H3C SecPath M9000 系列多业务安全网关

开局指导书

目 录

1 简述

1.1 产品介绍

H3C SecPath M9000 系列多业务安全网关是 H3C 公司结合云计算、IPv6、大数据及高性能计算的发展趋势，针对云计算数据中心、运营商 CGN、大型企业及园区网出口等市场推出的新一代高性能多业务安全网关。

1.2 系统介绍

1.2.1 M9016-V 系列外观介绍

H3C SecPath M9000 系列多业务安全网关包括 M9000 产品（M9006、M9010、M9014 和 M9016-V 四款产品）、M9000-S 产品（M9008-S、M9012-S 和 M9008-S-V 三款产品）、M9000-AI-E 产品（M9000-AI-E16 和 M9000-AI-E8 两款产品）。在不区分具体型号时，后续章节统称为 M9000 系列设备。M9000 产品特指 M9006、M9010、M9014 和 M9016-V 四款产品，M9000-S 产品特指 M9008-S、M9012-S 和 M9008-S-V 三款产品。M9000-AI-E 产品特指 M9000-AI-E16 和 M9000-AI-E8 两款产品，下图 1-1 主要介绍 M9016-V 的设备外观。

图1-1 M9016-V 设备外观

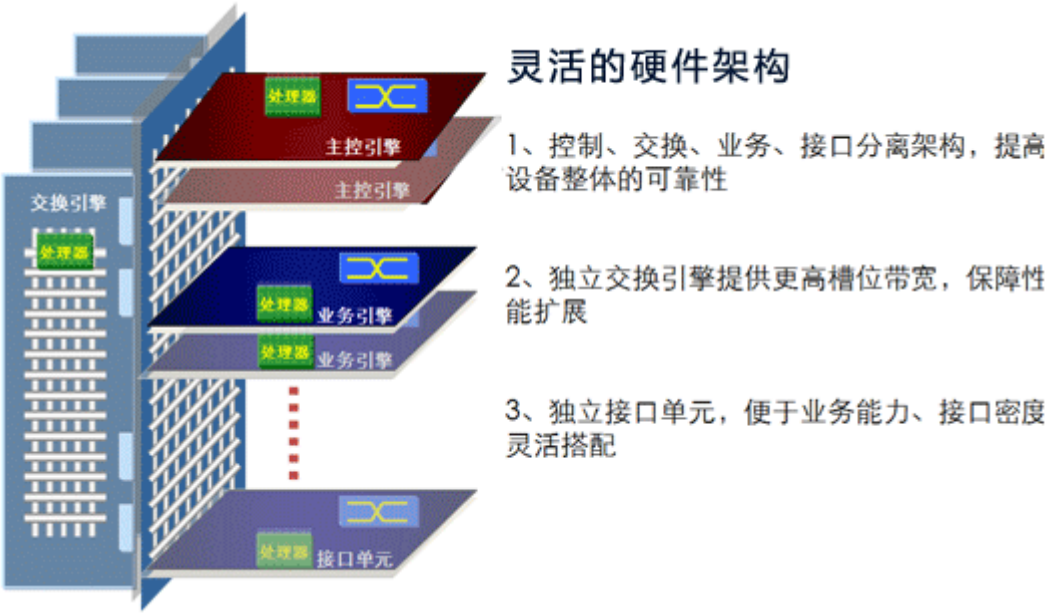
M9000/M9000-AI-E 产品主要由主控板区、接口板和业务板区、网板区、电源区、风扇区等几个部分组成，M9000-S 产品主要由主控板区、接口板和业务板区、电源区、风扇区等几个部分组成。

1.2.2 系统结构介绍

H3C SecPath M9000 系列多业务安全网关充分考虑网络应用对高可靠性的要求，采用领先的多核全分布式架构。主控引擎 1+1 冗余，提供整机统一配置管理，支持安全集群；业务引擎和接口单元支持混插，可以根据性能需求灵活进行选择；风扇模块冗余，风扇框支持风扇状态监控，风扇支持无级调速，可以根据环境温度、单板配置自动分组调速；电源模块 M+N 备份，交、直流电源模块支持热插拔，多电源模块负载分担，可灵活根据系统功耗配置模块数量，保证模块高效工作。设备所有单元均支持热插拔，充分满足网络维护、升级、优化的需求。

M9000 采用控制、业务、数据相分离的全分布式架构，控制引擎、交换引擎、业务引擎及接口单元硬件分离，解耦合系统关键部件，提高系统可靠性；独立的硬件交换引擎，支撑高性能安全业务无阻塞处理及转发。 独立的高性能控制引擎，实现系统统一配置管理和安全集群。

图1-2 硬件架构



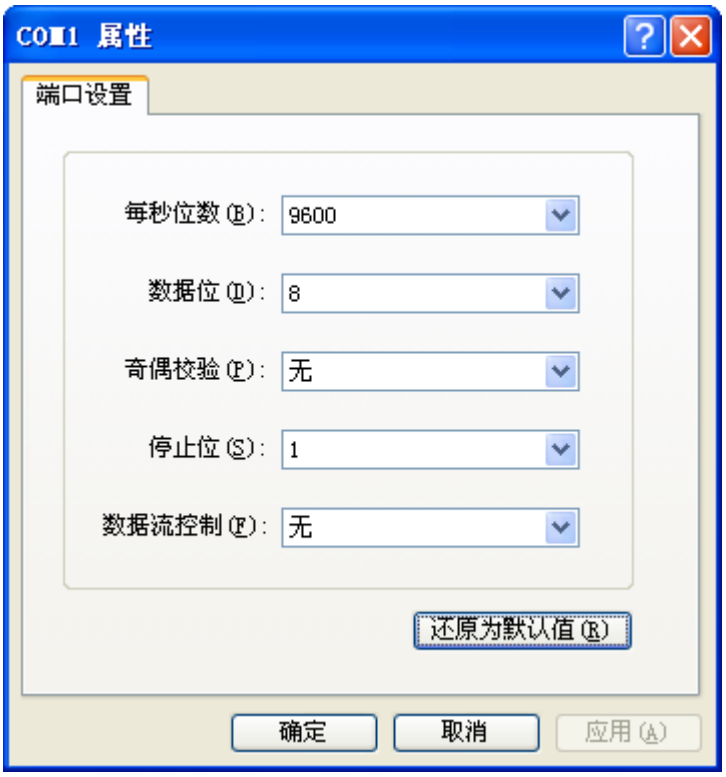
内置模块化软件系统，支持多进程的调度，进程间运行空间隔离，单个进程的异常不会影响系统其他部分，提高系统可靠性；支持权限管理功能，基于特性、命令行、系统资源、WEB 管理等级别定义用户读写权限，提高系统安全性；支持热补丁，不中断业务的情况下实现系统升级，提高系统易用性。

1.2.3 M9000 的管理

M9000 目前支持命令行管理，命令行可以提供全面的配置、信息查看、故障诊断等。

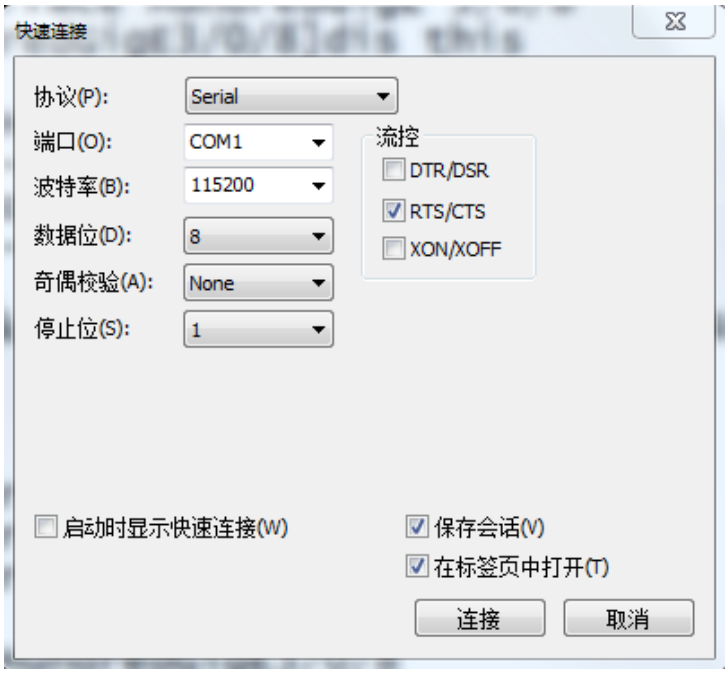
如 1-3 所示，M9000 主控板自带 Console 口，可以用串口线对 M9000 进行管理，其串口参数与管理 H3C 主网络设备设置相同。

图1-3 主控串口参数设置



在 M9000 中，业务板也有 Console 口，可以连接该 Console 口，对整台设备进行管理。在业务板启动过程中，业务板 Console 口显示的业务板的启动信息。M9016-V 的业务卡 NSQM1FWEFGA0 的业务卡串口波特率为 115200。

图1-4 业务卡串口参数设置



对业务板的 Console 口，主要用于业务板启动信息的查看，当业务板完全启动后，显示的信息为和主控板上的信息完全相同，为 M9000 的统一管理信息。

建议 Console 口采用主控板的 Console 口信息。

2 M9016-V 系列的硬件和版本升级

2.1 硬件说明

M9000 产品主要由主控板区、接口板、业务板区、网板区、电源区、风扇区等几个部分组成。下面两张图显示的是 M9016-V 的机箱的区域说明：

图2-1 M9016-V 前、后面板示意图

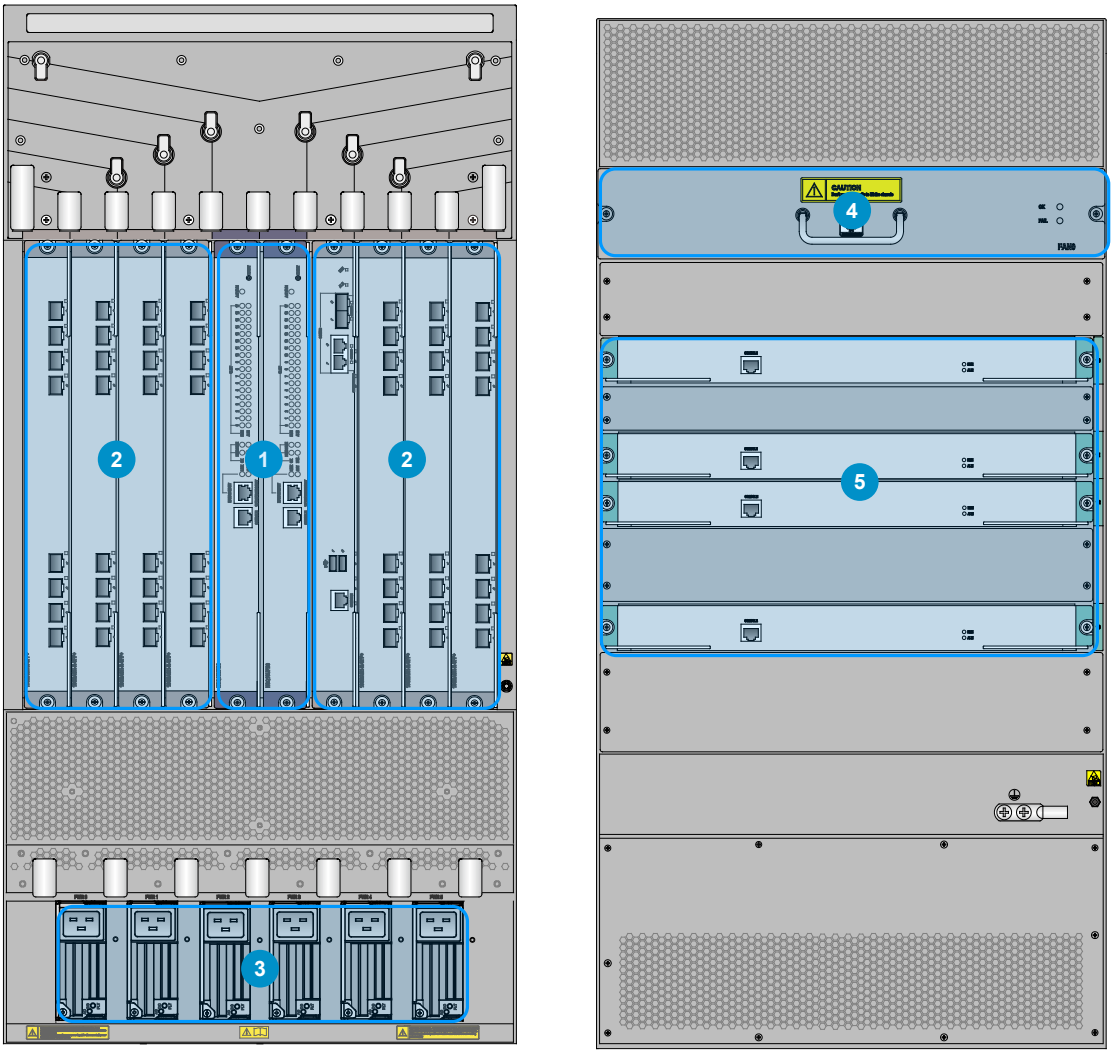


表2-1 机箱各区域说明

说明区域	区域说明	选配情况
①主控板区	安装主控板的槽位	主控板必配（机箱发货时不带主控板）
②接口板和业务板区	安装接口板或者业务板的槽位	接口板和业务板必配（机箱发货时不带接口板和业务板） 支持多种类型的接口板和业务板，请根据实际业务需求进行选择
③电源区	安装电源模块的槽位	电源模块必配（机箱发货时不带电源模块） • M9016-V 具有 6 个电源模块插槽
④风扇区	安装散热风扇框的槽位，位于机箱背面	风扇框必配（机箱发货时已安装好相应风扇框） • M9016-V：风扇框位于机箱背面的上方

说明区域	区域说明	选配情况
⑤网板区	安装交换网板的槽位	网板必配（机箱发货时不带网板） 每个机箱至少要配3块网板，最多可配置4块网板，并且要求编号最小的两个网板槽位中必须安装网板： • M9016-V 的 10 和 11 槽位必须安装网板

表2-2 M9016-V 产品支持的插卡

单板名称	单板类型	单板印丝名称
NSQM1SUPD0	主控板	NSQM1SUPD0
NSQM1FAB08E0	网板	NSQM1FAB08E0
NSQM1FWEFGA0	防火墙业务板	NSQM1FWEFGA0
NSQM1CGQ4TG24SHA0	接口卡	NSQM1CGQ4TG24SHA0

2.2 版本升级的内容

对 M9000 版本，要升级 2 个版本，主控版本和业务板软件版本。这两个版本要单独通过命令行升级。在升级时，需要指定主控、业务板所在的槽位号。下面以 M9016-V 为例，介绍升级过程。

2.3 M9016-V主控升级过程

- 在 V7 Comware 系统下升级，升级过程如下：

(1)首先把主控的.ipe 文件上传到业务卡 flash。上传操作可以通过 ftp 或者 tftp。

(2)上传成功后，设置该文件为某槽位主控的系统文件，如下：

```
<M9016-V>boot-loader file slot8.1#flash:/M9000.ipe slot 4 main
Verifying the file flash:/M9000.ipe on slot 8.1.............................Do
ne.
H3C SecPath M9016-V images in IPE:
  M9000-CMW710-BOOT-F9153P17.bin
  M9000-CMW710-SYSTEM-F9153P17.bin
This command will set the main startup software images. Please do not reboot any
 MPU during the upgrade. Continue? [Y/N]:y
Add images to slot 4.
Decompressing file M9000-CMW710-BOOT-F9153P17.bin to flash:/M9000-CMW710-BOOT-F9
153P17.bin.........................................Done.
Decompressing file M9000-CMW710-SYSTEM-F9153P17.bin to flash:/M9000-CMW710-SYSTE
M-F9153P17.bin.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.Done.
Verifying the file flash:/M9000-CMW710-BOOT-F9153P17.bin on slot 4....Done.
Verifying the file flash:/M9000-CMW710-SYSTEM-F9153P17.bin on slot 4............
.......Done.
```

```
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 4.
Decompression completed.
You are recommended to delete the .ipe file after you set startup software image
s for all slots.
Do you want to delete flash:/M9000.ipe now? [Y/N]:N
```

2.4 M9016-V业务板升级过程

- 在 V7 Comware 系统下升级：

(1)首先把业务板的.ipe 文件上传到业务卡 flash。上传操作可以通过 ftp 或者 tftp。

(2)上传成功后，设置该文件为某槽位业务板的系统文件，如下：

```
<M9016-V>boot-loader file slot8.1#flash:/M9000_fw5.ipe slot 8 cpu  1 main
Verifying the file flash:/M9000_fw5.ipe on slot 8.1..................Done.
Blade5fw images in IPE:
  BLADE5FWM9000-CMW710-BOOT-F9153P17.bin
  BLADE5FWM9000-CMW710-SYSTEM-F9153P17.bin
This command will set the main startup software images. Please do not reboot any
 MPU during the upgrade. Continue? [Y/N]:y
Add images to slot 8.1.
Decompressing file BLADE5FWM9000-CMW710-BOOT-F9153P17.bin to slot8.1#flash:/BLAD
E5FWM9000-CMW710-BOOT-F9153P17.bin....Done.
Decompressing file BLADE5FWM9000-CMW710-SYSTEM-F9153P17.bin to slot8.1#flash:/BL
ADE5FWM9000-CMW710-SYSTEM-F9153P17.bin.....................................
.....................Done.
Verifying the file flash:/BLADE5FWM9000-CMW710-BOOT-F9153P17.bin on slot 8.1...D
one.
Verifying the file flash:/BLADE5FWM9000-CMW710-SYSTEM-F9153P17.bin on slot 8.1..
.............Done.
The images that have passed all examinations will be used as the main startup so
ftware images at the next reboot on slot 8.1.
Decompression completed.
You are recommended to delete the .ipe file after you set startup software image
s for all slots.
Do you want to delete flash:/M9000_fw5.ipe now? [Y/N]:n
```

(3)加载版本完成后，检查版本是否是加载的版本，如下：

```
<M9016-V>display boot-loader

Software images on slot 4:

Current software images:

  flash:/M9000-CMW710-BOOT-E9153P1216.bin

  flash:/M9000-CMW710-SYSTEM-E9153P1216.bin

Main startup software images:

  flash:/M9000-CMW710-BOOT-F9153P17.bin

  flash:/M9000-CMW710-SYSTEM-F9153P17.bin

Backup startup software images:
```

```
  None
Software images on slot 5:
Current software images:
  flash:/M9000-CMW710-BOOT-E9153P1216.bin
  flash:/M9000-CMW710-SYSTEM-E9153P1216.bin
Main startup software images:
  flash:/M9000-CMW710-BOOT-F9153P17.bin
  flash:/M9000-CMW710-SYSTEM-F9153P17.bin
Backup startup software images:
  None
Software images on slot 8.1:
Current software images:
  flash:/BLADE5FWM9000-CMW710-BOOT-E9153P1216.bin
  flash:/BLADE5FWM9000-CMW710-SYSTEM-E9153P1216.bin
Main startup software images:
  flash:/BLADE5FWM9000-CMW710-BOOT-F9153P17.bin
  flash:/BLADE5FWM9000-CMW710-SYSTEM-F9153P17.bin
Backup startup software images:
  None
Software images on slot 9.1:
Current software images:
  flash:/BLADE5FWM9000-CMW710-BOOT-E9153P1216.bin
  flash:/BLADE5FWM9000-CMW710-SYSTEM-E9153P1216.bin
Main startup software images:
  flash:/BLADE5FWM9000-CMW710-BOOT-F9153P17.bin
  flash:/BLADE5FWM9000-CMW710-SYSTEM-F9153P17.bin
Backup startup software images:
  None
```

