NetScreen 概念与范例

ScreenOS 参考指南

第 7 卷 : NSRP

ScreenOS 4.0.0

编号 093-0525-000-SC

版本 F

Copyright Notice

NetScreen Technologies, Inc.
350 Oakmead Parkway
Sunnyvale, CA 94085 U.S.A.
www.netscreen.com

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

目录

前言

“NetScreen 冗余协议 (NSRP)”是一种专有协议，可提供配置、执行对象 (RTO) 冗余和高可用性 (HA) 集群中用于 NetScreen 设备的一种设备故障切换机制。

第 7 卷，“NSRP”提供了 NSRP 操作的概述，并说明了如何连接电缆、配置和管理一个冗余组中的 NetScreen 设备，从而使用 NSRP 提供高可用性。

约定

本书介绍了配置 NetScreen 设备的两种管理方法：Web 用户界面（WebUI）和命令行界面（CLI）。以下介绍这两种界面使用的约定。

WebUI 导航约定

贯穿本书的全部篇章，用一个尖角符号 (>) 来指示在 WebUI 中导航，其方法是单击菜单选项和链接。

范例：Objects > Addresses > List > New

要访问 new address configuration 对话框，请执行以下操作：

1. 在菜单栏中，单击 **Objects**。
   Objects 菜单选项展开，显示出一个 Objects 选项子菜单。
2. （Applet 菜单）将鼠标光标悬停在 **Addresses** 上。
   （DHTML 菜单）单击 **Addresses**。
   Addresses 选项展开，显示出一个 Addresses 选项子菜单。
3. 单击 **List**。
   出现通讯薄表。
4. 单击右上角的 **New** 链接。
   出现 new address configuration 对话框。

CLI 约定

手册中每一条 CLI 命令的说明，都会介绍命令语法的某些方面。此语法可包括选项、开关、参数及其它功能。为了阐明语法规则，一些命令的说明使用*相关性定义符*。这种定义符指出，哪些命令功能是必须遵循的，和适用于哪些环境中。

相关性定义符

每个语法说明中将介绍使用特殊字符来显示命令功能之间的相关性。

- { 和 } 符号表示一个必须遵循的功能。包含在这些符号中的功能，对执行命令非常重要。
- [和] 符号表示一个任选功能。包含在这些符号中的功能，尽管省略它们可能使命令执行后得到相反的结果，但它们对命令执行并不重要。
- | 符号表示两个功能之间的一个“或”关系。当这个符号出现在同一行上的两个功能之间时，可使用两个功能中的任一个（但不能两个都使用）。当这个符号出现在行尾时，可使用该行上的功能，或下一行上的功能。

嵌套的相关性

多数 CLI 命令有*嵌套的*相关性，这使得功能在某些环境中是可以选择的，而在另一些环境中，则是必须遵循的。三个假设的功能显示如下，以对这种原则进行示范。

```
[ feature_1 { feature_2 | feature_3 } ]
```

定义符 [和] 包围整个子句。因此，可省略 **feature_1**、**feature_2** 和 **feature_3**，而且，还能成功地执行这条命令。可是，因为 { 和 } 定义符包围 **feature_2** 和 **feature_3**，所以如果包括了 **feature_1**，则必须包括 **feature_2** 或 **feature_3** 中的任一个。否则，将不能成功执行该命令。

以下例子说明一些 **set interface** 命令功能的相关性。

```
set interface vlan1 broadcast { flood | arp [ trace-route ] }
```

这个 { 和 } 括号说明指定的任一个 **flood** 或 **arp** 是必须遵循的。但是，[和] 括号说明，关于 **arp** 的 **trace-route** 选项不是必须遵循的。因而，这条命令可以采取以下任一种格式：

```
ns-> set interface vlan1 broadcast flood
ns-> set interface vlan1 broadcast arp
ns-> set interface vlan1 broadcast arp trace-route
```

CLI 命令及功能的可用性

用本手册中的语法说明执行 CLI 命令，可能发现某些命令及其功能对于您的 NetScreen 设备型号是无效的。

因为 NetScreen 设备将未提供的命令功能视为语法不当，所以，试图使用这样的功能，通常将产生 **unknown keyword** 错误信息。出现这个信息时，用 **?** 开关确认该功能的 可用性。比如，以下命令列出了 **set vpn** 命令的可用选项：

```
ns-> set vpn ?
ns-> set vpn vpn_name ?
ns-> set vpn gateway gate_name ?
```

NETSCREEN 文档

要获得任何 NetScreen 产品的技术文档，请浏览 www.netscreen.com/support/manuals.html。欲访问最新的 NetScreen 技术文档，请参阅 **Current Manuals** 部分。欲从以前的版本中访问已存档的文档，请参阅 **Archived Manuals** 部分。

欲在 NetScreen 产品版本上获得最新的技术信息，请参阅该版本的发行说明文档。欲获得发行说明，请浏览 www.netscreen.com/support 并选择 **Software Download**。选择产品及其版本，然后单击 **Go**。（欲执行此下载任务，您必须是注册用户。）

如果在以下内容中发现任何错误或遗漏，请用下面的电子邮件地址与我们联系：

techpubs@netscreen.com

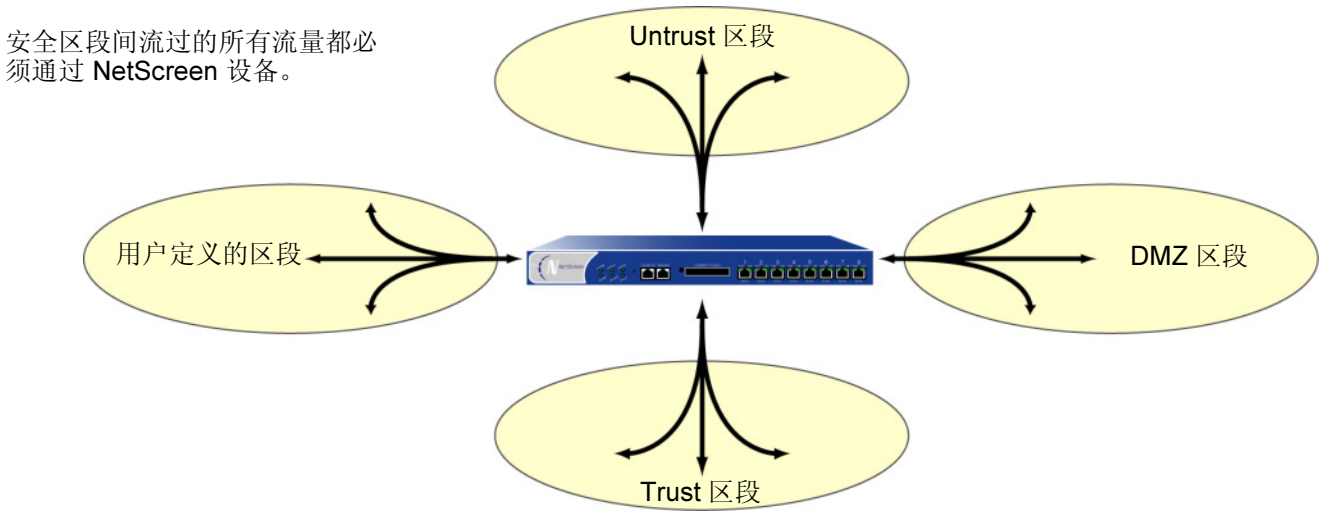
1

NSRP

“NetScreen 冗余协议 (NSRP)”是一种在选定的 NetScreen 设备上支持的、可提供高可用性 (HA) 服务的专有协议。本章解释 NSRP 的组件并描述如何为 HA 使用 NSRP 配置 NetScreen 设备。所涵盖的具体主题如下：

NSRP 概述

要正常起到网络防火墙的作用，必须将 NetScreen 设备放置在所有区段间流量都必须通过的单一点上。

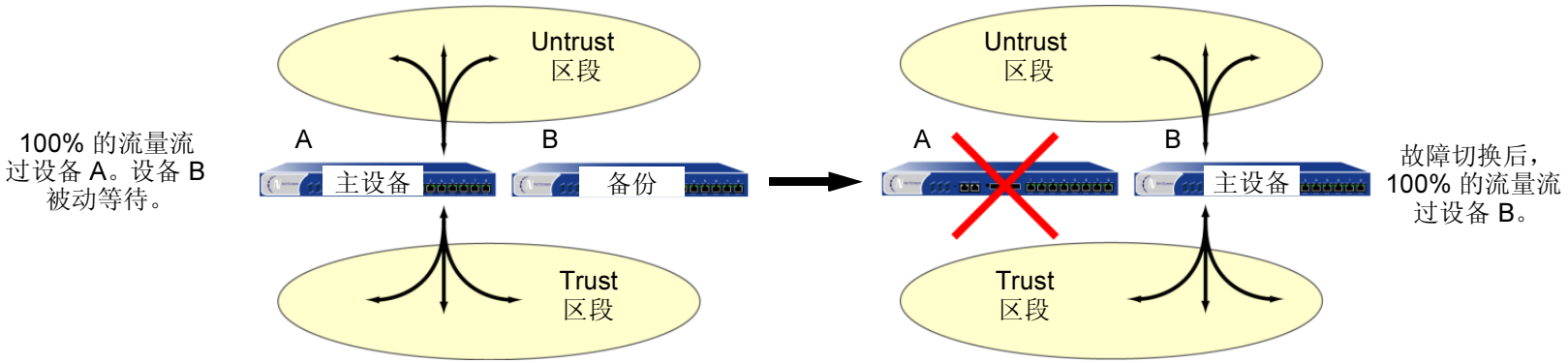


由于 NetScreen 设备是所有区段间流量都必须通过的单一点，因此，保持流量不中断流动至关重要，即使在设备或网络发生故障时也应如此。

要确保流量的连续流动，可以通过冗余集群方式用电缆连接并配置两台 NetScreen 设备，其中一台作为主设备，另一台作为它的备份。主设备将所有的网络和配置设置以及当前会话的信息传播到备份设备。主设备出现故障时，备份设备会晋升为主设备并接管流量处理。

注意：为简化故障切换概念，仅显示 Trust 和 Untrust 区段。

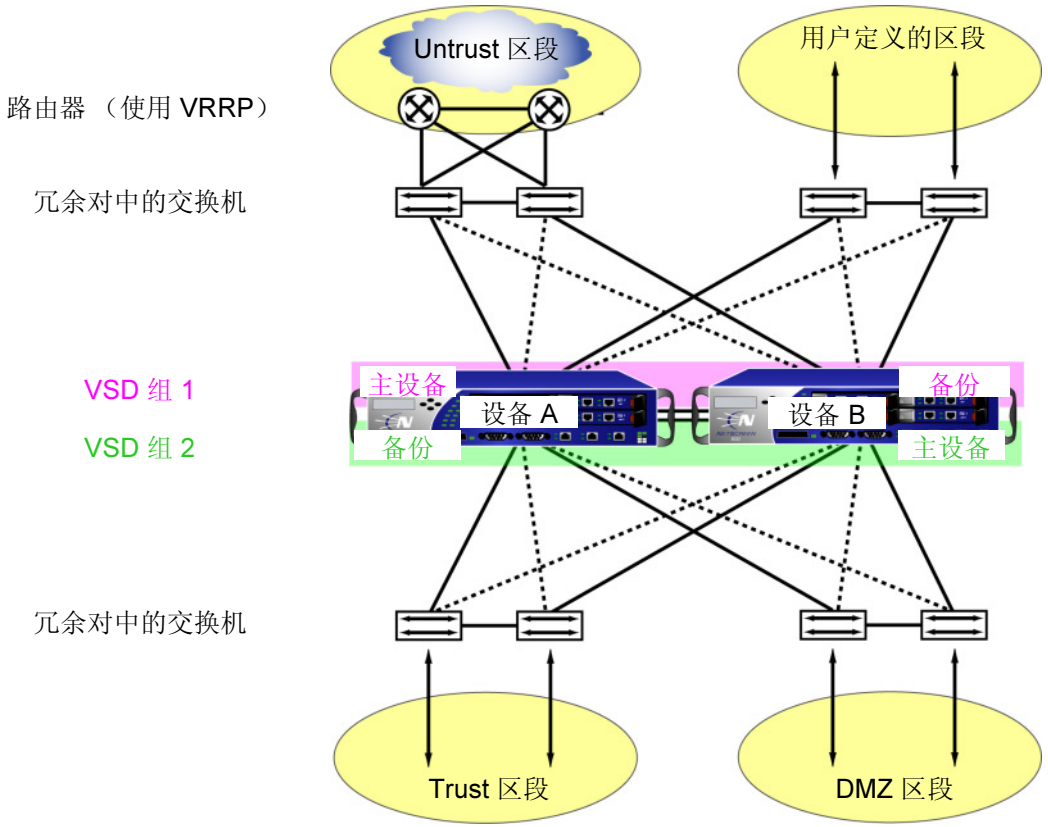
主动 / 被动故障切换



在这种情况下，两种设备处于主动 / 被动配置；即主设备为主动，处理所有防火墙和 VPN 活动，备份设备为被动[1]，等待主设备让位时接管。

1. 尽管备份设备感觉上处于被动，好象没有处理流量，但是它在维持与连续从主设备收到的配置设置和会话信息同步方面相当活跃。

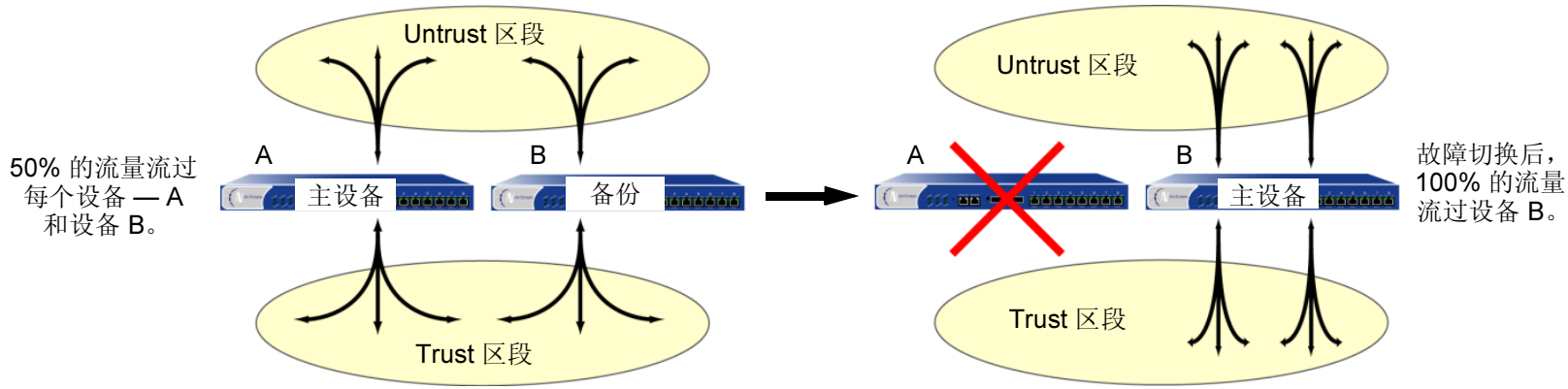
NetScreen 设备处于 “路由” 或 NAT 模式时，可以将冗余集群中的两台设备都配置为主动，通过具有负载均衡能力的路由器，运行诸如 “虚拟路由器冗余协议 (VRRP)” 等协议，共享它们之间分配的流量。通过使用 “NetScreen 冗余协议 (NSRP)” 创建两个虚拟安全设备 (VSD) 组，每个组都具有自己的虚拟安全接口 (VSI)，即可实现此目的。设备 A 充当 VSD 组 1 的主设备，并充当 VSD 组 2 的备份设备。设备 B 充当 VSD 组 2 的主设备，并充当 VSD 组 1 的备份设备。此配置称为双主动 （请参阅下图）。由于设备冗余，因此不存在单一故障点。



设备 A 和设备 B 各接收 50% 的网络和 VPN 流量。设备 A 出现故障时，设备 B 变成 VSD 组 1 的主设备，同时继续作为 VSD 组 2 的主设备，并处理 100% 的流量。在双主动配置中，故障切换产生的流量转移结果如下图所示。

注意：为简化故障切换概念，仅显示 Trust 和 Untrust 区段。

双主动故障切换



尽管处于双主动配置的两台设备分开的会话总数不能超过单个 NetScreen 设备的容量（否则，在出现故障切换时，多余的会话将丢失[2]），但添加的第二台设备使可用的潜在带宽加倍。第二台主动设备也保证两台设备都具有网络连接功能。

