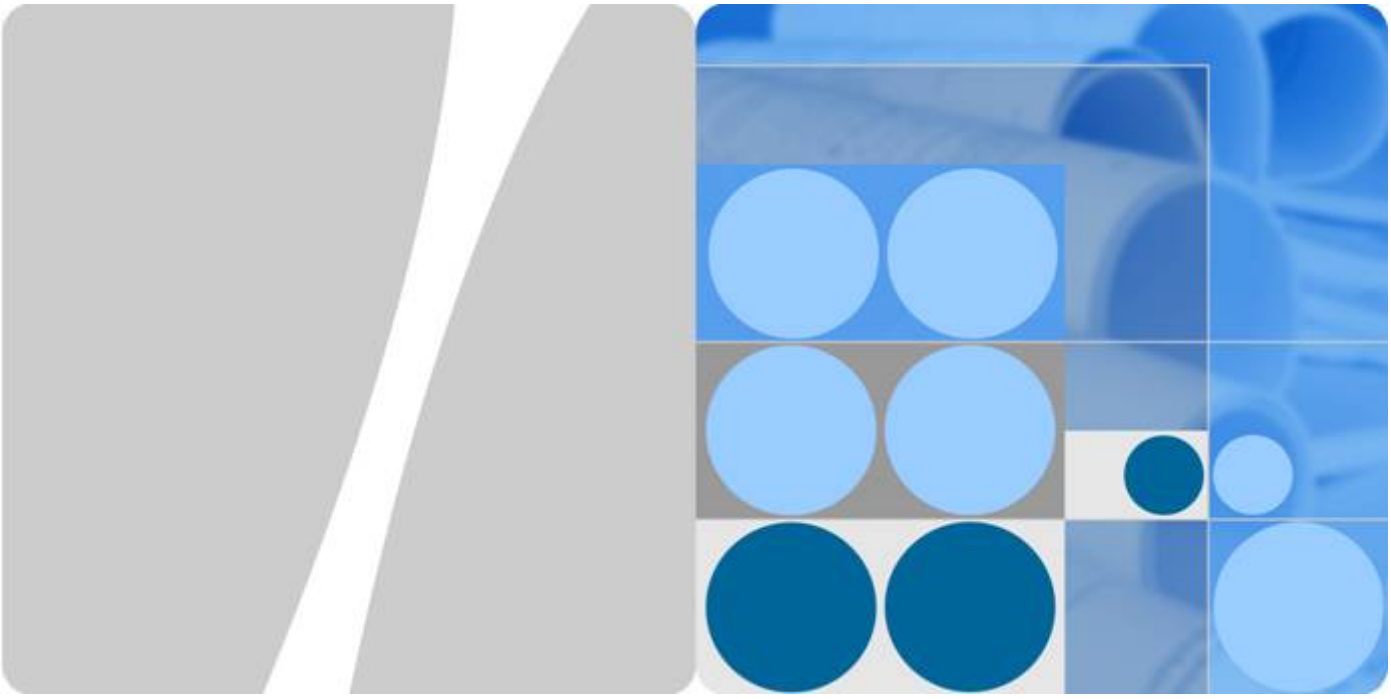


S 系列交换机

# 安全加固指南

文档版本　18

发布日期　2024-04-03

华为技术有限公司

**商标声明**


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

**注意**

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

# 华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://e.huawei.com

# 前言

## 读者对象

本文档适用于负责配置和管理交换机的网络工程师。您应该熟悉以太网基础知识，且具有丰富的网络部署与管理经验。

## 符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

| 符号 | 说明 |
| --- | --- |
| 须知 | 用于传递设备或环境安全警示信息。如不避免则可能会导致设备损坏、数据丢失、设备性能降低或其他不可预知的结果。<br>“须知”不涉及人身伤害。 |
| 说明 | 对正文中重点信息的补充说明。<br>“说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。 |

## 接口编号约定

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

## 安全约定

- 密码配置约定
  - 配置密码时请尽量选择密文模式(cipher)。为充分保证设备安全，请用户不要关闭密码复杂度检查功能，并定期修改密码。
  - 配置明文模式的密码时，请不要以“%^%#.....%^%#”、“%#%#.....%#%#”、“%@%@.....%@%@”或者“@%@%.....@%@%”作为起始和结束符。因为用这些字符为起始和结束符的是合法密文（本设备可以解密的密文），配置文件会显示与用户配置相同的明文。

  - 配置密文密码时，不同特性的密文密码不能互相使用。例如AAA特性生成的密文密码不能用于配置其他特性的密文密码。

- 加密算法约定

  目前设备采用的加密算法包括3DES、AES、RSA、SHA1、SHA2和MD5。3DES、RSA和AES加密算法是可逆的，SHA1、SHA2和MD5加密算法是不可逆的。DES/3DES/RSA(1024位以下)/MD5(数字签名场景和口令加密)/SHA1(数字签名场景)加密算法安全性低，存在安全风险。在协议支持的加密算法选择范围内，建议使用更安全的加密算法，比如AES/RSA(2048位以上)/SHA2/HMAC-SHA2。具体采用哪种加密算法请根据场景而定：对于管理员类型的密码，必须采用不可逆加密算法，推荐使用安全性更高的SHA2。

- 个人数据约定

  您购买的产品、服务或特性在业务运营或故障定位的过程中将可能获取或使用用户的某些个人数据（如终端用户的MAC地址或IP地址），因此您有义务根据所适用国家的法律制定必要的用户隐私政策并采取足够的措施以确保用户的个人数据受到充分的保护。

- 本文档中出现的“镜像端口、端口镜像、流镜像、镜像”等相关词汇仅限于为了描述该产品进行检测通信传输中的故障和错误的目的而使用，不涉及采集、处理任何个人数据或任何用户通信内容。

- 可靠性设计声明

  对于网络规划和站点设计，必须严格遵守可靠性设计原则，具备设备级和方案级保护。设备级保护包括双网双平面，双机、跨板双链路的规划原则，避免出现单点，单链路故障。方案级指FRR、VRRP等快速收敛保护机制。在应用方案级保护时，应避免保护方案的主备路径经过相同链路或者传输，以免方案级保护不生效。

# 特别声明

- 本文档仅作为使用指导，其内容（如Web界面、CLI命令格式、命令输出）依据实验室设备信息编写。文档提供的内容具有一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号不同、配置文件不同等原因，可能造成文档中提供的内容与用户使用的设备界面不一致。请以用户设备界面的信息为准，本文档不再针对前述情况造成的差异一一说明。
- 本文档中提供的最大值是设备在实验室特定场景（例如，被测试设备上只有某种类型的单板，或者只配置了某一种协议）达到的最大值。在现实网络中，由于设备硬件配置不同、承载的业务不同等原因会使设备测试出的最大值与文档中提供的数据不一致。
- 出于特性介绍及配置示例的需要，本文档可能会使用公网IP地址，如无特殊说明出现的公网IP地址均为示意，不指代任何实际意义。

# 目 录



# 1 概述

本文档针对安全加固策略，从攻击行为、安全策略和配置方法等方面指导用户加强网络安全和交换机安全。并且从管理平面、控制平面和转发平面指导用户对交换机进行加固维护。

**说明**

本手册不区分产品版本。不同形态、不同版本支持的功能可能存在差异，如需了解详细情况，请您参考配置指南手册。



## 1.1 交换机的安全隔离与防御机制

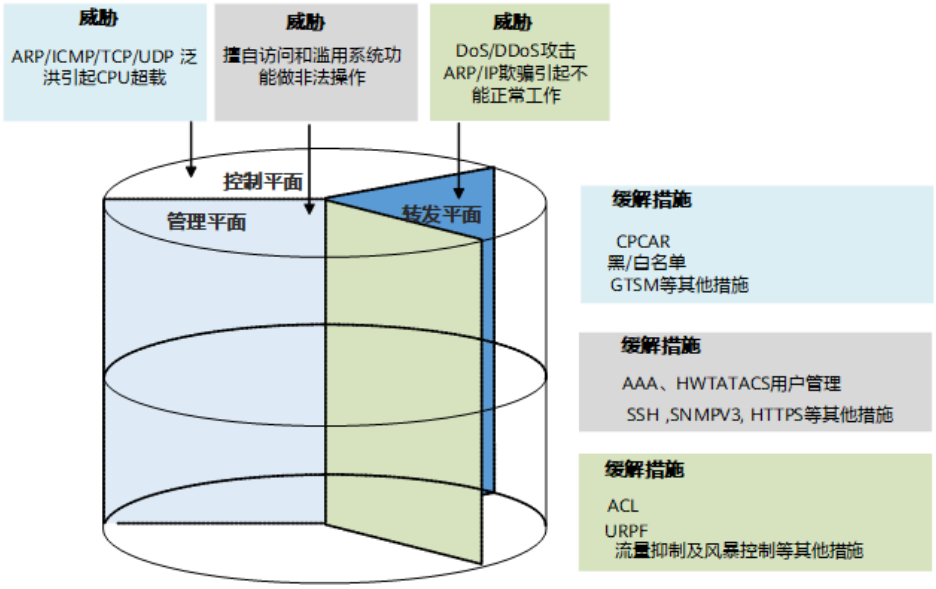
交换机遵循X.805的三层三面安全隔离机制，其体系架构如**图1-1**所示。

由于不同的数据流的重要程度不同、受到的安全威胁不同、对用户的影响不同，为避免数据流相互影响，交换机划分为三个不同的安全平面。

- 管理平面：关注管理用户的应用和业务数据的安全，即管理信息的安全，包括操作、维护和管理信息。
- 控制平面：交换机需要运行各种各样的协议来达成业务，这些协议自身需要考虑安全性，避免被攻击或者仿冒。
- 转发平面：信息流的转发主要通过IP报文的目的MAC地址、目的IP地址来查找路径转发；相关安全性主要针对转发路径上如何避免对交换机自身的恶意攻击行为，以及预防某些攻击流量在IP网络中的扩散。

通过将控制平面、管理平面和转发平面进行隔离，交换机能够保证任何一个平面在遭受攻击时，不会影响其他平面的正常运行。

**图 1-1** X.805 的三层三面安全隔离架构




# 1.2 交换机安全加固的原则

在进行交换机安全加固配置之前，您需要了解如下信息，以免对本手册列出的安全加固策略机械的复制，从而影响您的业务。

安全是一个持续改进的过程，从来没有一蹴而就的安全，也没有一劳永逸的安全。任何企图依靠某个策略就可以保证高枕无忧，或者任何企图依靠一次安全加固配置就万事大吉的想法，都是不合理的。

在进行安全加固之前，需要执行如下步骤。

- 深入了解业务需求：安全永远是为业务服务的，需要深入了解业务系统对安全防护的要求，才能制定合理的安全策略。
- 全面评估风险：需要综合分析业务系统面临的安全威胁，权衡业务系统的脆弱点，权衡业务系统的价值与安全加固的代价，全面实施安全风险评估，把不可接受的安全风险进行防护，把能够接受的风险作为残留风险接纳，并在业务系统生命周期中定期审视这些残留风险，评估其是否需要进行升级处理。
- 设计安全加固方案：在全面的风险评估基础上，设计切实满足业务的需求，设计出合理的方案。安全是设计出来的，不是配置出来的，希望每一个进行安全加固的工程师，深刻理解这一原则。
- 实施安全策略：将安全加固策略实施之前，请务必评估因为安全策略对业务带来的影响，避免由于不合理的安全策略造成业务损伤。

在完成安全加固之后，需要不断的监控和维护业务系统，以确保安全策略已经切实发挥作用并达到安全加固方案预期的效果，及时发现问题，并调整安全策略。安全加固是一个持续的改进过程。

# 1.3 交换机安全加固策略的级别

按照网络安全需求，可以将交换机的安全加固策略分为Level-1、Level-2两个级别。

- Level-1：代表的是必须要配置的安全加固策略。

- Level-2：代表的是加强的安全加固策略，用户可以根据自己的业务有选择的进行配置。

# 2 Level-1 的安全加固策略（必配）



## 2.1 缺省账号与密码

您可以在《S系列交换机缺省帐号与密码》（**企业网**、**运营商**）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

## 2.2 管理平面

### 2.2.1 数字证书管理

数字证书用于保证设备内的各服务间，以及设备与外部通信的安全性，防止通信数据在传输过程被篡改造成安全风险，提升系统的安全性。

设备支持上传CA（Certification Authority）证书和设备证书。

- CA证书（CA Certificate）

  又叫根证书，用于访问设备时校验设备证书，验证设备证书是否为本根证书签发。
- 设备证书（Device Certificate）
  - 设备证书：又叫本地证书，即公钥文件，它与私钥文件成对出现。由根证书签发获得，通常用于加密会话或数据，为接入该服务的请求提供安全保障。
  - 私钥文件（Private Key File）：与设备证书成对出现，用于解密设备证书加密的数据。
  - 私钥密码：用于对私钥文件进行加密保护。

设备出厂时，主控都会预置CA证书和本地证书，并存放到NVRAM内存中，且不支持删除和修改。设备启动会自动将CA证书和设备证书导入default域。预置证书详情请参见**表2-1**。设备中使用证书的模块及相关描述请参见**表2-2**。

如果设备无法向CA申请本地证书，部分业务会使用设备内部生成的自签名证书，并将生成的证书以文件形式保存在存储器中，实现简单的证书颁发功能。

- 自签名证书（Self-signed Certificate）

  自签名证书也是一种根证书，是自己颁发给自己的证书，即证书中的颁发者和主体名相同。

自签名证书详情请参见**表2-3**。设备中使用自签名证书的模块及相关描述请参见**表2-4**。

**说明**

使用默认的证书可能存在安全风险，为了提高系统安全性，强烈建议将预置证书替换成自身的数字证书，并定期更新证书和密钥。

申请者无法向CA申请本地证书时，可以通过设备生成自签名证书，实现简单证书颁发功能。

设备不支持对其生成的自签名证书进行生命周期管理（如证书更新、证书撤销等），为了确保设备和证书的安全，建议用户替换为自己的本地证书。

**表 2-1** 预置数字证书

| 证书名称 | 证书文件 | 证书功能 | 证书的颁发者 | 证书的拥有者 | 说明 |
| --- | --- | --- | --- | --- | --- |
| default_ca | CA证书：default_ca.cer | 验证对端华为设备身份。 | 华为根证书：<br>Huawei Equipment CA<br>华为二级证书：<br>Huawei Equipment CA<br>华为保留证书：<br>Huawei Equipment CA | 华为根证书：<br>Huawei Equipment CA<br>华为二级证书：<br>Huawei Enterprise Network Product CA<br>华为保留证书：<br>Huawei Fixed Network Product CA | 将预置CA证书导入default域后，如果需要使用其他CA证书，先使用**pki delete-certificate ca realm** *default* 命令将预置CA证书从default域移除，再导入新证书。**default_ca.cer**为系统预留的预置CA证书名称，新导入的证书不能命名为**default_ca.cer**。 |

| 证书名称 | 证书文件 | 证书功能 | 证书的颁发者 | 证书的拥有者 | 说明 |
| --- | --- | --- | --- | --- | --- |
| default_local | 设备证书：default_local.cer | 供其他设备验证本端设备身份。 | Huawei Enterprise Network Product CA | 设备 | 根据具体业务选择是否使用此证书进行身份认证。<br>将预置设备证书导入default域后，如果需要使用其他设备证书，先使用**pki delete-certificate local realm** *default*命令将预置设备证书从default域移除，再导入新证书。<br>**default_local.cer**为系统预留的预置设备证书名称，新导入的设备证书不能命名为**default_local.cer**。 |

**表 2-2** 数字证书使用情况

| 使用证书的特性/模块 | 证书用途 | 是否默认使用预置证书 | 是否支持用户替换为非预置证书 | 是否涉及申请多个证书、加载顺序是否有要求 | 自行申请证书时对格式、名称的要求 | 自行申请证书时对Common Name等字段的要求 |
| --- | --- | --- | --- | --- | --- | --- |
| CAPWAP | • DTLS加密场景：用于AP开局，通过证书认证接入AC。<br>• 非DTLS加密场景：通过证书认证走DTLS密钥协商过程，协商出敏感信息加密和完整性校验密钥。 | 是 | 不支持 | 不涉及 | 无 | 无 |

| 使用证书的特性/模块 | 证书用途 | 是否默认使用预置证书 | 是否支持用户替换为非预置证书 | 是否涉及申请多个证书、加载顺序是否有要求 | 自行申请证书时对格式、名称的要求 | 自行申请证书时对Common Name等字段的要求 |
| --- | --- | --- | --- | --- | --- | --- |
| 云管理 | 控制器纳管设备场景中，控制器与设备进行连接，使用证书进行双向认证。<br>SSH建立管理通道、HTTPS传输文件。 | 是 | 支持<br>替换指导请见《配置交换机与iMaster NCE-Campus通信》章节。 | 不涉及 | 无 | 设备证书的Common Name使用ESN作为标识。 |
| HTTP2.0 | 设备进行数据上报使用的性能通道，使用证书进行双向认证。 | 是 | 支持 | 不涉及 | 无 | 无 |

**表 2-3** 自签名证书

| 证书名称 | 证书功能 | 证书的颁发者 | 证书的拥有者 |
| --- | --- | --- | --- |
| 自签名证书 | 设备颁给自己的证书，实现简单的证书颁发功能。 | 设备 | 设备 |

**表 2-4** 自签名证书使用情况

| 使用证书的特性/模块 | 证书用途 | 是否默认使用自签名证书 | 是否支持用户替换为自己的证书 | 是否涉及申请多个证书、加载顺序是否有要求 | 自行申请证书时对格式、名称的要求 | 自行申请证书时对Common Name等字段的要求 |
| --- | --- | --- | --- | --- | --- | --- |
| WEB | WEB客户端验证服务端的合法性。 | 是 | 是<br>替换指导请见《配置通过Web网管登录设备》章节。 | 不涉及 | 无 | 无 |
| Portal HTTPS重定向 | Portal服务器验证设备的合法性。 | 是 | 否 | 不涉及 | 无 | 无 |

如果您需要在以下场景完成与外部通信证书的上传或更新，请根据指导进行操作。

- 当通信双方需要通过数字证书来进行身份认证时，可以通过命令行上传该数字证书。
- 当存在以下场景时，可以通过命令行更新相应的数字证书：
  - 为了确保设备的安全性，替换设备的预置证书。
  - 日常维护中用户认为当前数字证书不安全，要求替换当前的证书。
  - 系统上报**hwPKICACertNearlyExpired**告警、**hwPKILocalCertNearlyExpired**告警、**hwPKICACertInvalid**告警或**hwPKILocalCertInvalid**告警。
  - 升级前需要替换预置的证书，如果不替换，升级后各服务间或者与外部通信时可能对接失败。

## 对系统的影响

无

## 前提条件

- 当需要上传或更新CA证书时，需要提前获取根证书。
- 当需要上传或更新设备证书时，需要提前获取设备证书、私钥文件及私钥密码。

## 操作步骤

1. 将获取到的证书、私钥文件上传至Flash存储器根目录下
2. 执行命令**system-view**，进入系统视图。

3. 执行命令**pki realm** *realm-name*，创建PKI域并进入PKI域视图，或者直接进入PKI域视图。
4. 执行命令**quit**，返回到系统视图。
5. 执行命令**pki import-certificate ca realm** *realm-name* { **der** | **pkcs12** | **pem** } [ **filename** *filename* ] [ **replace** ] [ **no-check-validate** ] [ **no-check-hash-alg** ]或执行命令**pki import-certificate ca realm** *realm-name* **pkcs12 filename** *filename* [ **no-check-validate** ] [ **no-check-hash-alg** ] **password** *password*，将CA证书导入到设备的内存中。

   **说明**

   配置**replace**参数后，如果域下有相同证书，会删除原有证书及对应的RSA密钥对，导入新的证书。

   当原有证书对应的RSA密钥对没有被非当前域引用时，则删除证书和密钥对；当原有证书对应的RSA密钥对被非当前域或CMP会话所引用时，只删除原有证书，不删除密钥对。
6. 执行命令**pki import-certificate local realm** *realm-name* { **der** | **pkcs12** | **pem** } [ **filename** *filename* ] [ **replace** ] [ **no-check-validate** ] [ **no-check-hash-alg** ]或执行命令**pki import-certificate local realm** *realm-name* **pkcs12 filename** *filename* [ **no-check-validate** ] [ **no-check-hash-alg** ] **password** *password*，将设备证书导入到设备的内存中。