(4)重启设备，变为升级以后的版本，检查版本信息如下。

```
[M9016-V]dis version
H3C Comware Software, Version 7.1.064, Feature 9153P17
Copyright (c) 2004-2020 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath M9016-V uptime is 0 weeks, 0 days, 0 hours, 11 minutes
Last reboot reason : User reboot

Boot image: flash:/M9000-CMW710-BOOT-F9153P17.bin
Boot image version: 7.1.064, Feature 9153P17
  Compiled Jul 17 2020 14:00:00
System image: flash:/M9000-CMW710-SYSTEM-F9153P17.bin
System image version: 7.1.064, Feature 9153P17
```

```
  Compiled Jul 17 2020 14:00:00


LPU 0:
Uptime is 0 weeks,0 days,0 hours,7 minutes
H3C SecPath M9016-V LPU with 1 LS1043A Processor
BOARD TYPE:         NSQM1CGQ4TG24SHA0
DRAM:               2048M bytes
PCB 1 Version:      VER.A
Bootrom Version:    108
CPLD 1 Version:     002
CPLD 2 Version:     001
Release Version:    H3C SecPath M9016-V-9153P17
Patch Version  :    None
Reboot Cause   :    UserReboot

LPU 1:
Uptime is 0 weeks,0 days,0 hours,7 minutes
H3C SecPath M9016-V LPU with 1 LS1043A Processor
BOARD TYPE:         NSQM1CGQ4TG24SHA0
DRAM:               2048M bytes
PCB 1 Version:      VER.A
Bootrom Version:    108
CPLD 1 Version:     002
CPLD 2 Version:     001
Release Version:    H3C SecPath M9016-V-9153P17
Patch Version  :    None
Reboot Cause   :    UserReboot

MPU(M) 4:
Uptime is 0 weeks,0 days,0 hours,11 minutes
H3C SecPath M9016-V MPU(M) with 1 XLP316 Processor
BOARD TYPE:         NSQM1SUPD0
DRAM:               8192M bytes
FLASH:              500M bytes
NVRAM:              512K bytes
PCB 1 Version:      VER.A
Bootrom Version:    132
CPLD 1 Version:     004
CPLD 2 Version:     003
CPLD 3 Version:     003
Release Version:    H3C SecPath M9016-V-9153P17
Patch Version  :    None
Reboot Cause   :    UserReboot

MPU(S) 5:
Uptime is 0 weeks,0 days,0 hours,11 minutes
H3C SecPath M9016-V MPU(S) with 1 XLP316 Processor
```

```
BOARD TYPE:         NSQM1SUPD0
DRAM:               8192M bytes
FLASH:              500M bytes
NVRAM:              512K bytes
PCB 1 Version:      VER.A
Bootrom Version:    132
CPLD 1 Version:     003
CPLD 2 Version:     003
CPLD 3 Version:     003
Release Version:    H3C SecPath M9016-V-9153P17
Patch Version  :    None
Reboot Cause   :    UserReboot

LPU 8:
Uptime is 0 weeks,0 days,0 hours,6 minutes
H3C SecPath M9016-V LPU with 1 XLP308 Processor
BOARD TYPE:         NSQM1FWEFGA0
DRAM:               2048M bytes
FLASH:              8M bytes
PCB 1 Version:      VER.A
PCB 2 Version:      VER.A
Bootrom Version:    100
CPLD 1 Version:     001
CPLD 2 Version:     002
Release Version:    H3C SecPath M9016-V-9153P17
Patch Version  :    None
Reboot Cause   :    UserReboot
SLOT 8 CPU 1
CPU type:           Multi-core CPU
DDR4 :              49152M bytes
FLASH:           7122M bytes
Board PCB Version:  Ver.A
CPLD Version:       5.0
Release Version:    SecBlade FW Enhanced-9153P17
FPGA 0 Version:     B50506
FPGA 0 DATE:        2020.07.21
FPGA 1 Version:     B50506
FPGA 1 DATE:        2020.07.21
Basic  BootWare Version:1.04
Extend BootWare Version:1.04

LPU 9:
Uptime is 0 weeks,0 days,0 hours,6 minutes
H3C SecPath M9016-V LPU with 1 XLP308 Processor
BOARD TYPE:         NSQM1FWEFGA0
DRAM:               2048M bytes
FLASH:              8M bytes
PCB 1 Version:      VER.A
```

```
PCB 2 Version:      VER.A
Bootrom Version:    100
CPLD 1 Version:     002
CPLD 2 Version:     002
Release Version:    H3C SecPath M9016-V-9153P17
Patch Version  :    None
Reboot Cause   :    UserReboot
SLOT 9 CPU 1
CPU type:           Multi-core CPU
DDR4 :              49152M bytes
FLASH:           7122M bytes
Board PCB Version:  Ver.A
CPLD Version:       5.0
Release Version:    SecBlade FW Enhanced-9153P17
FPGA 0 Version:     B50506
FPGA 0 DATE:        2020.07.21
FPGA 1 Version:     B50506
FPGA 1 DATE:        2020.07.21
Basic  BootWare Version:1.04
Extend BootWare Version:1.04

NPU 10:
Uptime is 0 weeks,0 days,0 hours,8 minutes
H3C SecPath M9016-V NPU with 1 XLS208 Processor
BOARD TYPE:         NSQM1FAB08E0
DRAM:               1024M bytes
PCB 1 Version:      VER.B
Bootrom Version:    511
CPLD 1 Version:     005
Release Version:    H3C SecPath M9016-V-9153P17
Patch Version  :    None
Reboot Cause   :    UserReboot

NPU 11:
Uptime is 0 weeks,0 days,0 hours,8 minutes
H3C SecPath M9016-V NPU with 1 XLS208 Processor
BOARD TYPE:         NSQM1FAB08E0
DRAM:               1024M bytes
PCB 1 Version:      VER.B
Bootrom Version:    518
CPLD 1 Version:     005
Release Version:    H3C SecPath M9016-V-9153P17
Patch Version  :    None
Reboot Cause   :    UserReboot

NPU 12:
Uptime is 0 weeks,0 days,0 hours,8 minutes
H3C SecPath M9016-V NPU with 1 XLS208 Processor
```

```
BOARD TYPE:          NSQM1FAB08E0
DRAM:                1024M bytes
PCB 1 Version:       VER.B
Bootrom Version:     518
CPLD 1 Version:      005
Release Version:     H3C SecPath M9016-V-9153P17
Patch Version   :    None
Reboot Cause    :    UserReboot

NPU 13:
Uptime is 0 weeks,0 days,0 hours,8 minutes
H3C SecPath M9016-V NPU with 1 XLS208 Processor
BOARD TYPE:          NSQM1FAB08E0
DRAM:                1024M bytes
PCB 1 Version:       VER.B
Bootrom Version:     518
CPLD 1 Version:      005
Release Version:     H3C SecPath M9016-V-9153P17
Patch Version   :    None
Reboot Cause    :    UserReboot
```

2.5 注意事项

- 如果系统为双主控，另外一块主控需要单独设置。如另外一块主控在 slot 5，则应键入命令：boot-loader file flash:/m9000.ipe slot 5 main。也可以同时设置两块主控，设置如下：boot-loader file flash:/m9000.ipe all main。
- 如果设备有多块业务板卡，需要对每一块业务板卡升级且 slot 号要设置正确。

3 防火墙基础配置

3.1 防火墙的几个基本概念

3.1.1 安全域

防火墙作为网络安全设备，按照业务的重要性高低，将网络分为若干个安全域，安全域以防火墙接口为边界。引入安全域的概念之后，安全管理员将安全需求相同的接口进行分类（划分到不同的安全域），能够实现策略的分层管理。

目前，M9000 系列的缺省安全域为 Management、Local、Trust、Untrust、DMZ 域。默认管理接口属于 Management 安全域中，并且 Management 域与 Local 域默认双向放通。

创建安全域后，设备上各接口的报文转发遵循以下规则：

- 一个安全域中的接口与一个不属于任何安全域的接口之间的报文，会被丢弃。
- 属于同一个安全域的各接口之间的报文缺省会被丢弃。
- 安全域之间的报文由安全策略进行安全检查，并根据检查结果放行或丢弃。若安全策略不存在或不生效，则报文会被丢弃。

- 非安全域的接口之间的报文被丢弃。
- 目的地址或源地址为本机的报文，缺省会被丢弃，若该报文与安全策略匹配，则由安全策略进行安全检查，并根据检查结果放行或丢弃。

3.1.2 流和会话

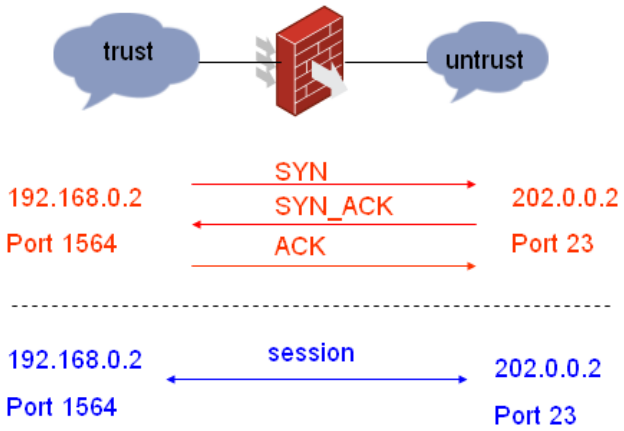
流（Flow）是一个单方向的概念，根据报文所携带的三元组或者五元组唯一标识。根据 IP 层协议的不同，流分为四大类：

- TCP 流：通过五元组唯一标识。
- UDP 流：通过五元组唯一标识。
- ICMP 流：通过三元组 + ICMP type + ICMP code 唯一标识。
- RAW IP 流：不属于上述协议，通过三元组标识。

会话（Session）是一个双向的概念，一个会话通常关联两个方向的流，一个为会话发起方（Initiator），另外一个为会话响应方（Responder）。通过会话所属的任一方向的流特征都可以唯一确定该会话以及方向。

对于 TCP/UDP/ICMP/RAW IP 流，首包进入防火墙时开始创建会话，后续相同的报文或者返回报文可以匹配该会话。以 TCP 三次握手为例：

图3-1 会话建立



如图 3-1 所示，Trust 域的 192.168.0.2:1564 访问 Untrust 域的 202.0.0.2 的 23 端口，首包 syn 报文开始创建一个双向会话（192.168.0.2:1564<---->202.0.0.2:23），后续 SYN_ACK 和 ACK 报文都匹配到此会话后，完整的会话创建完成。后续数据流如果匹配到此会话则放行通过。

4 M9000 系列多业务安全网关的远程管理概述

对 M9000 系列设备，可以通过 Telnet、SSH、MIB 进行远程管理。缺省情况下，系统是无法通过 Telnet 远程登录的。系统默认的启动配置如下：

- 缺省用户为 admin,密码 admin。
- 终端 VTY 用户登录方式为 password 方式，但是没有设置登录 password。
- Telnet、SSH、SNMP 服务关闭。

- 管理口默认绑定 management vpn-instance，存在默认地址。
- 管理口默认加入 management 域中，management 域与 local 域默认双向放通。
- 默认没有任何安全策略，除了 management 域与 local 域互通外，其他域间流量全部禁止。

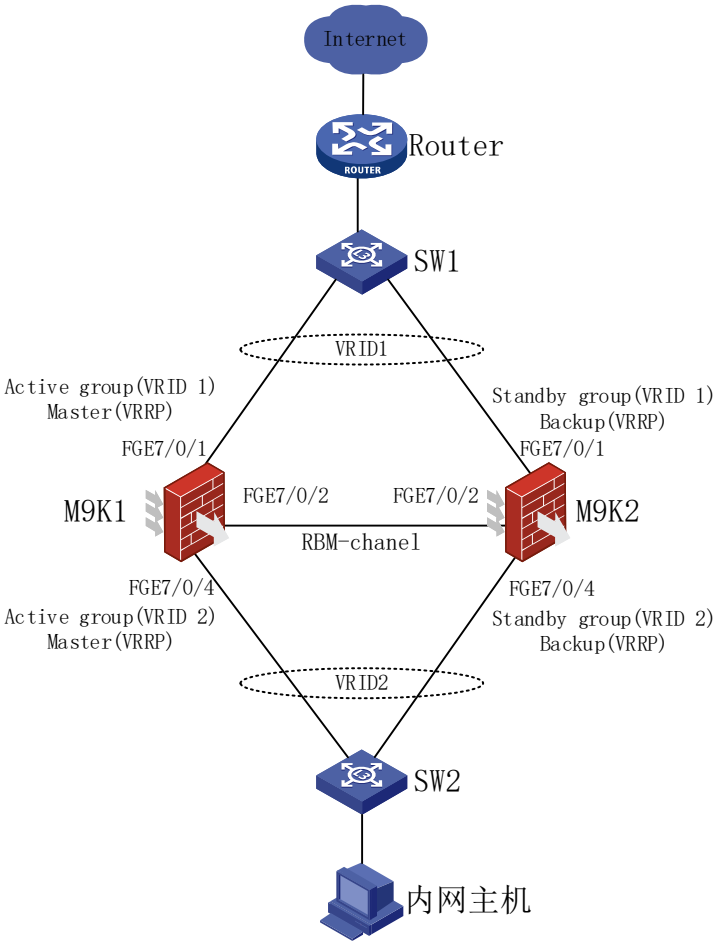
5 典型组网

5.1 M9000 VRRP+RBM主备组网基本功能

5.1.1 组网需求

如图 5-1 所示，2 台 M9K 通过三层口连接到内部网络和外部网络，防火墙分别和上下行交换机连接。

图5-1 VRRP+RBM 主备组网基本功能组网图



5.1.2 配置思路

- 配置接口地址并加入安全域，保证传输可达。
- 配置 RBM 组，包含控制通道和数据通道，备份模式等信息。

- 配置 VRRP 备份组。

5.1.3 配置步骤

(1) 确保主备设备的软硬件环境一致。

在配置远端备份管理功能之前，请先保证主/备设备的硬件环境和软件环境的一致性。

(2) 配置 M9K1

配置接口 IP 地址,将接口加入安全域。

```
[M9K1]interface FortyGigE 7/0/2
[M9K1-FortyGigE7/0/2]ip address 11.1.1.1 255.255.255.0
[M9K1]interface FortyGigE 7/0/1
[M9K1-FortyGigE7/0/1]ip address 20.1.1.1 255.255.255.0
[M9K1]interface FortyGigE 7/0/4
[M9K1-FortyGigE7/0/4]ip address 30.1.1.1 255.255.255.0
[M9K1]security-zone name Untrust
[M9K1-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K1]security-zone name Trust
[M9K1-security-zone-Trust]import interface FortyGigE7/0/4
[M9K1]security-zone name RBM
[M9K1-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[M9K1]security-policy ip
[M9K1-security-policy-ip]rule name Trust-Untrust
[M9K1-security-policy-ip-0-Trust-Untrust]source-zone Trust
[M9K1-security-policy-ip-0-Trust-Untrust]destination-zone Untrust
[M9K1-security-policy-ip-0-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功。

```
[M9K1]security-policy ip
[M9K1-security-policy-ip]rule name Local-RBM
[M9K1-security-policy-ip-1-Local-RBM]source-zone Local
[M9K1-security-policy-ip-1-Local-RBM]destination-zone RBM
[M9K1-security-policy-ip-1-Local-RBM]action pass
[M9K1-security-policy-ip]rule name RBM-Local
[M9K1-security-policy-ip-2-RBM-Local]source-zone RBM
[M9K1-security-policy-ip-2-RBM-Local]destination-zone Local
[M9K1-security-policy-ip-2-RBM-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.2，端口号使用默认的 66064。

```
[M9K1]remote-backup group
[M9K1-remote-backup-group]remote-ip 11.1.1.2
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.1。

```
[M9K1-remote-backup-group]local-ip 11.1.1.1
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K1-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为主管理设备。

```
[M9K1-remote-backup-group]device-role primary
```

配置 RBM 双机热备的模式为主备模式。（默认是主备模式）

```
[M9K1-remote-backup-group]undo backup-mode
```

开启 RBM 热备功能。

```
[M9K1-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K1-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K1-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 1 分钟。

```
[M9K1-remote-backup-group]delay-time 1
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/1 建 VRRP 备份组 1，其虚拟 IP 地址为 20.1.1.3，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]vrrp vrid 1 virtual-ip 20.1.1.3 active
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/4 创建 VRRP 备份组 2，其虚拟 IP 地址为 30.1.1.3，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/4
[M9K1-FortyGigE7/0/4]vrrp vrid 2 virtual-ip 30.1.1.3 active
```

若存在 HTTP 或 DNS 应用协议的流量，还需开启对应的会话备份功能。

```
<M9K1>system
[M9K1]session synchronization http
[M9K1]session synchronization dns
```

(3) 配置 M9K2

配置接口 IP 地址, 将接口加入安全域。

```
[M9K2]interface FortyGigE 7/0/2
[M9K2-FortyGigE7/0/2] ip address 11.1.1.2 255.255.255.0
[M9K2]interface FortyGigE 7/0/1
[M9K2-FortyGigE7/0/1] ip address 20.1.1.2 255.255.255.0
[M9K2]interface FortyGigE 7/0/4
[M9K2-FortyGigE7/0/4] ip address 30.1.1.2 255.255.255.0
[M9K2]security-zone  name Untrust
[M9K2-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K2]security-zone  name Trust
[M9K2-security-zone-Trust]import interface FortyGigE7/0/4
[M9K2]security-zone  name RBM
[M9K2-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[M9K2]security-policy ip
[M9K2-security-policy-ip]rule name Trust-Untrust
[M9K2-security-policy-ip-0-Trust-Untrust]source-zone Trust
[M9K2-security-policy-ip-0-Trust-Untrust]destination-zone Untrust
[M9K2-security-policy-ip-0-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功。

```
[M9K2]security-policy ip
[M9K2-security-policy-ip]rule name Local-RBM
[M9K2-security-policy-ip-1-Local-RBM]source-zone Local
```

```
[M9K2-security-policy-ip-1-Local-RBM]destination-zone RBM
[M9K2-security-policy-ip-1-Local-RBM]action pass
[M9K2-security-policy-ip]rule name RBM-Local
[M9K2-security-policy-ip-2-RBM-Local]source-zone RBM
[M9K2-security-policy-ip-2-RBM-Local]destination-zone Local
[M9K2-security-policy-ip-2-RBM-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.1，端口号使用默认的 66064。

```
<M9K2>system-view
[M9K2]remote-backup group
[M9K2-remote-backup-group]remote-ip 11.1.1.1
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.2。

```
[M9K2-remote-backup-group]local-ip 11.1.1.2
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K2-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为备管理设备。

```
[M9K2-remote-backup-group]device-role secondary
```

配置 RBM 双机热备的模式为主备模式。（默认是主备模式）。