除 NSRP 集群（主要负责在组成员间传播配置并通告每个成员的当前 VSD 组状态）外，还可以将设备 A 和设备 B 配置为 RTO 镜像组中的成员，该镜像组负责维持一对设备之间执行对象 (RTO)[3] 的同步性。主设备让位时，通过维持所有当前会话，备份设备可立即用最短的服务停顿时间承担主地位。

2. 双主动配置的每台设备都可在短期内容忍流量激增超过单个设备容量的 50% 的情况；但是，在此阶段出现故障切换时，多余的流量将丢失。
3. RTO 是设备正常操作时在 NetScreen 设备内存中动态创建的对象。RTO 允许设备了解它周围的网络并实施其策略。RTO 的示例有 TCP/UDP 会话、IPSec 阶段 2 安全联盟 (SA)、 DHCP 分配、 RSA 和 DSS 密钥对、 ARP 表和 DNS 高速缓存。

除冗余设备外，还可以在 NetScreen 设备上配置冗余物理接口。如果一级端口失去网络连接，则二级端口承担连接的任务。有关冗余接口的详细信息，请参阅第 37 页上的 “冗余接口”。

在某些 NetScreen 设备中，也存在冗余物理 HA 接口，它不仅处理不同种类的 HA 通信，而且彼此充当备份。缺省情况下， HA1 处理控制消息， HA2 处理数据消息。如果失去任一 HA 链接，则另一链接可承担起两种消息类型。在没有专用 HA 接口的 NetScreen 设备上，必须将一个或两个物理以太网接口绑定到 HA 区段上。（有关详细信息，请参阅第 37 页上的 “双 HA 接口”。）

由于 NSRP 通信的机密特性，可以通过加密和认证保障所有 NSRP 流量的安全。对于加密和认证， NSRP 分别支持 DES 和 MD5 算法。（有关这些算法的详细信息，请参阅第 **4**-7 页上的 “协议”）

注意： *如果将 HA 电缆直接从一台 NetScreen 设备连接到另一台设备 （即不通过一个交换机转发其它种类的网络流量），则不必使用加密和认证。*

如果要用 “简单网络管理协议 (SNMP)” 监控 NetScreen 设备，可从 www.netscreen.com 下载专用的 NSRP MIB。（有关 SNMP 的详细信息，请参阅第 **3**-66 页上的 “SNMP”）

NSRP 由两个基本元素组成，在以下部分中有相关的详细说明：

- 第 15 页上的 “NSRP 集群”
- 第 23 页上的 “VSD 组”

对于基本主动/被动 NSRP 配置的范例，请参阅第 10 页上的 “范例：主动/被动配置的 NSRP”。对于双主动 NSRP 配置的范例，请参阅第 51 页上的 “范例：双主动配置的 NSRP”。

NSRP 和 NETSCREEN 的操作模式

NetScreen 设备接口可按以下三种模式之一运行，分别是：NAT 模式、“路由”模式和“透明”模式。当接口为 NAT 或“路由”模式时， NetScreen 设备在 OSI 模式中的“Layer 3 （第 3 层）”运行。安全区段接口有 IP 地址，并且 NetScreen 设备象“Layer 3 （第 3 层）”路由器那样转发流量。当接口为 “透明”模式时， NetScreen 设备在“Layer 2 （第 2 层）”运行。安全区段接口没有 IP 地址，并且 NetScreen 设备象“Layer 2 （第 2 层）”交换机那样转发流量。

当 NetScreen 设备在“Layer 3（第 3 层）”（NAT 或“路由”模式）中运行时，它可以是双主动或主动 / 被动 NSRP 配置。要管理备份设备，必须使用设置每个安全区段接口的管理 IP 地址[4]。

当 NetScreen 设备在 “Layer 2 （第 2 层）”（“透明”模式）运行时，它只能是主动 / 被动 NSRP 配置。要管理备份设备，请使用在 VLAN1 接口上设置的管理 IP 地址。

基本主动 / 被动 NSRP 配置

执行最基本的主动 / 被动 NSRP 配置十分简单。可以通过使用单个 CLI 命令 **—set nsrp cluster id** *number*— 或在 WebUI 中键入 NSRP 集群 ID 的单一编号，将设备放在 NSRP 集群和 VSD 组中。

可以用 CLI 命令 **set nsrp rto sync all**，启用自动 RTO 同步，或在 WebUI 中，选择 Network > Redundancy > General 页中的 **NSRP RTO Mirror Synchronization** 选项，然后单击 **Apply**。

下一步，必须选择设备要监控的端口，以便在检测到监控的任何一个端口上失去网络连接时，设备进行故障切换。

注意：*在 NSRP 起到作用前，必须首先按第 47 页上的 “全网状配置的电缆连接”中的说明将两台 NetScreen 设备用电缆连接起来。另外，如果要维持 NSRP 集群中 NetScreen 设备的一个或多个物理接口的管理流量的网络连接，在启用 NSRP 前，应首先按第 **3**-39 页上的 “管理 IP”中的说明为这些接口设置管理 IP 地址。*

4. 除 VSD 组 0 以外，不能在 VSI 上为任何 VSD 组设置一个管理 IP 地址。

缺省设置

NSRP 的基本配置使用以下缺省设置：

- VSD 组信息
  - VSD group ID: 0 （VSD 组 ID：0）
  - Device priority in the VSD group: 100 （VSD 组中的设备优先级：100）
  - Preempt option: disabled （抢先选项：禁用）
  - Preempt hold-down time: 0 seconds （抢先抑制时间：0 秒）
  - Initial state hold-down time: 5 seconds （初始状态抑制时间：5 秒）
  - Heartbeat interval: 1000 milliseconds （心跳信号间隔：1000 毫秒）
  - Lost heartbeat threshold: 3 （失去心跳信号临界值：3）
- RTO 镜像信息
  - RTO synchronization: disabled （RTO 同步：禁用）
  - Heartbeat interval: 4 seconds （心跳信号间隔：4 秒）
  - Lost heartbeat threshold: 16 （失去心跳信号临界值：16）
- NSRP 链接信息
  - Number of gratuitous ARPs: 5 （无偿的 ARP 数量：5）
  - NSRP encryption: disabled （NSRP 加密：禁用）
  - NSRP authentication: disabled （NSRP 认证：禁用）
  - Interfaces monitored: none （监控的接口：无）
  - Secondary path: none （二级路径：无）

在 NSRP 集群中设置一个 NetScreen 设备时，NetScreen 设备自动创建 VSD 组 0 并将物理接口转换到用于 VSD 组 0[5] 的 “虚拟安全接口 (VSI)” 中。

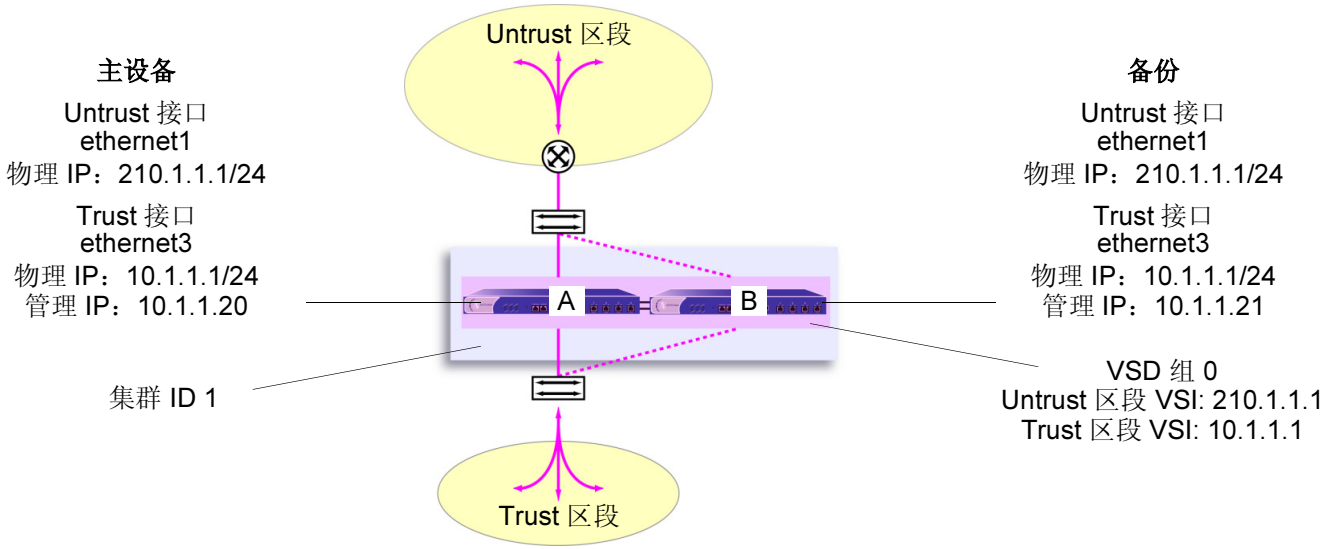
5. 用于指示 VSI 的惯例为 **<interface_name>:<VSD_group_ID>**。例如，以下指示用于 VSD 组 1 的冗余接口 *red1* 为 VSI：**red1:1**。但是，如果 VSD 组 ID 为 0，则不指定 VSD 组 ID。例如，如果用于 VSD 组 0 的冗余接口 *red2* 为 VSI，则它仅显示为 **red2**。

范例：主动 / 被动配置的 NSRP

下例中，首先在每个 NetScreen 设备上设置 Trust 区段接口的管理 IP 地址 - NetScreen-A 为 10.1.1.20，NetScreen-B 为 10.1.1.21。然后将每台设备指派给 NSRP 集群 ID 1。设备成为 NSRP 集群的成员时，它们的物理接口的 IP 地址自动变成用于 VSD 组 ID 0 的“虚拟安全接口 (VSI)”的 IP 地址。每个 VSD 成员的缺省优先级为 100，具有最低 MAC 地址的设备变成 VSD 组的主设备。

配置设备以监控端口 ethernet1 和 ethernet3，以便在任何一个端口失去网络连接时触发设备故障切换。也启用 RTO 的自动同步。

注意：*这是一个非常简单的范例，并且有关 NSRP 配置的基本元素的说明也包含其中。有关生成的完整配置的详细信息，请参阅第 51 页上的“范例：双主动配置的 NSRP”。*



WebUI

NetScreen-A

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：

   Zone Name: Untrust

   IP Address/Netmask: 210.1.1.1/24

2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：

   Zone Name: Trust

   IP Address/Netmask: 10.1.1.1/24

   Manage IP: 10.1.1.20

3. Network > Redundancy > Settings：输入以下内容，然后单击 **Apply**：

   Cluster ID: 1

   > Monitor Port Edit: 选择 **ethernet1** 和 **ethernet3**，然后单击 **Apply**，设置监控的端口并返回到 “General NSRP” 配置页。

   NSRP RTO Mirror Synchronization: （选择）[6]

6. 如果没有启用自动 RTO 同步选项，则可以用 CLI 命令 **exec nsrp sync rto all** 手动同步 RTO。

NetScreen-B

1. Network > Interfaces > Edit（对于 ethernet1）：输入以下内容，然后单击 **OK**：

   Zone Name: Untrust

   IP Address/Netmask: 210.1.1.1/24

2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：

   Zone Name: Trust

   IP Address/Netmask: 10.1.1.1/24

   Manage IP: 10.1.1.21

3. Network > Redundancy > Settings：输入以下内容，然后单击 **Apply**：

   Cluster ID: 1

   > Monitor Port Edit: 选择 **ethernet1** 和 **ethernet3**，然后单击 **Apply**，设置监控的端口并返回到 “General NSRP” 配置页。

   NSRP RTO Mirror Synchronization: （选择）

CLI

NetScreen-A

1. set interface ethernet1 zone untrust
2. set interface ethernet1 ip 210.1.1.1/24
3. set interface ethernet3 zone trust
4. set interface ethernet3 ip 10.1.1.1/24
5. set interface ethernet3 manage-ip 10.1.1.20
6. set nsrp rto-mirror sync[7]
7. set nsrp monitor interface ethernet1
8. set nsrp monitor interface ethernet3
9. set nsrp cluster id 1
10. save

NetScreen-B

1. set interface ethernet1 zone untrust
2. set interface ethernet1 ip 210.1.1.1/24
3. set interface ethernet3 zone trust
4. set interface ethernet3 ip 10.1.1.1/24
5. set interface ethernet3 manage-ip 10.1.1.21
6. set nsrp rto-mirror sync
7. set nsrp monitor interface ethernet1

7. 如果没有启用自动 RTO 同步选项，则可以用 CLI 命令 **exec nsrp sync rto all** 手动同步 RTO。

8. set nsrp monitor interface ethernet3
9. set nsrp cluster id 1
10. save

注意：*执行此配置后，键入* ***get nsrp*** *命令，检查设备自动创建的、并且记录在第 8 页上的缺省 NSRP 设置。*

NSRP 集群

NSRP 集群由一组实施相同的整体安全策略并且共享相同的配置设置的 NetScreen 设备组成。将 NetScreen 设备分配给 NSRP 集群时，对一个集群成员的配置所作的任何更改都将传播给其它成员。同一 NSRP 集群的成员保持如下所述的相同设置：

- 策略和策略对象 （如地址、服务、 VPN、用户和调度）
- 系统参数 （如认证服务器设置、 DNS、 SNMP、系统日志、 URL 阻塞、防火墙检测选项等等）

集群的成员不传播下列配置设置：

不传播的命令	
NSRP	• set/unset nsrp cluster id *number* • set/unset nsrp auth password *pswd_str* • set/unset nsrp encrypt password *pswd_str* • set/unset nsrp monitor interface *interface* • set/unset nsrp vsd-group id *id_num* { mode *string* | preempt | priority *number* } • set/unset nsrp rto-mirror …
接口	• set/unset interface *interface* manage-ip *ip_addr* • set/unset interface *interface* phy … • set/unset interface *interface* bandwidth *number* • set/unset interface redundant *number* phy primary *interface* • 属于本地接口的所有命令
IP 跟踪	• 所有 IP 跟踪命令 (set/unset nsrp track-ip …)
控制台设置	• 所有控制台命令 (set/unset console …)
主机名	• set/unset hostname *name_str*

不传播的命令	
SNMP	• set/unset snmp name *name_str*
虚拟路由器	• set/unset vrouter *name_str* router-id *ip_addr*
清除*	• 所有清除命令 (clear admin, clear dhcp, …)
调试†	• 所有调试命令 (debug alarm, debug arp, …)

* 缺省情况下，NSRP 集群成员不传播 **clear** 命令。要将一个 clear 命令传播到 NSRP 集群中的所有设备，请将关键字 **cluster** 插入命令中。例如，**clear cluster admin …**、 **clear cluster dhcp …**

† 缺省情况下， NSRP 集群成员不传播 **debug** 命令。要将一个 debug 命令传播到 NSRP 集群中的所有设备，请将关键字 **cluster** 插入 **debug** 命令中。例如，**debug cluster alarm …**、 **debug cluster arp …**

在两台 NetScreen 设备能提供冗余网络连接前，必须通过指派介于 1 到 7 之间的集群 ID[8]，将它们分组到同一 NSRP 集群中。当 NetScreen 设备成为集群的一个成员时，它自动成为 VSD 组 0 的一员，并且所有接口变成 VSD 组 0 的 VSI。如果要保留某些接口作为本地接口并从选择接口创建 VSI，则必须执行以下操作：

1. 移除 VSD 组 0。

   所有集群成员上的全部接口都变成本地接口。

2. 创建另一个 VSD 组，如 VSD 组 1。
3. 为该 VSD 组创建 VSI。

有关 VSD 组的详细信息，请参阅第 23 页上的 “VSD 组”。

集群成员也可同步执行对象 (RTO)，它可使新选定的 VSD 组主设备在故障切换后维持不中断的网络和 VPN 服务。（有关 RTO 的详细信息，请参阅第 21 页上的 “执行对象”）

8. 指派 ID 为 0，从集群中移除设备。

集群名称

由于 NSRP 集群成员可以具有不同的主机名称，由此故障切换可破坏 SNMP 通信和数字证书的有效性，原因是 SNMP 通信和证书的正常工作依赖于设备的主机名称。

