UNIS 交换机安全加固手册（Uniware V7）

目 录

1 本书约定

1.1 读者对象

本手册主要适用于如下工程师：

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

1.2 接口编号约定

本手册中出现的接口编号仅作示例，并不代表设备上的实际接口编号。实际使用过程中，请以设备上存在的接口编号为准。

1.3 特别申明

本文档不严格与具体软、硬件版本对应，如果使用过程中与产品实际情况有差异，请以设备实际情况为准。

本文档中的配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下举例中的配置不冲突。

本文中的内容为通用性技术信息，某些信息可能不适用于您所购买的产品。

2 概述

本文档针对基于 Uniware V7 系统的交换机，指导用户从管理平面、控制平面和转发平面对设备进行加固维护。

2.1 安全威胁

2.1.1 管理平面和控制平面的安全威胁

设备的管理平面给网络管理人员提供 Telnet、SSH、Web、SNMP 等方式来管理设备；设备的控制平面用于控制和管理所有网络协议的运行，为转发平面提供数据转发所必须的各种网络信息和转发查询表项。

由于网络设备之间或网络设备与其它网络实体之间的通信可能会穿过各种各样的中间系统，而中间系统的可信性以及对端身份的真实性会给设备的管理平面和控制平面带来各种安全威胁。另外，如果设备上的安全策略配置不当，也会威胁到设备的安全。

设备的管理平面和控制平面常见的安全威胁主要包括以下几类：

- 非授权的访问

攻击者通过伪装身份、重放管理会话或者中间人攻击来获取管理员权限，这会危害到设备的安全以及设备所处网络的安全。建议管理员使用强身份认证，以及支持防重放、信息完整性验证的安全通道来访问设备。同时，建议在设备上启用操作日志、安全日志功能对管理行为进行记录和审计。

- 弱密钥

  弱密钥很容易被破解。设备上支持启用密码策略来防止用户配置弱密钥。

- 敏感信息泄漏

  由于网络节点间的通信所经过的中间系统的可信性无法保障，通信内容可能会被窥探；设备存储介质中的信息也可能在介质转移、替换的过程中存在信息泄露的风险。为了防止信息泄露，设备的管理通道需要使用安全协议保护，例如 SSH、IPsec、SFTP、HTTPS 等，禁止使用 Telnet、FTP、TFTP、HTTP 等没有保护的通道进行通信。另外，建议使用配置文件加密功能，以及对从现网替换下来且不再使用的存储介质进行格式化。

- 消息篡改和伪造

  报文在网络中传输的过程中，可能会被恶意篡改，或者被攻击者捕获之后重放，攻击者借此向设备中注入恶意的数据，或直接破坏设备的合法数据。例如，通过更改路由协议报文的数据来破坏或改变设备的路由表，使用户的流量无法正常转发。为防止该类型攻击，可使用带完整性验证，防重放等功能的安全协议对数据进行保护。

- DDoS

  DDoS（Distributed Denial of Service，分布式拒绝服务）是指攻击者利用大流量来消耗设备的 CPU、内存、连接数、带宽等资源，使合法用户无法使用网络。可使用白名单，黑名单，以及限制未识别流量上送控制平面的速率来防止此类攻击。

- 管理员配置失误

  管理员配置失误会造成设备的访问控制策略、权限控制策略的配置错误，或者造成授权不当的结果。为了及早发现此类问题，可以通过实施前对配置进行审核，实施后定期观察实施效果、查看操作日志和系统运行日志来发现配置中的错误。

2.1.2 转发平面的安全威胁

设备的转发平面需要处理各端口上大量不同类型数据流量的转发任务。如果数据流量不合法，或者转发平面处理资源被挤占，将会影响设备对正常数据流量的处理效率，甚至导致非法流量向网络中扩散。常见的转发平面威胁如下：

- 畸形报文攻击

  畸形报文攻击利用网络设备处理报文的漏洞使设备出现异常，使设备无法提供正常服务。可以打开攻击检测与防范中相应攻击的开关来防止此类攻击。

- DDoS 攻击

  攻击者使用大流量对设备进行攻击，消耗设备的 CPU、内存、连接、带宽等资源。对于这类威胁，可以通过限制设备资源占用以及识别合法用户等措施，尽量保证已识别的合法用户对网络的使用，并对未识别的用户的流量进行一定限制。

- 身份仿冒

  网络中的很多攻击行为都伴随着身份仿冒，而网络的开放性给身份识别带来了困难，尤其是在转发平面。转发平面提供了一些基本的方法可在一定程度上防止身份仿冒，比如 IP Source Guard、SYN Cookie、ARP/ND 检测等。

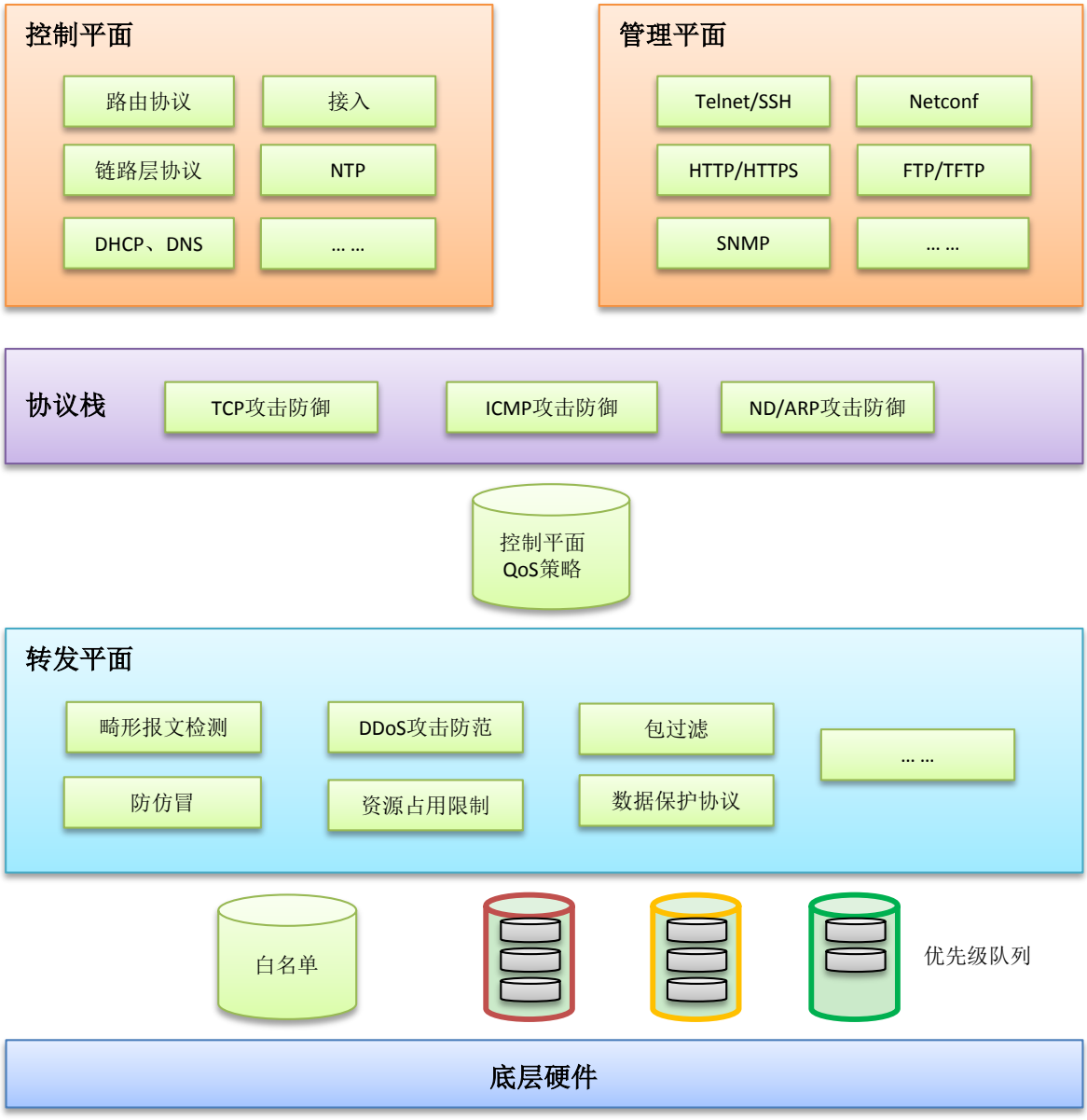
- 消息篡改和伪造

  消息的完整性至关重要，虚假的数据会使网络故障、甚至瘫痪。可以使用 IPsec、MACsec 等安全协议来保护网络数据，提供完整性、私密性、身份验证等功能。

2.2 安全体系架构

Uniware 系统的安全体系架构如图 2-1 所示：

图2-1 Uniware 系统安全体系架构图



设备基于以上安全体系架构在不同层面实施相应的安全防护，具体过程如下：

(1) 对于硬件转发类设备，收到目的地址为本机的报文并上送 CPU 处理前，会通过以下两种通道机制来保证上层的控制平面/管理平面不会受到 DoS/DDoS 等大流量的攻击：

- 白名单：对于已经建立连接，并确认来源是可靠的报文，设备会下发白名单保证其优先上送 CPU。
- 优先级队列：对于由控制平面、管理平面处理的应用流量，在设备没有与其建立连接之前，因不能匹配到白名单，会进入优先级队列，根据不同的应用优先级处理。

(2) 对于由转发平面转发的报文，设备提供了一系列的措施来保证设备的安全和网络用户的安全：

- 畸形报文检测
- 包过滤
- 防仿冒，例如 uRPF、IP Source Guard
- DDoS 攻击防范
- 资源占用限制：包括连接数限制、ARP/ND 表项限制等等，防止 DDoS 等恶意流量攻击。
- 数据保护协议：IPsec、MACSec 等，为本机和用户数据提供数据私密性、完整性、放重放等安全保护。

(3) 对于目的地址为本机的业务报文，可以采用以下安全加固策略：

a. 通过控制平面的 QoS 策略对上送控制平面/管理平面的流量进行限制，例如限制带宽等。另外，各协议本身（TCP、ICMP/ICMPv6、ARP/ND）也有相应的防护措施。

b. 在控制平面/管理平面，各业务模块采用相应的安全协议或安全选项，对业务报文提供更好的安全服务。

2.3 安全加固的基本原则

虽然设备可提供丰富的安全加固策略，但对于设备而言，并不是实施的安全加固策略越多效果越好。每一项安全加固措施对网络、业务都有或多或少的影响，比如会影响设备性能、内存资源、部署成本、用户使用习惯。所以，需要根据网络和业务的特点来综合评估可能存在的风险和威胁，并在充分了解到各类安全加固策略可能对网络和业务产生的影响后作出恰当的选择。

安全加固策略选择的普遍原则如下：

- 根据安全风险和威胁发生的可能性由大到小的顺序，依次考虑相应的安全加固策略；
- 按照安全加固策略对网络和业务影响程度由小到大的顺序，逐步实施各策略，并观察效果；
- 每一次安全加固策略实施后要观察效果，并根据效果调整当前策略以及选择后续的加固策略；
- 遵循业务优先原则，将安全加固策略对业务的影响降到最低，或者将其控制在可接受的范围内。

3 管理平面安全加固

3.1 登录及访问设备的安全

3.1.1 通过 Console 口/USB 口登录设备

【安全威胁】

Console 口/USB 口均属于物理接口，通过它们进行登录是登录设备的基本方式之一。

缺省情况下，通过 Console 口登录时认证方式为 none，可直接登录，登录成功之后用户角色为 network-admin。通过 USB 口登录时认证方式为 none，可直接登录，登录成功之后用户角色为 network-admin。

如果攻击者获取了 Console 口/USB 口的使用权限，在缺省情况下可以非常容易登录到设备上，获取到设备的管理权限。

【安全加固策略】

可以在用户线/用户线类视图下配置以下两种认证方式，提高通过 Console 口/USB 口登录设备的安全性：

- password 方式：表示下次使用该用户线登录时，需要输入密码。只有密码正确，用户才能登录到设备上。配置认证方式为 password 后，请妥善保存密码。FIPS 模式下不支持该认证方式。
- scheme 方式：表示下次使用该用户线登录设备时需要进行用户名和密码认证，用户名或密码错误，均会导致登录失败。配置认证方式为 scheme 后，请妥善保存用户名及密码。

【注意事项】

改变 Console 口/USB 口登录的认证方式后，新认证方式对新登录的用户生效。

FIPS 模式下，不支持 password 和 none 方式，仅支持 scheme 方式。

【配置举例】

- 通过 Console 口登录（以 Console 用户线视图为例）

  # 在 Console 用户线视图下设置认证方式为密码认证（password 方式）。

  ```
  <Sysname> system-view
  [Sysname] line console 0
  [Sysname-line-console0] authentication-mode password
  ```

  # 设置认证密码为明文 Plat&0631!（Plat&0631!仅为示例）。

  ```
  [Sysname-line-console0] set authentication password simple Plat&0631!
  ```

  # 在 Console 用户线视图下设置认证方式为 AAA 认证（scheme 方式）。

  ```
  <Sysname> system-view
  [Sysname] line console 0
  [Sysname-line-console0] authentication-mode scheme
  [Sysname-line-console0] quit
  ```

  # 在 ISP 域视图下为 login 用户配置认证方法。

  如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

- 通过 Console 口登录（以 AUX 用户线视图为例）

  # 在 AUX 用户线视图下设置认证方式为密码认证（password 方式）。

  ```
  <Sysname> system-view
  [Sysname] line aux 0
  [Sysname-line-aux0] authentication-mode password
  ```

  # 设置认证密码为明文 Plat&0631!（Plat&0631!仅为示例）。

  ```
  [Sysname-line-aux0] set authentication password simple Plat&0631!
  ```

  # 在 AUX 用户线视图下设置认证方式为 AAA 认证（scheme 方式）。

  ```
  <Sysname> system-view
  [Sysname] line aux 0
  [Sysname-line-aux0] authentication-mode scheme
  ```

在 ISP 域视图下为 login 用户配置认证方法。

如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

- 通过 USB 口登录（以 USB 用户线视图为例）

  # 在 USB 用户线视图下设置认证方式为密码认证（password 方式）。

  ```
  <Sysname> system-view
  [Sysname] line usb 0
  [Sysname-line-usb0] authentication-mode password
  ```

  # 设置认证密码为明文 Plat&0631!（Plat&0631!仅为示例）。

  ```
  [Sysname-line-usb0] set authentication password simple Plat&0631!
  ```

  # 在 USB 用户线视图下设置认证方式为 AAA 认证（scheme 方式）。

  ```
  <Sysname> system-view
  [Sysname] line usb 0
  [Sysname-line-usb0] authentication-mode scheme
  ```

  # 在 ISP 域视图下为 login 用户配置认证方法。

  如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

3.1.2 通过 Stelnet 登录设备

【安全威胁】

在使用 Stelnet 登录设备的组网环境中，设备将会面临以下安全威胁：

- 攻击者监听到设备的 SSH 服务端口后，可通过多次尝试连接，获取设备的访问权限。
- 设备可支持的 SSH 用户数有限，攻击者通过伪造 IP 地址，仿冒大量的合法用户登录设备，使得用户数达到上限后，其他合法用户无法登录。

【安全加固策略】

针对以上攻击行为，可以在设备上配置如下安全策略：

- password 认证

  利用 AAA 对客户端身份进行认证。用户在客户端上输入用户名和密码后，该密码将被加密后发送给服务器，通过服务器验证用户名和密码的合法性后，用户才可以登录设备。

- publickey 认证

  采用数字签名的方式来认证客户端。客户端发送包含用户名、公钥和公钥算法或者携带公钥信息的数字证书的认证请求给服务器端。服务器对公钥进行合法性检查，如果合法，则发送消息请求客户端的数字签名；如果不合法，则直接发送失败消息；服务器收到客户端的数字签名之后，使用客户端的公钥对其进行解密，并根据计算结果返回认证成功或失败的消息。

- password-publickey 认证

  对于 SSH2 版本的客户端，要求同时进行 password 和 publickey 两种方式的认证，且只有两种认证均通过的情况下，才认为客户端身份认证通过；对于 SSH1 版本的客户端，只要通过其中任意一种认证即可。

- keyboard-interactive 认证

  该认证方式与 password 认证方式类似，相较于 password 认证，该认证方式提供了可变的交互信息。客户端进行 keyboard-interactive 认证时，如果远程认证服务器要求用户进行交互认证，则远程认证服务器会在发送给服务器端的认证回应消息中携带一个提示信息，该提示信息被服务器端透传给客户端，在客户端终端上显示并要求用户输入指定的信息。当用户提交正确的信息后，若远程认证服务器继续要求用户输入其它的信息，则重复以上过程，直到用户输入了所有远程认证服务器要求的信息后，远程认证服务器才会返回认证成功的消息。

- 关闭 Stelnet 服务

  当设备上开启 Stelnet 服务器功能后，SSH 服务端口号易被攻击者扫描到。安全起见，在不使用 Stelnet 服务时，可以关闭 Stelnet 服务器功能。

- 改变 SSH 服务端口号

  缺省情况下，SSH 服务的端口号为知名端口号 22，易被扫描和攻击。通过修改 SSH 服务的端口号为非知名端口号，可以降低被扫描的风险。

- 对 SSH 用户进行访问控制

  只有匹配 ACL 中 permit 规则的 IPv4 SSH 客户端可以访问设备,其他客户端不可以访问设备。

- 限制同时在线的最大 SSH 用户数

  当前在线 SSH 用户数超过设定的最大值时，系统会拒绝新的 SSH 连接请求。

【注意事项】

改变 Stelnet 登录的认证方式后，新认证方式对新登录的用户生效。

【配置举例】

- # 配置服务器采用 password 认证（用户名 client001 仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] ssh user client001 service-type stelnet authentication-type password
  ```

  # 若进行本地认证，则还需要创建本地用户；若在远程服务器（如 RADIUS 服务器）进行认证，则还需要在服务器上创建相应的 SSH 用户。相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

- # 配置服务器采用 publickey 认证（用户名 client002、公钥 clientkey 仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] ssh user client002 service-type stelnet authentication-type publickey assign publickey clientkey
  ```

  # 创建同名的本地用户，用于下发授权属性：工作目录、用户角色。相关配置的详细介绍请参见“安全配置指导”中的“AAA”

- # 关闭 Stelnet 服务。

  ```
  <Sysname> system-view
  [Sysname] undo ssh server enable
  ```

- # 设置 SSH 服务端口号为 1025（1025 仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] ssh server port 1025
  ```

- # 只允许 IPv4 地址为 1.1.1.1 的 SSH 用户向设备发起 SSH 访问（ACL2001 仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] acl basic 2001
  [Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
  ```

```
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ssh server acl 2001
```

- # 限制同时在线的最大 SSH 用户数为 16（16 仅为示例）。

```
<Sysname> system-view
[Sysname] aaa session-limit ssh 16
```

3.1.3 通过 RESTful 访问设备

【安全加固策略】

基于 HTTP 的 RESTful 方式登录设备并不安全，推荐用户使用基于 HTTPS 的 RESTful 方式登录设备。在设备上开启基于 HTTPS 的 RESTful 功能，可以进一步提高基于 HTTPS 的 RESTful 功能的安全性。

【配置举例】

开启基于 HTTPS 的 RESTful 功能。

```
<Sysname> system-view
[Sysname] restful https enable
```

3.1.4 通过 SNMP 访问设备

【安全威胁】

设备作为 SNMP Agent 时，将面临以下安全威胁：

- SNMPv1 和 SNMPv2c 的团体名被窃取，非法 NMS 使用该团体名访问设备。
- SNMP 报文被窃听、篡改。
- NMS 对一些重要参数误操作，导致设备不能正常工作。

【安全加固策略】

针对以上攻击行为，设备提供了以下功能来加强通过 SNMP 访问设备的安全性：

- 当不需要通过 NMS 管理设备时，可关闭 SNMP 功能。（SNMP 功能缺省处于关闭状态）
- 除了 SNMPv1、SNMPv2c 版本，设备支持安全性更高的 SNMPv3 三种版本。SNMPv3 采用用户名认证，可配置认证密码和加密密码。其中，
  - 用户名和认证密码用于对 NMS 进行身份认证，以免非法 NMS 访问设备；
  - 加密密码用于对 NMS 和设备之间传输的报文进行加密，以免报文被窃听。
- 支持 VACM 和 RBAC 两种访问控制方式。
  - VACM（基于视图的访问控制模型）：将团体名/用户名与指定的 MIB 视图进行绑定，可以限制 NMS 能够访问哪些 MIB 对象，以及对 MIB 对象可执行读操作还是读写操作。
  - RBAC（基于角色的访问控制）：创建团体名/用户名时，可以指定对应的用户角色，通过用户角色下制定的规则，来限制 NMS 能够访问哪些 MIB 对象，以及对 MIB 对象可执行读操作还是读写操作。

  RBAC 配置方式限制的是 MIB 节点的读写权限，VACM 配置方式限制的是 MIB 视图的读写权限，而一个视图中通常包括多个 MIB 节点。所以，RBAC 配置方式更精准、更灵活。
- 支持引用 ACL 限制可以登录的 NMS。
- 设备在发送告警信息可以携带安全参数，只有符合安全参数要求的 NMS 才能接收该告警信息。

【注意事项】

只有 NMS 和设备使用的 SNMP 版本、团体名（或者用户名、密码）相同时，NMS 才能和 Agent 建立连接。

【配置举例】

- 关闭 SNMP 功能。

  # 关闭 SNMP 功能。

  ```
  <Sysname> system-view
  [Sysname] undo snmp-agent
  ```

- 配置具有认证和加密机制的 SNMPv3 版本来管理设备，并通过用户角色控制 NMS 对 MIB 节点的访问权限

  # 配置设备支持 SNMPv3 版本。

  ```
  <Sysname> system-view
  [Sysname] snmp-agent sys-info version v3
  ```

  # 创建用户角色 test 并配置访问权限：用户只能读节点 snmpMIB（OID 为 1.3.6.1.6.3.1）下的对象，不可以访问其它 MIB 对象。（各参数仅为示例）

  ```
  [Sysname] role name test
  [Sysname-role-test] rule 1 permit read oid 1.3.6.1.6.3.1
  ```

  # 配置用户角色 test 具有 system（OID 为 1.3.6.1.2.1.1）的读权限与 interfaces（OID 为 1.3.6.1.2.1.2）的读写权限，以便接口状态变化时，Agent 会向 NMS 发送告警信息。（各参数仅为示例）

  ```
  [Sysname-role-test] rule 2 permit read oid 1.3.6.1.2.1.1
  [Sysname-role-test] rule 3 permit read write oid 1.3.6.1.2.1.2
  [Sysname-role-test] quit
  ```

  # 创建用户 RBACtest，为其绑定用户角色 test，认证算法为 SHA-1，认证密码为 123456TESTauth&!，加密算法为 AES，加密密码是 123456TESTencr&!。（各参数仅为示例）

  ```
  [Sysname] snmp-agent usm-user v3 RBACtest user-role test simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&!
  ```

- 配置 ACL 限制可以访问设备的 NMS

  # 创建 SNMPv3 组 testGroup，并加入一个用户 testUser，安全级别为认证加密，认证算法为 SHA-1，认证密码为 123456TESTauth&!，加密算法为 AES，加密密码是 123456TESTencr&!，只有 IP 地址为 1.1.1.1 的 NMS 可以使用用户名 testUser 访问设备。

  ```
  <Sysname> system-view
  [Sysname] acl basic 2000
  [Sysname-acl-ipv4-basic-2000] rule permit source 1.1.1.1 0
  [Sysname-acl-ipv4-basic-2000] rule deny source any
  [Sysname-acl-ipv4-basic-2000] quit
  [Sysname] snmp-agent group v3 testGroup authentication
  [Sysname] snmp-agent usm-user v3 testUser testGroup simple authentication-mode sha 123456TESTauth&! privacy-mode aes128 123456TESTencr&! acl 2000
  ```