```
[M9K2-remote-backup-group]undo backup-mode
```

开启 RBM 热备功能。

```
[M9K2-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K2-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K2-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 1 分钟。

```
[M9K2-remote-backup-group]delay-time 1
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/1 创建 VRRP 备份组 1，其虚拟 IP 地址为 20.1.1.3，并配置其属于 VRRP standby 组。

```
[M9K2]interface FortyGigE7/0/1
[M9K2-FortyGigE7/0/1]vrrp vrid 1 virtual-ip 20.1.1.3 standby
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/4 创建 VRRP 备份组 2，其虚拟 IP 地址为 30.1.1.3，并配置其属于 VRRP standby 组。

```
[M9K2]interface FortyGigE7/0/4
[M9K2-FortyGigE7/0/4]vrrp vrid 2 virtual-ip 30.1.1.3 standby
```

若存在 HTTP 或 DNS 应用协议的流量，还需开启对应的会话备份功能。

```
<M9K2> system
[M9K2]session synchronization http
[M9K2]session synchronization dns
```

(4) 配置 SW1

在 SW1 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

(5) 配置 SW2

在 SW2 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

(6) 配置 Router

#配置路由信息，去往内网主机流量下一跳 IP 地址为 VRRP 备份组 1 的虚拟地址 20.1.1.3，去往 Internet 流量的下一跳地址为出接口对端 IP 地址。

(7) 配置内网主机

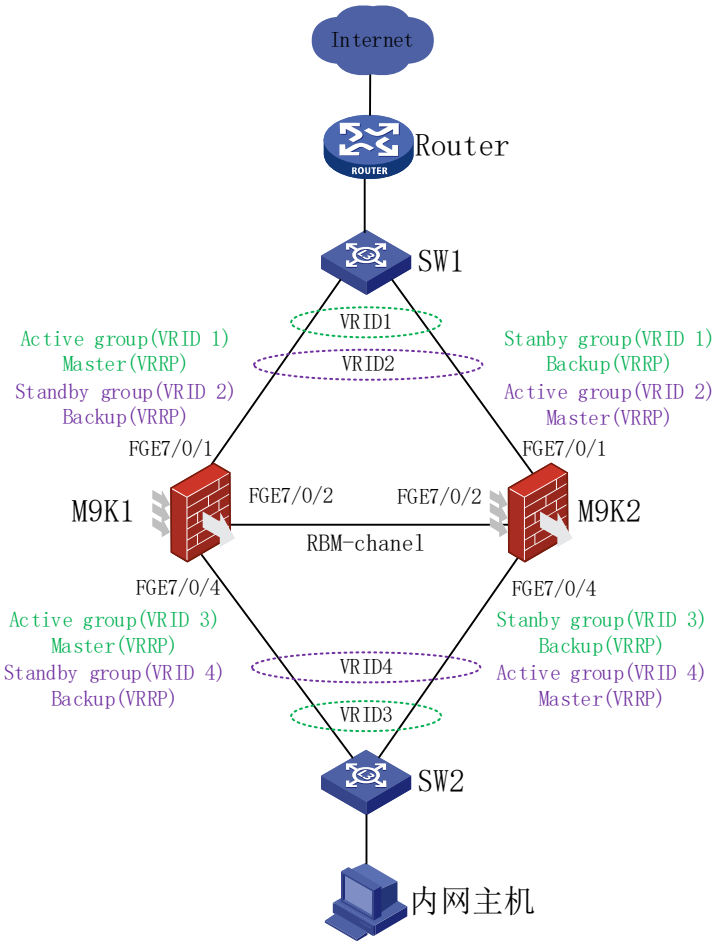
#配置主机默认网关为 VRRP 备份组 2 的虚地址 30.1.1.3。

5.2 M9000 VRRP+RBM双主组网基本功能

5.2.1 组网需求

如图 5-2 所示，2 台 M9K 通过三层口连接到内部网络和外部网络，防火墙分别和上下行交换机连接。

图5-2 VRRP+RBM 双主组网基本功能组网图



5.2.2 配置思路

- 配置接口地址并加入安全域，保证传输可达。
- 配置 RBM 组，包含控制通道和数据通道，备份模式等信息。
- 配置 VRRP 备份组。

5.2.3 配置步骤

(1) 确保主备设备的软硬件环境一致

在配置远端备份管理功能之前，请先保证主/备设备的硬件环境和软件环境的一致性。

(2) 配置 M9K1

配置接口 IP 地址, 将接口加入安全域。

```
[M9K1]interface FortyGigE 7/0/2
[M9K1-FortyGigE7/0/2]ip address 11.1.1.1 255.255.255.0
[M9K1]interface FortyGigE 7/0/1
[M9K1-FortyGigE7/0/1]ip address 20.1.1.1 255.255.255.0
[M9K1]interface FortyGigE 7/0/4
[M9K1-FortyGigE7/0/4]ip address 30.1.1.1 255.255.255.0
[M9K1]security-zone  name Untrust
[M9K1-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K1]security-zone  name Trust
[M9K1-security-zone-Trust]import interface FortyGigE7/0/4
[M9K1]security-zone  name RBM
[M9K1-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[M9K1]security-policy ip
[M9K1-security-policy-ip]rule name Trust-Untrust
[M9K1-security-policy-ip-0-Trust-Untrust]source-zone Trust
[M9K1-security-policy-ip-0-Trust-Untrust]destination-zone Untrust
[M9K1-security-policy-ip-0-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功。

```
[M9K1]security-policy ip
[M9K1-security-policy-ip]rule name Local-RBM
[M9K1-security-policy-ip-1-Local-RBM]source-zone Local
[M9K1-security-policy-ip-1-Local-RBM]destination-zone RBM
[M9K1-security-policy-ip-1-Local-RBM]action pass
[M9K1-security-policy-ip]rule name RBM-Local
[M9K1-security-policy-ip-2-RBM-Local]source-zone RBM
[M9K1-security-policy-ip-2-RBM-Local]destination-zone Local
[M9K1-security-policy-ip-2-RBM-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.2，端口号使用默认的 66064。

```
[M9K1]remote-backup group
[M9K1-remote-backup-group]remote-ip 11.1.1.2
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.1。

```
[M9K1-remote-backup-group]local-ip 11.1.1.1
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K1-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为主管理设备。

```
[M9K1-remote-backup-group]device-role primary
```

配置 RBM 双机热备的模式为双主模式。

```
[M9K1-remote-backup-group]backup-mode dual-active
```

开启 RBM 热备功能。

```
[M9K1-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K1-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K1-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 1 分钟。

```
[M9K1-remote-backup-group]delay-time 1
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/1 建 VRRP 备份组 1，其虚拟 IP 地址为 20.1.1.3，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]vrrp vrid 1 virtual-ip 20.1.1.3 active
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/1 建 VRRP 备份组 2，其虚拟 IP 地址为 20.1.1.4，并配置其属于 VRRP standby 组。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]vrrp vrid 2 virtual-ip 20.1.1.4 standby
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/4 创建 VRRP 备份组 3，其虚拟 IP 地址为 30.1.1.3，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/4
[M9K1-FortyGigE7/0/4]vrrp vrid 3 virtual-ip 30.1.1.3 active
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/4 创建 VRRP 备份组 4，其虚拟 IP 地址为 30.1.1.4，并配置其属于 VRRP standby 组。

```
[M9K1]interface FortyGigE7/0/4
[M9K1-FortyGigE7/0/4]vrrp vrid 4 virtual-ip 30.1.1.4 standby
```

若存在 HTTP 或 DNS 应用协议的流量，还需开启对应的会话备份功能。

```
<M9K1>system
[M9K1]session synchronization http
[M9K1]session synchronization dns
```

(3) 配置 M9K2

配置接口 IP 地址, 将接口加入安全域。

```
[M9K2]interface FortyGigE 7/0/2
[M9K2-FortyGigE7/0/2]ip address 11.1.1.2 255.255.255.0
[M9K2]interface FortyGigE 7/0/1
[M9K2-FortyGigE7/0/1]ip address 20.1.1.2 255.255.255.0
[M9K2]interface FortyGigE 7/0/4
[M9K2-FortyGigE7/0/4]ip address 30.1.1.2 255.255.255.0
[M9K2]security-zone  name Untrust
[M9K2-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K2]security-zone  name Trust
[M9K2-security-zone-Trust]import interface FortyGigE7/0/4
[M9K2]security-zone  name RBM
[M9K2-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[M9K2]security-policy ip
[M9K2-security-policy-ip]rule name Trust-Untrust
```

```
[M9K2-security-policy-ip-0-Trust-Untrust]source-zone Trust
[M9K2-security-policy-ip-0-Trust-Untrust]destination-zone Untrust
[M9K2-security-policy-ip-0-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功。

```
[M9K2]security-policy ip
[M9K2-security-policy-ip]rule name Local-RBM
[M9K2-security-policy-ip-1-Local-RBM]source-zone Local
[M9K2-security-policy-ip-1-Local-RBM]destination-zone RBM
[M9K2-security-policy-ip-1-Local-RBM]action pass
[M9K2-security-policy-ip]rule name RBM-Local
[M9K2-security-policy-ip-2-RBM-Local]source-zone RBM
[M9K2-security-policy-ip-2-RBM-Local]destination-zone Local
[M9K2-security-policy-ip-2-RBM-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.1，端口号使用默认的 66064。

```
<M9K21>system-view
[M9K2]remote-backup group
[M9K2-remote-backup-group]remote-ip 11.1.1.1
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.2。

```
[M9K2-remote-backup-group]local-ip 11.1.1.2
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K2-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为备管理设备。

```
[M9K2-remote-backup-group]device-role secondary
```

配置 RBM 双机热备的模式为双主模式。

```
[M9K2-remote-backup-group]backup-mode dual-active
```

开启 RBM 热备功能。

```
[M9K2-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K2-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K2-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 1 分钟。

```
[M9K2-remote-backup-group]delay-time 1
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/1 创建 VRRP 备份组 1，其虚拟 IP 地址为 20.1.1.3，并配置其属于 VRRP standby 组。

```
[M9K2]interface FortyGigE7/0/1
[M9K2-FortyGigE7/0/1]vrrp vrid 1 virtual-ip 20.1.1.3 standby
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/1 创建 VRRP 备份组 2，其虚拟 IP 地址为 20.1.1.4，并配置其属于 VRRP active 组。

```
[M9K2]interface FortyGigE7/0/1
[M9K2-FortyGigE7/0/1]vrrp vrid 2 virtual-ip 20.1.1.4 active
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/4 创建 VRRP 备份组 3，其虚拟 IP 地址为 30.1.1.3，并配置其属于 VRRP standby 组。

```
[M9K2]interface FortyGigE7/0/4
```

```
[M9K2-FortyGigE7/0/4]vrrp vrid 3 virtual-ip 30.1.1.3 standby
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/4 创建 VRRP 备份组 4，其虚拟 IP 地址为 30.1.1.4，并配置其属于 VRRP active 组。

```
[M9K2]interface FortyGigE7/0/4
[M9K2-FortyGigE7/0/4]vrrp vrid 4 virtual-ip 30.1.1.4 active
```

若存在 HTTP 或 DNS 应用协议的流量，还需开启对应的会话备份功能。

```
<M9K2> system
[M9K2]session synchronization http
[M9K2]session synchronization dns
```

(4) 配置 SW1

在 SW1 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

(5) 配置 SW2

在 SW2 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

(6) 配置 Router

#配置路由信息，去往一部分内网流量的下一跳 IP 地址为 VRRP 备份组 1 的虚拟 IP 地址 20.1.1.3，去往另一部分内网流量的下一跳 IP 地址为 VRRP 备份组 1 的虚拟 IP 地址 20.1.1.4，去往 Internet 流量的下一跳 IP 地址为出接口对端的 IP 地址。

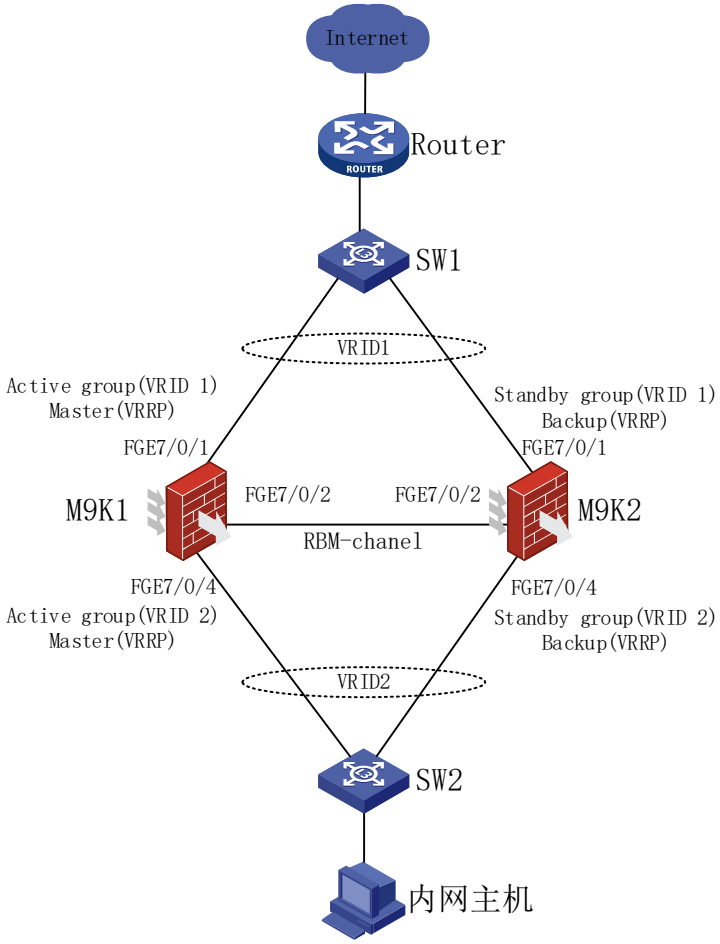
(7) 配置内网主机

#配置一部分主机的默认网关为 VRRP 备份组 3 的虚拟 IP 地址 30.1.1.3，配置另一部分主机的默认网关为 VRRP 备份组 4 的虚拟 IP 地址 30.1.1.4。

5.3 M9000 VRRP+RBM主备组网中动态NAT基本功能

5.3.1 组网需求

图5-3 VRRP+RBM 主备组网中动态 NAT 基本功能组网图



5.3.2 配置思路

- 配置 VRRP+RBM 主备组网基础配置。
- 配置 NAT 地址池，地址池绑定 VRRP 备份组。
- 接口应用出方向动态 NAT 配置。

5.3.3 配置步骤

(1) 配置 VRRP+RBM 主备组网环境

参考上文的“M9000 的 VRRP+RBM 主备组网基本功能”完成组网环境配置。

(2) 配置动态 NAT

在此配置举例中，仅需要在主管理设备 M9K1 上配置 NAT 的相关配置，M9K1 上的 NAT 配置会自动同步到从管理设备 M9K2。

配置 NAT 地址组 1，其地址成员范围为 139.1.1.1 到 139.1.1.80。

```
[M9K1]nat address-group  1
[M9K1-address-group-1]address 139.1.1.1 139.1.1.80
```

配置 NAT 地址池 1 与 VRRP 备份组 1 绑定。

```
[M9K1-address-group-1]vrrp vrid 1
```

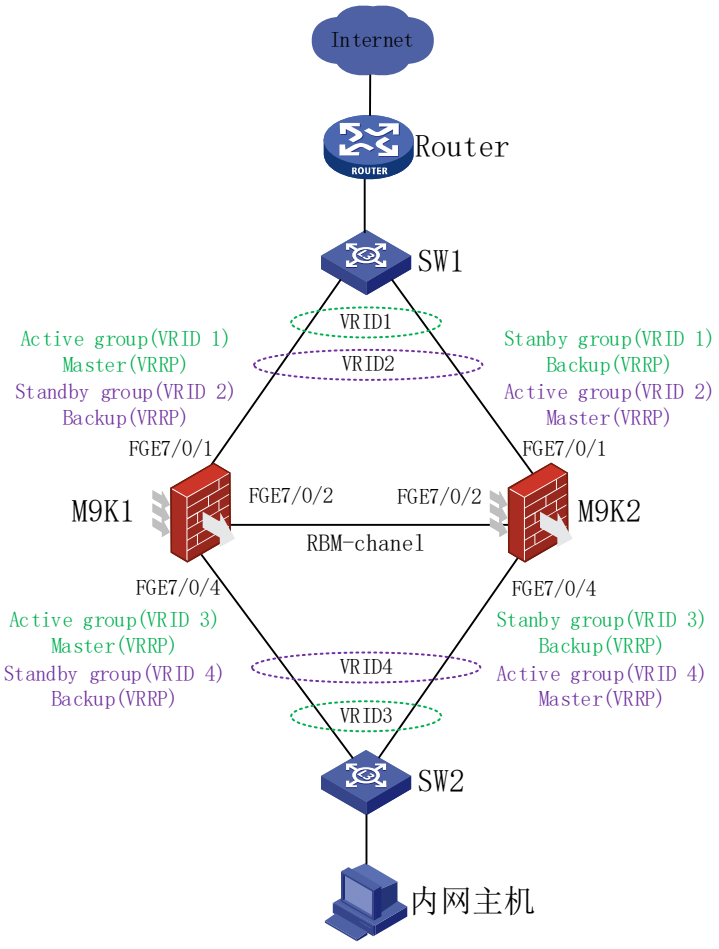
在接口上配置出方向动态地址转换，允许使用地址组 1 中的地址池进行源地址转换，并在转换过程中使用端口信息。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]nat outbound address-group 1
```

5.4 M9000 VRRP+RBM双主组网中动态NAT基本功能

5.4.1 组网需求

图5-4 VRRP+RBM 双主组网中动态 NAT 基本功能组网图



5.4.2 配置思路

- 配置 VRRP+RBM 主备组网基础配置。
- 配置 NAT 地址池，地址池绑定 VRRP 备份组。
- 接口应用出方向动态 NAT 配置。

5.4.3 配置步骤

(1) 配置 VRRP+RBM 主备组网环境

参考上文的“M9000 的 VRRP+RBM 双主组网基本功能”完成组网环境配置。

(2) 配置动态 NAT

在此配置举例中，仅需要在主管理设备 M9K1 上配置 NAT 的相关配置，M9K1 上的 NAT 配置会自动同步到从管理设备 M9K2。

配置 NAT 地址组 1，其地址成员范围为 139.1.1.1 到 139.1.1.80。

```
[M9K1]nat address-group  1
[M9K1-address-group-1]address 139.1.1.1 139.1.1.80
```

配置 NAT 地址池 1 与 VRRP 备份组 1 绑定。

```
[M9K1-address-group-1]vrrp vrid 1
```

配置 NAT 地址组 2，其地址成员范围为 139.1.2.1 到 139.1.2.80。

```
[M9K1]nat address-group  2
[M9K1-address-group-2]address 139.1.2.1 139.1.2.80
```

配置 NAT 地址池 1 与 VRRP 备份组 1 绑定。

```
[M9K1-address-group-2]vrrp vrid 2
```

#配置 ACL 3000，仅允许 30.1.1.1/25 网段的报文通过。

```
[M9K1]acl advanced  3000
[M9K1-acl-ipv4-adv-3000]rule permit ip source 30.1.1.1 0.0.0.127
```

#配置 ACL 3001，仅允许 30.1.1.129/25 网段的报文通过。

```
[M9K1]acl advanced  3001
[M9K1-acl-ipv4-adv-3001]rule permit ip source 30.1.1.129 0.0.0.127
```