要为所有集群成员定义单独的名称，请键入以下 CLI 命令：

set nsrp cluster name *name_str*

为 NetScreen 设备配置 SNMP 主机名 (**set snmp name** *name_str*)，以及在 PKCS10 证书请求文件中定义通用名称时使用集群名称。

所有集群成员单独名称的使用，可实现 SNMP 通信和数字证书在设备故障切换后继续使用而不中断。

范例：创建 NSRP 集群

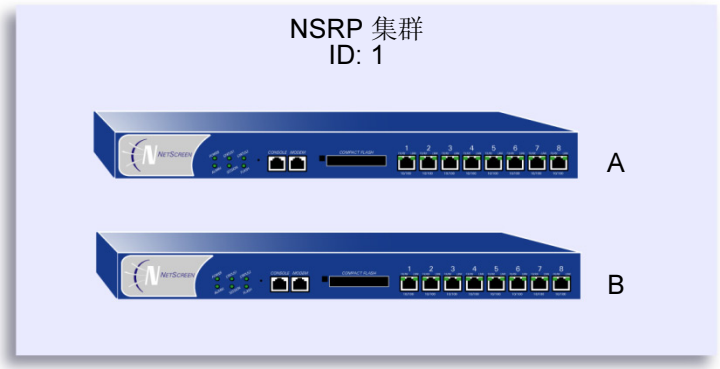
在本例中，将设备 A 和设备 B 分组到 NSRP 集群 ID 1 中，集群名称为“cluster1”。也可在每台设备上指定以下设置：

NSRP 通信安全：指派密码为 725dCaIgDL 和 WiJoaw4177，创建认证和加密密钥以保证 NSRP 通信安全。

将两台设备都分组到相同集群中并给定它们相同的认证和加密密码后，可以在设备 A 或设备 B 上输入下列设置（在集群中一台设备上输入的大部分设置将传播给另一台设备。对于不传播命令的列表，请参阅第 15 页上的“不传播的命令”）。

- **端口监控：**选择 ethernet1（绑定到 Untrust 区段）和 ethernet2（绑定到 Trust 区段）以监控第 2 层网络连接。
- **二级链接：**在 HA1 和 HA2 链接都停止作业时，指定 ethernet2 接口传送 VSD 心跳信号。此功能的目的是，防止在两个 HA 链接都失败时出现多个 VSD 组主设备。
- **无偿 ARP 广播：**将 ARP 广播的数量指定为四（缺省值为五）。出现故障切换后，ARP 广播通知周围网络设备新的主设备的 MAC 地址。

（这些设备上的所有接口都变成 VSD 组 0 的 VSI。在“VSD 组”部分，为这些设备创建次级 VSD 组。请参阅第 26 页上的“范例：创建两个 VSD 组”。）



WebUI

设备 A

1. Network > Redundancy > Settings：输入以下内容[9]，然后单击 **Apply**：

   Cluster ID: 1

   NSRP Authentication Password: （选择）725dCaIgDL

   NSRP Encryption Password: （选择）WiJoaw4177

设备 B

2. Network > Redundancy > Settings：输入以下内容[10]，然后单击 **Apply**：

   Cluster ID: 1

   > Monitor Port Edit: 选择 **ethernet1** 和 **ethernet2**，然后单击 **Apply**。

   Secondary Link: ethernet2

   Number of Gratuitous ARPs to Resend: 4

   NSRP Authentication Password: （选择）725dCaIgDL

   NSRP Encryption Password: （选择）WiJoaw4177

9. 可以通过 CLI 仅设置一个集群名称。

10. 由于端口监控、二级路径以及 ARP 规范传播给具有相同集群 ID 的所有设备，因此不必在设备 B 上输入它们。但是，为了安全起见，必须在集群的每个成员上输入认证和加密密码。

CLI

设备 A

1. set nsrp cluster id 1
2. set nsrp auth password 725dCaIgDL
3. set nsrp encrypt password WiJoaw4177
4. save

设备 B

1. set nsrp cluster id 1
2. set nsrp auth password 725dCaIgDL
3. set nsrp encrypt password WiJoaw4177
4. save
5. set nsrp cluster name cluster1
6. set nsrp monitor interface ethernet1
7. set nsrp monitor interface ethernet2
8. set nsrp secondary-path ethernet2
9. set nsrp arp 4
10. save

执行对象

执行对象 (RTO) 是正常操作过程中在内存中动态创建的代码对象。RTO 的示例有会话表条目、ARP 高速缓存条目、DHCP 租用和 IPSec 安全联盟 (SA) 等。出现故障切换时，由新的主设备维持当前的 RTO 以避免服务中断[11]，这是很关键的。要实现此目的，由 NSRP 集群的成员备份 RTO。配合工作时，每个成员从其它成员备份 RTO，使双主动 HA 方案中的任一 VSD 组的主设备让位时都能维持 RTO。

在当前的 ScreenOS 版本中，不必将一个或多个 RTO 镜像组配置为与 NSRP 集群中成员的 RTO 同步。将 NetScreen 设备定义为集群的一员，并指定 RTO 同步自动启用本地设备，以便发送和接收 RTO。

缺省情况下，NSRP 集群成员不会同步 RTO。启用 RTO 同步前，必须首先同步集群成员之间的配置。除非集群中两个成员的配置相同，否则 RTO 同步可能会失败。（有关同步过程的范例，请参阅第 36 页上的 “范例：将设备添加到活动的 NSRP 集群”和第 51 页上的 “范例：双主动配置的 NSRP”。）

要启用 RTO 同步，请执行以下操作之一：

WebUI

Network > Redundancy > Settings：选择 **NSRP RTO Mirror Synchronization** 复选框，然后单击 **Apply**。

CLI

1. set nsrp rto-mirror sync
2. save

11. 使用策略可指定要备份的会话和不备份的会话。对于不希望备份的会话的流量，请应用禁用 HA 会话备份选项的策略。在 WebUI 中，清除 **HA Session Backup** 复选框。在 CLI 中，在 **set policy** 命令中使用 **no-session-backup** 参数。缺省情况下，会话备份会启用。

RTO 镜像状态

两个 NSRP 集群成员发起它们的 RTO 镜像关系的过程由两种操作状态 — 设置和活动来开发。通过这些状态的设备过程如下：

1. 将第一台设备添加到组中后，其状态为设置。在设置状态中，设备等待其对等方加入组。作为 RTO 的接收方，它定期传送接收方就绪消息 (receiver-ready)，宣布自身的可用性。作为 RTO 的发送方，它处于等待状态，直到从具有相同集群 ID 的设备获得接收方就绪消息为止。
2. 添加对等方，并且两台设备的电缆都正确连接为 HA 后（请参阅第 47 页上的“全网状配置的电缆连接”），会出现以下操作：
   a. 接收方发送一条接收方就绪消息。
   b. 发送方获得接收方就绪消息，并立即发送组活动消息，以便通知其对等方自己的状态现在为活动。
   c. 接收方然后也将自己的状态更改为活动。

除了将 RTO 从发送方传递到接收方外，两个活动镜像都按用户定义的间隔发送 RTO 心跳信号，与它们的操作状态进行通信。要定义间隔，请使用下列 CLI 命令：**set nsrp rto-mirror hb-interval** *number*。

如果设备没有从它的对等方收到指定的连续心跳信号，则它会将其状态从活动更改为设置。要定义状态转变所需的失去心跳信号临界值，请使用以下 CLI 命令：**set nsrp rto-mirror hb-threshold** *number*。

注意：*要维持同样的 RTO 心跳信号设置，应传播* ***set nsrp rto-mirror hb-interval*** *number 和* ***set nsrp rto-mirror hb-threshold*** *number。*

可以在充当 NSRP 集群中发送方的设备上使用以下命令禁用 RTO 会话同步：**set nsrp rto-mirror session off**。在设备上发布此命令只禁用该设备与集群中其它设备的会话同步。

VSD 组

“虚拟安全设备 (VSD)”组是一对物理 NetScreen 设备，它们共同组成一个单独的 VSD。一个物理设备充当 VSD 组的主设备。 VSD 的 “虚拟安全接口 (VSI)”被绑定到主设备的物理接口上。另一个物理设备充当备份[12]。如果主设备出现故障，则 VSD 故障切换到备份设备，并且 VSI 绑定转移到备份设备的物理接口，该备份设备立即晋升为主设备。

通过将两台 NetScreen 设备分组到两个 VSD 组中，每台物理设备在一个组中作为主设备，在另一个组中作为备份，两台设备都可作为主设备来积极处理流量，同时在发生故障切换时互相备份。

根据初始 NSRP 配置，优先级编号最接近 0 的 VSD 组成员成为主设备 （缺省值为 100。）如果两台设备具有相同的优先级值，则具有最小 MAC 地址的设备成为主设备。

抢先选项

通过将要成为主设备的设备设置为抢先模式，可以确定更好的优先级编号 （接近零）是否能发起故障切换。如果在该设备上启用抢先选项，则在当前主设备具有较小的优先级编号 （远离零）时，该设备变成 VSD 组的主设备。如果禁用此选项，优先级比备份设备低的主设备可保持其位置（除了某些其它因素，如内部问题或错误的网络连接方式，导致故障切换外）。

使用抑制时间延迟故障切换，可防止在邻接的交换机端口忽隐忽现时快速故障切换造成的混乱，也可确保在新的主设备可用前，周围的网络设备有足够的时间协商新的链接。要启用或禁用抢先选项，请使用以下 CLI 命令：

set/unset nsrp vsd-group id *number* **preempt**

可以使用以下 CLI 命令将抑制时间 （用于延迟抢先故障切换）设置为介于 0 到 600 秒之间的任何时间长度：

set nsrp vsd-group id *number* **preempt hold-down** *number*

12. 在当前版本中，一个 VSD 组可以有两个成员。在以后的版本中，可以有两个以上的成员。在这种情况下，一台设备充当主设备，另一台设备充当一级备份，其余的 VSD 组成员充当备份。

VSD 组成员状态

VSD 组的成员可以是以下六种状态之一：

- 主设备 – 处理发送到 VSI 的流量的 VSD 组成员的状态。
- 一级备份 – 当前主设备让位后应变成主设备的 VSD 组成员的状态。选择过程使用设备优先级确定要晋升的成员。请注意，在选择新的主设备时， RTO 对等方优先于任何其它 VSD 组成员，即使该成员具有更好的优先分级。
- 备份 – 监控一级备份的状态并在当前设备让位时，将一个备份设备选择为一级备份的 VSD 组成员的状态。
- 初始 – 启动设备或通过 **set nsrp vsd-group id** *id_num* 命令添加设备时， VSD 组成员加入 VSD 时的瞬间状态。

  使用 **set nsrp vsd-group init-hold** *number* 命令，可指定 VSD 组成员在初始状态中停留的时间。缺省 （最小）设置为 5。要确定初始状态抑制时间，将暂停初始化值乘以 VSD 心跳信号间隔 （暂停初始化 x 心跳信号间隔 = 初始状态抑制时间）。例如，如果暂停初始化值为 5，心跳信号间隔为 1,000 毫秒，则初始状态抑制时间为 15,000 毫秒，或为 5 秒 (5 x 1,000 = 5,000)。

  注意：*如果减少 VSD 心跳信号间隔，则应增加暂停初始化值。有关配置心跳信号间隔的信息，请参阅第 25 页上的 “心跳信号消息”。*

- 无资格 – 管理员有意指派一个 VSD 组成员，使其不能参与选择过程的状态。要做到这一点，请使用 **set nsrp vsd-group id** *id_num* **mode ineligible** 命令。
- 不可操作 – 系统检查并确定设备有内部问题 （如没有处理板）或网络连接问题 （如接口链接失败）后 VSD 组成员的状态。

  注意：*设备从无资格状态 （使用* ***exec nsrp vsd-group id*** *id_num* ***mode { backup | init | master | pb }*** *命令）或不可操作状态 （系统或网络问题已修正）返回时，必须首先通过初始状态。*

通过观察辅助模块上的 HA LED 可确定设备状态。不同颜色 — 黑色、绿色、黄色、红色 — 的含义如下：

- 黑色：设备对于 NSRP 没有启用。
- 绿色：设备对于 NSRP 启用；它是一个或多个 VSD 组中的主设备；并且没有处于不可操作模式。
- 黄色：设备对于 NSRP 启用；它不是任意 VSD 组中的主设备；并且没有处于不可操作模式。
- 红色：设备对于 NSRP 启用，但是它当前处于不可操作模式。

心跳信号消息

每个 VSD 组成员 （即使它处于初始、无资格或不可操作状态）都可通过每隔一秒[13] 发送心跳信号消息与它的组成员进行通信。这些消息使每个成员知道其它每个成员当前的状态。心跳信号消息包括下列信息：

- 设备的设备 ID
- VSD 组 ID
- VSD 组成员状态 （主设备、一级备份或备份）
- 设备优先级
- RTO 对等方信息

发送 VSD 心跳信号的间隔可以配置 （200、 600、 800 或 1,000 毫秒；缺省值为 1,000 毫秒）。可普遍应用到所有 VSD 组的 CLI 命令为 **set nsrp vsd-group hb-interval** *number*。也可配置失去心跳信号临界值，用于确定认为 VSD 组成员丢失的时间。可普遍应用到所有 VSD 组的 CLI 命令为 **set nsrp vsd hb-threshold** *number*。失去心跳信号临界值的最小值为 3。

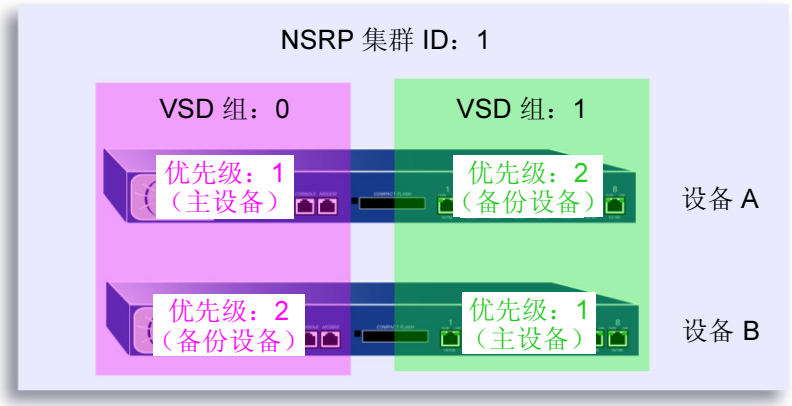
心跳信号消息通过 HA1 链接发送。有关 HA1 和 HA2 接口以及通过每个接口进行通信的消息类型的详细信息，请参阅第 37 页上的 “双 HA 接口”。

13. 如果设备处于不可操作状态，并且所有 HA 链接都中断，则它既不能发送也不能接收 VSD 心跳信号消息，除非为这些消息配置了二级路径。有关配置二级路径的详细信息，请参阅第 18 页上的 “范例：创建 NSRP 集群”。

范例：创建两个 VSD 组

本例继续进行设备 A 和设备 B 的配置，它们已经是同一 NSRP 集群和 VSD 组 0 的成员 （请参阅第 18 页上的 “范例：创建 NSRP 集群”）。

在本例中，创建第二个 VSD 组 — “组 1”。在 “组 0”中指派设备 A 的优先级为 1，在 “组 1”中的缺省优先级为 (100)。在 “组 1”中指派设备 B 的优先级为 1，在 “组 0”中的缺省优先级为 (100)。在两个 VSD 组中，在主设备上启用抢先选项并将抢先抑制时间设置为 10 秒。如果两台设备都是活动的，则设备 A 始终是 “组 1”的主设备，设备 B 是 “组 2”的主设备。



WebUI

设备 A

1. Network > Redundancy > VSD Group > Edit（对于 VSD 组 0）：输入以下内容，然后单击 **OK**：

   Priority: 1

   Enable Preempt: （选择）

   Preempt Hold-Down Time (sec): 10

2. Network > Redundancy > VSD Group > New：在 “Group ID” 字段中，键入 **1**，然后单击 **OK**。

设备 B

3. Network > Redundancy > VSD Group > Edit（对于 VSD 组 1）：输入以下内容，然后单击 **OK**：

   Priority: 1

   Enable Preempt: （选择）

   Preempt Hold-Down Time (sec): 10

CLI

设备 A

1. set nsrp vsd-group id 0 priority 1
2. set nsrp vsd-group id 0 preempt hold-down 10
3. set nsrp vsd-group id 0 preempt
4. set nsrp vsd-group id 1
5. save

