取决于所使用的 Portal 服务器的类型。

各类 Web 认证中有部分参数是可以共用，有些是不能共用的，请仔细阅读，避免参数配置不当导致 Web 认证使用不正常。

功能特性

功能特性	作用
锐捷一代Web认证	网络中部署了 Portal 服务器且 Portal 服务器仅支持一代 Web 认证
锐捷二代Web认证	网络中的部署了 Portal 服务器且 Portal 服务器兼容中移动 portal 规范
锐捷内置Portal Web认证	网络中没有部署 Portal 服务器，需要设备支持页面交互功能

1.3.1 锐捷一代Web认证

HTTP 拦截

HTTP 拦截指网络设备将原本需要转发的 HTTP 报文拦截下来，不进行转发。这些 HTTP 报文是连接在网络设备下的用户的浏览器所发出的，但目的并不是网络设备本身。例如，某用户通过 IE 浏览器访问 www.google.com，网络设备本应该将这些 HTTP 请求报文转发到网关的，但如果启动 HTTP 拦截，这些报文将不被转发。

HTTP 拦截之后，网络设备需要将用户的 HTTP 连接请求转向自己，于是网络设备和用户之间将建立起连接会话。网络设备将利用 HTTP 重定向功能，将重定向页面推送给用户，用户的浏览器上将弹出一个页面，这个页面可以是认证页面，也可以是下载软件的链接等等。

在 Web 认证功能中，哪些用户所发出的到哪个目的端口的 HTTP 报文需要进行拦截，哪些不需要，都是可以设置的。一般地，未经过认证的用户发出的 HTTP 请求报文会被拦截，已通过认证的用户将不被拦截。HTTP 拦截是 Web 认证功能的基础，一旦浏览器发出的 HTTP 报文被拦截，就会自动触发 Web 认证的过程。

HTTP 重定向

根据 HTTP 协议规定，正常情况下，用户的浏览器发出 HTTP GET 或 HEAD 请求报文后，如果接收一方能够提供资源，则以 200 报文响应，如果本地不能提供资源，则可以使用 302 报文响应。在 302 响应报文中，提供了一个新的站点路径，用户收到响应后，可以向这个新的站点重新发出 HTTP GET 或 HEAD 报文请求资源，这就是重定向。

HTTP 重定向是 Web 认证的重要环节，是发生在 HTTP 拦截之后的，利用的就是 HTTP 协议中的 302 报文的特性。HTTP 拦截过程将使得网络设备和用户之间建立起连接会话，随后用户将（本应发给其他站点的）HTTP GET 或 HEAD 报文发给网络设备，网络设备收到后，回应以 302 报文，并且在 302 报文中加入重定向页面的站点路径，这样用户将向这个站点路径重新发出请求，就会获取到重定向的页面。

由于越来越多的应用程序基于 HTTP 协议运行，采用 302 重定向报文有可能会将大量的非浏览器发出的 HTTP 流引向 Portal 服务器，影响网络认证，因此设备的重定向技术采用的是通过 js 脚本代替 302 报文，这一技术称为降噪。

工作原理

组网拓扑图同 图 1-2Web 认证方案网络拓扑图。

Web 认证的角色：

1. 认证客户端：通常是浏览器，运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
2. 网络设备：在网络拓扑中一般是接入层设备（例如在无线网络中可以是无线 AP），一般与用户终端设备直接相连接，在设备上需要启动 Web 认证功能。
3. Portal 服务器：提供 Web 认证的认证界面和相关操作。Portal 服务器接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，将此信息发送到认证服务器进行认证，然后通告用户和网络设备认证结果。图中为锐捷 ePortal 服务器。
4. Radius 服务器：提供基于 RAIUS 协议的远程用户认证，Portal 服务器从 HTTP 中获取用户的认证账号信息，然后通过 RADIUS 协议向 Radius 服务器请求认证。Radius 服务器通过 RADIUS 协议向 Portal 服务器反馈认证结果。图中为锐捷 SAM 服务器。

Web 认证的流程：

1. 在认证之前，设备将未认证用户发出的所有 HTTP 请求都拦截下来，并重定向到 Portal 服务器去，这样在用户的浏览器上将弹出一个认证页面。
2. 在认证过程中，用户在认证页面上输入认证信息（用户名、口令、校验码等等）与 Portal 服务器交互，完成身份认证的功能。
3. 在认证通过后，Portal 服务器将通知设备该用户已通过认证，设备将允许用户访问互联网资源。

详细的原理图如下图所示：(图中以 AP 为例)

图 1-2 锐捷一代 Web 认证流程图

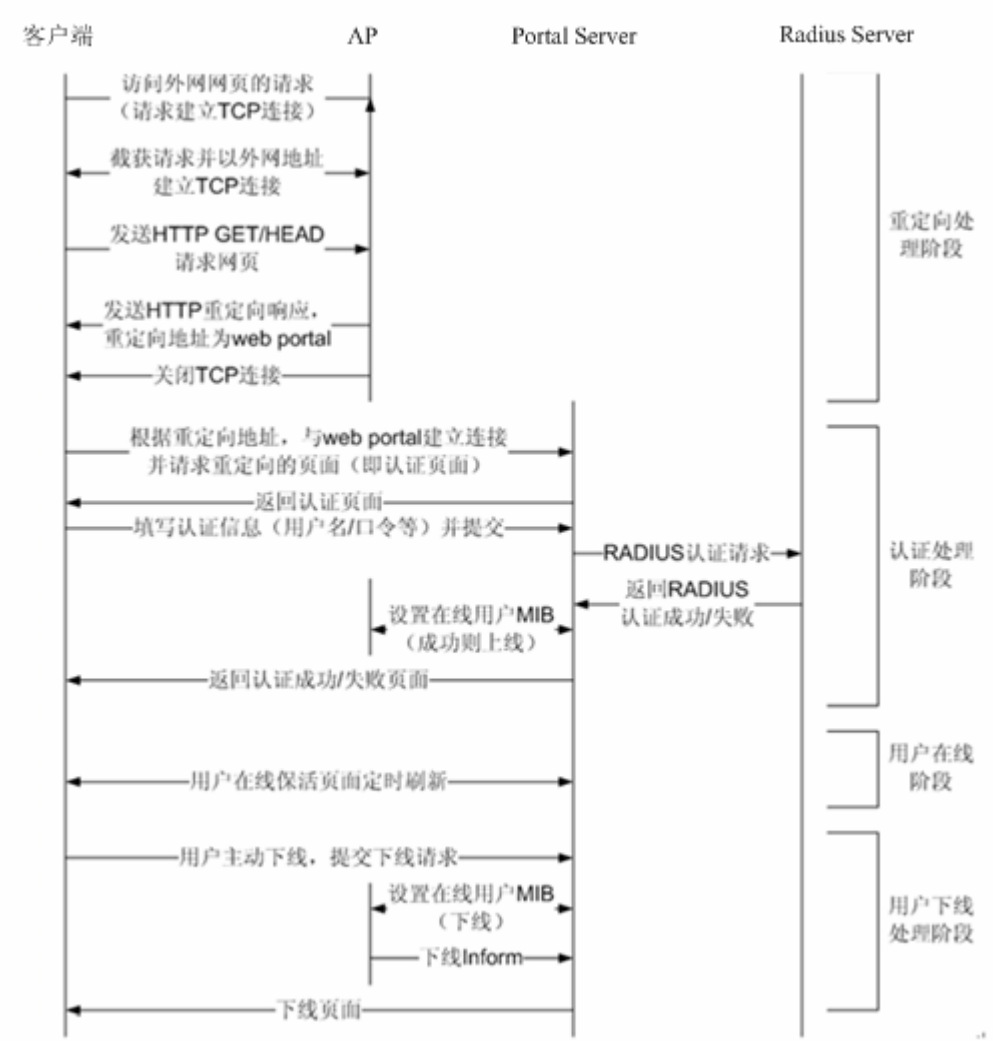


图 2

用户下线流程：

用户下线分两种类型,一种是设备端检测到用户下线,比如用户时长到达,流量用完,链路断开等;一种是 Portal 服务器端发现用户下线,比如用户通过下线页面触发了下线申请,保活页面失效等。

1. 第一种情况，设备发现用户下线时,通告 Portal 服务器用户下线，服务器设置设备删除用户信息（通过 SNMP 协议）。Portal 服务器向用户返回下线页面。
2. 第二种情况， Portal 服务器发现用户下线后,通告设备用户下线（通过 SNMP 协议）。Portal 服务器向用户返回下线页面。
3. 2 种情况下，Portal 服务器都会向 Radius 服务器发起计费结束请求，通告 Radius 服务器用户下线。

相关配置

↘ 创建配置模板

缺省情况下无配置。

在全局配置模式下使用 **web-auth template eportalv1** 命令创建模板。

可以使用该配置模板进行 web 认证功能。

配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式使用 **ip** { *ip-address* }来配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

配置服务器认证 URL

缺省情况下无配置。

在模板配置模式使用 **url** { *url-string* }来配置。

用户重定向到的 URL 地址，通常使用 portal 认证页面地址。

配置绑定模式

缺省情况下为 ip+mac 绑定。

在模板配置模式使用 **bindmode** 来配置。

对于跨三层网络认证的环境，由于经过路由后 mac 地址已经变了，需要配置为仅 ip 绑定模式。

配置通信加密密钥

缺省情况下无配置。

在全局配置模式下使用 **web-auth portal key** { *string* }来配置通信加密密钥。

用作 URL 参数加密，避免信息泄漏。

开启 web 认证

缺省情况下该功能关闭。

在接口模式下使用 **web-auth enable** 命令开启用户所在端口 web 认证受控。

开启认证后端口下未认证用户会被重定向到认证页面。

配置 web 认证 SNMP 协议服务器

缺省情况下无配置。

在全局配置模式下使用 **snmp-server host** { *ip-address* } **version 2c** { *community-string* } **web-auth** 来配置 web 认证 SNMP 协议服务器。

设备可以通过 inform/trap 报文通告用户下线消息给配置的服务器。

配置服务器 SNMP 通信团体字

缺省情况下无配置。

在全局配置模式下使用 **snmp-server community** {*community-string*} **rw** 来配置服务器 SNMP 通信团体字。

服务器通过该团体字来读写设备的用户表项信息。

↘ 启用 SNMP TRAP/INFORM 通告功能

缺省情况下无配置。

在全局配置模式下使用 **snmp-server enable traps web-auth** 来配置启用 SNMP TRAP/INFORM 通告功能。

使能通告功能，用于设备向服务器通告用户下线消息。

1.3.2 锐捷二代Web认证

HTTP 拦截

同锐捷一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同锐捷一代 Web 认证的 HTTP 重定向技术。

工作原理

组网拓扑图同 图 1-3 Web 认证方案网络拓扑图。

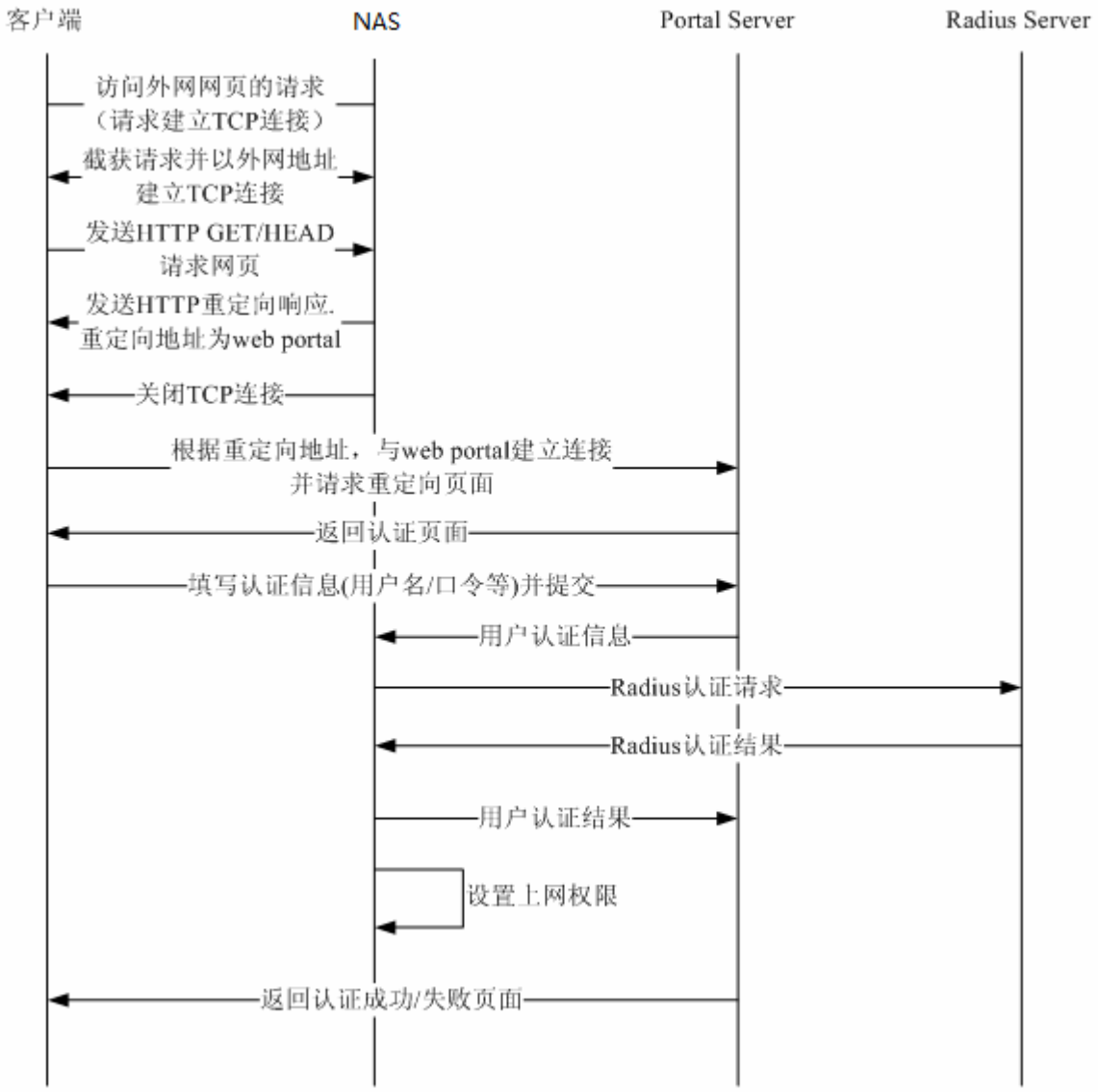
Web 认证的角色：

1. 认证客户端：通常是一个浏览器，运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
2. 网络设备：在网络拓扑中一般是接入层设备（例如在无线网络中可以是无线 AP），一般与用户终端设备直接相连接，在设备上需要启动 Web 认证功能。设备接收 Portal 服务器发过来的用户认证信息，并向 Radius 服务器发起认证请求，根据认证结果设置用户是否可以上网，同时向 Portal 服务器反馈认证结果。
3. Portal 服务器：提供 Web 认证的认证界面和相关操作。Portal 服务器接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，将此信息发送到网络设备，同时根据网络设备反馈的认证结果，通过页面反馈给用户。图中为锐捷 ePortal 服务器。
4. Radius 服务器：提供基于 RADIUS 协议的远程用户认证。图中为锐捷 SAM 服务器。

Web 认证主要流程：

1. 在认证之前，设备将未认证用户发出的所有 HTTP 请求都拦截下来，并重定向到 Portal 服务器去，这样在用户的浏览器上将弹出一个认证页面。
2. 在认证过程中，用户在认证页面上输入认证信息（用户名、口令、校验码等等）与 Portal 服务器交互。
3. Portal 服务器将用户的认证信息发给设备
4. 设备向 Radius 服务器发起认证，并将认证结果反馈给 Portal 服务器。
5. Portal 服务器向用户返回页面，提示认证结果（成功或失败）。

图 1-4 锐捷二代 Web 认证流程



用户下线流程：

用户下线分两种类型,一种是设备端检测到用户下线,比如用户时长到达,流量用完,链路断开等;一种是 portal 服务器端发现用户下线,比如用户通过下线页面触发了下线申请等。

1. 用户主动点击页面上的下线按钮，选择下线，Portal 服务器通告设备将用户下线。
2. 设备检测到终端低流量将用户下线，具体依赖所配置的低流量检测参数而定。
3. RADIUS 服务器因为某种策略原因，将用户踢线，设备通告 Portal 服务器，Portal 服务器向终端推送下线页面。

相关配置

创建配置模板

缺省情况下无配置。

在全局配置模式下使用 **web-auth template{eportalv2 |** *template-name* **v2}**命令创建二代模板。

可以使用该配置模板进行 web 认证功能。

配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式使用 **ip** { *ip-address* }来配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

配置服务器认证 URL

缺省情况下无配置。

在模板配置模式使用 **url** { *url-string* }来配置。

用户重定向到的 URL 地址，通常使用 portal 认证页面地址。

配置绑定模式

缺省情况下为 ip+mac 绑定。

在模板配置模式使用 **bindmode** 来配置。

对于跨三层网络认证的环境，由于经过路由后 mac 地址已经变了，需要配置为仅 ip 绑定模式。

配置通信加密密钥

缺省情况下无配置。

在全局配置模式下使用 **web-auth portal key** { *string* }来配置通信加密密钥。

用作 URL 参数加密，避免信息泄漏。

开启 web 认证

缺省情况下该功能关闭。

在接口模式下使用 **web-auth enable{eportalv2 |** *template-name* **v2}**命令开启用户所在端口 web 认证受控。

开启认证后端口下未认证用户会被重定向到认证页面。

配置启用 AAA 认证

缺省情况下关闭 AAA 认证。

在全局配置模式下使用 **aaa new-model** 命令来开启 AAA 认证功能。

二代 Web 认证功能需要依赖于 AAA 认证功能，使用时需要开启 AAA 功能。

配置 RADIUS 服务器和通信密钥

缺省情况下无配置。

在全局配置模式下使用 **radius-server host** 命令来配置 RADIUS 服务器和通信密钥。

对应于 web 认证中的 RADIUS 服务器。用于为 Web 认证用户进行身份校验。

↘ 配置 AAA 模块 web 认证的方法列表

缺省情况下无配置。

在全局配置模式下使用 **aaa authentication web-auth** 命令来配置二代 web 认证的认证方法。

Web 认证功能可以配置使用该方法列表来进行认证交互。

↘ 配置 AAA 模块网络记账方法列表

缺省情况下无配置。

在全局配置模式下使用 **aaa accounting network** 命令来配置网络记账方法。

Web 认证功能可以配置使用该方法列表来进行记账交互。

↘ 配置 web 认证使用的 AAA 认证方法列表名

缺省情况下使用 default 方法。

在模板配置模式下使用 **authentication** 命令来配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起认证请求。

↘ 配置 web 认证使用的 AAA 认证记账列表名

缺省情况下使用 default 方法。

在模板配置模式下使用 **accounting** 命令来配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起记账请求。

↘ 配置 portal 服务器的通信 UDP 端口号

缺省情况下使用 50100 端口号。

在模板配置模式下使用 **port** 命令来配置。

设备通过发送报文到该端口来同 portal 服务器进行交互。

1.3.3 锐捷内置Portal Web认证

HTTP 拦截

同锐捷一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同锐捷一代 Web 认证的 HTTP 重定向技术。

工作原理

相比图 1-5 Web 认证方案网络拓扑图，内置 Portal Web 认证没有 Portal 服务器。

Web 认证的角色：

1. 认证客户端：通常是一个浏览器，运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
2. 网络设备：在网络拓扑中一般是接入层设备，一般与用户终端设备直接相连接(有线或者无线)，在设备上需要启动内置 Portal Web 认证功能。由设备解析用户在页面中输入的帐号并向 Radius 服务器发起认证请求，根据认证结果设置用户是否可以上网，同时向终端浏览器推送认证结果。
3. Radius 服务器：提供基于 RADIUS 协议的远程用户认证。图中为锐捷 SAM 服务器。

Web 认证主要流程：

1. 在认证之前，设备将未认证用户发出的所有 HTTP 请求都拦截下来，并重定向到本机内置 Portal，这样在用户的浏览器上将弹出一个认证页面。
2. 在认证过程中，用户在认证页面上输入认证信息（用户名、口令、校验码等等）与内置 Portal 交互。
3. 设备向 Radius 服务器发起认证，并根据认证结果向用户返回页面，提示认证结果（成功或失败）。

用户下线流程：

1. 用户主动点击页面上的下线按钮，选择下线，设备检测到此页面动作，将用户下线。
2. 设备检测到终端低流量将用户下线，具体依赖所配置的低流量检测参数而定。
3. RADIUS 服务器因为某种策略原因，将用户踢线，设备向终端推送下线页面。

相关配置

↘ 创建配置模板

缺省情况下无配置。

在全局配置模式下使用 **web-auth template iportal** 命令创建模板。

可以使用该配置模板配置内置 Portal Web 认证相关参数。

↘ 配置页面包

缺省情况下使用设备出厂自带的页面包。

在模板配置模式使用 **page-suite** 来配置使用指定的页面包。

指定页面包之前需要先将页面包下载到 FLASH 中。

↘ 配置广告推送地址

缺省情况下无配置。

在模板配置模式使用 **popup** *url* 来配置。

该功能允许给用户推送指定页面地址。

配置广告推送方式

缺省情况认证后推送。

在模板配置模式使用 **popup mode** 来配置推送模式，有登录推送、认证后推送两种选项。

配置绑定模式

缺省情况下为 ip+mac 绑定。

在模板配置模式使用 **bindmode** 来配置。

对于跨三层网络认证的环境，由于经过路由后 mac 地址已经变了，需要配置为仅 ip 绑定模式。

开启 web 认证

缺省情况下该功能关闭。

在接口模式下使用 **web-auth enable iportal** 命令开启用户所在端口 web 认证受控。

开启认证后端口下未认证用户会被重定向到认证页面。

配置启用 AAA 认证

缺省情况下关闭 AAA 认证。

在全局配置模式下使用 **aaa new-model** 命令来开启 AAA 认证功能。

二代 Web 认证功能需要依赖于 AAA 认证功能，使用时需要开启 AAA 功能。

配置 RADIUS 服务器和通信密钥

缺省情况下无配置。

在全局配置模式下使用 **radius-server host** 命令来配置 RADIUS 服务器和通信密钥。

对应于 Web 认证中的 RADIUS 服务器，用于为 Web 认证用户进行身份校验。

配置 AAA 模块 web 认证的方法列表

缺省情况下无配置。

在全局配置模式下使用 **aaa authentication iportal** 命令来配置二代 web 认证的认证方法。

Web 认证功能可以配置使用该方法列表来进行认证交互。

配置 AAA 模块网络记账方法列表

缺省情况下无配置。

在全局配置模式下使用 **aaa accounting network** 命令来配置网络记账方法。

Web 认证功能可以配置使用该方法列表来进行记账交互

配置 web 认证使用的 AAA 认证方法列表名

缺省情况下使用 default 方法。

在模板配置模式下使用 **authentication** 命令来配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起认证请求。

↘ 配置 web 认证使用的 AAA 认证记账列表名

缺省情况下使用 default 方法。

在模板配置模式下使用 **accounting** 命令来配置。

Web 认证功能通过该方法列表名字向 AAA 功能发起记账请求。

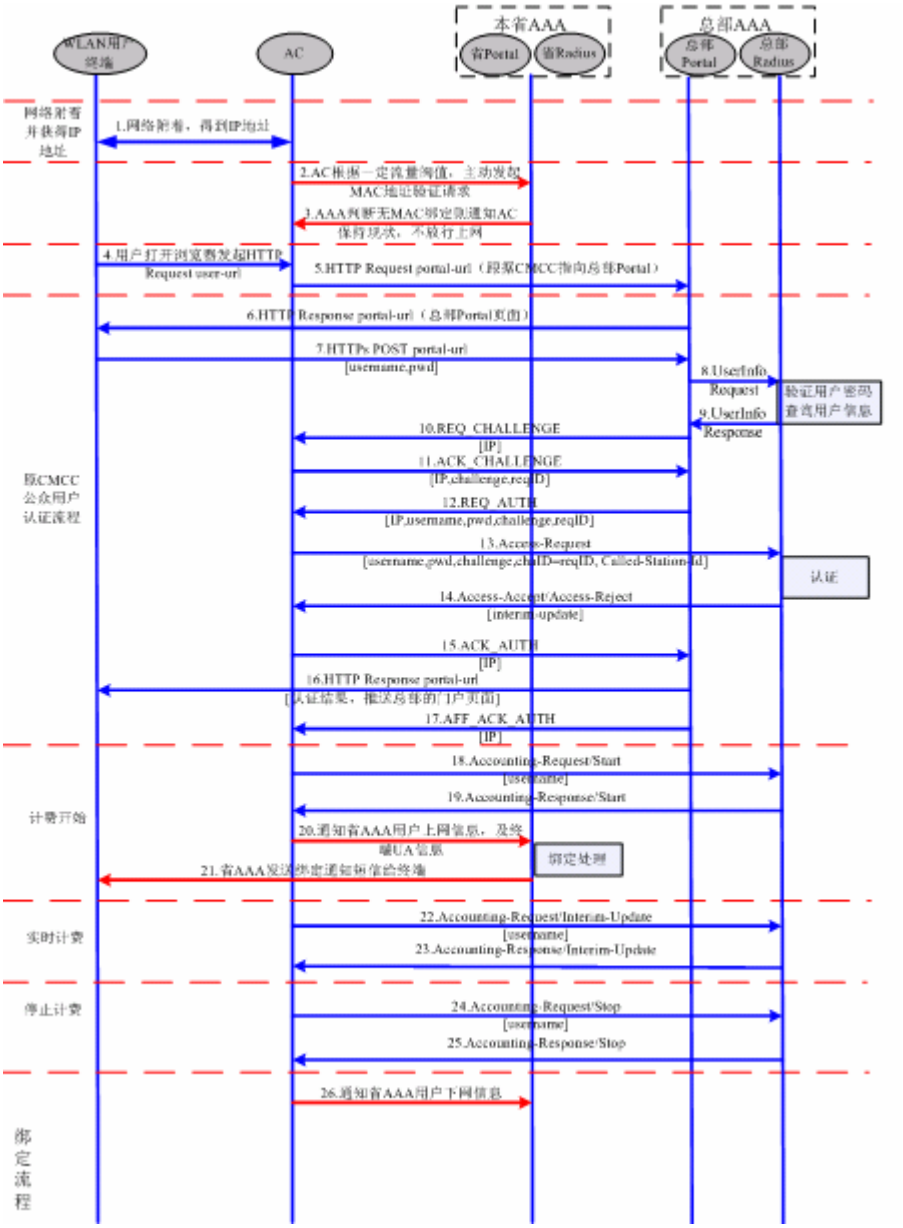
1.3.4 锐捷MAC短信认证

工作原理

STA 关联上开启 MAC 短信认证功能的 SSID 后，通过 DHCP 获取 IP 地址，获取到 IP 后，允许使用网络，但用户在指定周期内使用了指定阈值的流量时，AC 向绑定 Portal 服务器发起 MAC 绑定查询。如果用户为已绑定状态，绑定 Portal 发起认证请求，用户进行认证；如果用户为未绑定状态，用户需要通告 Portal 认证来接入网络。

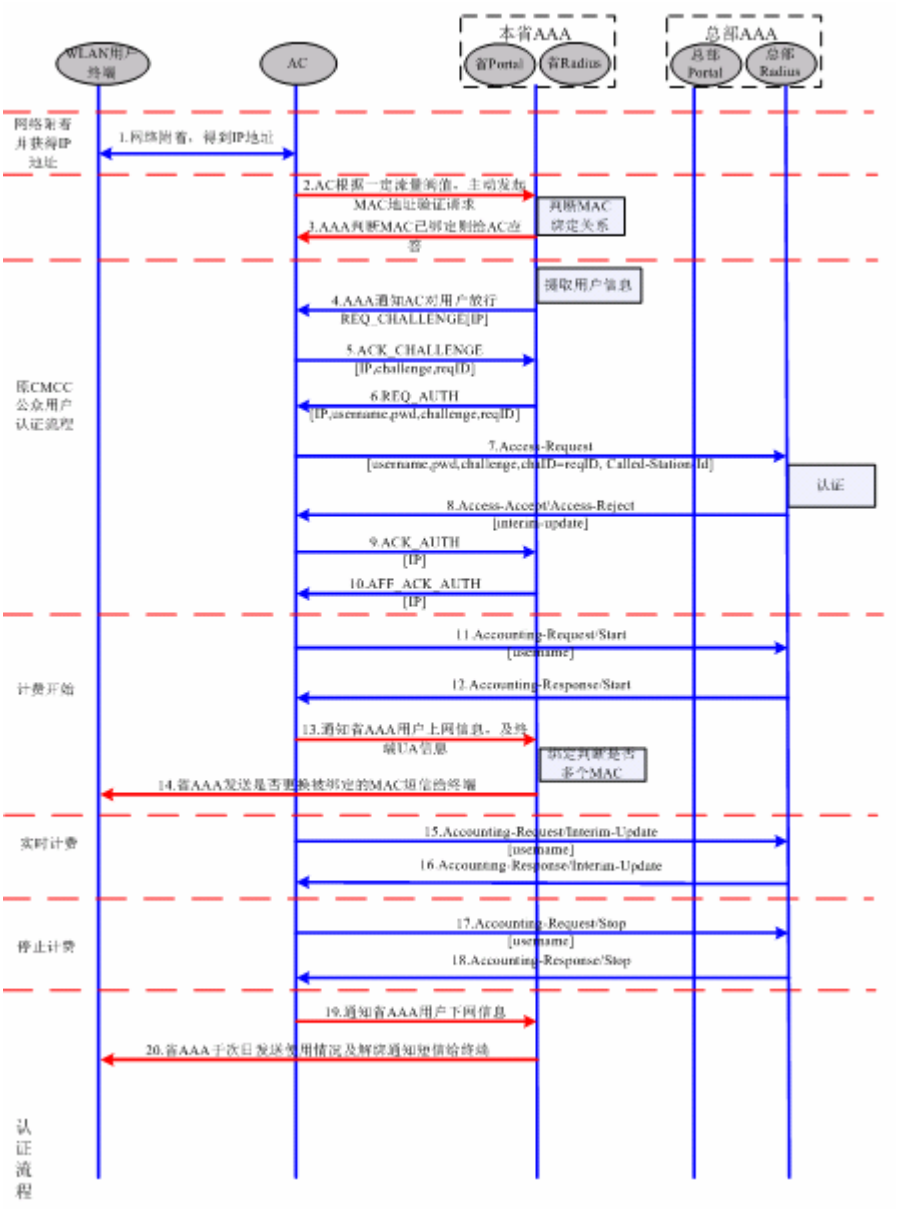
↘ 未绑定用户上网流程

该流程为未绑定用户在开启 MAC 短信认证的 SSID 中接入网络的流程，相比普通的二代 web 认证流程，增加了 MAC 绑定查询和上下线通告绑定 Portal 服务器，其他流程没有变化。未绑定用户进行 Portal 认证时，如果在重定向页面中勾取了“绑定”复选框，绑定服务器会对用户进行绑定，以后用户可以直接走已绑定用户上网流程，方便快捷。



↘ 已绑定用户的上网流程

该流程为已绑定用户上网流程，相比正常的 Portal 认证，用户不需要通过打开浏览器来认证上网，关联网络后自动完成网络接入，极大方便了用户使用无线网络。



1.3.5 RIPT

无线设备上 WEB 认证支持 RIPT 功能，在 AC 故障或者 AC 和 AP 断开连接时，可以使得 AP 上的 WEB 认证模块继续对外提供认证服务。

工作原理

通过 AC 上配置 RIPT AP 组，开启 RIPT 功能（RIPT 的详细配置见《RIPT 配置手册》）。在 RIPT 的 AP 认证模式下，AC 上的 WEB 认证相关的配置下发到 RIPT 的 AP 上，AP 即可作为接入设备单独对外提供完整的 WEB 认证服务（STA 不必在 AC 上进行 WEB 认证）。AP 上认证通过的用户信息同步到 AC 上，AC 上可查看认证用户状况。

↘ **下发配置**

RIPT 的 AP 认证模式下，AC 上配置 aaa，radius 以及 rsna 开启 WEB 认证受控口，可以下发到支持 RIPT 的对应 AP 上。下发到 AP 的配置完备之后，AP 即可对外提供 WLAN 服务，包括 WEB 认证服务。

↘ 同步 AP 的用户信息到 AC

STA 连接上对外提供 WEB 认证服务的 RIPT AP，进行认证。AP 上认证通过的 WEB 用户信息可以同步到 AC 上，方便 AC 上查看认证用户状况。

1.3.6 WiFiDog

HTTP 拦截

同锐捷一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同锐捷一代 Web 认证的 HTTP 重定向技术。

工作原理

组网拓扑图同 图 1-1 Web 认证方案网络拓扑图。

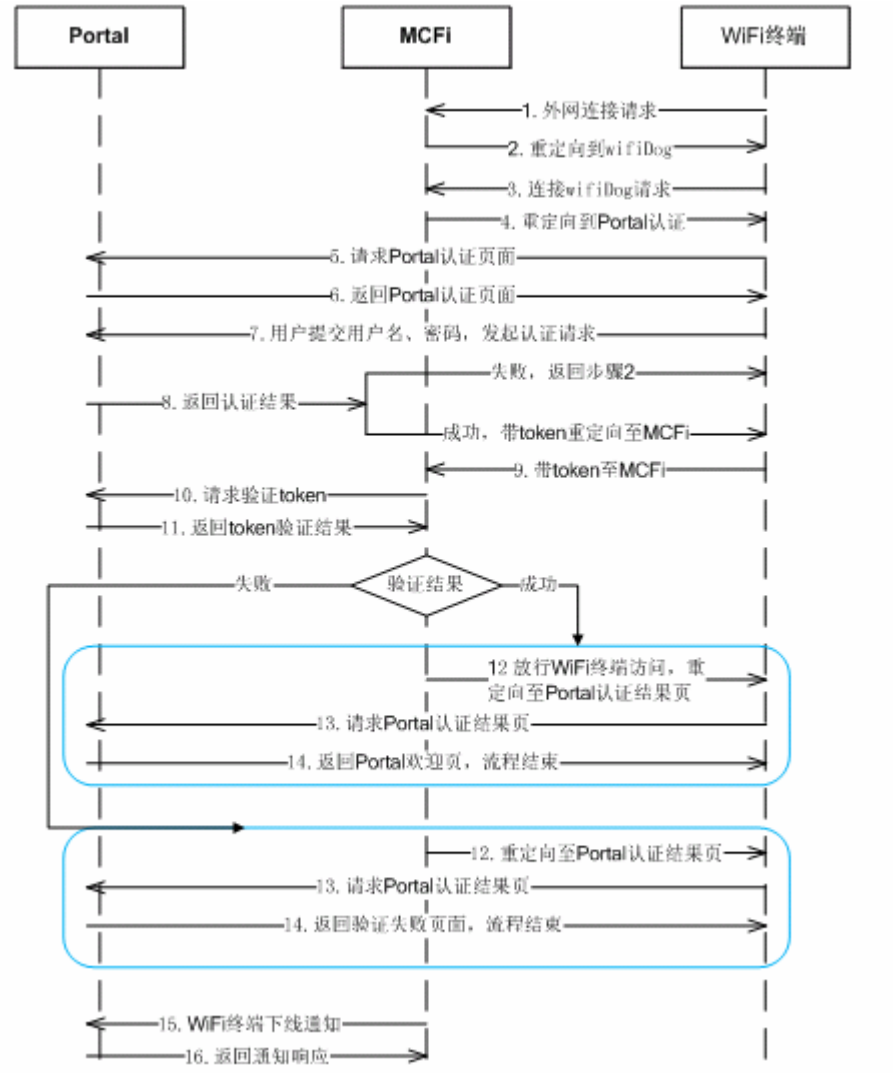
Web 认证的角色：

1. 认证客户端：通常是一个浏览器，运行 HTTP 协议，用户通过浏览器上网时浏览器将发出 HTTP 请求。
2. 网络设备：在网络拓扑中一般是接入层设备（例如在无线网络中可以是无线 AP），一般与用户终端设备直接相连接，在设备上需要启动 Web 认证功能。设备控制用户的上网权限，接收认证客户端发来的 token 校验请求或放行网络的请求，同时还负责向 Portal 服务器校验 token 信息。
3. Portal 服务器：提供 Web 认证的认证界面和相关操作。Portal 服务器接受认证客户端发出的基于 HTTP 的认证请求，提取其中的账号信息，后台认证后，此认证结果经认证客户端中转给网络设备，网络设备校验完成后再要求认证客户端重定向端 Portal 服务器的相关页面。
4. 认证服务器：提供用户认证服务，具体协议由 Portal 服务器和认证服务器协商决定（例如 radius 协议）。

WiFiDog 认证主要流程：

1. 在认证之前，设备将未认证用户发出的所有 HTTP 请求都拦截下来，并重定向到 Portal 服务器去，这样在用户的浏览器上将弹出一个认证页面。
2. 在认证过程中，用户在认证页面上输入认证信息（用户名、口令、校验码等等）与 Portal 服务器交互。
3. Portal 服务器后台对用户信息进行合法性校验，若认证失败则返回失败页面给客户端，否则将客户端重定向到网络设备
4. 网络设备收到认证客户端的请求后，向 Portal 服务器发起校验，根据校验结果，将客户端重定向到 portal 服务器相关页面

图 1-6 WiFiDog 认证流程



用户下线流程：

用户下线分两种类型,一种是设备端检测到用户下线,比如用户时长到达,流量用完,链路断开等;一种是用户主动点击下线按钮。

1. 用户主动点击页面上的下线按钮，选择下线，此时会同时向 portal 服务器和网络设备发起下线请求(也可能不是同时，具体取决与 portal 服务器的实现 ）。
2. 设备检测到终端低流量将用户下线，具体依赖所配置的低流量检测参数而定。

相关配置

↘ 创建配置模板

缺省情况下无配置。

在全局配置模式下使用 **web-auth template** { **wifidog** | *template-name* **wifidog** }命令创建 WiFiDog 模板。

可以使用该配置模板进行 web 认证功能。

配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式使用 **ip** { *ip-address* }来配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

配置服务器认证 URL

缺省情况下无配置。

在模板配置模式使用 **url** { *url-string* }来配置。

用户重定向到的 URL 地址，通常使用 portal 认证页面地址。

配置设备 IP

缺省情况下无配置。

在模板配置模式使用 **nas-ip** { *ip-address* }来配置。

设置 wifidog 的设备接入服务 ip，用于服务器向此 ip 发起通讯。

配置的设备接入服务 ip 不能够被设置成直通地址

配置接入服务 ip 为设备 ip 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 web 管理界面。

如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1， 2.2.2.2 等。

一般情况下使用设备的真实 ip 直接登录管理设备是不安全的，安全的做法是把管理设备的 ip 映射成外网 ip。管理设备使用外网 ip 进行管理。由于外网和服务器之间是有防火墙这类的安全设备来防护，可以保证安全性。而直接通过内网访问则不会有任何防护，如设备的真实 ip 对用户可见容易使设备直面攻击。建议配置为虚拟 ip。

配置 Gateway ID

缺省情况下配置为设备的 MAC 地址

在模板配置模式使用 gateway-id { string }来配置

该参数为 wifidog 协议交互报文中需要携带的参数，开放命令给对接第三方 portal 使用.

开启 web 认证

缺省情况下该功能关闭。

在接口模式下使用 **web-auth enable** { **eportalv2 |** *template-name* **v2** }命令开启用户所在端口 web 认证受控。

开启认证后端口下未认证用户会被重定向到认证页面。

1.3.7 微信连Wifi认证

HTTP 拦截

同锐捷一代 Web 认证的 HTTP 拦截技术。

HTTP 重定向

同锐捷一代 Web 认证的 HTTP 重定向技术。

工作原理

组网拓扑图同 图 1-1 Web 认证方案网络拓扑图。

Web 认证的角色：

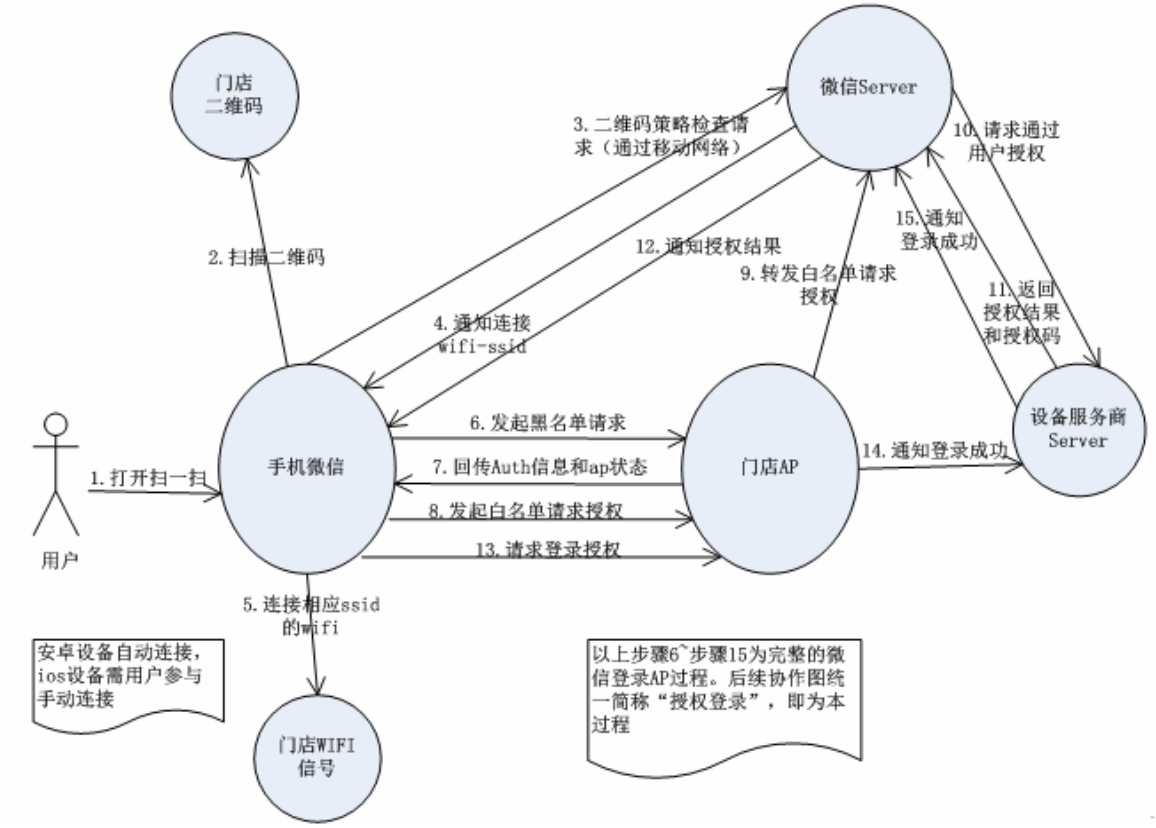
1. 用户：通过微信连接 Wifi 上网的用户。
2. 门店 AP：即胖 AP 或者 AC。
3. 设备服务商 Server：Portal 或认证服务器，泛指 MCP、WMC，或者是第三方服务器。
4. 微信 Server：微信后台服务器。

微信连 wifi 认证扫一扫流程：

1. 用户通过微信扫一扫 Wi-Fi 二维码发起连接；
2. 微信客户端识别出二维码并调用微信 Server（这里是通过手机的移动网络）；
3. 微信 Server 通过二维码策略检查请求；
4. 微信 Server 返回 SSID 并通知连接 Wi-Fi；
5. 微信客户端开始请求连接 AP；
6. 连接上 AP 后，微信客户端发起黑名单请求，请求地址为 http://10.1.0.6/redirect，这个请求的目的是为了让 AP 能鉴别出是微信客户端发起的请求；
7. AP 识别出是黑名单请求，则通过 302 重定向请求，并带上一个 auth 参数，该 auth 参数可以通过加密方式携带手机 MAC 地址和 AP MAC 地址；
8. 微信客户端拿到这个 auth 参数后，将携带 auth 参数发起白名单请求，这个请求是向微信 Server 发起的，目的是请求授权 WIFI 上网，但由于 AP 还未认证通过，因此需要将微信 Server 的 IP 加到 AP 的白名单列表里，这样 AP 才能放行认证请求，所以称为白名单请求；
9. AP 识别出请求 IP 在白名单列表中，放行请求，请求通过 AP 到达微信 Server；

10. 微信 Server 向设备商 Server 发起授权请求，这个 http 请求对应到接口 8（一定要提前调用接口 13 设置好设备商 Server 的 URL 地址和 token 参数）；
11. 设备商 Server 对这个请求进行授权，并返回认证地址和认证参数（对应接口 8 中 login 参数）；
12. 微信 Server 将这个认证地址和认证参数返回给微信客户端；
13. 微信客户端请求这个认证地址（即 Login 请求）；
14. AP 或者设备商 Server 做上网认证操作，AP 放行这个手机 MAC 地址，并且服务商 Server 调用接口 7 通知微信 Server 上网成功（第 15 微信连 Wi-Fi 11 步），AP 同时 302 重定向，重定向需带上 res=success 返回，微信客户端根据这个参数确定上网授权成功，微信客户端展示 Wi-Fi 连接成功页面；

图 1-7 微信连 wifi 认证扫一扫流程

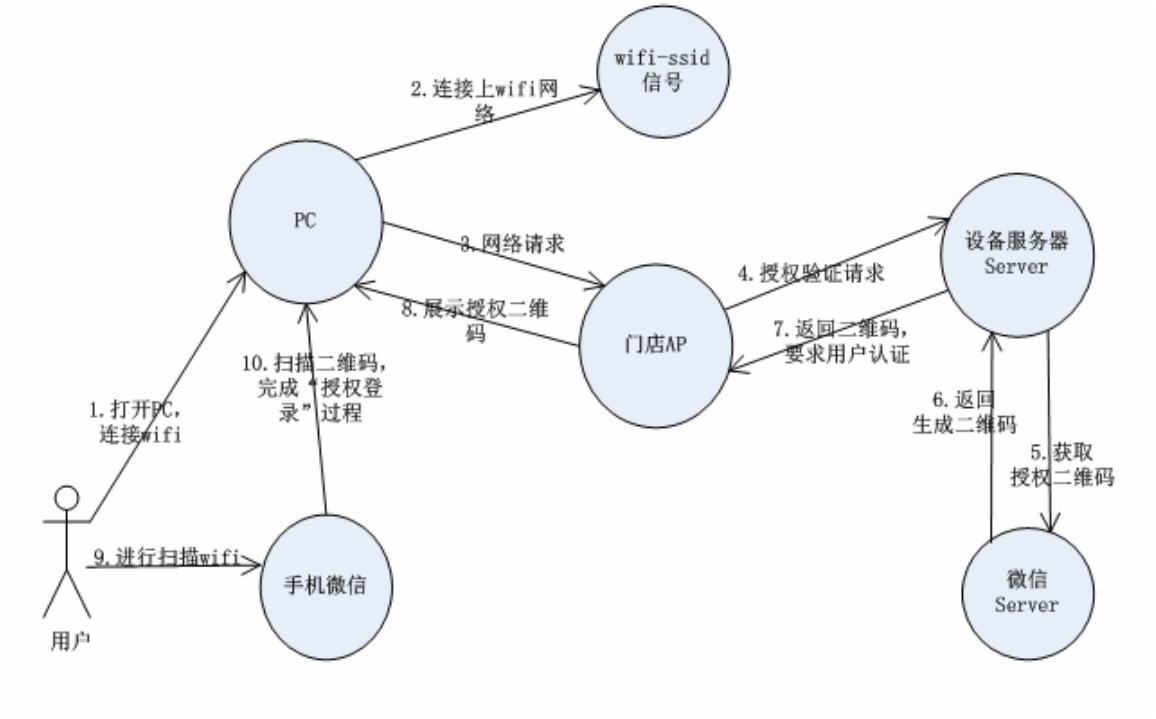


pc 设备动态二维码实现多设备上网流程：

用户打开 PC 连接 WI-FI, 选择连接 SSID（第 1，2 步），当用户再打开浏览器连接某一网站的时候，会发起一个网络请求(第 3 步)，AP 会 302 一个传统 Portal 认证页给浏览器。由于需要支持手机扫 PC 上的二维码上网，这个时候 AP 会再发起一个请求到设备商 Server（第 4 步）,设备商 Server 再调用微信 Server(接口 2)获取二维码图片的 URL(第 5 步)。微信 Server 返回生成的二维码图片 URL（第 6 步）,设备商 Server 再返回二维码图片 URL 给 AP（第 7 步），AP 返回给浏览器

的 302Portal 认证页面上面潜嵌入二维码图片，此时手机扫一扫该为二维码(第 10 步)，后面的流程就和手机上网流程是一致的了。

图 1-8 pc 设备动态二维码实现多设备上网流程



用户下线是设备端检测到用户下线,比如用户时长到达,流量用完,链路断开等。

1. 设备检测到终端低流量将用户下线，具体依赖所配置的低流量检测参数而定。
2. 链路断开的时间依据防抖配置的参数决定。

相关配置

↘ 创建配置模板

缺省情况下无配置。

在全局配置模式下使用 **web-auth template** { **wechat** | *template-name* **wechat** }命令创建微信连 wifi 认证模板。

可以使用该配置模板进行 web 认证功能。

↘ 配置服务器 IP 地址

缺省情况下无配置。

在模板配置模式使用 **ip** { *ip-address* }来配置服务器 IP 地址。

访问服务器的请求被设备放行，并且支持对发往服务器的请求进行限速保护。

↘ 配置服务器 URL

缺省情况下无配置。

在模板配置模式使用 **service-url** { *url-string* }来配置。

设备和服务器通讯使用的 url 地址。

配置设备 IP

缺省情况下无配置。

在模板配置模式使用 **nas-ip** 来配置。

设置微信连 wifi 认证的设备接入服务 ip，用于服务器向此 ip 发起通讯。

配置的设备接入服务 ip 不能够被设置成直通地址

配置接入服务 ip 为设备 ip 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 web 管理界面。

如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1， 2.2.2.2 等。

一般情况下使用设备的真实 ip 直接登录管理设备是不安全的，安全的做法是把管理设备的 ip 映射成外网 ip。管理设备使用外网 ip 进行管理。由于外网和服务器之间是有防火墙这类的安全设备来防护，可以保证安全性。而直接通过内网访问则不会有任何防护，如设备的真实 ip 对用户可见容易使设备直面攻击。建议配置为虚拟 ip。

配置与服务器通讯使用的加密秘钥

缺省情况下无配置。

在模板配置模式使用 **key** {*key-string* }来配置。

该秘钥是用来加密用户认证的信息德尔，需要和服务器上配置的秘钥一致。

开启 web 认证

缺省情况下该功能关闭。

在 wlansec 模式下使用 **web-auth portal** { **wechat |** *template-name* **wechat** }和 **webauth** 命令开启用户所在端口 web 认证受控。

开启认证后端口下未认证手机终端用户会被重定向到服务器一键上网页面，未认证的 pc 用户会被重定向到二维码页面。

微信连 wifi1.0 版本配置单体逃生功能

缺省情况下该功能关闭。

在模板配置模式使用 **escape interval** *seconds* **online-time** *minutes* 来配置。

配置后，设备收到用户的黑名单请求就开启定时器（间隔由 **interval** *seconds* ）,到期后如果还没有收到登录授权请求，设备就让用户逃生，放行表项。逃生用户的上网时长由 **online-time** *minutes* 指定。

微信连 wifi3.0 版本配置开启单体逃生功能

缺省情况下该功能关闭。

在模板配置模式使用 **escape user-try-auth** *counts* **online-time** *minutes* 来配置。

配置之后，如果终端因为多次点击微信认证发起临时放行请求次数达到配置值而未认证成功，则放行表项，让用户逃生可以上网。逃生用户的上网时长 **online-time** *minutes* 指定。

配置集体逃生功能

缺省情况下该功能关闭。

在全局配置模式 wlansec 配置模式下使用 **web-auth wechat-escape interval** *minutes* **times** *count* 来配置。
wlansec 模式下配置仅 11.1(5)B23 支持该功能。wlansec 模式下配置优先生效，若 wlansec 下未配置则使用全局模式配置。

配置后 ,设备开始统计单体逃生用户数 ,如果一定间隔内(由 **interval** *minutes* 指定)单体逃生用户数达到阀值(由 **times** *count* 指定)，就开启集体逃生，后面接入的所有用户都直接逃生免认证。

如果要取消集体逃生状态，可以在全局配置模式使用 **web-auth wechat-escape recover** 恢复成单体逃生状态。

配置服务器检测功能

缺省情况下该功能关闭。

在全局配置模式使用 **web-auth wechat-check interval** *minutes* 来配置。

配置后，设备开始对服务器进行检测，如果一定间隔内（由 **interval** *minutes* 指定）检测到服务器没有应答或者回应不可用，同时设备配置了集体逃生功能，后面接入的所有用户都直接逃生免认证。

如果要取消服务器检测，可以在全局配置模式使用 **no web-auth wechat-check** 取消服务器检测功能。

配置临时放行功能

缺省情况下该功能关闭。

在模板配置模式使用 **temporary-permit** *seconds* 来配置。

配置后，设备收到用户的黑名单请求，就临时安装用户的源 ip 表项，放行用户。该表项老化时间由参数 seconds 指定。

1.4 配置详解

配置项	配置建议 & 相关命令	
配置一代Web认证功能	⚠ 必须配置。用于配置一代 Web 认证功能基本参数	
	web-auth template eportalv1	创建一代 eportalv1 模板
	ip { *ip-address* }	配置服务器的 IP 地址
	url { *url-string* }	配置服务器的主页地址
	web-auth portal key { *key-string* }	配置服务器通信密钥
	snmp-server community { *community-string* } **rw**	配置 SNMP 通信团体字
	snmp-server host { *ip-address* } **inform version** 2c { *community-string* } **web-auth**	配置 SNMP 通信服务器
	snmp-server enable traps web-auth	使能 web 认证 trap/inform 通告

	web-auth enable	在接口上使能 web 认证
配置二代web认证功能	⚠ 必须配置。用于配置二代 Web 认证功能基本参数	
	aaa new-model	开启 AAA 功能
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	配置 RADIUS 服务器和密钥
	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2...*]	配置 Web 认证方法列表(使用 RADIUS 认证)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2...*]	配置网络记账方法列表(使用 RADIUS 记账)
	web-auth template { **eportalv2** | *portal-name* **v2** }	创建二代认证模板
	ip { *ip-address* }	配置服务器的 IP 地址
	url { *url-string* }	配置服务器的主页地址
	web-auth portal key { *key-string* }	配置服务器通信密钥
	web-auth enable { **eportalv2** | *template-name* }	在接口上使能 Web 认证
配置内置Portal Web认证	⚠ 必须配置。用于配置内置 Portal Web 认证功能基本参数	
	aaa new-model	开启 AAA 功能
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	配置 RADIUS 服务器和密钥
	aaa authentication iportal { **default** | *list-name* } *method1* [*method2...*]	配置 Web 认证方法列表(使用 RADIUS 认证)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2...*]	配置网络记账方法列表(使用 RADIUS 记账)
	web-auth template iportal	创建内置 Portal Web 认证模板
	web-auth enable iportal	在接口上使能 Web 认证
配置WIFIDOG	⚠ 必须配置。用于配置 WIFIDOG 认证功能基本参数	
	web-auth template wifidog	创建 Portal Web 认证模板
	ip { *ip-address* }	配置服务器的 ip 地址
	url { *url-string* }	配置服务器的 url 链接
	nas-ip { *ip-address* }	配置接入服务 ip 地址
	web-auth portal wifidog	使用 wifidog 这个模板
	webauth	开启 web 认证

配置MAC短信认证	⚠ 必须配置。用于配置内置 Portal Web 认证功能基本参数	
	aaa new-model	开启 AAA 功能
	radius-server host { *ip-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] **key** { *string* }	配置 RADIUS 服务器和密钥
	web-auth template eportalv2	创建 Portal Web 认证模板
	web-auth sms-flow interval *interval* **threshold** *flows*	配置 mac 短信查询周期与阈值
	web-auth bind-portal *string* **[type { group-spec | local-spec}]**	配置 MAC 短信认证绑定的服务器
	web-auth winterface *string*	配置重定向 URL 中 winterface 字段参数
	web-auth wlan-ac-ip *ipv4*	配置重定向 URL 中 ACIP 字段参数
配置微信连wifi认证	⚠ 必须配置。用于配置微信连 wifi 认证功能基本参数	
	web-auth template { **wechat | (***portal-name* **wechat** *)*}	创建微信连 wifi 认证模板
	ip { *ip-address* }	配置服务器的 ip 地址
	service-url { *url-string* }	配置服务器的 url 链接
	nas-ip { *ip-address* }	配置接入服务 ip 地址
	key { *key-string* }	配置服务器的加密密钥
	web-auth portal wechat	使用 webchat 这个模板
	webauth	开启 web 认证
配置认证方法列表名	⚠ 可选配置。在 template 模板下指定认证方法列表名，和 AAA 模块的方法列表配置保持一致	
	authentication { *mlist-name* }	配置认证方法列表名(仅二代和内置)
配置记账方法列表名	⚠ 可选配置。在 template 模板下指定记账方法列表名，和 AAA 模块的方法列表配置保持一致	
	accounting { *mlist-name* }	配置记账方法列表名(仅二代和内置)
配置Portal服务器通信端口	⚠ 可选配置。在 template 模板下指定 Portal 服务器通信端口，需要和服务器端的的通信端口一致	
	port { *port-num* }	配置 portal 服务器通信端口
配置绑定模式	⚠ 可选配置。在 template 模板下指定用户表项绑定模式	
	bindmode {ip-mac-mode | ip-only-mode}	配置模板表项绑定模式
配置定制页面包	⚠ 选配置。在 template 模板下指定内置 Portal Web 认证使用特定的页面包。	
	page-suite *file-name*	指定内置 Portal 使用特定的页面包

配置广告推送地址	⚠ 选配置。在 template 模板下配置广告推送功能。	
	popup *url*	配置广告 url
	popup popup-mode [login-popup | online-popup]	配置弹出广告的方式
配置广告推送方式	⚠ 可选配置。在 template 模板下配置广告推送方式。	
	popup popup-mode [login-popup | online-popup]	配置弹出广告的方式
配置定制化URL格式	⚠ 可选配置。在 template 模板下配置重定向 URL 格式。	
	fmt custom	配置重定向 URL 的格式
设置重定向的HTTP端口	⚠ 可选配置。用于指定重定向 TCP 拦截端口，补充拦截环境中的特定端口报文进行重定向	
	http redirect port { *port-num* }	配置重定向 TCP 拦截端口
设置Web认证模块SYSLOG功能	⚠ 可选配置。用于配置 web 认证 SYSLOG 功能	
	web-auth logging enable {*num* }	配置 web 认证 SYSLOG 输出速率
设置未认证用户的最大HTTP会话数	⚠ 可选配置。用于调整 HTTP 会话数限制，对于后台会话数较多的场景需要放宽限制	
	http redirect session-limit { *session-num* } [**port** { *port-session-num* }]	配置用户的 HTTP 会话限制数
设置维持重定向连接的超时时间	⚠ 可选配置。用于修改重定向连接超时时间，在网络环境较差时调大参数有利于完成重定向	
	http redirect timeout { *seconds* }	用于设置重定向连接超时时间
设置直通ARP资源范围	⚠ 可选配置。用于放行指定地址的 ARP，开启 ARP CHECK 时需要放行网关 ARP	
	http redirect direct-arp { *ip-address* [*ip-mask*] }	用于配置直通 ARP 资源范围
设置无需认证用户IP范围	⚠ 可选配置。用于配置特殊用户不用认证就能上网	
	web-auth direct-host { *ipv4-address* [*ip-mask*] [**arp**] | *ipv6-address* | *mac-address*} [**port** *interface-name*]	用于配置免认证用户
设置在线用户信息的更新时间间隔	⚠ 可选配置。用于配置用户信息的更新周期	
	web-auth update-interval *{ seconds }*	用于配置用户信息更新周期
配置Portal检测	⚠ 可选配置。用于检测 Portal 服务器是否可用，如果不可用，则进行切换，该功能要结合主备 Portal 使用。	
	web-auth portal-check [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries]	配置 Portal 检测的周期、超时时间、超时重传次数
	web-auth ping [**interval** *minutes*] [**retry** *times*]	配置 ping 检测的周期和超时重传次数

配置Portal逃生	⚠ 可选配置。配置当 Portal 服务器不可用时，新接入用户免认证。	
	web-auth portal-escape	配置 Portal 不可用时新接入用户免认证。
配置DHCP地址核查	⚠ 可选配置。用于检测认证用户的 ip 地址是否是 DHCP 服务器分配的，如果不是则拒绝认证请求。	
	web-auth dhcp-check	检测终端的 ip 地址是否是 DHCP 服务器分配
配置关闭链路检测	⚠ 可选配置。用于防抖，用户断开链路时，可以保证 Web 认证表项不删除，当用户再次接入时则无需认证就可以继续上网。	
	no web-auth sta-leave detection	配置关闭链路检测
配置关闭Portal协议扩展	⚠ 可选配置。对接锐捷 Portal 服务器软件时需要开启扩展，对接标准中移动 Portal 服务器，需要关闭扩展。	
	no web-auth portal extension	配置关闭 Portal 协议扩展
配置黑白名单	⚠ 可选配置。配置黑名单表示某些网络资源认证通过也不可访问，配置白名单表示某些资源不用认证也可以访问。	
	web-auth acl {black-ip *ip*|**black-port** *port*|**black-url** *name*|**white-url** *name*}	配置黑白名单
配置防抖动计费	⚠ 可选配置。配置防抖时间是否算入在线时长，提高计费精度。具体的防抖时间则需要参考具体产品的防抖功能的设置情况。	
	web-auth accounting jitter-off	配置防抖时间，no 选项表示防抖时间不算入在线时长
配置Portal通信端口	⚠ 可选配置。配置后设备与 Portal 服务器通信的源端口为所配置端口。	
	ip portal source-interface interface-type interface-num	指定设备与 Portal 服务器的通信接口
配置宁盾系统兼容URL	⚠ 可选配置。配置 web 重定向 URL 支持宁顿系统。	
	web-auth dkey-compatible url-parameter *string*	配置 URL 兼容宁盾系统。
配置内置WEB认证NAT功能	⚠ 可选配置。配置内置 web 认证支持 NAT。	
	iportal nat enable	支持内置 web 认证 NAT
配置内置WEB认证重传次数	⚠ 可选配置。配置内置 web 认证 http 连接重传次数。	
	iportal retransmit *count*	配置内置 web 认证 http 连接重传次数
配置内置WEB认证服务选择	⚠ 可选配置。配置内置 web 认证使用的服务类型。	
	iportal service [internet *internet-name*] **[local** *local-name* **]**	配置内置 web 认证使用的服务类型

配置WEB记账方法列表	⚠ 可选配置。基于不同的模板，指定 web 认证记账方法。	
	web-auth accounting v2 { default | *name* **}**	基于不同的模板，指定 web 认证记账方法
配置WEB认证方法列表	⚠ 可选配置。基于不同的模板，指定 web 认证方法。	
	web-auth authentication v2 { default | *name* **}**	基于不同的模板，指定 web 认证方法
配置微信认证支持IOS自动弹窗控制命令	⚠ 可选配置。IOS 系统关联上无线后即可自动弹出 web 配置页面。	
	http redirect adapter ios	IOS 系统关联上无线后即可自动弹出 web 配置页面
配置wlansec下的用户在线检测	⚠ 可选配置。用于配置 wlansec 下的用户在线检测	
	web-auth offline-detect interval *interval* **flow** *thredshold*	用于配置 wlansec 下的用户在线检测
配置Portal协议 0x05 号属性透传功能	⚠ 可选配置。用于配置 portal 协议 0x05 号属性透传功能	
	web-auth portal-attribute [5 | textinfo]	用于配置 portal 协议 0x05 号属性透传功能
配置Portal认证账号唯一性检查功能	⚠ 可选配置。用于配置 portal 认证账号唯一性检查功能	
	web-auth portal-valid unique-name	用于配置 portal 证账号唯一性检查功能
无线wifidog一键配置	⚠ 可选配置。用于无线 wifidog 一键配置	
	web-auth wifidog-template wlan-range portal-ip nas-ip url [perception]	无线 wifidog 一键配置
无线微信连wifi一键配置	⚠ 可选配置。用于无线 wechat 一键配置	
	web-auth wechat-template wlan-range portal-ip nas-ip [ios-adapter | perception]	无线微信连 wifi 一键配置

1.4.1 配置一代Web认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证

注意事项

无

配置方法

配置 portal 服务器

- 必须配置，要成功应用 Web 认证功能，必须设置并应用 portal 服务器。
- 当接入/汇聚设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户才可以直接与这个地址进行 HTTP 通讯。

配置设备与认证服务器之间的通信密钥

- 必须配置，要成功应用 Web 认证功能，必须设置接入/汇聚设备与认证服务器进行通信的密钥。
- 当设备发现未认证用户在访问网络资源时，设备将通过重定向功能，向用户弹出认证页面，通过认证页面，引导用户向认证服务器发起认证。在认证过程中，设备与认证服务器间通过密钥对部分数据进行加密，以加强安全性。

设置设备与认证服务器之间的 SNMP 网管参数

- 必须配置，要成功应用 Web 认证功能，必须设置设备与认证服务器之间的 SNMP 网管通信参数。
- 接入/汇聚设备和认证服务器之间通过SNMP/MIB对认证用户进行管理，在设备上，使用MIB来管理认证用户表，认证服务器通过访问这个 MIB，可以获取用户相关的统计信息，以及进行控制用户的上线、下线的操作。当用户下线时，设备将发送 SNMP-Inform 消息给认证服务器。

在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时这个端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

创建模板

【命令格式】 **web-auth template eportalv1**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 eportalv1 为默认的一代 web 认证模板

配置服务器 IP

【命令格式】 **ip** { *ip-address* }
【参数说明】 portal 服务器的地址
【命令模式】 web 认证模板配置模式
【使用指导】 -

配置服务器 URL

【命令格式】 **url** { *url-string* }
【参数说明】 portal 服务器的认证页面地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置 Portal 服务器 URL 格式

【命令格式】 **fmt { ace | ruijie }**
【参数说明】 portal 服务器的 url 格式
【命令模式】 Web 认证模板配置模式
【使用指导】 fmt 参数为 ace 时，支持 ACE 联动。

配置用户绑定模式

【命令格式】 **bindmode { ip-mac-mode | ip-only-mode }**
【参数说明】 用户的绑定模式
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置重定向方式

【命令格式】 **redirect { http | js }**
【参数说明】 重定向报文的封装格式
【命令模式】 Web 认证模板配置模式
【使用指导】 某些 app 无法执行 javascript 脚本动作时，需要配置成 http 封装格式触发重定向

配置用户绑定模式

【命令格式】 **bindmode { ip-mac-mode | ip-only-mode }**
【参数说明】 用户的绑定模式
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置重定向方式

【命令格式】 **redirect { http | js }**
【参数说明】 重定向报文的封装格式
【命令模式】 Web 认证模板配置模式
【使用指导】 某些 app 无法执行 javascript 脚本动作时，需要配置成 http 封装格式触发重定向

配置服务器加密密钥

【命令格式】 **web-auth portal key** { *key-string* }
【参数说明】 portal 服务器的加密密钥，配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符。
【命令模式】 全局配置模式
【使用指导】 -

配置服务器 SNMP 通信团体字

【命令格式】 **snmp-server community** { *community-string* } **rw**
【参数说明】 *community-string*：Community 字符串；
rw：由于需要对 MIB 进行 Set 操作，因此需要设置成 RW，支持读写操作；
【命令模式】 全局配置模式
【使用指导】 设置 SNMP Community，认证服务器可以使用这个 Community 管理接入/汇聚设备上的在线用户。

配置服务器 SNMP 通信服务器

【命令格式】 **snmp-server host** { *ip-address* } **inform version** 2c { *community-string* } **web-auth**
【参数说明】 *ip-address*：目的主机地址，也就是认证服务器的地址。
community-string：通信团体字，发送 SNMP-Inform 消息使用的 Community 字符串。
【命令模式】 全局配置模式
【使用指导】 设置发送 Web 认证消息的目的主机，类型、版本、Community 等参数。
inform：设置发送 SNMP-Inform 类型的消息。由于接入/汇聚设备在用户下线的时候向认证服务器发送消息，为了防止消息丢失，所以采用 SNMP-Inform 而不是 SNMP-Trap。
version 2c：SNMPv2 以后的版本才支持 SNMP-Inform 类型，因此这里不能设置为 SNMPv1。
web-auth：指明发送 Web 认证消息采用上述的参数。

SNMP 的配置命令和其他具体内容参见“SNMP 配置指南”中的相关章节。

这里列出的 SNMP 通信参数是以 SNMPv2 的设置为例的，如果要求设备和认证服务器之间的 SNMP 网管通信有更高的安全性，可以考虑采用 SNMPv3。这样，SNMP Community 的设置需要改为 SNMP User，并且 SNMP-Inform 的版本也需要改为 SNMPv3 版本的，另外还需要设置和 SNMPv3 相关的安全参数，具体参见“SNMP 配置”中相关的章节，这里不再进行详细介绍。

配置使能 web 认证 trap/inform 通告

【命令格式】 **snmp-server enable traps web-auth**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 设置接入/汇聚设备允许向外发送 Web 认证的消息，消息类型包括 Trap 和 Inform。
web-auth：即 Web 认证的消息。

配置接口上启用 web 认证

【命令格式】 **web-auth enable**
【参数说明】 -
【命令模式】 接口配置模式

【使用指导】 -

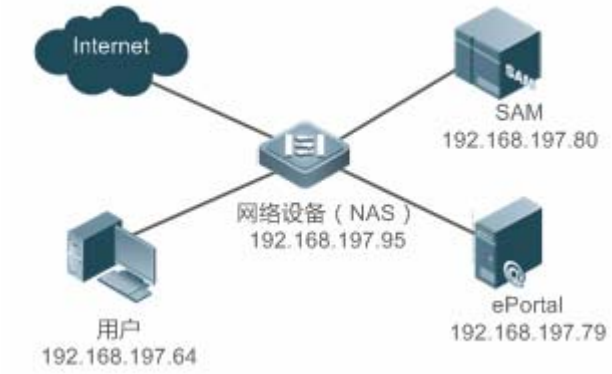
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

一代 web 认证

【网络环境】

图 1-9



【配置方法】

- 在网络设备上设置认证服务器的 IP 地址及与认证服务器进行通信的密钥(ruijie)
- 在网络设备上设置认证页面的主页地址
- 设置网络设备与认证服务器之间的 SNMP 网管参数(团体字 public)
- 在网络设备上对 GigabitEthernet 0/2、GigabitEthernet 0/3 两个端口上开启 Web 认证功能

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#web-auth template eportalv1
Ruijie(config.tmplt.eportalv1)#ip 192.168.197.79
Ruijie(config.tmplt.eportalv1)#exit
Ruijie(config)# web-auth portal key ruijie
```

```
Ruijie(config)# web-auth template eportalv1
Ruijie(config.tmplt.eportalv1)#url http://192.168.197.79:8080/eportal/index.jsp
Ruijie(config.tmplt.eportalv1)#exit
```

```
Ruijie(config)# snmp-server community public rw
Ruijie(config)# snmp-server enable traps web-auth
Ruijie(config)# snmp-server host 192.168.197.79 inform version 2c public web-auth
Ruijie(config)# exit
```

```
Ruijie(config)# interface range GigabitEthernet 0/2-3
Ruijie(config-if-range)# web-auth enable
Ruijie(config-if-range)# exit
```

【检验方法】

- web 认证配置是否成功

```
Ruijie(config)#show running-config
…
snmp-server host 192.168.197.79 inform version 2c public web-auth
snmp-server enable traps web-auth
snmp-server community public rw
…
web-auth template eportalv1
 ip 192.168.197.79
 url http://192.168.197.79:8080/eportal/index.jsp
!
web-auth portal key ruijie
…
interface GigabitEthernet 0/2
 web-auth enable
!
interface GigabitEthernet 0/3
 web-auth enable
```

```
Ruijie#show web-auth control
 Port                      Control  Server Name           Online User Count
 ------------------------- -------- --------------------- -----------------
…
 GigabitEthernet 0/2        On       eportalv1             0
 GigabitEthernet 0/3        On       eportalv1             0
…
```

```
Ruijie#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:      eportalv1
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-mac-mode
  Type:      v1
……
```

常见错误

- Portal 服务器和设备间的 SNMP 参数配置不正确导致用户无法认证上线。
- 跨三层部署 Web 认证，模板中的绑定模式需要选择 ip-only-mode。
- 和 vrrp 一起使用的时候，需要通过 `snmp-server trap-source ip` 命令指定 vrrp 地址，否则 Portal 服务器无法正确处理 trap 报文。

1.4.2 配置二代Web认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证，支持 IPV6。

注意事项

- 二代 Web 认证支持中移动 Portal 规范，同时做了扩展以支持锐捷 Portal 服务器，实际部署时需要根据服务器情做相关兼容性配置，具体参考后续章节的说明。
- 在配置二代Web认证的Portal服务器的URL时，如果URL里面带有IPv6 地址，需要将ipv6 地址用中括号包含起来。例如：配置IPv6 地址为 2001::1 时，实际配置应该为url http://[2001::1]/index.jsp。
- fmt 参数为 cmcc-normal 和 cmcc-ext1 时，其中 IP 仅支持 IPV4 形式，若 IP 为 IPV6 形式，则该 Portal 服务器配置将失效。

配置方法

配置开启 AAA 认证

- 必须配置，要使用二代 Web 认证功能，必须开启 AAA 认证。
- 二代 web 认证向服务器发起认证的功能由设备完成，在设备 AAA 功能实现。

配置 RADIUS 服务器和密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置 RADIUS 服务器。
- 用户账户信息保存在 RADIUS 服务器上，设备需要连接 RADIUS 服务器来确认用户身份合法性。

配置 AAA 中 web 认证方法

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 认证方法。
- 认证方法列表将 web 认证的请求和 RADIUS 服务器关联起来，设备依据认证方法列表来选择认证方式和对应的服务器。

配置 AAA 网络记账方法

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 网络记账方法。
- 记账方法用于关联对应的记账方式和服务器，web 认证需要记账功能记录用户信息或费用。

配置 portal 服务器

- 必须配置，要成功应用二代 Web 认证功能，必须设置并应用 portal 服务器。

- 当接入/汇聚设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户才可以直接与这个地址进行 HTTP 通讯。

配置设备与认证服务器之间的通信密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置接入/汇聚设备与认证服务器进行通信的密钥。
- 当设备发现未认证用户在访问网络资源时，设备将通过重定向功能，向用户弹出认证页面，通过认证页面，引导用户向认证服务器发起认证。在认证过程中，设备与认证服务器间通过密钥对部分数据进行加密，以加强安全性。

设置全局/接口上使用的 portal 服务器

- 二代认证必须配置，要成功应用二代 Web 认证功能，必须在全局/接口上指定使用二代 portal。
- 设备会优先选择所在接口配置的 portal 服务器，如果所在接口不存在 portal 服务器配置，设备会选择全局配置的 portal 服务器，全局不存在配置时默认使用 eportalv1。设备将用户重定向到所选择的 portal 服务器。

在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时这个端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

开启 AAA 功能

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 aaa 的方法列表等命令需要在功能开启后才能输入

配置 RADIUS 服务器和密钥

【命令格式】 **radius-server host** { *ip-address* } [**auth-port** *port-number1*] [**acct-port** *port-number 2*] **key** { *string* }
【参数说明】 *ip-address*：服务器 IP 地址
port-number1：认证端口号
port-number2：记账端口号
string：密钥字符串
【命令模式】 全局配置模式

【使用指导】 认证端口默认 1812，记账端口默认 1813

配置 AAA 中 Web 认证方法列表

【命令格式】 **aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 *list-name*：方法列表名

method1：方法 1

method2：方法 2

【命令模式】 全局配置模式

【使用指导】 二代 web 认证通常使用 RADIUS 认证方法

配置网络记账方法列表

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]

【参数说明】 *list-name*：方法列表名

method1：方法 1

method2：方法 2

【命令模式】 全局配置模式

【使用指导】 二代 web 认证通常使用 RADIUS 记账方法

创建模板

【命令格式】 **web-auth template** { **eportalv2 |** *portal-name* **v2** }

【参数说明】 自定义的 portal 服务器名

【命令模式】 全局配置模式

【使用指导】 eportalv2 为默认的二代 web 认证模板

配置服务器 IP

【命令格式】 **ip** { *ip-address* | *ipv6-address* }

【参数说明】 portal 服务器的地址

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置服务器 URL

【命令格式】 **url** { *url-string* }

【参数说明】 portal 服务器的认证页面地址

【命令模式】 Web 认证模板配置模式

【使用指导】 以 http://或 https://开头

配置 Portal 服务器 URL 格式

【命令格式】 **fmt { cmcc-ext1 | cmcc-ext2 | cmcc-mtx | cmcc-normal | cmcc-ext3 | ct-jc | cucc| ruijie | custom }**

【参数说明】 portal 服务器的 url 格式

【命令模式】 Web 认证模板配置模式

【使用指导】 fmt 参数为 cmcc-normal 和 cmcc-ext1 时，其中 IP 仅支持 IPV4 形式，若 IP 为 IPV6 形式，则该 Portal 服务

器配置将失效。

fmt 参数为 cmcc-ext2，支持辽宁移动 portal 格式。

fmt 参数为 cmcc- ext3 时，支持宁波/嘉兴移动 AC 厂商 URL 格式。

fmt 参数为 cmcc-mtx 时，支持移动 AC 厂商 URL 格式。

fmt 参数为 ct-jc 时，支持电信集采 URL 格式。

fmt 参数为 cucc 时，支持山东联通 portal 格式。

fmt 参数为 custom 时，定制化格式。

配置重定向方式

【命令格式】 **redirect { http | js }**

【参数说明】 重定向报文的封装格式

【命令模式】 Web 认证模板配置模式

【使用指导】 某些 app 无法执行 javascript 脚本动作时，需要配置成 http 封装格式触发重定向

配置服务器加密密钥

【命令格式】 **web-auth portal key** { *key-string* }

【参数说明】 portal 服务器的加密密钥，。配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符。

【命令模式】 全局配置模式

【使用指导】 -

配置接口上启用 Web 认证

【命令格式】 **web-auth enable** { **eportalv2 |** *template-name* }

【参数说明】 自定义模板名

【命令模式】 接口配置模式

【使用指导】 -

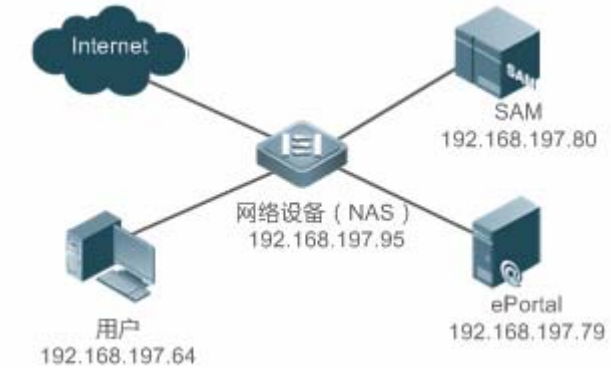
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

二代 Web 认证

【网络环境】

图 1-10



【配置方法】

- 在网络设备上开启 AAA
- 在网络设备配置 RADIUS 服务器和密钥
- 在网络设备配置 AAA 的 web 认证默认方法列表和默认网络记账方法列表
- 在网络入设备上设置认证服务器的 IP 地址及与认证服务器进行通信的密钥(ruijie)
- 在网络设备上设置认证页面的主页地址
- 在网络设备上配置全局使用二代 portal 进行认证
- 在网络设备上对 GigabitEthernet 0/2、GigabitEthernet 0/3 两个端口上开启 Web 认证功能

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 192.168.197.79 key ruijie
Ruijie(config)#aaa authentication web-auth default group radius
Ruijie(config)#aaa accounting network default start-stop group radius
Ruijie(config)#web-auth template eportalv2
Ruijie(config.tmplt.eportalv2)#ip 192.168.197.79
Ruijie(config.tmplt.eportalv2)#exit
Ruijie(config)#web-auth portal key ruijie
Ruijie(config)# web-auth template eportalv2
Ruijie(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp
Ruijie(config.tmplt.eportalv2)#exit
Ruijie(config)# interface range GigabitEthernet 0/2-3
Ruijie(config-if-range)# web-auth enable eportalv2
Ruijie(config-if-range)# exit
```

【检验方法】

- web 认证配置是否成功

```
Ruijie(config)#show running-config
…
aaa new-model
aaa authentication web-auth default group radius
aaa accounting network default start-stop group radius
…
radius-server host 192.168.197.79 key ruijie
…
web-auth template eportalv2
 ip 192.168.197.79
 url http://192.168.197.79:8080/eportal/index.jsp
!
web-auth portal key ruijie
…
interface GigabitEthernet 0/2
 web-auth enable eportalv2
```

```
!
interface GigabitEthernet 0/3
 web-auth enable eportalv2
```

```
Ruijie#show web-auth control
 Port                       Control  Server Name           Online User Count
 -------------------------- -------- --------------------- -----------------
…
 GigabitEthernet 0/2         On       eportalv2             0
 GigabitEthernet 0/3         On       eportalv2             0
…
```

```
Ruijie#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-mac-mode
  Type:      v2
  Port:      50100
  State:     Active
  Acctmlist: default
  Authmlist: default
…
```

常见错误

- Portal 服务器和设备间的 key 配置错误或者有一方配置了加密，一方未配置导致认证异常
- Radius 服务器和设备间参数配置不正确导致认证异常
- Portal 服务器不支持中移动 portal 协议规范导致无法对接

1.4.3 配置内置Portal Web认证

配置效果

未认证用户能够被重定向到认证页面并完成认证，无需外置 Portal 服务器。

注意事项

- 部分设备，比如 AP110 并没有内置页面包，使用前需要先导入页面包，具体产品对页面包的支持情况，请参考具体产品的说明。
- EG 设备上是基于全集配置内置 Portal Web 认证。
- 如果要使用自定义页面包，必须严格按照定制规范章节给出的说明实现。

配置方法

配置开启 AAA 认证

- 必须配置，要使用二代 Web 认证功能，必须开启 AAA 认证。
- 内置 Portal Web 认证向服务器发起认证的功能由设备完成，在设备 AAA 功能实现。

配置 RADIUS 服务器和密钥

- 必须配置，要成功内置 Portal Web 认证功能，必须设置 RADIUS 服务器。
- 用户账户信息保存在 RADIUS 服务器上，设备需要连接 RADIUS 服务器来确认用户身份合法性。

配置 AAA 中 Web 认证方法

- 必须配置，要成功应用内置 Portal Web 认证功能，必须设置 AAA 认证方法。
- 认证方法列表将 Web 认证的请求和 RADIUS 服务器关联起来，设备依据认证方法列表来选择认证方式和对应的服务器。

配置 AAA 网络记账方法

- 可选配置，部分服务器要求认证和记账必须同时开启，因此是否配置记账要根据服务器特性决定。
- 记账方法用于关联对应的记账方式和服务器，Web 认证需要记账功能记录用户信息或费用。

配置内置 iportal 模板

- 必须创建 iportal 模板。
- 如果之前创建的认证、计费方法不是 default，则需要在模板中配置对应名字，否则默认使用 default。

在全局或者端口上开启 Web 认证功能

- 必须配置。

检验方法

- 未认证用户被要求认证，弹出页面为内置页面包中的对应页面文件。
- 已认证用户可以正常使用网络。

相关命令

开启 AAA 功能

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 aaa 的方法列表等命令需要在功能开启后才能输入

配置 RADIUS 服务器和密钥

【命令格式】 **radius-server host** { *ip-address* } [**auth-port** *port-number1*] [**acct-port** *port-number 2*] **key** { *string* }
【参数说明】 *ip-address*：服务器 IP 地址
port-number1：认证端口号
port-number2：记账端口号
string：密钥字符串
【命令模式】 全局配置模式
【使用指导】 认证端口默认 1812，记账端口默认 1813

配置 AAA 中 Web 认证方法列表

【命令格式】 **aaa authentication iportal** { **default** | *list-name* } *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2
【命令模式】 全局配置模式
【使用指导】 方法名需要和 AAA 的配置一致

配置网络记账方法列表

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2
【命令模式】 全局配置模式
【使用指导】 方法名需要和 AAA 的配置一致

创建模板

【命令格式】 **web-auth template iportal**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 -

配置用户认证前广告推送 URL

【命令格式】 **login-popup** { *url-string* }
【参数说明】 推送广告的地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置用户认证成功后广告推送 URL

【命令格式】 **online-popup {**url-string**}**
【参数说明】 推送广告的地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置定制页面包

【命令格式】 **page-suit** { *filename* }
【参数说明】 指定页面包的文件名。
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置内置广告弹出周期

【命令格式】 **time-interval** {*hour*}
【参数说明】 广告弹出周期。
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置接口上启用 web 认证

【命令格式】 **web-auth enable iportal**
【参数说明】 自定义模板名
【命令模式】 接口配置模式或者全居配置模式
【使用指导】 -

配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

内置 Portal Web 认证

【配置方法】
- 在网络设备上开启 AAA
- 在网络设备配置 RADIUS 服务器和密钥
- 在网络设备配置 AAA 的 Web 认证默认方法列表和默认网络记账方法列表
- 在网络设备上配置全局使用内置 Portal 进行认证
- 在网络设备上对 GigabitEthernet 0/2、GigabitEthernet 0/3 两个端口上开启 Web 认证功能

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 192.168.197.79 key ruijie
Ruijie(config)#aaa authentication iportal default group radius
Ruijie(config)#aaa accounting network default start-stop group radius
```

```
Ruijie(config)#web-auth template iportal
Ruijie(config.tmplt.iportal)#exit
Ruijie(config)# interface range GigabitEthernet 0/2-3
Ruijie(config-if-range)# web-auth enable iportal
Ruijie(config-if-range)# exit
```

【检验方法】

- web 认证配置是否成功

```
Ruijie(config)#show running-config
…
aaa new-model
aaa authentication web-auth default group radius
aaa accounting network default start-stop group radius
…
radius-server host 192.168.197.79 key ruijie
…
web-auth template iportal
!
…
interface GigabitEthernet 0/2
 web-auth enable iportal
!
interface GigabitEthernet 0/3
 web-auth enable iportal
```

```
Ruijie#show web-auth control
 Port                      Control  Server Name           Online User Count
 ------------------------- -------- --------------------- -----------------
…
 GigabitEthernet 0/2        On       iportal              0
 GigabitEthernet 0/3        On       iportal              0
…
```

```
Ruijie#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:      iportal
  Page-suit: default
  BindMode:  ip-mac-mode
  Type:      Intral Portal
  Advertising: null
  Advertising mode : online-popup
  Acctmlist: default
  Authmlist: default
```

```
...
```

常见错误

- 定制新页面包时未按定制规范制作
- 指定了定制页面包但是页面包未下载到 FLASH 或者未下载到指定目录

1.4.4 配置WiFiDog认证功能

配置效果

未认证用户能够被重定向到认证页面并完成认证

注意事项

无

配置方法

↘ 配置 portal 服务器

- 必须配置，要成功应用 Web 认证功能，必须设置并应用 portal 服务器。
- 当设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户可以直接与这个地址进行 HTTP 通讯。

↘ 配置设备 IP

- 必须配置，缺省情况下无配置。
- 该 IP 是给用户访问的，因此应该配置一个用户能访问到设备 IP.

↘ 在端口上开启 Web 认证功能

- 必须配置。
- 当 Web 认证功能基于端口开启时，默认情况下，端口未开启 Web 认证功能，此时这个端口下所连接的用户不进行 Web 认证。

检验方法

- 未认证用户被要求认证
- 已认证用户可以正常使用网络

相关命令

创建模板

【命令格式】 **web-auth template wifidog**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 wifidog 为默认的 WiFiDog 认证模板

配置服务器 IP

【命令格式】 **ip** { *ip-address* }
【参数说明】 portal 服务器的地址
【命令模式】 web 认证模板配置模式
【使用指导】 -

配置服务器 URL

【命令格式】 **url** { *url-string* }
【参数说明】 portal 服务器的认证页面地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://开头

配置设备 IP

【命令格式】 **nas-ip** { *ip-address* }
【参数说明】 设置 wifidog 的设备接入服务 ip，用于服务器向此 ip 发起通讯
【命令模式】 Web 认证模板配置模式
【使用指导】 配置的设备接入服务 ip 不能够被设置成直通地址
配置接入服务 ip 为设备 ip 时会导致此认证模板下的终端访问此 ip 时被设备拦截并转发给服务器，从而不能访问设备的 web 管理界面。
如有此认证模板下的终端直接访问此 ip 对此设备进行管理的需求，可将此接入服务 ip 设置为一个未使用的虚拟服务 ip，如 1.1.1.1， 2.2.2.2 等。

配置 Gateway ID

【命令格式】 **gateway-id** { *string* }
【参数说明】 Wifidog 协议使用的 gw-id 值，默认情况下为本设备的 MAC 地址
【命令模式】 Web 认证模板配置模式
【使用指导】 该参数为 wifidog 协议交互报文中需要携带的参数，开放命令给对接第三方 portal 使用.

配置接口上启用 web 认证

【命令格式】 **web-auth enable**
【参数说明】 -
【命令模式】 接口配置模式

【使用指导】 -

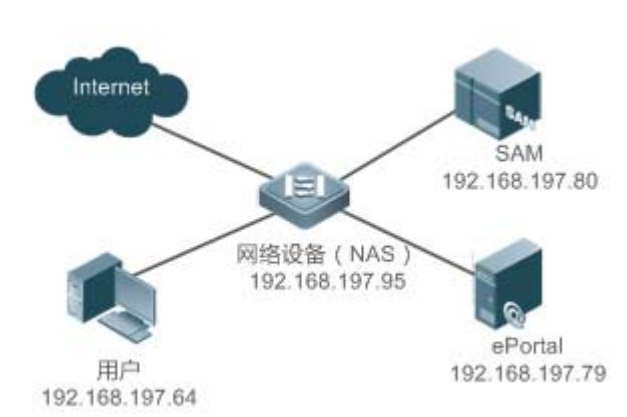
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

WiFiDog 认证

【网络环境】

图 1-11



【配置方法】

- 在网络设备上设置认证服务器的 IP 地址
- 在网络设备上设置认证页面的主页地址
- 在网络设备上设置设备 IP 地址
- 在网络设备上对 wlan 10 开启 Web 认证功能

```
Ruijie# config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#web-auth template wifidog
Ruijie(config.tmplt.wifidog)#ip 192.168.197.79
Ruijie(config.tmplt.wifidog)#url http://192.168.197.79/auth/wifidogAuth
Ruijie(config.tmplt.wifidog)#nas-ip 1.1.1.1
Ruijie(config.tmplt.wifidog)#exit
Ruijie(config)# wlansec 10
Ruijie(config-wlansec)# web-auth portal wifidog
Ruijie(config-if-range)# webauth
Ruijie(config-if-range)# exit
```

【检验方法】

- web 认证配置是否成功

```
Ruijie(config)#show running-config
…
web-auth template wifidog
 ip 192.168.197.79
 nas-ip 1.1.1.1
```

```
 url http://192.168.197.79/auth/wifidogAuth
…
wlansec 10
 web-auth portal wifidog
 webauth
```

```
Ruijie#show web-auth control
Port                        Control  Server Name           Online User Count
 -------------------------- -------- --------------------- ------------------
 wlansec 10                  On       wifidog               0                 …
```

```
Ruijie#show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:           wifidog
  Type:           wifidog
  Ip:             192.168.197.79
  Url:            http://192.168.197.79/auth/wifidogAuth
  NasIp:          1.1.1.1
……
```

常见错误

- 没配置设备 IP 导致无法重定向。

1.4.5 配置MAC短信认证功能

配置效果

未认证用户关联到 WLAN 后，允许使用网络，但用户在指定周期内使用了指定阈值的流量时，认证设备向绑定 Portal 服务器发起 MAC 绑定查询。如果用户为已绑定状态，绑定 Portal 发起认证请求，用户进行认证；如果用户为未绑定状态，用户需要通过 Portal 认证来接入网络。

注意事项

- MAC 短信认证功能只支持无线设备。
- 创建的 Portal 服务器 URL 必须是 cmcc-ext1 格式。

配置方法

↘ 开启 AAA 功能

- 必须配置，要使用二代 Web 认证功能，必须开启 AAA 认证。
- 二代 web 认证向服务器发起认证的功能由设备完成，在设备 AAA 功能实现。

【命令格式】 **aaa new-model**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 aaa 的方法列表等命令需要在功能开启后才能输入

配置 RADIUS 服务器和密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置 RADIUS 服务器。
- 用户账户信息保存在 RADIUS 服务器上，设备需要连接 RADIUS 服务器来确认用户身份合法性。

【命令格式】 **radius-server host** { *ip-address* } [**auth-port** *port-number1*] [**acct-port** *port-number 2*] **key** { *string* }
【参数说明】 *ip-address*：服务器 IP 地址
port-number1：认证端口号
port-number2：记账端口号
string：密钥字符串
【命令模式】 全局配置模式
【使用指导】 认证端口默认 1812，记账端口默认 1813

配置 AAA 中 Web 认证方法列表

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 认证方法。
- 认证方法列表将 web 认证的请求和 RADIUS 服务器关联起来，设备依据认证方法列表来选择认证方式和对应的服务器。

【命令格式】 **aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2
【命令模式】 全局配置模式
【使用指导】 二代 web 认证通常使用 RADIUS 认证方法

配置网络记账方法列表

- 必须配置，要成功应用二代 Web 认证功能，必须设置 AAA 网络记账方法。
- 记账方法用于关联对应的记账方式和服务器，web 认证需要记账功能记录用户信息或费用。

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
【参数说明】 *list-name*：方法列表名
method1：方法 1
method2：方法 2
【命令模式】 全局配置模式
【使用指导】 二代 web 认证通常使用 RADIUS 记账方法

创建模板

- 必须配置，要成功应用二代 Web 认证功能，必须设置并应用 portal 服务器。
- 当接入/汇聚设备发现未认证用户试图通过 HTTP 访问网络资源时，设备将用户的访问请求重定向到指定的 portal 认证页面，通过认证页面，引导用户向认证服务器发起认证。Portal 服务器地址将被设置为一个特殊的免认证的网络资源，未认证用户才可以直接与这个地址进行 HTTP 通讯。

【命令格式】 **web-auth template** { **eportalv2 |** *portal-name* **v2** }
【参数说明】 自定义的 portal 服务器名
【命令模式】 全局配置模式
【使用指导】 eportalv2 为默认的二代 web 认证模板

配置服务器 IP

【命令格式】 **ip** { *ip-address* | *ipv6-address* }
【参数说明】 portal 服务器的地址
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置服务器 URL

【命令格式】 **url** { *url-string* }
【参数说明】 portal 服务器的认证页面地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置 Portal 服务器 URL 格式

【命令格式】 **fmt { cmcc-ext1 | cmcc-normal | ruijie }**
【参数说明】 portal 服务器的 url 格式
【命令模式】 Web 认证模板配置模式
【使用指导】 fmt 参数为必须配置为 cmcc-ext1。

配置服务器加密密钥

- 必须配置，要成功应用二代 Web 认证功能，必须设置接入/汇聚设备与认证服务器进行通信的密钥。
- 当设备发现未认证用户在访问网络资源时，设备将通过重定向功能，向用户弹出认证页面，通过认证页面，引导用户向认证服务器发起认证。在认证过程中，设备与认证服务器间通过密钥对部分数据进行加密，以加强安全性。

【命令格式】 **web-auth portal key** { *key-string* }
【参数说明】 portal 服务器的加密密钥，。配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符。
【命令模式】 全局配置模式
【使用指导】 -

配置触发 MAC 绑定状态查询的周期和阈值

- 终端关联上打开 MAC 短信认证的 WLAN 后，可以在配置周期内使用免费流量，超过阈值后，触发 MAC 绑定查询。

【命令格式】 **web-auth sms-flow interval** *interval* **threshold** *flows*
【参数说明】 interval 为检测周期单位分钟，flows 为检测间隔，单位 KB

【命令模式】 全局配置模式
【使用指导】 -

配置绑定 Portal 服务器

- 必须配置。

【命令格式】 **web-auth bind-portal** *string* **[type {** *local-spec* **|** *group-spec***}]**
【参数说明】 string 为自定义模板名
【命令模式】 WLANSEC 配置模式
【使用指导】 -

配置 winterface 参数

- 配置重定向 URL 中带的 winterface 参数。

【命令格式】 **web-auth winterface** *string*
【参数说明】 winterface 参数字段
【命令模式】 WLANSEC 配置模式
【使用指导】 -

配置 AC IP ADDRESS

- 配置重定向 URL 中带的 ACIP 参数。

【命令格式】 **web-auth wlan-ac-ip** *ipv4*
【参数说明】 acip 参数字段
【命令模式】 WLANSEC 配置模式
【使用指导】 -

检验方法

- 未认证用户流量未达到阈值可以访问网络。
- 流量超过配置阈值后，触发认证。

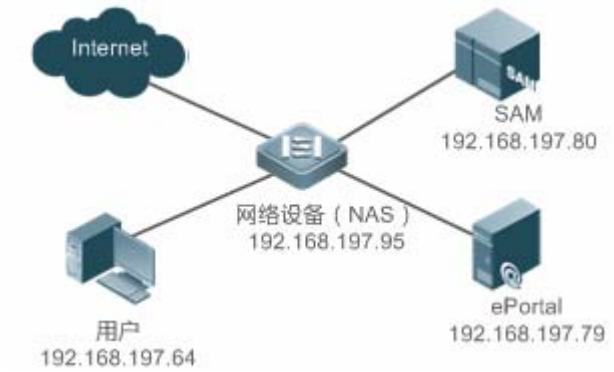
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

MAC 短信认证

【网络环境】

图 1-12



【配置方法】

- 在网络设备上开启 AAA
- 在网络设备配置 RADIUS 服务器和密钥
- 在网络设备配置 AAA 的 web 认证默认方法列表和默认网络记账方法列表
- 在网络入设备上设置认证服务器的 IP 地址及与认证服务器进行通信的密钥(ruijie)
- 在网络设备上设置认证页面的主页地址
- 在网络设备上 MAC 短信认证检测周期和阈值，指定 winterface 参数和 acip 参数
- 在网络设备上对 WLANSEC1 开启 MAC 短信认证功能

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 192.168.197.79 key ruijie
Ruijie(config)#aaa authentication web-auth default group radius
Ruijie(config)#aaa accounting network default start-stop group radius
Ruijie(config)#web-auth template eportalv2
Ruijie(config.tmplt.eportalv2)#ip 192.168.197.79
Ruijie(config.tmplt.eportalv2)#exit
Ruijie(config)#web-auth portal key ruijie
Ruijie(config)# web-auth template eportalv2
Ruijie(config.tmplt.eportalv2)#url http://192.168.197.79:8080/eportal/index.jsp
Ruijie(config.tmplt.eportalv2)#fmt cmcc-ext1
Ruijie(config.tmplt.eportalv2)#exit
Ruijie(config)# web-auth sms-flow interval 5 threshold 10
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# web-auth bind-portal eportalv2
Ruijie(config-if-range)# exit
```

【检验方法】

- web 认证配置是否成功

```
Ruijie(config)#show running-config
…
aaa new-model
aaa authentication web-auth default group radius
```

```
aaa accounting network default start-stop group radius
…
radius-server host 192.168.197.79 key ruijie
…
web-auth template eportalv2
 ip 192.168.197.79
 url http://192.168.197.79:8080/eportal/index.jsp
 fmt cmcc-ext1
!
web-auth portal key ruijie
web-auth sms-flow interval 5 threshold 10
…
wlansec 1
 web-auth bind-portal eportalv2
!
interface GigabitEthernet 0/3
 web-auth enable eportalv2
```

常见错误

- Portal 服务器和设备间的 key 配置错误或者有一方配置了加密，一方未配置导致认证异常
- Radius 服务器和设备间参数配置不正确导致认证异常
- Portal 服务器不支持中移动 portal 协议规范导致无法对接

1.4.6 配置微信连wifi认证功能

配置效果

1、 未认证手机终端用户关联到 WLAN 后，使用浏览器可以重定向到微信连 wifi 一键上网页面，通过页面上的链接可以直接唤醒微信客户端进行微信连 wifi 认证。
2、 未认证的手机终端用户扫描微信连 wifi 的二维码之后，可以进行微信连 wifi 认证
3、 未认证的 pc 用户关联到 WLAN 后，使用浏览器可以重定向到微信连 wifi 的二维码页面，通过关联同一个 WLAN 的手机终端用户扫描这个二维码，可以让 pc 用户直接认证通过上网。

注意事项

- 微信连 wifi 认证功能只支持无线设备。

配置方法

创建微信连 wifi 模板

- 必须配置，要使用微信连 wifi 认证，必须配置微信连 wifi 模板。

【命令格式】 **web-auth template** { **wechat | (***portal-name* **wechat** *)*}
【参数说明】 自定义的微信连 wifi 模板名-
【命令模式】 全局配置模式
【使用指导】 wechat 为默认的微信连 wifi 认证模板

配置服务器 IP

- 必须配置，要使用微信连 wifi 认证，必须配置服务器地址。

【命令格式】 **ip** *ip-address*
【参数说明】 配置 ip 地址
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置服务器 URL

- 必须配置，要使用微信连 wifi 认证，必须配置服务器的 url 地址。

【命令格式】 **service-url** { *url-string* }
【参数说明】 服务器的 url 地址
【命令模式】 Web 认证模板配置模式
【使用指导】 只要配置域名，不要以 http://或者 https://开头

配置 Portal 服务器的认证页面地址

- 缺省情况下配置为当前与服务器使用微信与短信共存认证时的短信认证重定向地址。

【命令格式】 **url** { *url-string* }
【参数说明】 该地址为使用微信与短信共存认证时的短信认证重定向地址
【命令模式】 Web 认证模板配置模式
【使用指导】 以 http://或 https://开头

配置与服务器通讯的加密密钥 KEY

- 必须配置，要使用微信连 wifi 认证，必须配置服务器的加密密钥。

【命令格式】 **key** *key-string*
【参数说明】 服务器的加密密钥。配置设备与认证服务器进行通信的密钥；密钥最大长度为 255 个字符
【命令模式】 Web 认证模板配置模式
【使用指导】 加密密钥必须和服务器上配置的一致，否则会出现对接不成功的问题。

配置使用微信连 wifi 的版本

- 可选配置，默认使用 1.0 的版本，可通过配置 16wifi 使用七彩的微信扫一扫功能。

【命令格式】 **version** {**1.0** | **16wifi | 3.0** }
【参数说明】 使用微信连 wifi 认证的版本。默认使用我司的微信连 wifi 的 1.0 版本。11.1(5)B9 版本默认使用的是我司的微

信连 wifi 的 3.0 版本。

【命令模式】 Web 认证模板配置模式

【使用指导】 使用 16wifi 版本，需要配置 http redirect port 4990 命令来拦截 tcp 4990 端口的报文。

配置开启 PC 免认证功能

- 可选配置，配置之后，通过终端识别识别成 PC 或者 Other 的终端不需要进行微信连 wifi 认证就可以上网。

【命令格式】 **free-auth pc**

【参数说明】

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置微信连 wifi 无感知认证功能

- 可选配置。

【命令格式】 **web-auth sta-perception enable**

【参数说明】

【命令模式】 全局配置模式和 WLAN 安全配置模式

【使用指导】 根据客户需求配置，开启之后同时要开启 ip dhcp snooping 功能才能实现无感知功能。

微信连 wifi1.0 版本配置开启单体逃生功能

- 可选配置，配置之后，如果终端在规定时间内没有发起登录授权请求，就认为服务器可能出故障了，于是放行表项，让用户逃生可以上网。

【命令格式】 **escape interval** *seconds* **online-time** *minutes*

【参数说明】 *seconds*：逃生判定定时器间隔，单位：秒钟，建议值为 5s

minutes：逃生用户可上网时长，单位：分钟，0 表示不限制上网时长

【命令模式】 Web 认证模板配置模式

【使用指导】 -

微信连 wifi3.0 版本配置开启单体逃生功能

- 可选配置，配置之后，如果终端因为多次点击微信认证发起临时放行请求次数达到配置值而未认证成功，则放行表项，让用户逃生可以上网。

【命令格式】 **escape user-try-auth** *counts* **online-time** *minutes*

【参数说明】 *counts*：配置用户尝试点击微信认证次数，达到配置次数仍未上线就让用户逃生。单位：次，建议值为 4 次

minutes：配置逃生用户的可用时长。单位：分钟

【命令模式】 Web 认证模板配置模式

【使用指导】 -

配置开启集体逃生功能

- 可选配置，配置后，设备开始统计单体逃生用户数，如果一定间隔内单体逃生用户数达到阀值，就开启集体逃生，后面接入的所有用户都直接逃生免认证。

- WLANSEC 配置模式下 11.1(5)B23 支持该功能。WLANSEC 模式下的配置优先生效，若 WLANSEC 模式下未配置则使用全局下的配置。
- 如果要取消集体逃生状态，可以在全局配置模式使用 **web-auth wechat-escape recover** 恢复成单体逃生状态。

【命令格式】 **web-auth wechat-escape interval** *minutes* **times** *count*
【参数说明】 *minutes*：集体逃生判定定时器间隔，单位：分钟，默认值为 60 分钟
count：用户数阀值，默认 5 个
【命令模式】 全局配置模式和 WLANSEC 配置模式
【使用指导】 WLANSEC 配置模式下，11.1(5)B23 支持该功能。

配置服务器检测功能

- 可选配置，配置后，设备开始对服务器进行检测，如果一定间隔内（由 **interval** *minutes* 指定）检测到服务器没有应答或者回应不可用，同时设备配置了集体逃生功能，后面接入的所有用户都直接逃生免认证。
- 如果要取消服务器检测，可以在全局配置模式使用 **no web-auth wechat-check** 取消服务器检测功能。

【命令格式】 **web-auth wechat-check interval** *minutest*
【参数说明】 *minutes*：服务器检测定时器间隔，单位：分钟，无默认值
【命令模式】 全局配置模式
【使用指导】 -

配置开启临时放行功能

- 可选配置，配置后，在认证过程中用户的报文直通（和 MCP 服务器，腾讯服务器交互的报文放行，但是黑名单、登录授权、强制关注等请求还会被拦截进行相关业务处理）。

【命令格式】 **temporary-permit** *seconds*
【参数说明】 *seconds*：临时放行的时长，单位：秒钟，建议值为 30s~60s
【命令模式】 Web 认证模板配置模式
【使用指导】 -

配置无感知的 ip 校验功能

- 可选配置，配置后，超过时间用户还未获取 IP 地址，就将被踢下线。

【命令格式】 **web-auth valid-ip-acct [timeout** *seconds***]**
【参数说明】 *seconds*： 允许等待用户获取 IP 的时间，单位：秒钟，默认值为 30s
【命令模式】 全局配置模式
【使用指导】 -

检验方法

- 未认证用户被要求认证

- 已认证用户可以正常使用网络

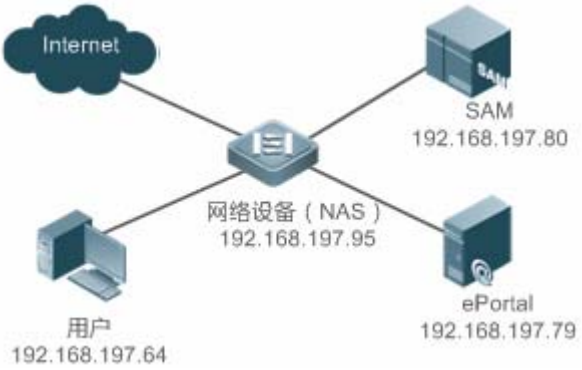
配置举例

以下配置举例，仅介绍与 Web 认证相关的配置。

微信连 wifi 认证

【网络环境】

图 1-10



【配置方法】

- 在网络设备上配置域名服务器地址 192.168.58.110
- 在网络设备上配置微信连 wifi 认证模板
- 在网络设备上配置服务器的 ip 和 service-url 地址
- 在网络设备上配置与服务器进行通信的加密密钥(ruijie)
- 在网络设备上配置设备的 ip 地址
- 在网络设备上配置使用的微信连 wifi 认证的版本(1.0)
- 在网络设备上对 WLANSEC1 应用模板并开启微信连 wifi 认证功能

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip name-server 192.168.58.110
Ruijie(config)#web-auth template wechat
Ruijie(config.tmplt.wechat)#ip 192.168.197.79
Ruijie(config.tmplt.wechat)#service-url wmc.ruijie.com.cn
Ruijie(config.tmplt.wechat)#key ruijie
Ruijie(config.tmplt.wechat)#nas-ip 1.1.1.1
Ruijie(config.tmplt.wechat)#version 1.0
Ruijie(config.tmplt.wechat)#exit
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# web-auth portal wechat
Ruijie(config-wlansec)# webauth
```

【检验方法】

- web 认证配置是否成功

```
Ruijie(config)#show running-config
…
```

```
ip name-server 192.168.58.110
…
web-auth template wechat
 ip 192.168.197.79
 service-url wmc.ruijie.com.cn http://192.168.197.79:8080/eportal/index.jsp
 key ruijie
 nas-ip 1.1.1.1
!…
wlansec 1
 web-auth portal wechat
 webauth
!
```

常见错误

- 服务器和设备间的 key 配置错误或者有一方配置了加密，一方未配置导致认证异常
- 设备 ip 地址配置成直通，web 认证无法收到认证报文，导致认证失败
- 域名服务器地址没有配置导致白名单解析失败，微信服务器地址没有放行
- 开启无感知认证时没有配置 ip dhcp snooping、ip dhcp snooping trust 和 web-auth sta-perception enable 命令，导致二次认证无感知失效

1.4.7 配置认证方法列表名

配置效果

- 当用户提交认证信息时，Portal 服务器会向设备发起认证请求，设备依据配置的认证方法列表名解析认证服务器等信息，发起认证过程。
- 配置认证方法列表名后，设备可以通过指定的方法列表名选择认证服务器进行认证。

注意事项

- 配置认证方法列表名前，必须保证在 AAA 中已经定义了该方法。对应定义命令为 **aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]。
- 无法分别给 ipv4 和 ipv6 认证指定不同的认证方法。

配置方法

- 可选配置
- 默认使用 default 方法，在 AAA 修改方法列表名或存在多个方法列表名时，使用本命令进行配置。

检验方法

- 在 AAA 中配置两个方法列表，方法列表 1 使用服务器 1，方法列表 2 使用服务器 2
- 在服务器 1 创建用户 a 和密码；服务器 2 创建用户 b
- 配置使用方法列表 1
- 用户使用账号 b 进行认证，认证失败
- 用户使用账户 a 进行认证，认证成功

相关命令

配置认证方法列表名

【命令格式】 **authentication** { *mlist-name* }
【参数说明】 方法列表名
【命令模式】 Web 认证模板配置模式
【使用指导】 应与 AAA 中 web 认证方法列表名一致

配置举例

配置认证方法列表名

【配置方法】
- 配置认证方法列表名为 mlist1

```
Ruijie(config.tmplt.iportal)#authentication mlist1
```

【检验方法】
- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-only-mode
  Type:      v2
  Port:      50100
  State:     Active
  Acctmlist: default
  Authmlist: mlist1
```

1.4.8 配置记账方法列表名

配置效果

- 用户认证通过后，设备会自动发起记账请求，请求的对象依赖于记账方法列表的配置，通常为认证所在服务器。
- 配置记账方法列表名后，设备可以通过指定的方法列表名选择记账服务器进行记账。

注意事项

- 配置记账方法列表名前，必须保证在 AAA 中已经定义了该方法。对应定义命令为 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]。
- 无法分别给 ipv4 和 ipv6 认证指定不同的记账方法。

配置方法

- 可选配置
- 默认使用 default 方法，在 AAA 修改方法列表名或存在多个方法列表名时，使用本命令进行配置。

检验方法

- 在 AAA 中配置两个记账方法列表，方法列表 1 使用服务器 1，方法列表 2 使用服务器 2
- 配置使用方法列表 1
- 用户使用合法账号进行认证上线
- 在服务器 1 和服务器 2 上分别查看用户记账信息；只有服务器 1 存在

相关命令

↘ 配置记账方法列表名

【命令格式】 **accounting** { *mlist-name* }
【参数说明】 方法列表名
【命令模式】 Web 认证模板配置模式
【使用指导】 应与 AAA 中网络记账方法列表名一致

配置举例

↘ 配置记账方法列表名

【配置方法】
- 配置记账方法列表名为 mlist1

```
Ruijie(config.tmplt.eportalv2)#accounting mlist1
```

【检验方法】

- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-mac-mode
  Type:      v2
  Port:      50100
  State:     Active
  Acctmlist: mlist1
  Authmlist: mlist1
```

1.4.9 配置Portal服务器通信端口

配置效果

- 设备检测到用户下线等情况时，需要同时通告 portal 服务器用户下线；设备和 portal 服务器使用 portal 协议进行交互，协议使用约定的端口号进行报文侦听和收发。
- 当 portal 服务器侦听端口改变时，设备需要修改 portal 服务器通信端口才能进行交互。
- 如果是内置 Portal Web 认证，此功能用于配置本机监听的 http 端口，默认是 8081.

注意事项

- 端口号配置需要和服务器实际使用端口相一致。
- 适用于二代 Web 认证和内置 Portal Web 认证，且两种认证的默认端口号不一样。二代 Web 认证端口号用于设备和 Portal 服务器交互 Portal 协议，内置 Portal Web 认证的端口号用于本机报文监听。

配置方法

- 可选配置
- 服务器不使用默认端口号或者本机监听端口有冲突需要调整时，使用本命令配置来保持一致。

检验方法

- 配置二代 Web 认证

- 改变服务器侦听端口为 10000
- 通过本命令配置端口号为 10000
- 用户 web 认证上线
- 在设备端踢用户下线，刷新在线页面，提示用户下线

相关命令

配置 portal 服务器通信端口

【命令格式】 **port** *port-num*

【参数说明】 *port-num*：端口号

【命令模式】 web 认证模板配置模式

【使用指导】 -

配置举例

配置 portal 服务器通信端口

【配置方法】
- 配置服务器通信端口为 10000

```
Ruijie(config.tmplt.eportalv2)#port 10000
```

【检验方法】
- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-only-mode
  Type:      v2
  Port:      10000
  Acctmlist:
  Authmlist:
```

1.4.10 配置绑定模式

配置效果

- 用户成功上线时，需要将用户表项写到转发规则中，指定不同的绑定模式，可以改变转发规则的匹配方式，影响用户的上网规则。比如仅 IP 绑定时，只要符合该 IP 的报文都被放行，用户都能上网；而 IP+MAC 绑定时，只有同时符合该 IP 和 MAC 的用户能访问网络。

注意事项

- 在三层认证场景中，设备看到的 MAC 地址都是用户网关地址，MAC 地址都不准确，此时应该采用仅 IP 绑定模式。

配置方法

- 可选配置，缺省默认：IP+MAC 绑定。
- 依据设备能获得的用户准确信息决定选择哪种绑定模式 ,当用户 IP、MAC 均准确时 ,比如二层网络部署 ,优先选择 IP+MAC 绑定；否则优先选择仅 IP 绑定模式。

检验方法

- 改变绑定模式为仅 IP 模式
- 用户认证上线
- 修改用户 MAC，或者使用另一台同 IP，不同 MAC 的客户端访问网络
- 用户上网正常

相关命令

配置绑定模式

【命令格式】 **bindmode {ip-mac-mode | ip-only-mode}**

【参数说明】 **ip-mac-mode**：IP+MAC 同时绑定

ip-only-mode：仅 IP 绑定

【命令模式】 web 认证模板配置模式

【使用指导】 -

配置举例

配置绑定模式

【配置方法】

- 配置绑定模式为仅 IP 模式

```
Ruijie(config.tmplt.eportalv2)#bindmode ip-only-mode
```

【检验方法】

- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
```

【配置方法】
- 配置绑定模式为仅 IP 模式

```
Ruijie(config.tmplt.eportalv2)#bindmode ip-only-mode
```

【检验方法】
- 查看配置是否成功

```
------------------------------------------------------------
  Name:       eportalv2
  Url:        http://17.17.1.21:8080/eportal/index.jsp
  Ip:         17.17.1.21
  BindMode:   ip-only-mode
  Type:       v2
  Port:       10000
  Acctmlist:
  Authmlist:
```

1.4.11 配置定制页面包

配置效果

- 用户可以指定内置 Portal 使用特定页面包，然后在这些页面包上嵌入一些特色内容或者信息，比如特有的 LOGO 或者公告信息等。

注意事项

- 页面包需要手工下载到设备的 FLASH 中，并且固定存放在./portal 目录下，如果未事先存放页面包或者存放目录错误，会导致无法推送页面，进而导致 web 认证时效。如果对页面包没特殊要求，可以使用设备默认页面包。
- 页面包的定制规范请参考”页面包定制规范”。

配置方法

- 可选配置，缺省使用设备自带的页面包。

检验方法

- 配置内置 Portal Web 认证。
- 下载新的页面包。
- 指定使用该页面包。
- 用户上网，登录页面为定制页面。

相关命令

↘ 配置定制页面包

【命令格式】 **page-suit** *filename*

【参数说明】 *filename*：定制页面包的文件名

【命令模式】 web 认证模板配置模式

【使用指导】 新的页面包需要提前下载到 FLASH 的./porta/zipl 目录。

配置举例

↘ 配置定制页面包

【配置方法】

- 配置定制页面包

```
Ruijie(config.tmplt.iportal)#page-suit ruijiepage
```

【检验方法】

- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      iportal
  Page-suit:    ruijiepage
  Advertising url:  default
  Advertising mode: online-popup
  Type:      Intral Portal
  Acctmlist:default
  Authmlist:default
```

1.4.12 配置广告推送方式

配置效果

- 可选则认证前弹出广告、认证后弹出广告。

注意事项

- 默认是认证成功后弹广告。
- 如果要实现用户不认证，只弹广告的效果，请选择 Advertising 功能，具体参考 Advertising 的配置手册。

配置方法

- 可选配置，缺省认证成功后弹广告。

检验方法

- 配置内置 Portal Web 认证
- 配置一个可访问互联网 url 地址
- 用户上网，认证成功后浏览器弹出一个新窗口并显示指定 url 的页面信息

相关命令

配置广告推送地址

【命令格式】 **popup mode [login-popup | online-popup]** *url*

【参数说明】 **login-popup** ：认证前弹出，也是登录的时候弹出

online-popup：认证成功后弹出

url：配置的需要弹出的 URL 地址

【命令模式】 web 认证模板配置模式

【使用指导】 根据实际需要选择，默认为认证后弹出。

配置举例

配置广告推送模式

【配置方法】

- 配置广告推送模式为仅推送不认证

```
Ruijie(config.tmplt.iportal)#popup http://www.ruijie.com.cn/
Ruijie(config.tmplt.iportal)#popup mode login-popup
```

【检验方法】

- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      iportal
  Page-suit:   default
  Advertising url:  http://www.ruijie.com.cn/
  Advertising mode: login-popup
  Type:      Intral Portal
  Acctmlist:default
  Authmlist:default
```

1.4.13 配置定制化URL格式

配置效果

- 用户配置了定制化 URL 后，重定向到 portal 的 URL 会根据定制化的参数进行设置。

注意事项

- 定制化配置后的参数不支持加密，所有参数都是明文进行传输。

配置方法

- 可选配置

检验方法

- 配置定制化 URL
- 未认证 pc，使用浏览器访问该端口的外网网络
- 用户访问请求被重定向，重定向 URL 参数与配置的定制化 URL 一致

相关命令

↘ 配置定制化 URL 格式

【命令格式】 **fmt custom [encrypt { md5 | des | des_ecb | des_ecb3 | none }] [user-ip** *userip-str* **] [user-mac** *usermac-str* **mac-format [dot | line | none]] [user-vid** *uservid-str* **] [user-id** *userid-str* **] [nas-ip** *nasip-str* **] [nas-id** *nasid-str* **] [nas-id2** *nasid2-str* **] [ac-name** *acname-str* **] [ap-mac** *apmac-str* **mac-format [dot | line | none]] [url** *url-str* **] [ssid** *ssid-str* **] [port** *port-str* **] [ac-serialno** *ac-sno-str* **] [ap-serialno** *ap-sno-str* **] [additional** *extern-str* **]**

【参数说明】 *userip-str*：用户 ip 对应的参数名称
usermac-str：用户 mac 对应的参数名称
uservid-str：用户 vid 对应的参数名称
userid-str：用户 id 对应的参数名称
nasip-str：设备 ip 对应的参数名称
nasid-str：NAS 设备 ID 对应的参数名称
nasid2-str：NAS 设备 ID 对应的参数名称(支持定制两个 nasid 参数)
ac-name：设备名称对应的参数名称
apmac-str：关联 AP 的 MAC 地址对应的参数名称
url-str：用户原始访问 url 对应的参数名称
ssid-str：SSID 对应的参数名称

port-str：用户认证端口对应的参数名称
ac-sno-str：ac 设备序列号对应的参数名称
ap-sno-str：ap 设备序列号对应的参数名称
extern-str：固定字符串，某些 portal 需要一些特定字符串标识
md5：所配置参数采用 md5 加密
des：所配置参数采用 des 加密
des_ecb：所配置参数采用 des_ecb 加密
des_ecb3：所配置参数采用 des_ecb3 加密
none：所配置参数不加密，明文传输

【命令模式】 模板配置模式
【使用指导】 支持添加或删除单个参数。

配置举例

↘ 配置定制化 URL 格式

【配置方法】
- 配置明文用户 ip，用户 mac，nasip，ssid，url 等参数作为重定向 URL 参数

```
Ruijie(config.tmplt.eportalv2)# fmt custom encry none user-ip userip user-mac usermac mac-format none nas-ip nasip ssid ssid url firsturl
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
fmt custom encry none user-ip userip user-mac usermac mac-format none nas-ip nasip ssid ssid url firsturl
```

1.4.14 设置重定向的HTTP端口

配置效果

- 当用户访问网络资源时(例如使用浏览器上网)，此时用户会发出 HTTP 报文，接入/汇聚设备通过拦截来自用户的 HTTP 报文，来判断用户是否在访问网络资源。当设备检测到未认证的用户在访问网络资源时，将阻止用户访问网络资源，并向用户弹出认证页面。缺省情况下，网络设备通过拦截用户发出的端口号为 80 的 HTTP 报文，来检测用户是否在访问网络资源。
- 设置重定向的 HTTP 端口后，可以对用户发出的特定目的端口号的 HTTP 请求进行重定向。

注意事项

- 接入/汇聚设备上常用的管理协议端口（例如 22、23、53）以及系统内部保留的端口，不允许被设置为重定向端口。实际上，除了 80 端口外，HTTP 协议很少会使用小于 1000 的端口号。为了避免与知名 TCP 协议端口冲突，除非必要，尽量不要设置较小端口号的端口作为重定向端口。

配置方法

- 可选配置
- 在配置自动获取客户端时，如果要新增网络设备拦截用户发出的特定端口号的 HTTP 报文，可以进行该配置。

检验方法

- 配置拦截端口
- 未认证 pc，使用浏览器访问该端口的外网网络
- 用户访问请求被重定向到认证页面

相关命令

↘ 设置重定向的 HTTP 端口

【命令格式】 **http redirect port** *port-num*

【参数说明】 *port-num*：端口号

【命令模式】 全局配置模式

【使用指导】 最大允许配置 10 个不同的目的端口号，默认端口号(80，443)不含在该总数量范围内。

配置举例

↘ 设置重定向的 HTTP 端口

【配置方法】
- 配置 8080 端口为重定向的 HTTP 端口

```
Ruijie(config)#http redirect port 8080
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show web-auth rdport
Rd-Port:
80 443 8080
```

1.4.15 设置Web认证模块SYSLOG功能

配置效果

- 当用户上下线时，web 认证模块会通过 SYSLOG 将上下线的用户信息和事件呈现给管理员。缺省情况下，该 SYSLOG 信息被屏蔽。
- 设置 SYSLOG 限速功能后，可以按照一定的速率将该信息呈现出来。

注意事项

- 当认证上下线速率很高时，频繁的 SYSLOG 输出会影响设备性能，同时导致输出信息刷屏。

配置方法

- 可选配置
- 需要查看基本上下线 SYSLOG 信息时，可以配置 SYSLOG 限速功能。

检验方法

- 配置 SYSLOG 限速
- 用户按照一定速率上下线
- SYSLOG 按照限制要求打印输出

相关命令

↘ 设置 SYSLOG 限速

【命令格式】 **web-auth logging enable** *num*

【参数说明】 *num*：SYSLOG 输出速率（条/秒）

【命令模式】 全局配置模式

【使用指导】 0 为不限制速率；不输出受限的 SYSLOG。受限的 SYSLOG 不包括严重级 SYSLOG，及异常错误输出的 SYSLOG。

配置举例

↘ 设置 SYSLOG 限速

【配置方法】

- 配置不限制 SYSLOG 输出

```
Ruijie(config)#web-auth logging enable 0
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth logging enable 0
…
```

1.4.16 设置未认证用户的最大HTTP会话数

配置效果

- 未认证的用户在访问网络资源时，用户 PC 会发出 HTTP 会话连接请求，HTTP 报文会被接入/汇聚设备拦截，并通过重定向要求用户进行 Web 认证。为了防止同一个未认证用户发起过多的 HTTP 连接请求，以节约网络设备的资源，需要在设备上限制未认证用户的最大 HTTP 会话数。
- 由于用户在认证时，会占用一个 HTTP 会话，而用户的其他应用程序也可能占用着 HTTP 会话，因而不建议设置未认证用户的最大 HTTP 会话数为 1。缺省情况下，全局每个未认证用户的最大 HTTP 会话数为 255，而每个端口下的未认证用户的 HTTP 会话总数最大为 300。

注意事项

- 如果一个用户在进行 Web 认证时，出现经常无法弹出认证页面的情况，则很可能是受到最大 HTTP 会话数的限制了。此时，应该建议用户暂时关闭一些可能会占用 HTTP 会话的应用程序，然后再进行 Web 认证。

配置方法

- 可选配置
- 要更改每个未认证用户的最大 HTTP 会话数及每个端口下的未认证用户的 HTTP 会话总数时，可进行该配置。
- 在配置自动获取 SU 客户端功能时， 需要进行该配置。

检验方法

- 修改未认证用户最大会话数
- 未认证用户构造相同会话不间断对设备进行连接
- 未认证用户通过浏览器访问外网，访问请求不被重定向，设备提示用户会话数超过限制

相关命令

↘ 设置每个未认证用户的最大 HTTP 会话数

【命令格式】 **http redirect session-limit** { *session-num* } [**port** { *port-session-num* }]

【参数说明】 *session-num*：最大会话数。取值范围 1-255，默认为 255。

port-session-num：端口最大会话数。取值范围 1-65535，默认为 300。

【命令模式】 全局配置模式

【使用指导】 无

配置举例

↘ 设置每个未认证用户的最大 HTTP 会话数

【配置方法】
- 设置每个未认证用户的最大 HTTP 会话数为 3

```
Ruijie(config)#http redirect session-limit 3
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show web-auth parameter
HTTP redirection setting:
  session-limit: 3
  timeout:       3
Ruijie(config)#
```

1.4.17 设置维持重定向连接的超时时间

配置效果

- 设置维持重定向连接的超时时间。因为未认证的用户通过 HTTP 访问网络资源时，其 TCP 连接请求将被拦截，实际上是与接入/汇聚设备建立起 TCP 连接。在连接建立后，设备需要等待用户发出的 HTTP 的 GET/HEAD 报文，然后回复 HTTP 重定向报文后才能关闭连接。设置这个限制可以防止用户不发 GET/HEAD 报文，而又长时间占用 TCP 连接。缺省情况下，维持重定向连接的超时时间为 3 秒。

注意事项

- 无

配置方法

- 可选配置
- 要更改维持重定向连接的超时时间时，可进行该配置。

检验方法

- 修改超时时间配置
- 使用网络发包工具构造建立 tcp 连接
- 查看设备上该 tcp 连接状态，超过超时时间后连接被关闭

相关命令

↘ 设置维持重定向连接的超时时间

【命令格式】 **http redirect timeout** { *seconds* }

【参数说明】 *Seconds*：重定向连接超时时间，单位为秒。取值范围 1-10。默认为 3 秒。

【命令模式】 全局配置模式

【使用指导】 无

配置举例

↘ 设置维持重定向连接的超时时间

【配置方法】

- 设置维持重定向连接的超时时间 5

