甲信三层以太网交换机 安全性通用配置（ACL ARP 防攻击 DHCP Snooping 等）配置指南(CLI)

(Rel_01)

北京甲信技术有限公司（以下简称“甲信”）为客户提供全方位的技术支持和服务。直接向甲信购买产品的用户，如果在使用过程中有任何问题，可与甲信各地办事处或用户服务中心联系，也可直接与公司总部联系。

读者如有任何关于甲信产品的问题，或者有意进一步了解公司其他相关产品，可通过下列方式与我们联系：

公司网址：　　www.jiaxinnet.com.cn

技术支持邮箱：　jxhelp@bjjx.cc

技术支持热线：　400-179-1180

公司总部地址：　北京市海淀区丹棱 SOHO 7 层 728 室

邮政编码:　　100080

声　明

目录

1 安全性 1
1.1 ACL 1
1.1.1 简介 1
1.1.2 配置准备 2
1.1.3 配置 ACL 2
1.1.4 应用 ACL 4
1.1.5 配置统计 4
1.1.6 配置限速 5
1.1.7 配置时间段 5
1.1.8 检查配置 6
1.1.9 维护 6
1.1.10 配置 ACL 示例 6
组网需求 6
1.2 AAA 8
1.2.1 简介 8
1.2.2 配置准备 9
1.2.3 缺省配置 9
1.2.4 配置 RADIUS 服务器 10
1.2.5 配置 TACACS+服务器 10
1.2.6 配置 AAA 服务器组 11
1.2.7 配置 AAA 方法 11
1.2.8 检查配置 12
1.2.9 配置 AAA 示例 12
1.2.10 检查结果 14
1.3 802.1x 14
1.3.1 简介 14
1.3.2 配置准备 17
1.3.3 802.1x 功能的缺省配置 17
1.3.4 配置 802.1x 基本功能 17
1.3.5 配置 802.1x 重认证 19

1.3.6 配置 802.1x 定时器 19
1.3.7 检查配置 19
1.3.8 配置 802.1x 示例 20
组网需求 20
1.4 PPPoE+ 22
1.4.1 简介 22
1.4.2 配置准备 23
1.4.3 PPPoE+功能的缺省配置 23
1.4.4 配置 PPPoE+基本功能 24
1.4.5 配置 PPPoE+报文信息 24
1.4.6 检查配置 26
1.4.7 维护 26
1.4.8 配置 PPPoE+示例 27
组网需求 27
1.5 安全 MAC 28
1.5.1 简介 28
1.5.2 配置准备 29
1.5.3 安全 MAC 功能的缺省配置 30
1.5.4 配置安全 MAC 基本功能 30
1.5.5 配置接口 Sticky 安全 MAC 地址 31
1.5.6 检查配置 32
1.5.7 维护 32
1.5.8 配置安全 MAC 示例 32
组网需求 32
1.6 风暴抑制与风暴控制 34
1.6.1 简介 34
1.6.2 配置准备 35
1.6.3 风暴抑制和风暴控制的缺省配置 35
1.6.4 配置风暴抑制功能 36
1.6.5 检查风暴抑制配置 36
1.6.6 配置风暴抑制应用示例 37

1.6.7 配置风暴控制功能 38
1.6.8 检查风暴控制配置 39
1.6.9 配置风暴控制应用示例 39
组网需求 39
1.7 ARP 防攻击 40
1.7.1 配置准备 40
1.7.2 ARP 防攻击缺省配置 40
1.7.3 配置 ARP 防攻击功能 40
1.7.4 检查配置 42
1.7.5 配置 ARP 防攻击示例 42
1.8 ND Snooping 44
1.8.1 简介 44
1.8.2 配置准备 44
1.8.3 ND Snooping 的缺省配置 45
1.8.4 配置 ND Snooping 45
1.8.5 检查配置 45
1.8.6 配置 ND Snooping 示例 46
组网需求 46
1.9 DHCP Snooping 47
1.9.1 简介 47
1.9.2 配置准备 48
1.9.3 DHCP Snooping 的缺省配置 49
1.9.4 配置 DHCP Snooping 49
1.9.5 配置 DHCP Snooping 支持 Option 82 功能 50
1.9.6 配置 DHCPv6 Snooping 50
1.9.7 检查配置 51
1.9.8 维护 52
1.9.9 配置 DHCP Snooping 示例 52
组网需求 52
1.10 IP Source Guard 54
1.10.1 简介 54

1.10.2 配置准备 55
1.10.3 IP Source Guard 功能的缺省配置 55
1.10.4 配置 IP Source Guard 绑定功能 56
1.10.5 配置 IP Source Guard 接口信任状态 56
1.10.6 检查配置 56
1.10.7 配置 IP Source Guard 示例 57
组网需求 57
1.11 CPU 防攻击 58
1.11.1 配置准备 58
1.11.2 配置 CPU 防攻击限速功能 58
1.11.3 配置 CPU 防攻击的攻击溯源功能 59
1.11.4 检查配置 60
1.11.5 维护 60
1.11.6 MAC 认证 61
1.11.7 简介 61
1.11.8 缺省配置 61
1.11.9 配置 MAC 认证 62
1.11.10 配置举例 63
配置步骤 63
1.12 URPF 64
1.12.1 简介 64
1.12.2 配置准备 65
1.12.3 缺省配置 65
1.12.4 配置 URPF 65
1.12.5 检查配置 65
1.13 Timerange 67
1.13.1 简介 67
1.13.2 配置准备 67
1.13.3 缺省配置 67
1.13.4 配置 timerange 67
1.13.5 检查配置 68

1.14 DOS 防攻击 69
1.14.1 简介 69
1.14.2 配置准备 70
场景 70
1.14.3 DOS 防攻击功能的缺省配置 71
1.14.4 配置畸形报文攻击防范 71
1.14.5 配置分片报文攻击防范 71
1.14.6 配置 TCP SYN 泛洪攻击防范 72
1.14.7 配置 UDP 泛洪攻击防范 72
1.14.8 配置 ICMP 泛洪攻击防范 72
1.14.9 检查配置 73
1.14.10 配置 DOS 防攻击示例 73
组网需求 73
配置步骤 73
检查结果 74

1 安全性

本章介绍安全特性的基本原理和配置过程，并提供相关的配置案例。

- ACL
- AAA
- 802.1x
- PPPoE+
- 安全 MAC
- 风暴抑制与风暴控制
- ARP 防攻击
- ND Snooping
- DHCP Snooping
- IP Source Guard
- CPU 防攻击
- URPF
- Timerange

1.1 ACL

1.1.1 简介

ACL（Access Control List，访问控制列表）是一系列有序规则的集合，通过应用这些规则控制设备接收或拒绝某些数据报文。

在网络中为了控制非法报文对网络的影响，需要在设备上配置一系列的规则，以决定什么样的数据包能够通过，这些规则就是通过 ACL 定义的。

访问控制列表是由 permit | deny 语句组成的一系列有顺序的规则，这些规则根据数据包的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、端口号等来描述。设备根据这些规则判断哪些数据包可以接收，哪些数据包需要拒绝。

1.1.2 配置准备

场景

网络设备为了过滤数据包，需要配置 ACL，以识别需要过滤的对象。在识别出特定的对象之后，才能根据预先设定的策略允许或禁止相应的数据包通过，，丢弃动作支持报文上送 CPU。当 ACL 否定目的 MAC 地址后，相应报文的源 MAC 地址不进行学习且不显示。

- 基本 IPv4 ACL：根据数据包 IP 头所携带的源 IP、目的 IP 地址制定分类规则。
- 扩展 IPv4 ACL：根据数据包 IP 头所携带的源 IP、目的 IP、承载的协议类型、使用的 TCP 或 UDP 端口号（默认为 0）等数据包的属性信息制定分类规则，支持限制 Telnet/SSH 登录。
- MAC ACL：根据数据包二层帧头携带的源 MAC 地址、目的 MAC 地址、二层协议类型等二层信息制定分类规则，ACL 拒绝的目的 MAC 地址报文，源 MAC 地址也不再学习、不显示。
- User ACL：可以以报文的报文头、IP 头等为基准，指定从第几个字节开始与掩码进行“与”操作，将从报文提取出来的字符串与用户定义的字符串进行比较，从而找到相匹配的报文，支持匹配以太网帧前 64 字节任意字段的信息。
- IPv6 ACL：根据数据包 IP 头所携带源 IPv6 地址信息、目的 IPv6 地址信息、IPv6 承载的协议类型、使用的 TCP 或 UDP 端口号（默认为 0）等数据包的属性信息制定分类规则，支持 IPv6 ACL 限制 Telnet/SSH 登录。
- 高级 ACL：根据数据包二层帧头携带的源 MAC 地址、目的 MAC 地址、IP 头所携带的源 IP、目的 IP 等数据包的属性信息制定分类规则。

根据实际场景的差异，应用 ACL 的方式有四种：基于整个设备、基于接口、基于从入接口到出接口的流和基于 VLAN。

前提

无

1.1.3 配置 ACL

请在设备上进行以下配置。步骤 3～步骤 7 请根据需要选择配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**acl-l2** *acl-number* [**name** *acl-name*] JX(config)#**acl-ipv4** *acl-number* [**name** *acl-name*] JX(config)#**acl-ipv6** *acl-number* [**name** *acl-name*] JX(config)#**acl-hybrid** *acl-number* [**name** *acl-name*] JX(config)#**acl-mpls** *acl-number* [**name** *acl-name*] JX(config)#**acl-userdefined** *acl-number* [**name** *acl-name*]	创建 ACL，进入 ACL 配置模式。 • 取值在 1～1000 之间时，进入基本 MAC ACL 配置模式 • 取值在 1001～2000 之间时，进入基本 IPV4 ACL 配置模式 • 取值在 2001～3000 之间时，进入扩展 HYBRID ACL 配置模式 • 取值在 3001～4000 之间时，进入 IPV6 ACL 配置模式 • 取值在 4001～5000 之间时，进入 MPLS ACL 配置模式 • 取值在 5001～6000 之间时，进入用户自定义 ACL 配置模式
3	JX(configure-acl-ipv4-*)#**rule** *rule-id* **ip src-ip** *ip-address* **dst-ip** *ip-address* JX(configure-acl-ipv4-*)#**rule** *rule-id* **icmp src-ip** *ip-address* **dst-ip** *ip-address* **icmp-type** *icmp-type* **icmp-code** *icmp-code* **[fragment]** JX(configure-acl-ipv4-*)#**rule** *rule-id* **tcp src-ip** *ip-address* **src-port** *port* **dst-ip** *ip-address* **dst-port** *port* { **syn** | **synack** | **ack** | **fin** } **[fragment]** JX(configure-acl-ipv4-*)#**rule** *rule-id* **igmp src-ip** *ip-address* **dst-ip** *ip-address* **[fragment]** JX(configure-acl-ipv4-*)#**rule** *rule-id* **udp src-ip** *ip-address* **src-port** *port* **dst-ip** *ip-address* **dst-port** *port* **[fragment]**	配置 IP ACL 的匹配规则。
4	JX(configure-acl-l2-*)#**rule** *rule-id* **ethernet src-mac** *mac-address* **dst-mac** *mac-address* JX(configure-acl-l2-*)#**rule** *rule-id* **src-mac ethernet** *mac-address* **dst-mac** *mac-address* **eth-type** { **ip** | **arp** | *ethtype* } JX(configure-acl-l2-*)#**rule** *rule-id* **src-mac ethernet** *mac-addr* **dst-mac** *mac-address* { **inner-vlan** | **outer-vlan** } *vlan-id* **8021p** *cos*	配置 MAC ACL 的规则。

步骤	配置	说明
5	JX(configure-acl-ipv6-*)#**rule** *rule-id* **ip src-ip** *ipv6-address* **dst-ip** *ipv6-address* JX(configure-acl-ipv6-*)#**rule** *rule-id* **tcp src-ip** *ipv6-address* **src-port** *port* **dst-ip** *ipv6-address* **dst-port** *port* { **syn** | **synack** | **ack** | **fin** } JX(configure-acl-ipv6-*)# **rule** *rule-id* **udp src-ip** *ipv6-address* **src-port** *port* **dst-ip** *ipv6-address* **dst-port** *port* JX(configure-acl-ipv6-*)#**rule** *rule-id* **icmp src-ip** *ipv6-address* **dst-ip** *ipv6-address* **icmp-type** *icmp-type* **icmp-code** *icmp-code* **[fragment]**	配置 IPv6 ACL 的规则。
6	JX(configure-acl-ipv6-*)#**rule** *rule-id* **field1** *data/mask/offset* {**field2** *data/mask/offset* | **field3** *data/mask/offset* | **field4** *data/mask/offset*}*	配置用户自定义 ACL 的规则。 data 表示需要匹配的信息，mask 表示对 data 做掩码操作，offset 表示该匹配信息距离报文头部的字节数，offset 必须能整除 4。
7	JX(configure-acl-ipv4-*)#**rule** *rule-id* **action** { **permit** | **deny** | **mirror** | **redirect** | **counter** }	配置基本 IP ACL 的动作。

1.1.4 应用 ACL

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式或者 VLAN 接口配置模式，以下以物理接口模式为例进行说明。
3	JX(config-ge-1/0/*)#**acl-l2 in** *acl-num*	在接口上应用 ACL。
	JX(config-ge-1/0/*)#**acl-l2 in** *name*	在接口上应用 ACL。
4	JX(config-ge-1/0/*)#**exit**	返回全局配置模式。

1.1.5 配置统计

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**counter** *counter-id* { **packet** | **byte** | **all** } **sort** { **green** | **red** | **greenred** | **greenyellow** | **redyellow** | **total** }	创建统计模版
3	JX(configure-acl-l2-*)#**rule** *rule-id* **action counter** *counter-id*	在 acl 中应用统计模版

1.1.6 配置限速

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**meter** *meter-id* **pps** *pps-value* **color** { **aware** | **blind** }	创建基于包个数的限速模版
3	JX(config)#**meter** *meter-id* **cir** { **kbps** | **mbps** | **gbps** } *cir-value* **cbs** { **bytes** | **kbytes** | **mbytes** } *cbs-value* **ebs** { **bytes** | **kbytes** | **mbytes** } *ebs-value* **color** { **aware** | **blind** }	创建单速三色的限速模版
4	JX(config)#**meter** *meter-id* **cir** { **kbps** | **mbps** | **gbps** } *cir-value* **cbs** { **bytes** | **kbytes** | **mbytes** } *cbs-value* **pir** { **kbps** | **mbps** | **gbps** } *pir-value* **pbs** { **bytes** | **kbytes** | **mbytes** } *pbs-value* **color** { **aware** | **blind** }	创建双速三色的限速模版
3	JX(configure-acl-l2-*)#**rule** *rule-id* **meter** *meter-id* **outaction** { **red-drop** | **yellow-drop** }	在 acl 中应用限速模版

1.1.7 配置时间段

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**acl-l2** *acl-id*	进入 acl list 视图

步骤	配置	说明
3	JX(configure-acl-l2-*)#**rule** *rule-id* **time-range** *timerange-list-id*	在 acl 中应用时间段

1.1.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show acl config**	查看 ACL 配置信息。
2	JX#**show acl interface**	查看接口 acl 配置信息。
3	JX#**show acl statistics**	查看 acl 统计信息。
4	JX#**show time-range list**	查看时间段配置相关信息。

1.1.9 维护

用户可以通过以下命令，维护设备 ACL 特性的运行情况和配置情况。

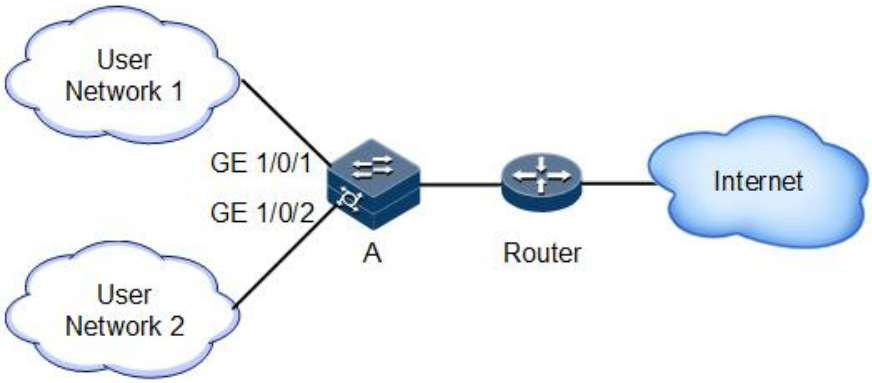
命令	描述
JX(config)#**reset acl statistics** [**acl** *acl-id* |**rule** *rule-id* | **direction** { **in** | **out** }]	清除全局 ACL 统计信息。
JX(config)#**reset acl statistics interface** *interface-type interface-number* [**acl** *acl-id* |**rule** *rule-id* | **direction** { **in** | **out** }]	清除接口 ACL 统计信息。

1.1.10 配置 ACL 示例

组网需求

如下图所示，想要控制在每天 00:00 到 08:00 之间，拒绝通过 SwitchA 访问互联网的请求，在每天 08:00 到 12:00 之间，限制访问速度为 10000pps

图 1-1 ACL 示例



配置步骤

步骤 1 配置 timerange。

```
JX#configure
JX(config)#timerange list 1
JX(config-timerange-1)#time-range 1 everyday 00:00:00 to 08:00:00
JX(config-timerange-1)#configure
JX(config)#timerange list 2
JX(config-timerange-1)#time-range 1 everyday 08:00:00 to 12:00:00
```