- 配置 NMS 告警功能

  # 开启 NMS 告警功能，告警信息发送到主机 1.1.1.2，使用的用户名为 testUser，需要认证和加密。（各参数仅为示例）

  ```
  <Sysname> system-view
  ```

```
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname
testUser v3 privacy
```

3.1.5 通过 Web 登录设备

【安全加固策略】

HTTP 登录并不安全，使用明文形式传输数据，攻击者很容易截取到报文。推荐用户使用 HTTPS 方式进行 Web 登录，由 SSL 为应用层传输提供安全性保证。在设备上开启 HTTPS 服务后，用户即可通过 HTTPS 登录设备。

缺省情况下，设备作为 HTTPS 服务器端使用自签名证书与客户端建立 SSL 连接，且 SSL 参数均为缺省值，存在一定安全隐患。通过在设备上配置 SSL 服务器端策略，可以进一步提高 HTTPS 登录的安全性。

还可以通过配置证书属性访问控制策略控制只有从合法 CA 服务器获取证书的客户端可以通过 HTTPS 登录设备。

【配置举例】

配置 SSL 服务器端策略 myssl。

详细配置请参考“安全配置指导”中的“SSL”。

配置证书访问控制策略 myacp 并建立控制规则。

详细配置请参考“安全配置指导”中的“PKI”。

配置 HTTPS 服务与 SSL 服务器端策略 myssl 关联（myssl 仅为示例）。

```
<Sysname> system-view
[Sysname] ip https ssl-server-policy myssl
```

配置 HTTPS 服务与证书属性访问控制策略 myacp 关联，确保只有从 CA 服务器获取证书的 HTTPS 客户端可以访问 HTTPS 服务器。（myacp 仅为示例）

```
[Sysname] ip https certificate access-control-policy myacp
```

开启 HTTPS 服务。

```
[Sysname] ip https enable
```

在 ISP 域视图下为 login 用户配置认证方法。

如果选择本地认证，请配置本地用户及相关属性；如果选择远程认证，请配置 RADIUS、HWTACACS 或 LDAP 方案。相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

3.1.6 文件访问安全

【安全威胁】

FTP 和 TFTP 是通用的文件传输协议，使用明文形式传输数据，攻击者很容易截取报文，自身的安全性能并不高。

【安全加固策略】

针对以上攻击行为，可采用 SFTP（Secure FTP）协议。SFTP 协议基于 SSH2，使用加密形式传输数据，可提供安全可靠的网络文件传输服务，使得用户可以安全登录到远程设备上进行文件管理操作，且能保证文件传输的安全性。

SFTP 提供如下安全策略：

- password 认证

  利用 AAA 对客户端身份进行认证。用户在客户端上输入用户名和密码后，该密码将被加密后发送给服务器，通过服务器验证用户名和密码的合法性后，用户才可以登录设备。

- publickey 认证

  采用数字签名的方式来认证客户端。客户端发送包含用户名、公钥和公钥算法或者携带公钥信息的数字证书的认证请求给服务器端。服务器对公钥进行合法性检查，如果合法，则发送消息请求客户端的数字签名；如果不合法，则直接发送失败消息；服务器收到客户端的数字签名之后，使用客户端的公钥对其进行解密，并根据计算结果返回认证成功或失败的消息。

- password-publickey 认证

  对于 SSH2 版本的客户端，要求同时进行 password 和 publickey 两种方式的认证，且只有两种认证均通过的情况下，才认为客户端身份认证通过；对于 SSH1 版本的客户端，只要通过其中任意一种认证即可。

- keyboard-interactive 认证

  该认证方式与 password 认证方式类似，相较于 password 认证，该认证方式提供了可变的交互信息。客户端进行 keyboard-interactive 认证时，如果远程认证服务器要求用户进行交互认证，则远程认证服务器会在发送给服务器端的认证回应消息中携带一个提示信息，该提示信息被服务器端透传给客户端，在客户端终端上显示并要求用户输入指定的信息。当用户提交正确的信息后，若远程认证服务器继续要求用户输入其它的信息，则重复以上过程，直到用户输入了所有远程认证服务器要求的信息后，远程认证服务器才会返回认证成功的消息。

- 改变 SSH 服务端口号

  缺省情况下，SSH 服务的端口号为知名端口号 22，易被扫描和攻击。通过修改 SSH 服务的端口号为非知名端口号，可以降低被扫描的风险。

- 对 SSH 用户进行访问控制

  只有匹配 ACL 中 permit 规则的 IPv4 SSH 客户端可以访问设备，其他客户端不可以访问设备。

- 限制同时在线的最大 SSH 用户数

  当前在线 SSH 用户数超过设定的最大值时，系统会拒绝新的 SSH 连接请求。

【配置举例】

- # 开启 SFTP 服务器功能，并配置服务器采用 password 认证（用户名 client001 仅为示例）。

```
<Sysname> system-view
[Sysname] sftp server enable
[Sysname] ssh user client001 service-type sftp authentication-type password
```

  # 若进行本地认证，则还需要创建本地用户；若在远程服务器（如 RADIUS 服务器）进行认证，则还需要在服务器上创建相应的 SSH 用户。相关配置的详细介绍请参见“安全配置指导”中的“AAA”。

- # 开启 SFTP 服务器功能，并配置服务器采用 publickey 认证（用户名 client002、公钥 clientkey 仅为示例）。

```
<Sysname> system-view
[Sysname] sftp server enable
[Sysname] ssh user client002 service-type sftp authentication-type publickey assign
publickey clientkey
```

  # 创建同名的本地用户，用于下发授权属性：工作目录、用户角色。相关配置的详细介绍请参见“安全配置指导”中的“AAA”

- # 设置 SSH 服务端口号为 1025（1025 仅为示例）。

```
<Sysname> system-view
[Sysname] ssh server port 1025
```

- # 只允许 IPv4 地址为 1.1.1.1 的 SSH 用户向设备发起 SSH 访问（ACL2001 仅为示例）。

```
<Sysname> system-view
[Sysname] acl basic 2001
[Sysname-acl-ipv4-basic-2001] rule permit source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2001] quit
[Sysname] ssh server acl 2001
```

- # 限制同时在线的最大 SSH 用户数为 16（16 仅为示例）。

```
<Sysname> system-view
[Sysname] aaa session-limit ssh 16
```

3.1.7 FC 端口安全

通常情况下，任意的设备（包括节点设备和交换机）都可以登录 FC 网络中的交换机。FC 端口安全提供基于端口级别的安全控制，可以防止未授权的设备登录到交换机，保证网络的安全。

在 VSAN 内开启了 FC 端口安全功能后，当设备（包括节点设备和交换机）请求登录交换机时，交换机将基于策略数据库对登录设备进行权限检查，如果登录设备符合授权登录条件，则允许其登录；否则，拒绝其登录。

FC 端口安全功能可以控制如下设备是否可以登录到交换机：

- N_Port：控制是否允许节点设备上的某个 N_Port 登录。N_Port 通过 PWWN（即 N_Port 的 WWN）进行标识。
- NP_Port：控制是否允许 NPV 交换机上的某个 NP_Port 登录。NP_Port 通过 PWWN（即 NP_Port 的 WWN）进行标识。
- 节点设备：控制是否允许节点设备上的所有 N_Port 登录。节点设备通过 NWWN（即节点的 WWN）进行标识。
- NPV 交换机：控制是否允许 NPV 交换机上的所有 NP_Port 登录。NPV 交换机通过 NWWN（即 NPV 交换机的 WWN）进行标识。
- FCF 交换机：控制是否允许 FCF 交换机登录。FCF 交换机通过 SWWN（即 FCF 交换机的 WWN）进行标识。

关于 FC 端口安全的详细信息，请参见“FC 和 FCoE 配置指导”中的“FC 端口安全”。

3.2 登录用户及权限管理

3.2.1 管理登录用户权限（RBAC）

RBAC（Role Based Access Control）通过建立“权限<->角色”的关联实现将权限赋予给角色，并通过建立“角色<->用户”的关联实现为用户指定角色，从而使用户获得相应角色所具有的权限。

通常，对登录设备人员的权限管理方式是将用户和权限进行简单的关联，这种绑定关系很难应对人员以及设备安全等级的变化。RBAC 的基本思想就是给用户指定角色，这些角色中定义了允许用户操作哪些系统功能以及资源对象。RBAC 采用权限与用户分离的思想，提高用户权限分配的灵活性，减小用户授权管理的复杂度，降低管理开销，间接地提高了设备在登录用户管理方面的安全性能。

关于 RBAC 的详细信息，请参见“基础配置指导”中的“RBAC”。

3.2.2 AAA（认证、授权、计费）

AAA（Authentication、Authorization、Accounting，认证、授权、计费）是网络安全的一种管理机制，它可以为登录设备的用户提供以下三种安全功能。

- 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 可以通过多种协议来实现，这些协议规定了设备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、HWTACACS（HW Terminal Access Controller Access Control System，HW 终端访问控制器控制系统协议）协议和 LDAP（Lightweight Directory Access Protocol，轻量级目录访问协议）协议，在实际应用中，最常使用 RADIUS 协议。LDAP 协议的支持情况与设备的型号有关，请以设备的实际情况为准。

虽然 HWTACACS 协议与 RADIUS 协议都实现了认证、授权和计费功能，且都使用共享密钥对传输的用户信息进行加密，也都有较好的灵活性和可扩展性，但是 HWTACACS 协议还具有以下优点：

- 协议使用 TCP，网络传输更可靠。
- 除了 HWTACACS 报文头，报文主体全部进行加密。
- 协议报文较为复杂，认证和授权分离，使得认证、授权服务可以分离在不同的服务器上实现。
- 支持对设备上命令行的使用进行授权和计费。

3.2.3 命令行授权

【安全加固策略】

缺省情况下，用户登录设备后可以使用的命令行由用户拥有的用户角色决定。当用户线采用 AAA 认证方式并配置命令行授权功能后，用户可使用的命令行将受到用户角色和 AAA 授权的双重限制。用户每执行一条命令都会进行授权检查，只有授权成功的命令才被允许执行。

【配置举例】

开启命令行授权功能，限制用户只能使用授权成功的命令。

```
<Sysname> system-view
[Sysname] line vty 0 4
[Sysname-line-vty0-4] authentication-mode scheme
[Sysname-line-vty0-4] command authorization
```

在 ISP 域视图下配置命令行授权方法。命令行授权方法可以和 login 用户的授权方法相同，也可以不同。相关详细介绍请参见“安全配置指导”中的“AAA”。

3.2.4 Password Control

Password Control 是设备提供的密码安全管理功能，它根据管理员定义的安全策略，对本地用户登录密码、super 密码的设置、老化、更新等方面进行管理，并对用户的登录状态进行控制。

保存在设备上的用户密码存在一些安全隐患，比如：

- 密码长度短、复杂度低、不限制尝试次数，攻击者可以简单快速地借助密码字典进行爆破攻击。
- 密码未设置老化时间、长期闲置，攻击者可通过长时间持续尝试的方法进行破解，一旦破解了该密码，则一劳永逸。
- 初始密码可能是统一规则的弱密码，如果不作更改，后期被攻破的可能性较大。

Password Control 可以解决上述问题，可提供以下密码管理功能：

1. 密码设置控制

- 密码最小长度限制
- 密码的组合检测功能
- 密码的复杂度检测功能

2. 密码更新与老化

- 密码更新管理
- 密码老化管理
- 密码过期提醒
- 密码老化后允许登录管理
- 密码历史记录

3. 用户登录控制

- 用户首次登录控制
- 密码尝试次数限制
- 用户帐号闲置时间管理

关于本地用户类型的详细介绍，请参见“安全配置指导”中的“AAA”。关于 super 密码的详细介绍，请参见“基础配置指导”中的“RBAC”。关于 Password Control 的详细信息，请参见“安全”中的“Password Control”。

3.2.5 修改 SmartMC 成员设备的密码

【安全加固策略】

SmartMC（Smart Management Center，智能管理中心）功能用于集中管理和维护网络边缘大量分散的网络设备。SmartMC 网络中有且只有一台设备为管理设备，其他设备均为成员设备。

对于自动加入 SmartMC 网络的成员设备，管理设备会使用缺省用户名 admin、密码 admin 与其建立 NETCONF 会话，并将其加入到 SmartMC 网络中。SmartMC 网络组建完成后，由于缺省用户 admin 的初始密码过于简单，以防被攻击者轻松破解利用，建议用户修改缺省用户 admin 的密码，提高 SmartMC 网络的安全性。注意，修改成员设备的密码只是修改了成员设备访问管理设备时的密码，修改完成后，还需要手动同步成员设备的本地 admin 密码。

【配置举例】

修改成员设备缺省用户的密码为 Admin123&（Admin123&仅为示例）。

```
<Sysname> system-view
[Sysname] smartmc tc password Admin123&
```

3.3 密码设置安全

设备提供如下几种密码（或密钥）设置方式：

- 明文方式：用户以明文方式输入密码，设备以密文或哈希方式存储该密码（具体以各业务模块实现为准）。
- 密文方式：用户以密文方式输入密码，设备以密文方式存储该密码。
- 哈希方式：用户以密文方式输入密码，设备以哈希方式存储该密码。

为了提高系统的安全性和可维护性，对密码的设置有以下建议：

- 提高密码的长度和复杂度，不要使用弱密码。
- 不同特性的密码不要重复使用，避免攻击者非法获取了某业务的密码后，对其它业务的安全性造成威胁。
- 以密文或哈希方式设置的密码必须可被设备解析，否则无法成功设置。这两种密码设置方式通常用于测试或配置恢复。正常业务需求下，请不要尝试自行构造密文密码或哈希密码用于设置业务密码。

3.4 设备管理安全

3.4.1 配置密码恢复功能

【安全威胁】

缺省情况下，设备上的密码恢复功能处于开启状态。当用户忘记 Console 口认证密码或者登录认证失败时，可通过 Console 口连接设备，并在硬件重启设备过程中根据提示按组合键<Ctrl+B>进入 BootWare 菜单，再选择对应的 BootWare 菜单选项来修复这个问题。这会给非法用户访问设备带来便利，非法用户可通过 Console 口访问设备。

【安全加固策略】

关闭密码恢复功能后，设备将处于一个安全性更高的状态，即当出现上述情况时，若想继续使用 Console 口登录设备，只能通过 BootWare 菜单选择将设备恢复为出厂配置之后方可继续操作，这样可以有效地防止非法用户获取启动配置文件。

【配置举例】

关闭密码恢复功能。

```
<Sysname> system-view
[Sysname] undo password-recovery enable
```

3.4.2 关闭 USB 接口

【安全威胁】

用户可通过 USB 口进行文件的上传和下载。同时开放 USB 接口也会给用户带来安全隐患，例如，感染 U 盘携带的病毒，重要文件被非法拷贝等。

【安全加固策略】

为了安全起见，建议在安全环境下按需开启 USB 接口，使用完毕后，立即关闭 USB 接口。

【注意事项】

如果您对 U 盘进行了分区，请先使用 **umount** 命令卸载所有 U 盘分区，否则不能关闭 USB 接口。

【配置举例】

关闭 USB 接口。

```
<Sysname> system-view
[Sysname] usb disable
```

3.4.3 配置内存告警门限

【安全威胁】

如果设备的空闲内存不够，会导致业务模块的表项无法下发，设备的重要数据无法保存，影响设备的正常运行。

【安全加固策略】（不支持预告警的设备）

使用内存告警门限功能后，系统会实时监控剩余空闲内存大小，当条件达到一级、二级、三级告警门限或者恢复正常状态门限时，就产生相应的告警/告警解除通知，通知关联的业务模块/进程采取相应的措施，以便最大限度的利用内存，又能保证设备的正常运行。

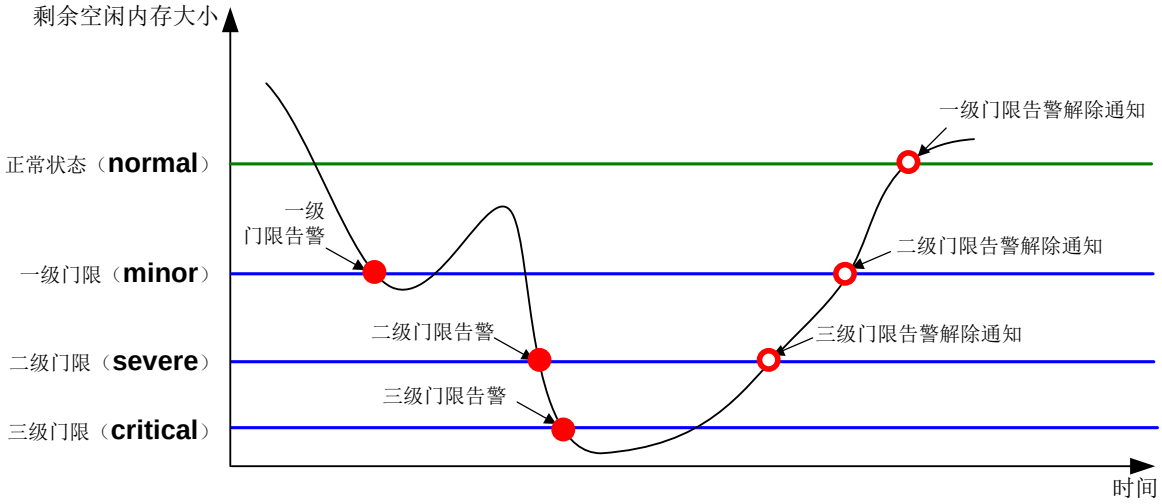
一级（**minor**）、二级（**severe**）和三级（**critical**）门限，对应的剩余空闲内存越来越少，紧急程度越来越严重。

- 当剩余空闲内存值从大于等于变成小于一级告警门限时，产生一级告警。
- 当剩余空闲内存值从大于等于变成小于二级告警门限时，产生二级告警。
- 当剩余空闲内存值从大于等于变成小于三级告警门限时，产生三级告警。
- 当剩余空闲内存值从小于等于变成大于二级告警门限时，产生三级告警解除通知。
- 当剩余空闲内存值从小于等于变成大于一级告警门限时，产生二级告警解除通知。
- 当剩余空闲内存值小于等于变成大于正常内存大小时，产生一级告警解除通知。

同一级别的告警/告警解除通知是交替进行的：当剩余空闲内存值小于某级告警门限，设备产生相应级别的告警，后续只有该告警解除了，剩余空闲内存值再次小于某级告警门限时，才会再次生成该级别的告警。

当剩余空闲内存大小如图 3-1 中曲线所示时，会生成如图 3-1 所示的告警和解除告警通知。

图3-1 内存告警示意图



【安全加固策略】（支持预告警的设备）

使用内存告警门限功能后，系统会实时监控剩余空闲内存大小，当条件达到一级、二级、三级告警门限或者恢复正常状态门限时，就产生相应的告警/告警解除通知，通知关联的业务模块/进程采取相应的措施，以便最大限度的利用内存，又能保证设备的正常运行。

除了一级、二级、三级告警，设备还支持预警功能。预警门限用于内存使用率尚处于正常范围内，但需要提醒用户提前关注内存的情况。预警恢复门限用于解除预警。

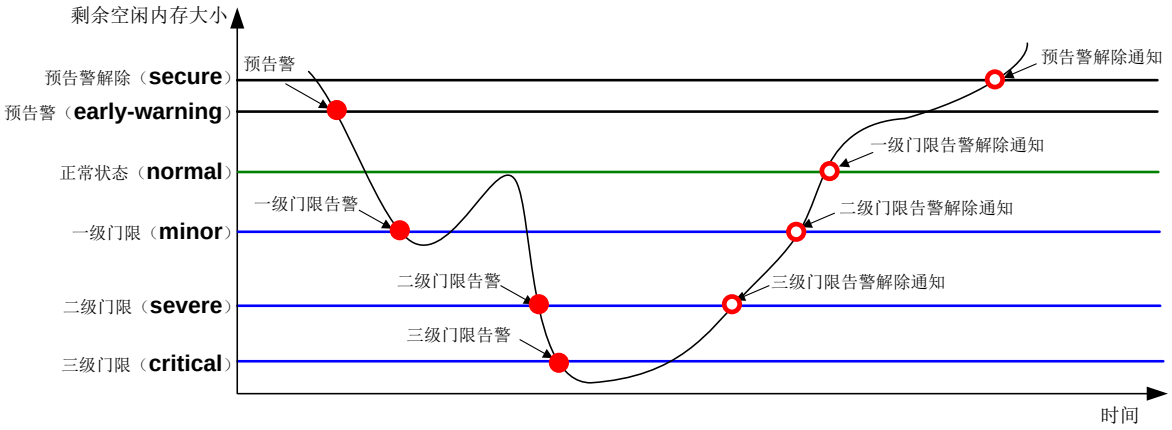
预告警（**early-warning**）、一级（**minor**）、二级（**severe**）和三级（**critical**）门限，对应的剩余空闲内存越来越少，紧急程度越来越严重。

- 当剩余空闲内存值从大于等于变成小于等于预告警门限时，产生预告警。
- 当剩余空闲内存值从大于等于变成小于等于一级告警门限时，产生一级告警。
- 当剩余空闲内存值从大于等于变成小于等于二级告警门限时，产生二级告警。
- 当剩余空闲内存值从大于等于变成小于等于三级告警门限时，产生三级告警。
- 当剩余空闲内存值从小于等于变成大于二级告警门限时，产生三级告警解除通知。
- 当剩余空闲内存值从小于等于变成大于一级告警门限时，产生二级告警解除通知。
- 当剩余空闲内存值小于等于变成大于正常内存大小时，产生一级告警解除通知。
- 当剩余空闲内存值小于等于变成大于预告警内存大小时，产生预告警解除通知。

同一级别的告警/告警解除通知是交替进行的：当剩余空闲内存值小于某级告警门限，设备产生相应级别的告警，后续只有该告警解除了，剩余空闲内存值再次小于某级告警门限时，才会再次生成该级别的告警。

当剩余空闲内存大小如图 3-2 中曲线所示时，会生成如图 3-2 所示的告警和解除告警通知。

图3-2 内存告警示意图



【注意事项】

当设备出现内存告警时，可删除暂时不用的配置或关闭部分功能来释放内存。但因为内存不足，部分配置可能删除失败。

【配置举例】

配置一级、二级、三级告警门限分别为 3000MB、2000MB、1000MB，当剩余空闲内存为 3500MB 时，恢复到正常状态。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] memory-threshold minor 3000 severe 2000 critical 1000 normal 3500
```

3.5 配置文件加密

【安全加固策略】

开启配置文件加密功能后，管理员每次执行 **save** 命令，设备都会先将当前生效的配置进行加密，再保存。配置文件加密功能支持使用公钥和私钥两种方式进行加密，由于所有运行 Uniware V7 平台软件的设备拥有相同的公钥和私钥，因此加密后的文件只能被所有运行 Uniware V7 平台软件的设备识别和解析。为了防止非法用户对加密后配置文件的解析，需确保只有合法用户才能获取加密后的配置文件，进一步提高配置文件的安全性。

【注意事项】

开启配置文件加密功能后，将不能使用 **more** 命令查看加密配置文件（后缀名为“.cfg”的配置文件）的内容，但是加密配置文件可以作为 **display diff** 命令的参数，进行两份配置文件之间的差异比较,可以使用 **display saved-configuration** 命令查看加密的下次启动配置文件内容。

【配置举例】

- # 设置保存配置文件时使用公钥进行加密。