```
Ruijie(config)#http redirect timeout 5
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show web-auth parameter
HTTP redirection setting:
  session-limit: 255
  timeout:       5
```

1.4.18 设置免认证网络资源范围

配置效果

- 在端口上启动 Web 认证或者 802.1x 认证后，未认证用户需先通过 Web 认证或者 802.1x 认证，才能访问网络资源。
- 使用此命令设置免认证的网络资源，可以允许未认证用户，也可以访问一些免认证的网络资源。
- 设置了免认证的网络资源，如果某网站属于免认证的网络资源，那么所有用户(包括未认证用户)都可以访问该网站。缺省情况下，没有设置免认证的网络资源，未认证用户不能访问网络资源。
- 支持 IPV6。

注意事项

- 设置免认证的网络资源和设置无需认证用户共享资源，这两者各自都不能超过 1000 个。此外，实际可用数量也会受其它安全功能占用表项的影响而减少。因此，如果需要设置的地址较多，请尽量使用网段的方式进行设置。
- http redirect direct-site 是配置免认证访问地址，http redirect 是配置 web 认证的服务器地址。从效果上看，用这两条命令配置的地址都是可以不用认证就直接访问的，但是实际用途是不一样的，因此实际使用时建议不要用 http redirect direct-site 来配置 web 认证服务器地址，否则会引起误解。
- IPv6 场景下，需要配置放行本地链路地址，否则会导致设备无法学习到终端的 mac 地址。

配置方法

- 可选配置
- 如果需要让未认证用户能够访问网络中的资源，使用本命令实现。

检验方法

- 配置免认证网络资源
- 未认证用户 PC 直接访问该资源，访问成功

相关命令

设置免认证网络资源范围

【命令格式】 **http redirect direct-site** { *ipv6-address* | *ipv4-address* [*ip-mask*] [**arp**] }

【参数说明】 *Ipv6-address*：免认证网络资源的 Ipv6 地址

Ipv4-address：免认证网络资源的 Ipv4 地址

ip-mask：免认证网络掩码

【命令模式】 全局配置模式

【使用指导】 ARP 放行请优先采用直通 ARP 命令

配置举例

设置免认证网络资源范围

【配置方法】

- 设置免认证的网络资源范围 192.168.0.0/16

```
Ruijie(config)#http redirect direct-site 192.168.0.0 255.255.0.0
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show web-auth direct-site
Direct sites:
  Address         Mask            ARP Binding
  --------------- --------------- -----------
  192.168.0.0     255.255.0.0     Off
Ruijie(config)#
```

1.4.19 设置直通ARP资源范围

配置效果

- 开启 ARP CHECK 或类似功能时，用户的 ARP 学习受控，导致用户无法学到网关及其他设备的 ARP，影响用户使用。此时可以通过设置直通 ARP 资源来对指定地址的 ARP 学习报文进行放行

注意事项

- 对于开启 ARP Check 情况，需要将二层接入设备下联 PC 的网关设置为直通 ARP 资源。需要注意以下问题：
  对同一地址/网段同时设置直通网站和直通 ARP 时，命令会自动进行合并；如果直通网站的配置没有指定 ARP 选项，合并后该选项会自动增加。
- 对于开启 ARP Check 情况，若下联 PC 的出口地址不是网关地址，也需要将出口地址设置为直通 ARP 资源。若存在多个出口地址，这些出口地址也需要设置为直通 ARP 资源。

配置方法

- 可选配置
- 如果设备启用了 ARP CHECK 功能，那么需要对免认证的网络资源范围和网关配置 ARP 直通。

检验方法

- 配置直通 ARP 资源
- 未认证用户 PC 上清空 ARP 缓存(Windows 执行命令 arp -d)
- 未认证用户 PC 执行 ping 直通 ARP 资源
- 未认证用户 PC 查看 ARP 缓存(Windows 执行命令 arp -a)，学习到直通 ARP 资源的 ARP 地址

相关命令

↘ 设置直通 ARP 资源范围

【命令格式】 **http redirect direct-arp** { *ip-address* [*ip-mask*] }

【参数说明】 *ip-address*：免认证网络 ip 地址

ip-mask：免认证网络掩码

【命令模式】 全局配置模式

【使用指导】 -

配置举例

↘ 设置直通 ARP 资源范围

【配置方法】

- 设置直通 ARP 资源范围 192.168.0.0/16

```
Ruijie(config)#http redirect direct-arp 192.168.0.0 255.255.0.0
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show web-auth direct-arp
Direct arps:
  Address         Mask
  --------------- ---------------
  192.168.0.0     255.255.0.0
```

【配置方法】
- 设置直通 ARP 资源范围 192.168.0.0/16

```
Ruijie(config)#http redirect direct-arp 192.168.0.0 255.255.0.0
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#
```

1.4.20 设置无需认证用户范围

配置效果

- 如果用户属于无需认证用户范围，那么该用户不需要通过 Web 认证，也能访问所有可达的网络资源。缺省时，没有设置无需认证用户，所有用户都必须先通过 Web 认证，才能访问网络资源。
- 支持 IP 地址和 MAC 地址设置。

注意事项

无

配置方法

- 可选配置
- 要设置无需认证用户时，可进行该配置。

检验方法

- 配置用户为无需认证用户
- 用户直接访问网络，访问成功

相关命令

↘ 设置无需认证用户 IP 范围

【命令格式】 **web-auth direct-host** { *ipv4-address* [*ip-mask*] [**arp**] | *ipv6-address* | *mac-address*} [**port** *interface-name*]

【参数说明】 *Ipv4-address*：免认证用户 IPv4 地址
Ipv6-address：免认证用户 IPv6 地址
ip-mask：免认证用户掩码
interface-name：接口名
arp :如果设备启用了 ARP CHECK 功能，那么需要对免认证的用户 IP 范围进行 ARP 绑定，需要配置 **arp** 关键字。仅在设置 IPv4 地址时需要。

mac-address：无需认证用户的 MAC 地址

【命令模式】 全局配置模式

【使用指导】 arp 字段用来设置放行 arp 报文，当开启 ARP-CHECK 功能时需要配置

配置 port 字段后，用户仅在所配置接口下时免认证功能生效，在其余接口上不生效

配置举例

↘ 设置无需认证用户 IP 范围

【配置方法】

- 设置无需认证用户 IP 范围

```
Ruijie (config)# web-auth direct-host 192.168.197.64
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show web-auth direct-host
Direct hosts:
  Address         Mask            Port            ARP Binding
  --------------- --------------- --------------- -------------
  192.168.197.64  255.255.255.255                 Off
Ruijie(config)#
```

1.4.21 设置在线用户信息的更新时间间隔

配置效果

- 接入/汇聚设备维护着在线用户信息，设备需要定时地更新在线用户信息，包括在线时间等，以监控在线用户使用网络资源的情况，比如：用户的在线时间大于或等于在线时限，该用户会被停止使用网络。

注意事项

- 用户更新时间必须配置为 60 的倍数，否则实际配置自动向上取最近的 60 倍数来生效。

配置方法

- 可选配置
- 要设置无需认证用户时，可进行该配置。

检验方法

- 配置用户信息更新时间
- 超过更新时间间隔后，查看在线用户信息

相关命令

↘ 设置在线用户信息更新时间间隔

【命令格式】 **web-auth update-interval** *{ seconds }*

【参数说明】 *Seconds*：信息更新时间间隔，单位为秒。取值范围 30-3600。默认为 180 秒。

【命令模式】 全局配置模式

【使用指导】 如果要恢复更新时间间隔为默认值，在全局配置模式下，使用 **no web-auth update-interval**

配置举例

↘ 设置已认证用户信息的更新时间间隔为 60 秒

【配置方法】

- 设置已认证用户信息的更新时间间隔为 60 秒

```
Ruijie (config)# web-auth update-interval 60
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show run | include web-auth update-interval
web-auth update-interval 60
```

1.4.22 配置Portal检测

配置效果

- 定时检测 Portal 服务器是否可用，如果不可用，切换到备用 Portal 服务器。
- 对于二代认证有两种检测方法，第一种方法，是设备构造 Portal 协议报文发给 Portal 服务器，并通过检测 Portal 服务器是否响应来确定服务器是否可用。第二种方法，是设备向服务器发 ping 报文，通过是否响应 ping 报文来检测。由于部分服务器或者中间网络会过滤 ping 报文，因此大部分情况下是选择方法一作为检测方法，只有在极个别环境，比如有特殊规范要求的，才选择 ping 检测。而一代认证，采用 connect 服务器端口是否可达的方式来判断服务是否可用。
- 针对二代认证的第一种检测方法，检测算法为每隔 **interval** 时间进行一次检测，每次检测最多发 **retransmit** 个报文，如果些报文服务器都不响应，则判断服务器不可用，否则可用。每个报文的超时时间由参数 **timeout** 决定。一代认证同样支持此配置。
- 该功能对一代，二代 Web 认证都有效。
- 如果配置了多个个 Portal 服务器，则称为主备 Portal。

注意事项

- 需要配置多个 Portal 服务器，这样检测到错误时才能实现切换。
- 为避免检测算法冲突，两种检测方法只能选一个，同时配置会引起检测冲突或者检测结果不准确。

- 配置时如果使用一代认证，系统会自动选择一代检测方式，二代认证同样会自动选择二代认证的检测方式

配置方法

- 可选配置。
- 配置多个一，二代 Web 认证的 Portal 模板。

检验方法

- 配置两个二代或一代 Portal 服务器模板，第一个模板指向的服务器不可用，第二个模板指向的服务器可用。
- 控制台出现 Portal 不可用的 log 时，用户打开浏览器登录认证，被重定向到第二个 Portal 服务器。

相关命令

↘ 设置 Portal 检测

【命令格式】 **web-auth portal-check** [**interval** *intsec* [**timeout** *tosec]* [**retransmit** retries]

【参数说明】 *intsec*：检测周期，默认 10 秒

tosec ：报文超时时间，默认 5 秒

intsec：超时重传次数，默认 3 次

【命令模式】 全局配置模式

【使用指导】 大部分网络环境中只有一台服务器，无需配置此功能，如果有多台，参数不宜配置太小，否则会出现短时间内设备发出太多报文，影响设备性能。

【命令格式】 **web-auth ping** [**interval** *minutes*] [**retry** *times*]

【参数说明】 *minutes*：检测周期，默认 1 分钟

times ：超时重传次数，默认 3 次

【命令模式】 全局配置模式

【使用指导】 大部分网络环境中只有一台服务器，无需配置此功能，如果有多台，参数不宜配置太小，否则会出现短时间内设备发出太多报文，影响设备性能。

配置举例

↘ 设置 Portal 检测

【配置方法】

- 配置 Portal 检测

```
Ruijie(config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
```

【配置方法】
- 配置 Portal 检测

```
Ruijie(config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

【检验方法】
- 查看配置是否成功

```
web-auth portal-check interval 20 timeout 2 retransmit 2
…
```

1.4.23 配置Portal逃生

配置效果

- 当配置的 Portal 服务器都不可用时，新接入网络的用户免认证。

注意事项

- 需要同时配置 Portal 检测功能。
- 如果配置了多个 Portal 服务器，则需要所有 Portal 服务器均不可用时逃生功能才会生效。
- 此功能仅针对 Portal 服务器，不针对 RADIUS 服务器。

配置方法

- 可选配置。
- 配置 Portal 检测功能。
- 配置 Portal 逃生功能。
- 可配置 nokick 属性。

检验方法

- 配置一个 Portal 服务器，服务器不可用。
- 配置 Portal 检测功能和逃生功能。
- 设备检测出 Portal 不可用后，用户接入网络，无需认证即可访问网络。

相关命令

↘ 设置 Portal 逃生

【命令格式】 **web-auth portal-escape [nokick]**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 如果网络中有一些关键业务不允许中断，可以配置此功能，这样当 Portal 服务器出现异常时，可以保证业务不受影响。配置此功能要同时配置 Portal 检测功能。

配置 nokick 属性后，逃生生效时，对已在线用户不做下线处理。删除该属性，会下线在线用户。

配置举例

设置 Portal 逃生

【配置方法】

- 配置 Portal 逃生

```
Ruijie(config)# web-auth portal-escape
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth portal-escape
…
```

1.4.24 配置DHCP地址核查

配置效果

- 只有通过 DHCP 分配地址的终端才允许进行认证。

注意事项

- 需要配置 DHCP SNOOPING 功能。
- 仅支持 IPV4。
- 仅支持二代 Web 认证和内置 Portal Web 认证。
- 网络部署时明确用户使用 DHCP 获得 IP 地址，不存在静态 IP 地址混用的情况，否则会影响静态 IP 地址的用户。
- 如果有少数用户需要用静态 IP 地址，可以通过配置直通地址放行，对这些用户不认证。

配置方法

- 可选配置。
- 配置 DHCP SNOOPING。
- 配置地址核查。

检验方法

- 配置 DHCP 地址核查功能。
- 终端配置静态地址，该地址未经 DHCP 服务器分配。
- 终端连接到网络，无法认证。

相关命令

↘ 设置 DHCP 地址核查

【命令格式】 **web-auth dhcp-check**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 网络部署时指定用户需要使用 DHCP 获取 IP 地址上网，配置此功能有助于屏蔽一些私设 IP 地址的用户认证上网。

配置举例

↘ 设置 DHCP 地址核查

【配置方法】
- 配置 DHCP 地址核查

```
Ruijie(config)# web-auth dhcp-check
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth dhcp-check
…
```

1.4.25 配置关闭链路检测

配置效果

- 终端通过Web认证后，断开链路，认证表项不会被删除，终端再次连接到网络时，只要IP地址和之前的一样，就可以继续上网。
- 该功能适用于有经常性移动办公的场所，或者部署了无线的 Web 认证但是所在场所无线信号不好。

注意事项

- 如果终端是通过 DHCP 获取 IP 地址，且 DHCP 地址池小于网络用户数，则不适合开该功能，因为当一个终端离开时，其 IP 地址有可能会被其它人获取，这会导致用户信息错误。
- 如果关闭链路检测，则用户下线只能通过点击页面主动下线、服务器踢线、设备配置低流量检测下线。因此配置此功能时，建议要同时开启低流量检测功能，具体参考 SCC 的配置手册。
- 对于无线环境，建议关闭链路检测功能，同时开启低流量检测，主要是因为无线连接受信号干扰导致掉线比较突出，关闭链路检测有助于提高无线体验。

配置方法

- 可选配置。
- 配置 Web 认证。
- 关闭链路检测功能。

检验方法

- 配置二代 Web 认证并关闭链路检测功能。
- 终端连接到网络，认证通过，断开网络，然后再连接到网络，在 IP 地址不变的情况下，无需认证即可访问网络。

相关命令

↘ 关闭链路检测功能

【命令格式】 **no web-auth sta-leave detection**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 无线环境或者有经常需要移动办公的有线环境可以关闭链路检测，同时需要开启低流量检测功能。

配置举例

↘ 关闭链路检测功能

【配置方法】
- 关闭链路检测功能

```
Ruijie(config)# no web-auth sta-leave detection
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
no web-auth sta-leave detection
…
```

1.4.26 配置关闭Portal协议扩展

配置效果

- 通过开关此功能来支持锐捷 Portal 服务器和标准中移动规范的 Portal 服务器。
- 对接标准中移动 Portal 规范服务器时，可选择多种重定向 URL 格式，用于兼容不同服务器。

注意事项

- 仅支持二代 Web 认证。
- 二代 Web 认证扩展了中移动 Portal 协议，实际使用时需要根据服务器情况选择是否运行在扩展模式。
- 如果 Portal 服务器为锐捷产品，则使用默认值，也就是扩展模式，如果 Portal 服务器为标准中移动 Portal 服务器，则需要关闭扩展。
- 如果 Portal 服务器为标准中移动 Portal 服务器产品，由于中移动 Portal 规范存在多种 url 重定向格式，需要依据实际的 Portal 服务器支持情况选择格式。

配置方法

- 可选配置。
- 根据服务器类型选择是否关闭扩展。
- 如果关闭扩展，根据服务器的支持情况选择合适的重定向 url 格式。

检验方法

- 分别选择锐捷 Portal 服务器和中移动标准 Portal 服务器作为二代 Web 认证的服务器。
- 终端连接到网络，均可正常认证并访问网络。

相关命令

↘ 关闭 Portal 协议扩展

【命令格式】 **no web-auth portal extension**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 环境中使用的是中移动标准 Portal 服务器，如果是锐捷 Portal 服务器，则需要开启扩展。

配置举例

↘ 关闭 Portal 协议扩展

【配置方法】
- 关闭 Portal 协议扩展

```
Ruijie(config)# no web-auth web-auth portal extension
Ruijie(config)# http redirect url-fmt ext1
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
no web-auth web-auth portal extension
http redirect url-fmt ext1
…
```

1.4.27 配置黑白名单

配置效果

- 白名单可以使用户在认证前可以访问部分网络资源，黑名单可以使用户在认证后无法访问部分网络资源。
- 黑白名单支持端口、url、ip 等信息过滤的过滤。

注意事项

- 黑白名单只支持配置最多 1000 条。
- 如果以域名形式配置，需要配置设备的 DNS 功能，使得设备可以正确解析 IP 地址。
- 部分域名有多 IP，仅支持一个域名最多 8 个 IP 地址。

配置方法

- 可选配置。
- 配置 DNS 域名解析。
- 配置黑白名单。

检验方法

- 配置一条白名单和一条黑名单。
- 终端认证前可以访问白名单地址。
- 终端认证后无法访问黑名单地址。

相关命令

配置黑白名单

【命令格式】 **web-auth acl {black-ip** *ip*|**black-port** *port*|**black-url** *name*|**white-url** *name*}

【参数说明】 *ip*：黑名单 ip 地址

port：黑名单端口

name：黑白名单的 url

【命令模式】 全局模式配置模式，无线上黑名单还支持 wlansec 模式

【使用指导】 允许认证前访问采用白名单，禁止认证后访问采用黑名单。

配置举例

配置认证模式

【配置方法】

- 配置黑白名单

```
Ruijie(config)# web-auth acl black-ip 192.168.1.2
Ruijie(config)# web-auth acl white-url www.ruijie.com.cn
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth acl black-ip 192.168.1.2
web-auth acl white-url www.ruijie.com.cn
…
```

1.4.28 配置防抖动计费

配置效果

- 如果设备配置了防抖功能或者低流量下线，通过此功能决定是否将防抖时间或者低流量检测时间计算入计费报文中的在线时长。此功能用于减小计费误差，如果环境中的计费策略允许不扣除这些检测时间，可以配置该功能。如果配置了防抖或者低流量检测，则默认情况防抖时间或者低流量检测时间不计如在线时长。

注意事项

- 设备需支持防抖功能或者低流量检测功能。
- 终端的下线动作是由链路长时间断开或者低流量检测导致。

- 由于防抖功能和流量检测功能可以同时开启，防抖计费只对其中先触发下线的生效，比如配置防抖时间 5 分钟，配置流量检测 10 分钟，如果终端离开网络，则防抖功能优先出发了 Web 认证将用户下线，因此计费报文中的在线时长只扣除 5 分钟。

配置方法

- 可选配置。
- 配置计费功能。
- 配置防抖功能或者低流量检测功能。
- 配置防抖计费功能。

检验方法

- 终端认证上线，然后通过低流量下线。
- 捕获设备发出的计费结束报文，确认其中的在线时间没有扣除流量检测时长。

相关命令

配置防抖动计费

【命令格式】 **web-auth accounting jitter-off**

【参数说明】 -

【命令模式】 全局模式配置模式

【使用指导】 根据服务器计费策略选择是将防抖时长或者低流量检测时长计算入计费结束报文的在线时长中，默认是不计入。

配置举例

配置防抖计费

【配置方法】

- 配置防抖计费

```
Ruijie(config)# web-auth accounting jitter-off
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth accounting jitter-off
…
```

1.4.29 配置Portal通信端口

配置效果

- 配置后设备与 Portal 服务器通信的源端口为所配置端口。

注意事项

- 端口只能配置一个。

配置方法

- 配置指定端口为 portal 通信口。

检验方法

- 开启 web 受控后，认证时服务器上抓包，认证报文源 IP 为指定端口的 IP。

相关命令

↘ 配置通信端口

【命令格式】 **ip portal source-interface interface-type interface-num**

【参数说明】

【命令模式】 全局模式配置模式。

【使用指导】

配置举例

↘ 配置 portal 通信端口

【配置方法】

- 使用聚合口当作 portal 通信口地址。

```
Ruijie(config)# ip portal source-interface Aggregateport 1
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
ip portal source-interface Aggregateport 1
```

1.4.30 配置宁盾系统兼容URL

配置效果

- 配置 web 重定向 URL 支持宁顿系统。

注意事项

- 无。

配置方法

↘ 配置宁顿系统兼容 URL 参数

- 全局模式下配置 post 参数。

【命令格式】 **web-auth dkey-compatible url-parameter** *string*
【参数说明】 string: post 参数内容
【命令模式】 全局配置模式。
【使用指导】 无。

检验方法

- 配置后执行重定向，重定向 URL 中会加入 post 参数。

配置举例

↘ 配置防降噪抑制功能

【配置方法】
- 配置兼容参数。

```
Ruijie(config)# web-auth dkey-compatible url-parameter login
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth dkey-compatible url-parameter login
```

1.4.31 配置内置WEB认证NAT功能

配置效果

- 配置内置 web 认证支持 NAT。

注意事项

- 只对内置 WEB 认证有效。

配置方法

↘ 配置 NAT 支持功能

- 全局模式下开启功能。

【命令格式】 **iportal nat enable**
【参数说明】
【命令模式】 全局配置模式。
【使用指导】 无。

检验方法

- 配置后 NAT 场景可以使用内置 web 认证。

配置举例

↘ 配置 NAT 功能支持

【配置方法】

- 配置 NAT 功能支持。

```
Ruijie(config)# iportal nat enable
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
iportal nat enable
```

1.4.32 配置内置WEB认证重传次数

配置效果

- 配置内置 web 认证 http 连接重传次数。

注意事项

- 重传次数只对内置页面推送的 http 连接有效。

配置方法

↘ 配置内置 web 认证 http 重传次数

- 全局模式下配置参数。

【命令格式】 **iportal retransmit** *count*
【参数说明】 count: 重传次数
【命令模式】 全局配置模式。
【使用指导】 无。

检验方法

- 配置后发送内置 web 认证请求后，断开连接，设备可以发出重传。

配置举例

↘ 配置重传次数

【配置方法】

- 配置重传次数。

```
Ruijie(config)# iportal retransmit 5
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
iportal retransmit 5
```

1.4.33 配置内置WEB认证服务选择

配置效果

- 配置内置 web 认证使用的服务类型。

注意事项

- 无。

配置方法

配置内置 web 认证服务类型

- 全局模式下配置服务类型。

【命令格式】 **iportal service [internet** *internet-name*] **[local** *local-name* **]**

【参数说明】 internet-name: 使用的外部服务名称

local-name:使用的内部服务名称

【命令模式】 全局配置模式。

【使用指导】 无。

检验方法

-

配置举例

配置服务类型

【配置方法】

- 配置服务类型。

```
Ruijie(config)# iportal service local local-srv
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
…
iportal service local local-srv
```

1.4.34 配置WEB记账方法列表

配置效果

- 基于不同的模板，指定 web 认证记账方法。

注意事项

- 不配置会使用默认记账方法进行记账。

配置方法

↘ 配置记账方法

- 全局或者模板配置模式下配置记账方法。

【命令格式】 **web-auth accounting v2 { default | *name* }**
【参数说明】 name：使用的记账列表名称
【命令模式】 全局或者模板配置模式。
【使用指导】 无。

检验方法

- 配置查看记账报文目的地址。

配置举例

↘ 配置记账方法

【配置方法】
- 配置记账方法。

```
Ruijie(config.tmplt.eportalv2)# web-auth accounting v2 default
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth accounting v2 default
```

1.4.35 配置WEB认证方法列表

配置效果

- 基于不同的模板，指定 web 认证方法。

注意事项

- 不配置会使用默认认证方法进行认证。

配置方法

↘ 配置认证方法

- 全局模式或者模板配置模式下配置记账方法。

【命令格式】 **web-auth authentication v2 { default | *name* }**
【参数说明】 name：使用的认证方法列表名称
【命令模式】 全局模式或者模板配置模式。
【使用指导】 无。

检验方法

- 配置查看认证报文目的地址。

配置举例

↘ 配置认证方法

【配置方法】
- 配置认证方法。

```
Ruijie(config.tmplt.eportalv2)# web-auth authentication v2 default
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
web-auth authentication v2 default
```

1.4.36 页面包定制规范

配置效果

- 使用内置 Porttal Web 认证时，允许定制自有 Web 页面，比如显示特定 LOGO 或者显示广告等。
- 单个也面包支持两套页面，以适配终端屏幕大小，比如小屏幕的移动终端。

注意事项

- 必须严格按照规范制作页面，避免新也面包无法使用。
- 页面包的文件数量不得超过 50 个（含 PC 版页面文件和移动终端版页面文件），每个页面文件名不得长于 32 字节
- 新也面包必须下载到./portal 目录下，新也面包名字不能默认页面包重叠，否则会覆盖默认页面包。
- 部分设备没有默认也面包，使用内置 Portal Web 认证时必须根据规范制定也面包并导入 FLASH。

配置方法

无

检验方法

- 用户连接到网络，打开浏览器认证，弹出定制页面。

相关命令

↘ 页面文件命名规范

页面文件名（含扩展名）	用途
login.htm	登录页面
online.htm	在线页面（用户登录成功之后的页面）
offline.htm	下线页面
login_mobile.htm	移动终端登录页面
online_mobile.htm	移动终端在线页面（用户登录成功之后的页面）
offline_mobile.htm	移动终端下线页面

↘ 登录页面制作规范

根据页面命名规范，PC 版的登录页面名称为 login.htm，移动终端版的登录页面名称为 login_mobile.htm。登录页面的内容规范说明如下：

- 表单元素

登录页面必须包含一个表单，提交方式固定为 POST。下面以 PC 版登录页面为例（移动终端版的类似），假设 PC 版的登录页面存放在/portal 目录下，相应的表单 html 编码大致如下：

```
<form method="post" action="/portal/login.htm">
...
</form>
```

一般来说，表单中需要包括以下页面元素：

1. 用户名文本框，用于给用户输入用户名，ID 为 username。(必选)
2. 密码文本框，用于给用户输入密码信息(不明文显示密码)，ID 为 password。(必选)
3. 登录按钮，用于 POST 方法提交表单。(必选)。
4. 显示认证失败原因的页面标签，ID 为 errormsg。(可选)，如果用户不关心登录失败的原因，那么登录页面中可以不包含该 errormsg 标签；如果想把认证失败的原因呈现给认证用户，那么就必须包括有这么一个可显示认证失败原因的区域，并且在页面加载的时候以 GET 的方式发送请求，请求内容为 errormessage，请求的结果将在 errormsg 标签中呈现。向服务器请求 errormsg 内容的脚本大致如下（以下只是一个例子，不代表是唯一写法）：

```
< script language=”javascript”>
//向服务器请求 errormessage 内容
function requestErrorMsg() {
    var _errormsg=document.getElementById(“errormsg”);
      var script=document.createElement(“script”);
script.src=”errormessage”+location.search;
_errormsg.appendChild(script);
}

//页面加载时需要调用 init 函数
function init() {
……
requestErrorMsg();
}
……
</script>
```

- 表单提交：

表单提交时，提交格式为 username=[AAAA]&password=[BBBB]&lang=[CCCC]，各个填充字段的含义如下：

[AAAA]：为用户在用户名文本框中填写的用户名。(必选)

[BBBB]：为用户在密码文本框中填写的密码。(必选)

[CCCC]：为用户当前的语言环境 (可选)，值 1 表示简体中文环境，2 表示英文环境，其他暂未定义，默认为简体中文，当语言环境是英文时，提交表单时需要将语言环境信息一并提交，否则象认证失败原因信息返回的是中文，与用户的实际语言环境就不一致了。

因此，登录页面的表单中至少要有 username 和 password 以及登录按钮这三个输入域（ 即 input 标签），如果登录页面有中英文环境，表单中还可能会有一个 lang 输入域，这个域一般是不可见的。

综上所述，可以得到登录页面最基本的 HTML 源码大致如下：

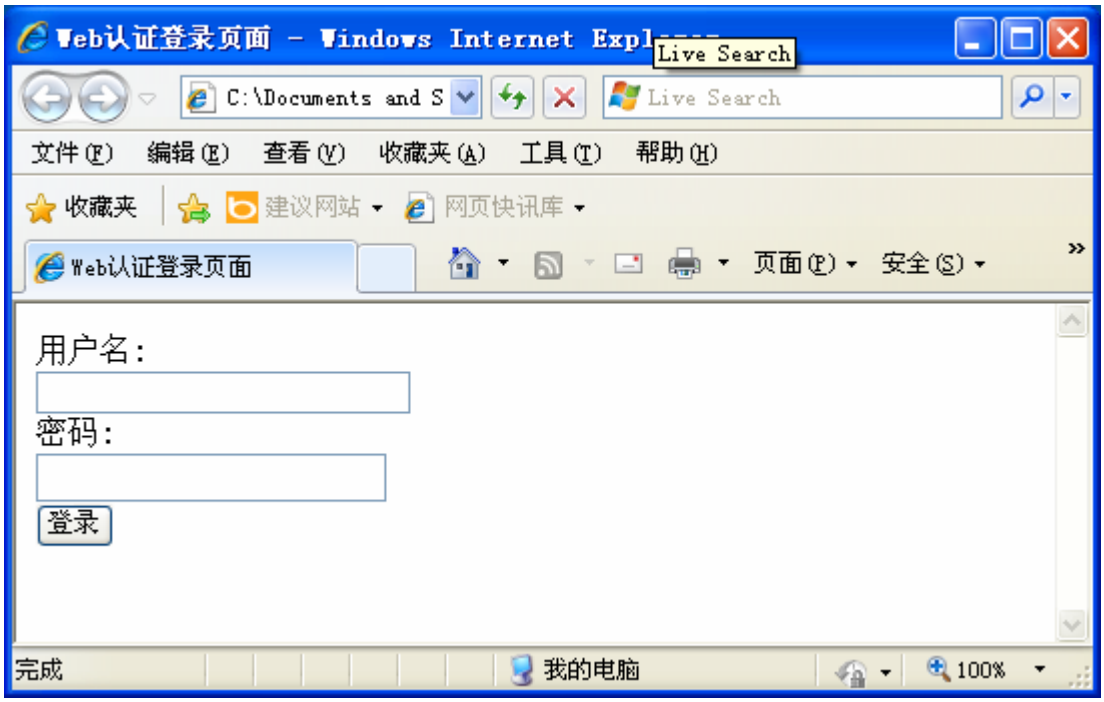
```
<html>
   <head>
   <title>Web 认证登录页面</title>
   </head>
   <script language=”javascript”>
    // 请求认证错误信息，如果认证成功或登录页面首次加载错误信息为空，不显示
    function requestErrorMsg() {
    var _errormsg=document.getElementById(“errormsg”);
       var script=document.createElement(“script”);
script.src=”errormessage”+location.search;
_errormsg.appendChild(script);
    }

function init() {
……
requestErrorMsg();
}

// 用户点登录按钮时执行的脚本。
function login() {
   document.getElementById('loginForm').action = "./login.htm"+location.search;
       document.getElementById('loginForm').submit();
       window.onbeforeunload = null;
       window.onunload = null;
}
……
```

```
</script>
   <body onload="init()">
      <form method="post" id=”loginForm”>
      用户名:<br>
      <input type="text" name="username" accesskey="u" size="25" value="" id="usrename">
      <br>
      密码:<br>
      <input type="password" name="password" accesskey="p" size="25"
           value="" id="password">
      <br>
<input type="button" onclick=”login()” value="登录" id=”loginButton”>
<input type="hidden" name="lang" value="" id="lan">
       <p name=”errormsg” id="errormsg"></p>
      </form>
   </body>
</html>
```

根据上述的定制，内置 portal 服务器向用户推送的登录页面样式大致如下：



通过上述的定制过程，登录页面已经具备了所有必要的元素，但这样的页面没有什么美观可言。用户可以在此基础之上进行美化，以及添加一些其他功能。比如添加背景、设置各种页面元素的样式等。

↘ 在线页面制作规范

在线页面的作用是告诉用户已经通过认证，可以正常使用网络。PC 版的在线页面名称为 online.htm，移动终端版的登录页面名称为 online_mobile.htm。

- 表单元素

在线页面必须包含一个表单，这个表单的作用是来提交下线请求的，因此，表单中也需要有一个下线按钮，表单的提交方式固定为 POST。下面以 PC 版的在线页面为例（移动终端版的类似），假设 PC 版的在线页面存放在/portal 目录下，相应的表单 html 编码大致如下：

```
<form method="post" action="/portal/online.htm">
...
</form>
```

在线页面的表单中需要包括以下页面元素：

1. ID 为 username 的页面标签，用于呈现用户的用户名信息。(可选)
2. ID 为 userip 的页面标签，用于呈现用户的 IP 地址。(可选)
3. ID 为 usermac 的页面标签，用于呈现用户的 MAC 地址。(可选)
4. ID 为 ssid 的页面标签，用于呈现用户所在的 SSID。(可选)
5. ID 为 availtime 的页面标签，用于呈现用户可用时长。(可选)
6. 下线按钮，用户想下线时可以点击该按钮，用于请求下线页面。(必选)

在线页面加载时需要通过 GET 方法向服务器请求用户信息，包括用户名、用户 IP 地址、用户 MAC 地址、关联的 SSID 以及可用时长，URI 为 getonlineinfo，为此需要实现 html 中 body 的 onload 方法。大致如下（只是举一个例子，不是唯一实现）：

```
<script language="javascript">
    // 获取在线用户信息,包括用户名、IP、MAC、关联信号、可用时长
    function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement(“script”);
        script.src="getonlineinfo"+location.search;
        _availTime.appendChild(script);
    }

    function init() {
        requestOnlineInfo();
```

```
    }
  </script>
<body onload="init()">
……
</body>
```

综上所述，可以得到在线页面最基本的 HTML 源码大致如下：

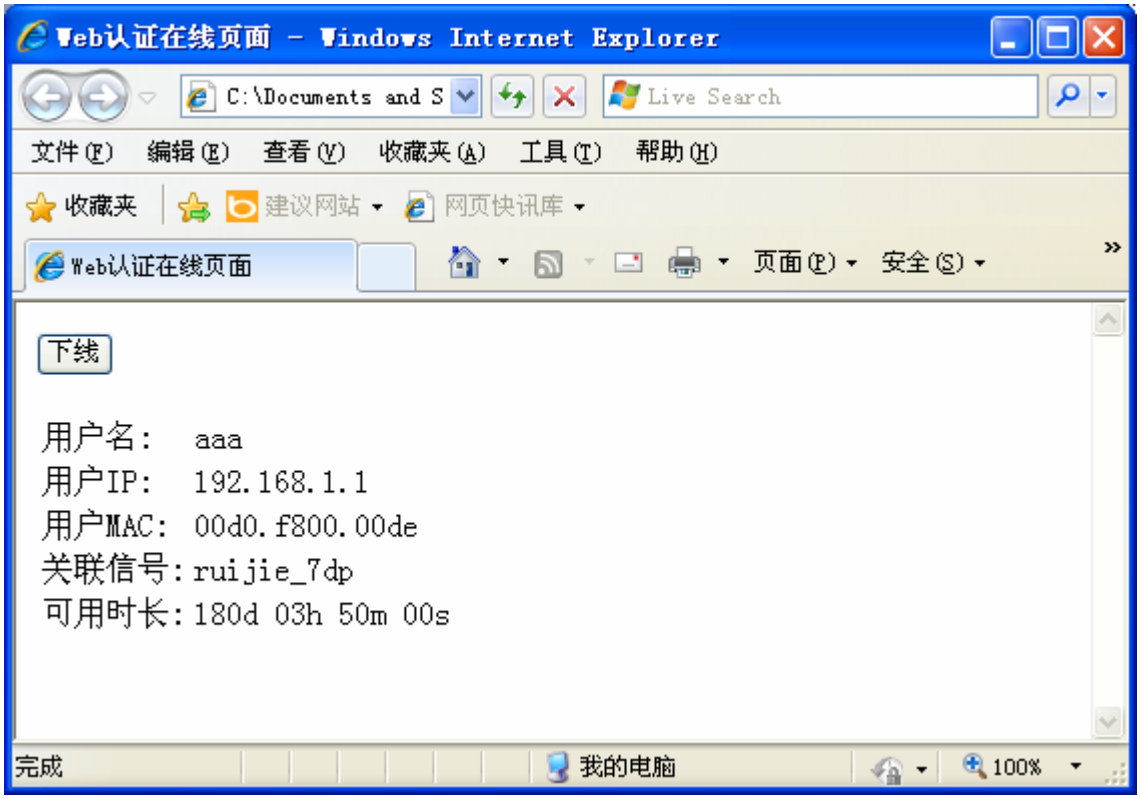
```
<html>
  <head>
  <title>Web 认证在线页面</title>
  </head>
  <script language="javascript">
    // 获取在线用户信息,包括用户名、IP、MAC、关联信号、可用时长
    function requestOnlineInfo() {
          var _availTime=document.getElementById("availtime");
          var script=document.createElement(“script”);
          script.src="getonlineinfo"+location.search;
          _availTime.appendChild(script);
    }

     function init() {
          requestOnlineInfo ();
    }
    // 用户点下线按钮时执行的脚本，请求的 URI 为 offline.htm。
    function logout() {
        document.logoutform.action = "./offline.htm"+location.search;
        document.logoutform.submit();
        window.onbeforeunload = null;
         window.onunload = null;
    }
```

```
    </script>

    <body onload="init()">
        <form method="post" action="/portal/offline.htm" id="logoutform">
        <input type="button" onclick="logout()" value="下线" id="logoutButton">
        </form>
         <table>
         <tr><td>用户名:</td><td id="username"></td></tr>
         <tr><td>用户 IP:</td><td id="userip"></td></tr>
         <tr><td>用户 MAC:</td><td id="usermac"></td></tr>
         <tr><td>关联信号:</td><td id="ssid"></td></tr>
         <tr><td>可用时长:</td><td id="availtime"></td></tr>
         </table>
    </body>
</html>
```

根据上述的定制，内置 portal 服务器向用户推送的登录页面样式大致如下：



上述的在线页面就已具备了所有必要的元素。用户可以在此基础之上进行美化，以及添加一些其他功能。比如添加背景、设置各种页面元素的样式等。

↘ 下线页面制作规范

当用户在在线页面上点击下线按钮后就会引出下线页面，其作用是告诉用户已经下线成功，如果要使用网络，需要重新进行认证。PC 版的在线页面名称为 offline.htm，移动终端版的登录页面名称为 offline_mobile.htm。

页面元素：

1. ID 为 timeused 的页面标签，用于呈现用户已用时长的信息。(可选)

在下线页面的加载过程中 ,需要向服务器发送 GET 请求获取已经用时长信息 ,请求的 URI 为 getofflineinfo。为此需要实现 html 中 body 的 onload 方法。获取已用时长信息时 ,可以动态创建 script, 比如要发送的字段信息包含在 script 的 src 中 ,script.src="getofflineinfo"。大致如下（只是举一个例子，不是唯一实现）：

```
<script language="javascript">
    // 获取已用时长信息
    function requestOfflineInfo() {
    var _timeused =document.getElementById("timeused");
    var script=document.createElement("script");
    script.src="getofflineinfo"+location.search;
      _timeused.appendChild(script);
```

```
}

function init() {
        requestUserInfo();
}
</script>
<body onload="init()">
……
</body>
```

下线页面整体最基本的 HTML 源码大致如下：

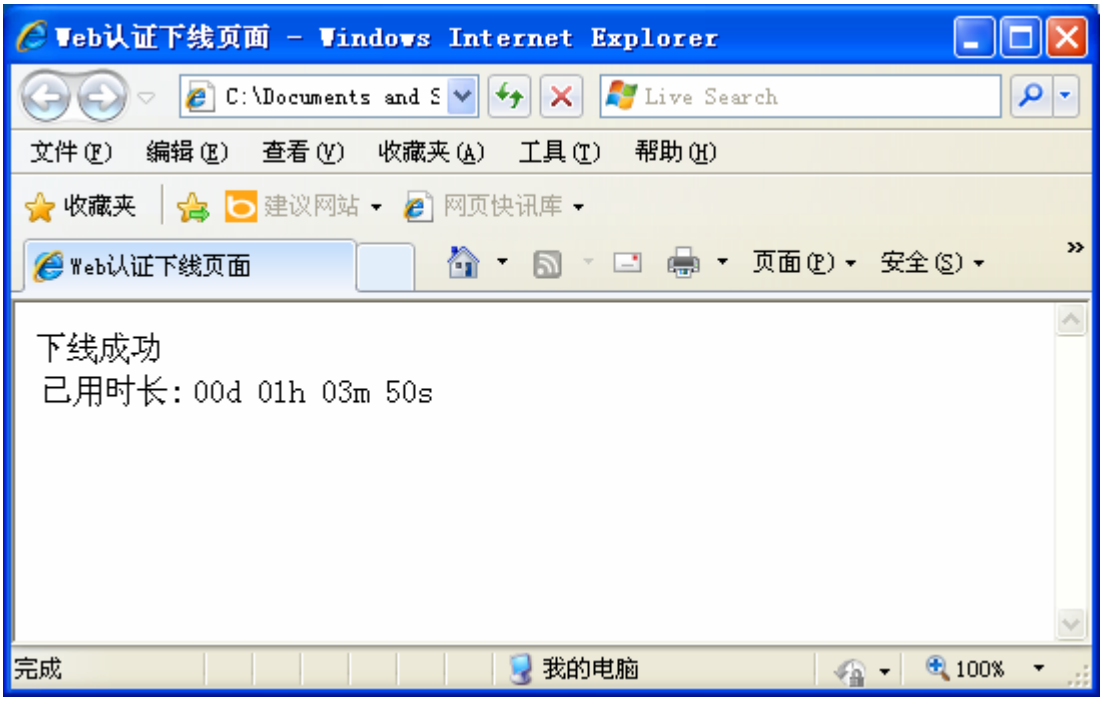
```
<html>
  <head>
  <title>Web 认证下线页面</title>
  </head>
  <script language="javascript">
    // 获取已用时长信息
    function requestOfflineInfo() {
      var _timeused=document.getElementById("timeused");
      var script=document.createElement("script");
      script.src="getofflineinfo"+location.search;
      _timeused.appendChild(script);
}

function init() {
        requestOfflineInfo();
}
  </script>

  <body onload="init()">
```

```
        下线成功<br>
    <table>
    <tr><td>已用时长:</td><td id="timeused"></td></tr>
    </table>
      </body>
</html>
```

根据上述的定制，内置 portal 服务器向用户推送的下线页面样式大致如下



上述的下线页面就已具备了所有必要的元素。用户可以在此基础之上进行美化，以及添加一些其他功能。比如添加背景、设置各种页面元素的样式等

↘ 页面打包规范

按照本规范定制好页面后，需要将所有页面和页面元素文件打包，上传到设备，然后使用该页面包。有关压打包的相关规范如下：

1. 按照本规范定制好页面后，需要将所有页面和页面元素文件（如图片文件、样式表文件等）打包成 ZIP 格式的压缩包，比如 portal1_page.zip。
2. 页面包中可以包含目录。如下图所示，portal1_page.zip 中就包含有 style 目录。目录里包含了页面的 css 文件及其他图片资源文件。

..(上层目录)				
style	81.28 KB	60.69 KB	文件夹	2012-11-15 10:34:48
check_offline.htm	9.81 KB	3.34 KB	HTML 文档	2012-11-15 10:35:38
offline.htm	6.40 KB	2.65 KB	HTML 文档	2012-11-15 10:34:24
online.htm	13.13 KB	4.14 KB	HTML 文档	2012-11-15 10:34:10
login.htm	11.79 KB	3.90 KB	HTML 文档	2012-11-15 10:33:54
check_offline_mobile.htm	9.38 KB	3.22 KB	HTML 文档	2012-10-31 14:24:46
login_mobile.htm	10.39 KB	3.21 KB	HTML 文档	2012-10-31 11:47:16
online_mobile.htm	13.96 KB	3.91 KB	HTML 文档	2012-10-22 17:26:46
favicon.ico	1 KB	1 KB	图标	2012-07-02 09:41:58
offline_mobile.htm	5.09 KB	2.01 KB	HTML 文档	2012-06-30 11:07:18

页面包打包之后，然后通过 TFTP 等工具上传到设备的 flash:/portal/zip/目录下。然后要为 portal 服务器指定使用该页面包(也就是将 portal 服务器与页面包关联)，为 portal 服务器指定页面包的具体过程，请参考 WEB 认证相关的配置指南。为 portal 服务器指定页面包之后，就可以看到 flash:/portal/ext_zip/目录下会生成一个与压缩包同名的目录，比如，压缩包名称为 portal1_page.zip，就会生成 flash:/portal/ext_zip/protal1_page/这个目录，压缩包中的内容会自动解压到该目录下。之后，portal 服务器就可以为用户推送用户指定的 WEB 认证页面了。

配置举例

配置定制也面包

【配置方法】

- 配置定制也面包

```
Ruijie(config.tmplt.iportal)#page-suit ruijiepage
```

【检验方法】

- 查看配置是否成功

```
Ruijie#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:      iportal
  Page-suit:    ruijiepage
  Advertising url:  default
  Advertising mode: online-popup
  Type:      Intral Portal
  Acctmlist:default
  Authmlist:default
```

1.4.37 升级兼容性说明

配置效果

- 部分配置命令在 11.X 系列软件上做了优化，格式上有所变化，具体参考后面的说明。
- 10.X 系列软件可以实现平滑升级，不会出现功能丢失的情况，但是升级后部分旧命令的显示会转化为新命令。
- 在 11.X 系列软件上对这部分旧命令执行 no 操作会提示不支持，需要用新的格式执行 no 操作。

注意事项

无

配置方法

- 部分格式变化的命令建议使用新格式配置。

检验方法

- 10.X 软件版本升级到 11.X 软件版本不会出现功能丢失，同时显示以及保存的格式采用新命令。
- 新格式命令的功能效果和旧命令一致。

相关命令

本小节

↘ 配置一代 web 认证的 portal 服务器 ip 地址

【命令格式】 **http redirect** *ip-address*

【参数说明】 *ip-address*：一代 web 认证的 eportal 服务器 ip 地址

【命令模式】 全局配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板，然后用模板模式下的 ip 命令配置和显示服务器的 ip 地址，具体参考 1.4.1 章节。

↘ 配置一代 web 认证的 portal 服务器资源地址

【命令格式】 **http redirect homepge** *url*

【参数说明】 *url*：一代 web 认证的 eportal 服务器资源地址

【命令模式】 全局配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板，然后用模板模式下的 url 命令配置和显示服务器地址，具体参考 1.4.1 章节。

↘ 配置 portal-server

【命令格式】 **portal-server [eportal1 | eportalv2]**

【参数说明】 **eportav1**：一代 web 认证的 portal 信息

eportav2：二代 web 认证的 portal 信息

【命令模式】 全局配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 或者 eportalv2 模板，然后用对应的信息填充，portal-server

主要参数包括服务器 ip 地址和 url 地址，会被模板中的 ip 命令和 url 命令替代。

配置接口 web 认证受控

【命令格式】 **web-auth port-control**

【参数说明】 无

【命令模式】 接口配置模式

【使用指导】 11.X 版本会将该命令转化 web-auth enable <type>这里的 type 是指一代或者二代，默认是一代。

配置仅 ip 绑定模式

【命令格式】 **web-auth port-control ip-only-mode**

【参数说明】 无

【命令模式】 接口配置模式

【使用指导】 11.X 版本首先会将该命令转化为一个 eportalv1 模板或者 eportalv2 模板，取决于实际配置。然后用模板模式下的 bindmode 命令配置和显示服务器绑定模式，具体参考 1.4.1 和 1.4.2 章节章节。

配置基于 vlan 的 web 认证功能

【命令格式】 **web-auth allow-vlan** *list*

【参数说明】 *list*：设置支持基于 VLAN 的 web 认证的 VLAN 列表为 list。

【命令模式】 全局配置模式

【使用指导】 11.X 版本会将该命令转化为一个 scc 免认证 vlan 命令。

显示一代 web 认证配置信息

【命令格式】 **show http redirect**

【参数说明】 无

【命令模式】 特权模式

【使用指导】 11.X 版本该旧命令不可用，改为 show web-auth template。

显示端口受控信息

【命令格式】 **show web-auth port-control**

【参数说明】 无

【命令模式】 特权模式

【使用指导】 11.X 版本该旧命令不可用，改为 show web-auth control。

配置举例

配置一代 web 认证

【配置方法】

- 产品运行 10.X 版本并且已经配置了一代 web 认证服务器 ip

```
Ruijie(config)# http redirect 192.168.197.64
```

- 产品升级到 11.X 版本

【检验方法】

- 升级后 show running-config，配置已更新为新命令格式

Ruijie#sh running-config

```
web-auth template eportalv1
  Ip 192.168.197.64
!
```

1.4.38 配置无线web认证降噪功能

配置效果

- 用户重定向过程访问某个目的 ip 的次数等于配置的次数，就把用户后续访问该目的 ip 的报文都丢弃不处理，达到降噪目的。

注意事项

- 需根据网络环境和实际需求配置降噪策略的两个参数(老化时间和命中次数),以免用户的正常报文被当作噪声报文丢弃，无法重定向。

配置方法

↘ 全局模式下配置。

【命令格式】 **web-auth noise** [**aging** *agmin*] [**hit** *times*]

【参数说明】 *agmin*：噪声表项老化时间，默认 1 分钟

times ：噪声判定规则：访问某个目的 ip 达到 *times* 次，就认为是噪声，默认 3 次

【命令模式】 全局模式

【使用指导】 无

检验方法

- 配置开启此功能后，重定向过程，用户访问某个目的 ip 次数到达配置的次数后，再次访问该目的 ip 就不会被重定向。等到噪声表项老化时间到期后，再访问该目的 ip 又可以被重定向。

配置举例

↘ 配置无线 web 认证降噪功能

【配置方法】

- 配置无线 web 认证降噪功能参数。

```
Ruijie(config)# web-auth noise aging 1 hit 3
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
```

1.4.39 配置微信认证IOS自动弹框控制命令

配置效果

- 微信认证（微信关注认证，微信连 wifi 等）场景下，IOS 终端能够自动弹窗并且显示 wifi 信号（结合微信流量放行功能，IOS 终端未上线前可以使用微信 App）。

注意事项

- 需配合微信流量放行（web-ctrl free-auth weixin）功能使用。
- 该功能开启，会降低重定向性能。
- 如果有放行苹果网站的相关配置，该功能开启无效。例如：下例任何一个配置都会导致该功能无效，

  web-ctrl free-auth iphone

  web-auth acl white-url http://www.apple.com.cn

  web-auth acl white-url http://captive.apple.com

配置方法

↘ 配置认证方法

- 全局模式下配置。

【命令格式】 **http redirect adapter ios**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 无

检验方法

- 配置开启此功能后，微信认证（微信关注认证，微信连 wifi 等）场景下，IOS 终端能够自动弹窗并且显示 wifi 信号（结合微信流量放行功能，IOS 终端未上线前可以使用微信 App）。

配置举例

↘ 配置认证方法

【配置方法】
- 打开 IOS 自动弹框控制开关功能。

```
Ruijie(config)# http redirect adapter ios
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
…
http redirect adapter ios
```

1.4.40 配置微信认证无感知命令

配置效果

- 微信认证（微信关注认证，微信连 wifi 等）场景下，用户第二次关联 SSID，无需经过认证流程，服务器直接设置上线。

注意事项

- 要开启 ip dhcp snooping 功能，该功能才生效。

配置方法

↘ 全局模式或者 WLAN 安全下配置。

【命令格式】 **web-auth sta-perception enable**
【参数说明】 无
【命令模式】 全局模式或者 WLAN 安全模式
【使用指导】 无

检验方法

- 配置开启此功能后，微信认证（微信关注认证，微信连 wifi 等）场景下，用户第二次关联 SSID，无需经过认证流程，服务器直接设置上线。

配置举例

↘ 配置微信认证无感知命令

【配置方法】
- 打开微信认证二次无感知开关功能。
- 非必须配置，在微信认证场景下配置有效。

```
Ruijie(config)# web-auth sta-perception enable
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config
```

1.4.41 配置wlansec下的用户检测

配置效果

- 当配置了 wlansec 下的用户在线检测功能后，在指定的周期内如果流量低于一定的门限，设备会自动将用户下线，以免造成持续计费而导致用户的经济损失。

注意事项

- 同全局的 SCC 配置命令：offline-detect interval *interval* thredshold *thredshold* 一样的效果。但是 wlansec 下的配置优先级更高。

配置方法

- 可选配置。默认为 15 分钟内无流量就将用户下线。

流量门限参数 flow 如果配置成 0，则表示进行无流量检测。

10.x 默认关闭 wlansec 下的流量检测，使用全局的配置。所以升级 11.x 后要手动关闭 wlansec 下的配置。

检验方法

- 配置了在线用户检测功能后，用户上线后，将指定的已认证终端关机，然后等待指定的周期，在设备上 show web user 查询命令确认指定的用户已经下线。

相关命令

配置 wlansec 下的用户检测

【命令格式】 **web-auth offline-detect interval** *interval* **flow** *thredshold*

no web-auth offline-detect

default web-auth offline-detect

【参数说明】 *interval*：下线检测周期，取值范围为 1-65535min，默认 15 min。

thredshold：流量门限，取值范围为 0-4294967294Bytes。默认为 0，表示无流量检测下线。

no web-auth offline-detect：关闭用户在线检测功能。

default web-auth offline-detect：恢复成默认值，即 15 分钟无流量就将已在线认证用户下线。

【缺省配置】 15 分钟

【命令模式】 wlansec 配置模式

【使用指导】 此命令可以用来配置用户在线活，指定在一定的时间段内在线认证用户的流量低于指定的门限时将用户下线。

配置举例

配置 wlansec 下的用户检测

【配置方法】

- 设置 wlansec 1 下的用户检测

```
Ruijie(config)#wlansec 1
Ruijie(config-wlansec)#web-auth offline-detect interval 30 flow 10000
```

【检验方法】

- 查看配置是否成功

```
Ruijie(config)#show running-config | be wlansec 1
wlansec 1
  web-auth offline-detect interval 30 flow 10000
…
```

1.4.42 配置Portal协议 0x05 号属性透传功能

配置效果

- 配置 Portal 协议 0x05 号属性透传功能，开启后 web 认证支持下面两个场景的属性透传功能：
  1、 和中移动 portal 协议对接时， web 认证会把错误标识封装到 0x05 号属性（ErrID）中并透传到 Portal Server。
  2、 和华为 portal 2.0 协议对接时，web 认证会把 RADIUS 等第三方鉴权设备的提示信息封装到 0x05 号属性（TextInfo）中并透传到 Portal Server。

注意事项

- 该功能默认是关闭的。

配置方法

- 可选配置
- 需要中移动 portal 协议规定 的 ErrID（0x05）属性时配置。
- 需要华为 portal 2.0 协议规定 的 TextInfo（0x05）属性时配置。

相关命令

↘ 全局模式下配置。

【命令格式】 **web-auth portal-attribute 5**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 一般在特定 Portal Server 需要设备上传错误标识（ErrID）时开启。

【命令格式】 **web-auth portal-attribute textinfo**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 一般在特定 Portal Server（使用华为 portal 2.0 协议规范）需要设备上传 RADIUS 等第三方鉴权设备的提示信息（TextInfo）时开启。

检验方法

- 开启此命令后，在回应 portal 的 ack 报文中会带上 0x05 号属性。

配置举例

↘ 配置 portal 协议 0x05 号属性透传功能

【配置方法】
- 配置 0x05 号属性透传功能。

```
Ruijie(config)# web-auth portal-attribute 5
```

或者：

```
Ruijie(config)# web-auth portal-attribute textinfo
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
```

1.4.43 配置Portal认证账号唯一性检查功能

配置效果

- 配置 Portal 认证账号唯一性检查功能，开启后 web 认证会检查用户认证请求的账号信息，如果发现该账号已经有其他用户在线，则直接应答 ACK_AUTH 带 ErrCode 2 给 Portal Server。有些 Portal Server 收到该种应答后，就会给用户推送“终端抢占”提示信息。

注意事项

- 该功能默认是关闭的。

配置方法

- 可选配置
- Portal Server 需要给用户推送“终端抢占”提示信息时配置。

相关命令

↘ 全局模式下配置。

【命令格式】 **web-auth portal-valid unique-name**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 一般在特定 Portal Server 需要给用户推送“终端抢占”提示信息时开启。

检验方法

- 开启此命令后，如果发现相同账号已经有其他用户在线，则直接应答 ACK_AUTH 带 ErrCode 2 给 Portal Server。

配置举例

↘ 配置 Portal 认证账号唯一性检查功能

【配置方法】
- 配置认证账号唯一性检查功能。

```
Ruijie(config)# web-auth portal-valid unique-name
```

【检验方法】
- 查看配置是否成功

```
Ruijie(config)#show running-config
```

1.4.44 配置无线wifidog一键配置

配置效果

- wifidog 的模板信息，端口受控，ios 弹窗，无感知配置可以集中一条命令配置生效。

注意事项

- 一键配置的 no 操作只能删除模板信息和受控端口，不对全局配置生效。

配置方法

配置无线 wifidog 一键配置

- 可选配置

【命令格式】 **web-auth wifidog-template** *template-name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-address* **nas-ip** *nas-ip-address* **url** *url-string* [**perception**]

【参数说明】 *template-name*：模板名称

wlanid-start：开启受控的 wlan 范围开始

wlanid-end：开启受控的 wlan 范围结束

portal-ip-address： portal 服务器的地址

nas-ip-address：设置 wifidog 的设备接入服务 ip，用于服务器向此 ip 发起通讯

url-string：portal 服务器的认证页面地址

perception：配置无感知功能

【命令模式】 全局模式

【使用指导】 在开始一键配置之前，必须先创建 wlansec，否则无法受控配置成功。

检验方法

- show run 配置正常

配置举例

配置无线 wifidog 一键配置

【配置方法】

- 无线 wifidog 一键配置

```
Ruijie(config)# web-auth wifidog-template aaa wlan-range 1 32 portal-ip 172.21.6.78 nas-ip
192.168.197.227 url http://172.21.6.78/auth/wifidogAuth
```

【检验方法】

- 使用 **show running-config** 命令，可以查看是否配置成功。

1.4.45 配置无线微信连wifi一键配置

配置效果

- 微信连 wifi 的模板信息，端口受控， ios 弹窗，无感知配置可以集中一条命令配置生效。

注意事项

- 一键配置的 no 操作只能删除模板信息和受控端口，不对全局配置生效。

配置方法

配置无线微信连 wifi 一键配置

- 可选配置

【命令格式】 **web-auth wechat-template** *template-name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-address* **nas-ip nas-ip-address** [**perception** | **ios-adapter**]

【参数说明】 template-name：模板名称
wlanid-start：开启受控的 wlan 范围开始
wlanid-end：开启受控的 wlan 范围结束
portal-ip-addr： portal 服务器的地址
nas-ip-addr：设置微信连 wifi 的设备接入服务 ip，用于服务器向此 ip 发起通讯
perception：配置无感知功能
ios-adapter：配置自动弹窗功能

【命令模式】 全局模式

【使用指导】 在开始一键配置之前，必须先创建 wlansec，否则无法受控配置成功。

检验方法

- show run 配置正常

配置举例

配置无线微信连 wifi 一键配置

【配置方法】
- 无线微信连 wifi 一键配置

```
Ruijie(config)# web-auth wechat-template aaa wlan-range 1 32 portal-ip 172.21.6.78 nas-ip 192.168.197.227
```

【检验方法】
- 使用 **show running-config** 命令，可以查看是否配置成功。

1.5 监视与维护

清除各类信息

作用	命令

强制用户下线	**clear web-auth user** { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* }
删除全部免认证网络资源	**clear web-auth direct-site**
删除全部免认证用户	**clear web-auth direct-host**
删除 web 黑白名单配置	**clear web-auth acl**

查看运行情况

作用	命令
查看 web 认证黑白名单。	**show web-auth acl**
查看 web 认证基本参数配置。	**show web-auth parameter**
查看 web 认证模板配置信息	**show web-auth template**
查看免 Web 认证的用户范围。	**show web-auth direct-host**
查看直通地址范围。	**show web-auth direct-site**
查看直通 ARP 范围。	**show web-auth direct-arp**
查看 TCP 拦截端口。	**show web-auth rdport**
接口上的认证配置信息。	**show web-auth control**
查看所有用户或是指定用户的在线信息。	**show web-auth user** { **all** | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string* | **session-id** *num* | **escape** }
显示 web 认证 CGI 配置	**show web-auth cgi**
查看全局 web 认证基本信息	**show web-auth global**
查看全局 web 认证方法	**show web-auth global authentication**
查看全局 web 认证定制页面包	**show web-auth global customized-pages**
查看内置认证服务器信息	**show web-auth global local-portal**
查看全局 web 认证模板信息	**show web-auth global template**
查看全局 web 认证类型	**show web-auth global webauth-type**
查看 web 认证配置信息	**show web-auth info**
查看内置 web 认证信息	**show web-auth local-portal**
查看 web 认证的 portal- check 信息	**show web-auth portal-check**
查看 web 认证降噪功能配置信息	**show web-auth noise**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
web 认证 debug	**debug web-auth all**

2 AAA

2.1 概述

AAA 是 Authentication Authorization and Accounting（认证、授权和记账）的简称，它提供了对认证、授权和记账功能进行配置的一致性框架，锐捷网络设备产品支持使用 AAA。

AAA 以模块方式提供以下服务：

认证：验证用户是否可获得访问权，可选择使用 RADIUS 协议、TACACS+协议或 Local（本地）等。身份认证是在允许用户访问网络和网络服务之前对其身份进行识别的一种方法。

授权：授权用户可使用哪些服务。AAA 授权通过定义一系列的属性对来实现，这些属性对描述了用户被授权执行的操作。这些属性对可以存放在网络设备上，也可以远程存放在安全服务器上。

记账：记录用户使用网络资源的情况。当 AAA 记账被启用时，网络设备便开始以统计记录的方式向安全服务器发送用户使用网络资源的情况。每个记账记录都是以属性对的方式组成，并存放在安全服务器上，这些记录可以通过专门软件进行读取分析，从而实现对用户使用网络资源的情况进行记账、统计、跟踪。

尽管 AAA 是最主要的访问控制方法，锐捷产品同时也提供了在 AAA 范围之外的简单控制访问，如本地用户名身份认证、线路密码身份认证等。不同之处在于它们提供对网络保护程度不一样，AAA 提供更高级别的安全保护。

使用 AAA 有以下优点：

- 灵活性和可控制性强
- 可扩充性
- 标准化认证
- 多个备用系统

协议规范

- 暂无相应规范

2.2 典型应用

典型应用	场景描述
无域环境下的认证、授权、记账	所有用户处于同一个域，进行认证、授权、记账
多域环境下的认证、授权、记账	处于不同域的用户，采用不同的方法进行认证、授权、记账

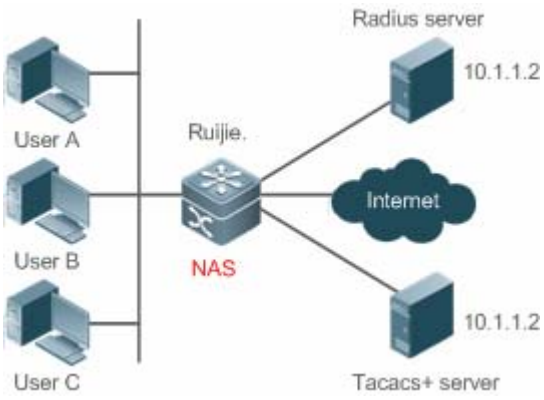
2.2.1 无域环境下的认证、授权、记账

应用场景

在 图 2-1 所示的网络应用中，为了更好地对网络访问控制器设备（NAS，以下简称网络设备）进行安全管理，需要满足如下应用要求：

1. 不同的管理人员有各自的用户账号，其用户名和口令不能共享，便于帐号管理和防止泄漏。
2. 对网络设备的访问需经过认证，用户认证的实现方式可以分为本地认证和集中认证，应采用集中认证和本地认证相结合的方式，集中认证为主用、本地认证为备用。在集中认证过程中，要求先通过 RADIUS 服务器认证，若无响应再转本地认证。
3. 在认证时，不同的用户可以被限制只能访问特定的网络设备。
4. 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限。
5. 服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计(本例采用 TACACS+进行记账）。

图 2-1



【注释】 UserA，UserB，UserC 直接或者通过网络和 NAS 相连接。
NAS 通常为接入交换机或者汇聚交换机。
RADIUS 服务器可以是 Windows 2000/2003 Server（IAS）、UNIX 系统所带组件，也可以是一些厂商提供的专用服务器软件。
TACACS+服务器可以是一些厂商提供的专用的服务器软件。

功能部属

- 在 NAS 上启用 AAA
- 在 NAS 上配置安全服务器
- 在 NAS 上配置本地用户

- 在 NAS 上配置认证
- 在 NAS 上配置授权
- 在 NAS 上配置记账

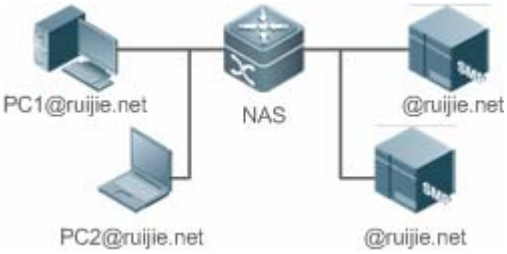
2.2.2 多域环境下的认证、授权、记账

应用场景

通过配置网络访问控制器设备实现基于域名的 AAA 服务，包括认证、授权、记账功能：

- 使用 802.1x 客户端进行登录认证，使用用户名为 PC1@ruijie.net 或 PC2@ruijie.com.cn，再输入正确的密码进行认证就可认证成功。
- 对用户进行分权限管理：把网络管理用户分为超级用户和普通用户。其中，超级用户对网络设备拥有查看和配置的权限，普通用户对网络设备只拥有特定的查看权限。
- 认证服务器端可将用户的认证信息、授权信息和网络行为记录在服务器中，以供日后查看和审计。

图 2-2



【注释】 PC1@ruijie.net，PC2@ruijie.com.cn 直接或者通过网络和 NAS 相连接。
NAS 通常为接入交换机或者汇聚交换机。
SAM 为锐捷公司提供的通用 RADIUS 服务器。

功能部属

- 在 NAS 上启用 AAA
- 在 NAS 上配置安全服务器
- 在 NAS 上配置本地用户
- 在 NAS 上定义 AAA 服务的方法列表
- 在 NAS 上打开基于域名的 AAA 服务开关
- 在 NAS 上创建域并配置域属性集

2.3 功能详解

基本概念

本地认证、远程服务器认证

对用户进行认证时，如果使用 NAS 上的用户数据库进行密码校验，就称为本地认证。

对用户进行认证时，如果使用远程服务器上的用户数据库进行密码校验，就称为远程服务器认证。目前，远程服务器认证主要是 RADIUS 服务器认证和 TACACA+服务器认证。

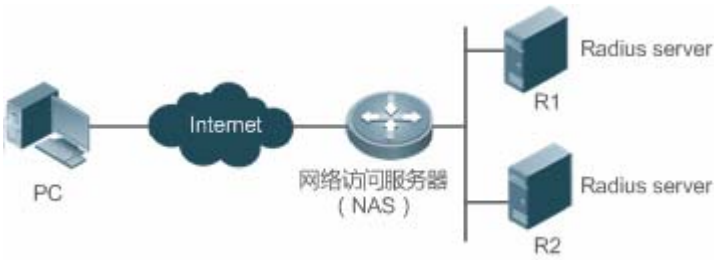
方法列表

由于对用户进行认证、授权和记账可以使用不同的安全方法，您需要使用方法列表定义一个使用不同方法对用户进行认证、授权和记账的前后顺序。方法列表可以定义一个或多个安全协议，这样可以确保在第一个方法失败时，有备用系统可用。锐捷产品使用方法列表中列出的第一个方法时，如果该方法无应答，则选择方法列表中的下一个方法。这个过程一直持续下去，直到与列出的某种安全方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则该安全功能宣告失败。

方法列表仅是定义将要被依次查询的、并用于认证用户身份的一系列安全方法。方法列表使您能够指定一个或多个用于身份认证的安全协议，这样确保在第一种方法失败的情况下，可以使用身份认证备份系统。我司产品使用第一种方法认证用户的身份，如果该方法无应答，将选择方法列表中的下一种方法。 这个过程一直持续下去，直到与列出的某种身份认证方法成功地实现通信或用完方法列表。如果用完方法列表而还没有成功实现通信，则身份认证宣告失败。

⚠ 只有在前一种方法没有应答的情况下，锐捷产品才会尝试下一种方法。例如在身份认证过程中，某种方法拒绝了用户访问，则身份认证过程结束，不再尝试其他的身份认证方法。

图 2-3



上图说明了一个典型的 AAA 网络配置，包含两台安全服务器：R1 和 R2 是 RADIUS 服务器。以及一台网络访问服务器（NAS），可以作为 RADIUS 客户端。

假设系统管理员已定义了一个方法列表，在这个列表中，R1 首先被用来获取身份信息，然后是 R2，最后是访问服务器上的本地用户名数据库。如果一个远程 PC 用户试图拨号进入网络，网络访问服务器首先向 R1 查询身份认证信息，假如用户通过了 R1 的身份认证，R1 将向网络访问服务器发出一个 ACCEPT 应答，这样用户即获准访问网络。如果 R1 返回的是 REJECT 应答，则拒绝用户访问网络，断开连接。如果 R1 无应答，网络访问服务器就将它看作 TIMEOUT，并向 R2 查询身份认证信息。这个过程会一直在余下的指定方法中持续下去，直到用户通过身份认证、被拒绝或对话被中止。如果所有的方法返回 TIMEOUT，则认证失败，连接将被断开。

REJECT 应答不同于 TIMEOUT 应答。REJECT 意味着用户不符合可用身份认证数据库中包含的标准，从而未能通过身份认证，访问请求被拒绝。TIMEOUT 则意味着安全服务器对身份认证查询未作应答，当检测到一个 TIMEOUT 时，AAA 选择身份认证方法列表中定义的下一个身份认证方法将继续进行身份认证过程。

在本文中，与 AAA 安全服务器相关的认证、授权和记账配置，均以 RADIUS 为例，而与 TACACS+有关的内容请另外参考“配置 TACACS+”。

AAA 服务器组

定义一个 AAA 服务器组，用于把一个或几个同一类型的服务器划分为同一组。配置方法列表时，引用该服务器组，则使用该方法列表进行认证、授权、记账操作时，首先向被引用服务器组中的服务器发起请求。

支持 VRF 的 AAA 组

Virtual Private Networks (VPNs)为用户提供了一种安全的方式在 ISP 骨干网上共享带宽。一个 VPN 即是共享路由的站点集。用户站点通过一到多个接口链接到服务提供商网络，VPN 路由表也叫 VPN routing/forwarding (VRF) table，AAA 可以为每个自定义服务器组指定 VRF。

使用指定有 VRF 的服务器组进行 AAA 操作时，向远程服务器发起请求报文。这些请求报文的源地址是根据服务器 IP 地址在配置的 VRF 中查找得到的一个合适的源 IP 地址。

如果使用命令 **ip radius/tacacs+ source-interface** 指定请求报文的源接口，则从该源接口获取的 IP 地址优先于 VRF 中查找得到的 IP 地址。

功能特性

功能特性	作用
AAA认证	验证是否允许用户接入网络
AAA授权	定义用户可以使用哪些服务或拥有哪些权限
AAA记账	记录用户使用网络资源的情况
AAA多域	针对不同域的 802.1x 用户，创建认证、授权和记账方案。

2.3.1 AAA认证

在 AAA 中，认证、授权和计费是三个独立的业务过程。认证是用来验证用户是否可以获得访问权，其职责是完成各接入或服务请求的用户名、密码和用户信息的交互认证过程。在 AAA 中，可以只使用认证，而不使用授权或计费。

要配置 AAA 身份认证，首先得定义一个身份认证方法的命名列表，然后各个应用使用已定义列表进行认证。方法列表定义了身份认证的类型和执行顺序。对于已定义的身份认证方法，必须有特定的应用才会被执行。默认方法列表是唯一的例外。所有应用在未进行配置时使用默认方法列表。

AAA 认证方案：

- 不认证（none）

对用户非常信任，不对其进行合法性检查。一般情况下不采用这种方法。

- 本地认证（local）

认证过程在 NAS 设备上完成，用户信息（包括用户名、密码和各种属性）直接配置在接入设备上。当配置 local 参数使用本地数据库进行验证时，需要使用 username password 命令预先在本地创建用户数据库。

- 远程服务器组认证（group）

认证过程在 NAS 和一个远程服务器组之间完成（一个服务器组可包含任意个相同类型的服务器），NAS 和远程服务器之间通过 RADIUS 或 TACACS+协议通信。用户信息集中在远程服务器上统一管理，可以实现大容量、高可靠性、支持多设备的集中式统一认证。为提防远程服务器组的服务器均无效时，可配置本地认证作为备选认证方式完成认证。

AAA 认证类型

锐捷产品目前支持以下认证类型：

- Login（登录）认证

针对 SSH、Telnet、FTP 等终端接入用户，在用户登录到 NAS 命令行界面时进行身份认证。

- Enable 认证

针对的是用户终端登录到 NAS 上的命令行界面以后，提升命令行界面执行权限时进行认证。即对 enable（进入特权模式）行为进行认证。

- PPP 认证

针对 PPP 拨号接入用户进行身份认证。

- DOT1X（IEEE802.1x）认证

针对 IEEE802.1x 接入用户进行身份认证。

- iportal（内置 portal）认证

针对使用一代 portal 服务器来进行身份认证。

- Web-auth（二代 portal）认证

针对使用二代 portal 服务器来进行身份认证。

相关配置

启动 AAA

缺省情况下，AAA 没有启动。

使用 **aaa new-model** 命令可以启动。

配置 AAA 认证方案

缺省情况下，没有配置任何 AAA 认证方案。

确定使用本地（Local）认证还是远程服务器认证。如果用户使用远程服务器认证，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 认证，则需要在 NAS 上配置本地用户数据库信息。

↘ 配置 AAA 认证方法

缺省情况下，没有配置任何 AAA 认证方法。

确定要配置的接入方式，针对不同接入方式配置不同的认证方法。

2.3.2 AAA授权

AAA 授权使管理员能够对用户可使用的服务或权限进行控制。启用 AAA 授权服务以后，网络设备通过本地或服务器中的用户配置文件信息对用户的会话进行配置。完成授权以后，该用户只能使用配置文件中允许的服务或只具备许可的权限。

↘ AAA 授权方案

- 直接授权（none）

对用户非常信任，直接授权用户的权限为接入设备允许用户所使用的默认权限。

- 本地授权（local）

授权过程在 NAS 设备上完成，根据 NAS 上为本地用户配置的相关属性进行授权。

- 远程服务器授权（group）

授权过程在 NAS 和远程服务器组之间完成。当远程服务器组的服务器均无效时，可以配置本地授权或直接授权作为备选授权方式完成授权。

↘ AAA 授权类型

- Exec 授权

针对的是用户终端登录到 NAS 上的 CLI 界面时，授予用户终端的权限级别（分为 0~15 级）。

- Config-commands 授权

对配置模式（包括全局配置模式及其子模式）下的命令进行授权。

- Console 授权

对通过控制台登录的用户所执行命令的授权。

- Command（命令）授权

用户终端登录到 NAS 上的 CLI 界面以后，针对具体命令的执行授权。

- Network（网络）授权

授予网络连接上的用户会话可用的服务。例如 PPP、SLIP 等网络连接接通过 Network 授权，可以获得诸如流量、带宽、超时等服务配置。

相关配置

↘ 启动 AAA

缺省情况下，AAA 没有启动。

使用 **aaa new-model** 命令可以启动。

↘ 配置 AAA 授权方案

缺省情况下，没有配置任何 AAA 授权方案。

确定使用本地(local)授权还是远程服务器授权。如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 授权，则需要在 NAS 上配置本地用户数据库信息。

↘ 配置 AAA 授权方法

缺省情况下，没有配置任何 AAA 授权方法。

确定要配置的接入方式，针对不同接入方式配置不同的认证方法。

2.3.3 AAA记账

在 AAA 中，记账是一个和认证、授权同级别的独立流程，其职责为发送记账开始、更新和结束请求给所配置的记账服务器，由服务器记录用户使用网络资源的情况，实现对用户的活动进行计费、审计以及跟踪等功能。

在 AAA 配置中，记账方案不是必须配置的。

↘ AAA 记账方案

- 不记账（none）

不对用户记账。

- 本地记账（local）

记账过程在 NAS 上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。

- 远程服务器组记账（group）

记账过程在接入设备和远程的服务器之间完成。当远程服务器组失效时，可配置本地记账作为备选记账方式完成记账。

↘ AAA 记账类型

- Exec 记账

针对的是用户终端登录到 NAS 上的 CLI 界面时，在登入和登出时分别进行记账。

- Command 记账

用户终端登录到 NAS 上的 CLI 界面以后，记录其具体执行的命令。

- Network 记账

记录与网络连接用户（如 802.1X、WEB 认证等用户）会话有关的信息。

相关配置

启动 AAA

缺省情况下，AAA 没有启动。

使用 **aaa new-model** 命令可以启动。

配置 AAA 记账方案

缺省情况下，没有配置任何 AAA 记账方案。

确定使用本地（Local）记账还是远程服务器记账。如果用户使用远程服务器记账，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 记账，则需要在 NAS 上配置本地用户数据库信息。

配置 AAA 记账方法

缺省情况下，没有配置任何 AAA 记账方案。

确定要配置的接入方式，针对不同接入方式配置不同的记账方法。

2.3.4 AAA多域

在多域环境下，同一台网络访问服务器（NAS）设备可为不同域中的用户提供 AAA 服务，各域中用户的属性（例如用户名及密码、服务类型、权限等）有可能各不相同，因此有必要通过设置域的方法把它们区分开，并为每个域单独配置包括 AAA 服务方法列表（例如使用的 RADIUS）在内的属性集。

本产品支持以下几种的形式的用户名

6. userid@domain-name
7. domain-name\userid
8. userid.domain-name
9. userid

对于第 4 种不带 domain-name 的形式的用户名（即以上第 4 种：userid），认为其域名称为 default，即为默认的域名。

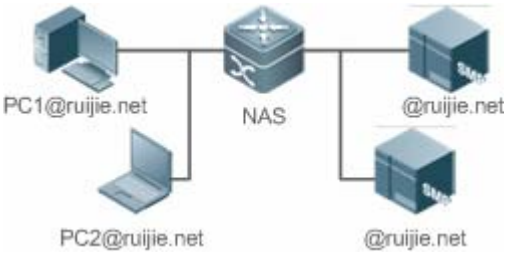
设备基于域名的 AAA 服务基本原理如下：

- 解析用户携带的域名称
- 根据域名称查找用户所配置的域
- 根据设备上域配置信息查找相应的 AAA 服务的方法列表名
- 根据方法列表名在系统中查找对应的方法列表
- 使用该方法列表提供 AAA 服务

上述任何一个步骤失败，用户将无法使用申请的 AAA 服务。

以下是典型的多个域环境拓扑图：

图 2-4



相关配置

↘ 启动 AAA

缺省情况下，AAA 没有启动。

使用 **aaa new-model** 命令可以启动。

↘ 定义 AAA 服务的方法列表

缺省情况下，没有配置任何 AAA 服务的方法列表。

配置方法列表请参照 5.2.1、5.2.2、5.2.3 章节

↘ 启用基于域名的 AAA 服务

缺省情况下，基于域名的 AAA 服务没有启动。

使用 **aaa domain enable** 命令可以启动基于域名的 AAA 服务。

↘ 创建域

缺省情况下，没有配置任何域。

使用 **aaa domain** *doman-name* 命令配置域名。

↘ 配置域属性集

缺省情况下，没有域属性集。

域属性集包括该域使用的认证、授权、记账方法列表；域的同时在线人数；是否去除用户名中的域名；域是否生效等。

↘ 查看域配置

使用 **show aaa domain** 查看域配置

系统最多支持配置 32 个域。

2.4 配置详解

配置项	配置建议 & 相关命令

配置AAA认证	如果要确认用户的身份，则必须配置。	
	aaa new-model	开启 AAA。
	aaa authentication login	定义 Login 认证的认证方法列表。
	aaa authentication enable	定义 enable 认证的方法类型和执行顺序。
	aaa authentication dot1x	定义 802.1x 认证的方法类型和执行顺序。
	aaa authentication ppp	定义 PPP 认证的方法类型和执行顺序。
	aaa local authentication attempts	设置 login 用户尝试登录次数的最大值。
	aaa local authentication lockout-time	设置 login 用户被锁定的时间长度。
	aaa local user allow public account	设置 Web 认证或者内置 Web 认证的情况下，本地账户(username 或者 subs)的能否被多个终端共享。
配置AAA授权	如果要对不同用户赋予不同的权限，限制用户可以使用的服务，则必须配置。	
	aaa new-model	开启 AAA。
	aaa authorization exec	定义 exec 授权的方法类型和执行顺序。
	aaa authorization commands	定义 command 授权的方法类型和执行顺序。
	aaa authorization network	为接入用户配置授权方法列表。
	authorization exec	在特定终端线路上应用 exec 授权方法。
	authorization commands	在特定终端线路上应用 command 授权方法。
配置AAA记账	如果要实现对用户使用网络资源情况的记账、统计和跟踪，则必须配置。	
	aaa new-model	开启 AAA。
	aaa accounting exec	定义 exec 记账的方法类型及方法执行顺序。
	aaa accounting commands	定义 command 记账的方法类型及方法执行顺序。
	aaa accounting network	定义 network 记账的方法类型及方法执行顺序。
	accounting exec	在特定终端线路上应用 exec 记账方法。
	accounting commands	在特定终端线路上应用 command 记账方法。
	aaa accounting update	开启记账更新功能。
	aaa accounting update periodic	设置记账更新时间间隔。
配置AAA服务器组	如果有多台服务器且需要能灵活选择服务器进行认证、授权和记账的处理，则建议配置。	
	aaa group server	创建 AAA 自定义服务器组。
	server	添加 AAA 服务器组成员。
	ip vrf forwarding	配置服务器组的 VRF 属性。
配置基于域名的AAA服务	如果需要通过域来对接入的 802.1x 用户进行 AAA 管理，则必须配置。	
	aaa new-model	开启 AAA。
	aaa domain enable	开启基于域名的 AAA 服务。
	aaa domain	创建域，并进入域配置模式。

	authentication dot1x	在域中，关联 802.1X 认证方法列表。
	accounting network	在域中，关联 Network 记账方法列表。
	authorization network	在域中，关联 Network 授权方法列表。
	state	设置域的状态。
	username-format	设置是否在用户名中携带域名信息。
	access-limit	设置当前域可容纳接入用户的数目限制。

2.4.1 配置AAA认证

配置效果

验证用户是否可以获得访问权。

注意事项

- 如果在一个认证方案中使用多种认证方法，则认证方法的执行顺序为配置的先后顺序。只有在当前认证方法没有响应的情况下，才会采用下一种认证方法；如果当前认证方法认证失败，则不会跳转到下一个认证方案进行认证。
- 由于none方法使得请求接入的任何用户在所有认证方法都没有应答情况下能通过身份认证，所以仅将它作为备用的身份认证方法。

> 一般情况下，不要使用 none 身份认证。在特殊情况(如所有可能的申请接入用户都是可信任的，而且用户的工作不允许有由于系统故障造成的耽搁)，可以在安全服务器无应答的情况下，将 none 作为最后一种可选的身份认证方法，建议在 none 认证方法前加上本地身份认证方法。

- AAA 认证开启的情况下，如果没有配置任何方法且不存在 default 认证方法时，对于控制台允许不认证直接登录；其他接入都要进行 local 认证。
- 如果进入 CLI 界面的时候经过了 Login 身份认证（none 方法除外），将记录当前使用的用户名。此时，进行 Enable 认证的时候，将不再提示输入用户名，直接使用与 Login 认证相同的用户名进行认证，注意输入的口令要与之匹配。
- 如果进入 CLI 界面的时候没有进行 Login 认证，或在 Login 认证的时候使用了 none 方法，将不会记录用户名信息。此时，如果进行 enable 认证，将会要求重新输入用户名。这个用户名信息不会被记录，每次进行 Enable 认证都要重新输入。

配置方法

开启 AAA

- 必须配置。
- 使用 **aaa new-model** 开启 AAA。
- 缺省情况下，没有启动 AAA。

定义 Login 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication login** 配置 Login 认证的方法类型和执行顺序。
- 如果为 Login 接入用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 Login 认证方法列表。

↘ 定义 Enable 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication enable** 配置 Enable 认证的方法类型和执行顺序。
- 如果为 Enable 过程配置认证方法列表（只能配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 Enable 认证方法列表。

↘ 定义 802.1x 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication dot1x** 配置 Login 认证的方法类型和执行顺序。
- 如果为 802.1x 接入用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 dot1x 认证方法列表。

↘ 定义 PPP 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication ppp** 配置 ppp 认证的方法类型和执行顺序。
- 如果为 PPP 拨号用户配置认证方法列表，则必须配置此命令。
- 缺省情况下，没有配置 ppp 认证方法列表。

↘ 定义 Web 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication web-auth** 配置 Web 认证的方法类型和执行顺序。
- 如果为 Web 认证用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 Web 认证方法列表。

↘ 定义内置 Web 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication iportal** 配置内置 Web 认证的方法类型和执行顺序。
- 如果为内置 Web 认证用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置内置 Web 认证方法列表。

↘ 定义 SSLVPN 认证的方法类型和执行顺序。

- 使用命令 **aaa authentication sslvpn** 配置 Web 认证的方法类型和执行顺序。
- 如果为 SSLVPN 认证用户配置认证方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置 SSLVPN 认证方法列表。

↘ 设置 login 用户尝试登录次数的最大值。

- 可选配置。
- 缺省情况下，允许 login 用户尝试密码的失败次数为 3 次。

设置 login 用户被锁定的时间长度。

- 可选配置。
- 缺省情况下，当 login 用户尝试登录的次数超过最大值，被锁定的时间为 15 分钟。

设置 Web 认证或者内置 Web 认证的情况下，本地账户（username 或者 subs）的能否被多个终端共享。

- 可选配置，该配置仅在 EG 系列产品上支持，其他产品默认支持本地账户可被多个终端共享。
- 缺省情况下，本地账户不能被多个终端共享。

检验方法

- 使用 show aaa method-list 查看已配置的方法列表信息。
- 使用 show aaa lockout 查看用户尝试登录失败次数的最大值和用户锁定的时间长度的配置信息。
- 使用 show running-config 查看 Login 认证、dot1x 认证关联认证方法列表的信息。

相关命令

开启 AAA

【命令格式】 **aaa new-model**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该命令是 AAA 的使能命令，如果您要使用 AAA 安全服务，就必须使用 **aaa new-model** 使能 AAA 安全服务。
如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

定义 Login 认证的方法类型和执行顺序。

【命令格式】 **aaa authentication login** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 Login 认证的默认方法。
list-name：定义一个 Login 认证的方法列表，可以是任何字符串。
method：必须是“local、none、group、subs”所列关键字之一，一个方法列表最多有 4 个方法。
local：使用本地用户名数据库进行身份认证。
none：不进行身份认证。
group：使用服务器组进行身份认证，目前支持 RADIUS 和 TACACS+服务器组。
subs：**使用 subs 数据库进行身份认证。**

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA 登录认证安全服务，用户就必须使用 AAA 进行 Login 认证协商。您必须使用 **aaa authentication login** 命令配置默认的或可选的方法列表用于 Login 认证。
只有前面的方法没有响应，才能使用后面的方法进行身份认证。
设置了 Login 认证方法后，必须将其应用在需要进行 Login 认证的终端线路上，否则将不生效。

定义 Enable 认证的方法类型和执行顺序

【命令格式】 **aaa authentication enable default** *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 Enable 认证的默认方法。

list-name：定义一个 Enable 认证的方法列表，可以是任何字符串。

method：必须是“enable、local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

enable：使用 enable 命令配置的密码进行认证。

local：使用本地用户名数据库进行身份认证。

none：不进行身份认证。

group：使用服务器组进行身份认证，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA 登录认证安全服务，用户就必须使用 AAA 进行 Enable 认证协商。您必须使用 **aaa authentication enable** 命令配置默认的或可选的方法列表用于 Enable 认证。

只有前面的方法没有响应，才能使用后面的方法进行身份认证。

↘ 定义 802.1x 认证的方法类型和执行顺序。

【命令格式】 **aaa authentication dot1x** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 dot1x 认证的默认方法。

list-name：定义一个 dot1x 认证的方法列表，可以是任何字符串。

method：必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

local：使用本地用户名数据库进行身份认证。

none：不进行身份认证。

group：使用服务器组进行身份认证，目前支持 RADIUS 服务器组。

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA 802.1X 安全服务，用户就必须使用 AAA 进行 802.1X 用户认证协商。您必须使用 **aaa authentication dot1x** 命令配置默认的或可选的方法列表用于 802.1X 用户认证。

只有前面的方法没有响应，才能使用后面的方法进行认证。

↘ 定义 PPP、Web 认证、内置 Web 认证和 SSLVPN 认证的方法类型和执行顺序。

【命令格式】 **aaa authentication** { **ppp | web-auth** | **iportal** | **sslvpn** } { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **ppp：配置 PPP 拨号认证的方法列表。**

web-auth：配置 Web 认证的方法列表。

iportal：配置内置 Web 认证的方法列表。

sslvpn：配置 SSLVPN 认证的方法列表。

default：使用该参数，则后面定义的方法列表作为 PPP 认证的默认方法。

list-name：定义一个 PPP 认证的方法列表，可以是任何字符串。

method：必须是“local、none、group、subs”所列关键字之一，一个方法列表最多有 4 个方法。

local：使用本地用户名数据库进行身份认证。

none：不进行身份认证。

group：使用服务器组进行身份认证，目前支持 RADIUS 和 TACACS+服务器组。

subs：使用 sub 数据库进行身份认证。

【命令模式】 全局模式

【使用指导】 如果设备启用 AAA PPP 安全服务，用户就必须使用 AAA 进行 PPP 用户认证协商。您必须使用 **aaa**

authentication ppp 命令配置默认的或可选的方法列表用于 PPP 用户认证。

只有前面的方法没有响应，才能使用后面的方法进行认证。

设置 login 用户尝试登录次数的最大值。

【命令格式】 **aaa local authentication attempts** *max-attempts*

【参数说明】 *max-attempts*：最大尝试失败次数，取值范围 1~2147483647

【命令模式】 全局模式

【使用指导】 该命令配置 Login 登录用户尝试登录失败次数。

设置 login 用户被锁定的时间长度。

【命令格式】 **aaa local authentication lockout-time** *lockout-time*

【参数说明】 *lockout-time*：锁定时间（单位：分钟），取值范围 1~2147483647

【命令模式】 全局模式

【使用指导】 配置 Login 登录用户尝试超过配置登录失败次数后被锁定的时间长度。

设置 login 用户被锁定的时间长度。

【命令格式】 **aaa local user allow public account**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 Web 认证或者内置 Web 认证的情况下，本地账户（username 或者 subs）的能否被多个终端共享。

配置举例

以下配置举例，仅介绍与 AAA 认证相关的配置。

AAA Login 认证配置示例。对 Login 用户先用 RADIUS 服务器进行认证，在远程服务器没有响应的情况下转本地认证。

【网络环境】

图 2-5

【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器认证，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 认证，则需要在 NAS 上配置本地用户数据库信息。（本例需要配置 RADIUS 服务器和本地数据库信息）

第三步 :根据不同接入用户类型(本例为 Login 用户),配置 AAA 认证方法列表(本例的认证方法是先 RADIUS 认证，无响应后转 Local 认证）。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user password  pass
```

```
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key ruijie
Ruijie(config)#aaa authentication login list1 group radius local
Ruijie(config)#line vty 0 20
Ruijie(config-line)#login authentication list1
Ruijie(config-line)#exit
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication login list1 group radius local

Accounting method-list:

Authorization method-list:
```

以 Telnet 用户为例，用户远程登录到 NAS 设备上，CLI 界面提示输入用户名/密码。
输入正确的用户名/密码，才能访问设备。

User

```
User Access Verification

Username:user
Password:pass
```

↘ AAA enable 认证配置示例。对 enable 认证先使用 RADIUS 服务器进行认证，在远程服务器没有响应的情况下转本地认证，在本地认证用户名不存在的情况下转 enable 密码认证。

【网络环境】
图 2-6

【配置方法】 第一步：开启 AAA。
第二步：如果用户使用远程服务器认证，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 Local 认证，则需要在 NAS 上配置本地用户数据库信息。如果使用 enable 密码认证，则需要在 NAS 上配置 enable 认证密码。
第三步：根据不同接入用户类型，配置 AAA 认证方法列表。

> Enable 认证方法列表全局只能定义一个，因此 Enable 认证不需要定义方法列表的名称，只要配置成默认的方法列表，配置以后，会自动被应用。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user privilege 15 password  pass
```

```
Ruijie(config)#enable secret w
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key ruijie
Ruijie(config)#aaa authentication enable default group radius local enable
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication enable default group radius local enable

Accounting method-list:

Authorization method-list:
```

用户级别切换到 15 级，CLI 提示认证。输入正确的用户名/密码，才能访问设备。

NAS

```
Ruijie>enable
Username:user
Password:pass
Ruijie#
```

↘ AAA 802.1x 认证配置示例。对 802.1x 接入用户先用 RADIUS 服务器进行认证，在远程服务器没有响应的情况下转本地认证。

【网络环境】

图 2-7

【配置方法】 第一步：开启 AAA。

第二步 :如果用户使用远程服务器认证 ,则需要先配置 RADIUS 服务器。如果使用 Local 认证 ,则需要在 NAS 上配置本地用户数据库信息。（本例需要配置 RADIUS 服务器和本地数据库信息）。目前，802.1X 认证不支持使用 TACACS+认证。

第三步：根据不同接入用户类型（本例为 802.1x 接入用户），配置 AAA 认证方法列表（本例的认证方法是先 RADIUS 认证，无响应后转 Local 认证）。

第四步：应用 AAA 认证方法。如果使用的是 default 认证方法，则可不必配置该步骤。

第五步：接口开启 802.1x 认证功能。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user1 password  pass1
Ruijie(config)#username user2 password  pass2
Ruijie(config)#aaa new-model
```

```
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key ruijie
Ruijie(config)#aaa authentication dot1x default group radius local
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#dot1 port-control auto
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication dot1x default group radius local

Accounting method-list:

Authorization method-list:
```

常见错误

- 没有配置 RADIUS 服务器或者 TACACS+服务器。
- 没有配置本地数据库用户名和密码。

2.4.2 配置AAA授权

配置效果

- 定义用户可以使用哪些服务或拥有哪些权限。

注意事项

- 关于 Exec 授权：Exec 授权通常结合 Login 认证一起使用，并可以在同一个线路上同时使用 Login 认证和 Exec 授权。但是要注意，由于授权和认证可以采用不同的方法和不同的服务器，因此对于相同的用户，认证和授权可能有不同的结果。用户登录时，如果 Exec 授权失败，即使已经通过了 Login 认证，也不能进入到 CLI 界面。
- 关于授权方法：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。
- 关于 Command 授权：Command 授权功能目前仅 TACACS+协议支持。
- 关于 Console 授权：RGOS 支持区分通过控制台登录和其他终端登录的用户，可以设置控制台登录的用户，是否需要进行命令授权。如果关闭了控制台的命令授权功能，则已经应用到控制台线路的命令授权方法列表将不生效。

配置方法

开启 AAA

- 必须配置。
- 使用 **aaa new-model** 开启 AAA。
- 缺省情况下，没有启动 AAA。

定义 exec 授权的方法类型和执行顺序。

- 使用 **aaa authorization exec** 命令配置 exec 授权的方法类型和执行顺序。
- 如果要为 exec 用户配置授权方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置授权方法。

Exec 用户（控制台用户，可以通过 Console 口或者 Telnet 连接设备，每个连接称为一个 EXEC 用户，如 Telnet 用户、SSH 用户）的默认级别为最低权限的访问级别。

定义 command 授权的方法类型和执行顺序。

- 使用 **aaa authorization commands** 命令配置 command 授权的方法类型和执行顺序。
- 如果要为 command 授权配置授权方法列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置授权方法。

为接入用户配置授权方法列表。

- 使用 **aaa authorization network** 命令为接入用户配置认证方法列表。
- 如果要为 network 用户配置授权列表（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置授权方法。

在特定终端线路上应用 exec 授权方法。

- 使用 **authorization exec** (line 模式下)命令为特定终端线路上应用 exec 授权方法。
- 如果要在特定线路上应用指定的 exec 授权方法列表，则必须配置此命令。
- 缺省情况下，所有终端线路关联 default 授权方法列表。

在特定终端线路上应用 command 授权方法。

- 使用 **authorization commands** (line 模式下)命令为特定终端线路上应用 command 授权方法。
- 如果要在特定线路上应用指定的 command 授权方法列表，则必须配置此命令。
- 缺省情况下，所有终端线路关联 default 授权方法列表。

开启需要对配置模式下的命令进行授权。

- 使用 **aaa authorization config-commands** 命令开启需要对配置模式下的命令进行授权的功能。

- 缺省情况下，对配置模式下的命令不开启授权功能。

↘ 开启对控制台的用户执行的命令进行授权。

- 使用 **aaa authorization console** 命令开启对控制台的用户执行的命令进行授权的功能。
- 缺省情况下，不开启对控制台的用户执行的命令进行授权的功能。

检验方法

使用 **show running-config** 命令查看以上配置是否生效。

相关命令

↘ 开启 AAA。

【命令格式】 **aaa new-model**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该命令是 AAA 的使能命令，如果您要使用 AAA 安全服务，就必须使用 **aaa new-model** 使能 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

↘ 定义 exec 授权的方法类型和执行顺序。

【命令格式】 **aaa authorization exec** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 exec 授权的默认方法。

list-name：定义一个 exec 授权的方法列表，可以是任何字符串。

method：必须是“local、none、group”所列关键字之一，一个方法列表最多有 4 个方法。

local：使用本地用户名数据库进行 exec 授权。

none：不进行 exec 授权。

group：使用服务器组进行 exec 授权，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 支持对登录到 NAS 的 CLI 界面的用户进行授权，赋予其 CLI 权限级别（0~15 级）。目前是对于通过了 Login 认证的用户，才进行 Exec 授权。如果 Exec 授权失败，则无法进入 CLI 界面。

配置了 Exec 授权方法后，必须将其应用在需要进行 Exec 授权的终端线路上，否则将不生效。

↘ 定义 command 授权的方法类型和执行顺序。

【命令格式】 **aaa authorization commands** *level* { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 command 授权的默认方法。

list-name：定义一个 command 授权的方法列表，可以是任何字符串。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行 command 授权。

group：使用服务器组进行 command 授权，目前 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 支持对用户可执行的命令进行授权，当用户输入并试图执行某条命令时，AAA 将该命令发送到安全服务器上，如果安全服务器允许执行该命令，则该命令被执行，否则该命令不执行，并会给出执行命令被拒绝的提示。

配置命令授权的时候需要指定命令的级别，这个级别是命令的默认级别（例如，某命令对于 14 级以上用户可见，则该命令的默认级别就是 14 级的）。

配置了命令授权方法后，必须将其应用在需要进行命令授权的终端线路上，否则将不生效。

↘ 为接入用户配置授权方法列表。

【命令格式】 **aaa authorization network** { **default** | *list-name* } *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 network 授权的默认方法。

list-name：定义一个 network 授权的方法列表，可以是任何字符串。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行身份认证。

group：使用服务器组进行 network 授权，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 支持对所有网络有关的服务请求如 PPP、SLIP 等协议进行授权。如果配置了授权，则对所有的认证用户或接口自动进行授权。

可以指定三种不同的授权方法，与身份认证一样，只有当前的授权方法没有响应，才能继续使用后面的方法进行授权，如果当前授权方法失败，则不再使用其他后继的授权方法。

RADIUS 或 TACACS+服务器是通过返回一系列的属性对来完成对认证用户的授权。所以网络授权是建立在认证的基础上的，只有认证通过了才有可能获取网络授权。

↘ 开启对配置模式（包括全局配置模式及其子模式）下的命令进行授权的功能。

【命令格式】 **aaa authorization config-commands**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 如果只对非配置模式（如特权模式）下的命令进行授权，可以使用该命令的 **no** 模式关闭配置模式的授权功能，则配置模式及其子模式下的命令不需要进行命令授权就可以执行。

↘ 开启对通过控制台登录的用户所执行的命令进行授权的功能。

【命令格式】 **aaa authorization console**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 RGOS 支持区分通过控制台登录和其他终端登录的用户，可以设置控制台登录的用户，是否需要进行命令授权。如果关闭了控制台的命令授权功能，则已经应用到控制台线路的命令授权方法列表将不生效。

配置举例

以下配置举例，仅介绍与 AAA 授权相关的配置。

↘ 配置 AAA exec 授权。VTY 线路 0~4 上的用户登录时采用 Login 认证，并且进行 exec 授权。其中 Login 认证采用本地认证，exec 授权先采用 RADIUS，如果没有响应可以采用本地授权。

【网络环境】

图 2-8

【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 local 授权，则需要在 NAS 上配置本地用户数据库信息。

第三步：根据不同接入方式和服务类型，配置 AAA 授权方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

Exec 授权通常结合 Login 认证一起使用，并可以在同一个线路上同时使用 Login 认证和 Exec 授权。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user password  pass
Ruijie(config)#username user privilege 6
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key  test
Ruijie(config)#aaa authentication login list1 group local
Ruijie(config)#aaa authorization exec list2 group radius local
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication list1
Ruijie(config-line)# authorization exec list2
Ruijie(config-line)#exit
```

【检验方法】 在 NAS 设备上，通过 **show run、show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication login list1 group local

Accounting method-list:

Authorization method-list:
aaa authorization exec list2 group radius local
```

```
Ruijie# show running-config
aaa new-model
!
aaa authorization exec list2 group local
aaa authentication login list1 group radius local
```

```
!
username user password  pass
username user privilege 6
!
radius-server host 10.1.1.1
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 authorization exec list2
 login authentication list1
!
End
```

↘ 配置 Command 授权。为 Login 用户设置命令授权，应用 default 授权方法：对 15 级命令进行授权，先使用 tacacs+ 服务器授权，无响应后转 local 授权。授权同时应用于控制台登录用户和其他终端登录的用户。

【网络环境】

图 2-9

【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 local 授权，则需要在 NAS 上配置本地用户数据库信息。

第三步：根据不同接入方式和服务类型，配置 AAA 授权方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user1 password pass1
Ruijie(config)#username user1 privilege 15
Ruijie(config)#aaa new-model
Ruijie(config)#tacacs-server host 192.168.217.10
Ruijie(config)#tacacs-server key aaa
Ruijie(config)#aaa authentication login default local
Ruijie(config)#aaa authorization commands 15 default group tacacs+ local
Ruijie(config)#aaa authorization console
```

【检验方法】 在 NAS 设备上，通过 **show run、show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication login default local
```

```
Accounting method-list:

Authorization method-list:
aaa authorization commands 15 default group tacacs+ local
```

```
Ruijie#show run
!
aaa new-model
!
aaa authorization console
aaa authorization commands 15 default group tacacs+ local
aaa authentication login default local
!
!
nfpp
!
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

配置 Network 授权。

【网络环境】

图 2-10

【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器授权，则需要先配置 RADIUS 或 TACACS+服务器。如果使用 local 授权，则需要在 NAS 上配置本地用户数据库信息。

第三步：根据不同接入方式和服务类型，配置 AAA 授权方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Ruijie#configure terminal
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key  test
Ruijie(config)#aaa authorization network default group radius none
Ruijie(config)# end
```

【检验方法】 在 NAS 设备上，通过 **show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:

Accounting method-list:

Authorization method-list:
aaa authorization network default group radius none
```

常见配置错误

无

2.4.3 配置AAA记账

配置效果

- 记录用户使用网络资源的情况。
- 记录用户进行设备管理时登入登出的过程、记录执行过的命令。

注意事项

关于记账方法：

- 如果在一个记账方案中使用多种记账模式，则记账模式的执行顺序为配置的先后顺序。只有在当前记账模式没有响应的情况下，才会采用下一种记账模式；如果当前记账模式失败，则不会采用下一种记账模式进行记账。
- 默认的记账方法（default 方法）列表一旦配置，将自动应用到所有终端上。在线路上应用非默认记账方法列表，将取代默认的方法列表。如果试图应用未定义的方法列表，则会给出一个警告提示信息，该线路上的记账将不会生效，直至定义了该记账方法列表才会生效。

关于 Exec 记账：

- 只有登录到 NAS 的用户终端通过了 Login 认证，才会进行 exec 记账。如果没有设置 Login 认证，或者认证时候采用了 none 方法，则不会进行 exec 记账。针对同一个用户终端的登录，登入时如果没有进行过 Start 记账，登出时也就不会进行 Stop 记账。

关于 Command 记账：

- Command 记账功能目前仅 TACACS+协议支持。

配置方法

开启 AAA。

- 必须配置。
- 使用 **aaa new-model** 开启 AAA。
- 缺省情况下，没有启动 AAA。

定义 exec 记账的方法类型及方法执行顺序。

- 使用命令 **aaa accounting exec** 配置 exec 记账的方法类型及方法执行顺序。
- 如果要为 exec 用户配置记账方法（包括配置 default 方法列表），则必须配置此命令。
- Exec 用户（控制台用户，可以通过 Console 口或者 Telnet 连接设备，每个连接称为一个 EXEC 用户，如 Telnet 用户、SSH 用户）的默认级别为最低权限的访问级别。
- 缺省情况下，没有配置记账方法。

定义 command 记账的方法类型及方法执行顺序。

- 使用命令 **aaa accounting commands** 配置 command 记账的方法类型及方法执行顺序。
- 如果要为 command 记账配置记账方法（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置记账方法。命令记账功能目前仅 TACACS+协议支持。

定义 network 记账的方法类型及方法执行顺序。

- 使用命令 **aaa accounting network** 配置 network 记账的方法类型及方法执行顺序。
- 如果要为 network 用户配置记账方法（包括配置 default 方法列表），则必须配置此命令。
- 缺省情况下，没有配置记账方法。

在特定终端线路上应用 exec 记账方法。

- 使用命令 **accounting exec**(line 模式下)配置在特定终端线路上应用 exec 记账方法。
- 如果要在特定线路上应用指定的 exec 记账方法列表，则必须配置此命令。
- 如果应用的是 default 方法列表，则可不必配置此命令。
- 缺省情况下，所有终端线路关联 default 方法列表。

在特定终端线路上应用 command 记账方法。

- 使用命令 **accounting commands**(line 模式下)配置在特定终端线路上应用 command 记账方法。
- 如果要在特定线路上应用指定的 command 记账方法列表，则必须配置此命令。
- 如果应用的是 default 方法列表，则可不必配置此命令。
- 缺省情况下，所有终端线路关联 default 方法列表。

802.1x 应用 network 记账方法

- 使用命令 **dot1x accounting network** 命令配置 802.1x 的 network 记账方法。
- 如果要指定 802.1X 记账方法，则必须配置此命令。
- 如果应用的是 default 方法列表，则可不必配置此命令。
- 缺省情况下，关联 default 方法列表。

开启记账更新功能。

- 可选配置。
- 该功能有助于提高记账准确性，建议配置。
- 缺省情况下，记账更新功能关闭。

设置记账更新时间间隔。

- 可选配置。
- 除非有明确要求，否则不建议配置。

检验方法

使用 **show running-config** 命令查看配置是否生效。

相关命令

开启 AAA。

【命令格式】 **aaa new-model**
【参数说明】 无
【命令模式】 全局模式
【使用指导】 该命令是 AAA 的使能命令，如果您要使用 AAA 安全服务，就必须使用 **aaa new-model** 使能 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

定义 exec 记账的方法类型及方法执行顺序。

【命令格式】 **aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 exec 记账的默认方法。
list-name：定义一个 exec 记账的方法列表，可以是任何字符串。
method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行 exec 记账。

group：使用服务器组进行 exec 记账，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 只有在用户通过了登录认证后，才会启用 Exec 记账功能，如果用户登录时未进行认证或认证采用的方法为 none，则不会进行 Exec 记账。

启用记账功能后，在用户登录到 NAS 的 CLI 界面时候，发送记账开始（Start）信息给安全服务器，在用户退出登录的时候，发送记账结束（Stop）信息给安全服务器。如果一个用户在登录时没有发出 Start 信息，在退出登录时也不会发出 Stop 信息。

配置了 Exec 记账方法后，必须将其应用在需要进行命令记账的终端线路上，否则将不生效。

定义 command 记账的方法类型及方法执行顺序。

【命令格式】 **aaa accounting commands** *level* { **default** | *list-name* } **start-stop** *method1* [*method2*...]

【参数说明】 *level*：要进行记账的命令级别，范围 0~15，决定哪个级别的命令执行时，需要记录信息。

default：使用该参数，则后面定义的方法列表作为 command 记账的默认方法。

list-name：定义一个 command 记账的方法列表，可以是任何字符串。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行 command 记账。

group：使用服务器组进行 command 记账，目前支持 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 只有在用户通过了登录认证后，才会启用命令记账功能，如果用户登录时未进行认证或认证采用的方法为 none，则不会进行命令记账。启用记账功能后，在用户每次执行指定级别的命令后，将所执行的命令信息，发送给安全服务器。

配置了命令记账方法后，必须将其应用在需要进行命令记账的终端线路上，否则将不生效。

定义 network 记账的方法类型及方法执行顺序。

【命令格式】 **aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]

【参数说明】 **default**：使用该参数，则后面定义的方法列表作为 network 记账的默认方法。

list-name：定义一个 command 记账的方法列表，可以是任何字符串。

start-stop：在用户访问活动开始和结束时均发送记账报文，开始记账报文无论是否成功启用记账，都允许用户开始进行网络访问。

method：必须是“none、group”所列关键字之一，一个方法列表最多有 4 个方法。

none：不进行 network 记账。

group：使用服务器组进行 network 记账，目前支持 RADIUS 和 TACACS+服务器组。

【命令模式】 全局模式

【使用指导】 RGOS 通过给安全服务器发送记录属性对来用户活动进行记账。使用关键字 **start-stop**，制定用户记账选项。

开启记账更新功能。

【命令格式】 **aaa accounting update**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 如果没有启用 AAA 安全服务，则不能使用记账更新。如果已经启用 AAA 安全服务，则该命令用设置记账更新

功能。

设置记账更新时间间隔。

【命令格式】 **aaa accounting update periodic** *interval*

【参数说明】 *Interval* ：记账更新间隔，以分钟为单位，最小为 1 分钟。

【命令模式】 全局模式

【使用指导】 如果没有启用 AAA 安全服务，则不能使用记账更新。如果已经启用 AAA 安全服务，则该命令用设置记账更新间隔。

配置举例

以下配置举例，仅介绍与 AAA 记账相关的配置。

配置 AAA exec 记账。VTY 线路 0~4 上的用户登录时采用 Login 认证，并且进行 exec 记账。其中 Login 认证采用本地认证，exec 记账采用 RADIUS 记账。

【网络环境】

图 2-11

【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器记账，则需要先配置 RADIUS 或 TACACS+服务器。

第三步：根据不同接入方式和服务类型，配置 AAA 记账方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user password  pass
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key  test
Ruijie(config)#aaa authentication login list1 group local
Ruijie(config)#aaa accounting exec list3 start-stop group radius
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication list1
Ruijie(config-line)# accounting  exec list3
Ruijie(config-line)#exit
```

【检验方法】 在 NAS 设备上，通过 **show run**、**show aaa method-list** 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication login list1 group local
```

```
Accounting method-list:
aaa accounting exec list3 start-stop group radius
Authorization method-list:
Ruijie# show running-config
aaa new-model
!
aaa accounting exec list3 start-stop group radius
aaa authentication login list1 group local
!
username user password  pass
!
radius-server host 10.1.1.1
radius-server key 7 093b100133
!
line con 0
line vty 0 4
 accounting  exec list3
 login authentication list1
!
End
```

↘ 配置 command 记账。为 Login 用户设置命令记账 ,应用 default 记账方法。其中 Login 认证采用本地认证 ,使用 tacacs+ 服务器记账。

【网络环境】

图 2-12

【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器记账，则需要先配置 RADIUS 或 TACACS+服务器。

第三步：根据不同接入方式和服务类型，配置 AAA 记账方法列表。

第四步：将方法应用于某个特定的接口或线路。如果使用的是 default 认证方法，则可以不必配置该步骤。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user1 password pass1
Ruijie(config)#username user1 privilege 15
Ruijie(config)#aaa new-model
Ruijie(config)#tacacs-server host 192.168.217.10
Ruijie(config)#tacacs-server key aaa
Ruijie(config)#aaa authentication login default local
```

```
Ruijie(config)#aaa accounting commands 15 default start-stop group tacacs+
```

【检验方法】 在 NAS 设备上，通过 show 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication login default local

Accounting method-list:
aaa accounting commands 15 default start-stop group tacacs+
Authorization method-list:
```

```
Ruijie#show run
!
aaa new-model
!
aaa authorization config-commands
aaa accounting commands 15 default start-stop group tacacs+
aaa authentication login default local
!
!
nfpp
!
vlan 1
!
username user1 password 0 pass1
username user1 privilege 15
no service password-encryption
!
tacacs-server host 192.168.217.10
tacacs-server key aaa
!
line con 0
line vty 0 4
!
!
end
```

↘ 配置 network 记账。为 802.1x 用户配置记账方法列表，采用 RADIUS 远程服务器认证和记账。

【网络环境】

图 2-13

【配置方法】 第一步：开启 AAA。

第二步：如果用户使用远程服务器记账，则需要先配置 RADIUS 服务器。

第三步：根据不同接入方式和服务类型，配置 AAA 方法列表。

第四步：应用方法列表。如果使用的是 default 认证方法，则可以不必配置该步骤。

802.1X 用户在认证通过后才能进行记账。

NAS

```
Ruijie#configure terminal
Ruijie(config)#username user password  pass
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key test
Ruijie(config)#aaa authentication dot1x aut1x group radius local
Ruijie(config)#aaa accounting network acc1x start-stop group radius
Ruijie(config)#dot1x authentication aut1x
Ruijie(config)#dot1x accounting acc1x
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#dot1 port-control auto
Ruijie(config-if-GigabitEthernet 0/1)#exit
```

【检验方法】 在 NAS 设备上，通过 show 命令查看配置效果。

NAS

```
Ruijie#show aaa method-list

Authentication method-list:
aaa authentication dot1x aut1x group radius local
Accounting method-list:
aaa accounting network acc1x start-stop group radius
Authorization method-list:
```

常见配置错误

无

2.4.4 配置AAA服务器组

配置效果

- 创建自定义服务器组，每个服务器组可添加一台或多台服务器。
- 配置认证、授权、记账方法列表时，引用服务器组的组名作为认证、授权、记账方法，则表示在进行认证、授权、记账请求时使用该服务器组中的服务器。
- 使用自定义服务器组可以实现认证、授权、记账相分离。

注意事项

在自定义服务器组中，只能指定并应用默认服务器组中的服务器。

配置方法

↘ 创建 AAA 自定义服务器组。

- 必选配置
- 在创建自定义服务组名的时候，组名尽可能有明确的含义。不可以使用预定义的关键字”radius”和“tacacs+”。

↘ 添加 AAA 服务器组成员。

- 必选配置
- 使用 sever 命令添加 AAA 服务器组的成员。
- 缺省情况下，自定义组中没有添加服务器。

↘ 配置服务器组的 VRF 属性。

- 可选配置
- 使用 **ip vrf forwarding** 命令配置服务器组的 VRF 属性。
- 缺省情况下，服务器组属于全局 VRF。

检验方法

使用命令 **show aaa group** 查看配置的服务器组信息。

相关命令

↘ 创建 AAA 自定义服务器组。

【命令格式】 **aaa group server** {**radius** | **tacacs+**} *name*

【参数说明】 *name*：服务器组的取名，目前不能为关键字“radius”，“tacacs+”，因为这是 RADIUS 和 TACACS+默认的服务器组名称。

【命令模式】 全局模式

【使用指导】 该命令配置 AAA 服务器组， 目前支持 RADIUS 和 TACACS+服务器组。

添加 AAA 服务器组成员。

【命令格式】 **server** *ip-addr* [**auth-port** *port1*] [**acct-port** *port2*]

【参数说明】 *ip-addr*：服务器 ip 地址

port1：服务器认证端口（仅 RADIUS 服务器组支持）

port2：服务器记账端口（仅 RADIUS 服务器组支持）

【命令模式】 服务器组配置模式

【使用指导】 往指定服务器中添加服务器，不指定端口时使用默认值。

配置服务器组的 VRF 属性。

【命令格式】 **ip vrf forwarding** *vrf_name*

【参数说明】 *vrf_name*：vrf 名字

【命令模式】 服务器组配置模式

【使用指导】 为指定服务器组选择 vrf

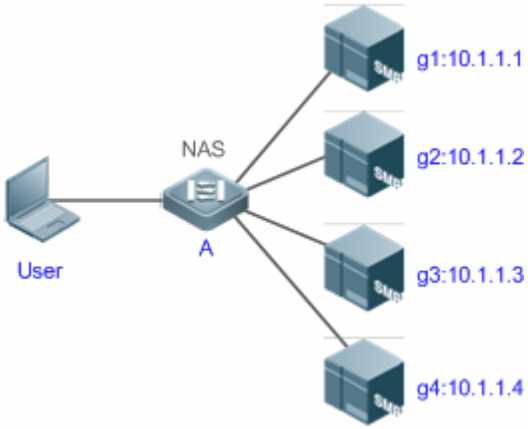
配置举例

以下配置举例，仅介绍与 AAA 服务器组相关的配置。

创建 AAA 自定义服务器组。RADIUS 服务器组 g1、g2，其中 g1 组的服务器的 IP 为 10.1.1.1 和 10.1.1.2，g2 组的服务器的 IP 为 10.1.1.3 和 10.1.1.4。

【网络环境】

图 2-14



【前置任务】 1，网络中已经完成了接口、IP 地址、Vlan 的配置，网络连通，NAS 设备到服务器的路由可达。

2，启用 AAA 服务。

【配置方法】 第一步：配置服务器（该服务器属于默认服务器组）

第二步：创建 AAA 自定义服务器组

第三步：在自定义服务器组中添加服务器组成员

NAS

```
Ruijie#configure terminal
```

```
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server host 10.1.1.2
Ruijie(config)#radius-server host 10.1.1.3
Ruijie(config)#radius-server host 10.1.1.4
Ruijie(config)#radius-server key secret
Ruijie(config)#aaa group server radius g1
Ruijie(config-gs-radius)#server 10.1.1.1
Ruijie(config-gs-radius)#server 10.1.1.2
Ruijie(config-gs-radius)#exit
Ruijie(config)#aaa group server radius g2
Ruijie(config-gs-radius)#server 10.1.1.3
Ruijie(config-gs-radius)#server 10.1.1.4
Ruijie(config-gs-radius)#exit
```

【检验方法】 在 NAS 设备上，通过 **show aaa group、show run** 命令查看配置效果。

NAS

```
Ruijie#show aaa group
Type        Reference  Name
----------  ---------- ----------
radius      1          radius
tacacs+     1          tacacs+
radius      1          g1
radius      1          g2
```

```
Ruijie#show run
!
radius-server host 10.1.1.1
radius-server host 10.1.1.2
radius-server host 10.1.1.3
radius-server host 10.1.1.4
radius-server key secret
!
aaa group server radius g1
 server 10.1.1.1
 server 10.1.1.2
!
aaa group server radius g2
 server 10.1.1.3
 server 10.1.1.4
!
!
```

常见配置错误

- 对于使用非默认认证、记账端口的 radius 服务器，在使用命令 server 添加服务器时要同时指定认证端口或记账端口。
- 目前，只有 RADIUS 类型的服务器组可以配置 VRF 属性。

2.4.5 配置基于域名的AAA服务

配置效果

针对不同域的 802.1x 用户，创建认证、授权和记账方案。

注意事项

关于域中引用方法列表：

- 在域配置模式下，选择 AAA 服务方法列表时，这些方法列表是在进入域配置模式前已经定义；否则在域配置模式下，允许选择 AAA 方法列表名，但提示配置不存在。
- 域选择的AAA服务方法列表名称必须和AAA服务所定义的方法列表名称必须一致。若不一致，不能够为该域中的用户提供合适的 AAA 服务。

关于缺省域：

- 缺省域（default）：在基于域名的 AAA 服务开关打开情况下，如果用户没有携带域信息，则使用缺省域。如果用户携带的域在系统中没有配置，则判定为非法用户，不提供 AAA 服务。初始时没有配置 default 域，需要手工指定创建。
- 基于域名的 AAA 服务开关打开时，默认情况下没有配置缺省域，需要手动配置完成。缺省域的名称为“default”，若配置缺省域后，用户不携带域信息时，使用缺省域进行提供 AAA 服务。若缺省域没有配置，则未携带域信息的用户不能使用 AAA 服务。

关于域名：

- 用户所携带的域名称与设备上所配置的域名的匹配采用最准确匹配。例如：设备上配置了 domain.com 和 domain.com.cn 两个域，一个用户的请求信息携带为 aaa@domain.com。则设备认为会判定该用户所属于的域为 domain.com 而不是域 domain.com.cn。
- 如果认证用户携带有域信息，而域没有在设备上配置，不能为该用户提供 AAA 服务。

配置方法

↘ 开启 AAA。

- 必须配置。
- 使用 **aaa new-model** 开启 AAA。
- 缺省情况下，没有启动 AAA。

↘ 开启基于域名的 AAA 服务。

- 必选配置。
- 使用 **aaa domain enable** 开启基于域名的 AAA 服务。
- 缺省情况下，基于域名的 AAA 服务关闭。

↘ 创建域，并进入域配置模式。

- 必选配置。
- 使用 **aaa domain** 命令创建域或者进入已配置的域。
- 缺省情况下，没有配置任何域。

↘ 在域中，关联 802.1X 认证方法列表。

- 使用 **authentication dot1x** 命令关联 802.1x 认证方法列表。
- 如果要在域中应用指定的 801.1x 认证方法，则必须配置此命令。
- 目前基于域名的 AAA 服务，仅被应用于 802.1x 接入服务。

↘ 在域中，关联 Network 记账方法列表。

- 使用 **accounting network** 命令关联 network 记账方法列表。
- 如果要在域中应用指定的记账方法，则必须配置此命令。
- 如果域中没有关联方法列表，则默认使用全局的 default 方法列表进行记账。

↘ 在域中，关联 Network 授权方法列表。

- 使用 **authorization network** 命令关联 network 授权方法列表。
- 如果要在域中应用指定的授权方法，则必须配置此命令。
- 如果域中没有关联方法列表，则默认使用全局的 default 方法列表进行授权。

↘ 设置域的状态。

- 可选配置
- 当域的状态为 block 时，属于该域的用户不能登录。
- 缺省情况下，当域被创建以后，其状态为 active，即允许任何属于该域的用户请求网络服务。

↘ 设置是否在用户名中携带域名信息。

- 可选配置
- 缺省情况下，NAS 与服务器交互时用户名中携带域信息。

↘ 设置当前域可容纳接入用户的数目限制。

- 可选配置
- 缺省情况下，不对当前域可容纳的接入用户数作限制。

检验方法

使用命令 **show aaa domain** 查看配置的域信息是否生效。

相关命令

开启 AAA。

【命令格式】 **aaa new-model**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 该命令是 AAA 的使能命令，如果您要使用 AAA 安全服务，就必须使用 **aaa new-model** 使能 AAA 安全服务。如果没有启用 AAA，则所有 AAA 命令将是不可配置的。

开启基于域名的 AAA 服务。

【命令格式】 **aaa domain enable**

【参数说明】 无

【命令模式】 全局模式

【使用指导】 进行基于域名的 AAA 服务配置，需要打开这个配置开关。

创建域，并进入域配置模式。

【命令格式】 **aaa domain** { **default** | *domain-name* }

【参数说明】 **default**：使用该参数，进行缺省域的配置

domain-name：指定域的名称

【命令模式】 全局模式

【使用指导】 指定基于域名的 AAA 服务配置。default 为缺省域配置，也就是如果用户没有携带域信息，网络设备所使用的方法列表。*domain-name* 为指定域名配置，如果用户携带该域名，则指定使用这个域所关联的方法列表。目前系统支持最多配置 32 个域。

在域中，关联 802.1X 认证方法列表。

【命令格式】 **authentication dot1x** { **default** | *list-name* }

【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表

list-name：指定方法列表名称

【命令模式】 域配置模式

【使用指导】 为域指定一个 802.1x 认证方法列表。

在域中，关联 Network 记账方法列表。

【命令格式】 **accounting network** { **default | *list-name* }

【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表

list-name：指定方法列表名称

【命令模式】 域配置模式

【使用指导】 为域指定使用的 Network 记账方法列表。

在域中，关联 Network 授权方法列表。

【命令格式】 **authorization network** { **default** | *list-name* }

【参数说明】 **default**：使用该参数，指定使用缺省配置方法列表

list-name：指定方法列表名称

【命令模式】 域配置模式

【使用指导】

设置域的状态。

【命令格式】 **state** { **block** | **active** }

【参数说明】 **block**：配置的域无效

active：配置的域有效

【命令模式】 域配置模式

【使用指导】 指定配置的域是否有效。

设置是否在用户名中携带域名信息。

【命令格式】 **username-format** { **without-domain** | **with-domain** }

【参数说明】 **without-domain**：剥离域信息

with-domain：不剥离域信息

【命令模式】 域配置模式

【使用指导】 在域配置模式下，配置 NAS 针对指定域与服务器交互时，用户名中是否携带域信息。

设置当前域可容纳接入用户的数目。

【命令格式】 **access-limit** *num*

【参数说明】 *num*：域用户的数量限制，只限制 802.1x 用户

【命令模式】 域配置模式

【使用指导】 使用该命令对域的用户数量进行限制。

配置举例

以下配置举例，仅介绍与多域 AAA 相关的配置。

配置基于域的 AAA 认证记账服务。实现使用 RADIUS 服务器对通过 NAS 接入的 802.1X 域用户（用户名为 user@domain.com）进行认证和记账。NAS 向服务器发送的用户名不携带域名，不限制接入用户数。

【网络环境】

图 2-15

【配置方法】 本例使用 RADIUS 认证和记账，需要提前配置 RADIUS 服务器。

第一步：开启 AAA
第二步：定义 AAA 服务的方法列表
第三步：开启基于域名的 AAA 服务
第四步：创建域
第五步：在指定域中关联 AAA 方法列表
第六步：设置域属性

NAS

```
Ruijie#configure terminal
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 10.1.1.1
Ruijie(config)#radius-server key  test
Ruijie(config)#aaa authentication dot1x default group radius
Ruijie(config)#aaa accounting network list3 start-stop group radius
Ruijie(config)# aaa domain enable
Ruijie(config)# aaa domain domain.com
Ruijie(config-aaa-domain)# authentication dot1x default
Ruijie(config-aaa-domain)# accounting  network list3
Ruijie(config-aaa-domain)# username-format without-domain
```

【检验方法】 在 NAS 设备上，通过 **show run**、**show aaa domain** 命令查看配置效果。

NAS

```
Ruijie#show aaa domain domain.com

=============Domain domain.com=============
State: Active
Username format: With-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x default
 accounting network list3
```

```
Ruijie#show run

Building configuration...
Current configuration : 1449 bytes
version RGOS 10.4(3) Release(101069)(Wed Oct 20 09:12:40 CST 2010 -ngcf67)
co-operate enable
!
aaa new-model
aaa domain enable
!
aaa domain domain.com
```

```
 authentication dot1x default
 accounting network list3
!
aaa accounting network list3 start-stop group radius
aaa authentication dot1x default group radius
!
nfpp
!
no service password-encryption
!
radius-server host 10.1.1.1
radius-server key test
!
line con 0
line vty 0 4
!
end
```

常见配置错误

无

2.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除被锁定的用户列表。	**clear aaa local user lockout** {**all** | **user-name** *username* }

查看运行情况

作用	命令
显示记账更新相关的信息。	**show aaa accounting update**
显示当前所有配置域信息。	**show aaa domain**
显示当前 login 的锁定配置参数。	**show aaa lockout**
显示 AAA 配置的所有服务器组。	**show aaa group**
显示 AAA 所有的方法列表。	**show aaa method-lis**
显示 AAA 用户相关信息。	**show aaa user**