   证书及其密钥对有两种存在形式，一种是证书文件中包含密钥对文件，两者以一个文件的形式存在；另一种是证书和密钥对相互独立以两个文件形式存在。不同形式下，将其导入内存所使用的方法不同。

   - 证书文件中包含密钥对文件。

     执行命令**pki import rsa-key-pair**一次导入证书文件和密钥对文件。

     **说明**

     证书文件中包含密钥对文件时，执行命令**pki import-certificate**只能导入证书文件，密钥对文件不会被导入。如果需要导入密钥对文件，可执行命令**pki import rsa-key-pair**将密钥对继续导入。
   - 证书文件和密钥对文件独立存在。

     i. 导入证书文件。

        执行命令**pki import-certificate**导入证书文件。

     ii. 导入密钥对文件。

        执行命令**pki import rsa-key-pair**导入密钥对文件。

   **说明**

   若用户无法辨别待导入证书的格式，可依次配置不同格式并检查是否成功导入证书。若不指定待导入证书的格式，系统将自行识别导入。

## 检查加固结果

- 执行命令**display pki certificate ca realm** *realm-name*，查看设备上已加载的CA证书的内容。
- 执行命令**display pki certificate local realm** *realm-name*，查看设备上已加载的设备证书的内容。

# 2.2.2 设备登录的安全

### 2.2.2.1 Console 口方式登录交换机

## 攻击行为

Console口（也称串口）属于物理接口，攻击者接触到Console口后，交换机将暴露给攻击者，交换机的安全无法保障。即使该攻击者没有破解用户名和密码，也能够对交换机造成损害。

在使用Console口登录的情况下，可能有潜在的攻击者通过网络连接尝试破解用户名和密码，获取交换机管理权限。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

当交换机第一次启用时，需要通过Console口进行第一次配置：

1. 将Console通信电缆的DB9（孔）插头插入PC机的串口，在交换机启动过程中，按下“CTRL+B”或者“CTRL+E”快捷键。
   - V200R019及之前版本：利用缺省密码进入BootROM或BootLoad菜单，修改BootROM或BootLoad的密码。
   - V200R020及之后版本：BootROM或BootLoad菜单缺省无密码。首次登录时系统提示必须设置新密码。
2. 交换机生成配置，此时必须修改Console口的登录密码，并记录所配置的登录密码。
   - V200R009及之前版本Console口默认无认证方式，无默认的用户名和密码，交换机允许用户登录并提示是否配置密码。为保证Console口安全，建议用户此时将Console用户界面的认证方式修改为AAA认证，并在AAA视图下配置用户名和密码。
   - V200R010至V200R019版本Console口默认为AAA认证，需要在AAA视图下配置用户名和密码。建议用户使用默认的认证方式。
   - V200R020及之后版本Console口默认为Password认证。首次登录时系统提示必须设置密码。

**说明**

您可以在《S系列交换机缺省帐号与密码》（**企业网**、**运营商**）文档中获取各种缺省帐号与密码信息。获取该文档需要权限，如需升级权限，请查看网站帮助。

由于交换机密码采用密文保存，用户需要记录此时配置的密码，以便日后管理登录Console口使用。

## 配置方法

- 修改BootROM或BootLoad密码

  有的设备支持BootROM菜单，有的设备支持BootLoad菜单，不同版本、不同形态可能有差异，请您以设备为准。

  **修改BootROM密码**

  交换机启动过程中，出现以下提示信息时，表示交换机启动了BootROM程序。

  当出现“Press Ctrl+B or Ctrl+E to enter BootROM menu :”时，及时（3秒内）按下快捷键Ctrl+B或Ctrl+E，进入BootROM主菜单。

  输入正确的BootROM密码，显示的BootROM主菜单如下：

框式交换机：

```
          MAIN  MENU

  1. Boot with default mode
  2. Boot from Flash
  3. Boot from CFCard
  4. Enter serial submenu
  5. Enter ethernet submenu
  6. Enter file system submenu
  7. Enter test submenu
  8. Enter password submenu
  9. Modify Flash description area
 10. Clear password for console user
 11. Reboot

Enter your choice(1-11): 8   //选择8，进入密码子菜单

      PASSWORD  SUBMENU

  1. Modify BootROM password
  2. Reset BootROM password
  3. Return to main menu

Enter your choice(1-3):1   //选择1，修改BootROM密码
Modify BootROM password
Old password:     //输入原密码
New password:     //输入新密码
Verify:           //再次输入新密码
```

盒式交换机：

```
        BootROM  MENU

  1. Boot with default mode
  2. Enter serial submenu
  3. Enter startup submenu
  4. Enter ethernet submenu
  5. Enter filesystem submenu
  6. Enter password submenu
  7. Clear password for console user
  8. Reboot
  (Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 6   //选择6，进入密码子菜单

      PASSWORD  SUBMENU

  1. Modify BootROM password
  2. Reset BootROM password
  3. Return to main menu

Enter your choice(1-3): 1   //选择1，修改BootROM密码

Old password:     //输入原密码
New password:     //输入新密码
Verify:           //再次输入新密码

Write password to flash ...
```

**修改BootLoad密码**

交换机启动过程中，出现以下提示信息时，表示设备启动了BootLoad程序。当出现“Press CTRL+B to enter BootLoad menu :”时，及时（3秒内）按下快捷键Ctrl+B，进入BootLoad菜单。

框式交换机：

```
      BootLoad Menu

  1. Boot with default mode
  2. Enter ethernet submenu
  3. Modify Flash description area
```

```
    4. File system submenu
    5. Enter password submenu
    6. Clear password for console user
    7. Reboot

Enter your choice(1-7):    //选择5，进入密码子菜单

 PASSWORD  SUBMENU

    1. Modify bootload password
    2. Reset bootload password
    3. Return

Enter your choice(1-3):    //选择1，修改BootLoad密码

Old password:     //输入原密码
New password:     //输入新密码
Verify:           //再次输入新密码
```

盒式交换机：

```
        BootLoad Menu

   1. Boot with default mode
   2. Enter serial submenu
   3. Enter startup submenu
   4. Enter ethernet submenu
   5. Enter filesystem submenu
   6. Enter password submenu
   7. Clear password for console user
   8. Reboot
   (Press Ctrl+E to enter diag menu)

Enter your choice(1-8):    //选择6，进入密码子菜单

      PASSWORD  SUBMENU

    1. Modify bootload password
    2. Reset bootload password
    3. Return to main menu

Enter your choice(1-3):    //选择1，修改BootLoad密码

Enter your choice(1-3): 1

Old password:     //输入原密码
New password:     //输入新密码
Verify:           //再次输入新密码
```

- 配置AAA认证

  将Console用户界面的认证方式配置为AAA认证，并在AAA视图下配置用户名admin1234和密码Helloworld@6789。

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] authentication-mode aaa
[HUAWEI-ui-console0] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[HUAWEI-aaa] local-user admin1234 service-type terminal
```

## 检查加固结果

- 执行命令**display current-configuration configuration user-interface**，查看Console口的配置情况。

### 2.2.2.2 SSH 方式登录交换机

## 攻击行为

- 暴力破解密码

  攻击者在侦听到SSH端口后，尝试进行连接，交换机提示认证，则会进行暴力破解尝试通过认证，获取访问权限。

- 拒绝服务式攻击

  SSH Server支持的用户数有限，在用户登录达到上限后，其他用户将无法登录。这个可能是正常使用造成，也可能是攻击者造成。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- 密码认证和Public-Key认证

  SSH Server支持密码认证和Public-Key认证，只有通过认证的用户才能登录交换机，进入命令行界面。

- 关闭服务

  当开启SSH Server服务器时，交换机将开启Socket服务，易被攻击者扫描。当不使用SSH Server时，可以关闭SSH Server。

- 变更端口号

  缺省情况下，SSH服务器的端口号为22。端口号22属于知名端口号，易被扫描和攻击。可以修改SSH Server的端口为私有端口，减小被扫描攻击的概率。

- ACL

  在用户界面视图（user-interface）可以配置各个VTY通道的ACL过滤规则，通过ACL控制允许登录的客户端IP。

- 配置SSH服务器源接口

  V200R020C00之前版本，SSH服务器端缺省接收来自所有接口登录连接请求，存在安全风险，建议使用**ssh server-source -i**命令指定SSH服务器端的源接口。V200R020C00及之后版本，SSH服务器端缺省不接收来自任何接口登录连接的请求，需要通过**ssh server-source -i**命令指定SSH服务器端的源接口，不建议配置**ssh server-source all-interface**命令配置SSH服务器的源接口为设备上所有配置了IPv4地址的接口。

  成功指定SSH服务器端的源接口后，系统只允许SSH用户通过指定的源接口登录服务器，通过其他接口登录的SSH用户都将被拒绝。但对于已登录到服务器的SSH用户不会产生影响，只限制后续登录的SSH用户。

## 配置方法

- 配置密码认证或者RSA认证
  - 密码认证：配置用户testuser的认证方式为密码认证

    ```
    <HUAWEI> system-view
    [HUAWEI] ssh user testuser
    [HUAWEI] ssh user testuser authentication-type password
    ```

  - RSA认证：配置用户testuser的认证方式为RSA认证（RSA要采用2048位及以上算法）

    ```
    <HUAWEI> system-view
    [HUAWEI] ssh user testuser
    [HUAWEI] ssh user testuser authentication-type rsa
    ```

- 关闭SSH服务

```
<HUAWEI> system-view
[HUAWEI] undo stelnet server enable
```

- 变更SSH服务器端口号为55535

```
<HUAWEI> system-view
[HUAWEI] ssh server port 55535
```

- 配置ACL 2000，允许源IP地址为10.1.1.1的用户登录到交换机

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] user-interface vty 14
[HUAWEI-ui-vty14] acl 2000 inbound  //当需要限制某个地址或地址段的用户登录到交换机时，使用inbound；当需要限制已经登录的用户登录到其它交换机时，使用outbound。
[HUAWEI-ui-vty14] quit
```

- 配置SSH服务器端的源接口为Loopback0

```
<HUAWEI> system-view
[HUAWEI] ssh server-source -i loopback 0  //执行本命令前，必须已经成功创建LoopBack接口，且接口下已配置IP地址。
```

## 检查加固结果

执行命令**display ssh server status**，查看SSH服务器全局配置信息。

## 2.2.2.3 Web 网管方式登录交换机

## 攻击行为

- 拒绝服务式攻击

  Web Server支持的用户数有限，在用户登录达到上限后，其他用户将无法登录。这个可能是正常使用造成，也可能是攻击者造成。

- 慢连接攻击

  在HTTP的报文头中声明较大的content-length，也就是报文内容的长度。在提交了头以后，将后面的报文体部分卡住不发送，这时服务器在接受了长度以后，就会等待客户端发送剩余的内容，攻击者保持连接并且以10秒～100秒/字节的速度去发送大量报文，就达到了消耗资源的效果。

  受到攻击后，会出现Web用户登录慢、用户掉线、频繁断连、无法登录等现象。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- AAA认证

  Web Server支持AAA认证，只有通过认证的用户才能登录交换机，进入控制页面。用户在进行登录时，要求输入用户名、密码和随机生成的验证码，减小了帐号被破解的概率。

- 关闭服务

  当开启Web Server服务器时，交换机将开启Socket服务，易被攻击者扫描。当不使用Web Server时，可以关闭Web Server。

- 变更端口号

  缺省情况下，Web Server的端口号是80，端口号80属于知名端口号，易被扫描和攻击。可以修改Web Server的端口为私有端口，减小被扫描攻击的概率。

- ACL

  在系统视图可以配置Web Server的ACL过滤规则，通过ACL控制允许登录的客户端源IP和源端口号，其他用户不允许登录。

- HTTP over SSL

  提供安全的传输服务，防止传输的数据被窃听获取。HTTP存在安全风险，从V200R005版本开始，交换机仅支持通过安全HTTP（即HTTPS）登录Web网管，不支持通过HTTP登录Web网管。

  V200R020C00之前版本，HTTPS服务器端缺省接收来自所有接口登录连接请求，存在安全风险，建议使用**http server-source -i**命令指定HTTPS服务器端的源接口。V200R020C00及之后版本，HTTPS服务器端缺省仅接收来自管理网口MEth0/0/1或VLANIF1登录连接的请求，当需要授权客户可以从其他接口登录服务器时，可以使用**http server-source -i**命令指定HTTPS服务器端的源接口，不建议配置**http server-source all-interface**命令配置HTTPS服务器的源接口为设备上所有配置了IPv4地址的接口。

  成功指定HTTPS服务器端的源接口后，只允许用户通过指定的源接口下的地址登录设备，其它地址的访问将会被拒绝。已经登录到服务器的HTTPS IPv4用户会被强制下线，需要重新登录。

## 配置方法

- 配置AAA认证

  配置认证方式配置为AAA认证，并在AAA视图下配置用户名client001和密码YsHsjx_202206。

  ```
  <HUAWEI> system-view
  [HUAWEI] aaa
  [HUAWEI-aaa] local-user client001 password irreversible-cipher YsHsjx_202206
  [HUAWEI-aaa] local-user client001 privilege level 15
  [HUAWEI-aaa] local-user client001 service-type http
  ```

- 配置关闭HTTP服务功能

  ```
  <HUAWEI> system-view
  [HUAWEI] undo http server enable
  ```

- 变更服务器端口号为55535

  ```
  <HUAWEI> system-view
  [HUAWEI] http server port 55535
  ```

- 配置ACL 3000，HTTP引用ACL 3000，表示只允许源IP地址为10.10.10.1、源端口号为80的设备通过HTTP方式登录交换机

  ```
  <HUAWEI> system-view
  [HUAWEI] acl 3000
  [HUAWEI-acl-adv-3000] rule 5 permit tcp source 10.10.10.1 0 source-port eq 80
  [HUAWEI-acl-adv-3000] quit
  [HUAWEI] http acl 3000
  ```

- 配置HTTP over SSL

  ```
  <HUAWEI> system-view
  [HUAWEI] ssl policy https_der
  [HUAWEI-ssl-policy-https_der] certificate load pem-cert 1_servercert_pem_dsa.pem key-pair dsa key-file 1_serverkey_pem_dsa.pem auth-code cipher YsHsjx_202206
  [HUAWEI-ssl-policy-https_der] quit
  [HUAWEI] http secure-server ssl-policy https_der
  [HUAWEI] http secure-server enable
  ```

## 检查加固结果

执行命令**display http server**，查看当前HTTPS服务器信息。

## 2.2.3 AAA 用户管理的安全

### 攻击行为

黑客可以通过用户名、密码等关键信息进行遍历尝试来获取系统管理员的登录权限。

### 安全策略

针对这种常见的用户名、密码攻击和破解尝试，可配置用户可认证失败次数和可再次进行认证的时间间隔的参数来防止非法用户登录。配置了这两个参数后，在用户登录失败N次后，会暂时将用户阻塞一段时间，降低试探成功的机率，增强交换机的安全性。

### 配置方法

使能本地帐号锁定功能，配置用户的重试时间间隔为6分钟、连续输入错误密码的限制次数为4次及帐号锁定时间为6分钟。

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-aaa-user wrong-password retry-interval 6 retry-time 4 block-time 6  // 缺省情况下，本地帐号锁定功能处于使能状态，用户的重试时间间隔为5分钟、连续认证失败的限制次数为3次，帐号锁定时间为5分钟。
```

### 检查加固结果

执行命令**display aaa configuration**，查看AAA的概要信息，如域、认证方案、授权方案、计费方案的使用情况。

## 2.2.4 SNMP 管理设备的安全

### 攻击行为

SNMP常见的攻击有：

- 攻击者通过改变发送报文的源IP，获取到授权用户的权限，从而执行未经授权的管理操作。
- 拦截管理站和SNMP代理间的通信，获取到用户名、密码或者团体名等信息，获取非法授权。
- 拦截SNMP消息，进行重排序、延迟、重发，从而影响正常操作，直到攻击者获得非法的未授权访问权限。

### 安全策略

SNMP是用于管理网络设备的协议。SNMP有三个版本：SNMPv1、SNMPv2、SNMPv3。

SNMPv1、SNMPv2为不安全协议，支持ACL和VACM（基于视图的访问控制）。通过给团体名关联ACL和MIB视图，将允许访问设备的网管和允许访问的节点限定在一定范围内，从而在一定程度上提供了系统安全的保护。

对于SNMPv3，增加了支持USM（基于用户的安全模型）的安全机制，通过对通信的数据进行认证和加密，解决消息被伪装、篡改、泄密等安全问题。

## 配置方法

出于安全考虑，建议配置认证加密的v3用户，并使用v3认证加密方式来管理交换机。通过给用户关联ACL、MIB视图限制用户的访问权限。

1. 配置ACL 2001，拒绝源IP地址10.138.20.123通过，允许源IP地址10.138.90.111通过。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule 5 deny source 10.138.20.123 0
[HUAWEI-acl-basic-2001] rule 10 permit source 10.138.90.111 0
[HUAWEI-acl-basic-2001] quit
```

2. 配置SNMP的访问控制列表，基于ACL 2001对用户进行过滤，限制访问交换机的网管。

```
[HUAWEI] snmp-agent acl 2001
```

3. 配置MIB视图，view名是iso-view，可访问iso为根的子树下的节点。

```
[HUAWEI] snmp-agent mib-view included iso-view iso
```

4. 配置v3组，组名是v3group，关联的读视图、写视图、通知视图都为iso-view，并关联ACL 2001，基于用户组进行过滤。

```
[HUAWEI] snmp-agent group v3 v3group privacy read-view iso-view write-view iso-view notify-view iso-view acl 2001
```

5. 配置一个SNMPv3用户，用户名为v3user，归属于v3group组。该用户的认证算法为sha（HMAC-SHA-96），认证密码为YsHsjx_202207，加密算法为aes256（AES-256），加密密码为YsHsjx_202206，关联ACL 2001，基于用户和用户组进行过滤。

```
[HUAWEI] snmp-agent usm-user v3 v3user group v3group
[HUAWEI] snmp-agent usm-user v3 v3user group v3group acl 2001
[HUAWEI] snmp-agent usm-user v3 v3user authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
[HUAWEI] snmp-agent usm-user v3 v3user privacy-mode aes256
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
```

**说明**

V200R019C00版本，系统软件中不包含**sha**参数，如需使用，需要安装**V200R019SPH007**补丁或SHA1插件，但是该算法安全性低。为了保证更好的安全性，建议配置**sha2-256**参数（HMAC-SHA2-256-192算法）。

您可以通过华为官网（**企业**、**运营商**）搜索“插件使用指南”，请根据交换机型号及软件版本选择相应的《插件使用指南》。如无权限，请联系技术支持人员。

## 检查加固结果

执行命令**display current-configuration | include snmp**，查看当前SNMP配置。

# 2.2.5 禁用不安全的管理协议从业务平面接入

## 安全策略

交换机业务口默认支持管理协议，同时交换机支持专用的管理网口使用管理协议登录，如果客户网络有专门的管理面规划，仅通过专用管理网口对设备进行管理，可以禁止业务口使用管理协议对设备登录。

## 配置方法

对于有专用管理网口的交换机，在防攻击策略视图下使用**deny**命令将上送CPU的Telnet\SSH\HTTP\SNMP\FTP\Ping（ICMP）等管理协议动作设置为丢弃，可以限制管理协议从业务平面接入。

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy 1
[HUAWEI-cpu-defend-policy-1] deny packet-type telnet
[HUAWEI-cpu-defend-policy-1] deny packet-type ssh
[HUAWEI-cpu-defend-policy-1] deny packet-type http
[HUAWEI-cpu-defend-policy-1] deny packet-type snmp
[HUAWEI-cpu-defend-policy-1] deny packet-type ftp
[HUAWEI-cpu-defend-policy-1] deny packet-type icmp
[HUAWEI-cpu-defend-policy-1] quit
[HUAWEI] cpu-defend-policy 1 global
```

对于没有专用管理网口的交换机，只有通过各管理协议支持的ACL来限制登录IP。

以Telnet协议为例，在Telnet服务器端配置编号为2000的访问控制列表，拒绝源IP地址10.1.1.1登录到交换机。

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule deny source 10.1.1.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] telnet server acl 2000
```