  ```
  <Sysname> system-view
  [Sysname] configuration encrypt public-key
  ```

- # 设置保存配置文件时使用私钥进行加密。

  ```
  <Sysname> system-view
  [Sysname] configuration encrypt private-key
  ```

3.6 安全日志

【安全加固策略】

查看系统日志是了解设备状态、定位和排除网络问题的一个重要方法，而在系统日志中与设备安全相关的安全日志显得尤为重要。但通常情况下，安全日志与其它日志一同输出，经常被淹没在大量的系统日志中，很难识别、不便于查看。针对这个问题，系统提供了安全日志同步保存功能和安全日志文件管理功能。

开启安全日志同步保存功能后，安全业务模块根据业务需要，会将某些信息同时封装成普通日志和安全日志，普通日志根据信息中心的配置可以输出到控制台、监视终端、日志缓冲区、日志主机等方向，安全日志只能按周期输出到安全日志文件。这样既实现了安全日志的集中管理，又有利于用户随时快捷地查看安全日志，了解设备状态。

安全日志同步保存功能的配置和安全日志文件的管理相互分离，安全日志文件实行专人专管：

- 设备管理员可配置安全日志同步保存功能，包括开启安全日志同步保存功能，开启安全日志同步保存功能，配置单个安全日志文件最大能占用的存储空间的大小，配置安全日志文件使用率的告警上限等。
- 安全日志管理员才能管理安全日志文件，例如修改安全日志文件的存储路径、手工将安全日志保存到安全日志文件等。安全管理员只能管理安全日志文件，不能对设备执行其他操作。

【配置举例】

- 配置安全日志同步保存功能

  # 开启安全日志同步保存功能。

  ```
  <Sysname> system-view
  [Sysname] info-center security-logfile enable
  ```

  # 配置安全日志自动保存到文件的频率为 600 秒。（600 秒仅为示例）

  ```
  [Sysname] info-center security-logfile frequency 600
  ```

  # 配置单个安全日志文件最大能占用的存储空间的大小为 2MB。（2MB 仅为示例）

  ```
  [Sysname] info-center security-logfile size-quota 2
  ```

- 管理安全日志文件

  # 以安全日志管理员身份登录设备。

  # 配置存放安全日志文件的目录为 flash:/test。（flash:/test 仅为示例）

  ```
  <Sysname> mkdir test
  Creating directory flash:/test... Done.
  <Sysname> system-view
  [Sysname] info-center security-logfile directory flash:/test
  [Sysname] quit
  ```

  # 手动将安全日志缓冲区中的内容保存到安全日志文件。

  ```
  <Sysname> security-logfile save
  The contents in the security log file buffer have been saved to the file
  flash:/seclog/seclog.log.
  ```

3.7 VXLAN安全

3.7.1 MAC 地址学习

【安全威胁】

在 VXLAN 网络中，设备学习 MAC 地址时可能存在以下安全威胁：

- 攻击者通过伪造 VXLAN 报文，使 VTEP 学习到错误的远端 MAC 地址。
- 若网络中存在环路或网络攻击，可能会造成不同以太网服务实例接口学习到相同的 MAC 地址，导致 MAC 地址不稳定。

【安全加固策略】

针对以上安全威胁，可以在 VTEP 和网关上配置如下安全策略：

- 关闭远端 MAC 地址自动学习功能

  为了避免 VTEP 学习到错误的远端 MAC 地址，可以关闭远端 MAC 地址自动学习功能，手动添加静态的远端 MAC 地址或通过 EVPN 的 MAC/IP 发布路由学习远端 MAC 地址。

- 配置 MAC 地址学习优先级

  为以太网服务实例配置不同的 MAC 地址学习优先级后，如果高优先级的以太网服务实例学习 MAC 地址时已经有低优先级的以太网服务实例或其它高优先级的以太网服务实例学习到该 MAC 地址，则覆盖之前的 MAC 地址表项；如果低优先级的以太网服务实例学习 MAC 地址时，已经有高优先级以太网服务实例学习到该 MAC 地址，则低优先级的以太网服务实例不学习该 MAC 地址，防止 MAC 地址不稳定对网络造成影响。

【配置举例】

关闭远端 MAC 地址自动学习功能。

```
<Sysname> system-view
[Sysname] vxlan tunnel mac-learning disable
```

配置以太网服务实例的 MAC 地址学习优先级为高优先级。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 1000
[Sysname-GigabitEthernet1/0/1-srv1000] mac-address mac-learning priority high
```

3.7.2 ARP/ND 安全

【安全威胁】

若攻击者向 EVPN VXLAN 网络中发送错误或畸形的 ARP/ND 报文，会使 VTEP 和网关学习到错误的 ARP/ND 表项，影响网络中报文的正常转发。

【安全加固策略】

为避免 VTEP 和网关学习到错误的 ARP/ND 表项，可手工关闭远端 ARP/ND 的自动学习功能，通过 EVPN 的 MAC/IP 发布路由中携带的 ARP/ND 信息形成 APR/ND 表项指导报文转发。

【注意事项】

本安全策略仅适用于 EVPN VXLAN 网络。

【配置举例】

关闭远端 ARP 自动学习功能。

```
<Sysname> system-view
[Sysname] vxlan tunnel arp-learning disable
```

关闭远端 ND 自动学习功能。

```
<Sysname> system-view
[Sysname] vxlan tunnel nd-learning disable
```

3.7.3 ARP 迁移抑制

【安全威胁】

EVPN VXLAN 网络中，采用分布式 EVPN 网关连接用户站点，若存在恶意攻击者在某站点使用与其它站点相同的 IP 地址向网络中发送报文，则会引起站点不断迁移，使分布式 EVPN 网关间形成环路并不断同步 ARP 信息，大量占用网络带宽，影响网络中报文的正常转发。

【安全加固策略】

在分布式 EVPN 网关上开启 ARP 反复迁移抑制功能，若 180 秒内某站点在分布式 EVPN 网关间进行了 5 次迁移，则抑制最后一次迁移，也不对外通告该站点的 ARP 信息，避免分布式 EVPN 网关间形成环路。

【配置举例】

分布式 EVPN 网关开启 ARP 迁移抑制功能。

```
<Sysname> system-view
[Sysname] evpn route arp-mobility suppression
```

3.7.4 泛洪抑制

【安全威胁】

在 VXLAN 网络中，VTEP 从本地站点内接收到目的 MAC 地址为广播、未知单播和未知组播的数据帧后，会在该 VXLAN 内除接收接口外的所有本地接口和 VXLAN 隧道上泛洪该数据帧，将该数据帧发送给 VXLAN 内的所有站点；VTEP 从 VXLAN 隧道接收到目的 MAC 地址为广播、未知单播和未知组播的数据帧后，会在该 VXLAN 内的所有本地接口上泛洪该数据帧。这样可能会导致广播风暴，影响设备的转发性能。

【安全加固策略】

通过配置 VSI 泛洪抑制功能，可以禁止某类数据帧在 VXLAN 内泛洪，以减少网络中的泛洪流量。

通过配置 AC 间泛洪抑制功能，可禁止在 AC 间泛洪流量，避免引起广播风暴。可以通过以下两种方式抑制 AC 间的泛洪流量：

- 所有端口隔离模式（all-port）：AC 接收到的泛洪报文在不同接口的以太网服务实例、同一接口的不同以太网服务实例上均不允许泛洪。
- 源端口隔离模式（source-port）：AC 接收到的泛洪报文不能在同一个接口的不同以太网服务实例上泛洪，可以在不同接口的以太网服务实例上泛洪。

【配置举例】

在 VSI 实例 vsi1 内禁止将本地站点内接收到的广播数据帧泛洪到远端站点。

```
<Sysname> system-view
[Sysname] vsi vsi1
```

```
[Sysname-vsi-vsi1] flooding disable broadcast
```

在 VSI 实例 vsi1 内禁止将接收到的未知单播数据帧泛洪到本地站点和远端站点。

```
<Sysname> system-view
[Sysname] vsi vsi1
[Sysname-vsi-vsi1] flooding disable unknown-unicast all-direction
```

配置 AC 间泛洪抑制模式为所有端口隔离模式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 1000
[Sysname-GigabitEthernet1/0/1-srv1000] flooding disable all-port
```

配置 AC 间泛洪抑制模式为源端口隔离模式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] service-instance 1000
[Sysname-GigabitEthernet1/0/1-srv1000] flooding disable source-port
```

4 控制平面安全加固

4.1 二层协议安全

4.1.1 生成树保护功能

【安全威胁】

- BPDU 攻击

  接入端口一般直接与用户终端（如 PC）或文件服务器相连，此时接入端口被设置为边缘端口以实现这些端口的快速迁移；当这些端口接收到 BPDU，系统会自动将这些端口设置为非边缘端口，重新计算生成树，从而引起网络拓扑结构的变化。这些端口正常情况下应该不会收到 STP 的 BPDU。如果有人伪造 BPDU 恶意攻击设备，就会引起网络震荡。

- 根桥攻击

  由于维护人员的错误配置或网络中的恶意攻击，网络中的合法根桥有可能会收到优先级更高的 BPDU，这样当前合法根桥会失去根桥的地位，引起网络拓扑结构的错误变动。这种不合法的变动，会导致原来应该通过高速链路的流量被牵引到低速链路上，导致网络拥塞。

- TC-BPDU 攻击

  在有人伪造 TC-BPDU 恶意攻击设备时，设备短时间内会收到很多的 TC-BPDU，频繁的刷新操作给设备带来很大负担，给网络的稳定带来很大隐患。

【安全加固策略】

针对以上攻击行为，可以在设备上配置如下安全策略：

- BPDU 保护

  在设备上部署 BPDU 保护功能，可以防止 BPDU 攻击。如果边缘端口收到了 BPDU，系统就将这些端口关闭，同时通知网管这些端口已被生成树协议关闭。

- 根保护

在设备的指定端口上部署根保护功能，通过维护指定端口的角色来保护根桥的地位，可以防止根桥频繁变动。

- TC-BPDU 攻击保护

  在设备上部署 TC-BPDU 攻击保护功能，可以防止 TC-BPDU 攻击。当设备在单位时间（固定为十秒）内收到 TC-BPDU 的次数大于 TC-BPDU 攻击保护功能所指定的最高次数（假设为 N 次），那么该设备在这段时间之内将只进行 N 次刷新转发地址表项的操作，而对于超出 N 次的那些 TC-BPDU，设备会在这段时间过后再统一进行一次地址表项刷新的操作，这样就可以避免频繁地刷新转发地址表项。

【配置举例】

- 配置 BPDU 保护
  - 方法一：

    # 在系统视图下开启 BPDU 保护功能，并配置端口为边缘端口。

    ```
    <Sysname> system-view
    [Sysname] stp bpdu-protection
    [Sysname] interface gigabitethernet 1/0/1
    [Sysname-GigabitEthernet1/0/1] stp edged-port
    ```

  - 方法二：

    # 在指定的边缘端口上开启 BPDU 保护功能。

    ```
    [Sysname] interface gigabitethernet 1/0/1
    [Sysname-GigabitEthernet1/0/1] stp edged-port
    [Sysname-GigabitEthernet1/0/1] stp port bpdu-protection enable
    ```

- 配置根保护

  # 开启端口的根保护功能。

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

- 配置 TC-BPDU 攻击保护

  # 配置在单位时间（固定为十秒）内，设备收到 TC-BPDU 后一定时间内，允许收到 TC-BPDU 后立即刷新转发地址表项的最高次数为 10（10 仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] stp tc-protection threshold 10
  ```

4.1.2 LLDP 邻居验证与超时保护功能

【安全加固策略】

- 邻居验证功能

  开启邻居验证功能后，如果满足表 4-1 所示的邻居验证通过条件，则接口可以继续收发数据报文；否则阻塞接口，即接口的链路层状态置为 DOWN，且不允许该接口继续收发数据报文。

  表4-1 邻居验证通过条件

配置的邻居识别信息	邻居验证通过条件
配置邻居Chassis ID TLV识别信息	接口从邻居收到的LLDPDU中携带的Chassis ID TLV与配置相同

配置邻居Port ID TLV识别信息	接口从邻居收到的LLDPDU中携带的Port ID TLV与配置相同
配置邻居Chassis ID TLV和Port ID TLV识别信息	接口从邻居收到的LLDPDU中携带的Chassis ID TLV和Port ID TLV与配置全部相同

- 超时保护功能

  通过部署超时保护功能，可以防止恶意攻击导致邻居老化后接口继续接收报文。邻居老化超时保护功能分为邻居老化超时后阻塞接口和邻居老化超时后关闭接口。

  - 阻塞接口：在超过老化时间后，如果接口收不到 LLDP 报文，则阻塞该接口，即接口的链路层协议状态置为 DOWN，且不允许该接口继续收发数据报文；如果接口收到 LLDP 报文，则该接口可以继续收发数据报文。接口收发协议报文不受影响。
  - 关闭接口：在超过老化时间后，会立刻关闭接口，即接口的状态置为 LLDP DOWN，且不允许该接口继续收发数据报文和协议报文。

【配置举例】

- 配置邻居验证功能

  # 进入接口视图。

  ```
  <Sysname> system-view
  [Sysname] interface gigabitethernet 1/0/1
  ```

  # 配置邻居 Chassis ID TLV 识别信息，邻居 Chassis ID TLV 别信息的邻居设备 Chassis ID 子类型编号为 4，邻居设备 Chassis ID 为 0012-2255-7766。（各参数仅为示例）

  ```
  [Sysname-GigabitEthernet1/0/1] lldp neighbor-identity chassis-id 4 0012-2255-7766
  ```

  # 配置邻居 Port ID TLV 识别信息，邻居 Port ID TLV 识别信息的邻居设备端口 ID 子类型编号为 5，邻居设备端口 ID 为 gigabitethernet1/0/1。（各参数仅为示例）

  ```
  [Sysname-GigabitEthernet1/0/1] lldp neighbor-identity port-id 5 gigabitethernet1/0/1
  ```

  # 开启邻居验证功能。

  ```
  [Sysname-GigabitEthernet1/0/1] lldp neighbor-protection validation
  ```

- 配置超时保护功能

  # 在指定接口上开启邻居超时保护功能并指定邻居老化超时后阻塞接口。

  ```
  <Sysname> system-view
  [Sysname] interface gigabitethernet 1/0/1
  [Sysname-GigabitEthernet1/0/1] lldp neighbor-protection aging block
  ```

4.2 ARP攻击防御

4.2.1 源 MAC 为组播的 ARP 表项检查功能

【安全威胁】

合法的 ARP 报文发送端 MAC 地址为单播，攻击源可以伪造发送端 MAC 地址为组播的 ARP 报文。如果网关学习到源 MAC 为组播地址的 ARP 表项，那么当它基于该类表项转发报文时，会将报文组播发送，严重占用网络资源。

【安全加固策略】

开启 ARP 表项的检查功能后，设备将不能学习 ARP 报文中发送端 MAC 地址为组播 MAC 的动态 ARP 表项，也不能手工添加 MAC 地址为组播 MAC 的静态 ARP 表项。

【配置举例】

开启动态 ARP 表项的检查功能。

```
<Sysname> system-view
[Sysname] arp check enable
```

4.2.2 泛洪类 ARP 报文攻击防范

1. ARP 防止 IP 报文攻击

【安全威胁】

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。

【安全加固策略】

为避免这种 IP 报文攻击所带来的危害，设备提供了下列两个功能：

- ARP 源抑制功能：如果发送攻击报文的源是固定的，可以采用 ARP 源抑制功能。开启该功能后，如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。
- ARP 黑洞路由功能：无论发送攻击报文的源是否固定，都可以采用 ARP 黑洞路由功能。开启该功能后，一旦接收到目标 IP 地址不能解析的 IP 报文，设备立即产生一个黑洞路由，并同时发起 ARP 主动探测，如果在黑洞路由老化时间内 ARP 解析成功，则设备马上删除此黑洞路由并开始转发去往该地址的报文，否则设备直接丢弃该报文。在删除黑洞路由之前，后续去往该地址的 IP 报文都将被直接丢弃。用户可以通过命令配置 ARP 请求报文的发送次数和发送时间间隔。等待黑洞路由老化时间过后，如有报文触发则再次发起解析，如果解析成功则进行转发，否则仍然产生一个黑洞路由将去往该地址的报文丢弃。这种方式能够有效地防止 IP 报文的攻击，减轻 CPU 的负担。

【配置举例】

- # 开启 ARP 源抑制功能，并指定 ARP 源抑制的阈值为 100（100 仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] arp source-suppression enable
  [Sysname] arp source-suppression limit 100
  ```

- # 开启 ARP 黑洞路由功能，并配置发送 ARP 探测报文个数为 5，发送 ARP 探测报文的时间间隔为 3 秒。（各参数仅为示例）

  ```
  <Sysname> system-view
  [Sysname] arp resolving-route enable
  [Sysname] arp resolving-route probe-count 5
  [Sysname] arp resolving-route probe-interval 3
  ```

2. 源 MAC 地址固定的 ARP 攻击检测功能

【安全威胁】

如果攻击源向设备发送大量的源 MAC 地址固定的 ARP 攻击报文，会导致设备表项被占满，无法学习合法的 ARP 表项。

【安全加固策略】

开启源 MAC 地址固定的 ARP 攻击检测功能后，设备会根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计，在 5 秒内，如果收到同一源 MAC 地址（源 MAC 地址固定）的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中。

当开启了 ARP 日志信息功能，且在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源 MAC 地址发送的 ARP 报文过滤掉。

【注意事项】

切换源 MAC 地址固定的 ARP 攻击检查模式时，如果从监控模式切换到过滤模式，过滤模式马上生效；如果从过滤模式切换到监控模式，已生成的攻击检测表项，到表项老化前还会继续按照过滤模式处理。

对于网关或一些重要的服务器，可能会发送大量 ARP 报文，为了使这些 ARP 报文不被过滤掉，可以将这类设备的 MAC 地址配置成保护 MAC 地址，这样，即使该设备存在攻击也不会被检测或过滤。

【配置举例】

开启源 MAC 地址固定的 ARP 攻击检测功能，并选择过滤模式。

```
<Sysname> system-view
[Sysname] arp source-mac filter
```

如果选择监控模式，则需要执行 `arp source-mac monitor` 命令。

配置源 MAC 地址固定的 ARP 报文攻击检测的阈值为 30 个（30 仅为示例）。

```
[Sysname] arp source-mac threshold 30
```

配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒（60 仅为示例）。

```
[Sysname] arp source-mac aging-time 60
```

配置保护 MAC 地址为 001e-1200-0213（001e-1200-0213 仅为示例）。

```
[Sysname] arp source-mac exclude-mac 001e-1200-0213
```

开启源 MAC 地址固定的 ARP 攻击检测日志信息功能。

```
[Sysname] arp source-mac log enable
```

3. ARP 报文限速

【安全威胁】

攻击源向设备发送大量的 ARP 攻击报文，导致设备表项被占满，无法学习合法的 ARP 表项。同时，会导致设备的 CPU 负担过重，造成其他功能无法正常运行甚至设备瘫痪。

【安全加固策略】

接口上开启 ARP 报文限速功能后，如果单位时间接口收到的 ARP 报文数量超过用户设定的限速值，则有如下处理机制：

- 当开启了 ARP 模块的告警功能后，设备将这个时间间隔内的超速峰值作为告警信息发送出去，生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关特性。有关告警信息的详细介绍请参见“网络管理和监控命令参考”中的 SNMP。
- 当开启了 ARP 限速日志功能后，设备将这个时间间隔内的超速峰值作为日志的速率值发送到设备的信息中心，通过设置信息中心的参数，最终决定日志报文的输出规则（即是否允许输出以及输出方向）有关信息中心参数的配置请参见“网络管理和监控配置指导”中的“信息中心”。

【配置举例】

开启 ARP 报文限速的告警功能。

```
<Sysname> system-view
[Sysname] snmp-agent trap enable arp rate-limit
```

开启 ARP 报文限速日志功能。

```
[Sysname] arp rate-limit log enable
```

配置当设备收到的 ARP 报文速率超过用户设定的限速值时，设备发送告警或日志的时间间隔为 120 秒（120 仅为示例）。

```
[Sysname] arp rate-limit log interval 120
```

在二层以太网接口 GigabitEthernet1/0/1 上开启 ARP 报文限速功能，并设置 ARP 报文限速速率为 50pps（50 仅为示例）。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp rate-limit 50
```

4.2.3 防御 ARP 欺骗类攻击功能

1. ARP 记录终端用户间 IP 地址冲突功能

【安全加固策略】

开启本功能后，ARP 模块收到非免费 ARP 报文时，会将 ARP 报文中的发送端 IP 地址和已有 ARP 表项中的 IP 地址进行比较。如果发现发送端 IP 地址和某条 ARP 表项中的 IP 地址相同，但 MAC 地址不同，则认为网络中存在终端用户间的 IP 地址冲突。此时，ARP 模块会生成终端用户间 IP 地址冲突表项，同时生成对应的 IP 地址冲突日志。生成的 IP 地址冲突日志将被发送给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。本功能可以防御仿冒用户类攻击行为。

【配置举例】

开启 ARP 记录终端用户间源 IP 地址冲突功能。

```
<Sysname> system-view
[Sysname] arp user-ip-conflict record enable
```

2. 源地址冲突提示功能

【安全威胁】

攻击者仿冒网关，发送错误的网关 IP 地址和 MAC 地址对应关系给合法客户端，导致合法客户端不能正常访问网关。

【安全加固策略】

开启源地址冲突提示功能后，设备接收到其它设备发送的 ARP 报文后，如果发现报文中的源 IP 地址和自己的 IP 地址相同，该设备会根据当前源 IP 地址冲突提示功能的状态，进行如下处理：

- 如果源 IP 地址冲突提示功能处于关闭状态时，设备发送一个免费 ARP 报文确认是否冲突，只有收到对应的 ARP 应答后才提示存在 IP 地址冲突。
- 如果源 IP 地址冲突提示功能处于开启状态时，设备立刻提示存在 IP 地址冲突。

【配置举例】

开启源 IP 地址冲突提示功能。

```
<Sysname> system-view
```

```
[Sysname] arp ip-conflict log prompt
```

3. ARP 报文源 MAC 地址一致性检查功能

【安全加固策略】

开启 ARP 报文源 MAC 地址一致性检查功能后，网关设备在进行 ARP 学习前将对 ARP 报文进行检查。如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 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。

【配置举例】

开启 ARP 报文源 MAC 地址一致性检查功能。

```
<Sysname> system-view
[Sysname] arp valid-check enable
```

4. 配置 ARP 主动确认功能

【安全威胁】

攻击者仿冒用户的 IP 地址发送 ARP 请求给网关，网关收到 ARP 表项后，新建了错误的 ARP 表项或更新已有 ARP 表项的 MAC 地址，则合法用户无法收到报文。

【安全加固策略】

配置 ARP 主动确认功能后，设备在新建或更新 ARP 表项前需进行主动确认，防止产生错误的 ARP 表项。

为了对 ARP 表项的学习执行更严格的检查，可以开启严格模式的 ARP 主动确认功能，具体机制如下：

- 收到目标 IP 地址为自己的 ARP 请求报文时，设备会发送 ARP 应答报文，但不建立 ARP 表项；
- 收到 ARP 应答报文时，需要确认本设备是否对该报文中的源 IP 地址发起过 ARP 解析：若发起过解析，解析成功后则设备启动主动确认功能，主动确认流程成功完成后，设备可以建立该表项；若未发起过解析，则设备丢弃该报文。

【配置举例】

开启严格模式的 ARP 主动确认功能。