查看调试信息

无

3 RADIUS

3.1 概述

RADIUS (Remote Authentication Dial-In User Service，远程认证拨号用户服务)是一种分布式的客户机/服务器系统。

RADIUS 与 AAA 配合对试图连接的用户进行身份认证，防止未经授权的访问。在 RGOS 的实现中，RADIUS 客户端运行在设备或网络访问服务器(NAS)上，并向中央 RADIUS 服务器发出身份认证请求，中央服务器包含了所有的用户身份认证和网络服务信息。除了提供认证服务之外，RADIUS 服务器还提供接入用户的授权和记账的服务。

RADIUS 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。由于 RADIUS 是一种完全开放的协议，很多系统如 UNIX、WINDOWS 2000、WINDOWS 2008 等均将 RADIUS 服务器作为一个组件安装，因此 RADIUS 是目前应用最广泛的安全服务器。

RADIUS 动态授权扩展协议（Dynamic Authorization Extensions to Remote Authentication Dial In User Service），在 IETF 的 RFC3576 中进行定义。该协议定义了一种针对用户下线管理方法。设备和 RADIUS 服务器之间通过 Disconnect-Messages（简称 DM)消息，将已认证通过的用户下线。该协议使得不同厂商间的设备和 RADIUS 服务器，在用户下线的处理上能够兼容。

DM 消息机制，由 RADIUS 服务器主动向设备发起用户下线请求，设备依据请求报文中携带的用户会话、用户名等信息来匹配用户并对其进行下线处理，然后将处理结果以回应报文形式返回给 RADIUS 服务器，以实现服务器对用户的下线管理功能。

协议规范

- RFC2865：Remote Authentication Dial In User Service (RADIUS)
- RFC2866：RADIUS Accounting
- RFC2867：RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC2868：RADIUS Attributes for Tunnel Protocol Support
- RFC2869：RADIUS Extensions
- RFC3576：Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

3.2 典型应用

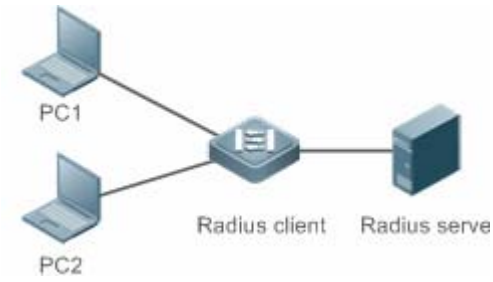
典型应用	场景描述
为接入用户提供认证、授权、记账服务	对网络中的接入用户进行认证、授权、记账，以防止未经授权的访问或操作。
已上线用户被服务器强制下线	对于已经认证的用户，服务器强制其下线

3.2.1 为接入用户提供认证、授权、记账服务

应用场景

RADIUS 的典型应用为对接入用户进行认证、授权、记账。网络设备作为 RADIUS 客户端，将用户信息发送给 RADIUS 服务器。RADIUS 服务器处理完成，给 RADIUS 客户端返回认证接受/认证拒绝/记账响应等信息。RADIUS 客户端根据 RADIUS 服务器的响应信息对接入用户进行相应处理。

图 3-1 典型的 RADIUS 网络配置



【注释】 PC1 和 PC2 作为接入用户通过有线或者无线方式和 RADIUS 客户端连接，并发起认证、记账请求。
Radius Client 通常为接入交换机或者汇聚交换机。
Radius Server 可以是 Windows 2000/2003 Server（IAS）、UNIX 系统所带组件，也可以是一些厂商提供的专用服务器软件。

功能部署

- 在 Radius Server 配置接入设备信息，包括接入设备 IP，共享密钥等。
- 在 Radius Client 配置 AAA 的认证、授权、记账方法列表。
- 在 Radius Client 配置 Radius server 信息，包括 IP，共享密钥等。
- 在 Radius Client 配置接入端口开启访问控制。
- 配置网络，使 Radius Client 和 Radius Server 之间通讯正常。

3.2.2 用户强制下线

应用场景

出于管理需要，RADIUS 服务器对于已经认证上线的用户，采取强制下线的措施。

网络配置请参考图 1-1

功能部署

在 1.2.1 的功能部署基础上加上以下部署：

- 在 Radius Client 使能 RADIUS 动态授权扩展功能

3.3 功能详解

基本概念

客户端/服务器模式

- 客户端：RADIUS 客户端作为 RADIUS 请求的发起端，通常运行在设备或者网络访问服务器(NAS)上，负责把用户信息发送给 RADIUS 服务器，并接受 RADIUS 服务器的返回信息，进行相应的处理。处理包括接受用户接入或者拒绝用户接入或者收集更多用户信息提供给服务器进行处理。
- 服务器：RADIUS 客户端和 RADIUS 服务器通常是多对一的关系。RADIUS 服务器维护所有的 RADIUS 客户端的 IP 和共享密钥信息，以及所有认证用户的信息。RADIUS 服务器接收 RADIUS 客户端的请求信息，并进行认证、授权、记账处理，然后返回客户端需要的认证、授权、记账信息。

RADIUS 报文结构

RADIUS 的报文结构如下图所示：

8	16	32bit
Code	Identifier	Length
Authenticator(16bytes)		
Attributes		

- Code — Code 域长度为一个字节，用于标识 RADIUS 报文的类型，取值及含义参考下表。

Code	报文类型	Code	报文类型
1	Access-Request 认证请求报文	4	Accounting-Request 记账请求报文
2	Access-Accept 认证接受报文	5	Accounting-Response 记账相应报文
3	Access-Reject 认证拒绝报文	11	Access-Challenge 认证质询报文

- Identifier — Identifier 域占用 1 个字节，用于匹配请求和响应报文。同一类型的请求报文和响应报文的 Identifier 值相同。
- Length — Length 域占用 2 个字节，标识整个 RADIUS 报文的长度，包括 Code、Identifier、Length、Authenticator、Attributes 在内。超过 Length 域的字节将被忽略。如果接收到的报文的实际长度小于 Length 的值，则丢弃该报文。
- Authenticator — Authenticator 域占用 16 个字节。RADIUS 客户端使用该域来验证服务器的回应报文。Authenticator 域也用于用户密码的加密/解密。

- Attributes — Attributes 域的长度是不定的，用于携带认证、授权、记账信息。Attributes 域通常包含多个属性。每个属性采用 TLV(Type、Length、Value)三元组的结构表示。其中，Type 为 1 个字节，表示属性的类型，下表列出了 RADIUS 认证、授权、记账常用的属性；Length 为 1 个字节，表示该属性的长度，单位为字节；Value 为该属性的信息。

属性号	属性名	属性号	属性名
1	User-Name	43	Acct-Output-Octets
2	User-Password	44	Acct-Session-Id
3	CHAP-Password	45	Acct-Authentic
4	NAS-IP-Address	46	Acct-Session-Time
5	NAS-Port	47	Acct-Input-Packets
6	Service-Type	48	Acct-Output-Packets
7	Framed-Protocol	49	Acct-Terminate-Cause
8	Framed-IP-Address	50	Acct-Multi-Session-Id
9	Framed-IP-Netmask	51	Acct-Link-Count
10	Framed-Routing	52	Acct-Input-Gigawords
11	Filter-ID	53	Acct-Output-Gigawords
12	Framed-MTU	55	Event-Timestamp
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
18	Reply-Message	64	Tunnel-Type
19	Callback-Number	65	Tunnel-Medium-Type
20	Callback-ID	66	Tunnel-Client-Endpoint
22	Framed-Route	67	Tunnel-Server-Endpoint
23	Framed-IPX-Network	68	Acct-Tunnel-Connection
24	State	69	Tunnel-Password
25	Class	70	ARAP-Password
26	Vendor-Specific	71	ARAP-Features
27	Session-Timeout	72	ARAP-Zone-Access
28	Idle-Timeout	73	ARAP-Security
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference

39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

共享密钥

RADIUS 客户端和 RADIUS 服务器进行通讯，相互之间通过共享密钥来确定对方的身份。共享密钥不能通过网络传输。此外，在传输过程中，为保证安全性，用户密码都是加密的。

RADIUS 服务器组

RADIUS 安全协议，也称 RADIUS 方法，是以 RADIUS 服务器组为单位进行配置的。每一个 RADIUS 方法对应一个 RADIUS 服务器组，每一个 RADIUS 服务器组可配置一至多台 RADIUS 服务器(关于使用 RADIUS 方法的细节信息，请参见“AAA 配置”章节)。如果您在一个 RADIUS 服务器组中配置了多台 RADIUS 服务器，那么当设备同第一台 RADIUS 服务器通讯失败，或者第一台 RADIUS 服务器变成不可达的状态时，设备将自动尝试同第二台 RADIUS 服务器通讯，以此类推，直到成功或者全部失败为止。

RADIUS 属性类型

- 标准属性

RFC 相关标准规定了 RADIUS 的属性号和属性的内容，但是对于某些属性类型，没有规定属性内容的格式。因此，为适应不同的 RADIUS 服务器要求，需要配置属性内容的格式。目前支持设置 RADIUS Calling-Station-ID 属性（属性号为 31 ）。

RADIUS Calling-Station-ID 属性用于网络设备向 RADIUS Server 发送请求报文时候，标识认证用户的身份。Calling-Station-ID 属性内容是字符串，可以有多种组成格式，由于要求必须能唯一标识一个用户，因此常选择使用用户的 MAC 地址作为其内容。例如在使用 IEEE 802.1X 认证时，选择使用安装 IEEE 802.1X 客户端所在设备的 MAC 地址。关于这 MAC 地址的格式，有以下几种：

格式	说明
ietf	IETF（RFC3580）规定的标准格式，使用 ‘-’ 作为分隔符。例如：00-D0-F8-33-22-AC
normal	常用的表示 MAC 地址的格式（点分十六进制格式），使用 ‘.’ 作为分隔符。例如：00d0.f833.22ac
unformatted	无格式，没有任何分隔符，默认使用这个格式。例如：00d0f83322ac

- 私有属性

RADIUS 协议是一个可扩展的协议。RFC2865 中定义了 26 号属性（Vendor-Specific）用于设备厂商对 RADIUS 协议进行扩展，以实现其私有的或者标准 RADIUS 没有定义的功能。锐捷公司支持的私有属性如表 1-3 所示。其中 TYPE 为锐捷产品私有属性类型的默认配置；扩展 TYPE 为扩展厂商类型的默认配置。

ID	功能	TYPE	扩展 TYPE
1	max-down-rate	1	76
2	port-priority	2	77
3	user-ip	3	3

4	vlan-id	4	4
5	last-supplicant-version	5	5
6	net-ip	6	6
7	user-name	7	7
8	password	8	8
9	file-directory	9	9
10	file-count	10	10
11	file-name-0	11	11
12	file-name-1	12	12
13	file-name-2	13	13
14	file-name-3	14	14
15	file-name-4	15	15
16	max-up-rate	16	16
17	current-supplicant-version	17	17
18	flux-max-high32	18	18
19	flux-max-low32	19	19
20	proxy-avoid	20	20
21	dailup-avoid	21	21
22	ip-privilege	22	22
23	login-privilege	42	42
26	ipv6-multicast-address	79	79
27	ipv4-multicast-address	87	87
62	sdg-type	62	62
85	sdg-zone-name	85	85
103	sdg-group-name	103	103

功能特性

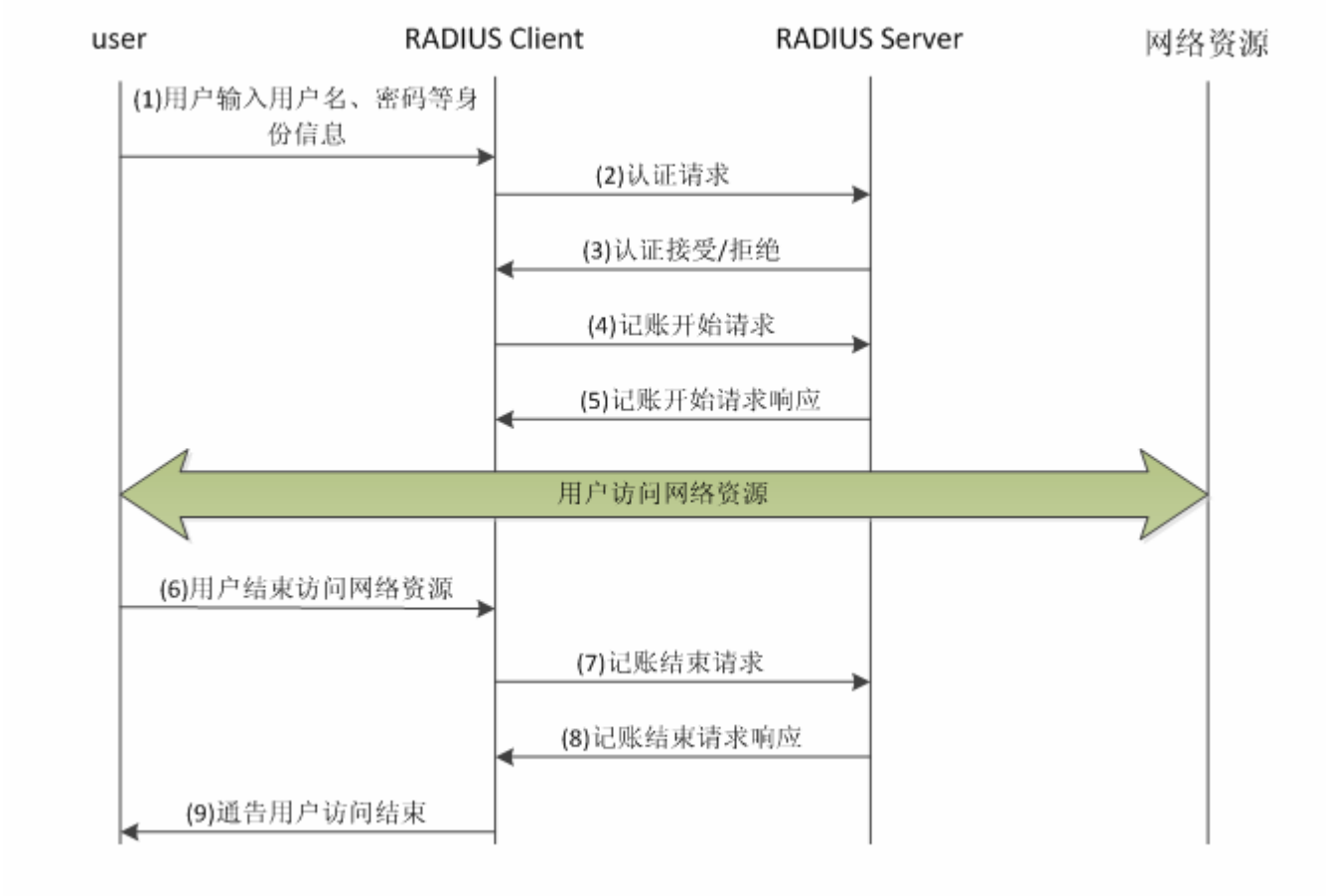
功能特性	作用
RADIUS认证、授权	对访问用户进行身份认证、记账，保护网络安全以及便于网络管理员进行管理。
指定RADIUS报文源地址	指定 RADIUS 客户端向 RADIUS 服务器传送报文时的源 IP 地址。
RADIUS超时重传	指定 RADIUS 服务器对 RADIUS 客户端传送的报文一定的时间内无响应时 RADIUS 客户端重传报文的参数。
RADIUS服务器可达性检测	RADIUS 客户端主动探测 RADIUS 服务器是否可达，并维护各 RADIUS 服务器的可达性状态。进行业务处理时，总是优先选择状态为可达的服务器，以提高 RADIUS 业务的处理性能。
RADIUS强制下线	对于已认证的用户，RADIUS 服务器主动要求其下线

3.3.1 RADIUS认证、授权、记账

对访问用户进行身份认证、记账，保护网络安全以及便于网络管理员进行管理。

工作原理

图 3-2



RADIUS 的认证和授权流程为：

(1) 用户输入用户名、密码等身份信息，传送给 RADIUS 客户端。

(2) RADIUS 客户端获取用户的用户名、密码信息，向 RADIUS 传送认证请求报文。其中密码是加密的，加密方法请参照 RFC2865。

(3) RADIUS 服务器根据用户名、密码信息，决定接受或拒绝此次认证请求。如果接受，同时下发授权信息。不同类型的访问用户，其授权信息也不相同。

RADIUS 的记账流程为：

(4)如果步骤(3)中 RADIUS 服务器返回认证接受，则 RADIUS 客户端紧接着发送记账开始请求报文。

(5)RADIUS 服务器回应记账开始响应报文，开始记账。

(6)用户结束访问网络资源，请求 RADIUS 客户端断开连接。

(7)RADIUS 客户端发送记账结束请求报文。

(8)RADIUS 服务器返回记账结束响应报文，停止记账。

(9)用户断开连接，无法再访问网络资源

相关配置

↘ 配置 RADIUS 服务器参数

缺省情况下，没有配置任何 RADIUS 服务器。

使用 **radius-server host** 命令可以配置 RADIUS 服务器的相关信息。

必须至少配置一个 RADIUS 服务器，RADIUS 相关业务才能正常运转。

↘ 配置 AAA 认证方法列表

缺省情况下，没有配置任何 AAA 认证方法列表。

使用 **aaa authentication** 命令配置不同用户类型的方法列表，并且认证方法选择 group radius。

必须配置相应用户类型的 aaa 认证方法列表，才能进行 radius 认证。

↘ 配置 AAA 授权方法列表

缺省情况下，没有配置任何 AAA 授权方法列表。

使用 **aaa authorization** 命令配置不同类型的授权方法列表，并且授权方法选择 group radius。

必须配置相应类型的 aaa 授权方法列表，才能进行 radius 授权。

↘ 配置 AAA 记账方法列表

缺省情况下，没有配置任何 AAA 记账方法列表。

使用 **aaa accounting** 命令配置不同类型的记账方法列表，并且记账方法选择 group radius。

必须配置相应类型的 aaa 记账方法列表，才能进行 radius 记账。

3.3.2 指定RADIUS报文源地址

指定 RADIUS 客户端向 RADIUS 服务器传送报文时的源 IP 地址。

工作原理

配置 RADIUS 时，通过指定 RADIUS 客户端向 RADIUS 服务器发送 RADIUS 报文的源 IP 地址，可以减少在 RADIUS 服务器上维护大量的 NAS 信息的工作量。

相关配置

缺省配置为使用全局路由寻路，确定发送 RADIUS 报文的源地址。

使用 **ip radius source-interface** 命令指定发送 RADIUS 报文的源接口，设备将把指定接口的第一个 ip 地址作为 radius 报文的源地址。

3.3.3 RADIUS超时重传

工作原理

RADIUS 客户端向 RADIUS 服务器传送报文后，启动定时器检测 RADIUS 服务器的响应，如果一定时间内 RADIUS 服务器没有响应，则 RADIUS 客户端重传报文。

相关配置

↘ 配置 RADIUS 服务器超时时间

缺省配置的超时时间为 5 秒。

使用命令 **radius-server timeout** 命令可以配置超时时间，时间范围为 1 到 1000 秒。

RADIUS 服务器的响应时间和其自身的性能、网络环境有关。需要根据实际情况配置合适的超时时间。

↘ 配置重传次数

缺省配置的重传次数为 3 次。

使用命令 **radius-server retransmit** 命令配置重传次数，范围 1 到 100 次。

↘ 配置记账更新是否重传

缺省配置为不会对计费更新报文进行重传。

使用命令 **radius-server account update retransmit** 命令配置二代 Web 认证用户的记账更新报文进行重传的功能。

3.3.4 RADIUS服务器可达性检测

工作原理

RADIUS 客户端主动探测 RADIUS 服务器是否可达，并维护各 RADIUS 服务器的可达性状态。进行业务处理时，总是优先选择状态为可达的服务器，以提高 RADIUS 业务的处理性能。

相关配置

↘ 配置设备判定 RADIUS 安全服务器不可达的标准

缺省配置的判定 RADIUS 服务器不可达的标准为同时满足以下两个条件：一、设备在 60 秒内内没有收到来自 RADIUS 安全服务器的正确响应报文；二、设备向同一个 RADIUS 安全服务器发送的请求报文连续超时次数达到 10 次。

使用命令 **radius-server dead-criteria** 可以配置设备判定 RADIUS 安全服务器不可达的标准。

↘ 配置主动探测 RADIUS 安全服务器的测试用户名

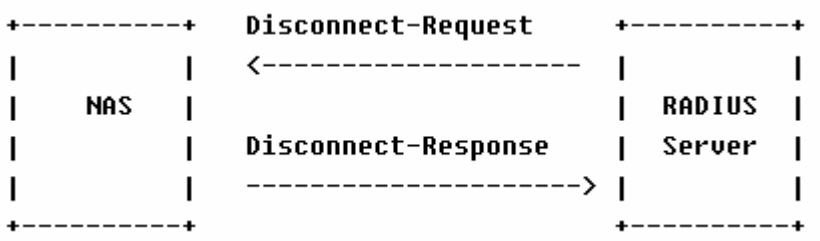
缺省配置时，不对 RADIUS 安全服务器指定主动探测的测试用户名。

使用命令 **radius-server host x.x.x.x testusername xxx** 来配置测试用户名。

3.3.5 RADIUS强制下线

工作原理

图 3-3 RADIUS 动态授权扩展 DM 消息交互图



RADIUS 服务器和设备之间的 DM 消息交互图如上。RADIUS 服务器发送 Disconnect-Request 消息到设备的 3799 UDP 端口，设备处理结束之后，将处理结果通过 Disconnect-Response 消息返回给 RADIUS 服务器。

相关配置

3.4 配置详解

配置项	配置建议 & 相关命令	
RADIUS基本配置	⚠ 必须配置。用于 radius 认证、授权、记账	
	radius-server host	配置远程 RADIUS 安全服务器的 IP 地址
	radius-server key	配置设备和 RADIUS 服务器进行通讯的共享密钥
	radius-server retransmit	配置设备在确认 RADIUS 无效以前发送请求的次数
	radius-server timeout	配置设备重传请求以前等待的时间
	radius-server account update retransmit	配置二代 Web 认证用户的记账更新报文进行重传的功能
	ip radius source-interface	配置 RADIUS 报文的源地址
配置RADIUS属性类型	⚠ 可选配置。用于定义设备封装和解析 radius 报文时对属性的处理。	
	radius-server attribute 31	配置 RADIUS 的 31 号属性（Calling-Stationg-ID）的 MAC 地址格式。

	radius-server attribute class	配置 RADIUS 的 Class 属性的解析方式。
	radius attribute	配置 RADIUS 私有属性类型
	radius set qos cos	配置设备处理服务器下发的私有属性 port-priority 为接口 cos 值。Cos 相关概念请参考“配置 Qos”
	radius support cui	配置设备支持 cui 属性
	radius vendor-specific	配置设备解析私有属性的方式
配置RADIUS可达性检测	⚠ 可选配置。用于检测 RADIUS 服务器是否可达，以及维护 RADIUS 服务器的可达性状态。	
	radius-server dead-criteria	配置全局的 RADIUS 安全服务器不可达的判定标准
	radius-server deadtime	配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长
	radius-server host	配置远程 RADIUS 安全服务器的 IP 地址 ,指定认证端口和记帐端口，指定主动探测的相关参数

3.4.1 RADIUS基本配置

配置效果

- 完成 RADIUS 基本配置，即可进行 RADIUS 认证、授权、记账。

注意事项

- 在设备上配置 RADIUS 之前，应确保 RADIUS 服务器的网络通讯良好。
- 使用命令 **ip radius source-interface** 配置 RADIUS 报文的源地址时，应确保此源地址和 RADIUS 服务器通讯良好。
- 如果进行 RADIUS IPv6 认证，应确保 RADIUS 服务器也支持 RADIUS IPv6 认证。

配置方法

↘ 配置远程 RADIUS 安全服务器

- 必须配置。
- 配置 RADIUS 安全服务器的 IP 地址、认证端口、记账端口、共享密钥。

↘ 配置设备和 RADIUS 服务器进行通讯的共享密钥。

- 可选配置。
- 这里通过全局配置对所有未配置共享密钥选项的服务器配置一个共享密钥。

⚠ 设备上的共享密钥和 RADIUS 服务器上的共享密钥必须一致。

↘ 配置设备在确认 RADIUS 无效以前发送请求的次数

- 可选配置。

- 根据实际网络环境，配置设备确认 RADIUS 无效以前发送请求的次数。

配置设备重传请求以前等待的时间

- 可选配置。
- 根据实际网络环境，配置设备重传请求以前等待的时间。

⚠ 在使用 RADIUS 安全协议的 802.1x 认证环境中，如果网络设备作为 802.1x 认证者，并且采用锐捷 SU 作为 802.1x 客户端软件时，建议在网络设备上设置 **radius-server timeout** 值为 3 秒（默认为 5 秒），设置 **radius-server retransmit** 值为 2 次（默认为 3 次）

配置二代 Web 认证用户的记账更新报文进行重传的功能

- 可选配置。
- 根据实际实际需要，决定是否开启二代 Web 认证用户的记账更新报文重传功能。

配置 RADIUS 报文的源地址

- 可选配置。
- 根据实际网络环境，配置 RADIUS 报文的源地址。

检验方法

- 配置 AAA 方法列表使用 RADIUS 方法，用户进行认证、授权、记账。
- 设备与 RADIUS 服务器进行交互，通过抓包可以看到是通过 RADIUS 协议进行通信的。

相关命令

配置远程 RADIUS 安全服务器

【命令格式】 **radius-server host** [**oob**] { *ipv4-address* | *ipv6-address* } [**auth-port** *port-number*] [**acct-port** *port-number*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]] [**key** [**0** | **7**] *text-string*]

【参数说明】 **oob** ： oob 认证，即向此服务器发送报文时源接口为 mgmt 口。

ipv4-address ：RADIUS 安全服务器主机的 IPv4 地址。

ipv6-address ：RADIUS 安全服务器主机的 IPv6 地址。

auth-port *port-number* ：RADIUS 身份认证的 UDP 端口，取值范围 0 - 65535，如果设置为 0，则该主机不进行身份认证。

acct-port *port-number* ：RADIUS 记帐的 UDP 端口，取值范围 0 - 65535，如果设置为 0，则该主机不进行记帐。

test username *name* ：开启对该 RADIUS 安全服务器的主动探测功能，并指定主动探测所使用的用户名。

idle-time *time*：配置设备向处于可达状态的 RADIUS 安全服务器发送测试报文的时间间隔。默认值为 60 分钟，可配置的范围为 1-1440 分钟（24 小时）。

ignore-auth-port：关闭对 RADIUS 安全服务器的认证端口的检测，默认开启。

ignore-acct-port：关闭对 RADIUS 安全服务器的记账端口的检测，默认开启。

key [**0** | **7**] *text-string* ：配置用于该服务器的共享密钥，未配置则使用全局配置。配置的密钥可以指定加密类型，0 为无加密，7 简单加密，默认为 0。

【命令模式】 全局模式。

【使用指导】 为了使用 RADIUS 实现 AAA 安全服务，必须定义 RADIUS 安全服务器。您可以使用 **radius-server host** 命令定义一个或多个 RADIUS 安全服务器。如果没有把 RADIUS 安全服务器配置在某个 RADIUS 服务器组中，则设备向 RADIUS 服务器发送 radius 报文时使用全局路由表，否则使用该 RADIUS 服务器组所对应的 vrf 路由表。

配置设备和 RADIUS 服务器进行通讯的共享密钥。

【命令格式】 **radius-server key** [**0** | **7**] *text-string*

【参数说明】 *text-string* ：共享密钥的文本。

0 | **7**：口令的加密类型，0 无加密，7 简单加密，默认为 0。

【命令模式】 全局模式

【使用指导】 共享密钥是设备和 RADIUS 安全服务器进行正确通信的基础。为了使设备和 RADIUS 安全服务器能进行通信，必须在设备和 RADIUS 安全服务器上定义相同的共享密钥。

配置设备在确认 RADIUS 无效以前发送请求的次数

【命令格式】 **radius-server retransmit** *retries*

【参数说明】 *retries*：RADIUS 尝试重发次数，取值范围是 1-100

【命令模式】 全局模式

【使用指导】 AAA 在使用下一个方法对用户进行认证的前提是当前认证的安全服务器没有反应。设备判断安全服务器没有反应的标准是安全服务器在设备重发指定次数 RADIUS 报文期间均没有应答，每次重发之间有超时间隔。

配置设备重传请求以前等待的时间

【命令格式】 **radius-server timeout** *seconds*

【参数说明】 *seconds* ：超时时间（单位为秒）。可设置的值范围为 1-1000 秒。

【命令模式】 全局模式

【使用指导】 使用该命令对重发报文的超时时间进行调整。

配置二代 Web 认证用户的记账更新报文进行重传的功能

【命令格式】 **radius-server account update retransmit**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置二代 Web 认证用户的记账更新报文进行重传的功能，默认不重传。该配置不影响其他类型的用户。

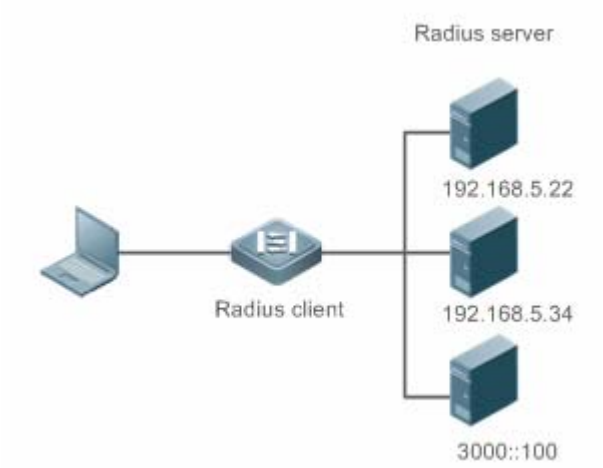
配置举例

以下配置举例，仅介绍与 RADIUS 相关的配置。

Login 用户使用 RADIUS 认证、授权、记账

【网络环境】

图 3-4



【配置方法】

- 配置启用 aaa。
- 配置 radius-server 信息。
- 配置使用 radius 的认证方法、授权方法、记账方法。
- 在接口上应用配置认证方法。

RADIUS Client

```
Ruijie# configure terminal
Ruijie (config)# aaa new-model
Ruijie (config)# radius-server host 192.168.5.22
Ruijie (config)# radius-server host 3000::100
Ruijie (config)# radius-server key aaa
Ruijie (config)# aaa authentication login test group radius
Ruijie (config)# aaa authorization exec test group radius
Ruijie (config)# aaa accounting exec test start-stop group radius
Ruijie (config)# line vty 0 4
Ruijie (config-line)# login authentication test
Ruijie (config-line)# authorization exec test
Ruijie (config-line)# accounting exec test
```

【检验方法】

在 PC 上 telnet 到设备上，要求输入用户名和密码。输入正确的用户名和密码，能够登录到设备上。并且被服务器授予一定的权限级别，仅运行执行该权限级别下的命令。在 RADIUS 服务器上可以查看到此用户的认证日志。用户对设备进行管理操作后退出登录，在 RADIUS 服务器上可以查看到此用户的记账信息。

```
Ruijie#show running-config
!
radius-server host 192.168.5.22
radius-server host 3000::100
radius-server key aaa
aaa new-model
aaa accounting exec test start-stop group radius
aaa authorization exec test group radius
```

```
aaa authentication login test group radius
no service password-encryption
ip tcp not-send-rst
!
vlan 1
!
line con 0
line vty 0 4
 accounting exec test
 authorization exec test
 login authentication test
!
```

常见错误

- 设备配置的 key 与服务器配置的 key 不一致。
- 没有配置方法列表。

3.4.2 配置RADIUS属性类型

配置效果

- 定义设备封装和解析 radius 报文时对属性的处理。

注意事项

- 设置 RADIUS 属性类型一节所涉及的私有属性均指锐捷公司的私有属性。

配置方法

↘ 配置 RADIUS 的 31 号属性（Calling-Stationg-ID）的 MAC 地址格式

- 可选配置
- 根据服务器类型，配置 Calling-Station-Id 的 MAC 地址格式为服务器支持的类型。

↘ 配置 RADIUS 的 Class 属性的解析方式

- 可选配置
- 根据服务器类型，配置对 Class 属性的解析方式。

↘ 配置 RADIUS 私有属性类型

- 可选配置
- 如果服务器为锐捷公司的应用服务器，则需要配置 RADIUS 私有属性类型来适应。

配置设备处理服务器下发的私有属性 port-priority 为接口的 cos 值

- 可选配置
- 根据需要，配置服务器下发的私有属性 port-priority 为接口的 cos 值。

配置设备支持 cui 属性

- 可选配置
- 根据需要，配置设备是否支持 RADIUS 的 CUI 属性。

配置设备解析私有属性的方式

- 可选配置
- 根据需要，配置设备解析锐捷私有属性时私有属性号的索引。

配置 RADIUS 是否支持解析报文中思科、华为、微软的私有属性

- 可选配置
- 根据需要，配置 RADIUS 是否支持解析报文中思科、华为、微软的私有属性，缺省支持。

检验方法

- 配置 AAA 方法列表使用 RADIUS 方法，用户进行认证、授权、记账
- 设备与 RADIUS 服务器进行交互，通过抓包查看 Calling-Station-Id 的 MAC 地址格式。
- 设备与 RADIUS 服务器进行交互，通过设备 debug 信息查看锐捷公司的私有属性被设备正确的解析。
- 设备与 RADIUS 服务器进行交互，通过设备 debug 信息查看 CUI 属性被设备正确的解析。

相关命令

配置 RADIUS 的 31 号属性（Calling-Stationg-ID）的 MAC 地址格式

【命令格式】 **radius-server attribute 31 mac format** { **ietf | normal | unformatted** }

【参数说明】 **ietf** ：指定 ETF（RFC3580）规定的标准格式，使用 ‘-’ 作为分隔符。例如：00-D0-F8-33-22-AC。

normal：指定常用的表示 MAC 地址的格式(点分十六进制格式),使用 ‘.’ 作为分隔符。例如 :00d0.f833.22ac。

unformatted：指定无格式，没有任何分隔符，默认使用这个格式。例如：00d0f83322ac。

【命令模式】 全局模式

【使用指导】 部分 RADIUS 安全服务器（主要用于 802.1x 认证）可能只识别 IETF 的格式，这种情况下需要将 Calling-Station-ID 属性设置为 IETF 格式类型。

配置 RADIUS 的 Class 属性的解析方式

【命令格式】 **radius-server attribute class user-flow-control { format-16bytes | format-32bytes }**

【参数说明】 **user-flow-control：**配置从 class 属性中解析限速配置。

format-16bytes：配置 class 属性中的限速值格式为 16 字节。

format-32bytes：配置 class 属性中的限速值格式为 32 字节。

【命令模式】 全局模式

【使用指导】 如果服务器通过 Class 属性下发限速值，则需要配置该命令。

配置 RADIUS 私有属性类型

【命令格式】 **radius attribute** { *id* | **down-rate-limit** | **dscp** | **mac-limit** | **up-rate-limit** } **vendor-type** *type*

【参数说明】 *id*：功能 id <1-255>

type：私有属性 type

down-rate-limit：下行速率限制属性

dscp：dscp 属性

mac-limit：mac-limit 属性

up-rate-limit：上行速率限制属性

【命令模式】 全局模式

【使用指导】 使用该命令配置私有属性类型值。

配置设备处理服务器下发的私有属性 port-priority 为接口的 cos 值

【命令格式】 **radius set qos cos**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置该命令，可以将传下的 qos 值作为 cos 值，默认时作为 dscp 值。

配置设备支持 cui 属性

【命令格式】 **radius support cui**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 配置该命令，使 radius 支持 cui 属性。

配置设备解析私有属性的方式

【命令格式】 **radius vendor-specific extend**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 使用该命令可对所有厂商 id 的属性按照配置是由类型识别。

配置 RADIUS 是否支持解析报文中思科、华为、微软的私有属性

【命令格式】 **radius vendor-specific attribute support** *vendor_name*

【参数说明】 *vendor_name*，产商的名称，可为 cisco、huawei、ms。

【命令模式】 全局模式

【使用指导】 使用该命令可以配置是否支持对报文中的思科、华为、微软的私有属性进行解析。

配置举例

以下配置举例，仅介绍与 RADIUS 相关的配置。

配置 RADIUS 属性类型

【网络环境】 单设备

【配置方法】
- 配置 RADIUS 的 Calling-Station-Id 的 MAC 地址格式。
- 配置私有属性类型值。
- 配置 radius 传下的 qos 值为接口 cos 值。
- 配置 radius 支持 cui 属性。
- 扩展为不区别私有厂商 id。
- 配置对收到的 radius 报文不支持解析思科的私有属性

```
Ruijie(config)# radius-server attribute 31 mac format ietf
Ruijie(config)# radius attribute 16 vendor-type 211
Ruijie(config)# radius set qos cos
Ruijie(config)# radius support cui
Ruijie(config)# radius vendor-specific extend
Ruijie(config)# no radius vendor-specific attribute support cisco
```

【检验方法】 通过抓包或者设备 debug 信息查看 radius 标准属性和私有属性的封装/解析是否正确。

3.4.3 配置RADIUS可达性检测

配置效果

设备维护所配置的每台 RADIUS 服务器的可达性状态：可达或者不可达。设备不会向处于不可达状态的 RADIUS 服务器发送接入用户的认证、授权和记账请求，除非，该 RADIUS 服务器所在的 RADIUS 服务器组的所有服务器均为不可达状态。

设备支持对指定的 RADIUS 服务器进行主动探测，默认关闭。如果您为指定的 RADIUS 服务器开启主动探测功能，那么设备将会根据配置，定期向该 RADIUS 服务器发送探测请求（认证请求或者记账请求）。其时间间隔周期为：

- 处于可达状态的 RADIUS 服务器：该 RADIUS 服务器的可达状态的主动探测间隔时间（默认值为 60 分钟）。
- 处于不可达状态的 RADIUS 服务器：固定为 1 分钟。

注意事项

为指定的 RADIUS 服务器开启主动探测功能，需要满足如下所有条件：

- 在设备上配置了该 RADIUS 服务器的测试用户名。

- 在设备上至少配置了一个该 RADIUS 服务器的被测端口（认证端口或者记账端口）。

对于一台处于可达状态的 RADIUS 服务器，当以下两个条件均满足时，设备认为该 RADIUS 服务器进入不可达状态：

- 距离上次收到该 RADIUS 服务器的正确响应超过 radius-server dead-criteria time seconds 设定的时间。
- 在上次收到该 RADIUS 服务器的正确响应之后，设备发往该 RADIUS 服务器的请求而未收到正确响应的次数（包括重传），达到 radius-server dead-criteria tries number 设定的次数。

对于一台处于不可达状态的 RADIUS 服务器，当以下任一条件满足时，设备认为该 RADIUS 服务器进入可达状态：

- 设备收到来自该 RADIUS 服务器的正确响应。
- 该 RADIUS 服务器处于不可达状态超过 **radius-server deadtime** 设定的时间，并且该 RADIUS 服务器没有启用主动探测功能。
- 在设备上更新该 RADIUS 服务器的认证端口或者记账端口。

配置方法

配置全局的 RADIUS 安全服务器不可达的判定标准

- 必须配置
- 配置全局的 RADIUS 安全服务器不可达的判定标准是开启主动探测功能的必要条件。

配置远程 RADIUS 安全服务器的 IP 地址，指定认证端口和记帐端口，指定主动探测的相关参数

- 必须配置
- 指定 RADIUS 服务器主动探测的相关参数是开启主动探测功能的必要条件。

配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长

- 可选配置
- RADIUS 服务器没有启用主动探测功能时，配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长才会生效。

检验方法

- 通过 **show radius server** 命令可以查看各个 RADIUS 服务器的可达性信息。

相关命令

配置全局的 RADIUS 安全服务器不可达的判定标准

【命令格式】 **radius-server dead-criteria** { **time** *seconds* [**tries** *number*] | **tries** *number* }

【参数说明】 **time** *seconds*：配置时间条件参数。设备在指定的时间内没有收到来自 RADIUS 安全服务器的正确响应报文，

则认为该 RADIUS 安全服务器满足不可达的时长条件。可设置的值的范围为 1-120 秒。

tries *number*：配置请求连续超时次数条件参数。当设备向同一个 RADIUS 安全服务器发送的请求报文连续超时次数达到所设定的次数，则认为该 RADIUS 安全服务器满足不可达的连续超时次数条件。可设置的值的范围为 1-100。

【命令模式】 全局模式

【使用指导】 如果一台 RADIUS 安全服务器同时满足时间条件和请求连续超时次数条件，则设备认为该 RADIUS 安全服务器不可达。使用该命令，用户可以对时间条件和请求连续超时次数条件的参数进行调整。

配置设备停止向不可达状态的 RADIUS 服务器发送请求报文的时长

【命令格式】 **radius-server deadtime** *minutes*

【参数说明】 *minutes*：配置设备停止向处于不可达状态的 RADIUS 安全服务器发送请求的时间，单位为分钟。可设置的值的范围为 1-1440 分钟（24 小时）。

【命令模式】 全局模式

【使用指导】 如果设备对一台 RADIUS 安全服务器启用了主动探测功能，那么 **radius-server deadtime** 的时间参数对该 RADIUS 安全服务器不起作用；否则，该 RADIUS 安全服务器，将在处于不可达状态的时间超过 **radius-server deadtime** 指定的时间时，被设备自动恢复为可达状态。

配置举例

以下配置举例，仅介绍与 RADIUS 相关的配置。

配置对 RADIUS 服务器进行不可达检测

【网络环境】

图 3-5

【配置方法】

- 配置全局的 RADIUS 安全服务器不可达的判定标准。
- 配置远程 RADIUS 安全服务器的 IP 地址，指定认证端口和记帐端口，指定主动探测的相关参数。

RADIUS Client

```
Ruijie(config)# radius-server dead-criteria time 120 tries 5
Ruijie(config)# radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90
```

【检验方法】 使设备与 192.168.5.22 服务器网络通讯断开。通过设备进行 radius 认证。120 秒后，使用命令 **show radius server** 命令查看服务器状态为 dead。

```
Ruijie#show running-config
…
radius-server host 192.168.5.22 test username test ignore-acct-port idle-time 90
radius-server dead-criteria time 120 tries 5
…
```

3.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
将 RADIUS 动态授权扩展功能的统计信息清零，重新开始统计。	**clear radius dynamic-authorization-extension statistics**

查看运行情况

作用	命令
显示 RADIUS 服务器全局参数。	**show radius parameter**
显示 RADIUS 服务器配置情况。	**show radius server**
显示 RADIUS 私有属性类型配置。	**show radius vendor-specific**
显示 RADIUS 动态授权扩展相关统计信息。	**show radius dynamic-authorization-extension statistics**
显示 RADIUS 认证相关统计信息	**show radius auth statistics**
显示 RADIUS 计费相关统计信息	**show radius acct statistics**
显示 RADIUS 服务器组的配置	**show radius group**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 radius 事件的调试开关。	**debug radius event**
打开 radius 报文打印的调试开关。	**debug radius detail**
打开 radius 动态授权扩展功能的调试开关。	**debug radius extension event**
打开 radius 动态授权扩展报文打印的调试开关。	**debug radius extension detail**

4 802.1x

4.1 概述

IEEE802.1x（Port-Based Network Access Control）是一个基于端口的网络访问控制标准，为 LAN 提供安全接入服务。

IEEE 802 LAN 中，用户只要能接到网络设备上，不需要经过认证和授权即可直接访问网络资源。这种不受控行为会给网络带来安全隐。IEEE 802.1x 协议就是为了解决 802 LAN 安全问题提出来的。

802.1x 支持 Authentication，Authorization，Accounting 三种安全应用，简称 AAA。

- Authentication： 认证，用于判定用户是否可以获得访问权，限制非法用户；
- Authorization： 授权，授权用户可以使用哪些服务，控制合法用户的权限；
- Accounting： 计账，记录用户使用网络资源的情况，为收费提供依据。

802.1x 可以部署在对接入用户进行控制的网络中，以实现对接入用户身份验证、授权服务等

协议规范

- IEEE802.1x ：Port-Based Network Access Control

4.2 典型应用

典型应用	场景描述
无线 802.1x 认证	企业部署无线网络，在无线控制器上开启 802.1x 认证

4.2.1 无线 802.1x认证

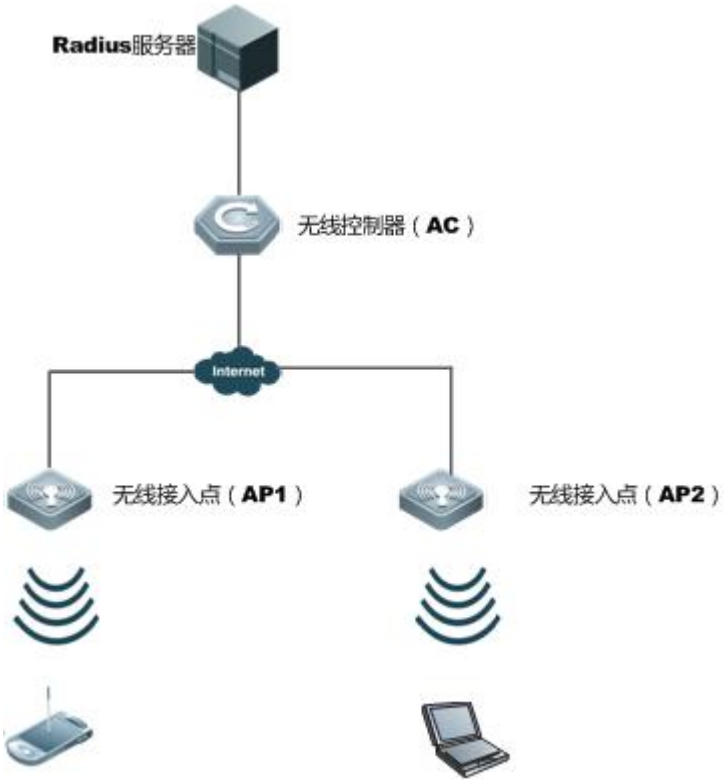
应用场景

企业部署瘦 AP 的无线认证环境，包括瘦 AP，无线控制器（AC）等，部署 802.1x 做无线安全准入，STA 访问企业网时需要先通过 802.1x 认证。

以下图为例：

- 用户终端上要装有 802.1x 的客户端软件（操作系统自带，或者锐捷 supplicant， 或者其他符合 IEEE802.1x 标准的客户端软件）
- 无线控制器支持 IEEE 802.1x；
- 有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器

图 4-1



【注释】 STA 支持 802.1x 认证，连接上 AP 之后，进行 802.1x 认证。无线控制器交换机部署 802.1x 身份认证。Radius 服务器运行 radius server 软件，执行身份校验。

功能部属

- 无线控制器通过 AP 广播的 WLAN 开启 802.1x 认证功能，实现关联的 STA 受控，只有认证通过的用户才能访问网络
- 配置 AAA 方法列表，使 802.1x 可以匹配正确的方法，使用正确的认证服务器
- 配置 radius 参数,参考 RDS-SCG 的说明，确保交换机可以和服务器正常通信
- 如果采用锐捷 radius 服务器，还需要配置 snmp 参数，可以支持 radius 服务器对设备进行查询设置等操作
- Radius 服务器创建帐号，注册接入交换机的 ip 地址，并配置 radius 相关参数，radius 服务器才会对交换机的请求作出响应

4.3 功能详解

基本概念

↘ 用户

802.1x 协议是基于 LAN 的一个协议，对用户的识别不是基于账号，而是基于物理信息，在 WLAN 里面，一个 MAC 地址表示一个用户。除了这个 1 信息是唯一外，其他信息都可以变，比如账号、ip 地址等。

radius

radius（remote authentication dial-in user service）是一种远程认证协议，在 RFC2865 中定义，有着广泛的支持。利用该协议，可以实现服务器远程部署并实施认证。实际部署 802.1x 时，server 通常都是选择远程部署，设备和 server 间的 802.1x 认证信息通过 radius 传输。

超时

认证过程中设备需要和终端、服务器通信，如果终端或服务器在协议指定的时间内没做出应答，则认为超时，超时会导致认证失败。实际部署时，需要注意 802.1x 协议有自己的超时时间，radius 协议也有自己的超时时间，配合使用时必须保证 802.1x 的超时时间大于 radius 的超时时间。

MAB

MAB 是指使用 MAC 地址作为用户名和密码进行认证，对于一些哑终端，比如网络打印机来说，无法安装 supplicant 软件，但是有需要做安全控制，此时可以通过 MAB 实现安全准入。

EAP

802.1x 协议使用 eap 协议承载认证信息，eap 协议在 rfc3748 中定义。eap 协议提供了一个通用的认证框架，在这个框架内可以嵌套多种认证方法，比如 MD5 认证、CHAP 认证、PAP 认证、TLS 认证等。锐捷 802.1x 认证支持 MD5、CHAP、PAP、PEAP-MSCHAP、TLS 等认证方法。

授权

授权是指用户认证通过后给用户绑定一定的服务，比如绑定 vlan、绑定 ACL 等。

计费

计费功能可以实现用户网络审计，比如使用网络的时间、产生的流量，这有利于网络运维和管理。

> 有些 radius 服务器，比如锐捷 SAM 和锐捷 SMP 软件，需要依靠计费报文来判断用户的上下线状态，因此选择这些服务器软件作为 radius 服务器时，必须要配置计费功能。

RIPT

边缘智能感知技术，应用该技术可以在 AC 故障或者 AC 和 AP 断开连接时，AP 可以继续对外提供 WLAN 服务。802.1x 支持该技术，可以在这种情况 AP 上的 802.1x 对外继续提供认证服务。

功能特性

功能特性	作用
认证	提供用户的安全准入，通过认证的用户才可以访问网络
授权	通过认证的用户具备的网络访问权限，比如、acl 绑定等。
计费	提供上网记录审计，比如上网时长、流量等。

4.3.1 认证

认证的目的是为了确认用户身份是否合法，避免非法用户接入网络。用户为了获得访问网络的权限，需要先通过身份认证，服务器确认账号正确后，用户才可以访问网络。在用户通过认证之前，只有 EAPOL 报文（Extensible Authentication Protocol over LAN，802.1x 协议报文）可以在网络上通行（用于认证）。

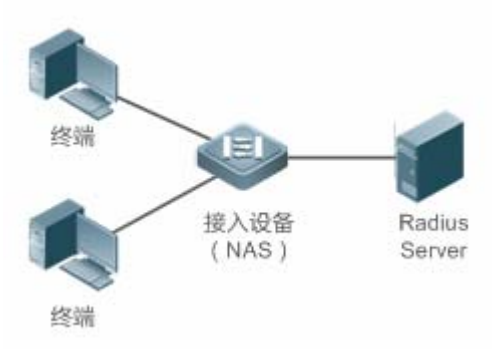
工作原理

802.1x 认证的原理比较简单，就是用户提交账号信息，设备将账号信息发给远程的 radius 服务器进行身份验证，认证通过后允许用户访问网络。

↘ 认证过程的角色

IEEE802.1x 标准认证体系由恳请者(supplicant)、认证者(authenticator)、认证服务器(server)三个角色构成，在实际应用中，三者分别对应为：终端（Client）、接入设备(network access server，NAS)、认证服务器(最常见的是 Radius 服务器)。

图 4-2



- 恳请者

恳请者是最终用户所扮演的角色，一般是个人 PC。它请求对网络服务的访问，并对认证者的请求报文进行应答。恳请者必须运行符合 IEEE 802.1x 客户端标准的软件，目前最典型的就是操作系统自带的 IEEE802.1x 客户端支持，另外，锐捷也已推出符合该客户端标准的 RG Supplicant 软件。

- 认证者

认证者一般为交换机或者无线访问热点等网络接入设备。该设备的职责是根据客户端当前的认证状态控制其与网络的连接状态。在客户端与服务器之间，该设备扮演着中介者的角色：从客户端要求用户名，核实从服务器端的认证信息，并且转发给客户端。因此，设备除了扮演 IEEE802.1x 的认证者的角色，还扮演 RADIUS Client 角色，因此我们把设备称作 network access server(NAS)，它要负责把从客户端收到的回应封装到 RADIUS 格式的报文并转发给 RADIUS Server，同时它要把从 RADIUS Server 收到的信息解释出来并转发给客户端。

扮演认证者角色的设备有两种类型的端口：受控端口（controlled Port）和非受控端口（uncontrolled Port）。连接在受控端口的用户只有通过认证才能访问网络资源；而连接在非受控端口的用户无须经过认证便可以直接访问网络资源。我们把用户连接在受控端口上，便可以实现对用户的控制；非受控端口主要是用来连接认证服务器，以便保证服务器与设备的正常通讯。

- 认证服务器

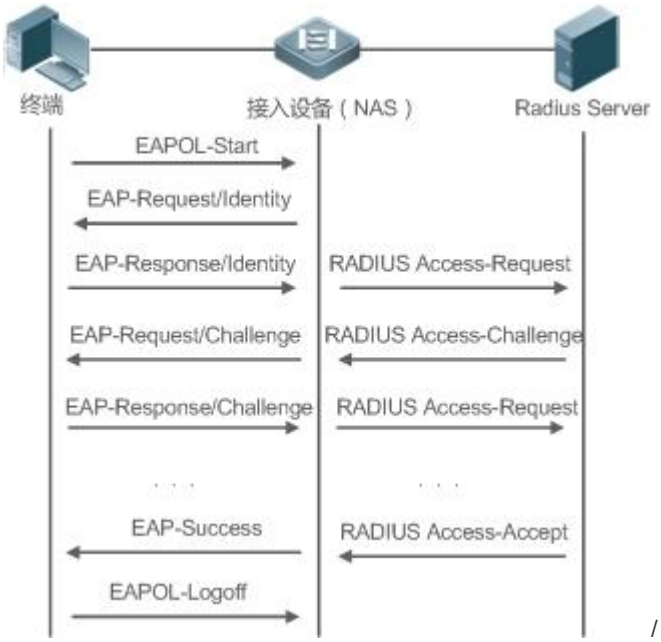
认证服务器通常为 RADIUS 服务器，认证过程中与认证者配合，为用户提供认证服务。认证服务器保存了用户名及密码，以及相应的授权信息，一台服务器可以对多台认证者提供认证服务，这样就可以实现对用户的集中管理。认证服务器还负责管理从认证者发来的记帐数据。锐捷 802.1x 兼容标准的 Radius Server，如微软 IAS/NPS、Free Radius Server、思科 ACS 等。

↘ 认证过程及报文交互

恳请者和认证者之间通过 EAPOL 协议交换信息，而认证者和认证服务器通过 RADIUS 协议交换信息，通过这种转换完成认证过程。EAPOL 协议封装于 MAC 层之上，类型号为 0x888E。同时，标准为该协议申请了一个组播 MAC 地址 01-80-C2-00-00-03，用于初始认证过程中的报文传递。我司认证客户端还有可能将 01-D0-F8-00-00-03 用于认证开始的报文。

下图是一次典型的认证过程中，三个角色设备的报文交互过程：

图 4-3



/

该过程是一个典型的由用户发起的认证过程。在一些特殊的情形下，设备也可能主动发出认证请求，过程与该图一致，只是少了用户主动发出请求这一步。

↘ 认证用户状态

802.1x 中根据端口的认证状态来决定该端口上的用户是否允许访问网络，锐捷产品扩展了 802.1X 协议， 默认是基于用户控制(以 mac 标识一个用户)，所以，默认是根据一个端口下的用户的认证状态来决定该用户是否允许访问网络资源。

一个非受控端口下的所有用户均可使用网络资源，而一个受控端口下的用户只有处于已认证状态（Authorized）才能访问网络资源。一个用户刚发起认证时，状态处于未认证状态（unauthorized），这时它不能访问网络，在认证通过后，该用户的状态会变为已认证状态（authorized），此时该用户便可以使用网络资源。

如果工作站不支持 802.1x，而该工作站连接在受控端口下，当设备请求该用户的用户名时，由于工作站不支持导致没对该请求做出响应。这就意味着该用户仍然处于未认证状态（unauthorized），不能访问网络资源。

相反地，如果工作站支持802.1x，而所连的设备不支持802.1x。用户发出的EAPOL-START 帧无人响应，用户在发送一定数目的 EAPOL-START 帧仍未收到回应的情形下，将认为自己所连的端口是非受控端口，而直接使用网络资源。

在支持 802.1x 的设备下，所有端口的默认设置是非受控端口，我们可以把一个端口设置成受控端口，从而要求这个端口下的所有用户都要进行认证。

当用户通过了认证（设备收到了从 RADIUS Server 服务器发来的成功报文），该用户便转变成已认证状态(authorized)，该用户可以自由使用网络资源。如果用户认证失败以至仍然处于未认证状态，可以重新发起认证。如果设备与 RADIUS server 之间的通讯有故障，那么该用户仍然处于未认证状态（unauthorized），网络对该用户来说仍然是不可使用的。

当用户发出 EAPOL-LOGOFF 报文后，该用户的状态由已认证(authorized)转向未认证状态(unauthorized)。

当设备重新启动，该设备上的所有用户均变为未认证状态(unauthorized)。

如果要强制一个终端免认证，可以通过添加静态 MAC 地址来实现。

↘ 搭建认证服务器

802.1x 认证使用 radius server 作为认证服务器，因此部署 802.1x 安全准入时，需要同时部署 radius server。常见的 radius server 有微软的 IAS/NPS、思科的 ACS 以及锐捷的 SAM/SMP 等。具体的部署步骤可参考对应软件的说明手册。

↘ 配置设备的认证参数

为了使用 802.1x 认证，需要在接入端口上开启 802.1x 认证功能，然后配置 aaa 的方法列表以及 radius 服务器参数。需要保证设备和 radius 服务器是可达的，需要保证 802.1x 的服务器超时时间是大于 radius 的服务器超时时间。

↘ supplicant

用户需要在终端上打开supplicant软件，输入账号并发起认证，如果使用的是操作系统自带的客户端，则操作系统在网络可用时会弹出对话框让用户输入账号。不同客户端软件的实现可能存在差异，界面的操作方式也可能存在差异，推荐使用锐捷 supplicant 软件作为认证客户端，如果使用其他软件，请参考相应的软件说明书。

↘ 下线

用户如果不想访问网络了，可以选择下线。下线有多种方式，包括：关机、端口网络连接、部分supplicant提供的下线功能。

4.3.2 授权

授权是指在用户通过认证之后，限定用户对网络使用的范围，比如 mac 绑定 ip、限制可上网时间或时段、可访问的 vlan、可享受的带宽等。

工作原理

授权是指将权限和用户绑定，根据前面的描述，用户以 mac+vid 标识，授权就是在 mac+vid 的基础上再增加一些绑定信息，比如绑定 vlan 等。

↘ ACL 授权

用户通过认证之后，服务器针对用户下发 acl 或者 ace，如果下发 acl，则需要事先在设备上配置好 acl，如果是下发 ace，则无需其他配置。ACL 授权基于 raius 的属性下发，支持标准属性、锐捷私有属性、思科私有属性，具体需要参考所使用的 radius 服务器的软件说明。

踢线

锐捷 802.1x 和锐捷 SAM/SMP 配合使用时，支持服务器对在线用户实施踢线，踢线后用户将无法访问网络。该功能在一些上网时段控制、上网费用实时检查的环境中可以使用。

VLAN 跳转

无线 802.1x 支持用户认证通过之后将该用户加入到服务器下发的 VLAN 中，该用户可以在该 VLAN 内通信。

4.3.3 计费

计费功能允许网络运营方对接入用户实施上网审计或者费用审计，通常包括时间和流量的审计等。

工作原理

设备配置计费功能，radius 服务器支持 rfc2869 定义的计费审计，用户上线时设备向服务器发送计费开始报文，服务器开始计费，用户下线时，设备向服务器发送计费结束报文，服务器完成一次审计，形成上网费用审计清单。关于计费，不同服务器可能会有不同实现，另外也不是所有服务器都支持计费功能，因此实际部署计费时需要参考服务器的使用说明。

计费开始

配置了计费功能情况下，用户通过认证后，设备会向服务器发送一个计费开始报文，报文携带用户的计费属性，比如用户名和计费 id 等，服务器收到报文后开始对用户计费。

计费更新

设备周期性的向服务器发送计费更新报文，计费更新报文可以使服务器的计费实时性特到提高。计费更新的间隔可以服务器下发，也可以设备上配置。

计费结束

用户下线后设备向服务器发送计费结束报文，携带用户的上网时长、上网消耗的流量等信息，服务器根据这些信息形成用户的上网记录。

4.3.4 RIPT

无线设备上 802.1x 支持 RIPT 功能，在 AC 故障或者 AC 和 AP 断开连接时，可以使得 AP 上的 802.1x 继续对外提供认证服务。

工作原理

通过 AC 上配置 RIPT AP 组，开启 RIPT 功能（RIPT 的详细配置见《WALN-RIPT》）。在 RIPT 的 AP 认证模式下，AC 上的 802.1x 认证相关的配置下发到 RIPT 的 AP 上，AP 即可作为接入设备单独对外提供完整的 802.1x 认证服务（STA 不必在 AC 上进行 802.1x 认证）。AP 上认证通过的用户信息同步到 AC 上，AC 上可查看认证用户状况。

↘ 下发配置

RIPT 的 AP 认证模式下，AC 上配置 aaa，radius 以及 rsna 开启 802.1x 受控口，可以下发到支持 RIPT 的对应 AP 上。下发到 AP 的配置完备之后，AP 即可对外提供 WLAN 服务，包括 802.1x 认证服务。

↘ 同步 AP 的用户信息到 AC

STA 连接上对外提供 802.1x 认证服务的 RIPT AP，进行认证。AP 上认证通过的 802.1x 用户信息可以同步到 AC 上，方便 AC 上查看认证用户状况。

4.4 配置详解

配置项	配置建议 & 相关命令	
配置 801.1x基本功能	⚠ 必须配置，用于部署基本的安全认证和计费。	
	aaa new-model	使能 aaa
	aaa authentication dot1x	配置认证方法列表
	aaa accounting networks	配置计费方法列表
	radius-server host	配置 radius 服务器
	radius-server key	配置设备和 radius 服务器通信的密钥
配置 802.1x协议参数	⚠ 可选配置。用于调整 802.1x 协议参数。 ⚠ 要确保 802.1x 的服务器超时时间大于 radius 的服务器超时时间。 ⚠ 锐捷客户端在线检测功能仅适用于锐捷 supplicant	
	dot1x re-authentication	配置重认证功能
	dot1x timeout re-authperiod	配置重认证间隔
	dot1x timeout tx-period	配置 request/id 报文重传间隔
	dot1x reauth-max	配置 request/id 报文重传次数
	dot1x timeout supp-timeout	配置 request/challenge 报文重传间隔
	dot1x max-req	配置 request/challenge 报文重传次数
	dot1x timeout server-timeout	配置服务器超时时间
	dot1x timeout quiet-period	配置认证失败后的静默时间
	dot1x auth-mode	配置认证模式(eap/chap/pap)
配置MAB	⚠ 可选配置，用于支持 mac 认证	
	dot1x-mab	配置无线 MAB 功能
	dot1x mab-username upper	配置 MAB 认证用户名用大写字母
配置扩展功能	⚠ 可选配置，配置同 mac 多帐号	

	dot1x multi-account enable	配置支持一个 mac 使用多账号认证
	dot1x valid-ip-acct enable	配置获取 IP 后开始计费功能
	dot1x valid-ip-acct timeout	配置用户认证通过之后，允许等待该用户获取 IP 的时间，超过该时间用户未获取 IP 地址将被踢下线
	dot1x event server-invalid action bypass-wlan	配置 RADIUS 服务器逃生
	dot1x encryption only	配置 802.1x 和 WEB 认证共用
	dot1x logging rate-limit	配置认证用户上线和下线的日志速率限制
	dot1x offline-detect	配置基于 WLAN 的用户流量检查功能
	dot1x user-trap enable	配置 802.1x 认证用户上线下线的 Trap 消息通告

4.4.1 配置 802.1x基本功能

配置效果

- 提供基本的认证和计费服务。
- 无线环境下 WLAN 的安全模式为 WPA 或 WPA2，开启该 WLAN 的 802.1X 受控，连接该 WLAN 的 STA 必须通过 802.1x 认证才能通信.
- 通过 radius 服务器命令配置服务器的 ip 和协议通信端口信息，配置设备和服务器间的 radius 加密密钥，确保通信安全.
- 使用全局命令 **aaa accounting update** 命令开启计费更新，计费更新间隔可以在设备上通过 **aaa accounting uptate interval** 命令配置参数，也可以在服务器上配置，这取决于服务器是否支持该功能。如果服务器有下发，则优先使用服务器下发的参数，如果服务器没下发，则使用本机配置参数.

注意事项

- 注意 radius 参数的配置准确性，确保基本的 radius 协议通信正常。
- 802.1x 使用的认证方法列表和计费发列表必须在 aaa 里面已经配置好了，否则会导致认证和计费出错。
- 802.1x 默认使用 default 方法类表，如果 aaa 配置的不是 default 方法列表，需要通过 dot1x authentication 和 dot1x accounting 命令重新制定 802.1x 使用的方法列表。
- 配合锐捷 SAM/SMP 软件使用时，必须配置计费功能，否则用户下线时服务器无法感知导致表项残留。

配置方法

↘ 使能 aaa

- 必须配置，使能 aaa 之后 802.1x 认证计费功能才会生效。

- 在使用 802.1x 对接入用户进行受控的设备开启

【命令格式】 **aaa new-model**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 默认关闭，部署 802.1x 认证必须要配置该命令

配置 aaa 认证方法

- 必须配置。
- 需要和 801.x 使用的认证方法一致
- 在使用 802.1x 对接入用户进行受控的设备开启

【命令格式】 **aaa authentication dot1x** *list-name* **group radius**
【参数说明】 *list-name* ：aaa 的 dot1x 认证方法列表
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 默认关闭
需要 802.1x 的认证方法一致

配置 radius 服务器参数

- 必须配置，可以实现设备和 radius 服务器的正常通信。
- 在使用 802.1x 对接入用户进行受控的设备开启

【命令格式】 **radius-server host** *ip-address* [**auth-port** *port1*] [**acct-port** *port2*]
【参数说明】 *ip-address*：指定服务器 ip 地址
port1 ：认证协议端口
port2 ：计费协议端口
【缺省配置】 默认无 radius 服务器参数
【命令模式】 全局模式
【使用指导】 -

配置 radius 服务器通信密钥

- 必须配置，可以实现设备和 radius 服务器的正常通信。
- 在使用 802.1x 对接入用户进行受控的设备开启

【命令格式】 **radius-server key** *string*
【参数说明】 *string*：radius 通信密钥
【缺省配置】 默认无 radius 通信密钥
【命令模式】 全局模式
【使用指导】 设备的 ip 地址必须和服务器上注册的设备地址一致
设备和服务器的通信的 key 也必须配置一致
如果服务器更改了默认的 radius 通信端口，则配置时也需要指定协议端口

配置无线 802.1x

- 必须配置。
- 在 AC 或者 AP 上配置。
- WLAN 开启 802.1X 受控的时候，只允许 802.11 管理帧和 EAP 报文通过，其它报文全部被丢弃处理。
- 相关命令请见《RSNA》手册

检验方法

开启 supplicant 软件并发起认证，输入正确的账号并发起认证，然后通过 802.1x 的检查和 radius 的检查确认配置是否准确。

通过 show dot1x summary 查看 802.1x 是否有创建认证表项

【命令格式】 **show dot1x summary**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 查看认证用户表项信息，通过该信息，可以知道认证终端当前处于什么阶段，比如正在认证、已经认证或者静默。

【命令展示】

```
Ruijie#show dot1x summary

ID        Username   MAC            Interface VLAN Auth-State      Backend-state Port-Status
User-Type Time
--------- ---------- -------------- --------- ---- ---------------- ------------- -----------
--------- -----------------
16777302  ts-user    b048.7a7f.f9f3 wlan 1    1    Authenticated    Idle          Authed
static    0days 0h 0m12s
```

通过 show aaa user all 查看 aaa 是否有用户表项

【命令格式】 **show aaa user all**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 显示 AAA 用户相关信息。

【命令展示】

```
Ruijie#show aaa user all

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

       Id ----- Name

 2345687901      wwxy

------------------------------
```

- 通过设备和服务器间的 radius 报文检测服务器是否响应了认证，如果没有响应，则属于网络不通或者参数配置错误，如果服务器直接返回拒绝，则需要查看服务器的 log 文件，看是因为什么原因，比如服务器的认证方法配置错误等。

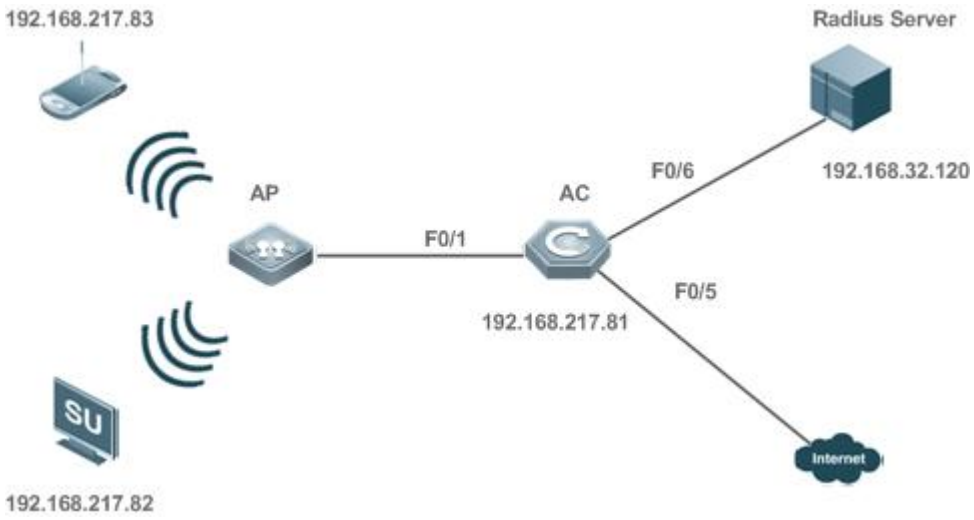
配置举例

以下配置举例，以锐捷 SAM 作为认证服务器。

配置 802.1x 认证

【网络环境】

图 4-4



【配置方法】

- 服务器上注册设备的 ip 信息，并配置设备和服务器的通信密钥
- 服务器上创建账号信息
- 设备使能 aaa
- 设备配置 radius 参数
- 设备接口上使能 802.1x 认证

如下为设备上的相关配置，服务器端的配置请参考具体服务器的配置指导手册：

```
ruijie# configure terminal
ruijie (config)# aaa new-model
ruijie (config)# radius-server host 192.168.32.120
ruijie (config)# radius-server key ruijie
ruijie (config)# wlansec 1

Ruijie(config-wlansec)# security rsn enable
Ruijie(config-wlansec)# security rsn ciphers aes enable
Ruijie(config-wlansec)# security rsn akm 802.1x enable
```

【检验方法】 测试是否可以正常认证以及认证前后的网络访问行为是否变化。

- 服务器创建账号，比如 username:tests-user,password:test。
- 终端未认证前无法 ping 通 192.168.32.120。

- 终端打开 supplicant 后输入账号并点击认证，认证成功，可 ping 通 192.168.32.120。
- 可以显示认证通过的用户信息

```
ruijie# show dot1x summary
ID        Username    MAC             Interface VLAN Auth-State      Backend-State
Port-Status User-Type Time
--------- ----------- --------------  --------- ---- ---------------- -------------
----------- --------- ------------------
16778217  ts-user     0023.aeaa.4286  Fa0/1     2    Authenticated    Idle          Authed
static    0days 0h 0m 7s
```

常见错误

- radius 参数配置错误。
- 服务器有特殊的接入策略，比如要求 radius 报文必须携带某些属性等。
- aaa 的方法列表和 802.1x 的方法类表不一致导致无法认证

4.4.2 配置 802.1x协议参数

配置效果

- 根据网络实际情况调整协议的参数值，比如服务器性能较差的环境中，可以将服务器超时时间适当配大。

注意事项

- 802.1x 协议有自己的服务器超时参数，radius 也有自己的服务器超时参数，默认情况下，802.1x 的超时参数是 5 秒，小于 radius 的超时参数 15 秒。实际使用时，需要确保 802.1x 的服务器超时参数大于 radius 的服务器超时参数。可使用 dot1x 服务器超时配置命令将 802.1x 的超时参数配置大, radius 的超时规则请参考 radius 配置手册.

配置方法

↘ 使能重认证

- 可选配置，开启后即可定期对在线用户重认证。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x re-authentication**
【参数说明】 -
【缺省配置】 默认关闭
【命令模式】 全局模式

【使用指导】 在需要对认证用户定时重认证时可以配置此命令

配置重认证间隔

- 可选配置，配置用户的重认证周期。
- 在设备开启 802.1x 认证之后配置，开启重认证功能后生效

【命令格式】 **dot1x timeout re-authperiod** *period*
【参数说明】 *period*：重认证间隔，单位秒，默认 3600 秒
【缺省配置】 默认 3600 秒
【命令模式】 全局模式
【使用指导】 根据需要来调整认证用户的重认证间隔

配置 request/id 报文重传间隔

- 可选配置，设备重传报文的周期，周期越长则报文重传时间也越长。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x timeout tx-period** *period*
【参数说明】 *period*：报文重传间隔，单位秒，默认 30 秒
【缺省配置】 默认 30 秒
【命令模式】 全局模式
【使用指导】 使用默认值即可，根据认证客户端响应设备请求的时间长短来调整该数值

配置 request/id 报文重传次数

- 可选配置，设备重传报文的次数，数值越大，重传次数就越大。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x reauth-max** *num*
【参数说明】 *num*：报文重传次数，默认 3
【缺省配置】 默认 3 次
【命令模式】 全局模式
【使用指导】 使用默认值即可，容易丢包的环境增大该值可以提高客户端收到设备报文的概率

配置 request/challenge 报文重传间隔

- 可选配置，设备重传 request/challenge 报文的间隔，数值越大，重传间隔就越大。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x timeout supp-timeout** *time*
【参数说明】 *time*：报文重传间隔，单位秒，默认 3 秒
【缺省配置】 默认 3 秒
【命令模式】 全局模式
【使用指导】 使用默认值即可，容易丢包的环境中可以增大该数值

配置 request/challenge 报文重传次数

- 可选配置，设备重传 request/challenge 报文的次数，数值越大，重传次数就越大。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x max-req** *num*
【参数说明】 *num*：报文重传次数，单位秒，默认 3
【缺省配置】 默认 3 次
【命令模式】 全局模式
【使用指导】 可选配置
使用默认值即可，容易丢包的环境中可以增大该数值

配置服务器超时时间

- 可选配置，设备服务器超时时间，数值越大，等待服务器超时的时间就越长。
- 在设备开启 802.1x 认证之后配置
- Radius 和服务器之间的通信超时必须大于 802.1x 的服务器超时时间

【命令格式】 **dot1x timeout server-timeout** *time*
【参数说明】 *time*：服务器超时时间，单位秒，默认 5 秒
【缺省配置】 默认 5 秒
【命令模式】 全局模式
【使用指导】 使用默认值即可，设备和服务器通信不稳定的环境中可以增大该数值

配置认证失败后的静默时间

- 可选配置，用户认证失败后的时间，数值越大，静默用户的时间就越长。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x timeout quiet-period** *time*
【参数说明】 *time*：认证失败后的静默时间，单位秒，默认 10 秒
【缺省配置】 默认 10 秒
【命令模式】 全局模式
【使用指导】 使用默认值即可，增大该数值可以降低认证失败的用户频繁向服务器发起认证增加服务器的负担

配置认证模式

- 可选配置，配置 802.1x 认证方式。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x auth-mode** {**eap** | **chap** | **pap**}
【参数说明】 eap：采用 eap 方式认证
chap ：采用 chap 方式认证
pap ：采用 pap 方式认证
【缺省配置】 默认 eap
【命令模式】 全局模式
【使用指导】 认证模式的选择取决于 supplicant 和认证服务器的支持情况。

检验方法

可以通过 show dot1x 查看参数配置是否生效。

配置举例

配置认证模式

【网络环境】 单机

【配置方法】 配置认证模式为 chap：

```
Ruijie(config)#dot1x auth-mode chap
```

【检验方法】 显示配置结果。

```
Ruijie(config)#show dot1x

802.1X basic information:
  802.1X Status ..................... enable
  Authentication Mode ............... chap
  Authorization mode ................ disable
  Total User Number ................. 0 (exclude dynamic user)
  Authenticated User Number ......... 0 (exclude dynamic user)
  Dynamic User Number ............... 0
  Re-authentication ................. disable
  Re-authentication Period .......... 3600 seconds
  Re-authentication max ............. 3 times
  Quiet Period ...................... 10 seconds
  Tx Period ......................... 30 seconds
  Supplicant Timeout ................ 3 seconds
  Server Timeout .................... 5 seconds
  Maximum Request ................... 3 times
  Client Online Probe ............... disable
  Eapol Tag ......................... disable
  802.1x redirect ................... disable
  Private supplicant only ........... disable
```

常见错误

- server-timeout 比 radius 超时参数小。

配置效果

- 支持下发 ACL 功能，用户认证通过之后，必须符合下发 ACL 的规则要求

注意事项

配置方法

4.4.3 配置MAB

配置效果

- 无线环境下支持基于 WLAN 开启 MAB 认证，部署该功能之后，设备自动将关联相应 WLAN 的 STA 的 MAC 作为用户名和密码向服务器发起认证

注意事项

- 无线的 WLAN 开启 MAB 认证时，该 WLAN 的安全模式必须是 OPEN 模式。

配置方法

↘ 配置无线 MAB

- 可选配置
- 在无线设备的 wlan 上配置

【命令格式】 **dot1x-mab**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 wlansec 模式
【使用指导】 WLAN 下客户端需要使用其 mac 需要做安全认证时配置该命令
仅无线平台可用

↘ 配置 MAB 认证用户名用大写字母

- 可选配置
- 在全局模式配置

【命令格式】 **dot1x mab-username upper**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 MAB 认证用户名中的字母默认为小写字母。配置本命令后，新的 MAB 认证的用户名将使用大写字母，以满

足要求 MAB 认证用户名为大写的服务器要求。

检验方法

通过哑终端接入网络是否可以访问网络验证 MAB 是否生效。

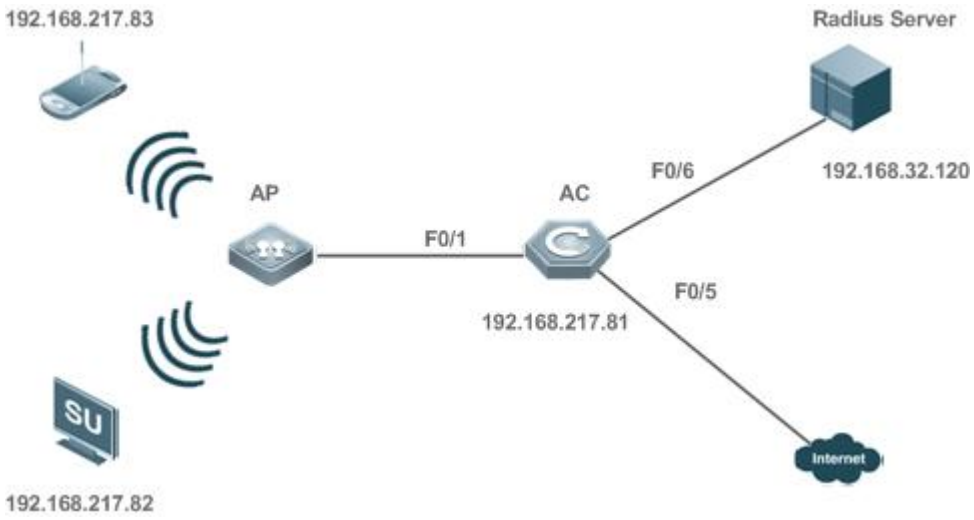
- 服务器和设备上先配置好 MAB 相关功能
- 不符合 MAC 地址账号的终端接入，无法访问网络
- 符合 MAC 地址账号的终端接入，可以访问网络

配置举例

配置无线 MAB 认证

【网络环境】

图 4-5



【配置方法】

- 服务器上注册设备的 ip 信息，并配置设备和服务器的通信密钥
- 服务器上创建账号信息
- 设备使能 aaa
- 设备配置 radius 参数
- 设备 wlan 上使能 MAB 认证功能

如下为设备上的相关配置，服务器端的配置请参考具体服务器的配置指导手册：

```
ruijie# configure terminal
ruijie (config)# aaa new-model
ruijie (config)# radius-server host 192.168.32.120
ruijie (config)# radius-server key ruijie
ruijie(config)#wlansec 1
ruijie(config-wlansec)#dot1x-mab
```

【检验方法】 测试是否可以正常认证以及认证前后的网络访问行为是否变化。

- 服务器创建账号，比如 username: 0023aeaa4286,password: 0023aeaa4286。
- 终端未认证前无法 ping 通 192.168.32.120。
- 终端连接上设备，认证成功，可 ping 通 192.168.32.120。
- 可以显示认证通过的用户信息

```
ruijie# show dot1x summary
ID        Username   MAC             Interface VLAN Auth-State      Backend-State
Port-Status User-Type Time
--------- ---------- --------------  --------- ---- ---------------- -------------
----------- --------- -------------------
16778217  0023aea...  0023.aeaa.4286  Fa0/1     2    Authenticated    Idle          Authed
static    0days 0h 5m 8s
```

常见错误

- 服务器上的 MAC 账号格式不准确。

4.4.4 扩展功能配置

配置效果

- 多账号功能支持一个终端重认证时切换账号，对于一些特殊场景，比如 windows 的域认证，存在接入域时多次认证且认证时会变更账号，该功能适用这类场景。
- 802.1X 支持用户获取 IP 地址后再开始计费，这样可以满足服务器要求用户计费时必须携带 IP 地址的要求。用户先认证上线，可以从 supplicant 或者 dhcp snooping 等获用户的 IP，获取到 IP 地址后 802.1x 才会发起计费请求。为避免设备长时间没有获取到认证客户端的 IP 导致一直不发起计费，该功能配备了一个 IP 检测超时时间。如果在配置的时间内(默认 5min) 没有获取到终端的 IP 地址，则将用户下线。
- 802.1X 功能支持 RADIUS 认证服务器不可用时，切换到预先配置的逃生 WLAN 功能。逃生 WLAN 一般是 OPEN 模式的，且服务默认不可用，当 802.1X 认证的 WLAN 服务不可用时打开该 WLAN 的服务，同时关闭 802.1x 认证的 WLAN 服务，用户切换到逃生 WLAN，可以正常访问网络。
- 802.1X 功能支持与 WEB 认证共用，当一个 WLAN 配置成与 WEB 认证共用时，进行 802.1X 认证的用户只起到加密作用，用户需要访问网络，还要进行 WEB 认证，用户的空口数据都是经过加密的，提高用户数据的安全性。
- 802.1X 功能支持对无线认证用户上线下线的打印 syslog 进行提示，可以根据认证环境中的用户认证速率调整用户上线下线的 syslog 的打印速率，避免大量用户上线下线而频繁打印 syslog 引起 CPU 利用率偏高。
- 在无线 802.1x 认证环境中，支持对认证用户上线和下线发送 SNMP Trap 消息给服务器，以通告认证用户上线和下线情况。

- 在无线802.1x认证环境中，支持基于WLAN开启流量监测功能，即通过认证的终端如果在指定时间内流量低于配置的阈值，将会被下线，使得服务器的计费可以及时处理。
- 802.1x 功能支持在获取了认证客户端的终端信息之后再向服务器发起计费，这样可以将认证客户端的终端信息传递到服务器。在有线设备上为避免长时间没有获取到认证客户端的终端信息而不向服务器发起计费，允许配置相应的超时时间，超过该时间设备如果还没有获取到终端信息，则直接向服务器发起计费。
- 部分服务器只会在用户首次认证时下发记账更新周期，用户重新认证时就不再下发记账更新周期，导致重认证之后用户使用了设备配置的记账更新周期，而不是优先使用服务器的记账更新周期。为保证可以始终按照服务器的记账更新周期发送记账更新报文，可以选择用户在线期间始终以首次认证时服务器下发的记账更新周期为准。
- 由于现场有 H3C 设备，mab 认证服务器配置用户名采用 xx-xx-xx-xx-xx-xx 格式，而我司设备 mab 认证默认用户名格式是 xxxxxxxxxxxx，所以增加命令控制格式。
- 无线终端采用静态 IP 地址，需要将 IP 地址上传给服务器；1x 默认的 IP 地址来源 dhcp snooping，现在新增 stamg 通告静态 IP 地址的来源，所以新增命令控制。

注意事项

- 部署计费的环境中，不能开启多帐号功能，否则会影响计费准确性。
- 配置用户获取 IP 地址之后再开始计费时，需要注意：ipv4 环境且部署了锐捷 supplicant 客户端，由于 supplicant 具备上传终端 ipv4 地址的能力，因此这个环境下无需开启这个功能; 部署静态 IP 的环境中无法使用该功能
- 建议逃生 WLAN 的 SSID 不能跟 802.1x 认证的 WLAN SSID 相同，这样在使用逃生 WLAN 服务时能够有直观的体现，并且当服务器不可用，需要切换 WLAN 时，用户需要手工切换一次 SSID，由于终端通常具有 SSID 记忆功能，因此一次切换以后，后续再出问题就可以自动切换了。
- 802.1X 用户只做加密，因此对 802.1X 用户的授权将不生效，例如服务器下发 acl,下发限速都将不生效，但用户需要接入网络时还需进行 WEB 认证，可以对 WEB 认证用户进行授权。

配置方法

↘ 配置多帐号认证

- 可选配置，允许同一个 mac 被多个帐号使用时可以配置此命令。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x multi-account enable**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 DOT1X认证中，某些环境中存在切换帐号认证的需求，比如部署windows的域认证，需要配置该功能，这样认证客户端可以在前一个帐号还没有下线的情况下，直接使用新的帐号发起认证。默认禁止切换帐号认证。

↘ 配置接口下的认证用户数限制

- 可选配置，可以限制受控口上线的用户数量，包括静态用户和动态用户。

- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x default-user-limit** *num*
【参数说明】 *num*:用户数限制
【缺省配置】 不限制端口用户
【命令模式】 接口模式
【使用指导】 默认不限制端口可以认证的用户数量，需要限制端口下可认证用户数时可配置此命令

配置获取 ip 后开始计费功能

- 可选配置，设备获取到客户端的 ip 地址之后，才会想服务器发出记账。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x valid-ip-acct enable**
【参数说明】
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 开启此命令后，在开启记账的情况下，只有获取到了认证客户端的 IP 之后，设备才会发起记账，超时没有获取到 IP 则将此用户强制下线；没有开启记账时开启此命令，设备获取到 IP 之后不会发起记账，而超时没有获取到 IP 则同样会将此用户强制下线。

配置用户认证通过之后，允许等待该用户获取 ip 的时间

- 可选配置，开启获取 ip 开始计费功能，允许等待获取该用户 ip 的时间。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x valid-ip -acct timeout** *time*
【参数说明】 *time*：超时时间，单位为分钟，默认为 5 分钟
【缺省配置】 默认为 5 分钟
【命令模式】 全局模式
【使用指导】 使用默认值即可，需要改变用户认证通过后等待获取 IP 的时间，可以使用此命令

配置 RADIUS 服务器逃生功能

- 可选配置。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x event server-invalid action bypass-wlan** *wlan_id*
【参数说明】 *wlan_id*：逃生的 wlan
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 无线设备支持
使用默认值即可，需要在服务器不可达时提供相应的 wlan，可以使用此命令

配置 802.1x 和 WEB 认证共用

- 可选配置，802.1x 和 WEB 认证共用时 802.1x 仅作加密功能时。

- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x encryption only**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 wlan 安全配置模式
【使用指导】 使用默认值即可。
无线设备上支持

配置 802.1x 认证用户上下线的 syslog 速率

- 可选配置，可以用来控制 802.1x 用户上线时打印 log 的速率。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x logging rate-limit** *value*
【参数说明】 *value*：每一秒打印用户上下线 syslog 的速率，默认是 5 条/s，0 表示不限速率
【缺省配置】 默认是 5 条/s
【命令模式】 全局模式
【使用指导】 一般使用默认值即可，如果有大量的认证用户频繁的上线下线，需要调低该速率
无线平台上支持

配置 802.1x 认证用户上下线的 SNMP Trap 通告

- 可选配置，可以用来开关 802.1x 用户上线时是否发送 trap 给 snmp 服务器。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x user-trap enable**
【参数说明】
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 无线 802.1x 认证设备上支持
需要向 SNMP 服务器发送认证用户上线和下线 Trap 消息时开启此命令，需要配置 SNMP 服务器并允许发送 Trap 消息，具体见 SNMP 配置

配置流量检查功能

- 可选配置，开启之后 802.1x 认证用户在检测时间周期内低于流量阈值则被踢下线，避免错误计费。
- 在设备开启 802.1x 认证之后配置

【命令格式】 **dot1x offline-detect {[interval** *val***] | [flow** *num***]}**
【参数说明】 *val*：检测时间，默认为 8 小时
num：流量阈值，则默认是 0KB
【缺省配置】 AC 上默认开启，AP 上默认关闭
【命令模式】 Wlan 安全模式
【使用指导】 无线 802.1x 认证设备上支持
为避免 STA 下线了，但设备还没完全探测到而继续对用户计费可以配置此命令

配置选择首次认证时通过服务器下发的记账更新周期

- 可选配置，指用户认证在线期间都使用首次认证时服务器下发的记账更新周期，忽略掉设备配置的记账更新周期。

【命令格式】 **dot1x acct-update base-on first-time server**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 部分服务器在用户重认证时不会下发记账更新周期，但是又要求必须按照用户首次认证时下发的记账更新周期来发送记账更新报文，可以配置此命令。

配置 mab 认证用户名的格式

- 可选配置，仅对 MAB 认证用户有效。

【命令格式】 **dot1x mab-username format with-dot | with-colon | with-hyphen**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 dot1x mab-username format with-dot 配置 mab 用户名格式 xxxx.xxxx.xxxx
dot1x mab-username format with-colon 配置 mab 用户名格式 xx:xx:xx:xx:xx:xx
dot1x mab-username format with-hyphen 配置 mab 用户名格式 xx-xx-xx-xx-xx-xx

配置获取静态 IP 地址

- 可选配置。对 802.1x 用户和 MAB 认证用户均有效。

【命令格式】 **dot1x get-static-ip enable**
【参数说明】 -
【缺省配置】 关闭
【命令模式】 全局模式
【使用指导】 无线中终端使用静态 IP 地址，需要将该静态 IP 地址上传给服务器时，可以开启这个功能；
注意，IP 地址是通过记账报文上传给服务器的，另外使用静态 IP 地址，会没有终端识别信息

检验方法

无。

配置举例

无。

4.5 监视与维护

清除各类信息

⚠ 关闭 802.1x 认证功能后，认证用户信息可以被清除。

作用	命令
清除 802.1x 认证用户信息。	**no do1x port-control auto**
清除 802.1x 认证用户信息	**clear dot1x user**
恢复 802.1x 的默认配置	**dot1x default**

查看运行情况

作用	命令
查看 radius 服务器参数和状态	**show radius server**
查看 802.1x 功能状态和协议参数	**show dot1x**
查看主动认证状态	**show dot1x auto-req**
查看接口受控情况	**show dot1x port-control**
查看客户端探测功能状态和参数	**show dot1x probe-timer**
查看认证用户表项信息	**show dot1x summary**
查看 equest/challenge 报文重传次数	**show dot1x max-req**
查看受控口信息	**show dot1x port-control**
查看重认证开关的状态	**show dot1x re-authentication**
查看 request/id 报文重传次数	**show dot1x reauth-max**
查看认证失败之后的静默时间	**show dot1x timeout quiet-period**
查看重认证周期	**show dot1x timeout re-authperiod**
查看服务器超时时间	**show dot1x timeout server-timeout**
查看客户端超时时间	**show dot1x timeout supptimeout**
查看 request/id 报文重传间隔	**show dot1x timeout tx-period**
根据 id 来查看用户信息	**show dot1x user id**
根据用户 mac 来查看用户信息	**show dot1x user mac**
根据用户名来查看用户信息	**show dot1x user name**
查看 RIPT 的 AP 上的认证用户概要信息	**show dot1x ript summary**
根据 id 来 RIPT 的 AP 上的查看用户信息	**show dot1x ript user id**
根据用户 mac 来 RIPT 的 AP 上的查看用户信息	**show dot1x ript user mac**

根据用户名来 RIPT 的 AP 上的查看用户信息	**show dot1x ript user name**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

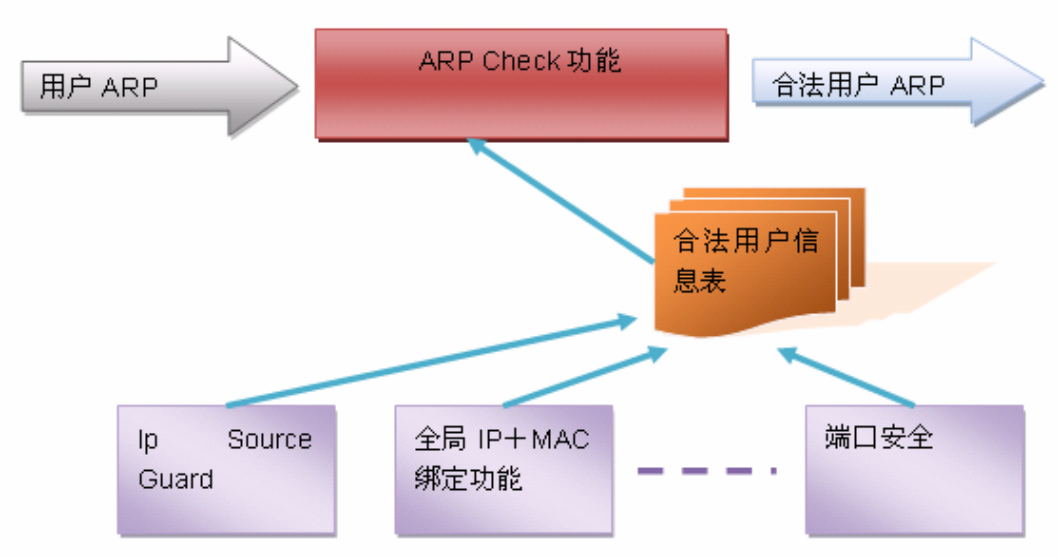
作用	命令
AAA 调试信息（详见 AAA 配置手册）	**debug aaa**
Radius 调试信息(详见 Radius 配置手册）	**debug radius**
打开 dot1x 事件相关的调试开关	**debug dot1x event**
打开 dot1x 报文处理相关的调试开关	**debug dot1x packet**
打开 dot1x 认证状态机相关的调试开关	**debug dot1x stm**
打开 dot1x 内部通信相关的调试开关	**debug dot1x com**
打开 dot1x 错误相关的调试开关	**debug dot1x error**

5 ARP Check

5.1 概述

ARP 报文检查（ARP-Check）功能，对端口下（包括有线接入的 2 层交换口、2 层 AP 口或者 2 层封装子接口和无线接入的 WLAN）的所有的 ARP 报文进行过滤，对所有非法的 ARP 报文进行丢弃，能够有效的防止网络中 ARP 欺骗，提高网络的稳定性。在支持 ARP Check 功能的设备中，ARP Check 功能能够根据 IP Source Guard、全局 IP+MAC 绑定、802.1X 认证、GSN 绑定、WEB 认证或者端口安全等安全应用模块所生成的合法用户信息(IP 或 IP+MAC)产生相应的 ARP 过滤信息，从而实现对网络中的非法 ARP 报文的过滤。

图 5-1



如上图所示，设备安全功能模块产生的合法用户信息(仅有 IP 或 IP + MAC)，ARP Check 功能使用这些信息用于检测端口下的所有的 ARP 报文中的 Sender IP 字段或<Sender IP, Sender MAC>是否满足合法用户信息表中的匹配关系，所有不在合法用户信息表中的 ARP 报文将被丢弃。

下文仅介绍 ARP Check 的相关内容。

协议规范

- RFC826：An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

5.2 典型应用

典型应用	场景描述
过滤网络上的非法ARP报文	网络上存在非法的用户，使用伪造的 ARP 报文进行攻击。

5.2.1 过滤网络上的非法ARP报文

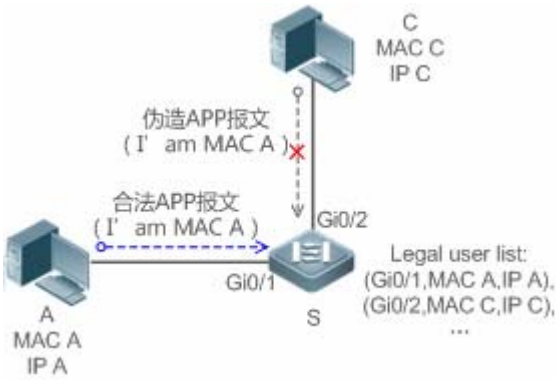
应用场景

检查来自非信任端口的 ARP 报文，过滤掉与 DHCP 服务器分配记录不匹配的 ARP 报文。

以下图为例，DHCP 客户端发送的 ARP 报文将被检查。

- 接收 ARP 报文的端口、ARP 报文的发送者 MAC 地址、ARP 报文的发送者 IP 地址必须与设备窥探的 DHCP 报文记录一致。

图 5-2



【注释】 S 为接入设备。
A、C 为用户 PC。

功能部属

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 监控。
- 设置接入设备 S 上所有下行端口为 DHCP 非信任端口。
- 在接入设备 S 上所有非信任端口上，开启 IP Source Guard 与 ARP Check 功能，实现 ARP 报文过滤。

5.3 功能详解

基本概念

↘ ARP Check 支持的安全功能模块

目前 ARP Check 支持的安全功能模块包括：

- 仅检测 IP 字段：端口安全的仅 IP 模式，Ip Source Guard 手工配置的仅 IP 模式。

- 检测 IP+MAC 字段：端口安全的 IP + MAC 绑定模式，全局 IP + MAC 绑定功能，802.1x IP 授权功能，IP Source Guard 功能，GSN 绑定功能，WEB 认证功能。

ARP-Check 两种模式

ARP-Check 有 2 种模式：打开和关闭，默认为关闭。

10. 打开模式

ARP Check 功能根据如下模块提供的 IP/IP+MAC 信息对 ARP 报文的合法性进行检测。

- 全局 IP + MAC 绑定
- 802.1X 的 IP 授权
- IP Source Guard
- GSN 绑定
- 端口安全
- WEB 认证
- 端口安全 IP+Mac 或 IP 绑定

⚠ 如果端口上仅开启 ARP-Check 功能，而没有开启上述模块提供合法用户信息，将导致来自这个端口的所有 ARP 报文被丢弃。

⚠ 当接口开启 arp-check 功能时，如果接口同时启用了 vrrp 功能，对于接口的实地址和虚地址都能当网关，需要配置放行接口实 ip 地址和 vrrp ip 地址，否则可能导致发往网关的 arp 报文被过滤。

11. 关闭模式

不检查端口上的 ARP 报文。

功能特性

功能特性	作用
非法ARP报文过滤	检查 ARP 报文的源 IP 与源 MAC 字段，达到过滤非法 ARP 报文的目的。

5.3.1 非法ARP报文过滤

在指定端口上开启 ARP 检查功能，达到过滤非法 ARP 报文的目的。

工作原理

设备把端口下接收到 ARP 报文的源 IP 与源 MAC 字段，与设备安全数据库中的合法用户记录进行匹配。若匹配成功，则正常转发报文；若匹配失败，则丢弃报文。

相关配置

↘ 启动端口上的 ARP Check 功能

缺省情况下，端口上的 ARP Check 功能关闭。

使用 **arp-check** 命令可以启动端口上的 ARP Check 功能。

若无特殊需求，一般在接入设备的端口上设置该功能。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置ARP-Check	⚠ 必须配置。用于使能 ARP-Check 服务。	
	arp-check	设置 ARP Check 功能为打开模式

5.4.1 配置ARP-Check

配置效果

- 过滤非法的 ARP 报文。

注意事项

- 打开 ARP Check 检测功能可能会使相关安全应用的策略数/用户数减少。
- 无法在镜像的目的口上配置 arp-check 功能。
- 无法在 DHCP Snooping 信任端口上配置 ARP Check 功能。
- 无法在全局 IP+MAC 的例外口配置 ARP Check 功能。
- 只能在有线的交换口、2 层 AP 口、2 层封装子接口以及无线的 WLAN 下配置开启，有线接入是在接口模式下配置，无线接入是在无线安全配置模式下配置。

配置方法

↘ 启动 ARP Check 功能

- 必选配置。功能默认关闭，如果管理员希望使用 ARP Check 功能，需要输入命令开启。

检验方法

- 使用 **show run** 命令，查看功能配置。
- 使用 **show interface** { *interface-type interface-number* } **arp-check list** 命令，查看过滤表项。

相关命令

开启 ARP 报文检查

【命令格式】 **arp-check**

【参数说明】 -

【命令模式】 接口配置模式或者无线安全配置模式

【使用指导】 根据安全应用模块的合法用户信息产生相应的 ARP 过滤信息，实现对网络中的非法 ARP 报文的过滤。

配置举例

以下配置举例，仅介绍与 ARP Check 相关的配置。

配置接口 ARP Check 模式为打开模式。

【配置方法】

- 开启 ARP Check 功能，限制 ARP 报文必须符合 IP Source Guard、端口安全或是全局 IP+MAC 绑定的表项。

```
Ruijie# configure terminal
Ruijie(config)#address-bind 192.168.1.3 00D0.F800.0003
Ruijie(config)#address-bind install
Ruijie(config)#ip source binding 00D0.F800.0002 vlan 1 192.168.1.4 interface gigabitEthernet 0/1
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)#arp-check
Ruijie(config-if-GigabitEthernet 0/1)#ip verify source port-security
Ruijie(config-if-GigabitEthernet 0/1)#switchport port-security
Ruijie(config-if-GigabitEthernet 0/1)#switchport port-security binding 00D0.F800.0001 vlan 1
192.168.1.1
Ruijie(config-if-GigabitEthernet 0/1)#exit
Ruijie(config)#interface gigabitEthernet 0/4
Ruijie(config-if-GigabitEthernet 0/4)#switchport port-security
Ruijie(config-if-GigabitEthernet 0/4)#switchport port-security binding 192.168.1.5
Ruijie(config-if-GigabitEthernet 0/4)#arp-check
Ruijie(config-if-GigabitEthernet 0/4)#exit
Ruijie(config)#interface gigabitEthernet 0/5
Ruijie(config-if-GigabitEthernet 0/5)#arp-check
Ruijie(config-if-GigabitEthernet 0/5)#end
Ruijie# configure terminal
Ruijie(config)#wlan-config 1 RUIJIE-SSID
Ruijie(config-wlan)#end
Ruijie#conf
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#wlansec 1
```

```
Ruijie(config-wlansec)# ip verify source port-security
Ruijie(config-wlansec)#arp-check
Ruijie(config-wlansec)#end
Ruijie#conf
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# ip source binding 0026.c79f.6e4c vlan 1 172.168.131.1 wlan 1
```

【检验方法】 使用 **show interface arp-check list** 命令，可以查看接口下实际生效的 ARP Check 表项。

```
Ruijie# show interface arp-check list

INTERFACE               SENDER MAC          SENDER IP           POLICY SOURCE
----------------------- ------------------- ------------------- --------------------
GigabitEthernet 0/1     00d0.f800.0003      192.168.1.3         address-bind
GigabitEthernet 0/1     00d0.f800.0001      192.168.1.1         port-security
GigabitEthernet 0/1     00d0.f800.0002      192.168.1.4         DHCP snooping
GigabitEthernet 0/4     00d0.f800.0003      192.168.1.3         address-bind
GigabitEthernet 0/4                         192.168.1.5         port-security
GigabitEthernet 0/5     00d0.f800.0003      192.168.1.3         address-bind

Ruijie# show wlan arp-check list

INTERFACE               SENDER MAC          SENDER IP           POLICY SOURCE
----------------------- ------------------- ------------------- --------------------
Wlan 1                  0026.c79f.6e4c      172.168.131.1       DHCP snooping
```

常见配置错误

- 接口需要检查 ARP 报文，但是将接口的 ARP Check 模式设置为关闭模式，导致功能无法生效。

5.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看端口下实际生效的 ARP Check 表项。	**show interface** [*interface-type interface-number*] **arp-check list**

查看WLAN下实际生效的ARP Check表项。	**show wlan** [*wlan-id*] **arp-check list**

查看调试信息

无

6 防网关 ARP 欺骗

6.1 概述

防网关 ARP 欺骗可以通过在逻辑端口上检查 ARP 报文的源 IP 地址（指 ARP 报文 Sender IP 字段）是否为自己配置的网关 IP 地址有效的预防针对网关的 ARP 欺骗。防网关 ARP 欺骗功能用于保护针对网关的 ARP 欺骗。

下文仅介绍防网关 ARP 欺骗的相关内容。

协议规范

- RFC 826：Ethernet Address Resolution Protocol

6.2 典型应用

无。

6.3 功能详解

基本概念

ARP

地址解析协议，即 ARP（Address Resolution Protocol），是根据 IP 地址获取物理地址的一个 TCP/IP 协议。其功能是：主机将 ARP 请求广播到网络上的所有主机，并接收返回消息，确定目标 IP 地址的物理地址，同时将 IP 地址和硬件地址存入本机 ARP 缓存中，下次请求时直接查询 ARP 缓存。地址解析协议是建立在网络中各个主机互相信任的基础上的，网络上的主机可以自主发送 ARP 应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记录在本地的 ARP 缓存中，这样攻击者就可以向目标主机发送伪 ARP 应答报文，使目标主机发送的信息无法到达相应的主机或到达错误的主机，构成一个 ARP 欺骗。

网关的 ARP 欺骗

针对网关的 ARP 欺骗是指用户 A 发送 ARP 报文请求网关的 MAC 地址，这时处于同一 VLAN 的用户 B 也会收到该 ARP 报文，因此用户 B 可以发送 ARP 响应报文，将报文的源 IP 填为网关 IP，而源 MAC 填为自己的 MAC 地址。用户 A 收到该 ARP 响应后，就会认为用户 B 的机器就是网关，因此用户 A 通讯中发往网关的报文都将发往用户 B， 这样用户 A 的通讯实际上都被截取了，造成 ARP 欺骗的效果。

功能特性

功能特性	作用
防网关ARP欺骗	阻断伪造网关和内网服务器 ARP 欺骗报文，保证用户能正常上网

6.3.1 防网关ARP欺骗

工作原理

防网关 ARP 欺骗

防网关 ARP 欺骗可以通过在逻辑端口上检查 ARP 报文的源 IP 是否为自己配置的网关 IP 有效的预防针对网关的 ARP 欺骗。如果是，则将该报文丢弃，防止用户收到错误的 ARP 响应报文。如果不是，则不对该报文进行处理。这样只有交换机上连设备能够下发网关的 ARP 报文，其它 PC 发送的假冒网关 ARP 响应报文将被交换机过滤。

相关配置

配置防网关 ARP 欺骗地址

- 缺省情况下，没有防网关 ARP 欺骗地址配置。
- 通过 **anti-arp-spoofing ip** 命令配置防网关 ARP 欺骗地址

6.4 配置详解

配置项	配置建议 & 相关命令	
配置防网关ARP欺骗	⚠ 可选配置	
	anti-arp-spoofing ip	在逻辑端口下配置防网关 ARP 欺骗，网关 IP 地址为指定 IP。

6.4.1 配置防网关ARP欺骗

配置效果

启用防网关 ARP 欺骗功能

配置方法

配置防网关 ARP 欺骗

- 必须配置，启用防网关 ARP 欺骗功能。

检验方法

- 通过 **show run** 查看配置信息。
- 通过 **show anti-arp-spoofing** 显示所有防网关 arp 欺骗信息

相关命令

配置防网关 ARP 欺骗

【命令格式】 **anti-arp-spoofing ip** *ip-address*
【参数说明】 *ip-address*：网关 IP 地址
【命令模式】 无线安全配置模式
【使用指导】 -

配置举例

无。

6.5 监视与维护

查看运行情况

作用	命令
显示所有防网关 arp 欺骗信息	**show anti-arp-spoofing**

查看调试信息

无

7 全局 IP+MAC 绑定

7.1 概述

通过手动配置全局 IP 和 MAC 地址绑定功能，可以对输入的报文进行 IP 地址和 MAC 地址绑定关系的验证。如果将一个指定的 IP 地址和一个 MAC 地址绑定，则设备只接收源 IP 地址和 MAC 地址均匹配这个绑定地址的 IP 报文；否则该 IP 报文将被丢弃。

利用地址绑定这个特性，可以严格控制设备的输入源的合法性。需要注意的是，通过地址绑定控制交换机的输入，将优先于 802.1X、端口安全以及 ACL 生效

下文仅介绍全局 IP+MAC 绑定的相关内容。

协议规范

- 无

7.2 典型应用

典型应用	场景描述
全局IP+MAC地址绑定	仅指定 IP 的主机可以访问网络，主机在同一台设备下是可以移动的

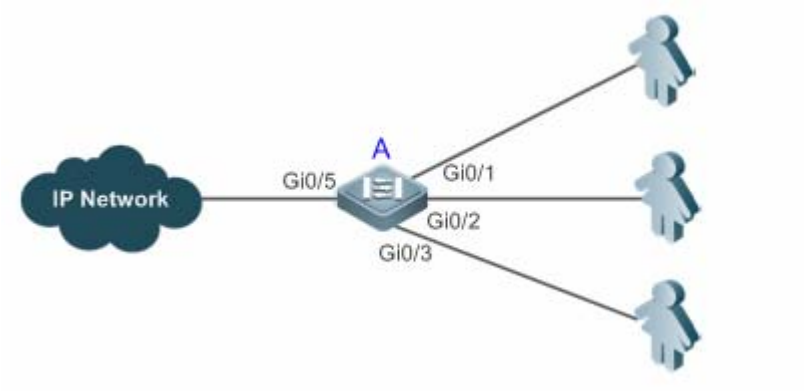
7.2.1 全局IP+MAC地址绑定

应用场景

为了方便管理，管理员为每台主机固定分配了一个 IP 地址。

- 仅指定 IP 的主机可以访问外部网络，防止非法主机盗用 IP。
- 主机可以在相同设备下可以自由移动。

图 7-1



【注释】 A 为接入设备。
User 为静态分配了 IP 地址的接入主机。
IP Network 为外部 IP 网络。

功能部属

- 手动配置全局 IP 和 MAC 地址绑定（本例列举 3 个用户）

用户	所属主机 MAC 地址	分配的 IP 地址
User1	00d0.3232.0001	192.168.1.10
User2	00d0.3232.0002	192.168.1.20
User3	00d0.3232.0003	192.168.1.30

- 全局使能 IP 和 MAC 地址绑定功能
- 将设备的上链口（本例为 Gi0/5 口）配置为例外口

7.3 功能详解

基本概念

↘ IPv6 地址绑定模式

IPv6 地址绑定模式包括兼容、宽松以及严格，默认为严格，针对 IPv4+MAC 绑定下的 IPv6 报文转发控制而言，不存在 IPv4+MAC 绑定时模式并不生效，所有 IPv4 报文和 IPv6 都可以放行，存在了 IPv4+MAC 绑定后模式生效，然后依据对应的转发规则控制 IPv4 和 IPv6 报文是否放行，转发规则如下表所示：

模式	IPv4 报文转发规则	IPv6 报文转发规则
严格	符合全局 IPv4+MAC 绑定条件的报文转发	符合 IPv6+MAC 绑定条件的报文转发(绑定由其他接入安全功能生成，比如端口安全、IPv6 Source Guard 等)

宽松	符合全局 IPv4+MAC 绑定条件的报文转发	如果存在 IPv6+MAC 的绑定那么符合绑定条件的报文转发（绑定由其他接入安全功能生成，比如端口安全、IPv6 Source Guard 等） 如果不存在 IPv6+MAC 的绑定，转发所有 IPv6 报文
兼容	符合全局 IPv4+MAC 绑定条件的报文转发	符合源 MAC 为全局 IPv4+MAC 绑定中的 MAC 地址的 IPV6 报文转发 符合全局 IPv6+MAC 绑定条件的报文转发(绑定由其他接入安全功能生成，比如端口安全、IPv6 Source Guard 等）

↘ 地址绑定例外端口

IP 地址和 MAC 地址绑定功能缺省对设备上的所有端口都生效，通过配置例外口的方式可以使绑定功能在部份端口上不生效。在应用中设备的上链端口的 IP 报文的绑定关系是不确定的，通常将设备的上链端口配置为例外口，此时上链端口则不进行 IP 地址与 MAC 地址的绑定检查。

功能特性

功能特性	作用
配置全局IP+MAC地址绑定	对 IPv4 报文或者 IPv6 报文进行转发控制
配置IPv6 地址绑定模式	改变 IPv6 报文的转发控制规则
配置地址绑定例外端口	全局地址绑定功能在对应端口上不生效

7.3.1 配置全局IP+MAC地址绑定

工作原理

配置 IP 和 MAC 地址绑定功能，可以对输入的报文进行 IP 地址和 MAC 地址绑定关系的验证。如果将一个指定的 IP 地址和一个 MAC 地址绑定，则设备只接收源 IP 地址和 MAC 地址均匹配这个绑定地址的 IP 报文；否则该 IP 报文将被丢弃。

相关配置

↘ 配置 IP+MAC 地址绑定

全局模式下，使用 **address-bind** 命令添加或者删除 IPv4+MAC 地址绑定。

↘ 配置使得 IP+MAC 地址绑定生效

全局模式下，使用 **address-bind install** 命令配置地址绑定功能生效，默认不生效。

7.3.2 配置IPv6 地址绑定模式

工作原理

存在全局 IPv4+MAC 地址绑定并且绑定开启的情况下，根据不同的模式控制 IPv6 报文的转发，模式包括严格、宽松或者兼容等。

相关配置

↘ 配置 IPv6 地址绑定模式

缺省情况下，地址绑定模式为严格。

使用 address-bind ipv6-mode 命令指定地址绑定模式。

7.3.3 配置地址绑定例外端口

工作原理

通过配置例外口的方式可以使绑定功能在部份端口上不生效。

相关配置

↘ 配置地址绑定例外端口

使用 **address-bind uplink** 命令可以配置例外端口，默认全部都是非例外端口。

7.4 配置详解

配置项	配置建议 & 相关命令	
配置全局IP+MAC地址绑定	⚠ 必须配置。用于生成地址绑定并开启绑定功能。	
	address-bind	配置生成全局 IPv4+MAC 地址绑定
	address-bind install	开启地址绑定功能
配置IPv6 地址绑定模式	⚠ 可选配置。用于改变 IPv6 地址绑定模式。	
	address-bind ipv6-mode	配置 IPv6 地址绑定模式
配置地址绑定例外端口	⚠ 可选配置。用于配置部分端口的地址绑定功能不生效。	
	address-bind uplink	配置地址绑定的例外端口

7.4.1 配置全局IP+MAC地址绑定

配置效果

- 生成全局 IPv4+MAC 地址绑定
- 开启地址绑定功能对 IPv4 或者 IPv6 报文进行转发控制

注意事项

- 如果执行 **address-bind install** 之后，没有配置 IP+MAC 绑定，则所有 IP+MAC 绑定功能不生效，所有报文可以通过。

配置方法

↘ 配置全局 IP+MAC 地址绑定

- 必须配置，全局配置模式下配置。

↘ 开启地址绑定功能

- 必须配置，全局配置模式下配置。

检验方法

使用 **show run** 或者 **show address-bind** 验证配置是否生效。

相关命令

↘ 配置全局 IP+MAC 地址绑定

【命令格式】 **address-bind** { *ip-address* | *ipv6-address* } *mac-address*

【参数说明】 *ip-address*：绑定的 IPv4 地址

ipv6-address：绑定的 IPv6 地址

mac-address：绑定的 MAC 地址

【命令模式】 全局配置模式

【使用指导】 配置 IP 地址和 MAC 地址的绑定关系

↘ 配置开启地址绑定功能

【命令格式】 **address-bind install**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 使全局 IP 和 MAC 地址绑定生效，控制 IPv4 或者 IPv6 报文的转发。

配置举例

↘ 配置全局 IP+MAC 地址绑定并使能地址绑定功能

【配置方法】
- 配置生成全局 IPv4+MAC 地址绑定
- 开启地址绑定功能

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001
Ruijie(config)# address-bind install
```

【检验方法】 查看设备上的全局 IP+MAC 地址绑定

```
Ruijie#show address-bind
Total Bind Addresses in System : 1
IP Address          Binding MAC Addr
---------------     -----------------
192.168.5.1         00d0.f800.0001
```

常见错误

- 无

7.4.2 配置IPv6 地址绑定模式

配置效果

- 改变 IPv6 地址绑定模式，IPv6 报文的转发规则发生变化。

注意事项

- 无

配置方法

↘ 配置 IPv6 地址绑定模式

- 可选配置，需要改变 IPv6 报文转发控制规则时来配置。

检验方法

- 使用 **show run** 验证配置是否生效。

相关命令

↘ 全局配置模式下配置 IPv6 地址绑定模式

【命令格式】 **address-bind ipv6-mode** { **compatible | loose | strict** }

【参数说明】 **compatible**：兼容模式

loose：宽松模式

strict：严格模式

【命令模式】 全局模式

【使用指导】 -

配置举例

↘ 配置 IPv6 地址绑定模式。

【配置方法】
- 配置全局 IP+MAC 地址绑定
- 开启地址绑定功能
- 配置 IPv6 地址绑定模式为兼容模式

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001
Ruijie(config)# address-bind install
Ruijie(config)# address-bind ipv6-mode compatible
```

【检验方法】 **show run** 查看设备上的配置

常见配置错误

- 无

7.4.3 配置地址绑定例外端口

配置效果

- 配置指定端口的地址绑定功能不生效，所有 IP 报文都可以转发

注意事项

- 只能在交换口或者 L2AP 口进行配置

配置方法

配置地址绑定例外端口

- 可选配置，全局配置模式下配置，需要特殊指定地址绑定功能不生效的端口时配置。

检验方法

使用 **show run** 或者 **show address-bind uplink** 验证配置是否生效。

相关命令

配置地址绑定例外端口

【命令格式】 **address-bind uplink** *interface-id*

【参数说明】 *interface-id*：交换口或 L2AP 口

【命令模式】 全局配置模式

【使用指导】 -

配置举例

配置地址绑定例外端口

【配置方法】
- 配置生成全局 IPv4+MAC 地址绑定
- 开启地址绑定功能
- 配置地址绑定例外端口

```
Ruijie# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# address-bind 192.168.5.1 00d0.f800.0001
Ruijie(config)# address-bind install
Ruijie(config)# address-bind uplink GigabitEthernet 0/1
```

【检验方法】 查看设备上的全局 IP+MAC 地址绑定

```
Ruijie#show address-bind
Total Bind Addresses in System : 1
IP Address          Binding MAC Addr
---------------     ----------------
192.168.5.1         00d0.f800.0001
Ruijie#show address-bind uplink
Port        State
----------  ---------
Gi0/1       Enabled
```

```
Default    Disabled
```

常见错误

- 无

7.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看设备上的 IP 地址与 MAC 地址绑定配置	**show address-bind**
查看设备上的例外口信息	**show address-bind uplink**

查看调试信息

无

8 DHCP Snooping

8.1 概述

DHCP Snooping：意为 DHCP 窥探，通过对 Client 和服务器之间的 DHCP 交互报文进行窥探实现对用户 IP 地址使用情况的记录和监控，同时还可以过滤非法 DHCP 报文，包括客户端的请求报文和服务端的响应报文。DHCP Snooping 记录生成的用户数据表项可以为 IP Source Guard 等安全应用提供服务。

下文仅介绍 DHCP Snooping 的相关内容。

协议规范

- RFC2131：Dynamic Host Configuration Protocol
- RFC2132：DHCP Options and BOOTP Vendor Extensions

8.2 典型应用

典型应用	场景描述
DHCP服务欺骗攻击防范	在网络上存在多个 DHCP 服务器，限制 DHCP 客户端只能从合法的 DHCP 服务获取网络配置参数。
DHCP报文泛洪攻击防范	在网络上存在恶意用户，频繁的发送 DHCP 请求报文。
伪造DHCP报文攻击防范	在网络上存在恶意用户，发送伪造的 DHCP 请求报文，比如 DHCP-Release 报文。
IP/MAC欺骗攻击防范	在网络上存在恶意用户，发送伪造的 IP 报文，如篡改了报文的源地址字段。
用户私设IP限制	在网络上存在用户，不按规定从 DHCP 服务器获取 IP 地址，私设 IP 地址。
ARP入侵检测	在网络上存在恶意用户，伪造 ARP 响应报文，意图拦截正常用户之间通信的报文。

8.2.1 DHCP服务欺骗攻击防范

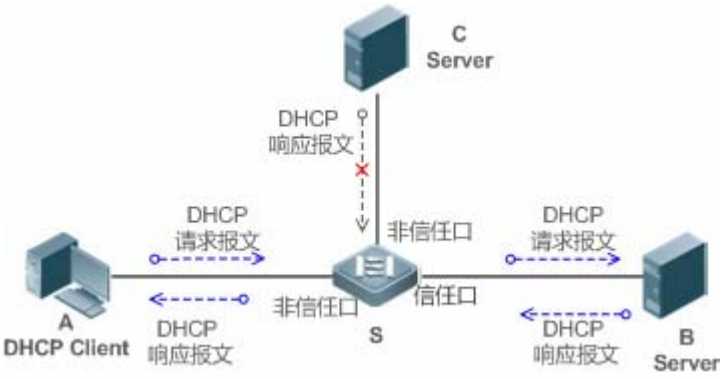
应用场景

在网络中可能存在多个 DHCP 服务器，需要保证用户 PC 只能从控制范围内的 DHCP 服务器获取网络配置参数。

以下图为例，DHCP 客户端仅与可信 DHCP 服务器通信。

- DHCP 客户端的请求报文只会传输到可信任的 DHCP 服务器。
- 只有可信任 DHCP 服务器的响应报文才会传输给客户端。

图 8-1



【注释】 S 为接入设备。

A 为用户 PC。

B 为控制范围内的 DHCP 服务器。

C 为不受控的 DHCP 服务器。

功能部署

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 报文监控。
- 设置接入设备 S 链接 DHCP 服务器 B 的端口为 DHCP TRUST 口，实现响应报文的转发。
- 设置接入设备 S 的其余端口为 DHCP UNTRUST 口，实现响应报文的过滤。

8.2.2 DHCP报文泛洪攻击防范

应用场景

在网络中可能存在恶意 DHCP 客户，高速率的发送 DHCP 请求报文，造成合法用户无法获得 IP、接入设备高负荷运行甚至瘫痪。需要保证网络系统运行稳定。

应用 DHCP 报文限速，DHCP 客户端仅能以低于规定的速率发送 DHCP 请求报文。

- DHCP 客户端的请求报文发送速率低于规定阀值。
- 超出限定的报文被丢弃。
- 开启 DHCP Snooping 与 ARP 模块的联动，删除不存在用户的用户表项。

功能部署

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 监控。
- 限制 UNTRUST 口的 DHCP 报文发送速率。
- 启动与 ARP 模块的联动，检测用户是否在线。

8.2.3 伪造DHCP报文攻击防范

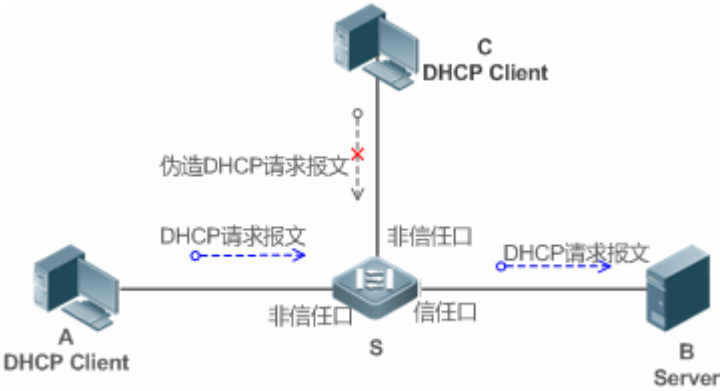
应用场景

在网络中可能存在恶意用户，伪造 DHCP 请求报文，一方面消耗了服务器的可用 IP，另一方面有可能抢夺合法用户的 IP。需要过滤掉接入网络上的非法 DHCP 报文。

以下图为例，DHCP 客户端发送的 DHCP 请求报文将被检查。

- DHCP 客户端的请求报文的源 MAC 字段与 DHCP 报文的客户硬件地址字段必须匹配。
- 客户端的 Release 报文与 Decline 报文必须与 Snooping 内部数据库的记录匹配。

图 8-2



【注释】 S 为接入设备。
A、C 为用户 PC。
B 为控制范围内的 DHCP 服务器。

功能部署

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 监控。
- 设置接入设备 S 链接 DHCP 服务器 B 的端口为 DHCP TRUST 口，实现响应报文的转发。
- 设置接入设备 S 的其余端口为 DHCP UNTRUST 口，实现 DHCP 报文的过滤。
- 在接入设备 S 上，所有 UNTRUST 口设置 DHCP 源 MAC 检查，过滤非法的 DHCP 报文。

8.2.4 IP/MAC欺骗攻击防范

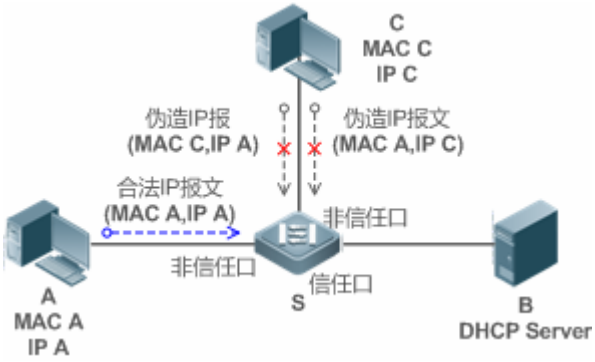
应用场景

检查来自 UNTRUST 口的 IP 报文，可以仅检查 IP 字段，也可以检查 IP+MAC 字段，过滤掉伪造的 IP 报文。

以下图为例，DHCP 客户端发送的 IP 报文将被检查。

- IP 报文的源地址字段必须和 DHCP 分配的 IP 地址匹配。
- 二层报文的源 MAC 字段必须和客户端 DHCP 请求报文中的客户硬件地址匹配。

图 8-3



【注释】 S 为接入设备。
A、C 为用户 PC。
B 为控制范围内的 DHCP 服务器。

功能部署

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 监控。
- 设置接入设备 S 上所有下行端口为 DHCP UNTRUST 口。
- 在接入设备 S 上，开启 IP Source Gourd 功能，实现 IP 报文过滤。
- 在接入设备 S 上，设置 IP Source Gourd 的匹配模式为 IP+MAC，实现对 IP 报文 MAC 字段与 IP 字段的检查。

8.2.5 用户私设IP限制

应用场景

检查来自 UNTRUST 口的 IP 报文，检查报文源地址是否和 DHCP 分配的地址一致。

若 IP 报文的源地址、连接端口、二层源 MAC 端口，与设备窥探的 DHCP 服务器分配记录不匹配，则丢弃报文。

该场景下设备的工作过程与上图一致。

功能部署

- 同场景“IP/MAC 欺骗攻击防范”。

8.2.6 ARP入侵检测

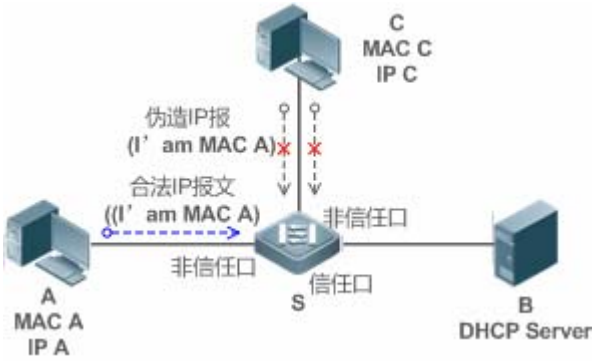
应用场景

检查来自 UNTRUST 口的 ARP 报文，过滤掉与 DHCP 服务器分配记录不匹配的 ARP 报文。

以下图为例，DHCP 客户端发送的 ARP 报文将被检查。

- 接收 ARP 报文的端口、报文的二层 MAC 地址、ARP 报文的发送者硬件地址必须与设备窥探的 DHCP 报文记录一致。

图 8-4



【注释】 S 为接入设备。
A、C 为用户 PC。
B 为控制范围内的 DHCP 服务器。

功能部署

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 监控。
- 设置接入设备 S 上所有下行端口为 DHCP UNTRUST 口。
- 在接入设备 S 上所有 UNTRUST 口上，开启 IP Source Guard 和 ARP Check 功能，实现 ARP 报文过滤。