步骤 2 配置 meter。

```
JX#configure
JX(config)#meter 1 pps 10000 color blind
```

步骤 3 配置 acl 匹配规则和动作。

```
JX#configure
JX(config)#acl-l2 1 name test
JX(configure-acl-l2-1)#rule 1 src-mac any dst-mac any
JX(configure-acl-l2-1)#rule 1 time-range 1
JX(configure-acl-l2-1)#rule 1 action deny
JX(configure-acl-l2-1)#rule 2 src-mac any dst-mac any
JX(configure-acl-l2-1)#rule 2 time-range 2
JX(configure-acl-l2-1)#rule 2 meter 1 outaction red-drop yellow-drop
```

步骤 4 在接口上应用 acl。

```
JX#configure
JX(config)#interface ge 1/0/1 to ge 1/0/2
JX(config-ge-1/0/1->ge-1/0/2)#acl-l2 in 1
```

检查结果

```
JX#show acl config
!
acl-l2 1 name test
 rule 1 src-mac any dst-mac any
 rule 1 time-range 1
 rule 1 action deny
 rule 2 src-mac any dst-mac any
```

```
 rule 2 time-range 2
 rule 2 meter 1 outaction red-drop yellow-drop
!
interface ge 1/0/1
 acl-l2 in name test
!
interface ge 1/0/2
 acl-l2 in name test
```

1.2 AAA

1.2.1 简介

AAA

AAA（Authentication、Authorization、Accounting，认证、授权、计费）是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

- 认证：确认访问网络的远程用户的身份，判断访问者是否为合法的网络用户。
- 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。例如，管理员授权办公用户才能对服务器中的文件进行访问和打印操作，而其它临时访客不具备此权限。
- 计费：记录用户使用网络服务过程中的所有操作，包括使用的服务类型、起始时间、数据流量等，用于收集和记录用户对网络资源的使用情况，并可以实现针对时间、流量的计费需求，也对网络起到监视作用。

AAA 采用客户端/服务器结构，客户端运行于 NAS（Network Access Server，网络接入服务器）上，负责验证用户身份与管理用户接入，服务器上则集中管理用户信息。

AAA 可以通过多种协议来实现，这些协议规定了 NAS 与服务器之间如何传递用户信息。目前设备支持 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）协议和 TACACS+（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）。

RADIUS

RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统）是一种用于对远程访问用户进行集中鉴别的标准化通信协议。RADIUS 使用 UDP 作为传输协议（端口 1812、1813），具有良好的实时性；同时也支持重传机制和备用服务器机制，从而具有较好的可靠性。

- 认证功能

RADIUS 使用客户端/服务器模式，网络访问设备作为 RADIUS 服务器的客户端。RADIUS 服务器负责接收用户的连接请求、对用户进行鉴别，然后将所有客户端所需的配置信息传回，以便为用户提供服务。通过这种方式可以控制用户对设备和网络的访问，提高网络的安全性。

客户端与 RADIUS 服务器之间的通信是通过共享密钥的使用来鉴别的，这个共享密钥不会通过网络传送。此外，任何用户口令在客户机和 RADIUS 服务器间发送时都需要进行加密过程，以避免有人通过嗅探非安全网络得到用户密码。

- RADIUS 计费功能

RADIUS 计费功能主要针对通过 RADIUS 认证的用户进行。在用户登录时给 RADIUS 计费服务器发送一个开始计费的报文，在登录期间根据计费策略给 RADIUS 计费服务器发送计费更新报文，退出登录时，给 RADIUS 计费服务器发送停止计费报文，报文里面包含用户的登录时间。通过这些报文，RADIUS 计费服务器可以记录每个用户的访问时间和操作。

TACACS+

TACACS+（Terminal Access Controller Access Control System，终端访问控制器访问控制系统）是一种与 RADIUS 类似的网络接入认证协议。其区别如下：

- TACACS+使用 TCP 端口 49，相对于 RADIUS 使用的 UDP 端口，具有更高的传输可靠性。
- TACACS+加密数据包除标准的 TACACS+头部外的整体，而包头中有一个区域会指示数据包是否加密。相对于 RADIUS 的只加密用户密码，安全性更高。
- TACACS+的认证功能与授权、计费功能相分离，部署更灵活。

综上所述，TACACS+较 RADIUS 更加安全、可靠，但是 RADIUS 作为一种开放性的协议，在网络中的应用更加广泛。

1.2.2 配置准备

场景

为了控制用户对设备和网络的访问，可以在网络中部署 RADIUS/TACACS+服务器对用户进行认证和计费。本设备可以作为 RADIUS/TACACS+服务器的代理设备，根据 RADIUS/TACACS+服务器反馈的结果对用户访问进行授权。TACACS+较 RADIUS 更加安全、可靠。

前提

无

1.2.3 缺省配置

设备上 AAA 的缺省配置如下。

功能	缺省值
RADIUS 认证服务器未响应之后的失效时间	60 秒
RADIUS 报文重传次数	3
RADIUS 报文重传时间间隔	2 秒

功能	缺省值
RADIUS 认证服务器未响应之后的失效时间	60 秒
TACACS 认证服务器 TCP 连接超时和收包超时时间	2 秒

1.2.4 配置 RADIUS 服务器

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)# **aaa**	进入 AAA 配置模式。
3	JX(config-aaa)#**radius-server deadtime** { *second* | **default** }	全局配置服务器未响应之后的失效时间，单位为秒，缺省值为 60 秒。
4	JX(config-aaa)#**radius-server max-retransmit** { *count* | **default** }	全局配置发送请求失败后的重传次数，缺省值为 3 次。
5	JX(config-aaa)#**radius-server retransmit-interval** { *interval* | **default** }	全局配置重传时间间隔，缺省值为 2 秒。
6	JX(config-aaa)#**radius-server host** *server-name* **ip-address** *ip-address* **key** *key* [**acct-port** *port-id* | **auth-port** *port-id* | **deadtime** { *second* | **default** } | **max-retransmit** { *count* | **default** } | **retransmit-interval** { *interval* | **default** } | **source-ip** *ip-address* [**source-vpn-instance** *vpn-name*] | **vpn-instance** *vpn-name*]*	创建 IPv4 RADIUS 服务器。
7	JX(config-aaa)#**radius-server host** *server-name* **ip6-address** *ipv6-address* **key** *key* [**acct-port** *port-id* | **auth-port** *port-id* | **deadtime** { *second* | **default** } | **max-retransmit** { *count* | **default** } | **retransmit-interval** { *interval* | **default** } | **source-ip6** *ipv6-address* [**source-vpn-instance** *vpn-name*] | **vpn-instance** *vpn-name*]*	创建 IPv6 RADIUS 服务器。

1.2.5 配置 TACACS+服务器

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**aaa**	进入 AAA 配置模式。
3	JX(config-aaa)#**tacacs-server deadtime** { *second* | **default** }	全局配置服务器未响应之后的失效时间，单位为秒，缺省值为 300 秒。
4	JX(config-aaa)#**tacacs-server timeout** { *second* | **default** }	全局配置与服务器的 TCP 连接超时和收包超时时间，缺省值为 2 秒。
5	JX(config-aaa)#**tacacs-server host** *server-name* **ip-address** *ip-address* **key** *key* [**deadtime** { *second* | **default** } | **port** *port-id* | **single-connection** { **enable** | **disable** } | **timeout** { *second* | **default** } | **source-ip** *ip-address* [**source-vpn-instance** *vpn-name*] | **vpn-instance** *vpn-name*]*	创建 IPv4 TACACS 服务器。
6	JX(config-aaa)#**tacacs-server host** *server-name* **ip6-address** *ipv6-address* **key** *key* [**deadtime** { *second* | **default** } | **port** *port-id* | **single-connection** { **enable** | **disable** } | **timeout** { *second* | **default** } | **source-ip6** *ipv6-address* [**source-vpn-instance** *vpn-name*] | **vpn-instance** *vpn-name*]*	创建 IPv6 TACACS 服务器。

1.2.6 配置 AAA 服务器组

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**aaa**	进入 AAA 配置模式。
3	JX (config-aaa)#**server-group** *group-name* { **radius-server** | **tacacs-server** } *server-name*	创建 AAA 服务器组或向 AAA 服务器组添加服务器

1.2.7 配置 AAA 方法

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#aaa	进入 AAA 配置模式。
3	JX(config-aaa)#aaa authentication { dot1x | login | mac-authen | enable } method *method-name* first { *group-name* | local } second { *group-name* | local | none } third { *group-name* | local | none }	配置 AAA 认证方法。 注意事项：服务器组最多配置两个。
4	JX(config-aaa)#aaa authorization { login | cmd } method *method-name* first { *group-name* | local } second { *group-name* | local | none } third { *group-name* | local | none }	配置 AAA 授权方法。 注意事项：服务器组最多配置两个。
5	JX (config-aaa)#aaa accounting { dot1x | login | mac-authen } method *method-name* first { *group-name* | local } second { *group-name* | local | none } third { *group-name* | local | none }	配置 AAA 计费方法。 注意事项：服务器组最多配置两个。

1.2.8 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show aaa config	查看 AAA 配置信息。
2	JX#show aaa information	查看 AAA 全局信息。
3	JX#show aaa server	查看 AAA 服务器信息。
4	JX#show aaa server-group	查看 AAA 服务器组信息。
5	JX#show aaa method	查看 AAA 方法信息。

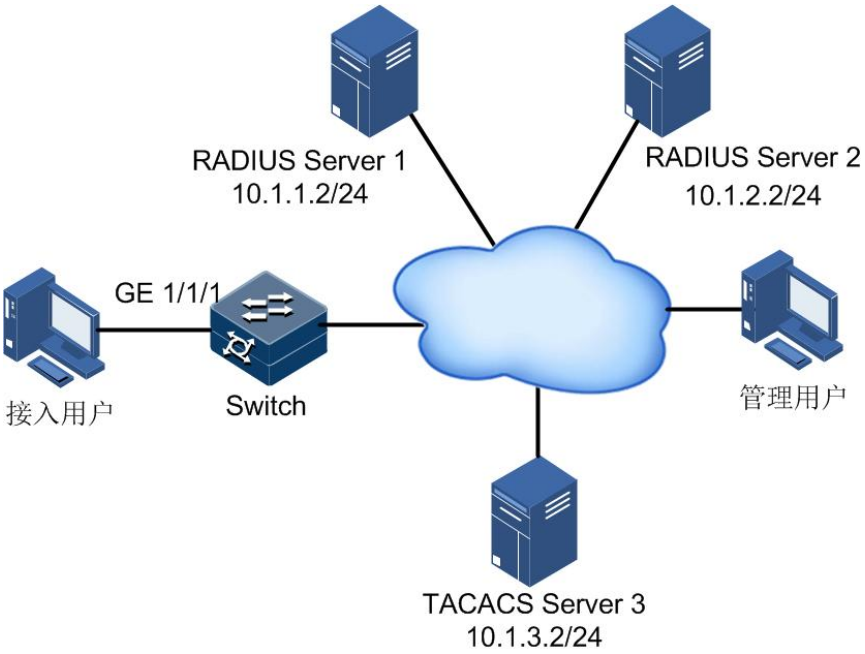
1.2.9 配置 AAA 示例

组网需求

如下图所示，实现接入用户和管理用户接入不同的服务器，要求配置如下：

- 在 Switch 上配置 IP 地址、Vlan 和路由，用于用户连接及认证。
- 创建本地用户，配置管理用户所用的 AAA 模板和方案，采用 TACACS Server 3 进行认证和授权，RADIUS Server 2 进行计费。
- 开启 Dot1x 功能，配置接入用户所使用的 AAA 模板和方案，采用 RADIUS Server 1 进行认证、计费和授权。

图 1-2 分域认证应用组网示意图



配置步骤

步骤 1 配置 IP 地址。

```
JX#config
JX(config)#interface vlan 1
JX(config-vlanif-1)#ip address 10.1.0.254/24
JX(config-vlanif-1)#exit
JX(config)ip route-static 0.0.0.0 0.0.0.0 10.1.0.1
```

步骤 2 配置 AAA 服务器。

```
JX(config)#aaa
JX(config-aaa)#radius-server host Server1 ip-address 10.1.1.2
JX(config-aaa)#radius-server host Server2 ip-address 10.1.2.2
JX(config-aaa)#tacacs-server host Server3 ip-address 10.1.3.2
```

步骤 3 配置 AAA 服务器组。

```
JX(config-aaa)#server-group Group1 radius-server Server1
JX(config-aaa)#server-group Group2 radius-server Server2
JX(config-aaa)#server-group Group3 tacacs-server Server3
```

步骤 4 配置 AAA 方法。

```
JX(config-aaa)#aaa authentication login method Method1 first Group3
JX(config-aaa)#aaa authorization login method Method2 first Group3
JX(config-aaa)#aaa accounting login method Method3 first Group2
JX(config-aaa)#aaa authentication dot1x method Method4 first Group1
JX(config-aaa)#aaa accounting dot1x method Method5 first Group1
switch(config-aaa)#exit
```

步骤 5 配置管理用户认证、授权、计费方法。

```
JX(config)#line vty * *
JX(config-line)#login authentication aaa method Method1
JX(config-line)#login authorization aaa method Method2
JX(config-line)#login accounting aaa method Method3
JX(config-line)#exit
```

步骤 6 配置接入用户认证、授权、计费方法。

```
JX(config)#dot1x start
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#dot1x enable
JX(config-ge-1/0/1)#dot1x aaa-authentication Method4
JX(config-ge-1/0/1)#dot1x aaa-accounting Method5
JX(config-ge-1/0/1)#exit
```

1.2.10 检查结果

步骤 1 通过 **show aaa config** 查看 AAA 配置是否正确。

```
JX#show aaa config
Version  : AAA_V7.00.00.00
!
aaa
 radius-server host Server1 ip-address 10.1.1.2
 radius-server host Server2 ip-address 10.1.2.2
 tacacs-server host Server3 ip-address 10.1.3.2
 server-group Group1 radius-server Server1
 server-group Group2 radius-server Server2
 server-group Group3 tacacs-server Server3
 aaa authentication login method Method1 first Group3
 aaa authorization login method Method2 first Group3
 aaa accounting login method Method3 first Group2
 aaa authentication dot1x method Method4 first Group1
 aaa accounting dot1x method Method5 first Group1
```

1.3 802.1x

1.3.1 简介

802.1x 是基于 IEEE 802.1x 协议即基于接口的网络接入控制技术。802.1x 功能的主要目的是解决局域网用户的接入认证和安全问题。

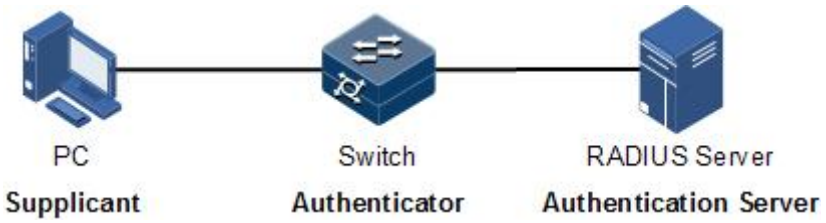
在网络设备的物理接入层对接入设备进行认证和控制，仅定义了设备接口和用户设备之间的点到点连接方式。连接在接口上的用户设备如果能够通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法通过交换机访问网络中的资源。

802.1x 体系结构

802.1x 认证采用客户端/服务器模式，如下图所示，包括以下 3 个部分：

- 申请者（Supplicant）：需要安装 802.1x 客户端软件（例如 Windows XP 自带的 802.1x 客户端）的用户侧设备，如计算机等。
- 认证者（Authenticator）：提供 802.1x 认证功能的接入控制设备，如交换机等。
- 认证服务器（Authentication Server）：用于对用户进行认证、授权和计费，通常使用 RADIUS 服务器作为 802.1x 认证服务器。

图 1-3 802.1x 认证体系结构



接口接入控制模式

认证者利用认证服务器对需要接入局域网的客户端进行认证，并根据认证结果对接入接口授权或者非授权状态进行控制。用户可以通过配置接口的接入控制模式来控制接口的接入状态。802.1x 认证支持三种接口接入控制模式：

- 协议授权模式（auto）：由协议状态机决定认证授权结果，在认证成功之前，仅允许收发 EAPoL 报文，不允许用户访问网络资源和交换机提供的服务。如果认证通过，则接口切换到授权状态，允许用户访问网络资源和交换机提供的服务。
- 强制接口授权模式（authorized-force）：接口始终处于授权状态，允许用户不经认证授权即可访问网络资源和交换机提供的服务。
- 强制接口非授权模式（unauthorized-force）：接口始终处于非授权状态，不允许用户访问网络资源和交换机提供的服务，即不允许用户进行认证。

802.1x 认证过程

802.1x 系统支持 EAP 中继和 EAP 终结两种方式完成与 RADIUS 服务器之间的认证过程。

- EAP 中继方式

申请者与认证服务器之间通过 EAP（Extensible Authentication Protocol，可扩展认证协议）报文交换信息。申请者与认证者之间则以 IEEE802.1x 协议所定义的 EAPoL（EAP over LAN，基于局域网的 EAP）报文交换信息。EAP 报文中封装了认证数据，该认证数据将被封装在 RADIUS 协议的报文中，以穿越复杂的网络到达认证服务器，这一过程称为 EAP 中继。

认证者或申请者均能发起 802.1x 认证过程。以申请者发起认证过程为例，EAP 中继认证过程如下：

1. 用户输入用户名和密码，申请者向认证者发送一个 EAPoL-Start 报文，开始一次 802.1x 认证；
2. 认证者向申请者发送 EAP-Request/Identity 报文，询问请求者的用户名；
3. 申请者响应一个 EAP-Response/Identity 给认证者，其中包括用户名信息；