## 检查加固结果

执行命令**display cpu-defend policy** [ *policy-name* ]，查看防攻击策略的配置信息。

# 2.2.6 管理平面防护 MPAC

## 攻击行为

在网络中，对于来自用户侧的报文，可能会对交换机造成如下影响：

- 上送CPU的报文过多，导致CPU占用率过高，性能下降，影响正常的业务。
- 对CPU的恶意攻击报文过多，导致CPU过于繁忙，从而影响其它业务正常运行，甚至导致系统中断。

## 安全策略

针对上述攻击行为，可以通过在子接口、主接口、全局进行MPAC策略的规则配置（包括允许或禁止某些协议的报文进行上送、允许或禁止符合某些源/目的IP地址的报文进行上送等）。

管理平面防护MPAC是一种主机防护技术。主机根据配置的相应管理平面接入控制策略对上送CPU的报文进行过滤，丢弃不必要的报文，从而防止恶意报文的攻击。

## 配置方法

配置基于IPv4的MPAC策略。

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 test  //创建一个IPv4 MPAC策略test
[HUAWEI-service-sec-test] rule 10 deny protocol ip source-ip 10.10.1.1 0
[HUAWEI-service-sec-test] quit
[HUAWEI] service-security global-binding ipv4 test  //全局应用控制接入策略test,可以在子接口、主接口、全局进行MPAC策略的规则配置，请根据需要选择
```

配置基于IPv6的MPAC策略。

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv6 test  //创建一个IPv6 MPAC策略test
[HUAWEI-service-sec-test] rule 10 deny protocol ip source-ip fc00::1/64
[HUAWEI-service-sec-test] quit
[HUAWEI] service-security global-binding ipv6 test  //全局应用控制接入策略test,可以在子接口、主接口、全局进行MPAC策略的规则配置，请根据需要选择
```

### 检查加固结果

执行命令**display service-security policy** { **ipv4** | **ipv6** } [ *security-policy-name* ]，查看MPAC策略的配置信息。

# 2.3 控制平面

## 2.3.1 本机防攻击

### 攻击行为

在网络中，存在着大量针对CPU的恶意攻击报文以及需要正常上送CPU的各类报文。针对CPU的恶意攻击报文会导致CPU长时间繁忙的处理攻击报文，从而引发其他业务的断续甚至系统的中断；大量正常的报文也会导致CPU占用率过高，性能下降，从而影响正常的业务。

### 安全策略

为了保护CPU，保证CPU对正常业务的处理和响应，交换机提供了本机防攻击功能。本机防攻击针对的是上送CPU的报文，主要用于保护设备自身安全，保证已有业务在发生攻击时的正常运转，避免设备遭受攻击时各业务的相互影响。

本机防攻击包括CPU防攻击、攻击溯源、端口防攻击和用户级限速四部分功能。

- CPU防攻击

  CPU防攻击可以针对上送CPU的报文进行限制和约束，使单位时间内上送CPU报文的数量限制在一定范围之内，从而保护CPU的安全，保证CPU对业务的正常处理。

  CPU防攻击的核心部分是CPCAR（Control Plane Committed Access Rate）功能。CPCAR通过对上送控制平面的不同业务的协议报文分别进行限速，来保护控制平面的安全。

- 攻击溯源

  攻击溯源可以针对DoS（Denial of Service）攻击进行防御。设备通过对上送CPU的报文进行分析统计，然后对统计的报文设置一定的阈值，将超过阈值的报文判定为攻击报文，再根据攻击报文信息找出攻击源用户或者攻击源接口，最后通过日志、告警等方式提醒管理员，以便管理员采用一定的措施来保护设备，或者直接丢弃攻击报文以对攻击源进行惩罚。

- 端口防攻击

  端口防攻击是针对DoS攻击的另一种防御方式。它基于端口维度进行防御，可以避免攻击端口的协议报文挤占带宽，导致其他端口的协议报文无法正常上送CPU处理而造成业务中断。

设备默认开启常见用户协议如ARP、ICMP、DHCP、IGMP的端口防攻击功能，在用户攻击发生时可以自动将攻击影响隔离到端口范围内，减少对其它端口的影响。

- 用户级限速

  用户级限速指的是基于用户MAC地址识别用户，然后对用户的特定协议报文（ARP/ND/DHCP Request/DHCPV6 Request/IGMP/8021x/HTTPS-SYN）进行限速，使得单个用户在受到DoS攻击的情况下，只影响本用户，不对其他用户带来影响。用户级限速的核心部分是HOST-CAR功能。缺省情况下，已经使能用户级限速功能。

## 配置方法

- 修改协议的CPCAR值

  **说明**

  调整CPCAR不当将会影响网络业务，如果需要调整CPCAR，建议联系技术支持工程师处理。

  通过减小协议CPCAR值或者设置协议CPCAR为**deny**，可以限制一些设备不需要处理或者优先级低的报文上送，保证系统正常运行。

  修改ICMP报文上送速率为64kbps，丢弃TTL-expired的上送报文。

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy 1
[HUAWEI-cpu-defend-policy-1] car packet-type icmp cir 64
[HUAWEI-cpu-defend-policy-1] deny packet-type ttl-expired
[HUAWEI-cpu-defend-policy-1] quit
[HUAWEI] cpu-defend-policy 1 global
[HUAWEI] cpu-defend-policy 1
```

- 配置黑名单禁止指定用户的协议报文上送

  在发现某协议CPCAR速率异常增大时，可以怀疑有用户的异常大流量上送，此时通过获取报文可以定位出大流量用户流量的特征，如果是固定源IP或固定源MAC等特征，则可以通过配置黑名单阻止异常流量的上送。

  禁止指定源MAC的ARP报文上送。

```
<HUAWEI> system-view
[HUAWEI] acl number 4000
[HUAWEI-acl-L2-4000] rule 10 permit l2-protocol 0x0806 0xffff source-mac 00e0-fc12-3456 ffff-ffff-ffff
[HUAWEI-acl-L2-4000] quit
[HUAWEI] cpu-defend policy 1
[HUAWEI-cpu-defend-policy-1] blacklist 1 acl 4000
[HUAWEI-cpu-defend-policy-1] quit
[HUAWEI] cpu-defend-policy 1 global
```

- 配置攻击溯源自动检测攻击源并进行防御

  攻击溯源功能可以实现自动检测攻击源和防御，提前规划和部署好攻击溯源可以大大提高现网运行安全性，在攻击发生时隔离攻击源，减少攻击对业务的影响。V200R009版本以及之后版本攻击溯源功能默认已经使能，不需要特意部署。

  针对ARP报文配置攻击溯源进行自动防御，配置每秒中采样到超过50pps认为发生了攻击，对该用户进行自动惩罚。

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy 1
[HUAWEI-cpu-defend-policy-1] auto-defend enable
[HUAWEI-cpu-defend-policy-1] auto-defend attack-packet sample 5
[HUAWEI-cpu-defend-policy-1] auto-defend threshold 50
[HUAWEI-cpu-defend-policy-1] auto-defend trace-type source-ip source-mac source-portvlan
[HUAWEI-cpu-defend-policy-1] auto-defend protocol arp
[HUAWEI-cpu-defend-policy-1] auto-defend action deny timer 300
```

```
[HUAWEI-cpu-defend-policy-1] auto-defend whitelist 1 interface gigabitethernet 1/0/0
[HUAWEI-cpu-defend-policy-1] quit
[HUAWEI] cpu-defend-policy 1 global
[HUAWEI] cpu-defend-policy 1
```

### 检查加固结果

执行命令**display cpu-defend policy** [ *policy-name* ]，查看防攻击策略的配置信息。

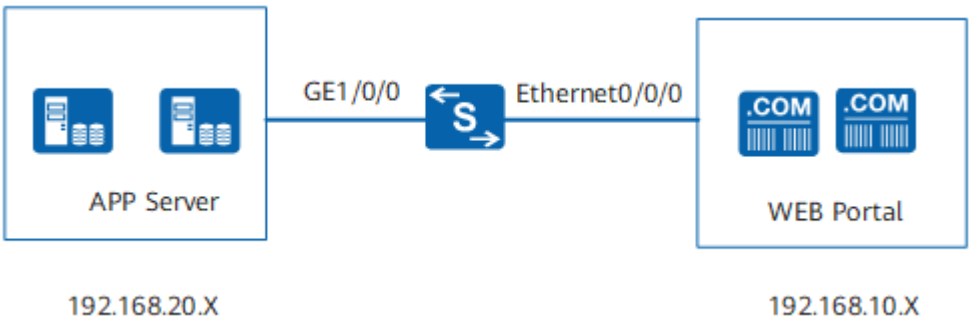
## 2.3.2 通过业务与管理隔离进行防攻击

### 攻击行为

如图2-1所示，192.168.10.X网段设备和交换机独立管理网口Ethernet0/0/0相连，并可以正常登录设备；192.168.20.X网段设备和交换机的业务口GE1/0/0相连，并可以正常登录设备。

如果不进行管理网口隔离，会出现192.168.20.X设备可以Ping通192.168.10.X设备现象，导致管理网口地址泄露，容易被攻击。

**图 2-1** 组网图




### 安全策略

为提高网络安全性，防止非法用户的攻击，系统默认将业务与管理进行隔离。

- **management-port isolate enable**命令用来使能管理口隔离功能，防止非法用户对转发报文进行攻击。设备将禁止管理口和业务口之间转发报文，即从管理口收到的报文不会从业务口转发出去，同样，从业务口收到的报文也不会从管理口转发出去。
- **management-plane isolate enable**命令用来使能管理面隔离功能，防止非法用户通过业务网络对管理网络造成攻击。设备将禁止非法用户通过业务口访问管理口，即业务口接收到目的地址是管理口地址的报文不能访问设备，反之，从管理口到业务口的访问则不做限制。

**说明**

以上提到的报文是指IP报文和MPLS报文。

### 配置方法

使能管理口隔离功能。

```
<HUAWEI> system-view
[HUAWEI] management-port isolate enable  //缺省情况下，该功能已使能
```

使能管理面隔离功能。

```
<HUAWEI> system-view
[HUAWEI] management-plane isolate enable  //缺省情况下，该功能已使能
```

### 检查加固结果

执行命令**display current-configuration | include management-plane isolate**，查看管理口隔离功能是否使能。

## 2.3.3 攻击防范

攻击防范是一种重要的网络安全特性。它通过分析上送CPU处理的报文的内容和行为，判断报文是否具有攻击特性，并配置对具有攻击特性的报文执行一定的防范措施。攻击防范主要分为畸形报文攻击防范、分片报文攻击防范和泛洪攻击防范。

### 2.3.3.1 畸形报文攻击防范

### 攻击行为

畸形报文攻击是通过向交换机发送有缺陷的IP报文，使得交换机在处理这样的IP包时会出现崩溃，给交换机带来损失。

畸形报文攻击主要有如下几种：

- 没有IP载荷的泛洪攻击
- IGMP空报文攻击
- LAND攻击
- Smurf攻击
- TCP标志位非法攻击

### 安全策略

为了避免交换机被畸形报文攻击导致瘫痪，保证正常的网络服务，可以配置畸形报文攻击防范。交换机对畸形报文攻击防范的主要措施是判断是否是几种畸形报文攻击报文类型之一，若是，则直接丢弃畸形报文。

### 配置方法

使能畸形报文攻击防范功能（缺省情况下，该功能处于使能状态）。

```
<HUAWEI> system-view
[HUAWEI] anti-attack abnormal enable
```

### 检查加固结果

执行命令**display anti-attack statistics abnormal**，查看畸形报文攻击防范的统计数据。

### 2.3.3.2 分片报文攻击防范

#### 攻击行为

攻击者通过向交换机发送分片出错的报文，使得交换机在处理分片错误的报文时消耗大量的CPU资源，给交换机带来损失。

分片报文攻击主要有如下几种：

- 分片数量巨大攻击
- 巨大offset攻击
- 重复分片攻击
- Tear Drop攻击
- Syndrop攻击
- NewTear攻击
- Bonk攻击
- Nesta攻击
- Rose攻击
- Fawx攻击
- Ping of Death攻击
- Jolt攻击

#### 安全策略

为了避免交换机被分片报文攻击导致瘫痪，保证正常的网络服务，可以配置分片报文攻击防范。对分片报文攻击防范的主要措施是进行速率限制，防止大量的分片报文造成CPU繁忙，保证CPU在造成攻击的情况下正常运行。

#### 配置方法

使能分片报文攻击防范功能（缺省情况下，该功能处于使能状态）。

```
<HUAWEI> system-view
[HUAWEI] anti-attack fragment enable
[HUAWEI] anti-attack fragment car cir 8000  //限制分片报文接收的速率，缺省情况下，分片报文的接收速率为155000000bit/s。
```

#### 检查加固结果

执行命令**display anti-attack statistics fragment**，查看分片报文攻击防范的统计数据。

### 2.3.3.3 TCP SYN 泛洪攻击防范

#### 攻击行为

TCP SYN泛洪攻击是一种古老而有效的攻击方式。它属于拒绝服务攻击，这类攻击完全依赖于TCP连接的建立方式。

攻击者向交换机发送SYN报文，然后对于交换机返回的SYN+ACK报文不作回应。交换机如果没有收到攻击者的ACK回应，就会一直等待，形成半连接。攻击者利用这种方式，让交换机上生成大量的半连接，迫使其大量资源浪费在这些半连接上。

## 安全策略

为了避免TCP SYN泛洪攻击，可以在交换机上配置TCP SYN泛洪攻击防范功能，通过限制TCP SYN报文的发送速率来防范TCP SYN泛洪攻击，保证受到攻击时系统资源不被耗尽。

## 配置方法

使能TCP SYN泛洪攻击防范功能（缺省情况下，该功能处于使能状态）。

```
<HUAWEI> system-view
[HUAWEI] anti-attack tcp-syn enable
[HUAWEI] anti-attack tcp-syn car cir 8000  //限制TCP SYN报文接收的速率。缺省情况下，TCP SYN报文接收的速率为155000000bit/s。
```

## 检查加固结果

执行命令**display anti-attack statistics tcp-syn**，查看TCP Syn报文攻击防范的统计数据。

### 2.3.3.4 UDP 泛洪攻击防范

## 攻击行为

- Fraggle攻击

  Fraggle攻击的原理是利用UDP 7号端口，7端口的服务和ICMP echo基本一样，都是把收到的报文载荷原封不动的回复回去，以测试源和目的之间的网络状况。和Smurf攻击的原理一样，把源地址伪造成受害者地址，目的地址写成某个广播地址，目的端口为7，源端口可以不是7，也可以是7。如果该广播网络有很多主机都启用了UDP echo服务，那么受害者将收到很多回复报文，达到攻击的效果。

- UDP诊断端口攻击

  对诊断端口（7-echo，13-daytime，19-Chargen等）随机发包，如果同时发送的数据包数量很大，造成泛洪，可能影响网络设备正常工作。很多设备厂家都会默认打开一些端口，以进行网络诊断、设备管理等作用，但同时也是暴露给攻击者一个很好的攻击机会。

## 安全策略

为了避免UDP泛洪攻击，可以在交换机上配置UDP泛洪攻击防范功能。交换机上配置UDP泛洪攻击防范功能，对于端口号为7、13和19的报文，直接丢弃。

## 配置方法

使能UDP泛洪攻击防范功能（缺省情况下，该功能处于使能状态）。

```
<HUAWEI> system-view
[HUAWEI] anti-attack udp-flood enable
```

### 检查加固结果

执行命令**display anti-attack statistics udp-flood**，查看UDP泛洪报文攻击防范的统计数据。

## 2.3.3.5 ICMP 泛洪攻击防范

### 攻击行为

如果攻击者在短时间内向交换机发送大量的ICMP响应请求报文，使交换机忙于回复这些请求，会造成交换机负担过重而不能处理正常的业务。

### 安全策略

为了避免ICMP泛洪攻击，可以在交换机上配置ICMP泛洪攻击防范功能。交换机上配置ICMP泛洪攻击防范功能，通过限制ICMP报文的速率来防范ICMP泛洪攻击。

### 配置方法

使能ICMP泛洪攻击防范功能（缺省情况下，该功能处于使能状态）。

```
<HUAWEI> system-view
[HUAWEI] anti-attack icmp-flood enable
[HUAWEI] anti-attack icmp-flood car cir 8000  //限制ICMP泛洪攻击报文接收的速率，缺省情况下，ICMP泛洪攻击报文接收的速率为155000000bit/s。
```

### 检查加固结果

执行命令**display anti-attack statistics icmp-flood**，查看ICMP泛洪报文攻击防范的统计数据。

# 2.3.4 无线用户接入安全

WLAN安全提供了WEP、WPA、WPA2、WPA3和WAPI四种安全策略机制。WEP使用共享密钥认证用户和加密业务报文，但易被破解，安全性低，不建议使用。

另外，交换机支持STA黑白名单功能，通过黑白名单功能设定一定的规则过滤无线客户端，实现对无线客户端的接入控制，以保证合法客户端能够正常接入WLAN网络，避免非法客户端强行接入WLAN网络。

## 2.3.4.1 WPA/WPA2

### 安全策略

由于WEP共享密钥认证采用的是基于RC4对称流的加密算法，需要预先配置相同的静态密钥，无论从加密机制还是从加密算法本身，都很容易受到安全威胁。为了解决这个问题，在802.11i标准没有正式推出安全性更高的安全策略之前，Wi-Fi联盟推出了针对WEP改良的WPA。WPA的核心加密算法还是采用RC4，在WEP基础上提出了临时密钥完整性协议TKIP（Temporal Key Integrity Protocol）加密算法，采用了802.1X的身份验证框架，支持EAP-PEAP、EAP-TLS等认证方式。随后802.11i安全标准组织又推出WPA2，区别于WPA，WPA2采用安全性更高的区块密码锁链-信息真实性检查码协议CCMP（Counter Mode with CBC-MAC Protocol）加密算法。

为了实现更好的兼容性，在目前的实现中，WPA和WPA2都可以使用802.1X的接入认证、TKIP或CCMP的加密算法，它们之间的不同主要表现在协议报文格式上，在安全性上几乎没有差别。

综上所述，WPA/WPA2安全策略涉及了链路认证阶段、接入认证阶段、密钥协商和数据加密阶段。

WPA/WPA2有两种认证方式：WPA/WPA2-PSK认证、WPA/WPA2-802.1X认证。

- WPA/WPA2-PSK认证

  WPA和WPA2都可以使用PSK认证，支持TKIP或AES两种加密算法，它们之间的不同主要表现在协议报文格式上，在安全性上几乎没有差别。

  WPA/WPA2-PSK认证主要用于个人、家庭与小型SOHO网络，对网络安全要求相对较低，不需要认证服务器。如果无线终端只支持WEP加密，则升级为PSK+TKIP无需升级硬件，而升级为PSK+AES可能需要升级硬件。

- WPA/WPA2-802.1X认证

  WPA和WPA2都可以使用802.1X认证，支持TKIP或AES两种加密算法，它们之间的不同主要表现在协议报文格式上，在安全性上几乎没有差别。

  WPA/WPA2-802.1X认证主要用于企业网络等安全要求较高的网络，需要独立的认证服务器。如果用户的设备只支持WEP加密，则升级为802.1X+TKIP无需升级硬件，而升级为802.1X+AES可能需要升级硬件。

无线终端的种类多种多样，支持的认证和加密方式也有所差异，为了便于多种类型的终端接入，方便网络管理员的管理，可以使用混合方式配置WPA和WPA2。配置安全策略为WPA-WPA2，则支持WPA或WPA2的终端都可以接入设备进行认证；配置加密方式为TKIP-AES，则支持TKIP加密或AES加密的终端都可以对业务报文进行加密。

## 配置方法

- 配置WPA/WPA2-PSK认证

  配置WPA-WPA2混合方式，使用AES和TKIP混合加密，认证方式为预共享密钥。

  ```
  <HUAWEI> system-view
  [HUAWEI] wlan
  [HUAWEI-wlan-view] security-profile name p1
  [HUAWEI-wlan-sec-prof-p1] security wpa-wpa2 psk pass-phrase YsHsjx_202206 aes-tkip
  ```