⚠ 上述所有安全控制功能仅对 DHCP UNTRUST 口生效。

8.3 功能详解

基本概念

↘ DHCP 请求报文

DHCP 客户端发往 DHCP 服务器的报文。包括 DHCP-DISCOVER 报文、DHCP-REQUEST 报文、DHCP-DECLINE 报文、DHCP-RELEASE 报文及 DHCP-INFORM 报文。

DHCP 应答报文

DHCP 服务器发往 DHCP 客户端的报文。包括 DHCP-OFFER 报文、DHCP-ACK 报文及 DHCP-NAK 报文。

DHCP Snooping TRUST 口

由于 DHCP 获取 IP 的交互报文是使用广播的形式，从而存在着非法的 DHCP 服务影响用户正常 IP 的获取，更有甚者通过非法的 DHCP 服务欺骗窃取用户信息的现象，为了防止非法的 DHCP 服务的问题，DHCP Snooping 把端口分为两种类型，TRUST 口和 UNTRUST 口，设备只转发 TRUST 口收到的 DHCP 应答报文，而丢弃所有来自 UNTRUST 口的 DHCP 应答报文，这样我们把合法的 DHCP Server 连接的端口设置为 TRUST 口，则其他口为 UNTRUST 口，就可以实现对非法 DHCP Server 的屏蔽。

在交换机设备上，所有交换口或者 2 层 AP 口默认均为 UNTRUST 口，可以配置指定 TRUST 口。在无线 AP（Access Point）设备上，所有 WLAN 均为 UNTRUST 口，不可配置指定 TRUST 口；当 AP 为 FAT 模式时，所有 2 层交换口和 2 层封装子接口默认均为 UNTRUST 口，可以配置指定为 TRUST 口；当 AP 为 FIT 模式时，所有 2 层交换口默认为 UNTRUST 口，可以配置指定为 TRUST 口，所有 2 层封装子接口均为 TRUST 口，不可以配置指定为 UNTRUST 口。在无线 AC（Access Control）设备上，所有 WLAN 均为 UNTRUST 口，不可配置指定为 TRUST 口，所有交换口和 2 层 AP 口默认为 UNTRUST 口，可以配置指定为 TRUST 口。

DHCP Snooping 报文抑制

在对个别用户禁用 DHCP 报文的情况下，需要屏蔽用户设备发出的任何 DHCP 报文，那么我们可以在 UNTRUST 口配置 DHCP 报文抑制功能，过滤掉该端口收到的所有 DHCP 报文。

基于 VLAN 的 DHCP Snooping

DHCP Snooping 功能生效是以 VLAN 为单位的，默认情况下打开 DHCP Snooping 功能，会在当前设备上的所有 VLAN 上使能 DHCP Snooping 功能，可以通过配置灵活的控制 DHCP Snooping 生效的 VLAN。

DHCP Snooping 绑定数据库

在 DHCP 环境的网络里经常会出现用户随意设置静态 IP 地址的问题，用户随意设置的 IP 地址不但使网络难以维护，而且会导致一些合法的使用 DHCP 获取 IP 的用户因为冲突而无法正常使用网络，DHCP Snooping 通过窥探 Client 和 Server 之间交互的报文，把用户获取到的 IP 信息以及用户 MAC、VID、PORT、租约时间等信息组成用户记录表项，从而形成 DHCP Snooping 的用户数据库，配合 ARP 检测功能或 ARP CHECK 功能的使用，进而达到控制用户合法使用 IP 地址的目的。

DHCP Snooping 速率限制

DHCP Snooping 对 DHCP 报文的速率限制可以选择通过 NFPP 的速率限制命令配置，NFPP 的配置请查看 NFPP 配置指导。

DHCP Option82 选项

DHCP Option82 选项又称为 DHCP 中继代理信息选项（Relay Agent Information Option），是 DHCP 报文中的一个选项。因为其选项编号为 82，故通常被简称为 Option82 选项。Option82 选项是为了增强 DHCP 服务器的安全性，改善 IP 地址的分配策略而提出的一种 DHCP 选项。该选项功能通常配置在网络接入设备的 DHCP 中继服务组件中，如 DHCP Relay、DHCP Snooping。该选项对 DHCP 客户端透明，由 DHCP 中继组件实现选项的添加与剥离。

非法 DHCP 报文

DHCP Snooping 通过对经过设备的 DHCP 报文进行合法性检查，丢弃不合法的 DHCP 报文，记录用户信息并生成 DHCP Snooping 绑定数据库供其他功能（如：ARP 检测功能）查询使用。以下几种类型的报文被认为是非法的 DHCP 报文

- UNTRUST 口收到的 DHCP 应答报文，包括 DHCPACK、DHCPNACK、DHCPOFFER 等。
- UNTRUST 口收到的带有网关信息【giaddr】的 DHCP request 报文。
- 打开 mac 校验时，源 MAC 与 DHCP 报文携带的【chaddr】字段值为不同的报文。
- DHCPRELEASE 报文中的用户在 DHCP Snooping 绑定数据库中存在，但是 DHCPRELEASE 报文的 UNTRUST 口和保存在 DHCP Snooping 绑定数据库中的 UNTRUST 口不一致，那么这个 DHCPRELEASE 报文是非法的。
- DHCP 报文格式不正确或是不完整的报文。

功能特性

功能特性	作用
过滤非法DHCP报文	对交互的 DHCP 报文进行合法性检查，丢弃那些非法报文（非法报文的介绍见上节的介绍）。仅向 TRUST 口转发合法的请求报文。
建立Binding数据库	窥探 DHCP 客户端与服务器的交互，生成 DHCP Snooping Binding 数据库，为其他安全过滤模块提供依据。

8.3.1 过滤非法DHCP报文

对来自 UNTRUST 口的 DHCP 报文进行合法性检查。依据上节“基本概念”中介绍的非法报文类型，进行过滤。控制报文的传播范围，防止恶意用户欺骗。

工作原理

窥探过程中，检查报文的接收端口、报文字段，达到过滤报文目的；修改报文的目的端口，达到控制报文传播范围的目的。

↘ 端口检查

接收到 DHCP 报文时，设备先判断接收报文的端口是否为 DHCP TRUST 口。若是 TRUST 口，跳过合法性检查、Binding 记录生成阶段，直接进入报文转发阶段。若是 UNTRUST 口，需要进行合法性检查。

↘ 检查报文封装及长度是否完整

设备检查报文是否为 UDP 报文，且目的端口为 67 或 68。检查数据包的实际长度与协议中的长度字段是否匹配。

↘ 检查 DHCP 报文字段及报文类型是否正确

依据上节“基本概念”中介绍的非法报文类型，先检查报文的【giaddr】、【chaddr】字段，再依据报文的实际类型，检查该类型特有的限制条件是否满足。

相关配置

↘ 启动全局 DHCP Snooping 功能

缺省情况下，DHCP Snooping 功能关闭。

使用 **ip dhcp snooping** 命令可以启动设备的 DHCP Snooping 功能。

必须首先开启全局 DHCP Snooping 功能，才能进一步在不同 VLAN 上启停 DHCP Snooping 功能。

↘ 设置 VLAN 上的 DHCP Snooping 功能

缺省情况下，当全局 DHCP Snooping 功能生效时，DHCP Snooping 功能对所有 VLAN 生效。

使用[**no**] **ip dhcp snooping vlan** 命令可以配置 DHCP Snooping 在某个 VLAN 上生效，或将该 VLAN 从 DHCP Snooping 生效的 VLAN 范围中去除。命令参数的取值范围为实际的 VLAN 编号范围。

↘ 配置 DHCP 源 MAC 检查功能

缺省情况下，设备不对报文的二层源 MAC 及 DHCP 报文的【chaddr】字段进行校验。

使用 **ip dhcp snooping verify mac-address** 命令，设备就会对 UNTRUST 口送上来的 DHCP Request 报文进行源 MAC 和【chaddr】字段的 MAC 地址进行校验检查，丢弃 MAC 值不相同的 DHCP 请求报文。

8.3.2 建立Binding数据库

窥探 DHCP 客户端与 DHCP 服务器的交互报文，依据合法 DHCP 报文信息，生成 DHCP Snooping Binding 表项。所有这些表项作为合法用户的信息表，提供给设备的其他安全模块使用，作为网络报文过滤的依据。

工作原理

窥探过程中，依据 DHCP 报文的类型，不断更新 Binding 数据库。

↘ 生成 Binding 记录

窥探到 TRUST 口上的 DHCPACK 报文时，提取出报文中的客户端 IP 地址、客户端 MAC 地址、租约时间字段，结合设备记录的客户端所在端口 ID（有线接口索引或者无线 WLAN ID）、客户端所属 VLAN，生成一条 Binding 记录。

↘ 删除 Binding 记录

记录的租约时间到期；或是窥探到客户端发送的合法 DHCP-RELEASE/DHCP-DECLINE 报文时；或是接收到来自 TRUST 口的 NAK 报文时；或是用户使用 clear 命令主动删除 Binding 记录时，删除对应的 Binding 记录。

相关配置

无需额外配置，只需要开启 DHCP Snooping 功能即可。

8.4 配置详解

配置项	配置建议 & 相关命令	
配置DHCP Snooping基本功能	⚠ 必选配置。用于建立 DHCP Snooping 服务。	
	ip dhcp snooping	启动 DHCP Snooping 功能
	ip dhcp snooping suppression	启动 DHCP 报文抑制功能
	ip dhcp snooping vlan	开关指定 VLAN 的 DHCP Snooping 功能
	ip dhcp snooping verify mac-address	配置 DHCP 源 MAC 检查功能
	ip dhcp snooping database write-delay	启动 DHCP Snooping Binding 记录定时保存功能
	ip dhcp snooping database write-to-flash	手动保存 DHCP Snooping Binding 记录
	renew ip dhcp snooping database	手动将保存在 flash 中的用户记录导入到 DHCP Snooping Binding 数据库中
	ip dhcp snooping trust	配置 DHCP Snooping TRUST 口
	ip dhcp snooping bootp	启动支持 bootp 功能
	ip dhcp snooping check-giaddr	启动 DHCP Snooping 支持处理 Relay 请求报文功能
	ip dhcp snooping clear-broadcast-flag	启动清除广播标志位功能
配置Option82 选项	⚠ 可选配置。用于优化 DHCP 服务器地址分配。	
	ip dhcp snooping Information option	在 DHCP 请求报文中加入 Option82 选项功能
	ip dhcp snooping information option format remote-id	设置 Option82 选项的子选项 remote-id 为自定义字符串的功能
	ip dhcp snooping vlan information option format-type circuit-id string	设置 Option82 选项的子选项 circuit-id 为自定义字符串的功能

8.4.1 配置DHCP Snooping基本功能

配置效果

- 开启 DHCP Snooping 服务。
- 生成 DHCP Snooping Binding 数据库。
- 控制 DHCP 报文的传播范围。
- 过滤非法的 DHCP 报文。

注意事项

- 设备连接可信 DHCP 服务器的端口必须设置成 DHCP TRUST 口。

- DHCP Snooping 生效的端口可以是有线的交换口、2 层 AP 口或者 2 层封装子接口，也可以是无线的 WLAN，端口下的配置分为接口模式下的配置以及无线安全模式下的配置。

配置方法

启动全局 DHCP Snooping 服务

- 必须配置。
- 若无特殊要求，应在接入设备上配置该功能。

按 VLAN 开关 DHCP Snooping 功能

- 如果有些 VLAN 不需要 DHCP Snooping 功能，可以关闭。
- 若无特殊要求，应在接入设备上配置该功能。

配置 DHCP TRUST 口

- 必须配置。
- 将设备连接可信 DHCP 服务器的端口设置成 DHCP TRUST 口。

启动 DHCP 源 MAC 地址检查

- 如果要求 DHCP 请求报文的【chaddr】字段必须与数据包的二层源 MAC 地址匹配，则必须配置。
- 若无特殊要求，应在接入设备的所有 UNTRUST 口上开启该功能。

启动 DHCP Snooping Binding 记录定时保存功能

- 如果要求设备重启后，之前窥探的 DHCP Snooping Binding 记录任然能够生效，需要启动该功能。
- 若无特殊要求，应在接入设备上开启该功能。

启动支持 BOOTP 功能

- 可选配置。
- 若无特殊要求，应在接入设备上开启该功能。

启动 DHCP Snooping 支持处理 Relay 请求报文功能

- 可选配置。
- 若无特殊要求，应在接入设备上开启该功能。

启动 DHCP Snooping 清除广播标志位功能

- 可选配置。
- 若无特殊要求，应在大二层无线场景下开启该功能。

检验方法

用户配置设备使用 DHCP 协议获取网络配置参数。

- 检查设备上的 DHCP Snooping Binding 数据库是否生成相应用户记录。

相关命令

配置打开和关闭 DHCP Snooping

【命令格式】 [**no**] **ip dhcp snooping**

【参数说明】 -。

【命令模式】 全局配置模式

【使用指导】 打开 DHCP Snooping 全局功能后，可以使用 **show ip dhcp snooping** 命令查看 DHCP Snooping 功能是否打开。

配置 DHCP Snooping 功能生效的 VLAN

【命令格式】 [**no**] **ip dhcp snooping vlan** { *vlan-rng* | {*vlan-min* [*vlan-max*] } }

【参数说明】 *vlan-rng*：DHCP Snooping 功能生效的 vlan 范围。

vlan-min：DHCP Snooping 功能生效的 vlan 下限。

vlan-max：DHCP Snooping 功能生效的 vlan 上限。

【命令模式】 全局配置模式

【使用指导】 通过配置该命令，将在指定的 VLAN 内打开 DHCP Snooping 功能，也可关闭指定 VLAN 的 DHCP Snooping 功能。该功能必须在打开 DHCP Snooping 全局开关的基础上生效。

配置端口 DHCP 报文抑制

【命令格式】 [**no**] **ip dhcp snooping suppression**

【参数说明】 -

【命令模式】 接口配置模式或者无线安全配置模式

【使用指导】 通过配置该命令，可拒绝该端口下所有 DHCP 请求报文，即禁止该端口下的所有用户通过 DHCP 方式申请地址。

配置 DHCP 源 MAC 检查功能

【命令格式】 [**no**] **ip dhcp snooping verify mac-address**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 源 MAC 地址检验功能，是对 DHCP CLIENT 发出的请求报文，检查链路层头部 MAC 地址和 DHCP 报文中的 CLIENT MAC 字段是否相同。源 MAC 地址检验失败时，报文将被丢弃。

配置定时写 DHCP Snooping 数据库信息到 flash

【命令格式】 [**no**] **ip dhcp snooping database write-delay** [*time*]

【参数说明】 *time*：两次将 DHCP Snooping 数据库写入 FLASH 的时间间隔。

【命令模式】 全局配置模式

【使用指导】 通过配置该命令，可以将 DHCP Snooping 数据库写入 FLASH 文件。可以防止设备重新启动后，用户信息丢

失，导致用户必须重新获取 IP 地址，才可以正常通讯。

手动把 DHCP Snooping 数据库信息写到 flash

【命令格式】 **ip dhcp snooping database write-to-flash**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 通过执行此命令，可以实时将 DHCP Snooping 数据库中动态用户信息写入 FLASH 文件。

手动地把当前 flash 中的信息导入 DHCP Snooping 绑定数据库

【命令格式】 **renew ip dhcp snooping database**
【参数说明】 -
【命令模式】 特权模式
【使用指导】 通过执行此命令，可以实时将 flash 文件信息导入 DHCP Snooping 数据库中。

配置端口为 TRUST 口

【命令格式】 [**no**] **ip dhcp snooping trust**
【参数说明】 -
【命令模式】 接口配置模式
【使用指导】 通过配置该命令，将连接合法 DHCP 服务器的端口配置为 TRUST 口。TRUST 端口收到的 DHCP 响应报文被正常转发，UNTRUST 端口收到的 DHCP 响应报文将被丢弃。

配置支持 BOOTP 功能

【命令格式】 [**no**] **ip dhcp snooping bootp**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 通过配置该命令，可支持 BOOTP 协议。

配置启动 DHCP Snooping 支持处理 Relay 请求报文功能

【命令格式】 [**no**] **ip dhcp snooping check-giaddr**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 开启此功能后，不能部署使用 Relay 请求生成的 DHCP Snooping 绑定表项的业务，如 IP Source Guard/802.1x 认证等，否则可能导致用户无法上网。
开启此功能后，不能配置 ip dhcp snooping verify mac-address，否则 Relay 的 DHCP 请求报文会被丢弃，导致用户无法获取地址。

配置启动 DHCP Snooping 清除广播标志位功能

【命令格式】 [**no**] **ip dhcp snooping clear-broadcast-flag**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 开启此功能后，DHCP Snooping 对非 DHCP Relay 的请求报文进行广播标志位检查，若标志位有置上则清

除，收到对应响应报文时将标志位置上并且二三层目的地址设置为广播地址。

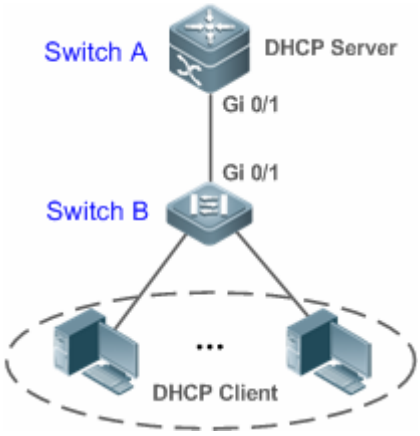
配置举例

以下配置举例，仅介绍与 DHCP Snooping 相关的配置。

DHCP 客户端用户通过合法 DHCP 服务器动态获取 IP 地址

【网络环境】

图 8-5



【配置方法】

- 在接入设备（本例为 Switch B）上开启 DHCP Snooping 功能
- 将上链口（本例为端口 Gi 0/1）设置为 TRUST 口。

B

```
B#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
B(config)#ip dhcp snooping
B(config)#interface gigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust
B(config-if-GigabitEthernet 0/1)#end
```

【检验方法】

确认 Switch B 的配置。

- 是否开启 DHCP Snooping 功能、配置的 DHCP Snooping TRUST 口是否为上链口。
- 查看 Switch B 的 DHCP Snooping 配置情况，关注点为 TRUST 口是否正确。

B

```
B#show running-config
!
ip dhcp snooping
!
interface GigabitEthernet 0/1
B#show ip dhcp snooping
Switch DHCP Snooping status                    :   ENABLE
DHCP Snooping Verification of hwaddr status    :   DISABLE
DHCP Snooping database write-delay time        :   0 seconds
DHCP Snooping option 82 status                 :   DISABLE
```

```
DHCP Snooping Support BOOTP bind status        :   DISABLE
Interface                      Trusted       Rate limit (pps)
-------------------------      -------       ----------------
GigabitEthernet 0/1            YES           unlimited
B#show ip dhcp snooping binding
Total number of bindings: 1
MacAddress         IpAddress       Lease(sec)   Type           VLAN  Interface
------------------ --------------- ------------ -------------- ----- --------------------
0013.2049.9014     172.16.1.2      86207        dhcp-snooping 1     GigabitEthernet 0/11
```

常见错误

- 没有将上链口设置为 DHCP TRUST 口。
- 在上链口上配置了其他的接入安全选项，导致配置 DHCP TRUST 口失败。

8.4.2 配置Option82 选项

配置效果

- 让 DHCP 服务器在进行地址分配时，能够获取更多的信息，做出更佳的地址分配。
- 选项对 DHCP 客户端透明，客户端无法感知到功能的开启或关闭。

注意事项

- 与 DHCP Relay 的 Option82 选项功能互斥。

配置方法

- 如果需要施加此项优化，则应该执行此配置项。
- 若无特殊要求，应在已经开启 DHCP Snooping 的接入设备上开启该功能。

检验方法

查看 DHCP Snooping 的配置选项，确保功能成功开启。

相关命令

↘ **在 DHCP 请求报文中加入 Option82 选项功能**

【命令格式】 [**no**] **ip dhcp snooping Information option** [**standard-format**]

【参数说明】 **standard-format**：Option82 选项使用标准格式。

【命令模式】 全局配置模式

【使用指导】 通过配置该命令，将在 DHCP 请求报文中添加 Option82 选项信息，DHCP 服务器根据 Option82 选项信息进行地址分配。

设置 Option82 选项的子选项 remote-id 为自定义字符串

【命令格式】 [**no**] **ip dhcp snooping information option format remote-id** { **string** *ASCII-string* | **hostname**}

【参数说明】 **string** *ASCII-string*：Option82 选项 remote-id 扩展格式内容为自定义字符串。

hostname：Option82 选项 remote-id 扩展格式内容为主机名。

【配置模式】 全局配置模式

【使用指导】 通过配置该命令，设置 DHCP 请求报文中添加 Option82 选项的 remote-id 子选项为自定义内容，DHCP 服务器根据 Option82 选项信息进行地址分配。

设置 Option82 选项的子选项 circuit -id 为自定义字符串

【命令格式】 [**no**] **ip dhcp snooping vlan** *vlan-id* **information option format-type circuit-id string** *ascii-string*

【参数说明】 *vlan-id*：DHCP 请求报文所在 VLAN。

ascii-string：Circuit ID 要填充的用户自定义的内容。

【配置模式】 接口配置模式

【使用指导】 通过配置该命令，设置 DHCP 请求报文中添加 Option82 选项的 circuit-id 子选项为自定义内容，DHCP 服务器根据 Option82 选项信息进行地址分配。

配置举例

下面是配置在 DHCP 请求报文中加入 Option82 选项功能的例子。

【配置方法】
- 配置 DHCP Snooping 基本功能。略
- 开启添加 Option82 选项功能。

B

```
Ruijie# configure terminal
Ruijie(config)# ip dhcp snooping information option
Ruijie(config)# end
```

【检验方法】 查看 DHCP Snooping 配置。

B

```
B#show ip dhcp snooping
Switch DHCP Snooping  status                    :   ENABLE
DHCP Snooping  Verification of hwaddr status    :   DISABLE
DHCP Snooping database write-delay time         :   0 seconds
DHCP Snooping option 82 status                  :   ENABLE
DHCP Snooping Support bootp bind status         :   DISABLE
Interface                    Trusted       Rate limit (pps)
------------------------     -------       ----------------
```

```
GigabitEthernet 0/1             YES           unlimited
```

常见配置错误

- 无

8.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清空 DHCP Snooping 数据库动态用户信息。	**clear ip dhcp snooping binding** [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id* | **wlan** *wlan-id*]

查看运行情况

作用	命令
显示 DHCP Snooping	**show ip dhcp snooping**
显示 DHCP Snooping 数据库信息	**show ip dhcp snooping binding**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 DHCP Snooping 事件的调试开关。	**debug snooping ipv4 event**
关闭 DHCP Snooping 事件的调试开关。	**no debug snooping ipv4 event**
打开 DHCP Snooping 报文的调试开关。	**debug snooping ipv4 packet**
关闭 DHCP Snooping 报文的调试开关。	**no debug snooping ipv4 packet**

9 IP Source Guard

9.1 概述

通过 IP Source Guard 绑定功能，可以通过硬件对 IP 报文进行过滤，从而保证只有 IP 报文硬件过滤数据库中存在对应信息的用户才能正常使用网络，防止了用户私设 IP 地址及伪造 IP 报文。下文仅介绍 IP Source Guard 的相关内容。

协议规范

- 无

9.2 典型应用

典型应用	场景描述
IP/MAC欺骗攻击防范	在网络环境中，防止用户私设 IP 地址或防止用户伪造 IP 报文进行攻击。

9.2.1 IP/MAC欺骗攻击防范

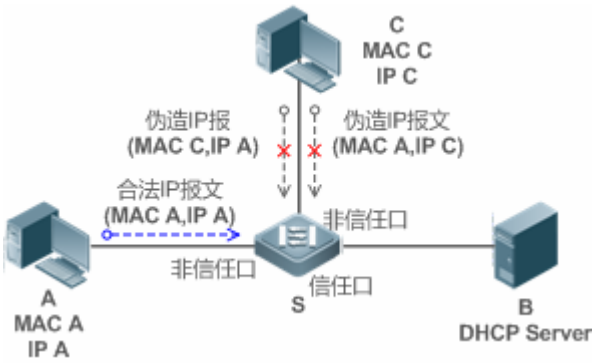
应用场景

检查来自非 DHCP 信任口的 IP 报文，可以仅检查 IP 字段，也可以检查 IP+MAC 字段，过滤掉伪造的 IP 报文。

以下图为例，DHCP 客户端发送的 IP 报文将被检查。

- IP 报文的源地址字段必须和 DHCP 分配的 IP 地址匹配。
- 二层报文的源 MAC 字段必须和客户端 DHCP 请求报文中的客户硬件地址匹配。

图 9-1



【注释】 S 为接入设备。

A、C 为用户 PC。

B 为控制范围内的 DHCP 服务器。

功能部署

- 在接入设备 S 上开启 DHCP Snooping 服务，实现 DHCP 监控。
- 设置接入设备 S 上所有下行接口为 DHCP 非信任口。
- 在接入设备 S 上，开启 IP Source Guard 功能，实现 IP 报文过滤。
- 在接入设备 S 上，设置 IP Source Guard 的匹配模式为 IP+MAC，实现对 IP 报文 MAC 字段与 IP 字段的检查。

9.3 功能详解

基本概念

源 IP

用户 IP 报文的源 IP 地址字段。

源 MAC

用户二层报文的源 MAC 地址字段。

基于源 IP 的过滤

IP 报文的过滤策略，检查所有经过该接口的 IP 报文（DHCP 报文除外），仅对报文的源 IP 地址进行检测。IP Source Guard 的缺省过滤策略。

基于源 IP + 源 MAC 的过滤

IP 报文的过滤策略，会对所有 IP 报文的源 IP + 源 MAC 进行检查，仅允许绑定用户记录数据库中存在的用户报文通过。

绑定用户记录数据库

IP Source Guard 安全控制的依据。 目前，绑定用户记录数据库中数据来自两个方面。一方面数据来自 DHCP Snooping 绑定数据库，当启动 IP Source Guard 功能后，DHCP Snooping 数据库信息将同步到 IP Source Guard 的绑定用户数据库中，这样 IP Source Guard 就可以在打开 DHCP Snooping 功能的设备上对客户端的 IP 报文进行严格过滤。另一方面数据来自用户的静态配置。

例外 VLAN

默认情况下端口开启 IP Source Guard 后，会对该端口包含的所有 VLAN 生效，用户可以指定例外 VLAN 不对该 VLAN 范围内的 IP 报文进行检查和过滤，即不受 IP Source Guard 的控制，每个端口最多可以指定 32 个例外 VLAN。

功能特性

功能特性	作用
检查报文源地址字段	对经过接口的 IP 报文进行基于源 IP 过滤，或是基于源 IP + 源 MAC 的过滤。

9.3.1 检查报文源地址字段

对经过端口的 IP 报文进行基于源 IP 过滤，或是基于源 IP + 源 MAC 的过滤。防止恶意用户伪造报文进行攻击。当用户不需要检查和过滤某 VLAN 范围内的 IP 报文时，可以指定例外 VLAN 对报文进行放行。

工作原理

打开 IP Source Guard 功能后，设备对经过端口的报文进行源地址检查，端口可以是有线接入的交换口、2 层 AP 口或者 2 层封装子接口，也可以是无线接入的 WLAN。只有源地址字段和 DHCP Snooping 生成的绑定用户记录集匹配，或是和管理员静态配置的用户集匹配的报文才能经过端口。匹配的方式有两种：

基于源 IP 地址过滤

只要报文的源 IP 字段属于绑定用户记录中的 IP 地址集合，就可以通过端口。

基于 IP+MAC 地址过滤

报文的二层源 MAC 与三层源 IP 必须和合法用户集中的某条记录完全匹配上，才能通过端口。

指定例外 VLAN

该 VLAN 范围的报文不被检查和过滤，直接通过端口。

相关配置

启动端口上的 IP Source Guard 功能

缺省情况下，端口上的 IP Source Guard 功能关闭。

使用 **ip verify source exclude-vlan** 命令可以启动或关闭端口上的 IP Source Guard 功能。

通常 IP Source Guard 功能需要 DHCP Snooping 功能的配合，因此，还需要启动 DHCP Snooping 功能。锐捷设备对启动 DHCP Snooping 功能的时机不做限制，用户可以在 IP Source Guard 启动之前或之后启动 DHCP Snooping。

配置静态 IP Source Guard 用户

缺省情况下，IP Source Guard 检查的合法用户集全部来自 DHCP Snooping 的绑定用户。

使用 **ip source binding** 命令可以添加额外的绑定用户记录。

端口上指定 IP Source Guard 的例外 VLAN

缺省情况下，IP Source Guard 对端口上包含的所有 VLAN 生效。

使用 **ip verify source** 命令可以指定例外 VLAN 不受 IP Source Guard 的控制。

与端口下的 IP Source Guard 配合使用，端口下必须先启动 IP Source Guard 才可以指定例外 VLAN，端口下关闭 IP Source Guard 后会自动清除指定的例外 VLAN。

端口可以是有线接入的交换口、2 层 AP 口或者 2 层封装子接口，也可以是无线接入的 WLAN。

9.4 配置详解

配置项	配置建议 & 相关命令	
配置IP Source Guard	必须配置。用于开启 IP Source Guard 服务。	
	ip verify source	启动端口上的 IP Source Guard 功能。
	ip source binding	配置静态绑定用户。
	Ip verify source exclude-vlan	端口上指定 IP Source Guard 的例外 VLAN

9.4.1 配置IP Source Guard

配置效果

- 对输入 IP 报文进行检查，过滤非法 IP 报文。

注意事项

- 打开 IP Source Guard 功能可能会影响 IP 报文的转发，一般情况下，该功能需要结合 DHCP Snooping 功能使用。
- 无法在 DHCP Snooping 信任端口上配置 IP Source Guard 功能。
- 无法在全局 IP+MAC 的例外口配置 IP Source Guard 功能。
- 只能在有线的交换口、2 层 AP 口、2 层封装子接口以及无线的 WLAN 下配置开启，有线接入是在接口模式下配置，无线接入是在无线安全配置模式下配置。

配置方法

- 开启 DHCP Snooping。
- 开启 IP Source Guard。

检验方法

使用设备提供的监控命令，查看 IP Source Guard 用户过滤表项。

相关命令

打开端口上的 IP Source Guard 功能

【命令格式】 **ip verify source** [**port-security**]

【参数说明】 **port-security**：配置 IP Source Guard 功能进行基于 IP+MAC 检测。

【命令模式】 接口模式或者无线安全配置模式

【使用指导】 通过该命令打开端口的 IP Source Guard 功能，可以对用户进行基于 IP 的检测，或者进行基于 IP+MAC 的检测。

在 IP 源地址绑定数据库中添加静态用户信息

【命令格式】 **ip source binding** *mac-address* **vlan** *vlan-id ip-address* **{interface** *interface-id* **| wlan** *wlan-id* **| ip-mac | ip-only }**

【参数说明】 *mac-address*：静态添加的用户的 MAC 地址。

vlan-id：静态添加的用户的 vlan id。

ip-address：静态添加的用户的 IP 地址。

interface-id：静态添加的用户所属的有线接口。

wlan-id：静态添加的用户所属的无线 WLAN

ip-mac：全局绑定的类型为 IP+MAC 绑定。

ip-only：全局绑定的类型为仅 IP 绑定。

【配置模式】 全局模式

【使用指导】 通过配置此命令可以允许部分用户通过 IP Source Guard 的检测，不需要通过 DHCP 方式进行统一控制。

接口上指定 IP Source Guard 的例外 VLAN

【命令格式】 **Ip verify source exclude-vlan** *vlan-id*

【参数说明】 *vlan-id*：不受接口上 IP Source Guard 控制的 vlan id。

【命令模式】 接口模式或者无线安全配置模式

【使用指导】 启动 IP Source Guard 的接口上，通过该命令可以控制该端口的某些 VLAN 不受 IP Source Guard 控制，这些 VLAN 范围内的 IP 报文不被检查和过滤而是直接放行。

配置举例

配置打开接口 1 的 IP Source Guard 功能。

【配置方法】

- 打开 DHCP Snooping 功能。略
- 开启 IP Source Guard。

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if-GigabitEthernet 0/1)# end
Ruijie(config)# wlansec 1
```

```
Ruijie(config-wlansec)# ip verify source port-security
Ruijie(config-wlansec)# end
```

【检验方法】 查看 IP Source Guard 用户过滤表项

```
Ruijie# show ip verify source
```

↘ 添加一个静态绑定用户。

【配置方法】

- 打开 DHCP Snooping 功能。略
- 开启 IP Source Guard。略
- 添加静态用户

```
Ruijie# configure terminal
Ruijie(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface GigabitEthernet 0/3
Ruijie(config)# end
```

【检验方法】 查看 IP Source Guard 用户过滤表项

```
Ruijie# show ip verify source
NO.    INTERFACE                FilterType FilterStatus           IPADDRESS       MACADDRESS
VLAN TYPE
-----  ------------------------ ---------- ---------------------  --------------- --------------
---- -------------
1      GigabitEthernet 0/3      UNSET      Inactive-restrict-off  192.168.4.243
00d0.f801.0101 1    Static
2      GigabitEthernet 0/1      IP-ONLY    Active                 Deny-All
3      WLAN 1                   IP-MAC     Active                 Deny-All
```

↘ 配置打开端口的 IP Source Guard 功能并指定例外 VLAN。

【配置方法】

- 打开 DHCP Snooping 功能。略
- 开启 IP Source Guard。

```
Ruijie(config)# interface GigabitEthernet 0/1
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source
Ruijie(config-if-GigabitEthernet 0/1)# ip verify source exclude-vlan 1
Ruijie(config-if)# end
Ruijie(config)# wlansec 1
Ruijie(config-wlansec)# ip verify source
Ruijie(config-wlansec)# ip verify source exclude-vlan 1
Ruijie(config-wlansec)# end
```

【检验方法】 查看接口上指定的例外 VLAN

```
Ruijie# show run
```

常见配置错误

- 在 DHCP Snooping 信任口开启 IP Source Guard。
- 未启动 IP Source Guard 就指定例外 VLAN。

9.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 IP Source Guard 用户过滤表项。	**show ip verify source** [**interface** *interface-id* | **wlan** *wlan-id*]
查看 IP 源地址绑定数据库的信息	**show ip source binding**

查看调试信息

无

10 DNS SNOOPING

10.1 概述

DNS Snooping：意为 DNS 窥探，通过对 Client 和服务器之间的 DNS 交互报文进行窥探实现对域名与 IP 地址对应表项的记录，同时还可以过滤非法 DNS 报文，包括客户端的请求报文和服务端的响应报文。

DNS Snooping提供如下功能：

■ 免认证URL，基于域名的直通地址设置。

下文仅介绍 DNS Snooping 的相关内容。

协议规范

- RFC1034：DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC1035：DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

10.2 典型应用

典型应用	场景描述
免认证URL	设备开启web认证功能，未认证用户无法正常访问网络内容。通过配置免认证URL，可以放行用户特定 URL 的流量。

10.2.1 免认证URL

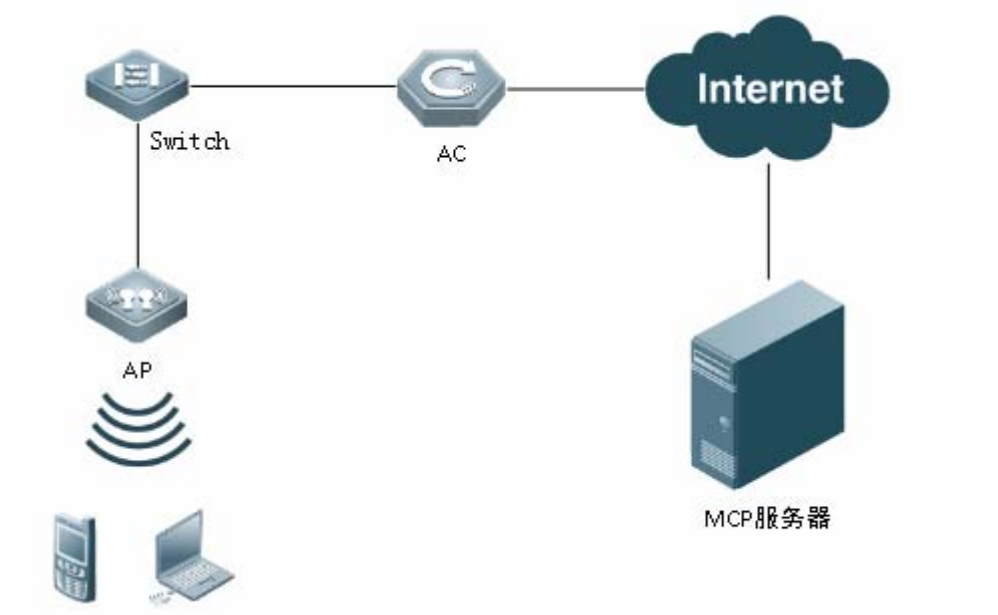
应用场景

如下图所示，设备与 MCP 服务器进行联动，使用微信关注认证完成对下联终端认证前网络访问权限的控制及认证。

认证前，终端仅能访问微信内容，通过关注微信公众号可通过认证。

认证后，终端的网络访问权限不受限制。

图 10-1



【注释】 Switch：交换机。
AC：无线控制器。
AP：无线接入点。
MCP：云服务器。

功能部属

- 在设备上开启微信关注认证功能，与 MCP 服务器进行联动。

10.3 功能详解

基本概念

↘ 免认证 APP

用户通过认证前就具有网络访问权限的应用，可以是微信软件，也可以是新浪微博等其它 APP。

↘ 免认证 URL

设备开启 web 认证功能，未认证用户无法正常访问网络内容。通过配置免认证 URL，可以放行用户特定 URL 的流量。

↘ CWMP 协议

CWMP（CPE WAN Management Protocol，CPE 广域网管理协议）是由 DSL（Digital Subscriber's Line，数字用户线路）论坛发起开发的技术规范之一，编号为 TR-069，所以又被称为 TR-069 协议。它提供了对下一代网络中家庭网络设备进行管理配置的通用框架、消息规范、管理方法和数据模型。

TR-069 协议实现十分复杂，对 APP 认证来说，TR-069 提供了设备与 MCP 服务器进行通信的网络通道。

功能特性

功能特性	作用
免认证URL	设备开启 web 认证功能，未认证用户无法正常访问网络内容。通过配置免认证 URL，可以放行用户特定 URL 的流量。

10.3.1 免认证URL

设备上配置免认证 URL，可以对未认证用户放行指定 URL 流量。

工作原理

设备上开启 web 认证功能，未认证用户无法正常访问网络内容。配置免认证 URL 后，设备检测到未认证用户的流量符合 URL 特征，会放行这部分流量，用户不通过认证便可以使用特定 URL。

10.4 配置详解

配置项	配置建议 & 相关命令	
配置免认证URL	⚠ 必须配置。基于全局配置免认证 APP。	
	free-url	配置免认证 URL，目前支持微信、新浪 APP 和 iphone 特定 APP 及指定 URL。
	ip dns snooping enable	开启 DNS 嗅探功能

10.4.1 配置免认证URL

配置效果

- 配置免认证 URL，可以对未认证用户放行指定 URL 流量。

注意事项

- 开启 web 认证的前提下，配置免认证 URL 才有实际效果。

配置方法

↘ 开启 DNS 嗅探功能

- 必须配置。

- 在设备上开启 DNS 嗅探功能。

【命令格式】 **ip dns snooping enable**
【参数说明】 -
【缺省配置】 开启
【命令模式】 全局配置模式
【使用指导】 使用该命令开启 DNS 嗅探功能

配置免认证 URL

- 必须配置。
- 在设备上配置免认证 URL。

【命令格式】 **free-url** { **weixin | sina | iphone | url** *url* }
【参数说明】 **weixin**：微信
sina：新浪 APP
iphone：iphone 特定 APP
url：指定的 url
【缺省配置】 缺省无配置
【命令模式】 全局配置模式
【使用指导】 免认证 URL 可以同时开启多个

检验方法

- 通过 **show free-url** 查看配置结果。
- 设备上开启 web 认证时，在未认证的终端上检查是否可以正常使用免认证 URL

配置举例

在设备上配置微信为免认证 URL

【配置方法】
- 进入全局配置模式。
- 配置微信为免认证 URL。

设备

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#ip dns snooping enable
Ruijie(config)# free-url weixin
Ruijie(config)# free-url *.baidu.com
Ruijie(config)#exit
```

【检验方法】 通过 **show free-url** 命令查看免认证 URL 信息。

设备

```
Ruijie(config)#show free-url
```

```
Total number of domain name   : 4

Total number of ip address    : 11


====================== free-url domain name table ========================

Host                    type

*.qpic.cn               weixin

*.weixin.qq.com         weixin

weixin.qq.com           weixin

*.baidu.com             url

==========================================================================


========================= free-url ip table ==============================

Host                    type    Address                         TTL(sec)

*.weixin.qq.com         weixin  61.151.224.41                   2118

                                140.207.135.125                 2118

                                140.207.54.47                   2118

*.qpic.cn               weixin  140.206.160.234                 2118

                                183.61.49.180                   151

                                101.226.129.204                 554

                                14.17.52.136                    16

weixin.qq.com           weixin  14.17.42.45                     800

*.baidu.com             url     115.239.210.246                 19

                                115.239.211.235                 2286

                                115.239.210.14                  284

==========================================================================
```

常见错误

- 无。

10.5 监视与维护

清除各类信息

无。

查看运行情况

作用	命令
查看免认证 URL 情况	**show free-url**
清除免认证 URL 信息	**clear free-url**

查看调试信息

输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 DNS SNOOPING 调试开关。	**debug dns-snooping**

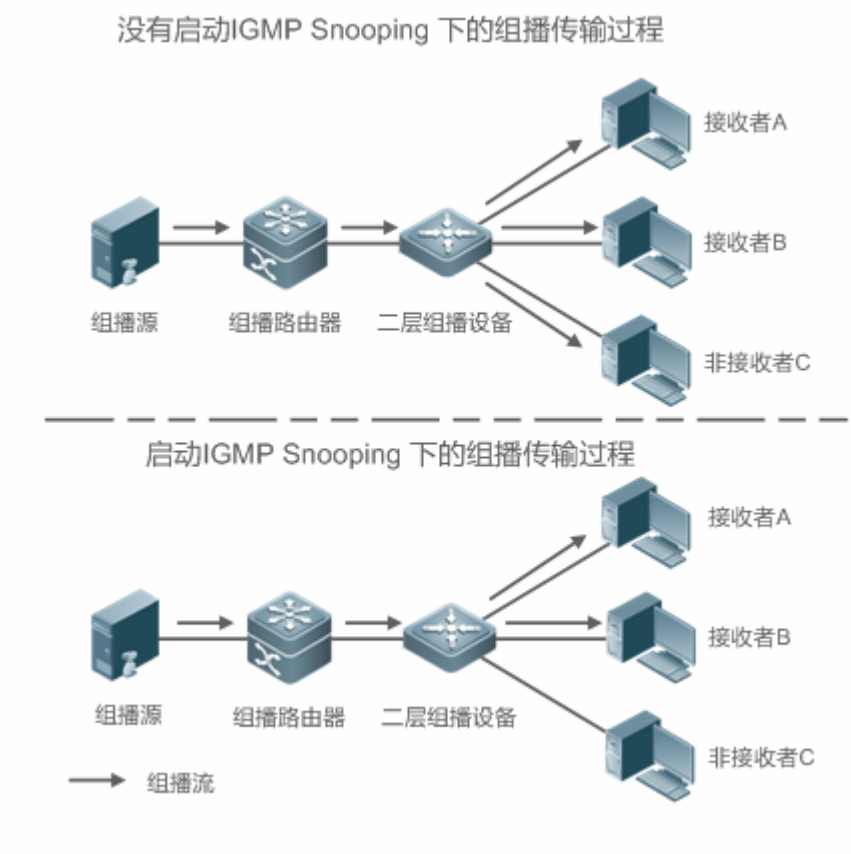
11 IGMP Snooping

11.1 概述

IGMP Snooping （Internet Group Management Protocol Snooping，组播侦听者发现协议窥探）是运行在 VLAN 上的 IP 组播窥探机制，用于管理和控制 IP 组播流在 VLAN 内的转发，实现二层组播功能。

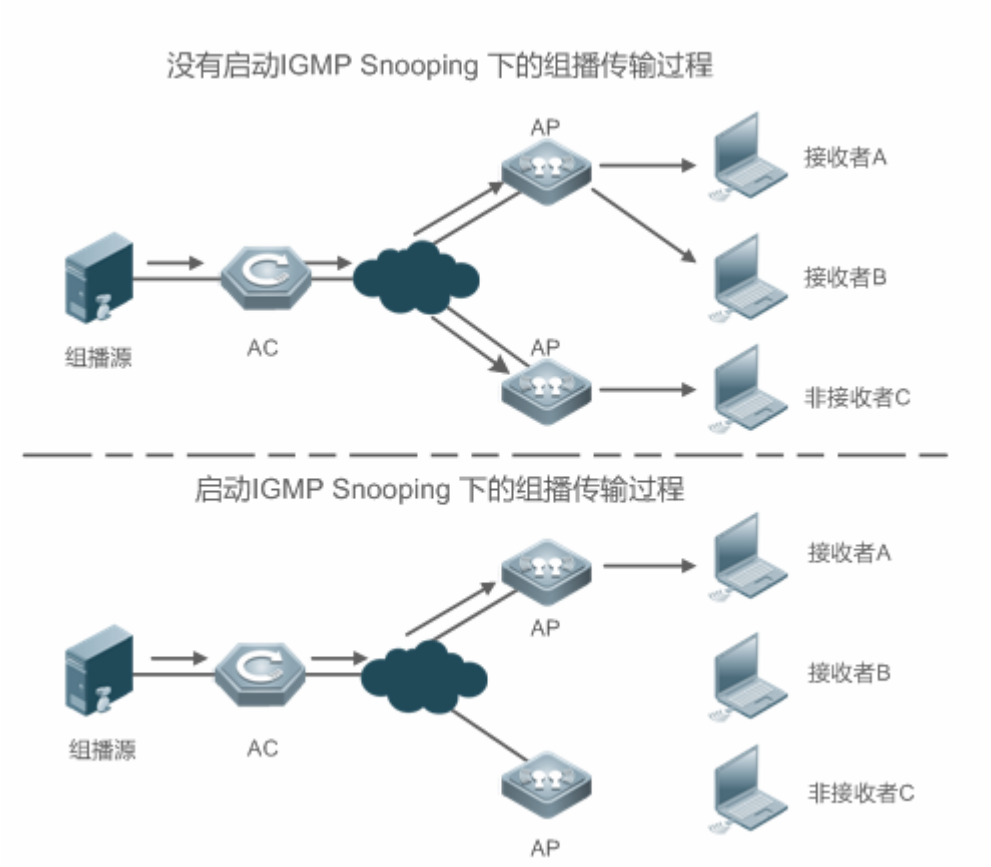
如下图所示，当二层组播设备没有运行 IGMP Snooping 时，IP 组播报文在 VLAN 内被广播；当二层组播设备运行了 IGMP Snooping 后，IP 组播报文只发给组成员接收者。

图 11-1 IP 组播流在 VLAN 内的转发（二层组播设备启动 IGMP Snooping 前后的对比）



如下图所示，在无线组播环境中，当无线设备没有运行 IGMP Snooping 时，组播数据报文在 AC 上 VLAN 内被广播，在 AP 上往所有的无线口广播；当无线 AC 和 AP 都运行了 IGMP Snooping 后，已知组播组的组播数据报文不会被广播，而是会精确转发给特定的接收者。

图 11-2 IP 组播流在 VLAN 内的转发(无线设备 AC、AP 启用 IGMP Snooping 前后对比)



协议规范

- RFC4541：Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

11.2 典型应用

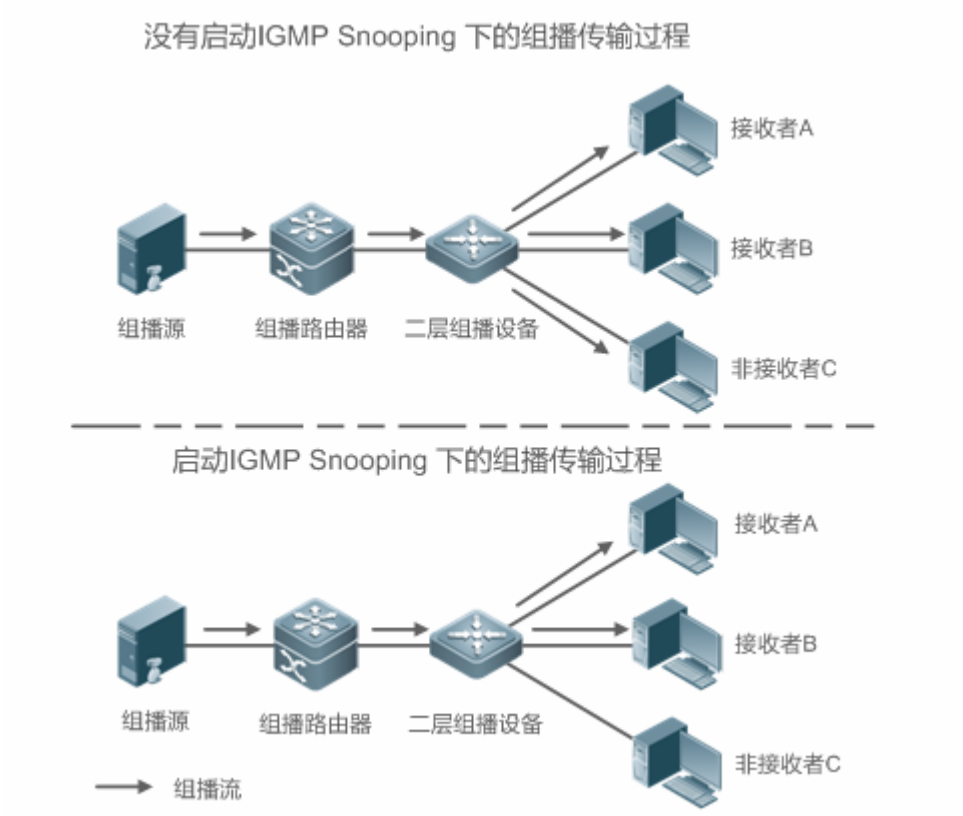
典型应用	场景描述
二层组播控制	二层组播精确转发，避免组播报文在二层泛洪。
组播转单播	实现 AP 与 STA 间组播报文转单播发送

11.2.1 二层组播控制

应用场景

组播报文需要通过二层交换机设备转发给用户，如下图所示，在未启用二层组播控制的情况下，报文是通过泛洪发送给所有的用户，即使没有该组播接收需求的用户也会接收到该组播流。当二层组播设备运行了 IGMP Snooping，进行二层组播控制后， IP 组播组的组播数据报文不会在 VLAN 内被广播，而是发给指定的接收者。

图 11-3 二层组播控制（组播 VLAN）



功能部属

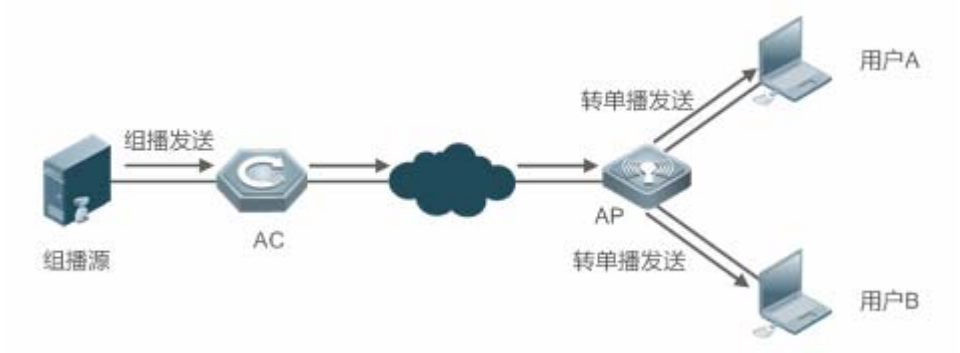
配置 IGMP Snooping 基本功能

11.2.2 组播转单播

应用场景

在未配置组播转单播功能时，报文通过组播的方式从 AP 发往 STA，由于目前无线网络中，对组播报文没有确认重传机制，导致比较严重的丢包，影响无线组播在视频点播等应用中的体验，为了降低丢包率，增强用户体验，无线组播在 AP 与 STA 之间采用组播转单播的方式进行传输。

图 11-4 组播转单播



功能部属

配置组播转单播功能

只有无线组播场景支持该功能

11.3 功能详解

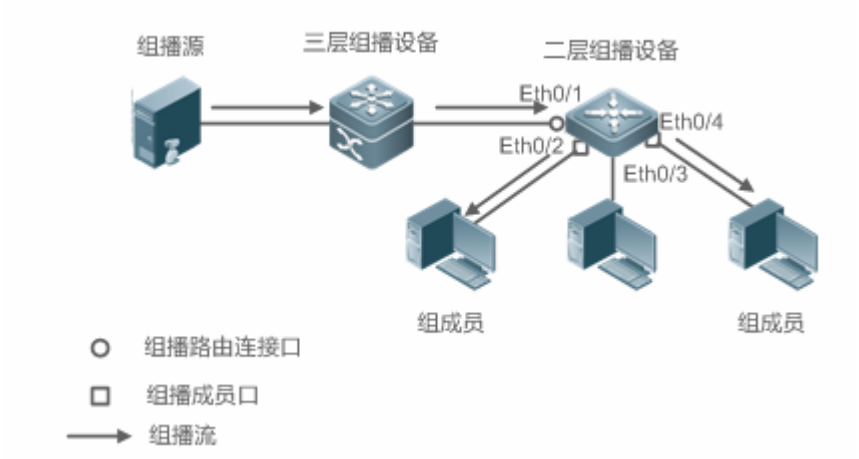
基本概念

路由连接口、成员口

IGMP Snooping 功能是基于 VLAN 进行的，相关的端口也是指 VLAN 内部的成员口。

运行 IGMP Snooping 的设备将 VLAN 内的接口标识为路由连接口或成员口，从而能够管理和控制 IP 组播流在 VLAN 内的转发。如下图所示，在二层组播设备上运行 IGMP Snooping，组播流从路由连接口进入，从成员口发出。

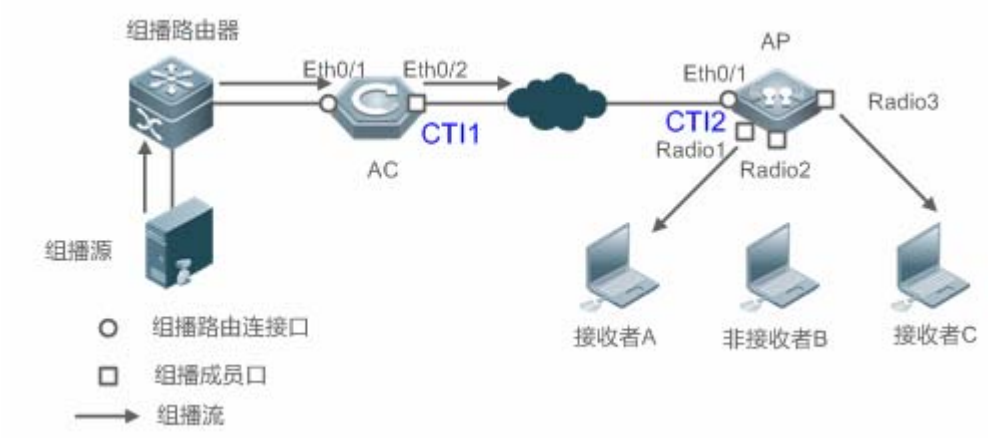
图 11-5 IGMP Snooping 的两类端口



- 路由连接口（Multicast Router Port）：二层组播设备上连接组播路由器（三层组播设备）的端口，指示组播源的方向。通过监听 IGMP 报文，二层组播设备可以自动发现并维护动态路由连接口。也允许用户配置静态路由连接口。
- 成员口(Member Port)：二层组播设备上连接组成员主机的端口，指示组成员的方向。又称侦听者端口(Listener Port)。通过监听 IGMP 报文，二层组播设备可以自动发现并维护动态成员口。也允许用户配置静态成员口。

由于无线设备同常见的有线设备相比较带有无线接口，而且无线设备 AC 与 AP 之间的通信是通过建立 CAPWAP 隧道通信的，AC 与 AP 建立 CAPWAP 隧道之后，分别在 AC 与 AP 上虚拟了 CTI1 和 CTI2 接口进行通信。结合下图说明无线 AC 与 AP 上的路由连接口与组成员口。

图 11-6 无线环境中两类端口



- 路由连接口(Multicast Router Port)：AC 设备接收到上游组播路由器(三层组播设备)发送过来的 PIM Hello 或者 IGMP Query 报文，形成了路由连接口 Eth0/1；AP 设备接收到 AC 设备转发下来的 PIM Hello 或者 IGMP Query 报文，也形成了路由连接口 CTI2。
- 组成员口(Member Port)：又称侦听者端口(Listener Port)，表示设备上连接组播组成员的端口，如 AP 设备上的 Radio1 和 Radio3 无线口接收到无线用户接收者发送过来的 Report 报文，就将相应无线口学习成为组成员端口；AC 设备上的虚拟接口 CTI1 接收到 AP 设备转发过来的 Report 报文，也学习成为组成员端口。

IGMP Snooping 转发表项

运行 IGMP Snooping 的设备按照 IGMP Snooping 转发表项转发 IP 组播报文。

IGMP Snooping 转发表项中包含如下信息：源地址（S）、组地址（G）、VLAN 号（VLAN_id）、路由连接口、成员口。表示：符合（S,G,VLAN_id）特征的报文，应该从路由连接口进入、从成员口发出。一个 IGMP Snooping 转发表项用一组（S,G,VLAN_id）来标识。

通过 **show ip igmp snooping gda-table** 命令查看 IGMP Snooping 转发表项。

```
Ruijie# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC  //动态成员口
  S: STATIC   //静态成员口
  M: MROUTE   //路由连接口，不区分静态或动态
```

```
(*, 233.3.6.29, 1):    //(源地址任意，组地址 233.3.6.29，VLAN1)
  VLAN(1) 3 OPORTS:
    GigabitEthernet 0/3(S)
    GigabitEthernet 0/2(M)
    GigabitEthernet 0/1(D)
    caPWAP-Tunnel 0/1(D)    // CAPWAP 隧道口
(*, 233.3.6.30, 1):    //(源地址任意，组地址 233.3.6.30，VLAN1)
  VLAN(1) 2 OPORTS:
    GigabitEthernet 0/2(M)
    GigabitEthernet 0/1(D)

(*,239.1.1.1, 1):  //(源地址任意， 组地址 239.1.1.1,VLAN 1)
    VLAN(1) 1 OPORTS:
        dot11radio 1/0.1 (D)  // 无线接口
```

功能特性

功能特性	作用
监听IGMP报文	发现并识别路由连接口和成员口，从而建立并维护 IGMP Snooping 转发表项。
IGMP Snooping工作模式	为用户 VLAN 提供独立组播服务或公共组播服务。
IGMP查询器	在没有三层组播设备的网络中，二层组播设备自己充当 IGMP 查询器。
组播转单播功能	实现 AP 与 STA 之间组播报文转单播发送
优化组播无线环境配置	忽略查询报文重置端口定时器功能

11.3.1 监听IGMP报文

运行 IGMP Snooping 的设备通过对收到的 IGMP 报文进行分析，发现并识别路由连接口和成员口，从而建立并维护 IGMP Snooping 转发表项。

工作原理

运行 IGMP Snooping 的设备可以识别并处理如下几类 IGMP 报文。

Query 报文

IGMP 查询者周期性发送普遍组 Query 报文。当 IGMP 查询者收到 Leave 报文时，发送指定组 Query 报文。

运行 IGMP Snooping 的设备在收到 Query 报文时，在此 VLAN 内执行如下动作：

- 将 IGMP 查询报文向所有端口（除该报文的接收端口）转发出去。
- 如果收到 IGMP 查询报文的端口是动态路由连接口，则重置其老化定时器。如果定时器超时，则该端口不再作为动态路由连接口。
- 如果收到 IGMP 查询报文的端口不是路由连接口，则将其作为动态路由连接口，并启动其老化定时器。如果定时器超时，则该端口不再作为动态路由连接口。
- 如果是普遍组查询报文,则对所有动态成员口重置其老化定时器。如果定时器超时，则该端口不再作为任意组的动态成员口。默认情况下采用 IGMP 查询报文携带最大响应时间作为老化定时器的超时时间，如果配置了“查询报文最大响应时间”，则使用“查询报文最大响应时间”作为老化定时器的超时时间。
- 如果是指定组查询报文，则对指定组的动态成员口重置其老化定时器。如果定时器超时，则该端口不再作为指定组的动态成员口。默认情况下采用 IGMP 查询报文携带最大响应时间作为老化定时器的超时时间，如果配置了“查询报文最大响应时间”，则使用“查询报文最大响应时间”作为老化定时器的超时时间。
- 如果配置关闭“动态学习路由连接口”功能，则 IGMP Snooping 不会学习动态路由连接口。

Report 报文

当组成员主机收到 Query 报文后，会应答 Report 报文。如果主机要加入某个组，也会主动发送 Report 报文。

锐捷产品对 IGMPv3 版本的 Report 报文，只对组信息部分进行处理，不支持对携带的源信息处理。

运行 IGMP Snooping 的设备在收到 Report 报文时，在此 VLAN 内执行如下动作：

- 将 Report 报文从所有路由连接口转发出去。如果设备上启动了“Report 报文抑制”功能，则在一个 IGMP 查询周期内，只会将每组收到的第一个 Report 报文转发出去。
- 如果收到 Report 报文的端口是动态成员口，则重置其老化定时器。如果定时器超时，则该端口不再作为指定组的动态成员口。
- 如果收到 Report 报文的端口不是成员口，则将其作为动态成员口，并启动其老化定时器。如果定时器超时，则该端口不再作为指定组的动态成员口。

Leave 报文

如果主机要离开某个组，会主动发送 Leave 报文。

运行 IGMP Snooping 的设备在收到 Leave 报文时，在此 VLAN 内执行如下动作：

- 将 Leave 报文从所有路由连接口转发出去。
- 如果收到 Leave 报文的端口是动态成员口，且配置了“快速离开”，端口将立即从指定组的 IGMP Snooping 转发表项中删除，该端口不再作为指定组的动态成员口。
- 如果收到 Leave 报文的端口是动态成员口，且未配置“快速离开”，则该端口状态保持不变

相关配置

配置静态路由连接口

使用 **ip igmp snooping vlan mrouter interface** 命令，可静态配置接口为路由连接口。

配置静态成员口

使用 **ip igmp snooping vlan static interface** 命令，可静态配置接口为成员口。

启动 Report 报文抑制功能

缺省未启用 Report 报文抑制功能

使用 **ip igmp snooping suppression enable** 命令，可配置报文抑制功能。

启用 Report 报文抑制功 能后，则在一个 IGMP 查询周期内，只会将每组收到的第一个 Report 报文转发出去。转发的 Report 报文的源 MAC 地址将替换成设备本身自己的源 MAC 地址。

配置快速离开功能

缺省未启用快速离开功能

使用 **ip igmp snooping fast-leave enable** 命令，可配置快速离开功能。

配置动态路由连接口学习功能

缺省启用动态路由连接口学习功能

使用 **no ip igmp snooping mrouter learn pim-dvmrp** 命令，可配置关闭动态路由连接口学习功能。

使用 **no ip igmp snooping vlan** *vid* **mrouter learn pim-dvmrp** 命令，可配置关闭指定 VLAN 的动态路由连接口学习功能。

配置动态路由连接口的老化定时器

缺省老化时间为 300 秒

端口收到 Query 报文时，启动或重置动态路由连接口的老化定时器，如果没有配置老化定时器的时间，将使用 Query 报文携带的最长响应时间做为动态路由连接口的老化时间。

使用 **ip igmp snooping dyn-mr-aging-time** 命令，可配置动态路由连接口的老化时间。

配置动态成员口的老化定时器

缺省老化时间为 260 秒

设备收到 Query 报文时，重置动态成员口的老化定时器，老化时间为 Query 报文携带的最长响应时间。

端口收到 Report 报文时，启动或重置动态成员口的老化定时器，老化时间为动态成员口老化时间。

使用 **ip igmp snooping host-aging-time** 命令，可配置动态成员口的老化时间。

配置查询报文最大响应时间

缺省无配置，使用查询报文携带的最大响应时间

使用 **ip igmp snooping query-max-response-time** 命令，可配置查询报文最大响应时间。

11.3.2 IGMP Snooping工作模式

运行 IGMP Snooping 的设备在 IVGL 模式，为用户 VLAN 提供独立组播服务。

工作原理

↘ IVGL（Independent VLAN Group Learning）

在 IVGL 模式下，运行 IGMP Snooping 的设备为每一个用户 VLAN 提供独立组播服务。

独立组播服务：组播流只能在所属 VLAN 内转发，用户主机只能在所属 VLAN 内申请组播流。

相关配置

↘ 启动 IGMP Snooping，选择工作模式

缺省未启动 IGMP Snooping。

使用 **ip igmp snooping** 命令，启动 IGMP Snooping，且运行 IVGL 模式。

11.3.3 IGMP查询器

在一个存在三层组播设备的网络中，由三层组播设备充当 IGMP 查询器。二层组播设备只需要监听 IGMP 报文，即可建立并维护转发表项，实现二层组播。

在一个没有三层组播设备的网络中，无法由三层组播设备充当 IGMP 查询器。为了使二层组播设备能够监听 IGMP 报文，必须在二层设备上配置 IGMP 查询器功能。二层组播设备即要充当 IGMP 查询器，又要监听 IGMP 报文，才能建立并维护转发表项，实现二层组播。

工作原理

IGMP 查询器功能由二层设备扮演 IGMP 路由查询的角色，定时发送 IGMP 查询报文，并对用户应答的 IGMP Report 报文进行侦听维护，建立二层组播的转发表项。IGMP 查询发送的查询报文的相关参数可由用户通过配置进行调整。

当设备接收到 PIM、DVMRP 协议报文时，认为网络中存在组播路由设备，为了避免影响组播路由设备的 IGMP 路由功能，设备的查询器功能将处于失效状态，由网络中的组播路由设备充当 IGMP 查询器功能。

当设备接收到其它设备的 IGMP 查询报文时，将进行 IGMP 查询器的竞选。

↘ 启动查询器

用户可配置在指定 VLAN 或所有 VLAN 上启用查询器功能。

全局查询器功能启用的情况下，指定 VLAN 的查询器功能才能生效。

指定查询器运行的 IGMP 版本

指定查询器发送的查询报文所使用的 IGMP 版本，可配置为 IGMPv1 或 IGMPv2 版本。

配置查询器的源 IP

配置查询器发送的查询报文所携带的源 IP 地址，可基于 VLAN 配置查询器发送的查询报文的源 IP 地址。

未配置查询器源 IP 的情况下，查询器功能不会生效。

配置查询器的查询间隔

配置全局查询器发送的查询报文的时间间隔，可基于 VLAN 配置不同 VLAN 的查询器的查询间隔。

配置查询报文的最大响应时间

配置查询器发送的查询报文中携带的最大响应时间，由于 IGMPv1 版本的协议不支持报文携带最大响应时间，所有该配置对于查询器运行 IGMPv1 版本时不生效。同时可基于不同 VLAN 的查询器配置不同的最大响应时间。

配置查询器的老化时间

当网络中还存在其它IGMP查询器设备时，当前设备设备将和其它设备进行查询器竞选，如果当前设备竞选失败处于于非查询器状态时，将启动查询器老化定时器，在定时器超期后，认为网络中的其它查询器设备失效，当前设备重新恢复为查询器设备。

相关配置

启动查询器

缺省情况下，设备不允许查询器功能。

通过 **ip igmp snooping querier** 命令可控制全局的查询器功能。

通过 **ip igmp snooping vlan** *num* **querier** 命令可控制指定 VLAN 的查询器功能

指定查询器运行的 IGMP 版本

缺省情况下，查询器使用 IGMPv2 版本。

通过 **ip igmp snooping querier version** 命令可控制全局的查询器的版本。

通过 **ip igmp snooping vlan querier version** 命令可控制指定 VLAN 的查询器版本

配置查询器的源 IP

缺省情况下，查询器的源 IP 为 0

通过 **ip igmp snooping querier address** 命令可设置全局的查询器源 IP。

通过 **ip igmp snooping vlan querier address** 命令可设置指定 VLAN 的查询器源 IP

配置查询器的查询间隔

缺省情况下，查询器的查询间隔为 60 秒

通过 **ip igmp snooping querier query-interval** 命令可设置全局的查询器查询间隔。

通过 **ip igmp snooping vlan querier query-interval** 命令可设置指定 VLAN 的查询器查询间隔

↘ 配置查询报文的最大响应时间

缺省情况下，查询器的查询间隔为 10 秒

通过 **ip igmp snooping querier max-response-time** 命令可设置全局查询器的查询报文最大响应时间。

通过 **p igmp snooping vlan querier max-response-time** 命令可设置指定 VLAN 查询器的查询报文最大响应时间

↘ 配置查询器的老化时间

缺省情况下，查询器老化时间间隔为 125 秒

通过 **ip igmp snooping querier max-response-time** 命令可设置全局的查询器老化时间间隔。

通过 **ip igmp snooping vlan querier max-response-time** 命令可设置指定 VLAN 的查询器老化时间间隔

11.3.4 组播转单播功能

只有在无线环境中才有组播转单播功能，在无线设备上配置组播转单播功能，AP 与 STA 之间的组播报文发送方式转变为单播方式发送。组播转单播功能运行于 AP 端。

工作原理

下面从无线环境的几个场景描述组播转单播的工作原理。

在胖 AP 模式下，IGMP Snooping 需要学习跟踪用户信息，当配置了组播转单播之后，无线组播快转模块通过组播转单播模块提供的接口查询那些用户需要转单播，进而将组播报文的目的 mac 替换为 STA 的 mac，目的 ip 替换未 STA 非配到的 ip 地址进行转单播发送。

在瘦 AP 集中转发模式下，报文在 AC 端根据记录的用户信息查找 STA 对应的 WLAN id 与 RADIO id，将报文进行 CAPWAP 封装发送到 AP，当报文到达 AP 之后，如果开启组播转单播，报文交给无线组播快转模块处理，无线组播快转模块查询组播转单播模块接口查询哪些用户需要转单播处理。进入将组播报文进行转单播处理发送。

在瘦 AP 本地转发模式下，报文转发到 AP，在 AP 上，判断如果开启组播转单播功能，报文交有无线组播快转模块处理，实现组播转单播功能。

相关配置

↘ 全局开启组播功能

缺省情况下，未开启全局组播通过 ip multicast wlan 开启全局组播，当开启全局组播，当 AC 接收到组播报文，组播将进行 CAPWAP 封装，并以 CAPWAP 单播方式发送到与此 AC 关联的 AP 设备上。

通过 **no ip multicast wlan** 恢复默认配置，当关闭全局组播，当 AC 接收到组播报文时，不进行任何处理，直接丢弃。

↘ 开启组播转单播功能

缺省情况下，未开启组播转单播功能

在 AC 设备的 ap-config 模式下配置 **igmp snooping mcast-to-unicast enable** 命令，开启组播转单播功能，或者在胖 AP 上，配置 **ip igmp snooping mcast-to-unicast enable** 命令开启组播转单播功能。

在 AC 设备的 ap-config 模式下配置 **no igmp snooping mcast-to-unicast enable** 命令，关闭组播转单播功能，或者在胖 AP 设备上，配置 **no ip igmp snooping mcast-to-unicast enable** 命令关闭组播转单播功能。

配置组播转单播的组播范围

默认情况下，所有组播组都可以尝试进行转单播发送。

以 AC 设备为例，在 ap-config 模式下配置 **igmp snooping mcast-to-unicast group-range** 命令，配置运行尝试进行组播转单播的组地址范围，或者在胖 AP 上，配置 **ip igmp snooping mcast-to-unicast group-range** 命令配置组播转单播的组地址范围。

在 ap-config 模式下配置 **no igmp snooping mcast-to-unicast group-range** 命令，恢复默认值，或者在胖 AP 上，通过配置 **ip igmp snooping mcast-to-unicast group-range** 恢复组播转单播的组地址范围。

配置组播转单播的最大组个数

默认情况下，组播转单播最大组个数为 64 个。

以 AC 设备为例，在 ap-config 模式下配置 **igmp snooping mcast-to-unicast max-group** 命令，配置允许最大组播转单播个数，或者在胖 AP 上，通过 **ip igmp snooping mcast-to-unicast max-group** 命令配置允许最大组播转单播个数。

在 ap-config 模式下配置 **no igmp snooping mcast-to-unicast max-group** 命令，恢复默认配置，或者在胖 AP 上，通过 **ip igmp snooping mcast-to-unicast max-group** 命令恢复允许最大组播转单播个数。

11.3.5 优化组播无线环境配置

工作原理

忽略查询报文重置端口定时器功能是指当设备接收到查询报文时不重新设置端口老化定时器。

在无线网络环境中，STA 比较多并且网络比较拥挤的时候，上游发出查询报文后，STA 发送上来的 IGMP report 报文有可能丢了，或者 STA 根本就没有收到查询报文，导致 AP 上收不到 STA 的回复，这样可能出现 STA 断流的情况。这种情况下我们可以配置该条命令，并结合成员端口老化时间的配置来保持 STA 可以支持在多个查询周期内不被老化，在这几个周期内收到 IGMP report 报文时把端口定时器时间重置为端口老化时间。

该配置对于下一次收到查询报文时生效，端口已被重置过的定时器不会被取消。该配置会延长老化的时间，要注意在合理的场景下使用。

相关配置

默认是该功能未打开。

以 AC 设备为例，在 ap-config 模式下配置 **igmp snooping ignore-query-timer** 命令，忽略查询报文重置端口老化定时器。

在 ap-config 模式下配置 **no igmp snooping ignore-query-timer** 命令，恢复默认配置。

11.4 配置详解

配置项	配置建议 & 相关命令	
配置IGMP Snooping基本功能（IVGL模式）	⚠ 必须配置。本配置项用于启动 IGMP Snooping 功能。	
	ip multicast wlan	开启全局组播状态
	ip igmp snooping	全局启动 IGMP Snooping 功能。
	igmp snooping	AC 上 ap-config 模式配置，开启 AP 的组播功能。
	no ip igmp snooping vlan *num*	在 VLAN 上关闭 IGMP Snooping 功能。
配置协议报文处理	⚠ 可选配置。用于调整协议报文处理相关配置。	
	ip igmp snooping vlan *vlan-id* **mrouter interface** *interface-id*	配置静态路由连接口。
	ip igmp snooping vlan *vid* **static** *group-address* **interface** *interface-type interface-number*	配置静态成员口。
	ip igmp snooping vlan *vlan-id* **mrouter learn pim-dvmrp**	启动动态学习路由连接口的功能。
	ip igmp snooping host-aging-time *time*	配置动态成员口老化时间。
	igmp snooping host-aging-time *time*	AC 上 ap-config 模式配置，配置 AP 的动态成员口老化时间。
	ip igmp snooping fast-leave enable	启动动态成员口“快速离开”功能。
	igmp snooping query-max-response-time *time*	AC 上 ap-config 模式配置，配置 AP 的查询报文最大响应时间。
	ip igmp snooping query-max-response-time *time*	配置 IGMP Query 报文的最大响应时间。
	ip igmp snooping suppression enable	启动 IGMP Report 报文抑制功能。
配置IGMP查询器	⚠ 可选配置。用于在没有三层组播设备的网络上提供 IGMP 查询器的功能。	
	ip igmp snooping querier	全局启动查询器功能。
	ip igmp snooping vlan *num* **querier**	在 VLAN 上启动查询器功能。
	ip igmp snooping querier version *num*	全局配置查询器运行的 IGMP 版本。
	ip igmp snooping vlan *num* **querier version** *num*	在 VLAN 上配置查询器运行的 IGMP 版本。
	ip igmp snooping querier address a.b.c.d	全局配置查询器的源 IP 地址。
	ip igmp snooping vlan *num* **querier address** a.b.c.d	在 VLAN 上配置查询器的源 IP 地址。
	ip igmp snooping querier query-interval *num*	全局设置查询间隔。

	ip igmp snooping vlan *num* **querier query-interval** *num*	在 VLAN 上设置查询间隔。
	ip igmp snooping querier max-response-time *num*	全局设置查询报文的最大响应时间。
	ip igmp snooping vlan *num* **querier max-response-time** *num*	在 VLAN 上设置查询报文的最大响应时间。
	ip igmp snooping querier timer expiry *num*	全局配置查询器老化定时器。
	ip igmp snooping vlan *num* **querier timer expiry** *num*	在 VLAN 上配置查询器老化定时器。
配置组播转单播	可选配置。	
	igmp snooping mcast-to-unicast enable	AC 上 ap-config 模式下配置，开启 AP 组播转单播功能。
	ip igmp snooping mcast-to-unicast enable	胖 AP 上 config 模式下配置，开启 AP 组播转单播功能。
	igmp snooping mcast-to-unicast group-range ***ip-addr ip-addr***	AC 上 ap-config 模式下配置，配置 AP 组播转单播最大组播范围。
	ip igmp snooping mcast-to-unicast group-range ***ip-addr ip-addr***	胖 AP 上 config 模式下配置，配置 AP 组播转单播最大组播范围。
	ip igmp snooping mcast-to-unicast max-group ***group-num***	胖 AP 上 config 模式下配置，配置 AP 允许组播转单播最大组播组个数。
	igmp snooping mcast-to-unicast max-group ***group-num***	AC 上 ap-config 模式下配置，配置 AP 允许组播转单播最大组播组个数。
配置优化无线组播环境	**ip igmp snooping ignore-query-timer**	胖 AP 上 config 模式下配置，忽略查询报文重置端口定时器功能。
	igmp snooping ignore-query-timer	AC 上 ap-config 模式下配置，配置 AP 忽略查询报文重置端口定时器功能。

11.4.1 配置IGMP Snooping基本功能（IVGL模式）

配置效果

- 启动 IGMP Snooipng，实现二层组播。
- 每个 VLAN 享有独立的组播服务。

配置方法

启动全局组播功能

必须配置。

启动全局组播配置，再启动 IGMP Snooping 功能才能生效。

全局启动 IGMP Snooping 功能

必须配置。

全局启动 IGMP Snooping 功能后，则所有 VLAN 上均启动了 IGMP Snooping 功能。

若无特殊要求，建议在所有连接用户主机的二层接入设备上全局启动 IGMP Snooping 功能。

启动 AP 的组播功能

必须配置。

在 AC 上 ap-config 模式配置 **igmp snooping 启动 AP 的组播功能。**

在指定 VLAN 上关闭 IGMP Snooping 功能

可选配置。如果希望在某些 VLAN 上不启用 IGMP Snooping 功能，则需要配置此命令。

必须首先全局启动 IGMP Snooping 功能，才能在指定 VLAN 上关闭 IGMP Snooping 功能。

在 IVGL 模式下，每个 VLAN 享受独立的组播服务，关闭任何一个 VLAN 的组播服务，都不会影响其他 VLAN 的组播服务。

检验方法

- 使用 **show ip igmp snooping gda-table** 命令，查看 IGMP Snooping 转发表项，确认成员口仅包括连接组成员主机的端口。
- 使用 **show ip igmp snooping** 命令，查看 IGMP Snooping 基本信息，确认 IGMP Snooping 工作在 IVGL 模式下。

相关命令

启动全局组播功能

【命令格式】 **ip multicast wlan**
【参数说明】 **-**
【命令模式】 全局模式
【使用指导】 配置此命令后，再配置 IGMP Snooping 命令才有效
缺省情况下，全局组播处于关闭状态。

全局启动 IGMP Snooping 功能

【命令格式】 **ip igmp snooping**
【参数说明】 **-**
【命令模式】 全局模式
【使用指导】 配置此命令后，所有 VLAN 启动 IGMP Snooping 功能。
缺省情况下，IGMP Snooping 处于关闭状态。

启动 AP 的组播共

【命令格式】 **igmp snooping**
【参数说明】 -
【命令模式】 ap-config 模式
【使用指导】 配置此命令后，启动对应 AP 的 IGMP Snooping 功能。
缺省情况下，AP 的 IGMP Snooping 处于关闭状态。

在指定 VLAN 上关闭 IGMP Snooping 功能

【命令格式】 **no ip igmp snooping vlan** *num*
【参数说明】 -
【命令模式】 全局模式
【使用指导】 必须首先全局启动 IGMP Snooping，才能在部分 VLAN 上关闭 IGMP Snooping 功能。
在 IVGL 模式下，可以在任意 VLAN 上关闭 IGMP Snooping 功能。

查看 IGMP Snooping 转发表项

【命令格式】 **show ip igmp snooping gda-table**
【参数说明】 -
【命令模式】 特权模式、全局模式、接口模式
【使用指导】 确认成员口仅包括连接组成员主机的端口。

查看 IGMP Snooping 工作模式

【命令格式】 **show ip igmp snooping**
【参数说明】 -
【命令模式】 特权模式、全局模式、接口模式
【使用指导】 如果 IGMP Snooping 运行在 IVGL 模式下，则可以看到如下信息：

```
IGMP Snooping running mode: IVGL
```

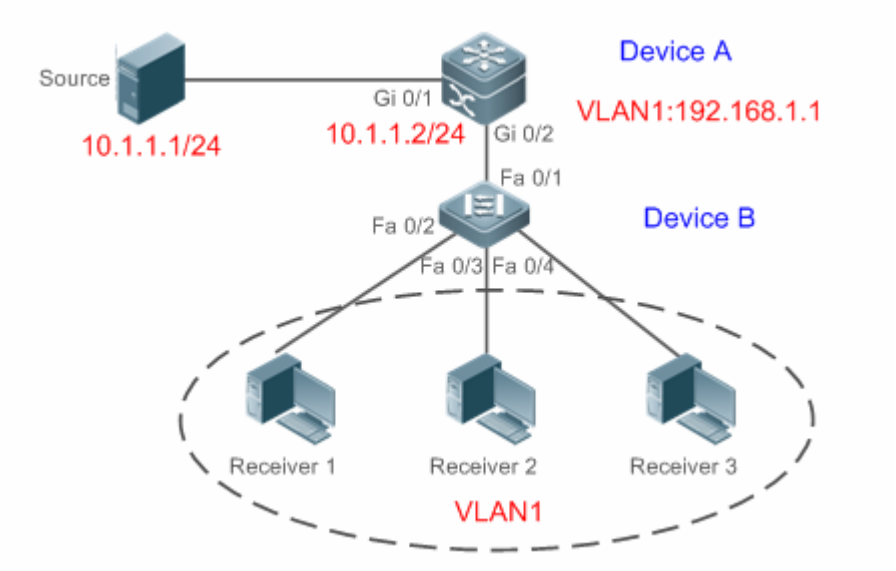
配置举例

以下配置举例，仅介绍与 IGMP Snooping 相关的配置。

在用户主机所在网段提供二层组播服务。

【网络环境】

图 11-7



A 作为组播路由设备，直连组播源。

B 作为二层接入设备，直连用户主机。

Receiver1、Receiver2、Receiver3 属于 VLAN1。

【配置方法】

- 在网络中配置 IP 地址、VLAN。（略）
- 在 A 上开启组播路由功能，并在三层接口上（Gi 0/1 和 VLAN 1）启动组播路由协议。
- 在 B 上开启 IGMP Snooping 功能，运行 IVGL 模式。

A

```
A# configure terminal
A(config)# ip multicast-routing
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
A(config-if-GigabitEthernet 0/1)# exit
A(config)# interface vlan 1
A(config-if-VLAN 1)# ip pim sparse-mode
A(config-if-VLAN 1)# exit
```

B

```
B# configure terminal
B(config)# ip igmp snooping ivgl
```

【检验方法】

使 Source（10.1.1.1）向 G（229.1.1.1）发送报文。使 Receiver1 加入 G。

- 确认 Receiver1 收到（10.1.1.1，229.1.1.1）报文。
- 查看 B 上的 IGMP Snooping 转发表项，确认（10.1.1.1，229.1.1.1，1)的成员口仅包括 Fa 0/2。
- 确认 B 上的 IGMP Snooping 工作模式为 IVGL。

B

```
B# show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
```

```
(*,224.1.1.1, 1):
  VLAN(1) 2 OPORTS:
    FastEthernet 0/1(M)
    FastEthernet 0/2(D)
```

```
B# show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)

vlan 1
-------------
IGMP Snooping state: Enable
Multicast router learning mode: pim-dvmrp
IGMP Fast-Leave: Disabled
IGMP VLAN querier: Disable
IGMP VLAN Mode: STATIC
```

常见错误

- 未能正确选择 IGMP Snooping 的工作模式。

11.4.2 配置协议报文处理

配置效果

- 配置指定接口为静态路由连接口，可接收所有组的组播流
- 配置指定接口为静态成员口，可接收指定组播组的组播流
- 配置 Report 报文抑制，在一个查询间隔内只会把第一个收到的特定 VLAN 和组的 Report 报文转发给路由连接口，后继的 Report 报文将不继续向路由连接口转发，这样可以减少网络中的报文数量。

- 配置快速离开，当设备某端口收到 Leave 报文时，直接从对应的转发表项的成员口中删除该端口
- 配置关闭动态路由连接口学习，设备将不学习任何路由连接口
- 可根据网络的负载以及组播路由设备的配置情况，调整路由连接口和成员口的老化时间;调整查询报文最大响应时间；

注意事项

- 必须配置 IGMP Snooping 基本功能，相关配置功能才能生效

配置方法

配置静态路由连接口

- 可选配置
- 如果要静态指定某个接口能够接收 VLAN 内的所有组播流，可在设备上执行此配置项

配置静态成员口

- 可选配置
- 如果要静态指定某个接口能够接收 VLAN 内的指定组播组的组播流，可在设备上执行此配置项

配置 Report 报文抑制

- 可选配置
- 当存在同一时间有大量的接收者需要接收同一个组播组的报文时，可通过在设备上配置 Report 报文抑制功能减少 Report 报文个数。

配置快速离开

- 可选配置
- 当接口下只存在一个接收者的时候，可通过在设备上配置快速离开，加速用户离开时的协议收敛。

配置关闭动态路由连接口学习

- 可选配置
- 当组播流指需要在二层拓扑内进行转发时，不需要发送到三层路由设备，可进行此项配置。

配置动态成员口的老化时间

- 可选配置
- 可根据连接的组播路由设备的 IGMP 查询报文发送间隔来调整该老化时间，一般设置为组播路由设备的 IGMP 查询报文发送时间间隔*2 + IGMP 最后查询响应时间

配置查询报文最大响应时间

- 可选配置
- 可根据连接网络负载情况进行时间调整

检验方法

- 使用 **show ip igmp snooping mrouter** 命令，查看已配置的静态路由连接口存在“S”标志。
- 使用 **show ip igmp snooping gda** 命令，查看已配置的静态成员口存在“S”标志。
- 使用 **show ip igmp snooping** 命令，查看 Report 报文抑制、快速离开、路由连接口学习、路由连接口老化时间、成员口老化时间、查询报文最大响应时间配置是否生效

相关命令

配置静态路由连接口

【命令格式】 **ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*

【参数说明】 *vid*：VLAN 编号，取值范围 1-4094

interface-type interface-number 接口名称

【命令模式】 全局模式

【使用指导】 在 SVGL 模式下，如果未配置 Sub VLAN，则只有属于 Share VLAN 的静态路由连接口的配置可生效，其它情况可配置但不生效；如果配置了 Sub VLAN，则属于 Share VLAN 或者非 Sub VLAN 的静态路由连接口的配置可生效，其它情况可配置但不生效；

在 SVGL-IVGL 模式下，如果未配置 Sub VLAN，所有 VLAN 的静态路由连接口的配置均可生效；如果配置了 Sub VLAN，则属于 Share VLAN 或者非 Sub VLAN 的静态路由连接口的配置可生效，其它情况可配置但不生效；

在 IVGL 模式下，所有 VLAN 的静态路由连接口的配置均可生效。

配置静态成员口

【命令格式】 **ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*

【参数说明】 *vid*: VLAN 编号，取值范围 1-4094

group-address: 组地址

interface-type interface-number: 接口名称

【命令模式】 全局模式

【使用指导】 默认情况下，无静态成员口配置

配置 Report 报文的抑制功能

【命令格式】 **ip igmp snooping suppression enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 当启用 Report 报文抑制功能后，在一个查询间隔内只会把第一个收到的特定 VLAN 和组的 Report 报文转发给路由连接口，后继的 Report 报文将不继续向路由连接口转发，这样可以减少网络中的报文数量。

只能抑制 IGMPv1/v2 的 Report 报文，对 IGMPv3 的 Report 报文无效。

配置端口快速离开功能

【命令格式】 **ip igmp snooping fast-leave enable**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 启用端口快速离开功能后，当设备某端口收到 Leave 报文时，直接从对应的转发表项的成员口中删除该端口。此后，当设备收到对应的特定组查询报文时，设备不再向该端口转发。其中，Leave 报文包括 IGMPv2 的 Leave 报文以及 IGMPv3 中 include 类型并且不带任何源地址的 Report 报文。

端口快速离开功能仅适用于设备一个端口下只连接一台主机的情况，可以节约带宽和资源。

配置动态学习路由连接口功能

【命令格式】 **ip igmp snooping** [**vlan** *vid*] **mrouter learn pim-dvmrp**

【参数说明】 **vlan** *vid*：指定 vlan。缺省则适用于所有 VLAN

【命令模式】 全局模式

【使用指导】 路由连接口是开启 IGMP Snooping 的组播设备上与开启组播路由协议的组播邻居设备直接相连的端口。缺省情况下，启用动态学习路由连接口功能，设备自动侦听 IGMP Query/DVMRP/PIM Hello 报文，动态识别路由连接口。

配置动态成员口老化时间

【命令格式】 **ip igmp snooping host-aging-time** *seconds*

【参数说明】 *seconds*: 老化时间

【命令模式】 全局模式

【使用指导】 动态成员端口老化时间是指当设备的某端口收到主机发送的加入某 IP 组播组的 IGMP 加入报文时，为这个动态成员端口设置的老化时间。

在收到 IGMP 加入报文后，会重置这个动态成员端口的老化定时器，定时器时间为 host-aging-time。如果定时器超时，则认为该端口下不存在接收组播报文的用户主机，组播设备就会把该端口从 IGMP Snooping 的成员口中删除。配置完该命令，后面收到的 IGMP 加入报文时设置的动态成员端口老化定时器的值为 host-aging-time。该配置在下一次收到加入报文时生效，当前已启动的成员口的定时器不会被更新。

配置查询报文响应时间

【命令格式】 **ip igmp snooping query-max-response-time** *seconds*

【参数说明】 *seconds*: 响应时间

【命令模式】 全局模式

【使用指导】 在收到 IGMP 普通查询报文后，组播设备会重置所有动态成员口的老化定时器，定时器时间为 query-max-response-time。如果定时器超时，则认为该端口下不存在接收组播报文的用户主机，组播设备就会把该端口从 IGMP Snooping 的成员口中删除。

在收到 IGMP 特定组查询报文后，组播设备会重置该特定组的所有动态成员口的老化定时器，定时器时间为 query-max-response-time。如果定时器超时，则认为该端口下不存在接收组播报文的用户主机，组播设备就会把该端口从 IGMP Snooping 的成员口中删除。

该配置在下一次收到查询报文时生效，当前已启动的定时器不会被更新。对于 IGMPv3 的特定组源查询报文，不做定时器的更新处理。

查看路由连接口

【命令格式】 **show ip igmp snooping mroute**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 如果路由连接口配置成功，则可以看到显示的接口信息中有“S”标志，如：

```
Ruijie(config)#show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 1):
  VLAN(1)  1 MROUTES:
    GigabitEthernet 0/1(S)
```

查看动态学习路由连接口

【命令格式】 **show ip igmp snooping**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 通过 **show ip igmp snooping** 命令，可查看动态路由连接口老化时间和学习状态：

```
Dynamic Mroute Aging Time : 300(Seconds)
Multicast router learning mode: pim-dvmrp
```

查看成员口

【命令格式】 **show ip igmp snooping gda-table**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 如果成员口配置成功，则可以看到显示的接口信息中有“S”标志，如：

```
Ruijie(config)#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 224.1.1.1, 1):
  VLAN(1) 1 OPORTS:
    GigabitEthernet 0/1(S
```

查看其它参数

【命令格式】 **show ip igmp snooping**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 通过 **show ip igmp snooping** 命令，可查看路由连接口老化时间、动态成员口老化时间、查询报文响应时间、Report 抑制和快速离开参数：

```
IGMP Fast-Leave: Enable
```

```
IGMP Report suppress: Enable
Query Max Respone Time: 20(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

配置举例

↘ 静态路由连接口和静态成员口配置

【配置方法】
- 配置 IGMP Snooping 基本功能。略
- 配置静态路由连接口和静态成员口

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping vlan 1 mrouter interface GigabitEthernet 0/0
Ruijie(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface GigabitEthernet 0/0
Ruijie(config)# end
```

【检验方法】 通过 show ip igmp snooping mrouter 和 show ip igmp snooping gda-table 查看静态配置是否成功

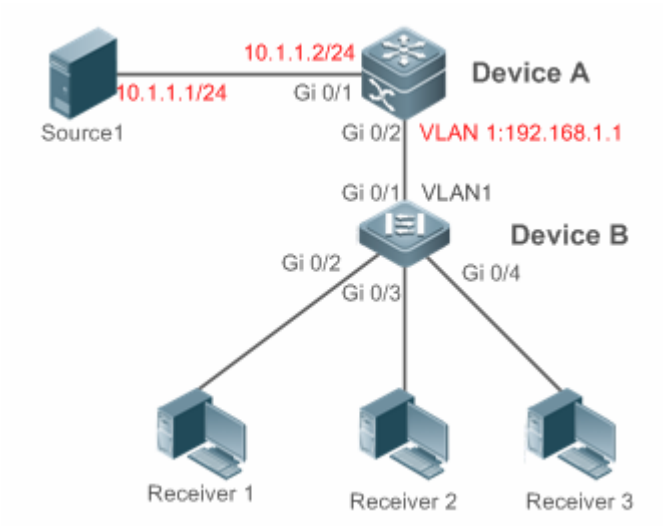
```
Ruijie#show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 1):
  VLAN(1)  1 MROUTES:
    GigabitEthernet 0/0(S)

Ruijie#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*, 224.1.1.1, 1):
  VLAN(1) 1 OPORTS:
    GigabitEthernet 0/0(SM)
```

↘ 配置 Report 报文抑制

【网络环境】

图 11-8



A 作为组播路由设备，直连组播源 Source1。

B 作为二层接入设备，直连用户主机，同时连接另一个组播源 Source2。

Receiver1、Receiver2、Receiver3 连接到 VLAN1

【配置方法】

- 在网络中配置 IP 地址、VLAN。（略）
- 在 A 上开启组播路由功能，并在三层接口上（Gi 0/1 和 VLAN 1）启动组播路由协议。
- 在 B 上开启 IGMP Snooping 功能，运行 IVGL 模式。
- 在 B 上配置 Report 报文抑制功能

A

```
A# configure terminal
A(config)# ip multicast-routing
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode
A(config-if-GigabitEthernet 0/1)# exit
A(config)# interface vlan 1
A(config-if-VLAN 1)# ip pim sparse-mode
A(config-if-VLAN 1)# exit
```

B

```
B# configure terminal
B(config)#ip igmp snooping ivgl
B(config)# ip igmp snooping suppression enable
```

【检验方法】 Receiver1 和 Receiver2 都加入组 239.1.1.1，从设备 B 的 Gi0/1 接口上能够看到只转发出了一个组地址 239.1.1.1 的 IGMP Report 报文。

B

```
B# show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
```

```
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Enable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

↘ 其它参数配置

【配置方法】

- 配置 IGMP Snooping 基本功能。略
- 配置快速离开
- 配置关闭路由口学习
- 配置路由连接口老化时间
- 配置成员口老化时间
- 配置查询报文响应时间

```
Ruijie# configure terminal
Ruijie(config)# ip igmp snooping fast-leave enable
Ruijie(config)# no ip igmp snooping mrouter learn pim-dvmrp
Ruijie(config)#ip igmp snooping host-aging-time 100
Ruijie(config)#ip igmp snooping query-max-response-time 60
Ruijie(config)# end
```

【检验方法】 通过 show ip igmp snooping 查看配置是否成功

```
Ruijie#show ip igmp snooping
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Enable
IGMP Report suppress: Enable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
Query Max Respone Time: 60(Seconds)
IGMP Preview group aging time : 60(Seconds)
Dynamic Host Aging Time : 100(Seconds)
```

常见配置错误

- IGMP Snooping 基本功能没有配置，或配置失败。

11.4.3 配置IGMP查询器

配置效果

- 本设备将充当 IGMP 查询器功能，定时发送 IGMP 查询报文，收集用户点播信息。

注意事项

- 必须配置 IGMP Snooping 基本功能。

配置方法

启动查询器

- 可选配置，要启用 IGMP 查询器，需要在全局上和指定 VLAN 上启用查询器功能
- 可选配置，用户可单独关闭某个 VLAN 的查询器功能。

配置查询器的源 IP

- 可选配置，配置查询器发送的查询报文所携带的源 IP 地址，可基于 VLAN 配置查询器发送的查询报文的源 IP 地址。
- 启动查询器功能后，必须为查询器指定一个源 IP 地址，否则查询器功能不生效。

配置查询报文的最大响应时间

- 可选配置，可调整 IGMP 查询报文中携带的最大响应时间值。由于 IGMPv1 版本的协议不支持报文携带最大响应时间，所有该配置对于查询器运行 IGMPv1 版本时不生效

配置查询器的查询间隔

- 可选配置，可调整 IGMP 查询器查询报文的发送间隔

配置查询器的老化时间

- 可选配置，可设置网络中其它 IGMP 查询器的老化时间

指定查询器运行的 IGMP 版本

- 可选配置，可设定 IGMP 查询的版本，默认使用 IGMP v2 版本

检验方法

- 使用 **show ip igmp snooping querier detail** 命令，查看配置是否生效。

相关命令

配置 IGMP 查询器功能

【命令格式】 **ip igmp snooping** [**vlan** *vid*] **querier**

【参数说明】 **vlan** *vid*：指定 VLAN。缺省则适用于所有 VLAN。

【命令模式】 全局模式

【使用指导】 当全局启动查询器功能后，再在 VLAN 上启用查询器功能，VLAN 上的查询器功能才能生效。

如果在全局上关闭了查询器功能，所有 VLAN 上的查询器功能将全部关闭。

配置 IGMP 查询器源 IP

【命令格式】 **ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*

【参数说明】 **vlan** *vid*：指定 VLAN。缺省则适用于所有 VLAN。

a.b.c.d：源 IP 地址

【命令模式】 全局模式

【使用指导】 启动查询器功能后，必须为查询器指定一个源 IP 地址，否则查询器功能不生效。

如果 VLAN 上指定了查询器的源 IP 地址，优先使用 VLAN 上的配置。

配置最大响应时间

【命令格式】 **ip igmp snooping** [**vlan** *vid*] **querier max-response-time** *seconds*

【参数说明】 **vlan** *vid*：指定 VLAN。缺省则适用于所有 VLAN。

seconds：最大响应时间。单位为秒，取值范围 1-25

【命令模式】 全局模式

【使用指导】 如果 VLAN 上指定了查询间隔，优先使用 VLAN 上的配置。

配置查询间隔

【命令格式】 **ip igmp snooping** [**vlan** *vid*] **querier address** *a.b.c.d*

【参数说明】 **vlan** *vid*：指定 VLAN。缺省则适用于所有 VLAN。

seconds：查询间隔。单位为秒，取值范围 1-18000

【命令模式】 全局模式

【使用指导】 如果 VLAN 上指定了查询间隔，优先使用 VLAN 上的配置。

配置查询器超时时间

【命令格式】 **ip igmp snooping** [**vlan** *vid*] **querier timer expiry** *seconds*

【参数说明】 **vlan** *vid*：指定 VLAN。缺省则适用于所有 VLAN。

seconds：超时时间。单位为秒，取值范围 60-300

【命令模式】 全局模式

【使用指导】 启用了查询器功能后，也可能在选举中落败。如果落败者在“查询器超时时间”内没有收到当前查询器发出的查询报文，则认为当前查询器失效，发起下一轮选举。

如果相应 VLAN 上已经配置了查询器超时时间，优先使用 VLAN 上的配置值。

配置查询器版本

【命令格式】 **ip igmp snooping** [**vlan** *vid*] **querier version 1**

【参数说明】 **vlan** *vid*：指定 VLAN。缺省则适用于所有 VLAN。

【命令模式】 全局模式

【使用指导】 查询器支持 IGMPv1 或 IGMPv2，默认情况下使用 IGMPv2，可使用命令设置查询器运行 IGMPv1

如果 VLAN 上已经配置了查询器运行的 IGMP 版本，优先使用 VLAN 上的配置。

查看 IGMP 查询器配置

【命令格式】 **show ip igmp snooping querier detail**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 如果 QinQ 配置成功，则可以看到如下信息：

```
Ruijie(config)#show ip igmp snooping querier detail
Vlan      IP Address           IGMP Version           Port
-----------------------------------------------------------


Global IGMP switch querier status
-----------------------------------------------------------
admin state                    : Enable
admin version                  : 2
source IP address              : 1.1.1.1
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 125

Vlan 1:   IGMP switch querier status
-----------------------------------------------------------
admin state                    : Disable
admin version                  : 2
source IP address              : 1.1.1.1
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 125
operational state              : Disable
operational version            : 2
```

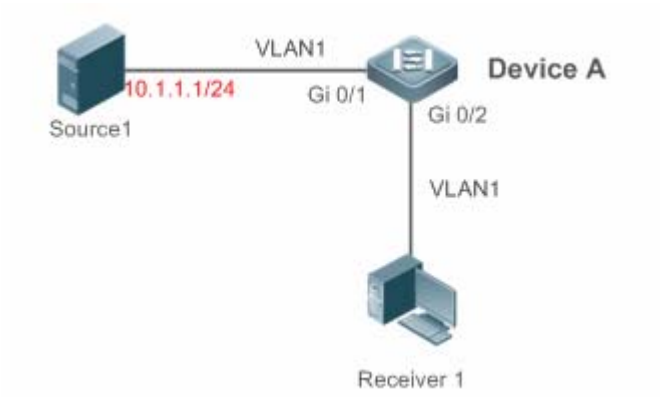
配置举例

以下配置举例，仅介绍与 IGMP Snooping 相关的配置。

启用 IGMP 查询器功能

【网络环境】

图 11-9



网络部署中组播流只需要在二层内进行转发，且网络中无三层组播功能的设备。

A 作为组播二层设备连接组播源和组播接收者。

【配置方法】

- 在 A 上开启 IGMP Snooping 功能，运行 IVGL 模式。
- 在 A 上配置 VLAN 1 的 IGMP 查询器功能

A

```
A(config)#ip igmp snooping ivgl
A(config)#ip igmp snooping querier
A(config)#ip igmp snooping querier address 10.1.1.1
A(config)#ip igmp snooping vlan 1 querier
```

【检验方法】 通过 show ip igmp snooping querier 命令，查看 VLAN 1 的查询器已生效

A

```
A(config)#show ip igmp snooping querier
Vlan      IP Address           IGMP Version           Port
-----------------------------------------------------------
1         10.1.1.1                2                   switch

A(config)#show ip igmp snooping querier vlan 1

Vlan 1:   IGMP switch querier status
-----------------------------------------------------------
elected querier is 10.1.1.1         (this switch querier)
-----------------------------------------------------------
admin state                    : Enable
admin version                  : 2
source IP address              : 10.1.1.1
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 125
operational state              : Querier
operational version            : 2
```

常见错误

- 未配置查询器源 IP，导致查询器不生效。

11.4.4 配置组播转单播

配置效果

- 在 AP 上启用组播转单播功能，组播报文在 AP 上转单播发送到 STA。

注意事项

- 必须配置 IGMP Snooping 基本功能。

配置方法

↘ 开启全局组播状态

- 必须配置，在全局模式下，开启全局组播状态。
- 如果在全局模式下不开启全局组播功能，报文到达无线设备时不做处理直接丢弃。

↘ 开启组播转单播

- 可选配置，配置是否开启组播转单播功能，当开启组播转单播功能之后，报文到达 AP 之后，判断哪些组播报文需要转单播处理，从而进行组播转单播发送。

↘ 配置组播转单播组播范围

- 可选配置，默认情况下，所有组播组都允许尝试转单播处理，为了最大限度的利用 AP 资源，可以配置一个组播范围允许报文进行组播转单播处理。

↘ 配置组播转单播最大组播组个数

- 可选配置，可调整最大允许进行组播转单播的个数
- 结合组播转单播组播范围一起使用。

检验方法

- 使用 **show ip igmp snooping** 命令，查看配置是否生效。

相关命令

↘ 配置全局组播功能

【命令格式】 **ip multicast wlan**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 当开启全局组播状态之后，组播报文到达 AC 才会处理，如果未开启全局组播状态，组播报文到达 AC 不予处理直接丢弃

配置组播转单播

【命令格式】 **igmp snooping mcast-to-unicast enable**

【参数说明】 -

【命令模式】 AC 上的 ap-config 模式或者胖 AP 的全局模式

【使用指导】 启用组播转单播功能之后， 当报文到达 AP，根据组播转单播策略，判断哪些用户需要进行转单播处理。

配置组播转单播最大组播组范围

【命令格式】 **igmp snooping mcast-to-unicast group-range** *ip-addr ip-addr*

【参数说明】 *ip-addr*：组播组范围，必需为合法组播地址，范围 224.0.1.0~239.255.255.255。

【命令模式】 AC 上的 ap-config 模式或者胖 AP 的全局模式

【使用指导】 如果未配置转播转单播组播组范围，默认所有组播组都允许尝试进行组播转单播。

配置组播转单播最大组播组个数

【命令格式】 **igmp snooping mcast-to-unicast max-group** *number*

【参数说明】 *number*：指定最大允许组播转单播组播组个数。缺省值为 64。范围 1~64

【命令模式】 AC 上的 ap-config 模式或者胖 AP 的全局模式

【使用指导】 和组播转单播最大组播组范围结合使用，合理分配带宽，有效控制 AP 资源。

查看组播转单播配置

【命令格式】 **show ip igmp snooping**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 如果 QinQ 配置成功，则可以看到如下信息：

```
Ruijie(config)#sh ip igmp snooping
WLAN Multicast: Enable
IGMP Snooping running mode: IVGL
IGMP Snooping M2U-Forward: Enable
IGMP Snooping Support M2U Max-Group Num: 64
IGMP Snooping M2U Group range: 233.3.3.1-233.3.3.64
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
```

```
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

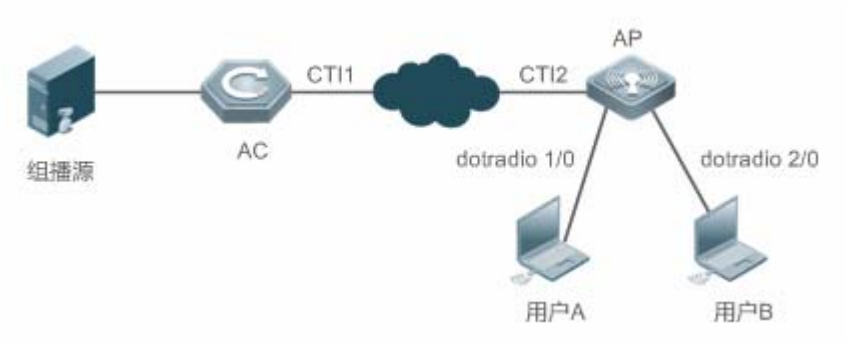
配置举例

以下配置举例，仅介绍与 IGMP Snooping 相关的配置。

启用组播转单播功能

【网络环境】

图 11-10



网络部署中组播流只需要在二层内进行转发，且网络中无三层组播功能的设备。

用户 A 与用户 B 为组播接收者。

【配置方法】

- 在 AC 上开启 IGMP Snooping 功能
- 在 AC 上开启全局组播状态
- 在 ap-config 模式下开启 IGMP Snooping 功能
- 在 ap-config 模式下开启组播转单播功能
- 在 ap-config 模式下配置组播转单播最大组播组范围
- 在 ap-config 模式下配置组播转单播最大组播组个数

A

```
A(config)#ip igmp snooping ivgl
A(config)#ip multicast wlan
A(config)#ap-confing all
A(config-ap)#igmp snooping
A(config-ap)#igmp snooping mcast-to-unicast enable
A(config-ap)#igmp snooping mcast-to-unicast group-range 233.1.1.1 233.255.255.255
A(config-ap)#igmp snooping mcast-to-unicast max-group 10
```

【检验方法】 通过 show ip igmp snooping 命令，查看配置是否生效

A

```
A(config)# sh ip igmp snooping
WLAN Multicast: Enable
IGMP Snooping running mode: IVGL
```

```
IGMP Snooping M2U-Forward: Enable
IGMP Snooping Support M2U Max-Group Num: 64
IGMP Snooping M2U Group range: 233.3.3.1-233.3.3.64
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Global Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 300(Seconds)
Dynamic Host Aging Time : 260(Seconds)
```

常见错误

- 未配置全局组播状态，导致组播报文无法处理

11.4.5 配置优化无线组播环境

配置效果

- 在无线设备上配置忽略查询报文重置端口定时器功能。

注意事项

- 必须配置 IGMP Snooping 基本功能。

配置方法

↘ 配置忽略查询报文重置端口老化定时器

- 可选配置，配置了忽略查询报文重置端口老化定时器，可以让端口在几个查询周期内不被老化。

检验方法

- 使用 **show ip igmp snooping** 命令，查看配置是否生效。

相关命令

配置忽略查询报文重置端口老化定时器

【命令格式】 **ip igmp snooping ignore-query-timer**

【参数说明】 -

【命令模式】 全局模式或者 ap-config 模式

【使用指导】 当配置了忽略查询报文重置端口老化定时器之后，端口在几个查询周期内不会老化掉，当端口收到 report 请求报文，端口老化定时器重置。

11.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除动态路由口、成员口。	**clear ip igmp snooping gda-table**

查看运行情况

作用	命令
查看 IGMP Snooping 基础配置。	**show ip igmp snooping** [**vlan** *vlan-id*]
查看路由连接口。	**show ip igmp snooping mrouter**
查看 IGMP Snooping 转发表项。	**show ip igmp snooping gda-table**
查看 IGMP 查询器。	**show ip igmp snooping querier** [**detail**]
查看用户信息	**Show ip igmp snooping user-info**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开与 IGMP Snooping 所有调试开关。	**debug igmp-snp**
打开 IGMP Snooping 事件的调试开关。	**debug igmp-snp event**
打开 IGMP Snooping 报文的调试开关。	**debug igmp-snp packet**
打开 IGMP Snooping 与 MSF 通信的调试开关。	**debug igmp-snp msf**
打开 IGMP Snooping 警告的调试开关。	**debug igmp-snp warning**

12 ACL

12.1 概述

ACLs (Access Control Lists，接入控制列表)，也称为访问列表（Access Lists），俗称为防火墙，在有的文档中还称之为包过滤。通过定义一些规则对网络设备接口上的数据报文进行控制：允许通过、丢弃。

根据使用 ACL 目的的不同可分为：安全 ACLs 和 QoS ACLs。

- 安全 ACLs 用于控制哪些数据流允许从网络设备通过。
- QoS ACLs 对这些数据流进行优先级分类和处理。

配置访问列表的原因比较多，最主要的主要有以下一些：

- 网络访问控制：为了确保网络安全，通过定义规则，可以限制用户访问一些服务（如只需要访问 WWW 和电子邮件服务，其他服务如 TELNET 则禁止），或者仅允许在给定的时间段内访问，或只允许一些主机访问网络等等。
- 优先服务保证：为一些重要的数据流进行优先分类处理，这就是 QoS ACLs 作用。有关 QoS ACLs 的使用请参考 QoS 相关的配置手册。

下文仅介绍 ACL 的相关内容。

协议规范

无

12.2 典型应用

典型应用	场景描述
企业内网访问控制应用	在企业网中根据需要对各个部门的网络访问权限进行控制和限制，比如服务器的访问限制、QQ 和 MSN 等聊天工具的使用限制等。

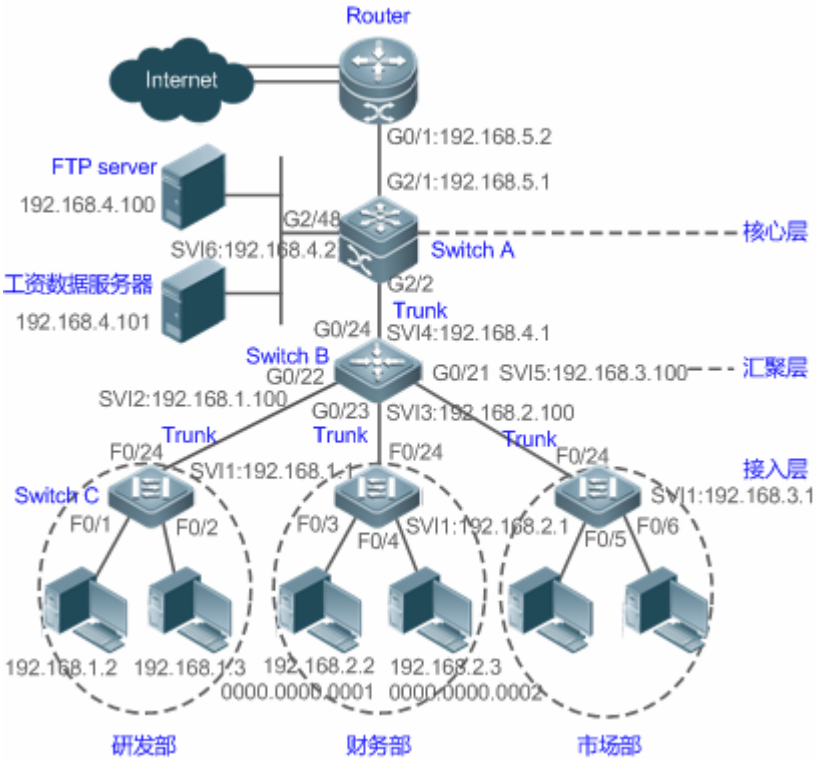
12.2.1 企业内网络访问控制应用

应用场景

Internet 病毒无处不在，需要封堵各种病毒的常用端口，以保障内网安全：

- 只允许内部 PC 访问服务器，不允许外部 PC 访问服务器。
- 不允许非财务部门 PC 访问财务部 PC；不允许非研发部门 PC 访问研发部 PC。
- 不允许研发部门人员在上班时间（即 9:00~18:00）使用 QQ、MSN 等聊天工具。

图 12-1



【注释】 接入层设备 C：连接各部门的 PC，通过千兆光纤(trunk 方式)连接汇聚层设备。
汇聚层设备 B：划分多个 VLAN，每个部门为一个 VLAN，通过万兆光纤(trunk 方式)上连核心层设备。
核心层设备 A：连接各种服务器，如 FTP，HTTP 服务器等，通过防火墙与 Internet 相连。

功能部属

- 通过在核心层设备（本例为设备 A）上联 Router 的端口（本例为 G2/1 口）上设置扩展 ACL 来过滤相关端口的数据包来达到防病毒的目的。
- 要求内部 PC 对服务器进行访问，不允许外部 PC 访问服务器，可以通过定义 IP 扩展 ACL 并应用到核心层设备（本例为设备 A）的下联汇聚层设备和服务器的接口（本例为 G2/2 口/SVI 2）上实现。
- 要求特定部门间不能互访，可通过定义 IP 扩展 ACL 实现(本例中分别在设备 B 的 G0/22、G0/23 上应用 IP 扩展 ACL)；
- 可通过配置时间 IP 扩展 ACL，限制研发部门在特定时间内使用 QQ/MSN 等聊天工具（本例中在设备 B 的 SVI 2 上应用时间 IP 扩展 ACL）。

12.3 功能详解

基本概念

↘ 访问列表

访问列表有：基本访问列表和动态访问列表。

用户可以根据需要选择基本访问列表或动态访问列表。一般情况下，使用基本访问列表已经能够满足安全需要。但经验丰富的黑客可能会通过一些软件假冒源地址欺骗设备，得以访问网络。而动态访问列表在用户访问网络以前，要求通过身份认证，使黑客难以攻入网络，所以在一些敏感的区域可以使用动态访问列表保证网络安全。

通过假冒源地址欺骗设备即电子欺骗是所有访问列表固有的问题，使用动态列表也会遭遇电子欺骗问题：黑客可能在用户通过身份认证的有效访问期间，假冒用户的地址访问网络。解决这个问题的方法有两种，一种是尽量将用户访问的空闲时间设置小些，这样可以使黑客更难以攻入网络，另一种是使用 IPSEC 加密协议对网络数据进行加密，确保进入设备时，所有的数据都是加密的。

访问列表一般配置在以下位置的网络设备上：

- 内部网和外部网（如 INTERNET）之间的设备
- 网络两个部分交界的设备
- 接入控制端口的设备.

