目 录

1 ND攻击防御 ····· 1-1
1.1 ND攻击防御简介 ····· 1-1
1.2 ND攻击防御配置任务简介 ····· 1-2
1.3 开启ND协议报文源MAC地址一致性检查功能 ····· 1-2
1.4 配置ND Detection功能 ····· 1-2
1.4.1 ND Detection功能简介 ····· 1-2
1.4.2 配置ND Detection功能 ····· 1-3
1.4.3 ND Detection功能显示和维护 ····· 1-4
1.4.4 ND Detection功能典型配置举例 ····· 1-4

1 ND攻击防御

1.1 ND攻击防御简介

IPv6 ND（IPv6 Neighbor Discovery，IPv6 邻居发现）协议使用五种类型的 ICMPv6 消息，实现下面五种功能：地址解析、验证邻居是否可达、重复地址检测、路由器发现/前缀发现及地址自动配置和重定向。

ND 协议使用的五种 ICMPv6 消息如下：

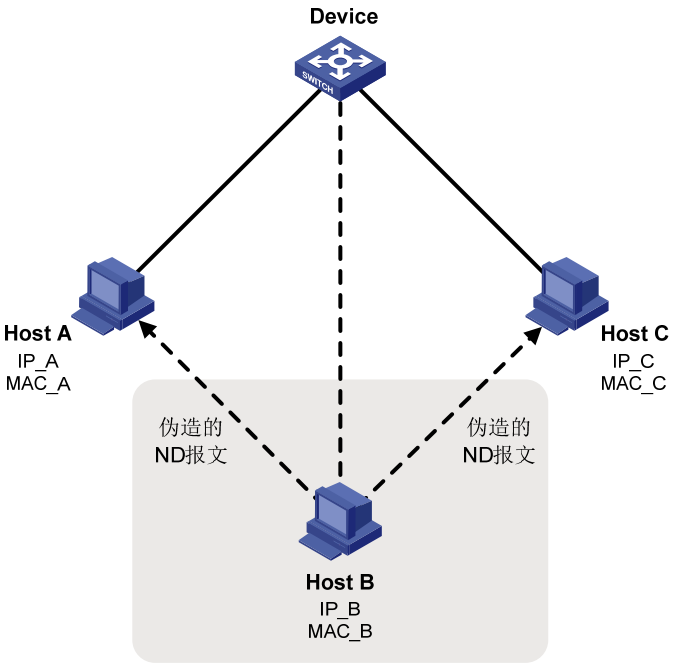
- 邻居请求消息 NS（Neighbor Solicitation）
- 邻居通告消息 NA（Neighbor Advertisement）
- 路由器请求消息 RS（Router Solicitation）
- 路由器通告消息 RA（Router Advertisement）
- 重定向消息 RR（Redirect）

关于 ND 协议五种功能的详细介绍，请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。

ND协议功能强大，但是却没有任何安全机制，容易被攻击者利用。如 图 1-1 所示，当Device作为接入设备时，攻击者Host B可以仿冒其他用户、仿冒网关发送伪造的ND报文，对网络进行攻击：

- 如果攻击者仿冒其他用户的 IPv6 地址发送 NS/NA/RS 报文，将会改写网关或者其他用户的 ND 表项，导致被仿冒用户的报文错误的发送到攻击者的终端上。
- 如果攻击者仿冒网关发送 RA 报文，会导致其他用户的 IPv6 配置参数错误和 ND 表项被改写。

图1-1 ND 攻击示意图



伪造的 ND 报文具有如下特点：

- 伪造的 ND 报文中源 MAC 地址和源链路层选项地址中的 MAC 地址不一致。
- 伪造的 ND 报文中源 IPv6 地址和源 MAC 地址的映射关系不是合法用户真实的映射关系。

根据上述攻击报文的特点，设备开发了多种功能对 ND 攻击进行检测，可以有效地防范 ND 攻击带来的危害。

1.2 ND攻击防御配置任务简介

表1-1 ND 攻击防御配置任务简介

配置任务		说明	详细配置
防止仿冒用户、仿冒网关攻击	开启ND协议报文源MAC地址一致性检查功能	可选 建议在网关设备上开启本功能	1.3
	配置ND Detection功能	可选 建议在接入设备上配置本功能	1.4

1.3 开启ND协议报文源MAC地址一致性检查功能

ND 协议报文源 MAC 地址一致性检查功能主要应用于网关设备上，防御 ND 报文中的源 MAC 地址和以太网数据帧首部中的源 MAC 地址不同的 ND 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，当用户 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，会有相关的日志信息输出。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”。为了防止设备输出过多的 ND 日志信息，一般情况下建议不要开启此功能。

表1-2 开启 ND 协议报文源 MAC 地址一致性检查功能

操作	命令	说明
进入系统视图	**system-view**	-
开启ND协议报文源MAC地址一致性检查功能	**ipv6 nd mac-check enable**	缺省情况下，ND协议报文源MAC地址一致性检查功能处于关闭状态
（可选）开启ND日志信息功能	**ipv6 nd check log enable**	缺省情况下，ND日志信息功能处于关闭状态

1.4 配置ND Detection功能

1.4.1 ND Detection功能简介

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

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

- 对于 ND 信任端口，不进行用户合法性检查；
- 对于 ND 非信任端口，如果收到 RA 和 RR 消息，则认为是非法报文直接丢弃，如果收到其它类型的 ND 报文，则需要进行用户合法性检查，以防止仿冒用户的攻击。