- 配置WPA/WPA2-802.1X认证

  配置WPA-WPA2混合方式，使用AES和TKIP混合加密，认证方式为802.1X。

  ```
  <HUAWEI> system-view
  [HUAWEI] wlan
  [HUAWEI-wlan-view] security-profile name p1
  [HUAWEI-wlan-sec-prof-p1] security wpa-wpa2 dot1x aes-tkip
  ```

## 检查加固结果

- 执行命令**display security-profile** { **all** | **name** *profile-name* }，查看安全模板的信息。
- 执行命令**display references security-profile name** *profile-name*，查看安全模板的引用信息。

### 2.3.4.2 WPA3

## 安全策略

相较于WPA/WPA2，WPA3主要在以下几个方面有所改进：

- 新增支持WPA3-SAE，提供更安全的握手协议。理论上SAE握手协议能够提供前向保密，即使攻击者知道了网络中的密码，也不能解密获取到流量。而在WPA2网络中，在得到密码后就可以解密之前获取的流量。所以，WPA3的SAE握手协议在这方面做出了很大的改进。
- 加强了算法强度，支持安全套件Suite B，也就是WPA3支持256位密钥的AES-GCM和384位曲线的椭圆曲线加密。

和WPA/WPA2类似，根据不同的使用场景和安全性要求，WPA3也可以分为企业版和个人版，即WPA3-802.1X和WPA3-SAE。

WPA3个人版引入了SAE握手协议，和WPA/WPA2-PSK认证相比，可以有效地抵御离线字典攻击，增加暴力破解的难度，并且SAE握手协议能够提供前向保密，即使攻击者知道了网络中的密码，也不能解密获取到流量，大大提升了WPA3个人网络的安全。

WPA3企业版仍然使用WPA2企业版的认证体系，采用可扩展认证协议EAP的方法进行身份验证，但是在算法强度上WPA3做了加强，将加密套件更换成了美国国家安全局定义的CNSA（Commercial National Security Algorithm）套件，CNSA套件具有强大的加密算法，被用在对安全性要求极高的场合。

WPA3企业版支持安全套件Suite B，该安全套件使用192 bit最小安全，支持GCMP-256（伽罗瓦/反模式协议，Galois Counter Mode Protocol）、GMAC-256（GCMP的伽罗瓦消息认证码，Galois Message Authentication Code）和SHA384。

由于WPA2仍在广泛使用，为了能兼容暂时不支持WPA3的终端能接入WPA3网络，Wi-Fi联盟规定了WPA3的过渡模式，即WPA3和WPA2在未来的一段时间里可以共存。该模式仅针对WPA3个人版，WPA3企业版不支持过渡模式。

针对于开放性Wi-Fi网络，WPA3也在OPEN认证的基础上做了升级，提出了OWE认证。OWE认证是基于机会性无线加密算法OWE（Opportunistic wireless encryption）的新一代开放网络认证方式，也叫做增强型开放网络认证（enhanced-open）。用户无需输入密码即可加入网络，设备使用AES加密算法对网络中的数据进行加密，保护用户设备与Wi-Fi网络之间的数据交换。

OWE认证过程与SAE认证过程相似，但是OWE省去了密码的维护，使用Diffie–Hellman协议进行密钥交换，生成用于后续四次握手过程的PMK。在确保开放性网络的便捷性的同时，OWE认证也保证了开放型网络的数据安全性。

由于部分终端不支持OWE认证，为了兼容此类终端，OWE还支持过渡模式，即不支持OWE认证的终端将以OPEN方式接入，支持OWE认证的终端将以OWE方式接入。OWE过渡模式认证仅支持AES加密方式。

V200R020C10及以后版本支持WPA3和OWE认证。

## 配置方法

- 配置WPA3-SAE认证，配置用户口令为YsHsjx_202206。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa3 sae pass-phrase YsHsjx_202206 aes
```

- 配置WPA3-802.1X认证方式。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa3 dot1x gcmp256
```

- 配置WPA2和WPA3认证，配置用户口令为YsHsjx_202206。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wpa2-wpa3 psk-sae pass-phrase YsHsjx_202206 aes
```

- 配置OWE认证。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security enhanced-open aes
```

- 配置OWE过渡模式认证，其中OPEN认证的SSID为wlan-net。

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security enhanced-open aes transition-ssid wlan-net
```

## 检查加固结果

- 执行命令**display security-profile** { **all** | **name** *profile-name* }，查看安全模板的信息。
- 执行命令**display references security-profile name** *profile-name*，查看安全模板的引用信息。

### 2.3.4.3 WAPI

## 安全策略

无线局域网鉴别与保密基础结构WAPI是中国提出的以802.11无线协议为基础的无线安全标准。WAPI能够提供比WEP和WPA更强的安全性，WAPI协议由以下两部分构成：

- 无线局域网鉴别基础结构WAI：用于无线局域网中身份鉴别和密钥管理的安全方案；
- 无线局域网保密基础结构WPI：用于无线局域网中数据传输保护的安全方案，包括数据加密、数据鉴别和重放保护等功能。

WAPI采用了基于公钥密码体制的椭圆曲线密码算法和对称密码体制的分组密码算法，分别用于无线设备的数字证书、证书鉴别、密钥协商和传输数据的加解密，从而实现设备的身份鉴别、链路验证、访问控制和用户信息的加密保护。

WAPI有两种认证方式：WAPI-PSK认证、WAPI-证书认证。

- WAPI-PSK认证

  WAPI-PSK认证，适用于家庭用户或小型企业网络，不需要额外的证书系统。

- WAPI-证书认证

  WAPI-证书认证，适用于大型企业网络或运营商网络，这种认证方式需要部署和维护昂贵的证书系统。WAPI证书采用X.509 V3证书，X.509 V3证书以Base64 binary为编码类型，以PEM格式进行存储，文件名的后缀为.cer。在为WAPI导入证书前，请确保证书文件存放在存储器的根目录。

WAPI定义了密钥的动态协商，但是如果STA长时间使用相同的加密密钥，仍然存在安全隐患。WAPI提供基于时间的密钥更新机制，单播会话密钥USK和组播会话密钥MSK都具有生命周期，当其生命周期结束时需要更新密钥。

## 配置方法

- 配置WAPI-PSK认证

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wapi psk pass-phrase YsHsjx_202206  //配置认证方式为PSK认证并输入密钥
```

- 配置WAPI-证书认证

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] security-profile name p1
[HUAWEI-wlan-sec-prof-p1] security wapi certificate  //配置认证方式为WAPI-证书认证
[HUAWEI-wlan-sec-prof-p1] wapi import certificate ac format pem file-name flash:/ae.cer  //加载AC的证书
[HUAWEI-wlan-sec-prof-p1] wapi import certificate asu format pem file-name flash:/as.cer  //加载ASU的证书
[HUAWEI-wlan-sec-prof-p1] wapi import certificate issuer format pem file-name flash:/as.cer  //加载颁发者的证书
[HUAWEI-wlan-sec-prof-p1] wapi import private-key format pem file-name flash:/ae.cer  //导入AC的私钥文件
[HUAWEI-wlan-sec-prof-p1] wapi asu ip 10.164.10.10  //配置ASU服务器IP地址10.164.10.10
```

## 检查加固结果

执行命令**display wlan wapi certificate file-name** *file-name*，查看WAPI-证书认证时导入的证书内容。

## 2.3.4.4 STA 黑白名单

## 安全策略

在WLAN网络环境中，可以通过黑白名单功能设定一定的规则过滤无线客户端，实现对无线客户端的接入控制，以保证合法客户端能够正常接入WLAN网络，避免非法客户端强行接入WLAN网络。

- 白名单列表：

  允许接入WLAN网络的STA的MAC地址列表。使能白名单功能后，只有匹配白名单列表的用户可以接入无线网络，其他用户都无法接入无线网络。

- 黑名单列表：

  拒绝接入WLAN网络的STA的MAC地址列表。使能黑名单功能后，匹配黑名单列表的用户无法接入无线网络，其他用户都可以接入无线网络。

**说明**

如果使能了STA白名单或黑名单，但其名单列表为空，则所有用户都可以接入无线网络。

## 配置方法

在交换机上可以配置多个STA黑白名单模板，引用到不同的VAP模板或者AP系统模板。对于一个VAP模板或者AP系统模板，同一时间仅能应用STA白名单生效或者STA黑名单生效。

- 配置STA白名单
  a. 配置STA白名单模板

```
<HUAWEI> system-view
[HUAWEI] wlan
```

```
[HUAWEI-wlan-view] sta-whitelist-profile name sta-whitelist-profile1  //创建名称为“sta-whitelist-profile1”的白名单模板
[HUAWEI-wlan-whitelist-prof-sta-whitelist-profile1] sta-mac 00E0-FC12-3456  //添加一个STA的MAC地址
[HUAWEI-wlan-whitelist-prof-sta-whitelist-profile1] quit
```

b. 应用配置到VAP模板或AP系统模板。用户根据需要选择应用到哪个模板。

- 应用配置到VAP模板

```
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1  //创建名称为“vap1”的VAP模板
[HUAWEI-wlan-vap-prof-vap1] sta-access-mode whitelist sta-whitelist-profile1  //将名称为“sta-whitelist-profile1”的STA白名单模板引用到名称为“vap1”的VAP模板
```

- 应用配置到AP系统模板

```
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1  //创建名称为“ap-system1”的AP系统模板
[HUAWEI-wlan-ap-system-prof-ap-system1] sta-access-mode whitelist sta-whitelist-profile1  //将名称为“sta-whitelist-profile1”的STA白名单模板引用到名称为“ap-system1”的AP模板
```

- 配置STA黑名单

a. 配置STA黑名单模板

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] sta-blacklist-profile name sta-blacklist-profile1  //创建名称为“sta-blacklist-profile1”的黑名单模板
[HUAWEI-wlan-blacklist-prof-sta-blacklist-profile1] sta-mac 00E0-FC34-5678  //添加一个STA的MAC地址
```

b. 应用配置到VAP模板或AP系统模板。用户根据需要选择应用到哪个模板。

- 应用配置到VAP模板

```
<HUAWEI> system-view
[HUAWEI] wlan
[HUAWEI-wlan-view] vap-profile name vap1  //创建名称为“vap1”的VAP模板
[HUAWEI-wlan-vap-prof-vap1] sta-access-mode blacklist sta-blacklist-profile1  //将名称为“sta-blacklist-profile1”的STA黑名单模板引用到名称为“vap1”的VAP模板
```

- 应用配置到AP系统模板

```
[HUAWEI] wlan
[HUAWEI-wlan-view] ap-system-profile name ap-system1  //创建名称为“ap-system1”的AP系统模板
[HUAWEI-wlan-ap-system-prof-ap-system1] sta-access-mode blacklist sta-blacklist-profile1  //将名称为“sta-blacklist-profile1”的STA黑名单模板引用到名称为“ap-system1”的AP模板
```

## 检查加固结果

- 执行命令**display sta-whitelist-profile** { **all** | **name** *profile-name* }，查看STA白名单模板的信息。
- 执行命令**display sta-blacklist-profile** { **all** | **name** *profile-name* }，查看STA黑名单模板的信息。
- 执行命令**display references sta-whitelist-profile name** *profile-name*，查看STA白名单模板的引用信息。
- 执行命令**display references sta-blacklist-profile name** *profile-name*，查看STA黑名单模板的引用信息。

# 2.4 转发平面

## 2.4.1 访问控制列表 ACL

### 安全策略

通过ACL可以实现对网络中报文流的精确识别和控制，达到控制网络访问行为、防止网络攻击和提高网络带宽利用率的目的，从而切实保障网络环境的安全性和网络服务质量的可靠性。

访问控制列表ACL是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。ACL通过规则对数据包进行分类，这些规则应用到交换机上，交换机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。例如可以用访问列表描述：拒绝任何用户终端使用Telnet登录本机，允许每个用户终端经由SMTP向本机发送电子邮件。

每个ACL中可以定义多个规则，根据规则的功能分为：基本ACL、基本ACL6、高级ACL、高级ACL6、二层ACL和用户自定义ACL。

其中：

- 基本ACL、基本ACL6、二层ACL属于Level-1级别
- 高级ACL、高级ACL6、用户自定义ACL属于Level-2级别

本节内容只介绍Level-1级别的ACL，Level-2级别的ACL请参看**3.3.1 访问控制列表 ACL**。

**表2-5**所示，基于ACL规则定义方式的划分如下。

**表 2-5** 基于 ACL 规则定义方式的 ACL 分类

| 分类 | 适用的IP版本 | 规则定义描述 | 编号范围 |
| --- | --- | --- | --- |
| 基本ACL | IPv4 | 仅使用报文的源IP地址、分片信息和生效时间段信息来定义规则。 | 2000～2999 |
| 二层ACL | IPv4&IPv6 | 使用报文的以太网帧头信息来定义规则，如根据源MAC（Media Access Control）地址、目的MAC地址、二层协议类型等。 | 4000～4999 |
| 基本ACL6 | IPv6 | 可使用IPv6报文的源IPv6地址、分片信息和生效时间段来定义规则。 | 2000～2999 |

### 配置方法

配置ACL 2001，允许源地址是192.168.32.1的报文通过。

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.32.1 0
```

### 检查加固结果

- 执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }，查看ACL的配置信息。
- 执行命令**display acl ipv6** { *acl6-number* | **name** *acl6-name* | **all** }，查看ACL6的配置信息。

## 2.4.2 流量抑制及风暴控制

### 安全策略

当交换机某个二层以太接口收到广播、组播或未知单播报文时，如果根据报文的目的MAC地址交换机不能明确报文的出接口，交换机会向同一VLAN内的其他二层以太接口转发这些报文，这样可能导致广播风暴，降低交换机转发性能。

引入流量抑制和风暴控制特性，可以控制这三类报文流量，防范广播风暴。

流量抑制主要通过配置阈值来限制流量，而风暴控制则主要通过关闭端口来阻断流量。

在树形组网端口下挂用户网络时，建议配置风暴控制，防止用户网络风暴影响整个网络。网络内部互联接口建议配置流量抑制，减少异常环路的广播风暴对整网业务的影响。

### 配置方法

- 配置接口流量抑制

  为了限制出入接口的广播、组播或未知单播类型报文的速率，防止广播风暴，可以在该接口上配置对应报文类型的流量抑制功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] broadcast-suppression 30
  [HUAWEI-GigabitEthernet1/0/1] multicast-suppression 30
  [HUAWEI-GigabitEthernet1/0/1] unicast-suppression 30
  [HUAWEI-GigabitEthernet1/0/1] quit
  ```

- 配置风暴控制

  为了限制进入接口的广播、组播或未知单播类型报文的速率，避免交换机受到大流量的冲击，可以在该接口上配置对应报文类型的风暴控制功能，在检测到流量超过阈值时系统会对该端口实施惩罚，以便隔离风暴对网络的影响。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] storm-control broadcast min-rate 5000 max-rate 8000
  [HUAWEI-GigabitEthernet1/0/1] storm-control action error-down
  [HUAWEI-GigabitEthernet1/0/1] storm-control enable trap
  ```

### 检查加固结果

- 执行命令**display flow-suppression interface** *interface-type interface-number*，查看流量抑制配置信息。
- 执行命令**display storm-control** [ **interface***interface-type interface-number* ]，查看接口的风暴控制信息。

# 2.4.3 基于可信路径的转发

## 安全策略

URPF根据报文的源IP地址查找路由表中是否存在去往该地址的路由，并判断报文入接口与路由出接口是否一致。如果路由表不存在去往该源IP地址的路由或报文入接口与路由出接口不一致，则丢弃该报文，从而预防IP欺骗。该策略针对伪造源IP地址的DoS攻击非常有效。

## 配置方法

在复杂的网络环境中，会遇到路由不对称的情况，即对端交换机记录的路由路径与本端不一致，此时使能URPF的交换机可能会丢弃从合法路径接收的报文，正常转发从非法路径接收的报文。为了解决该问题，交换机实现了以下两种URPF模式：

- **严格模式**

  严格模式下，交换机不仅要求路由表中存在去往报文源IP地址的路由，还要求报文入接口与路由出接口一致。

  建议在路由对称的环境下使用严格模式。例如两个网络边界交换机之间只有一条路径，此时使用严格模式能够保证网络的安全性。

- **松散模式**

  松散模式下，交换机仅要求路由表中存在去往报文源IP地址的路由，不要求报文入接口与路由出接口一致。

  建议在不能保证路由对称的环境下使用松散模式。例如两个网络边界交换机之间有多条路径，路由的对称性无法保证，此时松散模式既可以有效地阻止网络攻击，又可以避免合法报文被错误丢弃。

在二层接口GE1/0/1上使能URPF严格检查，并允许去往报文源IP地址的路由为缺省路由。

```
<HUAWEI> system-view
[HUAWEI] interface GigabitEthernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] urpf strict allow-default-route
```

## 检查加固结果

执行命令**display current-configuration interface**，查看接口下的配置。

# 3 Level-2 的安全加固策略（选配）



## 3.1 管理平面

### 3.1.1 信息中心的安全

#### 安全策略

当用户需要监控的交换机不在本地且需要查询该交换机产生的信息时，可以在该交换机上配置信息输出到日志主机，以方便用户在日志主机侧接收设备产生的信息。执行命令**info-center loghost**可以配置信息输出到日志主机。为了提高日志传输的安全性，需要选择参数**ssl-policy** *policy-name*配置基于TCP模式的SSL加密方式。

**说明**

V200R005版本以及之后版本支持ssl-policy policy-name参数。

#### 配置方法

向IPv4地址为192.168.2.2的日志主机发送信息。信息采用TCP模式进行传输，通过SSL策略进行加密，引用已创建好的SSL策略Example@123。

```
<HUAWEI> system-view
[HUAWEI] ssl policy Example@123
[HUAWEI-ssl-policy-Example@123] quit
[HUAWEI] info-center loghost 192.168.2.2 transport tcp ssl-policy Example@123
```

#### 检查加固结果

- 执行命令**display current-configuration | include info-center loghost**，查看日志主机是否已绑定SSL策略。
- 执行命令**display ssl policy**，查看SSL策略的配置信息。

## 3.1.2 HWTACACS 用户管理的安全

### 安全策略

HWTACACS是在TACACS+基础上进行了功能增强的一种安全协议。该协议与RADIUS协议类似，主要是通过“客户端—服务器”模式与HWTACACS服务器通信来实现多种用户的AAA功能，可用于PPP和Login用户的认证、授权和计费。

HWTACACS使用TCP协议传输，相对于采用UDP的RADIUS传输更可靠；同时除了对标准的HWTACACS报文头外，对报文主体全部进行MD5加密，保证了传输过程中高安全性，支持对报文加密的共享密钥可以由用户配置。

### 配置方法

配置共享密钥为YsHsjx_202206，该密钥用于对HWTACACS传输的报文进行MD5加密，增加传输安全性。同时配置密钥的时候采用**cipher**关键字，查看配置的时候显示的是经过加密以后的密钥，增加密钥的安全性。