4. 认证者将 EAP-Response/Identity 报文封装到 RADIUS 协议报文中，发送给认证服务器；
5. 认证服务器将接收到的用户名信息与数据库中的用户名表进行比对，找到该用户的口令信息，利用随机生成的加密字对口令信息进行加密处理。同时，认证服务器将此加密字发送给认证者，认证者再将此加密字发送给申请者；
6. 申请者利用接收到的加密字对口令进行加密，并通过认证者发送给认证服务器；
7. 认证服务器对比收到的加密口令与自身生成的加密口令否一致。如果认证成功，认证者将接口改为授权状态，允许用户通过接口访问网络，并发送 EAP-Success 报文给申请者；如果认证失败，则接口为非授权状态，并发送 EAP-Failure 报文给通知申请者。

- EAP 终结方式

将 EAP 报文在设备端终结并映射到 RADIUS 报文中，利用标准 RADIUS 协议完成认证、授权和计费过程。设备端支持与 RADIUS 服务器之间采用 PAP 或者 CHAP 认证方法。

在 EAP 终结方式中，用来对用户密码信息进行加密处理的随机加密字由设备端生成，之后设备端会把用户名、随机加密字和客户端加密后的密码信息共同发送给 RADIUS 服务器，进行相关的认证处理。

802.1x 定时器

802.1x 认证过程中，认证设备上涉及到 5 个定时器：

- Reauth-period：重认证定时器。在该定时器超时后，会重新发起 802.1x 认证。
- Quiet-period：静默定时器。用户认证失败以后，认证设备需要静默一段时间，静默定时器超时后再重新发起认证。在静默期间，交换机不处理认证报文。
- Tx-period：请求报文发送超时定时器。当交换机向用户请求端发送 Request/Identity 请求报文后，会启动该定时器，在该定时器超时后，用户端软件未成功发送认证应答报文，则设备重发认证请求报文，此报文共重发 3 次。
- Supp-timeout：申请者认证超时定时器。当交换机向用户请求端发送了用于请求用户端 MD5 加密密文的 Request/Challenge 请求报文后，交换机启动该定时器。若在该定时器设置的时长内用户请求端未成功响应，交换机将重发该报文，此报文共重发两次。
- Server-timeout：认证服务器超时定时器。该定时器定义认证者和认证服务器会话超时的总时长，此定时器超时后认证者结束同认证服务器会话，重新开始一次新的认证过程。

802.1x guest-vlan

在网络中，用户在未经过 802.1x 认证时只能访问有限资源，当配置 guest-vlan 功能后，设备对 untag 报文添加 guest-vlan，并允许该报文通过端口。

- 基于端口认证：认证时认证通过会删除端口的 guest-vlan。
- 基于用户认证：认证通过会保留端口的 guest-vlan。
- guset-vlan 不能是 supervlan，也不能是 voice-vlan。

1.3.2 配置准备

场景

为了实现对局域网用户的接入认证，并解决接入用户的安全问题，需要在设备上配置802.1x 认证。

对于认证通过的用户，允许其访问网络中的资源；如果认证未通过，则该用户无法访问网络资源。通过对用户接入接口的认证控制，达到对用户管理的目的。

前提

配置 802.1x 认证之前，如果使用 RADIUS 认证服务器，需要完成以下任务：

- 配置 RADIUS 服务器 IP 地址和 RADIUS 公有密钥。
- 交换机能够与 RADIUS 服务器 Ping 通。

1.3.3 802.1x 功能的缺省配置

设备上 802.1x 功能的缺省配置如下。

功能	缺省值
全局 802.1x 功能状态	禁止
接口 802.1x 功能状态	禁止
全局认证方式	**chap**
接口接入控制模式	**auto**
接口认证方式	**macbased**
RADIUS 服务器超时定时器时间	10s
802.1x 重认证功能状态	允许
802.1x 重认证定时器时间	5600s
802.1x 静默定时器时间	60s
请求报文重传定时器时间	30s
最大用户数	128

1.3.4 配置 802.1x 基本功能

注意

- 一个接口同一时刻只能处理一个用户认证请求。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dot1x { start | stop }**	使能或去使能全局 802.1x 功能。
3	JX(config)#**dot1x aaa authentication method** *method-name*	绑定全局 802.1x 认证时的 AAA 方法。
4	JX(config)#**dot1x max-user** *user-number*	配置全局 802.1x 认证最大用户数。
5	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
6	JX(config-ge-1/0/*)#**dot1x enable**	使能接口 802.1x 功能。
7	JX(config-ge-1/0/*)#**dot1x port-control { auto | force-auth | force-unauth }**	配置接口接入控制模式。
8	JX(config-ge-1/0/*)#**dot1x port-method { mac | port }**	配置接口认证方式。
9	JX(config-ge-1/0/*)#**dot1x max-user** *user-number*	配置 802.1x 端口允许认证的最大用户数。
10	JX(config-ge-1/0/*)#**nac guest-vlan** *vlan-id*	配置指定端口的 Guest VLAN，对 802.1x 协议和 mac 认证都生效。
11	JX(config-ge-1/0/*)#**dot1x critical-vlan** *vlan-id*	配置指定端口的 802.1x Critical VLAN。
12	JX(config-ge-1/0/*)#**dot1x restrict-vlan** *vlan-id*	配置指定端口的 802.1x Restrict VLAN。
13	JX(config-ge-1/0/*)#**dot1x reauthenticate all user**	手动触发指定端口下 802.1x 用户进行重认证。
14	JX(config-ge-1/0/*)#**dot1x delete all user**	强制将端口下 802.1x 用户下线。
15	JX(config-ge-1/0/*)#**dot1x quiet { disable | enable }**	使能或去使能端口 802.1x 用户静默功能。
16	JX(config-ge-1/0/*)#**dot1x quiet-times** *times*	配置端口 802.1x 用户触发静默功能的认证失败次数，默认 3 次。

说明

如果全局或接口模式下未使能 802.1x 功能，则接口下不能使能 802.1x 功能。

1.3.5 配置 802.1x 重认证

注意

重认证功能是针对已授权的用户发起的，所以在使能重认证功能之前，应该保证使能全局和接口 802.1x 功能。处于授权状态的接口在重认证过程中仍保持授权状态，如果重认证失败，才进入非授权状态。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/*)#**dot1x reauthenticate** { **enable** | **disable** }	使能 802.1x 重认证功能。

1.3.6 配置 802.1x 定时器

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/*)#**dot1x reauthenticate period** *time*	配置重认证定时器时间。
4	JX(config-ge-1/0/*)#**dot1x timer quiet-period** *time*	配置静默定时器时间。
5	JX(config-ge-1/0/*)#**dot1x supp period** *time*	配置 Request/MD5 Challenge 请求报文超时定时器。
6	JX(config-ge-1/0/*)#**dot1x server-timeout period** *time*	配置认证服务器超时定时器时间。
7	JX(config-ge-1/0/*)#**dot1x tx period** *time*	配置 Request/Identity 请求报文超时定时器。

1.3.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show dot1x config	查看所有 802.1x 相关配置信息。
2	JX#show dot1x information	查看 802.1x 协议统计信息。
3	JX#show dot1x user	查看 802.1x 协议认证的用户信息。
4	JX#show dot1x *interface-type interface-number*	查看接口下 802.1x 相关统计及配置信息。

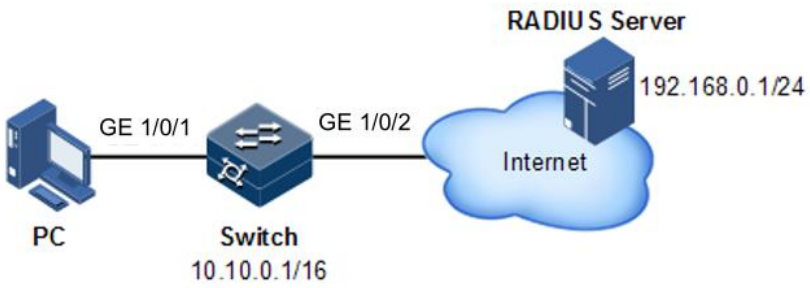
1.3.8 配置 802.1x 示例

组网需求

为了使用户访问外部网络，如下图所示，在交换机上配置 802.1x 认证，具体要求如下：

- 交换机的 IP 地址是 10.10.0.1，掩码是 255.255.0.0，缺省网关地址为 10.10.0.2。
- 通过 RADIUS 服务器进行认证和授权，RADIUS 服务器的 IP 地址是 192.168.0.1，密码是 JX。
- 在认证通过后，可以在 600s 后自动发起重认证过程。

图 1-4 802.1x 应用组网示意图



配置步骤

步骤 1 配置交换机 IP 地址及 RADIUS 服务器地址。

```
JX#config
JX(config)#interface vlan 1
JX(config-vlan1)#ip address 10.10.0.1/16
JX(config-vlan1)#exit
JX(config)#ip route 0.0.0.0 0.0.0.0 10.10.0.2
JX(config)#exit
JX(config)#aaa
JX(config-aaa)#radius-server host server1 ip-address 192.168.0.1 key 12345
JX(config-aaa)#server-group grp1 radius-server server1
JX(config-aaa)#aaa authentication dot1x method d1 first grp1
```

步骤 2 使能全局及接口 802.1x 认证功能。

```
JX#config
JX(config)#dot1x start
JX(config)#dot1x aaa authentication method d1
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#dot1x enable
JX(config-ge-1/0/1)#dot1x reauthenticate period 600
```

检查结果

通过 **show dot1x** 命令查看设备上 802.1x 功能的配置结果。

```
JX#show dot1x interface ge 1/0/1
Interface                  : ge 1/0/1
 Authentication Guest Vlan    : n/a
 Max User Num               : 1
 Default Max User Num        : 1
 Current User Num           : 1
 Authen Success User Num     : 0
 Authen Fail User Num        : 1
 Authen Timeout User Num     : 1
 Authenting User Num         : 0
 Authentication Method       : n/a
 Accounting Method           : n/a
 Quiet                      : Disable
 Reauthentication            : Enable
 Reauthentication Period     : 5600
 Mac Bypass                 : Disable
 Offline Detect             : Disable
 Restrict Vlan              : n/a
 Critical Vlan              : n/a
 TX Period                  : 30
 Supp Timeout Period         : 5
 Server time Period          : 120
 Port Control               : Auto
 Port Method                : Mac Based
 Port Auth State            : Unauthenticated
 Auth Method                : Chap
 Not Eapol Trigger           : Disable
 Trigger Authen Type         : None
 Trigger Auth Pkt Type       : ARP NDP DHCP DHCP6
 Rx Eapol Start Pkt Num      : 61
 Rx Eapol Logoff Pkt Num     : 0
 Rx Eap Idenitity Pkt Num    : 12
 Rx Eap MD5 Pkt Num         : 5
 Tx Eap Success Pkt Num      : 0
 Tx Eap Fail Pkt Num         : 11
 Tx Eap Idenitity Pkt Num    : 6
 Tx Eap MD5 Pkt Num         : 5
```

1.4 PPPoE+

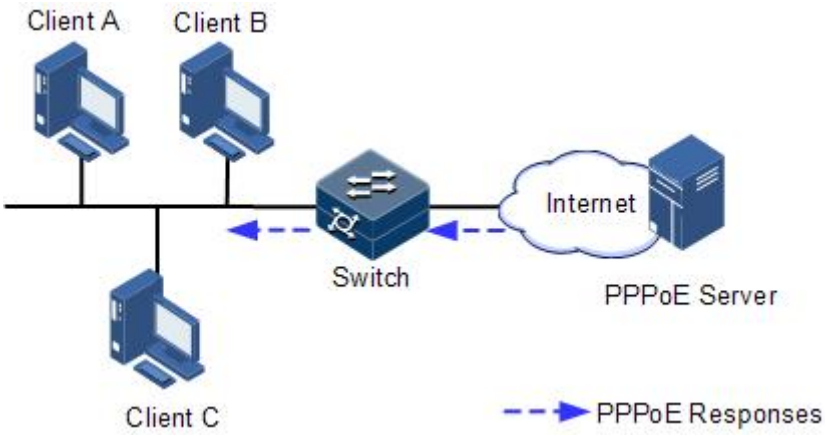
1.4.1 简介

PPPoE+（PPPoE Intermediate Agent，PPPoE 中继代理）协议用于对 PPPoE（Point to Point Protocol Over Ethernet，基于以太网承载点到点协议）认证报文进行处理，即对 PPPoE 报文附加更多接入设备信息，使服务器能获得足够的信息辨别用户。PPPoE+协议可以有效防止在 PPPoE 认证过程中的账号共享或者账号盗用问题，保证了网络的安全性。

使用 PPPoE 拨号方式连接网络，用户通过设备的不同接口，只要通过同一个认证服务器认证成功，就可以使用这个账号访问网络。但是服务器仅根据包含用户名和密码的认证信息，很难对用户进行区分。增加 PPPoE+特性以后，认证时除了需要用户名和密码信息外，在认证报文中还将携带设备接口等信息。如果认证服务器识别的接口号等信息与配置不一致，则认证不通过，这样就可以防止非法用户盗用其他合法用户的账号进行上网。

PPPoE 协议采用客户端/服务器模式，如下图所示，Switch 起到中继代理的作用，用户通过 PPPoE 认证连接网络。如果服务器需要定位用户，在认证报文中则需要更多的客户信息。

图 1-5 用户通过 PPPoE 认证连接网络示意图



用户通过 PPPoE 访问网络需要经过两个阶段：第一个阶段是发现阶段，即认证阶段，第二个阶段是会话阶段。PPPoE+功能需要处理的就是发现阶段的报文。

- 客户端通过 PPPoE 访问网络，首先会发送一个广播报文 PADI（PPPoE Active Discovery Initiation，PPPoE 活动发现发起报文），该报文的作用是查找认证服务器；
- 收到 PADI 报文的认证服务器会发送一个单播 PADO（PPPoE Active Discovery Offer，PPPoE 活动发现提供报文）报文响应；
- 如果有多个认证服务器发送了 PADO 报文，客户端会从中选择一个，发送单播 PADR（PPPoE Active Discovery Request，PPPoE 活动发现请求报文）报文请求认证；
- 认证服务器收到 PADR 报文后，如果判定用户合法，则发送一个单播报文 PADS（PPPoE Active Discovery Session-confirmation，PPPoE 活动发现会话确认报文）作为 PADR 的响应。至此，发现阶段完毕。

PPPoE+的主要功能是在 PADI 和 PADR 报文中添加用户标识信息，服务器可以判定标识信息是否和用户账号匹配，决定是否分配资源。

1.4.2 配置准备

场景

为了防止在 PPPoE 认证过程中有非法用户接入，需要配置 PPPoE+功能，在 PPPoE 协议报文中加入附加的用户标识信息。

由于添加的用户标识信息和具体的交换机及接口相关，因此认证服务器可以将用户和交换机以及接口等信息绑定。从而有效防止账号共享和账号盗用问题，还可以更好的定位用户，以保证网络的安全性。

前提

无

1.4.3 PPPoE+功能的缺省配置

设备上 PPPoE+功能的缺省配置如下。

功能	缺省值
全局 PPPoE+功能状态	禁止
接口 PPPoE+功能状态	禁止
全局 PPPoE+Tag 的收包处理策略	replace
Circuit ID 的填充模式	SwitchCommon 模式
Circuit ID 信息	接口名/外层 VLAN 号/内层 VLAN 号
Circuit ID 的附加字符串	无
Remote ID 填充的 MAC 地址	交换机的 MAC 地址
Remote ID 填充形式	二进制形式
接口信任状态	非信任接口
PPPoE+ Tag 收包处理策略	替换

说明

缺省情况下，PPPoE 报文可以通过接口并且不会被附加任何信息。

1.4.4 配置 PPPoE+基本功能

注意

PPPoE+功能用于处理 PADI 和 PADR 报文，只针对 PPPoE 的客户端。一般只有连接客户端的接口使能 PPPoE+功能，而信任接口是指交换机与 PPPoE 服务器连接的接口，这两种接口角色是互斥的，即一个接口不能既使能 PPPoE+功能又是信任接口。

使能 PPPoE+功能

使能设备全局和接口的 PPPoE+功能后，发送到该接口的 PPPoE 认证报文会附加上用户信息，再发往信任接口。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#pppoeplus start`	使能全局 PPPoE+功能。
3	`JX(config)#interface` *interface-type interface-number*	进入二层物理接口配置模式。
4	`JX(config-ge-1/0/1)#pppoeplus enable`	使能接口 PPPoE+功能。

配置 PPPoE+信任接口

配置 PPPoE+信任接口主要是为了降低 CPU 使用率，信任接口收到的 PPPoE 报文不会上送 CPU 处理，由交换芯片直接转发。通常配置在与 PPPoE 服务器相连的接口上。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#interface` *interface-type interface-number*	进入二层物理接口配置模式。
3	`JX(config-ge-1/0/1)#pppoeplus trust`	配置 PPPoE+的信任接口。

1.4.5 配置 PPPoE+报文信息

PPPoE+功能主要是对 PPPoE 报文中的一个特定 Tag 进行处理，这个 Tag 包含 Circuit ID 和 Remote ID 两个字段。其中：

- Circuit ID 填充的是接收客户端请求报文接口的接口名、所属于的 VLAN ID（包括外层 VLAN ID 和内层 VLAN ID）
- Remote ID 填充的是接收客户端请求报文接口的 MAC 地址或者交换机的 MAC 地址。