在接口上配置出方向动态地址转换，允许使用地址组 1 中的地址对匹配 ACL 3000 的报文进行源地址转换，并在转换过程中使用端口信息；允许使用地址组 2 中的 IP 地址对匹配 ACL 3001 的报文进行源地址转换，并在转换过程中使用端口信息。

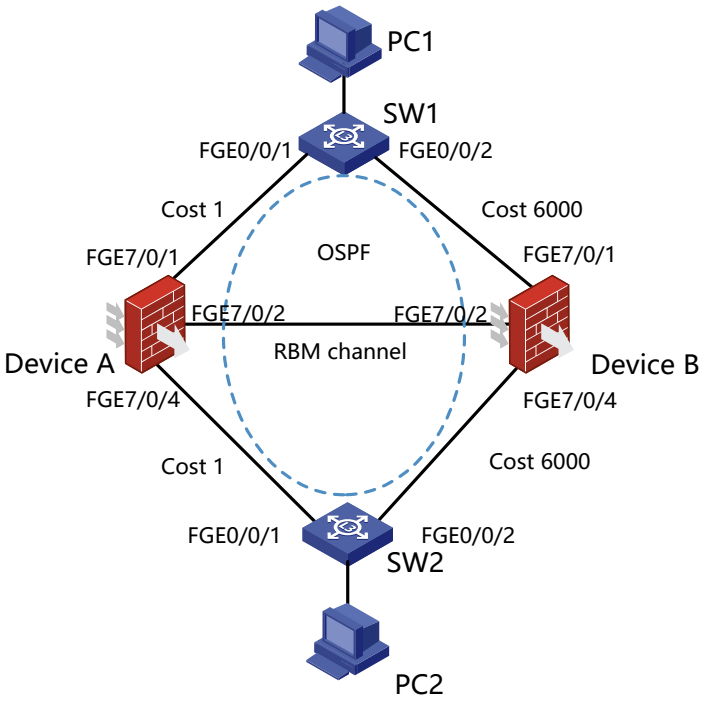
```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]nat outbound 3000 address-group 1
[M9K1-FortyGigE7/0/1]nat outbound 3001 address-group 2
```

5.5 M9000 动态路由+RBM主备组网基本功能

5.5.1 组网需求

如图 5-5 所示，2 台防火墙通过三层口连接到内部网络和外部网络，防火墙分别和上下行交换机连接。

图5-5 动态路由+RBM 主备组网基本功能组网图



5.5.2 配置思路

- 配置接口地址并加入安全域，保证传输可达。
- 配置 RBM 组，包含控制通道和数据通道，备份模式等信息。
- 配置动态路由。

5.5.3 配置步骤

(1) 确保主备设备的软硬件环境一致

在配置远端备份管理功能之前，请先保证主/备设备的硬件环境和软件环境的一致性。

(2) 配置 Device A

配置接口 IP 地址，将接口加入安全域。

```
[Device A]interface FortyGigE 7/0/2
[Device A-FortyGigE7/0/2]ip address 11.1.1.1 255.255.255.0
[Device A]interface FortyGigE 7/0/1
[Device A-FortyGigE7/0/1]ip address 20.1.1.1 255.255.255.0
[Device A]interface FortyGigE 7/0/4
[Device A-FortyGigE7/0/4]ip address 30.1.1.1 255.255.255.0
[Device A]security-zone  name Untrust
[Device A-security-zone-Untrust]import interface FortyGigE7/0/1
[Device A]security-zone  name Trust
[Device A-security-zone-Trust]import interface FortyGigE7/0/4
[Device A]security-zone  name RBM
[Device A-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[Device A]security-policy ip
[Device A-security-policy-ip]rule name Trust-Untrust
[Device A-security-policy-ip-0-Trust-Untrust]source-zone Trust
[Device A-security-policy-ip-0-Trust-Untrust]destination-zone Untrust
[Device A-security-policy-ip-0-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功。

```
[Device A]security-policy ip
[Device A-security-policy-ip]rule name Local-RBM
[Device A-security-policy-ip-1-Local-RBM]source-zone Local
[Device A-security-policy-ip-1-Local-RBM]destination-zone RBM
[Device A-security-policy-ip-1-Local-RBM]action pass
[Device A-security-policy-ip]rule name RBM-Local
[Device A-security-policy-ip-2-RBM-Local]source-zone RBM
[Device A-security-policy-ip-2-RBM-Local]destination-zone Local
[Device A-security-policy-ip-2-RBM-Local]action pass
```

#配置安全策略使安全域 Trust 和 Untrust 与安全域 Local 之间的报文互通，保证动态路由可以协商成功。

```
[Device A]security-policy ip
[Device A-security-policy-ip]rule name Local-Trust
[Device A-security-policy-ip-3-Local-Trust]source-zone Local
[Device A-security-policy-ip-3-Local-Trust]destination-zone Trust
[Device A-security-policy-ip-3-Local-Trust]action pass
[Device A-security-policy-ip]rule name Trust-Local
[Device A-security-policy-ip-4-Trust-Local]source-zone Trust
[Device A-security-policy-ip-4-Trust-Local]destination-zone Local
[Device A-security-policy-ip-4-Trust-Local]action pass
[Device A-security-policy-ip]rule name Local-Unrust
[Device A-security-policy-ip-5-Local-Untrust]source-zone Local
[Device A-security-policy-ip-5-Local-Untrust]destination-zone Untrust
[Device A-security-policy-ip-5-Local-Untrust]action pass
[Device A-security-policy-ip]rule name Unrust Local
[Device A-security-policy-ip-6-Untrust-Local]source-zone Untrust
[Device A-security-policy-ip-6-Untrust-Local]destination-zone Local
[Device A-security-policy-ip-6-Untrust-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.2，端口号使用默认的 60064。

```
[Device A]remote-backup group
[Device A-remote-backup-group]remote-ip 11.1.1.2
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.1。

```
[Device A-remote-backup-group]local-ip 11.1.1.1
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[Device A-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为主管理设备。

```
[Device A-remote-backup-group]device-role primary
```

开启 RBM 热备功能。

```
[Device A-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[Device A-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[Device A-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 30 分钟。

```
[Device A-remote-backup-group]delay-time 30
```

开启 RBM 调整设备上动态路由协议 OSPF 的开销值功能，并以绝对值方式对外通告开销值，绝对值为 6000。

```
[Device A-remote-backup-group]adjust-cost ospf enable absolute 6000
```

配置设备上的 OSPF 功能，OSPF 协议自身的链路开销值建议保持默认配置即可。

```
[Device A]router id 20.1.1.1
[Device A]ospf
[Device A-ospf-1]area 0
[Device A-ospf-1-area-0.0.0.0]network 20.1.1.0 0.0.0.255
[Device A-ospf-1-area-0.0.0.0]network 30.1.1.0 0.0.0.255
```

创建 Track 项 1 与接口 FortyGigE 7/0/1 链路状态关联。

```
[Device A]track 1 interface  FortyGigE 7/0/1 physical
```

创建 Track 项 2 与接口 FortyGigE 7/0/4 链路状态关联。

```
[Device A]track 2 interface  FortyGigE 7/0/4 physical
```

配置 RBM 与序号为 1 和 2 的 Track 项联动。

```
[Device A]remote-backup group
[Device A-remote-backup-group]track 1
[Device A-remote-backup-group]track 2
```

(3)　配置 Device B

配置接口 IP 地址, 将接口加入安全域。

```
[Device B]interface FortyGigE 7/0/2
[Device B-FortyGigE7/0/2]ip address 11.1.1.2 255.255.255.0
[Device B]interface FortyGigE 7/0/1
[Device B-FortyGigE7/0/1]ip address 20.1.10.2 255.255.255.0
[Device B]interface FortyGigE 7/0/4
[Device B-FortyGigE7/0/4]ip address 30.1.10.2 255.255.255.0
[Device B]security-zone  name Untrust
[Device B-security-zone-Untrust]import interface FortyGigE7/0/1
[Device B]security-zone  name Trust
[Device B-security-zone-Trust]import interface FortyGigE7/0/4
[Device B]security-zone  name RBM
[Device B-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[Device B]security-policy ip
[Device B-security-policy-ip]rule name Trust-Untrust
[Device B-security-policy-ip-0-Trust-Untrust]source-zone Trust
[Device B-security-policy-ip-0-Trust-Untrust]destination-zone Untrust
[Device B-security-policy-ip-0-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功。

```
[Device B]security-policy ip
```

```
[Device B-security-policy-ip]rule name Local-RBM
[Device B-security-policy-ip-1-Local-RBM]source-zone Local
[Device B-security-policy-ip-1-Local-RBM]destination-zone RBM
[Device B-security-policy-ip-1-Local-RBM]action pass
[Device B-security-policy-ip]rule name RBM-Local
[Device B-security-policy-ip-2-RBM-Local]source-zone RBM
[Device B-security-policy-ip-2-RBM-Local]destination-zone Local
[Device B-security-policy-ip-2-RBM-Local]action pass
```

#配置安全策略使安全域 Trust 和 Untrust 与安全域 Local 之间的报文互通，保证动态路由可以协商成功。

```
[Device B]security-policy ip
[Device B-security-policy-ip]rule name Local-Trust
[Device B-security-policy-ip-3-Local-Trust]source-zone Local
[Device B-security-policy-ip-3-Local-Trust]destination-zone Trust
[Device B-security-policy-ip-3-Local-Trust]action pass
[Device B-security-policy-ip]rule name Trust-Local
[Device B-security-policy-ip-4-Trust-Local]source-zone Trust
[Device B-security-policy-ip-4-Trust-Local]destination-zone Local
[Device B-security-policy-ip-4-Trust-Local]action pass
[Device B-security-policy-ip]rule name Local-Unrust
[Device B-security-policy-ip-5-Local-Untrust]source-zone Local
[Device B-security-policy-ip-5-Local-Untrust]destination-zone Untrust
[Device B-security-policy-ip-5-Local-Untrust]action pass
[Device B-security-policy-ip]rule name Unrust Local
[Device B-security-policy-ip-6-Untrust-Local]source-zone Untrust
[Device B-security-policy-ip-6-Untrust-Local]destination-zone Local
[Device B-security-policy-ip-6-Untrust-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.1，端口号使用默认的 60064。

```
[Device B]remote-backup group
[Device B-remote-backup-group]remote-ip 11.1.1.1
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.2。

```
[Device B-remote-backup-group]local-ip 11.1.1.2
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[Device B-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为主管理设备。

```
[Device B-remote-backup-group]device-role secondary
```

开启 RBM 热备功能。

```
[Device B-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[Device B-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[Device B-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 30 分钟。

```
[Device B-remote-backup-group]delay-time 30
```

开启 RBM 调整设备上动态路由协议 OSPF 的开销值功能，并以绝对值方式对外通告开销值，绝对值为 6000。

```
[Device B-remote-backup-group]adjust-cost ospf enable absolute 6000
```

配置设备上的 OSPF 功能，OSPF 协议自身的链路开销值建议保持默认配置即可。

```
[Device B]router id 20.1.10.1
[Device B]ospf
[Device B-ospf-1]area 0
[Device B-ospf-1-area-0.0.0.0]network 20.1.10.0 0.0.0.255
[Device B-ospf-1-area-0.0.0.0]network 30.1.10.0 0.0.0.255
```

创建 Track 项 1 与接口 FortyGigE 7/0/1 链路状态关联。

```
[Device B]track 1 interface  FortyGigE 7/0/1 physical
```

创建 Track 项 2 与接口 FortyGigE 7/0/4 链路状态关联。

```
[Device B]track 2 interface  FortyGigE 7/0/4 physical
```

#配置 RBM 与序号为 1 和 2 的 Track 项联动。

```
[Device B]remote-backup group
[Device B-remote-backup-group]track 1
[Device B-remote-backup-group]track 2
```

(4) 配置 SW1

配置接口 FortyGigE0/0/1 的 IP 地址为 20.1.1.2/24

配置接口 FortyGigE0/0/1 的 IP 地址为 20.1.10.2/24

配置 OSPF 路由协议，保证路由可达。

(5) 配置 SW2

配置接口 FortyGigE0/0/1 的 IP 地址为 30.1.1.2/24

配置接口 FortyGigE0/0/1 的 IP 地址为 30.1.10.2/24

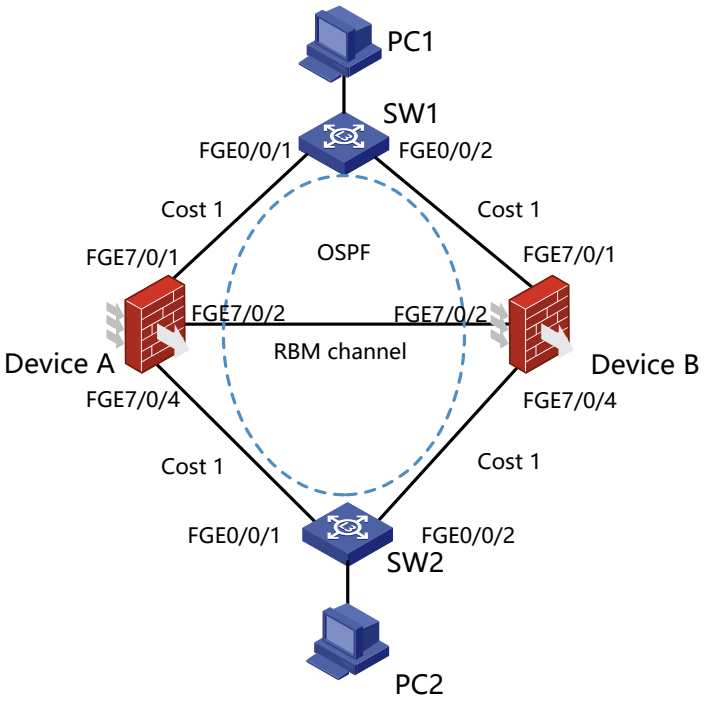
配置 OSPF 路由协议，保证路由可达。

5.6 M9000 动态路由+RBM双主组网基本功能

5.6.1 组网需求

如图 5-6 所示，2 台防火墙通过三层口连接到内部网络和外部网络，防火墙分别和上下行交换机连接。

图5-6 动态路由+RBM 双主组网基本功能组网图



5.6.2 配置思路

- 配置接口地址并加入安全域，保证传输可达。
- 配置 RBM 组，包含控制通道和数据通道，备份模式等信息。
- 配置动态路由。

5.6.3 配置步骤

(1) 确保主备设备的软硬件环境一致

在配置远端备份管理功能之前，请先保证主/备设备的硬件环境和软件环境的一致性。

(2) 配置 Device A

配置接口 IP 地址, 将接口加入安全域。

```
[Device A]interface FortyGigE 7/0/2
[Device A-FortyGigE7/0/2]ip address 11.1.1.1 255.255.255.0
[Device A]interface FortyGigE 7/0/1
[Device A-FortyGigE7/0/1]ip address 20.1.1.1 255.255.255.0
[Device A]interface FortyGigE 7/0/4
[Device A-FortyGigE7/0/4]ip address 30.1.1.1 255.255.255.0
[Device A]security-zone  name Untrust
[Device A-security-zone-Untrust]import interface FortyGigE7/0/1
[Device A]security-zone  name Trust
[Device A-security-zone-Trust]import interface FortyGigE7/0/4
[Device A]security-zone  name RBM
[Device A-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[Device A]security-policy ip
[Device A-security-policy-ip]rule name Trust-Untrust
[Device A-security-policy-ip-0-Trust-Untrust]source-zone Trust
[Device A-security-policy-ip-0-Trust-Untrust]destination-zone Untrust
[Device A-security-policy-ip-0-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功。

```
[Device A]security-policy ip
[Device A-security-policy-ip]rule name Local-RBM
[Device A-security-policy-ip-1-Local-RBM]source-zone Local
[Device A-security-policy-ip-1-Local-RBM]destination-zone RBM
[Device A-security-policy-ip-1-Local-RBM]action pass
[Device A-security-policy-ip]rule name RBM-Local
[Device A-security-policy-ip-2-RBM-Local]source-zone RBM
[Device A-security-policy-ip-2-RBM-Local]destination-zone Local
[Device A-security-policy-ip-2-RBM-Local]action pass
```

#配置安全策略使安全域 Trust 和 Untrust 与安全域 Local 之间的报文互通，保证动态路由可以协商成功。

```
[Device A]security-policy ip
[Device A-security-policy-ip]rule name Local-Trust
[Device A-security-policy-ip-3-Local-Trust]source-zone Local
[Device A-security-policy-ip-3-Local-Trust]destination-zone Trust
[Device A-security-policy-ip-3-Local-Trust]action pass
[Device A-security-policy-ip]rule name Trust-Local
[Device A-security-policy-ip-4-Trust-Local]source-zone Trust
[Device A-security-policy-ip-4-Trust-Local]destination-zone Local
[Device A-security-policy-ip-4-Trust-Local]action pass
[Device A-security-policy-ip]rule name Local-Unrust
[Device A-security-policy-ip-5-Local-Untrust]source-zone Local
[Device A-security-policy-ip-5-Local-Untrust]destination-zone Untrust
[Device A-security-policy-ip-5-Local-Untrust]action pass
[Device A-security-policy-ip]rule name Unrust Local
[Device A-security-policy-ip-6-Untrust-Local]source-zone Untrust
[Device A-security-policy-ip-6-Untrust-Local]destination-zone Local
[Device A-security-policy-ip-6-Untrust-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.2，端口号使用默认的 60064。

```
[Device A]remote-backup group
[Device A-remote-backup-group]remote-ip 11.1.1.2
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.1。

```
[Device A-remote-backup-group]local-ip 11.1.1.1
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[Device A-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为主管理设备。

```
[Device A-remote-backup-group]device-role primary
```

配置 RBM 双机热备的模式为双主模式

```
[Device A-remote-backup-group]backup-mode dual-active
```

开启 RBM 热备功能。

```
[Device A-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[Device A-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[Device A-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 30 分钟。

```
[Device A-remote-backup-group]delay-time 30
```

开启 RBM 调整设备上动态路由协议 OSPF 的开销值功能，并以绝对值方式对外通告开销值，绝对值为 6000。

```
[Device A-remote-backup-group]adjust-cost ospf enable absolute 6000
```

配置设备上的 OSPF 功能，OSPF 协议自身的链路开销值建议保持默认配置即可。

```
[Device A]router id 20.1.1.1
[Device A]ospf
[Device A-ospf-1]area 0
[Device A-ospf-1-area-0.0.0.0]network 20.1.1.0 0.0.0.255
[Device A-ospf-1-area-0.0.0.0]network 30.1.1.0 0.0.0.255
```

创建 Track 项 1 与接口 FortyGigE 7/0/1 链路状态关联。

```
[Device A]track 1 interface  FortyGigE 7/0/1
```

创建 Track 项 2 与接口 FortyGigE 7/0/4 链路状态关联。

```
[Device A]track 2 interface  FortyGigE 7/0/4
```

配置 RBM 与序号为 1 和 2 的 Track 项联动。

```
[Device A]remote-backup group
[Device A-remote-backup-group]track 1
[Device A-remote-backup-group]track 2
```

(3) 配置 Device B

配置接口 IP 地址, 将接口加入安全域。