设备 B

6. set nsrp vsd-group id 1 priority 1
7. set nsrp vsd-group id 1 preempt hold-down 10
8. set nsrp vsd-group id 1 preempt
9. save

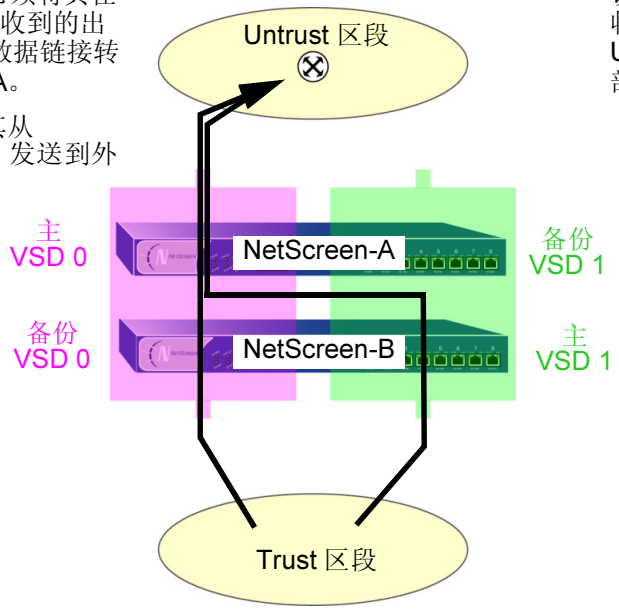
VSI 和静态路由

创建 VSD 组后，必须将“虚拟安全接口 (VSI)”绑定到 VSD。将 NetScreen 设备放置在 NSRP 集群中时，所有安全区段接口都变成 VSD 组 0 的 VSI。对于在 NetScreen 设备上配置的每个安全区段，必须用其它 ID 将 VSI 手动指派给 VSD。

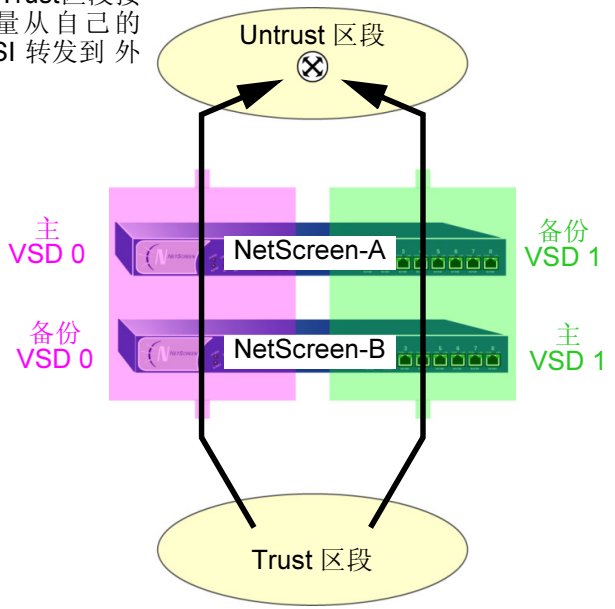
缺省情况下，NetScreen 设备将一个条目添加到它的路由表中，用于 VSI 的直接子网。对于直接子网以外地址的静态路由，必须为每个 VSI 手动建立路由表条目，通过它们，NetScreen 设备将流量转发到那些地址。例如，如果有两个 VSD 并且要将缺省路由配置到 Untrust 区段中的路由器，则必须为两个 VSD 的 Untrust 区段 VSI 建立路由表条目。如果仅在一个 VSD （如 VSD 0）上设置缺省路由，则充当另一 VSD （如 VSD 1）主设备的 NetScreen 设备必须将所有发送给它的出站流量通过 HA 数据链接发送到充当 VSD 0 主设备的设备。

如果缺省路由只设置在VSD 0 上，则作为 VSD 1 主设备的 NetScreen-B 必须将其在 Trust 区段 VSI 接收到的出站流量 通过 HA 数据链接转发到 NetScreen-A。

NetScreen-A 将其从 Untrust 区段 VSI 发送到外部路由器。



如果缺省路由设置在 VSD 0 和 1 上，则两台 NetScreen 设备都将它们在Trust区段接收到的出站流量从自己的 Untrust 区段 VSI 转发到 外部路由器。



范例：Trust 和 Untrust 区段 VSI

本范例建立在以前的范例第 26 页上的 “范例：创建两个 VSD 组”上，并假定已经在设备 A 和设备 B 上完成了以下操作：

- 将两台设备都放置在 NSRP 集群 1 中
- 创建了 VSD 组 1（将设备放置在 NSRP 集群 1 中时， NetScreen 设备自动创建 VSD 组 0）
- 将 ethernet1 绑定到 Untrust 区段并将其 IP 地址指派为 210.1.1.1/24
- 将 ethernet3 绑定到 Trust 区段并将其 IP 地址指派为 10.1.1.11/24

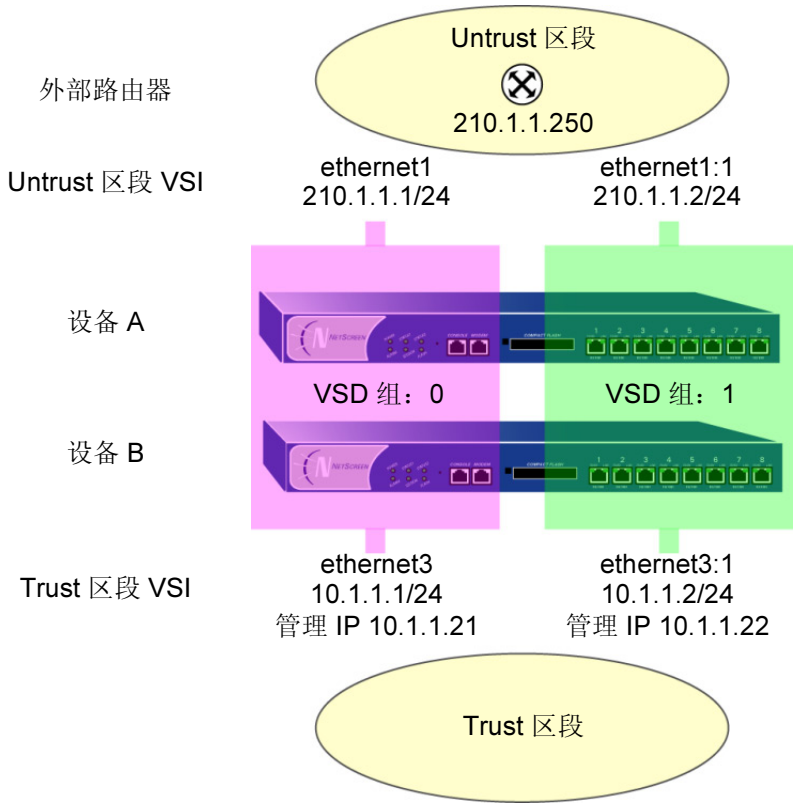
将 10.1.1.21 定义为设备 A 的 ethernet3 上的管理 IP，将 10.1.1.22 定义为设备 B 的 ethernet3 上的管理 IP。然后为 VSD 组 1 创建以下 VSI：

- Untrust 区段 VSI ethernet1:1 (210.1.1.2/24)
- Trust 区段 VSI ethernet3:1 (10.1.1.2/24)

NetScreen 设备使用将设备放置在 NSRP 集群中时已经指派给本地接口的 IP 地址，自动为 VSD 组 0 创建 VSI。在本范例中，VSD 组 0Untrust 区段 VSI 为 ethernet1[14]，IP 地址为 210.1.1.1/24。VSD 组 0Trust 区段 VSI 为 ethernet3，IP 地址为 10.1.1.1/24。

最后，将两个缺省路由设置到地址为 210.1.1.250 的 Untrust 区段中的外部路由器 — 一个用于 VSD 0 上的 Untrust 区段 VSI，另一个用于 VSD 1 上的 Untrust 区段 VSI。所有安全区段都在 trust-vr 路由域中。

14. VSD 组 ID “0”不会出现在 VSD 0 的 VSI 名称中。 VSI 仅由 *ethernet1* 识别，而不是由 *ethernet1:0* 识别。



WebUI (设备 A)

管理 IP 地址

1. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：

   Zone Name: Trust

   IP Address/Netmask: 10.1.1.1/24

   Manage IP: 10.1.1.21

WebUI (设备 B)

管理 IP 地址

2. Network > Interfaces > Edit（对于 ethernet3）：输入以下内容，然后单击 **OK**：

   Zone Name: Trust

   IP Address/Netmask: 10.1.1.1/24

   Manage IP: 10.1.1.22

虚拟安全接口

3. Network > Interfaces > New VSI IF：输入以下内容，然后单击 **OK**：

   Interface Name: VSI Base: ethernet1

   VSD Group: 1

   IP Address/netmask: 210.1.1.2/24

4. Network > Interfaces > New VSI IF：输入以下内容，然后单击 **OK**：

   Interface Name: VSI Base: ethernet3

   VSD Group: 1

   IP Address/netmask: 10.1.1.2/24

路由

5. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：

   Network Address: 0.0.0.0

   Netmask: 0.0.0.0

   Gateway: （选择）

   Interface: ethernet1:1

   Gateway IP Address: 210.1.1.250

6. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：

   Network Address: 0.0.0.0

   Netmask: 0.0.0.0

   Gateway: （选择）

   Interface: ethernet1:2

   Gateway IP Address: 210.1.1.250

CLI (设备 A)

管理 IP 地址

1. set interface ethernet3 manage-ip 10.1.1.21

CLI (设备 B)

管理 IP 地址

2. set interface ethernet3 manage-ip 10.1.1.22

虚拟安全接口

3. set interface ethernet1:1 ip 210.1.1.2/24
4. set interface ethernet3:1 ip 10.1.1.1.2/24

路由

5. set vrouter trust-vr route 0.0.0.0/0 interface ethernet1 gateway 210.1.1.250
6. set vrouter trust-vr route 0.0.0.0/0 interface ethernet1:1 gateway 210.1.1.250
7. save

配置、文件和 RTO 同步

将新设备添加到 NSRP 集群中时，必须使 VSD 组主设备的配置和文件（如 PKI 公开 / 私有密钥文件）与新设备同步。同步配置文件后，必须同步执行对象 (RTO)。集群成员由于任何原因而无法同步后，也必须同步配置、文件和 RTO。

同步配置

如果在一台设备上进行任何配置更改，而集群中的另一设备重新启动（或者如果所有 HA 链接都出现故障）时，配置设置就有可能变得不同步。要发现一台设备的配置与另一台设备的配置是否超出同步，请使用 **exec nsrp sync global-config check-sum** 命令。输出结果说明两台设备的配置是在同步范围内还是超出同步范围，并提供本地和远程设备的校验和。

如果配置超出同步，请使用以下命令将它们同步：**exec nsrp sync global-config save**。同步配置前，如果没有在本地设备上使用 **unset all** 命令，则本地设备将远程设备的配置附加到现有设置上。但是，在同步配置后，每个复制的设置都将生成一条错误消息。要避免在同步配置时生成错误消息，可执行以下操作：

1. 将本地和远程配置下载到工作站。
2. 使用应用程序（如 WinDiff）识别文件间的差异。
3. 在本地设备上手动输入在远程设备上添加、修改或删除的设置。

注意：*由于 NetScreen 设备使用 “NetScreen 可靠传输协议 (NSTP)”，它与 TCP 非常类似（只是更轻量），因此集群中活动设备上的配置很少变成不同步。*

同步文件

如果需要同步一个特定文件，请在要同步文件的设备上输入以下命令：**exec nsrp sync file name** *name_str* **from peer**。如果要同步所有文件，请输入 **exec nsrp sync file from peer**。

同步 RTO

如果在集群中的一台设备上启用了 RTO 镜像同步 （请参阅第 21 页上的 “执行对象”），则设备重新启动时， RTO 会自动重新同步。但是，如果禁用 RTO 镜像同步 （可能在设备上执行调试或维护），则再次启用 RTO 同步时，必须手动重新同步所有 RTO。要做到这一点，请使用 **exec nsrp sync rto all** 命令。如果仅重新同步选定的 RTO（如 ARP、DNS、会话或 VPN），可以使用以下 CLI 命令：**exec nsrp sync rto { arp | auth-table | dns | l2tp | session | vpn }**。

要在 NSRP 集群中的成员检测集群中的其它成员时启用自动开始 RTO 同步，请使用 **set nsrp rto-mirror sync** 命令。需要手动同步 RTO 时，请使用 **exec nsrp sync rto { arp | auth-table | dns | l2tp | session | vpn }** 命令。

范例：手动重新同步 RTO

在本范例中，设备 A 和设备 B 在 NSRP 集群 1 以及 VSD 组 1 和 2 中。设备 A 是 VSD 组 1 的主设备，是 VSD 组 2 的备份设备。设备 B 是 VSD 组 2 的主设备，是 VSD 组 1 的备份设备。

要在设备 B 上进行一些故障排除操作，同时又不希望将它从网络断开。可强制设备 B 变成 VSD 组 2 中的备份设备，然后禁用 RTO 同步。设备 A 变成两个 VSD 组的主设备。完成对设备 B 的故障排除后，请再次启用 RTO 镜像同步，然后手动重新同步从设备 A 到设备 B 的 RTO。最后重新将设备 B 指派为 VSD 组 2 的主设备。

WebUI

> ***注意：****RTO 的手动同步只能通过 CLI 进行。*

CLI

设备 B

1. exec nsrp vsd-group id 2 mode backup
2. unset nsrp rto-mirror sync

   设备 B 不再处理流量，也不使 RTO 与设备 A 同步。此时，可以对设备 B 进行故障排除，而不会影响设备 A 的流量处理性能。
3. set nsrp rto-mirror sync
4. exec nsrp sync rto all from peer
5. exec nsrp vsd-group id 2 mode master

范例：将设备添加到活动的 NSRP 集群

在本范例中，将以前起到安全设备作用的设备 A 添加到 NSRP 集群中的 VSD 组 0 和 1 中，该集群的 ID 为 1，名称为“cluster1”。必须撤消设备 A 上以前的配置，重新启动它，然后从两个 VSD 组的主设备同步配置、文件和 RTO。然后将设备 A 指派为 VSD 组 0 的主设备。

WebUI

> ***注意：****冷启动同步功能只能通过 CLI 进行。*

CLI

设备 A

1. unset all[15]

   出现以下提示：“Erase all system config, are you sure y / [n]?”
2. 按 **Y** 键。

   系统配置返回到出厂缺省设置。
3. reset

   系统重新启动。
4. set nsrp cluster id 1
5. set nsrp cluster name cluster1
6. exec nsrp sync file
7. exec nsrp sync global-config
8. set nsrp rto-mirror sync
9. exec nsrp vsd-group id 0 mode master
10. save all[16]

15. 如果不首先使用 **unset all** 命令，则 **exec nsrp sync global-config** 命令将新的配置设置附加到现有的设置上。（注意：NetScreen 设备为每个实现同步的复制设置生成一条错误消息。）

16. 使用 **save all** 命令保存所有虚拟系统和根级中的配置。而使用 **save** 命令仅保存根级中的配置。

冗余接口

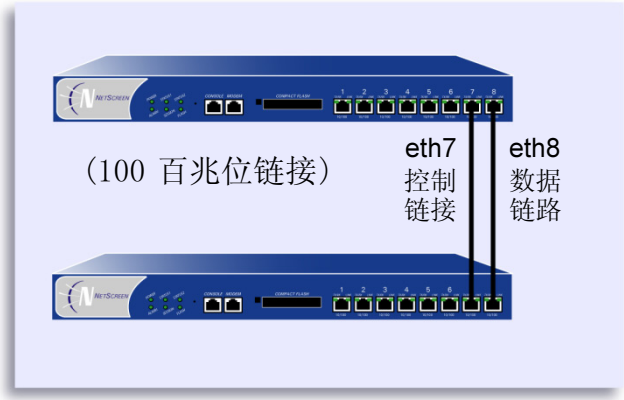
NSRP 的基本原则是没有单一故障点。除冗余设备外，NetScreen 设备具有专用的物理冗余 HA 接口（HA1 和 HA2）或可以将两个通用接口绑定到 HA 区段，以提供 HA 接口冗余。