访问控制列表语句的执行必须严格按照表中语句的顺序，从第一条语句开始比较，一旦一个数据包的报头跟表中的某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。

输入/输出 ACL、过滤域模板及规则

输入 ACL 在设备接口接收到报文时，检查报文是否与该接口输入 ACL 的某一条 ACE 相匹配；输出 ACL 在设备准备从某一个接口输出报文时，检查报文是否与该接口输出 ACL 的某一条 ACE 相匹配。

在制定不同的过滤规则时，多条规则可能同时被应用，也可能只应用其中几条。只要是符合某条 ACE，就按照该 ACE 定义的处理报文(Permit 或 Deny)。ACL 的 ACE 根据以太网报文的某些字段来标识以太网报文的，这些字段包括：

二层字段(Layer 2 Fields)：

- 48 位的源 MAC 地址(必须申明所有 48 位)
- 48 位的目的 MAC 地址(必须申明所有 48 位)
- 16 位的二层类型字段

三层字段(Layer 3 Fields)：

- 源 IP 地址字段(可以申明全部源 IP 地址值，或使用子网来定义一类流)
- 目的 IP 地址字段(可以申明全部目的 IP 地址值，或使用子网来定义一类流)
- 协议类型字段

四层字段(Layer 4 Fields)：

- 可以申明一个 TCP 的源端口、目的端口或者都申明，还可以申明源端口或目的端口的范围。
- 可以申明一个 UDP 的源端口、目的端口或者都申明，还可以申明源端口或目的端口的范围。

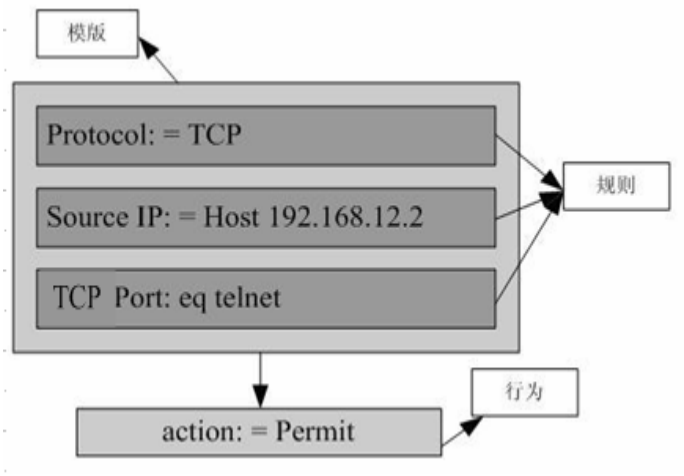
过滤域指的是，在生成一条 ACE 时，根据报文中的哪些字段用以对报文进行识别、分类。过滤域模板就是这些字段组合的定义。比如，在生成某一条 ACE 时希望根据报文的目的 IP 字段对报文进行识别、分类，而在生成另一条 ACE 时，希望根据的是报文的源 IP 地址字段和 UDP 的源端口字段，这样，这两条 ACE 就使用了不同的过滤域模板。

规则(Rules)，指的是 ACE 过滤域模板对应的值。 比如有一条 ACE 内容如下：

```
permit tcp host 192.168.12.2 any eq telnet
```

在这条 ACE 中，过滤域模板为以下字段的集合：源 IP 地址字段、IP 协议字段、目的 TCP 端口字段。对应的值(Rules)分别为：源 IP 地址 = Host 192.168.12.2；IP 协议 = TCP；TCP 目的端口 = Telnet。

图 12-2 对 ACE：permit tcp host 192.168.12.2 any eq telnet 的分析



过滤域模板可以是三层字段(Layer 3 Field)和四层字段(Layer 4 Field)字段的集合，也可以是多个二层字段(Layer 2 Field)的集合，但标准与扩展的 ACL 的过滤域模板不能是二层和三层、二层和四层、二层和三层、四层字段的集合。要使用二层、三层、四层字段集合，可以应用 Expert 扩展访问控制列表（Expert ACLs）。

OUT 方向 ACL 关联 SVI 的注意事项：支持 IP 标准，IP 扩展，MAC 扩展，专家级 ACL 应用。

对 ACL 中匹配目的 IP 和目的 MAC 有一些限制，如果在 MAC 扩展和专家级 ACL 中匹配目的 MAC，将这样的 ACL 应用到 SVI 的 OUT 方向时，表项会被设置，但无法生效。如果想要在 IP 扩展，专家级 ACL 中匹配目的 IP，而目的 IP 不在所关联的 SVI 的子网 IP 范围内时，该配置的 ACL 将无法生效。比如 VLAN 1 的地址为 192.168.64.1 255.255.255.0，创建一条 IP 扩展的 ACL， ace 为 deny udp any 192.168.65.1 0.0.0.255 eq 255，将该 ACL 应用到 VLAN 1 的出口，将无法生效，因为目的 IP 不在 VLAN 1 子网 IP 范围内，如果 ace 为 deny udp any 192.168.64.1 0.0.0.255 eq 255 将可以生效，因为目的 IP 符合规定。

设备上，作用在物理口和 AP 口上的 OUT 方向 ACL，仅支持匹配知名报文（单播、组播），不支持匹配未知名单播，即对于未知名报文或者广播报文，端口上配置的 OUT 方向 ACL 不生效。

当配置专家级的 ACL，并应用在接口的 out 方向时，如果该 ACL 中的某些 ACE 包含三层匹配信息(比如 IP，L4port 等)，将导致从应用接口进入的非 IP 报文无法受该 ACL 的 permit 和 deny 规则控制。

应用 ACL 时，如果 ACL（包括 IP 访问列表和 Expert 扩展访问列表）中的 ACE 匹配了非 L2 字段，比如 SIP，DIP 时，对于带标签的 MPLS 报文匹配是无效的。

功能特性

功能特性	作用
IP访问列表	可以根据 IPv4 报文头部的三层或四层信息对进出设备的 IPv4 报文进行控制。
MAC扩展访问列表	可以根据以太网报文的二层头部信息对进出设备的二层报文进行控制。
Expert扩展访问列表	IP访问列表和MAC扩展访问列表的组合，从而实现在同一条规则中可以实现同时根据报文的二层头部信息和报文三层或四层信息对进出设备的报文进行控制，以决定是丢弃还是放过指定的报文。
IPv6 访问列表	可以根据 IPv6 报文头部的三层或四层信息对进出设备的 IPv6 报文进行控制
安全通道	可以让报文不经过 dot1x、web 认证等接入控制的检查，以满足特定场景的需求
SVI Router ACL	可以同一 VLAN 内的用户可以正常通信

12.3.1 IP访问列表

IP 访问列表主要用于对进出设备的 IPv4 报文进行精细化控制，用户可以根据实际需要阻止或允许特定的 IPv4 报文进入网络，从而实现控制 IP 用户访问网络资源的目的。

工作原理

在 IP 访问列表中定义一系列的 IP 访问规则，然后将访问列表应用在接口的入方向或出方向上，当然还可以对 IP 访问列表进行全局应用，IPv4 报文进出设备时，设备就会通过判断报文是否与规则匹配来决定是否转发或阻断报文。

要在设备上配置访问列表，必须为协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出了可以使用编号来指定访问列表的协议以及每种协议可以使用的访问列表编号范围。

协议	编号范围
标准 IP	1-99，1300 - 1999
扩展 IP	100-199，2000 - 2699

基本访问列表包括标准 IP 访问列表和扩展 IP 访问列表，访问列表中定义的典型规则主要包含以下匹配域：

- 源 IP 地址
- 目的 IP 地址
- IP 协议号
- 四层源端口号或 ICMP type
- 四层目的端口号或 ICMP code

标准 IP 访问列表（编号为 1 - 99，1300 - 1999）主要是根据源 IP 地址来进行转发或阻断分组的，扩展 IP 访问列表（编号为 100 – 199，2000 - 2699）可以对上述匹配域进行组合来控制报文的转发或阻断。

对于单一的访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。不过，使用的语句越多，阅读和理解访问列表就越来越困难。

路由类产品上，ACL 规则中的 ICMP code 匹配域对于 ICMP type 为 3 的 ICMP 报文无效。如果 ACL 规则中配置了要匹配 ICMP 报文的 code 字段，当 type 为 3 的 ICMP 报文进入设备执行 ACL 匹配时，匹配结果可能与预期的不一样。

隐含“拒绝所有数据流”规则语句

在每个 IP 访问列表的末尾隐含着一条“拒绝所有数据流”规则语句，因此如果分组与任何规则都不匹配，将被拒绝。

如下例：

```
access-list 1 permit host 192.168.4.12
```

此列表只允许源主机为 192.168.4.12 的报文通过，其它主机都将被拒绝。因为这条访问列表最后包含了一条规则语句：access-list 1 deny any。

又如：

```
access-list 1 deny host 192.168.4.12
```

如果列表只包含以上这一条语句，则任何主机报文通过该端口时都将被拒绝。

> 在定义访问列表的时候，要考虑到路由更新的报文。由于访问列表末尾“拒绝所有数据流”，可能导致所有的路由更新报文被阻断。

输入规则语句的顺序

加入的每条规则都被追加到访问列表的最后（但在默认规则语句之前），访问列表规则语句的输入次序非常重要，它决定了该规则语句在访问列表中的优先级，设备在决定转发还是阻断报文时，是按规则语句创建的次序将进行比较的，找到匹配的规则语句后，便不再检查其他规则语句。

假设创建了一条规则语句，它允许所有的数据流通过，则后面的语句将不被检查。

如下例：

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255  eq  telnet any
```

由于第一条规则语句拒绝了所有的 IP 报文，所以 192.168.12.0/24 网络的主机 Telnet 报文将被拒绝，因为设备在检查到报文和第一条规则语句匹配，便不再检查后面的规则语句。

相关配置

配置 IP 访问列表

缺省情况下，设备上无任何 IP 访问列表。

在配置模式下使用 **ip access-list** { **standard | extended** } {*acl-name* | *acl-id*} 命令可以创建一个标准 IP 访问列表或扩展 IP 访问列表，并进入标准或扩展 IP 访问列表模式。

配置 IP 访问列表匹配规则

缺省情况下，创建的 IP 访问列表中会有一条隐含的 deny 所有 IPv4 报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有 IPv4 报文，因此，如果用户想允许某些特定的 IPv4 报文进出设备，就得往访问列表中配置一些匹配规则。

对于标准 IP 访问列表，可以通过以下方式配置匹配规则：

- 不管是命名的标准 IP 访问列表，还是数值索引的标准 IP 访问列表，都可以在标准 IP 访问列表模式下使用[*sn*] { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*]命令为访问列表配置一条匹配规则。
- 数值索引的标准 IP 访问列表，除了可以在标准 IP 访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 **access-list** *acl-id* { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*] 命令为标准 IP 访问列表配置一条匹配规则。

对于扩展 IP 访问列表，可以通过以下方式配置匹配规则：

- 不管是命名的扩展 IP 访问列表，还是数值索引的扩展 IP 访问列表，都可以在扩展 IP 访问列表模式下使用[*sn*] { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [[**precedence** *precedence* [**tos** *tos*]] | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*]命令为访问列表配置一条匹配规则。
- 数值索引的扩展 IP 访问列表，除了可以在扩展 IP 访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 **access-list** *acl-id* { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [[**precedence** *precedence* [**tos** *tos*]] | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*]命令为标准 IP 访问列表配置一条匹配规则。

↘ 应用 IP 访问列表

缺省情况下，设备上的所有接口都没有应用 IP 访问列表，也就是说 IP 访问列表不会对进出设备的 IP 报文进行匹配过滤。

在接口模式下使用 **ip access-group** { *acl-id* **|** *acl-name* } { **in** | **out** }[**reflect**] 命令可以让一个标准 IP 访问列表或扩展 IP 访问列表在指定的接口上生效。路由器默认关闭自反 ACL，可以通过配置 **reflect** 启用自反 ACL。自反 ACL 工作原理：a.根据由内网始发流量的第三层和第四层信息自动生成一个临时性的访问表，临时性访问表的创建依据下列原则： IP 协议号不变，源 IP 地址和目的 IP 地址严格对调，TCP/UDP 源端口和目的端口严格对调。b.只有当返回流量的第三、四层信息与先前基于出站流量创建的临时性访问表的第三、四层信息严格匹配时，路由器才会允许此流量进入内部网络。

12.3.2 MAC扩展访问列表

MAC 扩展访问列表主要是基于报文的二层头部来对进出设备的报文进行精细化控制，用户可以根据实际需要阻止或允许特定的二层报文进入网络，从而实现控制保护网络资源不受攻击或者基于些控制用户访问网络资源的目的。

工作原理

在 MAC 扩展访问列表中定义一系列的 MAC 访问规则，将访问列表应用在接口的入方向或出方向上，报文进出设备时，设备就会通过判断报文是否与规则匹配来决定是否转发或阻断报文。

要在设备上配置 MAC 扩展访问列表，必须给访问列表指定一个唯一的名称或编号，以便唯一标识每个访问列表。下表列出可以使用编号来指定 MAC 扩展访问列表编号范围。

协议	编号范围
MAC 扩展访问列表	700-799

MAC 扩展访问列表中定义的典型规则主要有以下：

- 源 MAC 地址
- 目标 MAC 地址
- 以太网协议类型

从上面的规则字段可以看出，MAC 扩展访问列表（编号 700 -799）主要是根据源或目的 MAC 地址以及报文的以太网类型来匹配报文分组的。

对于单一的 MAC 扩展访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。不过，使用的语句越多，阅读和理解访问列表就越来越困难。

如果 MAC 扩展访问列表规则中没有指定是针对 IPv6 报文，即没有定义以太网类型字段或定义的以太网类型字段值不是 0x86dd，那么 MAC 扩展访问列表不对去匹配 IPv6 报文，如果用户想匹配过滤 IPv6 报文，请使用 IPv6 扩展访问列表。

隐含“拒绝所有数据流”规则语句

在每个 MAC 扩展访问列表的末尾隐含着一条“拒绝所有数据流”规则语句，因此如果分组与任何规则都不匹配，将被拒绝。

如下例：

```
access-list 700 permit host 00d0.f800.0001 any
```

此列表只允许来自 MAC 地址为 00d0.f800.0001 的主机发出的报文通过，来自其它主机都将被拒绝。因为这条访问列表最后包含了一条规则语句：access-list 700 deny any any。

相关配置

配置 MAC 扩展访问列表

缺省情况下，设备上无任何 MAC 扩展访问列表。

在配置模式下使用 **mac access-list extended** {*acl-name* | *acl-id* } 命令可以创建一个 MAC 扩展访问列表，并进入 MAC 扩展访问列表模式。

配置 MAC 扩展访问列表匹配规则

缺省情况下，创建的 MAC 扩展访问列表中会有一条隐含的 deny 所有二层报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有二层报文，因此，如果用户想允许某些特定的二层报文进出设备，就得往访问列表中配置一些匹配规则。

可以通过以下方式配置匹配规则：

- 不管是命名的 MAC 扩展访问列表，还是数值索引的 MAC 扩展访问列表，都可以在 MAC 扩展访问列表模式下使用[*sn*] { **permit** | **deny** } {**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos*] [**inner** *cos*] [**time-range** *tm-rng-name*]命令为访问列表配置一条匹配规则。
- 数值索引的 MAC 扩展访问列表，除了可以在 MAC 扩展访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 **access-list** *acl-id* { **permit** | **deny** } {**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos*] [**inner** *cos*] [**time-range** *time-range-name*]命令为 MAC 扩展访问列表配置一条匹配规则。

应用 IP 访问列表

缺省情况下，设备上的所有接口都没有应用 MAC 扩展访问列表，也就是说创建的 MAC 扩展访问列表不会对进出设备的二层报文进行匹配过滤。

在接口模式下使用 **mac access-group** { *acl-id* **|** *acl-name* } { **in** | **out** } 命令可以让一个 MAC 扩展访问列表在指定的接口上生效。

12.3.3 Expert扩展访问列表

如果用户想在同一条规则中既对报文的二层信息匹配，又对报文的三层信息进行匹配，那么就可以选择 Expert 扩展访问列表。可以将 Expert 扩展访问列表看作是 IP 访问列表和 MAC 扩展访问列表的一种结合与增强，之所以说是一种结合与增强，是因为 Expert 扩展访问列表中的规则不仅可以包含 IP 访问列表规则和 MAC 扩展访问列表规则，同时可以指定基于 VLAN ID 来匹配报文。

工作原理

在 Expert 扩展访问列表中定义一系列的访问规则，将访问列表应用在接口的入方向或出方向上，报文进出设备时，设备就会通过判断报文是否与访问规则匹配来决定是否转发或阻断报文。

要在设备上配置 Expert 扩展访问列表，必须给协议的访问列表指定一个唯一的名称或编号，以便在协议内部能够唯一标识每个访问列表。下表列出 Expert 访问列表的编号范围。

协议	编号范围
Expert 扩展访问列表	2700-2899

创建 expert 扩展访问列表时，定义的规则可以应用于所有的分组报文，通过判断分组是否与规则匹配来决定是否转发或阻断分组报文。

Expert 访问列表中定义的典型规则主要有以下：

- 基本访问列表和 MAC 扩展访问列表所有的信息
- VLAN ID

Expert 扩展访问列表（编号 2700 -2899）为基本访问列表和 MAC 扩展访问列表的综合体，并且能对 VLAN ID 进行过滤。

对于单一的 Expert 扩展访问列表来说，可以使用多条独立的访问列表语句来定义多种规则，其中所有的语句需引用同一个编号或名字，以便将这些语句绑定到同一个访问列表。

如果 Expert 扩展访问列表规则中没有指定是针对 IPv6 报文，即没有定义以太网类型字段或以太网类型字段不是 0x86dd，那么 Expert 扩展访问列表不对去匹配 IPv6 报文，如果用户想匹配过滤 IPv6 报文，请使用 IPv6 扩展访问列表。

隐含“拒绝所有数据流”规则语句

在每个 Expert 扩展访问列表的末尾隐含着一条“拒绝所有数据流”规则语句，因此如果分组与任何规则都不匹配，将被拒绝。

如下例：

```
access-list 2700 permit 0x0806 any any any any any
```

此列表只允许以太网类型为 0x0806(即 ARP)的报文通过，其他类型的报文都将被拒绝。因为这条访问列表最后包含了一条规则语句：access-list 2700 deny any any any any。

相关配置

配置 Expert 扩展访问列表

缺省情况下，设备上无任何 Expert 扩展访问列表。

在配置模式下使用 **expert access-list extended** {*acl-name* | *acl-id* } 命令可以创建一个 Expert 扩展访问列表，并进入 Expert 扩展访问列表模式。

配置 Expert 扩展访问列表匹配规则

缺省情况下，创建的 Expert 扩展访问列表中会有一条隐含的 deny 所有报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有二层报文，因此，如果用户想允许某些特定的二层报文进出设备，就得往访问列表中配置一些匹配规则。

可以通过以下方式配置匹配规则：

- 不管是命名的 Expert 扩展访问列表，还是数值索引的 Expert 扩展访问列表，都可以在 Expert 扩展访问列表模式下使用 [*sn*] { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]]命令为访问列表配置一条匹配规则。
- 数值索引的 MAC 扩展访问列表，除了可以在 MAC 扩展访问列表模式下使用前面提到的命令配置匹配规则外，还可以在配置模式下使用 **access-list** *acl-id* { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]]命令为 Expert 扩展访问列表配置一条匹配规则。

应用 Expert 扩展访问列表

缺省情况下，设备上的所有接口都没有应用 Expert 扩展访问列表，也就是说创建的 Expert 扩展访问列表不会对进出设备的所有二三层报文进行匹配过滤。

在接口模式下使用 **expert access-group** { *acl-id* **|** *acl-name* } { **in** | **out** } 命令可以让一个 Expert 扩展访问列表在指定的接口上生效。

12.3.4 IPv6 访问列表

IPv6 访问列表主要用于对进出设备的 IPv6 报文进行精细化控制，用户可以根据实际需要阻止或允许特定的 IPv6 报文进入网络，从而实现控制 IPv6 用户访问网络资源的目的。

工作原理

在IPv6访问列表中定义一系列的IPv6访问规则，并将访问列表应用在接口的入方向或出方向上，IPv6报文进出设备时，设备就会通过判断报文是否与规则匹配来决定是否转发或阻断报文。

要在设备上配置访问列表，必须为协议的访问列表指定一个唯一的名称。

与 IP 访问列表、MAC 扩展访问列表以及 Expert 扩展访问列表不同，创建 IPv6 访问列表时只能指定名称，不能指定编号。

设备接口的入方向或出方向上只能应用一条 IP 访问列表或一条 MAC 扩展访问列表，或者应用一条 Expert 扩展访问列表，除此之外，还可以再应用一条 IPv6 访问列表。

隐含“拒绝所有数据流”规则语句

在每个 IPv6 访问列表的末尾隐含着一条“拒绝所有 IPv6 数据流”规则语句，因此如果报文与任何规则都不匹配，将被拒绝。

如下例：

```
ipv6 access-list ipv6_acl
 10 permit ipv6 host 200::1 any
```

此列表只允许源主机为200::1的IPv6报文通过，其它主机发出的IPv6报文都将被拒绝。因为这条访问列表最后包含了一条规则语句：deny ipv6 any any。

IPv6 访问列表虽然有默认拒绝所有 IPv6 报文的规则语句，但不会过滤 ND 报文。

输入规则语句的顺序

加入的每条规则都被追加到访问列表的最后（但在默认规则语句之前），访问列表规则语句的输入次序非常重要，它决定了该规则语句在访问列表中的优先级，设备在决定转发还是阻断报文时，是按规则语句创建的次序将进行比较的，找到匹配的规则语句后，便不再检查其他规则语句。

假设创建了一条规则语句，它允许所有的IPv6数据流通过，则后面的语句将不被检查。

如下例：

```
ipv6 access-list ipv6_acl
 10 permit ipv6 any any
 20 deny ipv6 host 200::1 any
```

由于第一条规则语句放过了所有的IPv6报文，所以主机200::1发出的IPv6报文都无法命中序号为20的那条deny规则而被放过。因为设备在检查到报文和第一条规则语句匹配，便不再检查后面的规则语句。

相关配置

配置 IPv6 访问列表

缺省情况下，设备上无任何IPv6访问列表。

在配置模式下使用 **ipv6 access-list** *acl-name* 命令可以创建一个IPv6访问列表，并进入IPv6访问列表模式。

配置 IPv6 访问列表匹配规则

缺省情况下，创建的 IPv6 访问列表中会有一条隐含的 deny 所有 IPv6 报文的匹配规则，这条表项对用户不可见，但当将访问列表应用在接口上时，就会生效，也就是会丢弃所有 IPv6 报文，因此，如果用户想允许某些特定的 IPv6 报文进出设备，就得往访问列表中配置一些匹配规则。

在 IPv6 访问列表模式下使用[*sn*] {**permit** | **deny** } *protocol* {*src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any**} {*dst-ipv6-pfix/pfix-len* | **host** *dst-ipv6-addr* | **any**} [**range** *lower upper*] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range***tm-rng-name*]命令配置一条 IPv6 访问列表规则。

应用 IPv6 访问列表

缺省情况下，设备上的所有接口都没有应用任何 IPv6 访问列表，也就是说 IPv6 访问列表不会对进出设备的 IPv6 报文生效。

在接口模式下使用 **ipv6 traffic-filter** *acl-name* { **in** | **out** } 命令可以让一个 IPv6 访问列表在指定的接口上生效。

12.3.5 安全通道

在某些应用场景中，可能会需要保证符合某些特征的报文绕过接入控制应用的检查，比如 dot1x 认证前，要允许用户登录到指定的资源站点上下载 dot1x 认证客户端；使用安全通道可以达到这个目的。将安全 ACL 通过安全通道配置命令应用到全局或者接口，就表示该 ACL 是一条安全通道

工作原理

安全通道其实也是一个访问控制列表，可以基于全局或者接口配置。报文进入到接口时，首先进行安全通道的检查，如果满足安全通道的匹配条件，将绕过接入控制比如端口安全，web 认证、dot1x，Ip+MAC 绑定的检查直接进入交换机。应用于全局的安全通道对所有非例外口都生效。

- 应用于安全通道的访问控制列表的 deny 行为不生效，并且不存在末尾隐含着一条“拒绝所有数据流”规则的语句，如果报文不符合安全通道的匹配条件，将按流程进行接入控制的检查；
- 全局安全通道的例外口最多可以设置 8 个且全局安全通道的例外口不能用来设置基于接口的安全通道。
- 如果接口上应用了安全通道，并且还存在全局的安全通道，那么全局安全通道不在这个接口上生效。
- 基于端口可迁移认证模式和安全通道共用时，安全通道不生效。
- 不支持将 IPv6 访问列表配置成安全通道。
- 仅在交换机设备上支持安全通道。

相关配置

配置访问列表

在配置安全通道功能之前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表、MAC 扩展访问列表以及 Expert 扩展访问列表的相关章节说明。

配置接口安全通道

缺省情况下，设备上无任何的接口安全通道配置。

在接口模式下使用 **security access-group** {*acl-id* | *acl-name* }命令配置接口安全通道。

配置全局安全通道

缺省情况下，设备上无任何的全局安全通道配置。

在配置模式下使用 **security global access-group** {*acl-id* | *acl-name* }命令配置全局安全通道。

配置全局安全通道例外口

缺省情况下，设备上无任何的全局安全通道例外口配置。

在接口模式下使用 **security uplink enable** 命令将指定接口配置为全局安全通道例外口。

12.3.6 SVI Router ACL

默认情况下，应用在 SVI 接口上的访问列表会同时对 VLAN 内二层转发的报文及 VLAN 间的路由报文生效，从而导致同一 VLAN 内不同用户之间无法正常通信等异常现象。为此，提供了一种切换手段，可以使得应用在 SVI 接口上的访问列表仅对 VLAN 间的路由报文生效。

工作原理

缺省情况下，SVI Router ACL 功能默认关闭，SVI ACL 同时对 VLAN 间的三层转发报文及 VLAN 内的桥转发报文生效。SVI Router ACL 功能开启后，SVI ACL 仅对 VLAN 间的三层转发报文生效。

相关配置

配置访问列表

在配置带 SVI Router ACL 之前，一般来说要先配置访问列表应用，在应用访问列表前，必须先配置访问列表，访问列表的配置说明请参考相关的章节。

配置访问列表规则

访问列表规则的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

应用访问列表

访问列表的应用配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。应用时，在 SVI 对应的接口模式应用。

配置 SVI Router ACL

全局模式使用 **svi router-acls enable** 命令开启 SVI Router ACL 功能，使得应用在 SVI 接口上的访问列表仅对三层转发的报文生效，而不对同一 VLAN 内二层转发的报文生效。

12.4 配置详解

配置项	配置建议 & 相关命令	
配置IP访问列表功能	⚠ 可选配置。用于匹配过滤 IPv4 报文。	
	ip access-list standard	配置 IP 标准访问列表
	ip access-list extended	配置 IP 标准访问列表
	permit host any time-range	配置 permit 类型的 IP 标准访问列表规则
	deny host any time-range	配置 deny 类型的 IP 标准访问列表规则
	permit host any host any tos dscp precedence fragment time-range	配置 permit 类型的 IP 扩展访问列表规则
	deny host any host any tos dscp precedence fragment time-range	配置 deny 类型的 IP 扩展访问列表规则
	ip access-group in out	应用 IP 标准或 IP 扩展访问列表
配置MAC扩展访问列表	⚠ 可选配置。用于匹配过滤二层报文	
	mac access-list extended	配置 MAC 扩展访问列表
	permit any host any host cos inner time-range	配置 permit 类型的 MAC 扩展访问列表规则
	deny any host any host cos inner time-range	配置 deny 类型的 MAC 扩展访问列表规则
	mac access-group in out	应用 MAC 扩展访问列表
配置Expert扩展访问列表	⚠ 可选配置。用于匹配过滤二三层报文	
	expert access-list extened	配置 Expert 扩展访问列表
	permit cos inner VID inner host any host any host any host any precedence tos fragment range time-range	配置 permit 类型的 Expert 扩展访问列表规则
	deny cos inner VID inner host any host any host any host any precedence tos fragment range time-range	配置 deny 类型的 Expert 扩展访问列表规则
	expert access-group in out	应用 Expert 扩展访问列表
配置IPv6 访问列表	⚠ 可选配置。用于匹配过滤 IPv6 报文	
	ipv6 access-list	配置 IPv6 访问列表
	permit host any host any range dscp flow-label fragment time-range	配置 permit 类型的 IPv6 访问列表规则

	deny host any host any range dscp flow-label fragment time-range	配置 deny 类型的 IPv6 访问列表规则
	ipv6 traffic-filter in out	应用 IPv6 扩展访问列表
配置安全通道	⚠ 可选配置。用于符合规则的报文直接跳过接入控制各种应用（比如 dot1x，web 认证）的检查。	
	security access-group	在接口模式下开启安全通道功能
	security global access-group	在配置模式下开启安全通道功能
	security uplink enable	在接口模式下将该接口配置成全局安全通道的例外口
配置访问列表注释信息	⚠ 可选配置。用于为访问列表或访问列表规则配置注释信息便于用户识别。	
	list-remark	在访问列表模式下为访问列表配置注释信息
	access-list list-remark	在全局模式为访问列表配置注释信息。
	remark	在访问列表模式下为规则配置注释信息

12.4.1 配置IP访问列表

配置效果

通过配置 IP 访问列表，并将访问列表应用到设备的接口上，就可以对在该接口进出的所有 IPv4 报文进行控制，禁止或允许特定的 IPv4 报文进入网络，从而实现控制 IP 用户访问网络资源的目的。

注意事项

无

配置方法

↘ 配置 IP 访问列表

- 必须配置。要实际针对 IPv4 用户访问网络资源的控制，首先必须配置 IP 访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。IP 访问列表只对被配置的设备上有效，不会影响网络中的其他设备。

↘ 配置 IP 访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有 IPv4 报文进入设备。

↘ 应用 IP 访问列表

- 必须配置。要使得 IP 访问列表真正生效，就必须将 IP 访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 IP 访问列表。

检验方法

可以通过以下方法检验 IP 访问列表的配置效果：

- 通过 ping 的方式检查 IP 访问列表是否真的在指定接口上生效。比如，IP 访问列表里配置了禁止某个 IP 主机或某个 IP 范围的主机不允许访问网络，通过 ping 的方式检验是否真的 ping 不通来验证。
- 通过访问网络相关资源的方式来检验 IP 访问列表是否真的在指定接口上生效，比如访问 internet 网，或通过 ftp 访问网络上的 ftp 资源等。

相关命令

配置 IP 访问列表

【命令格式】 **ip access-list** { **standard | extended** } {*acl-name* | *acl-id* }

【参数说明】 **standard**：该选项若被配置，表示要创建一个标准 IP 访问列表。

extended：该选项若被配置，表示要创建一个扩展 IP 访问列表。

acl-name：该选项若被配置，表示创建一个命名的标准 IP 或扩展 IP 访问列表，长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头，也不能为“in”或“out”。

acl-id：为访问列表编号，以此来唯一标识一条访问列表，该选项若被配置，表示创建一个数值索引的标准 IP 或扩展 IP 访问列表，如果创建的是标准 IP 访问列表，*acl-id* 的取值范围为 1-99，1300 – 1999，如果创建的是扩展 IP 访问列表，*acl-id* 的取值范围为 100-199，2000 – 2699。

【命令模式】 配置模式

【使用指导】 此命令可以用来配置标准 IP 或扩展 IP 访问列表，并进入标准 IP 或扩展 IP 访问列表配置模式。如果只想通过检查报文的源 IP 地址来控制用户的网络资源访问权限，那么可以配置标准 IP 访问列表；如果想通过检查报文的源 IP 地址、目的 IP 地址、报文的协议号、TCP/UDP 源或目的端口号来控制用户的网络资源访问权限，那么就需要配置扩展 IP 访问列表。

配置 IP 访问列表规则

- 为标准 IP 访问列表配置规则。

  有两种方式可以为标准 IP 访问列表配置规则：

【命令格式】 [*sn*] { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*]

【参数说明】 *sn*：为规则表项的序号，取值范围为[1，2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的。

permit：该选项若被配置，表示本规则属于允许通过类的；

deny：该选项若被配置，关键字表示本规则属于禁止通过类的；

host *source*：该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；
any：该选项若被配置，表示要匹配任意主机发出的 IP 报文；
source source-wildcard：该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；
time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

【命令模式】 标准 IP 访问列表模式
【使用指导】 此命令在标准 IP 访问列表模式下为访问列表配置规则，该访问列表可以是命名访问列表，也可以是数字索引的访问列表。

【命令格式】 **access-list** *acl-id* { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*]
【参数说明】 *acl-id*：数值索引访问列表的编号，以此来唯一标识一条访问列表。取值范围为： 1-99，1300 - 1999
permit：该选项若被配置，表示本规则属于允许通过类的；
deny：该选项若被配置，关键字表示本规则属于禁止通过类的；
host *source*：该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；
any：该选项若被配置，表示要匹配任意主机发出的 IP 报文；
source source-wildcard：该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；
time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

【命令模式】 标准 IP 访问列表模式
【使用指导】 此命令在配置模式下为数字索引的 IP 访问列表配置规则。这种配置方式无法为命名的标准 IP 访问列表配置规则。

- 为扩展 IP 访问列表配置规则。

  有两种方式可以为扩展 IP 访问列表配置规则：

【命令格式】 [*sn*] { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [[**precedence** *precedence* [**tos** *tos*]] | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*]
【参数说明】 *sn*：规则表项的序号，取值范围为[1，2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的
permit：该选项若被配置，表示本规则属于允许通过类的；
deny：该选项若被配置，关键字表示本规则属于禁止通过类的；
protocol： IP 协议号，取值范围[0，255]；为方便使用，系统提供了常用 IP 协议号的简称以取代对应的 IP 协议号具体数值，包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp。

host *source*：该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；
source source-wildcard：该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；
host *destination*：该选项若被配置，表示要匹配目的 IP 为某一台特定主机的 IP 报文；**any** 关键字表示要匹配发往任意主机的 IP 报文。
destination destination-wildcard：该选项若被配置，表示要匹配目标为某一个 IP 网段主机的报文。
any：该选项若被配置，表示要匹配任意主机发出的 IP 报文或者要匹配发往任意主机的 IP 报文；
precedence *precedence*：该选项若被配置，表示要匹配 IP 报文头部中的优先级域。
tos *tos*：该选项若被配置，表示要匹配 IP 报文头部中的服务类型域。
dscp *dscp*：该选项若被配置，表示要匹配 IP 报文头部的 dscp 域。
fragment：该选项若被配置，表示只要匹配非首片的 IP 分片报文。
time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

【命令模式】 扩展 IP 访问列表模式
【使用指导】 此命令在扩展 IP 访问列表模式下为访问列表配置规则，该访问列表可以是命名访问列表，也可以是数字索引的访问列表。

【命令格式】 **access-list** *acl-id* { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [[**precedence** *precedence* [**tos** *tos*]] | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*]
【参数说明】 *acl-id*：数值索引访问列表的编号，以此来唯一标识一条访问列表。取值范围为：100-199，2000 - 2699
sn：规则表项的序号，取值范围为[1，2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的
permit：该选项若被配置，表示本规则属于允许通过类的；
deny：该选项若被配置，关键字表示本规则属于禁止通过类的；
protocol： IP 协议号，取值范围[0，255]；为方便使用，系统提供了常用 IP 协议号的简称以取代对应的 IP 协议号具体数值，包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp。
host *source*：该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；
source source-wildcard：该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；
host *destination*：该选项若被配置，表示要匹配目的 IP 为某一台特定主机的 IP 报文；**any** 关键字表示要匹配发往任意主机的 IP 报文。
destination destination-wildcard：该选项若被配置，表示要匹配目标为某一个 IP 网段主机的报文。
any：该选项若被配置，表示要匹配任意主机发出的 IP 报文或者要匹配发往任意主机的 IP 报文；
precedence *precedence*：该选项若被配置，表示要匹配 IP 报文头部中的优先级域。
tos *tos*：该选项若被配置，表示要匹配 IP 报文头部中的服务类型域。
dscp *dscp*：该选项若被配置，表示要匹配 IP 报文头部的 dscp 域。
fragment：该选项若被配置，表示只要匹配非首片的 IP 分片报文。

time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

【命令模式】 扩展 IP 访问列表模式

【使用指导】 此命令在配置模式下为数字索引的 IP 访问列表配置规则。这种配置方式无法为命名的标准 IP 访问列表配置规则。

应用 IP 访问列表

【命令格式】 **ip access-group** { *acl-id* **|** *acl-name* } { **in** | **out** } [**reflect**]

【参数说明】 *acl-id*：该选项若被配置，表示要将一个数值索引的标准 IP 或扩展 IP 访问列表应用在接口上。

acl-name：该选项若被配置，表示要将一个命名的标准 IP 或扩展 IP 访问列表应用在接口上。

in：该选项若被配置，表示这个访问列表对进入该接口的 IP 报文进行控制。

out：该选项若被配置，表示这个访问列表对从该接口发出的 IP 报文进行控制。

reflect: 该选项若被配置，表示启用自反 ACL。

【命令模式】 接口模式

【使用指导】 此命令可以让 IP 访问列表在指定的接口上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

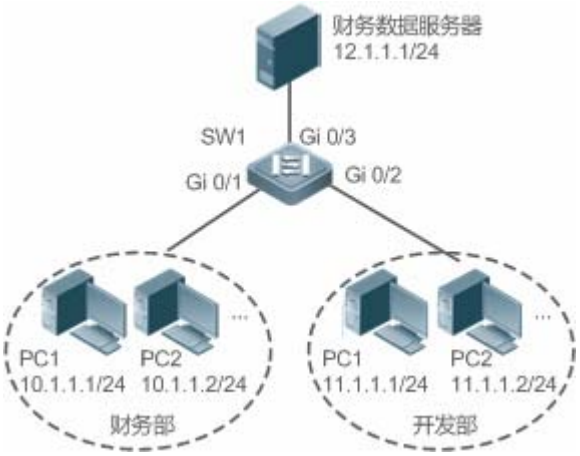
配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

通过 IP 访问列表，禁止财务部以外的部门访问财务数据服务器

【网络环境】

图 12-3



【配置方法】

- 配置 IP 访问列表
- 在 IP 访问列表中添加访问规则
- 将 IP 访问列表应用在连接财务数据服务器接口的出方向上

SW1

```
sw1(config)#ip access-list standard 1
sw1(config-std-nacl)#permit 10.1.1.0 0.0.0.255
```

```
sw1(config-std-nacl)#deny 11.1.1.1 0.0.0.255
sw1(config-std-nacl)#exit
sw1(config)#int gigabitEthernet 0/3
sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 out
```

【检验方法】
- 从开发部的某台 PC 机上 ping 财务数据服务器，确认 ping 不通。
- 从财务部的某台 PC 机上 ping 财务数据服务器，确认 ping 得通

SW1

```
sw1(config)#show access-lists

ip access-list standard 1
 10 permit 10.1.1.0 0.0.0.255
 20 deny 11.1.1.0 0.0.0.255

sw1(config)#show access-group
ip access-group 1 out
Applied On interface GigabitEthernet 0/3
```

12.4.2 配置MAC扩展访问列表

配置效果

通过配置 MAC 扩展访问列表，并将访问列表应用到设备的接口上，就可以对在该接口进出的所有二层报文进行控制，禁止或允许特定的二层报文进入网络，从而实现基于二层报文头来控制用户访问网络资源的目的。

注意事项

无

配置方法

配置 MAC 扩展访问列表

- 必须配置。要基于二层报文头信息（比如用户 PC 的 MAC 地址）控制用户访问网络资源的权限，首先必须配置 MAC 扩展访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。MAC 扩展访问列表只在被配置的设备上有效，不会影响网络中的其他设备。

配置 MAC 扩展访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有以太网二层报文进入设备。

应用 MAC 扩展访问列表

- 必须配置。要使得 MAC 扩展访问列表真正生效，就必须将 MAC 扩展访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 MAC 扩展访问列表。

检验方法

可以通过以下方法检验 MAC 扩展访问列表的配置效果：

- 如果 MAC 扩展访问列表希望放过或过滤某些 IP 报文，可以通过 ping 的方式检查这样的 MAC 扩展访问列表规则是否真的在指定接口上生效。比如，MAC 扩展访问列表里配置了禁止以太网类型为 0x0800 即 IP 报文从接口进入设备，可以通过 ping 的方式检验是否真的 ping 不通来验证。
- 如果 MAC 扩展访问列表希望放过或过滤某些非 IP 报文，比如 ARP 报文，这种报文也可以通过 ping 的方式检查这样的 MAC 扩展访问列表规则是否真的在指定接口上生效，比如想过滤掉 ARP 报文，可以通过 ping 的方式检验是否真的 ping 不通来验证。
- 另外，还可以通过构造符合指定特征的二层报文来检验 MAC 扩展访问列表是否真的生效。典型地可以使用两台 PC 机，一台构造二层报文并发送，另一台开启抓包软件抓包，根据访问列表规则指定的动作检查报文的转发是否如预期(转发或不转发) 。

相关命令

配置 MAC 扩展访问列表

【命令格式】 **mac access-list extended** {*acl-name* | *acl-id* }

【参数说明】 *acl-name*：该选项若被配置，表示创建一个命名的 MAC 扩展访问列表，长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头，也不能为“in”或“out”。

acl-id：为访问列表编号，以此来唯一标识一条访问列表，该选项若被配置，表示创建一个数值索引的 MAC 扩展访问列表，取值范围为 700-799。

【命令模式】 配置模式

【使用指导】 此命令可以用来配置 MAC 扩展访问列表，并进入 MAC 扩展访问列表配置模式。如果想通过检查以太网报文的二层信息来控制用户的网络资源访问权限，那么就可以配置 MAC 扩展访问列表。

配置 MAC 扩展访问列表规则

有两种方法为 MAC 扩展访问列表配置规则：

- 在 MAC 扩展访问列表模式中配置规则

【命令格式】 [*sn*] { **permit** | **deny** } {**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos* [**inner** *cos*]] [**time-range** *tm-rng-name*]

【参数说明】 *sn*：为规则表项的序号，取值范围为[1，2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号

就为 11，此外，递增值是可以通过命令调整的。

permit：该选项若被配置，表示本规则属于允许通过类的；

deny：该选项若被配置，关键字表示本规则属于禁止通过类的；

any：该选项若被配置，表示要匹配任意主机发出的二层报文；

host *src-mac-addr*：该选项若被配置，表示要匹配源 MAC 为某一台主机发出的二层报文；

any：该选项若被配置，表示要匹配目的为任意主机发出的二层报文；

host *dst-mac-addr*：该选项若被配置，表示要匹配目的 MAC 为某一台主机的二层报文；

ethernet-type：该选项若被配置，表示要匹配指定以太网类型的二层报文；

cos *cos*：该选项若被配置，表示要匹配二层报文里的外层 TAG 的优先级字段；

inner *cos*：该选项若被配置，表示要匹配二层报文里的内层 TAG 的优先级字段；

time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

【命令模式】 MAC 扩展访问列表模式

【使用指导】 此命令在 MAC 扩展访问列表模式下为访问列表配置规则，该访问列表可以是命名访问列表，也可以是数字索引的访问列表。

- 在全局模式中为 MAC 扩展访问列表配置规则

【命令格式】 **access-list** *acl-id* { **permit** | **deny** } {**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos* [**inner** *cos*]] [**time-range** *tm-rng-name*]

【参数说明】 *acl-id*：数值索引访问列表的编号，以此来唯一标识一条访问列表。取值范围为：700-799

permit：该选项若被配置，表示本规则属于允许通过类的；

deny：该选项若被配置，关键字表示本规则属于禁止通过类的；

host *src-mac-addr*：该选项若被配置，表示要匹配源 MAC 为某一台主机发出的二层报文；

host *source*：该选项若被配置，表示要匹配源 MAC 为某一台主机发出的二层报文；

any：该选项若被配置，表示要匹配目的为任意主机发出的二层报文；

host *dst-mac-addr*：该选项若被配置，表示要匹配目的 MAC 为某一台主机的二层报文；

ethernet-type：该选项若被配置，表示要匹配指定以太网类型的二层报文；

cos *cos*：该选项若被配置，表示要匹配二层报文里的外层优先级字段；

inner *cos*：该选项若被配置，表示要匹配二层报文里的内层优先级字段；

time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册。

【命令模式】 全局模式

【使用指导】 此命令在配置模式下为数字索引的 MAC 扩展访问列表配置规则。这种配置方式无法为命名的 MAC 扩展访问列表配置规则。

应用 MAC 扩展访问列表

【命令格式】 **mac access-group** { *acl-id* | *acl-name* } { **in** | **out** }

【参数说明】 *acl-id*：该选项若被配置，表示要将一个数值索引的 MAC 扩展访问列表应用在接口上。

acl-name：该选项若被配置，表示要将一个命名的 MAC 扩展访问列表应用在接口上。

in：该选项若被配置，表示这个访问列表对进入该接口的二层报文进行控制。

out：该选项若被配置，表示这个访问列表对从该接口发出的二层报文进行控制。

【命令模式】 接口模式

【使用指导】 此命令可以让 MAC 扩展访问列表在指定的接口上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

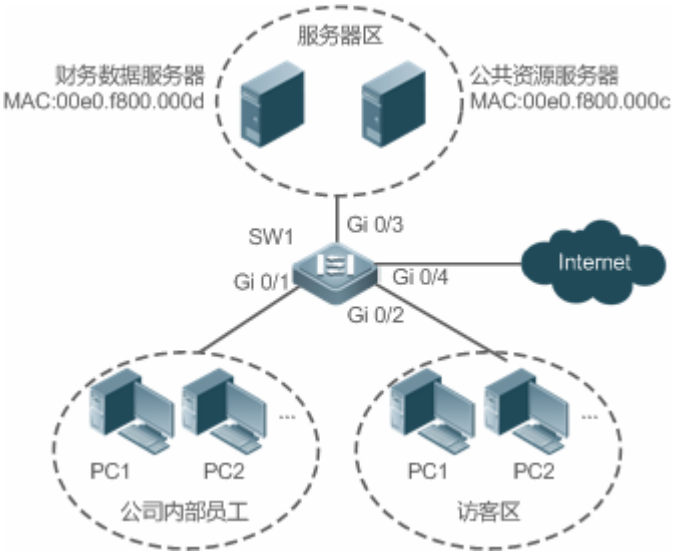
配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

通过 MAC 扩展访问列表，限制来访客户可访问的资源

【网络环境】

图 12-4



【配置方法】

- 配置 MAC 扩展访问列表
- 在 MAC 扩展访问列表中添加访问规则
- 将 MAC 扩展访问列表应用在连接访客区接口的出方向上，允许访客 PC 访问 Internet 以及公司内部的公共服务器，但不允许访问公司的账务数据服务器，即禁止访问 MAC 地址为 00e0.f800.000d 的服务器。

SW1

```
sw1(config)#mac access-list extended 700
sw1(config-mac-nacl)#deny any host 00e0.f800.000d
sw1(config-mac-nacl)#permit any any
sw1(config-mac-nacl)#exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)#mac access-group 700 in
```

【检验方法】

- 从访客 PC 机上 ping 财务数据服务器，确认 ping 不通。
- 从访问 PC 机上 ping 公共资源服务器，确认可以 ping 得通。
- 在访问 PC 机上访问 Internet，比如访问百度，确认可以打开主页。

SW1

```
sw1(config)#show access-lists
mac access-list extended 700
```

```
 10 deny any host 00e0.f800.000d etype-any
 20 permit any any etype-any
sw1(config)#show access-group
mac access-group 700 in
Applied On interface GigabitEthernet 0/2
```

12.4.3 配置Expert扩展访问列表

配置效果

通过配置 Expert 扩展访问列表，并将访问列表应用到设备的接口上，可以同时基于二层和三层信息对在该接口进出的报文进行控制，禁止或允许特定的报文进入网络；另外，还可以通过配置 Expert 扩展访问列表实现基于 VLAN 来对所有二层报文进行控制，从而实现允许或拒绝某些网段的用户访问网络资源。一般来说，如果想在一条访问列表中混合使用 IP 访问规则以及 MAC 扩展访问规则时，就可以使用 Expert 扩展访问列表

注意事项

无

配置方法

配置 Expert 扩展访问列表

- 必须配置。要基于二层报文头信息(比如 VLAN ID)控制用户访问网络资源的权限，首先必须配置 Expert 扩展访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。Expert 扩展访问列表只在被配置的设备上有效，不会影响网络中的其他设备。

配置 Expert 扩展访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有报文进入设备。

应用 Expert 扩展访问列表

- 必须配置。要使得 Expert 扩展访问列表真正生效，就必须将访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口的入或出方向上应用 Expert 扩展访问列表。

检验方法

可以通过以下方法检验 Expert 扩展访问列表的配置效果：

- 如果 Expert 扩展访问列表中配置了 IP 访问规则，放过或过滤某些 IP 报文，通过 ping 的方式来检验规则是否生效。

- 如果 Expert 扩展访问列表中配置了 MAC 访问规则，放过或过滤某些二层报文，比如 ARP 报文，这种报文也可以通过 ping 的方式检查这样的 MAC 访问列表规则是否真的在指定接口上生效，比如想过滤掉 ARP 报文，可以通过 ping 的方式检验是否真的 ping 不通来验证。
- 如果 Expert 扩展访问列表中配置了带有 VLAN ID 的访问规则，希望放过或过滤某些二层网段的报文，典型假设不想让 VLAN 1 的用户与 VLAN 2 的用户互访问，可以在 VLAN 1 所在的 PC 机上 ping VLAN 2 的 PC 机，如果 ping 不通就表示规则生效。

相关命令

配置 Expert 扩展访问列表

【命令格式】 **expert access-list extended** {*acl-name* | *acl-id* }

【参数说明】 *acl-name*：该选项若被配置，表示创建一个命名的 Expert 扩展访问列表，长度范围[1，99]。访问列表名称不能以数字 0 - 9 开头，也不能为“in”或“out”。

acl-id：为访问列表编号，以此来唯一标识一条访问列表，该选项若被配置，表示创建一个数值索引的 Expert 扩展访问列表，取值范围为 2700-2899。

【命令模式】 配置模式

【使用指导】 此命令可以用来配置 MAC 扩展访问列表，并进入 Expert 扩展访问列表配置模式。

配置 Expert 扩展访问列表规则

有两种方法为 Expert 扩展访问列表配置规则：

- 在 Expert 扩展访问列表模式中配置规则

【命令格式】 [*sn*] { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]]

【参数说明】 *sn*：为规则表项的序号，取值范围为[1，2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的。

permit：该选项若被配置，表示本规则属于允许通过类的；

deny：该选项若被配置，关键字表示本规则属于禁止通过类的；

protocol：IP 协议号，取值范围[0, 255]；为方便使用，系统提供了常用 IP 协议号的简称以取代对应的 IP 协议号具体数值，包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp

ethernet-type：该选项若被配置，表示要匹配指定以太网类型的二层报文；

cos *out*：该选项若被配置，表示要匹指定二层报文外层 TAG 中的优先级字段；

cos inner *in*：该选项若被配置，表示要匹指定二层报文内层 TAG 中的优先级字段；

VID *out*：该选项若被配置，表示要匹指定二层报文外层 TAG 中的 VLAN ID 字段；

VID inner *in*：该选项若被配置，表示要匹指定二层报文内层 TAG 中的 VLAN ID 字段；

source source-wildcard：该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；
host *source*：该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；
any：该选项若被配置，表示要匹配任意主机发出的 IP 报文；
host *source-mac-address*：该选项若被配置，表示要匹配源 MAC 为某一台主机发出的二层报文；
any：该选项若被配置，表示要匹配目的为任意主机发出的二层报文；
destination destination-wildcard：该选项若被配置，表示要匹配目标为某一个 IP 网段的报文；
host *destination*：该选项若被配置，表示要匹配目的 IP 为某一台主机的 IP 报文；
any：该选项若被配置，表示要匹配发往任意目标的 IP 报文；
host *destination-mac-address*：该选项若被配置，表示要匹配目的 MAC 为某一台主机的二层报文；
any：该选项若被配置，表示要匹配目标为任意主机的二层报文；
precedence *precedence*：该选项若被配置，表示要匹配 IP 报文头部中的优先级域。
tos *tos*：该选项若被配置，表示要匹配 IP 报文头部中的服务类型域。
dscp *dscp*：该选项若被配置，表示要匹配 IP 报文头部的 dscp 域。
fragment：该选项若被配置，表示只要匹配非首片的 IP 分片报文。
time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

【命令模式】 Expert 扩展访问列表模式

【使用指导】 此命令在 Expert 扩展访问列表模式下为访问列表配置规则，该访问列表可以是命名访问列表，也可以是数字索引的访问列表。

- 在全局模式下为 Expert 扩展访问列表配置规则

【命令格式】 **access-list** *acl-id* { **permit** | **deny** } [*protocol* | [*ethernet-type*] [**cos** [*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] { *source source-wildcard* | **host** *source* | **any** } { **host** *source-mac-address* | **any** } { *destination destination-wildcard* | **host** *destination* | **any** } { **host** *destination-mac-address* | **any** } [**precedence** *precedence*] [**tos** *tos*] [**fragment**] [**range** *lower upper*] [**time-range** *time-range-name*]]

【参数说明】 *acl-id*：数值索引访问列表的编号，以此来唯一标识一条访问列表。取值范围为：2700-2899
permit：该选项若被配置，表示本规则属于允许通过类的；
deny：该选项若被配置，关键字表示本规则属于禁止通过类的；
protocol：IP 协议号，取值范围[0, 255]；为方便使用，系统提供了常用 IP 协议号的简称以取代对应的 IP 协议号具体数值，包括 eigrp、gre、icmp、igmp、ip、ipinip、nos、ospf、tcp、udp
ethernet-type：该选项若被配置，表示要匹配指定以太网类型的二层报文；
cos *out*：该选项若被配置，表示要匹指定二层报文外层 TAG 中的优先级字段；
cos inner *in*：该选项若被配置，表示要匹指定二层报文内层 TAG 中的优先级字段；
VID *out*：该选项若被配置，表示要匹指定二层报文外层 TAG 中的 VLAN ID 字段；
VID inner *in*：该选项若被配置，表示要匹指定二层报文内层 TAG 中的 VLAN ID 字段；
source source-wildcard：该选项若被配置，表示要匹配某一个 IP 网段的内主机发出的报文；
host *source*：该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IP 报文；
any：该选项若被配置，表示要匹配任意主机发出的 IP 报文；
host *source-mac-address*：该选项若被配置，表示要匹配源 MAC 为某一台主机发出的二层报文；
any：该选项若被配置，表示要匹配目的为任意主机发出的二层报文；
destination destination-wildcard：该选项若被配置，表示要匹配目标为某一个 IP 网段的报文；
host *destination*：该选项若被配置，表示要匹配目的 IP 为某一台主机的 IP 报文；

any：该选项若被配置，表示要匹配发往任意目标的 IP 报文；

host *destination-mac-address*：该选项若被配置，表示要匹配目的 MAC 为某一台主机的二层报文；

any：该选项若被配置，表示要匹配目标为任意主机的二层报文；

precedence *precedence*：该选项若被配置，表示要匹配 IP 报文头部中的优先级域。

tos *tos*：该选项若被配置，表示要匹配 IP 报文头部中的服务类型域。

dscp *dscp*：该选项若被配置，表示要匹配 IP 报文头部的 dscp 域。

fragment：该选项若被配置，表示只要匹配非首片的 IP 分片报文。

time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册。

【命令模式】 Expert 扩展访问列表模式

【使用指导】 此命令在配置模式下为数字索引的 Expert 扩展访问列表配置规则。这种配置方式无法为命名的 Expert 扩展访问列表配置规则。

应用 Expert 扩展访问列表

【命令格式】 **expert access-group** { *acl-id* **|** *acl-name* } { **in** | **out** }

【参数说明】

acl-id：该选项若被配置，表示要将一个数值索引的 Expert 扩展访问列表应用在接口上。

acl-name：该选项若被配置，表示要将一个命名的 Expert 扩展访问列表应用在接口上。

in：该选项若被配置，表示这个访问列表对进入该接口的二层报文进行控制。

out：该选项若被配置，表示这个访问列表对从该接口发出的二层报文进行控制。

【命令模式】 接口模式

【使用指导】 此命令可以让 Expert 扩展访问列表在指定的接口上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

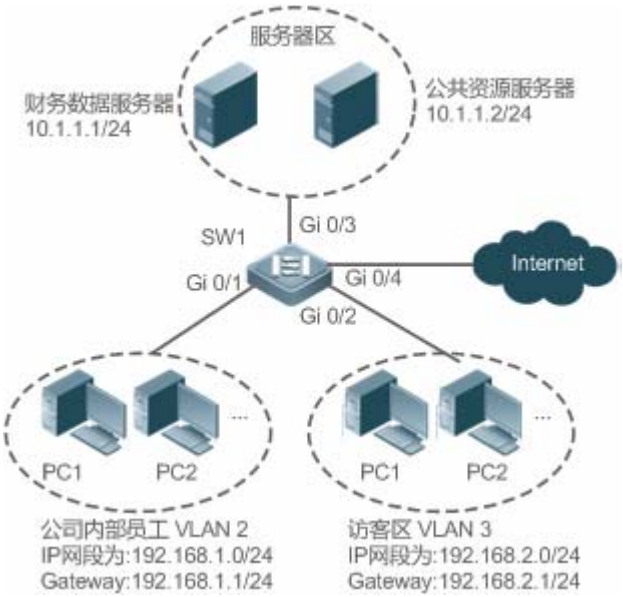
配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

通过 Expert 扩展访问列表，限制来访客区户可访问的资源，要求访客不能与公司内部员工互访，但能访问公共资源服务器，且不能访问公司核心的账务数据服务器。

【网络环境】

图 12-5



【配置方法】

- 配置 Expert 扩展访问列表
- 在访问列表中添加规则，禁止访客区 VLAN 3 网段内主机发出目标为内部员工 VLAN2 网段的报文进入网络。
- 在访问列表中添加规则，禁止访客访问核心账务数据服务器规则，
- 再添加一条规则，允许所有报文通过；
- 最后再将访问列表应用在与访客区相连交换机接口的入方向上。

SW1

```
sw1(config)#expert access-list extended 2700
sw1(config-exp-nacl)#deny ip any any 192.168.1.0 0.0.0.255 any
sw1(config-exp-nacl)#deny ip any any host 10.1.1.1 any
sw1(config-exp-nacl)#pemit any any any any
sw1(config-exp-nacl)#exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)#expert access-group 2700 in
```

【检验方法】

- 从访客 PC 机上 ping 财务数据服务器，确认 ping 不通。
- 从访客 PC 机上 ping 公共资源服务器，确认可以 ping 得通。
- 从访客 PC 机上 ping 公司内部员工网关 192.168.1.1，确定 ping 不通。
- 在访问 PC 机上访问 Internet，比如访问百度，确认可以打开主页。

SW1

```
sw1(config)#show access-lists
expert access-list extended 2700
 10 deny ip any any 192.168.1.0 0.0.0.255 any
 20 deny ip any any host 10.1.1.1 any
 30 permit ip any any any any

sw1(config)#show access-group
```

```
expert access-group 2700 in
Applied On interface GigabitEthernet 0/2
```

12.4.4 配置IPv6 扩展访问列表

配置效果

通过配置 IPv6 访问列表，并将访问列表应用到设备的接口上，就可以对在该接口进出的所有 IPv6 报文进行控制，禁止或允许特定的 IPv6 报文进入网络，从而实现控制 IPv6 用户访问网络资源的目的。

注意事项

无

配置方法

配置 IPv6 访问列表

- 必须配置。要实际针对 IPv6 用户访问网络资源的控制，首先必须配置 IPv6 访问列表。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。IPv6 访问列表只对被配置的设备上有效，不会影响网络中的其他设备。

配置 IPv6 访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，默认禁止所有 IPv6 报文进入设备。

应用 IPv6 访问列表

- 必须配置。要使得 IPv6 访问列表真正生效，就必须将 IPv6 访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 IPv6 访问列表。

检验方法

可以通过以下方法检验 IPv6 访问列表的配置效果：

- 通过 ping 的方式检查 IPv6 访问列表是否真的在指定接口上生效。比如，IPv6 访问列表里配置了禁止某个 IPv6 主机或某个 IPv6 地址范围内的主机不允许访问网络，可以通过 ping 的方式检验是否真的 ping 不通来验证。
- 通过访问网络相关资源的方式来检验 IPv6 访问列表是否真的在指定接口上生效，比如访问 IPv6 网站等。

相关命令

配置 IPv6 访问列表

【命令格式】 **ipv6 access-list** *acl-name*

【参数说明】 *acl-name*：该选项若被配置，表示创建一个命名的标准 IP 或扩展 IP 访问列表，长度范围[1, 99]。访问列表名称不能以数字 0 - 9 开头，也不能为“in”或“out”。

【命令模式】 配置模式

【使用指导】 此命令可以用来配置 IPv6 访问列表，并进入 IPv6 访问列表配置模式。

配置 IPv6 访问列表规则

- 当要匹配 TCP 或 UDP 报文时。可以使用如下方式为 IPv6 访问列表配置规则：

【命令格式】 [*sn*] {**permit** | **deny** } *protocol* {*src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any**} {*dst-ipv6-pfix/pfix-len* | **host** *dst-ipv6-addr* | **any**} [*op dstport* | **range** *lower upper*] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range***tm-rng-name*]

【参数说明】 *sn*：为规则表项的序号，取值范围为[1，2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的。

permit：该选项若被配置，表示本规则属于允许通过类的；

deny：该选项若被配置，关键字表示本规则属于禁止通过类的；

protocol： IPv6 协议号，取值范围[0，255]；为方便使用，系统提供了常用 IPv6 协议号的简称以取代对应的协议号具体数值，包括 **icmp**、**ipv6**、**tcp**、**udp**。

src-ipv6-prefix/prefix-len：该选项若被配置，表示要匹配某一个 IPv6 网段的内主机发出的报文；

host *src-ipv6-addr*：该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IPv6 报文;

any：该选项若被配置，表示要匹配任意主机发出的 IPv6 报文；

dst-ipv6-pfix/pfix-len：该选项若被配置，表示要匹配目标 IP 是某一个 IPv6 网段的内主机的 IPv6 报文；

host *dst-ipv6-addr*：该选项若被配置，表示要匹配目标 IP 为某一台主机的 IPv6 报文;

any：该选项若被配置，表示要匹配发往任意主机的 IPv6 报文；

op dstport：该选项若被配置，表示要匹配 TCP 或 UDP 报文中的四层目的端口号，其中 op 参数可以是 **eq**、**neq**、**gt**、**lt**，分别对应等于、不等于、大于、小于这四个不同的操作；

range *lower upper*：该选项若被配置，表示要匹配 TCP 或 UDP 报文中某个范围内的四层目的端口号；

dscp *dscp*：该选项若被配置，表示要匹配 IPv6 报文头部的 dscp 域；

flow-label *flow-label*：该选项若被配置，表示要匹配 IPv6 报文头部的流标签域；

fragment：该选项若被配置，表示只要匹配非首片的 IPv6 分片报文；

time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

【命令模式】 IPv6 访问列表模式

【使用指导】 此命令在 IPv6 访问列表模式下为访问列表配置规则。

- 当要匹配 TCP 或 UDP 以外的 IPv6 报文时。可以使用如下方式为标准 IPv6 访问列表配置规则：

【命令格式】 [*sn*] { **permit** | **deny** } *protocol* { *src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any** } { *dst-ipv6-pfix/pfix-len* | **host** *dst-ipv6-addr* | **any** } [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range***tm-rng-name*]

【参数说明】 *sn*：为规则表项的序号，取值范围为[1，2147483647]。这个序号决定了这条规则表项在该访问列表中的优先级，序号越小，优先级越大，优先级大的会优先去匹配报文。如果配置匹配规则时没有指定序号，系统会自动分配一个序号，序号的分配原则为在当前访问列表最后一条匹配规则的序列基础之上加上一个递增值，递增值默认为 10，假设当前访问列表最后一条匹配规则的序号为 100，则缺省情况下新增的这条匹配规则序号就为 11，此外，递增值是可以通过命令调整的。

permit：该选项若被配置，表示本规则属于允许通过类的；

deny：该选项若被配置，关键字表示本规则属于禁止通过类的；

protocol： IPv6 协议号，取值范围[0，255]；为方便使用，系统提供了常用 IPv6 协议号的简称以取代对应的协议号具体数值，包括 **icmp**、**ipv6**、**tcp**、**udp**。

src-ipv6-prefix/prefix-len：该选项若被配置，表示要匹配某一个 IPv6 网段的内主机发出的报文；

host *src-ipv6-addr*：该选项若被配置，表示要匹配源 IP 为某一台主机发出的 IPv6 报文;

any：该选项若被配置，表示要匹配任意主机发出的 IPv6 报文；

dst-ipv6-pfix/pfix-len：该选项若被配置，表示要匹配目标 IP 是某一个 IPv6 网段的内主机的 IPv6 报文；

host *dst-ipv6-addr*：该选项若被配置，表示要匹配目标 IP 为某一台主机的 IPv6 报文;

any：该选项若被配置，表示要匹配发往任意主机的 IPv6 报文；

dscp *dscp*：该选项若被配置，表示要匹配 IPv6 报文头部的 dscp 域；

flow-label *flow-label*：该选项若被配置，表示要匹配 IPv6 报文头部的流标签域；

fragment：该选项若被配置，表示只要匹配非首片的 IPv6 分片报文；

time-range *time-range-name*：该选项若被配置，表示该匹配规则关联了一个时间区，只有在指定的时间区间内该规则才会生效，否则不生效，更多关于关时间区的描述，请参考 time range 的配置手册

【命令模式】 IPv6 访问列表模式

【使用指导】 此命令在 IPv6 访问列表模式下为访问列表配置规则。

应用 IPv6 访问列表

【命令格式】 **ipv6 traffic-filter** *acl-name* { **in** | **out** }

【参数说明】 *acl-name*： IPv6 访问列表的名称。

in：该选项若被配置，表示这个访问列表对进入该接口的 IPv6 报文进行控制。

out：该选项若被配置，表示这个访问列表对从该接口发出的 IPv6 报文进行控制。

【命令模式】 接口模式

【使用指导】 此命令可以让 IPv6 访问列表在指定的接口上生效，同时需要指定对进入设备的报文生效，还是从设备转发出去的报文生效。

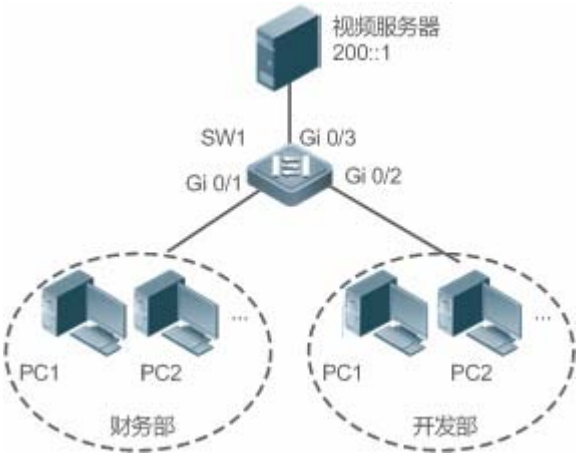
配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

↘ 通过 IPv6 访问列表，禁止开发部门访问视频服务器

【网络环境】

图 12-6



【配置方法】

- 配置 IP6 访问列表
- 在 IPv6 访问列表中添加禁止访问视频服务器 IPv6 地址规则
- 在 IPv6 访问列表中添加允许所有 IPv6 报文通过规则
- 将 IPv6 访问列表应用在开发部门所在接口的入方向上

SW1

```
sw1(config)#ipv6 access-list dev_deny_ipv6video
sw1(config-ipv6-nacl)#deny ipv6 any host 200::1
sw1(config-ipv6-nacl)#permit ipv6 any any
sw1(config-ipv6-nacl)#exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6video in
```

【检验方法】

- 从开发部的某台 PC 机上 ping 视频服务器，确认 ping 不通。

SW1

```
sw1(config)#show access-lists

ipv6 access-list dev_deny_ipv6video
 10 deny ipv6 any host 200::1
 20 permit ipv6 any any

sw1(config)#show access-group
ipv6 traffic-filter dev_deny_ipv6video in
Applied On interface GigabitEthernet 0/2
```

12.4.5 配置安全通道

配置效果

通过配置安全通道功能，可以使得符合安全通道规则的报文绕过接入控制相关业务。如果用户上联的设备接口上开启了某个接入控制应用比如 dot1x，但在进行 dot1x 认证前，又要允许用户登录到某个站点上下载一些资源（比如下载锐捷 SU 客户端），这种情况就可以通过配置安全通道来实现。

注意事项

无

配置方法

配置访问列表

- 必须配置。要实现安全通道功能，首先要配置访问列表，访问列表的配置方法请参考相关章节说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。配置仅在本设备上有效，不会影响网络中的其他设备。

配置访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，相当于安全通道功能不生效。访问列表规则配置请参考相关章节的说明。

配置接口安全通道或全局安全通道

- 如果想让安全通道在接口上生效，就在接口上配置安全通道；如果想让安全通道全局生效，就要配置全局安全通道，必须配置其中之一。
- 可以根据用户的分布，在接入、汇聚或核心设备配置安全通道功能。

配置全局安全通道例外口

- 可选配置。如果配置了全局安全通道，但又不想让安全通道在某些接口上生效，就需要将这些接口配置为全局安全通道的例外口。

配置接入控制应用

- 可选配置，为了验证安全通道功能，可以在接口上开启 dot1x 或 web 认证功能。
- 可以根据用户的分布，在接入、汇聚或核心设备配置接入控制功能。

检验方法

可以通过在受接入控制业务控制的用户 PC 机上 ping 安全通道指定放过的资源（设备或服务器）来验证安全通道。

相关命令

配置访问列表

访问列表的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

配置访问列表规则

访问列表规则的配置方法请参考IP访问列表、MAC扩展访问列表、Expert扩展访问列表以及IPv6访问列表的相关章节说明。

配置接口安全通道

【命令格式】 **security access-group** {*acl-id* | *acl-name* }

【参数说明】 *acl-id*：该选项若被配置，表示要将指定编号的访问列表配置成安全通道。

acl-name：该选项若被配置，表示要将指定的命名访问列表配置成安全通道

【命令模式】 接口模式

【使用指导】 通过该命令在指定接口上将指定的 ACL 配置成安全通道。

配置全局安全通道

【命令格式】 **security global access-group** {*acl-id* | *acl-name* }

【参数说明】 *acl-id*：该选项若被配置，表示要将指定编号的访问列表配置成安全通道。

acl-name：该选项若被配置，表示要将指定的命名访问列表配置成安全通道

【命令模式】 配置模式

【使用指导】 通过该命令将指定的 ACL 配置成全局安全通道。

配置全局安全通道例外口

【命令格式】 **security uplink enable**

【参数说明】 无

【命令模式】 接口模式

【使用指导】 通过该命令将指定的接口配置成全局安全通道例外口。

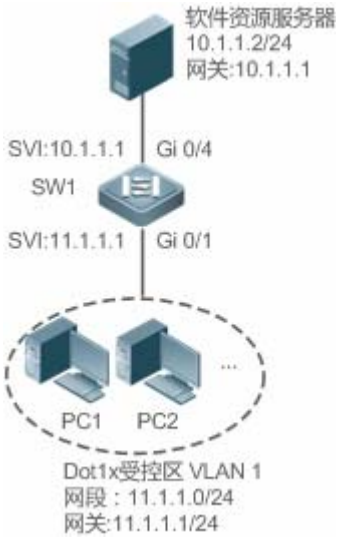
配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

在 dot1x 认证环境中，通过安全通道，允许用户认证前从服务器上下载 SU 客户端软件

【网络环境】

图 12-7



【配置方法】

- 配置 Expert 扩展访问列表 exp_ext_esc
- 在访问列表中添加允许目的主机 10.1.1.2 地址规则
- 在访问列表中添加允许 DHCP 报文通过规则
- 在访问列表中添加允许 ARP 报文通过规则
- 在 dot1x 受控区接口上将访问列表 exp_ext_esc 配置为安全通道

SW1

```
sw1(config)#expert access-list extended exp_ext_esc
sw1(config-exp-nacl)# permit ip any any host 10.1.1.2 any
sw1(config-exp-nacl)# permit 0x0806 any any any any any
sw1(config-exp-nacl)# permit tcp any any any any eq 67
sw1(config-exp-nacl)# permit tcp any any any any eq 68
sw1(config)#int gigabitEthernet 0/1
sw1(config-if-GigabitEthernet 0/1)# security access-group exp_ext_esc
```

【检验方法】

- 在销售部内的某台 PC 机 ping 销售服务器地址，确认可以 ping 得通。
- 在研发一部和研发二部的 PC 机上 ping 销售服务器地址，确认 ping 不通。

```
sw1#show access-lists
expert access-list extended exp_ext_esc
 10 permit ip any any host 10.1.1.2 any
 20 permit arp any any any any any
 30 permit tcp any any any any eq 67
 40 permit tcp any any any any eq 68……

sw1#show running-config interface gigabitEthernet 0/1

Building configuration...
Current configuration : 59 bytes
```

```
interface GigabitEthernet 0/1
 security access-group exp_ext_esc
```

12.4.6 配置基于时间区的规则

配置效果

如果想让访问列表的某些规则在指定的时间生效，或在指定的时间内失效，比如让 ACL 在一个星期的某些时间段内生效等。可以配置基于时间区的访问列表规则 .

注意事项

无

配置方法

配置访问列表

- 必须配置。要实现基于时间区生效的规则，首先要配置访问列表，访问列表的配置方法请参考相关章节说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。配置仅在本设备上有效，不会影响网络中的其他设备。

配置带时间区的访问列表规则

- 必须配置。配置时需要带上对应的时间区选项，时间区的配置请参考时间区相关的配置手册。

应用访问列表

- 必须配置。要使得访问列表规则在指定的时间区内生效，就必须访问列表应用到设备的特定接口上。
- 可以根据用户的分布，在接入、汇聚或核心设备的指定接口上应用 IP 访问列表。

检验方法

在生效时间区内，可以通过 ping 或构造符合规则报文的方式来进行检验规则是否生效来检验；在失效时间区内，可以通过 ping 或构造符合规则报文的方式来进行检验规则是否不生效来检验。

相关命令

配置访问列表

访问列表的配置命令请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

配置带时间区的访问列表规则

访问列表规则的配置命令请参考IP访问列表、MAC扩展访问列表、Expert扩展访问列表以及IPv6访问列表的相关章节说明。

应用访问列表

访问列表规则的应用命令请参考IP访问列表、MAC扩展访问列表、Expert扩展访问列表以及IPv6访问列表的相关章节说明。

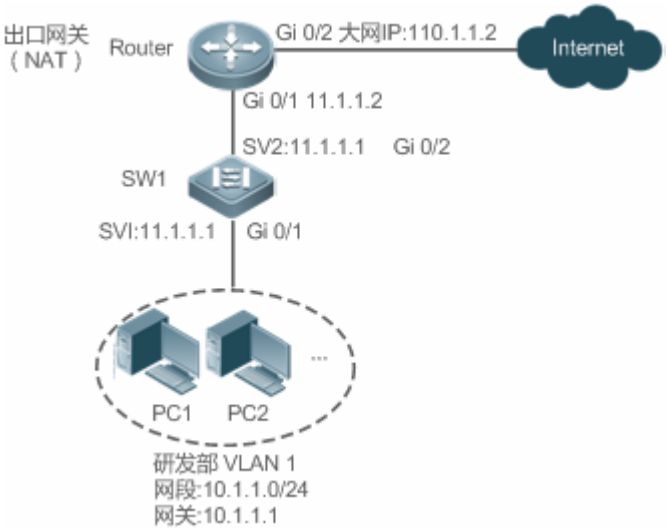
配置举例

以下配置举例，仅介绍与 ACL 相关的配置。

配置基于时间区的访问列表规则，只允许研发部门在每天的 12:00 到 13:30 访问 internet

【网络环境】

图 12-8



【配置方法】

- 配置名称为 access-internet 的时间区，并添加每天 12:00 到 13:30 的时间段表项。
- 配置 IP 访问列表 ip_std_internet_acl。
- 在访问列表中添加允许源 IP 网段为 10.1.1.0/24 的地址规则，关联的时间区为 access-internet。
- 在访问列表中添加禁止源 IP 网段为 10.1.1.0/24 的地址规则。表明时间区之外都不允许访问 internet
- 在访问列表中添加允许所有的地址规则
- 将访问列表应用在设备与出口网关相连接口的出方向上。

SW1

```
Ruijie(config)# time-range access-internet
Ruijie(config-time-range)# periodic daily 12:00 to 13:30
Ruijie(config-time-range)# exit
sw1(config)# ip access-list standard ip_std_internet_acl
sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet
sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255
sw1(config-std-nacl)# permit any
sw1(config-std-nacl)# exit
sw1(config)#int gigabitEthernet 0/2
sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl out
```

【检验方法】
- 在时间区生效期内（12:00 至 13:30），从研发部分内的某台 PC 机访问百度主页，确认可以访问。
- 在时间区失效期（12:00 至 13:30 这个时段外），从研发部分内的某台 PC 机访问百度主页，确认不能访问。

SW1

```
sw1#show time-range

time-range entry: access-internet (inactive)
  periodic Daily 12:00 to 13:30

sw1#show access-lists

ip access-list standard ip_std_internet_acl
 10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive)
 20 deny 10.1.1.0 0.0.0.255
 30 permit any

sw1#show access-group
ip access-group ip_std_internet_acl out
Applied On interface GigabitEthernet 0/2
```

12.4.7 配置访问列表注释信息

配置效果

在实际的网络维护过程中，如果配置了很多访问列表且没有为这些访问列表配置注释信息，时间一长往往会难以区分这些访问列表的用途。为访问列表配置注释信息，可以方便理解 ACL 用途．

注意事项

无

配置方法

↘ 配置访问列表

- 必须配置。要实现安全通道功能，首先要配置访问列表，访问列表的配置方法请参考相关章节说明。
- 可以根据用户的分布情况，在接入、汇聚或核心设备上配置。配置仅在本设备上有效，不会影响网络中的其他设备。

↘ 配置访问列表注释信息

- 可选配置。为便于管理和理解所配置的访问列表，可以为访问列表配置注释信息。

配置访问列表规则

- 可选配置。访问列表里允许无规则，没有配置规则时，相当于安全通道功能不生效。访问列表规则配置请参考相关章节的说明。

配置访问列表规则注释信息

- 可选配置。为便于理解所配置的访问列表，除了可以为访问列表本身配置注释信息外，还可以为规则配置注释信息。

检验方法

可以通过在设备上使用 **show access-lists** 命令验证访问列表注释信息，。

相关命令

配置访问列表

访问列表的配置方法请参考 IP 访问列表、MAC 扩展访问列表、Expert 扩展访问列表以及 IPv6 访问列表的相关章节说明。

配置访问列表注释信息

有以下两种方式为访问列表配置注释信息：

【命令格式】 **list-remark** *comment*

【参数说明】 *comment*：注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符

【命令模式】 访问列表模式

【使用指导】 通过该命令为指定的访问列表配置注释信息

【命令格式】 **access-list** *acl-id* **list-remark** *comment*

【参数说明】 *acl-id*：访问列表编号

comment：注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符

【命令模式】 配置模式

【使用指导】 通过该命令为指定的访问列表配置注释信息

配置访问列表规则

访问列表规则的配置方法请参考IP访问列表、MAC扩展访问列表、Expert扩展访问列表以及IPv6访问列表的相关章节说明。

配置访问列表规则注释信息

有以下两种方式为访问列表规则配置注释信息：

【命令格式】 **remark** *comment*

【参数说明】 *comment*：注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符

【命令模式】 访问列表模式

【使用指导】 通过该命令为指定的访问列表规则配置注释信息

【命令格式】 **access-list** *acl-id* **remark** *comment*

【参数说明】 *acl-id*：访问列表编号

comment：注释信息。长度[1, 100]，超过 100 个字符将被截短至 100 个字符

【命令模式】 配置模式

【使用指导】 通过该命令为访问列表规则添加注释信息

配置举例

无

12.5 监视与维护

清除各类信息

作用	命令
清除访问列表报文匹配计数	**clear counters access-list** [*acl-id* | *acl-name*]

查看运行情况

作用	命令
查看基本访问列表	**show access-lists** [*acl-id* | *acl-ame*] [**summary**]
显示指定接口上绑定的重定向表项，不输入接口则显示所有接口上绑定的重定向表项。	**show redirect** [**interface** *interface-name*]
显示接口上应用的访问列表配置信息。	**show access-group** [**interface** *interface-name*]
显示接口上应用的 IP 访问列表配置信息。	**show ip access-group** [**interface** *interface-name*]
显示接口上应用的 MAC 扩展访问列表配置信息。	**show mac access-group** [**interface** *interface-name*]
显示接口上应用的 Expert 扩展访问列表配置信息。	**show expert access-group** [**interface** *interface-name*]
显示接口上应用的 IPv6 访问列表配置信息。	**show ipv6 traffic-filter** [**interface** *interface-name*]

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令

监视访问列表运行过程信息	**debug acl acld event**
调试查看 ACL 客户端的信息	**debug acl acld client-show**
调试查看所有 ACL 客户端创建的访问列表信息	**debug acl acld acl-show**

13 SCC

13.1 概述

SCC (Security Control Center，安全控制中心)为各种接入控制和网络安全业务提供了公共的配置方法和策略整合服务，从而使得各种接入控制业务以及网络安全业务能够在一台设备上共存，实现多元化的接入安全控制需求，以满足不同的接入场景需要。

典型的接入控制业务如 dot1x、web 认证、arp check、ip source guard 等；网络安全业务如 ACL、NFPP、防网关 ARP 欺骗等。当设备上同时开启两个或两个以上的上述接入控制业务或网络安全业务时，或者同时开启接入控制业务和网络安全业务时，SCC 通过相关的策略整合负责协调共存关系。

有关接入控制和网络安全业务相关的说明请参考相应的配置指南，下文仅介绍 SCC 的相关内容。

协议规范

无

13.2 典型应用

典型应用	场景描述
高校大二层校园网访问控制应用	在高校校园网中学生可通过 dot1x 客户端认证上网或通过 web 认证来上网，同时要防止相互间 ARP 欺骗。另外，允许某些部门（比如校长办公室）的终端设备无需认证就能上网。

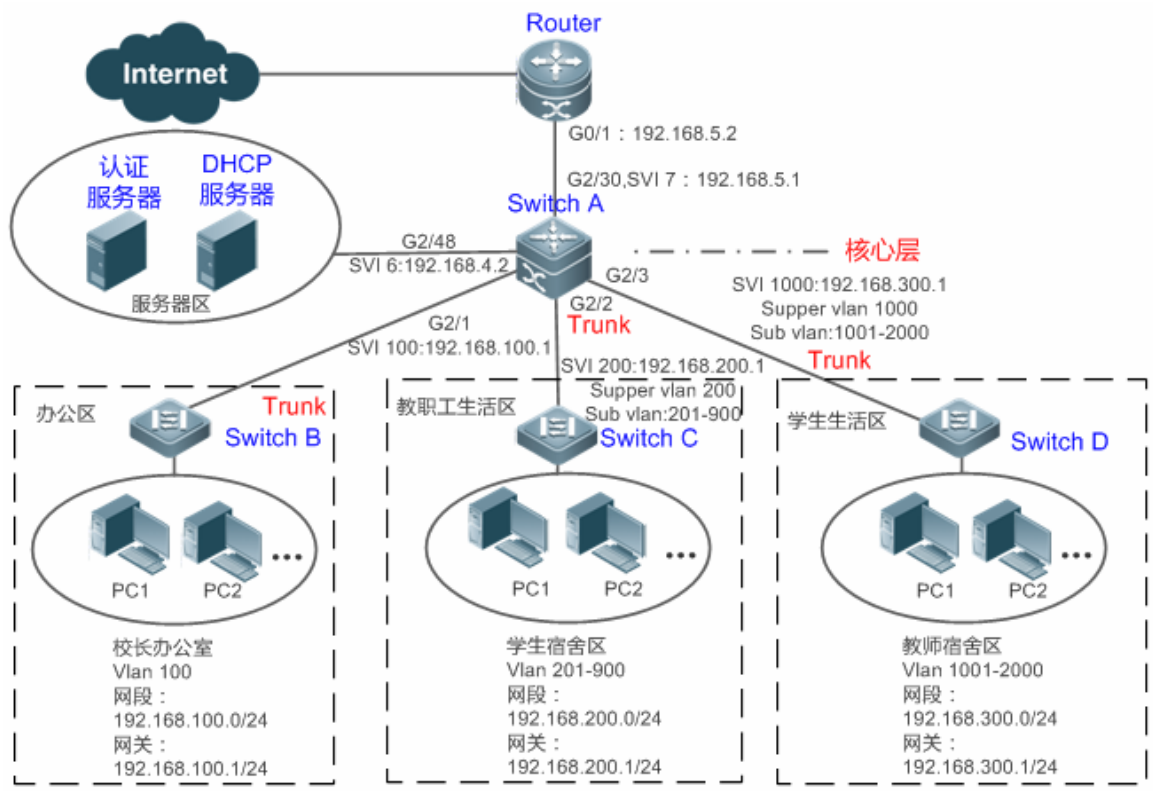
13.2.1 高校大二层校园网访问控制应用

应用场景

在高校校园网中，学生上网前一般都需要前进行 1x 认证或 web 认证，从而方便计费，以保障高校的利益：

- 学生可以通过 dot1x 客户端认证上网，也可以通过 web 认证上网。
- 防止学生相互间进行 ARP 欺骗，以保证网络的稳定性。
- 允许某些部门（如校长办公室）的终端无需认证就能上网。

图 13-1



【注释】 传统的高校校园网网络是分层设计的，有接入层、汇聚层和核心层，用户接入控制在接入层上完成；而在高校大二层校园网中，用户的接入控制是由核心设备来承担的，核心设备以下都是二层设备，中间不再有汇聚。核心设备与用户接入交换设备（如上图的 switch B、switch C 以及 switch D）之间都是 TRUNK 口。

接入层设备 B、C、D：连接各部门的 PC，各个接入端口配置成 Acess 口，VLAN 与核设备对应下联端口上配置的 SUB VLAN 相对应，这样每个接入用户处于不同的 VLAN 中，防止相互间进行 arp 欺骗。

核心层设备 A：连接各种服务器，如认证服务器、DHCP 服务器等。并在下联端口上配置 Supper VLAN 和 Sub VLAN。一个 Super VLAN 对应多个 Sub vlan，每个 Sub VLAN 代表一个接入用户。

功能部属

- 核心设备上通过 vlan + 端口号来区分不同的接入用户，每个接入用户（当然也可以是一组用户）一个 vlan。接入层设备下联用户的端口配置成 Access 口，并按规划为每个用户配置一个用户 vlan，核心设备上不转发 ARP 请求报文，只有被请求用户已认证才作应答，以此来达到防止用户间的 ARP 欺骗问题。核心设备 switch A 上面将用户 VLAN 作为 Sub VLAN，并配置 Super VLAN 以及将 Super VLAN 对应的 SVI 配置成用户网关。
- 通过在核心设备（本例为设备 A）下联教职工生活区和学生生活区的端口上同时开启 dot1x 认证和 web 认证功能来达到由用户自由选择使用哪种认证方式的目的。
- 对于特殊部门（本例为校长办公室）可以划到单独特定的一个 VLAN 中，通过配置这个 VLAN 为免认证 VLAN 的方式来达到不需要通过认证即可上网的目的。

13.3 功能详解

基本概念

用户在线检测

对于计费用户来说，用户认证上线之后就会开始计费，用户离开时需要主动下线才能真正结束计费过程，但有可能用户上网结束离开时忘记了主动下线或者因终端原因无法主动下线等原因，继续产生上网费用从而导致用户的经济损失。为了更加精确地判断用户是否真的在上网，可以预设在一个时间段内用户流量低于某个值或者在一个时间段内用户无流量时就认为用户没有使用网络，直接将该用户进行下线操作。

功能特性

功能特性	作用
用户在线检测	可以指定是否对在线用户进行流量检测，在一段时间内流量低于某个值时设备主动将用户下线。

13.3.1 用户在线检测

用户在上好网之后，有可能会忘了点下线或者由于终端缘故无法主动下线，这个时候会造成持续计费而招致经济损失。在这种情况下，为了保障上网用户的利益，设备提供了判断用户是否在线即用户在线检测功能，由设备来判断用户是否真的在线，如果设备认为用户不在线，主动将该用户进行下线。

工作原理

在设备上预设一个指定的检测周期，在这个周期内如果用户流量低于某个值时就认为此时用户没有使用网络，从而直接将该用户进行下线操作。

用户在线检测功能仅针对通过 dot1x 认证或 web 认证上线的用户。

13.3.2 用户策略规则

用户认证成功后，服务器有可能会下发该用户的一些控制策略名称，此时，需要 scc 对控制策略名称进行解析，并转化成功对应的策略规则，进行安装生效。

工作原理

在设备上先配置相关的策略名称，策略下可配置具体限速策略和过滤策略，用户认证通过后，同时设置这个策略名称时，相应的限速策略和过略策略生效。

策略配置仅针对通过 dot1x 认证或 web 认证上线的用户。

13.4 配置详解

配置项	配置建议 & 相关命令	
配置用户在线检测	⚠ 可选配置。用于指定是否开启用户在线检测功能	
	offline-detect interval thredshold	配置用户在线检测参数
	no offline-detect	关闭用户在线检测功能
	default offline-detect	恢复成缺省的用户在线检测方式
配置用户策略规则	⚠ 可选配置。用于指定用户策略使用的具体规则	
	[no] rate-policy	进入限速策略配置模式。
	upstream average-rate burst-rate	配置上行限速流量平均值和突发值。
	no upstream	删除上行限速流量配置
	downstream average-rate burst-rate	配置下行限速流量平均值和突发值。
	no downstream	删除下行限速流量配置
	[no] filter-policy	进入过滤策略配置模式。
	filter-acl	配置过滤策略关联的安全 acl
	no filter-acl	删除过滤策略关联的安全 acl
	[no] service-policy	进入用户策略配置模式。
	rate-policy apply	配置使用的限速策略。
	no rate-policy	删除使用的限速策略
	filter-policy apply	配置使用的过滤策略
	no filter-policy	删除使用的过滤策略

13.4.1 配置用户在线检测

配置效果

当配置了认证用户在线检测功能后，在指定的周期内如果流量低于一定的门限，设备会自动将用户下线，以免造成持续计费而导致用户的经济损失。

注意事项

配置如果配置无流量下线，需要注意的是，终端一般来说都会默认运行 360 安全卫士等软件，这些软件会时不时地往外发送报文，此时，只有终端关机的情况下设备才会将用户下线、

配置方法

↘ **配置用户在线检测**

- 可选配置。默认为 8 小时内无流量就将用户下线。
- 只对被配置的设备上有效，不会影响网络中的其他设备。

流量门限参数 thredshold 如果配置成 0，则表示进行无流量检测。

【命令格式】 **offline-detect interval** *interval* **thredshold** *thredshold*
no offline-detect
default offline-detect

【参数说明】 *interval*：下线检测周期，交换机设备上取值范围为 6-65535min；非交换机设备取值范围为 1-65535min。默认 8 小时，即 480min。
thredshold：流量门限，取值范围为 0-4294967294Bytes。默认为 0，表示无流量检测下线。
no offline-detect：关闭用户在线检测功能。
default offline-detect：恢复成默认值，即 8 小时无流量就将已在线认证用户下线。

【缺省配置】 8 小时

【命令模式】 全局模式

【使用指导】 此命令可以用来配置用户在线活，指定在一定的时间段内在线认证用户的流量低于指定的门限时将用户下线。使用 **no offline-detect** 命令关闭用户在线检测功能，使用 **default offline-detect** 恢复成缺省的检测方式。

检验方法

可以通过以下方法检验认证用户在线检测的配置效果：

- 配置了在线用户检测功能后，用户上线后，将指定的已认证终端关机，然后等待指定的周期，在设备上使用 dot1x 或 web 认证提供的在线用户查询命令确认指定的用户已经下线。

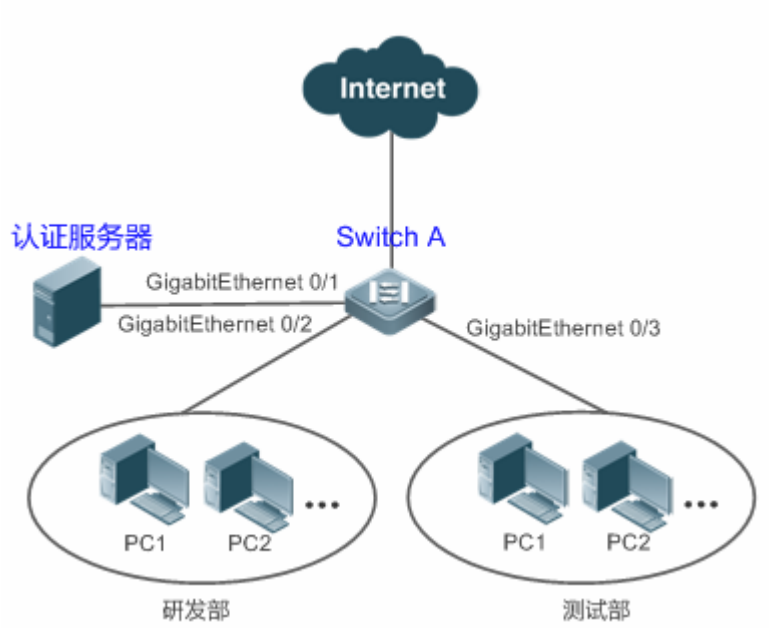
配置举例

以下配置举例，仅介绍与 SCC 相关的配置。

通过用户在线检测功能，指定 5min 内无流量就将用户下线。

【网络环境】

图 13-2



【配置方法】

- 在接入端口 Gi 0/2 上开启 dot1x 受控，并配置认证所需参数，基于 MAC 认证
- 配置用户在线检测功能，指定 5min 内无流量就将用户下线。

Switch A

```
sw1(config)# offline-detect interval 5 threshold 0
```

【检验方法】

- 在研发部中的一台电脑上通过 dot1x SU 客户端认证上线，然后将电脑直接关机，等待 6min 后，在 switch1 设备上使用 dot1x 提供的在线用户查询命令确认该用户已经下线。

Switch A

```
sw1(config)#show running-config | include offline-detect
offline-detect interval 5
```

13.4.2 配置用户策略规则

配置效果

当配置了策略规则后，认证通过的用户，指定了对应策略名称后，可以根据策略配置的规则，对该用户进行限速设置。

注意事项

需要认证服务器支持对应的策略属性下发。目前策略规则支持无线平台的限速配置和过滤配置。

配置方法

↘ 配置用户策略规则

- 可选配置。
- 先配置限速策略和过滤策略，然后在用户策略规则中指定使用的限速策略名称。

上下行限速参数突发值不小于平均值。

【命令格式】 **rate-policy** *name*
{downstream | upstream } average-rate *avg-threshold* **burst-rate** *burst-threshold*
【参数说明】 *name*：限速策略名称
avg-threshold：流量限速平均值，取值范围为 8-261120，单位为 KBps。
burst-threshold：流量限速突发值,取值范围为 8-261120,单位为 KBps,突发值不小于平均值。
【缺省配置】 无
【命令模式】 全局模式
【使用指导】 需要先配置限速策略规则。

【命令格式】 **filter-policy** *name*
filter-acl { *acl-name* | *acl-id* }
【参数说明】 *name*：过滤策略名称
acl-name：过滤策略关联的安全 acl 的 acl-name。
acl-id：过滤策略关联的安全 acl 的 acl-id。
【缺省配置】 无
【命令模式】 全局模式
【使用指导】 需要先配置过滤策略规则。

【命令格式】 **service-policy** *service-name*
rate-policy *rate-name* **apply**
filter-policy *filter-name* **apply**
【参数说明】 *service-name*：用户策略名称。
rate-name：使用的限速策略名称。
filter-name：使用的过滤策略名称。
【缺省配置】 无
【命令模式】 全局模式
【使用指导】 配置限速策略和过滤策略规则后，才能在用户策略规则中使用。

检验方法

可以通过以下方法检验策略规则配置效果：

- 配置了限速策略规则后，用户认证上线，查看 wqos 对应的限速策略表项。
- 配置了过滤策略规则后，用户认证上线，查看 aclk 对应的用户 acl 应用表项。

配置举例

以下配置举例，仅介绍与 SCC 相关的配置。

通过用户策略规则功能，指定认证用户的限速策略。

【配置方法】
- 在 WLAN 1 上开启 WEB 受控，并在服务器配置对应的用户策略名称。
- 配置用户策略规则，指定限速策略。

Switch A

```
AC(config)# rate-policy user-rate
AC(config-rate-policy)#upstream average-rate 10 burst-rate 10
AC(config-rate-policy)#downstream average-rate 10 burst-rate 10
AC(config)# ip access-list extended user_2000
AC(config)# filter-policy user-filter
AC(config-filter-policy)#filter-acl user_2000AC(config)# service-policy user-policy
AC(config-service-policy)# rate-policy user-rate apply
AC(config-service-policy)# filter-policy user-filter apply
```

【检验方法】
- 认证通过后，查看用户的报文上下行速率。

13.5 监视与维护

清除各类信息

无

查看运行情况

-

查看调试信息

输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
监视 SCC 运行过程信息	**debug scc event**
调试查看当前 SCC 的相关用户表项	**debug scc user [mac | author | mac]**
调试查看当前 SCC 中保存的所有业务下发的相关 ACL 摘要信息	**debug scc acl-show summary**
调试查看当前 SCC 中保存的所有 ACL 信息	**debug scc acl-show all**

14 PASSWORD-POLICY

14.1 概述

Password Policy(口令策略)是设备本地认证时提供的口令安全功能，它依据管理员设置的口令安全策略对用户的登录密码和用户的登录状态进行控制。

下文仅介绍 Password Policy 的相关内容。

协议规范

暂无可遵循的协议规范或标准。

14.2 功能详解

基本概念

口令最小长度限制

根据系统的安全要求，管理员可设置用户口令的最小长度。当用户配置口令时，如果输入的口令长度小于限定的最小长度，系统将不允许用户设置该口令，并提示出错信息，提醒用户重新设置口令。

强口令检测功能

口令的复杂度越低，其被成功破解的可能性就越大，比如与账号同名的口令、只包含字符或数字的简单口令等。出于安全性考虑，管理员可以打开强口令检测或能，确认用户设置的口令具有较高的复杂度。打开强口令检测功能后，对不符合口令强度检测策略的如下口令提示告警：

1、与账号同名的口令；

2、只包含字符或数字的简单口令。

口令生存周期

口令生存周期用于限制用户口令的使用时间。当口令的使用时间超过限定值后，需要用户更换口令。

当用户登录时，如果用户输入已经过期的口令，系统将提示该口令已经过期，需要重新设置口令。在重新设置口令时，如果输入的新口令不符合要求，或者连续两次输入的新口令不一致，系统将要求用户继续重新输入。

口令重复使用限制功能

当用户修改口令时，系统会要求用户设置新的口令，旧的口令将被记录下来，形成该用户的历史记录。如果用户新设置的口令以前被使用过，系统将给出错误提示，并要求用户重新设置口令。

可以配置每个用户口令历史记录的最大条数，当口令历史记录的条数超过配置的最大条数时，新的口令历史记录将覆盖该用户最老的一条口令历史记录。

↘ 口令加密存储

出于安全考虑，管理员可以打开口令加密存储功能，打开此功能后，进行**show running-config**查看配置或**write**保存配置文件时，用户设置的各种口令将变成密文；如果再次关闭口令加密存储功能，已经变为密文的口令不会恢复为明文。

14.3 配置详解

配置项	配置建议 & 相关命令	
配置口令安全策略基本功能	⚠ 可选配置。用于配置口令安全相关的策略组合。	
	password policy life-cycle	设置口令生存周期。
	password policy min-size	限制用户口令的最小长度。
	password policy no-repeat-times	限制重复使用最近几次已配置过的口令。
	password policy strong	打开强口令检测功能。
	service password-encryption	设置口令加密存储。

14.3.1 配置口令安全策略基本功能

配置效果

- 为设备的本地认证提供口令安全策略，用户可以配置不同的安全策略来实现口令安全管理的目的。

注意事项

- 配置了口令安全策略后，只对全局口令（通过 **enable password**、**enable secret** 命令配置）和本地用户口令（通过 **username** *name* **password** *password* 命令配置），对于 Line 模式下面的口令不生效。

配置方法

↘ 设置口令生存周期

- 可选配置。
- 若无特殊要求，应在每台需要设置口令生存周期的设备上面配置。

↘ 限制用户口令的最小长度

- 可选配置。
- 若无特殊要求，应在每台需要限制口令最小长度的设备上面配置。

限制重复使用最近几次已配置过的口令

- 可选配置。
- 若无特殊要求，应在每台需要限制重复使用最近几次已配置过的口令的设备上面配置。

打开强口令检测功能

- 可选配置。
- 若无特殊要求，应在每台需要进行强口令检测的设备上面配置。

设置口令加密存储

- 可选配置。
- 若无特殊要求，应在每台需要设置口令加密存储的设备上面配置。

检验方法

在设备上面配置一个本地用户，并为此用户配置合法、非法口令。

- 配置合法的口令时，设备能否正确添加用户口令。
- 配置非法的口令时，设备能否提示相应的 Log 信息。

相关命令

设置口令生存周期

【命令格式】 **password policy life-cycle** *days*

【参数说明】 **life-cycle** *days*：口令生存周期，单位：天，范围：1~65535。

【命令模式】 全局配置模式

【使用指导】 口令生存周期用来限制用户口令的使用时间，当口令超过生存周期后，系统在下一次用户登录时，将提示用户修改口令。

限制用户口令的最小长度

【命令格式】 **password policy min-size** *length*

【参数说明】 **min-size** *length*：指定口令最小长度，范围：1~31。

【命令模式】 全局配置模式

【使用指导】 此命令用来配置口令的最小长度限制，若没有配置口令的最小长度限制，用户设置口令时将不进行口令最小长度限制。

限制重复使用最近几次已配置过的口令

【命令格式】 **password policy no-repeat-times** *times*

【参数说明】 **no-repeat-times** *times*：最近几次已配置过的口令，范围：1~31。

【命令模式】 全局配置模式

【使用指导】 开启此功能后，用户最近几次使用过的旧口令将被记录下来，形成该用户的口令历史记录。如果用户新设置的

口令以前被使用过，系统将给出错误提示，口令更改失败。

可以配置用户口令历史记录的最大条数，当口令历史记录的条数超过配置的最大历史记录条数时，新的口令历史记录将覆盖该用户最老的一条口令历史记录。

打开强口令检测功能

【命令格式】 **password policy strong**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 开启了此功能后，能够在新建用户时对不符合口令强度策略的如下口令配置提示告警：

1、与账号同名的口令；

2、只包含字符或数字的简单口令。

设置口令加密存储

【命令格式】 **service password-encryption**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 没有设置口令加密存储前，用户配置过程，使用的各种口令均以明文显示和存储，除非是直接使用密文进行配置。出于安全考虑，可以打开口令加密存储功能，打开此功能后，进行 **show running-config** 或 **write** 保存时，用户设置的各种口令将变成密文；如果再次关闭口令加密存储功能，已经变为密文的口令不会恢复为明文。

查看用户设置的口令安全策略信息

【命令格式】 **show password policy**

【参数说明】 -

【命令模式】 特权模式、全局模式、接口模式

【使用指导】 查看设备上设置的口令安全策略信息。

配置举例

以下配置举例，介绍口令安全策略相关的配置。

在设备上面

【网络环境】 假设网络环境中，有以下口令安全需求：

1、口令最小长度大于等于 8 个字符；

2、口令生存时间为 90 天；

3、口令使用加密存储和传输；

4、口令重复使用历史记录条数 3 条；

5、不允许口令与用户名一样或者只包含简的字符或数字。

【配置方法】

- 配置口令最小长度：8。
- 配置口令生存周期：90 天。
- 开启口令加密存储功能。

- 配置口令重复使用历史记录条数：3。
- 开启强口令检测功能。

```
Ruijie# configure terminal
Ruijie(config)# password policy min-size 8
Ruijie(config)# password policy life-cycle 90
Ruijie(config)# service password-encryption
Ruijie(config)# password policy no-repeat-times 3
Ruijie(config)# password policy strong
```

【检验方法】 用户设置了相关口令安全策略相关的配置后，在新增用户和口令的时候，将会依据口令安全策略进行相关的检测。

- 通过 show password policy，查看用户设置的口令安全策略信息。

```
Ruijie# show password policy

Global password policy configurations:

 Password encryption:                Enabled

 Password strong-check:              Enabled

 Password min-size:                  Enabled (8 characters)

 Password life-cycle:                Enabled (90 days)

 Password no-repeat-times:           Enabled (max history record: 3)
```

常见错误

- 设置口令过期前开始提醒的时间大于口令生存周期。

14.4 监视与维护

查看运行情况

作用	命令
查看用户设置的口令安全策略信息	**show password policy**

15 SSH

15.1 概述

SSH（Secure Shell，安全外壳）连接提供的功能类似于一个 Telnet 连接，与 Telnet 不同的是基于该连接所有的传输都是加密的。当用户通过一个不能保证安全的网络环境远程登录到设备时，SSH 特性可以提供安全的信息保障和强大的认证功能，以保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

设备支持 SSH 服务器功能，可以接受多个 SSH 客户端的连接。同时，设备还支持 SSH 客户端功能，允许用户与支持 SSH 服务器功能的设备建立 SSH 连接，从而实现本地设备通过 SSH 安全登录到远程设备上进行管理的功能。

目前，设备作为 SSH 服务器或 SSH 客户端时，支持 SSHv1 和 SSHv2 两个版本。锐捷 SSH 服务同时支持 IPv4 和 IPv6 两种协议。

下文仅介绍 SSH 的相关内容。如无特殊说明，文中的 SSH 均指 SSHv2。

协议规范

- RFC 4251：The Secure Shell (SSH) Protocol Architecture
- RFC 4252：The Secure Shell (SSH) Authentication Protocol
- RFC 4253：The Secure Shell (SSH) Transport Layer Protocol
- RFC 4254：The Secure Shell (SSH) Connection Protocol
- RFC 4419：Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol
- RFC 4716：The Secure Shell (SSH) Public Key File Format
- RFC 4819：Secure Shell Public Key Subsystem
- RFC 3526：More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 2409：The Internet Key Exchange (IKE)
- RFC 1950：ZLIB Compressed Data Format Specification version 3.3
- draft-ietf-secsh-filexfer-05：SSH File Transfer Protocol
- draft-ylonen-ssh-protocol-00：The SSH (Secure Shell) Remote Login Protocol 其协议版本为 1.5，Comware 实现了协议的 Server 功能，没有实现 Client 功能

15.2 典型应用

典型应用	场景描述
SSH设备管理	用户使用 SSH 对设备进行管理
SSH本地线路认证	采用本地线路口令认证方式进行 SSH 用户认证

SSH的AAA认证	采用 AAA 认证方式进行 SSH 用户认证
SSH公钥认证	采用公钥认证方式进行 SSH 用户认证
SSH文件传输	用户使用客户端的 SCP 命令与 SSH 服务器端进行数据传输

15.2.1 SSH设备管理

应用场景

用户可以使用 SSH 对设备进行管理，前提是必须打开 SSH Server 功能，默认情况下是关闭该功能的。由于 Windows 自带的 Telnet 组件不支持 SSH，因此必须使用第三方客户端软件，当前兼容性较好的客户端包括：Putty，Linux，SecureCRT。下面以客户端软件 Putty 为例介绍 SSH Client 的配置，组网图如下所示。

图 15-1 SSH 设备管理组网图

功能部署

SSH Client 的配置要点如下：

- 打开 Putty 客户端工具软件。
- 在 Putty 中的 Session 选项卡中填写 SSH Server 的主机 IP、SSH 端口号 22 以及连接类型为 SSH。
- 在 Putty 中的 SSH 选项卡中选择 SSH 协议版本号为 2。
- 在 Putty 中的 SSH 选项卡中选择认证方式为“Keyboard-interactive”。
- 点击 open 按钮连接服务器主机。
- 在用户名密码认证窗口输入正确的用户名与密码进入终端登录界面。

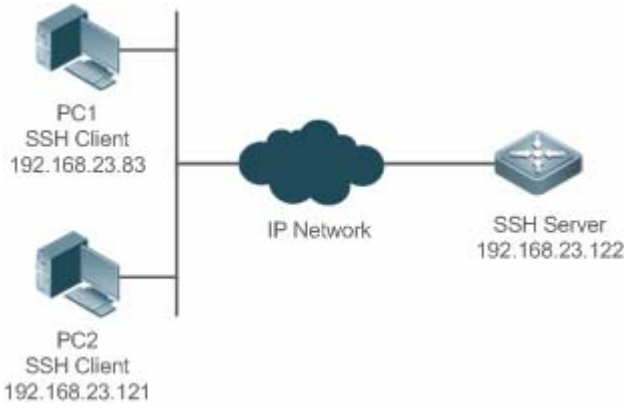
15.2.2 SSH本地线路认证

应用场景

SSH 用户可以采用本地线路口令认证方式进行用户认证，如下图所示。为了保证数据信息交换的安全，PC1、PC2 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。具体要求如下：

- SSH 用户采用的认证方式为线路口令认证。
- 同时启用 0-4 这五条线路，其中线路 0 的登录口令为“passzero”，其余四条线路的登录口令均为“pass”，用户名任意。

图 15-2 SSH 本地线路口令保护组网图



功能部署

- SSH Server 的配置要点如下：

3. 全局打开 SSH Server。SSH Server 默认支持 SSH1 和 SSH2 两个版本。
4. 配置密钥。通过该密钥，SSH 服务器将从 SSH 客户端收到的口令密文进行解密，将解密后的明文同服务器上保存的口令进行比较，并返回认证成功或失败的消息。SSH 1 使用 RSA 密钥；SSH 2 使用 RSA 或者 DSA 密钥。
5. 配置 SSH 服务器 FastEthernet 0/1 接口的 IP 地址。SSH 客户端通过该地址连接 SSH 服务器。SSH 客户端至 SSH 服务器路由可达。

- SSH Client 的配置要点如下：

SSH 客户端软件有多种，例如 Putty、Linux、OpenSSH 等，本文中仅以客户端软件 Putty 为例，说明 SSH 客户端的配置方法。

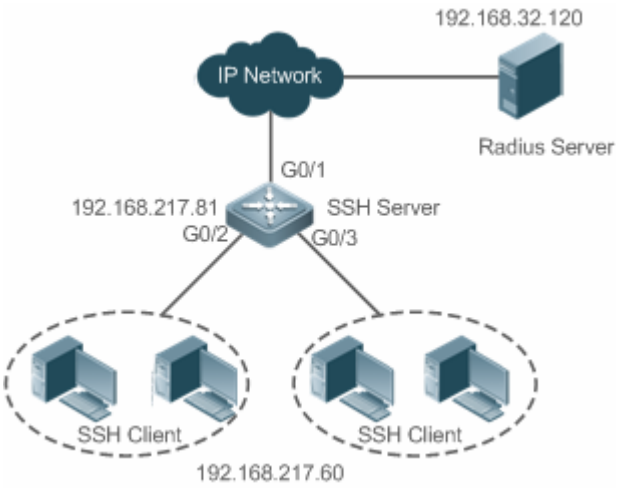
1. 打开 Putty 的连接框，选择使用 SSH1 进行认证登录，使用 SSH2 认证方法类似。
2. 设置 SSH 服务器的 IP 地址与连接端口号，由组网拓扑图可知，服务器主机 IP 为 192.168.23.122，连接端口号为 22，点击 open 按钮进行连接。由于当前认证方式不需要用户名，此处“用户名”可以任意输入，但是不能为空（本例用户名设置为 anyname）。

15.2.3 SSH的AAA认证

应用场景

SSH 用户可以采用 AAA 认证方式进行用户认证，如下图所示。为了保证数据信息交换的安全，PC 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。为了更好地进行安全管理，SSH 客户端登录用户界面采用 AAA 认证方式；同时出于稳定性方面考虑，在 AAA 认证方法列表中配置两种认证方法：Radius 服务器认证和本地认证。优先选择 Radius 服务器，当 Radius 服务器没有响应时选择本地认证方法。

图 15-3 SSH AAA 认证组网图



功能部署

- SSH 客户端到 SSH 服务器端的路由可达，SSH 服务器到 Radius 服务器端的路由可达。
- 在网络设备上进行 SSH Server 相关配置。
- 在网络设备上进行 AAA 认证相关配置。AAA 通过创建方法列表来定义身份认证、类型，然后将这些方法列表应用于特定的服务或接口上。

15.2.4 SSH公钥认证

应用场景

SSH 用户可以采用 Public-key 认证方式进行用户认证，公钥算法为 RSA 或 DSA，如下图所示。通过配置客户端使用 SSH 协议与服务器端进行安全连接。

图 15-4 SSH 公钥认证组网图

功能部署

- 客户端公钥认证方式，首先要在客户端生成一个密钥对（RSA 或 DSA），然后将其中的公钥放置在 SSH 服务器上，并选择使用 Public-Key 认证方式。

- 在客户端生成了密钥以后，SSH 服务器端需要将客户端的公钥文件复制到 flash 中，并且与 SSH 用户名关联。每个用户可以关联一个 RSA 公钥和一个 DSA 公钥。

15.2.5 SSH文件传输

应用场景

服务器端开启 SCP 服务，客户端通过 SCP 命令与服务器端进行数据传输，如下图所示。

图 15-5 SSH 文件传输组网图

功能部署

- 服务器端开启 SCP 服务。
- 客户端使用 SCP 命令上传文件至服务器端，或从服务器端下载文件。

15.3 功能详解

基本概念

用户认证机制

- password 认证

password 认证是指客户端向服务器发出用户认证请求，并将加密的用户名和密码发送给服务器；服务器将收到信息进行解密，同时将此信息与设备上保存的客户端用户名和密码进行比较，然后返回用户认证成功或失败的消息。

- public-key 认证

public-key 认证是指利用 RSA 或 DSA 等数字签名算法对客户端进行认证。客户端向服务器发送 public-key 认证请求，包括用户名、公钥和公钥算法等信息。服务器收到该信息后先检查公钥的合法性，如果不合法，则直接发送认证失败；否则，服务器对客户端进行数字签名认证，并返回用户认证成功或失败的消息。

public-key 认证仅针对客户端版本为 SSH2.0 的用户。

SSH 的通讯交互

在整个服务器端与客户端的 SSH 通讯交互过程中，为了实现安全通道，需要经历如下七个阶段：

- 建立连接阶段

服务器端在端口 22 监听，等待客户端的连接。当客户端发起 Socket 初始连接请求时，客户端与服务器端建立起了 TCP Socket 连接。

- 版本号协商阶段

如果连接成功，服务器端向客户端发送版本协商报文，客户端收到该报文后进行解析，并向服务端回应客户端决定采用的协议版本号。服务器端将对此信息进行分析，协商版本成功或失败。

- 密钥交换与算法协商阶段

如果版本号协商成功，进入密钥交换与算法协商。服务器端与客户端互相向对端发送算法协商报文，并根据本端支持的算法来确定最终使用的算法。另外，服务器端与客户端利用密钥交换算法、主机密钥等相关信息，生成会话密钥以及会话 ID，利用它们进行后续的用户认证以及数据传输的加解密。

- 用户认证阶段

在加密通道建立起来之后，进入用户认证阶段。客户端向服务器端发送认证请求，服务器端对客户端进行认证，直到认证成功或者认证次数达到设定的上限，服务器端关闭连接为止。

- 会话请求阶段

认证成功后，客户端向服务器端发送会话请求，服务器等待并处理客户端的请求，请求被处理成功之后，SSH 进入会话交互阶段。

- 会话交互阶段

在会话请求成功之后，进入会话交互阶段。加密的数据在双向就可以进行传送并处理。客户端将需要执行的命令发送给服务器端，服务器接收到该命令后进行解密、解析并处理，并将执行的结果进行加密后发给客户端进行解密处理。

- 会话关闭阶段

在服务器端和客户端结束会话时，断开 socket 连接，会话被关闭。

功能特性

功能特性	作用
SSH Server	网络设备上打开 SSH Server，用户可以通过 SSH 客户端安全地连接网络设备。
SCP服务	开启 SCP 服务后，用户可以直接下载网络设备上的文件，以及将本地文件上传至网络设备，同时所有交互数据以密文形式进行传输，具有认证和安全性等特性。

15.3.1 SSH Server

网络设备上打开 SSH Server，用户可以通过 SSH 客户端安全地连接网络设备；同时，可以关闭 SSH Server，断开全部 SSH 用户的连接。

工作原理

SSH Server 具体工作原理可参考基本概念章节中的“SSH 的通讯交互”小节。在实际以应用中，开启 SSH Server 服务，同时可根据相关应用需求设置以下功能点。

设置版本号：使 SSH Server 支持 SSHv1 与 SSHv2 两种客户端的连接。

设置用户认证超时时间：使 SSH Server 从接受用户连接请求开始计时，存在两种情况：用户认证成功或认证超时断开客户端的连接。

设置用户重认证次数：使 SSH Server 从接受用户连接请求开始进行认证，如果达到重认证次数仍未认证成功，则提示认证失败。

公钥认证：公钥算法为 RSA 或 DSA，在客户端与服务端之间提供安全连接。通过将客户端的公钥文件与用户名进行关联，同时，在客户端配置公钥认证方式，而且指定对应的私钥文件。这样，在客户端登录认证时，即可实施公钥认证进行安全连接。

相关配置

↘ SSH Server 开启

缺省情况下，SSH Server 处于关闭状态。

在全局配置模式下，执行**[no] enable service ssh-server** 命令可以打开或关闭 SSH Server.

同时需要生成 SSH 密钥，使 SSH Server 的状态成为 ENABLE。

↘ 设置 SSH Server 支持的版本

缺省情况下，SSH Server 所支持的版本兼容 SSH1 与 SSH2，使用 SSH 1 或者 SSH2 的客户端都可以连接。

使用 **ip ssh version** 命令来配置 SSH Server 所支持的 SSH 连接的协议版本。

如果设置了版本 1 或者 2，只允许对应版本的 SSH 客户端才能够连接。

↘ 设置 SSH Server 的用户认证超时时间

缺省情况下，超时时间为 120 秒。

执行 **ip ssh time-out** 命令配置 SSH Server 用户认证的超时时间。执行 **no** 命令可以使超时时间恢复为缺省值。从接受用户连接请求开始计时，当超过指定时间没有认证成功时，则认为认证超时失败。

↘ 设置 SSH Server 的重认证次数

缺省情况下，重认证次数为 3 次。

执行 **ip ssh authentication-retries** 命令配置 SSH Server 进行用户认证的重认证次数。执行 **no** 命令可以使重认证次数恢复为缺省值。当超过 SSH Server 配置的重认证次数，仍没有认证成功，则认为用户认证失败。

↘ 启动 SSH Server 的公钥认证

执行 **ip ssh peer** 命令开启或取消客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。

15.3.2 SCP服务

SSH Server 提供 SCP（Secure Copy，安全复制）服务，用于服务器端与客户端之间文件的安全传输。

工作原理

SCP 协议是一个支持网络文件传输的协议。它运行在 22 端口，基于 BSD RCP 协议；而 RCP 又基于 SSH 协议提供加密和认证。其中，RCP 负责文件的传输，而 SSH 协议负责认证和加密。

在服务器端开启 SCP 服务后，当用户使用 SCP 客户端进行文件上传与下载时，SCP 客户端会先解析命令行参数，然后打开一个到远程服务器的连接，再通过这个连接起另一个 SCP 进程。这个进程的运行方式可以是源模式(source)，也可以是宿模式(sink)，（前者是数据提供者；后者是数据的目的地）。前者读取文件并通过 SSH 连接发送到另一端，后者通过 SSH 连接接收文件。

相关配置

↘ 启动 SCP 服务

缺省不开启 SCP 服务器功能。

执行 **ip scp server enable** 命令在网络设备上打开或关闭 SCP 服务器功能。

15.4 配置详解

配置项	配置建议 & 相关命令	
配置SSH Server	⚠ SSH Server 打开功能必须配置。	
	enable service ssh-server	配置 SSH Server 打开功能
	disconnect ssh [**vty**] *session-id*	断开已经建立的 SSH 连接
	crypto key generate { **rsa** | **dsa** }	生成密钥
	ip ssh version { **1** | **2** }	配置 SSH Server 支持版本
	ip ssh time-out *time*	配置 SSH 用户认证超时时间
	ip ssh authentication-retries *retry times*	配置 SSH 重认证次数
	ip ssh peer *test* **public-key rsa flash**:*rsa.pub*	设置用户 *test* 关联的 RSA 公钥文件
	ip ssh peer *test* **public-key dsa flash**:*dsa.pub*	设置用户 *test* 关联的 DSA 公钥文件
配置SCP服务	⚠ 必须配置。	
	ip scp server enable	开启 SCP 服务器功能

15.4.1 配置SSH Server

配置效果

- 在网络设备上打开 SSH Server 功能，用户可以通过 SSH 客户端安全地连接网络设备，同时所有交互信息均以密文形式进行传输，具有认证和安全性等特性。
- 用户可以采用多种认证方式进行 SSH 用户认证，包括：本地线路口令认证、AAA 认证、公钥认证等认证方式。
- 用户可以生成或删除服务器密钥。

- 用户可以配置服务器支持的 SSH 协议版本。
- 用户可以设置认证超时时间。
- 用户可以设置重认证次数。

注意事项

- 配置设备为 SSH Server，前提是必须保证设备所处网络环境通信正常，管理员能够连接到设备的管理界面进行相应地配置。
- 删除密钥时，不存在命令 **no crypto key generate**；而是通过命令 **crypto key zeroize** 命令删除密钥。
- SSH 模块不支持热备，因此在支持管理板热备份的产品中，管理板切换动作发生后，若新的主板上没有SSH密钥文件，则必须通过命令 **crypto key generate** 重新生成密钥后方可使用 SSH。

配置方法

配置 SSH Server 打开功能

- 必须配置。
- 缺省情况下，SSH Server 处于关闭状态。在全局配置模式下，打开 SSH Server，同时需要生成 SSH 密钥，使 SSH Server 的状态成为 ENABLE。

配置 SSH Server 支持版本

- 可选配置。
- 缺省情况下，SSH Server 兼容版本 1 和 2，使用 SSH 1 或者 SSH2 的客户端都可以连接。如果设置了版本 1 或者 2，只允许对应版本的 SSH 客户端才能够连接。

配置 SSH 用户认证超时时间

- 可选配置。
- 缺省情况下，SSH Server 的用户认证超时时间为 120 秒。可以根据需要配置用户认证的超时时间，取值范围为 1~120s，单位为秒。

配置 SSH 重认证次数

- 可选配置。
- 设置 SSH 用户请求连接的认证重试次数，防止恶意猜测等非法行为。缺省情况下，SSH Server 的重认证次数为 3 次，即可以允许用户尝试三次输入用户名与密码进行认证尝试。可以根据需要配置用户认证的重认证次数，取值范围为 0~5。

配置 SSH 基于公钥的认证

- 可选配置。

- 根据 SSH 协议，只有 SSHv2 才支持基于公钥的认证，SSHv1 不支持。该配置将客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。

检验方法

- 使用 **show ip ssh** 命令，可以查看 SSH Server 当前支持的 SSH 协议版本、用户认证的超时时间及重认证次数。
- 通过执行 **show crypto key mypubkey** 命令，查看密钥的公开部分信息是否存在来确认密钥是否已经生成。
- 在 SSH 客户端配置相应的公钥认证登录方式，并指定对应的私钥文件，观察是否可以正常登录。如果可以正常登录，表示客户端的公钥文件与用户名关联成功，公钥认证通过。

相关命令

配置 SSH Server 打开功能

【命令格式】 **enable service ssh-server**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 关闭 SSH Server，需要在全局配置模式下，执行 **no enable service ssh-server** 命令，使 SSH Server 的状态成为 DISABLE。

断开已经建立的 SSH 连接

【命令格式】 **disconnect ssh** [**vty**] *session-id*

【参数说明】 **vty**：已经建立的 vty 连接

session-id：已经建立的 SSH 连接会话号，取值范围为 0~35

【命令模式】 特权用户模式

【使用指导】 通过输入指定的 SSH 连接会话号，断开已经建立的 SSH 连接。或者输入指定的 VTY 连接会话号，断开指定的 SSH 连接。只能断开 SSH 类型的连接。

生成密钥

【命令格式】 **crypto key generate** { **rsa | dsa** }

【参数说明】 **rsa**： 生成 rsa 密钥

dsa：生成 dsa 密钥

【命令模式】 全局模式

【使用指导】 删除密钥时，不存在命令 no crypto key generate；而是通过命令 **crypto key zeroize** 命令删除密钥。

根据SSH协议，SSH 1使用RSA密钥；SSH 2使用RSA或DSA密钥。

如果已生成 RSA 密钥，则 SSH1 与 SSH2 都可用；如果仅生成 DSA 密钥，则仅有 SSH2 可以使用。

配置 SSH Server 支持版本

【命令格式】 **ip ssh version** { **1 | 2** }

【参数说明】 **1**： 配置 SSH Server 仅支持 SSH1 的客户端连接请求

2： 配置 SSH Server 仅支持 SSH2 的客户端连接请求

【命令模式】 全局模式

【使用指导】 **no ip ssh version** 命令恢复 SSH 为缺省配置，支持 SSHv1 与 SSHv2。

配置 SSH 用户认证超时时间

【命令格式】 **ip ssh time-out** *time*

【参数说明】 *time*：配置用户认证的超时时间，取值范围为 1~120s，单位为秒

【命令模式】 全局模式

【使用指导】 **no ip ssh time-out** 命令恢复 SSH 的缺省用户认证超时时间为 120 秒。

配置 SSH 重认证次数

【命令格式】 **ip ssh authentication-retries** *retry times*

【参数说明】 *retry times*： 配置用户认证的重认证次数，取值范围为 0~5

【命令模式】 全局模式

【使用指导】 **no ip ssh authentication-retries** 命令恢复 SSH 的重认证次数为 3 次。

配置 SSH 基于 rsa 公钥的认证

【命令格式】 **ip ssh peer** *test* **public-key rsa flash**:*rsa.pub*

【参数说明】 *test*：用户名

rsa： public-key 类型为 rsa

rsa.pub：公钥文件名

【命令模式】 全局模式

【使用指导】 设置用户 *test* 关联的 RSA 公钥文件。

根据 SSH 协议，只有 SSHv2 才支持基于公钥的认证，SSHv1 不支持。该命令将客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。

配置 SSH 基于 dsa 公钥的认证

【命令格式】 **ip ssh peer** *test* **public-key dsa flash**:*dsa.pub*

【参数说明】 *test*：用户名

dsa： public-key 类型为 dsa

dsa.pub：公钥文件名

【命令模式】 全局模式

【使用指导】 设置用户 *test* 关联的 DSA 公钥文件。

根据 SSH 协议，只有 SSHv2 才支持基于公钥的认证，SSHv1 不支持。该命令将客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。

配置举例

以下配置举例，仅介绍与 SSH 相关的配置。

生成服务器端的公共密钥

【配置方法】

- 使用 **crypto key generate** { **rsa | dsa** }命令生成服务器公共密钥，以 rsa 为例如下。

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# crypto key generate rsa
Choose the size of the rsa key modulus in the range of 512 to 2048
and the size of the dsa key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
```

- rsa 密钥生成成功提示信息：

```
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

- rsa 密钥生成失败提示信息：

```
% Generating 512 bit RSA1 keys ...[fail]
% Generating 512 bit RSA keys ...[fail]
```

【检验方法】

- 使用 **show crypto key mypubkey rsa** 命令，通过查看 rsa 密钥的公开部分信息是否存在来确认 rsa 是否已经生成。

SSH Server

```
Ruijie(config)#show crypto key mypubkey rsa
% Key pair was generated at: 1:49:47 UTC Jan 4 2013
 Key name: RSA1 private
 Usage: SSH Purpose Key
 Key is not exportable.
 Key Data:
        AAAAAwEA AQAAAHJM 6izXt1pp rUSOEGZ/ UhFpRRrW nngP4BU7 mG836apf jajSYwcU
        8O3LojHL ayJ8G4pG 7j4T4ZSf FKg09kfr 92JpRNHQ gbwaPc5/ 9UnTtX9t qFIKDj1j
        0dKBcCfN trOr/CT+ cs5tlGKV SOICGifz oB+pYaE=

% Key pair was generated at: 1:49:47 UTC Jan 4 2013
 Key name: RSA private
 Usage: SSH Purpose Key
 Key is not exportable.
 Key Data:
        AAAAAwEA AQAAAHJf LwKnzOgO F3RlKhTN /7PmQYoE v0a2VXTX 8ZCa7Sll EghLDLJc
        w3T5JQXk Rr3iBD5s b1EeOL4b 21ykZt/u UetQOQ8O sISgIfZ9 8o5No3Zz MPMOLnQR
        G4c7/28+ GOHzYkTk 4IiQuTIL HRgtbyEY XCFaaxU=
```

设置 SSH Server 的版本

【配置方法】

- 使用 **ip ssh version { 1 | 2 }**命令设置 SSH Server 的版本，以只使用版本 2 为例。

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh version 2
```

【检验方法】 ● 使用 **show ip ssh** 命令，可以查看 SSH Server 当前支持的 SSH 协议版本。

SSH Server

```
Ruijie(config)#show ip ssh
SSH Enable - version 2.0
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: disabled
```

设置 SSH Server 的用户认证超时时间

【配置方法】 ● 使用 **ip ssh time-out** *time* 命令设置用户认证超时时间，以配置 100s 为例。

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh time-out 100
```

【检验方法】 ● 使用 **show ip ssh** 命令，可以查看 SSH Server 用户认证的超时时间配置信息。

SSH Server

```
Ruijie(config)#show ip ssh
SSH Enable - version 2.0
Authentication timeout: 100 secs
Authentication retries: 3
SSH SCP Server: disabled
```

设置 SSH Server 的用户重认证次数

【配置方法】 ● 使用 **ip ssh authentication-retries** *retry times* 命令设置 SSH Server 用户认证的重认证次数 ,以 2 次为例。

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh authentication-retries 2
```

【检验方法】 ● 使用 **show ip ssh** 命令，可以查看 SSH Server 用户认证的重认证次数配置信息。

SSH Server

```
Ruijie(config)#show ip ssh
SSH Enable - version 2.0
Authentication timeout: 100 secs
Authentication retries: 3
SSH SCP Server: disabled
```

公钥认证

【配置方法】 ● 使用 **ip ssh peer** *username* **public-key** { **rsa** | **dsa** } *filename* 命令 ,将客户端的公钥文件和用户名关联，客户端登录认证时，通过用户名指定使用的公钥文件。以 rsa 为例如下：

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:rsa.pub
```

【检验方法】 ● 在 SSH 客户端配置相应的公钥认证登录方式，并指定对应的私钥文件，观察是否可以正常登录。如果可以正常登录，表示客户端的公钥文件与用户名关联成功，公钥认证通过。

配置 SSH 设备管理

【网络环境】

图 15-6

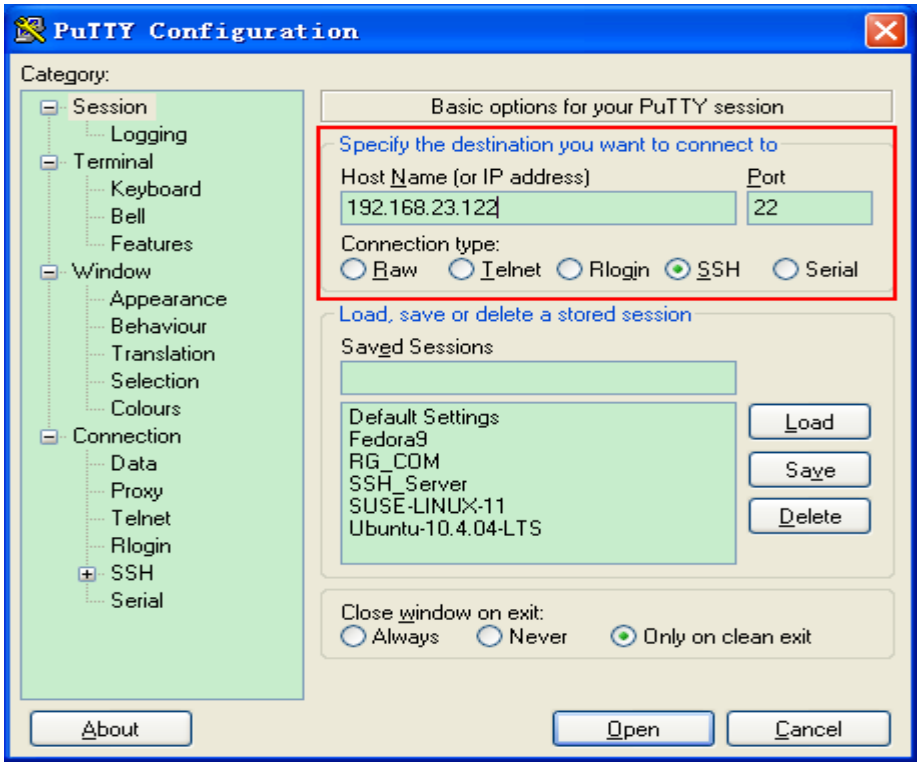
用户可以使用 SSH 对设备进行管理，前提是必须打开 SSH Server 功能，默认情况下是关闭该功能的。由于 Windows 自带的 Telnet 组件不支持 SSH，因此必须使用第三方客户端软件，当前兼容性较好的客户端包括：Putty，Linux，SecureCRT。以客户端软件 Putty 为例介绍 SSH Client 的配置。

【配置方法】

- 打开 Putty 客户端工具软件。
- 在 Putty 中的 Session 选项卡中填写 SSH Server 的主机 IP（192.168.23.122）、SSH 端口号 22 以及连接类型为 SSH。
- 在 Putty 中的 SSH 选项卡中选择 SSH 协议版本号为 2。
- 在 Putty 中的 SSH 选项卡中选择认证方式为“Keyboard-interactive”。
- 点击 open 按钮连接服务器主机。
- 在用户名密码认证窗口输入正确的用户名与密码进入终端登录界面。

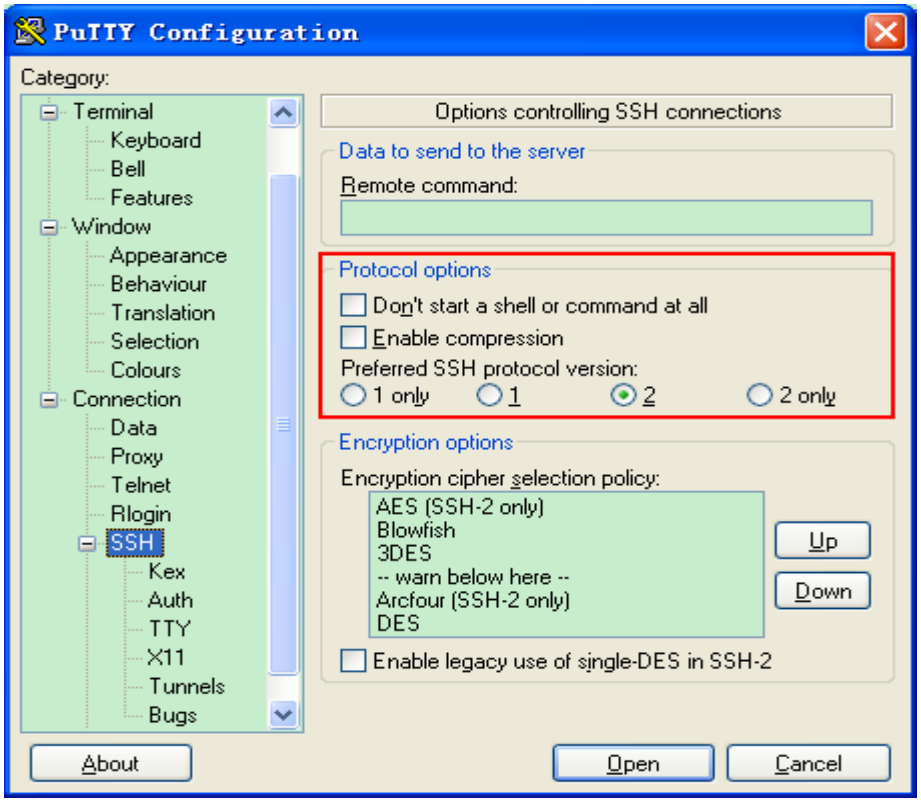
SSH Client

图 15-7



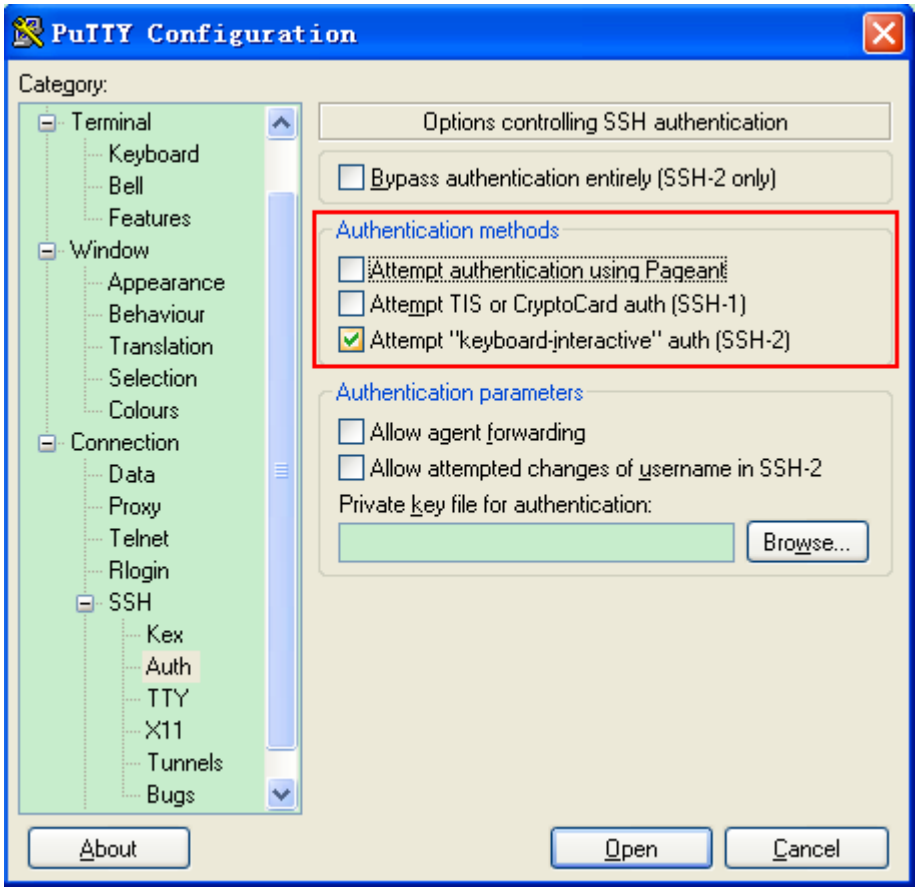
Host Name(or IP address) 就是要登陆的主机的 IP 地址 ,这里为 192.168.23.122。Port 为端口号 22 ,即 SSH 监听的默认端口号。Connection type 为连接类型 SSH。

图 15-8



如上图，使用 SSH 协议 2 进行登陆，因此在 Protocol options 中 Preferred SSH protocol version 选择 2。

图 15-9



如上图，配置 SSH 的认证方式，在 Authentication methods 复选框中，我们选择“keyboard-interactive”，支持用户名密码的认证方式。

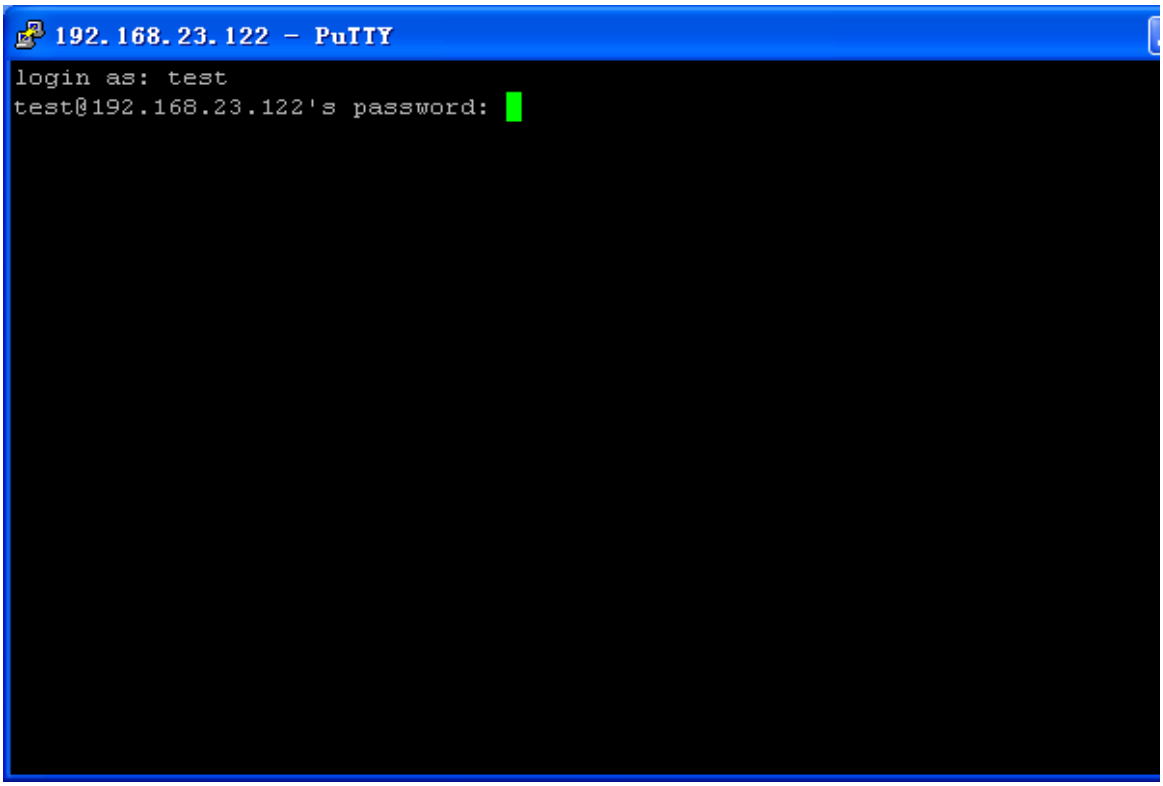
然后，点击 open 按钮，连接刚配置的服务器主机，如下图所示：

图 15-10

这里询问正在登陆服务器主机 192.168.23.122 的客户端，是否接收服务端发送过来的密钥，选择“是”（接受而且保存），选择“否”（只接受一次），选择“取消”（放弃连接）。

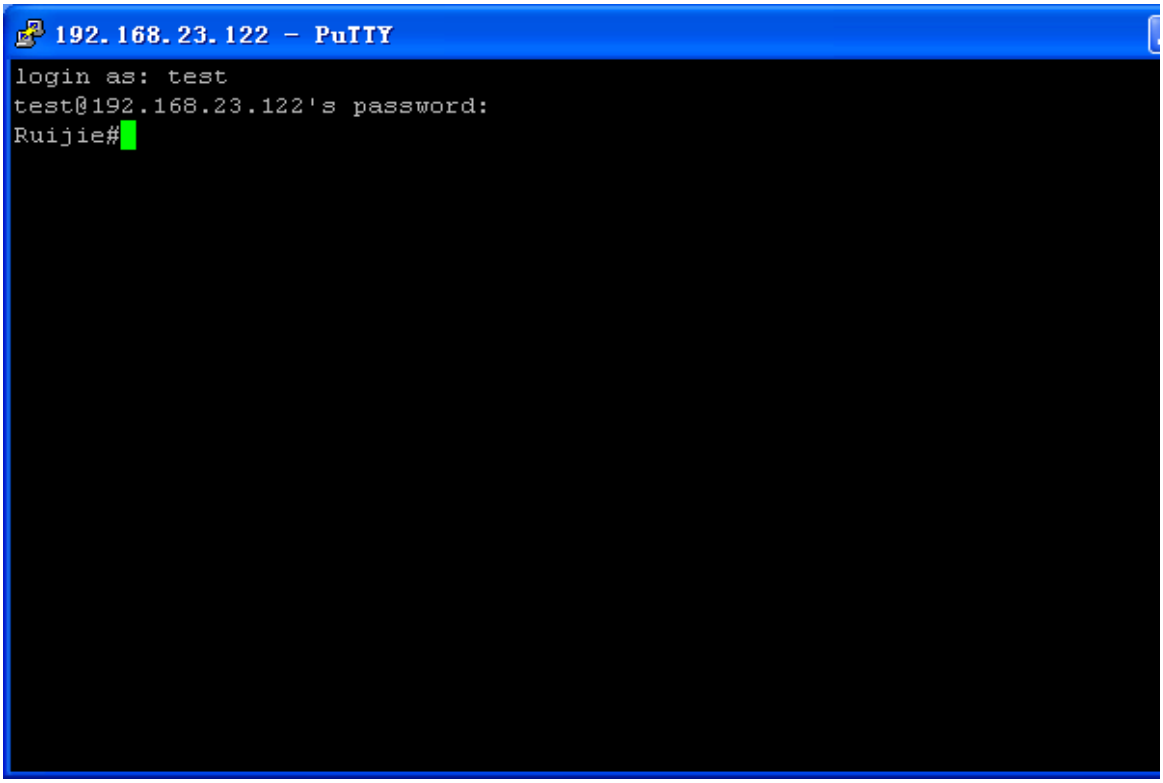
如果选择“是”，接着，会出现下面的用户名密码登录认证对话框，如下图所示：

图 15-11



此时，输入正确的用户名和密码，即可登录 SSH 终端界面，如下图所示：

图 15-12



【检验方法】

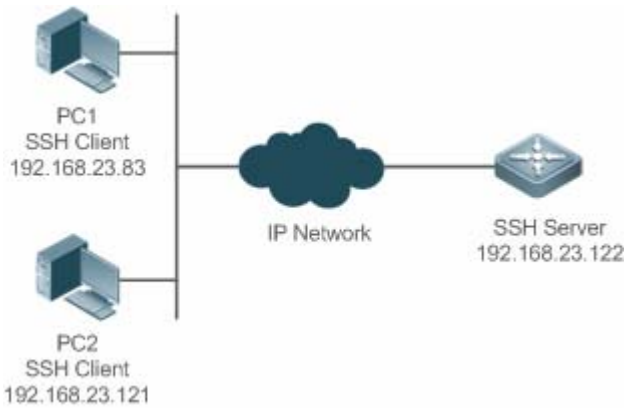
- 通过 **show ip ssh** 命令来显示 SSH Server 当前生效的配置信息。
- 通过 **show ssh** 命令来显示已经建立的 SSH 连接的每个连接信息。