```
[Device B]interface FortyGigE 7/0/2
[Device B-FortyGigE7/0/2]ip address 11.1.1.2 255.255.255.0
[Device B]interface FortyGigE 7/0/1
[Device B-FortyGigE7/0/1]ip address 20.1.10.2 255.255.255.0
[Device B]interface FortyGigE 7/0/4
[Device B-FortyGigE7/0/4]ip address 30.1.10.2 255.255.255.0
[Device B]security-zone  name Untrust
[Device B-security-zone-Untrust]import interface FortyGigE7/0/1
[Device B]security-zone  name Trust
[Device B-security-zone-Trust]import interface FortyGigE7/0/4
[Device B]security-zone  name RBM
[Device B-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[Device B]security-policy ip
[Device B-security-policy-ip]rule name Trust-Untrust
[Device B-security-policy-ip-0-Trust-Untrust]source-zone Trust
[Device B-security-policy-ip-0-Trust-Untrust]destination-zone Untrust
[Device B-security-policy-ip-0-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功。

```
[Device B]security-policy ip
[Device B-security-policy-ip]rule name Local-RBM
[Device B-security-policy-ip-1-Local-RBM]source-zone Local
[Device B-security-policy-ip-1-Local-RBM]destination-zone RBM
[Device B-security-policy-ip-1-Local-RBM]action pass
[Device B-security-policy-ip]rule name RBM-Local
[Device B-security-policy-ip-2-RBM-Local]source-zone RBM
[Device B-security-policy-ip-2-RBM-Local]destination-zone Local
[Device B-security-policy-ip-2-RBM-Local]action pass
```

#配置安全策略使安全域 Trust 和 Untrust 与安全域 Local 之间的报文互通，保证动态路由可以协商成功。

```
[Device B]security-policy ip
[Device B-security-policy-ip]rule name Local-Trust
[Device B-security-policy-ip-3-Local-Trust]source-zone Local
[Device B-security-policy-ip-3-Local-Trust]destination-zone Trust
[Device B-security-policy-ip-3-Local-Trust]action pass
[Device B-security-policy-ip]rule name Trust-Local
[Device B-security-policy-ip-4-Trust-Local]source-zone Trust
[Device B-security-policy-ip-4-Trust-Local]destination-zone Local
[Device B-security-policy-ip-4-Trust-Local]action pass
[Device B-security-policy-ip]rule name Local-Unrust
[Device B-security-policy-ip-5-Local-Unrust]source-zone Local
[Device B-security-policy-ip-5-Local-Unrust]destination-zone Unrust
[Device B-security-policy-ip-5-Local-Unrust]action pass
[Device B-security-policy-ip]rule name Unrust Local
[Device B-security-policy-ip-6-Unrust-Local]source-zone Unrust
[Device B-security-policy-ip-6-Unrust-Local]destination-zone Local
[Device B-security-policy-ip-6-Unrust-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.1，端口号使用默认的 60064。

```
[Device B]remote-backup group
[Device B-remote-backup-group]remote-ip 11.1.1.1
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.2。

```
[Device B-remote-backup-group]local-ip 11.1.1.2
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[Device B-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为主管理设备。

```
[Device B-remote-backup-group]device-role secondary
```

配置 RBM 双机热备的模式为双主模式。

```
[Device B-remote-backup-group]backup-mode dual-active
```

开启 RBM 热备功能。

```
[Device B-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[Device B-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[Device B-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 30 分钟。

```
[Device B-remote-backup-group]delay-time 30
```

开启 RBM 调整设备上动态路由协议 OSPF 的开销值功能，并以绝对值方式对外通告开销值，绝对值为 6000。

```
[Device B-remote-backup-group]adjust-cost ospf enable absolute 6000
```

配置设备上的 OSPF 功能，OSPF 协议自身的链路开销值建议保持默认配置即可。

```
[Device B]router id 20.1.10.1
[Device B]ospf
[Device B-ospf-1]area 0
[Device B-ospf-1-area-0.0.0.0]network 20.1.10.0 0.0.0.255
[Device B-ospf-1-area-0.0.0.0]network 30.1.10.0 0.0.0.255
```

创建 Track 项 1 与接口 FortyGigE 7/0/1 链路状态关联。

```
[Device B]track 1 interface  FortyGigE 7/0/1 physical
```

创建 Track 项 2 与接口 FortyGigE 7/0/4 链路状态关联。

```
[Device B]track 2 interface  FortyGigE 7/0/4 physical
```

#配置 RBM 与序号为 1 和 2 的 Track 项联动。

```
[Device B]remote-backup group
[Device B-remote-backup-group]track 1
[Device B-remote-backup-group]track 2
```

(4) 配置 SW1

配置接口 FortyGigE0/0/1 的 IP 地址为 20.1.1.2/24

配置接口 FortyGigE0/0/1 的 IP 地址为 20.1.10.2/24

配置 OSPF 路由协议，保证路由可达。

(5) 配置 SW2

配置接口 FortyGigE0/0/1 的 IP 地址为 30.1.1.2/24

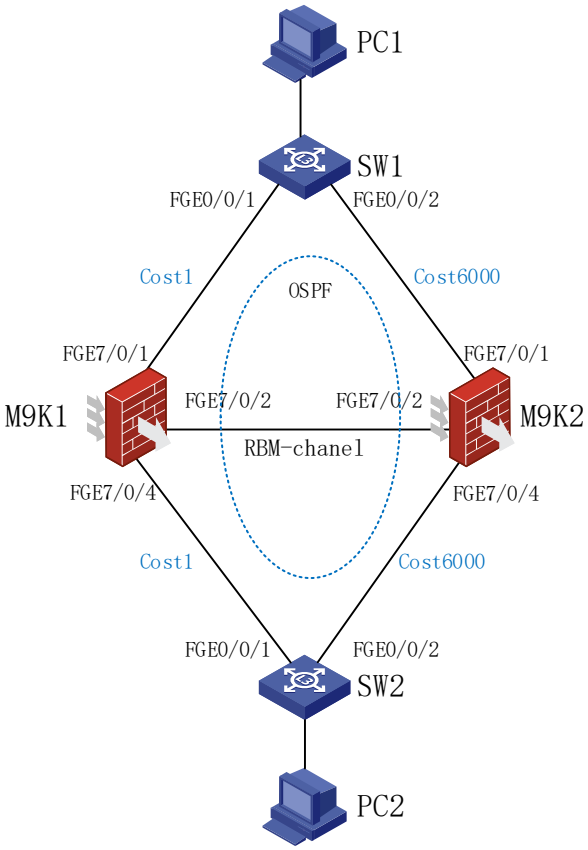
配置接口 FortyGigE0/0/1 的 IP 地址为 30.1.10.2/24

配置 OSPF 路由协议，保证路由可达。

5.7 M9000 动态路由+RBM主备组网中动态NAT基本功能

5.7.1 组网需求

图5-7 动态路由+RBM 主备组网中动态 NAT 基本功能组网图



5.7.2 配置思路

- 配置 VRRP+RBM 主备组网基础配置。
- 接口应用出方向动态 NAT 配置。

5.7.3 配置步骤

(1) 配置 VRRP+RBM 主备组网环境

参考上文的“M9000 的动态路由+RBM 主备组网基本功能”完成组网环境配置。

(2) 配置动态 NAT

在此配置举例中，仅需要在主管理设备 M9K1 上配置 NAT 的相关配置，M9K1 上的 NAT 配置会自动同步到从管理设备 M9K2。

配置 NAT 地址组 1，其地址成员范围为 139.1.1.1 到 139.1.1.80。

```
[M9K1]nat address-group  1
[M9K1-address-group-1]address 139.1.1.1 139.1.1.80
```

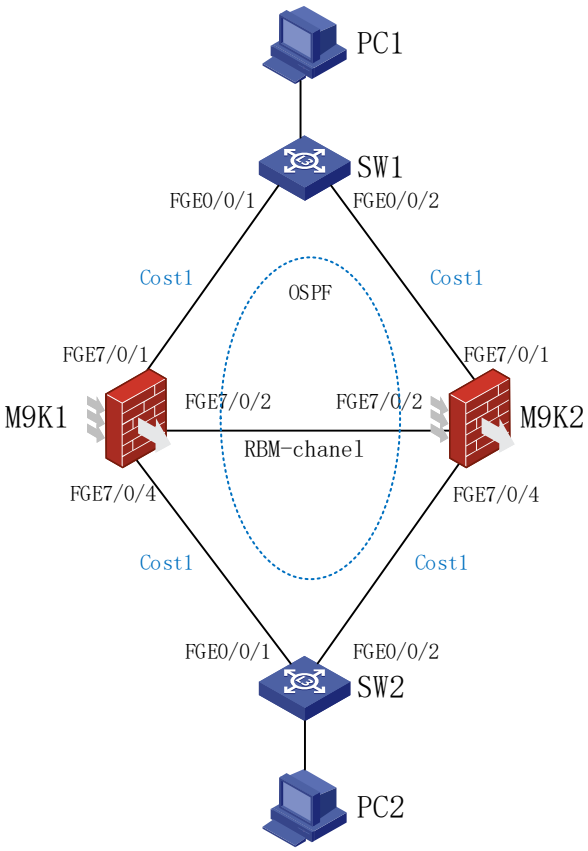
在接口上配置出方向动态地址转换，允许使用地址组 1 中的地址池进行源地址转换，并在转换过程中使用端口信息。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]nat outbound address-group 1
```

5.8 M9000 动态路由+RBM双主组网中动态NAT基本功能

5.8.1 组网需求

图5-8 动态路由+RBM 双主组网中动态 NAT 基本功能组网图



5.8.2 配置思路

- 配置 VRRP+RBM 主备组网基础配置。
- 接口应用出方向动态 NAT 配置。

5.8.3 配置步骤

(1) 配置 VRRP+RBM 主备组网环境

参考上文的“M9000 的动态路由+RBM 主备组网基本功能”完成组网环境配置。

(2) 配置动态 NAT

在此配置举例中，仅需要在主管理设备 M9K1 上配置 NAT 的相关配置，M9K1 上的 NAT 配置会自动同步到从管理设备 M9K2。

配置 NAT 地址组 1，其地址成员范围为 139.1.1.1 到 139.1.1.80。

```
[M9K1]nat address-group  1
[M9K1-address-group-1]address 139.1.1.1 139.1.1.80
```

配置端口 NAT 端口资源拆分功能。在主管理设备下发此命令后，被管理设备会自动下发 nat remote-backup port-alloc secondary 命令。主管理设备使用数值较小的一半端口，从管理设备使用数值大较大的一半端口。

```
[M9K1]nat remote-backup port-alloc primary
```

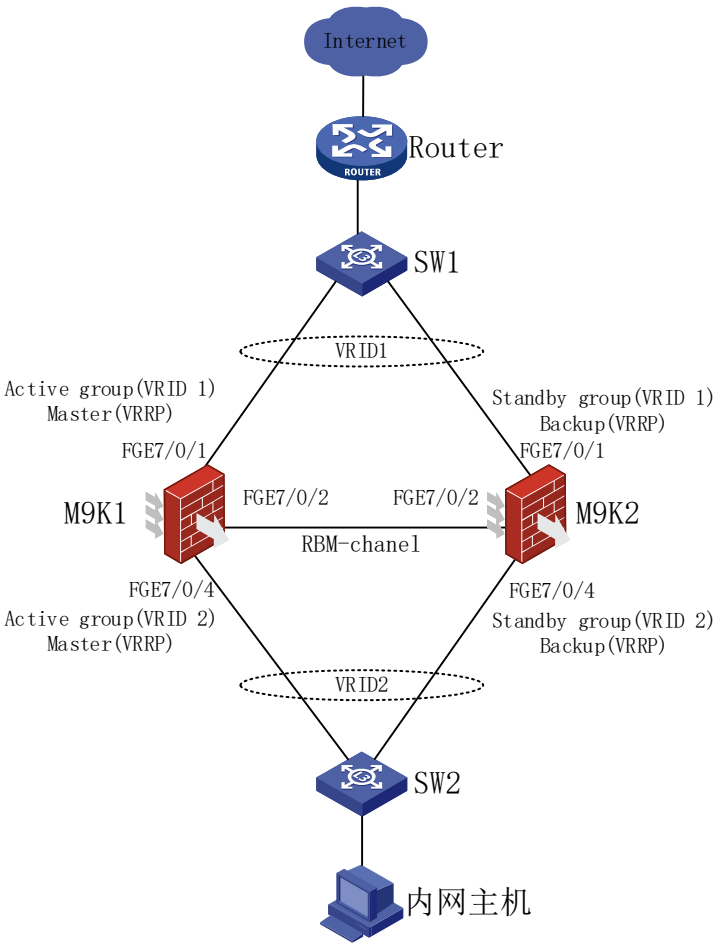
在接口上配置出方向动态地址转换，允许使用地址组 1 中的地址池进行源地址转换，并在转换过程中使用端口信息。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]nat outbound address-group 1
```

5.9 M9000 RBM与Track联动基本功能

5.9.1 组网需求

图5-9 VRRP+RBM 主备组网基本功能组网图



5.9.2 配置思路

- 配置 VRRP+RBM 主备组网基础配置。

- 配置 Track 与接口关联。
- 配置 RBM 组与 Track 项关联。

5.9.3 配置步骤

(1) 配置 VRRP+RBM 主备组网环境

参考上文的“M9000 的动态路由+RBM 主备组网基本功能”完成组网环境配置。

(2) 配置 TRACK 与接口关联

在 M9K1 上创建 Track 项 1 与接口 FortyGigE 7/0/1 链路状态关联。

```
[M9K1]track 1 interface  FortyGigE 7/0/1
```

在 M9K1 上创建 Track 项 2 与接口 FortyGigE 7/0/4 链路状态关联。

```
[M9K1]track 2 interface  FortyGigE 7/0/4
```

在 M9K2 上创建 Track 项 1 与接口 FortyGigE 7/0/1 链路状态关联。

```
[M9K2]track 1 interface  FortyGigE 7/0/1
```

在 M9K2 上创建 Track 项 2 与接口 FortyGigE 7/0/4 链路状态关联。

```
[M9K2]track 2 interface  FortyGigE 7/0/4
```

(3) 配置 RBM 组与 Track 项关联

#在 M9K1 上配置 RBM 与序号为 1 和 2 的 Track 项联动。

```
[M9K1]remote-backup group
[M9K1-remote-backup-group]track 1
[M9K1-remote-backup-group]track 2
```

#在 M9K2 上配置 RBM 与序号为 1 和 2 的 Track 项联动。

```
[M9K2]remote-backup group
[M9K2-remote-backup-group]track 1
[M9K2-remote-backup-group]track 2
```

#在 TRACK 关联的接口故障时会触发 RBM 主备切换，由于 RBM 默认会监控接口板、业务卡状态，所以接口卡、业务卡故障无需单独配置 Track 项。

(4) 配置 RBM 组与 Track 项关联

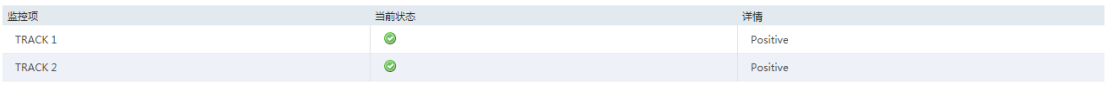
#在 M9K1 上配置 RBM 与序号为 1 和 2 的 Track 项联动。

```
[M9K1]remote-backup group
[M9K1-remote-backup-group]track 1
[M9K1-remote-backup-group]track 2
```

#在 M9K2 上配置 RBM 与序号为 1 和 2 的 Track 项联动。

```
[M9K2]remote-backup group
[M9K2-remote-backup-group]track 1
[M9K2-remote-backup-group]track 2
```

（5）WEB 上查看 track 项状态

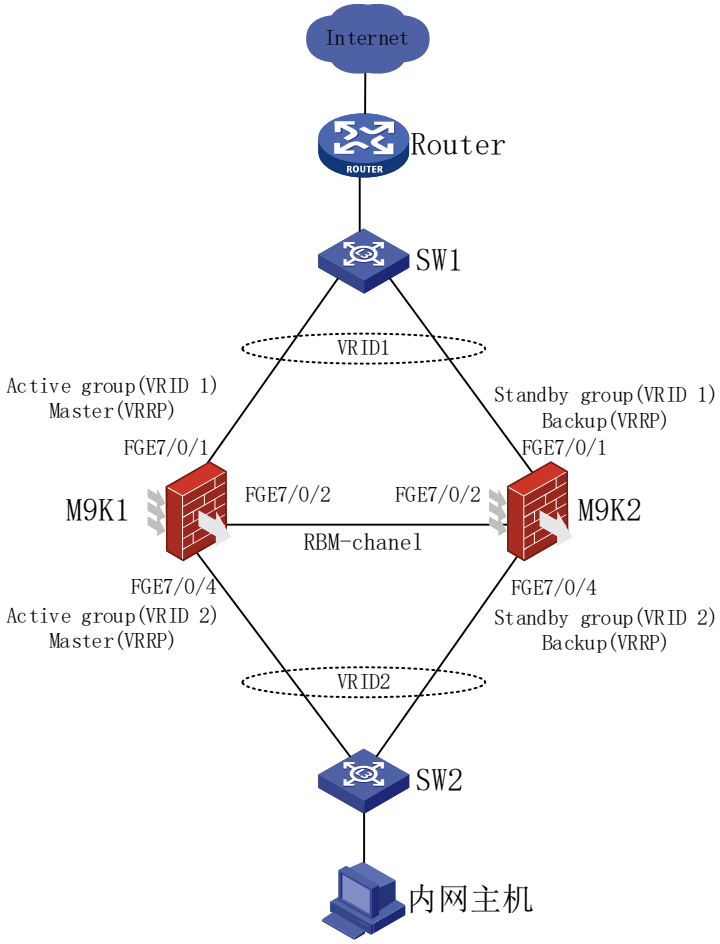


5.10 M9000 VRRP IPv6+RBM主备组网基本功能

5.10.1 组网需求

如图 5-12 所示，2 台 M9K 通过三层口连接到内部网络和外部网络，防火墙分别和上下行交换机连接。

图5-10 VRRP IPv6+RBM 主备组网基本功能组网图



5.10.2 配置思路

- 配置接口地址并加入安全域，保证传输可达。
- 配置 RBM 组，包含控制通道和数据通道，备份模式等信息。
- 配置 VRRP IPv6 备份组。

5.10.3 配置步骤

(1) 确保主备设备的软硬件环境一致。

在配置远端备份管理功能之前，请先保证主/备设备的硬件环境和软件环境的一致性。

(2) 配置 M9K1

配置接口 IP 地址,将接口加入安全域。

```
[M9K1]interface FortyGigE 7/0/2
[M9K1-FortyGigE7/0/2] ip address 11.1.1.1 255.255.255.0
[M9K1]interface FortyGigE 7/0/1
[M9K1-FortyGigE7/0/1] ipv6 address 1008:91::3/98
[M9K1]interface FortyGigE 7/0/4
[M9K1-FortyGigE7/0/4] ipv6 address 1008:92::3/98
[M9K1]security-zone name Untrust
[M9K1-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K1]security-zone name Trust
[M9K1-security-zone-Trust]import interface FortyGigE7/0/4
[M9K1]security-zone name RBM
[M9K1-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[M9K1]security-policy ipv6
[M9K1-security-policy-ipv6]rule name Trust-Untrust
[M9K1-security-policy-ipv6-0-Trust-Untrust]source-zone Trust
[M9K1-security-policy-ipv6-0-Trust-Untrust]destination-zone Untrust
[M9K1-security-policy-ipv6-0-Trust-Untrust]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.2，端口号使用默认的 66064。