```
<Sysname> system-view
[Sysname] arp active-ack strict enable
```

5. 授权 ARP 功能

【安全加固策略】

开启授权 ARP（Authorized ARP）功能后，在动态学习 ARP 的过程中，只有和 DHCP 服务器生成的租约或 DHCP 中继生成的安全表项一致的 ARP 报文才能够被学习。配置接口的授权 ARP 功能后，可以防止用户仿冒其他用户的 IP 地址或 MAC 地址对网络进行攻击，保证只有合法的用户才能使用网络资源，增加了网络的安全性。关于 DHCP 服务器和 DHCP 中继的介绍，请参见“三层技术-IP 业务配置指导”中的“DHCP 服务器”和“DHCP 中继”。

【配置举例】

在 VLAN 接口 10 上开启授权 ARP 功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] arp authorized enable
```

6. ARP Detection 功能

【安全加固策略】

- 用户合法性检查：对于 ARP 信任接口，不进行用户合法性检查；对于 ARP 非信任接口，进行包括基于用户合法性规则检查、IP Source Guard 静态绑定表项的检查、基于 DHCP Snooping 表项的检查和基于 802.1X 安全表项来检查 ARP 报文的发送端 IP 地址和发送端 MAC 地址。只要符合三者中的任何一个，就认为该 ARP 报文合法，进行转发。如果所有检查都没有找到匹配的表项，则认为是非法报文，直接丢弃。
- 报文有效性检查：对于 ARP 信任接口，不进行报文有效性检查；对于 ARP 非信任接口，需要根据配置对 MAC 地址和 IP 地址不合法的报文进行过滤。可以选择配置源 MAC 地址、目的 MAC 地址或 IP 地址检查模式。
  - 源 MAC 地址的检查模式：会检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致则认为有效，否则丢弃报文；
  - 目的 MAC 地址的检查模式（只针对 ARP 应答报文）：会检查 ARP 应答报文中的目的 MAC 地址是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，需要被丢弃；
  - IP 地址检查模式：会检查 ARP 报文中的源 IP 或目的 IP 地址，如全 1、或者组播 IP 地址都是不合法的，需要被丢弃。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。
- ARP 报文强制转发：对于从 ARP 信任接口接收到的 ARP 报文不受此功能影响，按照正常流程进行转发；对于从 ARP 非信任接口接收到的并且已经通过用户合法性检查的 ARP 报文的处理过程如下：
  - 对于 ARP 请求报文，通过信任接口进行转发；
  - 对于 ARP 应答报文，首先按照报文中的以太网目的 MAC 地址进行转发，若在 MAC 地址表中没有查到目的 MAC 地址对应的表项，则将此 ARP 应答报文通过信任接口进行转发。

【配置举例】

- # 配置用户合法性规则，规则编号为 0，规则内容为转发源地址为 10.1.1.1，掩码为 255.255.0.0，源 MAC 地址为 0001-0203-0405，掩码为 ffff-ffff-0000 的 ARP 报文。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] arp detection rule 0 permit ip 10.1.1.1 255.255.0.0 mac 0001-0203-0405
ffff-ffff-0000
```

  # 在 VLAN10 内开启 ARP Detection 功能。

```
[Sysname] vlan 10
[Sysname-vlan10] arp detection enable
[Sysname-vlan10] quit
```

  # 配置二层以太网接口 GigabitEthernet1/0/1 为 ARP 信任接口。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

- # 开启对 ARP 报文的 MAC 地址和 IP 地址的有效性检查。

```
<Sysname> system-view
[Sysname] arp detection validate dst-mac ip src-mac
```

  # 在 VLAN10 内开启 ARP Detection 功能。

```
[Sysname] vlan 10
```

```
[Sysname-vlan10] arp detection enable
[Sysname-vlan10] quit
```

配置二层以太网接口 GigabitEthernet1/0/1 为 ARP 信任接口。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

- # 开启 VLAN 2 的 ARP 报文强制转发功能。

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp restricted-forwarding enable
```

7. ARP 自动扫描、固化功能

【安全加固策略】

ARP 自动扫描功能一般与 ARP 固化功能配合使用，用来防御局域网内的 ARP 欺骗行为：

- 开启 ARP 自动扫描功能后，设备会对局域网内的邻居自动进行扫描（向邻居发送 ARP 请求报文，获取邻居的 MAC 地址，建立动态 ARP 表项）。
- 开启固化功能后，设备会将当前的 ARP 动态表项（包括 ARP 自动扫描生成的动态 ARP 表项）转换为静态 ARP 表项。通过对动态 ARP 表项的固化，可以有效防止攻击者修改 ARP 表项。

【注意事项】

接口上开启了 ARP 自动扫描功能后，会向扫描区间的所有 IP 地址同时发送 ARP 请求报文，这会造成设备瞬间 CPU 利用率过高、网络负载过大的问题。您可以通过设置接口发送 ARP 报文的速率解决此问题。

固化生成的静态 ARP 表项数量同样受到设备可以支持的静态 ARP 表项数目的限制，由于静态 ARP 表项数量的限制可能导致只有部分动态 ARP 表项被固化。

【配置举例】

对 VLAN 接口 10 上的主 IP 地址网段内的邻居进行 ARP 自动扫描。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] arp scan
[Sysname-Vlan-interface10] quit
```

将设备上的动态 ARP 表项转化成静态 ARP 表项。

```
[Sysname] arp fixup
```

8. ARP 网关保护功能

【安全威胁】

攻击者发送错误的网关 IP 地址和 MAC 地址对应关系给合法客户端，导致合法客户端不能正常访问网关。

【安全加固策略】

在设备上不与网关相连的接口上开启 ARP 网关保护功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址是否和配置的被保护网关的 IP 地址相同。如果相同，则认为此报文非法，将其丢弃；否则，认为此报文合法，继续进行后续处理。

【注意事项】

不能在同一个接口上配置 ARP 网关保护功能和 ARP 过滤保护功能。

【配置举例】

在二层以太网网接口 GigabitEthernet1/0/1 下开启 ARP 网关保护功能，受保护的网关 IP 地址为 1.1.1.1。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

9. ARP 过滤保护功能

【安全威胁】

- 攻击者发送错误的网关 IP 地址和 MAC 地址对应关系给合法客户端，导致合法客户端不能正常访问网关。
- 攻击者发送伪造的合法客户端的 IP 地址和 MAC 地址的对应关系给网关或其他客户端，导致网关或其他客户端无法与合法客户端正常通信。

【安全加固策略】

在接口上开启 ARP 过滤保护功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址和源 MAC 地址是否和允许通过的 IP 地址和 MAC 地址相同：

- 如果相同，则认为此报文合法，继续进行后续处理；
- 如果不相同，则认为此报文非法，将其丢弃。

【注意事项】

不能在同一个接口上配置 ARP 网关保护功能和 ARP 过滤保护功能。

【配置举例】

在二层以太网接口 GigabitEthernet1/0/1 下开启 ARP 过滤保护功能，允许源 IP 地址为 1.1.1.1、源 MAC 地址为 0e10-0213-1023 的 ARP 报文通过。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 0e10-0213-1023
```

10. ARP 报文发送端 IP 地址检查功能

【安全加固策略】

配置 ARP 报文发送端 IP 地址检查功能后，网关设备在进行 ARP 学习前将对 ARP 报文进行检查。如果指定 VLAN 内的 ARP 报文的发送端 IP 地址不在指定源 IP 地址范围内，则认为是攻击报文，将其丢弃；否则，继续进行 ARP 学习。

【配置举例】

在 VLAN 2 内配置可接受的 ARP 报文中 sender IP 的地址范围为 1.1.1.1～1.1.1.20。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname–vlan2] arp sender-ip-range 1.1.1.1 1.1.1.20
```

4.3 ND攻击防御

4.3.1 ND Snooping

【安全加固策略】

ND Snooping 功能用于二层交换网络环境，设备通过侦听 ND 或者数据报文来创建 ND Snooping 表项，该表项内容包括报文的源 IPv6 地址、源 MAC 地址、所属 VLAN 和报文入端口等信息。

ND Snooping 表项可以配合 ND Detection 和 IPv6 Source Guard 功能使用，以防止网络中的攻击源发送非法 ND 报文攻击网关等行为。

【配置举例】

在 VLAN 10 内开启学习 ND Snooping 表项的功能。

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] ipv6 nd snooping enable global
[Sysname-vlan10] ipv6 nd snooping enable link-local
[Sysname-vlan10] quit
```

配置二层以太网接口 GigabitEthernet1/0/1 学习 ND Snooping 表项的最大个数为 64（本例中的参数仅为示例）。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd snooping max-learning-num 64
[Sysname-GigabitEthernet1/0/1] quit
```

配置表项的 VALID 状态的超时时间为 250 秒（本例中的参数仅为示例）。

```
[Sysname] ipv6 nd snooping lifetime valid 250
```

配置发送两次 DAD NS 报文进行探测的时间间隔为 200 毫秒（本例中的参数仅为示例）。

```
[Sysname] ipv6 nd snooping dad retrans-timer 200
```

4.3.2 ND 协议报文源 MAC 地址一致性检查功能

【安全威胁】

如果网络中存在攻击源向设备发送大量 ND 报文，则会造成设备需要处理大量的 ND 报文，增加了 CPU 的负担。

【安全加固策略】

当攻击报文的源 MAC 地址和以太网数据帧首部中的源 MAC 地址不一致时，可以通过 ND 协议报文源 MAC 地址一致性检查功能避免此类攻击。开启本特性后，网关设备会对接收的 ND 协议报文进行检查。如果 ND 报文中的源 MAC 地址和以太网数据帧首部中的源 MAC 地址不一致，则认为是攻击报文，将其丢弃；否则，继续进行 ND 学习。

若开启 ND 日志信息功能，当 ND 报文中的源 MAC 地址和以太网数据帧首部中的源 MAC 地址不同时，会打印相关的日志信息。设备生成的 ND 日志信息会交给信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

【配置举例】

开启 ND 协议报文源 MAC 地址一致性检查功能。

```
<Sysname> system-view
```

```
[Sysname] ipv6 nd mac-check enable
```

开启 ND 日志信息功能。

```
[Sysname] ipv6 nd check log enable
```

4.3.3 ND Detection 功能

【安全加固策略】

ND Detection 功能主要用来在接入设备上检查收到的 ND 报文是否合法。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。

用户合法性检查将从非信任端口接收到的 ND 报文中的源 IPv6 地址和源 MAC 地址与设备上保存的表项进行比较，以便检查用户是否合法。用户合法性检查使用的表项包括 IPv6 Source Guard 静态绑定表项、ND Snooping 表项和 DHCPv6 Snooping 安全表项的检查。只要 ND 报文中的信息与任意一条表项相同，就认为该 ND 报文合法。

【注意事项】

配置 ND Detection 功能时，必须至少配置 IPv6 Source Guard 静态绑定表项、DHCPv6 Snooping 功能和 ND Snooping 功能三者之一，否则所有从 ND 非信任接口收到的 ND 报文都将被丢弃。

【配置举例】

在 VLAN10 内开启 ND Detection 功能。

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] ipv6 nd detection enable
[Sysname-vlan10] quit
```

配置二层以太网接口 GigabitEthernet1/0/1 为 ND 信任接口。

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd detection trust
```

开启 ND Detection 日志功能。

```
[Sysname] ipv6 nd detection log enable
```

4.3.4 RA Guard 功能

【安全威胁】

网关设备通过发送 RA（Router Advertisement，路由器通告）消息给网络中的用户，使用户能够正确完成前缀发现、地址自动分配过程。如果网络中的攻击源发送伪造的 RA 消息报文，用户收到这些 RA 消息报文后，会生成错误的 IPv6 地址，导致用户无法访问外网。

【安全加固策略】

在二层接入设备上配置 RA Guard 功能后，二层接入设备收到目的 MAC 地址为单播或组播地址的 RA 报文时，RA Guard 功能按照如下方式处理 RA 报文：

- 如果接收 RA 报文的接口配置了接口角色，则系统根据接口角色来选择转发还是丢弃该报文：
  - 若接口角色为路由器，则直接转发 RA 报文；
  - 若接口角色为用户，则直接丢弃 RA 报文。
- 如果接收 RA 报文的接口没有配置接口角色，则该报文继续匹配该接口所属 VLAN 内的 RA Guard 策略：
  - 若 RA Guard 策略中未配置任何匹配规则，则应用该策略的接口直接转发 RA 报文；

- 若 RA Guard 策略中配置了匹配规则，则 RA 报文需匹配策略下所有规则成功才会被转发；否则，该报文即被丢弃。

【配置举例】

配置二层以太网接口 GigabitEthernet1/0/1 的接口角色为用户。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ipv6 nd raguard role host
[Sysname-GigabitEthernet1/0/1] quit
```

创建 RA Guard 策略 policy1。

```
[Sysname] ipv6 nd raguard policy policy1
```

配置 RA Guard 策略。请至少选择其中一项匹配规则进行配置。

- 配置 ACL 匹配规则，引用的规则编号为 2001（本例中的参数仅为示例）。

  ```
  [Sysname-raguard-policy-policy1] if-match acl 2001
  ```

- 配置被管理地址标志位匹配规则，设置被管理地址标志位为 1（本例中的参数仅为示例）。

  ```
  [Sysname-raguard-policy-policy1] if-match autoconfig managed-address-flag on
  ```

- 配置其他信息标志位匹配规则，设置其他信息标志位为 1（本例中的参数仅为示例）。

  ```
  [Sysname-raguard-policy-policy1] if-match autoconfig other-flag on
  ```

- 配置 RA 报文内跳数匹配规则，设置 RA 报文跳数最大值为 128（本例中的参数仅为示例）。

  ```
  [Sysname-raguard-policy-policy1] if-match hop-limit maximum 128
  ```

- 配置前缀匹配规则，引用 ACL 规则编号为 2000（本例中的参数仅为示例）。

  ```
  [Sysname-raguard-policy-policy1] if-match prefix acl 2000
  ```

- 配置前缀匹配规则，配置匹配的路由器最高优先级为中级（本例中的参数仅为示例）。

  ```
  [Sysname-raguard-policy-policy1] if-match router-preference maximum medium
  [Sysname-raguard-policy-policy1] quit
  ```

在 VLAN 100 下应用 RA Guard 策略 policy1。

```
[Sysname] vlan 100
[Sysname-vlan100] ipv6 nd raguard apply policy policy1
[Sysname-vlan100] quit
```

开启 RA Guard 日志功能。

```
[Sysname] ipv6 nd raguard log enable
```

4.3.5 IPv6 Destination Guard 功能

【安全威胁】

攻击源向设备发送大量地址未解析的IPv6攻击报文，设备收到这些报文后，需要启动ND解析操作，占用大量 CPU 资源，严重影响设备性能。

【安全加固策略】

开启了 IPv6 Destination Guard 功能后，设备将会执行以下处理：

(1) 根据报文的目的 IPv6 地址和出接口对应关系查询设备记录的 DHCPv6 中继表项：

- 如果查到有对应的 DHCPv6 中继表项，则从出接口发起 ND 解析，解析成功后则转发该报文，解析不成功则丢弃该报文；
- 如果未查到对应的 DHCPv6 中继表项，则继续进行如下处理。

(2) 根据报文的目的 IPv6 地址和出接口的对应关系查询设备记录的 IP Source Guard 表项：

- 如果查到有对应的 IP Source Guard 表项，则从出接口发起 ND 解析，解析成功后则转发该报文，解析不成功则丢弃该报文；
- 如果未查到 IP Source Guard 表项，则不会发起 ND 解析，直接丢弃该报文。

当设备存在 CPU 使用率超过指定的阈值，系统内存使用率超过指定的阈值或未解析的 ND 表项数目超过某个值等情况时，设备就会进入压力模式。压力模式下，如果设备继续进行大量 ND 解析工作，会发生 CPU 满负荷运行导致系统崩溃的问题。通过指定 **stressed** 参数，保证设备在进入压力模式后，才开启 IPv6 Destination Guard 功能。这时，设备只会对 IPv6 Destination Guard 功能检查通过的报文进行 ND 解析，未经过 IPv6 Destination Guard 功能检查的报文不进行 ND 解析，从而进一步减轻了 CPU 和内存的负担。

【注意事项】

如果接口上配置了 IPv6 Destination Guard 功能，接口 IPv6 Destination Guard 功能的状态以接口的配置为准，不受全局 IPv6 Destination Guard 功能的影响。如果接口上未配置 IPv6 Destination Guard 功能，接口 IPv6 Destination Guard 功能的状态以全局的配置为准。

【配置举例】

开启压力模式的全局 IPv6 Destination Guard 功能。

```
<Sysname> system-view
[Sysname] ipv6 destination-guard global enable stressed
```

在 VLAN 接口 10 上开启 IPv6 Destination Guard 功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ipv6 destination-guard enable
```

4.4 接入业务安全

4.4.1 802.1X

1. 802.1X 静默功能

【安全威胁】

当认证失败的 802.1X 用户再次发起认证时，设备会对其进行认证处理。如果大量含有错误认证信息（例如错误用户名或错误的密码等）的 802.1X 用户频繁发起认证，会导致设备处理用户认证信息时占用大量资源，从而无法处理正常用户的认证信息。

【安全加固策略】

开启静默定时器功能后，当 802.1X 用户认证失败以后，设备静默一段时间，在静默期间，设备不对 802.1X 认证失败的用户进行认证处理。

在网络处在风险位置，容易受攻击的情况下，可以适当地将静默定时器值调大一些，反之，可以将其调小一些来提高对用户认证请求的响应速度。

【配置举例】

开启静默定时器功能，并配置静默定时器的值为 100 秒（100 仅为示例）。

```
<Sysname> system-view
[Sysname] dot1x quiet-period
[Sysname] dot1x timer quiet-period 100
```

2. 在线用户握手安全功能

【安全威胁】

如果在线的 802.1X 认证用户使用非法的客户端与设备交互，会逃过代理检测、双网卡检测等 iNode 客户端的安全检查功能，存在安全隐患。

【安全加固策略】

开启在线用户握手安全功能后，设备会通过检验客户端上传的握手报文中携带的验证信息，来确认用户是否使用 iNode 客户端进行握手报文的交互。如果握手检验不通过，则会将用户置为下线状态。

【注意事项】

只有设备上的在线用户握手功能处于开启状态时，安全握手功能才会生效。

在线用户握手安全功能仅能在 iNode 客户端和 iMC 服务器配合使用的组网环境中生效。

【配置举例】

在端口 GigabitEthernet1/0/1 上开启在线用户握手安全功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] dot1x handshake
[Sysname-GigabitEthernet1/0/1] dot1x handshake secure
```

4.4.2 端口安全

端口安全用于在端口上提供基于 MAC 地址的网络接入控制，它提供了以下安全特性：

- Need To Know 特性（NTK）

  Need To Know 特性通过检测从端口发出的数据帧的目的 MAC 地址，保证数据帧只能被发送到已经通过认证或被端口学习到的 MAC 所属的设备或主机上，从而防止非法设备窃听网络数据。

- 入侵检测（Intrusion Protection）特性

  入侵检测特性对端口接收到的数据帧进行检测，源 MAC 地址未被端口学习到的报文或未通过认证的报文，被认为是非法报文，如果发现非法报文，则对接收非法报文的端口采取相应的安全策略，包括端口被暂时断开连接、永久断开连接或 MAC 地址被阻塞一段时间，以保证端口的安全性。

- 控制 MAC 地址学习和用户认证

  通过定义不同的端口安全模式来实现：

  - 控制 MAC 学习类：无需认证，包括端口自动学习 MAC 地址和禁止 MAC 地址学习两种模式。
  - 认证类：利用 MAC 地址认证和 802.1X 认证机制来实现，包括单独认证和组合认证等多种模式。

  配置了安全模式的端口上收到用户报文后，首先查找 MAC 地址表，如果该报文的源 MAC 地址已经存在于 MAC 地址表中，则端口转发该报文，否则根据端口所采用的安全模式进行 MAC 地址学习或者触发相应的认证，并在发现非法报文后触发端口执行相应的安全防护措施（Need To Know、入侵检测）或发送 Trap 告警。缺省情况下，端口出方向的报文转发不受端口安全限制，若触发了端口 Need To Know，则才受相应限制。关于各模式的具体工作机制，以及是否触发 Need To Know、入侵检测的具体情况请参见表 4-2。

表4-2 端口安全模式描述表

端口安全采用方式	安全模式		触发的安全防护措施
端口控制MAC地址学习	autoLearn		NTK/入侵检测
	secure		
端口采用802.1X认证	userLogin		无
	userLoginSecure		NTK/入侵检测
	userLoginSecureExt		
	userLoginWithOUI		
端口采用MAC地址认证	macAddressWithRadius		NTK/入侵检测
端口采用802.1X和MAC地址认证组合认证	Or	macAddressOrUserLoginSecure	NTK/入侵检测
		macAddressOrUserLoginSecureExt	
	Else	macAddressElseUserLoginSecure	
		macAddressElseUserLoginSecureExt	

关于端口安全的详细信息，请参见“安全配置指导”中的“端口安全”。

4.4.3 Portal

1. 控制 Portal 用户的接入

【安全威胁】

在 Portal 组网环境中，设备将会面临以下安全威胁：

- 非法用户使用穷举法试探合法用户的密码。
- 非法用户接入网络。

【安全加固策略】

针对以上安全威胁，可以在设备上配置 Portal 仅允许 DHCP 用户上线功能。通常，攻击者的 IP 地址为静态配置的，因此通过禁止 IP 地址为静态配置的 Portal 认证用户上线可以一定程度上避免被攻击的风险。

【注意事项】

Portal 仅允许 DHCP 用户上线功能，仅在采用接入设备作为 DHCP 服务器的组网中生效，且不会影响已经在线的用户。

在 IPv6 网络中，开启 Portal 仅允许 DHCP 用户上线功能后，终端仍会使用临时 IPv6 地址进行 Portal 认证，从而导致认证失败，所以终端必须关闭临时 IPv6 地址。

Portal 认证前域中的用户在指定时间内认证失败达到限定次数后不会被阻塞。

【配置举例】

在接口 Vlan-interface100 上配置仅允许通过 DHCP 获取 IP 地址的客户端上线功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal user-dhcp-only
```

2. 限制 Portal 最大用户数

【安全加固策略】

在线 Portal 用户数过多，会导致系统资源不足。为解决这个问题，可以限制在线 Portal 用户数，当在线 Portal 用户数超过设定的最大值时，系统会拒绝新的 Portal 用户接入。

【注意事项】

建议将全局最大Portal用户数配置为所有开启Portal的接口上的最大IPv4 Portal用户数和最大IPv6 Portal 用户数之和，但不超过整机最大 Portal 用户数，否则会有部分 Portal 用户因为整机最大用户数已达到而无法上线。

【配置举例】

- 配置全局 Portal 最大用户数

  # 配置全局 Portal 最大用户数为 100。