用户合法性检查是根据 ND 报文中源 IPv6 地址和源 MAC 地址，检查用户是否是报文收到端口所属 VLAN 上的合法用户，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。只要能查询到表项，就认为该 ND 报文合法，进行转发。如果没有匹配的表项，则认为是非法报文，直接丢弃。

IPv6 Source Guard 静态绑定表项通过 **ipv6 source binding** 命令生成，详细介绍请参见“安全配置指导”中的“IP Source Guard”。DHCPv6 Snooping 安全表项通过 DHCPv6 Snooping 功能自动生成，详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCPv6 Snooping”。ND Snooping 表项通过 ND Snooping 功能自动生成，详细介绍请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。

1.4.2 配置ND Detection功能

表1-3 配置 ND Detection 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入VLAN视图	**vlan** *vlan-id*	-
开启ND Detection功能	**ipv6 nd detection enable**	缺省情况下，ND Detection功能处于关闭状态。即不进行用户合法性检查
退回系统视图	**quit**	-
进入二层以太网接口视图或二层聚合接口视图	**interface** *interface-type interface-number*	-
（可选）将不需要进行用户合法性检查的端口配置为ND信任端口	**ipv6 nd detection trust**	缺省情况下，端口为ND非信任端口

说明

- 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 非信任端口收到的 ND 报文都将被丢弃。
- 在与 ND Detection 功能配合时，IPv6 Source Guard 绑定表项中必须指定 VLAN 参数，且该 VLAN 为配置 ND Detection 功能的 VLAN，否则 ND 报文将无法通过接口的 IPv6 Source Guard 静态绑定表项的检查。

1.4.3 ND Detection功能显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 ND Detection 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，用户可以执行 **reset** 命令清除 ND Detection 的统计信息。

表1-4 ND Detection 功能显示和维护

操作	命令
显示ND Detection丢弃报文的统计信息	**display ipv6 nd detection statistics** [**interface** *interface-type interface-number*]
清除ND Detection的统计信息	**reset ipv6 nd detection statistics** [**interface** *interface-type interface-number*]

1.4.4 ND Detection功能典型配置举例

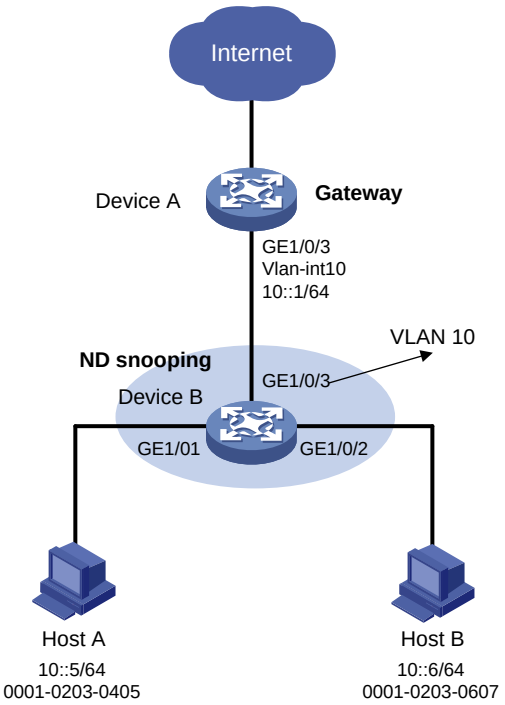
1. 组网需求

用户 Host A 和 Host B 通过 DeviceB 接入网关 Device A。用户 Host A 的 IPv6 地址是 10::5/64，MAC 地址是 0001-0203-0405。用户 Host B 的 IPv6 地址是 10::6/64，MAC 地址是 0001-0203-0607。

要求：在 Device B 上配置 ND Detection 功能对用户的合法性进行检查，保证合法用户的报文可以被正常转发，非法用户的报文被丢弃。

2. 组网图

图1-2 配置 ND Detection 组网图



3. 配置步骤

(1) 配置 Device A

创建 VLAN 10。

```
<DeviceA> system-view
[DeviceA] vlan 10
[DeviceA-vlan10] quit
```

配置端口 GigabitEthernet1/0/3 允许 VLAN 10 的报文通过。

```
[DeviceA] interface gigabitethernet 1/0/3
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 10
[DeviceA-GigabitEthernet1/0/3] quit
```

配置 VLAN 接口 10 的 IPv6 地址。

```
[DeviceA] interface vlan-interface 10
[DeviceA-Vlan-interface10] ipv6 address 10::1/64
[DeviceA-Vlan-interface10] quit
```

(2) 配置 Device B

创建 VLAN 10。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
```

配置端口 GigabitEthernet1/0/1～GigabitEthernet1/0/3 允许 VLAN 10 的报文通过。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type access
[DeviceB-GigabitEthernet1/0/1] port access vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type access
[DeviceB-GigabitEthernet1/0/2] port access vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 10
[DeviceB-GigabitEthernet1/0/3] quit
```

开启 ND Detection 功能。

```
[DeviceB] vlan 10
[DeviceB-vlan10] ipv6 nd detection enable
```

开启 ND Snooping 表项获取功能，通过 ND 报文的源地址（包括全球单播地址和链路本地地址）生成 ND Snooping 表项。

```
[DeviceB-vlan10] ipv6 nd snooping enable global
[DeviceB-vlan10] ipv6 nd snooping enable link-local
[DeviceB-vlan10] quit
```

将上行端口 GigabitEthernet1/0/3 配置为 ND 信任端口，下行端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 采用缺省配置，即为 ND 非信任端口。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] ipv6 nd detection trust
```

4. 验证配置

完成上述配置后，对于端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 收到的 ND 报文，基于 ND Snooping 安全表项进行检查。