```
[M9K1]remote-backup group
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.2

```
[M9K1-remote-backup-group]remote-ip 11.1.1.2
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.1。

```
[M9K1-remote-backup-group]local-ip 11.1.1.1
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K1-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为主管理设备。

```
[M9K1-remote-backup-group]device-role primary
```

配置 RBM 双机热备的模式为主备模式。（默认是主备模式）

```
[M9K1-remote-backup-group]undo backup-mode
```

开启 RBM 热备功能。

```
[M9K1-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K1-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K1-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 30 分钟。

```
[M9K1-remote-backup-group]delay-time 30
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/1 创建 VRRP IPv6 备份组 1，其虚拟 IPv6 地址为 1008:91::1，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]
vrrp ipv6 vrid 1 virtual-ip FE80:1091::1 link-local active
vrrp ipv6 vrid 1 virtual-ip 1008:91::1
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/4 创建 VRRP IPv6 备份组 2，其虚拟 IPv6 地址为 1008:92::1，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/4
[M9K1-FortyGigE7/0/4]
vrrp ipv6 vrid 2 virtual-ip FE80:1092::1 link-local active
vrrp ipv6 vrid 2virtual-ip 1008:92::1
```

(3) 配置 M9K2

配置接口 IP 地址, 将接口加入安全域。

```
[M9K2]interface FortyGigE 7/0/2
[M9K2-FortyGigE7/0/2] ip address 11.1.1.2 255.255.255.0
[M9K2]interface FortyGigE 7/0/1
[M9K2-FortyGigE7/0/1] ipv6 address 1008:91::4/98
[M9K2]interface FortyGigE 7/0/4
[M9K2-FortyGigE7/0/4] ipv6 address 1008:92::4/98
[M9K2]security-zone  name Untrust
[M9K2-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K2]security-zone  name Trust
[M9K2-security-zone-Trust]import interface FortyGigE7/0/4
[M9K2]security-zone  name RBM
[M9K2-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[M9K2]security-policy ipv6
[M9K2-security-policy-ipv6]rule name Trust-Untrust
[M9K2-security-policy-ipv6-0-Trust-Untrust]source-zone Trust
[M9K2-security-policy-ipv6-0-Trust-Untrust]destination-zone Untrust
[M9K2-security-policy-ipv6-0-Trust-Untrust]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.1，端口号使用默认的 66064。

```
<M9K2>system-view
[M9K2]remote-backup group
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.1。

```
[M9K2-remote-backup-group]remote-ip 11.1.1.1
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.2。

```
[M9K2-remote-backup-group]local-ip 11.1.1.2
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K2-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为备管理设备。

```
[M9K2-remote-backup-group]device-role secondary
```

配置 RBM 双机热备的模式为主备模式。（默认是主备模式）。

```
[M9K2-remote-backup-group]undo backup-mode
```

开启 RBM 热备功能。

```
[M9K2-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K2-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K2-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 30 分钟。

```
[M9K2-remote-backup-group]delay-time 30
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/1 创建 VRRP IPv6 备份组 1，其虚拟 IPv6 地址为 1008:91::1，并配置其属于 VRRP standby 组。

```
[M9K2]interface FortyGigE7/0/1
[M9K2-FortyGigE7/0/1]
vrrp ipv6 vrid 1 virtual-ip FE80:1091::1 link-local standby
vrrp ipv6 vrid 1 virtual-ip 1008:91::1
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/4 创建 VRRP IPv6 备份组 2，其虚拟 IPv6 地址为 1008:92::1，并配置其属于 VRRP standby 组。

```
[M9K2]interface FortyGigE7/0/4
[M9K2-FortyGigE7/0/4]
vrrp ipv6 vrid 2 virtual-ip FE80:1092::1 link-local standby
vrrp ipv6 vrid 2 virtual-ip 1008:92::1
```

(4) 配置 SW1

在 SW1 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

(5) 配置 SW2

在 SW2 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

(6) 配置 Router

#配置路由信息，去往内网主机流量下一跳 IPv6 地址为 VRRP IPv6 备份组 1 的虚拟地址 1008:91::1，去往 Internet 流量的下一跳地址为出接口对端 IPv6 地址。

(7) 配置内网主机

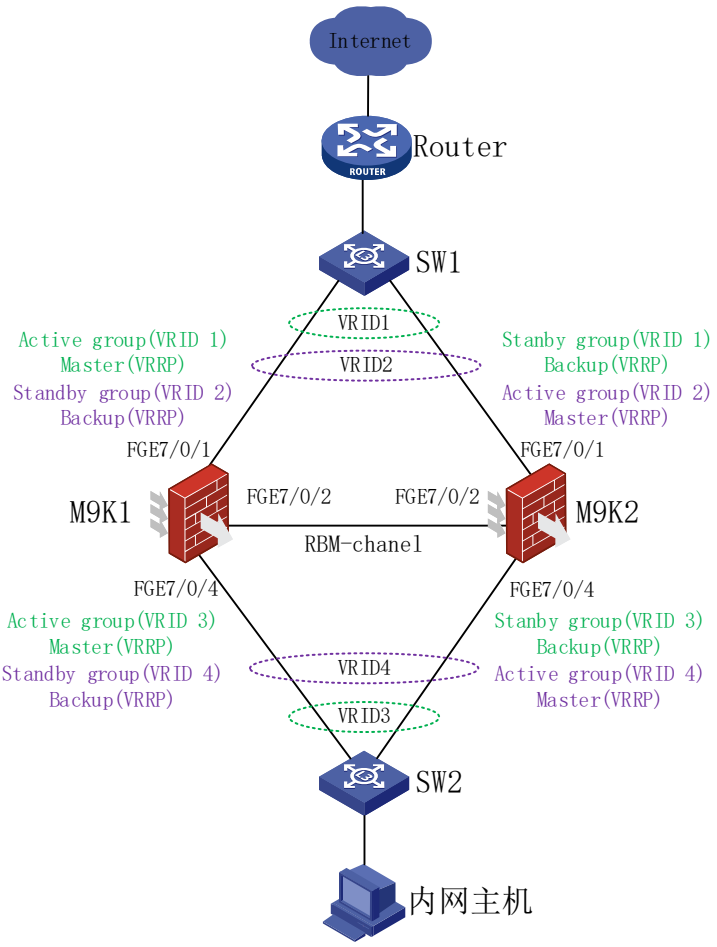
#配置主机 IPv6 默认网关为 VRRP IPv6 备份组 2 的虚地址 1008:92::1。

5.11 M9000 VRRP IPv6+RBM双主组网基本功能

5.11.1 组网需求

如图 5-13 所示，2 台 M9K 通过三层口连接到内部网络和外部网络，防火墙分别和上下行交换机连接。

图5-11 VRRP IPv6+RBM 双主组网基本功能组网图



5.11.2 配置思路

- 配置接口地址并加入安全域，保证传输可达。
- 配置 RBM 组，包含控制通道和数据通道，备份模式等信息。
- 配置 VRRP IPv6 备份组。

5.11.3 配置步骤

(1) 确保主备设备的软硬件环境一致

在配置远端备份管理功能之前，请先保证主/备设备的硬件环境和软件环境的一致性。

(2) 配置 M9K1

配置接口 IPv6 地址，将接口加入安全域。

配置接口 IP 地址，将接口加入安全域。

```
[M9K1]interface FortyGigE 7/0/2
[M9K1-FortyGigE7/0/2] ip address 11.1.1.1 255.255.255.0
[M9K1]interface FortyGigE 7/0/1
[M9K1-FortyGigE7/0/1] ipv6 address 1008:91::3/98
[M9K1]interface FortyGigE 7/0/4
```

```
[M9K1-FortyGigE7/0/4] ipv6 address 1008:92::3/98
[M9K1]security-zone name Untrust
[M9K1-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K1]security-zone name Trust
[M9K1-security-zone-Trust]import interface FortyGigE7/0/4
[M9K1]security-zone name RBM
[M9K1-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[M9K1]security-policy ipv6
[M9K1-security-policy-ipv6]rule name Trust-Untrust
[M9K1-security-policy-ipv6-0-Trust-Untrust]source-zone Trust
[M9K1-security-policy-ipv6-0-Trust-Untrust]destination-zone Untrust
[M9K1-security-policy-ipv6-0-Trust-Untrust]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.2，端口号使用默认的 66064。

```
[M9K1]remote-backup group
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.2

```
[M9K1-remote-backup-group]remote-ip 11.1.1.2
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.1。

```
[M9K1-remote-backup-group]local-ip 11.1.1.1
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K1-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为主管理设备。

```
[M9K1-remote-backup-group]device-role primary
```

配置 RBM 双机热备的模式为双主模式。（默认是主备模式）

```
[M9K1-remote-backup-group]backup-mode dual-active
```

开启 RBM 热备功能。

```
[M9K1-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K1-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K1-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 30 分钟。

```
[M9K1-remote-backup-group]delay-time 30
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/1 建 VRRP IPv6 备份组 1，其虚拟 IPv6 地址为 1008:91::1，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]
vrrp ipv6 vrid 1 virtual-ip FE80:1091::1 link-local active
vrrp ipv6 vrid 1 virtual-ip 1008:91::1
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/1 建 VRRP IPv6 备份组 2，其虚拟 IPv6 地址为 1008:91::2，并配置其属于 VRRP standby 组。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]
vrrp ipv6 vrid 2 virtual-ip FE80:1091::2 link-local standby
vrrp ipv6 vrid 2 virtual-ip 1008:91::2
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/4 创建 VRRP IPv6 备份组 3，其虚拟 IPv6 地址为 1008:92::1，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/4
[M9K1-FortyGigE7/0/4]
vrrp ipv6 vrid 3 virtual-ip FE80:1092::1 link-local active
vrrp ipv6 vrid 3 virtual-ip 1008:92::1
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/4 创建 VRRP IPv6 备份组 4，其虚拟 IP 地址为 1008:92::2，并配置其属于 VRRP standby 组。

```
[M9K1]interface FortyGigE7/0/4
[M9K1-FortyGigE7/0/4]
vrrp ipv6 vrid 4 virtual-ip FE80:1092::2 link-local standby
vrrp ipv6 vrid 4 virtual-ip 1008:92::2
```

(3) 配置 M9K2

```
[M9K2]interface FortyGigE 7/0/2
[M9K2-FortyGigE7/0/2] ip address 11.1.1.2 255.255.255.0
[M9K2]interface FortyGigE 7/0/1
[M9K2-FortyGigE7/0/1] ipv6 address 1008:91::4/98
[M9K2]interface FortyGigE 7/0/4
[M9K2-FortyGigE7/0/4] ipv6 address 1008:92::4/98
[M9K2]security-zone  name Untrust
[M9K2-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K2]security-zone  name Trust
[M9K2-security-zone-Trust]import interface FortyGigE7/0/4
[M9K2]security-zone  name RBM
[M9K2-security-zone-RMB]import interface FortyGigE7/0/2
```

配置安全策略，放通 Trust 至 Untrust 安全域。

```
[M9K2]security-policy ipv6
[M9K2-security-policy-ipv6]rule name Trust-Untrust
[M9K2-security-policy-ipv6-0-Trust-Untrust]source-zone Trust
[M9K2-security-policy-ipv6-0-Trust-Untrust]destination-zone Untrust
[M9K2-security-policy-ipv6-0-Trust-Untrust]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.1，端口号使用默认的 66064。

```
<M9K2>system-view
[M9K2]remote-backup group
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.1。

```
[M9K2-remote-backup-group]remote-ip 11.1.1.1
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.2。

```
[M9K2-remote-backup-group]local-ip 11.1.1.2
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K2-remote-backup-group]data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为备管理设备。

```
[M9K2-remote-backup-group]device-role secondary
```

配置 RBM 双机热备的模式为双主模式。（默认是主备模式）。

```
[M9K2-remote-backup-group] backup-mode dual-active
```

开启 RBM 热备功能。

```
[M9K2-remote-backup-group]hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K2-remote-backup-group]configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K2-remote-backup-group]configuration sync-check interval 12
```

#开启 RBM 双机热备流量回切功能，且延迟切换的时间为 30 分钟。

```
[M9K2-remote-backup-group]delay-time 30
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/1 建 VRRP IPv6 备份组 1，其虚拟 IPv6 地址为 1008:91::1，并配置其属于 VRRP standby 组。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]
vrrp ipv6 vrid 1 virtual-ip FE80:1091::1 link-local standby
vrrp ipv6 vrid 1 virtual-ip 1008:91::1
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/1 建 VRRP IPv6 备份组 2，其虚拟 IPv6 地址为 1008:91::2，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1]
vrrp ipv6 vrid 2 virtual-ip FE80:1091::2 link-local active
vrrp ipv6 vrid 2 virtual-ip 1008:91::2
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/4 创建 VRRP IPv6 备份组 3，其虚拟 IPv6 地址为 1008:92::1，并配置其属于 VRRP standby 组。

```
[M9K1]interface FortyGigE7/0/4
[M9K1-FortyGigE7/0/4]
vrrp ipv6 vrid 3 virtual-ip FE80:1092::1 link-local standby
vrrp ipv6 vrid 3 virtual-ip 1008:92::1
```

配置 RBM 与 VRRP IPv6 关联。在接口 FortyGigE7/0/4 创建 VRRP IPv6 备份组 4，其虚拟 IP 地址为 1008:92::2，并配置其属于 VRRP active 组。

```
[M9K1]interface FortyGigE7/0/4
[M9K1-FortyGigE7/0/4]
vrrp ipv6 vrid 4 virtual-ip FE80:1092::2 link-local active
vrrp ipv6 vrid 4 virtual-ip 1008:92::2
```

(4) 配置 SW1

在 SW1 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

(5) 配置 SW2

在 SW2 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

(6) 配置 Router

#配置路由信息，去往一部分内网流量的下一跳 IPv6 地址为 VRRP IPv6 备份组 1 的虚拟 IPv6 地址 1008:91::1，去往另一部分内网流量的下一跳 IPv6 地址为 VRRP IPv6 备份组 2 的虚拟 IPv6 地址 1008:91::2，去往 Internet 流量的下一跳 IPv6 地址为出接口对端的 IP 地址。

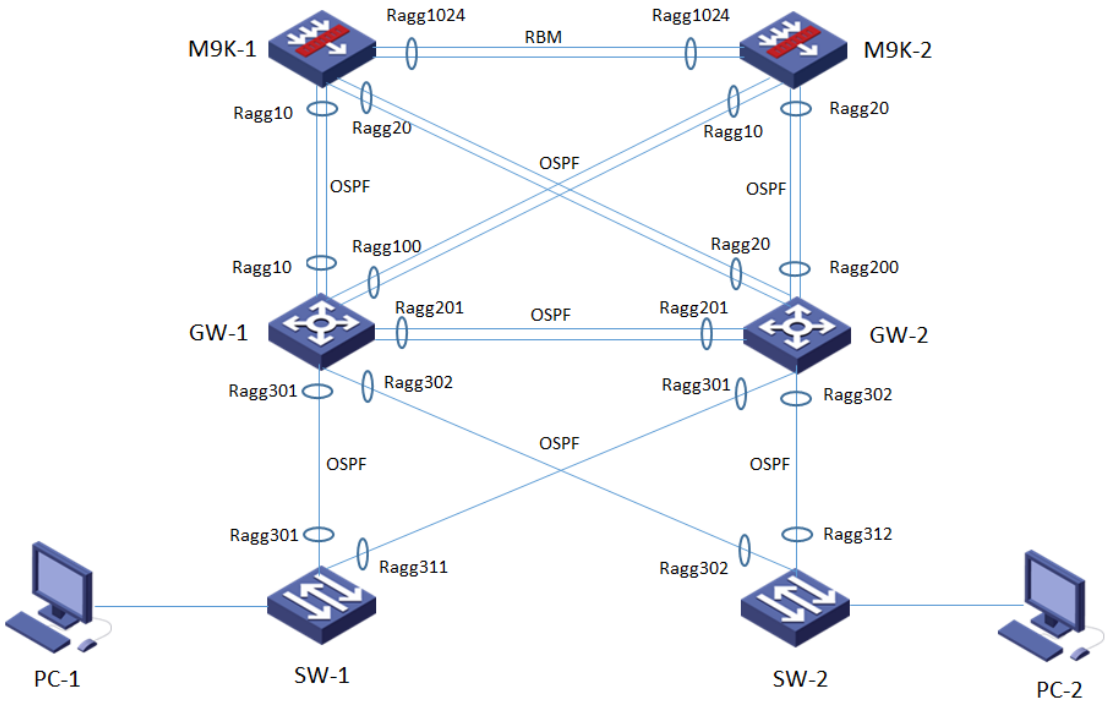
(7) 配置内网主机

#配置一部分主机的默认网关为 VRRP IPv6 备份组 3 的虚拟 IPv6 地址 1008:92::1，配置另一部分主机的默认网关为 VRRP IPv6 备份组 4 的虚拟 IPv6 地址 1008:92::2。

5.12 M9000 RBM+context+OSPF+VRF主备配置举例

5.12.1 组网需求

图5-12 RBM+context+OSPF+VRF 主备组网图



5.12.2 配置思路

- 配置前确保设备的软硬件环境一致
- 本配置中仅以 2 个租户为例
- 配置安全域及安全策略保证网络可达

5.12.3 配置步骤

(1) 配置 Device A

RBM 接口配置

```
#
interface Route-Aggregation1024
 ip address 137.0.0.5 255.255.255.0
 link-aggregation mode dynamic
 ipv6 address 137::5/64
#
interface Ten-GigabitEthernet0/0/20
 port link-mode route
```

```
 port link-aggregation group 1024
#
interface Ten-GigabitEthernet1/0/20
 port link-mode route
 port link-aggregation group 1024
#
```
#业务聚合口配置

```
#
interface Route-Aggregation10
link-aggregation mode dynamic
#
interface Route-Aggregation20
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet0/0/23
 port link-mode route
port link-aggregation group 10
#
interface Ten-GigabitEthernet1/0/23
 port link-mode route
port link-aggregation group 10
#
interface Ten-GigabitEthernet0/0/24
 port link-mode route
 port link-aggregation group 20
#
interface Ten-GigabitEthernet1/0/24
 port link-mode route
 port link-aggregation group 20
#
```
Track 配置

```
track 1 interface Ten-GigabitEthernet0/0/23 physical
track 2 interface Ten-GigabitEthernet1/0/23 physical
track 3 interface Ten-GigabitEthernet0/0/24 physical
track 4 interface Ten-GigabitEthernet1/0/24 physical
```
使用两台 Device 进行 HA 组网，Device A 作为主设备，Device B 作为备设备。当 Device A 或其链路发生故障时，由 Device B 接替 Device A 继续工作，保证业务不中断。

```
#
remote-backup group
```

```
 data-channel interface Route-Aggregation1024
 undo configuration auto-sync enable              #与 H3C 控制器配合需加此命令
 configuration sync-check interval 1
 delay-time 30
 adjust-cost ospf enable absolute 100
 adjust-cost ospfv3 enable absolute 100
 track 1
 track 2
 track 3
 track 4
 local-ipv6 137::5
 remote-ipv6 137::3
 device-role primary
#
```

#创建 context A