```
<HUAWEI> system-view
[HUAWEI] hwtacacs-server template test1
[HUAWEI-hwtacacs-test1] hwtacacs-server shared-key cipher YsHsjx_202206
```

### 检查加固结果

执行命令**display hwtacacs-server template** *template-name* **verbose**，查看HWTACACS认证、计费、授权的统计信息。

## 3.1.3 链路层安全

### 攻击行为

一般情况下，绝大部分数据在局域网链路中都是以明文形式传输的，这样就会存在许多安全隐患，比如：银行帐户的信息被窃取、篡改，遭受恶意网络攻击等。

### 安全策略

针对上述攻击行为，可以部署MACsec功能。网络中部署MACsec后，可对传输的以太网数据帧进行保护，降低信息泄露和遭受恶意网络攻击的风险。

MACsec是基于802.1AE和802.1X协议的局域网上的安全通信方法。它通过身份认证、数据加密、完整性校验、重播保护等功能保证以太网数据帧的安全性，防止设备处理有安全威胁的报文。

MACsec采用插件化交付方式，系统软件中不包含上述功能，需单独加载相应的插件。缺省情况下，交换机不支持MACsec功能。从V200R009版本开始，加载MACsec插件后支持MACsec功能。

### 配置方法

关于MACSec的配置方法，您可以通过华为官网浏览和获取MACsec的相关资料，搜索“插件使用指南”，请根据交换机型号及软件版本选择相应的《插件使用指南》。如无权限，请联系技术支持人员。

# 3.2 控制平面

## 3.2.1 ARP 的安全

### 3.2.1.1 防 ARP 欺骗攻击

#### 攻击行为

ARP欺骗指恶意用户通过发送伪造的ARP报文，恶意修改网关或网络内其他主机的ARP表项，造成用户或网络的报文转发异常。

- 恶意用户仿冒其他用户向网关发送ARP报文，导致网关学习到错误的用户ARP表项。
- 恶意用户仿冒网关发出ARP报文，导致网络中其他用户学习到错误的网关ARP表项。
- 恶意用户通过构造畸形的ARP报文进行攻击，导致交换机学习到错误的ARP表项。

#### 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- ARP表项固化

  交换机支持三种ARP表项固化模式，这三种模式适用于不同的应用场景，且是互斥关系。

  - **fixed-mac**方式适用于用户MAC地址固定，但用户接入位置频繁变动的场景。当用户从不同接口接入交换机时，交换机上该用户对应的ARP表项中的接口信息可以及时更新。
  - **fixed-all**方式适用于用户MAC地址固定，并且用户接入位置相对固定的场景。
  - **send-ack**方式适用于用户的MAC地址和接入位置均频繁变动的场景。
- 动态ARP检测（DAI）

  使能DAI的交换机会将ARP报文对应的源IP、源MAC、接口、VLAN信息和绑定表中的信息进行比较，如果信息匹配，说明发送该ARP报文的用户是合法用户，允许此用户的ARP报文通过，否则就认为是攻击，丢弃该ARP报文。绑定表通常通过DHCP Snooping动态生成，也可手工配置指定。
- ARP防网关冲突

  为了防范攻击者仿冒网关，当用户主机直接接入网关时，可以在网关交换机上使能ARP防网关冲突攻击功能。当交换机收到的ARP报文存在下列情况之一：

  - ARP报文的源IP地址与报文入接口对应的VLANIF接口的IP地址相同。
  - ARP报文的源IP地址是入接口的虚拟IP地址，但ARP报文源MAC地址不是VRRP虚MAC。

  交换机就认为该ARP报文是与网关地址冲突的ARP报文，交换机将生成ARP防攻击表项，并在后续一段时间内丢弃该接口收到的同VLAN以及同源MAC地址的ARP报文，这样就可以防止与网关地址冲突的ARP报文在VLAN内广播。
- 免费ARP报文主动丢弃

在确认攻击来自免费ARP报文之后，可以在网关交换机上使能免费ARP报文主动丢弃功能，使网关交换机直接丢弃免费ARP报文。

- 发送ARP免费报文

  在网关交换机上配置发送免费ARP报文的功能，用来定期更新合法用户的ARP表项，使得合法用户ARP表项中记录的是正确的网关地址映射关系。

- ARP报文内MAC地址一致性检查

  交换机收到ARP报文时，对以太报文头中的源、目的MAC地址和ARP报文中的源、目的MAC地址进行一致性检查。如果以太网数据帧首部中的源/目的MAC地址和ARP报文中的源/目的MAC地址不同，则认为是攻击报文，将其丢弃；否则，继续进行ARP学习。可以有效防止恶意用户通过构造畸形ARP报文对网络或者网络交换机的攻击。

- ARP报文合法性检查

  为了防止非法ARP报文的攻击，可以在接入交换机或网关交换机上配置ARP报文合法性检查功能，用来对MAC地址和IP地址不合法的ARP报文进行过滤。交换机提供以下三种可以任意组合的检查项配置：

  - IP地址检查：交换机会检查ARP报文中的源IP和目的IP地址，全0、全1、或者组播IP地址都是不合法的，需要丢弃。对于ARP应答报文，源IP和目的IP地址都进行检查；对于ARP请求报文，只检查源IP地址。
  - 源MAC地址检查：交换机会检查ARP报文中的源MAC地址和以太网数据帧首部中的源MAC地址是否一致，一致则认为合法，否则丢弃报文。
  - 目的MAC地址检查：交换机会检查ARP应答报文中的目的MAC地址是否和以太网数据帧首部中的目的MAC地址一致，一致则认为合法，否则丢弃报文。

- ARP网关保护功能

  在交换机与网关相连的接口上配置ARP网关保护功能，可以防止攻击者仿冒网关。

- ARP表项严格学习

  配置ARP表项严格学习功能后，只有本交换机主动发送的ARP请求报文的应答报文才能触发本交换机学习ARP，其他交换机主动向本交换机发送的ARP报文不能触发本交换机学习ARP，这样可以拒绝大部分的ARP报文攻击。

- DHCP触发ARP学习

  在DHCP用户场景下，当DHCP用户数目很多时，交换机进行大规模ARP表项的学习和老化会对交换机性能和网络环境形成冲击。为了避免此问题，可以在网关交换机上使能DHCP触发ARP学习功能。当DHCP服务器给用户分配了IP地址，网关交换机会根据VLANIF接口上收到的DHCP ACK报文直接生成该用户的ARP表项。

- VPLS网络中ARP代理

  在VPLS网络中，为了防止PW侧的伪造ARP报文被广播到AC侧形成ARP欺骗攻击，可以在PE交换机上使能在VPLS网络中的ARP代理功能。

## 配置方法

- 配置ARP表项固化

  使能ARP表项固化功能，指定固定模式为固化MAC方式。

  ```
  <HUAWEI> system-view
  [HUAWEI] arp anti-attack entry-check fixed-mac enable  //可以在全局和VLANIF接口下配置，请根据需要选择
  ```

- 配置动态ARP检测（DAI）

  使能接口GE1/0/1下的动态ARP检测功能。

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] arp anti-attack check user-bind enable  //可以在接口视图或者VLAN视图下配置，请根据需要选择
```

- 配置ARP防网关冲突

  使能ARP防网关冲突攻击功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] arp anti-attack gateway-duplicate enable
  ```

- 配置免费ARP报文主动丢弃

  全局使能免费ARP报文主动丢弃功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] arp anti-attack gratuitous-arp drop  //可以在全局和VLANIF接口下配置，请根据需要选择
  ```

- 配置发送ARP免费报文

  在接口VLANIF10下使能发送免费ARP报文的功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface vlanif 10
  [HUAWEI-Vlanif10]  arp gratuitous-arp send enable  //可以在全局和VLANIF接口下配置，请根据需要选择
  ```

- 配置ARP报文内MAC地址一致性检查

  使能指定接口的ARP报文内MAC地址一致性检查。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] arp validate source-mac destination-mac
  ```

- 配置ARP报文合法性检查

  使能ARP报文合法性检查功能，并指定ARP报文合法性检查时检查源MAC地址。

  ```
  <HUAWEI> system-view
  [HUAWEI] arp anti-attack packet-check sender-mac
  ```

- 配置ARP表项严格学习

  指定接口的ARP表项严格学习功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface vlanif 100
  [HUAWEI-Vlanif100] arp learning strict force-enable  //可以在全局和VLANIF接口下配置，请根据需要选择
  ```

- 配置DHCP触发ARP学习

  使能接口VLANIF100的DHCP触发ARP学习功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] vlan batch 100
  [HUAWEI] dhcp enable
  [HUAWEI] interface vlanif 100
  [HUAWEI-Vlanif100] arp learning dhcp-trigger
  ```

- VPLS网络中ARP代理

  使能在VPLS网络中的ARP代理功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] dhcp enable
  [HUAWEI] dhcp snooping enable
  [HUAWEI] dhcp snooping over-vpls enable
  [HUAWEI] arp over-vpls enable
  ```

## 检查加固结果

- 执行命令**display arp anti-attack configuration** { **arp-rate-limit** | **arp-speed-limit** | **entry-check** | **arpmiss-rate-limit** | **arpmiss-speed-limit** | **gateway-duplicate** | **log-trap-timer** | **packet-check** | **all** }，查看ARP防攻击配置。

- 执行命令**display arp learning strict**，查看全局和所有VLANIF接口上的ARP表项严格学习情况。

### 3.2.1.2 防 ARP 泛洪攻击

## 攻击行为

当网络中出现过多的ARP报文时，会导致网关设备CPU负载加重，影响设备正常处理用户的其它业务。另一方面，网络中过多的ARP报文会占用大量的网络带宽，引起网络堵塞，从而影响整个网络通信的正常运行。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- ARP表项限制

  设备基于接口限制学习ARP表项的总数目，可以有效地防止ARP表项溢出，保证ARP表项的安全性。

- ARP速率抑制

  设备对单位时间内收到的ARP报文进行数量统计，如果ARP报文的数量超过了配置的阈值，超出部分的ARP报文将被忽略，设备不作任何处理，有效防止ARP表项溢出。

- ARP表项严格学习

  设备仅学习本端发送的ARP请求报文的应答报文，并不学习其它设备向交换机发送的ARP请求报文和非本端发送的ARP请求报文的应答报文，可以拒绝掉ARP请求报文攻击和非自己发送的ARP请求报文对应的应答报文攻击。

- ARP端口级防护

  设备基于端口对ARP上送速率进行监控，当某端口ARP上送控制面报文速率超过特定阈值时，会将该端口的ARP报文通过单独通道上送控制面，避免攻击影响正常的ARP报文。此外，设备还支持将攻击端口的ARP报文阻塞一段时间，而不是通过单独的通道上送。

- ARP用户级防护

  设备对用户（基于MAC地址或者IP地址）上送控制面的ARP报文速率进行监控，当某用户ARP报文速率超过特定阈值时，会将该用户ARP报文丢弃一段时间。

**说明**

较为低端的盒式交换机不支持ARP端口级防护或者ARP用户级防护。

## 配置方法

- ARP表项限制

  配置指定接口最多可以学习到的ARP表项数量。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp-limit maximum 20
```

- ARP速率抑制

  对ARP报文采用基于源IP地址进行时间戳抑制，速率为每秒50个ARP报文。

```
<HUAWEI> system-view
[HUAWEI] arp speed-limit source-ip maximum 50
```

- 配置ARP表项严格学习

  ARP表项严格学习既可以基于全局，也可以基于指定的接口配置，两者有如下的关系：

  - 当全局和接口同时配置了ARP严格学习功能时，采用接口下配置的策略。
  - 当接口下没有配置ARP严格学习功能时，采用全局下配置的ARP严格学习策略。

  使能全局的ARP表项严格学习功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] arp learning strict
  ```

  使能指定接口的ARP表项严格学习功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface vlanif 100
  [HUAWEI-Vlanif100] arp learning strict force-enable
  ```

- 配置ARP端口级防护

  ARP端口级防护默认开启，无需手工配置。此外，还可以配置ARP报文限速。

  配置接口GE1/0/1在1秒钟内最多允许50个ARP报文通过，当ARP报文超过该限速值时，60秒内持续丢弃该接口下的所有ARP报文

  ```
  <HUAWEI> system-view
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] arp anti-attack rate-limit enable
  [HUAWEI-GigabitEthernet1/0/1] arp anti-attack rate-limit packet 50 block-timer 60
  ```

- 配置ARP用户级防护

  ARP用户级防护基于用户MAC地址或者IP地址进行。同时为避免合法的地址被过滤掉，需要通过攻击溯源白名单剔除合法的接口（一般指上行接口或者网络侧接口）。

  ```
  <HUAWEI> system-view
  [HUAWEI] cpu-defend policy antiatk
  [HUAWEI-cpu-defend-policy-antiatk] auto-defend enable
  [HUAWEI-cpu-defend-policy-antiatk] auto-defend threshold 30
  [HUAWEI-cpu-defend-policy-antiatk] auto-defend attack-packet sample 5
  [HUAWEI-cpu-defend-policy-antiatk] undo auto-defend trace-type source-portvlan
  [HUAWEI-cpu-defend-policy-antiatk] undo auto-defend protocol tcp telnet ttl-expired igmp icmp dhcpv6 mld nd
  [HUAWEI-cpu-defend-policy-antiatk] auto-defend action deny timer 300
  [HUAWEI-cpu-defend-policy-antiatk] auto-defend whitelist 1 interface gigabitethernet 1/0/1  //将上行接口或者网络侧接口加入白名单
  [HUAWEI-cpu-defend-policy-antiatk] auto-defend whitelist 2 interface gigabitethernet 2/0/0  //将上行接口或者网络侧接口加入白名单
  [HUAWEI-cpu-defend-policy-antiatk] quit
  [HUAWEI] cpu-defend-policy antiatk  //在主控板上应用防攻击策略
  [HUAWEI] cpu-defend-policy antiatk global  //在所有接口板或设备上应用防攻击策略
  ```

## 检查加固结果

- 执行命令**display arp-limit** [ **interface** *interface-type interface-number*[*.subinterface-number* ] ] [ **vlan** *vlan-id* ]，查看接口可以学习到的动态ARP表项数目的最大值。
- 执行命令**display arp learning strict**，查看全局和所有VLANIF接口上的ARP表项严格学习情况。

# 3.2.2 DHCP 的安全

### 3.2.2.1 DHCP 服务器欺骗

## 攻击行为

由于DHCP服务器和DHCP客户端之间没有认证机制，所以如果在网络上随意添加一台DHCP服务器，它就可以仿冒DHCP服务器为客户端分配IP地址以及其他网络参数。DHCP服务器仿冒者通过二层网络接入汇聚交换机，当交换机下接终端通过DHCP申请地址时，DHCP服务器仿冒者先于其它DHCP服务器回应并分配地址给客户端，进而引起网络地址分配错误，导致网络业务异常。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- DHCP服务器过滤

  在交换机上配置流策略过滤，仅允许合法的DHCP服务器的回应报文经过交换机转发。

- DHCP Snooping

  在交换机上配置DHCP Snooping功能，同时配置合法DHCP服务器端口为信任接口，进行非法DHCP服务器过滤。

## 配置方法

- 配置DHCP服务器合法性过滤

  合法的DHCP服务器具有特定的IP地址，DHCP服务器回应报文属UDP报文，且源端口号为67，可以通过策略进行DHCP合法性过滤，屏蔽不合法的DHCP服务器。

  以DHCP服务器合法端口角度考虑，可以配置如下策略过滤。

  a. 配置合法与非法DHCP服务器过滤规则。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl name dhcp-valid
  [HUAWEI-acl-adv-dhcp-valid] rule permit udp source-port eq bootps
  [HUAWEI-acl-adv-dhcp-valid] quit
  [HUAWEI] acl name dhcp-invalid
  [HUAWEI-acl-adv-dhcp-invalid] rule deny udp source-port eq bootps
  [HUAWEI-acl-adv-dhcp-invalid] quit
  ```

  b. 应用过滤规则，允许合法端口。

  ```
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] traffic-filter inbound acl name dhcp-valid
  [HUAWEI-GigabitEthernet1/0/1] quit
  ```

  c. 应用过滤规则，屏蔽其它非法端口。

  ```
  [HUAWEI] traffic-filter inbound acl name dhcp-invalid
  ```

- 配置DHCP Snooping合法性检查

  配置合法DHCP服务器端口为信任接口。

  ```
  <HUAWEI> system-view
  [HUAWEI] dhcp enable
  [HUAWEI] dhcp snooping enable
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] dhcp snooping enable
  [HUAWEI-GigabitEthernet1/0/1] dhcp snooping trusted
  [HUAWEI-GigabitEthernet1/0/1] quit
  ```

  其它用户侧接口或者VLAN配置DHCP Snooping。

  ```
  [HUAWEI] interface gigabitethernet 2/0/0
  [HUAWEI-GigabitEthernet2/0/0] dhcp snooping enable
  ```

## 检查加固结果

- 执行命令**display traffic-applied** [ **interface** [ *interface-type interface-number* ] | **vlan** [ *vlan-id* ] ] { **inbound** | **outbound** } [ **verbose** ]，查看全局、VLAN或接口上应用的基于ACL的简化流策略的配置信息。
- 执行命令**display dhcp snooping configuration** [ **vlan** *vlan-id* | **interface** *interface-type interface-number* | **bridge-domain** *bd-id* ]，查看DHCP Snooping的配置信息。

### 3.2.2.2 DHCP 泛洪攻击

## 攻击行为

当交换机做为DHCP服务器或者中继角色时，如果恶意用户发送大量的DHCP报文到交换机，侵占交换机DHCP处理能力，导致其它合法DHCP交互无法正常进行，进而导致终端无法申请地址或者无法续租地址。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- DHCP端口级防护

  交换机基于端口对DHCP上送速率进行监控，当某端口DHCP上送控制面报文速率超过特定阈值时，会将该端口的DHCP报文通过单独通道上送控制面，避免攻击影响正常的DHCP报文。

- DHCP用户级防护

  交换机对用户（基于MAC地址或者IP地址）上送控制面的DHCP报文速率进行监控，当某用户DHCP报文速率超过特定阈值时，会将该用户DHCP报文丢弃一段时间。

**说明**

较为低端的盒式交换机不支持DHCP端口级防护或者DHCP用户级防护。对于支持的款型，DHCP端口级防护属系统默认打开的功能，不需要手工配置；而DHCP用户级防护需要手工打开。

## 配置方法

DHCP用户级防护基于用户MAC地址或者IP地址进行。同时为避免合法的地址被过滤掉，需要通过攻击溯源白名单剔除合法的DHCP服务器地址。

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy antiatk
[HUAWEI-cpu-defend-policy-antiatk] auto-defend enable
[HUAWEI-cpu-defend-policy-antiatk] auto-defend threshold 30
[HUAWEI-cpu-defend-policy-antiatk] auto-defend attack-packet sample 5
[HUAWEI-cpu-defend-policy-antiatk] undo auto-defend trace-type source-portvlan
[HUAWEI-cpu-defend-policy-antiatk] undo auto-defend protocol tcp telnet ttl-expired igmp icmp dhcpv6 mld nd
[HUAWEI-cpu-defend-policy-antiatk] auto-defend action deny timer 300
[HUAWEI-cpu-defend-policy-antiatk] auto-defend whitelist 1 interface gigabitethernet 1/0/1 //将上行接口或者网络侧接口加入白名单
[HUAWEI-cpu-defend-policy-antiatk] auto-defend whitelist 2 interface gigabitethernet 2/0/0 //将上行接口或者网络侧接口加入白名单
[HUAWEI-cpu-defend-policy-antiatk] quit
[HUAWEI] cpu-defend-policy antiatk  //在主控板上应用防攻击策略
[HUAWEI] cpu-defend-policy antiatk global  //在所有接口板或设备上应用防攻击策略
```

### 检查加固结果

执行命令**display auto-defend configuration**，查看攻击溯源的配置信息。

## 3.2.3 路由协议的安全

### 3.2.3.1 BGP/BGP4+

### 攻击行为

- DOS攻击

  攻击者可以发送各种类型的报文攻击交换机，如果是多播协议报文、或者目的地址是交换机自身接口（包括Loopback口）IP地址时，交换机就会直接将报文上送CPU。这样就会耗费交换机的CPU和系统资源，造成DoS攻击。

- 构造错误BGP协议报文

  攻击者通过构造超长的AS_Path属性报文，对交换机进行错误报文攻击。

- 数据包五元组攻击

  BGP使用TCP作为传输协议，只要TCP数据包的源地址、目的地址、源端口、目的端口和TCP序号是正确的，BGP就会认为这个数据包有效，但数据包的大部分参数对于攻击者来说是不难获得的。

- GTSM攻击

  攻击者模拟真实的BGP协议对交换机不断发送报文，导致交换机因处理这些攻击报文而使系统异常繁忙，CPU占用率过高。

### 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- CPCAR

  BGP会话创建后通过下发白名单，应用层联动模块检测上送的协议报文，对匹配白名单的协议报文，允许其以大带宽和高速率上送，对于不在白名单内报文，限制其以默认带宽和速率上送，从而避免DoS报文攻击。同时在接口上应用CPCAR限制BGP报文上送速率，保证CPU不受攻击，保证网络的正常运行。

- AS_Path数量控制

  BGP接收路由时会检查AS_Path属性中的AS号是否超限。如果超限则丢弃路由，路由发布也会检查AS_Path属性中的AS号是否超限，如果超限，则不发布此路由，防止恶意构造超长AS_Path属性的错误报文对交换机进行报文攻击。