配置 Circuit ID

Circuit ID 有三种填充模式：ascii 模式、default 模式和 user-define 模式。

各 Circuit ID 填充模式意义如下：

- ascii：即 Circuit ID 填充为命令行配置的字符串。
- default：即 Circuit ID 为默认值。
- user-define：即按照用户自定义格式填充 Circuit ID。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**pppoeplus default circuit-id format** { **ascii** | **default** | **user-define** } *string*	配置交换机 Circuit ID。（default 模式不需要再配置字符串）
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
4	JX(config-ge-1/0/1)#**pppoeplus circuit-id format** { **ascii** | default| **user-define** } *string*	在接口上配置 Circuit ID。 （default 模式不需要再配置字符串，如果接口和全局都配置了 circuit-id，则接口的配置优先生效）

配置 Remote ID

Remote ID 有三种填充模式：ascii 模式、default 模式和 user-define 模式。

各 Remote ID 填充模式意义如下：

- ascii：即 Circuit ID 填充为命令行配置的字符串。
- default：即 Circuit ID 为默认值。
- user-define：即按照用户自定义格式填充 Circuit ID。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**pppoeplus default remote-id format** { **ascii** | **default** | **user-define** } *string*	配置交换机 Remote ID。（default 模式不需要再配置字符串）
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。

步骤	配置	说明
4	JX(config-ge-1/0/1)#**pppoeplus remote-id format** { **ascii** | default| **user-define** *string* }	在接口上配置 Remote ID。 （default 模式不需要再配置字符串，如果接口和全局都配置了 remote-id，则接口的配置优先生效）

配置 PPPoE+Tag 处理策略

由于某些原因，如某些信息字段的 Tag 可能是客户端伪造的，需要将报文原有的 Tag 替换掉。配置 PPPoE+Tag 收包处理策略为替换后，如果 PPPoE 报文已经携带信息字段 Tag，会将其替换；如果配置 PPPoE+Tag 收包处理策略为保持，则如果 PPPoE 报文已经携带信息字段 Tag，就保留原 tag；如果配置 PPPoE+Tag 收包处理策略为丢弃，则如果 PPPoE 报文已经携带信息字段 Tag，就会丢弃原 tag。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**pppoeplus default policy** { **drop** | **keep** | **replace** }	配置全局的 PPPoE+Tag 的收包处理策略。
	JX(config-ge-1/0/1)# **pppoeplus policy** { **drop** | **keep** | **replace** }	配置接口上的 PPPoE+Tag 的收包处理策略。如果接口和全局都配置了收包处理策略，则接口的配置优先生效

1.4.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show pppoeplus config**	查看 PPPoE+的配置信息。
2	JX#**show pppoeplus information**	查看 PPPoE+模块当前的全局配置信息，包括默认配置信息。

1.4.7 维护

用户可以通过以下命令，维护 PPPoE+特性的运行情况和配置情况。

命令	描述
JX(config)#**reset pppoeplus statistic** [**interface** *interface-type interface-number*]	清除 PPPoE+的统计信息，支持指定端口清除统计信息。

命令	描述
JX#**show pppoeplus interface** [*interface-type interface-number*]	查看 PPPoE+的接口上的配置和统计信息。

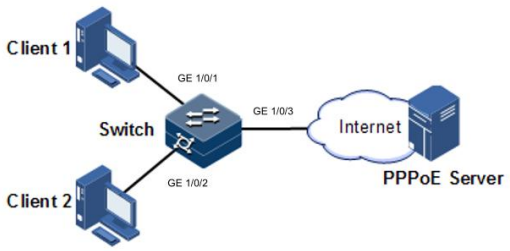
1.4.8 配置 PPPoE+示例

组网需求

如下图所示，为了防止在 PPPoE 认证过程中非法用户的接入，对用户上网进行控制和监管，可以在交换机上配置 PPPoE+功能，具体要求如下：

- 接口 GE 1/0/1 和 GE 1/0/2 分别连接 Client 1 和 Client 2，GE 1/0/3 连接 PPPoE 服务器；
- 使能全局 PPPoE+功能和 GE 1/0/1、GE 1/0/2、GE 1/0/3 的 PPPoE+功能，配置 GE 1/0/3 为信任接口；
- 配置 Circuit ID 类型为用户自定义，格式为接口名加外层 VLAN ID 加设备名；配置 Remote ID 类型为 ascii，内容为 01:02:03:04:05:06；
- 配置接口 GE 1/0/1 和 GE 1/0/2 的 PPPoE+Tag 的收包处理策略。

图 1-6 PPPoE+应用组网示意图



配置步骤

步骤 1 使能全局 PPPoE+功能，并使能 GE 1/0/1、GE 1/0/2 和 GE 1/0/3 的 PPPoE+功能。

```
JX(config)#pppoeplus start
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#pppoeplus enable
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#pppoeplus enable
JX(config-ge-1/0/2)#exit
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#pppoeplus enable
JX(config-ge-1/0/3)#exit
```

步骤 2 配置 GE 1/0/3 为信任接口。

```
JX#config
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#pppoeplus trust
JX(config-ge-1/0/3)#exit
```

步骤 3 配置 circuit-id 和 remote-id 的格式。

```
JX(config)#pppoeplus default circuit-id format
user-defined %portname:%svlan:%devicename
JX(config)#pppoeplus default remote-id format ascii 01:02:03:04:05:06
```

步骤 4 配置 GE 1/0/1 和 GE 1/0/2 的 PPPoE+Tag 的收包处理策略。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#pppoeplus policy keep
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#pppoeplus policy drop
JX(config-ge-1/0/2)#exit
```

检查结果

通过 **show pppoeplus config** 命令查看设备上 PPPoE+功能的配置结果。

```
JX#show pppoeplus config
!
pppoeplus start
pppoeplus default remote-id format ascii 01:02:03:04:05:06
pppoeplus default circuit-id format
user-defined %portname:%svlan:%devicename
!
interface ge 1/0/1
 pppoeplus enable
 pppoeplus policy keep
!
interface ge 1/0/2
 pppoeplus enable
 pppoeplus policy drop
!
interface ge 1/0/3
 pppoeplus enable
 pppoeplus trust
```

1.5 安全 MAC

1.5.1 简介

接口安全 MAC 主要应用于网络边缘用户侧的交换设备上，用于保证某个接口接入数据的安全性，根据源 MAC 地址对输入的报文加以控制。用户可以启动接口安全功能来限制和区分哪些用户可以通过安全接口来访问网络，只有接口安全 MAC 地址才能够访问网络，非安全 MAC 地址均按照用户配置的接口访问违例模式处理。

安全 MAC 地址分类

设备支持的安全 MAC 地址分为以下两类：

- 安全 MAC 地址

动态安全 MAC 地址是由设备自己学习得到的。用户可以在允许学习的 MAC 地址最大数目范围内，将学习到的 MAC 地址都设置为安全 MAC 地址。该类安全 MAC 地址不会被老化，但是不支持配置加载。

- Sticky 安全 MAC 地址

Sticky 安全 MAC 地址由用户在安全接口手动配置生成或者由安全 MAC 地址转化而来。与安全 MAC 地址不同，Sticky 安全 MAC 地址需要配合 Sticky 学习功能一起使用，支持配置加载：

说明

- 当 Sticky 学习功能使能时，接口下学习到的所有安全 MAC 地址均转换为 Sticky 安全 MAC 地址。
- 当 Sticky 学习功能禁止时，接口下所有 Sticky 安全 MAC 地址均转换为安全 MAC 地址。

安全 MAC 违例处理方式

当接口安全 MAC 的数目已经达到最大数目时，再有陌生源 MAC 报文输入则视为违规操作。对于非法的用户接入，根据安全 MAC 的违规策略配置交换机的不同处理方式如下：

- Protect 模式：对于非法接入的用户，安全接口直接丢弃该用户的报文。
- Restrict 模式：对于非法接入的用户，安全接口丢弃该用户的报文，同时在控制台打印 Syslog 信息，并发送告警信息至网管系统。
- Shutdown 模式：对于非法接入的用户，安全接口丢弃该用户的报文，同时在控制台打印 Syslog 信息、发送告警信息至网管系统并将该安全接口关闭。

注意

当发生 MAC 地址飘移，即安全接口 A 收到一个已经存在于安全接口 B 中的安全 MAC 所对应用户的访问时，安全接口 A 将其作为违例处理。

1.5.2 配置准备

场景

为了保证交换机接口接入数据的安全性，可以根据源 MAC 地址对输入的报文加以控制。通过安全 MAC 可以将接入接口配置成只允许特定的几个用户接入，也可以配置成允许特定数量的用户从该接口接入。但接入的用户超过限制时，接入的报文将按照安全 MAC 的违规策略进行处理。

前提

无

1.5.3 安全 MAC 功能的缺省配置

设备上安全 MAC 功能的缺省配置如下。

功能	缺省值
接口安全 MAC 功能状态	禁止
动态安全 MAC Sticky 学习功能状态	禁止
接口安全 MAC Trap 功能状态	禁止
接口安全 MAC 违规处理方式	**restrict**
接口安全 MAC 的最大数量	1024

1.5.4 配置安全 MAC 基本功能

注意

- 不建议用户在聚合组的单个成员接口上使能接口安全 MAC 功能。
- 不建议用户在同一接口上使能接口安全 MAC 功能的同时，使用 MAC 地址管理功能来配置静态 MAC 地址，会导致接口安全 MAC 功能失效。
- 当 802.1x 接口认证方式为基于 MAC 地址进行认证时，安全 MAC 功能与 802.1x 功能互斥，不建议用户在同一接口上同时进行配置。
- 安全 MAC 功能与基于接口和基于接口 VLAN 的 MAC 地址数目限制互斥，不能同时配置。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#interface` *interface-type interface-number*	进入二层物理接口配置模式。
3	`JX(config-ge-1/0/1)#port-security enable`	使能接口安全 MAC 功能。
4	`JX(config-ge-1/0/1)#port-security maximum` *maximum*	配置接口安全 MAC 最大数目。
5	`JX(config-ge-1/0/1)#port-security protect-action { protect | restrict | shutdown }`	配置安全 MAC 违例模式。

步骤	配置	说明
6	JX(config-ge-1/0/1)#**shutdown** JX(config-ge-1/0/1)#**no shutdown**	将因违反接口安全 MAC 而被关闭的接口重新开启。
7	JX(config)# **port-security error-down recovery-interval** *second*	(可选)配置接口安全 MAC 恢复时间。

说明

当安全 MAC 违规策略为 Shutdown 模式时，可以使用该命令将因违反接口安全 MAC 而被关闭的接口重新开启。

当接口 Up 以后，配置的安全 MAC 违例模式继续保持。

1.5.5 配置接口 Sticky 安全 MAC 地址

注意

建议用户不要在 Sticky 安全 MAC 功能禁止的情况下配置 Sticky 安全 MAC 地址，否则可能导致功能异常。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
3	JX(config-ge-1/0/1)#**port-security enable**	使能接口安全 MAC 功能。
4	JX(config-ge-1/0/1)#**port-security mac-address sticky enable**	使能 Sticky 安全 MAC 学习功能。
5	JX(config-ge-1/0/1)#**port-security mac-address sticky vlan** *vlan-id* **mac** *mac-address*	手动配置接口 Sticky 安全 MAC 地址。

说明

Sticky 安全 MAC 学习功能使能后，动态安全 MAC 地址转换为 Sticky 安全 MAC 地址；手动设置的 Sticky 安全 MAC 地址生效。

1.5.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show mac-address config**	查看安全 MAC 的配置信息。
2	JX#**show mac-address** { **security** | **sticky** }	查看安全 MAC 地址表项信息。

1.5.7 维护

用户可以通过以下命令，维护设备安全 MAC 特性的运行情况和配置情况。

命令	描述
JX(config)#**no mac-address** { **security** | **sticky** } [*interface-type interface-number*]	清除指定类型的安全 MAC。

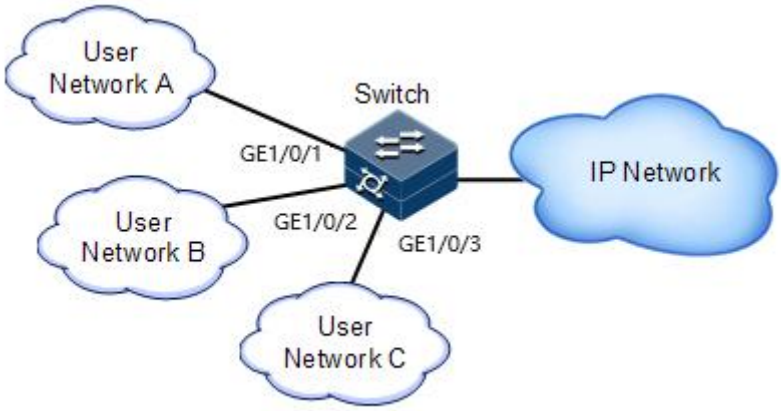
1.5.8 配置安全 MAC 示例

组网需求

如下图所示，交换机下联 3 个用户网络，为了保证交换机接口接入数据的安全性，要求配置如下：

- 接口 GE 1/0/1 最大允许 3 个用户接入网络。其中一个指定用户的 MAC 地址为 0000.0000.0001。其他 2 个用户为动态学习。违例模式采用 Protect 模式
- 接口 GE 1/0/2 最大允许 2 个用户接入网络。这 2 个用户的 MAC 地址通过学习确定。违例模式采用 Restrict 模式。
- 接口 GE 1/0/3 要求最大允许 1 个用户接入网络。该指定用户的 MAC 地址为 0000.0000.0002，违例模式采用 Shutdown 模式。

图 1-7 安全 MAC 应用组网示意图



配置步骤

步骤 1 配置 GE 1/0/1 接口安全 MAC。

```
JX#config
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#port-security enable
JX(config-ge-1/0/1)#port-security maximum 3
JX(config-ge-1/0/1)#port-security mac-aopddress sticky enable
JX(config-ge-1/0/1)#port-security mac-address sticky vlan 1
mac 00:00:00:00:00:01
JX(config-ge-1/0/1)#quit
```

步骤 2 配置 GE 1/0/2 的接口安全 MAC。

```
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#port-security enable
JX(config-ge-1/0/2)#port-security maximum 2
JX(config-ge-1/0/2)#port-security protect-action restrict
JX(config-ge-1/0/2)#quit
```

步骤 3 配置 GE 1/0/3 的接口安全 MAC。

```
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#port-security enable
JX(config-ge-1/0/3)#port-security maximum 1
JX(config-ge-1/0/3)#port-security protect-action shutdown
JX(config-ge-1/0/3)#port-security mac-address sticky enable
JX(config-ge-1/0/3)#port-security mac-address sticky vlan 1
mac 00:00:00:00:00:02
JX(config-ge-1/0/3)#quit
```

检查结果

通过 **show mac-address config** 查看安全 MAC 的接口配置是否正确。

```
JX#show mac-address config
!
```

```
mac-address aging-time 500
!
interface ge 1/0/1
 port-security enable
 port-security maximum 3
 port-security mac-address sticky enable
!
interface ge 1/0/2
 port-security enable
 port-security maximum 2
!
interface ge 1/0/3
 port-security enable
 port-security protect-action shutdown
 port-security mac-address sticky enable
```

通过 **show mac-address sticky** 查看设备上接口安全 MAC 地址配置及学习情况。