  ```
  <Sysname> system-view
  [Sysname] portal max-user 100
  ```

- 配置接口上的 Portal 最大用户数
  - （IPv4 网络）

    # 在接口 Vlan-interface100 上配置 IPv4 Portal 最大用户数为 100。

    ```
    <Sysname> system-view
    [Sysname] interface vlan-interface 100
    [Sysname-Vlan-interface100] portal ipv4-max-user 100
    ```

  - （IPv6 网络）

    # 在接口 Vlan-interface100 上配置 IPv6 Portal 最大用户数为 100。

    ```
    <Sysname> system-view
    [Sysname] interface vlan-interface 100
    [Sysname-Vlan-interface100] portal ipv6-max-user 100
    ```

3. Portal 授权信息严格检查

【安全加固策略】

严格检查模式用于配合服务器上的用户授权控制策略，它仅允许接口上成功下发了授权信息的用户在线。开启 Portal 授权信息的严格检查模式后，当认证服务器下发的授权 ACL、User Profile 在设备上不存在或者设备下发 ACL、User Profile 失败时，设备将强制 Portal 用户下线。若同时开启了对授权 ACL 和对授权 User Profile 的严格检查模式，则只要其中任意一个授权属性未通过严格授权检查，则用户就会下线。

【配置举例】

在接口 Vlan-interface100 上开启对授权 ACL 的严格检查模式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal authorization acl strict-checking
```

4.4.4 限制 Web 认证最大用户数

【安全加固策略】

在线 Web 认证用户数过多，会导致系统资源不足。为解决这个问题，可以限制在线 Web 认证用户数，当在线 Web 认证用户数超过设定的最大值时，系统会拒绝新的 Web 认证用户接入。

【注意事项】

若配置的 Web 认证最大用户数小于当前已经在线的 Web 认证用户数，则该命令可以执行成功，且在线 Web 认证用户不受影响，但系统将不允许新的 Web 认证用户接入。

【配置举例】

在接口 GigabitEthernet1/0/1 上配置 Web 认证最大用户数为 32（32 仅为示例）。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] web-auth max-user 32
```

4.4.5 FIP Snooping

FCoE 增加了组网的灵活性，在 ENode 和 FCF 交换机之间可以存在 Transit 交换机，这就使得 FCF 交换机和 ENode 之间的物理连接不再是点对点连接，这样会出现未注册的 ENode 设备也可能通过 FCF 交换机和 FC SAN 中的设备进行通信。比如，两个 ENode 通过一台 Transit 交换机接入到同一台 FCF 交换机，如果有一个 ENode 在 FCF 交换机上成功注册，则 FCF 交换机上的接口会变为 up，此时，另外一个没有注册的 ENode 就可以通过该 FCF 交换机和 FC SAN 中的设备进行通信了。

FIP Snooping 通过对报文 MAC 地址的检查来限定 ENode 发送的报文仅能转发给 FCF 交换机，不能转发给 ENode，且只有成功注册的 ENode 发送的 FCoE 报文才能被 Transit 交换机转发给 FCF 交换机，以及限定 FCF 交换机发送的 FCoE 报文仅能被 Transit 交换机转发给已经注册的 ENode。

关于 FIP Snooping 的详细信息，请参见“FC 和 FCoE 配置指导”中的“FIP Snooping”。

4.4.6 HTTPS 重定向

1. 配置 HTTPS 重定向服务关联的 SSL 服务器端策略

【安全威胁】

缺省情况下，HTTPS 重定向服务使用设备自签名的证书，SSL 参数均为缺省值。这种方式简化了配置，但是存在安全隐患。

【安全加固策略】

可以通过配置 SSL 服务器端策略，并将其与 HTTPS 重定向服务进行关联，来增强 HTTPS 重定向服务的安全性。

【注意事项】

如果关联的 SSL 服务器端策略不存在，则无法完成 HTTPS 报文的重定向。允许用户先关联一个不存在的 SSL 服务器端策略，再对该策略进行相关配置。

【配置举例】

指定 HTTPS 重定向服务关联的 SSL 服务器端策略为 policy1。

```
<Sysname> system-view
[Sysname] http-redirect ssl-server-policy policy1
```

4.5 DHCP安全

4.5.1 DHCP Flood 攻击防范功能

【安全威胁】

攻击源发送大量 DHCP 请求报文给 DHCP 服务器，占用 DHCP 服务器大量的 CPU 资源并耗尽 DHCP 服务器上的地址空间，使合法的 DHCP 客户端无法获取到 IP 地址。

【安全加固策略】

在开启 DHCP 服务器/DHCP 中继功能的接口配置 DHCP Flood 攻击防范功能后，DHCP 服务器/DHCP 中继会根据 DHCP 报文中的源 MAC 地址统计收到的 DHCP 报文数，并创建一个 check 状态的 DHCP 防 Flood 攻击表项。当收到某个 MAC 地址对应 DHCP 客户端发送的报文数在指定的时间内达到配置的最大报文数时，DHCP 服务器/DHCP 中继认为受到了该 DHCP 客户端的攻击，DHCP 防 Flood 攻击表项状态从 check 状态变成 restrain 状态，且 DHCP 服务器/DHCP 中继丢弃该 DHCP 客户端发送的 DHCP 报文。当某个 MAC 地址对应的 DHCP Flood 攻击表项老化时间到达后，设备会删除此表项，之后设备再次收到源 MAC 地址为此 MAC 地址的 DHCP 请求报文时会重新统计接收到的报文数目。

【注意事项】

DHCP 和 DHCPv6 组网中均支持 DHCP Flood 攻击防范功能。

【配置举例】

- 在普通组网配置 DHCP Flood 攻击防范功能。

  # 配置 DHCP Flood 攻击检测最大报文数为 2，检测时间为 9000 毫秒（本例中的参数仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] dhcp flood-protection threshold 2 9000
  ```

  # 配置 DHCP Flood 攻击表项老化时间为 90 秒（本例中的参数仅为示例）。

  ```
  [Sysname] dhcp flood-protection aging-time 90
  ```

  # 在接口 Vlan-interface100 上开启 DHCP Flood 攻击防范功能。

  ```
  [Sysname] interface vlan-interface 100
  [Sysname-Vlan-interface100] dhcp flood-protection enable
  ```

- 在 VXLAN 组网配置 DHCP Flood 攻击防范功能。

  # 配置 DHCP Flood 攻击检测最大报文数为 2，检测时间为 9000 毫秒（本例中的参数仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] dhcp flood-protection threshold 2 9000
  ```

  # 配置 DHCP Flood 攻击表项老化时间为 90 秒（本例中的参数仅为示例）。

  ```
  [Sysname] dhcp flood-protection aging-time 90
  ```

  # 在 VSI 1 上开启 DHCP Flood 攻击防范功能。

  ```
  [Sysname] vsi 1
  [Sysname-vsi-1] dhcp flood-protection enable
  ```

- 配置 DHCPv6 Flood 攻击防范功能

  # 配置 DHCPv6 Flood 攻击检测最大报文数为 2，检测时间为 9000 毫秒（本例中的参数仅为示例）。

```
<Sysname> system-view
[Sysname] ipv6 dhcp flood-protection threshold 2 9000
```
配置 DHCPv6 Flood 攻击表项老化时间为 90 秒。
```
[Sysname] ipv6 dhcp flood-protection aging-time 90
```
在 VSI 1 上开启 DHCPv6 Flood 攻击防范功能。
```
[Sysname] vsi 1
[Sysname-vsi-1] ipv6 dhcp flood-protection enable
```

4.5.2 防止 DHCP 饿死攻击功能

【安全威胁】

DHCP 饿死攻击是指攻击者伪造 chaddr 字段各不相同的 DHCP 请求报文，向 DHCP 服务器申请大量的 IP 地址，导致 DHCP 服务器地址池中的地址耗尽，无法为合法的 DHCP 客户端分配 IP 地址，或导致 DHCP 服务器消耗过多的系统资源，无法处理正常业务。

【安全加固策略】

如果封装 DHCP 请求报文的数据帧的源 MAC 地址各不相同，则通过限制接口可以学习到的 MAC 地址数，并配置学习到的 MAC 地址数达到最大值时，丢弃源 MAC 地址不在 MAC 地址表里的报文，能够避免攻击者申请过多的 IP 地址，在一定程度上阻止了 DHCP 饿死攻击。此时，不存在 DHCP 饿死攻击的接口下的 DHCP 客户端可以正常获取 IP 地址，但存在 DHCP 饿死攻击的接口下的 DHCP 客户端仍可能无法获取 IP 地址。

如果封装 DHCP 请求报文的数据帧的 MAC 地址都相同，则通过上述方法无法防止 DHCP 饿死攻击。在这种情况下，需要开启 DHCP 服务器/DHCP 中继的 MAC 地址检查功能。开启该功能后，DHCP 服务器/DHCP 中继检查接收到的 DHCP 请求报文中的 chaddr 字段和数据帧的源 MAC 地址字段是否一致。如果一致，则认为该报文合法，进行后续处理；如果不一致，则丢弃该报文。

【配置举例】

在接口 Vlan-interface100 上开启 DHCP 服务器的 MAC 地址检查功能。
```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] dhcp server check mac-address
```
在接口 Vlan-interface100 上开启 DHCP 中继的 MAC 地址检查功能。
```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] dhcp relay check mac-address
```

4.5.3 DHCP 用户类白名单功能

【安全威胁】

DHCP 支持按照用户类分配 IP 地址。DHCP 服务器会根据用户所在的用户类，从对应的地址空间中选择地址分给用户。当某些用户类中存在攻击源时，攻击源获取到地址后，就能在网络中发起攻击行为。

【安全加固策略】

为了避免上述问题，用户可以将不存在攻击源的用户类加入白名单。DHCP 服务器只有收到属于用户类白名单的 DHCP 客户端发送的请求报文，才会进行处理。

【注意事项】

- 如果某个用户类未加入白名单，则该用户类对应的所有 DHCP 客户端都无法获取到 IP 地址。
- 如果 DHCP 客户端请求的是静态绑定租约，则 DHCP 服务器不进行白名单检查直接处理。

【配置举例】

在 DHCP 地址池 0 中开启 DHCP 用户类白名单功能（本例中的参数仅为示例）。

```
<Sysname> syatem-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] verify class
```

在 DHCP 地址池 0 中配置 DHCP 白名单包括的用户类名为 test1 和 test2。

```
[Sysname-dhcp-pool-0] valid class test1 test2
```

4.5.4 DHCP 中继用户地址表项管理功能

【安全威胁】

在通过 DHCP 获取地址的组网环境中，所有合法客户端都通过 DHCP 方式获取到 IP 地址。某些非法主机使用自身伪造的 IP 地址发送攻击报文攻击网关，影响网关设备的正常工作。

【安全加固策略】

- DHCP 中继用户地址表项记录功能

  开启本功能后，当客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址时，DHCP 中继可以自动记录客户端 IP 地址与硬件地址的绑定关系，生成 DHCP 中继的用户地址表项。

  本功能与其他 IP 地址安全功能（如 ARP 地址检查、授权 ARP 和 IP Source Guard）配合，可以实现只允许匹配用户地址表项中绑定关系的报文通过 DHCP 中继。从而，保证非法主机不能通过 DHCP 中继与外部网络通信。

- DHCP 中继动态用户地址表项定时刷新功能

  DHCP 中继动态用户地址表项定时刷新功能开启时，DHCP 中继每隔指定时间采用客户端获取到的 IP 地址向 DHCP 服务器发送 DHCP-REQUEST 报文：

  - 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-ACK 报文或在指定时间内未接收到 DHCP 服务器的响应报文，则表明这个 IP 地址已经可以进行分配，DHCP 中继会删除动态用户地址表中对应的表项。为了避免地址浪费，DHCP 中继收到 DHCP-ACK 报文后，会发送 DHCP-RELEASE 报文释放申请到的 IP 地址。
  - 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-NAK 报文，则表示该 IP 地址的租约仍然存在，DHCP 中继不会删除该 IP 地址对应的表项。

- DHCP 中继的用户下线探测功能

  如果在接口上配置了 DHCP 中继的用户下线检测功能，则当 ARP 表项老化时，DHCP 中继认为该表项对应的用户已经下线，删除对应的用户地址表项，并通过发送 Release 报文通知 DHCP 服务器删除下线用户的 IP 地址租约。

【注意事项】

手工删除 ARP 表项，不会触发 DHCP 中继删除对应的用户地址表项。

【配置举例】

开启 DHCP 中继用户地址表项记录功能。

```
<Sysname> system-view
```

```
[Sysname] dhcp relay client-information record
```

开启 DHCP 中继动态用户地址表项定时刷新功能。

```
[Sysname] dhcp relay client-information refresh enable
```

配置 DHCP 中继动态用户地址表项的刷新时间间隔为 100 秒（本例中的参数仅为示例）。

```
[Sysname] dhcp relay client-information refresh interval 100
```

开启用户下线探测功能。

```
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] dhcp client-detect
```

4.5.5 DHCP 中继支持代理功能

【安全威胁】

非法用户向 DHCP 服务器发送攻击报文后，影响 DHCP 服务器正常工作。

【安全加固策略】

开启 DHCP 中继支持代理功能后，DHCP 中继收到 DHCP 服务器的应答报文，会把报文中的 DHCP 服务器地址修改为中继的接口地址，并转发给 DHCP 客户端。当 DHCP 客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址等网络参数后，DHCP 客户端会把 DHCP 中继当作自己的服务器，来进行后续的 DHCP 功能的报文交互。从而达到了把真正的 DHCP 服务器和 DHCP 客户端隔离开，保护 DHCP 服务器的目的。

【配置举例】

配置接口 Vlan-interface100 工作在 DHCP 代理模式。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] dhcp select relay proxy
```

4.5.6 DHCPv6 服务器记录的地址租约表项转化为 IP Source Guard 动态表项功能

【安全加固策略】

开启本功能后，DHCPv6 服务器记录的地址租约表项会转化为 IP Source Guard 动态表项，并将对应的 IP Source Guard 表项上报给控制器进行管理。控制器通过查询上报的 IP Source Guard 动态表项信息，对表项对应的终端用户进行定位和监控等操作。

【配置举例】

开启 DHCPv6 服务器记录的地址租约表项转化为 IP Source Guard 动态表项的功能。

```
<Sysname> system-view
[Sysname] ipv6 dhcp server entry-convert enable
```

4.5.7 DHCP Snooping

DHCP Snooping 是 DHCP 的一种安全特性。DHCP Snooping 设备位于 DHCP 客户端与 DHCP 服务器之间，或 DHCP 客户端与 DHCP 中继之间。DHCP Snooping 的作用是：

- 保证客户端从合法的服务器获取 IP 地址

  为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口：

  - 信任端口正常转发接收到的 DHCP 报文。

- 不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。

- 记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系

  DHCP Snooping 通过监听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息。DHCP Snooping 表项可以供 ARP Detection 和 IP Source Guard 等安全功能使用。

关于 DHCP Snooping 的详细信息，请参见“三层技术-IP 业务配置指导”中的“DHCP Snooping”。
关于 DHCPv6 Snooping 的详细信息，请参见“三层技术-IP 业务配置指导”中的“DHCPv6 Snooping”。

4.5.8 DHCPv6 guard

DHCPv6 guard 功能可保证设备从信任的 DHCPv6 服务器获取地址，并可根据 DHCPv6 报文源地址、分配给用户的 IPv6 地址或 DHCPv6 服务器优先级等信息对 DHCPv6 应答报文进行过滤，保证 DHCPv6 客户端从指定的 DHCPv6 服务器上获取前缀、地址或其他参数。与 DHCP snooping 功能相比，DHCP guard 功能可以对 DHCP 服务器进行更加精细地过滤。

关于 DHCPv6 guard 的详细信息，请参见“三层技术-IP 业务配置指导”中的“DHCPv6 guard”。

4.6 DNS安全

【安全威胁】

网络攻击者通过 DHCP 服务器为设备分配错误的域名后缀和域名服务器地址，会导致设备域名解析失败，或解析到错误的结果。

【安全加固策略】

在设备上指定 DNS 信任接口后，域名解析时只采用信任接口动态获得的域名后缀和域名服务器信息，非信任接口获得的信息不能用于域名解析，从而在一定程度上避免这类攻击。

【配置举例】

指定 VLAN 接口 2 为 DNS 信任接口（本例中的参数仅为示例）。

```
<Sysname> system-view
[Sysname] dns trust-interface vlan-interface 2
```

4.7 ICMP安全

【安全威胁】

ICMP 差错报文通常被网络层或传输层协议用来在异常情况发生时通知相应设备，以便进行控制和管理。当网络攻击源发送 ICMP 差错报文进行恶意攻击时，会改变设备的报文转发路径，影响报文的正常发送。

【安全加固策略】

常见的 ICMP 差错报文包括 ICMP 重定向报文、ICMP 超时报文和 ICMP 目的不可达报文。为了防止攻击，建议关闭这些 ICMP 报文发送功能。

【配置举例】

- 配置 ICMPv4 安全功能。

关闭设备的 ICMP 重定向报文发送功能。

```
<Sysname> system-view
[Sysname] undo ip redirects enable
```

关闭设备的 ICMP 超时报文发送功能。

```
[Sysname] undo ip ttl-expires enable
```

关闭设备的 ICMP 目的不可达报文发送功能。

```
[Sysname] undo ip unreachables enable
```

- 配置 ICMPv6 安全功能。

  # 关闭设备的 ICMPv6 目的不可达报文发送功能。

  ```
  <Sysname> system-view
  [Sysname] undo ipv6 unreachables enable
  ```

  # 关闭设备的 ICMPv6 超时报文发送功能。

  ```
  [Sysname] undo ipv6 hoplimit-expires enable
  ```

  # 关闭设备的 ICMPv6 重定向报文发送功能。

```
[Sysname] undo ipv6 redirects enable
```

4.8 TCP安全

4.8.1 SYN Cookie 功能

【安全威胁】

SYN Flood 攻击是指攻击者向设备发送大量请求建立 TCP 连接的 SYN 报文，而不回应设备的 SYN ACK 报文，导致设备上建立了大量的 TCP 半连接，从而达到耗费设备资源，使设备无法处理正常业务的目的。

【安全加固策略】

SYN Cookie 功能用来防止 SYN Flood 攻击。配置 SYN Cookie 功能后，当设备收到 TCP 连接请求时，不建立 TCP 半连接，而直接向发起者回复 SYN ACK 报文。设备接收到发起者回应的 ACK 报文后，建立连接，并进入 ESTABLISHED 状态。通过这种方式，可以避免在设备上建立大量的 TCP 半连接。

【配置举例】

开启 SYN Cookie 功能。

```
<Sysname> system-view
[Sysname] tcp syn-cookie enable
```

4.8.2 禁止发送 TCP 报文时添加 TCP 时间戳选项信息

【安全威胁】

TCP 报文携带 TCP 时间戳选项信息时，建立 TCP 连接的两台设备通过 TCP 报文中的时间戳字段就可计算出 RTT（Round Trip Time，往返时间）值。在某些组网中，TCP 连接上的中间设备获取到 TCP 时间戳信息，学习到 TCP 连接成功的时间。如果中间设备存在攻击源，则 TCP 连接存在安全隐患。

【安全加固策略】

为了防止上述攻击，可以在 TCP 连接的任意一端关闭发送 TCP 报文时添加时间戳选项信息功能。

【配置举例】

配置发送 TCP 报文时不添加 TCP 时间戳选项信息。

```
<Sysname> system-view
[Sysname] undo tcp timestamps enable
```

4.9 路由协议安全

4.9.1 RIP/RIPng

【安全威胁】

攻击者仿冒 RIP 邻居或修改 RIP 路由信息，可能会使设备学习到错误的路由或引发网络中断。

【安全加固策略】

RIP 和 RIPng 提供了如下几种安全策略：

- 对 RIP-1 和 RIPng 报文的零域检查

  RIP-1 和 RIPng 报文中的有些字段必须为零，称之为零域。用户可配置 RIP-1 在接收报文时对零域进行检查，零域值不为零的 RIP-1 报文将不被处理。

- 对接收到的 RIP 路由更新报文进行源 IP 地址检查

  RIP 在接收报文时进行源 IP 地址检查，即检查发送报文的接口 IP 地址与接收报文接口的 IP 地址是否处于同一网段。如果没有通过检查，则该 RIP 报文将不被处理。

- RIPv2 的报文认证机制

  设备在发送报文时携带验证信息，在接收报文时对验证信息进行校验，如果报文校验失败，则该报文将被丢弃。这样可以避免设备接收无法信任的设备的 RIPv2 报文。

- RIPng 基于 IPsec 安全框架的认证方式

  设备在发送的报文中会携带配置好的 IPsec 安全框架的 SPI（Security Parameter Index，安全参数索引）值，接收报文时通过 SPI 值进行 IPsec 安全框架匹配：仅接收安全框架匹配的报文；否则该报文将被丢弃，无法正常建立邻居和学习路由。IPsec 安全框架的具体情况请参见“安全配置指导”中的“IPsec”。

【配置举例】

开启进程号为 1 的 RIP 进程对 RIP-1 报文的零域检查功能。

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] checkzero
```

开启对接收到的 RIP 路由更新报文进行源 IP 地址检查的功能。

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] validate-source-address
```

在接口 Vlan-interface10 上配置 RFC 2453 格式的 MD5 明文验证，密钥为 154&rose（154&rose 仅为示例）。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] rip version 2
[Sysname-Vlan-interface10] rip authentication-mode md5 rfc2453 plain 154&rose
```

开启进程号为 100 的 RIPng 进程对 RIPng 报文的零域检查功能。

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] checkzero
```

配置接口 Vlan-interface10 应用的 IPsec 安全框架为 profile001（profile001 仅为示例）。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ripng ipsec-profile profile001
```

4.9.2 OSPF/OSPFv3

【安全加固策略】

OSPF/OSPFv3 报文验证功能可避免路由信息外泄或者 OSPF 路由器受到恶意攻击。建立 OSPF/OSPFv3 邻居关系时，在发送的报文中携带配置的验证信息；接收报文时对验证信息进行校验。只有通过校验的报文才能接收，否则将不会接收报文，无法建立邻居。

除此之外，OSPFv3 还可通过基于 IPsec 安全框架的认证方式来对 OSPFv3 报文进行有效性检查和验证。IPsec 安全框架的详细介绍请参见“安全配置指导”中的“IPsec”。

GTSM（Generalized TTL Security Mechanism，通用 TTL 安全保护机制）功能可避免设备受到 CPU 利用（CPU-utilization）等类型的攻击（如 CPU 过载）。当设备收到来自 OSPF 普通邻居或虚连接邻居的报文时，会判断报文的 TTL 是否在 255-“*hop-count*”+1 到 255 之间。如果在，就上送报文；如果不在，则直接丢弃报文。

【配置举例】

配置 OSPF 区域 0 使用 MD5 明文验证模式，验证字标识符为 15，验证密钥为 abc。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5 15 plain abc
```

配置接口 Vlan-interface10 采用 MD5 明文验证模式，验证字标识符为 15，验证密钥为 Ab&123456。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf authentication-mode md5 15 plain Ab&123456
```

配置 OSPFv3 区域 1 使用 keychain 验证模式，keychain 名为 test（test 仅为示例）。

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] authentication-mode keychain test
```

配置 OSPFv3 进程 1 区域 0 的安全框架为 profile001（profile001 仅为示例）。

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0] enable ipsec-profile profile001
```

开启接口 Vlan-interface10 的 GTSM 功能，并指定最大跳数为 254（254 仅为示例）。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] ospf ttl-security hops 254
```