另外，您可以创建冗余安全区段接口。

双 HA 接口

所有在集群成员之间传递的 NSRP 信息都是通过两个 HA 接口传递的。为更好地分配超出带宽的带宽， HA1 处理 NSRP 控制消息而 HA2 处理网络数据消息。如果任一端口在有千兆位 HA1 和 HA2 接口的 NetScreen 设备上发生故障，另一个活动端口则会承担这两种信息流。对于必须将 100 百兆位接口用于数据链路的 NetScreen 设备，数据链路发生故障会导致仅有一个活动 HA 链接来控制消息。如果控制链接在此类设备上故障，那么数据链路就变成控制链接，并仅能发送和接收控制消息。

如果 HA1 或 HA2 之一出现故障，则会通过另一个 HA 链接来发送控制和数据消息。



如果 ethernet7 或 ethernet8 之一发生故障，则仅通过另一个 HA 链接来发送控制消息。

注意：*如果在 HA 端口之间使用交换机，则应使用基于端口的 VLAN，它不会与先前封包上的 VLAN 标记发生冲突。*

在没有专用 HA 接口的 NetScreen 设备上，必须将一个或两个物理以太网接口绑定到 HA 区段上。如果将一个千兆位接口绑定到 HA 区段上，则该 HA 链接同时支持控制和数据消息。如果将一个百兆位接口绑定到 HA 区段上，则该 HA 链接将仅支持控制消息。如果将两个接口（千兆位或 100 百兆位）绑定到 HA 区段上，则绑定到该区段的第一个接口变为控制链接，而绑定到该区段的第二个接口变为数据链路。（有关将接口绑定到区段的信息，请参阅第 **2**-89 页上的“将接口绑定到安全区段”。）

在没有专用 HA 接口的 NetScreen 设备上，也可以指定一个接口来绑定到安全区段以处理 HA 控制消息。使用 CLI 命令 **set nsrp interface** *interface*。

控制消息

有两种控制消息：心跳信号和 HA 消息。

心跳信号：定时发送心跳信号可在 NSRP 集群成员、VSD 组成员和 RTO 镜像之间建立和维持通信。心跳信号不断通告发送方成员的状态、其系统的使用状况以及网络的连通性。三种心跳信号消息如下：

- HA 物理链接心跳信号
- VSD 心跳信号
- RTO 心跳信号

HA 物理链接心跳信号从 NSRP 每个成员的 HA1 和 HA2 接口向其它成员广播消息。这些消息的目的是监视 HA 接口的使用状况。例如，如果一个成员没有从 HA1 收到三个连续的心跳信号，则这些设备会将控制消息的传输转移给 HA2。

VSD 心跳信号是从 VSD 组中每个成员的 HA1 接口进行广播的。 VSD 组使用这些消息来监视其所有成员的从属状态。例如，如果主设备通告它变为不可操作，则主要备份设备立刻变为 VSD 组的主设备。

镜像组的每个成员从 HA1 接口广播 RTO 心跳信号。这些消息的目的是找到一个活动的对等方，然后发送组活动消息来维持镜像关系。例如，如果一个设备没有从它的对等方收到 16 个连续的 RTO 心跳信号，则它会将其状态从活动转变为固定。

注意：*如果从镜像组中删除了一个设备，它将进入未定义状态，并且会将一条“组拆分”消息传送到其对等方。该对等方立即从活动状态改变为固定状态（而不会等待丢失心跳信号）以超越临界值。*

HA 消息：两种 HA 消息如下：

- 配置消息 – 主设备向其它 VSD 组成员发送的网络和配置设置
- RTO 消息 – 主设备向其它 RTO 镜像发送的 RTO

HA 消息中包括在不引起服务中断的情况下而使备份设备变为主设备的信息。

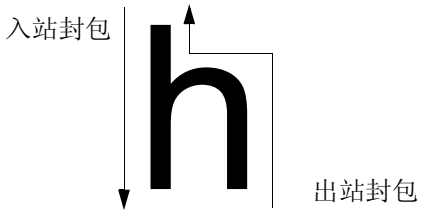
数据消息（封包交换）

数据消息为穿越防火墙的 IP 封包，VSD 组中的备份必须将它们转发给作为主设备的设备。当封包到达双主动配置中 NetScreen 设备的接口时，该设备首先识别哪个 VSD 组必须处理该封包。如果收到封包的设备是识别 VSD 组的主设备，它自己将处理该封包。如果该设备不是主设备，它会通过 HA 数据链路将封包转发给主设备。

例如，一个负载均衡路由器可能会在会话中向设备 A（VSD 组 1 的主设备）发送第一个封包，该设备会在其会话表中创建一个条目。如果路由器通过轮询方式（即，路由器依次向每个 NetScreen 设备发送封包）发送封包来执行负载均衡，则该路由器可能将下一封包发送到设备 B（VSD 组 1 的备份）。因为在设备 A 中存在一个会话条目，所以设备 B 通过数据链路[17] 将封包转发给设备 A，由它来进行处理。

17. 如果没有数据链路，则收到封包的 NetScreen 设备立即将它丢弃。

仅在 NetScreen 设备处于 “路由” 模式中的双主动配置时，入站封包才会通过数据链路转发。当处于 NAT 模式时，虽然接收返回出站封包的 NetScreen 设备可能会通过数据链路将其转发给具有该封包所属会话条目的设备，但是路由器总是将进入封包发送到 MIP、VIP 或 VPN 通道网关。此种封包转发方式产生了一个 “h” 形的路径。像字母 *h* 的笔划一样，入站封包通过一个设备直接发送，但是出站封包通过其它设备发送到中途，然后通过数据链路转发给第一个设备。



安全区段冗余接口

应用相似类型的虚拟化，允许 VSI 将其绑定从一个设备的物理接口转移到另一设备的物理接口，VSI 可以将其绑定从同一设备的一个物理接口转移到另一个物理接口。例如，如果从主接口到交换机的链接断开，则该链接会切换到次接口，从而防止设备从 VSD 主设备向备份设备进行故障切换。

可将 VSI 绑定到下列接口类型之一：

- 子接口
- 物理接口
- 冗余接口，将其依次绑定到两个物理接口

注意：*不能将子接口与冗余接口一起分组。但是，可以在冗余接口上定义一个 VLAN，同样也可以在子接口上定义一个 VLAN。有关子接口和 VLAN 的信息，请参阅第* ***6****-19 页上的“定义子接口和 VLAN 标记”。*

范例：为 VSI 创建冗余接口

在本例中，设备 A 和 B 是双主动配置的两个 VSD 组（VSD 组 0 和 VSD 组 1）的成员。设备 A 是 VSD 组 0 的主设备和 VSD 组 1 的备份。设备 B 是 VSD 组 1 的主设备和 VSD 组 0 的备份。NetScreen 设备链接到两对冗余交换机，即 Untrust 区段中的交换机 A 和 B，以及 Trust 区段中的交换机 C 和 D。

注意：*本例仅介绍在设备 A 上创建冗余接口。因为设备 A 和 B 是同一 NSRP 集群的成员，设备 A 会将所有的接口配置传播给设备 B，除了管理 IP 地址，该地址应在两个设备上的 redundant2 接口上输入：设备 A 10.1.1.3，设备 B 10.1.1.4。*

将 ethernet1/1 和 ethernet1/2 放置在 redundant1 中，将 ethernet2/1 和 ethernet2/2 放置在 redundant2 中。在 redundant2 接口中，将设备 A 的管理 IP 定义为 10.1.1.21，并在次接口中将设备 B 的管理 IP 定义为 10.1.1.22。

绑定到同一冗余接口的物理接口连接到不同的交换机：

- 在 Untrust 区段中将物理接口绑定到冗余接口：ethernet1/1 到交换机 A， ethernet1/2 到交换机 B
- 在 Trust 区段中将物理接口绑定到冗余接口：ethernet2/1 到交换机 C， ethernet2/2 到交换机 D

注意：*物理接口并不一定要与绑定它们的冗余接口位于同一安全区段。*

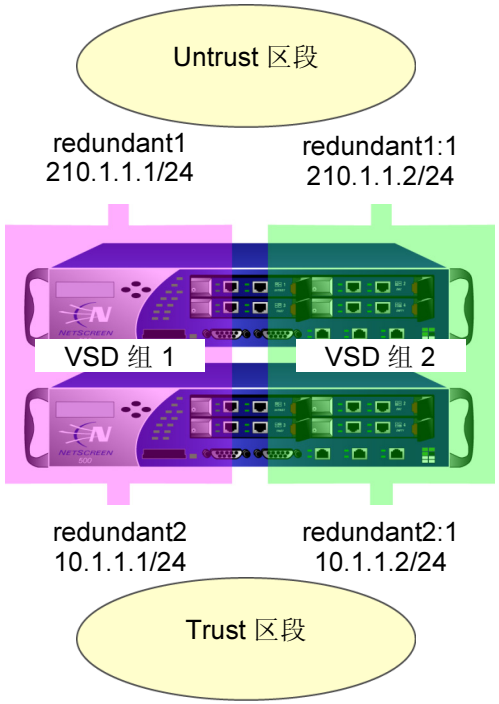
首先将 ethernet1/1 和 ethernet2/1 放置在它们对应的冗余接口中后，就已经将它们指定为主接口。（您可以通过 CLI 命令 **set interface** *interface1* **phy primary** *interface2* 来改变这种主状态分配。）如果到主接口的链接断开，则 NetScreen 设备会通过次接口到另一个交换机重新路由流量，而不要求 VSD 主设备进行故障切换。

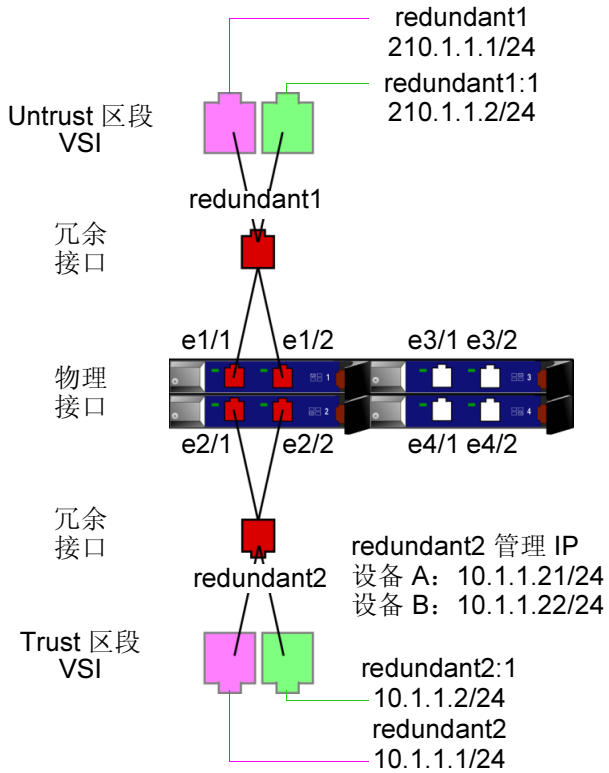
在本例中， ethernet1/1 上的电缆断开，引起了端口故障切换到 ethernet1/2。因此，所有由设备 A 和 B 接收和发送的流量都通过交换机 B。重新连接设备 A 上从 ethernet1/1 到交换机 A 的电缆，会自动使该接口重新获得其先前的优先级。

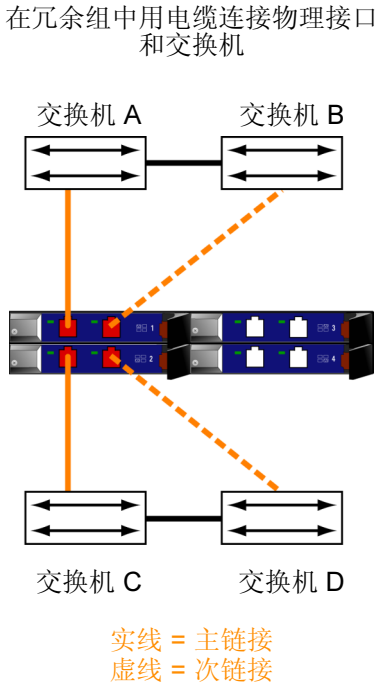
VSI 的 IP 地址为：

VSD 组 0 的 VSI		VSD 组 1 的 VSI	
redundant1	210.1.1.1/24	redundant1:1	210.1.1.2/24
redundant2	10.1.1.1/24	redundant2:1	10.1.1.2/24

注意：*如果多个 VSI 在同一个冗余接口、物理接口或子接口上，则这些 VSI 的 IP 地址可以在同一子网中或在不同的子网中。如果 VSI 在不同的接口上，则它们必须在不同的子网中。*







WebUI (设备 A)

冗余接口

1. Network > Interfaces > New Redundant IF：输入以下内容，然后单击 **OK**：

   Interface Name: redundant1

   Zone Name: Untrust

   IP Address/Netmask: 210.1.1.1/24

2. Network > Interfaces > Edit (对于 ethernet1/1)：在“As member of”下拉列表中选择 **redundant1**，然后单击 **OK**。
3. Network > Interfaces > Edit (对于 ethernet1/2)：在“As member of”下拉列表中选择 **redundant1**，然后单击 **OK**。
4. Network > Interfaces > New Redundant IF：输入以下内容，然后单击 **OK**：

   Interface Name: redundant2

   Zone Name: Trust

   IP Address/Netmask: 10.1.1.1/24

   Manage IP: 10.1.1.21

5. Network > Interfaces > Edit（对于 ethernet2/1）：在“As member of”下拉列表中选择 **redundant2**，然后单击 **OK**。
6. Network > Interfaces > Edit（对于 ethernet2/2）：在“As member of”下拉列表中选择 **redundant2**，然后单击 **OK**。

虚拟安全接口

7. Network > Interfaces > New VSI IF：输入以下内容，然后单击 **OK**：

   Interface Name: VSI Base: redundant1

   VSD Group: 1

   IP Address/netmask: 210.1.1.2/24

8. Network > Interfaces > New VSI IF：输入以下内容，然后单击 **OK**：

   Interface Name: VSI Base: redundant2

   VSD Group: 1

   IP Address/netmask: 10.1.1.2/24

WebUI (设备 B)

Network > Interfaces > Edit （对于 redundant2）：在 Manage IP 字段中键入 **10.1.1.22**，然后单击 **OK**。

注意：*必须为每个 VSD 中每个 VSI 的直接子网以外的地址输入静态路由。有关为两个 Untrust 区段 VSI 添加缺省路由的示例，请参阅第 51 页上的 “范例：双主动配置的 NSRP”。*

CLI (设备 A)

冗余接口

1. set interface redundant1 zone untrust
2. set interface redundant1 ip 210.1.1.1/24
3. set interface ethernet1/1 group redundant1
4. set interface ethernet1/2 group redundant1
5. set interface redundant2 zone trust
6. set interface redundant2 ip 10.1.1.1/24
7. set interface redundant2 manage-ip 10.1.1.21
8. set interface ethernet2/1 group redundant2
9. set interface ethernet2/2 group redundant2

虚拟安全接口

10. set interface redundant1:1 ip 210.1.1.2/24
11. set interface redundant2:1 ip 10.1.1.2/24
12. save

CLI (设备 B)

13. set interface redundant2 manage-ip 10.1.1.22
14. save

> ***注意：****必须为每个 VSD 中的 每个 VSI 的直接子网以外的地址输入静态路由。有关为两个 Untrust 区段 VSI 添加缺省路由的示例，请参阅**第 51 页上的 “范例：双主动配置的 NSRP”**。*