```
JX(config)#show mac-address sticky
  MacAddress         VLAN/VSI/BD Learned-From    Type        Valid
-------------------------------------------------------------------------
  0000:0000:0001      1/--/--     ge-1/0/1        sticky      yes
  0000:0000:0002      1/--/--     ge-1/0/3        sticky      yes
-------------------------------------------------------------------------
  Total:2       Static:0       Dynamic:0       Blackhole:0
  Sticky:2      Security:0      Snooping:0
```

1.6 风暴抑制与风暴控制

1.6.1 简介

二层网络是一个广播域，当接口接收到大量的广播、未知组播和未知单播报文时，就会产生广播风暴。如果不对广播风暴进行限制，就会耗费大量的网络带宽，造成网络速率下降，甚至造成通信中断，影响正常报文的转发。

风暴抑制与风暴控制能对网络中的广播流量进行限制，能在广播流量激增时抑制广播风暴的产生，从而保证正常报文的转发。

广播风暴产生

下面几种情况可能会产生广播风暴：

- 未知单播报文：目的 MAC 地址不在 MAC 地址表中的单播报文，即 DLF（Destination Lookup Failure，寻找目标失败）报文，如果某段时间内此种报文流量过多，进行大量的广播发送，可能会形成广播风暴。
- 未知组播报文：目的 MAC 地址不在 MAC 地址表中的组播报文，如果某段时间内此种报文流量过多，进行大量的广播发送，可能会形成广播风暴。
- 广播报文：目的 MAC 地址为广播的报文，如果某段时间内此种报文流量过多，可能会形成广播风暴。

风暴抑制原理

风暴抑制是对网络上可能形成广播风暴的广播、未知组播或未知单播报文进行过滤。当设备接收到的广播报文超过一定阈值时，将进行相应的动作。

风暴控制原理

风暴控制是对网络上可能形成广播风暴的广播、未知组播或未知单播报文进行过滤。当设备接收到的广播报文超过一定阈值时，将自动丢弃收到的广播报文。当未启用该功能或广播报文未达到一定阈值时，广播报文将被正常广播到设备的其它接口。

风暴抑制与风暴控制方式

方式有以下几种：

- BPS（Bits Per Second，每秒位数）：每秒允许通过的位数。
- PPS（Packets Per Second，每秒包数）：每秒允许通过的包数。
- Percent：以接口最大速率的百分比进行限速，仅物理口支持

1.6.2 配置准备

场景

在二层网络中配置风暴抑制功能，当网络中未知组播、未知单播和广播报文增多时可以抑制广播风暴的产生，从而保证正常报文的转发。

前提

无

1.6.3 风暴抑制和风暴控制的缺省配置

设备上风暴抑制的缺省配置如下。

功能	缺省值
广播流量风暴抑制状态	禁用
未知单播流量的风暴抑制状态	禁用
未知组播流量的风暴抑制状态	禁用
接口的风暴抑制动作	无
接口的恢复周期	30s
接口风暴抑制 Trap 功能	禁用
广播流量风暴控制状态	禁用
未知单播流量的风暴控制状态	禁用
未知组播流量的风暴控制状态	禁用

1.6.4 配置风暴抑制功能

注意

风暴抑制和基于 VLAN 的流量限速功能会相互影响，不建议用户在同一接口上同时开启这两个功能。

风暴抑制与风暴控制无法在同一接口上配置

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口节点。
3	JX(config-ge-1/0/1)#**storm-suppression** { **unknown-unicast** | **unknown-multicast** | **broadcast** } **min-rate** { **kbps** | **mbps** | **gbps** } *rate-value* **max-rate** { **kbps** | **mbps** | **gbps** } *rate-value*	使能接口下的风暴抑制功能，使用 BPS 配置风暴抑制的限速阈值。
	JX(config-ge-1/0/*)#**storm-suppression** { **unknown-unicast** | **unknown-multicast** | **broadcast** } **min-rate** *rate-value* **max-rate** *rate-value*	使能接口下的风暴抑制功能，使用 PPS 配置风暴抑制的限速阈值。
	JX(config-port-channel*)#**storm-suppression** { **unknown-unicast** | **unknown-multicast** | **broadcast** } **min-rate percent** *rate-value* **max-rate percent** *rate-value*	使能接口下的风暴抑制功能，使用比例配置风暴抑制的限速阈值。
4	JX(config-ge-1/0/1)#**storm-suppression action** { **block** | **error-down** | **none** }	配置接口的风暴抑制动作。
5	JX(config-ge-1/0/1)#**storm-suppression interval** *interval*	配置风暴抑制关闭接口后接口的恢复周期。
6	JX(config-ge-1/0/1)#**storm-suppression snmp-trap enable**	使能接口风暴抑制 Trap 功能。
7	JX(config-ge-1/0/1)#**exit**	返回全局配置模式。

1.6.5 检查风暴抑制配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#show storm-suppression interface [*interface-type interface-number*]	查看风暴抑制接口配置信息。
2	JX#show storm-suppression information	查看风暴抑制全局配置信息。

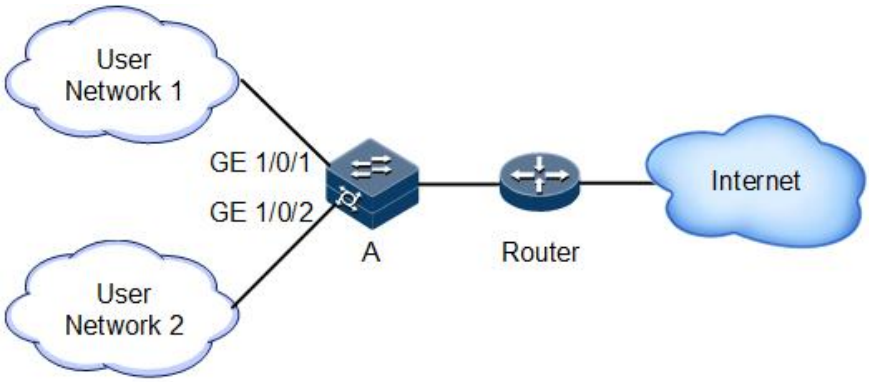
1.6.6 配置风暴抑制应用示例

组网需求

如下图所示，当 Switch A 的 GE 1/0/1 和 GE 1/0/2 接口接收到大量的未知单播或广播报文，Switch A 就会向 VLAN 内除了接收接口之外的所有接口转发这些报文，就可能会导致广播风暴，降低 Switch A 的转发性能。

为限制广播风暴对 Switch A 的影响，需要在 Switch A 的 GE 1/0/1 和 GE 1/0/2 接口上部署风暴抑制功能，分别限制来自用户网络 1 和用户网络 2 的广播报文，抑制阈值为 640kbit/s，若超限，则执行 shutdown 操作，低于 320kbit/s 才打开端口。

图 1-8 风暴抑制应用组网示意图



配置步骤

步骤 1 配置风暴抑制阈值。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#storm-suppression broadcast min-rate kbps 320 max-rate
kbps 640
JX(config-ge-1/0/1)#storm-suppression action error-down
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#storm-suppression broadcast min-rate kbps 320 max-rate
kbps 640
JX(config-ge-1/0/2)#storm-suppression action error-down
```

检查结果

通过 **show storm-control** 查看风暴抑制配置是否正确。

```
JX# show storm-suppression interface
NOTE :
  UNMC: unknown multicast ; BC: broadcast ; UNC: unknown unicast
 Interface      Type    State   RateMode  Min/MaxRate          Action/Status
Interval
------------------------------------------------------------------------
----------------------
 ge-1/0/1       UNC     disable bps       n/a                  none/normal
5
                UNMC    disable bps       n/a                  none/normal
5
                BC      enable  bps       320/640 (kbit/s)      none/errordown
5
 ge-1//2        UNC     disable bps       n/a                  none/normal
5
                UNMC    disable bps       n/a                  none/normal
5
                BC      enable  bps       320/640 (kbit/s)      none/errordown
5
------------------------------------------------------------------------
----------------------
```

1.6.7 配置风暴控制功能

注意

风暴控制和基于 VLAN 的流量限速功能会相互影响，不建议用户在同一接口上同时开启这两个功能。

风暴抑制与风暴控制无法在同一接口上配置

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口节点。
3	JX(config-ge-1/0/*)#**storm-control** { **unknown-unicast** | **unknown-multicast** | **broadcast** | **unicast** | **multicast** } **cir** { **kbps** | **mbps** | **gbps** } *cir-value* **cbs** { **bytes** | **kbytes** | **mbytes** } *cbs-value*	使能接口下的风暴控制功能，使用 BPS 配置风暴控制的限速阈值。
	JX(config-ge-1/0/*)#**storm-control** { **unknown-unicast** | **unknown-multicast** | **broadcast** | **unicast** | **multicast** } **pps** *pps-value*	使能接口下的风暴控制功能，使用 PPS 配置风暴控制的限速阈值。

步骤	配置	说明
	JX(config-port-channel*)#**storm-control { unknown-unicast | unknown-multicast | broadcast | unicast | multicast } percent** *<1-100>*	使能接口下的风暴控制功能，使用比例配置风暴控制的限速阈值。
4	JX(config-ge-1/0/*)#**exit**	返回全局配置模式。

1.6.8 检查风暴控制配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show storm-control interface** [*interface-type interface-number*]	查看风暴控制接口配置信息。

1.6.9 配置风暴控制应用示例

组网需求

如图 8-7 所示，当 Switch A 的 GE 1/0/1 和 GE 1/0/2 接口接收到大量的未知单播或广播报文，Switch A 就会向 VLAN 内除了接收接口之外的所有接口转发这些报文，就可能会导致广播风暴，降低 Switch A 的转发性能。

为限制广播风暴对 Switch A 的影响，需要在 Switch A 的 GE 1/0/1 和 GE 1/0/2 接口上部署风暴控制功能，分别限制来自用户网络 1 和用户网络 2 的广播报文，承诺信息速率为 640kbit/s，承诺突发长度为 6400kbytes，超过的报文全丢弃。

配置步骤

步骤 1 配置风暴抑制阈值。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#storm-control broadcast cir kbps 640 cbs kbytes 6400
JX(config-ge-1/0/1)#exit
JX(config)#interface ge 1/0/2
```

检查结果

通过 **show storm-control** 查看风暴控制配置是否正确。

```
JX# show storm-control interface
 NOTE :
  UNC: unknown unicast ; UNMC: unknown multicast ; NC: known unicast
  NMC: known multicast ; MC: all multicast ; UC: all unicast ; BC: broadcast
 Interface          Type       State      RateMode    RateValue
-------------------------------------------------------------------------
-------
 ge-1/0/1           UNC        disable     pps         n/a
                   UNMC       disable     pps         n/a
```

```
                    BC          enable      bps         cir: 640(kbit/s),cbs:
6555600(byte)
                    UC          disable     pps         n/a
                    MC          disable     pps         n/a
 ge-1/0/2             UNC          disable      pps          n/a
                    UNMC        disable     pps         n/a
                    BC          enable      bps         cir: 640(kbit/s),cbs:
6555600(byte)
                    UC          disable     pps         n/a
                    MC          disable     pps         n/a
```

1.7 ARP 防攻击

1.7.1 配置准备

场景

ARP 协议有简单、易用的优点，但是也因为其没有任何安全机制而容易被攻击发起者利用。

攻击者可以仿冒用户、仿冒网关发送伪造的 ARP 报文，使网关或主机的 ARP 表被篡改。如果网络中有主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备，则会造成下面的危害：

- 设备向目的网段发送大量 ARP 请求报文，加重目的网段的负载。
- 设备会试图反复地对目标 IP 地址进行解析，增加了 CPU 的负担。

为避免这种 IP 报文攻击所带来的危害，设备提供了下 ARP 防攻击功能。

前提

无

1.7.2 ARP 防攻击缺省配置

缺省没有配置任何 ARP 防攻击配置

1.7.3 配置 ARP 防攻击功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#config	进入全局配置模式。

步骤	配置	说明
2	JX(config)# **arp-antiattack src-ip enable**	针对 ARP 源 IP 地址的 ARP 冲突检测。通过 ARP 报文中的源 IP 地址，查找 ARP 表，如果找到了对应的 ARP 表项，并且 ARP 表项中对应的 MAC 地址和 ARP 报文中的源 MAC 地址不一致，则认为是 ARP 冲突。会丢弃该 ARP 报文，防止攻击者篡改 ARP 表中的 MAC 地址。
3	JX(config)# **arp-antiattack src-mac enable**	针对 ARP 源 MAC 地址的 ARP 冲突检测。通过 ARP 报文中的源 MAC 地址，查找 ARP 表，如果找到了对应的 ARP 表项，并且 ARP 表项中对应的 IP 地址和 ARP 报文中的源 IP 地址不一致，则认为是 ARP 冲突。会丢弃该 ARP 报文，防止攻击者篡改 ARP 表中的 IP 地址。
4	JX(config)# **arp-antiattack arp-cheat enable**	仿冒本设备的 ARP 欺骗检测。检测设备收到 ARP 报文里的源或者目的 IP 地址，以及源 MAC 地址和 ARP 报文类型，判断 ARP 报文是否是仿冒本设备的攻击包，如果判断为攻击包，则会丢弃该 ARP 报文，并发送一个本设备的免费 ARP。
5	JX(config)# **arp-antiattack gratuitous-arp enable**	免费 ARP 报文主动丢弃。使能免费 ARP 报文主动丢弃功能后，设备直接丢弃免费 ARP 报文，可以防止设备因处理大量免费 ARP 报文，导致 CPU 负荷过重而无法处理其他业务。
6	JX(config)# **arp-antiattack gateway-cheat enable**	ARP 防网关冲突。通过 ARP 防网关冲突功能，可以防止用户仿冒网关发送 ARP 报文，非法修改网络内其他用户的 ARP 表项。ARP 防网关冲突和动态 ARP 检测不能同时配置。
7	JX(config-vlan*)# **arp-antiattack check user-bind enable** **或** JX(config-ge-*/*/*)# **arp-antiattack check user-bind enable**	动态 ARP 检测，即 DAI(Dynamic ARP Inspection)。使能动态 ARP 检测 DAI(Dynamic ARP Inspection)功能后，当设备收到 ARP 报文时，将此 ARP 报文的源 IP、源 MAC、收到 ARP 报文的接口及 VLAN 信息和 DHCP Snooping 绑定表的信息进行比较，如果信息匹配，则认为是合法用户，允许此用户的 ARP 报文通过，否则认为是攻击，丢弃该 ARP 报文。本功能仅适用于 DHCP Snooping 场景。

步骤	配置	说明
8	JX(config-vlan*)# **arp-antiattack check user-bind check-item { interfce | ip-address | mac-address }** **或** JX(config-ge-*/*/*)# **arp-antiattack check user-bind check-item { vlan | ip-address | mac-address }**	动态 ARP 检测的检测项，三个检查项可自由组合。默认是三个检查项都检查。

1.7.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show arp-antiattack config**	查看 ARP 防攻击配置信息。

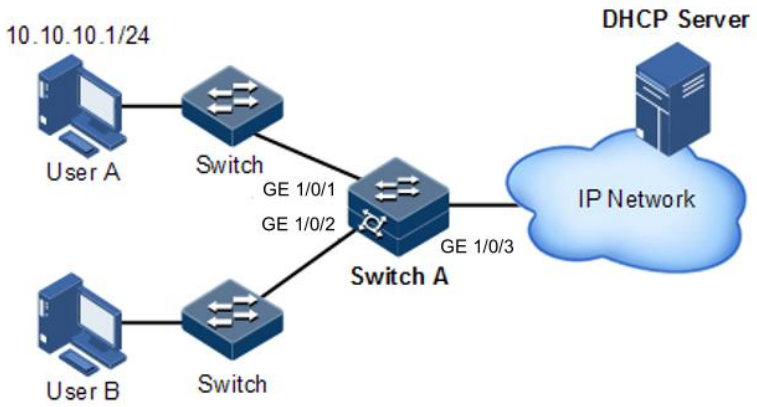
1.7.5 配置 ARP 防攻击示例

组网需求

为了防止 ARP 攻击，如下图所示，需要在 Switch A 设备上配置 ARP 防攻击功能。要求如下：

- 免费 ARP 报文不允许通过，使能针对 ARP 源 IP 地址和源 mac 地址的 ARP 冲突检测，以及仿冒本设备的 ARP 欺骗检测功能。
- Switch A 作为 User A 的网关，使能 ARP 防网关冲突。
- 清除 Switch A 上的 ARP 防网关冲突配置，Switch A 提供 User B 到 DHCP Server 的二层可达性，在 GE 1/0/2 上配置动态 ARP 检测功能。

图 1-9 动态 ARP 检测应用组网示意图



配置步骤

步骤 1 配置针对 ARP 源 IP 地址的 ARP 冲突检测。

```
JX#config
JX(config)#arp-antiattack src-ip enable
```

步骤 2 配置针对 ARP 源 MAC 地址的 ARP 冲突检测。

```
JX(config)# arp-antiattack src-mac enable
```

步骤 3 使能仿冒本设备的 ARP 欺骗功能。

```
JX(config)#arp-antiattack arp-cheat enable
```

步骤 4 使能免费 ARP 报文主动丢弃。

```
JX(config)#arp-antiattack gratuitous-arp enable
```

步骤 5 使能 ARP 防网关冲突。

```
JX(config)#arp-antiattack gateway-cheat enable
```

步骤 6 使能动态 ARP 检测，要先去使能 ARP 防网关冲突。

```
JX(config)#arp-antiattack gateway-cheat disable
JX(config)#interface ge 1/0/2
JX(config-ge-1/0/2)#arp-antiattack check user-bind enable
JX(config-ge-1/0/2)#exit
JX(config)#
```

检查结果

通过 **show arp-antiattack config** 命令查看设备上 ARP 防攻击的配置。

```
JX#show arp-antiattack config

Version: ANTIARP_VL2.10.00.00
!
```

```
arp-antiattack src-ip enable
arp-antiattack src-mac enable
arp-antiattack arp-cheat enable
arp-antiattack gratuitous-arp enable
arp-antiattack gateway-cheat enable