4.9.3 IS-IS

【安全加固策略】

IS-IS 提供邻居关系验证、区域验证以及路由域验证功能。设备将验证密钥按照设定的方式封装到相应的报文中，在接收报文时检查报文中携带的验证密钥，如果验证密钥不匹配，则该报文将被丢弃。不同的 IS-IS 安全加固策略应用场景不同，具体如下：

- 邻居关系验证：可以确认邻居的正确性和有效性，防止与无法信任的路由器形成邻居。验证密钥将会按照设定的方式封装到 Hello 报文中，并检查接收到的 Hello 报文中携带的验证密钥，通过检查才会形成邻居关系，否则无法形成邻居关系。
- 区域验证：可以防止从不可信任的路由器学习到的路由信息加入到本地 Level-1 的 LSDB 中。验证密钥将会按照设定的方式封装到 Level-1 报文（LSP、CSNP、PSNP）中，并检查收到的 Level-1 报文中携带的验证密钥，通过检查的 Level-1 报文才会被接收，否则该报文将会被丢弃。
- 路由域验证：可以防止将不可信的路由信息注入当前路由域。验证密钥将会按照设定的方式封装到 Level-2 报文（LSP、CSNP、PSNP）中，并检查收到的 Level-2 报文中携带的验证密钥，通过检查的 Level-2 报文才会被接收，否则该报文将会被丢弃。

【配置举例】

为接口 Vlan-interface10 配置邻居关系采用简单明文验证模式，验证密钥为 Ab&123456（Ab&123456 仅为示例）。

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] isis authentication-mode simple plain Ab&123456
```

在 IS-IS 进程 1 下配置区域采用简单明文验证模式，验证密钥为 Ab&123456（Ab&123456 仅为示例）。

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] area-authentication-mode simple plain Ab&123456
```

配置路由域采用简单明文验证模式，认证密钥为 Ab&123456（Ab&123456 仅为示例）。

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] domain-authentication-mode simple plain Ab&123456
```

4.9.4 BGP

1. 限制从 BGP 对等体/对等体组接收的路由数量

【安全威胁】

非法用户通过向设备发送大量 BGP 路由的方式对设备进行攻击，浪费系统资源，引起网络故障。

【安全加固策略】

为了预防这种攻击，设备可以限制从指定对等体/对等体组接收路由的数量，并且在接收到的 BGP 路由达到配置值时，可以选择如下处理方式：

- 路由器中断与该对等体/对等体组的 BGP 会话，不再尝试重建会话。
- 路由器保持与该对等体/对等体组的 BGP 会话，可以继续接收路由，仅打印日志信息。
- 路由器保持与该对等体/对等体组的 BGP 会话，丢弃超出限制的路由，并打印日志信息。
- 路由器中断与该对等体/对等体组的 BGP 会话，经过指定的时间后自动与对等体/对等体组重建会话。

【配置举例】

在 BGP IPv4 单播地址族视图下，设置允许从对等体 1.1.1.1 收到的路由数量为 10000。如果从对等体 1.1.1.1 收到的路由数量超过 10000，则断开与该对等体的会话。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp-default] address-family ipv4 unicast
[Sysname-bgp-default-ipv4] peer 1.1.1.1 route-limit 10000
```

2. 建立安全的 BGP 会话

【安全威胁】

攻击者可以冒充合法用户与设备建立 BGP 会话，或窃取并篡改 BGP 报文，影响 BGP 路由的学习。

【安全加固策略】

BGP 使用 TCP 作为其传输层协议，为了避免受到以上两种方式的攻击，可以为 BGP 对等体配置 BGP 的 MD5 认证或 keychain 认证：

- 为 BGP 建立 TCP 连接时进行 MD5 认证，只有两台设备配置的密钥相同时，才能建立 TCP 连接，从而避免与非法的设备建立 TCP 连接。
- 传递 BGP 报文时，对封装 BGP 报文的 TCP 报文段进行 MD5 运算，从而保证 BGP 报文不会被篡改。
- 为 BGP 建立 TCP 连接时，配置 keychain 认证，只有两台配置 keychain 认证的设备满足以下条件时才能正常建立 TCP 连接、交互 BGP 消息：
  - 同一时间内使用的 key 的标识符相同。
  - 相同标识符的 key 的认证算法和认证密钥一致。

【配置举例】

在 BGP 实例视图下，配置本地路由器 10.1.100.1 与对等体 10.1.100.2 之间的 BGP 会话使用 MD5 认证，密钥为明文字符串 358$aabbcc。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 10.1.100.2 password simple 358$aabbcc
```

在 BGP 实例视图下，配置 IP 地址为 10.1.1.1 的对等体使用名为 abc 的 keychain 认证。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer 10.1.1.1 as-number 100
[Sysname-bgp-default] peer 10.1.1.1 keychain abc
```

3. BGP GTSM

【安全威胁】

攻击者向网络设备发送大量有效的 IP 报文时，对网络设备造成 CPU 利用（CPU-utilization）等类型的攻击。

【安全加固策略】

GTSM（Generalized TTL Security Mechanism，通用 TTL 安全保护机制）是一种简单易行的、对基于 IP 协议的上层业务进行保护的安全机制。GTSM 通过检查接收到的 IP 报文头中的 TTL 值是否在一个预先定义好的范围内，来判断 IP 报文是否合法。用户可以指定本地设备到达某个对等体的最大跳数，则从该对等体接收到的 BGP 报文的合法 TTL 范围为 255-“最大跳数”+1 到 255。只有来自该对等体的报文 TTL 值在该合法范围内时，才将报文上送 CPU 处理；否则，直接丢弃报文。另外，配置 BGP GTSM 功能后，设备会将发送报文的初始 TTL 设置为 255。

【注意事项】

对于直连 EBGP 对等体，GTSM 可以提供最佳的保护效果；对于非直连 EBGP 或 IBGP 对等体，由于中间设备可能对 TTL 值进行篡改，GTSM 的保护效果受到中间设备安全性的限制。

【配置举例】

在 BGP 实例视图下，为已经创建的对等体组 test 开启 BGP GTSM 功能，并指定对等体组中的对等体到达本地设备的最大跳数为 1。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test ttl-security hops 1
```

4. BGP RPKI

【安全威胁】

BGP 路由中的 AS_PATH 属性记录了某条路由从本地到某个 IP 地址（网段）所要经过的所有 AS 号。其中，该 IP 地址（网段）所处的 AS 称为源 AS。如果攻击者篡改了源 AS，则会导致指定 IP 地址（网段）不可达甚至网络瘫痪。攻击者还可以通过构造非法的源 AS 向网络设备通告路由，窃取 BGP 路由信息。

【安全加固策略】

配置 BGP RPKI（Resource Public Key Infrastructure，资源公钥基础设施）功能后，设备在收到 BGP 路由的时候，会验证源 AS 是否合法，并根据验证结果来决定是否使用该 BGP 路由以及是否发布该路由。

【配置举例】

开启 BGP RPKI 功能，指定 BGP RPKI 服务器地址为 1.1.1.1，配置与 RPKI 服务器建立连接的端口号为 1234。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] rpki
[Sysname-bgp-default-rpki] server tcp 1.1.1.1
[Sysname-bgp-default-rpki-server] port 1234
```

5. BGP 通过 IPsec 保护 IPv6 BGP 报文

【安全加固策略】

为了避免路由信息外泄或者非法者对设备进行恶意攻击，可以利用 IPsec 安全隧道对 IPv6 BGP 报文进行保护。通过 IPsec 提供的数据机密性、完整性、数据源认证等功能，确保 IPv6 BGP 报文不会被侦听或恶意篡改，并避免非法者构造 IPv6 BGP 报文对设备进行攻击。

在互为 IPv6 BGP 邻居的两台设备上都配置通过 IPsec 保护 IPv6 BGP 报文后，一端设备在发送 IPv6 BGP 报文时通过 IPsec 对报文进行加封装，另一端设备接收到报文后，通过 IPsec 对报文进行解封装。如果解封装成功，则接收该报文，正常建立 IPv6 BGP 对等体关系或学习 IPv6 BGP 路由；如果设备接收到不受 IPsec 保护的 IPv6 BGP 报文，或 IPv6 BGP 报文解封装失败，则会丢弃该报文。

【配置举例】

配置 IPsec 安全提议和手工方式的 IPsec 安全框架。相关配置的详细介绍请参见“安全配置指导”中的“IPsec”。

在 BGP 实例视图下，为对等体组 test 应用安全框架 profile001。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-default] peer test ipsec-profile profile001
```

4.10 组播安全

4.10.1 IGMP Snooping/MLD Snooping

1. 配置组播组过滤器

【安全威胁】

恶意用户通过变换组地址，使用一些无效组播组频道加入，造成设备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。

【安全加固策略】

在使能了 IGMP Snooping/MLD Snooping 的二层设备上，通过配置组播组过滤器，可以限制用户对组播节目的点播。当用户点播某个组播节目时，主机会发起一个 IGMP/MLD 成员关系报告报文，该报文将在二层设备上接受组播组过滤器的检查，只有通过了检查，二层设备才会将该主机所属的端口加入到出端口列表中，从而达到控制用户点播组播节目的目的。

【配置举例】

全局配置组播组过滤器，以限定 VLAN 2 内的主机只能加入组播组 225.1.1.1。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] igmp-snooping
[Sysname-igmp-snooping] group-policy 2000 vlan 2
```

全局配置 IPv6 组播组过滤器，以限定 VLAN 2 内的主机只能加入 IPv6 组播组 FF03::101。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] mld-snooping
```

```
[Sysname-mld-snooping] group-policy 2000 vlan 2
```

在端口 GigabitEthernet1/0/1 上配置组播组过滤器，以限定端口 GigabitEthernet1/0/1 下 VLAN 2 内的主机只能加入组播组 225.1.1.1。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 225.1.1.1 0
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping group-policy 2000 vlan 2
```

在端口 GigabitEthernet1/0/1 上配置 IPv6 组播组过滤器，以限定端口 GigabitEthernet1/0/1 下 VLAN 2 内的主机只能加入 IPv6 组播组 FF03::101。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source ff03::101 128
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping group-policy 2000 vlan 2
```

2. 禁止端口成为动态路由器端口

【安全威胁】

在组播用户接入网络中，用户主机在某些情况下（比如测试）发出 IGMP/MLD 普遍组查询报文或 IPv4/IPv6 PIM Hello 报文，此时存在如下安全威胁：

- 如果二层设备收到了某用户主机发来的 IGMP/MLD 普遍组查询报文或 IPv4/IPv6 PIM Hello 报文，那么接收报文的端口就将成为动态路由器端口，从而使 VLAN 内的所有组播报文都会向该端口转发，导致该主机收到大量无用的组播报文。
- 用户主机发送 IGMP/MLD 普遍组查询报文或 IPv4/IPv6 PIM Hello 报文，也会影响该接入网络中三层设备上的组播路由协议状态（如影响 IGMP/MLD 查询器或 DR 的选举），严重时可能导致网络中断。

【安全加固策略】

当配置了禁止端口成为动态路由器端口功能后，即使该端口收到了 IGMP/MLD 普遍组查询报文或 IPv4/IPv6 PIM Hello 报文，该端口也不会成为动态路由器端口，从而能够有效解决上述问题，提高网络的安全性和对组播用户的控制能力。

【配置举例】

禁止端口 GigabitEthernet1/0/1 在 VLAN 2 内成为动态路由器端口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] igmp-snooping router-port-deny vlan 2
```

禁止端口 GigabitEthernet1/0/1 在 VLAN 2 内成为动态路由器端口。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mld-snooping router-port-deny vlan 2
```

4.10.2 PIM/IPv6 PIM

1. 配置 Hello 报文过滤器

【安全威胁】

在 PIM 域中，设备上每个运行了 PIM 协议的接口通过定期向本网段的所有 PIM 设备（224.0.0.13）组播 PIM Hello 报文来发现 PIM 邻居，维护各设备之间的 PIM 邻居关系，从而构建和维护 SPT。当设备上存在大量恶意 Hello 报文时，正常的 PIM 邻居建立机制受到干扰，导致 PIM 邻居关系无法正确建立，继而设备受到各种 PIM 协议报文攻击。

【安全加固策略】

可以通过在接口上配置 Hello 报文过滤器，通过 ACL 规则限制合法的 Hello 报文源地址范围，从而丢弃恶意的报文，提高设备对 PIM 协议报文处理的安全性。

【配置举例】

在接口 VLAN-interface 100 上配置合法 Hello 报文的源地址范围，只允许与来自网段 10.1.1.0/24 中的设备建立 PIM 邻居关系。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] quit
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] pim neighbor-policy 2000
```

在接口 VLAN-interface 100 上配置合法 Hello 报文的源地址范围，只允许与来自网段 FE80:101::101/64 中的设备建立 IPv6 PIM 邻居关系。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source fe80:101::101 64
[Sysname-acl-ipv6-basic-2000] quit
[Sysname] interface vlan-interface 100
[Sysname- Vlan-interface100] ipv6 pim neighbor-policy 2000
```

4.10.3 MSDP

【安全加固策略】

通过在 MSDP 对等体上配置 MD5 认证功能，为 TCP 连接设置 MD5 认证密钥并由 TCP 完成认证。只有认证通过，才可以正常建立 TCP 连接，从而阻止非法报文的恶意攻击。

【注意事项】

参与 MD5 认证的两端 MSDP 对等体必须配置相同的认证方式和密钥，否则将由于不能通过认证而无法建立 TCP 连接。

【配置举例】

在公网实例中配置与 MSDP 对等体 10.1.100.1 建立 TCP 连接时进行 MD5 认证，并以明文方式设置密钥为 850$aabbcc。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 10.1.100.1 password simple 850$aabbcc
```

4.11 MPLS安全

4.11.1 LDP

【安全威胁】

LDP 消息中的内容容易被窃取和篡改。当设备收到攻击者伪造的 LDP 报文时，会与之建立 TCP 连接，从而被攻击者捕获设备信息，造成设备重要信息泄露。

【安全加固策略】

为了提高 LDP 会话的安全性，可以配置在 LDP 会话使用的 TCP 连接上采用 MD5 认证，来验证 LDP 消息的完整性，防止网络攻击和恶意探测。

【配置举例】

配置公网 LDP 的 MD5 认证功能：与对等体 3.3.3.3 建立的 LDP 会话上采用 MD5 认证，以明文方式设置密钥，密钥值为 pass。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-ldp] md5-authentication 3.3.3.3 plain pass
```

4.11.2 RSVP

【安全加固策略】

为了防止伪造的资源预留请求非法占用网络资源，RSVP 采用逐跳认证机制来验证 RSVP 消息的合法性。一条链路两端的设备上需要配置相同的认证密钥，只有这样，设备之间才可以正确地交互 RSVP 消息。

【注意事项】

RSVP 认证功能可以在如下视图配置：

- RSVP 视图：该视图下的配置对所有 RSVP SA 生效。
- RSVP 邻居视图：该视图下的配置只对与指定 RSVP 邻居之间的 RSVP SA 生效。
- 接口视图：该视图下的配置只对根据指定接口下的配置生成的 RSVP SA 生效。

三个视图下配置的优先级从高到低依次为：RSVP 邻居视图、接口视图、RSVP 视图。

【配置举例】

在 RSVP 视图下全局开启 RSVP 认证功能，并指定认证密钥为明文@aa2019（@aa2019 仅为示例）。

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] authentication key plain @aa2019
```

在 RSVP 邻居视图下开启本地设备与邻居 1.1.1.9 之间的认证功能，并指定认证密钥为明文@aa2019（@aa2019 仅为示例）。

```
<Sysname> system-view
[Sysname] rsvp
[Sysname-rsvp] peer 1.1.1.9
[Sysname-rsvp-peer-1.1.1.9] authentication key plain @aa2019
```

在接口 Vlan-interface100 上开启 RSVP 认证功能，并配置认证密钥为明文@aa2019（@aa2019 仅为示例）。

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-GigabitEthernet1/0/1] rsvp authentication key plain @aa2019
```

4.12 控制平面限速及丢包告警

4.12.1 协议报文限速

【安全威胁】

设备上的控制平面是指运行大部分路由交换协议进程的处理单元，它的主要工作是进行协议报文的解析和协议的运行。与之相对应的核心物理实体是 CPU，它具备灵活的报文处理能力，但数据吞吐能力有限。如果大量协议报文同时上送 CPU，会使 CPU 一直忙于处理协议报文而无法顾及其它任务，最终导致过载甚至设备瘫痪。

【安全加固策略】

可以通过 QoS 策略实现协议报文限速：在流分类中配置匹配指定协议报文的规则，在流行为中配置限速动作，最后将 QoS 策略应用在控制平面上，达到对上送 CPU 的协议报文速率进行限制的目的，保证 CPU 的正常运转。

【配置举例】

定义流分类 c，配置匹配控制平面 DHCP 协议报文的规则（DHCP 仅为示例）。

```
<Sysname> system-view
[Sysname] traffic classifier c
[Sysname-classifier-c] if-match control-plane protocol dhcp
[Sysname-classifier-c] quit
```

定义流行为 b，动作为报文限速，速率为 500 个报文每秒（500 仅为示例）。

```
[Sysname] traffic behavior b
[Sysname-behavior-b] packet-rate 500
[Sysname-behavior-b] quit
```

定义策略 p，并为流分类 c 指定流行为 b。

```
[Sysname] qos policy p
[Sysname-qospolicy-p] classifier c behavior b
[Sysname-qospolicy-p] quit
```

将策略 p 应用到指定 slot 的控制平面。

```
[Sysname] control-plane slot 1
[Sysname-cp-slot1] qos apply policy p inbound
```

4.12.2 控制平面协议丢包告警日志

【安全威胁】

设备上的控制平面是指运行大部分路由交换协议进程的处理单元，它的主要工作是进行协议报文的解析和协议的运行。与之相对应的核心物理实体是 CPU，它具备灵活的报文处理能力，但数据吞吐能力有限。如果同一时刻上送控制平面的报文过多，则有可能在上送过程中被控制平面限速策略丢弃。丢包将严重影响协议的正常运行，所以需及时记录并以合适的方式发出警示。

【安全加固策略】

用户可以通过开启控制平面协议丢包告警日志信息记录功能，使得设备周期性将丢包信息以日志的方式发送到信息中心，并通过设置信息中心的参数，决定日志信息的输出规则（即是否允许输出以及输出方向）。

【配置举例】

开启所有控制平面协议丢包告警日志功能（all 仅为示例）。

```
<Sysname> system-view
[Sysname] qos control-plane logging protocol all enable
```

配置控制平面协议丢包告警日志信息的生成与发送周期为 60 秒（60 仅为示例）。

```
[Sysname] qos control-plane logging interval 60
```

4.13 WLAN管理与接入安全（仅支持融合AC产品适用）

4.13.1 CAPWAP 隧道加密

【安全威胁】

CAPWAP 隧道中传输报文，可能会被外部网络恶意攻击、截获报文，然后对报文内容进行更改或者伪造报文，攻击网络环境中的 AC 等设备。

【安全加固策略】

CAPWAP 隧道加密功能使用 DTLS（Datagram Transport Layer Security，数据包传输层安全性协议）协议对 CAPWAP 控制隧道和数据隧道中交互的隧道报文进行加密处理，从而保障了 CAPWAP 隧道报文的安全性。

开启 CAPWAP 隧道加密功能后：

- AC 回复 AP 的 Discovery Response 报文中将携带加密标志位，AP 接收到 Discovery Response 报文后将与该 AC 进行 DTLS 握手，然后完成 CAPWAP 隧道的建立。在 AP 与 AC 完成 DTLS 握手后交互的 CAPWAP 控制隧道报文将被加密传输。
- AP 在收到 AC 回复的第一个数据隧道保活报文（keepalive 报文）后，将与 AC 通过控制隧道交换包括密钥在内的加密信息，交换完成后再对 CAPWAP 数据隧道报文进行加密传输（不加密 Keepalive 报文）。

【配置举例】

在 AP1 上开启 AP 的 CAPWAP 控制隧道加密功能。

```
<Sysname> system-view
[Sysname] wlan ap ap1 model WA4320i-ACN
[Sysname-wlan-ap-ap1] tunnel encryption enable
This operation will restart the AP. Continue? [Y/N]
```

在 AP1 上开启 AP 的 CAPWAP 数据隧道加密功能。

```
<Sysname> system-view
[Sysname-wlan-ap-ap1] data-tunnel encryption enable
This operation will restart the AP. Continue? [Y/N]
```

4.13.2 WLAN 客户端接入控制功能

【安全威胁】

在实际 WLAN 网络应用中，若非法客户端接入无线服务，会泄露无线用户的个人信息并向设备发起一系列安全攻击，比如对 AP 发起泛洪报文攻击，使 AP 不能正常工作，对无线网络的安全造成威胁。

【安全加固策略】

通过配置客户端接入控制功能，使用黑白名单和 ACL 规则限制接入无线网络的客户端，可以过滤非法客户端，确保无线网络的安全。

【注意事项】

当配置了客户端二次接入认证的时间间隔或者 AP 收到客户端的攻击报文时，AC 才会将该客户端的 MAC 地址添加到动态黑名单中：

- 配置动态黑名单基于 AP 生效，AP 将拒绝该客户端的接入，但仍可以从 AC 下的其他 AP 接入。
- 配置动态黑名单基于 AC 生效，AC 下相连的所有 AP 都将拒绝该客户端接入。

动态黑名单表项具有一定的老化时间。当到达老化时间时，AC 会将 MAC 地址从动态黑名单中删除。

在 AP 部署较密集的无线网络环境下，建议用户配置动态黑名单基于 AC 生效。

新配置的动态黑名单老化时间只对新加入动态黑名单的客户端生效。

若客户端同时存在于白名单和动态黑名单中时，则白名单生效。

【配置举例】

- 配置使用黑白名单限制接入 WLAN 网络的客户端

  # 配置允许接入 WLAN 网络的白名单表项为 001c-f0bf-9c92（001c-f0bf-9c92 仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] wlan whitelist mac-address 001c-f0bf-9c92
  ```

  # 配置禁止接入 WLAN 网络的静态黑名单表项为 001c-f0bf-9c92（001c-f0bf-9c92 仅为示例）。

  ```
  <Sysname> system-view
  [Sysname] wlan static-blacklist mac-address 001c-f0bf-9c92
  ```

  # 配置动态黑名单基于 AC 生效。（仅以基于 AC 生效为例）

  ```
  <Sysname> system-view
  [Sysname] undo wlan dynamic-blacklist active-on-ap
  ```

  # 配置客户端二次接入认证的时间间隔为 100 秒。

  ```
  [Sysname] wlan client reauthentication-period 100
  ```

  # 配置动态黑名单表项的老化时间为 3600 秒（3600 仅为示例）。

  ```
  [Sysname] wlan dynamic-blacklist lifetime 3600
  ```

- 配置使用 ACL 规则限制接入 WLAN 网络的客户端

  # 配置 ACL 4000（仅以基于接入的 ACL 规则为例）（各参数仅为示例）。

  ```
  <Sysname> system-view
  [Syname] acl mac 4000
  [Syname-acl-mac-4000] rule 0 permit source-mac 001e-35b2-000e ffff-ffff-ffff
  [Syname-acl-mac-4000] rule 1 permit source-mac 000e-35b2-000f ffff-ff00-0000
  [Syname-acl-mac-4000] rule 2 deny
  [Syname-acl-mac-4000] quit
  ```

在 AP 下，配置基于 ACL 的接入控制为 4000，仅允许 MAC 地址为 001e-35b2-000e 以及匹配 OUI（Organizationally unique identifier，组织唯一标识符）值为 000e-35 的无线客户端接入（各参数仅为示例）。

```
[Sysname] wlan ap ap1 model WA4320i-ACN
[Sysname-wlan-ap-ap1] access-control acl 4000
```