设置过程

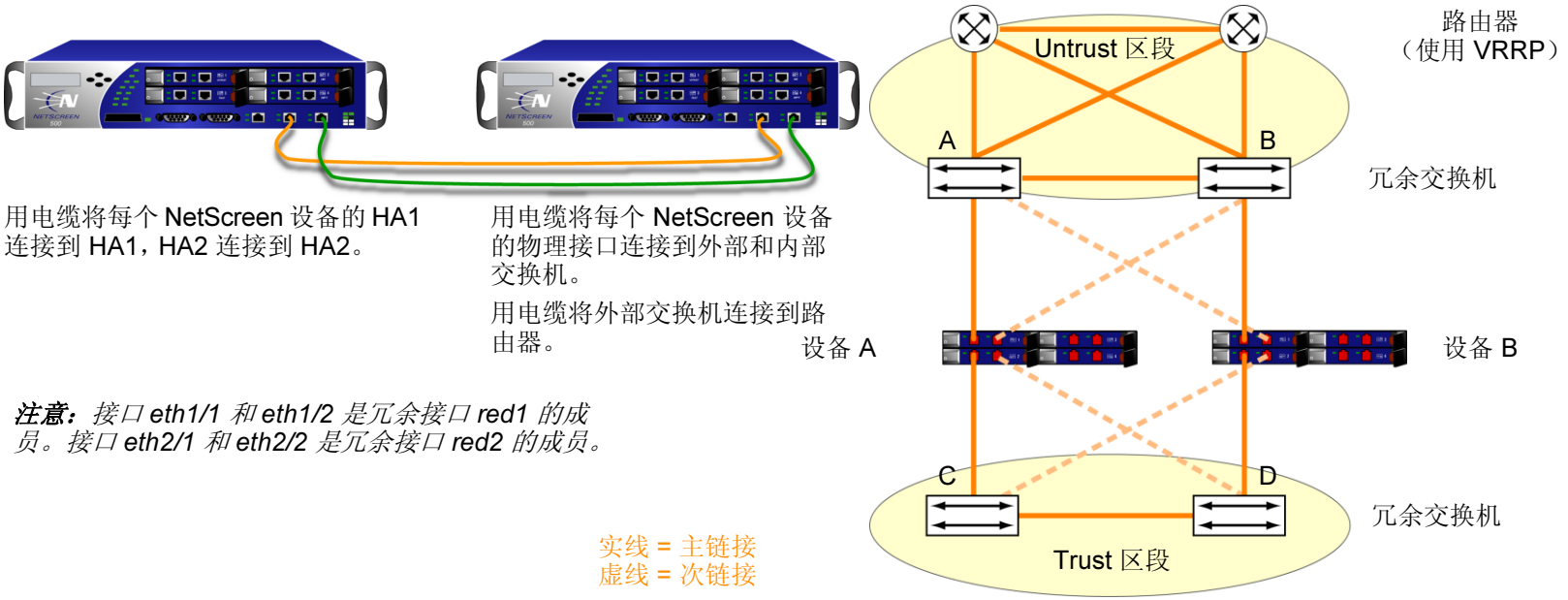
要配置两个 NetScreen 设备使其具有高可用性，必须用电缆将它们连接到网络并将它们互相连接，然后用 NSRP 将它们配置为 HA。

全网状配置的电缆连接

下面的图表说明了两个设备 NetScreen 之间的电缆连接，以及它们同内部交换机和外部交换机的冗余对之间的电缆连接。外部交换机然后将与一对运行 VRRP 的冗余路由器连接，完成全网状配置。第一个图表显示带有专用 HA 接口的 NetScreen 设备。第二个图表显示用网络接口来处理 HA 流量的两个 NetScreen 设备。

注意： *根据配置 NetScreen 设备的拓扑结构以及您使用的交换机和路由器种类的不同，在下图中提供的电缆连接可能会与您网络的要求有所不同。*

带有专用 HA 接口的 NetScreen 设备



注意： *接口 eth1/1 和 eth1/2 是冗余接口 red1 的成员。接口 eth2/1 和 eth2/2 是冗余接口 red2 的成员。*

如下所示，用电缆连接全网状配置中的 NSRP 的两个 NetScreen 设备 （设备 A 和设备 B）：

NetScreen A 和 NetScreen B：HA 链接

1. 用电缆将每个 NetScreen 设备的 HA1 接口连接在一起。
2. 用电缆将每个 NetScreen 设备的 HA2 接口连接在一起。

NetScreen A：Redundant1 (eth1/1 和 eth1/2)， Untrust 区段

3. 用电缆将 ethernet1/1 和外部交换机 A 相连接。（ethernet1/1 是绑定到 Untrust 区段中冗余接口 red1 上的两个物理接口之一。）
4. 用电缆将 ethernet1/2 和外部交换机 B 相连接。（ethernet1/2 是绑定到 Untrust 区段中 red1 上的另一个物理接口。）

NetScreen A：Redundant2 (eth2/1 和 eth2/2)， Trust 区段

5. 用电缆将 ethernet2/1 和外部交换机 C 相连接。（ethernet2/1 是绑定到 Trust 区段中冗余接口 red2 上的两个物理接口之一。）
6. 用电缆将 ethernet2/2 和外部交换机 D 相连接。（ethernet2/2 是绑定到 Trust 区段中 red2 上的另一个物理接口。）

NetScreen B：Redundant1 (eth1/1 和 eth1/2)， Untrust 区段

7. 用电缆将 ethernet1/1 和外部交换机 B 相连接。（ethernet1/1 是绑定到 Untrust 区段中冗余接口 red1 上的两个物理接口之一。）
8. 用电缆将 ethernet1/2 和外部交换机 A 相连接。（ethernet1/2 是绑定到 Untrust 区段中 red1 上的另一个物理接口。）

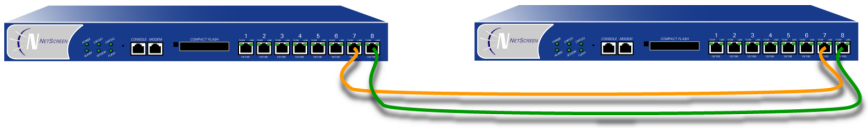
NetScreen B：Redundant2 (eth2/1 和 eth2/2)， Trust 区段

9. 用电缆将 ethernet2/1 和外部交换机 D 相连接。（ethernet2/1 是绑定到 Trust 区段中冗余接口 red2 上的两个物理接口之一。）
10. 用电缆将 ethernet2/2 和外部交换机 C 相连接。（ethernet2/2 是绑定到 Trust 区段中 red2 上的另一个物理接口。）

交换机和路由器

11. 用电缆将冗余外部交换机连接在一起。
12. 将外部交换机用电缆与冗余路由器相连接，其配置与 NetScreen 设备连接到交换机所使用的配置相同。
13. 用电缆将外部冗余交换机连接在一起。

用网络接口来处理 HA 链接的 NetScreen 设备



将 ethernet7 和 ethernet8 绑定到每个 NetScreen 设备的 HA 区段。

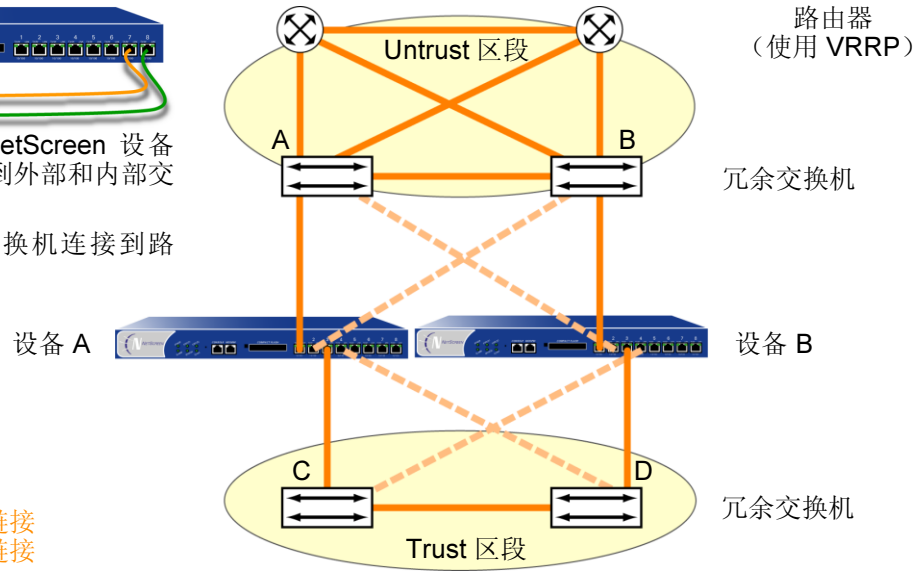
然后将绑定到 HA 区段的接口用电缆连接在一起：

- 设备 A 上的 eth7 连接到 设备 B 上的 eth7
- 设备 A 上的 eth8 连接到 设备 B 上的 eth8

***注意：** 接口 eth1 和 eth2 是冗余接口 red1 的成员。接口 eth3 和 eth4 是冗余接口 red2 的成员。*

用电缆将每个 NetScreen 设备的物理接口连接到外部和内部交换机。

用电缆将外部交换机连接到路由器。



将 ethernet7 和 ethernet8 绑定到两个 NetScreen 设备（设备 A 和设备 B）上的 HA 区段后，如下所示，用电缆按全网状配置连接 NSRP 的 NetScreen 设备：

NetScreen A 和 NetScreen B：HA 链接

1. 用电缆将每个 NetScreen 设备的 ethernet7 接口连接在一起。
2. 用电缆将每个 NetScreen 设备的 ethernet8 接口连接在一起。

NetScreen A：Redundant1 (ethernet1 和 ethernet2)， Untrust 区段

3. 用电缆将 ethernet1 和外部交换机 A 相连接。（ethernet1 是绑定到 Untrust 区段中冗余接口 red1 上的两个物理接口之一。）
4. 用电缆将 ethernet2 和外部交换机 B 相连接。（ethernet2 是绑定到 Untrust 区段中 red1 上的另一个物理接口。）

NetScreen A：Redundant2 (ethernet3 和 ethernet4)， Trust 区段

5. 用电缆将 ethernet3 和外部交换机 C 相连接。（ethernet3 是绑定到 Trust 区段中冗余接口 red2 上的两个物理接口之一。）
6. 用电缆将 ethernet4 和外部交换机 D 相连接。（ethernet4 是绑定到 Trust 区段中 red2 上的另一个物理接口。）

NetScreen B：Redundant1 (ethernet1 和 ethernet2)， Untrust 区段

7. 用电缆将 ethernet1 和外部交换机 B 相连接。（ethernet1 是绑定到 Untrust 区段中冗余接口 red1 上的两个物理接口之一。）
8. 用电缆将 ethernet2 和外部交换机 A 相连接。（ethernet2 是绑定到 Untrust 区段中 red1 上的另一个物理接口。）

NetScreen B：Redundant2 (ethernet3 和 ethernet4)， Trust 区段

9. 用电缆将 ethernet3 和外部交换机 D 相连接。（ethernet3 是绑定到 Trust 区段中冗余接口 red2 上的两个物理接口之一。）
10. 用电缆将 ethernet4 和外部交换机 C 相连接。（ethernet4 是绑定到 Trust 区段中 red2 上的另一个物理接口。）

交换机和路由器

11. 用电缆将冗余外部交换机连接在一起。
12. 将外部交换机用电缆与冗余路由器相连接，其配置与 NetScreen 设备连接到交换机所使用的配置相同。
13. 用电缆将外部冗余交换机连接在一起。

NSRP 配置

在用电缆将 NetScreen 设备连接在一起和连接到周围的网络设备后，需要将它们配置为 HA。全部配置包括以下步骤：

1. 创建 NSRP 集群，它将自动创建 VSD 组 0 和启用 RTO 同步
2. 在集群中创建第二个 VSD 组

范例：双主动配置的 NSRP

在本例中，用 ID 1 创建 NSRP 集群并将两个 NetScreen 设备 （设备 A 和设备 B）命名为 “cluster1”，它们没有配置任何用户定义的其它设置。

注意：*为启用命令传播，必须先定义每个设备上的集群 ID 号。下列设置不能传播，并且必须在集群中的每个设备上进行配置：VSD 组、 VSD 优先级、认证和加密密码、接口监控、管理 IP 地址，以及 IP 跟踪设置。所有其它命令在集群中的设备间是可以传播的。*

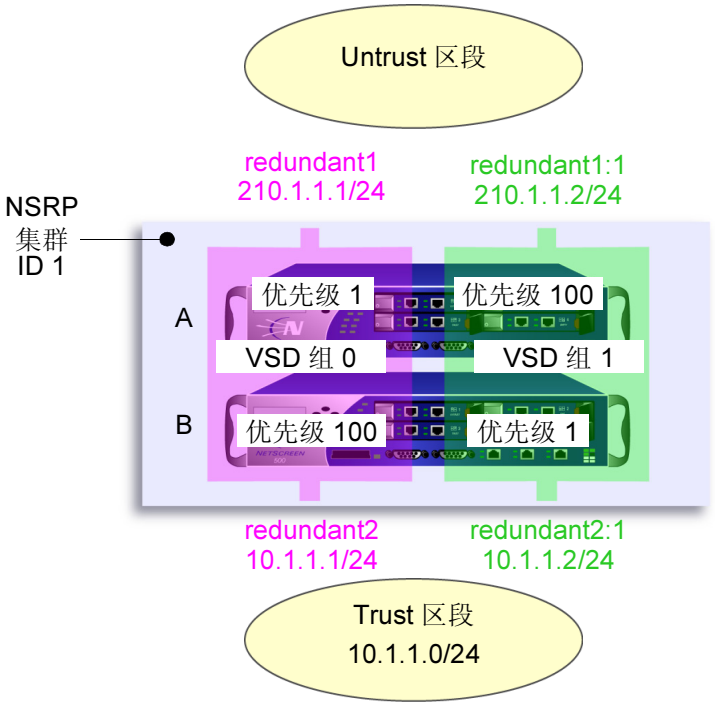
当创建了 NSRP 集群后， NetScreen 设备自动创建 VSD 组 0[18]。您可以定义 VSD 组 1。指定在 VSD 组 0 中设备 A 的优先级为 1，在 VSD 组 1 中优先级为 100 （缺省值）。指定在 VSD 组 1 中设备 A 的优先级为 1，在 VSD 组 0 中保留其优先级为缺省值 (100)。

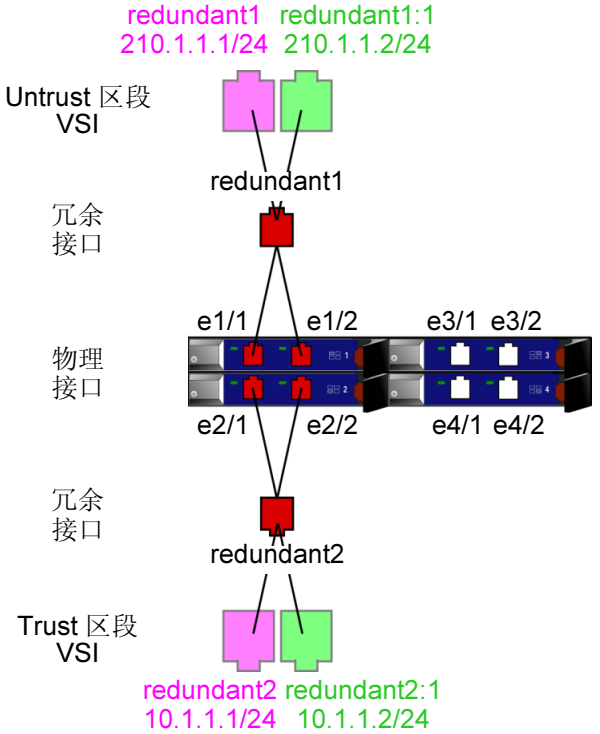
设置接口监控选项来监控所有绑定到冗余接口的物理接口，以保证第 2 层网络的连通性。如果任何被监控接口的任何主接口出现故障，该设备会立即切换到次接口。

也可以将 ethernet2/1 定义为 VSD 心跳信号消息的次链接，以及定义某设备发生 4 次故障切换后无偿的 ARP 数。因为 HA 电缆直接在两个 NetScreen 设备之间运行，所以 NSRP 集群成员之间的通信不需要认证和加密。

也可以为每个 Untrust 区段 VSI 设置一个到缺省网关 (210.1.1.250) 的路由，以及为每个 Trust 区段 VSI 设置一个到外部网络的路由。所有安全区段都在 trust-vr 路由域中。

18. VSD 组 ID “0”不会出现在 VSD 0 中的 VSI 名称中。 VSI 仅由 *redundant1* 就可以识别，而不需使用 *redundant1:0*。





Untrust区段中缺省网关的 IP 地址为 210.1.1.250。

在此显示的地址和配置对于两个 NetScreen 设备都是一样的。

唯一的不同就是管理 IP 地址。

在设备 A 上，管理 IP 为 10.1.1.21 而且是在 redundant2 接口上。

在设备 B 上，管理 IP 为 10.1.1.22 而且是在 redundant2 接口上。

WebUI (设备 A)