```
Ruijie#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
Ruijie#show ssh
Connection Version Encryption       Hmac         State           Username
         0     2.0 aes256-cbc       hmac-sha1    Session started test
```

配置 SSH 本地线路认证

【网络环境】

图 15-13



SSH 用户可以采用本地线路口令认证方式进行用户认证，如图所示。为了保证数据信息交换的安全，PC1、PC2 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。具体要求如下：

- SSH 用户采用的认证方式为线路口令认证。
- 同时启用 0-4 这五条线路 ,其中线路 0 的登录口令为“passzero”,其余四条线路的登录口令均为“pass”，用户名任意。

【配置方法】 SSH Server 的配置要点如下：

- 全局打开 SSH Server。SSH Server 默认支持 SSH1 和 SSH2 两个版本。
- 配置密钥。通过该密钥，SSH 服务器将从 SSH 客户端收到的口令密文进行解密，将解密后的明文同服务器上保存的口令进行比较，并返回认证成功或失败的消息。SSH 1 使用 RSA 密钥；SSH 2 使用 RSA 或者 DSA 密钥。
- 配置 SSH 服务器 FastEthernet 0/1 接口的 IP 地址。SSH 客户端通过该地址连接 SSH 服务器。SSH 客户端至 SSH 服务器路由可达。

SSH Client 的配置要点如下：

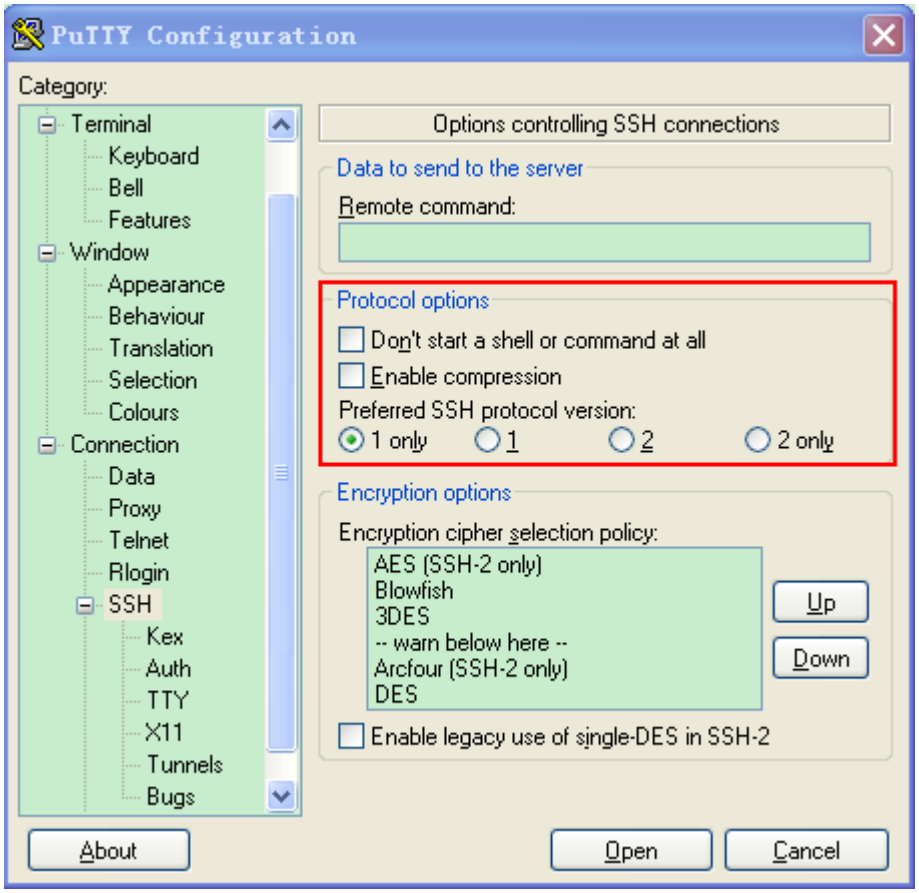
- SSH 客户端软件有多种，例如 Putty、Linux、OpenSSH 等，本文中仅以客户端软件 Putty 为例，说明 SSH 客户端的配置方法。具体配置方法请参见“配置步骤”。

SSH Server 配置 SSH 相关功能之前，请先确保 SSH 用户到 SSH 服务器所在网段的路由可达。接口 IP 配置如拓扑图所示。具体 IP 及路由配置过程此处省略。

```
Ruijie(config)# enable service ssh-server
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
Ruijie(config)#interface fastEthernet 0/1
Ruijie(config-if- fastEthernet 0/1)#ip address 192.168.23.122 255.255.255.0
Ruijie(config-if- fastEthernet 0/1)#exit
Ruijie(config)#line vty 0
Ruijie(config-line)#password passzero
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#login
Ruijie(config-line)#exit
Ruijie(config)#line vty 1 4
Ruijie(config-line)#password pass
Ruijie(config-line)#privilege level 15
Ruijie(config-line)#login
Ruijie(config-line)#exit
```

SSH Client（PC1/PC2）

图 15-14



然后，设置 SSH 服务器的 IP 地址与连接端口号，由组网拓扑图可知，服务器主机 IP 为 192.168.23.122，连接端口号为 22（具体设置方式可参考《SSH 设备管理配置举例》），点击 open 按钮进行连接。由于当前认证方式不需要用户名，此处“用户名”可以任意输入，但是不能为空（本例用户名设置为 anyname）。

【检验方法】

- 通过 **show running-config** 命令来查看当前配置信息的正确性
- 验证 SSH Client 的配置

SSH Server

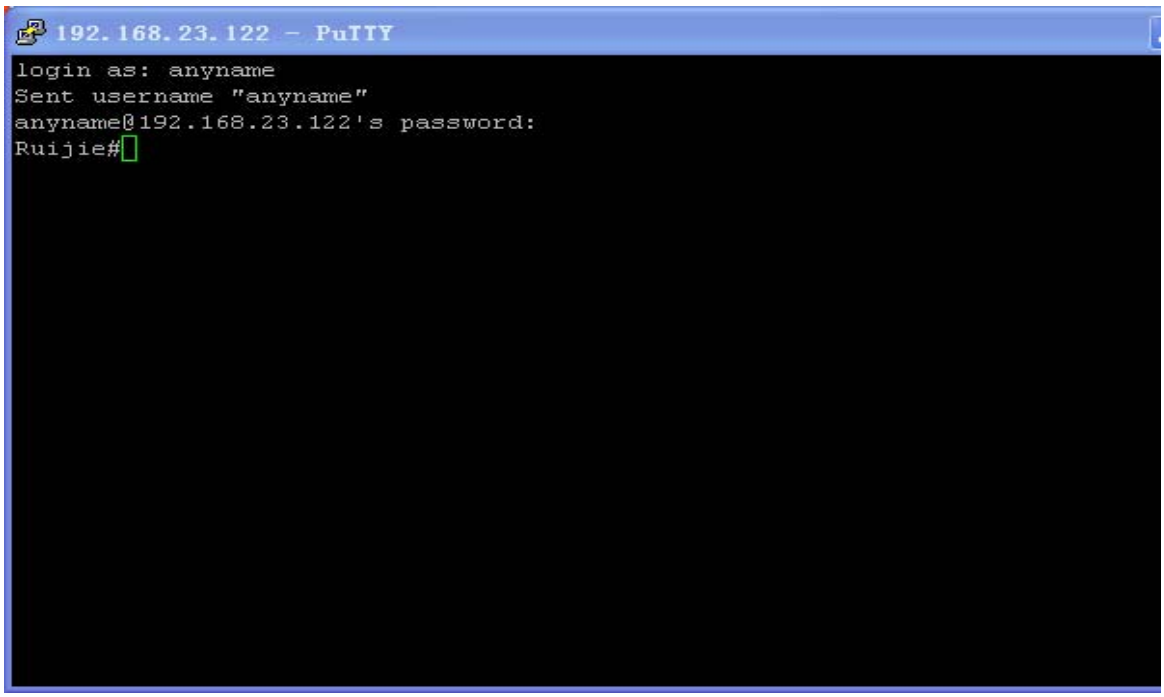
```
Ruijie#show running-config
Building configuration...
!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server
!
interface fastEthernet 0/1
 ip address 192.168.23.122 255.255.255.0
!
line vty 0
privilege level 15
```

```
 login
 password passzero
line vty 1 4
privilege level 15
 login
 password pass
!
end
```

SSH Client

建立连接，输入正确的口令。线路 0 的登录口令为“passzero”，其余四条线路的登录口令均为“pass”，即可进入 SSH Server 的操作界面。如图所示：

图 15-15

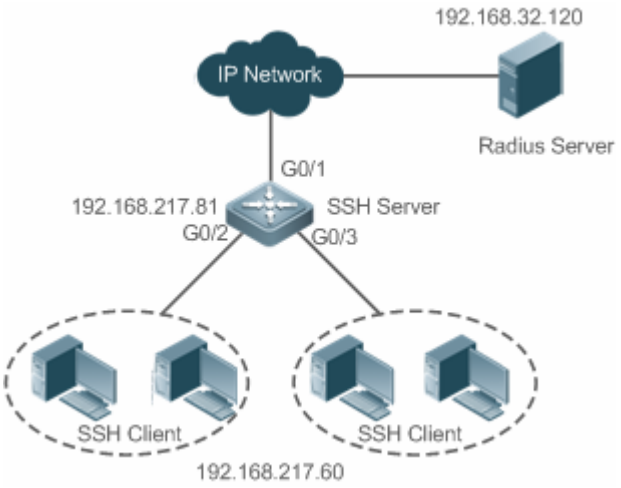



```
Ruijie#show users
Line             User         Host(s)              Idle       Location
---------------- ------------ -------------------- ---------- ------------------
*  0 con 0       ---          idle                 00:00:00   ---
   1 vty 0       ---          idle                 00:08:02   192.168.23.83
   2 vty 1       ---          idle                 00:00:58   192.168.23.121
```

配置 SSH 的 AAA 认证

【网络环境】

图 15-16



SSH 用户可以采用 AAA 认证方式进行用户认证，如图所示。为了保证数据信息交换的安全，PC 作为 SSH 客户端，采用 SSH 协议登录到打开 SSH Server 的网络设备上。为了更好地进行安全管理，SSH 客户端登录用户界面采用 AAA 认证方式；同时出于稳定性方面考虑，在 AAA 认证方法列表中配置两种认证方法：Radius 服务器认证和本地认证。优先选择 Radius 服务器，当 Radius 服务器没有响应时选择本地认证方法。

【配置方法】

- SSH 客户端到 SSH 服务器端的路由可达，SSH 服务器到 Radius 服务器端的路由可达。
- 在网络设备上进行 SSH Server 相关配置。配置要点在上一个例子中已有描述，不再重复说明。
- 在网络设备上进行 AAA 认证相关配置。AAA 通过创建方法列表来定义身份认证、类型，然后将这些方法列表应用于特定的服务或接口上。

SSH Server

```
Ruijie(config)# enable service ssh-server
Ruijie(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
Ruijie(config)#crypto key generate dsa
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit DSA keys ...[ok]
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-gigabitEthernet 1/1)#ip address 192.168.217.81 255.255.255.0
Ruijie(config-if-gigabitEthernet 1/1)#exit
Ruijie#configure terminal
```

```
Ruijie(config)#aaa new-model
Ruijie(config)#radius-server host 192.168.32.120
Ruijie(config)#radius-server key aaaradius
Ruijie(config)#aaa authentication login method group radius local
Ruijie(config)#line vty 0 4
Ruijie(config-line)#login authentication method
Ruijie(config-line)#exit
Ruijie(config)#username user1 privilege 1 password 111
Ruijie(config)#username user2 privilege 10 password 222
Ruijie(config)#username user3 privilege 15 password 333
Ruijie(config)#enable secret w
```

【检验方法】

- 通过 **show running-config** 命令来查看当前配置信息的正确性
- 在 Radius Server 上的设置。本例以 SAM 服务器为例进行说明。
- 在 PC 机上建立远程 SSH 连接。
- 查看登录用户。

```
Ruijie#show run
aaa new-model
!
aaa authentication login method group radius local
!
username user1 password 111
username user2 password 222
username user2 privilege 10
username user3 password 333
username user3 privilege 15
no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface gigabitEthernet 1/1
 no ip proxy-arp
 ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
```

```
 login authentication method
!
End
```

【系统管理】-【设备管理】中，添加设备 IP 地址：192.168.217.81，添加设备 Key：aaaradius

【安全管理】-【设备管理权限】中，设置登录用户的权限。

【安全管理】-【设备管理员】中，添加用户名：user；口令：pass。

SSH 客户端软件设置、建立连接；SSH 客户端的创建方法请参见上例。

输入正确的口令，SSH 用户名为：user；口令为：pass。登录成功。

```
Ruijie#show users
    Line         User         Host(s)              Idle       Location
   0 con 0                    idle                 00:00:31
 * 1 vty 0      user          idle                 00:00:33    192.168.217.60
```

配置 SSH 公钥认证

【网络环境】

图 15-17

SSH 用户可以采用 Public-key 认证方式进行用户认证，公钥算法为 RSA 或 DSA，如图所示。通过配置客户端使用 SSH 协议与服务器端进行安全连接。

【配置方法】

- 客户端公钥认证方式，首先要在客户端生成一个密钥对（这里以 RSA 密钥对为例），然后将其中的公钥放置在 SSH 服务器上，并选择使用 Public-Key 认证方式。

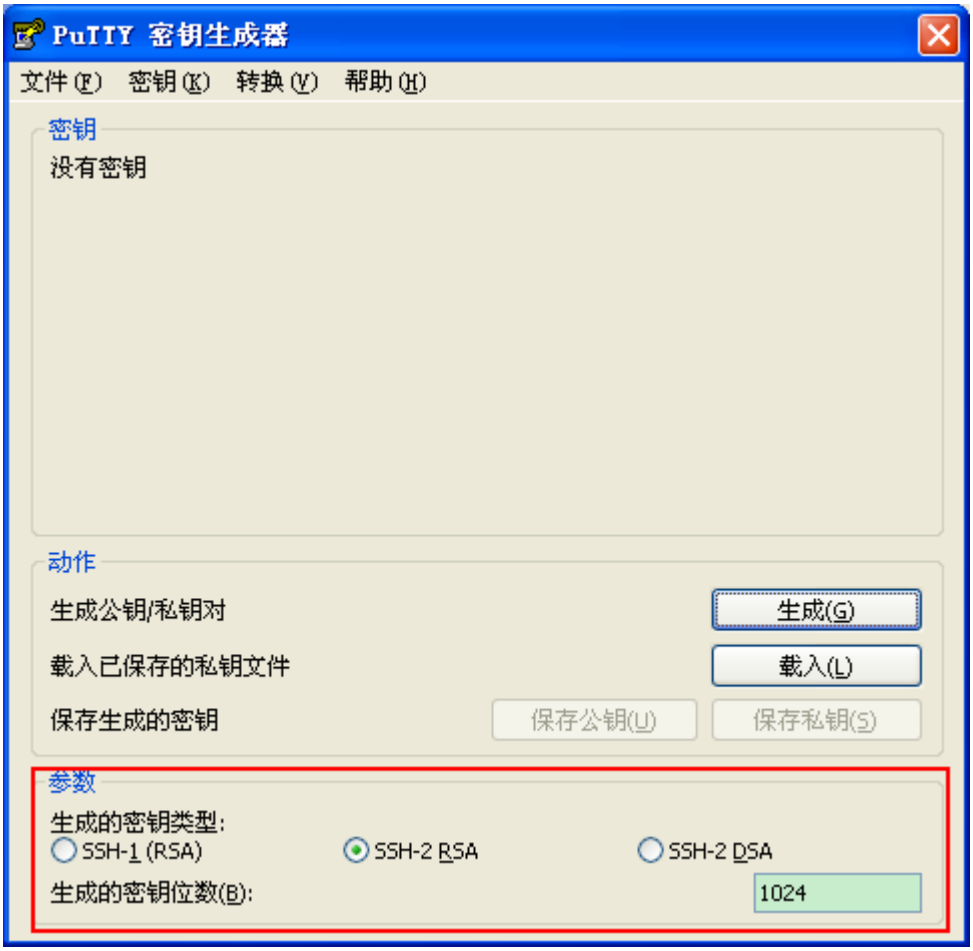
> 在客户端生成密钥对之后，需要将保存的公钥文件上传至服务器端，同时完成服务器的相关配置之后，才可以继续进行客户端的配置以及客户端与服务器端的连接。

- 在客户端生成了密钥以后，SSH 服务器端需要将客户端的公钥文件复制到 flash 中，并且与 SSH 用户名关联。每个用户可以关联一个 RSA 公钥和一个 DSA 公钥。

SSH Client

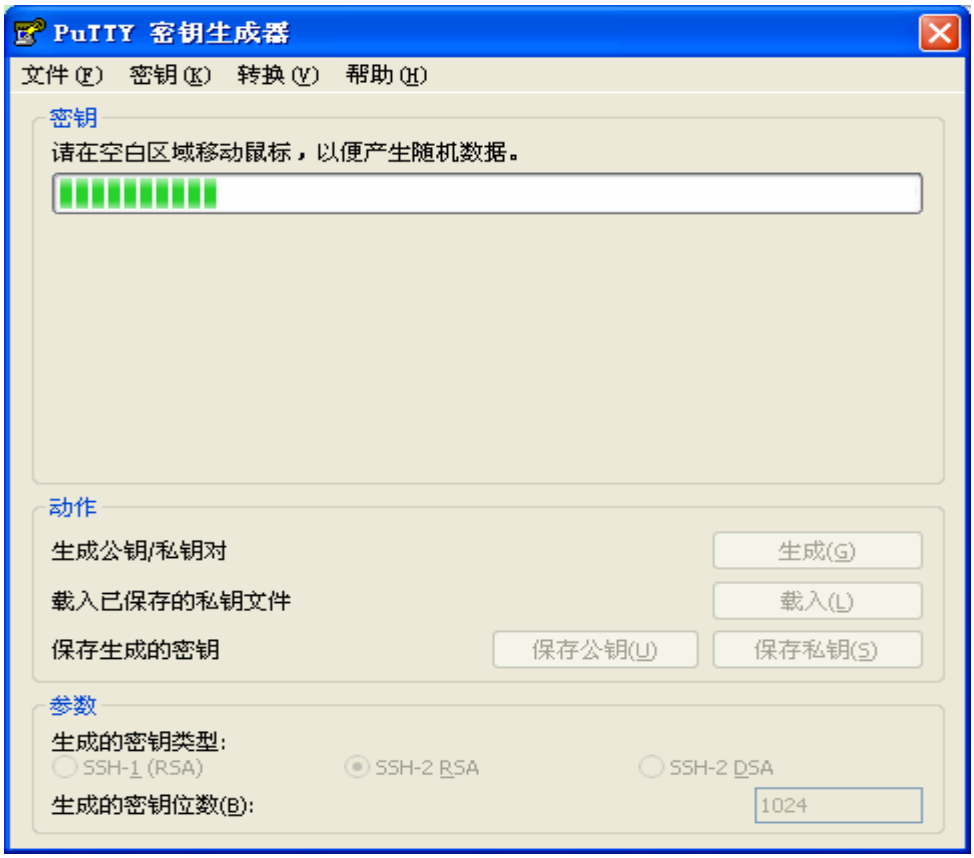
在客户端运行 puttygen.exe 软件，在参数选项栏中选择“SSH-2 RSA”，单击“生成”按钮产生密钥。如下图所示：

图 15-18



生成密钥的时候要除了绿色进度条外的地方不断晃动鼠标，否则进度条显示不动，密钥产生停止，如下图所示：

图 15-19

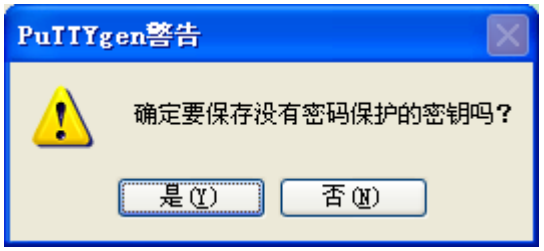


为了保证 RSA 公钥认证的安全性，生成 RSA 密钥对时，RSA 密钥对的长度必须大于或等于 768 位。这里设置为 1024：

图 15-20

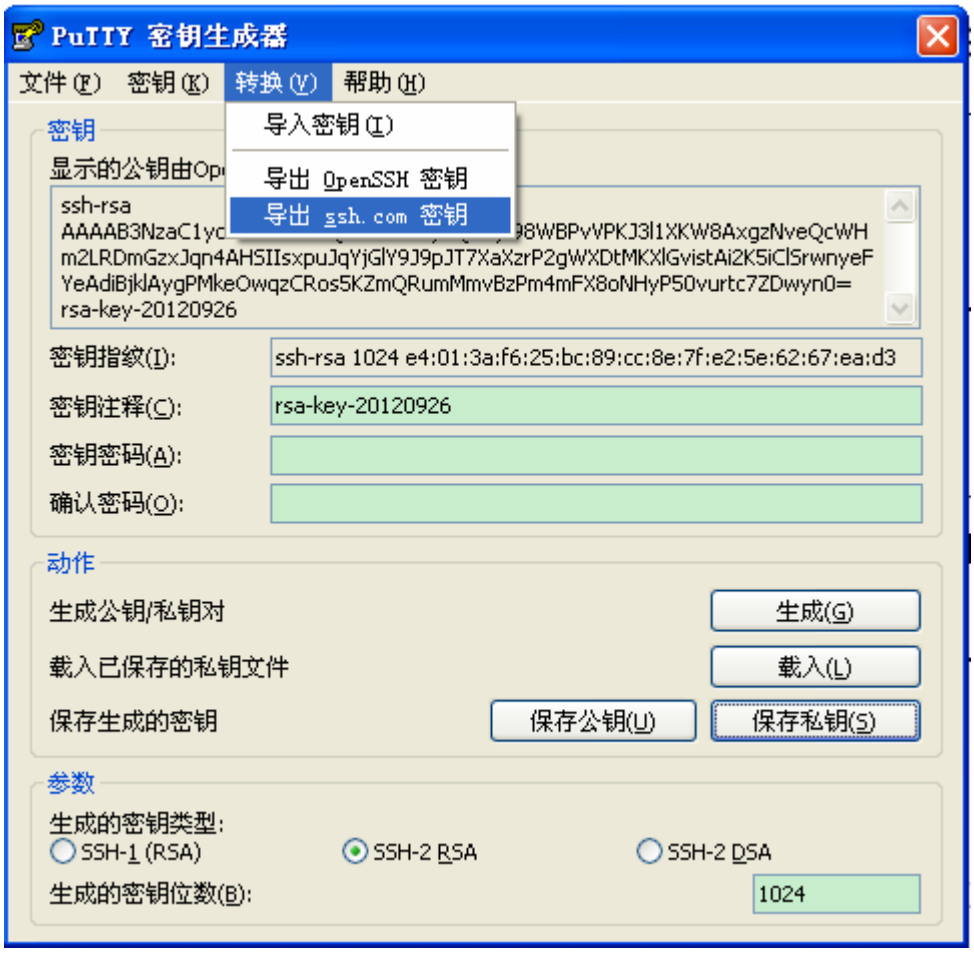
密钥对产生之后，点击“保存公钥”按钮，输入公钥名“test_key.pub”，选择保存路径，点击保存；点击“保存私钥”按钮，弹出如下图所示的警告，选择“是”，输入私钥文件名“test_private”，并点击保存。

图 15-21



一定要选择使用 OpenSSH 格式的密钥文件，否则不能使用。puttygen.exe 能生成 OpenSSH 格式的密钥对，但是 Putty 客户端却不能直接使用，还需要使用 puttygen.exe 工具把私钥转换成 Putty 格式。放在服务器上的公钥文件不需要转换，还是 OpenSSH 格式。如下图所示。

图 15-22



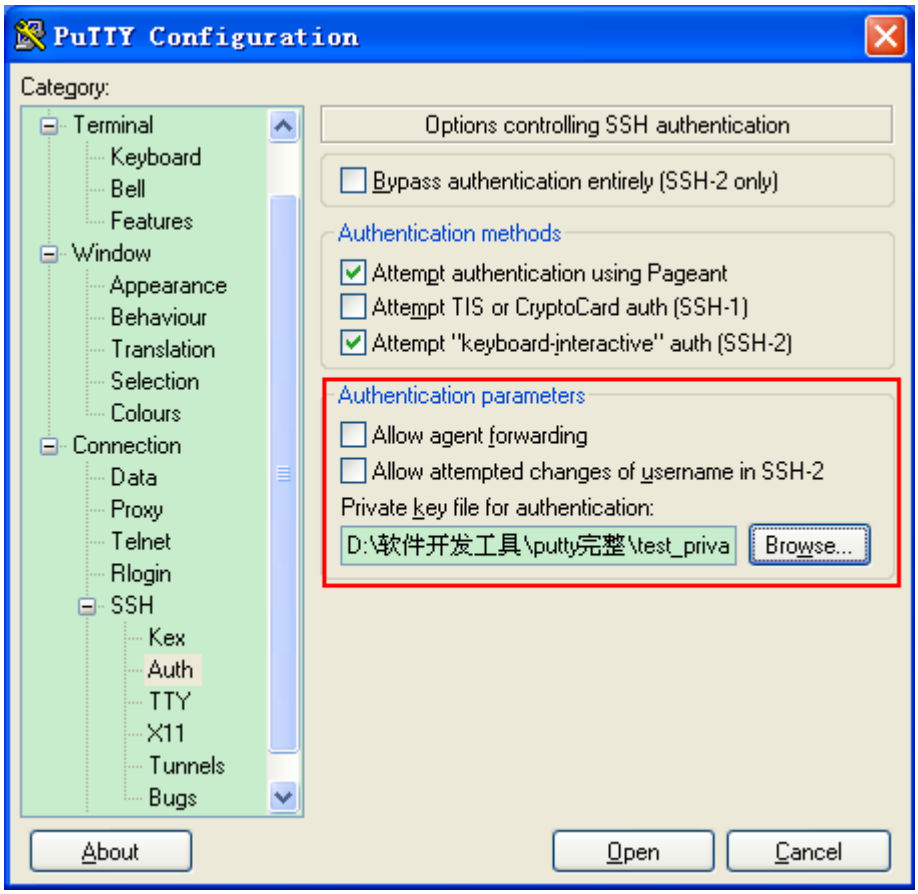
SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip ssh peer test public-key rsa flash:test_key.pub
```

【检验方法】

- 客户端与服务器端的基本配置完成之后，在 Putty 客户端中指定私钥文件 test_private，并设置服务器主机 IP 为 192.168.23.122，端口号为 22，建立客户端与服务器端的连接，这样，客户端就可以使用公钥认证方式登录网络设备了。

图 15-23



常见错误

- 使用命令 **no crypto key generate** 删除密钥。

15.4.2 配置SCP服务

配置效果

在网络设备上打开 SCP 服务器功能，用户可以直接对网络设备上的文件进行下载，以及将本地文件上传至网络设备，同时所有交互数据以密文形式进行传输，具有认证和安全性等特性。

注意事项

- SSH Server 已经完成配置。

配置方法

配置 SCP 服务功能

- 必须配置。
- 缺省情况下，SCP 功能处于关闭状态。在全局配置模式下，通过 **ip scp server enable** 命令开启 SCP 功能。

检验方法

使用 **show ip ssh** 命令，可以查看 SCP 服务器功能是否打开。

相关命令

配置 SCP 服务功能

【命令格式】 **ip scp server enable**
【参数说明】 -
【命令模式】 全局模式
【使用指导】 该命令打开开启 SCP 服务器功能。
no ip scp server enable 命令关闭 SCP 服务器功能。

配置举例

开启 scp 功能

【配置方法】
- 使用 **ip scp server enable** 开启 SCP 服务器功能。

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

【检验方法】
- 使用 **show ip ssh** 命令，可以查看 SCP 服务器功能是否打开。

```
Ruijie(config)#show ip ssh
SSH Enable - version 1.99
Authentication timeout: 120 secs
Authentication retries: 3
SSH SCP Server: enabled
```

配置 SSH 文件传输

【网络环境】
图 15-24

服务器端开启 SCP 服务，客户端通过 SCP 命令与服务器端进行数据传输。

【配置方法】
- 服务器端开启 SCP 服务。

SCP 服务器使用的是 SSH 线程，客户端连接网络设备进行 SCP 传输时候会占用一个 VTY 连接（通过 show user 命令查看的时候，会发现用户类型为 SSH）。

- 客户端使用 SCP 命令上传文件至服务器端，或从服务器端下载文件。

SCP 命令的语法：

```
scp [-1246BCpqrv] [-c cipher] [-F ssh_config] [-i identity_file]
    [-l limit] [-o ssh_option] [-P port] [-S program]
    [[user@]host1:]file1 [...] [[user@]host2:]file2
```

部分选项说明：

-1 ：使用 SSH1 版本（若不指定则默认使用 SSH2）；
-2 ：使用 SSH2 版本（默认）；
-C ：指定使用压缩传输；
-c ：指定使用的加密算法；
-r ：指定传输整个目录；
-i ：指定使用的密钥文件；
-l ：限制传输速度（单位 Kbits）；
其他具体的参数可以查看 scp.0 文件。

选项大部分与客户端有关，少数是客户端和服务器都需要支持的选项，锐捷网络设备上的 SCP 服务器端不支持-d -p -q -r 选项，使用这些选项时候会提示不支持。

SSH Server

```
Ruijie# configure terminal
Ruijie(config)# ip scp server enable
```

【检验方法】

- 文件传输举例，以在 Ubuntu 7.10 系统上操作为例：

指定用户名是 test，从 IP 为 192.168.23.122 的网络设备上，将 config.text 文件复制到本地的/root 目录下。

```
root@dhcpd:~# scp test@192.168.23.122:/config.text /root/config.text
test@192.168.195.188's password:
config.text                   100% 1506     1.5KB/s   00:00
Read from remote host 192.168.195.188: Connection reset by peer
```

常见配置错误

无

15.5 监视与维护

查看运行情况

作用	命令
显示 SSH Server 的当前生效的配置信息	**show ip ssh**

显示已经建立的 SSH 连接的每个连接信息	**show ssh**
显示 SSH Server 公共密钥的公开密钥部分的信息	**show crypto key mypubkey**

查看调试信息

输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 SSH 基本连接信息的调试开关	**debug ssh**

配置指南-系统配置

本分册介绍系统配置配置指南相关内容，包括以下章节：

1. 命令行界面
2. 基础管理
3. LINE
4. SNMP
5. HTTP 服务
6. 系统日志
7. RLOG
8. CWMP
9. LED
10. PKG_MGMT
11. NTP
12. SNTP
13. TIME RANGE

1 命令行界面

1.1 概述

命令行界面(Command Line Interface，CLI)是用户与网络设备进行文本指令交互的窗口，用户可以在命令行界面输入命令，实现对网络设备的配置和管理。

协议规范

命令行界面无对应的协议规范。

1.2 典型应用

典型应用	场景描述
通过CLI配置管理网络设备	通过在命令行界面输入命令对网络设备进行配置管理。

1.2.1 通过CLI配置管理网络设备

应用场景

以下图为例，用户通过终端登录网络设备 A，在命令行界面输入命令实现对设备的配置管理。

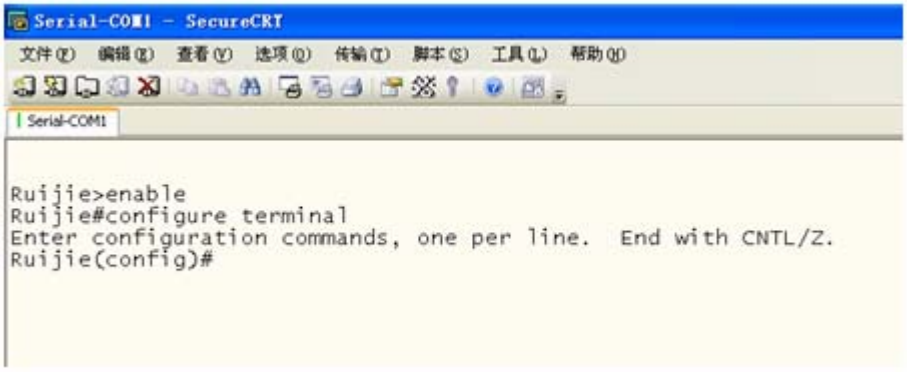
图 1-1

【注释】 A 为需要被管理的网络设备
PC 为用户端。

功能部署

下图列举了在 PC 上通过 Secure CRT 与网络设备 A 建立连接，并打开命令行界面配置命令。

图 1-2



1.3 功能详解

功能特性

功能特性	作用
访问CLI	登录网络设备进行配置管理。
命令模式	命令行接口分为若干种命令模式，不同的命令模式可使用的命令不同。
系统帮助	用户在 CLI 配置过程中可获取系统的帮助信息。
简写命令	如果输入的字符足够识别唯一的命令关键字，可以不必完整输入。
命令的no和default选项	通过 **no** 或 **default** 命令，禁止某个功能特性、执行与命令本身相反的操作或恢复缺省配置。
错误命令的提示信息	当用户输入错误命令时，会弹出相应的错误提示信息。
历史命令	用户可以通过快捷键的方式查询、调用历史命令。
编辑特性	系统提供相关快捷键便于用户编辑命令。
show命令的查找和过滤	用户可以在 **show** 命令输出的信息中查找或过滤指定的内容。
命令别名	配置命令的别名，可以替代命令执行配置。

1.3.1 访问CLI

在使用 CLI 之前，用户需要通过一个终端或 PC 和网络设备连接。启动网络设备，在网络设备硬件和软件初始化后就可以使用 CLI。在首次使用网络设备时，只能通过串口（Console）连接网络设备，称为带外（Out band）管理方式。在进行了相关配置后，还可以通过 Telnet 虚拟终端方式连接和管理网络设备。

1.3.2 命令模式

设备可供使用的命令非常多，为便于使用这些命令，将命令按功能进行分类。命令行接口分为若干个命令模式，所有命令都注册在某种（或几种）命令模式下。当使用某条命令时，需要先进入这个命令所在的模式。不同的命令模式之间既有联系又有区别。

当用户和网络设备管理界面建立一个新的会话连接时，用户首先处于用户模式（User EXEC 模式）。在此模式下，只可以使用少量命令，并且命令的功能也受到一些限制，例如像 show 命令等。用户模式的命令的操作结果不会被保存。

要使用更多的命令，首先须进入特权模式（Privileged EXEC 模式）。通常，在进入特权模式时必须输入特权模式的口令。在特权模式下，用户可以使用所有的特权命令，并且能够由此进入全局配置模式。

使用配置模式（全局配置模式、接口配置模式等）的命令，会对当前运行的配置产生影响。如果用户保存了配置信息，这些命令将被保存下来，并在系统重新启动时再次执行。要进入各种配置模式，首先必须进入全局配置模式。在全局配置模式下配置，可以进入接口配置模式等各种配置子模式。

各个命令模式概要如下（假定网络设备的名字为缺省的“Ruijie”）：

命令模式	访问方法	提示符	离开或访问下一模式	关于该模式
User EXEC (用户模式)	访问网络设备时默认进入该模式。	Ruijie>	输入 **exit** 命令离开该模式。 要进入特权模式，输入 **enable** 命令。	使用该模式来进行基本测试、显示系统信息。
Privileged EXEC (特权模式)	在用户模式下，使用 **enable** 命令进入该模式。	Ruijie#	要返回到用户模式，输入 **disable** 命令。 要进入全局配置模式，输入 **configure** 命令。	使用该模式来验证设置命令的结果。该模式是具有口令保护的。
Global configuration (全局配置模式)	在特权模式下，使用 **configure** 命令进入该模式。	Ruijie(config)#	要返回到特权模式，输入 **exit** 命令或 **end** 命令，或者键入 Ctrl+C 组合键。 要进入接口配置模式，输入 **interface** 命令。在 **interface** 命令中必须指明要进入哪一个接口配置子模式。 要进入 VLAN 配置模式，输入 **vlan** *vlan_id* 命令。	使用该模式的命令来配置影响整个网络设备的全局参数。
Interface configuration (接口配置模式)	在全局配置模式下，使用 **interface** 命令进入该模式。	Ruijie(config-if)#	要返回到特权模式，输入 **end** 命令，或键入 Ctrl+C 组合键。 要返回到全局配置模式，输入 **exit** 命令。在 **interface** 命令中必须指明要进入哪一个接口配置子模式。	使用该模式配置网络设备的各种接口。
Config-vlan (VLAN 配置模式)	在全局配置模式下，使用 **vlan** *vlan_id* 命令进入该模式。	Ruijie(config-vlan)#	要返回到特权模式，输入 **end** 命令，或键入 Ctrl+C 组合键。 要返回到全局配置模式，输入 **exit** 命令。	使用该模式配置 VLAN 参数。

1.3.3 系统帮助

用户在输入命令行的过程中，可以通过如下方式获取系统帮助。

1. 在任意模式的命令提示符下，输入问号（?）列出当前命令模式支持的命令及其描述信息。

例如：

```
Ruijie>?
Exec commands:
  <1-99>      Session number to resume
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  exit        Exit from the EXEC
  help        Description of the interactive help system
  lock        Lock the terminal
  ping        Send echo messages
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
```

2. 在一条命令的关键字后空格并输入问号（?），可以列出该关键字关联的下一个关键字或变量。

例如：

```
Ruijie(config)#interface ?
  Aggregateport     Aggregate port interface
  Dialer            Dialer interface
  GigabitEthernet   Gigabit Ethernet interface
  Loopback          Loopback interface
  Multilink         Multilink-group  interface
  Null              Null interface
  Tunnel            Tunnel interface
  Virtual-ppp       Virtual PPP interface
  Virtual-template  Virtual Template interface
  Vlan              Vlan interface
  range             Interface range command
```

如果该关键字后带的是一个参数值，则列出该参数的取值范围及其描述信息，如下所示：

```
Ruijie(config)#interface vlan ?
  <1-4094>  Vlan port number
```

3. 在输入不完整的命令关键字后输入问号（?），可以列出以该字符串开头的所有命令关键字。

例如：

```
Ruijie#d?
debug  delete  diagnostic  dir  disable  disconnect
```

4. 在输入不完整的命令关键字后，如果该关键字后缀唯一，可以键入<Tab>键生成完整关键字。

例如：

```
Ruijie# show conf<Tab>
Ruijie# show configuration
```

5. 在任何命令模式下，还可以通过 **help** 命令获取帮助系统的摘要描述信息。

例如：

```
Ruijie(config)#help
Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?'.)
```

1.3.4 简写命令

如果命令比较长，想简写命令，只需要输入命令关键字的一部分字符，且这部分字符足够识别唯一的命令关键字即可。

例如进入 GigabitEthernet 0/1 接口配置模式的命令“**interface** *gigabitEthernet 0/1*”可以简写成：

```
Ruijie(config)#int g0/1
Ruijie(config-if-GigabitEthernet 0/1)#
```

1.3.5 命令的no和default选项

大部分命令有 **no** 选项。通常，使用 **no** 选项来禁止某个特性或功能，或者执行与命令本身相反的操作。例如接口配置命令 **no shutdown** 执行关闭接口命令 **shutdown** 的相反操作，即打开接口。使用不带 **no** 选项的关键字，打开被关闭的特性或者打开缺省是关闭的特性。

配置命令大多有 **default** 选项，命令的 **default** 选项将命令的设置恢复为缺省值。大多数命令的缺省值是禁止该功能，因此在许多情况下 **default** 选项的作用和 **no** 选项是相同的。然而部分命令的缺省值是允许该功能，在这种情况下，**default** 选项和 **no** 选项的作用是相反的。这时 **default** 选项打开该命令的功能，并将变量设置为缺省的允许状态。

各命令的 **no** 或 **default** 选项作用请参见相应的命令手册。

1.3.6 错误命令的提示信息

当用户输入错误命令时，会弹出相应的错误提示信息。

常见的 CLI 错误信息：

错误信息	含义	如何获取帮助
% Ambiguous command: "show c"	用户没有输入足够的字符，网络设备无法识别唯一的命令。	重新输入命令，紧接着发生歧义的单词输入一个问号。可能输入的关键字将被显示出来。
% Incomplete command.	用户没有输入该命令的必需的关键字或者变量参数。	重新输入命令，输入空格再输入一个问号。可能输入的关键字或者变量参数将被显示出来。
% Invalid input detected at '^' marker.	用户输入命令错误，符号（^）指明了产生错误的单词的位置。	在所在地命令模式提示符下输入一个问号 ,该模式允许的命令的关键字将被显示出来。

1.3.7 历史命令

系统能够自动保存用户最近输入的历史命令，用户可以通过快捷键的方式查询、调用历史命令。

操作方法如下：

操作	结果
Ctrl-P 或上方向键	在历史命令表中浏览前一条命令。从最近的一条记录开始，重复使用该操作可以查询更早的记录。
Ctrl-N 或下方向键	在使用了 Ctrl-P 或上方向键操作之后，使用该操作在历史命令表中回到更近的一条命令。重复使用该操作可以查询更近的记录。

标准的终端支持方向键，例如 VT100 系列。

1.3.8 编辑特性

用户在进行命令行编辑时，可以使用如下按键或快捷键：

功能	按键、快捷键	说明
在编辑行内移动光标。	左方向键或 Ctrl-B	光标移到左边一个字符。
	右方向键或 Ctrl-F	光标移到右边一个字符。
	Ctrl-A	光标移到命令行的首部。
	Ctrl-E	光标移到命令行的尾部。
删除输入的字符。	Backspace 键	删除光标左边的一个字符。
	Delete 键	删除光标右边的一个字符。
输出时屏幕滚动一行或一页。	Return 键	在显示内容时用回车键将输出的内容向上滚动一行，显示下一行的内容，仅在输出内容未结束时使用。
	Space 键	在显示内容时用空格键将输出的内容向上滚动一页，显示下一页内容，仅在输出内容未结束时使用。

当编辑的光标接近右边界时，命令行会整体向左移动 20 个字符，命令行前部被隐藏的部分被符号（$）代替，可以使用相关按键或快捷键将光标移到前面的字符或者回到命令行的首部。

例如配置模式的命令 **access-list** 的输入可能超过一个屏幕的宽度。当光标第一次接近行尾时，命令行整体向左移动 20 个字符，命令行前部被隐藏的部分被符号（$）代替。每次接近右边界时都会向左移动 20 个字符长度。

```
access-list 199 permit ip host 192.168.180.220 host
$ost 192.168.180.220 host 202.101.99.12
$0.220 host 202.101.99.12 time-range tr
```

可以使用 Ctrl-A 快捷键回到命令行的首部，这时命令行尾部被隐藏的部分将被符号（$）代替：

```
access-list 199 permit ip host 192.168.180.220 host 202.101.99.$
```

默认的终端行宽是 80 个字符。

1.3.9 show命令的查找和过滤

要在 **show** 命令输出的信息中查找指定的内容，可以在使用以下命令：

命令	作用
show *any-command* | **begin** *regular-expression*	在 **show** 命令的输出内容中查找指定的内容，将第一个包含该内容的行以及该行以后的全部信息输出。

支持在任意模式下执行 **show** 命令。

查找的信息内容需要区分大小写，以下相同。

要在 **show** 命令的输出信息中过滤指定的内容，可以使用以下命令：

命令	作用
show *any-command* | **exclude** *regular-expression*	在 **show** 命令的输出内容中进行过滤，除了包含指定内容的行以外，输出其他的信息内容。
show *any-command* | **include** *regular-expression*	在 show 命令的输出内容中进行过滤，仅输出包含指定内容的行，其他信息将被过滤。

要在 **show** 命令的输出内容中进行查找和过滤，需要输入管道符号（竖线，"|"）。在管道字符之后，可以选择查找和过滤的规则和查找和过滤的内容（字符或字符串），并且查找和过滤的内容需要区分大小写：

```
Ruijie#show running-config | include interface
interface GigabitEthernet 0/0
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
interface GigabitEthernet 0/4
interface GigabitEthernet 0/5
interface GigabitEthernet 0/6
interface GigabitEthernet 0/7
interface Mgmt 0
```

1.3.10 命令别名

用户可以指定任意单词作为命令的别名，来简化命令行字符串的输入。

配置效果

1. 一个单词代替一条命令。

例如：将“**ip route** *0.0.0.0 0.0.0.0192.1.1.1*”配置别名“mygateway”，执行该命令只要输入“mygateway”即可。

2. 一个单词代替一条命令的前半部分，再输入后半部分。

例如：将“**ip address**”配置别名“ia”，执行 IP 地址配置可以先输入“ia”，再输入指定的 IP 地址及掩码。

配置方法

系统默认别名

在普通或特权用户模式下，部分命令存在默认的别名，可以通过 **show aliases** 命令查看：

```
Ruijie(config)#show aliases
Exec mode alias:
  h                    help
  p                    ping
  s                    show
  u                    undebug
  un                   undebug
```

这些默认的别名不能删除。

配置命令别名

相关命令如下：

【命令格式】 **alias** *mode command-alias original-command*

【参数说明】 *mode*：别名所代表的命令所处的命令模式。

command-alias：命令别名。

original-command：别名所代表的实际命令。

【命令模式】 全局模式

【使用指导】 在全局配置模式下，输入 **alias** ?可以列出当前可以配置别名的全部命令模式。

查看命令别名设置

使用 **show aliases** 命令可以查看系统中的别名设置。

注意事项

- 别名替代的命令必须是命令行的第一个字符开始。
- 别名替代的命令必须是一个完整的输入形式。
- 命令别名在使用时必须完整输入，否则不能被识别。

配置举例

↘ 定义一个别名替代整条命令

【配置方法】 在全局配置模式下，配置命令别名“ir”代表默认路由设置“**ip route** *0.0.0.0 0.0.0.0 192.168.1.1*”

```
Ruijie#configure terminal
Ruijie(config)#alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

【检验方法】

- 通过 **show alias** 查看别名是否设置成功。

```
Ruijie(config)#show alias
Exec mode alias:
  h                    help
  p                    ping
  s                    show
  u                    undebug
  un                   undebug
Global configuration mode alias:
  ir             ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

- 使用设置好别名执行命令，通过 **show running-config** 查看是否配置成功。

```
Ruijie(config)#ir
Ruijie(config)#show running-config

Building configuration...
!
alias config ir ip route 0.0.0.0 0.0.0.0 192.168.1.1 //配置别名
...
ip route 0.0.0.0 0.0.0.0 192.168.1.1  //输入别名“ir”的配置结果
!
```

↘ 定义一个别名替代一个命令的前半部分

【配置方法】 在全局配置模式下，配置命令别名“ir”代表默认路由设置的“**ip route**”

```
Ruijie#configure terminal
Ruijie(config)#alias config ir ip route
```

【检验方法】

- 通过 **show alias** 查看别名是否设置成功。

```
Ruijie(config)#show alias
Exec mode alias:
  h                    help
  p                    ping
  s                    show
  u                    undebug
  un                   undebug
Global configuration mode alias:
  ir            ip route
```

- 输入别名“ir”，再配置后半部分命令“0.0.0.0 0.0.0.0 192.168.1.1”。
- 通过 **show running-config** 查看是否配置成功。

```
Ruijie(config)#ir 0.0.0.0 0.0.0.0 192.168.1.1
Ruijie(config)#show running

Building configuration...
!
alias config ir ip route    //配置别名
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1    //输入别名“ir”及后半部分命令的配置结果
!
```

命令别名支持的系统帮助

3. 命令别名支持帮助信息，在别名前面会显示一个星号（*），格式如下：

```
*command-alias=original-command
```

例如，在 EXEC 模式下，默认的命令别名“s”表示“**show**”关键字。输入“s?”，可以获取’s’开头的关键字和别名的帮助信息：

```
Ruijie#s?
*s=show  show  start-chat  start-terminal-service
```

4. 如果别名所代表的命令不止一个单词，在帮助信息中将携带引号显示。

例如，在 EXEC 模式下配置别名“sv”代替命令 **show version**，输入“s?”，可以获取’s’开头的关键字和别名的帮助信息：

```
Ruijie#s?
*s=show  *sv="show version" show  start-chat
start-terminal-service
```

5. 获取系统帮助时，命令别名可以获取与该命令相关的帮助信息。

例如，配置接口模式下的命令别名“ia”代表“**ip address**”，在接口模式下输入“ia？”，可获取等同“**ip address**？”的帮助信息，并且将别名替换成实际的命令：

```
Ruijie(config-if)#ia ?
  A.B.C.D  IP address
  dhcp     IP Address via DHCP
Ruijie(config-if)#ip address
```

如果在命令之前输入了空格，将无法获取该别名表示的命令。

2 基础管理

2.1 概述

基础管理为首次接触网络设备管理的入门手册，介绍一些常用的网络设备管理、监控和维护的功能。

下文仅介绍基础管理的相关内容。

协议规范

无

2.2 典型应用

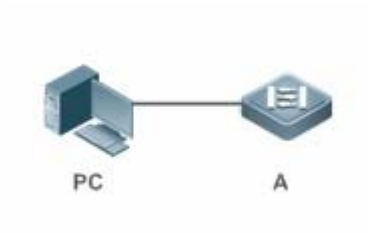
典型应用	场景描述
网络设备的管理	用户通过终端登录网络设备，在命令行界面输入命令实现对设备的配置管理。

2.2.1 网络设备的管理

应用场景

在本文档中，所涉及的管理都是通过命令行界面进行的，用户通过终端登录网络设备 A，在命令行界面输入命令实现对设备的配置管理。如下图所示：

图 2-1



2.3 功能详解

基本概念

TFTP

TFTP（Trivial File Transfer Protocol,简单 文件传输协议）是TCP/IP协议族中的一个用于客户机与 服务器之间进行简单文件传输的协议。

AAA

AAA（Authentication Authorization Accounting，认证授权计帐）。

Authentication认证：验证用户的身份与可使用的 网络服务。

Authorization 授权：依据认证结果开放网络服务给用户。

Accounting计帐：记录用户对各种网络服务的用量，并提供给 计费系统。整个系统在 网络管理与安全问题中十分有效。

RADIUS

RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统）是目前应用最广泛的 AAA协议。

Telnet

Telnet是位于OSI模型的第 7 层---应用层上的一种协议， 是一个通过创建 虚拟终端提供连接到远程 主机 终端仿真的TCP/IP协议。这一协议需要通过用户名和口令进行认证，是Internet远程登陆服务的标准协议。应用Telnet协议能够把 本地用户所使用的计算机变成远程 主机系统的一个 终端。

系统信息

系统信息主要包括系统描述，系统上电时间，系统的硬件版本，系统的软件版本，系统的 Ctrl 层软件版本，系统的 Boot 层软件版本。

硬件信息

硬件信息主要包括物理设备信息及设备上的插槽和模块信息。设备本身信息包括：设备的描述，设备拥有的插槽的数量。插槽信息：插槽在设备上的编号，插槽上模块的描述（如果插槽没有插模块，则描述为空），插槽所插入模块包括物理端口数，插槽最多可能包含的端口的最大个数（所插模块包括的端口数）。

功能特性

功能特性	作用
控制用户访问	通过使用口令保护和划分特权级别来控制网络上的终端访问网络设备。
控制登录认证	启用 AAA 的模式下，用户登录网络设备进行管理的时候可以通过一些服务器来根据用户名和密码进行用户的管理权限的认证。
系统基本参数	系统的各项参数，例如时钟，标题，控制台速率等。
查看配置信息	查看系统配置信息主要包括查看系统正在运行的配置信息，以及查看存储在 NVRAM（非易失性随机存取存储器）上设备的配置等。
使用Telnet	Telnet 属于 TCP/IP 协议族的应用层协议，它给出通过网络提供远程登录和虚拟终端通讯功能的规范。
重启	介绍系统重启。

2.3.1 控制用户访问

通过使用口令保护和划分特权级别来控制网络上的终端访问网络设备。

工作原理

↘ 授权级别

网络设备的命令行界面针对用户划分 0-15 共 16 个授权级别，不同级别的用户可以执行的命令是不同的。数字小的级别权限较小，其中 0 级为最低级别，只能执行少数几条命令；15 级为最高级别，可以执行所有的命令。0-1 级一般称为普通用户级别，不允许对设备进行配置（默认不允许进入全局配置模式），2-15 级一般称为特权用户级别，可以对设备进行配置。

↘ 口令类别

口令分为 password 和 security 两种。password 为简单加密的口令，只能设置为 15 级口令。security 口令为安全加密口令，可以为 0～15 级设置口令。如果系统中同级别同时存在以上两种口令，则 password 口令不生效。如果设置非 15 级的 password 口令，则会给出警告提示，并自动转为 security 口令；如果设置 15 级的 password 口令和 security 口令完全相同，则会给出警告提示；口令必须以加密形式保存，password 口令使用简单加密，security 口令使用安全加密。

↘ 口令保护

在网络设备上为每个特权级别设置口令，当用户想升高权限级别时，需要输入目的级别对应的口令，口令校验通过以后才允许升高权限级别。用户降低级别则不需要通过口令校验。

缺省时系统只有两个受口令保护的授权级别：普通用户级别（1 级）和特权用户级别（15 级）。但是用户可以为每个模式的命令划分 16 个授权级别。通过给不同的级别设置口令，就可以通过不同的授权级别使用不同的命令集合。

在特权用户级别口令没有设置的情况下，进入特权级别亦不需要口令校验。为了安全起见，我们提醒您最好为特权用户级别设置口令。

↘ 命令授权

每一条命令都有最低执行级别的要求，如果用户的权限级别达不到要求是无法执行该命令的。此时可以通过命令授权操作，将命令执行权限授予某个特权级别，将允许权限达到（大于或等于）该级别的用户执行该命令。

相关配置

↘ 设置 password 口令

- 使用 **enable password** 命令设置 password 口令。

↘ 设置 secret 口令

- 使用 **enable secret** 命令设置安全口令。
- 需要在切换用户级别时进行 secret 口令校验，可以配置此项。功能与 password 口令相同，但使用了更好的口令加密算法。为了安全起见，建议使用 secret 口令。

设置命令的级别

- 使用 **privilege** 命令设置命令的级别。
- 如果想让更多的授权级别使用某一条命令，则可以将该命令设置较低的用户级别；而如果想让命令的使用范围小一些，则可以将该命令设置较高的用户级别。

升高/降低用户级别

- 使用 **enable** / **disable** 命令升高/降低用户级别。
- 已经登录网络设备的用户，可以通过改变当前的用户级别，以访问不同级别的命令。

启用 line 线路口令保护

- 对远程登录（如 TELNET）进行口令验证，要配置 **line** 口令保护。
- 应先使用 **password**[**0** | **7**] *line* 命令配置 *line* 线路口令，然后执行 **login** 命令启动口令保护。
- 终端在缺省情况下不支持 **lock** 命令。

2.3.2 控制登录认证

在未启用 AAA 模式下，用户登录网络设备进行管理的时候，如果线路上设置了登陆认证（login），需要通过线路上所配置的口令进行校验，通过校验的用户才允许登录。如果线路上设置了本地认证（login local），则需要通过本地用户数据库来根据用户名和密码进行用户的管理权限的认证。

在启用 AAA 模式下，用户登录网络设备进行管理的时候，可以利用一些服务器根据用户名和密码进行用户的管理权限的认证，通过认证的用户才允许登录。

例如，利用 RADIUS 服务器，根据用户登录时的用户名和密码，控制用户对网络设备的管理权限。通过这种方式，网络设备不再用本地保存的密码信息进行认证，而是将加密后的用户信息发送到 RADIUS 服务器上进行验证。服务器统一配置用户的用户名、用户密码、共享密码和访问策略等信息，便于管理和控制用户访问，提高用户信息的安全性。

工作原理

线路口令

配置线路（line）口令的目的，是为了在未启用 AAA 模式的情况下，用于终端登录时的口令校验。启用了 AAA 模式以后，线路上的口令校验将不生效。

本地认证

配置本地认证的目的，是为了在未启用 AAA 模式的情况下，通过本地用户数据库来根据用户名和密码进行用户的管理权限的认证。启用了 AAA 模式以后，线路上的本地认证设置将不生效。

AAA 模式

AAA 是认证、授权和记账（Authentication, Authorization and Accounting）的简称，AAA 是一种体系结构框架，它提供包括认证、授权和记账在内三个互相独立的安全功能。启用了 AAA 模式以后，终端登录时候需要根据 AAA 所设置的登录认证方法列

表的要求，通过一些服务器（或本地用户数据库）来根据用户名和密码进行用户的管理权限的认证。AAA 功能详解参见 AAA 配置指南。

相关配置

↘ 配置本地用户

- 使用 **username** 命令配置用于本地身份认证和授权的账号信息，包括用户名、密码以及可选的授权信息。

↘ 线路登录进行本地认证

- 使用 **login local** 命令在 AAA 关闭时，LINE 线路登录认证时走本地用户认证。
- 应在每台设备上配置。

↘ 线路登录进行 AAA 认证

- AAA 打开的情况下，默认使用 **default** 认证方法。
- 使用 **login authentication** 命令在 LINE 线路上配置登录认证方法列表。
- AAA 设置为采用本地认证方法时需要配置。

↘ 设置连接超时时间

- 缺省的超时时间为 10 分钟。
- 使用 **exec-timeout** 命令设置连接超时时间。当前已接受的连接，在指定时间内，没有任何输入时，将中断此连接。
- 在需要延长或缩短这段等待时间时，应执行此配置项。

↘ 设置会话超时时间

- 缺省的超时时间为 0 min，代表永不超时。
- 使用 **session-timeout** 命令设置会话超时时间。
- 当前 LINE 上已经建立的会话，在指定时间内，没有任何输入信息，将中断当前连接到远程终端的会话。并且恢复终端为空闲状态。在需要延长或缩短这段等待时间时，应执行此配置项。

↘ 会话锁定

- 终端在缺省情况下不支持 **lock** 命令。
- 使用 **lockable** 命令允许用户锁住当前线路所连接的终端。
- 要使用会话锁定功能，需要在 line 配置模式下启用锁住 line 终端的功能，并在相应终端的 EXEC 模式下，通过使用 **lock** 命令锁住终端。

2.3.3 系统基本参数

↘ 系统时间

网络设备的系统时钟主要用于系统日志等需要记录事件发生时间的地方。该时钟提供具体日期(年、月、日)和时间(时、分、秒)以及星期等信息。

对于一台网络设备，当第一次使用时你需要首先手工配置网络设备系统时钟为当前的日期和时间。

配置系统名称和命令提示符

为了管理的方便，可以为一台网络设备配置系统名称(System Name)来标识它。默认系统名为“Ruijie”，如果系统名称超过 32 个字符，则截取其前 32 个字符。默认情况下，系统名称作为默认的命令提示符，提示符将随着系统名称的变化而变化。

标题

标题可以提供一些常规的登录提示信息。可以创建的标题（banner）类型有两种：每日通知和登录标题。

- 每日通知针对所有连接到网络设备的用户，当用户登录网络设备时，通知消息将首先显示在终端上。利用每日通知，你可以发送一些较为紧迫的消息（比如系统即将关闭等）给用户。
- 登录标题显示在每日通知之后，它的主要作用是提供一些常规的登录提示信息。

配置控制台速率

通过配置控制台接口可以对网络设备进行管理。当网络设备第一次使用的时候，必须采用通过控制台口方式对其进行配置。使用时可以根据实际需求，改变网络设备串口的速率。需要注意的是，用来管理网络设备的终端的速率设置必须和网络设备的控制台的速率一致。

设置连接超时

配置设备的连接超时时间，控制该设备已经建立的连接（包括已接受连接，以及该设备到远程终端的会话）。当空闲时间超过设置值，没有任何输入输出信息时，中断此连接。

相关配置

设置系统的日期和时钟

- 使用**clock set**命令通过手工的方式来设置网络设备上的时间。当你设置了网络设备的时钟后，网络设备的时钟将以你设置的时间为准一直运行下去，即使网络设备下电，网络设备的时钟仍然继续运行。

更新硬件时钟

- 如果硬件时钟和软件时钟不同步，使用 **clock update-calendar** 命令可以通过软件时钟的日期和时间复制给硬件时钟。

设置系统名称

- 使用 **hostname** 命令可以修改默认的系统名称。
- 缺省的主机名为 Ruijie。

设置命令提示符

- 通过 **prompt** 命令可以设置用户命令接口的提示符。

设置每日通知

- 缺省没有每日通知。
- 使用 **banner motd 命令**配置每日通知信息。
- 每日通知针对所有连接到网络设备的用户，当用户登录网络设备时，通知消息将首先显示在终端上。利用每日通知，你可以发送一些较为紧迫的消息（比如系统即将关闭等）给用户。

配置登录标题

- 缺省没有登录标题。
- 使用 **banner login** 命令设置登录标题，用于提供一些常规的登录提示信息。

设置控制台的传输速率

- 使用 **speed** 命令配置终端设备的速率。
- 缺省的速率是 9600。

2.3.4 查看配置信息

查看系统配置信息主要包括查看系统正在运行的配置信息，以及查看存储在 NVRAM（非易失性随机存取存储器）上设备的配置等。

工作原理

系统正在运行的配置信息

系统正在运行的配置信息即 running-config 是系统上所有的组件模块当前运行的配置的总和，具有实时性的特点。在查看的时候，先需要向所有的运行组件请求搜集配置，并经过一定的编排组合后显示给用户。正因为实时性的特点，只有运行中的组件才可能提供此配置信息，如果组件未加载则不会显示其配置。这样，在系统启动、组件进程重启、以及运行热补丁的过程中，组件处于不稳定状态情况下所收集的系统运行配置会有一定的差异。 例如在某一时段收集的信息中缺乏某个组件的配置，过一段时间后再收集就有了。

系统的启动配置信息

存储在 NVRAM（非易失性随机存取存储器）上设备的配置即 startup-config 为设备启动时执行的配置，在系统重新启动后将会导入 startup-config 成为新的运行配置。查看永久配置的过程就是读取设备 NVRAM 上的 startup-config 文件信息并显示。

相关配置

查看系统正在运行的配置信息

执行 **show running-config** [**interface** *interface*] 命令查看系统正在运行的配置信息或某个接口下的配置信息。

查看设备的启动配置信息

执行 **show startup-config** 命令查看设备的启动配置信息。

保存设备的启动配置信息

执行 **write** 命令或者 **copy running-config startup-config** 将设备的当前正在运行的配置信息，保存成为新的启动配置信息。

2.3.5 使用Telnet

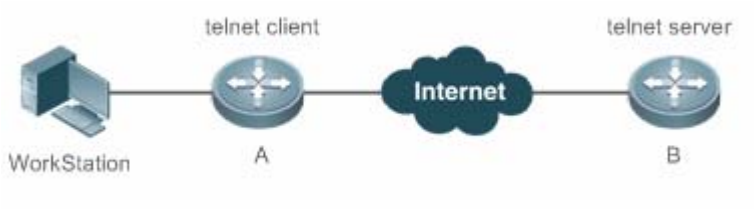
工作原理

Telnet 属于 TCP/IP 协议族的应用层协议，它给出通过网络提供远程登录和虚拟终端通讯功能的规范。

Telnet Client 服务为已登录到本网络设备上的本地用户或远程用户提供使用本网络设备的 Telnet Client 程序访问网上其他远程系统资源的服务。如下图所示用户在微机上通过终端仿真程序或 Telnet 程序建立与网络设备 A 的连接后，可通过输入 telnet 命令再登录设备 B，并对其进行配置管理。

锐捷网络的 Telnet 程序同时支持使用 IPV4 和 IPV6 地址进行通讯。作为 Telnet Server，可以同时接受 IPV4 和 IPV6 的 Telnet 连接请求。作为 Telnet Client，可以向 IPV4 和 IPV6 地址的主机发起连接请求。

图 2-1



相关配置

使用 telnet client

- 使用 **telnet** 命令通过 telnet 登录到远程设备。

恢复已建立的 Telnet Client 会话连接

- 执行**<1-99>**命令恢复已建立的 Telnet Client 会话连接。

断开挂起的 Telnet Client 连接

- 执行 **disconnect** *session-id* 命令断开指定的 Telnet Client 连接。

使用 Telnet Server

- 使用 **enable service telnet-server** 命令打开 Telnet Server 服务。
- 需要使用 Telnet 登录本地设备时，需要打开该服务。

2.3.6 重启

定时重启功能，它在某些场合下(比如出于测试目的或其它需要)可以为用户提供操作上的便利。

- 指定系统在经过一定时间间隔后重启。这里的时间间隔由 *mmm* 或 *hhh:mm* 决定，以分钟为单位，用户可以任选一种格式输入。用户可以在这里为这个计划起一个助记名，以便能直观地反映该重启的用途。
- 指定系统在将来的某个时间点重启。输入的时间值必须是将来的某个时间点。

⚠ 如果用户要使用 **at** 选项，则要求当前系统必须支持时钟功能。建议使用之前先配置好系统的时钟，以便更切合您的用途。如果用户之前已经设置了重启计划，则后面再设置的计划将覆盖前面的设置。如果用户已经设置了重启计划，假如在该计划生效前用户重启了系统，则该计划将丢失。

⚠ 重启计划中的时间与当前时间的跨度不能超过 31 天并且要大于当前系统时间。同时用户在设置了重启计划之后最好不要再修改系统时钟,否则有可能会导致设置失效，比如将系统时间调到重启时间之后。

相关配置

↘ 设置重启

- 使用 **reload** 命令设置重启策略。
- 使用该命令可以指定设备在指定的时刻启动，方便进行管理。

2.4 配置详解

配置口令与权限	⚠ 可选配置。设置口令与命令级别划分。	
	enable password	设置 password 口令
	enable secret	设置 secret 口令
	enable	升高用户级别
	disable	降低用户级别
	privilege	设置命令的级别划分
	password	指定 line 线路口令
	login	启用 line 线路口令保护
配置登录与认证	⚠ 可选配置。配置不同登录方式及认证。	
	username	配置本地用户账号以及可选的授权信息
	login local	线路登录进行本地认证
	loginauthentication	线路登录进行 AAA 认证
	telnet	使用 Telnet Client
	enable service telnet-server	使用 Telnet Server
	exec-timeout	配置连接超时时间

	session-timeout	配置会话超时时间
	lockable	启用锁住 line 终端的功能
	lock	锁住当前 line 终端
设置系统基本参数	可选配置。设置系统基本参数。	
	clock set	设置系统的日期和时钟
	clock update-calendar	更新硬件时钟
	hostname	设置系统名称
	prompt	设置命令提示符
	banner motd	设置每日通知
	bannerlogin	配置登录标题
	speed	设置控制台的传输速率
打开或关闭指定的服务	可选配置。打开与关闭指定的服务。	
	enable service	打开某项服务。
设置重启策略	可选配置。设置系统重启时的策略。	
	reload	重启设备。

2.4.1 配置口令与权限

配置效果

- 设置用户的口令，可以控制对网络设备的访问。
- 对命令使用权限进行分级，对于特定级别的命令，只有达到或高于这个级别的用户才可以使用。
- 将命令的使用权授予较低的用户级别，让更多的授权级别使用该条命令。
- 该命令的使用权授予较高的用户级别，则该命令的使用范围会缩小。

注意事项

- 在设置口令中，如果使用带**level**关键字时，则为指定特权级别定义口令。设置了特定级别的口令后，给定的口令只适用于那些需要访问该级别的用户。
- 缺省没有设置任何级别的 password 或 secret 口令，如果没有指定 level，则缺省的级别是 15 级。
- 如果设置非 15 级的 password 口令，系统将自动转换为 secret 口令，并给出提示信息。
- 如果同时设置了 password 口令和 secret 口令，则系统将选择使用 secret 口令。

配置方法

设置 password 口令

- 可选配置。需要在切换用户级别时进行 password 口令校验，可以配置此项。
- 使用 **enable password** 命令设置 password 口令。

设置 secret 口令

- 可选配置。需要在切换用户级别时进行 secret 口令校验，可以配置此项。
- 使用 **enable secret** 命令设置安全口令。
- 功能与 password 口令相同，但使用了更好的口令加密算法。为了安全起见，建议使用 secret 口令。

设置命令的级别

- 可选配置。
- 如果想让更多的授权级别使用某一条命令，则可以将该命令设置较低的用户级别；而如果想让命令的使用范围小一些，则可以将该命令设置较高的用户级别。

升高/降低用户级别

- 已经登录网络设备的用户，可以通过改变当前的用户级别，以访问不同级别的命令。
- 使用 **enable** / **disable** 命令升高/降低用户级别。

启用 line 线路口令保护

- 可选配置。对远程登录（如 TELNET）进行口令验证，要配置 **line** 口令保护。
- 应先使用 **password**[**0** | **7**] *line* 命令配置 *line* 线路口令，然后执行 **login** 命令启动口令保护。

⚠ 如果没有配置登录认证，即使配置了 **line** 口令，登录时，也不会提示用户输入口令进行认证。

检验方法

- 可以使用 **show privilege** 命令查看当前用户级别。
- 可以使用 **show running-config** 命令查看配置。

相关命令

设置 password 口令

【命令格式】 **enable password** [**level** *level*] { *password* | [**0** | **7**] *encrypted-password* }

【参数说明】 *level*：用户的级别。

password：用户进入特权 EXEC 配置层的口令。

0：表示输入的口令字符串为明文字符串。

7：表示输入的口令字符串为密文字符串。

encrypted-password：口令文本。必须包含 1 到 26 个大小写字母和数字字符。

口令前面可以有前导空格，但被忽略。中间及结尾的空格则作为口令的一部分。

【命令模式】 全局模式

【使用指导】 目前只能设置 15 级用户的口令，并且只能在未设置 security 口令的情况下有效。

如果设置非 15 级的口令，系统将会给出一个提示，并自动转为 security 口令。

如果设置的 15 级 password 口令和 15 级安全口令完全相同，系统将会给出一个警告信息。

如果指定了加密类型，然后输入一条明文口令，则不能重新进入特权 EXEC 模式。不能恢复用任意方法加密的已丢失口令。只能重新配置设备口令。

设置 secret 口令

【命令格式】 **enable secret** [**level** *level*] {*secret* | [**0 | 5**] *encrypted-secret* }

【参数说明】 *level*：用户的级别。

secret：用户进入特权 EXEC 配置层的口令。

0 | 5：口令的加密类型，0 无加密，5 安全加密。

encrypted-password：口令文本。

【命令模式】 全局配置模式

【使用指导】 配置不同权限级别的安全的口令。

升高用户级别

【命令格式】 **enable** [*privilege-level*]

【参数说明】 *privilege-level*：权限等级。

【命令模式】 特权用户模式

【使用指导】 从权限较低的级别切换到权限较高的级别需要输入相应级别的口令。

降低用户级别

【命令格式】 **disable** [*privilege-level*]

【参数说明】 *privilege-level*：权限等级

【命令模式】 特权用户模式

【使用指导】 从权限较高的级别切换到权限较低的级别需要输入相应级别的口令。

使用该命令从特权用户模式退到普通用户模式。如果加上权限等级 ,则将当前权限等级降低到指定的权限等级。

disable 命令后面所跟权限等级必须小于当前权限等级。

设置命令的级别划分

【命令格式】 **privilege** *mode* [**all**] {**level** *level* | **reset**} *command-string*

【参数说明】 *mode* :要授权的命令所属的 CLI 命令模式 ,例如 :config 表示全局配置模式 ;exec 表示特权命令模式 ,interface 表示接口配置模式等等。

all：将指定命令的所有子命令的权限，变为相同的权限级别。

level *level*：授权级别，范围从 0 到 15。

reset：将命令的执行权限恢复为默认级别。

command-string：要授权的命令。

【命令模式】 全局模式

【使用指导】 可以在全局配置模式下使用 **no privilege** *mode* [**all**]**level** *level command* 命令，恢复一条已知的命令授权。

指定 line 线路口令

【命令格式】 **password**[**0** | **7**] *line*

【参数说明】 **0**：以明文方式配置口令。

7：以密文方式配置口令。

line：配置的口令字符串。

【命令模式】 **line** 配置模式

【使用指导】 -

启用 line 线路口令保护

【命令格式】 **login**

【参数说明】 **-**

【配置模式】 **line** 配置模式

【使用指导】 -

配置举例

配置命令授权

【网络环境】 将 **reload** 命令及其子命令授予级别 1 并且设置级别 1 为有效级别（通过设置口令为"**test**"）。

【配置方法】

- 将 **reload** 命令及其子命令授予级别 1

```
Ruijie# configure terminal
Ruijie(config)# privilege exec all level 1 reload
Ruijie(config)# enable secret level 1 0 test
Ruijie(config)# end
```

【检验方法】

- 进入 1 级，查看 **reload** 命令及子命令是否存在。

```
Ruijie# disable 1
Ruijie> reload ?
at                      reload at<cr>
```

常见错误

- 无

2.4.2 配置登录与认证

配置效果

- 建立线路登录身份认证。
- 通过网络设备上的 telnet 命令登录到远程设备上去。
- 当前已接受的连接，在指定时间内，没有任何输入信息，服务器端将中断此连接。
- 当前 LINE 上已经建立的会话，在指定时间内，没有任何输入信息，将中断当前连接到远程终端的会话。并且恢复终端为空闲状态。
- 使用锁住会话终端的功能，以防止访问。终端被锁定后，在终端下输入任何字符，系统都会提示输入解锁口令，口令认证成功后，系统自动解锁。

注意事项

- 无

配置方法

配置本地用户

- 必选配置。
- 使用 **username** 命令配置用于本地身份认证和授权的账号信息，包括用户名、密码以及可选的授权信息
- 应在每台设备上配置本地身份认证的账号信息

线路登录进行本地认证

- 必选配置。
- 在 AAA 关闭时，LINE 线路登录认证时走本地用户认证。
- 应在每台设备上配置。

线路登录进行 AAA 认证

- 可选配置。AAA 设置为采用本地认证方法时需要配置。
- AAA 认证模式打开时，设置线路登录进行 AAA 认证。
- 应在每台设备上配置。

使用 telnet client

- 通过 telnet 登录到远程设备。

恢复已建立的 Telnet Client 会话连接

- 可选配置。Telnet Client 会话连接暂时退出后，如果需要恢复该连接，可以使用本命令恢复。

断开挂起的 Telnet Client 连接

- 可选配置。如果需要断开指定的 Telnet Client 连接，可以在 Telnet Client 设备上执行该配置项。

使用 Telnet Server

- 可选配置。需要使用 Telnet 登录本地设备时，需要打开该服务。
- 打开 Telnet Server 服务。

设置连接超时时间

- 可选配置。
- 当前已接受的连接，在指定时间内，没有任何输入时，将中断此连接。
- 在需要延长或缩短这段等待时间时，应执行此配置项。

设置会话超时时间

- 可选配置。
- 当前 LINE 上已经建立的会话，在指定时间内，没有任何输入信息，将中断当前连接到远程终端的会话。并且恢复终端为空闲状态。
- 在需要延长或缩短这段等待时间时，应执行此配置项。

会话锁定

- 可选配置。在已建立会话后需要临时离开设备时，在设备上执行会话锁定功能。
- 要使用会话锁定功能，需要在 line 配置模式下启用锁住 line 终端的功能，并在相应终端的 EXEC 模式下，通过使用 **lock** 命令锁住终端。

检验方法

- 使用 **show running-config** 命令可以查看配置。
- 在 AAA 关闭时，配置了本地用户以后，并在线路上设置采用本地认证。用户登录时将提示输入用户名和口令，认证通过后才允许进入命令行界面。
- 在AAA打开时，配置了本地用户后，并在AAA的登录认证方法中指定采用本地方法。用户登录时将提示输入用户名和口令，认证通过后才允许进入命令行界面。
- 已经登录进入命令行界面的用户，可以使用 **show user** 命令查看当前登录的用户信息。
- 在本地设备上开启 Telnet Server 后，用户可以使用 Telnet 客户端连接本地设备。
- 用户在被锁住的界面上输入回车后，会提示输入口令，只有口令与之前所设置的相符，才会解锁这个终端会话。
- 使用 **show sessions** 命令，可以查看已经建立的 Telnet Client 实例的每个实例信息。

相关命令

配置本地用户

【命令格式】 **username** *name* [**login mode** { **console** | **ssh** | **telnet** }] [**online amount** *number*] [**permission** *oper-mode path*] [**privilege** *privilege-level*] [**reject remote-login**] [**web-auth**] [**pwd-modify**] [**nopassword** | **password** [**0** | **7**] *text-string*]

【参数说明】 *name*：用户名。

login mode：配置账号的登录方式限制。

console：限制账号的登录方式为 console。

ssh：限制账号的登录方式为 ssh。

telnet：限制账号的的登录方式为 telnet。

online amount *number*：配置账号的同时在线数量。

permission *oper-mode path*：配置账号对指定文件的操作权限，*op-mode* 表示操作模式，*path* 表示作用的文件或者目录的路径。

privilege *privilege-level*：配置账号的权限级别，取值范围 0 到 15。

reject remote-login：限制使用该账号进行远程登录。

web-auth：此账号只能用于 web 认证。

pwd-modify：允许使用该账号的 web 认证用户修改密码，该选项只有在配置了 **web-auth** 之后才可用。

nopassword：该账号不配置密码。

password [**0** | **7**] *text-string*：配置账号的密码，0 表示输入明文密码，7 表示输入密文密码，默认为输入明文密码。

【命令模式】 全局配置模式

【使用指导】 用于建立本地用户数据库，供认证使用。

如果指定加密类型为 7，则输入的合法密文长度必须为偶数。

通常无须指定加密类型为 7。一般情况下，只有当复制并粘贴已经加密过的口令时，才需要指定加密类型为 7。

线路登录进行本地认证

【命令格式】 **login local**

【参数说明】 -

【命令模式】 line 配置模式

【使用指导】 如果没有启用 AAA 安全服务，则该命令用于配置 LINE 线路登录认证时走本地用户认证。这里的本地用户是指通过 **username** 命令配置的用户信息。

线路登录进行 AAA 认证

【命令格式】 **loginauthentication** { **default** | *list-name* }

【参数说明】 **default**：默认的认证方法列表名。

list-name：可选的方法列表名。

【配置模式】 line 配置模式

【使用指导】 AAA 认证模式打开时，设置线路登录进行 AAA 认证。认证时使用 AAA 方法列表中的认证方法，包括 Radius 认证、本地认证、无认证等。

使用 Telnet Client

【命令格式】 **telnet** *host* [*port*] [**/source** { **ip** *A.B.C.D* **| ipv6** *X:X:X:X::X* **| interface** *interface-name* }]

【参数说明】 *Host*：Telnet 服务器的 IPV4 地址、IPV6 地址或者主机名。

Port：Telnet 服务器的 TCP 端口号，默认值为 23。

/source:指定 Telnet 客户端使用的源 IP 或者源接口。

ip *A.B.C.D*：指定 Telnet 客户端使用的源 IPV4 地址。

ipv6 *X:X:X:X::X*：指定 Telnet 客户端使用的源 IPV6 地址。

interface *interface-name*：指定 Telnet 客户端使用的源接口。

【命令模式】 特权用户模式

【使用指导】 通过 telnet 登录到远程设备，可以是 IPV4 主机名或者 IPV6 主机名、IPV4 地址或者 IPV6 地址。

恢复已建立的 Telnet Client 会话连接

【命令格式】 <1-99>

【参数说明】 -

【命令模式】 普通用户模式

【使用指导】 该命令用于恢复使用已经建立的 Telnet Client 会话连接。当使用 **telnet** 命令发起 Telnet Client 会话连接时，可以使用热键 (ctrl+shift+6 x) 暂时退出该连接。如果需要恢复该连接，可以使用**<1-99>**命令进行恢复。同时，如果连接已建立，可以使用 **show sessions** 命令查看已建立的连接信息。

断开挂起的 Telnet Client 连接

【命令格式】 **disconnect** *session-id*

【参数说明】 *session-id*：挂起的 Telnet Client 连接会话号。

【命令模式】 普通用户模式

【使用指导】 通过输入指定的 Telnet Client 连接会话号，断开指定的 Telnet Client 连接。

使用 Telnet Server

【命令格式】 **enable service telnet-server**

【参数说明】 -

【配置模式】 全局模式

【使用指导】 打开 Telnet Server 服务；该命令同时打开 IPV4 和 IPV6 服务。

配置连接超时时间

【命令格式】 **exec-timeout** *minutes* [*seconds*]

【参数说明】 *minutes*：指定的超时时间的分钟数。

seconds：指定的超时时间的秒数。

【命令模式】 line 配置模式

【使用指导】 配置 LINE 上，已接受连接的超时时间，当超过配置时间，没有任何输入时，将中断此连接。

在 LINE 配置模式下使用 **no exec-timeout** 命令，取消 LINE 下连接的超时设置。

配置会话超时时间

【命令格式】 **session-timeout** *minutes*[**output**]

【参数说明】 *minutes*：指定的超时时间的分钟数。

output：是否将输出数据也作为输入，来判断是否超时。

【命令模式】 line 配置模式

【使用指导】 配置 LINE 上，连接到远程终端的会话超时时间，在指定时间内，没有任何输入时，将中断此会话。

在 LINE 配置模式下使用 **no session-timeout** 命令，取消 LINE 下到远程终端的会话超时时间设置。

启用锁住 line 终端的功能

【命令格式】 **lockable**

【参数说明】 -

【命令模式】 line 配置模式

【使用指导】 -

锁住当前 line 终端

【命令格式】 **lock**

【参数说明】 **-**

【配置模式】 line 配置模式

【使用指导】 -

配置举例

建立与远程网络设备的 Telnet 会话

【配置方法】

- 建立与远程网络设备的 Telnet 会话，远程网络设备的 IP 地址是 192.168.65.119。
- 建立与远程网络设备的 Telnet 会话，远程网络设备的 IPV6 地址是 2AAA:BBBB::CCCC。

```
Ruijie# telnet 192.168.65.119
Trying 192.168.65.119 ... Open
User Access Verification
Password:
Ruijie# telnet 2AAA:BBBB::CCCC
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification
Password:
```

【检验方法】

- 如果能正常与远程设备建立会话，则配置成功。

连接超时

【配置方法】

- 设置超时时间为 20min

```
Ruijie# configure terminal//进入全局配置模式
Ruijie# line vty 0                          //进入 LINE 配置模式
Ruijie(config-line)#exec-timeout 20   //设置超时时间为 20min
```

【检验方法】

- 连接到本地设备的终端，在这段时间内容没有任何输入，将断开连接并退出。

↘ 设置超时时间为 20min

【配置方法】 ● 设置超时时间为 20min

```
Ruijie# configure terminal//进入全局配置模式
Ruijie(config)# line vty 0                    //进入 LINE 配置模式
Ruijie(config-line)#session-timeout 20//设置超时时间为 20min
```

【检验方法】 ● 连接到远程设备的终端，在这段时间内容没有任何输入，将断开连接并退出。

常见配置错误

- 无

2.4.3 设置系统基本参数

配置效果

- 设置系统的基本参数。

注意事项

- 无

配置方法

↘ 设置系统的日期和时钟

- 必选配置。
- 通过手工的方式来设置网络设备上的时间。当你设置了网络设备的时钟后，网络设备的时钟将以你设置的时间为准一直运行下去，即使网络设备下电，网络设备的时钟仍然继续运行。

⚠ 但是对于没有提供硬件时钟的网络设备，手工设置网络设备上的时间实际上只是设置软件时钟，它仅对本次运行有效，当网络设备下电后，手工设置的时间将失效。

↘ 更新硬件时钟

- 可选配置。
- 如果硬件时钟和软件时钟不同步，需要通过软件时钟的日期和时间复制给硬件时钟时，执行此配置项。

↘ 设置系统名称

- 可选配置。可以修改默认的系统名称。

设置命令提示符

- 可选配置。可以修改默认的命令提示符名称。

设置每日通知

- 可选配置。在希望告知使用者一些重要提示或警告信息时，可以选择在系统上设置每日通知。
- 你可以创建包含一行或多行信息的通知信息，当用户登录网络设备时，这些信息将会被显示。

配置登录标题

- 可选配置。如果希望对使用者在登录或退出作一些重要信息的提示，可以选择配置此项。

设置控制台的传输速率

- 可选配置。可以修改默认的控制台速率。

检验方法

- 使用 **show clock** 命令来显示系统时间信息。
- 标题的信息将在你登录网络设备时显示。
- 使用 **show version** 命令查看系统、版本信息。

相关命令

设置系统的日期和时钟

【命令格式】 **clock set** *hh:mm:ss month day year*

【参数说明】 *hh:mm:ss*：当前时间，格式为小时（24 小时制）：分钟 ： 秒。

day：日期（1-31），一个月中的日期。

month：月份（1-12），一年中的月份。

year：公元年（1993-2035），不能使用缩写。

【命令模式】 特权用户模式

【使用指导】 使用该命令设置系统时间，方便管理。

对于没有提供硬件时钟的网络设备，使用 **clock set** 设置网络设备上的时间仅对本次运行有效，当网络设备下电后，手工设置的时间将失效。

更新硬件时钟

【命令格式】 **clock update-calendar**

【参数说明】 -

【命令模式】 特权用户模式

【使用指导】 软件时钟就会覆盖硬件时钟的值。

设置系统名称

【命令格式】 **hostname** *name*

【参数说明】 *name*：系统名称，名称必须由可打印字符组成，长度不能超过 63 个字节。

【命令模式】 全局模式

【使用指导】 在全局配置模式下使用 **no hostname** 来将系统名称恢复位缺省值。

设置命令提示符

【命令格式】 **prompt** *string*

【参数说明】 *string*：名称必须由可打印字符组成，如果长度超过 32 个字符，则截取其前 32 个字符。

【命令模式】 特权用户模式

【使用指导】 在全局配置模式下使用 **no prompt** 来将命令提示符恢复为缺省值。

设置每日通知

【命令格式】 **banner motd** *c message c*

【参数说明】 *c*：分界符，这个分界符可以是任何字符(比如'&'等字符)。

【命令模式】 全局配置模式

【使用指导】 输入分界符后，然后按回车键，即可以开始输入文本，需要在键入分界符并按回车键来结束文本的输入。需要注意的是，如果键入结束的分界符后仍然输入字符，则这些字符将被系统丢弃。通知信息的文本中不应该出现作为分界符的字母，文本的长度不能超过 255 个字节。

配置登录标题

【命令格式】 **banner login** *c message c*

【参数说明】 *c*：分界符，这个分界符可以是任何字符(比如'&'等字符)。

【命令模式】 全局配置模式

【使用指导】 输入分界符后，然后按回车键，即可以开始输入文本，需要在键入分界符并按回车键来结束文本的输入，需要注意的是，如果键入结束的分界符后仍然输入字符，则这些字符将被系统丢弃。登录标题的文本中不应该出现作为分界符的字母，文本的长度不能超过 255 个字节。

在全局配置模式下使用 **no banner login** 来删除登录标题。

设置控制台的传输速率

【命令格式】 **speed** *speed*

【参数说明】 *speed*：，单位是 bps。对于串行接口。只能将传输速率设置为 9600、19200、38400、57600、115200 中的一个，缺省的速率是 9600。

【命令模式】 line 配置模式

【使用指导】 用户可以根据需要来设置异步线路的波特率。命令 **speed** 将同时设置异步线路的接收速率以及发送速率。

配置举例

配置系统时间

【配置方法】

- 把系统时间改成 2003-6-20，10:10:12

```
Ruijie# clock set 10:10:12 6 20 2003        //设置系统时间和日期
```

【检验方法】 ● 在特权模式下使用 **show clock** 命令来显示系统时间信息

```
Ruijie# show clock          //确认修改系统时间生效
clock: 2003-6-20 10:10:54
```

配置每日通知

【配置方法】 ● 使用(#)作为分界符，每日通知的文本信息为“Notice: system will shutdown on July 6th.”

```
Ruijie(config)# banner motd #//开始分界符
Enter TEXT message.  End with the character '#'.
Notice: system will shutdown on July 6th.# //结束分界符
Ruijie(config)#
```

【检验方法】 ● 使用 **show running-config** 命令查看配置。

● 使用控制台、Telnet 或 SSH 连接本地设备，进入命令行界面之前时将显示每日通知信息。

```
C:\>telnet 192.168.65.236
Notice:  system will shutdown on July 6th.
Access for authorized users only. Please enter your password.
 User Access Verification
Password:
```

配置登录标题

【配置方法】 ● 使用(#)作为分界符，登录标题的文本为“Access for authorized users only. Please enter your password.”

```
Ruijie(config)# banner login #//开始分界符
Enter TEXT message.  End with the character '#'.
Access for authorized users only. Please enter your password.
#                                                    //结束分界符
Ruijie(config)#
```

【检验方法】 ● 使用 **show running-config** 命令查看配置。

● 使用控制台、Telnet 或 SSH 连接本地设备，进入命令行界面之前时将显示登录标题信息。

```
C:\>telnet 192.168.65.236
Notice:  system will shutdown on July 6th.
Access for authorized users only. Please enter your password.
 User Access Verification
Password:
```

如何将串口速率设置为 57600 bps

【配置方法】 ● 将串口速率设置为 57600 bps

```
Ruijie# configure terminal        //进入全局配置模式
Ruijie(config)# line console 0    //进入控制台线路配置模式
Ruijie(config-line)# speed 57600  //设置控制台速率为 57600
Ruijie(config-line)# end           //回到特权模式
```

【检验方法】

- 使用 **show** 命令查看。

```
Ruijie# show line console 0      //查看控制台配置
CON      Type     speed    Overruns
* 0      CON      57600    0
Line 0, Location: "", Type: "vt100"
Length: 25 lines, Width: 80 columns
Special Chars: Escape  Disconnect  Activation
               ^^x     none        ^M
Timeouts:      Idle EXEC    Idle Session
               never        never
History is enabled, history size is 10.
Total input: 22 bytes
Total output:  115 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times
Modem: READY
```

常见配置错误

- 无

2.4.4 打开或关闭指定的服务

配置效果

- 在系统运行过程中，可以动态地调整系统所提供的服务，打开与关闭指定的服务（SNMP Server / SSH Server / Telnet Server）。

注意事项

-

配置方法

↘ 打开 SNMP Server / SSH Server / Telnet Server

- 可选配置。在需要使用这些服务时执行此配置项。

检验方法

- 使用 **show running-config** 命令查看配置。
- 使用 **show services** 命令查看服务的开启状态。

相关命令

打开 SSH-Server/telnet-server/snmp-agent

【命令格式】 **enable service** { **ssh-server** | **telnet-server** | **snmp-agent** }

【参数说明】 **ssh-server**：打开与关闭 SSH Server，该命令同时打开 IPv4 和 IPv6 服务。

telnet-server：打开与关闭 Telnet Server，该命令同时打开 IPv4 和 IPv6 服务。

snmp-agent：打开与关闭 Snmp Agent，该命令同时打开 IPv4 和 IPv6 服务。

【命令模式】 全局模式

【使用指导】 该命令用于打开与关闭指定的服务。

配置举例

打开 SSH Server

【配置方法】

- 打开 SSH Server

```
Ruijie# configure terminal  //进入全局配置模式
Ruijie(config)#enable service ssh-server    //打开 SSH Server
```

【检验方法】

- 使用 **show running-config** 命令查看配置。
- 使用 **show ip ssh** 命令查看 SSH 服务配置和运行状况。

常见配置错误

无

2.4.5 设置重启策略

配置效果

设备在某些情况下需要重启，设置重启策略能使设备按照预设的方式进行重启。

注意事项

无

配置方法

直接重启

表示立即重启设备，用户可以在特权模式下直接键入 **reload** 命令来重启系统。

定时重启

```
reload  at  hh:mm:ss month day year
```

指定系统在将来的某个时间点重启。输入的时间值必须是将来的某个时间点。参数 month day year 是可选的,如果用户没有输入，则默认是系统时钟的年月日。

⚠ 如果用户要使用 **at** 选项，则要求当前系统必须支持时钟功能。建议使用之前先配置好系统的时钟，以便更切合您的用途。如果用户之前已经设置了重启计划，则后面再设置的计划将覆盖前面的设置。如果用户已经设置了重启计划，假如在该计划生效前用户重启了系统，则该计划将丢失。

⚠ 重启计划中的时间要大于当前系统时间。同时用户在设置了重启计划之后最好不要再修改系统时钟,否则有可能会导致设置失效，比如将系统时间调到重启时间之后。

检验方法

-

相关命令

重启设备

【命令格式】 **reload** [**at** { *hh* [:*mm* [:*ss*]] } [*month* [*day* [*year*]]]]

【参数说明】 **at** *hh:mm:ss*：设置重启的时：分：秒，省略的部分使用系统当前的设置值。

month：月份（1-12）。

day：日期，从 1 到 31。

year：公元年（1993-2035），不能使用缩写。

【命令模式】 特权用户模式

【使用指导】 使用该命令可以指定设备在指定的时刻启动，方便进行管理。

常见错误

无

2.5 监视与维护

查看运行情况

作用	命令
show clock	显示当前系统时间。

show line { **console** *line-num* | **vty** *line-num* **|** *line-num* }	查看线路的配置信息。
show reload	查看系统的重新启动设置。
show running-config [**interface** *interface*]	查看当前设备系统正在运行的配置信息或某个接口下的配置信息。
show startup-config	查看存储在 NVRAM（非易失性随机存取存储器）上设备的配置。
show this	查看系统当前模式下生效的配置信息。
show sessions	显示已经建立 Telnet Client 实例的每个实例信息。

3 LINE

3.1 概述

在网络设备上一般都具有多种类型的终端线路（line），并针对这些终端按类进行分组管理，对这些终端进行的配置称为线路（line）配置。在网络设备上，终端线路类型分为 CTY、VTY 等。

协议规范

- 无

3.2 典型应用

典型应用	场景描述
通过控制台访问设备	通过控制台进入网络设备的命令行界面。
通过 VTY 访问设备	通过 Telnet 或 SSH 进入网络设备的命令行界面。

3.2.1 通过控制台访问设备

应用场景

图 3-1

【注释】 A 为需要被管理的网络设备。
PC 为网络管理站。

功能部属

网络管理站使用串口线连接被管理的网络设备的控制台端口，用户在网络管理站上，通过控制台软件（超级终端或其他终端仿真软件）连接网络设备上的控制台并进入命令行界面，对网络设备进行配置和管理。

3.2.2 通过VTY访问设备

应用场景

图 3-2

【注释】 A 为需要被管理的网络设备。
PC 为网络管理站。

功能部属

网络管理站和被管理的网络设备通过网络连接，用户在网络管理站上，通过 VTY 客户端软件（例如 Putty），使用 Telnet 或 SSH 连接网络设备上并进入命令行界面，对网络设备进行配置和管理。

3.3 功能详解

基本概念

↘ CTY

CTY 线路类型指的是控制台端口（Console Port），大多数网络设备都会具有一个控制台端口，用户可以使用控制台终端，通过这个端口访问本地系统。

↘ VTY

VTY 线路类型是虚拟终端线路，并没有与之对应的硬件，虚拟终端线路用于 Telnet 或 SSH 连接。

功能特性

功能特性	作用
基本功能	配置终端，显示、清除终端连接信息等。

3.3.1 基本功能

工作原理

无

相关配置

↘ 清除终端连接

当用户终端已经与设备连接时，对应的终端线路就处于占用状态，此时使用 **show user** 命令可以查看这些终端线路的连接状态。如果要使用户终端断开与网络设备的连接，可以使用 **clear line** 命令指定清除一个终端。被清除的终端线路上如果有关联的通讯协议（例如 Telnet、SSH 等）将会断开，已经进入的命令行界面也会退出。清除后的终端线路将恢复为非占用的状态，用户可以重新建立起连接。

↘ 设置 VTY 终端数目

使用 **line vty** 命令不仅可以进入 VTY 线路配置模式，还可以指定 VTY 终端的数目。

默认的 VTY 终端数目为 5 个，编号为 0~5。可以将终端数目最多扩展到 36 个，扩展的编号为 5~35。扩展的终端可以被删除，但默认的终端不可删除。

3.4 配置详解

配置项	配置建议 & 相关命令	
进入line模式	⚠ 必选配置。用于进入 line 模式。	
	line [**console** | **vty**] *first-line* [*last-line*]	进入到指定的 LINE 模式
	line vty *line-number*	增加或减少当前可以使用的 VTY 连接数目

3.4.1 进入line模式

配置效果

进入 line 模式进行其他功能项的配置。

注意事项

无

配置方法

进入 LINE 模式

- 必选配置。
- 若无特殊情况，应在每台设备上进入 line 模式进行功能配置。

增加/减少 LINE VTY 数目

- 可选配置。
- 在需要增加或减少 LINE 线路时应使用此配置项。

检验方法

使用 **show line** 命令查看线路的配置信息。

相关命令

进入 LINE 模式

【命令格式】 **line** [**console** | **vty**] *first-line* [*last-line*]

【参数说明】 **console**：控制台口。

vty：虚终端线路，适用于 Telnet 或 SSH 连接。

first-line：要进入的 *first-line* 编号。

last-line：要进入的 *last-line* 编号。

【命令模式】 全局配置模式

【使用指导】 -

增加/减少 LINE VTY 数目

【命令格式】 **line vty** *line-number*

【参数说明】 *line-number*：VTY 连接数目，范围：0~35。

【命令模式】 全局配置模式

【使用指导】 使用 **no line vty** *line-number* 命令减少当前可以使用的 VTY 连接数目。

查看线路配置信息

【命令格式】 **show line** { **console** *line-num* | **vty** *line-num* **|** *line-num* }

【参数说明】 **console**：控制台口。

vty：虚终端线路，适用于 Telnet 或 SSH 连接。

line-num：查看的 line 线路。

【命令模式】 特权配置模式

【使用指导】 -

配置举例

【网络环境】

图 3-3

【配置方法】

- PC 使用控制台线连接网络设备 A，通过控制台终端进入命令行界面。
- 执行 **show user** 查看终端线路连接状态。
- 执行 **show line console** 0 查看控制台线路状态。
- 进入全局配置模式，使用 **line vty** 命令将 VTY 终端数目扩展至 36 个。

A

```
Ruijie#show user
Line             User         Host(s)              Idle       Location
---------------- ------------ -------------------- ---------- ------------------
*  0 con 0       ---          idle                 00:00:00   ---

Ruijie#show line console 0

CON     Type    speed   Overruns
* 0     CON     9600    0
Line 0, Location: "", Type: "vt100"
Length: 24 lines, Width: 79 columns
Special Chars: Escape  Disconnect  Activation
               ^^x     ^D          ^M
Timeouts:      Idle EXEC    Idle Session
               00:10:00     never
History is enabled, history size is 10.
Total input: 490 bytes
Total output:  59366 bytes
Data overflow:  0 bytes
stop rx interrupt:  0 times

Ruijie#show line vty ?
  <0-5>    Line number

Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#line vty 35
```

```
Ruijie(config-line)#
*Oct 31 18:56:43: %SYS-5-CONFIG_I: Configured from console by console
```

【检验方法】

- 输入 **show line** 命令，获取帮助时可以发现终端数量已经被扩展。
- 执行 **show running-config** 命令查看配置。

A

```
Ruijie#show line vty ?
  <0-35>  Line number

Ruijie#show running-config

Building configuration...
Current configuration : 761 bytes

version 11.0(1C2B1)(10/16/13 04:23:54 CST -ngcf78)
ip tcp not-send-rst
vlan 1
!
interface GigabitEthernet 0/0
!
interface GigabitEthernet 0/1
 ip address 192.168.23.164 255.255.255.0
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
interface GigabitEthernet 0/4
!
interface GigabitEthernet 0/5
!
interface GigabitEthernet 0/6
!
interface GigabitEthernet 0/7
!
interface Mgmt 0
!
line con 0
line vty 0 35
 login
!
```

```
end
```

常见错误

无

3.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除线路的连接状态。	**clear line** { **aux** *line-num* | **console** *line-num* | **tty** *line-num* | **vty** *line-num* **|** *line-num* }

查看运行情况

作用	命令
查看线路的配置信息。	**show line** { **aux** *line-num* | **console** *line-num* | **tty** *line-num* | **vty** *line-num* **|** *line-num* }
显示当前 line 线路的历史记录命令	**show history**
显示当前 line 线路权限级别	**show privilege**
显示线路登录用户信息	**show user** [**all**]

4 SNMP

4.1 概述

SNMP 是 Simple Network Management Protocol（简单网络管理协议）的缩写，在 1988 年 8 月就成为一个网络管理标准 RFC1157。到目前，因众多厂家对该协议的支持，SNMP 已成为事实上的网管标准，适合于在多厂家系统的互连环境中使用。利用 SNMP 协议，网络管理员可以对网络上的节点进行信息查询、网络配置、故障定位、容量规划，网络监控和管理是 SNMP 的基本功能。

↘ SNMP 协议版本

目前 SNMP 支持以下版本：

- SNMPv1 ：简单网络管理协议的第一个正式版本，在 RFC1157 中定义。
- SNMPv2C：基于共同体（Community-Based）的 SNMPv2 管理架构，在 RFC1901 中定义。
- SNMPv3 ：通过对数据进行鉴别和加密，提供了以下的安全特性：

6. 确保数据在传输过程中不被篡改；
7. 确保数据从合法的数据源发出；
8. 加密报文，确保数据的机密性。

协议规范

- RFC 1157，Simple Network Management Protocol (SNMP)
- RFC 1901，Introduction to Community-based SNMPv2
- RFC 2578，Structure of Management Information Version 2 (SMIv2)
- RFC 2579，Textual Conventions for SMIv2
- RFC 3411，An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412，Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413，Simple Network Management Protocol (SNMP) Applications
- RFC 3414，User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3415，View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3416，Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417，Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418，Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 3419，Textual Conventions for Transport Addresses

4.2 典型应用

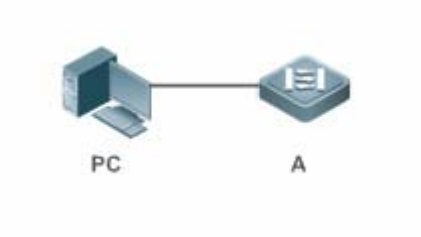
典型应用	场景描述
通过SNMP管理网络设备	通过 SNMP 网络管理器对网络设备进行管理和监控。

4.2.1 通过SNMP管理网络设备

应用场景

以下图为例，用户通过 SNMP 网络管理器，来对网络设备 A 进行管理和监控。

图 4-1



【注释】 A 为需要被管理的网络设备。
PC 为网络管理站。

功能部属

网络管理站和被管理的网络设备通过网络连接，用户在网络管理站上，通过 SNMP 网络管理器，访问网络设备上的管理信息数据库，以及接收来自网络设备主动发出的消息，来对网络设备进行管理和监控。

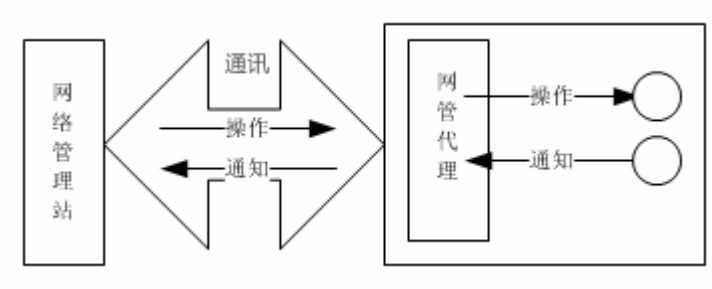
4.3 功能详解

基本概念

SNMP 是一个应用层协议，为客户机/服务器模式，包括三个部分：

- SNMP 网络管理器
- SNMP 代理
- MIB 管理信息库

图 4-2 网络管理站（NMS）与网管代理（Agent）的关系图



SNMP 网络管理器

SNMP 网络管理器，是采用 SNMP 来对网络进行控制和监控的系统，也称为 NMS (Network Management System)。

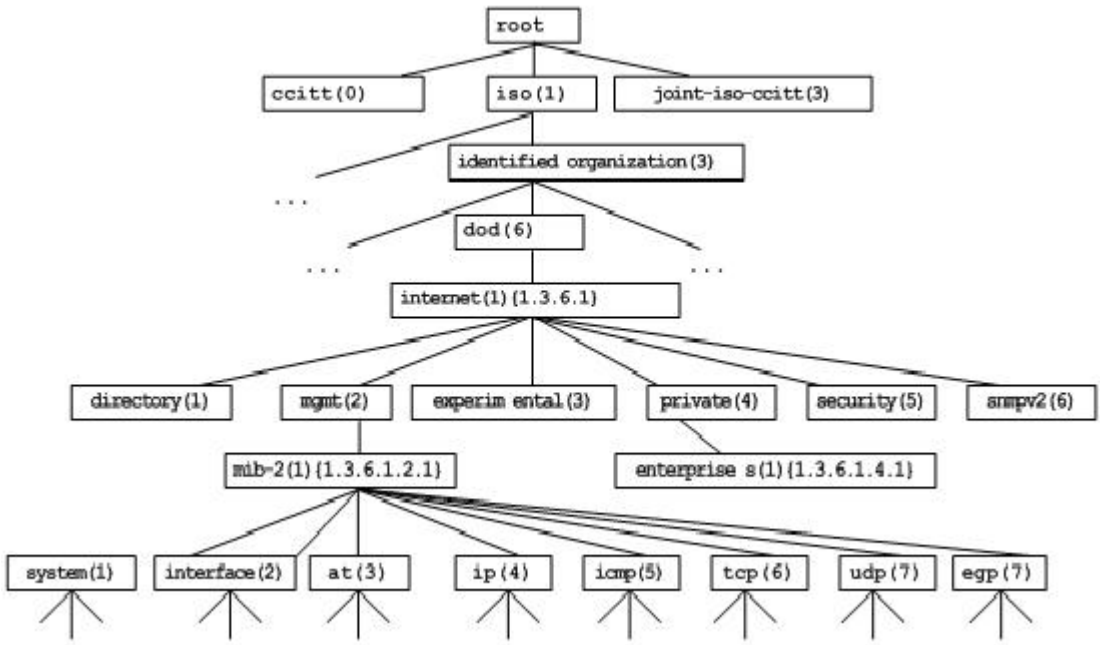
SNMP 代理

SNMP 代理（SNMP Agent，下文简称为 Agent）是运行在被管理设备上的软件，负责接受、处理并且响应来自 NMS 的监控和控制报文，也可以主动发送一些消息报文给 NMS。

MIB

MIB（Management Information Base）是一个虚拟的网络管理信息库。被管理的网络设备中包含大量信息，为了能在 SNMP 报文中唯一的标识某个特定的管理单元，MIB 采用树形层次结构来描述，树的节点表示某个特定的管理单元。为了唯一标识网络设备中的某个管理单元 System，可以采用一串的数字来表示，MIB 则是网络设备的单元标识符的集合。

图 4-3 MIB 树形层次结构



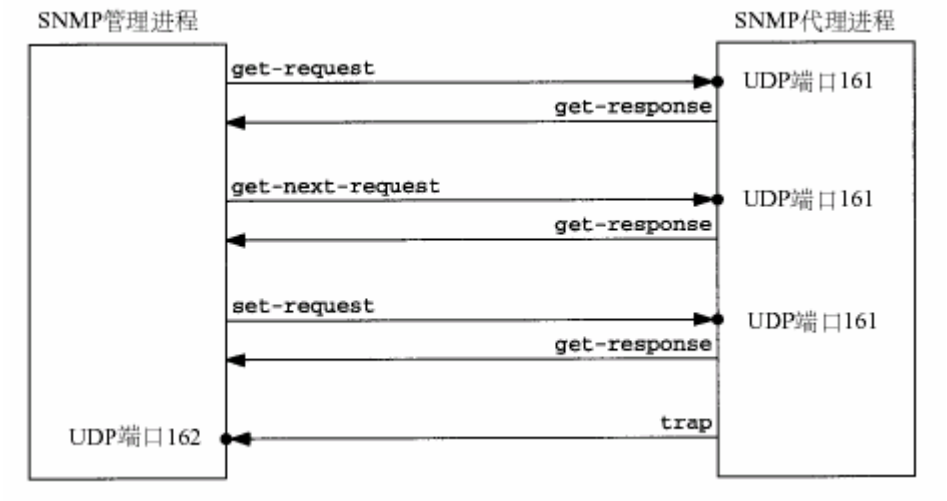
操作类型

SNMP 协议中的 NMS 和 Agent 之间的交互信息，定义了 6 种操作类型：

- Get-request 操作：NMS 从 Agent 提取一个或多个参数值。
- Get-next-request 操作：NMS 从 Agent 提取一个或多个参数的下一个参数值。
- Get-bulk 操作：NMS 从 Agent 提取批量的参数值；
- Set-request 操作：NMS 设置 Agent 的一个或多个参数值。
- Get-response 操作：Agent 返回的一个或多个参数值，是 Agent 对 NMS 前面 3 个操作的响应操作。
- Trap 操作：Agent 主动发出的报文，通知 NMS 有某些事情发生。

前面的 4 个报文是由 NMS 向 Agent 发出的，后面两个是 Agent 发给 NMS 的(注意：SNMPv1 版本不支持 Get-bulk 操作)。下图描述了这几种操作。

图 4-4 SNMP 的报文类型



NMS 向 Agent 发出的前面 3 种操作和 Agent 的应答操作采用 UDP 的 161 端口。Agent 发出的 Trap 操作采用 UDP 的 162 端口。

功能特性

功能特性	作用
SNMP基本功能	配置网络设备上的 SNMP 代理，实现对网络上的节点进行信息查询、网络配置、故障定位、容量规划等基本功能。
SNMPv1 及SNMPv2C	采用基于共同体的安全架构，包括认证名和访问权限。
SNMPv3	SNMPv3 重新定义了 SNMP 架构 ,主要是在安全功能上进行了增强 ,包括支持基于用户的安全模型，以及支持基于视图的访问控制模型等。SNMPv3 架构内已经包含了 SNMPv1 和 SNMPv2C 所有的功能。

4.3.1 SNMP基本功能

工作原理

工作过程

SNMP协议交互是应答式的（报文交互参见 图 4-4 SNMP的报文类型）。NSM向Agent主动发起请求，包括Get-request、Get-next-request、Get-bulk和Set-request，Agent接收请求并完成操作后以Get-response作为应答。Agent有时候也会向NSM主动发出Trap和Inform消息，其中Trap消息不需要应答，而Inform消息则需要NSM回送一个Inform-response应答，表示收到消息，否则Agent将会重发Inform消息。

相关配置

屏蔽或关闭 SNMP 代理

缺省时启动 SNMP 功能。

使用 **no snmp-server** 命令屏蔽 SNMP 代理功能。

执行 **no enable service snmp-agent** 命令，直接关闭 SNMP 所有服务。

设置 SNMP 基本参数

缺省时系统联系方式、系统位置和设备的网元信息为空；序列号缺省值是 60FF60；缺省最大数据报文长度 1572 字节；缺省的 SNMP 服务 UDP 端口号是 161。

使用 **snmp-server contact** 命令配置或删除系统联系方式。

使用 **snmp-server location** 命令配置或删除系统位置。

使用 **snmp-server chassis-id** 命令配置系统序列码或恢复缺省值。

使用 **snmp-server packetsize** 命令配置代理最大数据报文长度或恢复缺省值。

使用 **snmp-server net-id** 命令配置或删除设备的网元信息。

使用 **snmp-server udp-port** 命令设置 SNMP 服务 UDP 端口号或恢复缺省值。

配置 SNMP 主机地址

缺省情况下，没有 SNMP 主机。

使用 **snmp-server host** 命令配置 Agent 主动发送消息的 NMS 主机地址或删除指定 SNMP 主机地址。发给主机的消息可以绑定 SNMP 的版本、接收端口、认证名或用户。该命令与 **snmp-server enable traps** 命令一起使用，主动给 NMS 发送 Trap 消息。

设置 Trap 消息参数

缺省情况下，禁止 SNMP 向 NMS 主动发送 Trap 消息；打开接口发送 Link Trap 功能；关闭发送系统重启 Trap 功能；Trap 消息缺省不带私有字段。

缺省时，SNMP 报文从哪个接口出去，就使用哪个接口的 IP 地址作为源地址。

缺省时 Trap 消息报文的队列长度为 10，发送 Trap 消息的时间间隔为 30 秒。

使用 **snmp-server enable traps** 命令配置 Agent 主动或禁止向 NMS 发送 Trap 消息。

使用 **snmp trap link-status** 命令打开或关闭接口发送 Link Trap 功能。

使用 **snmp-server trap-source** 命令指定发送消息的源地址或恢复缺省值。

使用 **snmp-server queue-length** 命令设置 Trap 消息报文的队列长度或恢复缺省值。

使用 **snmp-server trap-timeout** 命令设置发送 Trap 消息的时间间隔或恢复缺省值。

使用 **snmp-server trap-format private** 命令设置或关闭发送 Trap 消息时携带私有字段的功能。

使用 **snmp-server system-shutdown** 命令打开或关闭发送系统重启 Trap 功能。

↘ 设置 SNMP 攻击防护检测功能

缺省情况下，没有打开 SNMP 攻击防护检测功能。

使用 **snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }命令设置打开攻击防护检测功能。

4.3.2 SNMPv1 及SNMPv2C

SNMPv1 和 SNMPv2C 都采用基于共同体(Community-based)的安全架构。通过定义主机地址以及认证名(Community String)来限定能够对代理的 MIB 进行操作的管理者。

工作原理

SNMPv1 和 SNMPv2 版本使用认证名来鉴别是否有权使用 MIB 对象。为了能够管理设备，网络管理系统 (NMS)的认证名必须同设备中定义的某个认证名一致。

SNMPv2C 增加了 Get-bulk 操作机制并且能够对管理工作站返回更加详细的错误信息类型。Get-bulk 操作能够一次性地获取表格中的所有信息或者获取大批量的数据，从而减少请求-响应的次数。SNMPv2C 错误处理能力的提高包括扩充错误代码以区分不同类型的错误，而在 SNMPv1 中这些错误仅有一种错误代码。现在通过错误代码可以区分错误类型。由于网络上可能同时存在支持 SNMPv1 和 SNMPv2C 的管理工作站，因此 SNMP 代理必须能够识别 SNMPv1 和 SNMPv2C 报文，并且能返回相应版本的报文。

↘ 安全

一个认证名有以下属性：

- 只读(Read-only)：为被授权的管理工作站提供对所有 MIB 变量的读权限。
- 读写(Read-write)：为被授权的管理工作站提供对所有 MIB 变量的读写权限。

相关配置

↘ 设置认证名及访问权限

所有认证名的缺省访问权限为只读。

使用 **snmp-server community** 命令配置或删除认证名和访问权限。

该命令为启用设备 SNMP 代理功能的第一个重要命令，指定了团体的属性、允许访问 MIB 的 NMS 范围等等。

4.3.3 SNMPv3

SNMPv3 重新定义了 SNMP 架构，将之前的 SNMPv1 和 SNMPv2 的功能也纳入到 SNMPv3 体系中。

工作原理

网络管理系统（NMS）和 SNMP 代理（SNMP Agent）都称为 SNMP 实体。在 SNMPv3 架构中，SNMP 实体分为引擎和应用两大部分，其中 SNMP 引擎用于发送和接收信息、鉴定和加密信息以及对管理对象的控制访问。SNMP 应用指的是 SNMP 内部的应用程序，利用 SNMP 引擎提供的服务进行工作。

SNMPv3 版本使用基于用户的安全模型（USM）来鉴别是否有权使用 MIB 对象。为了能够管理设备，网络管理系统（NMS）的用户和安全级别必须同设备中定义的某个 SNMP 用户一致。

SNMPv3 版本规定 NSM 在管理设备的时候，必须先得知设备上 SNMP Agent 的引擎标识。SNMPv3 定义了 Discover 和 Report 操作机制，NSM 在不知道 Agent 引擎标识的情况下，可以先向 Agent 发送 Discover 报文，而 Agent 以 Report 响应，并在响应报文中携带了引擎标识信息。此后，NSM 和 Agent 之间的管理操作必须携带该引擎标识。

↘ 安全

- SNMPv3 通过安全模型以及安全级别来确定对数据采用哪种安全机制进行处理。目前可用的安全模型有三种类别：SNMPv1、SNMPv2C、SNMPv3。SNMPv3 将 SNMPv1 和 SNMPv2C 也纳入到安全模型中。

SNMPv1 及 SNMPv2C 安全模型和级别

安全模型	安全级别	鉴别	加密	说明
SNMPv1	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性
SNMPv2c	noAuthNoPriv	认证名	无	通过认证名确认数据的合法性

SNMPv3 安全模型以及安全级别

安全模型	安全级别	鉴别	加密	说明
SNMPv3	noAuthNoPriv	用户名	无	通过用户名确认数据的合法性
SNMPv3	authNoPriv	MD5 或者 SHA	无	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制
SNMPv3	authPriv	MD5 或者 SHA	DES	提供基于 HMAC-MD5 或者 HMAC-SHA 的数据鉴别机制提供基于 CBC-DES 的数据加密机制

↘ 引擎标识

引擎标识用于唯一标识一个 SNMP 引擎。由于每个 SNMP 实体仅包含一个 SNMP 引擎，它将在一个管理域中唯一标识一个 SNMP 实体。因此，作为一个实体的 SNMPv3 代理必须拥有一个唯一的引擎标识，即 SnmpEngineID。

引擎标识为一个 OCTET STRING，长度为 5～32 字节长。在 RFC3411 中定义了引擎标识的格式：

- 前 4 个字节标识厂商的私有企业号（由 IANA 分配），用 HEX 表示。
- 第 5 个字节表示剩下的字节如何标识：
- 0：保留
- 1：后面 4 个字节是一个 Ipv4 地址。
- 2：后面 16 个字节是一个 Ipv6 地址。
- 3：后面 6 个字节是一个 MAC 地址。
- 4：文本，最长 27 个字节，由厂商自行定义。
- 5：16 进制值，最长 27 个字节，由厂商自行定义。
- 6-127：保留。
- 128-255：由厂商特定的格式。

相关配置

↘ 配置 MIB 视图和组

缺省配置一个 default 视图，允许访问所有的 MIB 对象。

缺省没有配置用户组。

使用 **snmp-server view** 命令配置或删除视图；使用 **snmp-server group** 命令配置或删除用户组。

可以配置一条或者多条指令，来指定多个不同的共同体名称，使得网络设备可以供不同的权限的 NMS 的管理。

↘ 配置 SNMP 用户

缺省没有配置用户。

配置 **snmp-server user** 命令配置或删除用户。

NMS 只有使用合法的用户才能同代理进行通信。

对于 SNMPv3 用户，可以指定安全级别(是否需要进行认证、是否需要进行加密等)、认证算法(MD5 或 SHA)、认证口令、加密算法（目前只有 DES）和加密口令。

4.3.4 SNMP MIB缓存功能

在多台设备虚拟化成一台，统一管理模式下，NMS 获取相关的 MIB 变量时，需要通过主机往从机/备机进行 MIB 变量的收集，在设备台数比较多的情况下，整个收集过程消耗的时间比较长，增加了 NMS 获取 MIB 数据的延时。

工作原理

为了减少整个操作过程的延时，可以启用 SNMP MIB 缓存功能，由主机提前收集从/备机的 MIB 变量的数据，并缓存在主机上面，NMS 在读取 MIB 变量值时，直接对缓存数据进行读取，避免访问从//备机的时间消耗。

相关配置

↘ 配置 SNMP MIB 缓存功能

缺省没有开启 SNMP MIB 缓存功能。

使用 **snmp-server cache enable** 命令配置 SNMP MIB 缓存功能。

↘ 配置 SNMP MIB 缓存更新时间

缺省缓存更新时间为 300 秒。

使用 **snmp-server cache update-timer** *seconds* 命令配置 SNMP MIB 缓存更新时间。

↘ 配置指定 OID 节点启用缓存功能和缓存更新时间

缺省未启用 MIB 节点缓存功能，默认缓存更新时间为全局配置的缓存更新时间。

使用 **snmp-server cache oid** *oid-string* **[update-timer** *seconds***]**命令配置指定 OID 节点启用缓存功能，以及指定的 OID 节点缓存更新时间。

4.4 配置详解

配置项	配置建议 & 相关命令	
配置SNMP基本功能	⚠ 必须配置。使用户可以通过 NMS 访问 Agent。	
	enable service snmp-agent	启动 Agent 功能。
	snmp-server community	配置认证名和访问权限。
	snmp-server user	配置 SNMP 用户信息。
	snmp-server view	配置 SNMP 视图。
	snmp-server group	配置 SNMP 用户组。
	snmp-server authentication	配置 SNMP 攻击防护检测功能
启用Trap功能	⚠ 可选配置。使 Agent 主动向 NMS 发送 Trap 消息。	
	snmp-server host	配置 NMS 主机地址。
	snmp-server enable traps	Agent 主动向 NMS 发送 Trap 消息。
	snmp trap link-status	打开接口发送 Link Trap 功能。
	snmp-server system-shutdown	打开发送系统重启 Trap 功能。
	snmp-server trap-source	指定发送 Trap 消息的源地址。
	snmp-server trap-format private	发送 Trap 消息时携带私有字段
屏蔽Agent功能	⚠ 可选配置。在不需要 Agent 服务的时候，屏蔽 Agent 功能。	
	no snmp-server	屏蔽 Agent 功能。

设置SNMP控制参数	⚠ 可选配置。用于设置或修改 SNMP 控制参数。	
	snmp-server contact	设置设备的联系方式。
	snmp-server location	设置设备位置。
	snmp-server chassis-id	设置设备序列码。
	snmp-server net-id	设置设备的网元信息。
	snmp-server packetsize	修改最大数据报文长度。
	snmp-server udp-port	修改 SNMP 服务 UDP 端口号。
	snmp-server queue-length	修改 Trap 消息报文的队列长度。
	snmp-server trap-timeout	修改发送 Trap 消息的时间间隔。
配置 SNMP MIB 缓存功能	⚠ 可选配置。用于设置或修改 SNMP MIB 缓存功能。	
	snmp-server cache enable	配置全局 SNMP MIB 缓存功能。
	snmp-server cache update-timer	配置 SNMP MIB 全局缓存更新时间。
	snmp-server cache oid	配置指定 OID 节点启用缓存功能和缓存更新时间。

4.4.1 配置SNMP基本功能

配置效果

使用户可以通过 NMS 访问 Agent。

注意事项

- 网络设备上默认没有设置认证名，无法使用 SNMPv1 或 SNMPv2C 访问网络设备的 MIB。设置认证名时，如果没有指定访问权限，则默认的访问权限是只读（Read-only）。