JX#show arp-antiattack config
Version: ANTIARP_VL2.10.00.00
!
arp-antiattack src-ip enable
arp-antiattack src-mac enable
arp-antiattack arp-cheat enable
arp-antiattack gratuitous-arp enable
!
interface ge 1/0/2
 arp-antiattack check user-bind enable
```

1.8 ND Snooping

1.8.1 简介

ND（Neighbor Discovery，邻居发现）是确定邻居节点之间关系的一组消息和进程。邻居发现协议替代了 IPv4 的 ARP（Address Resolution Protocol）、ICMP 路由器发现（Router Discovery）和 ICMP 重定向（Redirect）消息，并提供了地址冲突检测、邻居地址解析、确定邻居可达性以及进行主机地址配置等功能。

ND Snooping 功能主要应用于接入设备上，检查用户的合法性。对于合法用户的 ND 报文进行正常转发，否则直接丢弃，从而防止仿冒用户、仿冒网关的攻击。

用户合法性检查是根据 ND 报文中源 IPv6 地址和源 MAC 地址，检查用户是否是报文收到端口所属 VLAN 上的合法用户。

ND Snooping 功能将接入设备上的端口分为两种：ND 信任端口、ND 非信任端口。

- 对于 ND 信任端口：不进行用户合法性检查。从 ND 信任端口接收到的 ND 报文，设备可以进行正常转发。
- 对于 ND 非信任端口：从 ND 非信任端口接收到的 RA 报文，设备会认为是非法报文直接丢弃；从 ND 非信任端口接收到的 NA/RS/NS 报文，则会通过 ND 报文合法性检查功能进行绑定表匹配检查，当不符合绑定表关系时，设备会认为是非法报文直接丢弃；从 ND 非信任端口接收到的其他类型报文，设备进行正常转发。

1.8.2 配置准备

场景

ND Snooping 用来防止网络中常见的 ND 欺骗攻击，实现了对不安全来源的 ND 报文进行隔离。是否对 ND 报文信任通过配置接口的信任状态实现，而是否符合要求则通过配置绑定表实现。

前提

无

1.8.3 ND Snooping 的缺省配置

设备上 ND Snooping 的缺省配置如下。

功能	缺省值
ND Snooping 接口信任状态	不信任
全局 ND Snooping 功能	未启动
端口 ND Snooping 功能	未使能
NS、NA、RS 报文检查功能	未使能

1.8.4 配置 ND Snooping

请在需要的设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**nd-snooping start**	开启全局 ND Snooping 功能。
3	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口或 VLAN 接口配置模式。
4	JX(config-ge-1/0/*)#**nd-snooping enable**	配置连接网关的接口开启 ND Snooping 功能。
5	JX(config-ge-1/0/*)#**nd-snooping trust**	配置连接网关的接口为信任接口。
6	JX(config)#**nd-snooping check** { **na** | **ns** | **rs** } **enable**	开启 ND Snooping 对 ns、na、rs 报文的合法性检查。

1.8.5 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

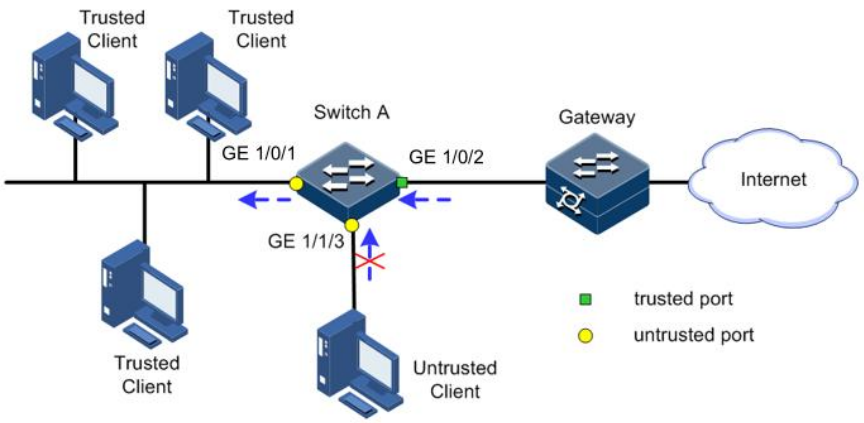
序号	检查项	说明
1	JX#**show nd-snooping config**	查看 ND Snooping 功能配置信息。
2	JX#**show nd-snooping user-bind**	查看 ND Snooping 用户绑定表。
3	JX#**show nd-snooping prefix**	查看 ND Snooping 前缀表。

1.8.6 配置 ND Snooping 示例

组网需求

如下图所示，某局域网络用户主机通过 Switch A 连接网关设备，由于网络中未部署 DHCPv6 服务器，这些主机需要根据网关分配给用户网络前缀信息，通过无状态地址自动配置方式获取 IPv6 地址。为防止非法用户发送 NA/NS/RS/RA 报文，导致合法主机无法获取 IPv6 地址，需要在 Switch 上开启 ND Snooping 功能，对非法的报文进行拦截。

图 1-10 配置 ND Snooping 组网示意图



配置步骤

步骤 1 在 Switch 上创建 VLAN 10 并激活。

配置 Switch。

```
JX#config
JX(config)#hostname SwitchA
SwitchA(config)#vlan 10
```

步骤 2 将 Switch A 的接口 GE 1/0/2 以 Access 模式加入 VLAN 10，设置接口 GE 1/0/1 为 Trunk 模式并允许 VLAN 10 通过。

```
SwitchA(config)#interface ge 1/0/2
SwitchA(config-ge-1/0/2)#port link-type access
SwitchA(config-ge-1/0/2)#port default vlan 10
SwitchA(config-ge-1/0/2)#exit
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#port link-type trunk
SwitchA(config-ge-1/0/1)#port trunk allow-pass vlan 10
SwitchB(config-ge-1/0/1)#exit
```

步骤 3 全局和 VLAN 10 分别使能 ND Snooping 功能，配置 GE 1/0/1 为信任接口。

```
SwitchA(config)#nd-snooping start
```

```
SwitchA(config)#vlan 10
SwitchA(config-vlan-10)#nd-snooping enable
SwitchA(config-vlan-10)#exit
SwitchA(config)#interface ge 1/0/1
SwitchA(config-ge-1/0/1)#nd-snooping enable
SwitchA(config-ge-1/0/1)#nd-snooping trust
SwitchA(config-ge-1/0/1)#exit
```

步骤 4 使能 ND 协议报文合法性检查功能。

```
SwitchA(config)#nd-snooping check na enable
SwitchA(config)#nd-snooping check ns enable
SwitchA(config)#nd-snooping check rs enable
```

检查结果

通过 **show nd-snooping config** 命令查看配置是否正确。

```
JX#show nd-snooping config
!
nd-snooping start
nd-snooping check na enable
nd-snooping check ns enable
nd-snooping check rs enable
!
vlan 10
 nd-snooping enable
!
interface ge 1/0/1
nd-snooping enable
nd-snooping trust
```

1.9 DHCP Snooping

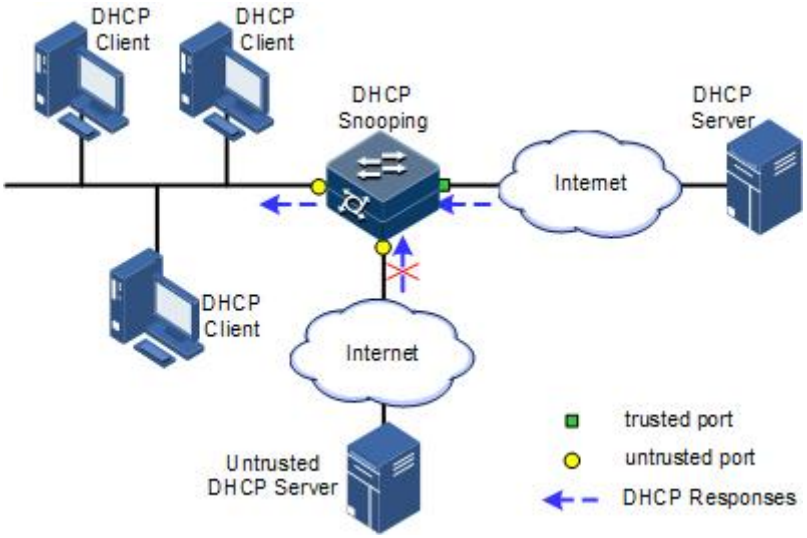
1.9.1 简介

DHCP Snooping 是 DHCP 的一种安全特性，具有如下功能：

- 保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址；

网络中如果存在私自架设的伪 DHCP 服务器，则可能导致 DHCP 客户端获取错误的 IP 地址和网络配置参数，无法正常通信。如图 8-11 所示，为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将接口设置为信任接口和不信任接口：信任接口正常转发接收到的 DHCP 报文；不信任接口接收到来自 DHCP 服务器的回应报文后将其丢弃。

图 1-11 DHCP Snooping 组网示意图



- 记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系。

DHCP Snooping 通过监听请求和信任接口收到的回应报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、获取到的 IP 地址、与 DHCP 客户端连接的接口及该接口所属的 VLAN 等信息。利用这些信息可以实现：

- ARP Detection：根据 DHCP Snooping 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。
- IP Source Guard：通过动态获取 DHCP Snooping 表项对接口转发的报文进行过滤，防止非法报文通过该接口。
- VLAN 映射：发送给用户的报文通过查找映射 VLAN 对应的 DHCP Snooping 表项中的 DHCP 客户端 IP 地址、MAC 地址和原始 VLAN 的信息，将报文的映射 VLAN 修改为原始 VLAN。

DHCP 报文中的 Option 字段记录了 DHCP 客户端的位置信息。管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。

如果设备配置了 DHCP Snooping 支持 Option 功能：

- 当设备接收到 DHCP 请求报文时，将根据报文中是否包含 Option 字段以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给 DHCP 服务器；
- 当设备接收到 DHCP 回应报文时，如果报文中含有 Option 字段，则删除该字段，并转发给 DHCP 客户端；如果报文中不含有 Option 字段，则直接转发。

1.9.2 配置准备

场景

DHCP Snooping 作为 DHCP 的一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，并记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系。

DHCP 报文中的 Option 字段记录了 DHCP 客户端的位置信息。管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。配置了 DHCP Snooping 支持 Option 功能的交换机设备可以根据报文中是否包含 Option 字段，对其进行相应的处理。

前提

无

1.9.3 DHCP Snooping 的缺省配置

设备上 DHCP Snooping 的缺省配置如下。

功能	缺省值
全局 DHCP Snooping 状态	禁止
接口 DHCP Snooping 状态	去使能
接口信任状态	不信任
DHCP Snooping 支持 Option 82	禁止

1.9.4 配置 DHCP Snooping

通常情况下，需要确保设备连接 DHCP 服务器侧的接口为信任状态，连接用户侧的接口为不信任状态。

对于启动了 DHCP Snooping 的设备，如果没有配置 DHCP Snooping 支持 Option 功能，则设备将不会对报文的 Option 字段进行任何处理。对于没有携带 Option 字段的报文，设备也不会进行插入处理。

缺省情况下设备所有接口的 DHCP Snooping 功能均已使能，但只有在使能全局 DHCP Snooping 功能后，接口的 DHCP Snooping 功能才会生效。

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#dhcp-snooping start`	使能全局 DHCP Snooping 功能。
3	`JX(config)#interface` *interface-type interface-number*	进入物理接口配置模式。
4	`JX(config-ge-1/0/*)#dhcp-snooping enable`	使能接口的 DHCP Snooping 功能，支持 QinQ 接口。
5	`JX(config-ge-1/0/*)#dhcp-snooping trust`	配置 DHCP Snooping 信任接口。
6	`JX(config-ge-1/0/*)#dhcp-snooping max-user-number { number | default }`	配置 DHCP Snooping 绑定表容量。

步骤	配置	说明
7	JX(config-ge-1/0/*)#**dhcp-snooping server-filter enable**	配置 DHCP Snooping 信任 server 配置功能
8	JX(config-ge-1/0/*)#**dhcp-snooping check user-bind enable**	配置 DHCP 报文进行绑定表匹配检测功能
9	JX(config-ge-1/0/*)#**dhcp-snooping check mac-address enable**	配置 DHCP 用户上送的请求报文头中的 MAC 地址是否合法功能
10	JX(config-ge-1/0/*)#**dhcp-snooping option82 enable**	配置 DHCP Snooping 支持 Option82 功能。
11	JX(config)#**exit**	返回全局配置模式。

1.9.5 配置 DHCP Snooping 支持 Option 82 功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dhcp-snooping start**	使能全局 DHCP Snooping 功能。
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
4	JX(config-ge-1/0/*)#**dhcp-snooping enable**	使能接口的 DHCP Snooping 功能。
5	JX(config-ge-1/0/*)#**dhcp-snooping option82 enable**	配置全局开启 DHCP Snooping 支持 Option 82 功能。
6	JX(config-ge-1/0/*)#**dhcp-snooping option82 circuit-id format { default | user-defined** format-string }	配置 DHCP Snooping Option82 的 circuitID 字段内容。
7	JX(config-ge-1/0/*)#**dhcp-snooping option82 remote-id format { default | user-defined** format-string }	配置 DHCP Snooping Option82 的 remoteID 字段内容。
8	JX(config-ge-1/0/*)#**dhcp-snooping option82 { drop | keep | append }**	配置 DHCP Snooping 对含 Option 82 的 DHCP 请求报文处理策略。
9	JX(config-ge-1/0/*)#**exit**	返回全局配置模式。

1.9.6 配置 DHCPv6 Snooping

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。

步骤	配置	说明
2	JX(config)#**dhcp-snooping start**	使能全局 DHCP Snooping 功能。
3	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
4	JX(config-ge-1/0/*)#**dhcpv6-snooping enable**	使能接口的 DHCPv6 Snooping 功能。
5	JX(config-ge-1/0/*)#**dhcpv6-snooping trust**	配置 DHCPv6 Snooping 信任接口。
6	JX(config-ge-1/0/*)#**dhcpv6-snooping max-user-number** { *number* | **default** }	配置 DHCPv6 Snooping 绑定表容量。
7	JX(config-ge-1/0/*)#**dhcpv6-snooping option18 enable**	使能 DHCPv6 Snooping 支持 Option18 功能。
8	JX(config-ge-1/0/*)#**dhcpv6-snooping option18 format** { **default** | **user-defined** format-string }	配置 DHCPv6 Snooping Option18 的内容。
9	JX(config-ge-1/0/*)#**dhcpv6-snooping option37 enable**	使能 DHCPv6 Snooping 支持 Option37 功能。
10	JX(config-ge-1/0/*)#**dhcpv6-snooping option37 format** { **default** | **user-defined** format-string }	配置 DHCPv6 Snooping Option37 的内容。

1.9.7 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show dhcp-snooping config**	查看 DHCP Snooping 功能配置信息。
2	JX#**show dhcp-snooping user-bind**	查看 DHCP Snooping 绑定表信息。
3	JX#**show dhcp-snooping statistics**	查看 DHCP Snooping 的报文统计信息。
4	JX#**show dhcp-snooping interface**	查看 DHCP Snooping 的接口配置信息。
5	JX#**show dhcp-snooping vlan**	查看 DHCP Snooping 的 vlan 配置信息。
6	JX#**show dhcpv6-snooping config**	查看基于 ipv6 的 DHCP Snooping 功能配置信息。
7	JX#**show dhcpv6-snooping user-bind**	查看基于 ipv6 的 DHCP Snooping 绑定表信息。
8	JX#**show dhcpv6-snooping statistics**	查看基于 ipv6 的 DHCP Snooping 的报文统计信息。
9	JX#**show dhcpv6-snooping interface**	查看基于 ipv6 的 DHCP Snooping 的接口配置信息。

序号	检查项	说明
10	JX#show dhcpv6-snooping vlan	查看基于 ipv6 的 DHCP Snooping 的 vlan 配置信息。

1.9.8 维护

用户可以通过以下命令，维护设备 DHCP Snooping 特性的运行情况和配置情况。

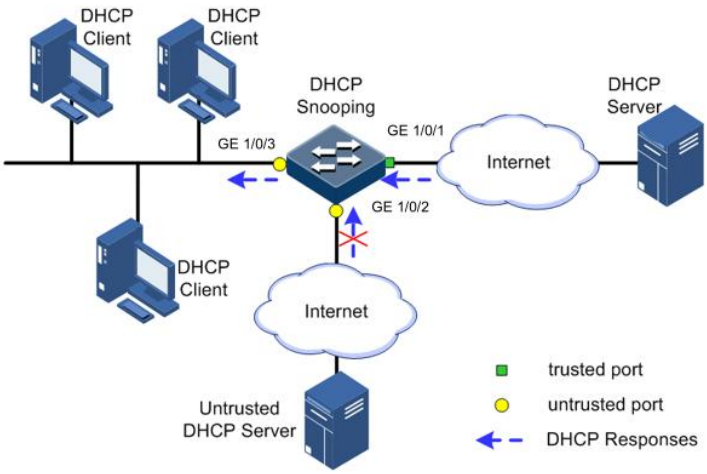
命令	描述
Rasiecom(config)#reset dhcp-snooping user-bind	清除 dhcpsnoop ipv4 协议下的用户绑定表信息
Rasiecom(config)#reset dhcpv6-snooping user-bind	清除 dhcpsnoop ipv6 协议下的用户绑定表信息
Rasiecom(config)#reset dhcp-snooping statistics	清除 dhcpsnoop ipv4 协议下的用户接口配置统计信息
Rasiecom(config)#reset dhcpv6-snooping statistics	清除 dhcpsnoop ipv6 协议下的用户接口配置统计信息

1.9.9 配置 DHCP Snooping 示例

组网需求

如图 8-12 所示，Switch 作为 DHCP Snooping 设备，需要保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址，此外为了便于对客户端的管理，还需要设备支持 Option82 功能，在接口 GE 1/01/3 上配置电路 ID 子选项信息填充内容为 JX，远程 ID 子选项信息填充内容为 user01。

图 1-12 配置 DHCP Snooping 组网示意图



配置步骤

步骤 1 配置全局 DHCP Snooping 功能。

```
JX#config
JX(config)#dhcp-snooping start
```

步骤 2 配置信任接口。

```
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#dhcp-snooping enable
JX(config-ge-1/0/1)#dhcp-snooping trust
JX(config-ge-1/0/1)#exit
```

步骤 3 配置 DHCP Snooping 支持 Option82 功能并配置 Option82 字段。

```
JX(config)#interface ge 1/0/3
JX(config-ge-1/0/3)#dhcp-snooping enable
JX(config-ge-1/0/3)#dhcp-snooping option82 enable
JX(config-ge-1/0/3)#dhcp-snooping option82 remote-id format user-defined
'user01'
JX(config-ge-1/0/3)#dhcp-snooping option82 circuit-id format user-defined
'JX'
JX(config-ge-1/0/3)#exit
```

检查结果

通过 **show dhcp-snooping config** 命令查看 DHCP 服务器配置是否正确。

```
JX#show dhcp-snooping config
 Version : DHCPSNOOP_V7.00.03.00
!
dhcp-snooping start
!
interface ge 1/0/1
 dhcp-snooping enable
```