集群和 VSD 组

1. Network > Redundancy > Settings > Monitor Port Edit：选择以下内容，然后单击 **Apply**：
   ethernet1/1
   ethernet1/2
   ethernet2/1
   ethernet2/2
2. Network > Redundancy > Settings：输入以下内容，然后单击 **Apply**：
   Cluster ID: 1
   NSRP RTO Mirror Synchronization: （选择）
3. Network > Redundancy > VSD Group > Edit（对于 Group ID 0）：输入以下内容，然后单击 **OK**：
   Priority: 1
   Enable Preempt: （选择）
   Preempt Hold-Down Time (sec): 10[19]
4. Network > Redundancy > VSD Group > New：输入以下内容，然后单击 **OK**：
   Group ID: 1
   Priority: 100
   Enable Preempt: （清除）
   Preempt Hold-Down Time (s): 0

19. 抑制时间可以为 0 到 255 秒中的任何长度，有效的延迟故障切换可防止快速故障切换带来的混乱。

WebUI (设备 B)

集群和 VSD 组

5. Network > Redundancy > Settings > Monitor Port Edit：选择以下内容，然后单击 **Apply**：

   ethernet1/1

   ethernet1/2

   ethernet2/1

   ethernet2/2

6. Network > Redundancy > Settings：选择以下内容[20]，然后单击 **Apply**：

   Cluster ID: 1

   Secondary Link: ethernet2/1[21]

   Number of Gratuitous ARPs to Resend: 4[22]

   NSRP RTO Mirror Synchronization: （选择）

7. Network > Redundancy > VSD Group > New：输入以下内容，然后单击 **OK**：

   Group ID: 1

   Priority: 1

   Enable Preempt: （选择）

   Preempt Hold-Down Time (sec): 10

20. 可以通过 CLI 只设置集群名称。

21. 如果 HA1 和 HA2 链接都断开，则 VSD 心跳信号消息通过 Trust 区段中的 ethernet2/1 传递。

22. 此设置将指定当一个设备故障切换后，新 VSD 组的主设备会发送 4 个无偿的 ARP 封包来宣布 VSI 和虚拟 MAC 地址关联到新主设备。

冗余接口和管理 IP

8. Network > Interfaces > New Redundant IF：输入以下内容，然后单击 **OK**：

   Interface Name: redundant1

   Zone Name: Untrust

   IP Address/Netmask: 210.1.1.1/24

9. Network > Interfaces > Edit (对于 ethernet1/1)：在“As member of”下拉列表中选择 **redundant1**，然后单击 **OK**。
10. Network > Interfaces > Edit (对于 ethernet1/2)：在“As member of”下拉列表中选择 **redundant1**，然后单击 **OK**。
11. Network > Interfaces > New Redundant IF：输入以下内容，然后单击 **OK**：

    Interface Name: redundant2

    Zone Name: Trust

    IP Address/Netmask: 10.1.1.1/24

    Manage IP: 10.1.1.22

12. Network > Interfaces > Edit（对于 ethernet2/1）：在“As member of”下拉列表中选择 **redundant2**，然后单击 **OK**。
13. Network > Interfaces > Edit（对于 ethernet2/2）：在“As member of”下拉列表中选择 **redundant2**，然后单击 **OK**。

虚拟安全接口

14. Network > Interfaces > New VSI IF：输入以下内容，然后单击 **OK**：

    Interface Name: VSI Base: redundant1

    VSD Group: 1

    IP Address/netmask: 210.1.1.2/24

15. Network > Interfaces > New VSI IF：输入以下内容，然后单击 **OK**：
    Interface Name: VSI Base: redundant2
    VSD Group: 1
    IP Address/netmask: 10.1.1.2/24

路由

16. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：
    Network Address/Netmask: 0.0.0.0/0
    Gateway: （选择）
    Interface: redundant1
    Gateway IP Address: 210.1.1.250
17. Network > Routing > Routing Table > trust-vr New：输入以下内容，然后单击 **OK**：
    Network Address: 0.0.0.0/0
    Gateway: （选择）
    Interface: redundant1:1
    Gateway IP Address: 210.1.1.250

WebUI (设备 A)

管理 IP 地址

18. Network > Interfaces > Edit（对于 redundant2）：在 Manage IP 字段中输入 **10.1.1.21**，然后单击 **OK**。

CLI (设备 A)

集群和 VSD 组

1. set nsrp cluster id 1
2. set nsrp vsd-group id 0 preempt hold-down 10[23]
3. set nsrp vsd-group id 0 preempt
4. set nsrp vsd-group id 0 priority 1
5. set nsrp vsd-group id 1
6. set nsrp monitor interface ethernet1/1
7. set nsrp monitor interface ethernet1/2
8. set nsrp monitor interface ethernet2/1
9. set nsrp monitor interface ethernet2/2
10. set nsrp rto-mirror sync
11. set interface redundant2 manage-ip 10.1.1.3
12. save

23. 抑制时间可以为 0 到 255 秒中的任何长度，有效的延迟故障切换可防止快速故障切换带来的混乱。

CLI (设备 B)

集群和 VSD 组

1. set nsrp cluster id 1[24]
2. set nsrp cluster name cluster1
3. set nsrp rto-mirror sync
4. set nsrp vsd-group id 1 priority 1[25]
5. set nsrp vsd-group id 1 preempt hold-down 10[26]
6. set nsrp vsd-group id 1 preempt
7. set nsrp monitor interface ethernet1/1[27]
8. set nsrp monitor interface ethernet1/2
9. set nsrp monitor interface ethernet2/1
10. set nsrp monitor interface ethernet2/2
11. set nsrp secondary-path ethernet2/1[28]
12. set nsrp arp 4[29]
13. set arp always-on-dest[30]

---

24. 因为设备 A 和 B 同是一个 NSRP 集群的成员，所以在设备 B 上后续输入的所有命令 （除了另外注释）都将传播给设备 A。
25. 此命令不传播。
26. 此命令不传播。
27. **set nsrp monitor interface** *interface* 命令不传播。
28. 如果 HA1 和 HA2 链接都出错，则 VSD 心跳信号消息通过 Trust 区段中的 ethernet2/1 传递。
29. 此设置将指定当一个设备故障切换后，新 VSD 组的主设备会发送 4 个无偿的 ARP 封包来宣布 VSI 和虚拟 MAC 地址关联到新主设备。
30. 输入此命令后， NetScreen 设备总是执行 ARP 查找来获得目标 MAC 地址，而不是从原始以太网帧的源 MAC 中获得。本例中的外部路由器组成了一个运行 VRRP 的虚拟路由器。从此路由器发送来的帧使用虚拟 IP 地址作为源 IP，而不是用物理 MAC 地址作为源 MAC。如果该路由器故障切换且 NetScreen 设备从进入帧的源 MAC 中获得 MAC，则它将会把返回流量引导到错误位置。通过执行 ARP 查找获得目标 MAC，NetScreen 设备可以将流量正确发送到新的物理 MAC 地址所在的位置。

冗余接口和管理 IP

14. set interface redundant1 zone untrust
15. set interface redundant1 ip 210.1.1.1/24
16. set interface ethernet1/1 group redundant1
17. set interface ethernet1/2 group redundant1
18. set interface redundant2 zone trust
19. set interface redundant2 ip 10.1.1.1/24
20. set interface redundant2 manage-ip 10.1.1.22
21. set interface ethernet2/1 group redundant2
22. set interface ethernet2/2 group redundant2

虚拟安全接口

23. set interface redundant1:1 ip 210.1.1.2/24
24. set interface redundant2:1 ip 10.1.1.2/24

路由

25. set vrouter trust-vr route 0.0.0.0/0 interface redundant1 gateway 210.1.1.250
26. set vrouter trust-vr route 0.0.0.0/0 interface redundant1:1 gateway 210.1.1.250
27. save

CLI (设备 A)

管理 IP 地址

28. set interface redundant2 manage-ip 10.1.1.21
29. save

虚拟系统支持

如虚拟系统要故障切换，则它必须处于 VSD 组中。要使 VSD 组支持虚拟系统，必须为每个虚拟系统创建 VSI。一个虚拟系统有自己的 Trust 区段 VSI，并且它可以有自己的 Untrust 区段 VSI。虚拟系统还可以与根级共享 Untrust 区段 VSI。当虚拟系统具有自己的 Untrust 区段 VSI 时，它们必须彼此在不同的子网中，它们与根级的 Untrust 区段 VSI 也应该在不同的子网中。所有的 Trust 区段虚拟系统 VSI 也必须彼此在不同的子网中。

范例：虚拟系统间负载共享的 VSI

两个 NetScreen 设备（设备 A 和设备 B）处于双主动全网状配置中。您已经将设备 A 的根系统配置为 VSD 0 的主设备，设备 B 的根系统配置为 VSD 组 1 的主设备。根系统中的 VSD 0 和 1 的 Trust 和 Untrust 区段 VSI 如下所示：

VSD 组 0 的 VSI		VSD 组 1 的 VSI	
redundant1	210.1.1.1/24	redundant1:1	210.1.1.2/24
redundant2	10.1.1.1/24	redundant2:1	10.1.1.2/24

（有关根系统 VSD 组的完全配置，请参阅第 51 页上的 “范例：双主动配置的 NSRP”。）

在本例中，为 NSRP 配置了两个虚拟系统（vsys1 和 vsys2）。为了提供虚拟系统内向流量的负载共享[31]，VSD 的从属关系按如下方式分配：

- Vsys1 是 VSD 组 0 的成员。
- Vsys2 是 VSD 组 1 的成员。

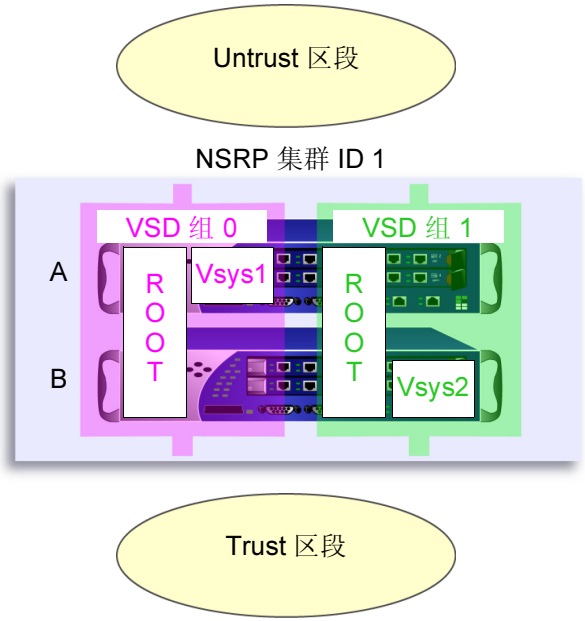
NetScreen 设备通过分配虚拟系统的 VSD 组来共享内向流量负载。因为初始设计中将 vsys1 配置在设备 A 上，vsys2 配置在设备 B 上，所以向这些虚拟系统发送的内向流量被引导到含有它们的设备。

31. 请注意，在本例中，负载不是均匀分配的；即负载不均衡。两个 NetScreen 设备共享负载，设备 A 和 B 以动态变化的比例（60/40%、70/30% 等等）接收内向流量。

根系统在 VSD 组 0 和 1 中，且在两个 NetScreen 设备中是活动的。

Vsys1 在 VSD 组 0 中，且仅在设备 A 中是活动的。

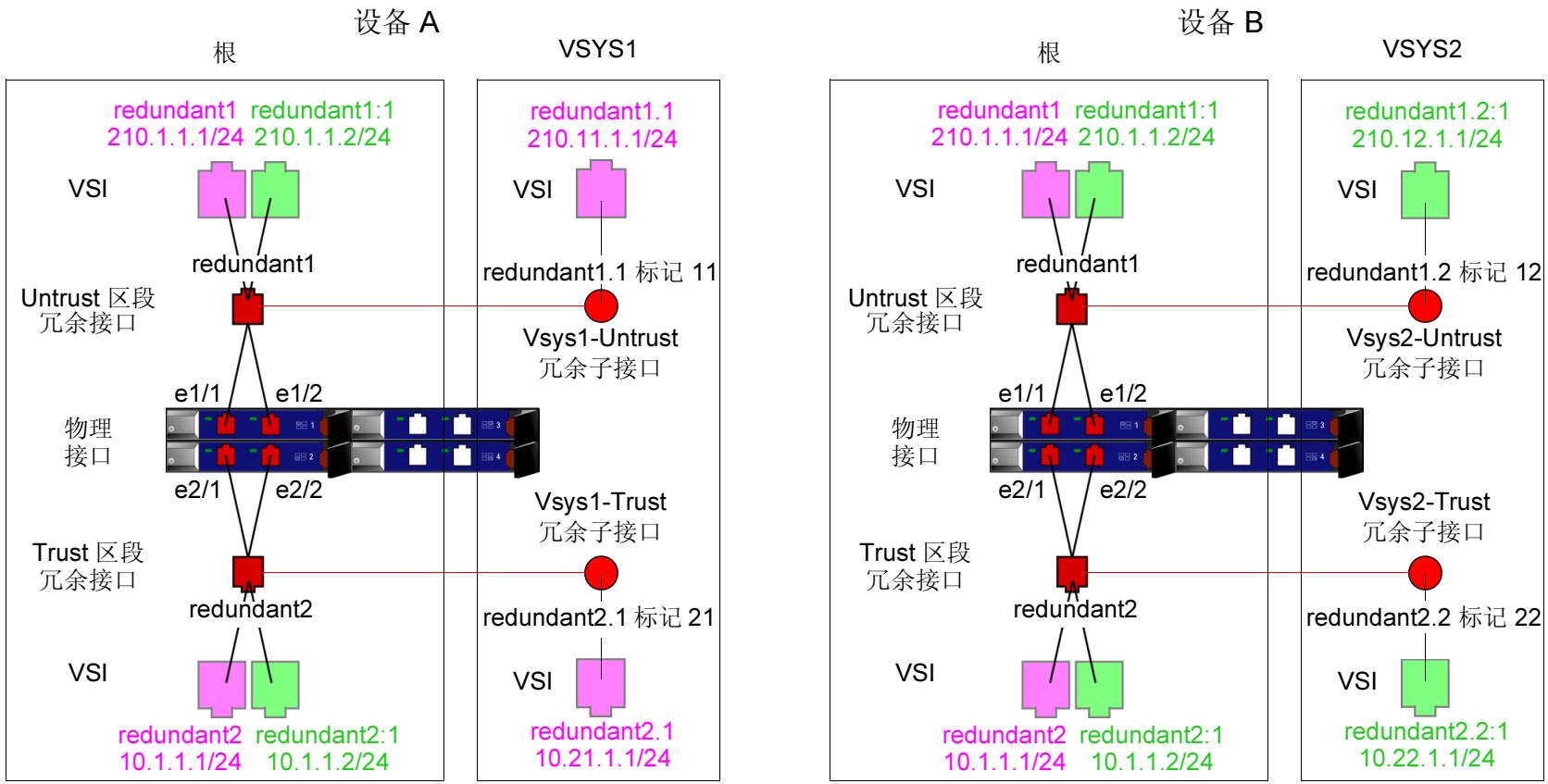
Vsys2 在 VSD 组 1 中，且仅在设备 B 中是活动的。



出站流量的缺省网关对于根系统和每个虚拟系统是不同的：

- Root: 210.1.1.250
- Vsys1: 210.11.1.250
- Vsys2: 210.12.1.250

因为本例是基于第 51 页上的 “范例：双主动配置的 NSRP” 的，在其中建立了 VSD 组 0 和 1，同时设置了 NSRP 集群 ID 1 中的设备，并且已经启用了 NSRP。所以，在设备 A 上配置的设置会自动传播给设备 B。



VSD 组 0 = 紫色 （注意：VSD 0 的 VSI 不显示它们的 VSD ID 号。）
VSD 组 1 = 绿色 （注意：VSD 1 的 VSI 用冒号 +1 表示它们的 VSD ID。）

WebUI

设备 A：根

> ***注意：****根系统的 NSRP 配置与第 51 页上的 “范例：双主动配置的 NSRP” 中的配置是一样的。*

设备 A：Vsys1

1. Vsys > New：输入以下内容，然后单击 **OK**：

   VSYS Name: vsys1[32]