配置方法

↘ 配置 SNMP 视图

- 可选配置。
- 使用基于视图的访问控制（VACM）功能时需要进行配置。

↘ 配置 SNMP 用户组

- 可选配置。
- 使用基于视图的访问控制（VACM）功能时需要进行配置。

↘ 配置认证名和访问权限

- 必选配置。
- 使用 SNMPv1 和 SNMPv2C 管理网络设备必须在 agent 设备上设置认证名。

配置 SNMP 用户信息

- 必选配置。
- 使用 SNMPv3 管理网络设备必须设置用户。

启动 Agent 功能

- 可选配置。
- 默认开启 Agent 功能，在 Agent 功能关闭后需要再次开启时，须使用此命令。

打开 SNMP 攻击防护检测功能

- 可选配置。
- 默认关闭 SNMP 攻击防护检测功能，在需要防止恶意攻击时，在 agent 上使用该配置项。

检验方法

使用 **show snmp** 命令查看设备上的 snmp 功能。

相关命令

配置 SNMP 视图

【命令格式】 **snmp-server view** *view-name oid-tree* { **include** | **exclude** }

【参数说明】 *view-name*：视图名。

oid-tree：视图关联的 MIB 对象，是一棵 MIB 子树。

include：标明该 MIB 对象子树被包含在视图之内。

exclude：标明该 MIB 对象子树被排除在视图之外。

【命令模式】 全局配置模式

【使用指导】 指定视图的名称，用于基于视图的管理。

配置 SNMP 用户组

【命令格式】 **snmp-server group** *groupname* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** } } [**read** *readview*] [**write** *writeview*] [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname* }]

【参数说明】 **v1** | **v2c** |**v3：**指明 SNMP 版本。

auth：该组的用户传输的消息需要验证但数据不需要保密，只对 v3 有效。

noauth：该组用户传输的消息不需要验证数据也不需要保密，只对 v3 有效。

priv：该组用户传输的消息需要验证同时传输的数据需要保密，只对 v3 有效。

readview：关联一个只读的视图。

writeview：关联一个读写视图。

aclnum：访问列表序列号，关联指定的访问列表，指定能访问 MIB 的 ipv4 NMS 地址范围。

aclname：访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv4 NMS 地址范围。

ipv6-aclname：ipv6 访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv6 NMS 地址范围。

【命令模式】 全局配置模式

【使用指导】 将某些用户和一个组关联，再将某个组与某个视图关联。一个组内的用户具有相同的访问权限。通过这种方式判定操作关联的管理对象是否在视图允许之内，只有在视图允许之内的管理对象才被允许访问。

配置认证名和访问权限

【命令格式】 **snmp-server community** [*0* | *7*] *string* [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*]] [**ipv6** *ipv6-aclname*] [*aclnum* | *aclname*]

【参数说明】 *0*：表示输入的团体字符串为明文字符串。

7：表示输入的团体字符串为密文字符串。

string：团体字符串，相当于 NMS 和 SNMP 代理之间的通信密码。

view-name：指定视图的名称，用于基于视图的管理。

ro：指定 NMS 对 MIB 的变量只能读，不能修改。

rw：NMS 对 MIB 的变量可读可写。

aclnum：访问列表序列号，关联指定的访问列表，指定能访问 MIB 的 ipv4 NMS 地址范围。

aclname：访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv4 NMS 地址范围。

ipv6-aclname：ipv6 访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv6 NMS 地址范围。

ipaddr：关联 NMS 地址，指定访问 MIB 的 NMS 地址。

【命令模式】 全局配置模式

【使用指导】 该命令为启用设备 SNMP 代理功能的第一个重要命令，指定了团体的属性、允许访问 MIB 的 NMS 范围等等。要关闭 SNMP 代理功能，执行 **no snmp-server** 命令即可。

配置 SNMP 用户

【命令格式】 **snmp-server user** *username groupname* { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** { **ipv6** *ipv6-aclname* | *aclnum* | *aclname* }]

【参数说明】 *username*：用户名。

groupname：该用户对应的组名。

v1 | **v2c** | **v3：**指明 SNMP 版本。只有 v3 支持后面的安全参数。

encrypted：指定的是密码输入的方式为密文输入。否则，以明文输入。如果选择了以密文输入，则需要输入连续的 16 进制数字字符表示的密钥。注意使用 MD5 的认证密钥长度为 16 字节，而 SHA 认证协议密钥长度为 20 字节。以两个字符表示一个字节。加密表示的密钥仅对本引擎有效。

auth：指定是否使用验证。

md5：指定使用 MD5 认证协议。**sha** 指定使用 SHA 认证协议。

auth-password：配置认证协议使用的口令字符串（不超过 32 个字符）。系统将这些口令转换成相应的认证密钥。

priv：指定是否使用保密。**des56** 指明使用 56 位的 DES 加密协议。

priv-password：为加密用的口令字符串（不超过 32 个字符）。系统将这个口令转换成相应的加密密钥。

aclnum：访问列表序列号，关联指定的访问列表，指定能访问 MIB 的 ipv4 NMS 地址范围。

aclname：访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv4 NMS 地址范围。

ipv6-aclname：ipv6 访问列表名称，关联指定的访问列表，指定能访问 MIB 的 ipv6 NMS 地址范围。

【命令模式】 全局配置模式

【使用指导】 配置用户的信息，以使 NMS 使用合法的用户同代理进行通信。

对于 SNMPv3 用户，可以指定安全级别、认证算法（MD5 或 SHA）、认证口令、加密算法（目前只有 DES）和加密口令。

启动 Agent 功能

【命令格式】 **enable service snmp-agent**

【参数说明】

【配置模式】 特权用户模式

【使用指导】 该命令用于启动设备的 SNMP 代理功能。

启动 SNMP 攻击防护检测功能

【命令格式】 **snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }

【参数说明】 *times*：连续认证失败的尝试次数。

lock：连续认证失败后，永久禁止该源 IP 地址重新进行认证访问，需要管理员手工解除。

lock-time *minutes*：连续认证失败后，禁止该源 IP 地址一段时间，超过限定时间后可以重新进行论证访问。

unlock：连续认证失败后，允许该源 IP 地址继续进行访问，相关于没有配置 SNMP 的攻击防护检测功能。

【命令模式】 全局配置模式

【使用指导】 配置 SNMP 攻击防护检测功能，以使在连续认证失败后做出对应的处理策略。

对于被永久禁止的源 IP 地址，只有管理员进行手动解除后，该源 IP 地址才能重新访问认证。

对于被禁止一段时间内认证的源 IP 地址，当设置的禁止时间超时或者管理员手工解除后该源 IP 地址才能重新访问认证。

显示 SNMP 的状态信息

【命令格式】 **show snmp** [**mib** | **user** | **view** | **group| host | locked-ip | process-mib-time**]

【参数说明】 **mib**：显示系统中支持的 snmp mib 信息。

user：显示 snmp 用户信息。

view：显示 snmp 视图信息。

group：显示 snmp 用户组信息。

host：显示用户配置的显示信息。

locked-ip：snmp 连续认证失败后被锁定的源 IP 地址信息。

process-mib-time：显示处理时间最长的 mib 节点。

【配置模式】 特权用户模式

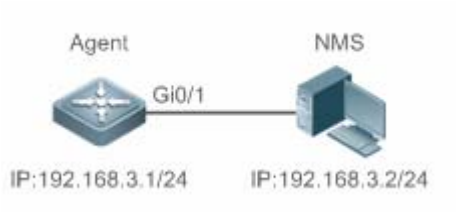
【使用指导】 -

配置举例

SNMPv3 配置举例

【网络环境】

图 4-5



- 网络工作站(NMS)基于用户的认证加密模式对网络设备(Agent)进行管理。例如 :使用用户名“user1”，认证方式为 MD5，认证密码为 123，加密算法为 DES56，加密密码为 321。
- 网络设备能够控制用户访问 MIB 对象的操作权限。例如：用户“user1”可以对 System（1.3.6.1.2.1.1）节点下的 MIB 对象进行读操作，其中只能对 SysContact（1.3.6.1.2.1.1.4.0）节点下的 MIB 对象进行写操作。
- 网络设备能够主动向网管工作站发送验证加密的消息。

【配置方法】

- 第一步，配置 MIB 视图和组。创建一个 MIB 视图 “view1”，包含关联的 MIB 对象（1.3.6.1.2.1.1）；再创建一个 MIB 视图“view2”，包含关联的 MIB 对象（1.3.6.1.2.1.1.4.0）。创建一个组“g1”，选择版本号为“v3”，配置安全级别为认证加密模式“priv”，并可读视图“view1”，可写视图“view2”。
- 第二步，配置 SNMP 用户。创建用户名“user1”，属于组“g1”，选择版本号为“v3”，配置认证方式为“md5”，认证密码为“123”，加密方式为“DES56”，加密密码为“321”。
- 第三步，配置 SNMP 主机地址。配置主机地址为 192.168.3.2，选择版本号为“3”，配置安全级别为认证加密模式“priv”，关联对应的用户名“user1”。使能 Agent 主动向 NMS 发送 Trap 消息。
- 第四步，配置 Agent 的 IP 地址。配置 Gi0/1 的接口地址为 192.168.3.1/24。

Agent

```
Ruijie(config)#snmp-server view view1 1.3.6.1.2.1.1 include
Ruijie(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include
Ruijie(config)#snmp-server group g1 v3 priv read view1 write view2
Ruijie(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321
Ruijie(config)#snmp-server host 192.168.3.2 traps version 3 priv user1
Ruijie(config)#snmp-server enable traps
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

【检验方法】

- 第一步，通过 **show running-config** 命令查看设备的配置信息。
- 第二步，通过 **show snmp user** 命令查看 SNMP 用户。
- 第三步，通过 **show snmp view** 命令查看 SNMP 视图。
- 第四步，通过 **show snmp group** 命令查看 SNMP 组。
- 第五步，通过 **show snmp host** 命令查看用户配置的主机信息。
- 第六步，安装 MIB-Browser 查询。

Agent

```
Ruijie# show running-config
!
interface gigabitEthernet 0/1
```

```
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
!
snmp-server view view1 1.3.6.1.2.1.1 include
snmp-server view view2 1.3.6.1.2.1.1.4.0 include
snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56
D5CEC4884360373ABBF30AB170E42D03
snmp-server group g1 v3 priv read view1 write view2
snmp-server host 192.168.3.2 traps version 3 priv user1
snmp-server enable traps
```

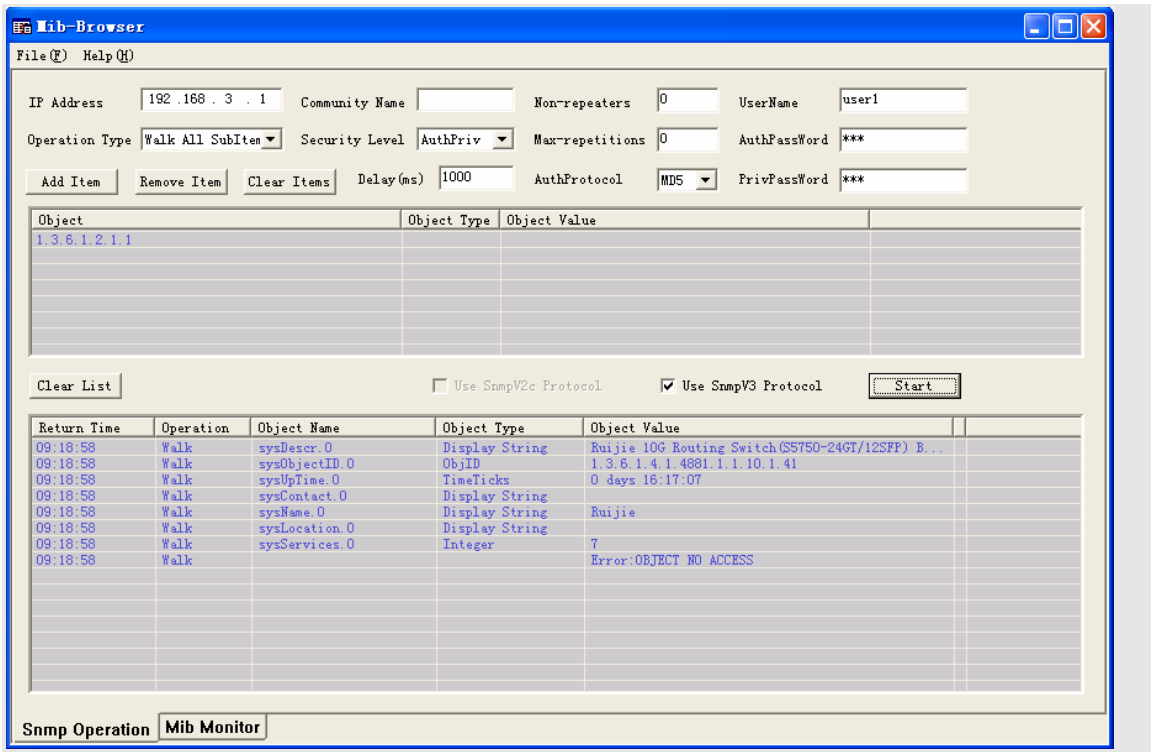
```
Ruijie# show snmp user
User name: user1
Engine ID: 800013110300d0f8221120
storage-type: permanent     active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

```
Ruijie#show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

```
Ruijie# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
readview: view1
writeview: view2
notifyview:
```

```
Ruijie#show snmp host
Notification host: 192.168.3.2
udp-port: 162
type: trap
user: user1
security model: v3 authPriv
```

安装 MIB-Browser ,在 IP Address 中输入设备的 IP 地址 :192.168.3.1 ,在 UserName 中输入“user1” ,在 Security Level 中选择 “AuthPriv”,在 AuthPassWord 中输入 “123”,在 AuthProtocol 中选择 “MD5”,在 PrivPassWord 中输入 “321”。点击 add item 按钮，选择要查询的 MIB 的具体管理单元，比如下图的 System。点击 Start 按钮，便开始对网络设备进行 MIB 的查询了，具体的查询结果见对话框的最下面的窗口：



常见错误

-

4.4.2 启用Trap功能

配置效果

使 Agent 主动向 NMS 发送 Trap 消息。

注意事项

-

配置方法

↘ 配置 snmp 主机地址

- 可选配置。
- 需要 Agent 主动发送消息时需要配置 NWS 的主机地址。

↘ Agent 主动向 NMS 发送 Trap 消息

- 可选配置。
- 当需要 agent 主动向 NMS 发送 Trap 消息时，需在 agent 上配置此项。

打开接口发送 Link Trap 功能

- 可选配置。
- 当需要接口发送 link trap 功能时，需在 agent 上配置接口打开此项。

打开发送系统重启 Trap 功能

- 可选配置。
- 当希望 RGOS 系统在设备 **reload/reboot** 以前给 NMS 发送 Trap 消息通知系统重启时，需在 agent 上配置此项。

指定发送 Trap 消息的源地址

- 可选配置。
- 当希望固定使用一个本地 IP 地址作为 SNMP 的源地址以便于管理时，需在 agent 上配置此项。

发送 Trap 消息时携带私有字段

- 可选配置。
- 当需要 Trap 消息携带私有字段时，需在 agent 上配置此项。

检验方法

通过 **show snmp** 命令显示 SNMP 的状态信息。

通过 **show running-config** 命令查看设备的配置信息。

相关命令

配置 NMS 主机地址

【命令格式】 **snmp-server host** { *host-addr* | **ipv6** *ipv6-addr* } [**traps | inrorms**] [**version** { **1** | **2c** | **3** { **auth** | **noauth** | **priv** }] *community-string* [**udp-port** *port-num*] [*notification-type*]

【参数说明】 *host-addr*：SNMP 主机地址。

ipv6-addr：SNMP 主机地址（ipv6 ）。

traps | informs：配置主机发送 trap 报文还是 inform 报文。

Version：选择 snmp 版本，V1、V2C、V3。

auth | **noauth** | **priv：**配置 V3 用户的安全级别。

community-string：团体字符串或用户名（V3 版本 ）。

port-num：配置 snmp 主机端口。

notification-type：主动发送的 Trap 类型，例如 snmp。

如果没有指定 Trap 类型，则包括所有 Trap 类型。

【命令模式】 全局配置模式

【使用指导】 该命令与全局配置命令 **snmp-server enable traps** 一起使用，主动给 NMS 发送 Trap 消息。

可以配置多个不同的 SNMP 主机用于接收 Trap 消息，一个主机可以使用不同 Trap 类型组合，不同的端口，对于相同主机，最后的一次配置会和前面的配置合并，即如要给相同主机发送不同 Trap 消息，可以分别配置不同 Trap 类型，最终这些配置会合并到一起。

配置 Agent 主动向 NMS 发送 Trap 消息

【命令格式】 **snmp-server enable traps** [*notification-type*]

【参数说明】 *notification-type*：启用对应事件的 Trap 通知，，有以下类型：

snmp: 启动 SNMP 事件的 TRAP 通知；

bridge: 启动 BRIDGE 事件的 TRAP 通知；

mac-notification: 启动 MAC 事件的 TRAP 通知；

ospf: 启动 OSPF 事件的 TRAP 通知；

urpf: 启动 URPF 事件的 TRAP 通知；

vrrp: 启动 VRRP 事件的 TRAP 通知；

web-auth: 启动 WEB 认证事件的 TRAP 通知。

【命令模式】 全局配置模式

【使用指导】 该命令必须与全局配置命令 **snmp-server host** 一起使用，才能发送 Trap 消息。

打开接口发送 Link Trap 功能

【命令格式】 **snmp trap link-status**

【参数说明】 **-**

【配置模式】 接口配置模式

【使用指导】 对于接口（以太网接口、Ap 接口、SVI 接口），当功能打开时，如果接口发生 Link 状态变化，SNMP 将发出 Link Trap，反之则不发。

打开发送系统重启 Trap 功能

【命令格式】 **snmp-server system-shutdown**

【参数说明】 -

【配置模式】 全局配置模式

【使用指导】 打开 SNMP 系统重启通知功能，会在设备 **reload/reboot** 以前给 NMS 发送 Trap 消息通知系统重启。

指定发送 Trap 消息的源地址

【命令格式】 **snmp-server trap-source** *interface*

【参数说明】 *interface*：用于作为 SNMP 源地址的接口。

【配置模式】 全局配置模式

【使用指导】 缺省情况下，SNMP 报文从哪个接口出去，就使用哪个接口的 IP 地址作为源地址，为了便于管理和识别，可以使用该命令固定使用一个本地 IP 地址作为 SNMP 的源地址。

配置发送 Trap 消息时携带私有字段

【命令格式】 **snmp-server trap-format private**

【参数说明】 -

【配置模式】 全局配置模式

【使用指导】 使用该命令可配置发送 Trap 消息携带私有格式字段，包含的字段目前支持的有告警发生时间，各个字段的具体数据类型和数据范围可参见 RUIJIE-TRAP-FORMAT-MIB.mib 文件说明。

配置举例

配置启用 trap 功能

【网络环境】

图 4-6

- 网管工作站（NMS）基于共同体认证模式对网络设备（Agent）进行管理，网络设备能够主动向网管工作站发送消息。

【配置方法】

- 第一步，配置 Agent 主动向 NMS 发送消息。配置 SNMP 主机地址为 192.168.3.2，消息格式为 Version 2c，认证名为 “user1”。使能 Agent 主动发送 Trap 消息。
- 第二步，配置 Agent 的 IP 地址。配置 Gi 0/1 的接口地址为 192.168.3.1/24。

Agent

```
Ruijie(config)#snmp-server host 192.168.3.2 traps version 2c user1
Ruijie(config)#snmp-server enable traps
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

【检验方法】

- 通过 **show running-config** 命令查看设备的配置信息。
- 通过 **show snmp** 命令显示 SNMP 的状态信息。

Agent

```
Ruijie# show running-config
ip access-list standard a1
 10 permit host 192.168.3.2
interface gigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
snmp-server view v1 1.3.6.1.2.1.1 include
snmp-server location fuzhou
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
snmp-server contact ruijie.com.cn
snmp-server community user1 view v1 rw a1
snmp-server chassis-id 1234567890
```

```
Ruijie#show snmp
Chassis: 1234567890
0 SNMP packets input
        0 Bad SNMP version errors
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        0 Number of requested variables
        0 Number of altered variables
        0 Get-request PDUs
        0 Get-next PDUs
        0 Set-request PDUs
0 SNMP packets output
        0 Too big errors (Maximum packet size 1472)
        0 No such name errors
        0 Bad values errors
        0 General errors
        0 Response PDUs
        0 Trap PDUs
SNMP global trap: enabled
SNMP logging: disabled
SNMP agent: enabled
```

常见错误

-

4.4.3 屏蔽Agent功能

配置效果

在不需要 Agent 服务的时候，屏蔽 Agent 功能。

注意事项

- 执行 **no snmp-server** 命令，可以在不需要代理服务的时候，屏蔽 SNMP 代理功能。
- 不同于屏蔽命令，执行 **no enable service snmp-agent** 命令，会直接关闭 snmp 所有服务(即 snmp 代理功能被禁用了，不接收报文、不发送响应报文及 trap ），不会屏蔽代理的配置信息。

配置方法

配置屏蔽设备 SNMP 代理

- 可选配置。
- 需要屏蔽所有 SNMP 代理服务配置时，可选用此项配置。

配置关闭设备 SNMP 代理

- 可选配置。
- 需要直接关闭所有服务时，应选用此配置项。

检验方法

通过 **show services** 命令查看 snmp 服务的开关状态信息。

通过 **show snmp** 命令显示 SNMP 的状态信息。

通过 **show running-config** 命令查看设备的配置信息。

相关命令

配置屏蔽设备 SNMP 代理功能

【命令格式】 **no snmp-server**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 SNMP 代理功能服务默认关闭，在设置 SNMP 代理参数（例如 NMS 主机地址、认证名和访问权限等）时，会自动打开 SNMP 代理服务，服务开关命令 **enable service snmp-agent** 也必须同时打开，SNMP 代理服务才能生效，但只要关闭了其中的一个，SNMP 代理服务将不会生效。使用 **no snmp-server** 命令可以关闭设备支持的所有版本 SNMP 的代理服务。

使用该命令的同时，将屏蔽所有 SNMP 代理服务配置（即使用 **show running-config** 命令查看时不会显示配置，重新开启 SNMP 代理服务可以恢复），而 **enable service snmp-agent** 命令则不会屏蔽 SNMP 代理配置。

配置关闭设备 SNMP 代理功能

【命令格式】 **no enable service snmp-agent**

【参数说明】 -

【配置模式】 全局配置模式

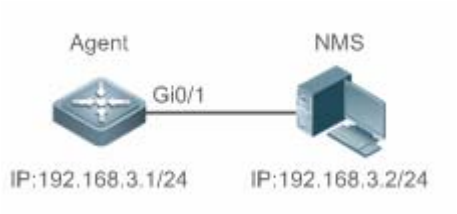
【使用指导】 关闭 SNMP 服务开关，但不会屏蔽 SNMP 代理参数。

配置举例

配置启用 snmp 服务功能

【网络环境】

图 4-7



通过设置 snmp 服务开关，以及设置 snmp 代理服务器，使得网管工作站（NMS）能通过 snmp 访问设备。

【配置方法】

- 配置启用 snmp 服务。
- 配置 snmp 代理服务器的参数，使服务生效。

A gent

```
Ruijie(config)#enable service snmp-agent
```

【检验方法】

- 通过 **show services** 命令查看 snmp 服务的开关状态信息。

Agent

```
Ruijie#show service
web-server   : disabled
web-server(https): disabled
snmp-agent    : enabled
ssh-server    : disabled
telnet-server : enabled
```

常见错误

-

4.4.4 设置SNMP控制参数

配置效果

对 SNMP 的 Agent 的基本参数进行配置，包括设备的联系方式、设备位置、序列号、发送 Trap 消息的参数等，NMS 通过访问设备的这些参数，便可以得知设备的联系人，设备所在的物理位置等信息。

注意事项

-

配置方法

↘ 配置系统的联系方式

- 可选配置。

- 当需要修改系统的联系方式时，需在 agent 上配置此项。

配置系统位置

- 可选配置。
- 当需要修改系统的系统位置时，需在 agent 上配置此项。

配置系统序列码

- 可选配置。
- 当需要修改系统的序列码时，需在 agent 上配置此项。

配置设备的网元信息

- 可选配置。
- 当需要修改网元编码信息时，需在 agent 上配置此项。

配置 SNMP 代理最大数据报文长度

- 可选配置。
- 当需要修改 SNMP 代理最大数据报文长度时，需在 agent 上配置此项。

配置 SNMP 服务 UDP 端口号

- 可选配置。
- 当需要修改 SNMP 服务的 UDP 端口号时，需在 agent 上配置此项。

配置 Trap 消息报文的队列长度

- 可选配置。
- 当希望通过调整消息队列大小来控制消息发送速度时，需在 agent 上配置此项。

配置发送 Trap 消息的时间间隔

- 可选配置。
- 当需要修改发送 Trap 消息的时间间隔时，需在 agent 上配置此项。

配置 SNMP 流控

- 可选配置。
- 如果 SNMP 的请求报文太多导致 SNMP 任务的 CPU 占用比较高，可以配置 SNMP 流控，限制 SNMP 任务每秒处理的请求报文个数，从而控制 SNMP 任务的 CPU 占用情况。

检验方法

通过 **show snmp** 命令显示 SNMP 的状态信息。

通过 **show running-config** 命令查看设备的配置信息。

相关命令

配置系统的联系方式

【命令格式】 **snmp-server contact** *text*

【参数说明】 *text*：描述系统联系方式的字符串。

【命令模式】 全局配置模式

【使用指导】

配置系统位置

【命令格式】 **snmp-server location** *text*

【参数说明】 *text*：描述系统信息的字符串。

【配置模式】 全局配置模式

【使用指导】

配置系统序列码

【命令格式】 **snmp-server chassis-id** *text*

【参数说明】 *text*：系统序列号的文本，可以是数字或字符。

【配置模式】 全局配置模式

【使用指导】 SNMP 系统序列号一般使用机器的序列号，以便对设备进行识别。

配置设备的网元信息

【命令格式】 **snmp-server net-id** *text*

【参数说明】 *text*：设置设备网元编码 text，text 是长度为 1~255 的字符串，区分大小写，可包含空格。

【配置模式】 全局模式

【使用指导】 配置设备网元编码信息。

配置 SNMP 代理最大数据报文长度

【命令格式】 **snmp-server packetsize** *byte-count*

【参数说明】 *byte-count*：数据包大小，从 484 字节到 17876 字节。

【配置模式】 全局模式

【使用指导】

配置 SNMP 服务 UDP 端口号

【命令格式】 **snmp-server udp-port** *port-num*

【参数说明】 *port-num*：指定 SNMP 服务的 UDP 端口号，即接收 SNMP 报文的协议端口号。

【配置模式】 全局模式

【使用指导】 指定接收 SNMP 报文的协议端口号。

配置 Trap 消息报文的队列长度

【命令格式】 **snmp-server queue-length** *length*

【参数说明】 *length*：队列长度，大小从 1 到 1000。

【配置模式】 全局配置模式

【使用指导】 通过调整消息队列大小和发送消息的时间间隔来控制消息发送速度，消息发送最大速度为 4 个每秒。

配置发送 Trap 消息的时间间隔

【命令格式】 **snmp-server trap-timeout** *seconds*

【参数说明】 *seconds*：间隔时间，单位为秒，取值范围：1 – 1000。

【配置模式】 全局配置模式

【使用指导】 通过调整消息队列大小和发送消息的时间间隔来控制消息发送速度，消息发送最大速度为 4 个每秒。

配置 SNMP 流控

【命令格式】 **snmp-server flow-control pps** [*count*]

【参数说明】 *count*：每秒处理的 SNMP 请求报文数量，范围<50-65535>。

【命令模式】 全局配置模式

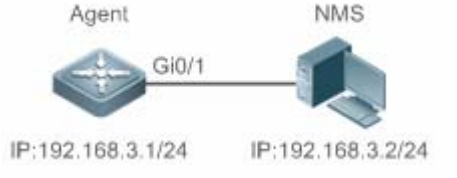
【使用指导】 如果 SNMP 的请求报文太多导致 SNMP 任务的 CPU 占用比较高，可以配置 SNMP 流控，限制 SNMP 任务每秒处理的请求报文个数，从而控制 SNMP 任务的 CPU 占用情况。

配置举例

设置 SNMP 的控制参数

【网络环境】

图 4-8



- 网管工作站（NMS）基于共同体认证模式对网络设备（Agent）进行管理，网管工作站能够获取设备的基本系统信息，如系统的联系方式、位置、序列码。

【配置方法】

- 第一步，配置 SNMP 代理参数。配置系统所处的位置、联系方式、序列码。
- 第二步，配置 Agent 的 IP 地址。配置 Gi 0/1 的接口地址为 192.168.3.1/24。

Agent

```
Ruijie(config)#snmp-server location fuzhou
Ruijie(config)#snmp-server contact ruijie.com.cn
Ruijie(config)#snmp-server chassis-id 1234567890
Ruijie(config)#interface gigabitEthernet 0/1
Ruijie(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0
Ruijie(config-if-gigabitEthernet 0/1)#exit
```

【检验方法】

- 第一步，查看设备的配置信息。

- 第二步，查看 SNMP 视图和组的信息。

Agent

```
Ruijie# show running-config
ip access-list standard a1
 10 permit host 192.168.3.2
interface gigabitEthernet 0/1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
snmp-server view v1 1.3.6.1.2.1.1 include
snmp-server location fuzhou
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
snmp-server contact ruijie.com.cn
snmp-server community user1 view v1 rw a1
snmp-server chassis-id 1234567890
```

```
Ruijie#show snmp view
v1(include) 1.3.6.1.2.1.1
default(include) 1.3.6.1
Ruijie#show snmp group
groupname: user1
securityModel: v1
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
groupname: user1
securityModel: v2c
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
```

常见错误

-

4.4.5 配置SNMP MIB缓存功能

配置效果

启用 SNMP MIB 缓存功能，由主机提前收集从/备机的 MIB 变量的数据，并缓存在主机上面，NMS 在读取 MIB 变量值时，直接对缓存数据进行读取，避免访问从//备机的时间消耗。从而加快 NMS 获取 MIB 信息的速度。

注意事项

- SNMP MIB 缓存只对特定的表格变量的 MIB 节点生效，配置 SNMP MIB 缓存时只需要配置 MIB 表格变量的根节点的 OID 即可。
- 启用缓存功能后，由于缓存采用定时更新，会出现 MIB 数据无法实时反应最新状态的情况。配置缓存更新时间过短，可能导致系统频繁进行缓存更新，消耗系统 CPU 资源；配置缓存更新时间过长，可能导致 MIB 数据更新延迟，无法实时反应系统状态。所以需要根据对 MIB 节点的实时性及系统资源对缓存更新时间进行调整

配置方法

配置全局 SNMP MIB 缓存功能

- 可选配置。
- 默认情况下关闭 SNMP MIB 缓存功能，当需要开启 SNMP MIB 缓存功能时，需要在设备上面配置此项。

配置 SNMP MIB 全局缓存更新时间

- 可选配置。
- 默认情况下 SNMP MIB 全局缓存更新时间为 300 秒，当需要修订全局缓存更新时间时，需要在设备上面配置此项。

配置指定 OID 节点启用缓存功能和缓存更新时间

- 可选配置。
- 默认情况下所有 MIB 节点均不启用缓存功能，如果要启动指定 MIB 节点的缓存功能，需要在设备上面配置此项。

检验方法

通过 **show running-config** 命令查看设备的配置信息。

相关命令

配置全局 SNMP MIB 缓存功能

【命令格式】 **snmp-server cache enable**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】

配置 SNMP MIB 全局缓存更新时间

【命令格式】 **snmp-server cache update-timer** *seconds*

【参数说明】 *seconds*：SNMP MIB 全局缓存更新时间，单位为秒，范围：60~3600。

【配置模式】 全局配置模式

【使用指导】

配置指定 OID 节点启用缓存功能和缓存更新时间

【命令格式】 **snmp-server cache oid** *oid-string* **[update-timer** *seconds***]**

【参数说明】 *oid-string*：MIB 节点 OID。

seconds：缓存更新时间，单位为秒，范围：60~3600。

【配置模式】 全局配置模式

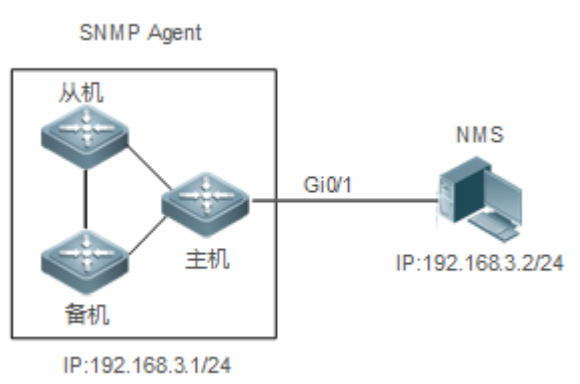
【使用指导】 如果未配置缓存更新时间，则使用全局配置的缓存更新时间作为该 OID 节点缓存的更新时间。

配置举例

设置 SNMP 的控制参数

【网络环境】

图 4-9



- 网管工作站（NMS）基于共同体认证模式对网络设备（SNMP Agent）进行管理，网管工作站能够获取网络设备的 MIB 节点信息，如 AP、STA 的上下线状态等。

【配置方法】

- 第一步，配置全局 SNMP MIB 缓存功能。
- 第二步，配置 SNMP MIB 全局缓存更新时间。
- 第三步，配置指定 OID 节点启用缓存功能。

Agent

```
Ruijie(config)# snmp-server cache enable
Ruijie(config)# snmp-server cache update-timer 600
Ruijie(config)# snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1
```

【检验方法】

- 第一步，查看设备的配置信息。

Agent

```
Ruijie# show running-config | include snmp
snmp-server cache enable
snmp-server cache update-timer 600
snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1
snmp-server enable traps
```

```
snmp-server community public rw
```

常见错误

-

4.5 监视与维护

清除各类信息

作用	命令
清除 SNMP 连续认证失败后被锁定的源 IP 地址表	**clear snmp locked-ip** [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]

查看运行情况

作用	命令
显示 SNMP 的状态信息	**show snmp** [**mib** | **user** | **view** | **group**| **host**]

5 HTTP 服务

5.1 概述

HTTP（Hypertext Transfer Protocol，超文本传输协议）用来在 Internet 上传递 Web 页面信息。HTTP 位于 TCP/IP 协议栈的应用层，传输层采用面向连接的 TCP。

HTTPS（Hypertext Transfer Protocol Secure）是支持 SSL（Secure Sockets Layer，安全套接层）协议的 HTTP 协议。主要作用是在不安全的网路上创建一个安全的通道，保证信息很难被监听以及对中间人攻击提供一定的合理保护。HTTPS 目前已被广泛用于互联网上安全敏感的通讯，如电子交易支付等。

协议规范

- RFC1945：Hypertext Transfer Protocol -- HTTP/1.0
- RFC2616：Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818：Hypertext Transfer Protocol Over TLS -- HTTPS

5.2 典型应用

典型应用	场景描述
HTTP应用服务	用户通过 Web 管理设备。

5.2.1 HTTP应用服务

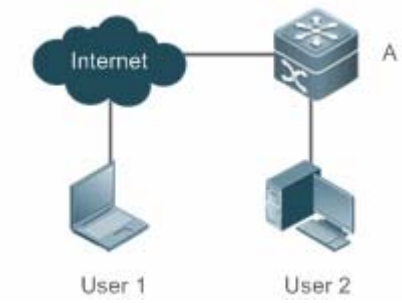
应用场景

设备开启 HTTP 服务后，用户只需在 PC 机浏览器中输入 http://+设备的 IP 地址，认证通过后就可以登陆到 Web 管理界面。在 Web 界面中，用户可以进行设备状态信息监控、配置设备、上传和下载文件等操作。

以下图为例，用户进行 Web 管理。

- 用户可以通过 Internet 进行远程访问设备，也可以在本地局域网中通过登陆 Web 服务器对设备进行配置管理。
- 用户可以根据实际情况，选择在设备上单独启用 HTTPS 服务或者 HTTP 服务，也可以同时启用 HTTPS 和 HTTP 服务。
- 用户还可以再浏览器上设置使用 HTTP/1.0 还是 HTTP/1.1 协议来访问设备的 HTTP 服务。

图 5-1



【注释】 A 为锐捷设备。

用户 User1 通过 Internet 网络访问设备。

用户 User2 通过局域网访问设备。

功能部署

- 设备运行 HTTP 协议，用户在 PC 浏览器中通过 http：//设备的 ip 地址，访问设备。
- 设备运行 HTTPS 协议，用户在 PC 浏览器中通过 https：//设备的 ip 地址，访问设备。

5.3 功能详解

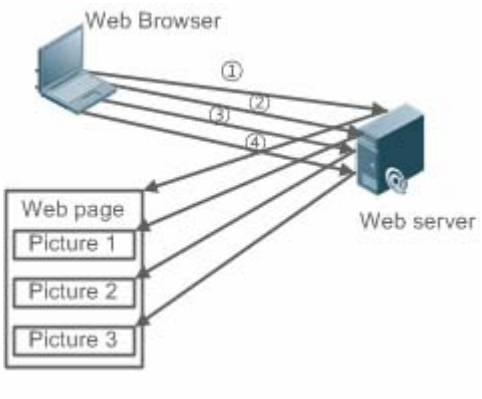
基本概念

HTTP 服务

HTTP 服务是指在 Internet 上利用 HTTP 协议传递 Web 页面信息。HTTP/1.0 是目前业界使用最广泛的 HTTP 协议版本，由于一个 Web 服务器每天可能有上万甚至上百万的访问量，为了便于连接管理，HTTP/1.0 采用短连接方式。一个请求创建一个 TCP 连接，请求完成后释放连接，服务器不需要记录和跟踪过去的请求。HTTP/1.0 虽然简化了连接管理，但是却引入了性能缺陷。

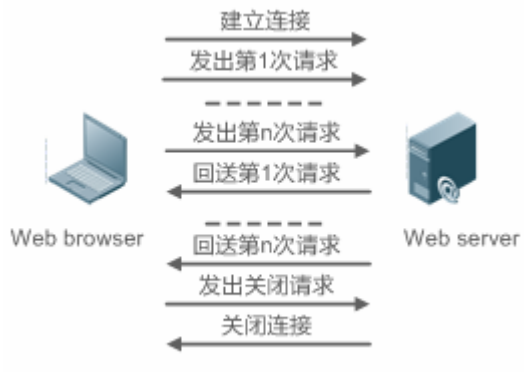
例如一个网页中可能需要很多图片，网页中包括的不是真正的图片内容，而是它们的 URL 连接地址，这样浏览器在访问过程中会发出多次请求，每次请求都要建立一个单独的连接，每次连接都是完全隔离的。建立和释放连接是一个相对费劲的过程，从而严重影响了客户机和服务器的性能，如下图所示。

图 5-2



HTTP/1.1 克服了这个缺陷。该版本支持持久连接，即一个连接可以传输多个请求和响应，这样客户机可以不用等待上一次请求完成就可以发送第二个请求，减少了网络时延，提高性能，如下图所示。

图 5-3



目前，锐捷设备支持 HTTP/1.0 和 HTTP/1.1 两种协议版本。

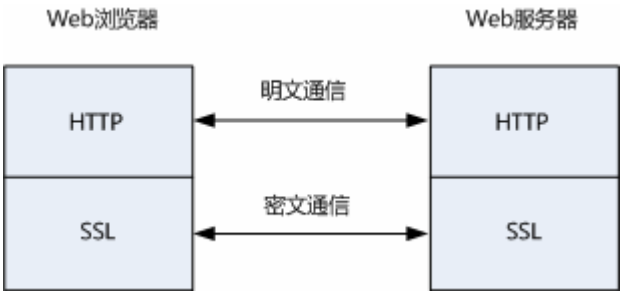
设备使用哪种协议版本由 Web 浏览器决定。

HTTPS 服务

HTTPS 服务就是在 HTTP 基础上加入 SSL 层，其安全基础是 SSL。要使协议能够正常运行，服务器必需有 PKI（Public Key Infrastructure，公钥基础设施）证书，而客户端则不一定。SSL 协议提供的服务主要有：

- 认证用户和服务器，确保数据发送到正确的客户机和服务器；
- 加密数据以防止数据中途被窃取；
- 维护数据的完整性，确保数据在传输过程中不被改变。

图 5-4



HTTP 升级服务

HTTP 升级包括 HTTP 本地升级和 HTTP 远程升级两种方式。

- 本地升级时，设备作为 HTTP 服务器，用户通过 Web 浏览器登陆到设备，将需要升级的文件上传到设备，实现设备上文件的升级。
- 远程升级时，设备作为客户端，连接到远程 HTTP 服务器上，通过获取服务器上的文件来实现本地文件的升级。

功能特性

功能特性	作用
HTTP服务	用户通过 Web 界面登陆到设备中进行配置与管理。
HTTP本地升级服务	将需要升级的文件上传到设备，实现设备上文件的升级。

5.3.1 HTTP服务

HTTP 是为 Web 管理提供服务，用户通过 Web 界面登陆到设备中进行配置与管理。

工作原理

Web 管理包括 Web 客户端和 Web 服务器，同理 HTTP 服务也采用客户端/服务器模式。HTTP 客户端内嵌在 Web 管理客户端的 Web 浏览器中，能够发送 HTTP 报文和接收处理 HTTP 响应报文。而 Web 服务器(即 HTTP 服务器)则内嵌于设备中。客户端和服务器之间的信息交互过程如下：

- 在客户端与服务器之间建立 TCP 连接，HTTP 服务默认端口号是 80，HTTPS 服务默认端口号是 443。
- 客户端向服务器发送请求消息。
- 服务器解析客户端发送的请求，请求内容包括获取 web 页面、执行 cli 命令，上传文件等。
- 服务器执行完请求内容后，将响应发送回给客户端。

相关配置

使能 HTTP 服务

缺省情况下，HTTP 服务功能关闭。

使用 **enable service web-server** 命令可以使能 HTTP 服务功能，包括 HTTP 服务和 HTTPS 服务。

必须使能 HTTP 服务功能，用户才能通过 Web 界面登陆到设备中进行配置与管理。

↘ 配置 HTTP 认证信息

缺省情况下，系统默认创建两个账号，admin 账号和 guest 账号，这两个账号不可被删除，只可修改密码。其中 guest 账号默认对应 level 2 权限，在 web 端只拥有查看系统首页的权限。管理员账号为 admin 对应 level 0 权限，在 web 端管理员账号拥有所有的功能，并且可以编辑其他管理账号并授权该账号可访问的页面，新添加的账号对应 level 1 权限。

使用 **webmaster level** 命令可以配置认证的用户名和密码。

通过配置该命令，用户需要输入所配置的用户名和密码进行认证才能登陆 Web 页面。

↘ 配置 HTTP 服务端口

缺省情况下，HTTP 服务端口为 80。

使用 **http port** 命令可以配置 HTTP 服务端口号，取值范围是 80 及 1025-65535。

通过配置 HTTP 服务端口号，可以减少非法用户对 HTTP 服务的攻击。

↘ 配置 HTTPS 服务端口

缺省情况下，HTTPS 服务端口为 443。

使用 **http secure-port** 命令可以配置 HTTPS 服务端口号，取值范围是 443 及 1025-65535。

通过配置 HTTPS 服务端口号，可以减少非法用户对 HTTPS 服务的攻击。

5.3.2 HTTP本地升级服务

设备作为 HTTP 服务器，用户通过 Web 浏览器登陆到设备，将需要升级的文件（包括组件包、web 包）上传到设备或者直接通过 tftp 上传文件到设备中。

工作原理

- 通过 Web 的“本地升级”功能上传组件包或 web 包
- 设备接收文件信息，接收成功后进行版本与合法性校验
- 文件校验成功后，如果是 web 包，直接升级；如果是组件包，用户在浏览器端通过是否重启设备来决定升级与否。

相关配置

↘ 更新 Web 包

使用 **upgrade web download** 命令从 TFTP 服务器上下载 WEB 包。

通过配置该命令，从 TFTP 服务器上下载 WEB 包，合法性校验通过后，WEB 包直接进行升级，无需重启设备。

也可以使用 **upgrade web** 命令直接升级本地存在的 WEB 包。

↘ 更新子系统组件

缺省情况下，不管是通过浏览器还是 TFTP 上传子系统组件，设备默认都是不升级的。

用户要升级子系统组件，都必须重启设备。

5.4 配置详解

配置项	配置建议 & 相关命令	
配置HTTP服务	⚠ 必须配置。用于启动 HTTP 服务。	
	enable service web-server	使能 HTTP 服务
	webmaster level	配置 HTTP 认证信息

	http port	配置 HTTP 服务端口
	http secure-port	配置 HTTPS 服务端口
配置HTTP本地升级	⚠ 必须配置。用于实现 HTTP 本地升级。	
	upgrade web	升级设备存放的 WEB 包。
	upgrade web download	自动从服务器上下载 WEB 包，并自动升级

5.4.1 配置HTTP服务

配置效果

设备开启 HTTP 服务，用户通过认证后可以登陆到 Web 管理界面，进行设备状态信息监控、配置设备、上传和下载文件等操作。

配置方法

↘ 使能 HTTP 服务

- 必须配置。
- 若无特殊要求，应在每台锐捷设备上使能 HTTP 服务，否则 web 服务不可访问。

↘ 配置 HTTP 认证信息

- 默认情况下，已经配置用户名 admin、guest，对应的密码是 admin、guest。
- 若无特殊要求，用户可以使用默认的用户名登陆 web 页面，直接通过 web 浏览器来更新认证信息；如果一直使用默认账户，会存在安全隐患，因为 IP 一旦泄露，非授权人员就可以通过 web 获取到设备的配置信息等。

↘ 配置 HTTP 服务端口

- 如果要求改变 HTTP 服务端口，则必须配置 HTTP 服务端口。
- 若无特殊要求，可以使用默认的 HTTP 服务端口 80 进行访问。

↘ 配置 HTTPS 服务端口

- 如果要求改变 HTTPS 服务端口，则必须配置 HTTPS 服务端口。
- 若无特殊要求，可以使用默认的 HTTPS 服务端口 443 进行访问。

检验方法

- 用户在浏览器上输入 http：//设备的 ip：服务端口，验证浏览器是否会跳转到认证页面。
- 用户在浏览器上输入 https：//设备的 ip：服务端口，验证浏览器是否会跳转到认证页面。

相关命令

↘ 使能 HTTP 服务

【命令格式】 **enable service web-server** [**http** | **https** | **all**]

【参数说明】 **http** | **https** | **all** :打开相应的服务。**http** 为打开 HTTP 服务，**https** 为打开 HTTPS 服务，**all** 为同时打开 HTTP 和 HTTPS 服务。缺省为同时打开 HTTP 和 HTTPS 服务。

【命令模式】 全局模式

【使用指导】 如果执行该命令时后面不跟任何关键字或者跟 **all**，则表示同时打开 HTTP 服务和 HTTPS 服务；如果跟 **http** 关键字，则表示只打开 HTTP 服务；如果跟 **https** 关键字，则表示只打开 HTTPS 服务。

使用 **no enable service web-server** 或者 **default enable service web-server** 用于关闭相应的 HTTP 服务。

如果该 **no 命令或 default** 命令后面不跟任何关键字，则表示关闭 HTTP 服务和 HTTPS 服务。

配置 HTTP 认证信息

【命令格式】 **webmaster level** *privilege-level* **username** *name* **password** { *password* | [**0 | 7**] *encrypted-password* }

【参数说明】 *privilege-level*：用户绑定权限等级。

name：用户名。

password：用户口令。

0 | 7：口令的加密类型，0 无加密，7 简单加密。缺省为 0。

encrypted-password：口令文本。

【命令模式】 全局模式

【使用指导】 在使用 HTTP Server 的时候，需要进行登陆认证才能进入 Web 页面。使用该命令配置 Web 登陆认证的用户名和密码。

执行 **no webmaster level** *privilege-level* 删除指定权限等级的所有用户名与密码。

执行 **no webmaster level** *privilege-level* **username** *name* 删除指定用户名和密码。

用户名和密码有三个权限等级；每个权限等级最多可以配置 10 个用户名和密码。

系统默认创建两个账号，admin 账号和 guest 账号，这两个账号不可被删除，只可修改密码。其中 guest 账号默认对应 level 2 权限，在 web 端只拥有查看系统首页的权限。管理员账号为 admin 对应 level 0 权限，在 web 端管理员账号拥有所有的功能，并且可以编辑其他管理账号并授权该账号可访问的页面，新添加的账号对应 level 1 权限。

配置 HTTP 服务端口

【命令格式】 **http port** *port-number*

【参数说明】 *port-number*：设置 HTTP 服务端口，取值范围为 80 及 1025-65535。

【命令模式】 全局模式

【使用指导】 使用该命令设置 HTTP 服务的端口。

配置 HTTPS 服务端口

【命令格式】 **http secure-port** *port-number*

【参数说明】 *port-number*：设置 HTTPS 服务端口，取值范围为 443 及 1025-65535。

【命令模式】 全局模式

【使用指导】 使用该命令设置 HTTPS 服务的端口。

配置举例

使用 Web 管理一台锐捷设备，通过 Web 浏览器登陆到锐捷中进行相关功能的配置

- 使用默认配置的 admin 认证信息进行登录。
- 为了提高安全性，要求 Web 浏览器即可以通过 HTTP 协议访问，也可以通过 HTTPS 协议访问。
- 要求自己配置 HTTP 服务端口，减少非法用户对 HTTP 的攻击。

【网络环境】

图 5-5

【配置方法】

- 需要配置同时打开 HTTP 和 HTTPS 服务。
- 可以配置 HTTP 服务端口号为 8080；HTTPS 服务端口号为 4430.

A

```
A#configure terminal
A(config)# enable service web-server
A(config)# http port 8080
A(config)# http secure-port 4430
```

【检验方法】 查看 HTTP 配置信息。

A

```
A# show web-server status
http server status: enabled
http server port: 8080
https server status:enabled
https server port: 4430
```

常见错误

- 如果 HTTP 服务端口不是默认的 80 与 443，用户在浏览器中必须输入配置的具体服务端口，否则 web 端无法访问设备。

5.4.2 配置HTTP本地升级

配置效果

用户可以通过浏览器或者 upgrade web 命令升级。

注意事项

- 通过浏览器上传 Web 包，只要上传成功，并且版本校验通过，设备默认会直接升级为最新的 Web 包。
- 通过 **upgrade web download** 命令，自动从 tftp 服务器下载文件，并自动升级。
- 通过 **upgrade web** 命令，自动升级本地文件系统的 WEB 包。

配置方法

无

检验方法

- 用户直接通过浏览器访问，通过查看最新的 WEB 页面。

相关命令

↘ 从 TFTP 服务器下载 Web 文件包

【命令格式】 **upgrade web download tftp:** *//path*

【参数说明】 tftp：表示通过普通数据口连接 ftfp 服务器下载 WEB 包

path：tftp 服务器上 WEB 包的路径

【命令模式】 特权模式

【使用指导】 该命令是从 tftp server 端中下载 WEB 包，并自动升级。

↘ 从升级设备的 Web 文件包

【命令格式】 **upgrade web** *uri*

【参数说明】 *uri*：WEB 包存放的本地路径。

【命令模式】 特权模式

【使用指导】 该命令用于升级设备内存放的 WEB 包，并自动升级。

配置举例

↘ 用户通过官网获取到最新的 Web 包，希望设备运行最新的 Web 包

【网络环境】

图 5-6

【配置方法】

- 与本地 PC 机相连，PC 机的 IP 地址是 10.10.10.13；给设备配置一个同网段的 IP 地址 10.10.10.131。
- 通过 web 登陆到设备中，并上传最新的 WEB 包到设备中。

A

```
A#configure terminal
A(config)# vlan 1
A(config-vlan)# exit
A(config)# interface vlan 1
A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0
A(config-VLAN 1)# exit
A(config)# enable service web-server
```

在 PC 机中，使用 WEB 页面的“本地升级”功能上传 WEB 包升级

【检验方法】 在 PC 机中，重新进行 Web 认证登陆，验证是否显示最新的 Web 页面。

↘ 通过 upgrade web download 方式升级 WEB 包

【网络环境】

图 5-7

【配置方法】

- 与本地 PC 机相连，PC 机的 IP 地址是 10.10.10.13；给设备配置一个同网段的 IP 地址 10.10.10.131。
- 打开 tftp 服务器。

A

```
A#configure terminal
A(config)# vlan 1
A(config-vlan)# exit
A(config)# interface vlan 1
A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0
A(config-VLAN 1)# end
A#upgrade web download tftp:// 10.10.10.13/web.upd
Press Ctrl+C to quit
!!!!!!!!
download 3896704 bytes
Begin to upgrade the web package...
```

```
Web package upgrade successfully.
```

【检验方法】 在 PC 机中，重新进行 Web 认证登陆，验证是否显示最新的 Web 页面。

↘ 通过 upgrade web 方式升级 WEB 包

【网络环境】

图 5-8

【配置方法】

- 与本地 PC 机相连，PC 机的 IP 地址是 10.10.10.13；给设备配置一个同网段的 IP 地址 10.10.10.131。
- 打开 tftp 服务器。

A

```
A#configure terminal
A(config)# vlan 1
A(config-vlan)# exit
A(config)# interface vlan 1
A(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0
A(config-VLAN 1)# end
A#copy tftp://10.10.10.13/web.upd flash:/web.upd
Press Ctrl+C to quit
!!!!!!!!
Accessing tftp:// 10.10.10.13/web.upd finished, 3896704 bytes prepared
Flushing data to flash:/web.upd...
Flush data done
A #upgrade web flash:/web.upd
Web package upgrade successfully.
A #
```

【检验方法】 在 PC 机中，重新进行 Web 认证登陆，验证是否显示最新的 Web 页面。

常见配置错误

- 通过浏览器访问，发现没有更新到新的 WEB 包，可能是本地浏览器有缓存；将浏览器的缓存清空，在重新访问一次。

5.5 监视与维护

清除各类信息

-

查看运行情况

作用	命令
查看 Web 服务配置信息和状态。	**show web-server status**

查看调试信息

-

6 系统日志

6.1 概述

设备在运行过程中，会发生各种状态变化如链路状态UP、DOWN等，也会遇到一些事件如收到异常报文、处理异常等。锐捷产品系统日志提供一种机制，在状态变化或发生事件时，就自动生成固定格式的消息（日志报文），这些消息可以被显示在相关窗口（控制台、监视终端等）上或被记录在相关媒介（内存缓冲区、日志文件）上或发送到网络上的一组日志服务器上，供管理员分析网络情况和定位问题。同时为了方便管理员对日志报文的读取和管理，这些日志报文可以被打上时间戳和序号，并按日志信息的优先级进行分级。

下文仅介绍系统日志的相关内容。

协议规范

- RFC 3164：The BSD syslog Protocol
- RFC 5424：The_Syslog_Protocol

6.2 典型应用

典型应用	场景描述
系统日志输出到控制台	通过控制台监控系统日志信息。
系统日志发送到日志服务器	通过服务器监控系统日志信息。

6.2.1 系统日志输出到控制台

应用场景

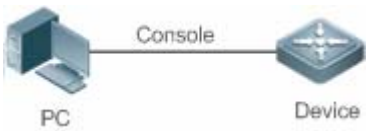
可以将系统日志输出到控制台，方便管理员监控系统的运行状态，网络部署要求如下：

1、 信息级别高于等于 informational（6 级）的日志信息允许输出到控制台。

2、 只允许 ARP 模块和 IP 模块的日志信息输出到控制台。

组网环境如下所示：

图 1-1 系统日志输出到控制台组网图



功能部属

设备端的配置要点如下：

1、 设置允许输出到控制台的日志信息级别为 informational（6 级）。

2、 设置日志信息的过滤方向为：terminal（终端方向）。

3、 设置日志信息的过滤方式为：contains-only（ “只包含”过滤方式）。

4、 设置日志信息的过滤规则为： “单个匹配”规则，模块名包含 ARP 或 IP。

6.2.2 系统日志发送到日志服务器

应用场景

可以将系统日志发送到日志服务器，方便管理员在服务器上统一监控设备的日志信息，假设网络中存在如下部署要求：

1、 系统日志信息发送到日志服务器上，日志服务器的 IP 地址为：10.1.1.1。

2、 信息级别高于等于 debugging（7 级）的所有模块的日志信息允许发送到日志服务器上。

3、 系统日志信息发送到日志服务器的报文源接口为 Loopback 0。

组网环境如下所示：

图 1-2 系统日志发送到日志服务器组网图

功能部属

设备端的配置要点如下：

1、 设置日志服务器 IPv4 地址：10.1.1.1。

2、 设置允许发送到服务器的日志信息级别为 debugging（7 级）。

3、 设置发往服务器的日志信息的源接口为 Loopback 0。

6.3 功能详解

基本概念

系统日志的分类

系统日志可以分为如下两类：

- log 类，日志类信息
- debug 类，调试类信息

系统日志的级别

系统日志按严重性划分为 8 个等级，严重性由高到底依次为：emergencies、alerts、critical、errors、warnings、notifications、informational 和 debugging，并分别对应于 0~7 这 8 个数值，值越小代表级别越高。

根据日志级别输出信息时，将会输出日志级别高于或等于所设置级别的日志，比如，输出规则中指定允许级别为 informational 的信息输出，则级别为 emergencies ~ informational 的信息均会输出。

相关日志级别的说明如下表所示：

关键字	级别	描述
emergencies	0	系统不能正常运行的信息
alerts	1	需要立即采取措施改正的信息
critical	2	严重情况
errors	3	错误信息
warnings	4	警告信息
notifications	5	普通但是需要关注的信息
informational	6	说明性的信息
debugging	7	调试信息

系统日志的输出方向

系统日志的输出方向，可以分为 5 类，分别为：console、monitor、server、buffer、file，各个输出方向上的缺省输出级别和输出的日志分类各不相同，用户在使用过程中，可以对不同的输出方向配置不同的过滤规则。

相关日志输出方向的说明如下表所示：

输出方向的名称	缺省输出方向	缺省输出级别	描述
console	控制台	debugging（7 级）	可以输出 log、debug 信息
monitor	监视终端	debugging（7 级）	可以输出 log、debug 信息，便于远程维护
server	日志服务器	informational（6 级）	可以输出 log、debug 信息
buffer	日志缓冲区	debugging（7 级）	可以输出 log、debug 信息，是设备运行过程中的一块缓存，用于记录系统日志
file	日志文件	informational（6 级）	可以输出 log、debug 信息，定时将缓存中的日志信息写入到文件当中

RFC3164 日志格式

按照系统日志的输出方向不同，系统日志可能有不同格式。

- 当输出方向为非日志服务器（控制台、监视终端、日志缓冲区和日志文件）时，系统日志格式为：

```
seq no: *timestamp: sysname %module-level-mnemonic: content
```

对应的格式中文件说明如下：

序列号：*时间戳：系统名称 %模块名-级别-助记符：日志文本

例如，用户退出配置模式时，在控制台可以看到格式如下的日志：

```
001233: *May 22 09:44:36: Ruijie %SYS-5-CONFIG_I: Configured from console by console
```

- 当输出方向为日志服务器，系统日志格式为：

```
<priority>seq no: *timestamp: sysname %module-level-mnemonic: content
```

对应的格式中文件说明如下：

<优先级>序列号：*时间戳：系统名称 %模块名-级别-助记符：日志文本

例如，用户退出配置模式时，在日志服务器可以看到格式如下的日志：

```
<189>001233: *May 22 09:44:36: Ruijie %SYS-5-CONFIG_I: Configured from console by console
```

下面对每一个字段做详细说明：

9. priority（优先级）

本字段只有在向日志服务器输出日志时才有效。

优先级的计算按如下公式：facility * 8 + level。其中：level 表示日志信息的级别；facility 表示设备值，在设置日志信息的设备值时可以设置，默认值为 local7（23），参数取值范围如下表所示：

numerical code（标号）	facility keyword（设备值关键字）	facility description（设备值描述）
0	kern	kernel messages
1	user	user-level messages
2	mail	mail system
3	daemon	system daemons
4	auth1	security/authorization messages
5	syslog	messages generated internally by syslogd
6	lpr	line printer subsystem
7	news	network news subsystem
8	uucp	UUCP subsystem
9	clock1	clock daemon
10	auth2	security/authorization messages
11	ftp	FTP daemon
12	ntp	NTP subsystem
13	logaudit	log audit
14	logalert	log alert
15	clock2	clock daemon
16	local0	local use 0 (local0)
17	local1	local use 1 (local1)
18	local2	local use 2 (local2)
19	local3	local use 3 (local3)

20	local4	local use 4 (local4)
21	local5	local use 5 (local5)
22	local6	local use 6 (local6)
23	local7	local use 7 (local7)

10. seq no（序列号）

系统日志的序列号为6位整型数，并按系统日志产生的条目逐条递增，缺省情况下，该字段信息不会显示出来，可以通过命令开启或关闭该字段信息的输出。

11. timestamp（时间戳）

时间戳记录了系统日志产生的时间，方便用户查看和定位系统事件。锐捷设备的系统日志时间戳格式有两种，分别为：datetime 格式和 uptime 格式。

如果当前设备不存在 RTC 时钟（一种用于记录系统绝对时间的硬件装置），缺省采用设备启动时间（uptime 格式）作为系统日志的时间戳。如果设备存在 RTC 时钟，则缺省采用设备绝对时间（datetime 格式）作为日志信息时间戳。

下面将对这两种时间戳格式进行详细说明：

- datetime 格式：

datatime 格式时间戳完整格式如下所示：

```
Mmm dd yyyy hh:mm:ss.msec
```

各个参数字段的说明如下表所示：

时间戳参数	参数名称	描述
Mmm	月份	Mmm 代表月份的英文缩写 ,1~12 月份依次为 :Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec
dd	天数	dd 代表当前月份对应的天数
yyyy	年份	yyyy 代表对应的年份，缺省情况下没有打开
hh	小时	hh 代表当前对应的小时数
mm	分钟	mm 代表当前对应的分钟数
ss	秒	ss 代表当前对应秒数
msec	毫秒	msec 代表当前对应的毫秒数

缺省情况下，系统输出的日志信息 datetime 格式时间戳不带年份和毫秒信息，用户可以通过命令开启或关闭系统日志的 datetime 格式时间戳是否携带年份和毫秒信息。

- uptime 格式：

uptime 格式时间戳完整格式如下所示：

```
dd:hh:mm:ss
```

整个时间戳字符串代表：系统自启机以来运行的天数：小时数：分钟数：秒数

12. sysname（系统名称）

该字段记录了生成该日志的设备名称，便于日志服务器标识该日志从哪个主机发送过来。缺省情况下，该字段信息不会显示出来，可以通过命令开启或关闭该字段信息的输出。

13. module（模块名）

该字段表示产生此日志的功能模块的名称，为一个 2~20 个字符的大写字符串(可包含大写字母、数字、下划线)。log 类的日志信息默认都要携带 module 字段，debug 类的日志信息有可能没有携带 module 字段。

14. level（日志级别）

系统日志的级别共分为 8 级，分别为 0~7 级。各模块生成的系统日志的级别在开发阶段已经确定，用户不能修改。

15. mnemonic（助记符）

该字段表示产生此日志的信息摘要，为一个 4~32 个字符的大写字符串(可包含大写字母、数字、下划线)。log 类的日志信息默认都要携带 mnemonic 字段，debug 类的日志信息有可能没有携带 mnemonic 字段。

16. content（日志文本）

该字段表示该系统日志的具体内容。

RFC5424 日志格式

对于所有输出方向，系统的日志格式统一为：

```
<priority>version timestamp sysname MODULE LEVEL MNEMONIC [structured-data] description
```

对应的格式中文件说明如下：

```
<优先级>版本号 时间戳 系统名称 模块名 级别 助记符 结构化参数区 信息内容
```

例如，用户退出配置模式时，在控制台可以看到格式如下的日志：

```
<133>1 2013-07-24T12:19:33.130290Z ruijie SYS 5 CONFIG - Configured from console by console
```

下面对每一个字段做详细说明：

1. priority（优先级）

优先级的计算按如下公式：facility * 8 + level。其中：level 表示日志信息的级别；facility 表示设备值，在设置日志信息的设备值时可以设置，开启 RFC5424 日志开关时，facility 默认值为 local0（16）。

2. version（版本号）

RFC5424 中规定版本号固定为 1。

3. timestamp（时间戳）

时间戳记录了系统日志产生的时间，方便用户查看和定位系统事件。锐捷设备在开启 RFC5424 日志开关时，系统日志时间戳格式统一成如下形式：

```
YYYY-MM-DDTHH:MM:SS.SECFRACZ
```

各个参数字段的说明如下表所示：

时间戳参数	参数名称	描述
YYYY	年份	YYYY 代表对应的年份
MM	月份	MM 代表当前年份对应的月份
DD	天数	DD 代表当前月份对应的天数
T	分隔符	日期必须以 T 结尾

HH	小时	HH 代表当前对应的小时数
MM	分钟	MM 代表当前对应的分钟数
SS	秒	SS 代表当前对应秒数
SECFRAC	毫秒	SECFRAC 代表当前对应的毫秒数（1~6 位）
Z	结束符	时间必须以 Z 结尾

4. sysname（系统名称）

该字段记录了生成该日志的设备名称，便于日志服务器标识该日志从哪个主机发送过来。

5. MODULE（模块名）

该字段表示产生此日志的功能模块的名称，为一个 2~20 个字符的大写字符串（可包含大写字母、数字、下划线）。log 类的日志信息默认都要携带 module 字段，debug 类的日志信息有可能没有携带 module 字段。

6. LEVEL（日志级别）

系统日志的级别共分为 8 级，分别为 0~7 级。各模块生成的系统日志的级别在开发阶段已经确定，用户不能修改。

7. MNEMONIC（助记符）

该字段表示产生此日志的信息摘要，为一个 4~32 个字符的大写字符串（可包含大写字母、数字、下划线）。log 类的日志信息默认都要携带 mnemonic 字段，debug 类的日志信息有可能没有携带 mnemonic 字段。

8. structured-data（结构化参数区）

该字段是 RFC5424 新引入的字段，是一种利于机器解析的方式描述日志的参数信息。每条日志可以包含 0 个或多个参数信息，若没有参数信息，必须使用字符 '-' 占位，每一个参数信息的格式为：

```
[SD_ID@enterpriseID PARAM-NAME=PARAM-VALUE]
```

各个参数字段的说明如下表所示：

结构化参数区	参数名称	描述
SD_ID	参数信息名字	参数信息名字通过大写显示，且同一条日志当中不能存在相同的参数信息名字
@	分隔符	只有自定义的参数信息才需要添加@enterpriseID，若为 RFC5424 标准所定义的参数信息，则不需要添加@enterpriseID
enterpriseID	厂商 ID	厂商 ID 由 IANA 维护，锐捷设备的厂商 ID 号固定为 4881，可以通过 IANA 网站进行查询： `http://www.iana.org/assignments/enterprise-numbers`
PARAM-NAME	参数名	参数名字段全部通过大写显示，且同一条日志当中结构化参数区不能存在相同的参数名
PARAM-VALUE	参数值	参数值字段需要添加双引号，其中：IP 地址、MAC 地址类型的值格式化为大写显示，其它类型的值依据实际情况而定

9. description（日志文本）

该字段表示该系统日志的具体内容。

功能特性

功能特性	作用
系统日志功能开关	用于设置系统日志功能的打开与否。
系统日志格式设置	用于设置系统日志的显示格式。
系统日志信息设置	用于设置系统日志发往各个方向的参数信息。
系统日志过滤功能设置	用于设置系统日志过滤功能的参数信息。
系统日志上送功能设置	用于设置系统日志上送功能的参数信息
系统日志监控功能设置	用于设置系统日志监控功能的参数信息。

6.3.1 系统日志功能开关

用于设置系统日志功能的打开与否，主要包括：日志开关、日志信息统计功能开关。

相关配置

↘ 打开日志开关

缺省情况下，日志开关是打开的。

使用 **logging on** 命令在全局配置模式下打开日志开关，打开日志开关后，系统产生的日志信息才能往各个输出方向输出，并用于监视系统的运行状态。

↘ 启用日志信息统计功能开关

缺省情况下，日志信息统计功能是关闭的。

使用**logging count**命令在全局配置模式下开启日志信息统计功能，打开日志信息统计功能后，系统将记录各模块产生的日志信息的次数，以及最后产生此日志信息的时间等。

6.3.2 系统日志格式设置

用于设置系统日志的显示格式，主要包括：RFC5424 日志格式、日志时间戳格式、日志系统名称、日志序列号等。

相关配置

↘ 启用 RFC5424 日志格式开关

缺省情况下，RFC5424 日志格式是关闭的。

切换成 RFC5424 日志格式后，旧日志格式中的命令 **service sequence-numbers**、**service sysname**、**service timestamps**、**service private-syslog**、**service standard-syslog** 将会失效并隐藏掉。

切换到旧的日志格式(即 RFC3164 日志格式)，则在 RFC5424 日志格式中使用的命令 **logging delay-send**、**logging policy**、**logging statistic** 将会失效并隐藏掉。

在新旧日志格式切换前后，**show logging** 和 **show logging config** 命令的显示内容也会有所变化。

启用日志信息时间戳开关

缺省情况下，系统日志使用的格式为 datetime 格式，且 datetime 时间戳格式没有携带年份和毫秒信息。

使用 **service timestamps** 命令在全局配置模式下打开系统日志的 datetime 格式的时间戳的年份和毫秒信息，或者将系统日志的格式修订成 uptime 格式。

启用日志信息系统名称开关

缺省情况下，系统输出的日志信息没有携带 sysname（系统名称）。

使用 **service sysname** 命令在全局配置模式下开启系统日志的 sysname（系统名称）。

启用日志信息序列号开关

缺省情况下，系统输出的日志信息没有携带序列号。

使用 **service sequence-numbers** 命令在全局配置模式下开启日志信息的序列号。

启用标准日志格式显示开关

缺省情况下，设备上面的日志信息显示格式如下：

```
*timestamp: %module-level-mnemonic: content
```

依次为：

```
*时间戳：%模块名-级别-助记符：日志文本。
```

使用 **service standard-syslog** 命令在全局配置模式下开启标准日志格式显示开关，开启标准日志格式显示开关后，设备输出的日志信息显示格式如下：

```
timestamp %module-level-mnemonic: content
```

与缺省情况相比，标准日志格式的时间戳中前面少了一个 ‘ * ‘、后面少了一个 ‘:’

启用私有日志格式显示开关

缺省情况下，设备上面的日志信息显示格式如下：

```
*timestamp: %module-level-mnemonic: content
```

依次是：

```
*时间戳：%模块名-级别-助记符：日志文本。
```

使用 **service private-syslog** 命令在全局配置模式下开启私有日志格式显示开关，开启私有日志格式显示开关后，设备输出的日志信息显示格式如下：

```
timestamp module-level-mnemonic: content
```

与缺省情况相比，私有日志格式的时间戳中前面少了一个 ‘ * ’ 、后面少了一个 ‘ : ’ ，模块名前面少了一个 ‘%’

6.3.3 系统日志信息设置

用于设置日志信息输出各个方向的参数信息，主要包括：日志信息输出控制台参数信息、日志信息输出监视终端参数信息、日志信息写入内存缓冲区参数信息、日志信息发往日志服务器参数信息、日志信息写入日志文件参数信息等。

相关配置

↘ 设置日志信息速率控制功能

缺省情况下，日志信息不进行速率限制。

使用 **logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]命令在全局配置模式下设置日志信息速率限制功能，限制每秒内允许输出的日志信息。

↘ 设置日志信息输出控制台的级别

缺省情况下，日志信息输出到控制台的级别为 debugging （7 级）。

使用命令 **logging console** [*level*]命令在全局配置模式下设置允许在控制台上显示的日志信息级别。

↘ 设备允许日志信息输出到监视终端

缺省情况下，日志信息不允许输出到监视终端。

使用命令 **terminal monitor** 命令在特权模式下设置允许将日志信息输出到监视终端。

↘ 设置日志信息输出到监视终端的级别

缺省情况下，日志信息输出到监视终端的级别为 debugging （7 级）。

使用命令 **logging monitor** [*level*]命令在全局配置模式下设置允许在监视终端上输出的日志信息级别。

↘ 设置日志信息写入到内存缓冲区的参数

缺省情况下，日志信息默认会写入到内存缓冲区，且默认级别为 debugging （7 级）。

使用 **logging buffered** [*buffer-size*] [*level*]命令在全局配置模式下设置日志写入的内存缓冲区的参数（包括缓冲区大小、日志信息等级）。

↘ 设置日志信息发送往日志服务器

缺省情况下，日志信息不会发往日志服务器。

使用 **logging server**] { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*]命令在全局配置模式下设置日志发往指定的日志服务器。

↘ 设置日志信息发往日志服务器的级别

缺省情况下，日志信息发往日志服务器的级别为 informational（6 级）。

使用命令 **logging trap** [*level*]命令在全局配置模式下设置允许发往日志服务器的日志信息级别。

↘ 设置日志信息发往日志服务器的设备值

在没有开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local7（23）；在开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local0（16）。

使用 **logging facility** *facility-type* 命令在全局配置模式下设置发往日志服务器的日志信息的系统设备值。

↘ 设置发往日志服务器的日志报文源地址

缺省情况下，发往 Syslog Server 的日志报文源地址为发送报文接口的 IP 地址。

使用 **logging source** [**interface**] *interface-type interface-number* 命令设置日志报文的源接口。倘若设备上未配置该源接口、或该源接口上未配置 IP 地址，则日志报文源地址也仍为发送报文接口的 IP 地址。

使用 **logging source** { **ip** *ip-address* | **ipv6** *ipv6-address* }命令设置日志报文的源 IP 地址。倘若设备上未配置该 IP 地址，则日志报文源 IP 地址仍为发送报文接口的 IP 地址。

↘ 设置日志信息写入到日志文件参数

缺省情况下，日志信息不会写入日志文件中，开启日志信息写文件功能后，默认的级别为 informational（6 级）。

使用 **logging file flash:***filename* [*max-file-size*] [level]命令在全局配置模式下设置日志信息写入的日志文件参数（包括文件存储的设备类型、文件名称、文件大小、日志信息等级）。

↘ 设置日志信息写入到日志文件的时间间隔

缺省情况下，日志信息写入日志文件的时间间隔为 3600 秒（1 小时）。

使用 **logging flash interval** *seconds* 命令在全局配置模式下设置日志信息写入日志文件的时间间隔。

↘ 设置日志信息写入到日志文件的保存时间

缺省情况下，系统对日志文件的保存时间是没有限制的。

使用 **logging life-time level** *level days* 命令在全局配置模式下设置日志信息的保存时间，方便管理员针对不同级别的日志信息指定不同的保存天数。

↘ 设置将缓冲区当中的日志信息立即写入到日志文件中

缺省情况下，设备产生的日志信息会先缓存在系统日志缓冲区中，只有当缓冲区满或定时器到期后，才会将缓冲区中的日志信息写入到日志文件中。

使用 **logging flash flush** 命令在全局配置模式下将系统缓冲区中的日志信息立即写入到日志文件中，方便用户进行日志信息收集。

6.3.4 系统日志过滤功能设置

缺省情况下，系统打出来的日志信息都可以输出到各个方向，当某些情况下，用户可能不关心某些日志信息或者只关心某些日志信息，则可以使用日志过滤功能，对该日志信息进行过滤。

工作原理

↘ 过滤方向

日志过滤方向主要分为以下四类：

- **buffer**：代表过滤掉去向日志缓冲区的日志信息（即 **show logging** 显示出来的日志信息）；
- **file**：代表过滤掉去向日志文件的日志信息；
- **server**：代表过滤掉去向日志服务器的日志信息；
- **terminal**：代表过滤掉去向控制台和监视终端（包括 Telnet/SSH 等）的日志信息；

以上四类过滤方向为或（|）关系，即可以联合使用（对往多个方向的日志信息进行过滤），也可以单独使用（只对往某一方向的日志信息进行过滤）。

↘ 过滤方式

日志过滤方式主要分为以下两种：

- **contains-only**：代表“只包含”，意思是：只输出包含在过滤规则里面的关键字的日志信息，其它没有包含在过滤规则里面的关键字的日志信息不会输出。某些情况下，用户可能只关心某些日志信息是否产生，则可以在设备上面应用“只包含”这一日志过滤类型，让包含了此规则的日志信息才输出到终端界面，方便用于观察某些事件是否有发生。
- **filter-only**：代表“只过滤”，意思是：将过滤掉包含在过滤规则里面的关键字的日志信息，不会输出这些过滤掉的日志信息。某些情况下，当遇到某一个模块打出来的日志信息太多，可能会引起终端界面出现刷屏，且用户又不关心此类日志信息的时候，可以在设备上面应用“只过滤”这一日志过滤类型，并配置对应的过滤规则，将刷屏的日志信息过滤掉。

以上两种过滤方式为互斥关系，即同一时刻只能配置一种过滤方式。

↘ 过滤规则

日志过滤规则主要分为以下两种：

- **exact-match**：代表精确匹配，若选择精确匹配，则后面的三个过滤选项（日志模块名、日志等级、日志助记符）都需要选上。某些情况下，用户可能只想过滤掉某一特定的日志信息，则可以使用“精确匹配”规则。
- **single-match**：代表单个匹配，若选择单个匹配，则后面的三个过滤选项（日志模块名、日志等级、日志助记符）只需要选择其中的一个。某些情况下，用户可能想过滤掉某一类型的日志信息，则可以使用“单个匹配”规则。

当用户配置的日志信息过滤规则中，若“单个匹配”规则和“精确匹配”规则中同时配置了一样的模块名、助记符或信息等级，则单个匹配规避的优先级高于精确匹配。

相关配置

↘ 设置日志信息的过滤方向

缺省情况下，日志信息的过滤方向为 all，即过滤去往所有方向的日志信息。

使用 **logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }命令在全局配置模式下设置日志信息的过滤方向，指定过滤去往哪几个方向的日志信息。

↘ 设置日志信息的过滤方式

缺省情况下，日志信息的过滤方式为“只过滤”。

使用 **logging filter type** { **contains-only** | **filter-only** }命令在全局配置模式下设置日志信息的过滤方式。

↘ 设置日志信息的过滤规则

缺省情况下，设备上面没有配置日志信息的过滤规则，不对日志信息进行过滤。

使用 **logging filter rule exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* 命令在全局配置模式下设置日志信息的“精确匹配”过滤规则。

使用 **logging filter rule single-match** { **level** *level* **| mnemonic** *mnemonic-name* | **module** *module-name* }命令在全局配置模式下设置日志信息的“单个匹配”过滤规则。

6.3.5 系统日志上送功能设置

日志上送功能分为分级上送、延迟上送及定时上送。在开启 RFC5424 日志格式的情况下，缺省情况下是可以往所有方向输出，并且打开日志延迟上送功能及关闭了定时上送功能；在没有开启 RFC5424 日志开关的情况下，分级上送、延迟上送、定时上送功能均不生效。

工作原理

↘ 分级上送

用户可以使用分级策略功能，将不同模块和严重级别的日志输出到不同目的地，例如：可以在命令行中配置，WLAN 模块的严重级别小于等于 4 的日志，实时发送到日志服务器；同时，WLAN 模块的严重级别大于等于 5 的日志，输出到本地日志文件中。

↘ 延迟上送

所谓的日志延迟上送功能是指：当日志触发后，不直接发送给日志服务器，而是由设备暂时缓存在日志文件中，设备每隔一定时间间隔，主动将日志文件通过 FTP 协议上传到 SYSLOG 服务器。

日志延迟发送功能主要用于：设备产生的日志信息量可能非常庞大，如果全部日志信息实时上送给服务器，设备和 SYSLOG 服务器都会存在性能压力，并对中间网络也会造成负担，而通过延迟上送给服务器的方式可以减少报文传输交互频率。

默认情况下，发送到远端服务器的日志文件名为：文件大小_设备 IP 地址_索引值.txt，若修改延迟上送的文件名，则发送到远端服务器的日志文件名为：配置的文件名前缀_文件大小_设备 IP 地址_索引值.txt；而保存在设备本地 Flash 的文件名则为：配置的文件名前缀_索引值.txt。默认的文件名前缀为 syslog_ftp_server，延迟上送的时间间隔是 3600 秒（1 小时），日志文件大小为 128K。

鉴于日志延迟上送的时间间隔最大可以设置成 65535 秒，即 18 小时，若用户将延迟上送时间间隔配置为较大的值，此时间间隔内产生的日志有可能超过一个文件的大小（128K），为了防止日志丢失，会写一个新的日志文件，并把索引值加 1，等到定时器到期后，会一次性把该时间间隔内缓存的所有日志文件发送到 FTP 或 TFTP 服务器。

由于设备上面用于缓存在本地日志文件的 Flash 空间大小有限，所以限制缓存在设备本地的日志文件个数最多为 8 个，在定时器到期之前，若缓存在设备本地的日志文件超过 8 个，则会先把之前产生的日志文件一次性发送到 FTP 或 TFTP 服务器。

↘ 定时上送

定时上送的日志主要是指设备性能统计数据的日志信息。定时上送的所有定时器都由 SYSLOG 模块统一管理，定时器到期，SYSLOG 模块就会调用各模块注册上来的日志处理函数，打印设备的性能统计日志，并实时发送给远端的 SYSLOG 服务器，服务器通过分析这些定时上送的日志来评估设备的性能。

日志定时上送的时间间隔默认为 15 分钟，为了使服务器能在同一时间点上收集到设备上的所有的性能统计日志，需要把不同统计对象的日志定时上送时间间隔设置成倍数关系，目前支持的配置值有 5 个，分别为：0、15、30、60、120，其中 0 代表关闭此统计对象的定时上送功能。

相关配置

↘ 设置日志分级上送策略

缺省情况下，设备日志是可以输出到所有方向。

使用 **logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }命令在全局配置模式下配置日志分级上报时所使用的分级策略。

↘ 设置延时上送日志输出到控制台和远程终端开关

缺省情况下，延时上送的日志输出到控制台和远程终端的开关是关闭的。

使用 **logging delay-send terminal** 命令在全局配置模式下打开延时上送日志输出到控制台和远程终端。

↘ 设置延时上送日志发往服务器的文件名

缺省情况下，发送到远端服务器的日志文件名为：文件大小_设备 IP 地址_索引值.txt，若修改延迟上送的文件名前缀，则发送到远端服务器的日志文件名为：配置的文件名前缀_文件大小_设备 IP 地址_索引值.txt；而保存在设备本地 Flash 的文件名则为：配置的文件名前缀_索引值.txt，默认的文件名前缀为 syslog_ftp_server。

使用 **logging delay-send file flash:***filename* 命令在全局配置模式下配置延迟上送时缓存在设备本地的日志文件名。

↘ 设置延时上送日志发往服务器的时间间隔

缺省情况下，发往远端服务器的时间间隔是 3600 秒（1 小时）。

使用 **logging delay-send interval** *seconds* 命令在全局配置模式下配置延迟上送的时间间隔。

↘ 设置延时上送日志发往服务器的地址和上报方式

缺省情况下，不向任何 FTP 或者 TFTP Server 发送日志信息。

使用 **logging delay-send server** { *ip-address* | **ipv6** *ipv6-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }命令在全局配置模式下配置日志延迟上送给服务器的地址和上报方式。

↘ 日志定时上送功能开关

缺省情况下，日志定时上送功能是关闭的。

使用 **logging statistic enable** 命令在全局配置模式下开启日志定时上送功能，打开日志定时上送功能后，系统将按一定的时间间隔输出一系列的性能统计数据，方便日志服务器对系统的性能进行跟踪。

↘ 设置定时上送日志输出到控制台和远程终端开关

缺省情况下，定时上送的日志输出到控制台和远程终端的开关是关闭的。

使用 **logging statistic terminal** 命令在全局配置模式下打开定时上送日志（系统性能统计日志）输出到控制台和远程终端。

↘ 设置定时上送的时间间隔

缺省情况下，所有统计对象的定时上送时间间隔都是 15 分钟。

使用 **logging statistic mnemonic** *mnemonic* **interval** *minutes* 命令在全局配置模式下配置日志定时上送的时间间隔。

6.3.6 系统日志监控功能设置

打开日志监控功能后，系统将对外界连接到设备的行为进行监控，并记录对应的 LOG 信息。

工作原理

在设备上面开启记录用户登录或退出 LOG 信息后，系统将对外界连接到设备的行为进行记录，记录的信息包括：登录的用户名、登录的源地址等。

在设备上面开启记录用户操作的 LOG 信息，系统将对修改设备配置的行为进行记录，记录的信息包括：操作的用户名、操作的源地址、操作的内容。

相关配置

↘ 设置用户登录或退出 LOG 信息

缺省情况下，用户登录或退出设备的时候，设备是不会记录相关的 Log 信息。

使用 **logging userinfo** 命令在全局配置模式下设置用户登录/退出的 Log 信息。设置此功能后，当外界通过 Telnet、SSH、HTTP 等方式连接到设备时，设备将打出对应的 Log 信息，方便管理员监控设备的连接情况。

↘ 设置用户操作的 LOG 信息

缺省情况下，用户修订设备配置的时候，设备是不会记录相关的操作 Log 信息。

使用**logging userinfo command-log**命令在全局配置模式下设置用户操作的Log信息。设置此功能后，当有用户修改设备配置时，系统就会打出相应的 Log 信息提醒设备管理员。

6.4 配置详解

配置项	配置建议&相关命令	
配置系统日志的显示格式	⚠ 可选配置，用于设置系统日志的显示格式	
	service timestamps [*message-type* [**uptime**| **datetime** [**msec**] [**year**]]]	设置系统日志的时间戳格式
	service sysname	设置系统日志格式中添加系统名称

	service sequence-numbers	设置系统日志格式中添加系列号
	service standard-syslog	设备系统日志格式为标准日志格式
	service private-syslog	设备系统日志格式为私有日志格式
	service log-format rfc5424	设备系统日志格式为 RFC5424 日志格式
配置系统日志输出到控制台	⚠ 可选配置，用于设置系统日志输出到控制台的参数信息	
	logging on	打开日志开关
	logging count	打开日志信息统计功能
	logging console [*level*]	设置日志信息允许输出到控制台的级别
	logging rate-limit { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]	设置日志信息速率限制功能
配置系统日志输出到监视终端	⚠ 可选配置，用于设置系统日志输出监视终端的参数信息	
	terminal monitor	允许在当前监视终端上显示日志信息
	logging monitor [*level*]	设置日志信息允许输出到监视终端的级别
配置系统日志写入到内存缓冲区	⚠ 可选择配置，用于设置系统日志写入内存缓冲区的参数信息	
	logging buffered [*buffer-size*] [*level*]	设置日志写入的内存缓冲区的参数(包括缓冲区大小、日志信息等级)
配置系统日志发送往日志服务器	⚠ 可选配置，用于设置系统日志发送到日志服务器的参数信息	
	logging server { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*]	设置日志发往指定的日志服务器
	logging trap [*level*]	设置允许发往日志服务器的日志级别
	logging facility *facility-type*	设置发往服务器的日志信息的系统设备值
	logging source [**interface**] *interface-type interface-number*	设置发往服务器的日志信息的源接口
	logging source { **ip** *ip-address* | **ipv6** *ipv6-address* }	设置发往服务器的日志信息的源地址
配置系统日志写入到日志文件	⚠ 可选配置，用于设置系统日志写入文件的参数信息	
	logging file flash:*filename* [*max-file-size*] [level]	设置日志信息写入的文件参数（包括文件存储的类型、文件名称、文件大小、日志信息等级）
	logging flash interval *seconds*	设置日志信息写入文件的频率 ,缺省值为 3600
	logging life-time level *level days*	设置日志信息写入文件的保存时间
配置系统日志过滤功能	⚠ 可选配置，用于设置系统日志的过滤功能参数信息	
	logging filter direction { **all** | **buffer** | **file** | **server** | **terminal** }	设置日志信息的过滤方向
	logging filter type { **contains-only** | **filter-only** }	设置日志信息的过滤方式

	logging filter rule exact-match module *module-name* **mnemonic** *mnemonic-name* **level** *level*	设置日志信息的“精确匹配”过滤规则
	logging filter rule single-match { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* }	设置日志信息的“单个匹配”过滤规则
配置系统日志分级上送功能	⚠ 可选配置，用于设置系统日志分级上送功能的参数信息	
	logging policy module *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }	配置按模块和严重级别将日志输出到不同目的地
配置系统日志延迟上送功能	⚠ 可选配置，用于设置系统日志延迟上送功能的参数信息	
	logging delay-send terminal	打开延时上送的日志输出到控制台和远程终端
	logging delay-send file flash:*filename*	配置延迟上送时缓存在设备本地的日志文件名
	logging delay-send interval *seconds*	配置日志延迟上送给服务器的时间间隔
	logging delay-send server { *ip-address* | **ipv6** *ipv6-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }	配置日志延迟上送的服务器地址和上报方式
配置系统日志定时上送功能	⚠ 可选配置，用于设置系统日志定时上送功能的参数信息	
	logging statistic enable	打开日志定时上送功能
	logging statistic terminal	打开定时上送的日志输出到控制台和远程终端
	logging statistic mnemonic *mnemonic* **interval** *minutes*	配置系统某个性能统计对象的定时上报时间间隔
配置系统日志监控功能	⚠ 可选配置，用于设置系统日志的监控功能参数信息	
	logging userinfo	开启记录用户登录/退出的日志信息
	logging userinfo command-log	开启记录用户操作的日志信息

6.4.1 配置系统日志的显示格式

配置效果

- 调整系统日志的显示格式。

注意事项

↘ **RFC3164 日志格式**

- 如果当前设备不存在 RTC 时钟（一种用于记录系统绝对时间的硬件装置），系统缺省采用设备启动时间（**uptime** 格式）作为日志信息时间戳，此时配置设备时间无效，如果设备存在 RTC 时钟，则缺省采用设备时间（**datetime** 格式）作为日志信息时间戳。
- 日志序列号是一个长整型数值，每产生一条日志，序列号就递增，但是由于日志序列号只显示6位整数，故当序列号从1开始每增加到 1000000 或序列号到达 2^32 时候就会发生一次翻转，即序列号又从 000000 开始显示。

RFC5424 日志格式

- 开启 RFC5424 日志格式后，日志时间戳统一成一种格式，不再区分 **uptime** 格式和 **datetime** 格式。
- RFC5424 日志格式中时间戳格式包括有时区和没有时区两种，当前只支持没有时区的显示格式。

配置方法

设置系统日志的时间戳格式

- 可选配置，缺省情况下系统日志的时间戳采用 **datetime** 格式。
- 若无特殊要求，在需要设置系统日志时间戳格式的设备上面配置。

设置系统日志格式中添加系统名称

- 可选配置，缺省情况下系统日志的格式中没有添加系统名称。
- 若无特殊要求，在需要为日志格式中添加系统名称的设备上面配置。

设置系统日志格式中添加系列号

- 可选配置，缺省情况下系统日志的格式中没有添加系列号。
- 若无特殊要求，在需要为日志格式添加序列号的设备上面配置。

设置系统日志格式为标准日志格式

- 可选配置，缺省情况下系统日志的格式中为默认格式。
- 若无特殊要求，在需要使用标准日志格式的设备上面配置。

设置系统日志格式为私有日志格式

- 可选配置，缺省情况下系统日志的格式中为默认格式。
- 若无特殊要求，在需要使用私有日志格式的设备上面配置。

设置系统日志格式为 RFC5424 日志格式

- 可选配置，缺省情况下系统关闭 RFC5424 日志格式。
- 若无特殊要求，在需要使用 RFC5424 日志格式的设备上面配置。

检验方法

- 通过触发系统产生一条日志信息，用于查看设置后的系统日志的显示格式。

相关命令

设置系统日志的时间戳格式

【命令格式】 **service timestamps** [*message-type* [**uptime** | **datetime** [**msec**] [**year**]]]

【参数说明】 *message-type*：日志类型，有两种 log 和 debug

uptime：设备启动时间，格式：*天*小时*分*秒，例：07:00:10:41

datetime：当前设备日期，格式：月 日期 时：分：秒，例：Jul 27 16:53:07

msec：当前设备日期支持毫秒显示

year：当前设备日期支持年份显示

【命令模式】 全局配置模式

【使用指导】 系统日志的时间戳格式有两种：设备启动时间(**uptime**)格式或者设备日期(**datetime**)格式，用户可以根据需要选择不同类型的时间戳格式。

设置系统日志格式中添加系统名称

【命令格式】 **service sysname**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 可以在日志信息中系统名称，加上系统名称以后，系统日志发送到服务器后，在服务器上，可以清楚地知道日志信息来自哪个设备。

设置系统日志格式中添加系列号

【命令格式】 **service sequence-numbers**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 可以在日志信息中加上序列号，序列号从 1 开始。加上序号以后，就可以非常清楚地知道日志信息有没有丢失，以及日志产生的先后顺序。

设置系统日志格式为标准日志格式

【命令格式】 **service standard-syslog**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 默认情况下，设备上面的日志信息显示格式如下（默认格式）：

```
*timestamp: %module-level-mnemonic: content
```

依次是：

```
*时间戳: %模块名-级别-助记符: 日志文本。
```

若打开标准日志格式显示功能，设备上面的日志信息显示格式如下：

```
timestamp %module-level-mnemonic: content
```

与缺省情况相比，标准日志格式的时间戳中前面少了一个 ‘*’、后面少了一个 ‘:’

设置系统日志格式为私有日志格式

【命令格式】 **service private-syslog**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 默认情况下，设备上面的日志信息显示格式如下（默认格式）：

```
*timestamp: %module-level-mnemonic: content
```

依次是：

*时间戳：%模块名-级别-助记符：日志文本。

若打开标准日志格式显示功能，设备上面的日志信息显示格式如下：

```
timestamp module-level-mnemonic: content
```

与缺省情况相比，私有日志格式的时间戳中前面少了一个'*'、后面少了一个':'，模块名前面少了一个'%'

设置系统日志格式为 RFC5424 日志格式

【命令格式】 **service log-format rfc5424**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】

切换成 RFC5424 日志格式后，旧日志格式中的命令 **service sequence-numbers**、**service sysname**、**service timestamps**、**service private-syslog**、**service standard-syslog** 将会失效并隐藏掉。

切换到旧的日志格式，则在 RFC5424 日志格式中使用的命令 **logging delay-send**、**logging policy**、**logging statistic** 将会失效并隐藏掉。

在新旧日志格式切换之后，**show logging** 和 **show logging config** 的命令的显示内容将会有所变化。

配置举例

配置 RFC3164 日志显示格式

【网络环境】 假设网络环境中，有以下日志时间戳格式设置要求：

1、切换日志格式为 RFC3164 格式；

2、日志时间戳格式调整为 **datetime** 格式，并且开启毫秒信息和年份信息的显示；

3、日志时间戳格式中要求添加系统名称；

4、日志时间戳格式中要求添加系列号。

【配置方法】

- 在设备上面配置系统日志的显示格式

```
Ruijie# configure terminal
Ruijie(config)# no service log-format rfc5424
Ruijie(config)# service timestamps log datetime year msec
Ruijie(config)# service timestamps debug datetime year msec
Ruijie(config)# service sysname
Ruijie(config)# service sequence-numbers
```

【检验方法】 用户设置了日志时间戳格式后，在系统新产生日志信息的时候，将会依据所设置的时间戳格式进行日志信息的构造和输出。

- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。
- 通过进入/退出全局配置模式触发产生一条新的日志信息，可以观察新产生的日志信息的时间戳格式。

```
Ruijie(config)#exit
001302: *Jun 14 2013 19:01:40.293: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on console
Ruijie#show logging config
Syslog logging: enabled
  Console logging: level informational, 1306 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level informational, 1306 messages logged
  File logging: level informational, 121 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 121 message lines logged,0 fail
```

配置 RFC5424 日志显示格式

【网络环境】 假设网络环境中，需要切换 RFC5424 日志格式要求：

1、切换日志格式为 RFC5424 格式。

【配置方法】

- 在设备上面配置系统日志的显示格式

```
Ruijie# configure terminal
Ruijie(config)# service log-format rfc5424
```

【检验方法】 用户把日志格式切换为 RFC5424 格式，设备日志就会按照 RFC5424 格式输出。

- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。
- 通过进入/退出全局配置模式触发产生一条新的日志信息，可以观察新产生的日志信息的格式。

```
Ruijie(config)#exit
<133>1 2013-07-24T12:19:33.130290Z ruijie SYS 5 CONFIG - Configured from console by console
Ruijie#show logging config

Syslog logging: enabled

  Console logging: level debugging, 4740 messages logged

  Monitor logging: level debugging, 0 messages logged

  Buffer logging: level debugging, 4745 messages logged
```

```
  Statistic log messages: disable
  Statistic log messages to terminal: disable
  Delay-send file name:syslog_ftp_server, Current write index:3, Current send index:3, Cycle:10
seconds
  Count log messages: enable
  Trap logging: level informational, 2641 message lines logged,4155 fail
    logging to  192.168.23.89
    logging to  2000::1
  Delay-send logging: 2641 message lines logged
    logging to  192.168.23.89  by tftp
```

6.4.2 配置系统日志输出到控制台

配置效果

- 可以将系统产生的日志信息输出到控制台，方便管理员监控系统的运行状态。

注意事项

- 如果系统产生的日志信息太多，则可以通过限制日志信息的速率来减少输出到控制台日志信息。

配置方法

↘ 打开日志开关

- 可选配置，缺省情况下系统日志开关已经打开。

↘ 打开日志信息统计功能

- 可选配置，缺省情况下系统日志信息统计功能是关闭的。
- 若无特殊要求，在需要打开日志信息统计功能的设备上面配置。

↘ 设置日志信息允许输出控制台的级别

- 可选配置，缺省级别为 debugging（7 级）。
- 若无特殊要求，在需要设置日志信息允许输出控制台级别的设备上面配置。

↘ 设置日志信息速率限制功能

- 可选配置，缺省情况下不进行速率限制。

- 若无特殊要求，在需要设置日志信息速率限制功能的设备上面配置。

检验方法

- 通过 **show logging config** 命令可以查看设置的允许输出控制台的日志级别参数。

相关命令

打开日志开关

【命令格式】 **logging on**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 缺省情况下，系统日志开关是打开的，一般情况下，不要关闭日志开关，如果觉得打印的信息太多，则可以通过设置不同设备日志信息的显示级别来减少日志信息的打印。

打开日志信息统计功能

【命令格式】 **logging count**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 缺省情况下，系统日志信息统计功能是关闭的。启用了日志报文统计功能后，从命令打开时将对系统中输出的日志信息进行分类统计，主要记录日志信息的产生次数，以及最后产生的时间等。

设置日志信息允许输出到控制台的级别

【命令格式】 **logging console** [*level*]

【参数说明】 *level*：日志信息的级别

【命令模式】 全局配置模式

【使用指导】 控制台默认允许显示的日志信息级别为 debugging（7 级）。可以通过特权命令 **show logging config** 来查看允许在控制台上显示的日志信息级别。

设置日志信息速率限制功能

【命令格式】 **logging rate-limit** { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]

【参数说明】 *number*：每秒钟内允许处理的日志信息，范围为 1~10000。

all：设置对所有的日志信息进行速率控制，包括 0~7 级所有日志信息。

console：设置每秒钟内允许在控制台上显示的日志信息数。

except *severity* :小于等于此严重性级别的日志信息 ,不进行速率控制 ;默认级别为 error(3) ,对小于等于 error 级别的日志信息不进行速率控制。

【命令模式】 全局配置模式

【使用指导】 默认情况下，不对日志信息进行速率限制。

配置举例

↘ 配置系统日志输出到控制台

【网络环境】 假设网络环境中，有以下日志输出控制台格式要求：

1、打开日志信息统计功能；

2、设置允许输出到控制台的日志信息级别为 informational（6 级）；

3、设置日志信息输出到控制台的速率为每秒 50 条；

【配置方法】

- 在设备上面配置系统日志输出到控制台

```
Ruijie# configure terminal
Ruijie(config)# logging count
Ruijie(config)# logging console informational
Ruijie(config)# logging rate-limit console 50
```

【检验方法】

- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。

```
Ruijie(config)#show logging config
Syslog logging: enabled
  Console logging: level informational, 1303 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 1303 messages logged
  File logging: level informational, 118 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 118 message lines logged,0 fail
```

6.4.3 配置系统日志输出到监视终端

配置效果

- 可以将系统产生的日志信息输出到远程监视终端，方便管理员监控系统的运行状态。

注意事项

- 如果系统产生的日志信息太多，则可以通过限制日志信息的速率来减少输出到监视终端的日志信息。
- 默认情况下，用户远程连接到设备后，当前监视终端上不允许输出日志信息。需要手动输入 **terminal monitor** 命令开启当前终端的日志信息输出功能。

配置方法

允许在当前监视终端上显示日志信息

- 必选配置，缺省情况下不允许在监视终端上显示日志信息。
- 若无特殊要求，应在每个连接到设备的监视终端配置。

设置日志信息允许输出到监视终端的级别

- 可选配置，缺省级别为 debugging（7 级）。
- 若无特殊要求，在需要设置日志信息允许输出到监视终端级别的设备上面配置。

检验方法

- 通过 **show logging config** 命令可以查看设置的允许输出到监视终的日志级别参数。

相关命令

允许在当前监视终端上显示日志信息

【命令格式】 **terminal monitor**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 默认情况下，用户远程连接到设备后，当前监视终端上不允许输出日志信息。需要手动输入 **terminal monitor** 命令开启当前终端的日志信息输出功能。

设置日志信息允许输出到监视终端的级别

【命令格式】 **logging monitor** [*level*]

【参数说明】 *level*：日志信息的级别

【命令模式】 全局配置模式

【使用指导】 监视终端默认允许显示的日志信息级别为 debugging（7 级）。

可以通过特权命令 **show logging config** 来查看允许在监视终端上显示的日志信息级别。

配置举例

配置系统日志输出到监视终端

【网络环境】 假设网络环境中，有以下日志信息输出到监视终端设置要求：

1、设置允许在监视终端上显示日志信息；

2、设置允许输出到控制台的日志信息级别为 informational（6 级）。

【配置方法】

- 在设备上面配置系统日志输出到监视终端

```
Ruijie# configure terminal
Ruijie(config)# logging monitor informational
Ruijie(config)# line vty 0 4
Ruijie(config-line)# monitor
```

【检验方法】

- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。

```
Ruijie#show logging config
Syslog logging: enabled
  Console logging: level informational, 1304 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level debugging, 1304 messages logged
  File logging: level informational, 119 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 119 message lines logged,0 fail
```

常见错误

- 若要取消当前终端的日志信息输出功能，需要使用的命令是：**terminal no monitor**，而不是 **no terminal monitor**。

6.4.4 配置系统日志写入到内存缓冲区

配置效果

- 可以将系统产生的日志信息写入到内存缓冲区，方便管理员通过 **show logging** 命令查看近期系统产生的日志信息。

注意事项

- 系统日志写入内存缓冲区后，当缓冲区满时，将循环覆盖重写。

配置方法

↘ 设置日志写入的内存缓冲区的参数

- 可选配置，缺省情况下系统会将日志信息写入到内存缓冲区，且默认级别为 debugging（7 级）。

- 若无特殊要求，在需要设置日志写入内存缓冲区级别的设备上面配置。

检验方法

- 通过 **show logging config** 命令可以查看设置的允许写入内存缓冲区的日志级别参数。
- 通过 **show logging** 命令可以查看系统写入内存缓冲区的日志信息。

相关命令

↘ 设置日志写入的内存缓冲区的参数

【命令格式】 **logging buffered** [*buffer-size*] [*level*]

【参数说明】 *buffer-size*：内存缓冲的大小

level：允许写入到内存缓冲区的信息级别

【命令模式】 全局配置模式

【使用指导】 默认写入内存缓冲区的日志信息级别为 debugging（7 级）。

可以通过特权命令 **show logging** 来查看允许写入内存缓冲区的日志信息级别和缓冲的大小等参数信息。

配置举例

↘ 配置系统日志写入到内存缓冲区的参数

【网络环境】 假设网络环境中，有以下日志信息写入到内存缓冲区设置要求：

1、设置日志内存缓冲区的大小为 128K（131072 字节）；

2、设置允许写入到内存缓冲区的日志信息级别为 informational（6 级）。

【配置方法】

- 在设备上面配置系统日志写入到内存缓冲区参数信息

```
Ruijie# configure terminal
Ruijie(config)# logging buffered 131072 informational
```

【检验方法】

- 通过 **show logging** 命令可以查看用户配置的相关参数信息及系统最近产生的日志信息。

```
Ruijie#show logging
Syslog logging: enabled
  Console logging: level informational, 1306 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level informational, 1306 messages logged
  File logging: level informational, 121 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
  Timestamp debug messages: datetime
  Timestamp log messages: datetime
  Sequence-number log messages: enable
```

```
  Sysname log messages: enable
  Count log messages: enable
  Trap logging: level informational, 121 message lines logged,0 fail
Log Buffer (Total 131072 Bytes): have written 4200
001301: *Jun 14 2013 19:01:09.488: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on
console
001302: *Jun 14 2013 19:01:40.293: Ruijie %SYS-5-CONFIG_I: Configured from console by admin on
console
// 这里省略其它日志信息，客户 show logging 时以实际为准。
```

6.4.5 配置系统日志发送往日志服务器

配置效果

- 可以将系统产生的日志信息发送往日志服务器，方便管理员在服务器上统一监控设备的日志信息。

注意事项

- 要将日志信息发送给日志服务器，必须打开日志信息的时间戳开关或序列号开关，否则日志信息将不会发给日志服务器。

配置方法

↘ 设置日志发往指定的日志服务器

- 必选配置，缺省情况下系统产生的日志信息不会发送日志服务器。
- 若无特殊要求，应在每台设备上面配置。

↘ 设置日志信息允许发往日志服务器的级别

- 可选配置，缺省情况下系统发往日志服务器的日志级别为 informational（6 级）。
- 若无特殊要求，在需要设置日志信息允许发往日志服务器级别的设备上面配置。

↘ 设置发往服务器的日志信息的系统设备值

- 可选配置，在没有开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local7（23）；在开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local0（16）。
- 若无特殊要求，在需要设置发往服务器的日志信息的系统设备值的设备上面配置。

↘ 设置发往服务器的日志信息的源接口

- 可选配置，缺省情况下发往日志服务器的日志报文源地址为发送报文接口的 IP 地址。

- 若无特殊要求，在需要设备发往服务器的日志信息的源接口的设备上面配置。

设置发往服务器的日志信息的源地址

- 可选配置，缺省情况下发往日志服务器的日志报文源地址为发送报文接口的 IP 地址。
- 若无特殊要求，在需要设置发往服务器的日志信息的源地址的设备上面配置。

检验方法

- 通过 **show logging config** 命令可以查看设置的日志服务器参数信息

相关命令

设置日志发往指定的日志服务器

【命令格式】 **logging server** { *ip-address* | **ipv6** *ipv6-address* } [**udp-prot** *port*]
或 **logging** { *ip-address* | **ipv6** *ipv6-address* } [**udp-prot** *port*]

【参数说明】 *ip-address*：接收日志信息的主机 IP 地址
ipv6 *ipv6-address*：指定接收日志信息的主机 IPV6 地址
udp-port *port*：指定日志主机的端口号（默认端口号为 514）

【命令模式】 全局配置模式

【使用指导】 该命令用于指定接收日志信息的日志服务器地址，可以同时指定多个日志服务器，日志信息将被同时分给配置的所有的日志服务器。

锐捷产品允许配置最多 5 个日志服务器。

设置日志信息允许发往日志服务器的级别

【命令格式】 **logging trap** [*level*]

【参数说明】 *level*：日志信息的级别

【命令模式】 全局配置模式

【使用指导】 默认发送往日志服务器的日志信息级别为 informational（6 级）。
可以通过特权命令 **show logging config** 来查看允许发送往日志服务器的级别。

设置发往服务器的日志信息的系统设备值

【命令格式】 **logging facility** *facility-type*

【参数说明】 *facility-type*：日志信息设备值

【命令模式】 全局配置模式

【使用指导】 在没有开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local7（23）；在开启 RFC5424 日志格式的情况下，日志信息发往服务器的系统设备值默认为 local0（16）。

设置发往服务器的日志信息的源接口

【命令格式】 **logging source** [**interface**] *interface-type interface-number*

【参数说明】 *interface-type*：接口类型

interface-number：接口编号

【命令模式】 全局配置模式

【使用指导】 默认情况下，发送给服务器的日志报文源 IP 地址是报文发送接口的 IP 地址。

为了便于跟踪管理，可以使用该命令将所有日志报文的源 IP 地址固定为某个接口的 IP 地址，这样管理员就通过唯一地址识别从哪台设备发送出来的日志报文，倘若设备上未配置该源接口或源接口上未配置 IP 地址，则日志报文源 IP 地址仍为报文发送接口的 IP 地址。

↘ 设置发往服务器的日志信息的源地址

【命令格式】 **logging source** { **ip** *ip-address* | **ipv6** *ipv6-address* }

【参数说明】 **ip** *ip-address*：指定向 IPV4 日志主机发送日志报文的源 IPV4 地址

ipv6 *ipv6-address*：指定向 IPV6 日志主机发送日志报文的源 IPV6 地址

【命令模式】 全局配置模式

【使用指导】 默认情况下，发送给 Syslog Server 的日志报文源 IP 地址是报文发送接口的 IP 地址。

为了便于跟踪管理，可以使用该命令将所有日志报文的源 IP 地址固定为某个 IP 地址，这样管理员就通过唯一地址识别从哪台设备发送出来的日志报文，倘若设备上未配置该 IP 地址，则日志报文源 IP 地址仍为报文发送接口的 IP 地址。

配置举例

↘ 配置系统日志发送往日志服务器

【网络环境】 假设网络环境中，有以下日志信息发送往日志服务器设置要求：

1、设置日志服务器 IPv4 地址：10.1.1.100；

2、设置允许发送到日志服务器的日志信息级别为 debugging（7 级）；

3、设置发往日志服务器的日志信息的源接口为 Loopback 0。

【配置方法】

- 在设备上面配置系统日志发送往日志服务器

```
Ruijie# configure terminal
Ruijie(config)# logging server 10.1.1.100
Ruijie(config)# logging trap debugging
Ruijie(config)# logging source interface Loopback 0
```

【检验方法】

- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。

```
Ruijie#show logging config
Syslog logging: enabled
  Console logging: level informational, 1307 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level informational, 1307 messages logged
  File logging: level informational, 122 messages logged
  File name:syslog_test.txt, size 128 Kbytes, have written 5 files
  Standard format:false
```

```
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence-number log messages: enable
Sysname log messages: enable
Count log messages: enable
Trap logging: level debugging, 122 message lines logged,0 fail
  logging to  10.1.1.100
```

6.4.6 配置系统日志写入到日志文件

配置效果

- 可以将系统产生的日志信息按指定的频率写入到日志文件，便于管理员在设备本地随时查看历史日志信息。

注意事项

- 系统产生的日志信息是先缓冲到内存缓冲区当中，然后当缓冲区的时候或定时(默认为间隔 1 小时)写入到日志文件的，并不是产生日志信息的时候就立即写入到日志文件当中。

配置方法

设置日志信息写入的日志文件参数

- 必选配置，缺省情况下系统产生的日志信息不会写入日志文件中。
- 若无特殊要求，应在每台设备上面配置。

设置日志信息写入文件的个数

- 可选配置，缺省情况下系统日志写入到文件的个数为 16。
- 若无特殊要求，在需要设置日志文件个数的设备上面配置。

设置日志信息写入文件的时间间隔

- 可选配置，缺省情况下系统日志写入到文件的时间间隔为每小时写一次。
- 若无特殊要求，在需要设置日志信息写入文件的时间间隔的设备上面配置。

设置日志信息写入文件的保存时间

- 可选配置，缺省情况下系统对日志文件的保存时间是没有限制的。
- 若无特殊要求，在需要设备日志信息写入文件的保存时间的设备上面配置。

设置将缓冲区当中的日志信息立即写入到日志文件中

- 可选配置，缺省情况下设备产生的日志信息会先缓存在系统日志缓冲区中，只有当缓冲区满或定时器到期后，才会将缓冲区中的日志信息写入到日志文件中。
- 若无特殊要求，应在用户收集日志文件的时候进行配置，且该命令配置一次作用一次，配置后立即将存在缓冲区中的日志信息写入到日志文件中。

检验方法

- 通过 **show logging config** 命令可以查看设置的日志服务器参数信息

相关命令

设置日志信息写入的日志文件参数

【命令格式】 **logging file** { **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* | **sd0**:*filename* } [*max-file-size*] [*level*]

【参数说明】 **flash**：日志文件选择保存在扩展 FLASH 当中。

usb0：日志文件选择保存在 USB0 当中，此选项需要设备具有 1 个 USB 接口时才支持，并插入扩展的 USB 设备。

usb1：日志文件选择保存在 USB1 当中，此选项需要设备具有 2 个 USB 接口时才支持，并插入扩展的 USB 设备。

sd0：日志文件选择保存在 SD 卡当中，此选项需要设备具有 SD 卡接口时才支持，并插入扩展的 SD 卡设备。

filename：日志文件名，不需要携带文件类型后缀，固定为 txt 类型。

max-file-size：日志文件的最大值。从 128K 到 6M bytes，缺省大小为 128K。

level：允许写入到日志文件的信息级别。

【命令模式】 全局配置模式

【使用指导】 该命令将在指定的文件存储设备上根据指定的文件名创建文件用于储存日志，文件大小会随日志增加而增加，但其上限以配置的 max-file-size 为准，若没有指定 max-file-size，则日志文件的大小默认为 128K。

配置该命令后，系统将日志信息保存到文件中，日志文件名不要带文件类型的后缀名。日志文件后缀为固定为 txt 类型，配置文件后缀名将被拒绝。

配置了日志写文件功能后，日志信息将间隔 1 小时，写入到文件当中，而日志文件的名称（假设此次已经配置：logging flie flash:syslog）依次为 syslog.txt、syslog_1.txt、syslog_2.txt…… syslog_14.txt、syslog_15.txt 总共 16 个日志文件。这 16 个日志文件循环重写 ,比如 :写完 syslog.txt 后 ,写 syslog_1.txt ,直至 syslog_15.txt，然后再返回来写 syslog.txt，这样子循环重写。

设置日志信息写入文件的时间间隔

【命令格式】 **logging flash interval** *seconds*

【参数说明】 *seconds*：日志信息写入到 FLASH 文件的时间间隔，范围：1~51840，单位：秒

【命令模式】 全局配置模式

【使用指导】 通过此命令设置日志信息保存到文件中的时间间隔，且从命令配置后开始计时。

设置日志信息写入文件的保存时间

【命令格式】 **logging life-time level** *level days*

【参数说明】 *level*：日志信息的级别。

days：日志信息保存时间。单位：天。保存时间不小于 7 天。

【命令模式】 全局配置模式

【使用指导】 用户开启了基于时间的日志保存功能，系统针对同一级别、同一天内产生的日志信息，写入到同一个日志文件中，日志文件的名称形如“yyyy-mm-dd_filename_level.txt”，其中：yyyy-mm-dd 为日志信息产生的当天绝对时间；filename 为 **logging file flash** 命令配置的日志文件名称，level 为对应的日志信息级别。

用户对某个等级的日志信息进行保存时间限制后，当对应级别的日志信息超过日志保存时间限制后，将进行删除。为了网管的方便，目前系统要求日志信息最少可以保存 7 天，最长可以保存 365 天。

为了兼容以前的配置命令，用户在没有开启基于时间的日志保存功能时，日志仍然基于文件大小进行日志信息的保存。

设置将缓冲区当中的日志信息立即写入到日志文件中

【命令格式】 **logging flash flush**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 在系统开启日志信息写日志文件功能后，设备产生的日志信息会先缓存在系统日志缓冲区中，只有当缓冲区满或定时器到期后，才会将缓冲区中的日志信息写入到日志文件中，可以通过该命令设置将系统缓冲区中的日志信息立即写入到日志文件中。

⚠ 用户配置 **logging flash flush** 命令时，配置一次作用一次，配置后立即将存在缓冲区中的日志信息写入到日志文件中

配置举例

配置系统日志写入到日志文件

【网络环境】 假设网络环境中，有以下日志信息写入到日志文件设置要求：

1、设置日志文件名称为 syslog；

2、设置允许输出到控制台的日志信息级别为 debugging（7 级）；

3、设备日志信息写入到文件的时间间隔为 10 分钟（600 秒）。

【配置方法】

- 在设备上面配置系统日志写入到日志文件

```
Ruijie# configure terminal
Ruijie(config)# logging file flash:syslog debugging
Ruijie(config)# logging flash interval 600
```

【检验方法】

- 通过 **show logging config** 命令可以查看用户配置的相关参数信息。

```
Ruijie(config)#show logging config
Syslog logging: enabled
  Console logging: level informational, 1307 messages logged
  Monitor logging: level informational, 0 messages logged
  Buffer logging: level informational, 1307 messages logged
```

```
File logging: level debugging, 122 messages logged
File name:syslog.txt, size 128 Kbytes, have written 1 files
Standard format:false
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence-number log messages: enable
Sysname log messages: enable
Count log messages: enable
Trap logging: level debugging, 122 message lines logged,0 fail
  logging to  10.1.1.100
```

6.4.7 配置系统日志过滤功能

配置效果

- 在某些情况下，管理员可能不想让某些日志信息显示出来，则可以通过此功能过滤系统产生的日志信息。
- 默认情况下，各个模块打出来的日志信息都可以显示到控制台或其它终端上面。设置日志信息过滤原则可以让某些日志信息打出到某些终端中，或者只想让某些日志信息打出到某些终端中。

注意事项

- 日志信息的两种过滤类型，分为：“只包含”和“只过滤”，某一时刻只能配置其中的一种类型。
- 当用户配置的日志信息过滤规则中，若单个匹配规则和精确匹配规则中同时配置了一样的模块名、助记符或信息等级，则单个匹配规避的优先级高于精确匹配。

配置方法

↘ 设置日志信息的过滤方向

- 可选配置，缺省情况下过滤方向为 all（即过滤所有方向的日志信息）。
- 若无特殊要求，在需要设置日志信息的过滤方向的设备上面配置。

↘ 设置日志信息的过滤方式

- 可选配置，缺省情况下日志过滤方式为“只过滤”。
- 若无特殊要求，在需要设置日志信息的过滤方式的设备上面配置。

↘ 设置日志信息的过滤规则

- 必选配置，缺省情况下，系统没有设置任何过滤规则，不对日志信息进行过滤。
- 若无特殊要求，在需要设置日志信息的过滤规则的设备上面配置。

检验方法

- 通过 **show running** 命令可以查看设置的日志过滤功能参数信息

相关命令

设置日志信息的过滤方向

【命令格式】 **logging filter direction** { **all** | **buffer** | **file** | **server** | **terminal** }

【参数说明】 **all**：代表过滤往所有方向的日志信息。

buffer：代表过滤往日志缓冲区的日志信息（即 show logging 显示出来的日志信息）；

file：代表只过滤往日志文件的日志信息；

server：代表只过滤往日志服务器的日志信息；

terminal：代表过滤往控制台和 VTY 终端（包括 Telnet/SSH 等）的日志信息。

【命令模式】 全局配置模式

【使用指导】 默认为 all，即过滤所有方向的日志信息。

default logging filter direction 命令恢复日志信息的过滤方向为 all。

设置日志信息的过滤方式

【命令格式】 **logging filter type** { **contains-only** | **filter-only** }

【参数说明】 **contains-only** 代表“只包含”，意思是：只输出包含了过滤规则里面的关键字的日志信息，其它没有包含过滤规则里面的关键字的日志信息不会输出；

filter-only 代表“只过滤”，意思是：将过滤掉包含了过滤规则里面的关键字的日志信息，不会输出这些过滤掉的日志信息。

【命令模式】 全局配置模式

【使用指导】 日志过滤方式分为“只包含”和“只过滤”两种方式。默认为 filter-only，即“只过滤”。

设置日志信息的过滤规则

【命令格式】 **logging filter rule** { **exact-match module** *module-name* **mnemonic** *mnemonic-name* **level** *level* | **single-match** { **level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name* } }

【参数说明】 **exact-match**：代表精确匹配，若选择精确匹配，则后面的三个过滤选项都需要选上。

single-match：代表单个匹配，若选择单个匹配，则后面的三个过滤选项只需要选择其中的一个。

module *module-name*：模块名，即填写要过滤的模块名称。

mnemonic *mnemonic-name*：助记符名称，即填写要过滤的日志信息助记符名称。

level *level*：日志信息级别，即填写要过滤的日志信息等级。

【命令模式】 全局配置模式

【使用指导】 日志过滤规则分为“精确匹配”和“单个匹配”两种过滤规则。

no logging filter rule exact-match [**module** *module-name* **mnemonic** *mnemonic-name* **level** *level*]命令删除日志信息的“精确匹配”过滤规则。支持一次性删除所有的“精确匹配”过滤规则，也可以逐条进行删除。

no logging filter rule single-match [**level** *level* | **mnemonic** *mnemonic-name* | **module** *module-name*]命令删除日志信息的“单个匹配”过滤规则。支持一次性删除所有的“单个匹配”过滤规则，也可以逐条进行删

除。

配置举例

配置系统日志过滤功能

【网络环境】 假设网络环境中，有以下日志信息过滤功能设置要求：

1、设置日志信息的过滤方向为 **terminal**、**server** 两个方向；

2、设置日志信息的过滤方式为“只过滤”；

3、设备日志信息的过滤规则为“单个匹配”，并且模块名包含 SYS 的日志信息过滤掉。

【配置方法】

- 在设备上面配置系统日志的过滤功能

```
Ruijie# configure terminal
Ruijie(config)# logging filter direction server
Ruijie(config)# logging filter direction terminal
Ruijie(config)# logging filter type filter-only
Ruijie(config)# logging filter rule single-match module SYS
```

【检验方法】

- 通过 **show running-config | include loggging** 命令可以查看用户配置的相关参数信息。
- 通过进入/退出全局配置模式，观察系统是否会输出日志信息。

```
Ruijie#configure
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#exit
Ruijie#
Ruijie#show running-config | include logging
logging filter direction server
logging filter direction terminal
logging filter rule single-match module SYS
```

6.4.8 配置系统日志分级上送功能

配置效果

- 用户可以使用分级策略功能，将不同模块和严重级别的日志输出到不同目的地，例如：可以在命令行中配置，WLAN 模块的严重级别小于等于 4 的日志，实时发送到日志服务器；同时，WLAN 模块的严重级别大于等于 5 的日志，输出到本地日志文件中。

注意事项

- 此功能只有在开启 RFC5424 日志开关的情况下，才会生效。

配置方法

↘ 配置日志分级上送策略

- 可选配置，缺省情况下日志可以输出到所有方向上；
- 若无特殊要求，在需要分级上送策略的设备上配置。

检验方法

- 通过 **show running** 命令可以查看设置的日志分级上送策略参数信息

相关命令

↘ 配置日志分级上送策略

【命令格式】 **logging policy module** *module-name* [**not-lesser-than**] *level* **direction** { **all** | **server** | **file** | **console** | **monitor** | **buffer** }

【参数说明】 *module-name*：分级策略的模块名。

not-lesser-than：指定该选项时，代表大于等于所配置的日志级别的日志才会按照所配置的方向输出，小于所配置的日志级别的日志会被过滤掉；没有指定该选项时，代表小于等于所配置的日志级别的日志才会按照所配置的方向输出，大于所配置的日志级别的日志会被过滤掉。

level：所要配置分级策略的日志级别。

all：在所有的方向上都实行日志分级策略

server：只在发往日志服务器方向上实行日志分级策略

file：只在输出到日志文件方向上实行日志分级策略

console：只在输出到控制台方向上实行日志分级策略

monitor：只在输出到远程终端方向上实行日志分级策略

buffer：只在保存到缓冲区方向上实行日志分级策略

【命令模式】 全局配置模式

【使用指导】 用于配置系统日志按模块和严重级别输出到不同的目的地。

配置举例

↘ 配置日志分级上送功能

【网络环境】 假设有以下日志信息分级上送功能设置要求：

1、配置 SYS 模块级别大于等于 5 级的日志只往控制台方向输出；

2、配置 SYS 模块级别小于等于 3 级的日志只往缓冲区方向输出。

【配置方法】
- 在设备上面配置分级上送功能

```
Ruijie# configure terminal
Ruijie(config)# logging policy module SYS not-lesser-than 5 direction console
Ruijie(config)# logging policy module SYS 3 direction buffer
```

【检验方法】
- 通过 **show running-config | include logging policy** 命令可以查看用户配置的相关参数信息。
- 通过进入/退出配置模式产生一条模块名为 SYS 的日志，查看输出的方向是否正确。

```
Ruijie#show running-config | include logging policy
logging policy module SYS not-lesser-than 5 direction console
logging policy module SYS 3 direction buffer
```

6.4.9 配置系统日志延迟上送功能

配置效果

- 默认情况下延迟上送的功能是开启的，时间间隔为 3600 秒（1 小时），上送给远端服务器的文件名为：文件大小_设备 IP 地址_索引值.txt，且延迟上送的日志不输出控制台和远程终端；
- 可以根据设备产生延迟上送日志的频率，配置延迟上送的时间间隔，这样子可以减轻设备、SYSLOG 服务器和中间网络的负担，并且可以根据用户需要，配置上送文件的文件名；

注意事项

- 此功能只有在开启 RFC5424 日志开关的情况下，才会生效；
- 一般情况下，最好关闭延时上送的日志输出到控制台和远程终端，避免设备上打印出较多的延迟上送的日志信息，增加网络设备自身的负担；
- 配置的文件名中不能出现字符点号（.），因为系统在生成本地缓存文件时，文件名会增加索引值和后缀（.txt），索引值是以递增形式变化的；也不能出现 PC 文件命名禁止的字符，例如：\/：* “<>|。例如：配置的文件名为 log_server，当前的索引值为 5，文件大小为 1000B，发送日志文件的设备 IP 地址为 10.2.3.5，则发送给远端服务器的日志文件名为：log_server_1000_10.2.3.5_5.txt，但是保存在设备本地的日志文件名为log_server_5.txt。若发送日志文件的设备IP地址为 IPv6 形式，因为 IPv6 地址有可能出现冒号（:），而冒号（:）又是 PC 文件命名所禁止的字符，所以需要用字符（-）来替代。例如：用户配置的文件名为 log_server，汉前的文件索引值为 6，文件大小为 1000B，发送日志文件的设备 IPv6 地址为 2001::1，则发送远端服务器的日志文件名为：log_server_1000_2001-1_6.txt，但是保存在本地的日志文件名为 log_server_6.txt。
- 若网络设备上产生的延迟上送的日志信息较少，可以将延迟上送的时间间隔设置长一点，让更多的延迟上送日志集中在一起发送给远端服务器。

配置方法

↘ 配置日志延迟上送输出到控制台和远程终端

- 可选配置，缺省情况下是关闭延迟上送日志输出到控制台和远程终端；
- 若无特殊要求，在需要查看延迟上送日志的设备上配置。

配置日志延迟上送的文件名

- 可选配置，缺省情况下延迟上送的文件名为文件大小_设备 IP 地址_索引值.txt；
- 若无特殊要求，在需要修改延迟上送文件名的设备上配置。

配置日志延迟上送的时间间隔

- 可选配置，缺省情况下延迟上送的时间间隔是 3600 秒（1 小时）；
- 若无特殊要求，在需要修改延迟上送时间间隔的设备上配置。

配置日志延迟上送的服务器地址和上报方式

- 可选配置，缺省情况下是文件不发往任何远程服务器；
- 若无特殊要求，在需要发送延迟上送日志给远程服务器的设备上配置。

检验方法

- 通过 **show running** 命令可以查看设置的日志延迟上送的参数信息

相关命令

配置日志延迟上送输出到控制台和远程终端

【命令格式】 **logging delay-send terminal**
【参数说明】 -
【命令模式】 全局配置模式
【使用指导】 用于打开延时上送的日志输出到控制台和远程终端。

配置日志延迟上送的文件名

【命令格式】 **logging delay-send file flash:***filename*
【参数说明】 **flash:***filename*：延迟上送的日志文件名。
【命令模式】 全局配置模式
【使用指导】 用于配置延迟上送时缓存在设备本地的日志文件名。

配置的文件名中不能出现字符点号（.），因为系统在生成本地缓存文件时，文件名会增加索引值和后缀（.txt），索引值是以递增形式改变，也不能出现 PC 文件命名禁止的字符，例如：\/：* “<>|。

例如：用户配置的文件名为 log_server，当前的文件索引值为 5，文件大小为 1000B，发送日志文件的设备 IP 地址为 10.2.3.5，则发送远端服务器的日志文件名为：log_server_1000_10.2.3.5_5.txt，但是保存在本地的日志文件名为 log_server_5.txt。

若发送日志文件的设备 IP 地址为 IPv6 形式，因为 IPv6 地址有可能出现冒号（:），而冒号（:）又是 PC 文件

命名所禁止的字符，所以需要用字符（-）来替代。

例如 :用户配置的文件名为 log_server ,汉前的文件索引值为 6 ,文件大小为 1000B ,发送日志文件的设备 IPv6 地址为 2001::1，则发送远端服务器的日志文件名为：log_server_1000_2001-1_6.txt，但是保存在本地的日志文件名为 log_server_6.txt。