```
 dhcp-snooping trust
!
interface ge 1/0/3
 dhcp-snooping enable
 dhcp-snooping option82 enable
 dhcp-snooping option82 remote-id format user-defined 'user01'
 dhcp-snooping option82 circuit-id format user-defined 'JX'
……
```

1.10 IP Source Guard

1.10.1 简介

IP Source Guard 功能用于对接口收到的报文进行过滤控制，通常配置在接入用户侧的接口上，以防止非法用户报文通过，从而限制了对网络资源的非法使用（比如非法主机仿冒合法用户 IP 接入网络），提高了接口的安全性。

IP Source Guard 绑定表项

IP Source Guard 用于匹配报文的特征项包括源 IP 地址、源 MAC 地址和 VLAN 标签，并且可支持接口与以下特征项的组合（以下简称绑定表项）：

- 接口＋IP
- 接口＋IP＋MAC
- 接口＋IP＋VLAN
- 接口＋IP＋MAC＋VLAN

按照绑定表项的产生方式，IP Source Guard 分为以下两种：

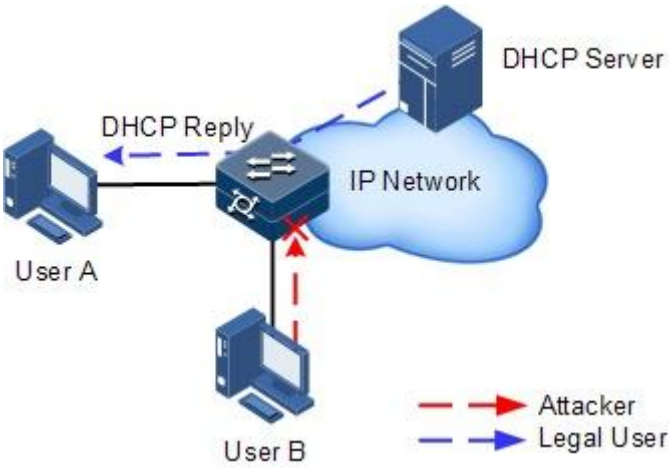
- 静态绑定：通过手工配置绑定信息，产生绑定表项来完成接口的控制功能，适用于主机数较少或者需要对某台主机进行单独绑定的情况。
- 动态绑定：通过 DHCP Snooping 自动获取绑定信息来完成接口的控制功能，适用于主机数较多并且采用 DHCP 进行动态主机配置的情况，可有效防止 IP 地址冲突和盗用等问题。

IP Source Guard 原理

IP Source Guard 的基本原理是在设备内部构建一个 IP 源绑定表，作为每个接口对接收数据包的检验依据。IP Source Guard 原理如下图所示，其转发原则如下：

- 所接收到的 IP 报文满足 IP 源绑定表中 Port/IP/MAC/VLAN 绑定表项的对应关系，则转发；
- 所接收到的 IP 报文为 DHCP 数据包，则转发；
- 所接收到的 IP 报文为其他情况，则丢弃。

图 1-13 IP Source Guard 功能示意图



当设备在转发 IP 报文时，将此 IP 报文中的源 IP、源 MAC、接口、VLAN 信息和绑定表的信息进行比较，如果信息匹配，说明是合法用户，则允许此报文正常转发；否则认为是攻击者，丢弃该用户发送的 IP 报文。

1.10.2 配置准备

场景

网络中常常存在针对 IP 源进行欺骗的攻击行为，如攻击者仿冒合法用户发送 IP 报文给服务器，或者伪造其他用户的源 IP 地址进行通信，从而导致合法用户不能正常获得网络服务。

通过 IP Source Guard 绑定功能，可以对接口转发的报文进行过滤控制，防止非法报文通过接口，从而限制了对网络资源的非法使用，如非法主机仿冒合法用户 IP 接入网络等，提高了接口的安全性。

前提

配置 IP Source Guard 之前，需要完成以下任务：

- 如果存在 DHCP 用户，则需要使能 DHCP Snooping 功能。

1.10.3 IP Source Guard 功能的缺省配置

设备上 IP Source Guard 功能的缺省配置如下。

功能	缺省值
接口 IP Source Guard 状态	禁止

1.10.4 配置 IP Source Guard 绑定功能

配置静态绑定功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**user-bind static ip** *ip-address/any* **mac** *mac-address/any* [**interface** *interface-type interface-number*] **vlan** *vlan-id/any*	配置静态绑定关系。
	JX(config)#**user-bind static ip6** *ipv6-address/any* **mac** *mac-address/any* [**interface** *interface-type interface-number***vlan** *vlan-id/any*	配置 IPv6 静态绑定关系。

1.10.5 配置 IP Source Guard 接口信任状态

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**interface** *interface-type interface-number*	进入物理接口配置模式。
3	JX(config-ge-1/0/*)#**ip source check user-bind enable**	使能接口 IP Source Guard 功能。

1.10.6 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show ip source check config**	查看 IP Source Guard 功能配置信息。
2	JX#**show ip source check interface**	查看已使能 IP Source Guard 的接口信息

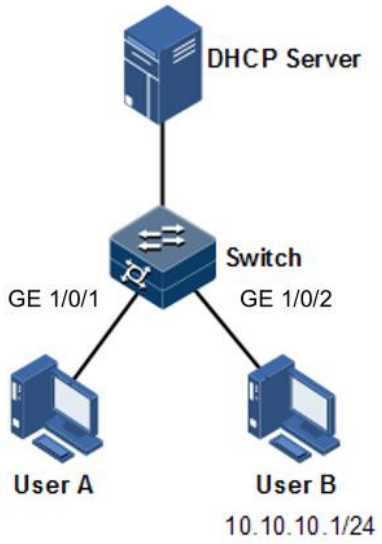
1.10.7 配置 IP Source Guard 示例

组网需求

如下图所示，为了防止 IP 地址盗用，需要在交换机上配置 IP Source Guard 功能，要求如下：

- 交换机允许接口 GE 1/0/1 上的所有 IP 报文通过；
- 接口 GE 1/0/2 允许指定 IP 地址为 10.10.10.1，子网掩码为 255.255.255.0 的 IP 报文以及符合 DHCP Snooping 学习到的动态绑定关系的报文通过；
- 其它接口仅允许通过 DHCP Snooping 学习的动态绑定关系的报文通过。

图 1-14 IP Source Guard 应用组网示意图



配置步骤

步骤 1 配置 IP Source Guard 功能。

```
JX#config
JX(config)#int ge 1/0/2
JX(config-ge-1/0/2)#ip source check user-bind enable
JX(config-ge-1/0/2)#exit
JX(config)#int ge 1/0/1
JX(config-ge-1/0/1)#ip source check user-bind enable
JX(config-ge-1/0/1)#exit
```

步骤 2 配置静态绑定表项。

```
JX(config)# user-bind static ip 10.10.10.1 mac any interface ge 1/0/2 vlan any
```

步骤 3 接口 GE 1/0/2 和其他接口配置 DHCP snooping 功能。

检查结果

通过 **show ip source check config** 命令查看 IP Source Guard 配置结果。

```
JX#show ip source check config
!
user-bind static ip 10.10.10.1 mac any interface ge 1/0/2 vlan any
!
interface ge 1/0/2
ip source check user-bind enable
!
interface ge 1/0/1
ip source check user-bind enable
```

通过 **show ip source check interface** 命令查看已使能 IP Source Guard 的接口信息。

```
JX#show ip source check interface
Interface         Check-Item        Alarm    Limit      DropPkts
-------------------------------------------------------------------
ge-1/0/2          ip,mac,vlan       disable  100        0
ge-1/0/1          ip,mac,vlan       disable  100        0
-------------------------------------------------------------------
```

1.11 CPU 防攻击

1.11.1 配置准备

场景

当设备短时间内接收到大量的攻击报文，导致 CPU 满负荷运转，利用率达到 100%，会导致设备的正常功能无法运行。使用 CPU 防攻击功能可以有效限制进入 CPU 的报文的速率。

前提

无

1.11.2 配置 CPU 防攻击限速功能

注意

CPU 防攻击的配置对各协议模块的功能有重要的影响，建议不要轻易修改 CPU 保护的参数配置，只有专家才能修改相关配置。

请在设备上进行以下配置。

步骤	配置	说明
1	JX#config	进入全局配置模式。

步骤	配置	说明
2	JX(config)# **cpu-defend policy test**	配置 CPU 防攻击的策略，设备在启动的时候，会下发并绑定一个默认策略，默认策略不能修改，但是设备可以更改绑定的策略。
3	JX(config-cpudefend-policy-test)# **car packet-type { arp | bfd | dhcpreply | dhcprequest | igmp | lacp | lldp | mld | stp-customer | telnet | ... } pps** *pps-value*	配置该策略的指定协议包类型的限速值。设备支持哪些协议包类型，取决于设备支持哪些协议。
4	JX(config-cpudefend-policy-test)# **packet-type { arp | bfd | dhcpreply | dhcprequest | igmp | lacp | lldp | mld | stp-customer | telnet | priority }** *priority-value*	配置该策略的指定协议包类型的优先级。设备支持哪些协议包类型，取决于设备支持哪些协议。
5	JX(config-cpudefend-policy-test)# **deny packet-type { arp | bfd | dhcpreply | dhcprequest | igmp | lacp | lldp | mld | stp-customer | telnet | ... }**	配置该策略的指定协议包类型的丢弃。设备支持哪些协议包类型，取决于设备支持哪些协议。
6	JX(config-cpudefend-policy-test)# **session-car packet-type { bgp | ftp | http | isis | ospf | ospfv3 | ssh | telnet | tftp | ... } pps** *pps-value*	配置该策略的指定协议包类型的动态链路保护功能的协议会话的限速值。
7	JX(config-cpudefend-policy-test)# **filter** *<1-8>* **{ acl-ipv4** *acl-listid* **| acl-ipv6** *acl-listid* **}**	配置该策略的过滤器。
8	JX(config)# **cpu-defend bind-policy test**	配置 CPU 防攻击的绑定策略。绑定后的策略不能修改，只能先解绑定后再修改。在基于 CPU 利用率动态调节模式下，该命令不可配置。
9	JX(config)# **cpu-defend mode { cpuratio-control | fixed }**	配置 CPU 防攻击的绑定策略的模式。分为基于 CPU 利用率动态调节和固定模式。默认是固定模式。
10	JX(config)# **cpu-defend { level1-policy** *policy-name* **| level2-policy** *policy-name* **| level3-policy** *policy-name* **}**	配置用于基于 CPU 利用率动态调节绑定策略模式下的各 level 的策略。
11	JX(config)# **cpu-defend { level1-cpuratio** *<1-100>* **| level2-cpuratio** *<1-100>* **}**	配置用于基于 CPU 利用率动态调节绑定策略模式下的 level-1 或者 level-2 的最大 CPU 利用率。

1.11.3 配置 CPU 防攻击的攻击溯源功能

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)# **cpu-defend policy test**	配置 CPU 防攻击的策略，设备在启动的时候，会下发并绑定一个默认策略，默认策略不能修改，但是设备可以更改绑定的策略。
3	JX(config-cpudefend-policy-test)# **auto-defend enable**	配置该策略的攻击溯源功能使能，缺省情况下，该功能是使能的。
4	JX(config-cpudefend-policy-test)# **auto-defend threshold** *threshold-value*	配置该策略的攻击溯源门限值。缺省值为 128pps。
5	JX(config-cpudefend-policy-test)# **auto-defend attack-packet sample** *sample-value*	配置该策略的攻击溯源采样比。缺省值为 8。
6	JX(config-cpudefend-policy-test)# **auto-defend alarm enable**	配置该策略的攻击溯源的告警功能使能。缺省为未使能。
7	JX(config-cpudefend-policy-test)# **auto-defend alarm threshold** *threshold-value*	配置该策略的攻击溯源的告警阈值。缺省值为每秒触发攻击溯源 128 次。
8	JX(config-cpudefend-policy-test)# **auto-defend action { deny | error-down }**	配置该策略的攻击溯源的惩罚动作。缺省为没有惩罚动作。
9	JX(config)# **cpu-defend bind-policy test**	配置 CPU 防攻击的应用。绑定后的策略不能修改，只能先解绑定后再修改。

1.11.4 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

序号	检查项	说明
1	JX#**show cpu-defend config**	查看 CPU 防攻击配置信息。
	JX#**show cpu-defend statistics**	查看 CPU 防攻击统计信息。
3	JX#**show auto-defend attack-source**	查看 CPU 防攻击攻击溯源信息

1.11.5 维护

命令	说明
JX(config)#**reset cpu-defend statistics**	清除全局的 CPU 防攻击统计信息。

1.11.6 MAC 认证

1.11.7 简介

MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，无需安装客户端软件。设备在启动了 MAC 地址认证的端口上首次检测到用户的 MAC 地址以后，启动对该用户的认证操作。认证过程中，不需要用户手动输入用户名或密码。若该用户认证成功，则允许其通过端口访问网络资源，否则该用户的 MAC 地址就被设置为静默 MAC。在静默时间内，来自此 MAC 地址的用户报文到达时，设备直接做丢弃处理，以防止非法 MAC 短时间内的重复认证。

MAC 认证用户的账号格式：

- MAC 地址账号：设备使用源 MAC 地址作为用户认证时的用户名和密码，或者使用 MAC 地址作为用户名，并配置密码。
- 固定用户名账号：所有 MAC 地址认证用户均使用设备上指定的一个固定用户名和密码替代用户的 MAC 地址作为身份信息进行认证。

认证方式：

- RADIUS 服务器认证方式进行 MAC 地址认证：当选用 RADIUS 服务器认证方式进行 MAC 地址认证时，设备作为 RADIUS 客户端，与 RADIUS 服务器配合完成 MAC 地址认证操作。
- 本地认证方式进行 MAC 地址认证：当选用本地认证方式进行 MAC 地址认证时，直接在设备上完成对用户的认证。需要在设备上配置本地用户名和密码。

重认证：

- MAC 地址重认证是指设备周期性对端口上在线的 MAC 地址认证用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线。

1.11.8 缺省配置

设备上 MAC 认证的缺省配置如下：

功能	缺省值
全局 MAC 认证功能状态	禁止
接口 MAC 认证功能状态	禁止
全局认证方式	**pap**
802.1x 重认证功能状态	允许
802.1x 重认证定时器时间	1800s
MAC 认证静默定时器时间	60s
最大用户数	256

1.11.9 配置 MAC 认证

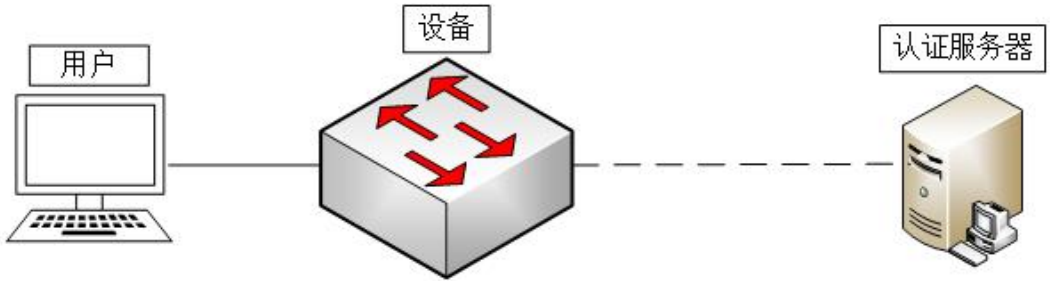
步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**mac-authen** { **start** | **stop** }	使能或去使能全局 MAC 认证功能。
3	JX(config)#**mac-authen aaa authentication method** *method-name*	绑定全局 MAC 认证时的 AAA 方法。
4	JX(config)#**mac-authen max-user** *user-number*	配置全局 MAC 认证最大用户数。
5	JX(config)#**interface** *interface-type interface-number*	进入二层物理接口配置模式。
6	JX(config-ge-1/0/*)#**mac-authen enable**	使能接口 MAC 认证功能。
7	JX(config-ge-1/0/*)#**mac-authen max-user** *user-number*	配置端口允许 MAC 认证的最大用户数。
8	JX(config-ge-1/0/*)#**authentication guest-vlan** *vlan-id*	配置指定端口的 Guest VLAN，对 802.1x 协议和 mac 认证都生效。
9	JX(config-ge-1/0/*)#**mac-authen critical-vlan** *vlan-id*	配置指定端口的 MAC 认证 Critical VLAN。
10	JX(config-ge-1/0/*)#**mac-authen restrict-vlan** *vlan-id*	配置指定端口的 MAC 认证 Restrict VLAN。
11	JX(config-ge-1/0/*)#**mac-authen reauthenticate all user**	手动触发指定端口下 802.1x 用户进行重认证。
12	JX(config-ge-1/0/*)#**mac-authen delete all user**	强制将端口下 MAC 认证用户下线。
13	JX(config-ge-1/0/*)#**mac-authen quiet** { **disable** | **enable** }	使能或去使能端口 MAC 认证用户静默功能。
14	JX(config-ge-1/0/*)#**mac-authen quiet-times** *times*	配置端口 MAC 认证用户触发静默功能的认证失败次数，默认 3 次。
15	JX(config-ge-1/0/*)#**mac-authen critical-vlan user aging** { **disable** | **enable** }	使能或去使能端口 MAC 认证超时用户老化功能。
16	JX(config-ge-1/0/*)#**mac-authen critical-vlan user reauthenticate** { **disable** | **enable** }	使能或去使能端口 MAC 认证超时用户重认证功能。
17	JX(config-ge-1/0/*)#**mac-authen restrict-vlan user aging** { **disable** | **enable** }	使能或去使能端口 MAC 认证失败用户重认证功能。
18	JX(config-ge-1/0/*)#**mac-authen restrict-vlan user reauthenticate** { **disable** | **enable** }	使能或去使能端口 MAC 认证失败用户重认证功能。
19	JX(config)#**show mac-authen config**	查看 MAC 认证向配置。
20	JX(config)#**show mac-authen information**	查看 MAC 认证的全局信息。

步骤	配置	说明
21	JX(config)#**show mac-authen** *interface-type interface-number*	查看指定接口的 MAC 认证相关信息。
22	JX(config)#**show mac-authen user**	查看当前 MAC 认证的用户。

1.11.10 配置举例

如下图所示，用户需要进行 MAC 认证，用户直接跟设备相连，设备可以访问认证服务器。

图 1-15 MAC 认证组网示意图



配置步骤

设备配置如下：