```
#
context test id 8
 context start
 location blade-controller-team 1
 allocate interface Route-Aggregation3 share
 allocate interface Route-Aggregation10 share
 allocate interface Route-Aggregation20 share
#
```

#配置 context A 中 2 个租户相关配置
#配置 VPN 实例

```
#
ip vpn-instance vrf1
ip vpn-instance vrf2
#
```

#配置动态路由 OSPF，保证路由可达

```
#
ospf 1001 router-id 10.10.1.2 vpn-instance vrf1
 description rou10.1001_tenant_1
 non-stop-routing
 import-route ospf 1002 type 1
 import-route ospf 10002 type 1
 area 0.0.0.0
#
ospf 1002 router-id 10.10.2.2 vpn-instance vrf1
 description rou10.1002_tenant_1
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
```

```
#
ospf 1003 router-id 10.10.3.2 vpn-instance vrf2
 description rou10.1003_tenant_2
 non-stop-routing
 import-route ospf 1004 type 1
 import-route ospf 10004 type 1
 area 0.0.0.0
#
ospf 1004 router-id 10.10.4.2 vpn-instance vrf2
 description rou10.1004_tenant_2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospf 10001 router-id 20.10.1.2 vpn-instance vrf1
 description rou20.1001_tenant_1
 non-stop-routing
 import-route ospf 1002 type 1
 import-route ospf 10002 type 1
 area 0.0.0.0
#
ospf 10002 router-id 20.10.2.2 vpn-instance vrf1
 description rou20.1002_tenant_1
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospf 10003 router-id 20.10.3.2 vpn-instance vrf2
 description rou20.1003_tenant_2
 non-stop-routing
 import-route ospf 1004 type 1
 import-route ospf 10004 type 1
 area 0.0.0.0
#
ospf 10004 router-id 20.10.4.2 vpn-instance vrf2
 description rou20.1004_tenant_2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospfv3 1001 vpn-instance vrf1
 router-id 10.10.1.2
 non-stop-routing
 import-route ospfv3 1002 type 1
 import-route ospfv3 10002 type 1
 area 0.0.0.0
#
ospfv3 1002 vpn-instance vrf1
```

```
 router-id 10.10.2.2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospfv3 1003 vpn-instance vrf2
 router-id 10.10.3.2
 non-stop-routing
 import-route ospfv3 1004 type 1
 import-route ospfv3 10004 type 1
 area 0.0.0.0
#
ospfv3 1004 vpn-instance vrf2
 router-id 10.10.4.2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospfv3 10001 vpn-instance vrf1
 router-id 20.10.1.2
 non-stop-routing
 import-route ospfv3 1002 type 1
 import-route ospfv3 10002 type 1
 area 0.0.0.0
#
ospfv3 10002 vpn-instance vrf1
 router-id 20.10.2.2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospfv3 10003 vpn-instance vrf2
 router-id 20.10.3.2
 non-stop-routing
 import-route ospfv3 1004 type 1
 import-route ospfv3 10004 type 1
 area 0.0.0.0
#
ospfv3 10004 vpn-instance vrf2
 router-id 20.10.4.2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
```

#配置 nat 地址组（业务配置，网络云通过 NFVO 平台下发）

```
#
nat address-group 1 name tenant_1
```

```
 address 222.1.1.2 222.1.1.2
#
nat address-group 2 name tenant_2
 address 222.1.2.2 222.1.2.2
#
```

#配置 ACL（业务配置，网络云通过 NFVO 平台下发）

```
#
acl advanced name tenant_1
 rule 0 permit ip vpn-instance vrf1
#
acl advanced name tenant_2
 rule 0 permit ip vpn-instance vrf2
#
```

#配置下行接口

```
#
interface Route-Aggregation10.1001
 description tenant_1
 ip binding vpn-instance vrf1
 ip address 10.10.1.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 1001 area 0.0.0.0
 ospfv3 1001 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 bfd enable
 ospfv3 network-type p2p
 vlan-type dot1q vid 1001
 ipv6 address 10:10:1::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation10.1003
 description tenant_2
 ip binding vpn-instance vrf2
 ip address 10.10.3.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
```

```
 ospf 1003 area 0.0.0.0
 ospfv3 1003 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 vlan-type dot1q vid 1003
 ipv6 address 10:10:3::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation20.1001
 description tenant_1
 ip binding vpn-instance vrf1
 ip address 20.10.1.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 10001 area 0.0.0.0
 ospfv3 10001 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 vlan-type dot1q vid 1001
 ipv6 address 20:10:1::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation20.1003
 description tenant_2
 ip binding vpn-instance vrf2
 ip address 20.10.3.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 10003 area 0.0.0.0
 ospfv3 10003 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
```

```
 vlan-type dot1q vid 1003
 ipv6 address 20:10:3::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
```

#配置上行接口

```
#
interface Route-Aggregation10.1002
 description tenant_1
 ip binding vpn-instance vrf1
 ip address 10.10.2.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 1002 area 0.0.0.0
 ospfv3 1002 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 nat outbound name tenant_1 address-group name tenant_1 vpn-instance vrf1----\\
```

（业务配置，网络云通过 NFVO 平台下发）

```
 vlan-type dot1q vid 1002
 ipv6 address 10:10:2::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation10.1004
 description tenant_2
 ip binding vpn-instance vrf2
 ip address 10.10.4.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 1004 area 0.0.0.0
 ospfv3 1004 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 nat outbound name tenant_2 address-group name tenant_2 vpn-instance vrf2----\\
```

（业务配置，网络云通过 NFVO 平台下发）

```
 vlan-type dot1q vid 1004
 ipv6 address 10:10:4::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation20.1002
 description tenant_1
 ip binding vpn-instance vrf1
 ip address 20.10.2.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 10002 area 0.0.0.0
 ospfv3 10002 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 nat outbound name tenant_1 address-group name tenant_1 vpn-instance vrf1----\\（业务配置，网络云通过 NFVO 平台下发）
 vlan-type dot1q vid 1002
 ipv6 address 20:10:2::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation20.1004
 description tenant_2
 ip binding vpn-instance vrf2
 ip address 20.10.4.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 10004 area 0.0.0.0
 ospfv3 10004 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 nat outbound name tenant_2 address-group name tenant_2 vpn-instance vrf2----（业务配置，网络云通过 NFVO 平台下发）
 vlan-type dot1q vid 1004
 ipv6 address 20:10:4::2/96
 bfd min-transmit-interval 100
```

```
 bfd min-receive-interval 100
 bfd detect-multiplier 4

#
```

#安全域

```
#
security-zone name Trust_vrf1
 import interface Route-Aggregation10.1001
 import interface Route-Aggregation20.1001
 #
security-zone name Untrust_vrf1
 import interface Route-Aggregation10.1002
 import interface Route-Aggregation20.1002
 #
security-zone name Trust_vrf2
 import interface Route-Aggregation10.1003
 import interface Route-Aggregation20.1003
#
security-zone name Untrust_vrf2
 import interface Route-Aggregation10.1004
 import interface Route-Aggregation20.1004
#
```

#安全策略（业务配置，网络云通过 NFVO 平台下发）

```
security-policy ip
 rule 0 name 0
  action pass
  vrf vrf1
  source-zone Trust-vrf1
  destination-zone local
   service ospf
  service bfd-control
  service ping
rule 1 name 1
  action pass
  vrf vrf1
  source-zone local
  destination-zone Trust-vrf1
  service ospf
  service bfd-control
  service ping
rule 2 name 2
  action pass
  vrf vrf1
  source-zone Untrust-vrf1
  destination-zone local
   service ospf
  service bfd-control
```

```
  service ping
rule 3 name 3
  action pass
  vrf vrf1
  source-zone local
  destination-zone Untrust-vrf1
  service ospf
  service bfd-control
  service ping
rule 4 name 4
  action pass
  vrf vrf2
  source-zone Trust-vrf2
  destination-zone local
   service ospf
  service bfd-control
  service ping
rule 5 name 5
  action pass
  vrf vrf2
  source-zone local
  destination-zone Trust-vrf2
  service ospf
  service bfd-control
  service ping
rule 6 name 6
  action pass
  vrf vrf2
  source-zone Untrust-vrf2
  destination-zone local
   service ospf
  service bfd-control
  service ping
rule 7 name 7
  action pass
  vrf vrf2
  source-zone local
  destination-zone Untrust-vrf2
  service ospf
  service bfd-control
  service ping
#

security-policy ipv6
rule 0 name 0
  action pass
  vrf vrf1
  source-zone Trust-vrf1
```

```
  destination-zone local
   service ospf
  service bfd-control
  service pingv6
rule 1 name 1
  action pass
  vrf vrf1
  source-zone local
  destination-zone Trust-vrf1
  service ospf
  service bfd-control
  service pingv6
rule 2 name 2
  action pass
  vrf vrf1
  source-zone Untrust-vrf1
  destination-zone local
   service ospf
  service bfd-control
  service pingv6
rule 3 name 3
  action pass
  vrf vrf1
  source-zone local
  destination-zone Untrust-vrf1
  service ospf
  service bfd-control
  service pingv6
#
rule 4 name 4
  action pass
  vrf vrf2
  source-zone Trust-vrf2
  destination-zone local
   service ospf
  service bfd-control
  service pingv6
rule 5 name 5
  action pass
  vrf vrf2
  source-zone local
  destination-zone Trust-vrf2
  service ospf
  service bfd-control
  service pingv6
rule 6 name 6
  action pass
  vrf vrf2
```

```
  source-zone Untrust-vrf2
  destination-zone local
   service ospf
  service bfd-control
  service pingv6
rule 7 name 7
  action pass
  vrf vrf2
  source-zone local
  destination-zone Untrust-vrf2
  service ospf
  service bfd-control
  service pingv6
#
```

(2) 配置 Device B

RBM 接口配置

```
#
interface Route-Aggregation1024
 ip address 137.0.0.3 255.255.255.0
 link-aggregation mode dynamic
 ipv6 address 137::3/64
#
interface Ten-GigabitEthernet0/0/20
 port link-mode route
 port link-aggregation group 1024
#
interface Ten-GigabitEthernet1/0/20
 port link-mode route
 port link-aggregation group 1024
#
```

#业务聚合口配置

```
#
interface Route-Aggregation10
link-aggregation mode dynamic
#
interface Route-Aggregation20
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet0/0/23
 port link-mode route
```

```
 port link-aggregation group 10
#
interface Ten-GigabitEthernet1/0/23
 port link-mode route
 port link-aggregation group 10
#
interface Ten-GigabitEthernet0/0/24
 port link-mode route
 port link-aggregation group 20
#
interface Ten-GigabitEthernet1/0/24
 port link-mode route
 port link-aggregation group 20
#
```

Track 配置

```
track 1 interface Ten-GigabitEthernet0/0/23 physical
track 2 interface Ten-GigabitEthernet1/0/23 physical
track 3 interface Ten-GigabitEthernet0/0/24 physical
track 4 interface Ten-GigabitEthernet1/0/24 physical
```

使用两台 Device 进行 HA 组网，Device A 作为主设备，Device B 作为备设备。当 Device A 或其链路发生故障时，由 Device B 接替 Device A 继续工作，保证业务不中断。

```
#
remote-backup group
 data-channel interface Route-Aggregation1024
 undo configuration auto-sync enable            #与 H3C 控制器配合需加此命令
 configuration sync-check interval 1
 delay-time 30
 adjust-cost ospf enable absolute 100
 adjust-cost ospfv3 enable absolute 100
 track 1
 track 2
 track 3
 track 4
 local-ipv6 137::3
 remote-ipv6 137::5 port 1024
 device-role secondary
#
```

#创建 context A

```
#
context test id 8
 context start
 location blade-controller-team 1
 allocate interface Route-Aggregation3 share
 allocate interface Route-Aggregation10 share
 allocate interface Route-Aggregation20 share
#
```

#配置 context A 中 2 个租户相关配置

#配置 VPN 实例

```
#
ip vpn-instance vrf1
ip vpn-instance vrf2
#
```

#配置动态路由 OSPF，保证路由可达

```
#
ospf 5001 router-id 100.10.1.2 vpn-instance vrf1
 description rou10.1001_tenant_1
 non-stop-routing
 import-route ospf 5002 type 1
 import-route ospf 50002 type 1
 area 0.0.0.0
#
ospf 5002 router-id 100.10.2.2 vpn-instance vrf1
 description rou10.1002_tenant_1
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospf 5003 router-id 100.10.3.2 vpn-instance vrf2
 description rou10.1003_tenant_2
 non-stop-routing
 import-route ospf 5004 type 1
 import-route ospf 50004 type 1
 area 0.0.0.0
#
ospf 5004 router-id 100.10.4.2 vpn-instance vrf2
 description rou10.1004_tenant_2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospf 50001 router-id 200.10.1.2 vpn-instance vrf1
 description rou20.1001_tenant_1
 non-stop-routing
 import-route ospf 5002 type 1
```

```
 import-route ospf 50002 type 1
 area 0.0.0.0
#
ospf 50002 router-id 200.10.2.2 vpn-instance vrf1
 description rou20.1002_tenant_1
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospf 50003 router-id 200.10.3.2 vpn-instance vrf2
 description rou20.1003_tenant_2
 non-stop-routing
 import-route ospf 5004 type 1
 import-route ospf 50004 type 1
 area 0.0.0.0
#
ospf 50004 router-id 200.10.4.2 vpn-instance vrf2
 description rou20.1004_tenant_2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospfv3 5001 vpn-instance vrf1
 router-id 100.10.1.2
 non-stop-routing
 import-route ospfv3 5002 type 1
 import-route ospfv3 50002 type 1
 area 0.0.0.0
#
ospfv3 5002 vpn-instance vrf1
 router-id 100.10.2.2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospfv3 5003 vpn-instance vrf2
 router-id 100.10.3.2
 non-stop-routing
 import-route ospfv3 5004 type 1
 import-route ospfv3 50004 type 1
 area 0.0.0.0
#
ospfv3 5004 vpn-instance vrf2
 router-id 100.10.4.2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
```

```
ospfv3 50001 vpn-instance vrf1
 router-id 200.10.1.2
 non-stop-routing
 import-route ospfv3 5002 type 1
 import-route ospfv3 50002 type 1
 area 0.0.0.0
#
ospfv3 50002 vpn-instance vrf1
 router-id 200.10.2.2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
ospfv3 50003 vpn-instance vrf2
 router-id 200.10.3.2
 non-stop-routing
 import-route ospfv3 5004 type 1
 import-route ospfv3 50004 type 1
 area 0.0.0.0
#
ospfv3 50004 vpn-instance vrf2
 router-id 200.10.4.2
 non-stop-routing
 default-route-advertise always type 1
 area 0.0.0.0
#
```

#配置 nat 地址组（业务配置，网络云通过 NFVO 平台下发）

```
#
nat address-group 1 name tenant_1
 address 222.1.1.2 222.1.1.2
#
nat address-group 2 name tenant_2
 address 222.1.2.2 222.1.2.2
#
```

#配置 ACL（业务配置，网络云通过 NFVO 平台下发）

```
#
acl advanced name tenant_1
 rule 0 permit ip vpn-instance vrf1
#
acl advanced name tenant_2
 rule 0 permit ip vpn-instance vrf2
#
```

#配置下行接口

```
#
interface Route-Aggregation10.1001
```

```
 description tenant_1
 ip binding vpn-instance vrf1
 ip address 100.10.1.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 5001 area 0.0.0.0
 ospfv3 5001 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 vlan-type dot1q vid 1001
 ipv6 address 100:10:1::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation10.1003
 description tenant_2
 ip binding vpn-instance vrf2
 ip address 100.10.3.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 5003 area 0.0.0.0
 ospfv3 5003 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 vlan-type dot1q vid 1003
 ipv6 address 100:10:3::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation20.1001
 description tenant_1
 ip binding vpn-instance vrf1
 ip address 200.10.1.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
```

```
 ospf network-type p2p
 ospf bfd enable
 ospf 50001 area 0.0.0.0
 ospfv3 50001 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 vlan-type dot1q vid 1001
 ipv6 address 200:10:1::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation20.1003
 description tenant_2
 ip binding vpn-instance vrf2
 ip address 200.10.3.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 50003 area 0.0.0.0
 ospfv3 50003 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 vlan-type dot1q vid 1003
 ipv6 address 200:10:3::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
```

#配置上行接口

```
#
interface Route-Aggregation10.1002
 description tenant_1
 ip binding vpn-instance vrf1
 ip address 100.10.2.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 5002 area 0.0.0.0
```

```
 ospfv3 5002 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 nat outbound name tenant_1 address-group name tenant_1 vpn-instance vrf1----\\（业务配置，网络云通过 NFVO 平台下发）
 vlan-type dot1q vid 1002
 ipv6 address 100:10:2::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation10.1004
 description tenant_2
 ip binding vpn-instance vrf2
 ip address 100.10.4.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 5004 area 0.0.0.0
 ospfv3 5004 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 nat outbound name tenant_2 address-group name tenant_2 vpn-instance vrf2----\\（业务配置，网络云通过 NFVO 平台下发）
 vlan-type dot1q vid 1004
 ipv6 address 100:10:4::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation20.1002
 description tenant_1
 ip binding vpn-instance vrf1
 ip address 200.10.2.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 50002 area 0.0.0.0
 ospfv3 50002 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
```

```
 ospfv3 bfd enable
 ospfv3 network-type p2p
 nat outbound name tenant_1 address-group name tenant_1 vpn-instance vrf1----\\（业务配置，网络云通过 NFVO 平台下发）
 vlan-type dot1q vid 1002
 ipv6 address 200:10:2::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
interface Route-Aggregation20.1004
 description tenant_2
 ip binding vpn-instance vrf2
 ip address 200.10.4.2 255.255.255.0
 ospf cost 10
 ospf timer hello 1
 ospf authentication-mode md5 1 plain 123456
 ospf network-type p2p
 ospf bfd enable
 ospf 50004 area 0.0.0.0
 ospfv3 50004 area 0.0.0.0
 ospfv3 cost 10
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 nat outbound name tenant_2 address-group name tenant_2 vpn-instance vrf2----\\（业务配置，网络云通过 NFVO 平台下发）
 vlan-type dot1q vid 1004
 ipv6 address 200:10:4::2/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#
```

#安全域

```
#
security-zone name Trust_vrf1
 import interface Route-Aggregation10.1001
 import interface Route-Aggregation20.1001
 #
security-zone name Untrust_vrf1
 import interface Route-Aggregation10.1002
 import interface Route-Aggregation20.1002
 #
security-zone name Trust_vrf2
 import interface Route-Aggregation10.1003
 import interface Route-Aggregation20.1003
#
security-zone name Untrust_vrf2
```

```
 import interface Route-Aggregation10.1004
 import interface Route-Aggregation20.1004
#
#安全策略（业务配置，网络云通过 NFVO 平台下发）
security-policy ip
 rule 0 name 0
  action pass
  vrf vrf1
  source-zone Trust-vrf1
  destination-zone local
   service ospf
  service bfd-control
  service ping
rule 1 name 1
  action pass
  vrf vrf1
  source-zone local
  destination-zone Trust-vrf1
  service ospf
  service bfd-control
  service ping
rule 2 name 2
  action pass
  vrf vrf1
  source-zone Untrust-vrf1
  destination-zone local
   service ospf
  service bfd-control
  service ping
rule 3 name 3
  action pass
  vrf vrf1
  source-zone local
  destination-zone Untrust-vrf1
  service ospf
  service bfd-control
  service ping
rule 4 name 4
  action pass
  vrf vrf2
  source-zone Trust-vrf2
  destination-zone local
   service ospf
  service bfd-control
  service ping
rule 5 name 5
  action pass
  vrf vrf2
```