- BGP MD5认证、BGP Keychain认证

  为了保证BGP协议免受攻击，可以在BGP邻居之间使用MD5认证或者Keychain认证来降低被攻击的可能性。

  - MD5算法配置简单，配置后生成单一密码，需要人为干预才可以更换密码。为了保证更好的安全性，建议不要使用MD5认证方式。
  - Keychain具有一组密码，可以根据配置自动切换，但是配置过程较为复杂，适用于对安全性能要求比较高的网络。

- BGP GTSM

  为防止攻击者模拟真实的BGP协议报文对交换机进行攻击，可以配置GTSM功能检测IP报文头中的TTL值。根据实际组网的需要，对于不符合TTL值范围的报文，

GTSM可以设置为通过或丢弃。当配置GTSM缺省动作为丢弃时，可以根据网络拓扑选择合适的TTL有效范围，不符合TTL值范围的报文会被交换机直接丢弃，这样就避免了网络攻击者模拟的BGP报文攻击交换机。

## 配置方法

- 修改BGP协议的CPCAR

  **说明**

  调整CPCAR不当将会影响网络业务，如果需要调整CPCAR，建议联系技术支持工程师处理。

  修改BGP协议上送速率为64kbps。

  ```
  <HUAWEI> system-view
  [HUAWEI] cpu-defend policy 1
  [HUAWEI-cpu-defend-policy-1] car packet-type bgp cir 64
  [HUAWEI-cpu-defend-policy-1] quit
  [HUAWEI] cpu-defend-policy 1 global
  [HUAWEI] cpu-defend-policy 1
  ```

- 配置AS_Path属性中AS号的最大个数

  设置AS_Path属性中AS号的最大个数为200。

  ```
  <HUAWEI> system-view
  [HUAWEI] bgp 100
  [HUAWEI-bgp] as-path-limit 200
  ```

- 配置Keychain认证

  为对等体配置名为example的Keychain认证。

  ```
  <HUAWEI> system-view
  [HUAWEI] keychain example mode absolute
  [HUAWEI-keychain-example] key-id 1
  [HUAWEI-keychain-example-keyid-1] algorithm sha-256
  [HUAWEI-keychain-example-keyid-1] key-string cipher YsHsjx_202206
  [HUAWEI-keychain-example-keyid-1] quit
  [HUAWEI-keychain-example] quit
  [HUAWEI] bgp 100
  [HUAWEI-bgp] peer 10.1.1.2 as-number 200
  [HUAWEI-bgp] peer 10.1.1.2 keychain example
  ```

- 配置BGP GTSM功能

  为对等体配置GTSM功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] bgp 100
  [HUAWEI-bgp] peer 10.1.1.2 as-number 200
  [HUAWEI-bgp] peer 10.1.1.2 valid-ttl-hops 1
  ```

  接下来，对于未匹配策略的报文，可以设置**gtsm default-action** { **drop** | **pass** }命令的**pass**参数或者执行**undo gtsm default-action drop**命令使报文通过过滤，或设置**drop**参数丢弃报文。对于丢弃的报文，可以通过命令**gtsm log drop-packet all**打开LOG信息开关，控制是否对报文被丢弃的情况记录日志，以方便故障的定位。

## 检查加固结果

- 执行命令**display bgp peer verbose**或**display bgp ipv6 peer verbose**，查看BGP/BGP4+对等体的详细信息。

### 3.2.3.2 OSPF/OSPFv3

## 攻击行为

- GTSM攻击

  攻击者模拟真实的OSPF/OSPFv3协议，对一台交换机不断发送报文，导致交换机因处理这些攻击报文而使系统异常繁忙，CPU占用率过高。

- 伪造报文攻击

  可能的攻击手段有：

  - 修改报文老化时间到最大老化时间，导致所有交换机废弃这个报文。
  - 发布合法的Max Sequence Number的LSA或者接近Max Seq Num的报文。
  - 邻居交换机重启时复位其加密序列号状态的时机，更改序列号。
  - 修改Hello报文中的邻居列表。

- 错误路由信息的注入

  OSPFv3接收所有来自合法设备的报文。所以，OSPFv3报文中携带的非法或错误路由信息可能对交换机造成攻击，这些信息会造成路由数据库运算错误，引起网络故障。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- OSPF/OSPFv3 GTSM

  GTSM机制通过TTL的检测达到防止GTSM攻击的目的。GTSM只会对匹配GTSM策略的报文进行TTL检查。对于未匹配策略的报文，可以设置为通过或丢弃。如果配置GTSM缺省报文动作为丢弃，就需要在GTSM中配置所有可能的设备连接情况，没有配置的设备发送的报文将被丢弃，无法建立连接。

- OSPF/OSPFv3报文验证

  OSPF/OSPFv3报文验证功能，可以防止伪造报文攻击。只有通过验证的报文才能接收，否则将不能正常建立邻居关系。使用区域验证时，一个区域中所有的交换机在该区域下的验证模式和口令必须一致。例如，在Area0内所有交换机上配置验证模式为简单验证，口令为abc。接口验证方式用于在相邻的交换机之间设置验证模式和口令，优先级高于区域验证方式。

- OSPFv3 IPSec验证

  OSPFv3 IPSec认证机制可以避免错误路由信息的引入。在通信两端对等体的OSPFv3上应用IPSec，OSPFv3只处理通过验证的报文。这样，OSPFv3可以避免接收来自未经验证对等体的错误路由数据。

## 配置方法

OSPF GTSM特性、OSPF区域验证和OSPF接口验证的配置方法如下。

- 配置OSPF GTSM特性

  使能OSPF GTSM功能，配置允许接收的公网OSPF报文的最大跳数为5。

  ```
  <HUAWEI> system-view
  [HUAWEI] ospf valid-ttl-hops 5
  ```

  接下来，对于未匹配策略的报文，可以设置**gtsm default-action** { **drop** | **pass** } 命令的**pass**参数或者执行**undo gtsm default-action drop**命令使报文通过过滤，或设置**drop**参数丢弃报文。对于丢弃的报文，可以通过命令**gtsm log drop-**

**packet all**打开LOG信息开关，控制是否对报文被丢弃的情况记录日志，以方便故障的定位。

- 配置OSPF区域认证

  指定OSPF区域0使用HMAC-SHA256验证模式。

  ```
  <HUAWEI> system-view
  [HUAWEI] ospf 100
  [HUAWEI-ospf-100] area 0
  [HUAWEI-ospf-100-area-0.0.0.0] authentication-mode hmac-sha256
  ```

- 配置OSPF接口认证

  在接口VLANIF100上配置OSPF的HMAC-SHA256验证模式。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface vlanif 100
  [HUAWEI-Vlanif100] ospf authentication-mode hmac-sha256
  ```

OSPFv3 GTSM特性、OSPFv3区域认证、OSPFv3进程认证、OSPFv3接口认证和OSPFv3 IPSec验证的配置方法如下。

- 配置OSPFv3 GTSM特性

  使能OSPFv3 GTSM特性，配置允许接收的公网OSPFv3报文的最大跳数为5。

  ```
  <HUAWEI> system-view
  [HUAWEI] ospfv3 valid-ttl-hops 5
  ```

  接下来，对于未匹配策略的报文，可以设置**gtsm default-action** { **drop** | **pass** }命令的**pass**参数或者执行**undo gtsm default-action drop**命令使报文通过过滤，或设置**drop**参数丢弃报文。对于丢弃的报文，可以通过命令**gtsm log drop-packet all**打开LOG信息开关，控制是否对报文被丢弃的情况记录日志，以方便故障的定位。

- 配置OSPFv3区域认证

  设置OSPFv3区域0使用HMAC-SHA256认证模式。

  ```
  <HUAWEI> system-view
  [HUAWEI] ospfv3 100
  [HUAWEI-ospfv3-100] area 0
  [HUAWEI-ospfv3-100-area-0.0.0.0] authentication-mode hmac-sha256 key-id 10 cipher YsHsjx_202206
  ```

- 配置OSPFv3进程认证

  设置OSPFv3进程100使用HMAC-SHA256认证方式。

  ```
  <HUAWEI> system-view
  [HUAWEI] ospfv3 100
  [HUAWEI-ospfv3-100] authentication-mode hmac-sha256 key-id 10 cipher YsHsjx_202206
  ```

- 配置OSPFv3接口认证

  在接口VLANIF100上设置OSPFv3 HMAC-SHA256认证模式。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface vlanif 100
  [HUAWEI-Vlanif100] ipv6 enable
  [HUAWEI-Vlanif100] ospfv3 1 area 0
  [HUAWEI-Vlanif100] ospfv3 authentication-mode hmac-sha256 key-id 10 cipher YsHsjx_202206
  ```

- 配置OSPFv3 IPSec验证
  - 对指定OSPFv3进程的所有报文进行安全联盟SA认证

    在OSPFv3进程下配置安全联盟，安全联盟名为sa1。（执行该命令前，交换机应该已经创建了名称为sa1的安全联盟。）

    ```
    <HUAWEI> system-view
    [HUAWEI] ospfv3 1
    [HUAWEI-ospfv3-1] ipsec sa sa1
    ```

- 对指定OSPFv3区域的所有报文进行安全联盟认证

  在OSPFv3区域下配置安全联盟，安全联盟名为sa2。（执行该命令前，交换机应该已经创建了名称为sa2的安全联盟。）

  ```
  <HUAWEI> system-view
  [HUAWEI] ospfv3 1
  [HUAWEI-ospfv3-1] area 10.0.0.0
  [HUAWEI-ospfv3-1-area-10.0.0.0] ipsec sa sa2
  ```

- 对指定OSPFv3接口接收和发送的所有报文进行安全联盟认证

  在VLANIF10接口上使能安全联盟，安全联盟名为sa3。（执行该命令前，交换机应该已经创建了名称为sa3的安全联盟。）

  ```
  <HUAWEI> system-view
  [HUAWEI] interface vlanif 10
  [HUAWEI-Vlanif10] ipv6 enable
  [HUAWEI-Vlanif10] ospfv3 1 area 0
  [HUAWEI-Vlanif10] ospfv3 ipsec sa sa3
  ```

- 对OSPFv3虚链路上接收和发送的所有报文进行安全联盟认证

  创建一条到10.110.0.3的虚连接。

  ```
  <HUAWEI> system-view
  [HUAWEI] ospfv3 1
  [HUAWEI-ospfv3-1] area 10.0.0.0
  [HUAWEI-ospfv3-1-area-10.0.0.0] vlink-peer 10.110.0.3
  ```

- 对OSPFv3伪链路上接收和发送的所有报文进行安全联盟SA认证

  创建一条OSPFv3伪连接，源地址为FC00:0:0:1001::1，目的地址为FC00:0:0:2001::1。

  ```
  <HUAWEI> system-view
  [HUAWEI] ospfv3 1 vpn-instance vrf1
  [HUAWEI-ospfv3-1] area 1
  [HUAWEI-ospfv3-1-area-0.0.0.1] sham-link fc00:0:0:1001::1 fc00:0:0:2001::1
  ```

## 检查加固结果

- 执行命令**display ospf** [ *process-id* ] **brief**，查看OSPF区域配置的认证方式。
- 执行命令**display ospf** [ *process-id* ] **interface** [ **all** | *interface-type interface-number* ] [ **verbose** ]，查看OSPF的接口信息。

### 3.2.3.3 RIP/RIPng

## 攻击行为

- 错误路由信息的注入

  对于合法来源的RIP/RIPng报文，若发送地址与配置网络匹配，交换机将会接收。将直达线路数据直接携带在报文中，所以，在RIP报文中携带的路由数据中可能存在非法或错误路由信息的攻击。这会造成计算路由数据库不准确，引起网络故障。

- 重放攻击

  攻击者截获RIP报文，之后重复向交换机发送报文，增加交换机的负担。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- RIP验证

RIPv2支持协议报文验证，以避免错误的路由数据，错误报文和来自网络的重放攻击。支持三种验证模式：简单验证模式、MD5验证模式、HMAC-SHA256验证模式。简单验证模式和MD5验证存在安全风险，推荐配置HMAC-SHA256密文验证方式。

- CPCAR

  通过对上送控制平面的RIP/RIPng分别进行限速，来保护控制平面的安全。

## 配置方法

- RIP验证

  配置通用格式的HMAC-SHA256验证，验证密码为YsHsjx_202206，验证标识符为255。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] rip authentication-mode hmac-sha256 cipher YsHsjx_202206
```

- 修改RIP/RIPng协议的CPCAR

  **说明**

  调整CPCAR不当将会影响网络业务，如果需要调整CPCAR，建议联系技术支持工程师处理。

  修改RIP协议上送速率为64kbps。

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy 1
[HUAWEI-cpu-defend-policy-1] car packet-type rip cir 64
[HUAWEI-cpu-defend-policy-1] quit
[HUAWEI] cpu-defend-policy 1 global
[HUAWEI] cpu-defend-policy 1
```

  修改RIPng协议上送速率为64kbps。

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy 1
[HUAWEI-cpu-defend-policy-1] car packet-type ripng cir 64
[HUAWEI-cpu-defend-policy-1] quit
[HUAWEI] cpu-defend-policy 1 global
[HUAWEI] cpu-defend-policy 1
```

## 检查加固结果

- 执行命令**display rip** *process-id* **interface** [ *interface-type interface-number* ] [ **verbose** ]，查看RIP的接口信息。
- 执行命令**display rip** [ *process-id* | **vpn-instance** *vpn-instance-name* ]，查看RIP进程的当前运行状态及配置信息。

### 3.2.3.4 IS-IS（IPv4）/IS-IS（IPv6）

## 攻击行为

攻击方可以捕获网络中的正确Hello报文或者链路状态报文，然后构造IS-IS可以识别的攻击报文发送到交换机。

## 安全策略

IS-IS认证是基于网络安全性的要求而实现的一种加密手段，可以预防上述攻击行为。

IS-IS认证通过在IS-IS报文中增加认证字段对报文进行加密。当本地交换机接收到远端交换机发送过来的IS-IS报文，如果发现认证密码不匹配，则将收到的报文进行丢弃，达到自我保护的目的。IS-IS认证包括：

- 接口的认证：通过配置IS-IS接口认证，可以封装认证信息到Hello报文中，以确认邻居的有效性和正确性。
- 区域或路由域的认证：通过配置区域或路由域的认证，会将认证密码封装在区域的IS-IS报文中，只有通过认证的报文才会被接收。

认证模式分为：简单认证、MD5认证和HMAC-SHA256认证。简单认证、MD5认证模式存在安全风险，推荐配置HMAC-SHA256认证模式。

## 配置方法

- 配置接口的认证

  为接口VLANIF100设置HMAC-SHA256认证密码YsHsjx_202206，密钥ID为33。

  ```
  <HUAWEI> system-view
  [HUAWEI] isis
  [HUAWEI-isis-1] network-entity 01.0000.0000.0001.00
  [HUAWEI-isis-1] quit
  [HUAWEI] interface vlanif 100
  [HUAWEI-Vlanif100] isis enable 1
  [HUAWEI-Vlanif100] isis authentication-mode hmac-sha256 key-id 33 cipher YsHsjx_202206
  ```

- 配置区域或路由域的认证

  a. 创建ISIS进程1。

  ```
  <HUAWEI> system-view
  [HUAWEI] isis 1
  ```

  b. 以下命令是并列关系，可以同时配置，请根据实际需要选择执行以下命令。

  i. 设置区域认证模式：认证模式为HMAC-SHA256，认证密码YsHsjx_202206，密钥ID为33。

  ```
  [HUAWEI-isis-1] area-authentication-mode hmac-sha256 key-id 33 cipher YsHsjx_202206
  ```

  ii. 设置路由域认证模式：认证模式为HMAC-SHA256，认证密码YsHsjx_202206，密钥ID为33。

  ```
  [HUAWEI-isis-1] domain-authentication-mode hmac-sha256 key-id 33 cipher YsHsjx_202206
  ```

## 检查加固结果

执行命令**display isis lsdb**，查看IS-IS的链路状态数据库信息。

# 3.2.4 MPLS 的安全

### 3.2.4.1 LDP

## 攻击行为

LDP会话过程中信息容易被篡改，另外攻击者模拟真实的LDP协议对交换机不断发送报文，导致交换机因处理这些攻击报文而使系统异常繁忙，CPU占用率过高。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- LDP MD5认证

  LDP MD5认证通过对同一信息段产生唯一摘要信息的特点来实现LDP报文防篡改校验，比一般意义上TCP校验更为严格。

  MD5算法配置简单，配置后生成单一密码，需要人为干预才可以切换密码，适用于需要短时间加密的网络。

  MD5属于不安全的加密算法，在对安全性要求较高的网络中，建议使用Keychain认证。

- LDP Keychain认证

  Keychain具有一组密码，可以根据配置自动切换，但是配置过程较为复杂，适用于对安全性能要求比较高的网络。

  对于同一邻居，在配置Keychain认证后，不能再配置MD5认证；同样，在配置MD5认证后，不能再配置Keychain认证。

- LDP GTSM

  GTSM通过判定报文的TTL值，确定报文是否有效，从而保护交换机免受攻击。在LDP对等体上配置GTSM功能，通过配置的TTL有效范围，对LDP对等体间的LDP消息报文进行TTL检测。如果LDP消息报文的TTL不符合配置的范围要求，就认为此报文为非法攻击报文予以丢弃，以免LDP协议在收到大量伪装报文时，因处理大量伪装报文而受到攻击，进而实现对上层协议的保护。

## 配置方法

- 配置LDP Keychain认证

  配置对LSR ID为2.2.2.2的对等体进行Keychain认证，引用的Keychain名称为kc1。

```
<HUAWEI> system-view
[HUAWEI] keychain kc1 mode absolute
[HUAWEI-keychain-kc1] key-id 1
[HUAWEI-keychain-kc1-keyid-1] algorithm sha-256
[HUAWEI-keychain-kc1-keyid-1] key-string YsHsjx_202206
[HUAWEI-keychain-kc1-keyid-1] quit
[HUAWEI-keychain-kc1] quit
[HUAWEI] mpls lsr-id 2.2.2.2
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] authentication key-chain peer 2.2.2.2 name kc1
```

  **须知**

  配置LDP Keychain认证会导致LDP会话重建，与原来会话相关的LSP将被删除。

- 配置LDP GTSM功能

  在LSR上配置传输地址为1.1.1.1的对等体发来的LDP报文的有效TTL范围是254～255。

```
<HUAWEI> system-view
[HUAWEI] mpls lsr-id 1.1.1.1
[HUAWEI] mpls
[HUAWEI-mpls] quit
[HUAWEI] mpls ldp
[HUAWEI-mpls-ldp] gtsm peer 1.1.1.1 valid-ttl-hops 2
```

  如果将hops设置为GTSM功能允许的最大有效跳数，当LDP对等体发来报文的TTL值在[255–hops+1，255]范围内，则接收该报文，否则丢弃该报文。

## 检查加固结果

执行命令**display gtsm configuration all**，查看GTSM策略配置信息。

### 3.2.4.2 RSVP

## 攻击行为

RSVP使用RawIP传递协议报文，而RawIP本身不提供安全性，报文容易被篡改，设备容易受到攻击。

RSVP协议在处理报文时，会检查报文的参数、格式、类型等各种信息，但这些参数对于攻击者来说是不难获得的，一种常用的攻击手段就是截获RSVP的报文，之后重复向交换机发送报文，增加交换机的负担，这种攻击方式称为重放攻击。

## 安全策略

RSVP认证通过使用密钥验证的方法来防止消息被篡改或伪造的恶意攻击。如果需要增强在网络阻塞等恶劣网络环境下系统对用户进行身份验证的能力，提高自身的安全性，推荐配置RSVP认证增强功能。RSVP认证增强功能包括：

- RSVP-TE握手机制：可以防止重放攻击。
- RSVP认证消息滑窗大小：避免因RSVP报文的失序导致邻居之间认证关系终止。

RSVP密钥验证可以在接口视图或者MPLS RSVP-TE邻居视图下进行配置。

- 配置接口视图下的RSVP密钥验证功能：应用于两个直连节点。
- 配置MPLS RSVP-TE邻居视图下的RSVP密钥验证功能：可以应用于任意两个互相配置为邻居的节点，推荐使用这种配置方式。