```
JX(config)#aaa
JX(config-aaa)#radius-server host server1 ip-address 192.168.5.66 key 12345
JX(config-aaa)#server-group grp1 radius-server server1
JX(config-aaa)#aaa authentication mac-authen method m1 first grp1
JX(config-aaa)#quit
JX(config)#mac-authen start
JX(config)#mac-authen aaa authentication method m1
JX(config)#mac-authen mode fixed-user username wwf password plain 12345
JX(config)#interface ge 1/0/1
JX(config-ge-1/0/1)#mac-authen enable
```

通过 show mac-authen information 命令查看 MAC 认证相关信息：

```
Max User Number                 : 256
  Default Max User Number          : 256
  Current User Number              : 1
  Auth Success User Number         : 1
  Auth Fail User Number            : 0
  Auth Timeout User Number         : 0
  UserName Passwor Format          : Fixed
  MacAdress UpperCase              : Disable
  MacAdress With Hypen             : Disable
```

```
Mac Auth Method                 : Pap
AAA Authentication Method         : m1
AAA Accounting Method            : n/a
Fixed User Name                 : wwf
Fixed Password                  : 12345
```

检查结果

通过命令 **show mac-authen user** 查看当前 MAC 认证的用户：

```
JX(config)# show mac-authen user
 S:Success, F:Fail, T:Timeout, J:Join, A:Authenticate, O:Origin, C:Current,
L:Last
 Interface    Mac-Address      AuthNum(S/F/T)  Vlan(J/A/O)     Result(C/L)
 ge 1/0/1     0010:9400:0001    1/0/0          11/0/11         Success/None
```

1.12 URPF

1.12.1 简介

通常情况下，路由器收到数据报文后，获取到数据包中的目的 IP 地址，针对目的 IP 地址查找本地路由转发表，如果有对应转发表项则转发数据报文；否则，将报文丢弃。由此看来，路由器转发报文时，并不关心数据包的源地址。这就给源地址欺骗攻击有了可乘之机。

源地址欺骗攻击为入侵者构造出一系列带有伪造源地址的报文，频繁访问目的地址所在设备或者主机；即使响应报文不能到达攻击者，也会对被攻击对象造成一定程度的破坏。

URPF（Unicast Reverse Path Forwarding，单播逆向路径转发）的主要功能是用于防止基于源地址欺骗的网络攻击行为。路由器接口一旦使能 URPF 功能，当该接口收到数据报文时，首先会对数据报文的源地址进行合法性检查，对于源地址合法性检查通过的报文，才会进一步查找去往目的地址的转发表项，进入报文转发流程；否则，将丢弃报文。

严格（strict）型 URPF 检测功能

不但要求路由器转发表中，存在去往报文源地址的路由；而且还要求报文的入接口与转发表中去往源地址路由的出接口一致，只有同时满足上述两个条件的报文，才被认为是合法报文。在一些特殊情况下（如存在非对称路径），严格型检查会错误的丢弃非攻击报文。

松散（loose）型 URPF 检测功能

仅要求路由器的转发表中，存在去往报文的源地址路由即可，不再检查报文的入接口与转发表中去往源地址的路由的出接口是否一致。当用户网络中存在非对称路径等无法保证报文入接口和设备去往源地址路由出接口一致的情况下，可以配置松散型 URPF 检查。

诸如 TCP Syn Flood、UDP flood 和 ICMP flood 等攻击，都可能通过借助源地址欺骗的方式攻击目标设备或者主机，造成被攻击者系统性能严重的降低，甚至导致系统崩溃。URPF 就是网络设备为了防范此类攻击而使用的一种常用技术。

1.12.2 配置准备

场景

Switch 通过上行接口与 ISP（Internet Service Provider）的路由器连接，下行接口接用户网络。管理员希望 Switch 能够防范下行接口源 IP 地址欺骗攻击，避免非法用户伪造源 IP 地址攻击合法用户。

前提

无

1.12.3 缺省配置

功能	缺省值
接口 URPF 功能	不使能

1.12.4 配置 URPF

步骤	配置	说明
1	JX#**configure**	进入全局配置模式。
2	JX(config)#**interface interface-type** *interface-number*	进入接口配置模式。
3	JX(config-ge-1/0/1)# **urpf { loose | strict } { allow-default-route }**	使能 URPF 功能 loose：松散模式 strict：严格模式 （可选）allow-default-route：允许匹配默认路由

1.12.5 检查配置

序号	检查项	说明
1	JX#**show urpf interface** {*interface-type interface-number* }	显示接口的 URPF 配置模式

1.13 Timerange

1.13.1 简介

部分功能需要定时启动，或者在某些周期内启动，就可以利用 timerange 命令加以限制。在配置可以搭配 timerange 的功能（如 ACL，POE,NQA 等）时，通过时间段索引引用这个时间范围

1.13.2 配置准备

场景

当设备需要在不同时间段执行不同的安全策略时，可以配置 timerange。

前提

无

1.13.3 缺省配置

功能	缺省值
timerange 功能	不使能

1.13.4 配置 timerange

请在设备上进行以下配置。

步骤	配置	说明
1	`JX#config`	进入全局配置模式。
2	`JX(config)#time-range list` *id*	创建时间段列表

步骤	配置	说明
3	JX(config-timerange-*)#**time-range** *timerange-id* **absolute from** *hour:minute:second year/month/monthday* **to** *hour:minute:second year/month/monthday* JX(config-timerange-*)#**time-range** *timerange-id* **everyhour** *minute:second* **to** *minute:second* JX(config-timerange-*)#**time-range** *timerange-id* **everyday** *hour:minute:second* **to** *hour:minute:second* JX(config-timerange-*)#**time-range** *timerange-id* **everyweek** *hour:minute:second* { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } **to** { **mon** | **tue** | **wed** | **thu** | **fri** | **sat** | **sun** } JX(config-timerange-*)#**time-range** *timerange-id* **everymonth** *hour:minute:second monthday* **to** *hour:minute:second monthday* JX(config-timerange-*)#**time-range** *timerange-id* **everyweekend** *hour:minute:second* **to** *hour:minute:second* JX(config-timerange-*)#**time-range** *timerange-id* **everyyear** *hour:minute:second month/monthday* **to** *hour:minute:second month/monthday*	创建时间段，可应用于 ACL 规则。 对时间段（周期时间段）：是指 everyxxx 描述的以一周为间隔的期性时间，同时可以依靠绝对时段指明时间范围有效日期。 对时间段：是指由 absolute 指定特定的时间范围。可以通过绝对间段指定的时间范围来限制相对间段（周期时间段）在什么时间围生效。 果该时间段配置了多个生效时，生效原则为：周期时间段之间“或”，周期时间段和绝对时间段间取“与”
4	JX(configure-acl-l2-*)#**rule** *rule-id* **time-range** *timerange-list-id*	在 acl 中应用时间段
5	JX(config)#**nqa schedule** *admin-name operate-tag* **time-range** *timer-ange-list*	在 nqa 中应用时间段

1.13.5 检查配置

序号	检查项	说明
1	JX#**show timerange list**	查看所有 timerange

1.14 DOS 防攻击

1.14.1 简介

畸形报文攻击防范

畸形报文攻击是通过向目标设备发送有缺陷的 IP 报文，使得目标设备在处理这样的 IP 报文时出错和崩溃，给目标设备带来损失。畸形报文攻击防范是指设备实时检测出畸形报文并予以丢弃，实现对本设备的保护。

分片报文攻击防范

分片报文攻击是通过向目标设备发送分片出错的报文，使得目标设备在处理分片错误的报文时崩溃、重启或消耗大量的 CPU 资源，给目标设备带来损失。分片报文攻击防范是指设备实时检测出分片报文并予以丢弃或者限速处理，实现对本设备的保护。

泛洪攻击防范

泛洪攻击是指攻击者在短时间内向目标设备发送大量的虚假报文，导致目标设备忙于应付无用报文，而无法为用户提供正常服务。

泛洪攻击防范是指设备实时检测出泛洪报文并予以丢弃或者限速处理，实现对本设备的保护。

泛洪攻击主要分为 TCP SYN 泛洪攻击、UDP 泛洪攻击和 ICMP 泛洪攻击。

(1) TCP SYN 泛洪攻击

TCP SYN 攻击利用了 TCP 三次握手的漏洞。在 TCP 的 3 次握手期间，当接收端收到来自发送端的初始 SYN 报文时，向发送端返回一个 SYN+ACK 报文。接收端在等待发送端的最终 ACK 报文时，该连接一直处于半连接状态。如果接收端最终没有收到 ACK 报文包，则重新发送一个 SYN+ACK 到发送端。如果经过多次重试，发送端始终没有返回 ACK 报文，则接收端关闭会话并从内存中刷新会话，从传输第一个 SYN+ACK 到会话关闭大约需要 30 秒。

在这段时间内，攻击者可能将数十万个 SYN 报文发送到开放的端口，并且不回应接收端的 SYN+ACK 报文。接收端内存很快就会超过负荷，且无法再接受任何新的连接，并将现有的连接断开。

设备对 TCP SYN 攻击处理的方法是在使能了 TCP SYN 泛洪攻击防范后对 TCP SYN 报文进行速率限制，保证受到攻击时设备资源不被耗尽。

(2) UDP 泛洪攻击

UDP 泛洪攻击是指攻击者在短时间内向目标设备发送大量的 UDP 报文，导致目标设备负担过重而不能处理正常的业务。UDP 泛洪攻击分为以下两类：

•Fraggle 攻击

Fraggle 攻击的原理是攻击者发送源地址为目标主机地址，目的地址为广播地址，目的端口号为 7 的 UDP 报文。如果该广播网络中有很多主机都

起用了 UDP 响应请求服务，目的主机将收到很多回复报文，造成系统繁忙，达到攻击效果。

使能泛洪攻击防范功能后，设备默认 UDP 端口号为 7 的报文是攻击报文，直接将其丢弃。

•UDP 诊断端口攻击

攻击者对 UDP 诊断端口（7-echo，13-daytime，19-Chargen 等 UDP 端口）发送报文，如果同时发送的数据包数量很大，造成泛洪，可能影响网络设备的正常工作。

使能泛洪攻击防范功能后，设备将 UDP 端口为 7、13 和 19 的报文认为是攻击报文，直接丢弃。

(3) ICMP 泛洪攻击

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

1.源设备向接收设备发出 ICMP 响应请求报文；

2.接收设备接收到 ICMP 响应请求报文后，会向源设备回应一个 ICMP 应答报文。

如果攻击者向目标设备发送大量的 ICMP 响应请求报文，则目标设备会忙于处理这些请求，而无法继续处理其他的数据报文，造成对正常业务的冲击。

设备针对 ICMP 泛洪攻击进行 CAR（Committed Access Rate）限速，保证 CPU 不被攻击，保证网络的正常运行。

1.14.2 配置准备

场景

设备经常会受到不同类型的网络攻击，这样会导致设备资源使用率过高，影响网络服务。为保障给用户提供安全的网络服务，在设备上部署 Dosantiattack 功能，主要防范的攻击类型包括：

畸形报文攻击防范，防止畸形报文攻击。

分片报文攻击防范，限制分片报文的速率，防止分片报文对 CPU 造成攻击，占用过多 CPU 和设备资源。

泛洪攻击防范，包括以下三种：

TCP SYN 泛洪攻击防范，限制 TCP SYN 报文的速率，防止 CPU 处理 TCP SYN 报文占用过多资源；

UDP 泛洪攻击防范，对特定端口发送的 UDP 报文直接丢弃；

ICMP 泛洪攻击防范，限制 ICMP 泛洪攻击报文的上送速率，防止 CPU 处理 ICMP 泛洪攻击报文占用过多资源。

前提

无。

1.14.3 DOS 防攻击功能的缺省配置

设备上 DOS 防攻击功能的缺省配置如下。

功能	缺省值
Dosantiattack 全局功能状态	禁用
畸形报文攻击防范功能	禁用
分片报文攻击防范功能	禁用
分片报文发送速率	155000000bit/s
TCP Syn 攻击防范功能	禁用
TCP Syn 泛洪报文发送速率	155000000bit/s
UDP 泛洪攻击防范功能	禁用
ICMP 泛洪攻击防范功能	禁用
ICMP 泛洪报文发送速率	155000000bit/s

1.14.4 配置畸形报文攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#config	进入全局配置模式。
2	JX(config)#dos-antiattack pkt-limit abnormal enable	使能畸形报文攻击防范功能。

1.14.5 配置分片报文攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#config	进入全局配置模式。
2	JX(config)#dos-antiattack pkt-limit fragment enable	使能畸形报文攻击防范功能。

步骤	配置	说明
3	JX(config)#**dos-antiattack pkt-limit fragment cir** { **kbps**|**mbps**|**gbps** } *cir-number* JX(config)#**dos-antiattack pkt-limit fragment pps** *pps-number*	限制分片报文接收的速率。

1.14.6 配置 TCP SYN 泛洪攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dos-antiattack pkt-limit tcp-syn enable**	使能 TCP SYN 泛洪攻击防范功能。
3	JX(config)#**dos-antiattack pkt-limit tcp-syn cir** { **kbps**|**mbps**|**gbps** } *cir-number* JX(config)#**dos-antiattack pkt-limit tcp-syn pps** *pps-number*	限制 TCP SYN 报文接收的速率。

1.14.7 配置 UDP 泛洪攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dos-antiattack pkt-limit udp-flood enable**	使能 UDP 泛洪攻击防范功能。

1.14.8 配置 ICMP 泛洪攻击防范

请在设备上进行以下配置。

步骤	配置	说明
1	JX#**config**	进入全局配置模式。
2	JX(config)#**dos-antiattack pkt-limit icmp-flood enable**	使能 ICMP 泛洪攻击防范功能。
3	JX(config)#**dos-antiattack pkt-limit icmp-flood cir** { **kbps**|**mbps**|**gbps** } *cir-number* JX(config)#**dos-antiattack pkt-limit icmp-flood pps** *pps-number*	限制 ICMP 泛洪攻击报文接收的速率。

1.14.9 检查配置

配置完成后，请在设备上执行以下命令检查配置结果。

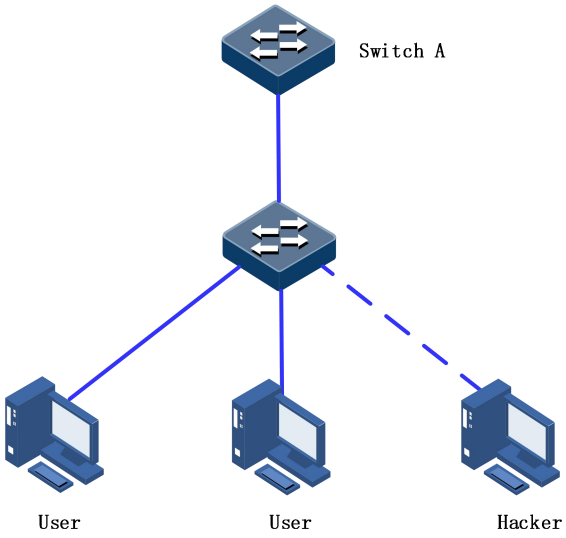
序号	检查项	说明
1	JX#show dos-antiattack config	查看 Dos 防攻击配置信息。
2	JX#show dos-antiattack statistics	查看 Dos 防攻击统计数据。

1.14.10 配置 DOS 防攻击示例

组网需求

如果局域网内存在 Hacker 向 SwitchA 发起畸形报文攻击、分片报文攻击和泛洪攻击，将会造成 SwitchA 瘫痪。为了预防这种情况，管理员希望通过在 SwitchA 上部署各种攻击防范措施来为用户提供安全的网络环境，保障正常的网络服务。

图 1-16 DOS 防攻击应用组网示意图



配置步骤

步骤 1 配置 DOS 防攻击功能。

```
JX#config
JX(config)#dos-antiattack pkt-limit enable
```

步骤 2 配置畸形报文攻击防范。

```
JX(config)#dos-antiattack pkt-limit abnormal enable
```

步骤 3 配置分片报文攻击防范，并限制分片报文接收的速率为 15kbit/s。

```
JX(config)#dos-antiattack pkt-limit fragment enable
JX(config)#dos-antiattack pkt-limit fragment cir kbps 15
```

步骤 4 配置 TCP SYN 攻击防范，并限制 TCP SYN 报文接收的速率为 15kbit/s。

```
JX(config)#dos-antiattack pkt-limit tcp-syn enable
JX(config)#dos-antiattack pkt-limit tcp-syn cir kbps 15
```

步骤 5 配置 UDP 泛洪攻击防范。

```
JX(config)#dos-antiattack pkt-limit udp-flood enable
```

步骤 6 配置ICMP泛洪攻击防范，并限制ICMP泛洪报文接收的速率为15kbit/s。

```
JX(config)#dos-antiattack pkt-limit icmp-flood enable
JX(config)#dos-antiattack pkt-limit icmp-flood cir kbps 15
```

检查结果

通过 **show dos-antiattack config** 命令查看 DOS 防攻击配置结果。

```
JX#show dos-antiattack config
!
!
dos-antiattack pkt-limit enable
!
dos-antiattack pkt-limit abnormal enable
dos-antiattack pkt-limit fragment enable
dos-antiattack pkt-limit fragment cir kbps 15
dos-antiattack pkt-limit tcp-syn enable
dos-antiattack pkt-limit tcp-syn cir kbps 15
dos-antiattack pkt-limit udp-flood enable
dos-antiattack pkt-limit icmp-flood enable
dos-antiattack pkt-limit icmp-flood cir kbps 15
```