4.13.3 WLAN 用户接入认证

WLAN 用户接入认证是一种基于用户的安全接入管理机制，根据用户 MAC 地址来进行访问控制。如果不对接入 WLAN 网络的用户进行身份认证，则任何用户都可以随意接入，会对无线网络安全造成严重威胁。

WLAN 用户接入认证主要包括 802.1X、MAC 地址认证和 OUI 认证三种认证方式：

- 802.1X 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议）来实现客户端、设备端和认证服务器之间认证信息的交换。
- MAC 地址认证不需要用户安装任何客户端软件。设备在检测到用户的 MAC 地址以后，对该用户进行认证操作。认证过程中，不需要用户手动输入用户名或者密码，若该用户认证成功，则允许其访问网络资源，否则该用户则无法访问网络资源。
- OUI（Organizationally Unique Identifier，全球统一标识符）是 MAC 地址的前 24 位（二进制），是 IEEE 为不同设备供应商分配的一个全球唯一的标识符。采用 OUI 认证方式后，如果用户的 MAC 地址与设备配置的 OUI 能匹配上，则认证成功，否则认证失败。

WLAN 用户接入认证支持以下几种认证模式：

表4-3 WLAN 用户接入认证模式描述表

认证模式		工作机制	入侵检测
缺省情况	bypass	不对用户进行认证	无效
采用802.1X认证	dot1x	只进行802.1X认证	可触发
采用MAC地址认证	mac	只进行MAC地址认证	可触发
采用802.1X和MAC地址认证组合认证	mac-then-dot1x	先进行MAC地址认证，如果失败，再进行802.1X认证，如果认证成功，则不进行802.1X认证	可触发
	dot1x-then-mac	先进行802.1X认证，如果失败，再进行MAC地址认证，如果认证成功，则不进行MAC地址认证	
	oui-then-dot1x	先进行OUI认证，如果失败，再进行802.1X认证，如果认证成功，则不进行802.1X认证	

关于 WLAN 用户接入认证的详细介绍，请参见“UNIS 融合 AC 用户手册”中“UNIS 融合 AC 配置指导”部分的“WLAN 用户接入认证”。

4.13.4 WLAN 用户安全

如果无线网络未采取任何安全措施，则任何用户都可以接入，既占用大量网络资源，又容易使无线网络遭受攻击和窃听。通过配置 WLAN 用户安全可以对用户进行链路层认证并对数据进行加密保护。

配置 WLAN 用户安全协议后，客户端发现周围的无线网络，需要通过链路层认证、链路服务协商和用户接入认证，才能安全地访问无线网络。WLAN 用户安全协议提供的服务主要包括：

- 链路认证服务
- 数据加密服务
- 用户接入认证服务

WLAN 用户安全协议主要包括 Pre-RSNA、802.11i 和 802.11w。其中，Pre-RSNA 机制最早出现，安全机制不太完善；802.11i 协议是对 Pre-RSNA 的增强，但仅对无线网络的数据报文进行了加密保护；802.11w 建立在 802.11i 框架上，对无线网络的管理帧进行保护，进一步增强了无线网络的安全性。

- Pre-RSNA 安全机制采用开放式系统认证（Open system authentication）和共享密钥认证（Shared key authentication）两种认证模式来进行客户端认证，并且采用 WEP 加密方式对数据进行加密来保护数据机密性，以对抗窃听。
- 802.11i 安全机制又被称为 RSNA（Robust Security Network Association，健壮安全网络连接）安全机制，包括 WPA（Wi-Fi Protected Access，Wi-Fi 保护访问）和 RSN（Robust Security Network，健壮安全网络）两种安全模式：
  - WPA 是一种比 WEP 加密性能更强的安全机制。在 802.11i 协议完善前，采用 WPA 为用户提供一个临时性的 WLAN 安全增强解决方案。
  - RSN 是按照 802.11i 协议为用户提供的一种 WLAN 安全解决方案。
- 保护管理帧功能通过保护无线网络中的管理帧来完善无线网络的安全性。802.11w 保护的管理帧包括解除认证帧，解除关联帧和部分强壮 Action 帧。

关于 WLAN 用户安全的详细信息，请参见“UNIS 融合 AC 用户手册”中“UNIS 融合 AC 配置指导”部分的“WLAN 用户安全”。

4.13.5 WIPS

在 WLAN 组网环境中，非法设备可能存在安全漏洞或被攻击者操纵，对无线网络的安全造成严重危害。WIPS（Wireless Intrusion Prevention System，无线入侵防御系统）是针对 802.11 协议开发的二层协议检测和防护功能。WIPS 通过对信道进行监听及分析处理，从中检测出威胁网络安全、干扰网络服务、影响网络性能的无线行为或设备，并能够对非法设备进行反制使其它无线终端无法与其关联。

关于 WIPS 的详细信息，请参见“UNIS 融合 AC 用户手册”中“UNIS 融合 AC 配置指导”部分的“WIPS”。

4.14 高可靠性协议报文认证

4.14.1 DLDP 报文认证

【安全加固策略】

配置 DLDP 认证模式和密码后，设备将接收的 DLDP 报文的认证信息与本端配置的认证信息进行比较，若一致则认证通过，否则丢弃该报文。DLDP 的认证模式包括：不认证、明文认证和 MD5 认证。

通过配置适当的 DLDP 认证模式和密码，可以防止网络攻击和恶意探测。

【配置举例】

配置 Device A 和 Device B 通过光纤/网线连接的接口间的 DLDP 认证模式均为明文认证，认证密码均为 1458abc$3。（各参数仅为示例）

- Device A 上的配置：

```
<DeviceA> system-view
[DeviceA] dldp authentication-mode simple
[DeviceA] dldp authentication-password simple 1458abc$3
```

- Device B 上的配置：

```
<DeviceB> system-view
[DeviceB] dldp authentication-mode simple
[DeviceB] dldp authentication-password simple 1458abc$3
```

4.14.2 VRRP 报文认证

【安全威胁】

非法用户构造 VRRP 通告报文攻击 VRRP 备份组，导致 VRRP 备份组无法正常运行。

【安全加固策略】

VRRP 通过在 VRRP 报文中增加认证字的方式，验证接收到的 VRRP 报文。VRRP 提供了两种认证方式：

- **simple**：简单字符认证。发送 VRRP 报文的路由器将认证字填入到 VRRP 报文中，而收到 VRRP 报文的路由器会将收到的 VRRP 报文中的认证字和本地配置的认证字进行比较。如果认证字相同，则认为接收到的报文是真实、合法的 VRRP 报文；否则认为接收到的报文是一个非法报文。
- **md5**：MD5 认证。发送 VRRP 报文的路由器利用认证字和 MD5 算法对 VRRP 报文进行摘要运算，运算结果保存在 Authentication Header（认证头）中。收到 VRRP 报文的路由器会利用认证字和 MD5 算法进行同样的运算，并将运算结果与认证头的内容进行比较。如果相同，则认为接收到的报文是真实、合法的 VRRP 报文；否则认为接收到的报文是一个非法报文。

【注意事项】

MD5 认证比简单字符认证更安全，但是 MD5 认证需要进行额外的运算，占用的系统资源较多。

一个接口上的不同备份组可以设置不同的认证方式和认证字；加入同一备份组的成员需要设置相同的认证方式和认证字。

使用 VRRPv3 版本的 IPv4 VRRP 不支持认证。使用 VRRPv3 版本时，此配置不会生效。

【配置举例】

设置 VLAN 接口 10 上备份组 1 发送和接收 IPv4 VRRP 报文的认证方式为 simple，认证字为 Sysname。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] interface vlan-interface 10
[Sysname-Vlan-interface10] vrrp vrid 1 authentication-mode simple plain Sysname
```

4.14.3 BFD 控制报文认证

【安全威胁】

本地设备收到伪造的 BFD 报文，例如包含错误状态信息的 BFD 时，BFD 会话状态发生变化，从而引起会话震荡，破坏 BFD 节点间的正常会话。

【安全加固策略】

在建立控制报文方式的 BFD 会话时，设备将认证信息封装到 BFD 控制报文中，在接收 BFD 控制报文时进行认证信息的检查，如果认证信息不匹配，则无法建立 BFD 会话。

【配置举例】

配置接口 Vlan-interface11 对单跳 BFD 控制报文进行简单明文认证，认证字标识符为 1，密钥为&Pk123456。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] interface vlan-interface 11
[Sysname-Vlan-interface11] bfd authentication-mode simple 1 plain &Pk123456
```

配置多跳 BFD 控制报文进行简单明文认证，认证字标识符为 1，密钥为&Pk123456。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] bfd multi-hop authentication-mode simple 1 plain &Pk123456
```

4.15 时间管理协议报文认证

4.15.1 NTP 服务的访问控制权限

【安全威胁】

一个使用 NTP 协议同步时间的网络中，如果没有配置 NTP 验证，非法的时间服务器就可以随意向网络中的设备发送时间同步信息，可能导致设备同步到错误的时间。

【安全加固策略】

可以通过关联 ACL 来限制对端设备对本地设备上 NTP 服务的访问控制权限。

NTP 服务的访问控制权限从高到低依次为 **peer**、**server**、**synchronization**、**query**。

- **peer**：完全访问权限。该权限既允许对端设备向本地设备的时间同步，对本地设备进行控制查询（查询 NTP 的一些状态，比如告警信息、验证状态、时间服务器信息等），同时本地设备也可以向对端设备的时间同步。
- **server**：服务器访问与查询权限。该权限允许对端设备向本地设备的时间同步，对本地设备进行控制查询，但本地设备不会向对端设备的时间同步。
- **synchronization**：仅具有访问服务器的权限。该权限只允许对端设备向本地设备的时间同步，但不能进行控制查询。
- **query**：仅具有控制查询的权限。该权限只允许对端设备对本地设备的 NTP 服务进行控制查询，但是不能向本地设备的时间同步。

以上定义的访问控制权限都可以关联 ACL，由 **ntp-service { peer | query | server | synchronization } acl** 命令配置。设备一旦收到 NTP 服务请求时，会先对其执行 ACL 规则匹配再为其分配 ACL 关联的访问控制权限。具体匹配规则如下：

当设备接收到 NTP 服务请求时，会按照权限从高到低的顺序依次进行匹配。匹配原则为：

- 如果没有指定权限应用的 ACL 或权限应用的 ACL 尚未创建，则继续匹配下一个权限。

- 如果所有的权限都没有应用 ACL 或权限应用的 ACL 尚未创建，则所有对端设备对本地设备 NTP 服务的访问控制权限均为 **peer**。
- 如果存在应用了 ACL 的权限，且该 ACL 已经创建，则只有 NTP 服务请求匹配了某个权限应用的 ACL 中的 **permit** 规则，发送该 NTP 服务请求的对端设备才会具有该访问控制权限。其他情况下（NTP 服务请求匹配某个权限应用的 ACL 中的 **deny** 规则或没有匹配任何权限的任何规则），发送该 NTP 服务请求的对端设备不具有任何权限。

配置 NTP 服务的访问控制权限，仅提供了一种最小限度的安全措施，更安全的方法是使用 NTP 验证功能。

【配置举例】

创建并配置与访问权限关联的 ACL。

具体配置请参见“ACL 和 QoS 配置指导”中的“ACL”

配置对端设备对本地设备 NTP 服务的访问控制权限（2001 仅为示例）。

```
<Sysname> system-view
[Sysname] ntp-service peer acl 2001
```

4.15.2 NTP 报文认证

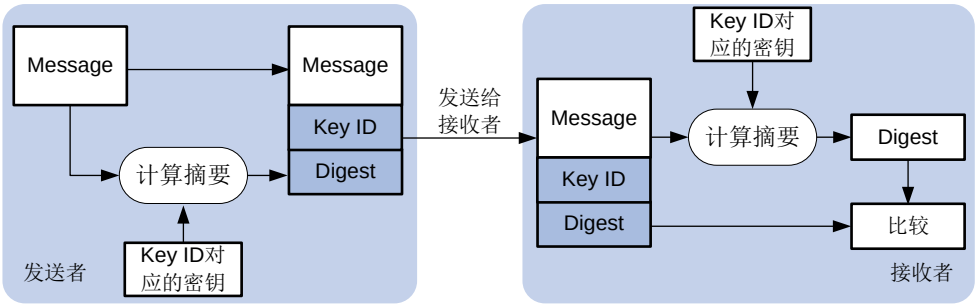
【安全威胁】

网络上大多数信息都需要记录时间，如果设备从非法的时间服务器上获取了时间信息，则会导致设备同步到错误的时间。

【安全加固策略】

NTP 通过验证功能来对接收到的 NTP 报文进行合法性验证。只有报文通过验证后，设备才会接收该报文，并从中获取时间同步信息；否则，设备会丢弃该报文。从而，保证设备不会与非法的时间服务器进行时间同步，避免时间同步错误。

图4-1 NTP 验证功能示意图



如图 4-1 所示，NTP 验证功能的工作过程为：

(2) NTP 报文发送者利用密钥 ID 标识的密钥对 NTP 报文进行加密运算，并将计算出来的摘要信息连同 NTP 报文和密钥 ID 一起发送给接收者。

(3) 接收者接收到该 NTP 报文后，根据报文中的密钥 ID 找到对应的密钥，并利用该密钥对报文进行相同的加密运算。接收者将运算结果与报文中的摘要信息比较，依据比较结果，有以下两种情况：

- 比较结果不相同，则丢弃该报文。

比较结果相同，则检查 NTP 报文发送者是否有权在本端使用该密钥 ID，检查通过，则接收该报文；否则，丢弃该报文。

【注意事项】

客户端和服务器、主动对等体和被动对等体、广播客户端和广播服务器、组播客户端和组播服务器上进行不同的配置时，NTP 验证结果有所不同，详细介绍请参见表 4-4、表 4-5、表 4-6、表 4-7。其中，表格中的“-”表示不管此项是否配置。

表4-4 客户端和服务器上进行不同配置时的 NTP 验证结果

客户端			服务器		结果
身份验证	关联密钥	关联密钥存在且为可信密钥	身份验证	关联密钥存在且为可信密钥	
是	是	是	是	是	身份验证成功
是	是	是	是	否	身份验证失败
是	是	是	否	-	身份验证失败
是	是	否	-	-	身份验证失败
是	否	-	-	-	不进行身份验证
否	-	-	-	-	不进行身份验证

表4-5 主动对等体和被动对等体上进行不同配置时的 NTP 验证结果

主动对等体				被动对等体		结果
身份验证	关联密钥	关联密钥存在且为可信密钥	时钟层数	身份验证	关联密钥存在且为可信密钥	
是	是	是	-	是	是	身份验证成功
是	是	是	-	是	否	身份验证失败
是	是	是	-	否	-	身份验证失败
是	否	-	-	是	-	身份验证失败
是	否	-	-	否	-	不进行身份验证
否	-	-	-	是	-	身份验证失败
否	-	-	-	否	-	不进行身份验证
是	是	否	大于被动对等体	-	-	身份验证失败
是	是	否	小于被动对等体	是	-	身份验证失败
是	是	否	小于被动对等体	否	-	不进行身份验证

表4-6 广播客户端和广播服务器上进行不同配置时的 NTP 验证结果

广播服务器			广播客户端		结果
身份验证	关联密钥	关联密钥存在且为可信密钥	身份验证	关联密钥存在且为可信密钥	
是	是	是	是	是	身份验证成功
是	是	是	是	否	身份验证失败
是	是	是	否	-	身份验证失败
是	是	否	是	-	身份验证失败
是	是	否	否	-	不进行身份验证
是	否	-	是	-	身份验证失败
是	否	-	否	-	不进行身份验证
否	-	-	是	-	身份验证失败
否	-	-	否	-	不进行身份验证

表4-7 组播客户端和组播服务器上进行不同配置时的 NTP 验证结果

组播服务器			组播客户端		结果
身份验证	关联密钥	关联密钥存在且为可信密钥	身份验证	关联密钥存在且为可信密钥	
是	是	是	是	是	身份验证成功
是	是	是	是	否	身份验证失败
是	是	是	否	-	身份验证失败
是	是	否	是	-	身份验证失败
是	是	否	否	-	不进行身份验证
是	否	-	是	-	身份验证失败
是	否	-	否	-	不进行身份验证
否	-	-	是	-	身份验证失败
否	-	-	否	-	不进行身份验证

【配置举例】

- 配置客户端/服务器模式的 NTP 验证功能。

  # 开启客户端的 NTP 验证功能。

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

  # 在 NTP 客户端创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

  ```
  [DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
  ```

在 NTP 客户端配置编号为 42 的密钥为可信密钥（42 仅为示例）。

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

在 NTP 客户端指定与编号 42 密钥关联的 NTP 服务器。

```
[DeviceA] ntp-service unicast-server 1.1.1.1 authentication-keyid 42
```

开启服务器端的 NTP 验证功能。

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

在 NTP 服务器端创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

在 NTP 服务器端配置编号为 42 的密钥为可信密钥（42 仅为示例）。

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

- 配置对等体模式的 NTP 验证功能。

  # 开启主动对等体的 NTP 验证功能。

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

  # 在 NTP 主动对等体创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

  ```
  [DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
  ```

  # 在 NTP 主动对等体配置编号为 42 的密钥为可信密钥（42 仅为示例）。

  ```
  [DeviceA] ntp-service reliable authentication-keyid 42
  ```

  # 在 NTP 主动对等体指定与编号 42 密钥关联的 NTP 被动对等体。

  ```
  [DeviceA] ntp-service unicast-peer 1.1.1.1 authentication-keyid 42
  ```

  # 开启被动对等体的 NTP 验证功能。

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

  # 在 NTP 被动对等体创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

  ```
  [DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
  ```

  # 在 NTP 被动对等体配置编号为 42 的密钥为可信密钥（42 仅为示例）。

  ```
  [DeviceB] ntp-service reliable authentication-keyid 42
  ```

- 配置广播模式的 NTP 验证功能。

  # 开启广播客户端的 NTP 验证功能。

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

  # 在 NTP 广播客户端创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

  ```
  [DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
  ```

  # 在 NTP 广播客户端配置编号为 42 的密钥为可信密钥（42 仅为示例）。

  ```
  [DeviceA] ntp-service reliable authentication-keyid 42
  ```

  # 开启广播服务器端的 NTP 验证功能。

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

在 NTP 广播服务器端创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

在 NTP 广播服务器端配置编号为 42 的密钥为可信密钥（42 仅为示例）。

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

将 NTP 广播服务器与编号 42 密钥关联。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ntp-service broadcast-server authentication-keyid 42
```

- 配置组播模式的 NTP 验证功能。

  # 开启组播客户端的 NTP 验证功能。

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

  # 在 NTP 组播客户端创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

  ```
  [DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
  ```

  # 在 NTP 组播客户端配置编号为 42 的密钥为可信密钥（42 仅为示例）。

  ```
  [DeviceA] ntp-service reliable authentication-keyid 42
  ```

  # 开启组播服务器端的 NTP 验证功能。

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

  # 在 NTP 组播服务器端创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

  ```
  [DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
  ```

  # 在 NTP 组播服务器端配置编号为 42 的密钥为可信密钥（42 仅为示例）。

  ```
  [DeviceB] ntp-service reliable authentication-keyid 42
  ```

  # 将 NTP 组播服务器与编号 42 密钥关联。

  ```
  [DeviceB] interface vlan-interface 1
  [DeviceB-Vlan-interface1] ntp-service multicast-server 224.0.1.1 authentication-keyid
  42
  ```

4.15.3 SNTP 报文认证

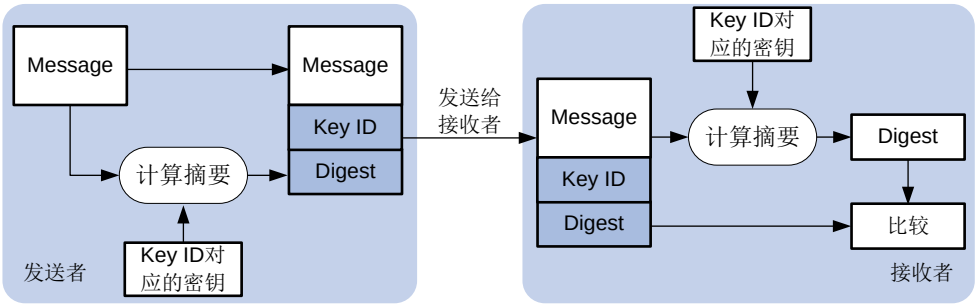
【安全威胁】

网络上大多数信息都需要记录时间，如果设备从非法的时间服务器上获取了时间信息，则会导致设备同步到错误的时间。

【安全加固策略】

SNTP 通过验证功能来对接收到的 SNTP 报文进行合法性验证。只有报文通过验证后，设备才会接收该报文，并从中获取时间同步信息；否则，设备会丢弃该报文。从而，保证设备不会与非法的时间服务器进行时间同步，避免时间同步错误。

图4-2 SNTP 验证功能示意图



如图 4-1 所示，SNTP 验证功能的工作过程为：

(2) SNTP 报文发送者利用密钥 ID 标识的密钥对 SNTP 报文进行加密运算，并将计算出来的摘要信息连同 SNTP 报文和密钥 ID 一起发送给接收者。

(3) 接收者接收到该 SNTP 报文后，根据报文中的密钥 ID 找到对应的密钥，并利用该密钥对报文进行相同的加密运算。接收者将运算结果与报文中的摘要信息比较，依据比较结果，有以下两种情况：

- 比较结果不相同，则丢弃该报文。

比较结果相同，则检查 SNTP 报文发送者是否有权在本端使用该密钥 ID，检查通过，则接收该报文；否则，丢弃该报文。

【注意事项】

客户端需要将指定密钥与对应的 NTP 服务器关联，并保证服务端有权在本端使用该密钥 ID 进行验证。

如果客户端没有成功启用 SNTP 验证功能，不论服务器端是否开启验证功能，客户端均可以与服务器端同步。

【配置举例】

- 配置客户端。

  # 开启 SNTP 客户端的身份验证功能。

  ```
  <DeviceA> system-view
  [DeviceA] sntp authentication enable
  ```

  # 在 SNTP 客户端创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

  ```
  [DeviceA] sntp authentication-keyid 42 authentication-mode md5 simple aNiceKey
  ```