## 配置方法

配置RSVP认证。

```
<HUAWEI> system-view
[Switch] keychain example mode absolute  //配置Keychain功能
[Switch-keychain-example] key-id 1
[Switch-keychain-example-keyid-1] algorithm hmac-sha-256
[Switch-keychain-example-keyid-1] key-string cipher YsHsjx_202206
[Switch-keychain-example-keyid-1] quit
[Switch-keychain-example] quit
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] mpls rsvp-te
[HUAWEI-mpls] quit
[HUAWEI] mpls rsvp-te peer 10.0.0.1
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] mpls rsvp-te authentication keychain example  //配置对等体进行Keychain认证，引用的Keychain名称为example
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] mpls rsvp-te authentication handshake  //配置RSVP-TE握手机制
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] mpls rsvp-te authentication window-size 64  //配置RSVP认证消息滑窗大小
[HUAWEI-mpls-rsvp-te-peer-10.0.0.1] quit
```

## 检查加固结果

执行命令**display mpls rsvp-te interface** [ *interface-type interface-number* ]，查看接口的RSVP-TE配置信息。

# 3.2.5 组播的安全

## 3.2.5.1 二层组播

### 攻击行为

- 恶意用户通过变换组地址加入，使用一些无效组播组频道加入，造成交换机上建立大量无效表项，占用大量系统资源，导致正常用户的点播无法成功。
- 恶意用户通过大量组播频道加入，占用系统资源，导致组播流量对接口带宽消耗很大。
- Query报文攻击，让交换机建立组播交换机端口，接收所有组播组的流量，造成大量流量通过该用户所在的端口发出，对接口带宽消耗很大。

### 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- 可以通过group-policy设定组策略，用来限定某个VLAN或某个接口下允许哪些组播组（组播源组）的加入，以防止恶意用户使用无效组播组频道加入。
- 可以通过二层组播CAC，设定组播组数量限制或带宽限制，用来限定某个VLAN或某个接口下允许加入的组播组的数量，可以设定未知组播组直接丢弃处理，以防止恶意用户通过大量组播频道加入。
- 可以通过设置交换机端口不学习，设定不通过协议报文学习交换机端口，以防止Query报文攻击。

### 配置方法

- 配置组播组策略

  可以在VLAN视图或者VSI视图配置组播组策略（根据业务部署，建议针对IPTV的组播组地址范围）

  允许VLAN 2的用户主机加入组播组225.1.1.123。

  ```
  <HUAWEI> system-view
  [HUAWEI] acl number 2000
  [HUAWEI-acl-basic-2000] rule permit source 225.0.0.0 0.0.0.255
  [HUAWEI-acl-basic-2000] quit
  [HUAWEI] igmp-snooping enable
  [HUAWEI] vlan 2
  [HUAWEI-vlan2] igmp-snooping enable
  [HUAWEI-vlan2] igmp-snooping group-policy 2000
  ```

- 配置CAC的组播组数量限制

  可以在VLAN视图、VSI视图或者接口视图下配置CAC的组播组数量限制

  配置VSI company1内的组播组数量限制值为1000。

  ```
  <HUAWEI> system-view
  [HUAWEI] mpls l2vpn
  [HUAWEI] vsi company1
  [HUAWEI-vsi-company1] l2-multicast limit max-entry 1000
  ```

- 设置端口不学习

  可以在VLAN视图、VSI视图或者接口视图下配置交换机端口不学习

  去使能VLAN 10内GE1/0/1的路由器端口动态学习功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] igmp-snooping enable
  ```

```
[HUAWEI] vlan 10
[HUAWEI-vlan10] igmp-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] undo igmp-snooping router-learning vlan 10
```

## 检查加固结果

- 执行命令**display igmp-snooping** [ **vlan** [ *vlan-id* ] ] **configuration**，查看IGMP Snooping的配置信息。
- 执行命令**display l2-multicast forwarding-table vlan** [ *vlan-id* [ [ **source-address** *source-address* ] **group-address** { *group-address* | **router-group** } ] ]，查看VLAN内的二层组播转发表信息。

## 3.2.5.2 三层组播

## 安全策略

交换机支持配置如下安全策略。

- PIM邻居过滤

  支持在接口配置ACL策略对在该接口接收到的Hello报文进行过滤，通过过滤后，才能建立邻居关系。

  当存在大量恶意Hello报文时，可以通过在接口配置只允许指定的Hello报文通过的策略，丢弃其他恶意报文。

- PIM加入过滤

  支持在接口配置ACL策略对在该接口接收到的join报文进行过滤检查，防止恶意的join报文攻击。

  当存在大量恶意Join报文时，可以通过在接口配置只允许指定的join报文通过的策略，丢弃其他恶意报文。

- MSDP MD5认证

  通过在MSDP PEER对等体上配置MD5认证功能，进行安全保护。Peer两侧必须都使能MD5认证，且配置的密码相同。配置该功能后，发送端PEER发送的MSDP消息进行MD5加密，再通过TCP连接传送到接收端PEER，接收端PEER根据统一的MD5加密规则以及报文中包含的密钥，对该MSDP消息进行解密，成功后上送给MSDP模块处理该MSDP消息。

  只有通过MD5认证的MSDP消息，才进行处理，从而阻止非法的恶意消息攻击。

- MSDP Keychain认证

  组播MSDP支持Keychain，通过使用Keychain和新的TCP扩展选项，每条TCP连接能够让用户配置一组密码，每个密码可以设置不同加密算法和有效期限，密码可以随时更换，大大提高了加密报文的安全性。

  只有通过了Keychain认证的消息，才进行处理，从而阻止非法的恶意消息攻击。

MD5属于不安全的认证算法，为了保证更好的安全性，建议您使用更安全的Keychain算法作为MSDP的认证算法。

## 配置方法

- PIM邻居过滤

  在公网实例下，配置VLANIF10接口与地址为10.4.4.4的交换机建立PIM邻居。

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 10.4.4.4 0.0.0.0
[HUAWEI-acl-basic-2001] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] pim neighbor-policy 2001
```

- PIM加入过滤

  在公网实例下，配置VLANIF10接收组地址范围是225.1.0.0/16的Join信息。

```
<HUAWEI> system-view
[HUAWEI] acl number 2001
[HUAWEI-acl-basic-2001] rule permit source 225.1.0.0 0.0.255.255
[HUAWEI-acl-basic-2001] quit
[HUAWEI] multicast routing-enable
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] pim join-policy asm 2001
```

- MSDP keychain认证

  为地址为10.1.1.2的MSDP对等体配置Keychain名称是example的Keychain认证。

```
<HUAWEI> system-view
[HUAWEI] keychain example mode absolute
[HUAWEI-keychain-example] key-id 1
[HUAWEI-keychain-example-keyid-1] algorithm sha-256
[HUAWEI-keychain-example-keyid-1] key-string cipher YsHsjx_202206
[HUAWEI-keychain-example-keyid-1] quit
[HUAWEI-keychain-example] quit
[HUAWEI] multicast routing-enable
[HUAWEI] msdp
[HUAWEI-msdp] peer 10.1.1.2 connect-interface vlanif 100
[HUAWEI-msdp] peer 10.1.1.2 keychain example
```

### 检查加固结果

执行命令**display msdp** [ **vpn-instance** *vpn-instance-name* | **all-instance** ] **peer-status** [ *peer-address* ]，查看MSDP对等体的详细信息。

## 3.2.6 SVF 系统的安全

### 3.2.6.1 防止跨网络仿冒 Parent 攻击

### 攻击行为

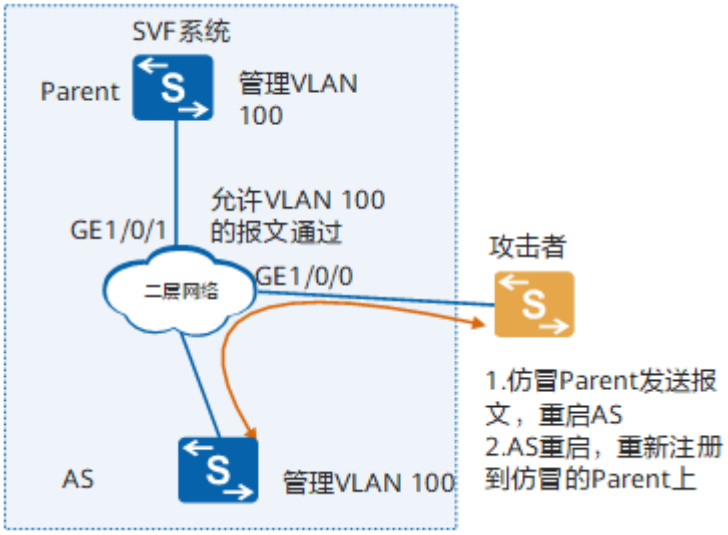
如图3-1所示，SVF系统的管理VLAN是100，AS跨网络连接Parent，中间的第三方网络上允许VLAN 100的报文通过。攻击者在VLAN100内通过仿冒Parent的方式向AS发送重启AS的报文，AS被重启后重新注册到攻击者仿冒的Parent上。

为避免这种攻击，有两种方法：

1. 配置攻击者可能连接的端口不加入VLAN 100。
2. 在攻击者可能连接的端口上配置DHCP Snooping功能，也可以同时配置ACL将CAPWAP报文丢弃。

**图 3-1** SVF 系统




## 安全策略

AS跨网络连接Parent时，AS和Parent之间的控制报文和数据报文会经过中间第三方网络，Parent和AS交互的控制报文在第三方网络上是非加密的数据报文。

为了提高SVF系统的安全性，防止有仿冒Parent的攻击者获取AS的控制权，用户可以在中间网络上将SVF系统的管理VLAN作为透传VLAN，避免攻击者发送的报文和SVF的管理报文在一个广播域。用户也可以在攻击者可能连接的中间网络端口上配置DHCP Snooping功能，避免攻击者仿冒Parent接管AS。

## 配置方法

在中间网络上配置DHCP Snooping功能。假如攻击者可能连接的端口是GE1/0/1，中间网络的网络侧端口是GE1/0/1。

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-Gigabitethernet1/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dhcp snooping trusted
```

## 检查加固结果

执行命令**display dhcp snooping configuration** [ **vlan** *vlan-id* | **interface** *interface-type interface-number* | **bridge-domain** *bd-id* ]，查看DHCP Snooping的配置信息。

## 3.2.6.2 CAPWAP 隧道加密

## 安全策略

Parent与AS之间通过CAPWAP隧道进行管理报文的传输，为了更好的保证隧道的私密性和安全性，用户可以选择对CAPWAP隧道进行DTLS加密，也可以修改加密敏感信息的共享加密密钥或配置CAPWAP报文完整性校验预共享密钥。

Parent与AS之间支持通过预共享密钥的方式对CAPWAP隧道进行加密，即Parent上和AS上分别预置一个密钥，当Parent与AS的预共享密钥吻合时，就可以成功协商并建立CAPWAP隧道。

在配置的过程中，需要注意的事项如下：

- 使能了DTLS隧道加密功能后，由于Parent与AS的CPU需要参与DTLS加密计算，AS上线性能会有所下降，因此建议在机密性要求非常高的场景，才使用DTLS加密功能。
- Parent和AS不能同时支持HA功能和CAPWAP隧道DTLS加密功能。如果同时开启这两个功能，当Parent发生主备倒换时，AS需要等待原来的CAPWAP链路自动老化后，才能重新建立新的CAPWAP链路，在此过程中AS业务会中断；当AS发生主备倒换时，AS会重新建立链路并上线，在此过程中AS业务也会中断。
- 当Parent切换CAPWAP隧道DTLS加密功能、修改加密敏感信息的共享加密密钥或配置CAPWAP报文完整性校验预共享密钥时，已经上线接入的AS会重新启动。
- 当有AS正在升级时，Parent不可以切换CAPWAP隧道DTLS加密功能、修改加密敏感信息的共享加密密钥或配置CAPWAP报文完整性校验预共享密钥。
- 在Parent使能了CAPWAP隧道DTLS加密功能且AS已上线接入的情况下，当在Parent上修改预共享密钥时，该密钥会自动下发至AS。建议用户不要在10分钟内重复修改密钥。

### 配置方法

配置CAPWAP隧道加密，需要分别在Parent上和AS上配置预共享密钥。

在Parent上配置预共享密钥。

```
<HUAWEI> system-view
[HUAWEI] capwap dtls psk YsHsjx_202208  //配置DTLS加密使用的预共享密钥为YsHsjx_202208
[HUAWEI] capwap dtls control-link encrypt  //使能控制隧道DTLS加密功能
[HUAWEI] capwap sensitive-info psk YsHsjx_202206  //修改敏感信息加密使用的预共享密钥为YsHsjx_202206
[HUAWEI] capwap message-integrity psk YsHsjx_202207  //配置CAPWAP报文完整性校验预共享密钥为YsHsjx_202207
```

在AS上配置预共享密钥。

```
<HUAWEI> as access dtls psk YsHsjx_202208  //配置DTLS加密使用的预共享密钥为YsHsjx_202208
```

### 检查加固结果

执行命令**display capwap configuration**，查看CAPWAP的配置信息。

## 3.2.7 NTP 的安全

### 安全策略

在对安全性要求较高的网络中，运行NTP协议时需要启用验证功能，用来防止恶意攻击造成时钟报文的数据更改。通过客户端和服务器端的密码验证，可以保证客户端只与通过验证的交换机进行同步，从而提高网络安全性。

### 配置方法

设置HMAC-SHA256身份验证密钥，密文密钥为"xyz123"，指定该密钥为可信密钥。

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication enable
```

```
[HUAWEI] ntp-service authentication-keyid 10 authentication-mode hmac-sha256 cipher xyz123
[HUAWEI] ntp-service reliable authentication-keyid 10
```

### 检查加固结果

执行命令**display current-configuration | include ntp-service**，查看ntp验证密钥信息。

## 3.2.8 MSTP 的安全

### 攻击行为

- 根桥变动攻击

  由于网络中的恶意攻击，网络中的合法根交换机有可能会收到优先级更高的BPDU报文，使得合法根交换机失去根交换机的地位，引起网络拓扑结构的错误变动。

- BPDU攻击

  边缘端口直接和用户终端相连，正常情况下，边缘端口不会收到BPDU报文。如果攻击者伪造BPDU恶意攻击交换机，当边缘端口接收到BPDU报文时，交换设备会自动将边缘端口设置为非边缘端口，并重新进行生成树计算，从而引起网络震荡。

### 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- 根保护

  为了防止根桥变动攻击，可以在交换机上部署根保护功能，通过维持指定端口的角色来保护根交换机的地位。

- BPDU保护

  为了防止BPDU攻击，可以在交换机上部署BPDU保护功能。

### 配置方法

- 配置根保护

  配置GE1/0/1的根保护功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] stp root-protection
  ```

- 配置BPDU保护

  配置交换机的BPDU保护功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] stp bpdu-protection
  ```

### 检查加固结果

执行命令**display stp**，查看生成树的状态和统计信息。

## 3.2.9 VRRP 的安全

### 攻击行为

单位时间内发送大量VRRP报文和构造不正确的VRRP协议报文来攻击交换机。

## 安全策略

针对以上攻击行为，可以在交换机上配置如下安全策略。

- 协议安全策略
  - 认证方式：VRRP支持在通告报文中设定不同的认证方式和认证字：包括无认证方式、简单字符（Simple）认证方式和MD5认证方式。目前仅VRRPv2版本支持认证。为了保证更好的安全性，建议您使用更安全的MD5算法作为VRRP的认证算法。
  - 报文校验：支持对备份组号、校验和、TTL、版本号、报文类型检测、定时器检测、虚拟地址个数、虚拟地址、报文长度检测等校验。交换机默认支持报文校验，不需要配置。
- 系统安全策略

  攻击报文抑制：如果单位时间内收到的报文数量大于20个或者为本机发出的报文，就认为该报文为攻击报文，直接丢弃。交换机默认支持攻击报文抑制，不需要配置。

## 配置方法

配置接口VLANIF100上VRID为1的备份组的认证方式为MD5认证，认证字为Example-1。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.1
[HUAWEI-Vlanif100] vrrp vrid 1 authentication-mode md5 Example-1
```

## 检查加固结果

执行命令**display vrrp**，查看当前VRRP备份组的状态信息和配置参数。

# 3.2.10 E-Trunk 的安全

## 安全策略

关于E-Trunk，交换机提供了如下安全策略。

- 为了提高系统的安全性，可以配置E-Trunk的加密密码。如果使用**simple**选项，密码将以明文形式保存在配置文件中，存在安全隐患。因此，建议使用**cipher**选项，将密码加密保存。
- 为了提高系统的安全性，可以配置E-Trunk的认证加密方式。**enhanced-hmac-sha256**算法较**hmac-sha256**、**hmac-sha1**安全，建议配置E-Trunk的认证加密方式使用**enhanced-hmac-sha256**算法。
- 缺省情况下，收发E-Trunk协议报文的UDP端口号是1025，可能存在与其他协议的UDP端口号冲突。为了保证E-Trunk协议报文正常转发，可以更改收发E-Trunk协议报文的UDP端口号。
- 当E-Trunk的主用设备发生故障时，为了防止非法用户通过获取主用设备发出的E-Trunk报文攻击备用设备，从而引起业务中断，可以使能E-Trunk序列号校验功能。

E-Trunk中的两端交换机上的加密密码、认证加密方式、序列号校验功能和UDP端口号必须一致。

## 配置方法

- 配置加密密码

  配置E-Trunk的密码为密文方式，密码为00E0FC000000。

  ```
  <HUAWEI> system-view
  [HUAWEI] e-trunk 1
  [HUAWEI-e-trunk-1] security-key cipher 00E0FC000000
  ```

- 配置认证加密方式

  配置E-Trunk1的认证加密方式为enhanced-hmac-sha256。

  ```
  <HUAWEI> system-view
  [HUAWEI] e-trunk 1
  [HUAWEI-e-trunk-1] authentication-mode enhanced-hmac-sha25
  ```

- 配置E-Trunk的端口号

  配置收发E-Trunk协议报文的UDP端口号1026。

  ```
  <HUAWEI> system-view
  [HUAWEI] e-trunk port 1026
  ```

  **说明**

  端口号取值范围是1025～65535。49152～65535由socket随机分配，配置收发E-Trunk协议报文的UDP端口号，建议不要配置这个范围段值，以免E-Trunk协议不可用。

- 使能序列号校验功能

  使能E-Trunk 1的序列号校验功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] e-trunk 1
  [HUAWEI-e-trunk-1] sequence enable
  ```

## 检查加固结果

执行命令**display e-trunk** { **brief** | *e-trunk-id* }，查看E-Trunk的信息。

# 3.2.11 EasyDeploy 系统的安全

## 安全策略

在批量升级和批量配置等场景下，为了增强Commander和Client之间通信的安全性，防止有仿冒的Commander获取Client的控制权，用户可以通过在Commander和Client上配置共享密钥。

- 共享密钥必须在Commander和Client上分别同时配置，且配置的密钥必须相同。
- 如果Commander上配置了shared-key，则此Commander不能管理V200R008C00版本以前的Client，也不能管理没有配置shared-key的Client。
- 共享密钥的配置不影响空配置设备部署。

## 配置方法

在Commander上配置共享密钥。

```
<HUAWEI> system-view
[HUAWEI] easy-operation shared-key cipher YsHsjx_202206
```

在Client上配置共享密钥。

```
<HUAWEI> system-view
[HUAWEI] easy-operation shared-key cipher YsHsjx_202206
```

### 检查加固结果

执行命令**display easy-operation configuration**，显示Commander的配置信息。

## 3.2.12 ICMPv6 防攻击

### 攻击行为

在网络正常的情况下，交换机可以正确接收ICMPv6报文。但是，在网络流量较大时，如果频繁出现主机不可达、端口不可达的现象，则交换机会接收大量的ICMPv6报文，这样会增大网络的流量负担，明显降低交换机的性能。同时，网络攻击者经常利用ICMPv6差错报文非法刺探网络内部结构以达到攻击目的。

### 安全策略

为了提高网络性能和增强网络安全，可以去使能系统接收ICMPv6应答报文、主机不可达报文、端口不可达报文功能，防止针对这些ICMPv6报文的安全攻击。

### 配置方法

去使能系统接收ICMPv6应答报文、主机不可达报文、端口不可达报文功能。

```
<HUAWEI> system-view
[HUAWEI] undo ipv6 icmp echo-reply receive
[HUAWEI] undo ipv6 icmp port-unreachable receive
[HUAWEI] undo ipv6 icmp host-unreachable receive
```