2. Vsys > Enter (vsys1) > Network > Interface > New Sub-IF：输入以下内容，然后单击 **OK**：

   Interface Name: Redundant1.1

   Zone Name: Untrust

   VLAN Tag: 11

3. Network > Interfaces > New VSI-IF：输入以下内容，然后单击 **OK**：

   VSI Base: Redundant1.1

   VSD Group: 0

   IP Address/Netmask: 210.11.1.1/24

4. Network > Interfaces > New Sub-IF：输入以下内容，然后单击 **OK**：

   Interface Name: Redundant2.1

   Zone Name: Trust-vsys-vsys1

   VLAN Tag: 21

5. Network > Interfaces > New VSI-IF：输入以下内容，然后单击 **OK**：

   VSD Group ID: 0

   IP Address/Netmask: 10.21.1.1/24

   Interface Mode: Route[33]

32. 如果您没有定义 vsys admin，则 NetScreen 设备会自动创建一个，并在该 vsys 名称上添加 “vsys_”。在本例中， vsys1 的 vsys admin 为 vsys_vsys1。
33. 虚拟系统可以处于 “路由” 或 “NAT” 模式，而与您在根级设置的模式无关。

6. Network > Routing > Routing Table > untrust-vr New：输入以下内容，然后单击 **OK**：
   Network Address/Netmask: 0.0.0.0/0
   Gateway: （选择）
   Interface: Redundant1
   Gateway IP Address: 210.11.1.250
7. 单击 **Exit Vsys** 以返回根级。

设备 A：Vsys2

8. Vsys > New：输入以下内容，然后单击 **OK**：
   VSYS Name: vsys2
9. Vsys > Enter (vsys2) > Network > Interface > New Sub-IF：输入以下内容，然后单击 **OK**：
   Interface Name: Redundant1.2
   Zone Name: Untrust
   VLAN Tag: 12
10. Network > Interfaces > New VSI-IF：输入以下内容，然后单击 **OK**：
    VSI Base: Redundant1.2
    VSD Group: 1
    IP Address/Netmask: 210.12.1.1
11. Network > Interfaces > New Sub-IF：输入以下内容，然后单击 **OK**：
    Interface Name: Redundant2.2
    Zone Name: Trust-vsys-vsys2
    VLAN Tag: 22

12. Network > Interfaces > New VSI-IF：输入以下内容，然后单击 **OK**：

    VSD Group ID: 1

    IP Address/Netmask: 10.22.1.1/24

    Interface Mode: Route

13. Network > Routing > Routing Table > untrust-vr New：输入以下内容，然后单击 **OK**：

    Network Address/Netmask: 0.0.0.0/0

    Gateway: （选择）

    Interface: Redundant1(untrust-vr)

    Gateway IP Address: 210.12.1.250

14. 单击 **Exit Vsys** 以返回根级。

设备 B

注意：*因为设备 A 会将其它配置的设置传播给设备 B，所有就不必在设备 B 中再次输入它们。*

CLI

设备 A：根

注意：根系统的 NSRP 配置与第 51 页上的 “范例：双主动配置的 NSRP” 中的配置是一样的。

设备 A：VSYS 1

1. ns-> set vsys vsys1
2. ns(vsys1)-> set interface redundant1.1 tag 11 zone untrust
3. ns(vsys1)-> set interface redundant1.1 ip 210.11.1.1/24
4. ns(vsys1)-> set interface redundant2.1 tag 21 zone trust-vsys1
5. ns(vsys1)-> set interface redundant2.1 ip 10.21.1.1/24
6. ns(vsys1)-> set interface redundant2.1 route[34]
7. ns(vsys1)-> set vrouter untrust-vr route 0.0.0.0/0 interface redundant1 gateway 210.11.1.250
8. ns(vsys1)-> save
9. ns(vsys1)-> exit

设备 A：VSYS 2

10. ns-> set vsys vsys2
11. ns(vsys2)-> set interface redundant1.2 tag 12 zone untrust
12. ns(vsys2)-> set interface redundant1.2:1 ip 210.12.1.1/24
13. ns(vsys2)-> set interface redundant2.2 tag 22 zone trust-vsys2
14. ns(vsys2)-> set interface redundant2.2:1 ip 10.22.1.1/24

34. 虚拟系统可以处于 “路由” 或 “NAT” 模式，而与您在根级设置的模式无关。

15. ns(vsys2)-> set interface redundant2.2:1 route
16. ns(vsys2)-> set vrouter untrust-vr route 0.0.0.0/0 interface redundant1 gateway 210.12.1.250
17. ns(vsys2)-> save
18. ns(vsys2)-> exit

设备 B

注意：*因为设备 A 会将其它配置的设置传播给设备 B，所有就不必在设备 B 中再次输入它们。*

路径监控

路径监控将检查 NetScreen 接口和其它设备接口之间的第 2 层和第 3 层网络连接。路径监控对于在冗余组中的设备是很有用的工具，用它可以确定设备的网络连接是否可以接受。

第 2 层路径监控的功能是检查物理端口是否处于活动状态并连接到其它网络设备。要通过 WebUI 启用第 2 层路径监控，请单击 **Network > Redundancy > Settings > Monitor Port Edit**，然后选择接口。要通过 CLI 启用第 2 层路径监控，请使用下面的命令：**set nsrp monitor interface** *interface*。

第 3 层路径监控，或 IP 跟踪的功能是向最多 16 个指定的 IP 地址以用户确定的间隔发送 ping 或 ARP 要求，然后监控目标是否响应。如果一个主设备（不是其备份设备）的跟踪 IP 总故障数超过设备的故障切换临界值，则备份设备自动升为主设备，而主设备将进入不可操作状态。（不可操作的 VSD 组成员会继续其 IP 路径跟踪活动。当该结果不再超过故障切换临界值后，它会从不可操作状态转变为初始状态，然后变为备份状态[35]。）

注意：*当使用“虚拟路由器冗余协议 (VRRP)”将路由器分组到冗余集群中时，如果该路由器不是虚拟 IP 地址的所有者（故障切换后可能会出现此情况），则作为主设备的路由器不会对该 IP 地址的 ping 请求做出响应。但是，主设备虚拟路由器一定会以虚拟的 MAC 地址响应 ARP 请求，无论它是否是该 IP 地址的所有者。（有关详细信息，请参阅 RFC 2338。）要在 IP 跟踪时使用 ARP，则轮询设备必须与 NetScreen 管理 IP 地址处于同一物理子网中。*

在跟踪 IP 地址时，可以从物理接口、冗余接口或子网上的管理 IP 地址发送 ping 或 ARP 请求。请注意，不能用 VSI 进行 IP 跟踪，因为该地址可在多个设备中改变其绑定。

35. 如果 VSD 组处于抢先模式且该设备具有高于当前主设备的优先级，则它会从不可操作状态转变为初始状态然后成为主设备。

设置临界值

IP 路径跟踪包括两种临界值：跟踪的 IP 故障临界值和设备故障切换临界值。

跟踪的 IP 故障临界值 – 从指定的 IP 地址引发 ping 或 ARP 响应的连续故障数，其中要求考虑已失败的尝试。没有超过临界值表示该地址的连通性是可接受的；超过了临界值就表示不可接受。您可以为每个 IP 地址设置此临界值，它可以是 1 到 200 之间的任何值。缺省值是 3。

设备故障切换临界值 – 使 VSD 组主设备让位的累积失败尝试的总权重值。（有关如何为跟踪的 IP 地址分配权重的信息，请参阅下一部分，“对跟踪的 IP 地址加权”。）您可以将设备故障切换临界值设置为 1 到 255 之间的任何值。缺省值是 255。

对跟踪的 IP 地址加权

通过在跟踪的 IP 地址上应用加权，或加权值，可以调整该地址连通性的重要性 （与其它跟踪的地址相比） 。您可以给相对较重要的地址分配相对较大的权重，而给相对不重要的地址分配相对较小的权重。当达到跟踪的 IP 故障临界值时，所分配的权重开始起作用。例如，某地址的权重为 10，超过该地址 “跟踪的 IP 故障临界值”与超过权重为 1 地址的 “跟踪的 IP 故障临界值”相比，前者更容易使设备发生故障切换。可以分配 1 到 255 之间的权重。缺省值是 255。

范例：配置路径跟踪

两个 NetScreen 设备处于双主动配置。每隔 10 秒，对 Untrust 区段的冗余集群中运行 VRRP 的两个外部路由器，两个设备将向其物理 IP 地址[36] 发送 ARP 请求，对 Trust 区段中的两个 Web 服务器将发送 ping 请求。设备故障切换临界值为 51。权重和跟踪的 IP 故障临界值如下所示：

- Untrust 区段中的冗余路由器
  - 210.1.1.250 – weight: 16, threshold 5
  - 210.1.1.251 – weight: 16, threshold 5
- Trust 区段中的 Web 服务器
  - 10.1.1.30 – weight 10, threshold 3
  - 10.1.1.40 – weight 10, threshold 3

向其中一个路由器发出 5 次连续尝试后，如果没有收到 ARP 响应，则认为尝试失败，并且对于总故障切换临界值其权重值为 16。向其中一个 Web 服务器发出 3 次连续尝试后，如果没有收到 ping 响应，则认为尝试失败，并且对于总故障切换临界值其权重值为 10。

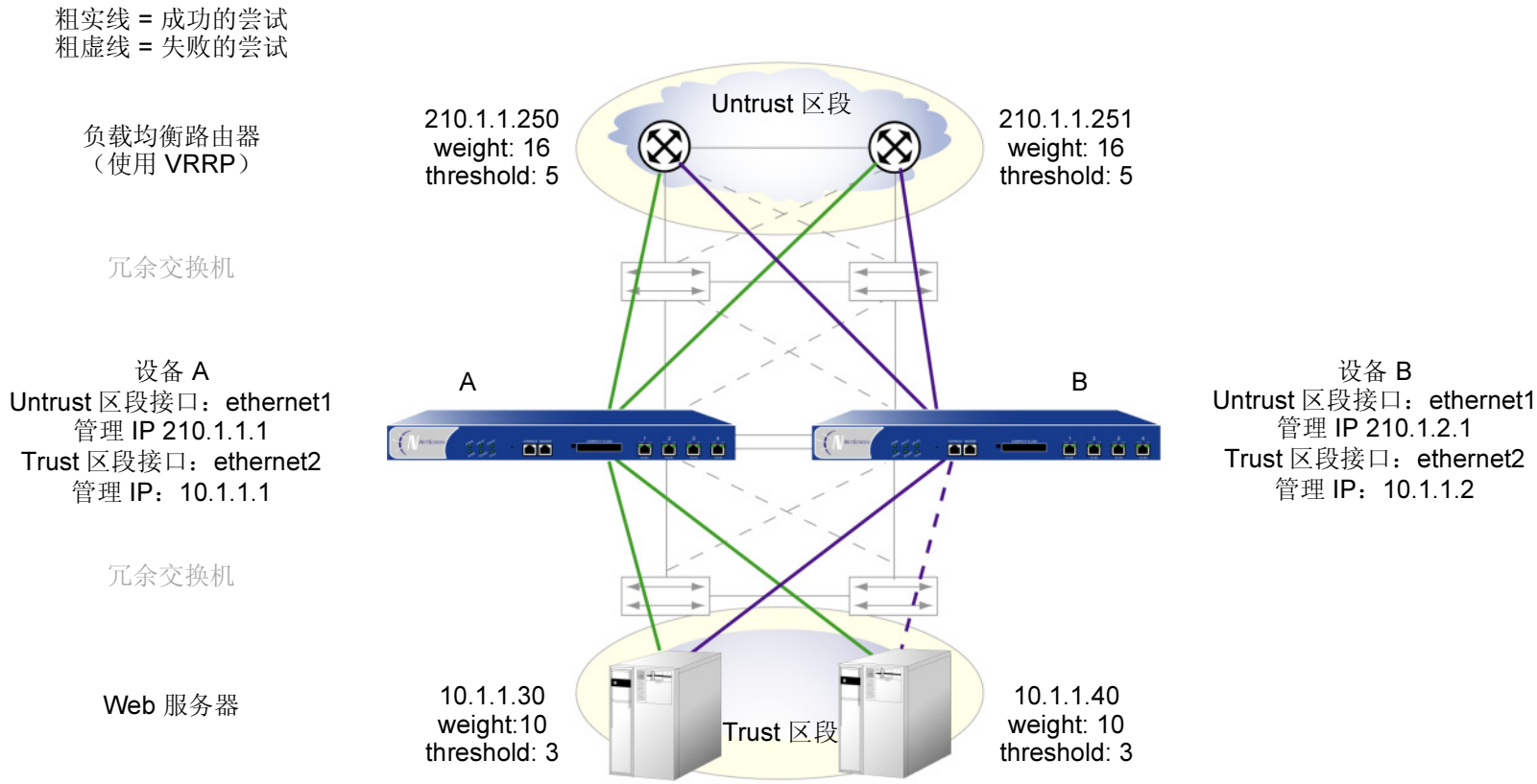
因为设备故障切换临界值为 51，所以发生设备切换前所有四个跟踪 IP 地址必须都出现故障。如果不能忍受这样多的故障，您可以把临界值降低到一个更容易接受的级别。

在本例中，设备 A 具有 100% 成功率，而设备 B 没有从 10.1.1.40 收到三个连续的响应，则相对于总故障临界值 51 它提供的值为 10。

注意：*IP 跟踪设置不会传播到 VSD 组中的其它设备。必须在组中的所有设备上输入相同的设置。*

在两个设备上， Untrust 区段接口为 ethernet1， Trust 区段接口为 ethernet2。在设备 A 上 ethernet1 的管理 IP 地址为 210.1.1.1，在设备 B 上为 210.1.1.2。在设备 A 上 ethernet2 的管理 IP 地址为 10.1.1.1，在设备 B 上为 10.1.1.2。所有的安全区段都在 trust-vr 路由域中。

36. 该物理 IP 地址为包含 VRRP 集群的物理路由器的专用地址。



WebUI

1. Network > Redundancy > Track IP > New：输入以下内容，然后单击 **OK**：

   Track IP: 210.1.1.250
   Method: ARP
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: ethernet1

2. Network > Redundancy > Track IP > New：输入以下内容，然后单击 **OK**：
   Track IP: 210.1.1.251
   Method: ARP
   Weight: 16
   Interval (sec): 10
   Threshold: 5
   Interface: ethernet1
3. Network > Redundancy > Track IP > New：输入以下内容，然后单击 **OK**：
   Track IP: 10.1.1.30
   Method: Ping
   Weight: 10
   Interval (sec): 10
   Threshold: 3
   Interface: ethernet2
4. Network > Redundancy > Track IP > New：输入以下内容，然后单击 **OK**：
   Track IP: 10.1.1.40
   Method: Ping
   Weight: 10
   Interval (sec): 10
   Threshold: 3
   Interface: ethernet2
5. Network > Redundancy > Track IP：选择 **Enable Track IP**，然后在 Failover Threshold 字段中输入 **51**。

CLI

1. set nsrp track-ip ip 210.1.1.250 interface ethernet1
2. set nsrp track-ip ip 210.1.1.250 interval 10
3. set nsrp track-ip ip 210.1.1.250 method arp
4. set nsrp track-ip ip 210.1.1.250 threshold 5
5. set nsrp track-ip ip 210.1.1.250 weight 16
6. set nsrp track-ip ip 210.1.1.251 interface ethernet1
7. set nsrp track-ip ip 210.1.1.251 interval 10
8. set nsrp track-ip ip 210.1.1.251 method arp
9. set nsrp track-ip ip 210.1.1.251 threshold 5
10. set nsrp track-ip ip 210.1.1.251 weight 16
11. set nsrp track-ip ip 10.1.1.30 interface ethernet2
12. set nsrp track-ip ip 10.1.1.30 interval 10
13. set nsrp track-ip ip 10.1.1.30 method ping[37]
14. set nsrp track-ip ip 10.1.1.30 threshold 3
15. set nsrp track-ip ip 10.1.1.30 weight 10
16. set nsrp track-ip ip 10.1.1.40 interface ethernet2
17. set nsrp track-ip ip 10.1.1.40 interval 10
18. set nsrp track-ip ip 10.1.1.40 method ping
19. set nsrp track-ip ip 10.1.1.40 threshold 3
20. set nsrp track-ip ip 10.1.1.40 weight 10
21. set nsrp track-ip threshold 51
22. set nsrp track-ip
23. save

37. 缺省情况下，IP 跟踪的方法是 ping 而跟踪的 IP 故障临界值为 3；所以，不需要指定它们。使用命令 **set nsrp track-ip ip 10.1.1.30** 和 **set nsrp track-ip ip 10.1.1.4S0** 就够了。

索引

Q

R

S

V

W

X

Y

Z