配置日志延迟上送的时间间隔

【命令格式】 **logging delay-send interval** *seconds*

【参数说明】 *seconds*：延迟上送的时间间隔（单位为秒）

【命令模式】 全局配置模式

【使用指导】 用于配置日志延迟上送给服务器的时间间隔。可以设置的范围为 600 ~ 65535，单位：秒。

配置日志延迟上送的服务器地址和上报方式

【命令格式】 **logging delay-send server** { *ip-address* | **ipv6** *ipv6-address* } **mode** { **ftp user** *username* **password** [**0** | **7**] *password* | **tftp** }

【参数说明】 *ip-address*：接收日志信息的服务器 IP 地址。

ipv6 *ipv6-address*：接收日志信息的服务器 IPV6 地址。

username：指定 ftp 服务器的用户名。

password：指定 ftp 服务器的密码。

0：(可选) 代表随后跟上的 *password* 为密码明文文本。

7：代表随后跟上的 *password* 为经过简单加密的密文文本。

【命令模式】 全局配置模式

【使用指导】 用于指定一个 FTP 或者 TFTP Server 来接收设备的日志信息。用户总共可以配置 5 个 FTP 或者 TFTP Server，且每一台服务器只能配置 FTP 或 TFTP 中一种，日志信息将同时发给配置的所有 FTP 或者 TFTP Server。

配置举例

配置日志延迟上送功能

【网络环境】 假设有以下日志信息延迟上送功能设置要求：

1、开启延迟上送日志输出到控制台和远程终端；

2、延迟上送的时间间隔为 7200 秒（2 小时）;

3、延迟上送的文件名为 syslog_ruijie；

4、延迟上送的服务器 ip 地址为 192.168.23.12、用户名 admin、密码 admin 和上送方式为 FTP。

【配置方法】

- 在设备上面配置延迟上送功能

```
Ruijie# configure terminal
Ruijie(config)# logging delay-send terminal
Ruijie(config)# logging delay-send interval 7200
Ruijie(config)# logging delay-send file flash:syslog_ruijie
Ruijie(config)# logging delay-send server 192.168.23.12 mode ftp user admin password admin
```

【检验方法】
- 通过 **show running-config | include logging delay-send** 命令可以查看用户配置的相关参数信息。
- 通过在延迟上送时间间隔内，产生延迟上送的日志，定时器到期后，查看是否有文件发送到远端的 FTP 服务器。

```
Ruijie#show running-config | include logging delay-send
logging delay-send terminal
logging delay-send interval 7200
logging delay-send file flash:syslog_ruijie
logging delay-send server 192.168.23.12 mode ftp user admin password admin
```

6.4.10 配置系统日志定时上送功能

配置效果

- 默认情况下，定时上送的功能是关闭的，所有统计对象的定时上送时间间隔为 15 分钟，且定时上送的日志不输出控制台和远程终端；
- 根据需要，可以修改统计对象的定时上送时间间隔，服务器将在所有统计对象的时间间隔的最小公倍数时间点上，收集到设备的所有的性能统计日志；

注意事项

- 此功能只有在开启 RFC5424 日志格式的情况下，才会生效；
- 只有打开日志定时上送功能的开关，日志定时上送时间间隔、输出到控制台和远程终端功能设置才会生效；
- 一般情况下，最好关闭定时上送的日志输出到控制台和远程终端，避免设备上日志定时上送功能定时器到期后，打印出较多的性能统计的日志信息，增加网络设备自身的负担
- 为了使服务器能在同一时间点上收集到设备上的所有的性能统计日志，当修改某一个统计对象的时间间隔，都会重新启动所有统计对象的定时上送的定时器。

配置方法

↘ 配置日志定时上送功能开关

- 可选配置，缺省情况下日志定时上送功能是关闭的；
- 若无特殊要求，在需要打开定时上送功能的设备上配置。

↘ 配置日志定时上送输出到控制台和远程终端

- 可选配置，缺省情况下定时上送日志输出到控制台和远程终端是关闭的；
- 若无特殊要求，在需要查看定时上送日志的设备上配置。

↘ 配置日志助记符定时上送的时间间隔

- 可选配置，缺省情况下所有统计对象的定时上送时间间隔都是 15 分钟；
- 若无特殊要求，在需要修改统计对象定时上送时间间隔的设备上配置。

检验方法

- 通过 **show running** 命令可以查看设置的日志定时上送功能参数信息

相关命令

配置日志定时上送功能开关

【命令格式】 **logging statistic enable**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 用于打开日志定时上送功能，打开日志定时上送功能后，系统将按一定的时间间隔输出一系列的性能统计数据，方便日志服务器对系统的性能进行跟踪。

配置日志定时上送输出到控制台和远程终端

【命令格式】 **logging statistic terminal**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 用于打开定时上送的日志输出到控制台和远程终端。

配置日志助记符定时上送的时间间隔

【命令格式】 **logging statistic mnemonic** *mnemonic* **interval** *minutes*

【参数说明】 *mnemonic*：日志定时上送的助记符字符串，用于标识系统性能统计对象。

minutes：定时上送的时间间隔，单位：分钟。

【命令模式】 全局配置模式

【使用指导】 用于配置系统某个性能统计对象的定时上报时间间隔。可以设置的时间间隔为 0、15、30、60、120 分钟，其中 0 表示关闭此统计对象的定时上送功能。

配置举例

配置日志分级上送功能

【网络环境】 假设有以下日志信息定时上送功能设置要求：

1、定时上送的功能是开启的；

2、开启定时上送日志输出到控制台和远程终端；

2、设置统计对象 TUNNEL_STAT 的定时上送的时间间隔为 30 分钟。

【配置方法】

- 在设备上面配置定时上送功能

```
Ruijie# configure terminal
```

```
Ruijie(config)# logging statistic enable
Ruijie(config)# logging statistic terminal
Ruijie(config)# logging statistic mnemonic TUNNEL_STAT interval 30
```

【检验方法】

- 通过 **show running-config | include logging statistic** 命令可以查看用户配置的相关参数信息。
- 通过在定时上送功能定时器到期后，查看是否有定时上送的日志产生，且在所有定时上送定时器时间间隔的最小公倍数时间点上，查看是否产生所有性能统计日志。

```
Ruijie#show running-config | include logging statistic
logging statistic enable
logging statistic terminal
logging statistic mnemonic TUNNEL_STAT interval 30
```

6.4.11 配置系统日志监控功能

配置效果

- 记录用户登录/退出的日志信息。开启记录用户登录/退出的日志信息后，当外界通过 Telnet/SSH 连接到设备时，设备将打出对应的 Log 信息，方便管理员监控设备的连接情况。
- 记录用户修订设备配置的日志信息。开启记录用户操作的日志信息后，当用户修订设备配置的时候，设备将打出对应的 Log 信息，方便管理员监控设备的配置修订情况。

注意事项

- 若设备上面同时配置 **logging userinfo** 和 **logging userinfo command-log**，则进行 **show running-config** 查看时，只会显示 **logging userinfo command-log**。

配置方法

↘ 开启记录用户登录/退出日志信息

- 可选配置，缺省情况下用户输入与日志信息输出同步功能是关闭的。
- 若无特殊要求，应在设备各个线路上面配置。

↘ 开启记录用户操作的日志信息

- 可选配置，缺省情况下用户输入与日志信息输出同步功能是关闭的。
- 若无特殊要求，应在设备各个线路上面配置。

检验方法

- 通过 **show running** 命令可以查看设置的用户输入同步输出功能参数信息

相关命令

开启记录用户登录/退出日志信息

【命令格式】 **logging userinfo**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 默认情况下，用户登录/退出设备的时候，设备是不会记录相关的 Log 信息。

开启记录用户操作的日志信息

【命令格式】 **logging userinfo command-log**

【参数说明】 -

【命令模式】 全局配置模式

【使用指导】 设置执行配置命令时，记录用户操作的 Log 信息。默认情况下，用户修订设备配置的时候，设备是不会记录相关的操作 Log 信息。

配置举例

配置系统日志监控功能

【网络环境】 假设在网络环境当中，有以下日志信息监控功能设置要求：

1、开启记录用户登录/退出日志信息；

2、开启记录用户操作的日志信息。

【配置方法】

- 在设备上面配置日志监控功能

```
Ruijie# configure terminal
Ruijie(config)# logging userinfo
Ruijie(config)# logging userinfo command-log
```

【检验方法】

- 通过 **show running-config | include logging** 命令可以查看用户配置的相关参数信息。
- 通过在设备全局配置模式里面配置一条命令，触发系统产生用户操作的日志信息。

```
Ruijie#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#interface gigabitEthernet 0/0
*Jun 16 15:03:43: %CLI-5-EXEC_CMD: Configured from console by admin command: interface
GigabitEthernet 0/0
Ruijie#show running-config | include logging
logging userinfo command-log
```

6.4.12 配置用户输入与日志信息同步输出功能

配置效果

- 默认情况下，用户输入与日志信息输出不同步。配置输入同步功能后，即使在用户输入的过程中打印日志，在打印结束后仍然会将用户之前的输入显示出来，从而保证输入的完整性和连贯性。

注意事项

- 该配置命令需要在线路配置模式下面进行配置，并且在每个需要开启此功能的线路上面均要进行配置。

配置方法

↘ 设置用户输入与日志信息输出同步功能

- 可选配置，缺省情况下用户输入与日志信息输出同步功能是关闭的。
- 若无特殊要求，应在设备各个需要开启此功能的线路上面配置。

检验方法

- 通过 **show running** 命令可以查看设置的用户输入同步输出功能参数信息

相关命令

↘ 设置用户输入与日志信息输出同步功能

【命令格式】 **logging synchronous**
【参数说明】 -
【命令模式】 线路配置模式
【使用指导】 此命令打开用户输入与日志信息输出同步功能，可以防止用户正在输入的字符时被打断。

配置举例

↘ 配置用户输入与日志信息输出同步功能

【网络环境】 假设在网络环境当中，有以下用户输入同步输出功能设置要求：
1、设置用户输入与日志信息同步输出功能。

【配置方法】
- 在设备上面配置用户

```
Ruijie# configure terminal
Ruijie(config)# line console 0
```

```
Ruijie(config-line)# logging synchronous
```

【检验方法】

- 通过 **show running-config | begin line** 命令可以查看用户配置的相关参数信息。

```
Ruijie#show running-config | begin line
line con 0
 logging synchronous
 login local
```

如下所示，当用户敲入“vlan”后接口 0/1 发生状态改变，打印日志，打印结束后日志模块会自动把用户已经输入的“vlan”打印出来，使得用户可以继续输入：

```
Ruijie(config)#vlan
*Aug 20 10:05:19: %LINK-5-CHANGED: Interface GigabitEthernet 0/1, changed state to up
*Aug 20 10:05:19: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet 0/1, changed state to up
Ruijie(config)#vlan
```

6.5 监视与维护

清除各类信息

⚠ 在设备运行过程中执行 **clear** 命令，可能因为重要信息丢失而导致业务中断。

作用	命令
清除内存缓冲区中的日志信息	**clear logging**

查看运行情况

作用	命令
查看内存缓冲区中的日志报文，以及日志相关统计信息，日志信息按时间戳从旧到新的顺序显示	**show logging**
查看内存缓冲区中的日志报文，以及日志相关统计信息，日志信息按时间戳从新到旧顺序显示	**show logging reverse**
查看系统日志配置的参数、统计信息	**show logging config**
查看系统中各模块日志信息统计情况	**show logging count**

7 RLOG

7.1 概述

RLOG 为日志上传模块。当设备需要上传日志到服务器时（如 ELOG，SNC），使用到本模块。

设备负责日志的采集，并通过 RLOG 将日志传给服务器。经过服务器端程序日志的解析后写入数据库。RLOG 可以用来上传设备运行信息，用户上网信息，系统安全信息等多种日志，在服务器端可以方便的查询到指定的记录。

下文仅介绍 RLOG 的相关内容。

协议规范

- 无

7.2 典型应用

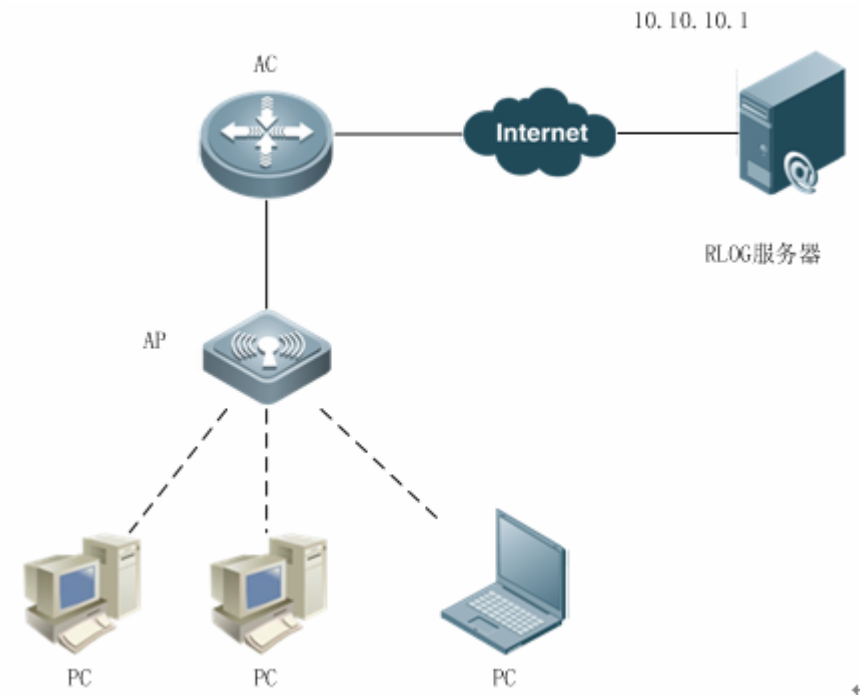
典型应用	场景描述
上传流日志	打开URL审计日志，RLOG将流日志上传到服务器，然后在服务器可以查询到每条数据流的详细记录。

7.2.1 上传流日志

应用场景

AP/AC 设备打开 RLOG 日志功能，打开 URL 审计日志记录功能，当用户通过 AP 上网时，就会有 URL 审计日志产生。流消亡时，流日志通过 RLOG 上传给 ELOG 服务器。

图 7-1



【注释】 AP 和 AC 分别为无线接入点和无线接入控制器。

功能部属

- AC/AP 中开启 URL 审计日志记录，开启 RLOG，并配置服务器。
- RLOG 服务器接收并解析日志，提供查询统计的服务。

7.3 功能详解

基本概念

无。

功能特性

功能特性	作用
上传日志	将 AP/AC 设备的日志上传到服务器。
每种日志单独配置服务器	每类日志，可以单独配置上传的服务器

7.3.1 上传日志

将设备日志上传到服务器。

工作原理

设备的功能模块，如流日志，设备审计，流量审计，内容审计等，生成对应的日志，通过 RLOG 接口，发送给服务器。服务器接收，解析，展现这些日志信息。

相关配置

↘ 开启模块功能

各个模块的缺省情况下，并不一定在工作，需要打开。

比如流量审计，开启命令为：flow-audit enable

↘ 配置日志发送功能

缺省情况下，未配置服务器和日志发送功能。

配置一台服务器：rlog server 192.168.1.100 port 20000

配置日志发往服务器：rlog type 25 server 192.168.1.100 priority 1

其中，日志类型 25 表示接口流量日志。

7.3.2 每种日志单独配置服务器

将设备不同的日志上传到不同的服务器。

工作原理

RLOG 模块在接收到功能模块的日志发送请求，根据配置，对不同类型的日志区分对待。

相关配置

↘ 开启模块功能

各个模块的缺省情况下，并不一定在工作，需要打开。

比如流量审计，开启命令为：flow-audit enable

↘ 配置日志发送功能

缺省情况下，未配置服务器和日志发送功能。

配置两台服务器：rlog server 192.168.1.100 port 20000

rlog server 192.168.1.101 port 20000

配置流日志发往服务器：rlog type 16 server 192.168.1.100 priority 1

配置接口流量日志发往服务器：rlog type 25 server 192.168.1.101 priority 1

其中，日志类型 16 表示流日志。

7.4 配置详解

配置项	配置建议 & 相关命令	
配置日志发送	⚠ 必须配置。用于指定服务器地址端口。	
	rlog server *ip-address* [**vrf** *vrf-name*] [**port** *port-num*]	指定日志服务器 ip 地址和 VRF 名或指定从管理口发送，并打开日志服务，端口默认是 20000
	rlog type *n* **server** *server-ip* **priority** *prio*	开启某个日志服务器上指定的日志，并设置优先级
配置日志发送参数	⚠ 可选配置。指定日志发送速率。	
	rlog export-rate *val*	指定日志服务导出速率(每秒发送日志最大个数)
	rlog set log-com	指定 RLOG 日志是否对多条日志进行合并发送
	rlog dev-ip *ip*	指定 RLOG 设备 ip
	rlog filter*acl_id*	配置日志过滤条件，目前不处理该信息

7.4.1 配置日志发送

配置效果

- 配置 RLOG 服务器。
- 配置某一种日志发往指定的服务器。

注意事项

- 无。

配置方法

↘ 配置 RLOG 服务器

- 必须配置。
- 若无特殊要求，可以配置一个服务器。

↘ 配置日志发送

- 必须配置。
- 一般需要哪种日志就配哪种日志。

检验方法

设备正常发送配置的日志

- 检查 RLOG 服务器能否成功接收每个日志报文。

相关命令

↘ 配置日志服务器

【命令格式】 **rlog server** *ip-address* [**vrf** *vrf-name*] [**port** *port-num*]

【参数说明】 *Ip-address* ：服务器 ip

port-num：服务器端口

vrf *vrf-name*：指定 VRF。

【命令模式】 配置模式

【使用指导】 配置日志服务器命令只是打开日志服务，输出日志内容并没有开启，单独打开该命令不会有日志内容输出。

例如流日志开关是 **ip session log-on**，需要单独打开。

若要取消服务器配置，则可以执行：**no rlog server** *ip-address*

↘ 配置日志发送

【命令格式】 **rlog type** *n* **server** *server-ip* **priority** *prio*

【参数说明】 *n*：RLOG 日志类型

server-ip：已配置的服务器 IP

prio：日志发送优先级，取值 0~7，取值越小优先级越高

【命令模式】 配置模式

【使用指导】 要取消发送某个日志，执行：**no rlog type** *n* **server** *server-ip*

目前支持的日志类型包括：

[16] RLOG_TYPE_FLOW, /* 流日志 */

[17] RLOG_TYPE_CPU_MEM, /* CPU 使用率，内存使用率日志 */

[18] RLOG_TYPE_DISC, /* 硬盘使用情况 */

[19] RLOG_TYPE_DEV_LOG, /* 设备审计的日志 */

[20] RLOG_TYPE_URL_AUDIT, /* URL 审计 */

[21] RLOG_TYPE_SESSION, /* 在线 ip 数，在线会话数日志 */

[22] RLOG_TYPE_IP_APP, /* 某个 IP,应用的流量 */

[23] RLOG_TYPE_IP, /* 某个 IP 的会话数 */

[24] RLOG_TYPE_CHANNEL, /* 某个通道的流量 */

[25] RLOG_TYPE_INTERFACE, /* 某个接口的流量 */

```
[26] RLOG_TYPE_IP_OFFLINE,              /* IP 下线通告 */
[27] RLOG_TYPE_MAIL_AUDIT,              /* 邮件审计 */
[28] RLOG_TYPE_TELNET_AUDIT,            /* telnet 审计 */
[29] RLOG_TYPE_WEB_SEARCH_AUDIT,        /* 搜索审计 */
[30] RLOG_TYPE_WEB_BBS_AUDIT,           /* web_bbs 审计 */
[31] RLOG_TYPE_IM_AUDIT,                /* IM 审计 */
[32] RLOG_TYPE_FTP_AUDIT,               /* FTP 审计 */
[33] RLOG_TYPE_WEB_AUDIT,               /* web 审计 */
[34] RLOG_TYPE_APP_AUDIT,               /* 应用控制审计 */
[35] RLOG_TYPE_FLOOD,                   /* 发现洪水攻击日志*/
[36] RLOG_TYPE_FLOOD_CEASEm,            /* 洪水攻击停止日志*/
[37] RLOG_TYPE_SCAN,                    /* 发现扫描日志*/
[38] RLOG_TYPE_SCAN_CEASE,              /* 扫描停止日志*/
[39] RLOG_TYPE_ATTACK_FRAG,             /*发现 IP 分片攻击*/
```

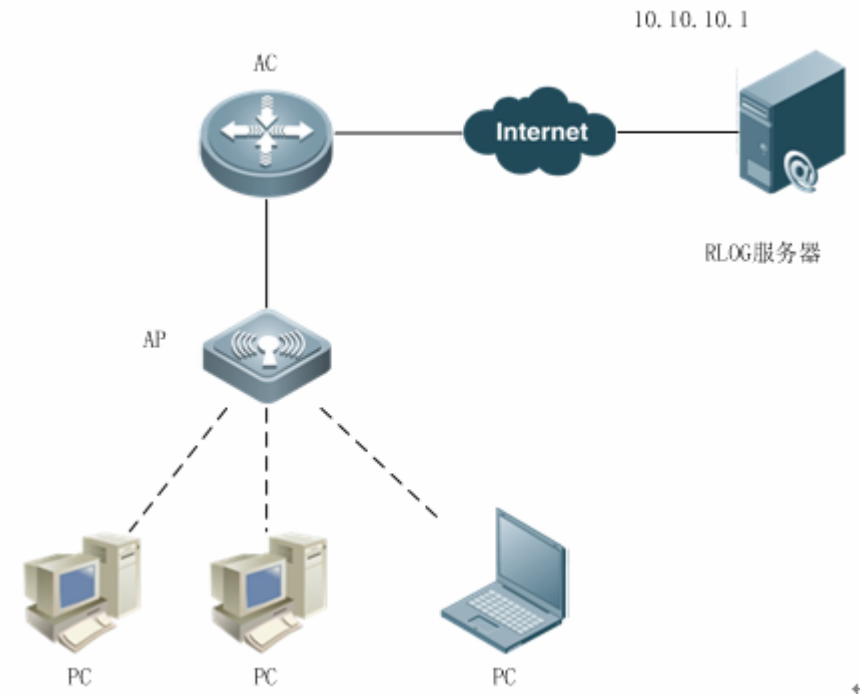
配置举例

以下配置举例，仅介绍与 RLOG 相关的配置。

配置流日志发送到服务器 10.10.10.1

【网络环境】

图 7-2



【配置方法】

- 在 AC/AP 上配置 RLOG 服务器的 ip 和端口
- 在 AC/AP 上配置流日志发送往服务器 10.10.10.1。
- 在 AC/AP 上打开流日志。

A

```
A# configure terminal
A(config)# rlog server 10.10.10.1 port 20000
A(config)# rlog type 16 server 10.10.10.1 priority 1
A(config)# ip session log-on
```

【检验方法】 检查 A 是否发送日志报文到 RLOG 服务器，也可以检查 RLOG 模块的日志发送计数是否增加。

- 检查 RLOG 模块的日志生成计数是否增加
- 检查 RLOG 日志发送计数是否增加

A

```
A# show rlog-status log
local rlog message:

remote rlog message:
[16]RLOG_TYPE_FLOW                : 0
[17]RLOG_TYPE_CPU_MEM             : 0
[18]RLOG_TYPE_DISC                : 0
[19]RLOG_TYPE_DEV_LOG             : 0
[20]RLOG_TYPE_URL_AUDIT           : 0
[21]RLOG_TYPE_SESSION             : 0
[22]RLOG_TYPE_IP_APP              : 0
[23]RLOG_TYPE_IP                  : 0
[24]RLOG_TYPE_CHANNEL             : 0
[25]RLOG_TYPE_INTERFACE           : 0
[26]RLOG_TYPE_IP_OFFLINE          : 0
[27]RLOG_TYPE_MAIL_AUDIT          : 0
[28]RLOG_TYPE_TELNET_AUDIT        : 0
[29]RLOG_TYPE_WEB_SEARCH_AUDIT    : 0
[30]RLOG_TYPE_WEB_BBS_AUDIT       : 0
[31]RLOG_TYPE_IM_AUDIT            : 0
[32]RLOG_TYPE_FTP_AUDIT           : 0
[33]RLOG_TYPE_WEB_AUDIT           : 0
[34]RLOG_TYPE_APP_AUDIT           : 0
[35]RLOG_TYPE_FLOOD               : 0
[36]RLOG_TYPE_FLOOD_CEASEm        : 0
[37]RLOG_TYPE_SCAN                : 0
[38]RLOG_TYPE_SCAN_CEASE          : 0
[39]RLOG_TYPE_ATTACK_FRAG         : 0
```

如果日志有生成，那么 RLOG_TYPE_FLOW 的日志计数会增加。

A

```
A# show rlog
rlog server is enable
```

```
 port 20000  server 192.168.1.100
 port 20000  server 10.10.10.1
rlog dev-ip 0.0.0.0
rlog export-rate 10000 rlog queue remain 10000
send log count : 0 error count : 0 errorno : 0
recv buf: 0 poll buf err: 0 push buf: 0 local buf: 0
recv err cnt: 0 depatch err cnt: 0

enable log combination: 0
```

如果发送成功，则 `send log count` 的值会增加。

常见错误

- 配置了 RLOG 服务器，没有指定日志发送到该服务器。
- 配置了 RLOG 日志和服务器，但是产生日志的开关没有打开。

7.4.2 配置日志发送参数

配置效果

- 使得 RLOG 工作得更加健康。

注意事项

- 必须了解每项参数配置的作用，和参数取值的意义之后再配置，否则可能导致 RLOG 不能正常工作。

配置方法

- 根据环境，有需要此项配置时才进行配置。

检验方法

- RLOG 发送日志正常，服务器能正常接收到日志。

相关命令

↘ 配置日志发送速率

【命令格式】 **rlog export-rate** *val*

【参数说明】 *Val*：每秒发送的日志条数上限值。

【命令模式】 配置模式

【使用指导】 配置取值必须考虑本设备的性能，RLOG 服务器的性能，以及设备的日志产生量。配置太小，容易造成日志发送丢失。配置过大，可能导致 CPU 持续偏高。

配置日志合并发送

【命令格式】 **rlog set log-com**

【参数说明】 -

【配置模式】 配置模式

【使用指导】 配置该命令后，多条日志会被拼接在一条报文中发送。需要 RLOG 服务器支持，配置时要先弄清楚服务器是否支持该功能。

配置设备 ip

【命令格式】 **rlog dev-ip** *ip*

【参数说明】 *ip*：指定设备 ip。

【配置模式】 配置模式

【使用指导】 部分日志需要取得本设备的 ip，该 ip 由本命令指定。有需要的时候才配置。

配置日志过滤条件

【命令格式】 **rlog filter***acl_id*

【参数说明】 access-list id

【配置模式】 配置模式

【使用指导】 当前版本不对该命令进行处理

配置举例

指定本设备 IP 为 10.10.10.1，日志发送速率为 10000，不合并日志。

【配置方法】

```
Ruijie# configure terminal
Ruijie(config)# rlog dev-ip 10.10.10.1
Ruijie(config)# rlog export-rate 10000
Ruijie(config)# end
```

【检验方法】 查看配置是否生效，服务器日志是否正常接收

```
Ruijie# show rlog
rlog server is enable
 port 20000  server 192.168.1.100
 port 20000  server 10.10.10.1
rlog dev-ip 10.10.10.1
rlog export-rate 10000 rlog queue remain 10000
send log count : 0 error count : 0 errorno : 0
recv buf: 0 poll buf err: 0 push buf: 0 local buf: 0
```

```
recv err cnt: 0 depatch err cnt: 0
```

常见配置错误

- 日志发送速率配置过小，导致日志丢失。

7.5 监视与维护

清除各类信息

无

查看运行情况

作用	命令
查看 RLOG 运行、配置情况	**show rlog**
查看 RLOG 支持的日志类型	**show rlog-type**
查看 RLOG 服务器状态	**show rlog-status** [**server** *ip*]
查看连接 RLOG 的功能模块个数	**show rlog-status client**
查看 RLOG 每种日志产生的日志个数	**show rlog-status log**

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
打开 RLOG debug 开关	**debug rlog info**
打开 RLOG 库的 debug 开关	**debug rlog lib**

8 CWMP

8.1 概述

CWMP 协议(CPE WAN Management Protocol 即 CPE 广域网管理协议)提供了设备统一管理的通用框架、消息规范、管理方法和数据模型，解决了用户侧设备数量繁多，部署分散，不易统一管理和维护的问题，提高了问题响应效率，节约了运维成本。

CWMP 协议主要提供下面一些功能：

- 自动配置和动态服务提供，用户侧设备启动初次接入网络时自动从管理服务器处获取配置，用户侧设备在运行过程中，管理服务器可以动态的改变其配置和状态；
- 主程序 / 配置文件管理，提供主程序和配置文件的升级及配置文件的上传；
- 软件模块功能的管理，通过各软件模块实现的数据模型对各软件模块进行管理；
- 状态行为监控，用户侧设备运行时状态及配置变化通告给管理服务器，通过这些实时变化的通告实现对用户侧设备的监控；
- 故障诊断，管理服务器通过用户侧设备提供的信息诊断或解决连接性问题及其他服务性问题，同时可以执行一些预定义的诊断行为。

下文仅介绍 CWMP 的相关内容。

协议规范

TR069 的协议规范详见官方论坛：http://www.broadband-forum.org/technical/trlist.php。以下是主要的几份规范：

- 《TR-069_Amendment-4.pdf》，CWMP 协议标准。
- 《TR-098_Amendment-2.pdf》，CWMP 协议网关产品数据模型规范。
- 《TR-106_Amendment-6.pdf》，CWMP 协议 CPE 数据模型标准。
- 《TR-181_Issue-2_Amendment-5.pdf》，CPE 数据模型 2 规范。
- 《tr-098-1-4-full.xml》，CWMP 协议网关产品数据模型定义。
- 《tr-181-2-4-full.xml》，CWMP 协议 CPE 数据模型 2 定义。

8.2 典型应用

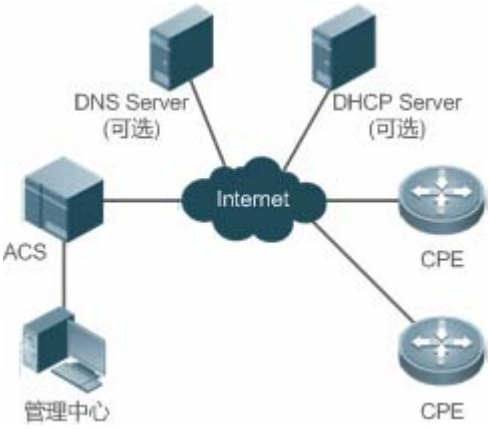
典型应用	场景描述
CWMP网络应用场景	通过配置 CPE 设备与 ACS 服务器建立连接,以实现 CPE 设备主程序升级，配置文件上传，恢复等功能。

8.2.1 CWMP网络应用场景

应用场景

CWMP 的网络结构中主要包括 CPE、ACS、管理中心、DHCP 服务器和 DNS 服务器。大量的 CPE 接受 ACS 的管理，管理中心通过控制 ACS 服务器，实现对 CPE 设备的管理控制，一般控制中心为 WEB 浏览器，通过 WEB 浏览器控制 ACS 服务器

图 8-1



【注释】
- DHCP 服务器用于动态获取 ACS 的 URL，如果使用静态配置 ACS 的 URL，DHCP 服务器在该网络中为可选元素
- DNS 服务器用于解析 ACS 或 CPE 的域名，如果 ACS 和 CPE 的 URL 中直接使用的是 IP 地址而不是域名，DNS 服务器在该网络中为可选元素

功能部属

- CPE 和 ACS 设备要运行 HTTP 协议

8.3 功能详解

基本概念

↘ 常用术语

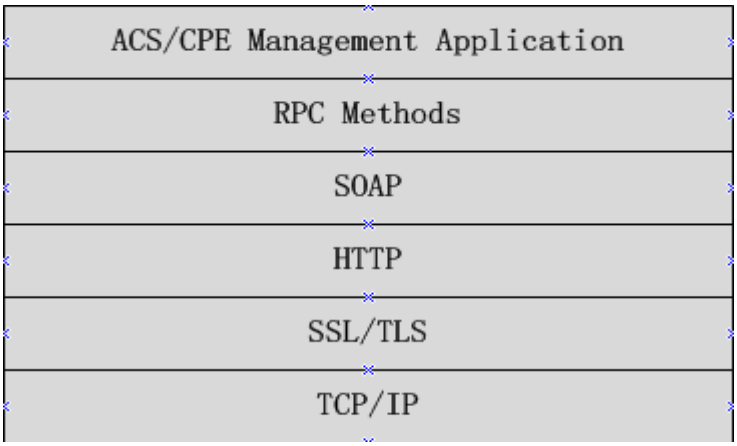
- CPE：Customer Premises Equipment (顾客预置设备)。
- ACS：Auto-Configuration Server (自动配置服务器)。

- RPC：Remote Procedure Call（远程过程调用）。
- DM：Data Model，数据模型。

协议结构

CWMP 的协议结构如下图所示：

图 8-2 CWMP 的协议结构



如图所示，协议规范将 CWMP 协议的工作分为 6 个层次，各层次的功能及作用说明如下：

- ACS/CPE Management Application

运用程序管理层，该层并非 CWMP 协议本身的范畴，它是指 CPE/ACS 的各功能模块为了支持 CWMP 的管理进行的开发，如同 SNMP 一样，各功能模块的 MIB 管理本身即不属于 SNMP 的协议范畴。

- RPC Methods

RPC 方法管理层， 该层提供了 ACS 与 CPE 之间交互的各种 RPC 方法，实现各种 RPC 方法的操作。

- SOAP

简单对象访问协议层， 该层提供了 CWMP 协议的 XML 形式封装与解封装，CWMP 消息格式必须符合 SOAP 的封装语法。

- HTTP

所有的 CWMP 消息最终通过 HTTP 协议进行传输， ACS 和 CPE 同时支持 HTTP 客户端和服务器端功能，服务器端用于监控对端的反响连接。

- SSL/TLS

该层提供 CWMP 协议的安全性保证，包括数据完整性，机密性及认证的保护。

- TCP/IP

TCP/IP 协议栈。

RPC 方法管理

ACS 对 CPE 的管理监控主要是通过 RPC 方法进行的，主要包括如下的一些方法：

- GET 系列方法

该系列方法主要用于 ACS 远程获取 CPE 支持的 RPC 方法、CPE 支持的数据模型参数名、数据模型参数的值和数据模型参数的属性。

- SET 系列方法

该系列方法主要用于 ACS 远程设置 CPE 支持的数据模型参数的值和数据模型参数的属性。

- INFORM 方法

INFORM 方法用于 CPE 向 ACS 通告自己的设备标识、参数信息及所发生的事件。INFORM 方法为 ACS 与 CPE 建立会话时交互的第一个方法。

- DownLoad 方法

DownLoad 方法实现 ACS 远程控制 CPE 下载文件的管理，包括 CPE 主程序升级的控制、配置文件升级的控制和 WEB 包升级的控制。

- UpLoad 方法

UpLoad 方法实现 ACS 远程控制 CPE 上传文件的管理，包括 CPE 配置文件上传的控制、日志文件上传的控制。

- Reboot 方法

Reboot 方法用于 ACS 远程控制 CPE 的重启行为。

会话管理

CWMP 协议工作的基础是 CWMP 协议会话，CWMP 的交互就是 CWMP 的会话交互，CWMP 协议在 ACS 与 CPE 之间的所有交互都以其会话为基础，通过会话传输、管理、维护其操作，实现 ACS 与 CPE 之间的有效交互，实现 ACS 对 CPE 的管理和监控。ACS 与 CPE 的一次会话过程即为两者建立 TCP 连接，Inform 协商开始到当前所有交互完成 TCP 连接断开为止，这个过程称之为一次会话过程。根据会话发起方角色的不同将其分为 CPE 主动发起的会话和 ACS 请求的会话两种，下面就这两种运用场景进行说明。

数据模型管理

CWMP 数据模型是 CWMP 工作的依据，CWMP 对所有功能模块的管理都是对 CWMP 数据模型的操作，各功能模块注册并实现自己支持数据模型，如果 SNMP 中各功能模块实现的 MIB 一样。

CWMP 数据模型以字符串的形式表示，为了区分数据模型的层次关系，以“.”分隔符区分上下级数据模型节点之间的关系，如 InternetGatewayDevice.LANDevice 的数据模型表示中，InternetGatewayDevice 为 LANDevice 的父数据模型节点，而 LANDevice 为 InternetGatewayDevice 子数据模型节点。

数据模型节点分为两类，一类为对象节点（object），一类为参数节点（parameter），也叫叶子节点。对象节点是指那些其下还有子节点的节点。而参数节点即没有子节点的叶子节点。对象节点分单实例对象节点和多实例对象节点，单实例对象节点指只存在单个实例对象的节点，多实例对象节点指存在多个实例对象的节点。数据模型节点分为可读节点和可读可写节点，可读节点只能读取其参数的值，不能进行修改，可读可写节点除了可读该节点参数值外还能对其进行修改。

数据模型节点存在两种属性，一种为是否通告的属性，即该数据模型对应参数值发生变化（非 CWMP 协议引起的变化）时是否将其通告给 ACS 服务器；一种是模型节点参数可被其他管理方式（非 ACS）写操作的标识，即其他管理方式如 Telnet 等是否可对该参数值进行修改。ACS 可以通过 RPC 方法修改数据模型的属性。

CWMP 协议对数据模型的管理通过对应的 RPC 方法进行。

事件管理

在 CPE 设备上，当一些 ACS 感兴趣或关心的事件发生时，CPE 需要将这些事件通告给 ACS，ACS 通过监控这些事件来监控 CPE 的工作状态，CWMP 的事件如同 SNMP 中的 TRAP 和产品日志功能中的日志信息。ACS 可以通过 RPC 方法控制和调整自己关心的事件，过滤掉不关心的事件类型。CWMP 中的事件总体分为两类，单量事件类型和增量事件类型，单量事件类型的事件是指同一个事件第二次发生时，该事件不再有量的变化而是丢弃老的，保留新的，增量事件类型是指同一事件后续多次发生时，老的不能丢弃，新产生的事件作为一个完整的事件保留，量上加 1。

CPE 产生的所有事件通过 INFORM 方法向 ACS 通告。

功能特性

功能特性	作用
主程序升级	ACS 通过 DownLoad 方法控制 CPE 的主程序升级
配置文件升级	ACS 通过 DownLoad 方法控制 CPE 的配置文件升级
配置文件上传	ACS 通过 UpLoad 方法控制 CPE 的配置文件上传
CPE备份恢复	当设备出现脱管状态时，远程设备恢复到脱管前的状态

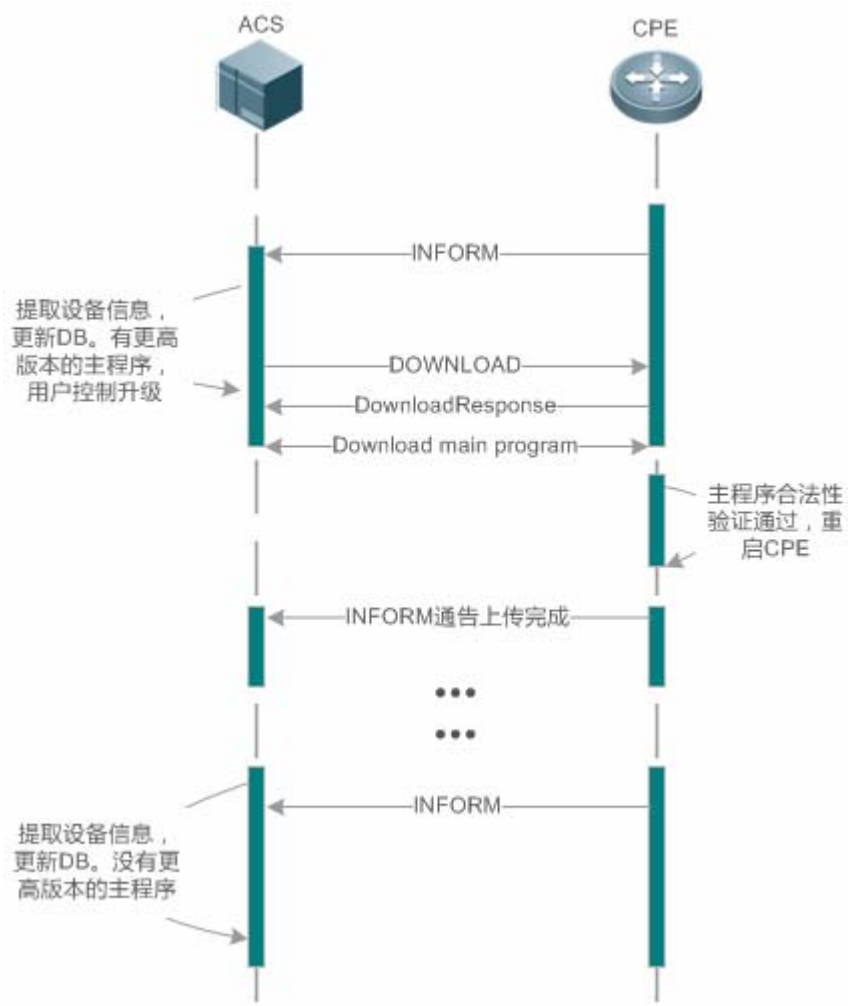
8.3.1 主程序升级

主程序升级，是指对各网元设备的主程序进行更新，通过主程序的升级来达到对设备版本的升级或更新换代

工作原理

↘ 主程序升级时序图

图 8-3



用户指定 CPE 升级主程序，ACS 向 CPE 下发升级主程序的 DownLoand 方法。CPE 从 DownLoad 方法中指定的文件服务器下载主程序，升级自身的主程序，更新完主程序后重启 CPE 设备，完成主程序的升级。CPE 重启后向 ACS 通告主程序管理升级完成。

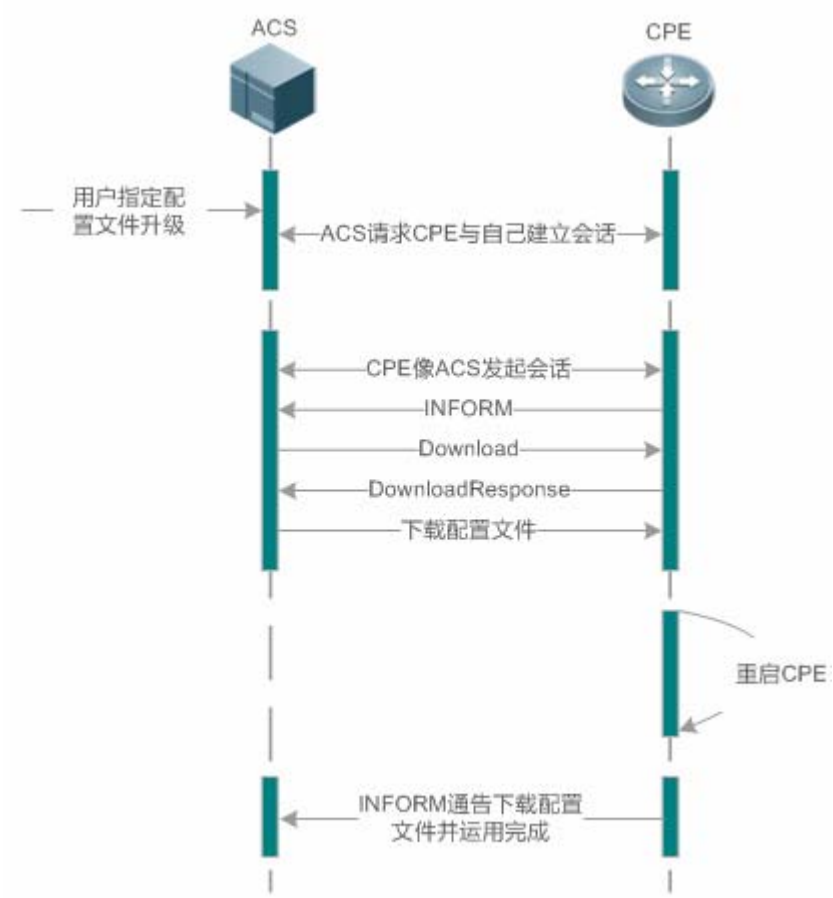
ACS 可以同时作为文件服务器，文件服务器也可以作为单独的服务器部署。

8.3.2 配置文件升级

配置文件升级，是指将整个设备的当前的配置文件替换为指定的配置，设备复位后，系统将运行全新的配置

工作原理

图 8-4



用户指定 CPE 升级配置文件，ACS 向 CPE 下发升级配置文件的 DownLoand 方法。CPE 从 DownLoad 方法中指定的文件服务器下载配置文件，升级自身的配置文件，更新完配置文件后重启 CPE 设备，完成配置文件的升级。CPE 重启后向 ACS 通告配置文件升级完成。

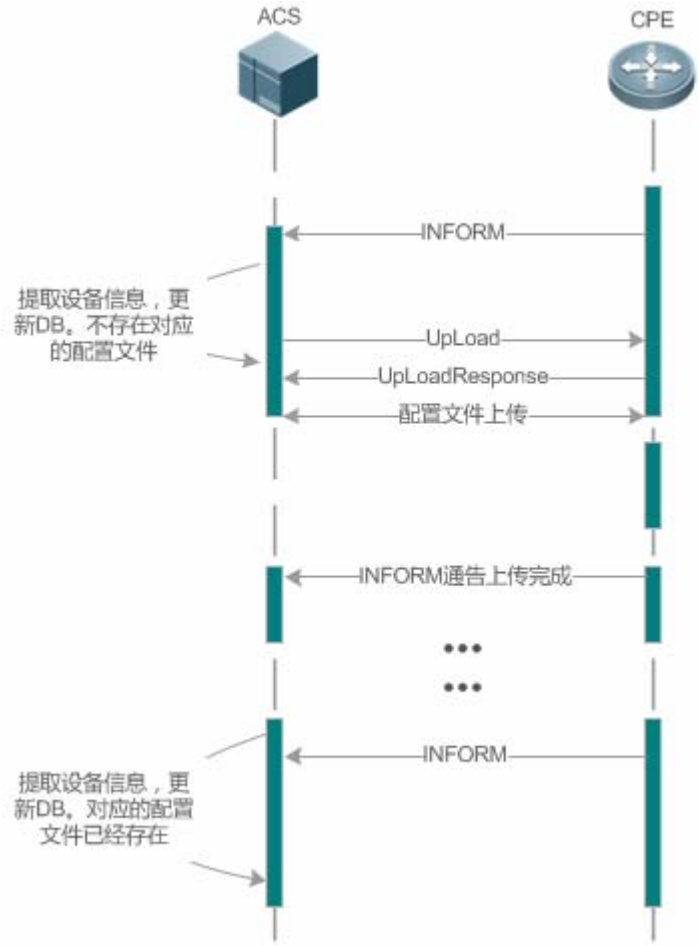
ACS 可以同时作为文件服务器，文件服务器也可以作为单独的服务器部署。

8.3.3 配置文件上传

配置文件上传，ACS 控制 CPE 的配置文件是通过 UpLoad 方法上传其配置文件

工作原理

图 8-5



CPE 初次上线 ACS，ACS 需要学习 CPE 的配置文件，学习过程如下：

- ACS 初次收到 CPE 的 INFORM 消息，根据 INFORM 消息中的设备信息，找到或建立对应的 CPE DB 信息；
- ACS DB 中还不存在当前 CPE 的配置文件，ACS 向该 CPE 下发上传配置文件的 Upload 方法；
- CPE 将当前的配置文件上传给 ACS 服务器；
- CPE 通告 ACS 配置文件上传完成。

8.3.4 CPE备份恢复

CPE 备份恢复，是指管理端由于一些异常的操作导致远程设备脱管，当这种情况发生时，需要远程设备恢复到脱管前的状态，恢复对远程设备的管理，重新对远程设备执行正确的管理与操作。

工作原理

在设备上配置 CPE 主程序/配置在异常情况下的恢复功能，指当 CPE 进行主程序/配置升级后无法连接 ACS，出现脱管现象时，能及时的恢复到脱管前的主程序和配置，恢复 ACS 对 CPE 的管理，这种情况的出现一般是下发了错误的主程序或配置所导致。

CPE 在每次接收主程序升级以及配置下发时，先备份当前的配置与主程序；并提供机制用于判断是否出现上述场景描述的问题，若出现，则将系统恢复到之前的可管理状态

8.4 配置详解

配置项	配置建议 & 相关命令	
建立CWMP基本连接	必须配置。配置 CPE 连接 ACS 时用于认证的用户名和密码及配置 ACS 连接 CPE 时用于认证的用户名和密码	
	cwmp	使能 CWMP 并进入 CWMP 配置模式
	acs usrname	配置 CPE 连接 ACS 时用于认证的用户名
	acs password	配置 CPE 连接 ACS 时用于认证的密码
	cpe usrname	配置 ACS 连接 CPE 时用于认证的用户名
	cpe password	配置 ACS 连接 CPE 时用于认证的密码
	可选配置。配置 CPE 及 ACS 设备的 URL	
	acs url	配置 CPE 连接 ACS 的 URL。
	cpe url	配置 ACS 连接 CPE 的 URL
配置CWMP相关属性	可选配置。配置 CPE 设备的基本功能（如 CPE 主程序/配置备份恢复功能，不向 ACS 上传配置文件和日志文件的管理等）	
	cpe inform	配置 CPE 周期性 INFORM 通告功能
	cpe back-up	配置 CPE 主程序/配置备份恢复功能
	disable download	配置关闭从 ACS 下载主程序和配置文件的功能
	disable upload	配置关闭向 ACS 上传配置文件和日志文件的功能
	timer cpe- timeout	配置 ACS 无响应 CPE 超时时间

8.4.1 建立CWMP基本连接

配置效果

- 实现 ACS 设备与 CPE 设备会话连接的建立

注意事项

- 无

配置方法

使能 CWMP 并进入 CWMP 配置模式

- 默认开启 CWMP 功能。
- CPE 设备上必须配置。

【命令格式】 **cwmp**
【参数说明】 -
【缺省配置】 CWMP 功能开启
【命令模式】 全局模式
【使用指导】 -

配置 CPE 连接 ACS 时用于认证的用户名

- ACS 设备上必须配置。
- 只能配置一个 ACS 用户名，多次配置 ACS 的用户名时，最新的配置生效。

【命令格式】 **acs username** *username*
【参数说明】 **username** *username*：配置 CPE 连接 ACS 用于认证的用户名。
【缺省配置】 无默认 ACS 用户名
【命令模式】 cwmp 配置模式
【使用指导】 -

配置 CPE 连接 ACS 时用于认证的密码

- ACS 设备上必须配置。
- ACS 用户密码可以为明文和密文形式，只能配置一个 ACS 用户密码，多次配置 ACS 的用户密码时，最新的配置生效。

【命令格式】 **acs password** {*password* | *encryption-type* *encrypted-password*}
【参数说明】 *password:* CPE 连接 ACS 用于认证的密码。
encryption-type: 可配置为 0 或 7，为 0 表示无加密，为 7 表示简单加密
encrypted-password: 密码文本
【缺省配置】 encryption-type 默认为 0，encrypted-password 默认为空。
【命令模式】 cwmp 配置模式
【使用指导】 -

配置 ACS 连接 CPE 时用于认证的用户名

- CPE 设备上必须配置。
- 只能配置一个 CPE 用户名，多次配置 CPE 的用户名时，最新的配置生效。

【命令格式】 **cpe username** *username*
【参数说明】 *Username:* 配置 ACS 连接 CPE 用于认证的用户名
【缺省配置】 无默认 CPE 用户名
【命令模式】 cwmp 配置模式
【使用指导】 -

配置 ACS 连接 CPE 时用于认证的密码

- CPE 设备上必须配置。
- CPE 用户密码可以为明文和密文形式，只能配置一个 CPE 用户密码，多次配置 CPE 的用户密码时，最新的配置生效。

【命令格式】 **cpe password** {*password* | *encryption-type* *encrypted-password*}

【参数说明】 *password:*ACS 连接 CPE 用于认证的密码。

encryption-type: 可配置为 0 或 7，为 0 表示无加密，为 7 表示简单加密

encrypted-password: 密码文本

【缺省配置】 encryption-type 默认为 0，encrypted-password 默认为空。

【命令模式】 cwmp 配置模式

【使用指导】 配置 ACS 连接 CPE 用于认证的密码，通常无须输入加密类型。一般情况下，只有当复制并粘贴已经加密过后该命令的密码时，才需要输入加密类型。有效密码的格式要求如下：

- 必须包含 1 到 26 个大小写字母和数字字符。
- 密码前面可以有前导空格，但被忽略。中间及结尾的空格则作为密码的一部分。
- encryption-type 为 7 时，输入的合法字符只能是数字 0~9、字符 a~f、A~F。

配置 CPE 连接 ACS 的 URL

- 可选配置，在 CPE 设备上配置。
- 只能配置一个 ACS URL，多次配置 ACS 的 URL 时，最新的配置生效，ACS 的 URL 必须是 HTTP 的形式。

【命令格式】 **acs url** *url*

【参数说明】 *url*：ACS 的 URL。

【缺省配置】 无默认 ACS URL

【命令模式】 CWMP 配置模式

【使用指导】 配置 CPE 连接 ACS 的 URL，在没有手动配置 ACS URL 的情况下，如果使用了 DHCP 获取到了动态的 ACS URL，将使用动态获取到的 ACS URL 向 ACS 发起连接。对 ACS 的 URL 格式要求如下：

- ACS 的 URL 格式必须为：http://host[:port]/path（或是 https://host[:port]/path）的格式。
- ACS URL 的最大长度为 255 个字符。

配置 ACS 连接 CPE 的 URL

- 可选配置，CPE 设备上配置。
- 只能配置一个 CPE URL，多次配置 CPE 的 URL 时，最新的配置生效。CPE 的 URL 必须是 HTTP 的形式，不支持域名的形式配置 CPE 的 URL。

【命令格式】 **cpe url** *url*

【参数说明】 *url*：cpe 的 URL。

【缺省配置】 无默认 CPE URL

【命令模式】 cwmp 配置模式

【使用指导】 配置 ACS 连接 CPE 的 URL，在没有手动配置的情况下，CPE 将根据 ACS 的 URL 自动选取 CPE 的 URL，CPE 的 URL 格式要求如下：

- CPE 的 URL 必须是 http://ip [: port]/″ 的格式。
- CPE URL 的最大长度为 255 个字符。

检验方法

- 通过 **show cwmp configuration** 命令查看。

【命令格式】 **show cwmp configuration**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 -

【命令展示】 1：显示 CWMP 功能的当前配置。

```
Ruijie(config-cwmp)#show cwmp configuration
CWMP Status                     : enable
ACS URL                         : http://www.ruijie.com.cn/acs
ACS username                    : admin
ACS password                    : ******
CPE URL                         : http://10.10.10.2:7547/
CPE username                    : ruijie
CPE password                    : ******
CPE inform status               : disable
CPE inform interval             : 60s
CPE inform start time           : 0:0:0 0 0 0
CPE wait timeout                : 50s
CPE download status             : enable
CPE upload status               : enable
CPE back up status              : enable
CPE back up delay time          : 60s
```

配置举例

以下配置举例，仅介绍 CWMP 相关的配置。

在 CPE 设备上配置用户名和秘码

【网络环境】

图 8-6

【配置方法】
- 使能 CWMP
- 在 CPE 设备上配置 CPE 连接 ACS 时用于认证的用户名和密码
- 在 CPE 设备上配置 ACS 连接 CPE 时用于认证的用户名和密码

CPE

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Ruijie(config)# cwmp
Ruijie(config-cwmp)# acs username USERB
Ruijie(config-cwmp)# acs password PASSWORDB
Ruijie(config-cwmp)# cpe username USERB
Ruijie(config-cwmp)# cpe password PASSWORDB
```

【检验方法】 ● 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

CPE

```
Ruijie # show cwmp configuration
CWMP Status                    : enable
ACS URL                        : http://10.10.10.1:7547/acs
ACS username                   : USERA
ACS password                   : ******
CPE URL                        : http://10.10.10.2:7547/
CPE username                   : USERB
CPE password                   : ******
```

配置 ACS 和 CPE 的 URL 连接

【网络环境】 同 图 8-6

【配置方法】 ● 配置 ACS 设备的 URL 地址

● 配置 CPE 设备的 URL 地址

CPE

```
Ruijie# configure terminal
Ruijie(config)# cwmp
Ruijie(config-cwmp)# acs url http://10.10.10.1:7547/acs
Ruijie(config-cwmp)# cpe url http://10.10.10.1:7547/
```

【检验方法】 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

CPE

```
Ruijie #show cwmp configuration
CWMP Status                    : enable
ACS URL                        : http://10.10.10.1:7547/acs
ACS username                   : USERA
ACS password                   : ******
CPE URL                        : http://10.10.10.2:7547/
```

常见错误

- 如果用户输入密码类型为密文，密文长度不为大于 2 且不超过 254 的偶数，则提示错误；
- 如果用户输入密码类型为明文，密码长度超过 126，则提示错误；
- 如果用户输入密码类型为明文，并且包含非法字符，则提示错误；

-
- 如果 ACS URL 地址为 NULL，则提示错误；
- 如果 CPE URL 地址为 NULL，则提示错误。

8.4.2 配置CWMP相关属性

配置效果

- 用于实现 CPE 设备常用功能的配置(如主程序/配置备份恢复，是否接受 ACS 下发主程序及配置文件，是否向 ACS 上传配置文件和日志文件等)

配置方法

↘ 配置 CPE 周期性通告功能

- 可选配置，单位为秒，取值范围 30～3600，缺省值 600s。
- 当 CPE 设备需要重新设定周期性通告时间的时候配置该功能。

【命令格式】 **cpe inform** [**interval** *seconds*] [**starttime** *time*]

【参数说明】 *seconds*： 配置 CPE 周期性 INFORM 通告时间间隔。单位为秒，取值范围 30～3600，缺省值 600。

time：开始周期性 INFORM 的日期时间，格式为 yyyy-mm-ddThh:mm:ss

【缺省配置】 CPE 的 INFORM 通告时间间隔为 600 秒

【命令模式】 cwmp 配置模式

【使用指导】 配置 CPE 周期性 INFORM 通告功能。

- 在没有配置 INFORM 开始时间的情况下，周期性 INFORM 从开启该功能开启，每经过一个 INFORM 周期通告一次。
- 在配置了 INFORM 开始日期时间的情况下，周期性 INFORM 的开始时间为该指定时间。如配置 INFORM 周期为 60 秒，开始时间为明天中午 12 点，则周期性 INFORM 通告从明天中午 12 点才开始，且每经过 60 秒 INFORM 通告一次。

↘ 配置关闭从 ACS 下载主程序和配置文件的功能

- 可选配置，默认开启下载主程序和配置文件的功能。
- 当 CPE 设备要关闭下载主程序和配置文件功能的时候，配置该功能。

【命令格式】 **disable download**

【参数说明】 -

【缺省配置】 CPE 文件下载功能为默认允许接收

【命令模式】 cwmp 配置模式

【使用指导】 配置关闭从 ACS 下载主程序和配置文件的功能。

- 这个命令对配置脚本文件不起作用，配置 disable 的情况下，配置脚本可以执行。

配置关闭向 ACS 上传配置文件和日志文件的功能

- 可选配置，默认为开启上传配置和日志文件功能。
- 当 CPE 设备要关闭上传配置文件和日志文件功能的时候，配置该功能。

【命令格式】 **disable upload**
【参数说明】
【缺省配置】 CPE 文件上传功能为开启
【命令模式】 cwmp 配置模式
【使用指导】 配置关闭向 ACS 上传配置和日志文件的功能。

配置 CPE 主程序/配置备份恢复功能

- 可选配置，默认开启 CPE 主程序/配置备份恢复功能，单位为秒，取值范围 30-10000，默认备份恢复时间为 60s。
- 恢复时间设置越大，CPE 启动恢复延迟时间越久。
- 当 CPE 设备需要修改 CPE 主程序/配置备份恢复功能的时间时，配置该功能。

【命令格式】 **cpe back-up** [**delay-time** *seconds*]
【参数说明】 *seconds:* CPE 主程序/配置备份恢复的延迟时间
【缺省配置】 CPE 备份恢复功能为开启，默认恢复时间为 60s
【命令模式】 cwmp 配置模式
【使用指导】 -

配置 ACS 无响应 CPE 超时时间

- 可选配置，单位为秒，取值范围 5～600，默认值为 5s。
- CPE 设备上配置，当 CPE 设备需要修改 ACS 无响应 CPE 超时时间时，配置该功能。

【命令格式】 **timer cpe- timeout** *seconds*
【参数说明】 *seconds:* 超时时间，单位为秒，取值范围 5～600。
【缺省配置】 默认值为 5 秒。
【命令模式】 cwmp 配置模式
【使用指导】 -

检验方法

- 通过 **show cwmp configuration** 命令查看。

【命令格式】 **show cwmp configuration**
【参数说明】 -
【命令模式】 特权模式
【使用指导】 -
【命令展示】 1：显示 CWMP 功能的当前配置。

```
Ruijie(config-cwmp)#show cwmp configuration
CWMP Status                    : enable
```

```
ACS URL                         : http://www.ruijie.com.cn/acs
ACS username                    : admin
ACS password                    : ******
CPE URL                         : http://10.10.10.2:7547/
CPE username                    : ruijie
CPE password                    : ******
CPE inform status               : disable
CPE inform interval             : 60s
CPE inform start time           : 0:0:0 0 0 0
CPE wait timeout                : 50s
CPE download status             : enable
CPE upload status               : enable
CPE back up status              : enable
CPE back up delay time          : 60s
```

配置举例

配置 CPE 周期 INFORM 通告时间间隔

【网络环境】 同 图 8-6

【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
- 配置 CPE 周期 INFORM 通告时间间隔为 60 秒

CPE

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#cpe inform interval 60
```

【检验方法】 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

CPE

```
Ruijie #show cwmp configuration
CWMP Status                     : enable
……
CPE inform interval             : 60s
```

配置关闭从 ACS 下载主程序和配置文件的功能

【网络环境】 同 图 8-6

【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
- 配置关闭从 ACS 下载主程序和配置文件的功能

CPE

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)#disable download
```

【检验方法】 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

CPE

```
Ruijie #show cwmp configuration
CWMP Status                     : enable
……
CPE download status             : disable
```

配置关闭向 ACS 上传配置文件和日志文件的功能

【网络环境】 同 图 8-6

【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
- 配置关闭向 ACS 上传配置文件和日志文件的功能

CPE

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)# disable upload
```

【检验方法】 通过在 CPE 设备上 **show** 命令查看命令是否配置成功

CPE

```
Ruijie #show cwmp configuration
CWMP Status                     : enable
……
CPE upload status              : disable
```

配置备份恢复的延迟时间

【网络环境】 同 图 8-6

【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
- 配置备份恢复的延迟时间为 30s

CPE

```
Ruijie#config
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)#cwmp
Ruijie(config-cwmp)# cpe back-up Seconds 30
```

【检验方法】
- 通过在 CPE 设备上 show 命令查看命令是否配置成功

CPE

```
Ruijie #show cwmp configuration
CWMP Status                     : enable
......
CPE back up delay time          : 30s
```

配置 CPE 无数据超时时间

【网络环境】 同 图 8-6

【配置方法】
- 开启 CWMP 功能并进入 CWMP 配置模式
- 配置备份恢复的延迟时间为 100s

CPE

```
Ruijie# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Ruijie(config)# cwmp
Ruijie(config-cwmp)# timer cpe-timeout 100
```

【检验方法】
- 通过在 CPE 设备上 show 命令查看命令是否配置成功

CPE

```
Ruijie#show cwmp configuration
CWMP Status                     : enable
......
CPE wait timeout                : 100s
```

常见配置错误

无

8.5 监视与维护

查看运行情况

作用	命令
显示 CWMP 功能的当前配置	**show cwmp configuration**
显示 CWMP 的当前运行状态	**show cwmp status**

9 LED

9.1 概述

LED（LightingEmittingDiode）即发光二极管的简称，是一种半导体固体发光器件。在 AP 上用来做状态指示灯，根据 AP 的不同状态，显示不同的颜色。

下文仅介绍 LED 的相关内容。

协议规范

无

9.2 典型应用

无

9.3 功能详解

我司 AP 上通常都有一个或者多个 LED 灯，用来表示 AP 的工作状态。例如，以太口有数据流的时候，以太口的 LED 灯就会闪烁。通常 LED 灯是通过 GPIO 或者 CPLD 来控制的，通过操作 GPIO 或者 CPLD，来改变灯的颜色状态，例如，绿色常亮、绿色闪烁和红色闪烁等。通过 LED 灯的不同颜色状态，来判断 AP 的工作状态是否正常。当 AP 出现故障时，也可以很容易通过灯的颜色状态来初步得出 AP 是什么故障。

9.4 配置详解

配置项	配置建议 & 相关命令	
配置静默模式	可选配置。配置 led 灯为静默状态	
	quiet-mode session	配置 led 静默模式

9.4.1 配置静默模式

配置效果

- 配置生效时，AP 上所有 LED 灯都会熄灭。

注意事项

- 必须先配置静默状态生效的时间

配置方法

↘ 配置 session

- 可选配置。
- 配置静默模式时，必须要向创建 session
- 配置 session 生效的时间

【命令格式】 **schedule session** *sid* **time-range** *n* **period** *day1* [**to** *day2*] **time** *hh1:mm1* **to** *hh2:mm2*

【参数说明】 sid：调度 session ID

n：调度 session 时间段编号

day1：调度 session 时间段的周期，day1 表示调度周期开始日期。日期有效值 { sun | mon | tue | wed | thu | fri | sat }

to day2：day2 表示调度周期结束日期，to day2 缺省表示调度时间段的周期只有一天。

time hh1:mm1 to hh2:mm2：调度 session 时间范围：hh1:mm1 和 hh2:mm2 分别是起始时间和结束时间的小时和分钟。小时取值范围[0，23]，分钟取值范围[0，59]

【缺省配置】 调度 session 时间段为空

【命令模式】 全局配置模式

【使用指导】 必现先创建一个 session

↘ 配置静默模式

- 可选配置。
- 配置 led 静默模式的 session

【命令格式】 **quiet-mode session** *session-num*

【参数说明】 session-num：指定 session-id

【缺省配置】 缺省是关闭的

【配置模式】 AP 配置模式

【使用指导】 必须先配置 session

检验方法

- 当系统时间在静默模式的时间范围内时，AP 上的所有 LED 都不亮。

配置举例

↘ 配置每周一晚上 11 点到周二早上 7 点的 LED 灯为静默模式

【配置方法】
- 配置 session
- 配置静默模式使用的 session-id

```
Ruijie# configure terminal
Ruijie(config)#schedule session 1
Ruijie(config)#schedule session 1 time-range 1 period Mon time 23:00 to 7:00
Ruijie(config)#ap-config 00d0.f822.33bc
Ruijie(config-ap)#quiet-mode session 1
```

【检验方法】 当系统时间在 session 配置的时间范围内时，AP 上所有的 LED 灯都会熄灭

常见配置错误

- 配置的 session id 不存在

9.5 监视与维护

清除各类信息

无

查看运行情况

无

查看调试信息

无

10 PKG_MGMT

10.1 概述

Package Management 是 RGOS 系统的包管理及升级模块，负责对设备内各个组件安装、升降级、查询、维护，其中升级是主要功能。通过对设备的软件进行升级，用户可以在系统上安装更加稳定的或含有更多的特性的软件版本，RGOS 系统采用模块化的构成方式，系统既可以进行整体升级和子系统的升级，也可以进行各个功能包的独立升级，还能以热补丁方式升级。

本文描述的组件升级涵盖了盒式设备和机架设备的组件升级，且本文只针对 11.0 以后的各项目平台，不涉及 11.0 以前项目升级到 11.0 以后项目。

协议规范

无

10.2 典型应用

典型应用	场景描述
升降级子系统组件	升降级盒式和机架设备的 boot，kernel，rootfs 等子系统组件。
升降级单个功能组件包	升降级盒式和机架设备单个功能组件包。
安装热补丁包	安装热补丁，对功能组件的某一部分进行修补。

10.2.1 升降级子系统组件

应用场景

升级子系统组件包，完成升级后设备内原先的系统软件全部被更新，整体软件功能得到增强。通常盒式设备子系统组件包称为 main 包。

该升级方式的主要特点是：升级完成后设备内所有软件都将更新，所有已知软件 bug 都将得到完整解决，但升级过程较长。

功能部署

盒式设备升级前可以将 main 包放在 TFTP 服务器程序的根目录下，通过网络下载设备内，再执行本地升级命令完成升级；也可以将 main 包拷贝到 U 盘内，插入设备再执行升级命令完成升级。

10.2.2 升降级单个功能组件包

应用场景

设备软件由若干功能组件组成，每个功能组件都是一个独立的功能模块。升级独立的功能组件包，在完成升级后仅该安装包对应功能模块的缺陷得到了修订、或者功能组件得到了增强，其它功能组件保持不变。

该升级场景的特点是：功能组件包通常较小，升级速度较快，升级完成后仅对应的功能模块得到改善，其它功能模块保持不变。

功能部署

升级功能组件包前，可以将其存放在TFTP服务器的根目录，通过网络下载安装到本地完成升级。也可将包存放在U盘内，插入设备完成升级。

10.2.3 安装热补丁包

应用场景

如果需要在不重启设备的条件下完成软件缺陷的修复，可安装热补丁包。该包仅适用于对特定软件版本的修复。通常只有当用户环境不能重启设备时，才会针对该软件版本发布专门的热补丁包用于缺陷修复。
热补丁升级最显著的特点是：升级完成后，设备无需重启即可修复缺陷。

功能部署

升级热补丁包前，可以将其存放在TFTP服务器的根目录，通过网络下载安装到本地完成升级，也可将包存放在U盘内，插入设备完成热补丁升级。

10.3 功能详解

基本概念

子系统

子系统以映像的方式存储于设备，RGOS 的子系统包括：

- boot：设备上电启动首先加载 boot 运行，它负责设备的基础初始化，加载并运行系统映像。
- kernel：它是系统的 OS 核心部分，负责屏蔽系统的硬件构成、给应用程序提供抽象的运行环境。
- rootfs：它是系统中应用程序的集合。

main 安装包

盒式设备子系统升降级时往往使用 main 安装包，该包是 boot，kernel 和 rootfs 子系统的合并包。该包可以用来完成系统整体升降级。

RGOS 的功能组件包

RGOS的功能组件包则是指实现某个功能的集合，在设备出厂时，所有已支持的功能均已包含在rootfs子系统中，通过升级单个功能组件包可以只更新系统内特定功能或特性。

热补丁包

热补丁包包含了若干功能组件的热补丁，升级该包可以依次为各功能组件包打上补丁，并且无需重启设备立刻具有新的功能特性。

⚠ 本文中的“安装包”均指包含子系统或功能模块的安装文件。

功能特性

功能特性	作用
子系统组件升降级及管理	升降级子系统。
功能组件升降级及热补丁包的安装	升降级功能组件或安装热补丁包。
功能组件及热补丁的管理	方便用户查询设备中存在的功能组件包及其版本和安装信息。

10.3.1 子系统组件升降级及管理

子系统的升降级就是将安装包内的子系统组件替换设备内的子系统组件，达到软件功能更新的目的。因为存在子系统冗余设计，所以升降级时往往并不是直接覆盖设备内当前正在使用的子系统，而是在设备内新增子系统然后再激活新增子系统。

工作原理

↘ 升降级

各子系统在设备内存在的形式各有不同，因此对子系统的升降级方式也各有差别：

- boot：该子系统一般以映像形式存在于 norflash 设备内，所以该子系统的升降级就是将映像写入 norflash 设备。
- kernel：该子系统以文件形式存在于特定分区，所以该子系统的升降级就是文件的写入。
- rootfs：该子系统一般以映像形式存在于 nandflash 设备内，所以该子系统的升降级就是将映像写入 nandflash 设备。

↘ 管理

查询当前有哪些子系统组件可用，之后依据实际需求，有选择性的加载子系统组件。

各子系统组件都包含冗余设计，在升降级过程中：

- boot：始终存在主、从两个 boot，升级只涉及主 boot，从 boot 始终冗余。
- kernel：至少存在一个冗余备份，若空间足够可存在多个冗余。
- rootfs：始终存在一个冗余备份。

对于 boot 组件因为较为特殊，并不将该组件纳入子系统管理的范畴。在升级 kernel 或 rootfs 子系统组件时升降级模块总是在配置文件记录当前使用的子系统组件和冗余的子系统组件以及各种版本管理信息。

相关配置

↘ 升级

- 将升级文件存放在设备本地后，使用 **upgrade** 命令升级。

10.3.2 功能组件升降级及管理

工作原理

功能组件升级的原理实际上就是组件文件的替换过程，即包内的组件文件替换设备中的组件文件。

功能组件及热补丁的管理是利用数据库记录功能组件和热补丁的信息。安装组件，显示组件信息，卸载组件实际上就是数据库添加，查询，删除的结果。

另外，需要注意当系统进行过补丁升级后，就不能再进行组件升级。

相关配置

↘ 升级

- 将升级文件存放在设备本地后，使用 **upgrade** 命令升级。

10.3.3 热补丁包的升降级及管理

工作原理

功能组件升级的原理实际上就是组件文件的替换过程，即包内的组件文件替换设备中的组件文件。
热补丁包升级原理类似，不同之处在于它只替换需要修订的文件，并且文件替换完成后，新文件自动生效。
另外，需要注意当系统进行过组件升级后，就不能再进行补丁升级。

↘ 管理

热补丁的管理同功能组件一样包含查询、安装、卸载等，这些操作对应着数据库的插入，查询、删除等操作。
热补丁和功能组件的管理是基于同一技术原理实现的，但是热补丁的不同之处在于，热补丁包含未安装，已安装，已激活这三种状态，其中：
已安装仅仅表明设备内存在热补丁，但是该补丁功能并没有真正生效，
已激活状态的热补丁才真正有效。

相关配置

↘ 升级

- 将升级文件存放在设备本地文件系统中后，使用 **upgrade** 命令升级。

↘ 热补丁的激活

- 使用 **patch active** 命令临时激活已安装的补丁，设备重启后补丁作用失效，需重新激活；
- 或使用 **patch running** 命令永久激活已安装的补丁，设备重启后仍然生效。
- 未激活的补丁不会真正生效。

↘ 热补丁的失效

- 如果需要使已激活的补丁失效，可通过 **patch deactive** 命令完成。

↘ 卸载热补丁

- **patch delete** 用于卸载热补丁。

10.4 配置详解

配置项	配置建议 & 相关命令
安装包升降级	⚠ 基本功能，用于子系统组件包，功能组件包及热补丁包的安装，升降级。该命令对于盒式、机架设备均有效

	upgrade *url*	*url* 为安装包存放的本地路径。该命令用于升级设备内存放的安装包。
	upgrade download tftp://*path*	*path* 为 tftp 服务器上安装包的路径，该命令自动从服务器上下载安装包，并自动升级

10.4.1 安装包升降级

配置效果

可用安装包包括板卡设备对应的 main 安装包，各功能组件包，热补丁包。

- 升级板卡设备对应的 main 安装包，完成升级后该板卡设备内原先的系统软件全部被更新，整体软件功能得到增强。
- 升级独立的功能组件包，在完成升级后仅该安装包对应功能模块的 bug 得到了修订，功能组件得到了增强，其它功能组件保持不变。
- 升级热补丁包，即在不重启设备的条件下完成软件缺陷修复，该包仅适用于对特定软件版本的升级。

通常发布 main 包来升级盒式设备。

注意事项

-

配置方法

升级板卡设备对应的 main 安装包

- 可选配置。设备内原先的系统软件全部需要被更新时，选择此配置项。
- 升级前需要将安装包下载到设备本地，使用 **upgrade** 命令升级。

通常发布 main 包来升级盒式设备

升级各功能组件包

- 可选配置。如果仅需要对某功能模块的缺陷进行修复，或增强该功能模块的性能的话，选择此配置项。
- 升级前需要将安装包下载到设备本地，使用 **upgrade** 命令升级。

升级热补丁包

- 可选配置。如果需要在不重启设备的条件下完成软件 bug 修订，选择此配置项。
- 升级前需要将安装包下载到设备本地。使用 **upgrade** 命令升级。
- 升级后需要激活补丁方能使用，该步骤是必选配置。激活方式有两种：使用 **patch active** 命令临时激活已安装的补丁；或使用 **patch running** 命令永久激活已安装的补丁。

用户场景下通常要求使用 **patch running** 命令永久激活补丁。仅当用户打算临时验证补丁功能时可使用 **patch active** 命令激活补丁。

↘ 子系统回滚

- 可选配置。如果需要将子系统回滚到升级前的状态，选择此配置，作用是使系统回归到升级前的状态。
- 使用 **upgrade** 命令升级子系统组件后（如 main 包）该配置才能生效。

⚠ 用户场景下使用 **upgrade** 命令升级子系统组件成功后，回滚命令仅能生效一次，不可连续回滚。

检验方法

- 完成升级子系统组件后可执行 **show upgrade history** 命令查看是否升级成功。
- 完成升级功能组件后可执行 **show component** 命令查看是否升级成功。
- 完成升级热补丁包后可执行 **show patch** 命令查看是否升级成功。

相关命令

↘ 查看设备内存放的安装包文件信息

【命令格式】 **show upgrade file** *url*

【参数说明】 *url* 设备文件系统内安装包存放路径

【命令模式】 特权模式

【使用指导】 -

↘ 显示当前系统升级历史信息

【命令格式】 **show upgrade history**

【参数说明】 无

【命令模式】 特权模式

【使用指导】 -

↘ 显示设备内可用的子系统组件

【命令格式】 **show subsys**

【参数说明】 **-**

【命令模式】 特权模式

【使用指导】 -

↘ 子系统组件回滚

【命令格式】 **upgrade rollback**

【参数说明】 **-**

【命令模式】 特权模式

【使用指导】 该命令撤销上一次子系统升级操作，使子系统返回升级前的状态。只有上次升级的是子系统且子系统升级成功才能进行回滚操作，回滚命令无法连续执行。

↘ 显示已安装的功能组件

【命令格式】 **show component**

【参数说明】 [*component _name*] 组件名称。

当不存在此参数值时：命令用于显示设备中所有已安装的组件及各组件的基本信息。

当存在此参数值时：命令用于显示对应组件的详细信息，并校验组件内容是否完整，检测该组件能否正常工作。

【命令模式】 特权模式

【使用指导】 -

↘ 显示安装的补丁包信息

【命令格式】 **show patch** [*package _name*]

【参数说明】 -

【命令模式】 特权模式

【使用指导】 -

↘ 临时激活已安装的补丁

【命令格式】 **patch active**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 只能对已安装补丁的设备执行该操作。该命令只能临时激活补丁，设备重启后补丁作用失效。

↘ 永久激活已安装的补丁

【命令格式】 **patch running**

【参数说明】 -

【命令模式】 特权模式

【使用指导】 只能对已安装补丁的设备执行该操作。该命令可永久激活补丁。

配置举例

↘ 盒式设备子系统安装包升级举例

【网络环境】 升级前必须将安装包拷入设备内，升级模块提供以下几种解决方案。

- 用户首先使用 **copy tftp**，**copy xmodem** 等文件系统命令将服务器上的安装包拷入设备文件系统，再使用 **upgrade** *url* 升级本地文件系统内的安装包；
- 直接使用 **upgrade download tftp:**//*path* 命令升级 tftp 服务器端存放的安装包文件；
- 将安装包拷入 U 盘内并插入设备，使用 **upgrade** *url* 命令升级位于 U 盘内的安装包。

【配置方法】

- 执行升级命令
- 完成子系统升级后设备重启生效

```
Ruijie# upgrade download tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin
Accessing tftp://192.168.201.98/eg1000m_main_1.0.0.0f328e91.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
 Upgrade processing is 10%
 Upgrade processing is 60%
 Upgrade processing is 90%

 Upgrade info [OK]
         Kernel version[2.6.32.91f9d21->2.6.32.9f8b56f]
         Rootfs version[1.0.0.2ad02537->1.0.0.1bcc12e8]
```

```
 Upgrade processing is 100%
 Reload system to take effect!
Reload system?(Y/N)y
 Restarting system.
```

【检验方法】

- 查看当前设备运行的版本信息，若版本信息发生变换说明升级成功

```
Ruijie#show upgrade history
Last Upgrade Information:
    Time:         2014-08-31 12:15:03
    Method:       LOCAL
Package Name: N18000_RGOS11.0(1)B1_CM_01200616_install.bin
Package Type: Distribution
```

↘ 盒式设备功能包升级举例

【网络环境】 升级前必须将安装包拷入设备内，升级模块提供以下几种解决方案。

- 用户首先使用 **copy tftp**，**copy xmodem** 等文件系统命令将服务器上的安装包拷入设备文件系统，再使用 **upgrade** *url* 升级本地文件系统内的安装包；
- 直接使用 **upgrade download tftp://***path* 命令升级 tftp 服务器端存放的安装包文件；
- 将安装包拷入 U 盘内并插入设备，使用 **upgrade** *url* 命令升级位于 U 盘内的安装包。
-

【配置方法】

- 执行升级命令
- 依照升级后的提示确定是否需要设备重启

```
Ruijie#upgrade sata0://bridge_eg1000m_2.3.1.1252ea-1.mips.rpm
  Upgrade processing is 10%
  Upgrade processing is 60%
  Upgrade processing is 90%

  Upgrade info [OK]
          bridge version[2.0.1.37cd5cda ->2.3.1.1252ea] [OK]
  Upgrade processing is 100%
  Reload system to take effect!
Reload system?(Y/N)y
Restarting system.
```

【检验方法】

- 查看当前设备功能组件版本信息，若版本信息发生变换说明升级成功

```
Ruijie# show component
 Package  :sysmonit
     Version:1.0.1.23cd34aa      Build time: Wed Dec  7 00:58:56 2011
     Size:12877    Install time :Wed  Mar 5 14:23:12 2012
     Description:this is a system monit package
     Required packages: None
```

```
------------------------------------------------------------------
package:bridge
    Version: 2.3.1.1252ea       Build time: Wed Dec  7 00:54:56 2011
    Size:26945    Install time : Wed Mar 19:23:15 2012
    Description:this is a bridge package
    Required packages: None
```

↘ 盒式设备补丁包安装举例

【网络环境】 升级前必须将安装包拷入设备内，升级模块提供以下几种解决方案。

- 用户首先使用 **copy tftp**，**copy xmodem** 等文件系统命令将服务器上的安装包拷入设备文件系统，再使用 **upgrade** *url* 升级本地文件系统内的安装包；
- 直接使用 **upgrade download tftp://***path* 命令升级 tftp 服务器端存放的安装包文件；
- 将安装包拷入 U 盘内并插入设备，使用 **upgrade** *url* 命令升级位于 U 盘内的安装包。

【配置方法】

- 执行升级命令
- 激活热补丁

```
Ruijie#upgrade download tftp://192.168.201.98/eg1000m_RGOS11.0(1C2)_20131008_patch.bin
Accessing tftp://192.168.201.98/eg1000m_RGOS11.0(1C2)_20131008_patch.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!
Transmission finished, file length 9868 bytes.
 Upgrade processing is 10%
 Upgrade processing is 60%

 Upgrade info [OK]
   patch_bridge version[1.0.0.1952]
 Upgrade processing is 90%

 Upgrade info [OK]
   patch_install version[1.0.0.192e35a]
Ruijie#patch running
 The patch on the system now is in running status
```

【检验方法】

- 查看当前设备安装热补丁信息

```
Ruijie# show patch
:patch package patch_install installed in the system, version:pa1
 Package : patch_bridge
 Status：running
 Version: pa1       Build time: Mon May 13 09:03:07 2013
     Size: 277      Install time: Tue May 21 03:07:17 2013
```

```
    Description: a patch for bridge
    Required packages: None
```

盒式设备子系统升级回滚配置举例

⚠ 只有当上次升级的是子系统且子系统升级成功才能进行子系统回滚操作，回滚命令无法连续执行

【网络环境】 升级前必须将安装包拷入设备内，升级模块提供以下几种解决方案。

- 用户首先使用 **copy tftp**，**copy xmodem** 等文件系统命令将服务器上的安装包拷入设备文件系统，再使用 **upgrade** *url* 升级本地文件系统内的安装包；
- 直接使用 **upgrade download tftp:**//*path* 命令升级 tftp 服务器端存放的安装包文件；
- 将安装包拷入 U 盘内并插入设备，使用 **upgrade** *url* 命令升级位于 U 盘内的安装包。

【配置方法】

- 执行子系统回滚命令
- 设备重启后回滚生效

```
Ruijie#upgrade rollback
 kernel rollback version[2.6.32.9f8b56f->2.6.32.91f9d21][OK]
 rootfs rollback version[1.0.0.1bcc12e8->1.0.0.2ad02537][OK]
 Rollback success!
 Reload system to take effect!
Reload system?(Y/N)y
Restarting system.
```

【检验方法】

- 查看当前设备运行的版本信息，若版本回复到升级前状态则子系统回滚成功

```
Ruijie#show upgrade history
Last Upgrade Information:
    Time:         2014-08-31 12:15:03
    Method:       LOCAL
Package Name: N18000_RGOS11.0(1)B1_CM_01200616_install.bin
Package Type: Distribution
```

常见错误

若升级过程中出现错误，升级模块会加以提示例如：

```
Upgrade info [ERR]
      Reason:creat config file err(217)
```

常见错误提示有以下几种：

- 安装包无效：可能的原因是该安装包已经被损坏或者根本不是一个安装包。该错误的处理方式要求用户重新获取安装包，再执行升级操作。
- 设备不支持安装包：可能的原因是误用了其它设备的安装包。该错误的处理方式要求用户重新获取并核对安装包后在执行升级操作。
- 设备空间不足：通常出现在机架设备中。该错误的处理方式是要求用户检查设备是否存在 U 盘，按要求这些设备往往附带 U 盘。

10.4.2 热补丁的失效与卸载

配置效果

使已激活的热补丁失效或者卸载热补丁。

注意事项

- 未激活的热补丁不生效，所以未激活的热补丁不能使其失效。

配置方法

↘ 使已激活的补丁失效

- 可选配置。如果需要使已激活的补丁失效，可通过 **patch deactive** 命令完成。

↘ 卸载热补丁

- 可选配置。如果需要卸载已安装的热补丁，可使用 **patch delete** 命令完成。

检验方法

- 可使用 **show patch** 命令检测补丁是否被激活或已经被卸载。

相关命令

↘ 使已激活的补丁作用失效

【命令格式】 **upgrade auto-sync policy**
【参数说明】 **-**
【命令模式】 特权模式
【使用指导】 只有对处于激活状态的补丁才能执行该操作，该操作使对应补丁失效。

↘ 卸载热补丁

【命令格式】 **patch delete**
【参数说明】 **-**
【命令模式】 特权模式
【使用指导】 用于清除设备上已存在的热补丁包。

配置举例

↘ 盒式设备使补丁作用失效并卸载补丁

【配置方法】
- 执行补丁失效命令
- 执行补丁卸载命令

```
Ruijie#patch deactive
Deactive the patch package success
Ruijie# patch delete
Clear the patch patch_bridge success
Clear the patch success
```

【检验方法】
- 查看补丁状态信息

```
Ruijie#show patch
No patch package installed in the system
```

常见配置错误

- 补丁未处于激活状态时就执行**patch deactive**命令。解决方法确认补丁所处的状态，只有当提示status：running时，才能执行 **patch deactive** 命令。

10.5 监视与维护

清除各类信息

作用	命令
删除已安装的热补丁包	**patch delete**

查看运行情况

作用	命令
显示当前设备已安装所有组件及各组件信息。	**show component** [*cpmponent _name*]
显示设备中已安装的热补丁包的相关信息。	**show patch** [*patch _name*]
显示存放在设备中可用的 kernel，rootfs 子系统组件，并指明设备将加载哪些 kernel，rootfs 组件。	**show subsys**
显示升级历史信息	**show upgrade history**

11 NTP

11.1 概述

NTP（Network Time Protocol，网络时间协议），用来使网络设备时间同步化的一种应用层协议。它可以使网络设备对其服务器或时钟源做同步化，提供高精准度的时间校正（LAN 上与标准时间差小于 1 毫秒，WAN 上几十毫秒），且可使用加密确认的方式来防止攻击。

目前我司设备支持 NTP 的客户端与服务器功能，即设备既可以从时间服务器上同步时间，也能够作为时间服务器对其他设备进行时间同步。在作为服务器工作时设备仅支持单播 Server 模式。

协议规范

- RFC 1305 ： Network Time Protocol (Version 3)

11.2 典型应用

典型应用	场景描述
基于外部时钟参考源同步时间	设备即作为客户端从外部时钟源同步时间，同步成功后又作为服务器向其他设备提供时间同步服务。
基于本地时钟参考源同步时间	设备将本地时钟作为 NTP 可靠参考时钟源，作为服务器向其它设备提供时间同步服务。

11.2.1 基于外部时钟参考源同步时间

应用场景

如图所示：

- DEVICE-A 作为可靠参考时钟源对外提供时间同步服务
- DEVICE-B 指定 DEVICE-A 为 NTP 服务器，从 DEVICE-A 同步时间。
- DEVICE-B 同步成功后向 DEVICE-C 提供时间同步服务。

图 11-1

功能部属

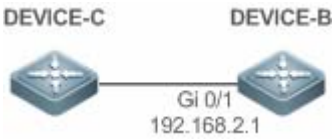
将 DEVICE-B 配置为 NTP 外部时钟参考模式

11.2.2 基于本地时钟参考源同步时间

应用场景

如图所示，DEVICE-B 将本地时钟作为 NTP 参考时钟源，向 DEVICE-C 提供时间同步服务。

图 11-2



功能部属

将 DEVICE-B 配置为 NTP 本地时钟参考模式。

11.3 功能详解

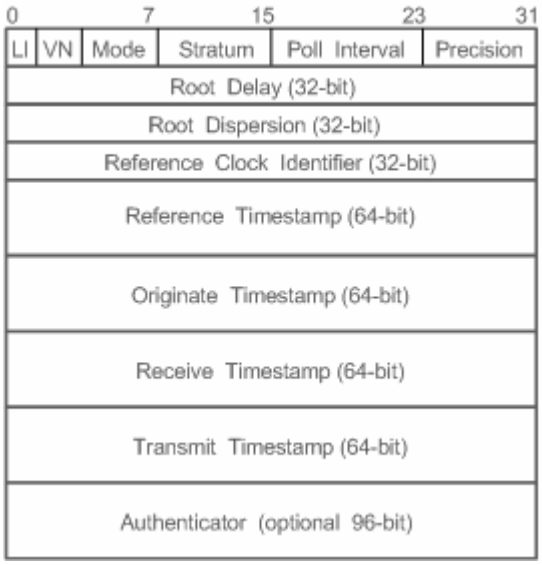
基本概念

↘ NTP 报文

根据 RFC1305 定义，NTP 采用 UDP 报文进行传输，UDP 端口号为 123。

NTP时间同步报文格式如 图 11-3

图 11-3 NTP 时间同步报文格式



- Leap Indicator（LI）：2 比特，闰秒标志。

00-无警告信息 01-上一分钟有 61 秒 10-上一分钟有 59 秒 11-时钟未同步

- Version Number（VN）：3 比特，NTP 版本号，当前版本号为 3。
- Mode：3 比特，NTP 工作模式。

0-未定义 1-主动对等体 2-被动对等体 3-客户端 4-服务器 5-广播 6-控制信息 7-保留

- Stratum：8 比特，本地时钟的层数（0-未定义 1-主参考时钟源 其它值-次参考时钟源）。
- Poll Interval：8 位整数，轮询时间（秒数）
- Precision：8 位整数，本地时钟的时间精度（秒数）
- Root Delay：32 位整数，到主参考时钟源的往返时间
- Root Dispersion：32 位整数，相对于祝参考时钟源的最大误差
- Reference Clock Identifier：32 比特，参考时钟源的标识
- Reference Timestamp：64 位时间戳，最后一次被设置或者被校正的时间
- Originate Timestamp：64 位时间戳，时间同步请求报文离开客户端的本地时间
- Receive Timestamp：64 位时间戳，时间同步请求报文到达服务器的本地时间
- Transmit Timestamp：64 位时间戳，时间同步响应报文离开服务器的本地时间
- Autherticator（可选）：验证信息

NTP 服务器

设备将本地时钟作为参考时钟源，为网络中的其它设备提供时间同步服务。

NTP 客户端

设备作为 NTP 客户端从网络中的 NTP 服务器同步时间。

↘ 层数（stratum）

NTP 使用“层数（stratum）”的概念来描述设备距离权威时钟源的“跳数（hops）”。一个层数为 1 的时间服务器应当有个直连的原子钟或电波钟；层数为 2 的时间服务器就从层数为 1 的服务器获取时间；层数为 3 的服务器就从层数为 2 的获取时间……如此递推。因此时钟层数数值更低的时钟源即被认为拥有更高的时钟精度。

↘ 硬件时钟

硬件时钟根据设备上的石英晶体振荡器频率工作，由设备的电池为其供电，设备关机后硬件时钟依然运行。在设备启动运行后，会从硬件时钟读取时间信息，作为设备的软件时间。

功能特性

功能特性	作用
NTP 时间同步	使网络设备根据其服务器或可靠时钟源进行时间同步，以实现高精准度的时间校正。
NTP 安全认证	通过 NTP 报文加密认证方式，防止非可靠时钟源对设备进行时间同步干扰。
NTP 访问控制	根据访问控制列表对收到的 NTP 报文进行源过滤。

11.3.1 NTP时间同步

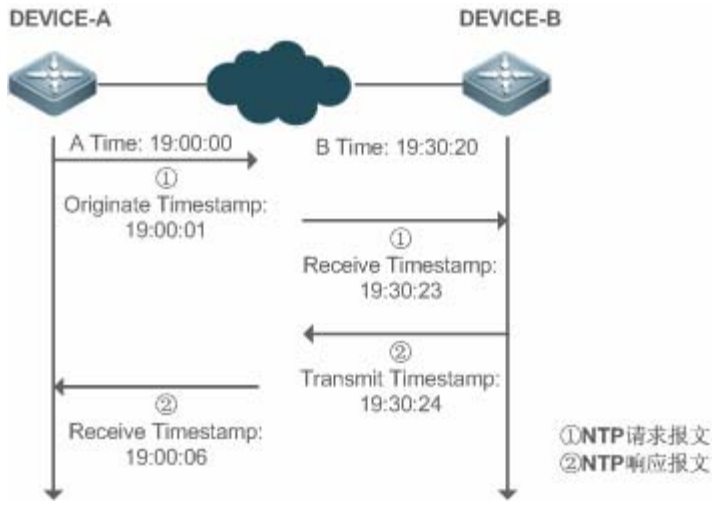
工作原理

NTP 同步时间的方式是通过客户端与服务器之间交互 NTP 报文：

- 客户端每隔 64 秒钟向所有服务器发送时间同步报文。收到服务器响应报文后，对所有服务器的响应报文进行过滤和选择，最后和优选服务器的时间进行同步。
- 服务器收时间同步请求报文时，将本地时钟作为参考源，按协议要求将本地时间信息填充到响应报文返回给客户端。

NTP时间同步报文格式如 图 11-4

图 11-4 NTP 基本工作原理图



DEVICE-B（下面简称 B）作为 NTP 参考时钟源，DEVICE-A（下面简称 A）作为 NTP 客户端从 DEVICE-B 同步时间，在某一时刻 A 的本地时钟为 19:00:00，B 的本地时钟为 19:30:20：

17. A 发出 NTP 请求报文，报文离开 A 的本地时间（T0）为 19:00:00，填充在 Originate Timestamp
18. 经过 2 秒的网络延时，B 收到请求报文的本地时间（T1）为 19:30:23，填充在 Receive Timestamp
19. B 处理 NTP 请求，1 秒后响应 NTP 报文，报文离开 B 的本地时间（T2）为 19:30:24，填充在 Transmit Timestamp
20. 经过 2 秒的网络延时，A 接收到响应报文，响应报文到达 A 的本地时间（T3）为 19:00:06

时间同步的具体算法如下：

- A 通过公式 ((T1-T0)+(T2-T3))/2 计算出 B 和 A 的时间差为 30 分 20 秒
- A 通过公式(T3-T0)-(T2-T1)计算出 A 和 B 的报文往返的延时为 4 秒

NTP 工作模式

- 外部时钟参考模式

在该模式下，设备即充当服务器又充当客户端，如果收到来自其它客户端发出的时间同步请求，必须先从指定服务器同步时间，同步成功后才可以向其它客户端提供时间同步服务。

- 本地时钟参考模式

在该模式下，设备默认本地时钟即为可靠时钟源，直接向其它客户提供时间同步服务。

相关配置

配置 NTP 服务器

- 缺省情况下，NTP 功能关闭。
- 通过 **ntp server** 命令指定 NTP 服务器（即外部时钟参考源），即可开启 NTP 功能。
- 配置后设备处于外部时钟参考模式。

实时同步

- 缺省情况下，设备每隔 64 秒进行一次时间同步。

更新硬件时钟

- 缺省情况下，设备同步完时间后不会把时间更新到硬件时钟。
- 配置 **ntp update-calendar** 命令可以使设备每次时间同步成功时会自动更新硬件时钟。

配置 NTP 主时钟

- 缺省情况下，设备处于外部时钟参考模式。
- 通过 **ntp master** 命令可以将设备配置为本地时钟参考模式。

11.3.2 NTP安全认证

为防止对时间服务器的恶意破坏，NTP 使用了识别(Authentication)机制，检查时间同步信息是否是真正来自所宣称的服务器并检查资料的返回路径，以提供对抗干扰的保护机制。

工作原理

NTP 客户端和服务器配置相同的密钥。发送请求报文和响应报文时，设备根据指定的密钥和 NTP 报文内容采用 MD5 算法计算出报文的哈希值填充到报文的认证信息。接收设备根据认证信息判断是否报文发送端是否可信的设备或者报文是否被篡改。

相关配置

配置 NTP 全局安全认证机制

- 缺省情况下，没有开启 NTP 安全认证机制。
- 通过 **ntp authenticate** 命令可开启 NTP 安全认证机制。

配置 NTP 全局认证密钥

- 缺省情况下，没有配置全局认证密钥。
- 通过 **ntp authentication-key** 命令可开启 NTP 安全认证机制。

配置 NTP 全局信任密钥 ID

- 缺省情况下，没有配置全局信任密钥。
- 通过 **ntp trusted-key** 命令设备作为参考时钟源对外提供时间同步服务的信任密钥。

配置外部参考时钟源的信任密钥 ID

- 通过 **ntp server** 指定外部参考时钟源的同时可以指定该时钟源的信任密钥。

11.3.3 NTP访问控制

工作原理

通过 ACL 提供了一种最小限度的安全措施

相关配置

配置 NTP 服务的访问控制权限

- 缺省情况下，没有 NTP 访问控制权限。
- 通过 **ntp access-group** 可配置 NTP 的访问控制权限。

11.4 配置详解

配置项	配置建议&相关命令	
配置 NTP 基本功能	⚠ 必须配置，用于开启 NTP 功能，开启后设备处于外部时钟参考模式。	
	ntp server	配置 NTP 服务器
	ntp update-calendar	自动更新硬件时钟
	⚠ 可选配置，用于将设备配置为本地时钟参考模式。	
	ntp master	配置 NTP 主时钟
	⚠ 可选配置，用于关闭 NTP 功能。	
	no ntp	关闭所有 NTP 功能，清空 NTP 配置。
	ntp disable	禁止接收指定接口的 NTP 报文
配置 NTP 安全认证	⚠ 可选配置，用于防止非可靠时钟源对设备进行时间同步干扰。	
	ntp authenticate	开启安全认证机制
	ntp authentication-key	设置安全认证全局密钥
	ntp trusted-key	配置时间同步服务可信密钥
	ntp server	配置外部参考时钟源的可信密钥
配置 NTP 访问控制	⚠ 可选配置，用于对收到的 NTP 报文进行源过滤。	
	ntp access-group	设置 NTP 的访问控制权限

11.4.1 配置NTP基本功能

配置效果

↘ 外部时钟参考模式

- 设备作为客户端，从外部参考时钟源同步时间到本地时钟
- 时间同步成功后，设备可作为时间同步服务器，对外提供时间同步服务

↘ 本地时钟参考模式

- 设备的本地时钟作为 NTP 参考时钟源，对外提供时间同步服务

注意事项

- 客户端/服务器模式，设备只有从外部的可靠时钟源同步成功后，才能作为时间同步服务器对外提供服务。
- 一旦配置本地时钟参考模式，系统便不会与比其时钟层数数值更高的时钟源进行同步。
- 将本地时钟设置为主时钟（尤其是指定了较低的时钟层数值时）很有可能将真正的有效时钟源覆盖。如果对同一网络中的多个设备都使用了该命令，则可能由于设备之间的时钟差异导致网络的时钟同步不稳定。
- 将本地时钟设置为主时钟前，如果系统从未与外部时钟源同步过，则有可能需要手动校准系统时钟以保证其不会有过大的偏差（关于如何手动校准系统时钟请参考配置指南中的系统时间配置部分）。

配置方法

配置 NTP 服务器

- 必须配置，至少指定一个外部参考时钟源（最多可配置 20 个不同的外部参考时钟源）。
- 如果需要关联配置 NTP 密钥，在配置 NTP 服务器前，必须先配置 NTP 安全认证。

自动更新硬件时钟

- 可选配置
- 默认情况下，时间同步成功后只更新系统时钟，不会更新硬件时钟。
- 配置此命令，时间同步成功后会自动更新硬件时钟。

配置 NTP 主时钟

- 如果需要将设备切换到本地时钟参考模式，可通过此命令。

关闭 NTP 功能

- 如果需要关闭 NTP 功能，并且清空 NTP 配置，可通过 **no ntp** 命令
- 默认情况，开启 NTP 功能后所有接口都可以接收 NTP 报文。如果需要禁止特定接口的 NTP 功能时可通过 **ntp disable** 命令。

检验方法

- 通过 **show ntp status** 查看 NTP 配置信息。
- 通过 **show clock** 查看是否完成时间同步

相关命令

配置 NTP 服务器

【命令格式】 **ntp server** { *ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain*}[**version** *version*][**source** *if-name*][**key** *keyid*][**prefer**]

【参数说明】 *ip-addr*：参考时钟源的 IPv4/IPv6 地址

domain：参考时钟源的 IPv4/IPv6 域名

version：NTP 版本号，取值为 1-3。

if-name：接口类型，包括 AggregatePort、Dialer GigabitEthernet、Loopback、Multilink、Null、Tunnel、Virtual-ppp、Virtual-template、Vlan 类型。

keyid：同参考时钟源通信采用的密钥(1-4294967295)

prefer：参考时钟源是否高优先级

【命令模式】 全局模式

【使用指导】 在缺省情况下，没有配置 NTP 服务器。锐捷的客户端系统支持最多同时与 20 个 NTP 服务器交互，(在全局认证以及密钥相关设置完成后）可以为每一个服务器设置一个认证密钥，发起与服务器的加密通信。

⚠ 如果需要设置认证密钥，在配置 NTP 服务器前必须先配置 NTP 安全认证。

与服务器的默认通信版本为 NTP 版本 3，同时可以配置发送 NTP 报文的源接口，并只在发送接口上接收对应服务器的 NTP 报文。

↘ 更新硬件时钟

【命令格式】 **ntp update-calendar**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 **-**

↘ 设置本地参考时钟源

【命令格式】 **ntp master** [*stratum*]

【参数说明】 *stratum*：指定本地时钟所处的层数，范围为 1～15；若不指定该参数则默认值为 8。

【命令模式】 全局模式

【使用指导】 -

↘ 关闭 NTP 功能

【命令格式】 **no ntp**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 此命令可以快速关闭 NTP 所有功能，并且清空 NTP 所有配置

↘ 禁止接口接收 NTP 报文

【命令格式】 **ntp disable**

【参数说明】 -

【命令模式】 接口模式

【使用指导】 -

配置举例

↘ NTP 外部时钟参考模式

【网络环境】

图 11-5

- DEVICE-B：配置为 NTP 外部时钟参考模式
- DEVICE-A：作为 DEVICE-B 的参考时钟源
- DEVICE-C：从 DEVICE-B 同步时间

【配置方法】

- DEVICE-A 配置本地时钟为 NTP 参考时钟源
- DEVICE-B 配置 DEVICE-A 为参考时钟源
- DEVICE-C 配置 DEVICE-B 为参考时钟源

DEVICE-A

```
A#configure terminal
A(config)# ntp master
A(config)#exit
```

DEVICE-B

```
B#configure terminal
B(config)# ntp server 192.168.1.1
B(config)# exit
```

DEVICE-C

```
C#configure terminal
C(config)# ntp server 192.168.2.1
C(config)# exit
```

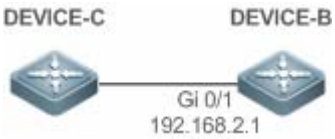
【检验方法】

- 在 DEVICE-B 上通过 **show ntp status** 查看 NTP 配置信息。
- DEVICE-B 会向 192.168.1.1 发送时间同步报文，从 DEVICE-A 同步时间。
- DEVICE-B 从 DEVICE-A 成功同步时间之后，可以响应 DEVICE-C 的时间同步请求。
- 在 DEVICE-B 和 DEVICE-C 上通过 **show clock** 命令可以查看时间是否成功同步。

↘ NTP 本地时钟参考模式

【网络环境】

图 11-6



- DEVICE-B：本地时钟为 NTP 参考时钟源
- DEVICE-C：从 DEVICE-B 同步时间

【配置方法】

- DEVICE-B 配置本地时钟为 NTP 参考时钟源
- DEVICE-C 配置 DEVICE-B 为参考时钟源

DEVICE-B

```
B#configure terminal
B(config)# ntp master
B(config)# exit
```

DEVICE-C

```
C#configure terminal
C(config)# ntp server 192.168.2.1
C(config)# exit
```

【检验方法】

- 在 DEVICE-C 上通过 **show clock** 命令可以查看时间是否成功同步。

11.4.2 配置NTP安全认证

配置效果

↘ 从可信参考时钟源同步时间

设备作为客户端，只从可信任的外部参考时钟源同步时间到本地时钟

↘ 给可信设备提供时间同步服务

设备的本地时钟作为 NTP 参考时钟源，只对可信的设备提供时间同步服务

注意事项

客户端和服务器的认证密钥必须一致。

配置方法

↘ 配置 NTP 全局安全认证机制

- 必须配置
- 默认情况下设备不开启安全认证机制。

↘ 配置 NTP 全局认证密钥

- 必须配置
- 默认情况下设备没有认证密钥。

↘ 配置 NTP 全局信任密钥 ID

- 可选配置
- 给可信设备提供时间同步服务，必须通过密钥 ID 指定可信认证密钥。
- 只允许配置一个信任密钥，所指定的认证密钥必须和可信设备一致。

↘ 配置外部参考时钟源的认证密钥 ID

- 可选配置
- 从可信参考时钟源同步时间，必须通过密钥 ID 指定可信认证密钥。
- 每个可信参考时钟源分别对应一个认证密钥，认证密钥必须和可信参考时钟源的密钥一致。

检验方法

- 通过 **show run** 查看配置是否正确
- 通过 **show clock** 查看是只否从可信设备同步时间

相关命令

开启安全认证机制

【命令格式】 **ntp authenticate**

【参数说明】 -

【命令模式】 全局模式

【使用指导】 缺省情况下，客户端不使用全局安全识别机制。如果未使用安全识别机制则不对通信进行加密处理。但是仅仅设置了全局安全标志，并不代表一定采用了加密方式完成服务器与客户端的通信，还必须完成其他全局密钥配置并设置服务器加密密钥才可能发起和服务器的加密通信。

设置全局认证密钥

【命令格式】 **ntp authentication-key** *key-id* **md5** *key-string* [*enc-type*]

【参数说明】 *key-id*：认证密钥的全局 ID（1-4294967295）。

key-string：密钥字符串。

enc-type：可选。输入的密钥是否加密（0 表示无加密，7 表示简单加密，默认为无加密）。

【命令模式】 全局模式

【使用指导】 -

设置 NTP 服务的可信密钥

【命令格式】 **ntp trusted-key** *key-id*

【参数说明】 *key-id*：认证密钥的全局 ID（1-4294967295）。

【命令模式】 全局模式

【使用指导】 -

设置外部参考时钟源的可信密钥

参考“配置NTP服务器”

配置举例

安全认证

【网络环境】

图 11-7

- DEVICE-B：配置为 NTP 客户端/服务器模式，给 DEVICE-C 提供需要安全认证的 NTP 服务，认证密钥为“abcd”
- DEVICE-A：作为 DEVICE-B 的参考时钟源

【配置方法】	● DEVICE-C：从 DEVICE-B 同步时间 ● DEVICE-B 配置 DEVICE-A 为参考时钟源 ● DEVICE-C 配置 DEVICE-B 为参考时钟源
DEVICE-B	B#configure terminal B(config)# ntp authentication-key 1 md5 abcd B(config)# ntp trusted-key 1 B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp authentication-key 1 md5 abcd C(config)# ntp server 192.168.2.1 key 1 C(config)# exit
【检验方法】	● DEVICE-B 会向 192.168.1.1 发送时间同步报文，携带认证信息，从 DEVICE-A 同步时间。 ● 在 DEVICE-B 上通过 **show clock** 命令查看时间是否成功同步。

配置举例

11.4.3 配置NTP访问控制

配置效果

NTP 服务的访问控制功能提供了一种最小限度的安全措施（更安全的方法是使用 NTP 身份验证机制）。

注意事项

- 目前系统暂未支持控制查询功能（用于通过网络管理设备对 NTP 服务器进行控制，如设置闰秒标记或监控其工作状态等）。虽然是按照上述顺序进行规则匹配，但涉及到与控制查询相关的请求都无法支持。
- 如果未配置任何访问控制规则，则所有访问都是允许的。但一旦配置了访问控制规则，则仅有规则中所允许的访问才能进行。

相关配置

↘ 设置 NTP 的访问控制权限

- 可选配置
- 通过 **ntp access-group** 配置 NTP 访问控制权限及对应的 ACL

检验方法

通过 **show run** 查看 NTP 配置是否正确配置

相关命令

配置 NTP 服务的访问控制权限

【命令格式】 **ntp access-group** { **peer** | **serve** |**serve-only** | **query-only** }*access-list-number* | *access-list-name*

【参数说明】 **peer**：既允许对本地 NTP 服务进行时间请求和控制查询，也允许本地设备与远程系统同步时间（完全访问权限）。

serve：允许对本地 NTP 服务进行时间请求和控制查询，但不允许本地设备与远程系统同步时间。

serve-only：仅允许对本地 NTP 服务进行时间请求。

query-only：仅允许对本地 NTP 服务进行控制查询。

access-list-number：IP 访问控制列表标号；范围为 1～99 和 1300～1999。关于如何创建 IP 访问控制列表请参考《ACL》中的相关描述。

access-list-name：IP 访问控制列表名。关于如何创建 IP 访问控制列表请参考《访问控制列表配置指南》中的相关描述。

【命令模式】 全局模式

【使用指导】 配置 NTP 访问控制权限。

当一个访问请求到达时，NTP 服务按照从最小访问限制到最大访问限制的顺序依次匹配规则，以第一个匹配到的规则为准。匹配顺序为 peer、serve、serve-only、query-only。

配置举例

NTP 访问控制权限配置

【配置方法】 配置只允许 192.168.1.1 的设备对本地设备进行时间同步请求

```
Ruijie(config)# access-list 1 permit 192.168.1.1
Ruijie(config)# ntp access-group serve-only 1
```

11.5 监视与维护

查看运行情况

作用	命令
show ntp status	显示当前的 NTP 信息

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令

debug ntp	打开调试功能。
no debug ntp	关闭调试功能。

12 SNTP

12.1 概述

SNTP (Simple Network Time Protocol，简单网络时间协议) 是 NTP 的简化版本，主要用来同步因特网中的计算机时钟。SNTP 适用于无需完全使用 NTP 功能的情况。

NTP 算法复杂，对系统要求较高。而 SNTP 在实现时，计算时间用了简单的算法，性能较高。而精确度一般也能达到 1 秒左右，也能基本满足绝大多数场合的需要。由于 SNTP 的报文和 NTP 的报文是完全一致的，所以设备实现的 SNTP Client 能完全兼容 NTP Server。

下文仅介绍 SNTP 的相关内容。

协议规范

- RFC 2030：Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI

12.2 典型应用

典型应用	场景描述
从NTP服务器同步时间	设备作为客户端，从 NTP 服务器同步时间

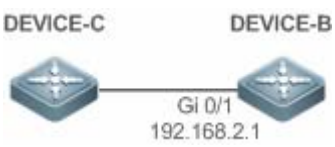
12.2.1 从NTP服务器同步时间

应用场景

如图所示，DEVICE-B 将本地时钟作为 NTP 参考时钟源，向 DEVICE-C 提供时间同步服务。

DEVICE-C 作为 SNTP 客户端，从 DEVICE-B 同步时间。

图 12-1



功能部属

- 指定 DEVICE-B 为 DEVICE-C 的 SNTP 服务器。

- DEVICE-C 开启 SNTP 功能

12.3 功能详解

基本概念

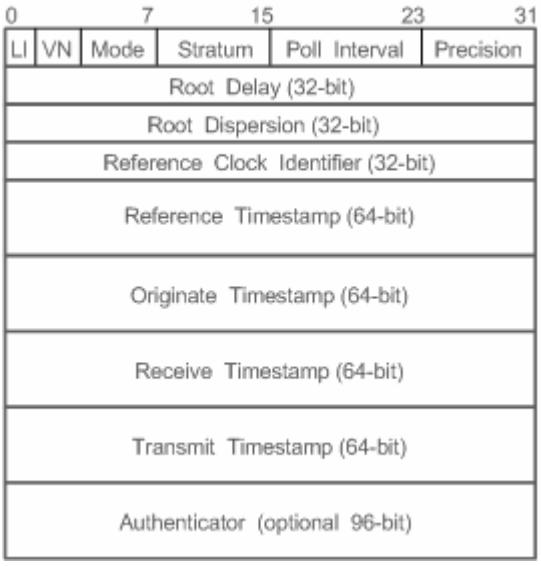
SNTP 报文

SNTPV4 是从 NTP 发展过来的，主要是简化 NTP 的功能。SNTPV4 并没有改变 NTP 规范和原有实现过程。SNTPV4 的消息格式于 RFC1305 中定义的 NTP 格式是一致的，只是一些数据域被初始化为预定的值。

同 RFC1305 定义，SNTP 采用 UDP 报文进行传输，UDP 端口号为 123。

NTP时间同步报文格式如 图 11-3

图 12-2 SNTP 时间同步报文格式



- Leap Indicator（LI）：2 比特，闰秒标志。

00-无警告信息 01-上一分钟有 61 秒 10-上一分钟有 59 秒 11-时钟未同步

- Version Number（VN）：3 比特，NTP/SNTP 版本号，当前版本号为 3。
- Mode：3 比特，SNTP/NTP 工作模式。

0-未定义 1-主动对等体 2-被动对等体 3-客户端 4-服务器 5-广播 6-控制信息 7-保留

- Stratum：8 比特，本地时钟的层数（0-未定义 1-主参考时钟源 其它值-次参考时钟源）。
- Poll Interval：8 位整数，轮询时间（秒数）
- Precision：8 位整数，本地时钟的时间精度（秒数）
- Root Delay：32 位整数，到主参考时钟源的往返时间

- Root Dispersion：32 位整数，相对于祝参考时钟源的最大误差
- Reference Clock Identifier：32 比特，参考时钟源的标识
- Reference Timestamp：64 位时间戳，最后一次被设置或者被校正的时间
- Originate Timestamp：64 位时间戳，时间同步请求报文离开客户端的本地时间
- Receive Timestamp：64 位时间戳，时间同步请求报文到达服务器的本地时间
- Transmit Timestamp：64 位时间戳，时间同步响应报文离开服务器的本地时间
- Authenticator（可选）：验证信息

功能特性

功能特性	作用
SNTP时间同步	从 SNTP/NTP 服务器同步时间到本地设备。

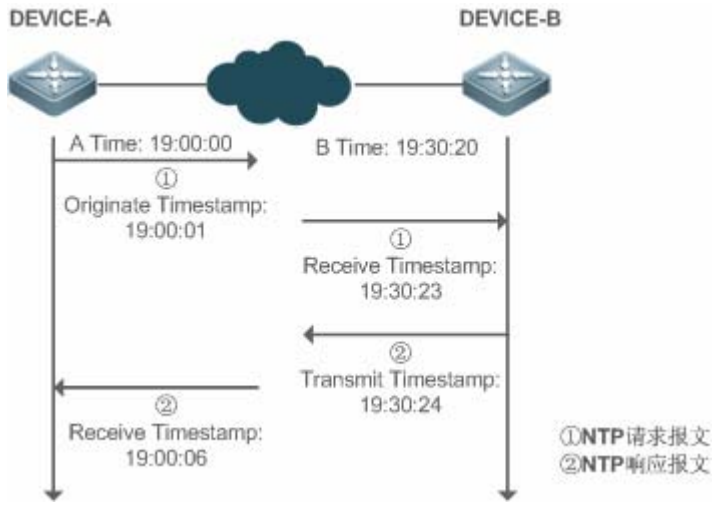
12.3.1 SNTP时间同步

工作原理

SNTP 同步时间的方式是与服务器之间交互 SNTP/NTP 报文。客户端每隔一段时间（默认是半小时）向服务器发送时间同步报文。收到服务器响应报文后进行时间同步。

SNTP时间同步报文格式如 图 11-4

图 12-3 SNTP 基本工作原理图



DEVICE-B（下面简称 B）作为 NTP 参考时钟源，DEVICE-A（下面简称 A）作为 SNTP 客户端从 DEVICE-B 同步时间，在某一时刻 A 的本地时钟为 19:00:00，B 的本地时钟为 19:30:20：

21. A 发出 SNTP/NTP 请求报文，报文离开 A 的本地时间（T0）为 19:00:00，填充在 Originate Timestamp
22. 经过 2 秒的网络延时，B 收到请求报文的本地时间（T1）为 19:30:23，填充在 Receive Timestamp
23. B 处理 NTP 请求，1 秒后响应 NTP 报文，报文离开 B 的本地时间（T2）为 19:30:24，填充在 Transmit Timestamp
24. 经过 2 秒的网络延时，A 接收到响应报文，响应报文到达 A 的本地时间（T3）为 19:00:06

时间同步的具体算法如下：

- A 通过公式 ((T1-T0)+(T2-T3))/2 计算出 B 和 A 的时间差为 30 分 20 秒
- A 通过公式(T3-T0)-(T2-T1)计算出 A 和 B 的报文往返的延时为 4 秒

相关配置

打开 SNTP

- 缺省 SNTP 状态是关闭的。
- 通过 **sntp enable** 命令开启 SNTP 功能

配置 SNTP 服务器

- 缺省情况下，没有配置 SNTP 服务器。
- 通过 s**ntp server** 命令指定 SNTP 服务器。

配置 SNTP 同步时钟间隔

- 缺省情况下，SNTP 同步时钟的间隔是 1800s。
- 通过 s**ntp interval** 命令指定 SNTP 服务器。

12.4 配置详解

配置项	配置建议&相关命令	
配置SNTP	⚠ 必须配置，用于开启 SNTP 功能	
	sntp enable	打开 SNTP
	sntp server	配置 SNTP Server 的地址
	⚠ 可选配置，用于调整 SNTP 时间同步间隔	
	sntp interval	配置 SNTP 同步时钟的间隔

12.4.1 配置SNTP

配置效果

SNTP Client 一定的时间间隔定期访问 NTP Server，可以定时校正时钟。

注意事项

通过 SNTP 协议通讯后获取的时间都是格林威治标准时间 (GMT)，为了准确的获取本地时间，需要设置本地时区来对标准时间进行调正。

配置方法

打开 SNTP

- 必须配置，缺省 SNTP 状态是 Disable。

配置 SNTP Server 的地址

- 必须配置，缺省没有设置 SNTP/NTP 服务器

配置 SNTP 同步时钟的间隔

- 可选配置
- 默认情况下，设备每隔半小时同步一次时间

检验方法

使用 **show sntp** 命令查看 SNTP 相关参数。

相关命令

打开 SNTP

【命令格式】 **sntp enable**
【参数说明】 **-**
【命令模式】 全局配置模式
【使用指导】 缺省 SNTP 状态是 Disable。
no sntp enable 全局配置命令来关闭 SNTP。

配置 SNTP/NTP Server 的地址

【命令格式】 **sntp server** *ip-address*
【参数说明】 *ip-address*：NTP/SNTP 服务器的 IP 地址。缺省没有设置任何 NTP/SNTP 服务器。
【命令模式】 全局配置模式
【使用指导】 由于 SNTP 协议和 NTP 完全兼容，所以这个 Server 完全可以配置成 internet 上公用的 NTP Server。
由于 SNTP 的报文和 NTP 的报文是完全一致的，所以 SNTP Client 能完全兼容 NTP Server。网络上存在着较多的 NTP Server，用户可以选择一个网络延迟较少的一个作为设备上的 SNTP Server。

配置 SNTP 同步时钟的间隔

【命令格式】 **sntp interval** *seconds*

【参数说明】 *seconds*：定时同步的间隔，单位为“秒”范围为 60 秒--65535 秒。缺省值为 1800s。

【命令模式】 全局配置模式

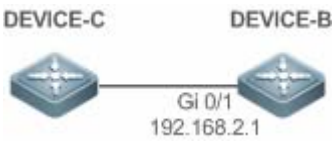
【使用指导】 该命令设置 SNTP Client 需要定时和 NTP/SNTP Server 同步时钟的时间间隔。

⚠ 这里设置的时间间隔不会立即生效，如果要立即生效，请配置完时间间隔后执行 **sntp enable** 命令。

配置举例

SNTP 时间同步

【网络环境】 图 12-4



- DEVICE-B：网络上的 NTP 服务器
- DEVICE-C：从 DEVICE-B 同步时间

【配置方法】 DEVICE-C 开启 SNTP 功能，NTP 服务器配置为 DEVICE-B

DEVICE-C

```
C#configure terminal
C(config)# sntp server 192.168.2.1
C(config)# sntp enable
C(config)# exit
```

【检验方法】

- 在 DEVICE-C 上通过 **show clock** 命令可以查看时间是否成功同步。
- 在 DEVICE-C 上 **show sntp** 查看 sntp 状态和服务器是否配置成功

12.5 监视与维护

清除各类信息

-

查看运行情况

作用	命令
show sntp	查看 SNTP 的相关参数

查看调试信息

⚠ 输出调试信息，会占用系统资源。使用完毕后，请立即关闭调试开关。

作用	命令
debug sntp	打开调试功能。

13 TIME RANGE

13.1 概述

Time range 是一个时间控制服务，它提供给某些应用进行时间控制。例如，如果想要让 ACL 在一个星期的某些时间段内生效，可以配置一个 time range 并让 ACL 和这个 time range 相关联。

13.2 典型应用

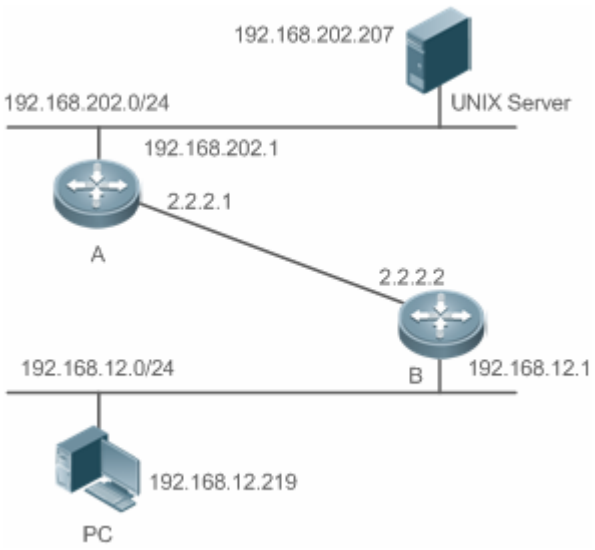
典型应用	场景描述
ACL中的time range应用	应用在 ACL 模块，满足 ACL 基于时间生效的需求。

13.2.1 ACL中的time range应用

应用场景

某单位限制只能在正常上班时间访问远程 UNIX 主机 TELNET 服务：

图 13-1



【注释】 要求通过在设备 B 上配置访问列表，实现以下安全功能：

192.168.12.0/24 网段的主机只能在正常上班时间访问远程 UNIX 主机 TELNET 服务。

功能部属

- 在网络设备 B 上使用 ACL 对来自 192.168.12.0/24 网段的 TELNET 访问进行控制，ACL 应用关联一个 time range，只有在工作时间才允许其访问 Unix 主机。

13.3 功能详解

基本概念

↘ 绝对时间区间

绝对时间区间是指可以为 time range 设置一个起始时间以及结束时间的区间。典型的绝对时间区间例如[2000 年 1 月 1 日 12：00，2001 年 1 月 1 日 12：00]。Time range 应用关联到这个 time range 之后，可以在该时间区间之内使某项功能起作用。

↘ 周期时间

周期时间是指可以为 time range 设置一个周期性的时间。典型的周期时间如“每周一 8：00 到每周五 17：00”。Time range 应用关联到这个 time range 之后，可以周期性地在每周一到每周五使某项功能起作用。

功能特性

功能特性	作用
使用绝对时间区间	设置绝对时间区间允许 time range 应用在这个绝对时间区间之内使某项功能生效。
使用周期时间	设置周期时间允许 time range 应用在某个周期性的时间之内使某项功能生效。

13.3.1 使用绝对时间区间

工作原理

基于 time range 的应用在开启某项功能时，会判断当前的时间是否处于绝对时间区间之内，如果在其中，则可以让该功能在当前时间生效或者在当前时间不生效。

相关配置

↘ 配置 time range

缺省情况下，没有配置 time range。

使用 **time-range** *time-range-name* 命令来配置一个 time range。

↘ 配置绝对时间区间

缺省情况下，绝对时间区间为[0 年 1 月 1 日 00：00，9999 年 12 月 31 日 23：59]。

使用 **absolute** { [**start** *time date*] [**end** *time date*] }命令来配置绝对时间区间。

13.3.2 使用周期时间

工作原理

基于 time range 的应用在开启某项功能时，会判断当前的时间是否处于周期时间之内，如果在其中，则可以让该功能在当前时间生效或者在当前时间不生效。

相关配置

↘ 配置 time range

缺省情况下，没有配置 time range。

使用 **time-range** *time-range-name* 命令来配置一个 time range。

↘ 配置周期时间

缺省情况下，没有配置周期时间。

使用 **periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time* 命令来配置周期时间。

13.4 配置详解

配置项	配置建议 & 相关命令	
配置time range	⚠ 必须配置。如果要使用 time range 功能，必须配置 time range。	
	time-range *time-range-name*	配置 time range。
	⚠ 可选配置。配置分类参数。	
	absolute { [**start** *time date*] | [**end** *time date*] }	配置绝对时间区间。
	periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*	配置周期时间。

13.4.1 配置time range

配置效果

- 配置 time range，配置其绝对时间区间或周期时间，以便让 time range 应用在对应的时间区间内使某项功能生效。

配置方法

↘ 配置 time range

- 必须配置。
- 在需要应用 time range 的设备上配置。

配置绝对时间区间

- 可选配置。

配置周期时间

- 可选配置。

检验方法

- 使用 **show time-range** [*time-range-name*]命令，可以查看所配置的 time range 信息。

相关命令

配置 time range

【命令格式】 **time-range** *time-range-name*

【参数说明】 *time-range-name*：要创建的 time range 的名字。

【命令模式】 全局模式

【使用指导】 有些应用（例如 ACL）可能基于时间运行，比如让 ACL 在一个星期的某些时间段内生效等。为了达到这个要求，必须首先配置一个 Time-Range。创建完 time range 之后，可以在 time range 模式中配置相应的时间控制。

配置绝对时间区间

【命令格式】 **absolute** { [**start** *time date*] [**end** *time date*] }

【参数说明】 **start** *time date*：区间的开始时间。

end *time date*：区间的结束时间。

【命令模式】 time-range 模式

【使用指导】 如果想要让某个功能在一个绝对时间区间内生效，可以使用 **absolute** 命令配置一个开始和结束的时间区间。

配置周期时间

【命令格式】 **periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time*

【参数说明】 *day-of-the-week*：周期时间开始或者结束是在星期几

time：周期时间开始或者结束是在几点几分

【命令模式】 time-range 模式

【使用指导】 如果想要让某个功能在一个周期时间内生效，可以使用 **periodic** 命令配置一个周期时间。

13.5 监视与维护

查看运行情况

作用	命令
显示 time range。	**show time-range** [*time-range-name*]