在网络状态良好的情况下，当需要恢复系统对ICMPv6报文的处理功能时，可以使能系统接收ICMPv6报文的功能。

```
<HUAWEI> system-view
[HUAWEI] ipv6 icmp all receive
```

### 检查加固结果

- 执行命令**display ipv6 interface** [ *interface-type interface-number* | **brief** ]，查看接口IPv6信息。
- 执行命令**display icmpv6 statistics** [ **interface** *interface-type interface-number* ]，查看ICMPv6流量统计信息。

## 3.2.13 携带路由选项的 IP 报文防攻击

### 攻击行为

攻击者向交换机发送大量携带路由选项的IP报文，导致交换机的转发性能下降，资源耗尽无法接受正常用户的请求，处于拒绝服务的状态。

### 安全策略

交换机支持IP报文可以携带路由选项，路由选项包括：

- 记录路径（RR）：记录转发路径上每台交换机的IP地址。
- 时间戳（TS）：记录转发路径上每台交换机的IP地址和时间。
- 源路由选项（SRR）：包括宽松的源路由选路（LSRR）和严格的源路由选路（SSRR）。

  - LSRR：为IP报文指定一系列必须经过的IP地址。
  - SSRR：为IP报文指定一系列必须经过的IP地址，且不能经过其他的IP地址。
- 路由告警（RA）：表示报文需要上送到路由协议层处理。

可以在接口视图下执行命令**discard** { **srr** | **rr** | **ra** | **ts** }避免交换机受到携带路由选项的IP报文的攻击。

## 配置方法

配置交换机丢弃带路由选项的IP报文。请根据不同的路由选项进行如下配置。

- 在接口VLANIF100上配置丢弃带记录路由选项的报文。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] discard rr
[HUAWEI-Vlanif100] quit
```

- 在接口VLANIF100上配置丢弃带时间戳选项的报文。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] discard ts
[HUAWEI-Vlanif100] quit
```

- 在接口VLANIF100上配置丢弃带IP源路由选项的报文。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] discard srr
[HUAWEI-Vlanif100] quit
```

- 在接口VLANIF100上配置丢弃带路由告警选项的报文。

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] discard ra
[HUAWEI-Vlanif100] quit
```

## 检查加固结果

执行命令**display current-configuration interface**，查看接口下的配置。

# 3.2.14 IP 地址欺骗防攻击

## 攻击行为

随着网络规模越来越大，通过伪造源IP地址实施的网络攻击（简称IP地址欺骗攻击）也逐渐增多。一些攻击者通过伪造合法用户的IP地址获取网络访问权限，非法访问网络，甚至造成合法用户无法访问网络，或者信息泄露。

## 安全策略

IPSG是一种基于二层接口的源IP地址过滤技术，它能够防止恶意主机伪造合法主机的IP地址来仿冒合法主机，还能确保非授权主机不能通过自己指定IP地址的方式来访问网络或攻击网络。

IPSG利用绑定表（源IP地址、源MAC地址、所属VLAN、入接口的绑定关系）去匹配检查二层接口上收到的IP报文，只有匹配绑定表的报文才允许通过，其他报文将被丢弃。

绑定表包括静态和动态两种。

- 基于静态绑定表的IPSG适用于局域网络中主机数较少且主机使用静态配置IP地址的情况。
- 基于动态绑定表的IPSG适用于局域网络中主机较多，或者主机使用DHCP动态获取IP地址的情况。

## 配置方法

- 配置基于静态绑定表的IPSG

  静态绑定表项括IPv4和IPv6两种绑定表项，请根据网络环境选择配置。以配置IPv4为例介绍配置方法。

  ```
  <HUAWEI> system-view
  [HUAWEI] user-bind static ip-address 10.0.0.1 mac-address 00e0-fc12-3456  //创建静态绑定表项
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] ip source check user-bind enable  //使能IPSG功能，可以在接口或者VLAN上使能该功能，请根据需要选择
  [HUAWEI-GigabitEthernet1/0/1] ip source check user-bind alarm enable  //使能IP报文检查告警功能
  [HUAWEI-GigabitEthernet1/0/1] ip source check user-bind alarm threshold 200  //丢弃报文阈值到达200将上报告警
  [HUAWEI-GigabitEthernet1/0/1] quit
  ```

- 配置基于动态绑定变的IPSG

  动态绑定表项包括IPv4和IPv6两种绑定表项，请根据网络环境选择配置。下面以通过DHCP方式获取IP地址的IPv4主机，可以配置DHCP Snooping生成DHCP Snooping动态绑定表项为例介绍配置方法。

  ```
  <HUAWEI> system-view
  [HUAWEI] dhcp enable
  [HUAWEI] dhcp snooping enable
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] dhcp snooping enable
  [HUAWEI-GigabitEthernet1/0/1] dhcp snooping trusted
  [HUAWEI-GigabitEthernet1/0/1] ip source check user-bind enable  //使能IPSG功能，可以在接口或者VLAN上使能该功能，请根据需要选择
  [HUAWEI-GigabitEthernet1/0/1] ip source check user-bind alarm enable  //使能IP报文检查告警功能
  [HUAWEI-GigabitEthernet1/0/1] ip source check user-bind alarm threshold 200  //丢弃报文阈值到达200将上报告警
  [HUAWEI-GigabitEthernet1/0/1] quit
  ```

## 检查加固结果

执行命令**display ip source check user-bind interface** *interface-type interface-number*，查看接口下IPSG的配置信息。

# 3.2.15 数据传输的安全

## 安全策略

在网络中为了防止数据在传输过程中被窃取和仿冒，可以通过IPSec对数据进行加密认证保护。

用IPSec保护数据之前，必须先建立安全联盟SA。SA是出于安全目的而创建的一个单向逻辑连接，是IPSec对等体（使用IPSec协议对数据进行保护的通信双方）之间对某些要素的约定。这些要素包括：

- 对等体间使用何种安全协议
- 安全协议支持的认证/加密算法
- 数据的封装模式

- SA的安全参数索引SPI（Security Parameter Index）
- SA的认证密钥/加密密钥

其中，前三项要素是通过IPSec安全提议来指定的。实际配置中，需要在IPSec对等体上先配置IPSec安全提议，再配置IPSec安全联盟。

## 配置方法

1. 配置IPSec安全提议

```
<HUAWEI> system-view
[HUAWEI] ipsec proposal newprop1  //创建名称为newprop1的IPSec安全提议
[HUAWEI-ipsec-proposal-newprop1] transform esp  //配置安全提议newprop1的安全协议为ESP
[HUAWEI-ipsec-proposal-newprop1] esp authentication-algorithm sha2-256  //配置ESP协议使用的认证算法为SHA-256
[HUAWEI-ipsec-proposal-newprop1] esp encryption-algorithm aes 256  //配置ESP协议的加密算法为AES-256
[HUAWEI-ipsec-proposal-newprop1] encapsulation-mode transport  //配置安全协议对数据的封装模式为transport
[HUAWEI-ipsec-proposal-newprop1] quit
```

2. 配置IPSec安全联盟

```
[HUAWEI] ipsec sa sa1  //创建安全联盟sa1
[HUAWEI-ipsec-sa-sa1] proposal newprop1  //指定安全联盟sa1引用名称为newprop1的IPSec安全提议
[HUAWEI-ipsec-sa-sa1] sa spi inbound esp 10000  //设置入方向SA的SPI为10000
[HUAWEI-ipsec-sa-sa1] sa spi outbound esp 20000  //设置出方向SA的SPI为20000
[HUAWEI-ipsec-sa-sa1] sa authentication-hex inbound esp cipher 112233445566778899aabbccddeeff00  //设置入方向SA的认证密钥为112233445566778899aabbccddeeff00
[HUAWEI-ipsec-sa-sa1] sa authentication-hex outbound esp cipher aabbccddeeff001100aabbccddeeff00  //设置出方向SA的认证密钥为aabbccddeeff001100aabbccddeeff00
```

## 检查加固结果

- 执行命令**display ipsec proposal** [ **name** *proposal-name* ]，查看IPSec安全提议的信息。
- 执行命令**display ipsec sa** [ **name** *sa-name* ] [ **brief** ]，查看安全联盟的配置信息。
- 执行命令**display ipsec statistics** [ **sa-name** *sa-name* **slot** *slot-number* ]，查看IPSec处理报文的统计信息。

# 3.2.16 IPv6 ND 协议的安全

## 攻击行为

在网络中，常见的ND攻击有如下两种情况：

- 地址欺骗攻击：攻击者仿冒其他用户的IP地址发送邻居请求报文NS/邻居通告报文NA/路由器请求报文RS，会改写网关上或者其他用户的ND表项，导致被仿冒用户无法正常接收报文，从而无法正常通信。同时攻击者通过截获被仿冒用户的报文，可以非法获取用户的游戏、网银等帐号口令，会造成这些用户的重大利益损失。
- RA攻击：攻击者仿冒网关向其他用户发送路由器通告报文RA，会改写其他用户的ND表项或导致其它用户记录错误的IPv6配置参数，造成这些用户无法正常通信。

## 安全策略

为了避免上述ND攻击带来的危害，交换机提供了ND Snooping功能以对ND攻击进行防范。ND Snooping是针对IPv6 ND的一种安全特性，用于二层交换网络环境。通过侦

听用户重复地址检测DAD过程的邻居请求报文NS来建立ND Snooping动态绑定表，从而记录下报文的源IPv6地址、源MAC地址、所属VLAN、入端口等信息，以防止后续仿冒用户、仿冒网关的ND报文攻击。

### 配置方法

使能ND Snooping功能时，必须先全局使能ND Snooping功能，再在接口或VLAN下使能ND Snooping功能。

在接口视图下使能时，则对特定接口生效；在VLAN视图下使能时，则对加入该VLAN的所有接口生效。

如果配置了接口为ND Snooping信任接口，则该接口会自动使能ND Snooping功能，无需再在该接口或VLAN下使能ND Snooping功能。

下面以在VLAN视图下配置ND Snooping为例，介绍ND Snooping的配置方法。

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable  //全局使能ND Snooping功能
[HUAWEI] vlan 10
[HUAWEI-vlan10] nd snooping enable  //在VLAN10内使能ND Snooping功能
[HUAWEI-vlan10] nd snooping check ns enable  //使能NS协议报文合法性检查功能
[HUAWEI-vlan10] nd snooping check na enable  //使能NA协议报文合法性检查功能
[HUAWEI-vlan10] nd snooping check rs enable  //使能RS协议报文合法性检查功能
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 1/0/3
[HUAWEI-GigabitEthernet1/0/3] nd snooping trusted  //配置GE1/0/3为信任接口
[HUAWEI-GigabitEthernet1/0/3] quit
```

从V200R010版本开始，支持在DHCPv6 Only场景下配置ND Snooping功能。DHCPv6 Only场景下，仅允许用户通过DHCPv6方式获取IPv6地址，用户私自配置IPv6地址和通过PD地址前缀自动生成IPv6地址被视为非法地址。在该场景下，为防止非法地址生成ND Snooping绑定表，会关闭ND Snooping功能。但这会导致无法进行ND协议报文合法性检查使网络存在地址欺骗攻击的风险。为解决该问题，可以配置命令**nd snooping enable dhcpv6 only**和**nd snooping trusted dhcpv6 only**，两个命令分别指的是开启DHCPv6 Only场景的ND Snooping功能和配置DHCPv6 Only场景的接口为ND Snooping信任接口。

### 检查加固结果

- 执行命令**display nd snooping statistics**，查看设备接收与丢弃的ND Snooping用户报文统计信息。
- 执行命令**display nd snooping configuration**，查看ND Snooping的配置信息。

# 3.3 转发平面

## 3.3.1 访问控制列表 ACL

### 安全策略

通过ACL可以实现对网络中报文流的精确识别和控制，达到控制网络访问行为、防止网络攻击和提高网络带宽利用率的目的，从而切实保障网络环境的安全性和网络服务质量的可靠性。

访问控制列表ACL是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。ACL通过规则对数

据包进行分类，这些规则应用到交换机上，交换机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。例如可以用访问列表描述：拒绝任何用户终端使用Telnet登录本机，允许每个用户终端经由SMTP向本机发送电子邮件。

每个ACL中可以定义多个规则，根据规则的功能分为：基本ACL、基本ACL6、高级ACL、高级ACL6、二层ACL和用户自定义ACL。

其中：

- 基本ACL、基本ACL6、二层ACL属于Level-1级别
- 高级ACL、高级ACL6、用户自定义ACL属于Level-2级别

本节内容只介绍Level-2级别的ACL，Level-1级别的ACL请参看**2.4.1 访问控制列表ACL**。

**表3-1**所示，基于ACL规则定义方式的划分如下。

**表 3-1** 基于 ACL 规则定义方式的 ACL 分类

| 分类 | 适用的IP版本 | 规则定义描述 | 编号范围 |
| --- | --- | --- | --- |
| 高级ACL | IPv4 | 既可使用IPv4报文的源IP地址，也可使用目的IP地址、IP协议类型、ICMP类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则。 | 3000～3999 |
| 用户自定义ACL | IPv4&IPv6 | 使用报文头、偏移位置、字符串掩码和用户自定义字符串来定义规则，即以报文头为基准，指定从报文的第几个字节开始与字符串掩码进行“与”操作，并将提取出的字符串与用户自定义的字符串进行比较，从而过滤出相匹配的报文。 | 5000～5999 |
| 高级ACL6 | IPv6 | 可以使用IPv6报文的源IPv6地址、目的IPv6地址IPv6协议类型、ICMPv6类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则。 | 3000～3999 |

## 配置方法

配置ACL 3000，匹配基于icmp protocol type的流分类。

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 1 permit icmp
```

## 检查加固结果

执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }，查看ACL的配置信息。

## 3.3.2 端口保护

### 安全策略

网络中，主机一般使用缺省网关与外部网络联系，如果缺省网关出接口发生故障，主机与外部网络的通信将被中断，无法保证业务的正常传输。端口保护功能很好的解决了这个问题。在不改变组网的情况下，将交换机上的两个接口组成一个端口保护组，实现主备接口的备份。当主用接口出现异常时，业务及时切换到备用接口上，以保证业务的无中断传输。

在正常工作状态下，主用接口承载业务数据传输。当主用接口发生故障，状态变为Down时，系统将自动切换业务到备用接口上，以保证业务的正常传送，提高交换机的可靠性。当备用接口承载业务后，如果主用接口恢复正常，业务也不会回切到主接口，只有当备用接口故障时，才会切换到主用接口。

一个端口保护组中只能包含一个主用接口和一个备用接口。

### 配置方法

配置端口保护组，将GE1/0/1作为主用接口、GE1/0/2作为备用接口加入到端口保护组中。

```
<HUAWEI> system-view
[HUAWEI] port protect-group 1
[HUAWEI-protect-group1] protect-group member gigabitethernet 1/0/1 master
[HUAWEI-protect-group1] protect-group member gigabitethernet 1/0/2 standby
```

### 检查加固结果

执行命令**display port protect-group** { **all** | *protect-group-index* }，查看端口保护组的成员接口信息。

## 3.3.3 端口隔离

### 安全策略

为了实现报文之间的二层隔离，用户可以将不同的端口加入不同的VLAN，但这样会浪费有限的VLAN资源。采用端口隔离功能，可以实现同一VLAN内端口之间的隔离。用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。

如果用户希望隔离同一VLAN内的广播报文，但是不同端口下的用户还可以进行三层通信，则可以将隔离模式设置为二层隔离三层互通；如果用户希望同一VLAN不同端口下用户彻底无法通信，则可以将隔离模式配置为二层三层均隔离即可。

### 配置方法

端口隔离包括双向隔离和单向隔离。缺省情况下，端口隔离模式是二层隔离三层互通，若需要配置二三层都隔离可以执行**port-isolate mode all**命令配置。

- 配置端口隔离组

  配置GE1/0/1和GE1/0/2进行隔离。

  配置GE1/0/1的端口隔离功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] port-isolate mode all
  ```

```
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port-isolate enable group 3
```

配置GE1/0/2的端口隔离功能。

```
<HUAWEI> system-view
[HUAWEI] port-isolate mode all
[HUAWEI] interface gigabitethernet 1/0/2
[HUAWEI-GigabitEthernet1/0/2] port-isolate enable group 3
```

- 配置单向隔离

  配置GE1/0/1和GE1/0/2单向隔离。

  ```
  <HUAWEI> system-view
  [HUAWEI] port-isolate mode all
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] am isolate gigabitethernet 1/0/2
  ```

## 检查加固结果

执行命令**display port-isolate group** { *group-id* | **all** }，查看端口隔离组的配置。

# 3.3.4 端口安全

## 安全策略

在对接入用户的安全性要求较高的网络中，可以配置端口安全功能，将接口学习到的MAC地址转换为安全动态MAC、安全静态MAC或Sticky MAC，接口学习的最大MAC数量达到上限后不再学习新的MAC地址，只允许这些MAC地址和交换机通信。这样可以阻止其他非信任的MAC主机通过本接口和交换机通信，提高交换机与网络的安全性。

## 配置方法

- 配置安全MAC功能

  配置GE1/0/1下最大只允许接入两个PC，因此限制接入安全MAC数量为2。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] port-security enable
  [HUAWEI-GigabitEthernet1/0/1] port-security max-mac-num 2
  [HUAWEI-GigabitEthernet1/0/1] port-security protect-action restrict
  [HUAWEI-GigabitEthernet1/0/1] quit
  ```

- 配置Sticky MAC功能

  配置GE1/0/1的Sticky MAC功能。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] port-security enable
  [HUAWEI-GigabitEthernet1/0/1] port-security mac-address sticky
  [HUAWEI-GigabitEthernet1/0/1] port-security max-mac-num 5
  [HUAWEI-GigabitEthernet1/0/1] quit
  ```

## 检查加固结果

- 执行命令**display mac-address security** [ **vlan** *vlan-id* | *interface-type interface-number* ] * [ **verbose** ]，查看安全动态MAC表项。
- 执行命令**display mac-address sec-config** [ **vlan** *vlan-id* | *interface-type interface-number* ] * [ **verbose** ]，查看配置的安全静态MAC表项。
- 执行命令**display mac-address sticky** [ **vlan** *vlan-id* | *interface-type interface-number* ] * [ **verbose** ]，查看Sticky MAC表项。

# 3.3.5 MAC 地址防漂移

## 安全策略

网络中产生环路或非法用户进行网络攻击都会造成MAC地址发生漂移，导致MAC地址不稳定。可以通过两种方法来避免这种情况：

- 提高接口MAC地址学习优先级

  接口配置不同的MAC地址学习优先级后，如果不同接口学到相同的MAC地址表项，那么高优先级接口学到的MAC地址表项可以覆盖低优先级接口学到的MAC地址表项，防止MAC地址发生漂移。

- 不允许相同优先级接口MAC地址漂移

  网络中交换机的上行接口连接服务器，下行接口连接用户。为防止非法用户伪造服务器MAC地址入侵交换机，可以配置不允许相同优先级的接口发生MAC地址漂移。这样接口将不再学习相同的MAC地址，非法用户将无法使用网络设备MAC地址干扰交换机与网络设备正常通信。

## 配置方法

- 配置接口MAC地址学习优先级

  GE1/0/1为网络侧端口，GE1/0/2为用户侧端口，可以配置GE1/0/1学习MAC地址优先级为3，高于GE1/0/2的默认优先级0。

  ```
  <HUAWEI> system-view
  [HUAWEI] interface gigabitethernet 1/0/1
  [HUAWEI-GigabitEthernet1/0/1] mac-learning priority 3
  ```

- 配置不允许相同优先级接口MAC地址漂移（缺省情况下，允许相同优先级的接口发生MAC地址漂移）

  配置不允许优先级为1的接口发生MAC地址漂移。

  ```
  [HUAWEI] undo mac-learning priority 1 allow-flapping
  ```

## 检查加固结果

- 执行命令**display current-configuration**，查看配置结果。

# 4 参考文档

如果您需要了解文档中所描述的功能的更加详细的内容，请您可以通过华为官网浏览和获取相应的产品文档。

- 交换机维护宝典中的“故障处理：防攻击”。
- 交换机产品文档中的“安全配置”。