  # 在 SNTP 客户端配置编号为 42 的密钥为可信密钥（42 仅为示例）。

  ```
  [DeviceA] sntp reliable authentication-keyid 42
  ```

  # 在 SNTP 客户端指定与编号 42 密钥关联的 NTP 服务器。

  ```
  [DeviceA] sntp unicast-server 1.1.1.1 authentication-keyid 42
  ```

- 配置服务器端。

  # 开启服务器端的 NTP 验证功能。

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

在 NTP 服务器端创建编号为 42 的 NTP 验证密钥，密钥值为 aNiceKey，以明文形式输入。（各参数仅为示例）

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 simple aNiceKey
```

在 NTP 服务器端配置编号为 42 的密钥为可信密钥（42 仅为示例）。

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

5 转发平面安全加固

5.1 安全隔离

5.1.1 端口隔离

接入同一个设备不同接口的多台主机中，若某台主机存在安全隐患，受到攻击后向同一 VLAN 内的其他主机发送大量单播、组播或广播报文，甚至传播病毒，会影响其他主机、占用网络带宽。通过端口隔离功能，将需要隔离的端口加入到同一个隔离组中，实现隔离组中端口之间的二层隔离，尽可能的将受到攻击时波及的范围控制在一个端口内，提高了网络的安全性。

关于端口隔离的详细信息，请参见“二层技术-以太网交换”中的“端口隔离”。

5.1.2 用户隔离（仅支持融合 AC 产品适用）

对使用同一无线服务或在同一 VLAN 进行通信的用户报文进行隔离，可达到提高用户安全性、缓解设备转发压力和减少射频资源消耗的目的。

用户隔离包括基于 SSID 的用户隔离和基于 VLAN 的用户隔离：

- 基于 SSID 的用户隔离：用于隔离同一 SSID 下的无线用户。
- 基于 VLAN 的用户隔离：用于隔离同一 VLAN 内的有线用户和无线用户。

关于用户隔离的详细信息，请参见“UNIS 融合 AC 用户手册”中“UNIS 融合 AC 配置指导”部分的“用户隔离”。

5.2 广播、组播、未知单播抑制

5.2.1 风暴抑制和流量阈值控制

【安全威胁】

当设备收到广播、组播或未知单播流量时，设备会向同一广播域内的其他接口转发这些报文，这样可能导致广播风暴，降低设备转发性能。

【安全加固策略】

通过部署风暴抑制或者流量阈值控制，对设备收到的广播、组播或未知单播流量进行监测和控制，可以防止产生广播风暴。

部署风暴抑制后，如果收到的广播/组播/未知单播流量超过用户设置的抑制阈值，系统会丢弃超出流量限制的报文，从而限制网络中的泛洪流量，保证网络业务的正常运行。

部署流量阈值控制后，如果收到的广播/组播/未知单播流量超过预先设置的上限阈值，设备根据配置来决定是阻塞该端口还是关闭该端口，以及是否输出 Log 和 Trap 信息。

【注意事项】

对于同一类型（广播、组播或未知单播）的报文流量，请不要同时配置风暴抑制功能和流量阈值控制，以免配置冲突，导致抑制效果不确定。

【配置举例】

在以太网接口 GigabitEthernet1/0/1 上开启广播、组播和未知单播风暴抑制功能，每秒最多允许 10000kbps 广播、组播和未知单播报文通过，对超出该范围的报文进行抑制。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] broadcast-suppression kbps 10000
[Sysname-GigabitEthernet1/0/1] multicast-suppression kbps 10000
[Sysname-GigabitEthernet1/0/1] unicast-suppression kbps 10000
```

在以太网接口 GigabitEthernet1/0/1 上开启广播、组播和未知单播流量阈值控制功能，上限阈值为 2000kbps、下限阈值为 1500kbps。当接口上任一流量超过上限阈值时阻塞该接口。在接口流量从小于等于上限阈值到大于上限阈值或者从超上限回落到小于下限阈值时输出 Log 信息。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] storm-constrain broadcast kbps 2000 1500
[Sysname-GigabitEthernet1/0/1] storm-constrain multicast kbps 2000 1500
[Sysname-GigabitEthernet1/0/1] storm-constrain unicast kbps 2000 1500
[Sysname-GigabitEthernet1/0/1] storm-constrain control block
[Sysname-GigabitEthernet1/0/1] storm-constrain enable log
```

配置名为 vpn1 的 VSI 的广播、组播、未知单播抑制带宽均为 100kbps。（各参数仅为示例）

```
<Sysname> system-view
[Sysname] vsi vpn1
[Sysname-vsi-vpn1] restrain broadcast 100
[Sysname-vsi-vpn1] restrain multicast 100
[Sysname-vsi-vpn1] restrain unknown-unicast 100
```

5.2.2 丢弃未知组播报文

【安全威胁】

未知组播数据报文是指在 IGMP Snooping/MLD Snooping 转发表中不存在对应转发表项的组播数据报文，若未开启丢弃未知组播数据报文功能，二层设备将在未知组播数据报文所属的 VLAN/VSI 内广播该报文。这样可能导致广播风暴，降低设备转发性能。

【安全加固策略】

开启了丢弃未知组播数据报文功能后，二层设备只向其路由器端口转发未知组播数据报文，不在 VLAN 内广播；如果二层设备没有路由器端口，未知组播数据报文报文会被丢弃，不再转发。相对于广播处理，这种方式可以降低瞬时带宽占用率。

【配置举例】

在 VLAN 2 内使能 IGMP Snooping，并开启丢弃未知组播数据报文功能。

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
```

```
[Sysname] vlan 2
[Sysname-vlan2] igmp-snooping enable
[Sysname-vlan2] igmp-snooping drop-unknown
```

在 VLAN 2 内使能 MLD Snooping，并开启丢弃未知 IPv6 组播数据报文功能。

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vlan 2
[Sysname-vlan2] mld-snooping enable
[Sysname-vlan2] mld-snooping drop-unknown
```

在 VSI aaa 内使能 IGMP Snooping，并开启丢弃未知组播数据报文功能。

```
<Sysname> system-view
[Sysname] igmp-snooping
[Sysname-igmp-snooping] quit
[Sysname] vsi aaa
[Sysname-vsi-aaa] igmp-snooping enable
[Sysname-vsi-aaa] igmp-snooping drop-unknown
```

在 VSI aaa 内使能 MLD Snooping，并开启丢弃未知 IPv6 组播数据报文功能。

```
<Sysname> system-view
[Sysname] mld-snooping
[Sysname-mld-snooping] quit
[Sysname] vsi aaa
[Sysname-vsi-aaa] mld-snooping enable
[Sysname-vsi-aaa] mld-snooping drop-unknown
```

5.3 MAC地址安全管理

5.3.1 黑洞 MAC 地址

【安全加固策略】

当出于网络安全的考虑需要禁止某个用户发送和接收报文时，可以将对应的 MAC 地址设置为黑洞 MAC 地址表项，当设备收到的报文源 MAC 地址或目的 MAC 地址与黑洞 MAC 地址表项匹配时，该报文被丢弃。

【配置举例】

将 dc2d-cb01-0101 配置为黑洞 MAC 地址表项（dc2d-cb01-0101 仅为示例）。

```
<Sysname> system-view
[Sysname] mac-address blackhole dc2d-cb01-0101 vlan 2
```

5.3.2 关闭 MAC 地址学习

【安全加固策略】

设备的 MAC 地址学习功能通常处于开启状态。有时为了保证设备的安全，需要关闭 MAC 地址学习功能。例如，非法用户使用大量源 MAC 地址不同的报文攻击设备，导致设备 MAC 地址表资源耗尽，造成设备无法根据网络的变化更新 MAC 地址表。关闭 MAC 地址学习功能可以有效防止这种攻击。

【配置举例】

关闭全局 MAC 地址学习功能。

```
<Sysname> system-view
[Sysname] undo mac-address mac-learning enable
```

关闭 VLAN 10 的 MAC 地址学习功能。

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] undo mac-address mac-learning enable
```

关闭端口 GigabitEthernet1/0/1 的 MAC 地址学习功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo mac-address mac-learning enable
```

关闭名为 vpn1 的 VSI 的 MAC 地址学习功能。

```
<Sysname> system-view
[Sysname] vsi vpn1
[Sysname-vsi-vpn1] undo mac-learning enable
```

5.3.3 控制 MAC 地址学习

【安全加固策略】

当非法用户使用大量源 MAC 地址不同的报文攻击设备时，会导致设备的 MAC 地址表变得庞大，可能引起设备转发性能下降的问题。为了避免网络受到冲击，可以配置 MAC 地址数学习上限功能。当 MAC 地址的学习数量达到上限时，则不再对 MAC 地址进行学习。同时还可以通过配置达到上限后的转发规则来控制是否允许系统转发源 MAC 不在 MAC 地址表中的报文。也可以开启告警功能在 MAC 地址数目达到最大值时、达到最大值后 MAC 地址数降低到最大值的 90%以下时生成日志信息。

【配置举例】

配置端口 GigabitEthernet1/0/1 的 MAC 地址数学习上限为 600，当端口学习的 MAC 地址数达到 600 时，禁止转发源 MAC 地址不在 MAC 地址表里的报文。（600 仅为示例）

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address max-mac-count 600
[Sysname-GigabitEthernet1/0/1] undo mac-address max-mac-count enable-forwarding
```

配置 VLAN 10 的 MAC 地址数学习上限为 600，当 VLAN 10 学习的 MAC 地址数达到 600 时，禁止转发源 MAC 地址不在 MAC 地址表里的报文。（600 仅为示例）

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] mac-address max-mac-count 600
[Sysname-vlan10] undo mac-address max-mac-count enable-forwarding
```

5.3.4 配置接口的 MAC 地址学习优先级

【安全威胁】

基于 MAC 地址转发报文的网络中，有时会因为下行接口的攻击行为或者环路，使得下行接口学习到网关等上层设备的 MAC 地址。例如，非法用户伪装成上层设备的 MAC 地址从下行接口入侵，干扰上层设备与其他设备的正常通信

【安全加固策略】

为了避免这种情况，将接口的 MAC 地址学习功能分为两个优先级：高优先级和低优先级。对于高优先级的接口，可以学习任何 MAC 地址；对于低优先级的接口，在学习 MAC 地址时需要查看高优先级接口是否已经学到该 MAC 地址，如果已经学到，则不允许学习该 MAC 地址。比如，可以将上行接口的MAC地址学习优先级配置为高优先级，下行接口的MAC地址学习优先级配置为低优先级，那么，下行接口就不会学到网关等上层设备的 MAC 地址，避免了攻击。

【配置举例】

配置端口 GigabitEthernet1/0/1 的 MAC 地址学习优先级为高优先级。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address mac-learning priority high
```

5.3.5 MAC 地址迁移上报和抑制功能

【安全威胁】

MAC 地址迁移是指：设备从某接口（假设接口 A）学习到某 MAC 地址，之后从另一接口（假设接口 B）接收到了以该 MAC 地址为源 MAC 地址的报文，且接口 B 与接口 A 所属的 VLAN 相同，则该 MAC 地址表项的出接口改为接口 B，此时认为该 MAC 地址从接口 A 迁移到接口 B。

如果 MAC 地址迁移频繁出现，且同一 MAC 地址总是在特定的两个接口之间迁移，那么网络中可能存在二层环路或存在非法用户将攻击报文的源 MAC 伪装成了合法用户的 MAC 地址。

【安全加固策略】

当监测到某端口频繁迁移时，用户可以通过配置 MAC 地址迁移抑制功能，使频繁迁移的端口 down，一定时间后该端口将自行恢复 up，或者用户通过手动方式将该端口 up。

【配置举例】

开启 MAC 地址迁移上报功能。

```
<Sysname> system-view
[Sysname] mac-address notification mac-move
```

在端口 GigabitEthernet1/0/1 上开启 MAC 地址迁移抑制功能。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] mac-address notification mac-move suppression
```

5.4 数据流保护

5.4.1 MACsec

MACsec 可为用户提供安全的 MAC 层数据发送和接收服务，包括用户数据加密、数据帧完整性检查及数据源真实性校验。

MACsec 通过如下机制来保护数据帧的安全：

- 数据加密

  开启了 MACsec 功能且启动了 MACsec 保护的端口发送数据帧时，需要对它进行加密；开启了 MACsec 功能的端口收到经过 MACsec 封装的数据帧时，需要对它进行解密。加解密所使用的密钥是通过 MKA 协议协商而来的。

- 完整性检查

  MACsec 封装的数据帧会使用 CAK 推导出的密钥进行 ICV（完整性校验值，Integrity Check Value）计算，并附加在 MACsec 报文的尾部。设备收到 MACsec 报文时，同样使用 MKA 协商出的密钥进行完整性检验值计算，然后将计算结果与报文中携带的 ICV 进行比较。如果比较结果相同，则表示报文合法；如果比较结果不相同，将依据配置的校验模式，决定是否丢弃报文。

- 重播保护机制

  MACsec 封装的数据帧在网络中传输时，可能出现报文顺序的重排。MACsec 重播保护机制允许数据帧有一定的乱序，这些乱序的报文序号在用户指定的窗口范围内可以被合法接收，超出窗口的报文会被丢弃。

关于 MACsec 的详细信息，请参见“安全配置指导”中的“MACsec”。

5.4.2 IPsec

IPsec 是一组安全协议集合，能够为承载于 IP 协议上的数据提供包括发送方认证、完整性验证和机密性保证等一整套安全服务，其包括 AH（Authentication Header，认证头）、ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Exchange，互联网密钥交换）和 IKEv2（Internet Key Exchange Version 2，互联网密钥交换第 2 版）等协议。其中，AH 协议和 ESP 协议用于提供安全服务，IKE 协议和 IKEv2 协议用于密钥交换。

关于 IPsec 的详细信息，请参见“安全配置指导”中的“IPsec”。

5.5 报文&流量过滤

5.5.1 ACL

ACL（Access Control List，访问控制列表）是一系列用于识别报文流的规则的集合。ACL 需要与其他功能配合使用，例如报文过滤、QoS 策略和策略路由等。这些功能通过引用 ACL 对收发报文进行精确识别，并对命中 ACL 规则的报文执行预先设定的策略，达到控制网络访问行为和提高网络带宽利用率等目的。

根据规则制订依据的不同，可以将 ACL 分为如表 5-1 所示的几种类型。

表5-1 ACL 的分类

ACL 类型	编号范围	适用的 IP 版本	规则制订依据
基本ACL	2000～2999	IPv4	报文的源IPv4地址
		IPv6	报文的源IPv6地址
高级ACL	3000～3999	IPv4	报文的源IPv4地址、目的IPv4地址、报文优先级、IPv4承载的协议类型及特性等三、四层信息
		IPv6	报文的源IPv6地址、目的IPv6地址、报文优先级、IPv6承载的协议类型及特性等三、四层信息
二层ACL	4000～4999	IPv4和IPv6	报文的源MAC地址、目的MAC地址、802.1p优先级、链路层协议类型等二层信息
用户自定义ACL	5000～5999	IPv4和IPv6	以报文头为基准，指定从报文的第几个字节开始与掩码进行“与”操作，并将提取出的字符串与用户定义的字符串进行

ACL 类型	编号范围	适用的 IP 版本	规则制订依据
			比较，从而找出相匹配的报文

关于 ACL 的详细信息，请参见“ACL 和 QoS 配置指导”中的“ACL”。

5.5.2 流量过滤

【安全威胁】

网络和设备在运行过程中，业务系统可能会因为外部的攻击流量引发系统过载或异常，最终导致业务不可用。通过流量过滤功能可以禁止某些流量特征的报文通过，保护网络和设备的正常运行，保证合法流量的正常转发。

【安全加固策略】

流量过滤功能通过 QoS 策略实现。将配置了流量过滤动作的 QoS 策略应用在指定位置（接口、全局或 VLAN 等），对符合流分类的流执行过滤动作（允许或禁止通过）。例如，可以根据网络的实际情况禁止从某个源 IP 地址发送过来的报文通过。

【配置举例】

定义高级 ACL 3000，匹配源 IP 地址为 10.0.0.2 的数据流。（各参数仅为示例）

```
<Device> system-view
[Device] acl advanced 3000
[Device-acl-ipv4-adv-3000] rule permit ip source 10.0.0.2 0
[Device-acl-ipv4-adv-3000] quit
```

定义类 classifier_1，匹配高级 ACL 3000。

```
[Device] traffic classifier classifier_1
[Device-classifier-classifier_1] if-match acl 3000
[Device-classifier-classifier_1] quit
```

定义流行为 behavior_1，动作为流量过滤（deny），对数据包进行丢弃。

```
[Device] traffic behavior behavior_1
[Device-behavior-behavior_1] filter deny
[Device-behavior-behavior_1] quit
```

定义策略 policy，为类 classifier_1 指定流行为 behavior_1。

```
[Device] qos policy policy
[Device-qospolicy-policy] classifier classifier_1 behavior behavior_1
[Device-qospolicy-policy] quit
```

将策略 policy 应用到端口 GigabitEthernet1/0/1 的入方向上。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] qos apply policy policy inbound
```

5.5.3 IP Source Guard

IP Source Guard 功能用于对接口收到的报文进行过滤控制。IP Source Guard 功能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，限制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），提高接口的安全性。

关于 IP Source Guard 的详细信息，请参见“安全配置指导”中的“IP Source Guard”。

5.5.4 IP Source Guard（仅支持融合 AC 产品适用）

IP Source Guard 功能用于对 AP 收到的上行数据报文进行过滤控制，以防止非法客户端的报文通过，比如非法客户端仿冒合法客户端 IP 接入网络，提高无线网络的安全性。

IP Source Guard 的具体工作机制如下：

(1) 生成绑定表项

- 对于使用 IPv4 地址的客户端，AP 会截获客户端发送的 ARP 报文或者与 DHCP 服务器间交互的 DHCPv4 报文，从报文中获取到客户端的 IP 地址，并与客户端的 MAC 地址形成绑定表项。
- 对于使用 IPv6 地址的客户端，有以下两种方式生成绑定表项。
  - DHCPv6 方式：AP 会截获客户端与 DHCPv6 服务器间交互的 DHCPv6 报文，从报文中获取到 DHCPv6 服务器为客户端分配的完整的 IPv6 地址，并与客户端的 MAC 地址形成绑定表项。
  - ND 方式：AP 监听网络中的 NS 和 NA 报文，从报文中获取 IPv6 地址，并与客户端的 MAC 地址形成绑定表项。

(2) 匹配绑定表项，过滤报文

AP 在收到客户端报文时，查找绑定表项，如果客户端发送报文的特征项（源 MAC 地址+源 IP 地址）与某个绑定表项匹配，则转发该报文，否则做丢弃处理。

对于 IPv4 报文，不仅要地址匹配绑定表项，还要求客户端使用的 IP 地址是通过 DHCP 方式获取的，才转发报文，否则做丢弃处理。

关于 IP Source Guard 的详细信息，请参见“UNIS 融合 AC 用户手册”中“UNIS 融合 AC 配置指导”部分的“IP Source Guard”。

5.5.5 MFF

MFF（MAC-Forced Forwarding，MAC 强制转发）可实现广播域内终端设备间的二层隔离和三层互通而无须划分 VLAN 或为每个 VLAN 规划不同的 IP 网段。MFF 通过 ARP 代答机制，强制终端设备将所有流量（包括同一子网内的流量）发送到网关，使网关可以监控数据流量，防止终端设备之间的恶意攻击。

关于 MFF 的详细信息，请参见“安全配置指导”中的“MFF”。

5.5.6 uRPF

对于使用基于 IP 地址验证用户身份的应用来说，基于源地址欺骗的攻击手段可能导致未被授权用户以他人，甚至是管理员的身份获得访问系统的权限。即使响应报文没有发送给攻击者或其它主机，此攻击方法也可能会造成对被攻击对象的破坏。

攻击者也可能同时伪造不同源地址的攻击报文或者同时攻击多个服务器，造成网络阻塞甚至网络瘫痪。

uRPF 可以有效防范上述攻击。一般情况下，设备在收到报文后会根据报文的目的地址对报文进行转发或丢弃。而 uRPF 可以在转发表中查找报文源地址对应的接口是否与报文的入接口相匹配，如果不匹配则认为源地址是伪装的并丢弃该报文，从而有效地防范网络中基于源地址欺骗的恶意攻击行为的发生。

关于 uRPF 的详细信息，请参见“安全配置指导”中的“uRPF”。

5.5.7 SAVI

SAVI（Source Address Validation Improvement，源地址有效性验证）特性用来在接入设备上以ND Snooping、DHCPv6 Snooping 及 IP Source Guard 中 IPv6 静态绑定表项为依据对源地址为全球单播类型的 IPv6 报文进行检查，避免非法报文通过接入设备进入内部网络。只要报文源地址与某绑定表项匹配，则认为该报文为合法报文，正常转发；否则将该报文丢弃。对于源地址为本地链路地址的 IPv6 报文，设备进行转发时不作 SAVI 检查。

关于 SAVI 的详细信息，请参见“安全配置指导”中的“SAVI”。

5.5.8 Voice VLAN 的安全模式

【安全威胁】

当 Voice VLAN 工作在普通模式下时，当端口加入 Voice VLAN 后，只要接收到携带 Voice VLAN Tag 的报文都会将其在 Voice VLAN 中进行转发，而不再进行源 MAC 地址是否为语音设备 OUI 地址的检查。对于 PVID 就是 Voice VLAN 的手工模式端口，会导致任意的 Untagged 报文都可以在 Voice VLAN 中传输。这样的处理方式很容易使 Voice VLAN 受到恶意用户的流量攻击。恶意用户可以构造大量带有 Voice VLAN Tag 或 Untagged 的报文，占用 Voice VLAN 的带宽，影响正常的语音通信。

【安全加固策略】

对于较不安全的网络，可以将 Voice VLAN 配置为安全模式。安全模式下，设备将对每一个要进入 Voice VLAN 传输的报文进行源 MAC 地址匹配检查，当报文的源 MAC 地址是可识别的 OUI 地址时，允许该报文在 Voice VLAN 内传输，否则将该报文丢弃。从而增加了安全性。

【注意事项】

建议用户尽量不要在 Voice VLAN 中同时传输语音和业务数据。如确有此需要，请确认 Voice VLAN 的安全模式已关闭，否则业务数据会被丢弃。

【配置举例】

开启 Voice VLAN 的安全模式。

```
<Sysname> system-view
[Sysname] voice-vlan security enable
```

5.6 攻击检测与防范

5.6.1 DoS 攻击检测与防范

部署于公网的网关设备，以及位于网关设备下游的主机或服务器容易受到各类单包攻击、扫描攻击和泛洪攻击等 DoS（Denial of Service，拒绝服务）攻击的侵害。受到 DoS 攻击的设备往往无法对正常用户的请求作出响应。

设备支持对如下 DoS 攻击进行有效防范：

- 单包攻击：ICMP redirect、ICMP unreachable、ICMP type、ICMPv6 type、Land、Large ICMP、Large ICMPv6、IP option、IP option abnormal、Fragment、Impossible、Tiny fragment、Smurf、TCP Flag、Traceroute、Winnuke、UDP Bomb、UDP Snork、UDP Fraggle、Teardrop、Ping of death、IPv6 ext-header
- 扫描攻击：IP Sweep、Port scan、分布式 Port scan

- 泛洪攻击：SYN flood、ACK flood、SYN-ACK flood、FIN flood、RST flood、DNS flood、DNS reply flood、HTTP flood、SIP flood、ICMP flood、ICMPv6 flood、UDP flood

关于 DoS 攻击检测与防范的详细信息，请参见“安全配置指导”中的“攻击检测与防范”。

5.6.2 Naptha 攻击防范

Naptha 属于 DDoS（Distributed Denial of Service，分布式拒绝服务）攻击方式，主要利用操作系统 TCP/IP 栈和网络应用程序需要使用一定的资源来控制 TCP 连接的特点，在短时间内不断地建立大量的 TCP 连接，并且使其保持在某个特定的状态（CLOSING、ESTABLISHED、FIN_WAIT_1、FIN_WAIT_2 和 LAST_ACK 五种状态中的一种），而不请求任何数据，那么被攻击设备会因消耗大量的系统资源而陷入瘫痪。

防止 Naptha 攻击功能通过加速 TCP 状态的老化，来降低设备遭受 Naptha 攻击的风险。开启防止 Naptha 攻击功能后，设备周期性地对各状态的 TCP 连接数进行检测。当某状态的最大 TCP 连接数超过指定的最大连接数后，将加速该状态下 TCP 连接的老化。

关于 Naptha 攻击防范的详细信息，请参见“安全配置指导”中的“TCP 攻击防御”。