```
  source-zone local
  destination-zone Trust-vrf2
  service ospf
  service bfd-control
  service ping
rule 6 name 6
  action pass
  vrf vrf2
  source-zone Untrust-vrf2
  destination-zone local
   service ospf
  service bfd-control
  service ping
rule 7 name 7
  action pass
  vrf vrf2
  source-zone local
  destination-zone Untrust-vrf2
  service ospf
  service bfd-control
  service ping
#

security-policy ipv6
rule 0 name 0
  action pass
  vrf vrf1
  source-zone Trust-vrf1
  destination-zone local
   service ospf
  service bfd-control
  service pingv6
rule 1 name 1
  action pass
  vrf vrf1
  source-zone local
  destination-zone Trust-vrf1
  service ospf
  service bfd-control
  service pingv6
rule 2 name 2
  action pass
  vrf vrf1
  source-zone Untrust-vrf1
  destination-zone local
   service ospf
  service bfd-control
  service pingv6
```

```
rule 3 name 3
  action pass
  vrf vrf1
  source-zone local
  destination-zone Untrust-vrf1
  service ospf
  service bfd-control
  service pingv6
#
rule 4 name 4
  action pass
  vrf vrf2
  source-zone Trust-vrf2
  destination-zone local
   service ospf
  service bfd-control
  service pingv6
rule 5 name 5
  action pass
  vrf vrf2
  source-zone local
  destination-zone Trust-vrf2
  service ospf
  service bfd-control
  service pingv6
rule 6 name 6
  action pass
  vrf vrf2
  source-zone Untrust-vrf2
  destination-zone local
   service ospf
  service bfd-control
  service pingv6
rule 7 name 7
  action pass
  vrf vrf2
  source-zone local
  destination-zone Untrust-vrf2
  service ospf
  service bfd-control
  service pingv6
#
```

(3) 配置 Gateway 1

创建 VPN 实例

```
#
ip vpn-instance vrf1_1
#
```

```
ip vpn-instance vrf1_2
#
ip vpn-instance vrf2_1
#
ip vpn-instance vrf2_2
#
```
#配置动态路由 OSPF，保证路由可达
```
#
ospf 1001 router-id 10.10.1.1 vpn-instance vrf1_1
 description rou10.1001_tenant_1
 non-stop-routing
 area 0.0.0.0
  network 10.10.1.0 0.0.0.255
  network 100.10.1.0 0.0.0.255
  network 101.1.1.0 0.0.0.255
  network 201.1.1.0 0.0.0.255
#
ospf 1002 router-id 10.10.2.1 vpn-instance vrf1_2
 description rou10.1002_tenant_1
 non-stop-routing
 area 0.0.0.0
  network 10.10.2.0 0.0.0.255
  network 100.10.2.0 0.0.0.255
  network 101.101.1.0 0.0.0.255
  network 201.1.2.0 0.0.0.255
#
ospf 1003 router-id 10.10.3.1 vpn-instance vrf2_1
 description rou10.1003_tenant_2
 non-stop-routing
 area 0.0.0.0
  network 10.10.3.0 0.0.0.255
  network 100.10.3.0 0.0.0.255
  network 101.1.3.0 0.0.0.255
  network 201.1.3.0 0.0.0.255
#
ospf 1004 router-id 10.10.4.1 vpn-instance vrf2_2
 description rou10.1004_tenant_2
 non-stop-routing
 area 0.0.0.0
  network 10.10.4.0 0.0.0.255
  network 100.10.4.0 0.0.0.255
  network 101.101.4.0 0.0.0.255
  network 201.1.4.0 0.0.0.255
#
ospfv3 1001 vpn-instance vrf1_1
 router-id 10.10.1.1
 non-stop-routing
 area 0.0.0.0
```

```
#
ospfv3 1002 vpn-instance vrf1_2
 router-id 10.10.2.1
 non-stop-routing
 area 0.0.0.0
#
ospfv3 1003 vpn-instance vrf2_1
 router-id 10.10.3.1
 non-stop-routing
 area 0.0.0.0
#
ospfv3 1004 vpn-instance vrf2_2
 router-id 10.10.4.1
 non-stop-routing
 area 0.0.0.0
#
```

#配置接口

```
#连接 RBM 主框租户 1 下行口
interface Route-Aggregation10.1001
 description tenant_1
 ip binding vpn-instance vrf1_1
 ip address 10.10.1.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$0NOjAriIRvuNdf58zgsncdYW6wNmt8NIUQ==
 ospf timer hello 1
 ospf network-type p2p
 ospf 1001 area 0.0.0.0
 ospf bfd enable
 ospfv3 1001 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 10:10:1::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 主框租户 1  上行口
interface Route-Aggregation10.1002
 description tenant_1
 ip binding vpn-instance vrf1_2
 ip address 10.10.2.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$2qq9v6mKvM/KeqPSTHC5qmWUAtr3iE0Ygg==
 ospf timer hello 1
 ospf network-type p2p
 ospf 1002 area 0.0.0.0
 ospf bfd enable
 ospfv3 1002 area 0.0.0.0
 ospfv3 timer hello 1
```

```
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 10:10:2::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 主框租户 2 下行口
interface Route-Aggregation10.1003
 description tenant_2
 ip binding vpn-instance vrf2_1
 ip address 10.10.3.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$1f0Dq/1fQR40tVY/HH2N7ML+hFnltK121g==
 ospf timer hello 1
 ospf network-type p2p
 ospf 1003 area 0.0.0.0
 ospf bfd enable
 ospfv3 1003 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 10:10:3::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 主框租户 2 上行口
interface Route-Aggregation10.1004
 description tenant_2
 ip binding vpn-instance vrf2_2
 ip address 10.10.4.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$+RZv1315VQ5UG+f30EBAdm+jRxfvWLYT6Q==
 ospf timer hello 1
 ospf network-type p2p
 ospf 1004 area 0.0.0.0
 ospf bfd enable
 ospfv3 1004 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 10:10:4::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 备框租户 1 下行口
interface Route-Aggregation100.1001
 description tenant_1
 ip binding vpn-instance vrf1_1
 ip address 100.10.1.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$3J1xMzfqWInp9vnegVPnVFzqp7Yjimfi4A==
```

```
 ospf timer hello 1
 ospf network-type p2p
 ospf 1001 area 0.0.0.0
 ospf bfd enable
 ospfv3 1001 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 100:10:1::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 备框租户 1 上行口
interface Route-Aggregation100.1002
 description tenant_1
 ip binding vpn-instance vrf1_2
 ip address 100.10.2.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$SzliQlQSbGN4qC0KYBdPxW+x0NP8zWQ0Wg==
 ospf timer hello 1
 ospf network-type p2p
 ospf 1002 area 0.0.0.0
 ospf bfd enable
 ospfv3 1002 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 100:10:2::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 备框租户 2 下行口
interface Route-Aggregation100.1003
 description tenant_2
 ip binding vpn-instance vrf2_1
 ip address 100.10.3.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$4eIKCEuoL5J4UjAiFfUd2fQUFgPLRAXLvg==
 ospf timer hello 1
 ospf network-type p2p
 ospf 1003 area 0.0.0.0
 ospf bfd enable
 ospfv3 1003 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 100:10:3::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
```

```
#连接 RBM 备框租户 2 上行口
interface Route-Aggregation100.1004
 description tenant_2
 ip binding vpn-instance vrf2_2
 ip address 100.10.4.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$XaWkQEp/AU8Ba5g+HHs2FtGd4ztD90rffw==
 ospf timer hello 1
 ospf network-type p2p
 ospf 1004 area 0.0.0.0
 ospf bfd enable
 ospfv3 1004 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 100:10:4::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 GW-2（租户 1）
interface Route-Aggregation201.1001
 description to-Border2_tenant_1
 ip binding vpn-instance vrf1_1
 ip address 201.1.1.1 255.255.255.0
 ospf cost 10
 ospf 1001 area 0.0.0.0
 ospfv3 1001 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 201:1:1::1/96
#连接 GW-2（租户 1）
interface Route-Aggregation201.1002
 description to-Border2_tenant_1
 ip binding vpn-instance vrf1_2
 ip address 201.1.2.1 255.255.255.0
 ospf cost 10
 ospf 1002 area 0.0.0.0
 ospfv3 1002 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 201:1:2::1/96
#连接 GW-2（租户 2）
interface Route-Aggregation201.1003
 description to-Border2_tenant_2
 ip binding vpn-instance vrf2_1
 ip address 201.1.3.1 255.255.255.0
 ospf cost 10
 ospf 1003 area 0.0.0.0
 ospfv3 1003 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 201:1:3::1/96
```

```
#连接 GW-2（租户 2）
interface Route-Aggregation201.1004
 description to-Border2_tenant_2
 ip binding vpn-instance vrf2_2
 ip address 201.1.4.1 255.255.255.0
 ospf cost 10
 ospf 1004 area 0.0.0.0
 ospfv3 1004 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 201:1:4::1/96
#连接 PC-1 方向交换机（租户 1）
interface Route-Aggregation301.1001
 description to-leaf
 ip binding vpn-instance vrf1_1
 ip address 101.1.1.2 255.255.255.0
 ospf cost 10
 ospf 1001 area 0.0.0.0
 ospfv3 1001 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 101:1:1::2/96
#连接 PC-1 方向交换机（租户 2）
interface Route-Aggregation301.1003
 description to-leaf_tenant_2
 ip binding vpn-instance vrf2_1
 ip address 101.1.3.2 255.255.255.0
 ospf cost 10
 ospf 1003 area 0.0.0.0
 ospfv3 1003 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 101:1:3::2/96
#连接 PC-2 方向交换机（租户 1）
interface Route-Aggregation302.1002
 description to-public
 ip binding vpn-instance vrf1_2
 ip address 101.101.1.2 255.255.255.0
 ospf cost 10
 ospf 1002 area 0.0.0.0
 ospfv3 1002 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 101:101:1::2/96
#连接 PC-2 方向交换机（租户 2）
interface Route-Aggregation302.1004
 description to-public_tenant_2
 ip binding vpn-instance vrf2_2
 ip address 101.101.4.2 255.255.255.0
 ospf cost 10
 ospf 1004 area 0.0.0.0
 ospfv3 1004 area 0.0.0.0
```

```
 ospfv3 cost 10
 ipv6 address 101:101:4::2/96
#
```

(4) 配置 Gateway 2

创建 VPN 实例

```
#
ip vpn-instance vrf1_1
#
ip vpn-instance vrf1_2
#
ip vpn-instance vrf2_1
#
ip vpn-instance vrf2_2
#
```

#配置动态路由 OSPF，保证路由可达

```
#
ospf 10001 router-id 20.10.1.1 vpn-instance vrf1_1
 description rou20.1001_tenant_1
 non-stop-routing
 area 0.0.0.0
  network 20.10.1.0 0.0.0.255
  network 102.1.1.0 0.0.0.255
  network 200.10.1.0 0.0.0.255
  network 201.1.1.0 0.0.0.255
#
ospf 10002 router-id 20.10.2.1 vpn-instance vrf1_2
 description rou20.1002_tenant_1
 non-stop-routing
 area 0.0.0.0
  network 20.10.2.0 0.0.0.255
  network 102.102.1.0 0.0.0.255
  network 200.10.2.0 0.0.0.255
  network 201.1.2.0 0.0.0.255
#
ospf 10003 router-id 20.10.3.1 vpn-instance vrf2_1
 description rou20.1003_tenant_2
 non-stop-routing
 area 0.0.0.0
  network 20.10.3.0 0.0.0.255
  network 102.1.3.0 0.0.0.255
  network 200.10.3.0 0.0.0.255
  network 201.1.3.0 0.0.0.255
#
ospf 10004 router-id 20.10.4.1 vpn-instance vrf2_2
 description rou20.1004_tenant_2
 non-stop-routing
 area 0.0.0.0
  network 20.10.4.0 0.0.0.255
```

```
  network 102.102.4.0 0.0.0.255
  network 200.10.4.0 0.0.0.255
  network 201.1.4.0 0.0.0.255
#
ospfv3 10001 vpn-instance vrf1_1
 router-id 20.10.1.1
 non-stop-routing
 area 0.0.0.0
#
ospfv3 10002 vpn-instance vrf1_2
 router-id 20.10.2.1
 non-stop-routing
 area 0.0.0.0
#
ospfv3 10003 vpn-instance vrf2_1
 router-id 20.10.3.1
 non-stop-routing
 area 0.0.0.0
#
ospfv3 10004 vpn-instance vrf2_2
 router-id 20.10.4.1
 non-stop-routing
 area 0.0.0.0
#
```

#配置接口

```
#连接 RBM 主框租户 1 下行口
interface Route-Aggregation20.1001
 description tenant_1
 ip binding vpn-instance vrf1_1
 ip address 20.10.1.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$P5xXCb+N+Ek7QJP6mRv75aFmyr+zklKIfA==
 ospf timer hello 1
 ospf network-type p2p
 ospf 10001 area 0.0.0.0
 ospf bfd enable
 ospfv3 10001 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 20:10:1::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 主框租户 1 上行口
interface Route-Aggregation20.1002
 description tenant_1
 ip binding vpn-instance vrf1_2
 ip address 20.10.2.1 255.255.255.0
```

```
 ospf authentication-mode md5 1 cipher $c$3$PAwIMWaO5+xwo8srZl2IAgkSWECGHWXX0g==
 ospf timer hello 1
 ospf network-type p2p
 ospf 10002 area 0.0.0.0
 ospf bfd enable
 ospfv3 10002 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 20:10:2::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 主框租户 2 下行口
interface Route-Aggregation20.1003
 description tenant_2
 ip binding vpn-instance vrf2_1
 ip address 20.10.3.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$qhw6oi05jtmT7VenjRoRrhKWS0x4XhXkxw==
 ospf timer hello 1
 ospf network-type p2p
 ospf 10003 area 0.0.0.0
 ospf bfd enable
 ospfv3 10003 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 20:10:3::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 主框租户 2 上行口
interface Route-Aggregation20.1004
 description tenant_2
 ip binding vpn-instance vrf2_2
 ip address 20.10.4.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$i/rk0lNgfn47LiX1xn9H4TgNuQgq4Qkqyg==
 ospf timer hello 1
 ospf network-type p2p
 ospf 10004 area 0.0.0.0
 ospf bfd enable
 ospfv3 10004 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 20:10:4::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
```

```
 bfd detect-multiplier 4
#连接 RBM 备框租户 1 下行口
interface Route-Aggregation200.1001
 description tenant_1
 ip binding vpn-instance vrf1_1
 ip address 200.10.1.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$os6VTxU42fr+SihvMI6xwldfNI8v2Hlh9w==
 ospf timer hello 1
 ospf network-type p2p
 ospf 10001 area 0.0.0.0
 ospf bfd enable
 ospfv3 10001 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 200:10:1::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 备框租户 1 上行口
interface Route-Aggregation200.1002
 description tenant_1
 ip binding vpn-instance vrf1_2
 ip address 200.10.2.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$OcjRgCJx1wKihfP37miCRj/aVC5hHuEjrg==
 ospf timer hello 1
 ospf network-type p2p
 ospf 10002 area 0.0.0.0
 ospf bfd enable
 ospfv3 10002 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 200:10:2::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 备框租户 2 下行口
interface Route-Aggregation200.1003
 description tenant_2
 ip binding vpn-instance vrf2_1
 ip address 200.10.3.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$CXlXQJu0llsXO1GVIGD3uJoEK3Mfcq1ITg==
 ospf timer hello 1
 ospf network-type p2p
 ospf 10003 area 0.0.0.0
 ospf bfd enable
 ospfv3 10003 area 0.0.0.0
```

```
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 200:10:3::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 RBM 备框租户 2 上行口
interface Route-Aggregation200.1004
 description tenant_2
 ip binding vpn-instance vrf2_2
 ip address 200.10.4.1 255.255.255.0
 ospf authentication-mode md5 1 cipher $c$3$6R644NUbpD+yGThVFFqd71eHXUZUCYW/Mw==
 ospf timer hello 1
 ospf network-type p2p
 ospf 10004 area 0.0.0.0
 ospf bfd enable
 ospfv3 10004 area 0.0.0.0
 ospfv3 timer hello 1
 ospfv3 bfd enable
 ospfv3 network-type p2p
 ipv6 address 200:10:4::1/96
 bfd min-transmit-interval 100
 bfd min-receive-interval 100
 bfd detect-multiplier 4
#连接 GW-1（租户 1）
interface Route-Aggregation201.1001
 description to-Border1
 ip binding vpn-instance vrf1_1
 ip address 201.1.1.2 255.255.255.0
 ospf cost 10
 ospf 10001 area 0.0.0.0
 ospfv3 10001 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 201:1:1::2/96
#连接 GW-1（租户 1）
interface Route-Aggregation201.1002
 description to-Border1
 ip binding vpn-instance vrf1_2
 ip address 201.1.2.2 255.255.255.0
 ospf cost 10
 ospf 10002 area 0.0.0.0
 ospfv3 10002 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 201:1:2::2/96
#连接 GW-1（租户 2）
interface Route-Aggregation201.1003
 description to-Border1_tenant_2
```

```
 ip binding vpn-instance vrf2_1
 ip address 201.1.3.2 255.255.255.0
 ospf cost 10
 ospf 10003 area 0.0.0.0
 ospfv3 10003 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 201:1:3::2/96
#连接 GW-1（租户 2）
interface Route-Aggregation201.1004
 description to-Border1_tenant_2
 ip binding vpn-instance vrf2_2
 ip address 201.1.4.2 255.255.255.0
 ospf cost 10
 ospf 10004 area 0.0.0.0
 ospfv3 10004 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 201:1:4::2/96
#连接 PC-1 方向交换机（租户 1）
interface Route-Aggregation301.1001
 description to-leaf
 ip binding vpn-instance vrf1_1
 ip address 102.1.1.2 255.255.255.0
 ospf cost 10
 ospf 10001 area 0.0.0.0
 ospfv3 10001 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 102:1:1::2/96
#连接 PC-1 方向交换机（租户 2）
interface Route-Aggregation301.1003
 description to-leaf_tenant_2
 ip binding vpn-instance vrf2_1
 ip address 102.1.3.2 255.255.255.0
 ospf cost 10
 ospf 10003 area 0.0.0.0
 ospfv3 10003 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 102:1:3::2/96
#连接 PC-2 方向交换机（租户 1）
interface Route-Aggregation302.1002
 description to-public
 ip binding vpn-instance vrf1_2
 ip address 102.102.1.2 255.255.255.0
 ospf cost 10
 ospf 10002 area 0.0.0.0
 ospfv3 10002 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 102:102:1::2/96
#连接 PC-2 方向交换机（租户 2）
```

```
interface Route-Aggregation302.1004
 description to-public_tenant_2
 ip binding vpn-instance vrf2_2
 ip address 102.102.4.2 255.255.255.0
 ospf cost 10
 ospf 10004 area 0.0.0.0
 ospfv3 10004 area 0.0.0.0
 ospfv3 cost 10
 ipv6 address 102:102:4::2/96
#
```

5.12.4 配置注意事项

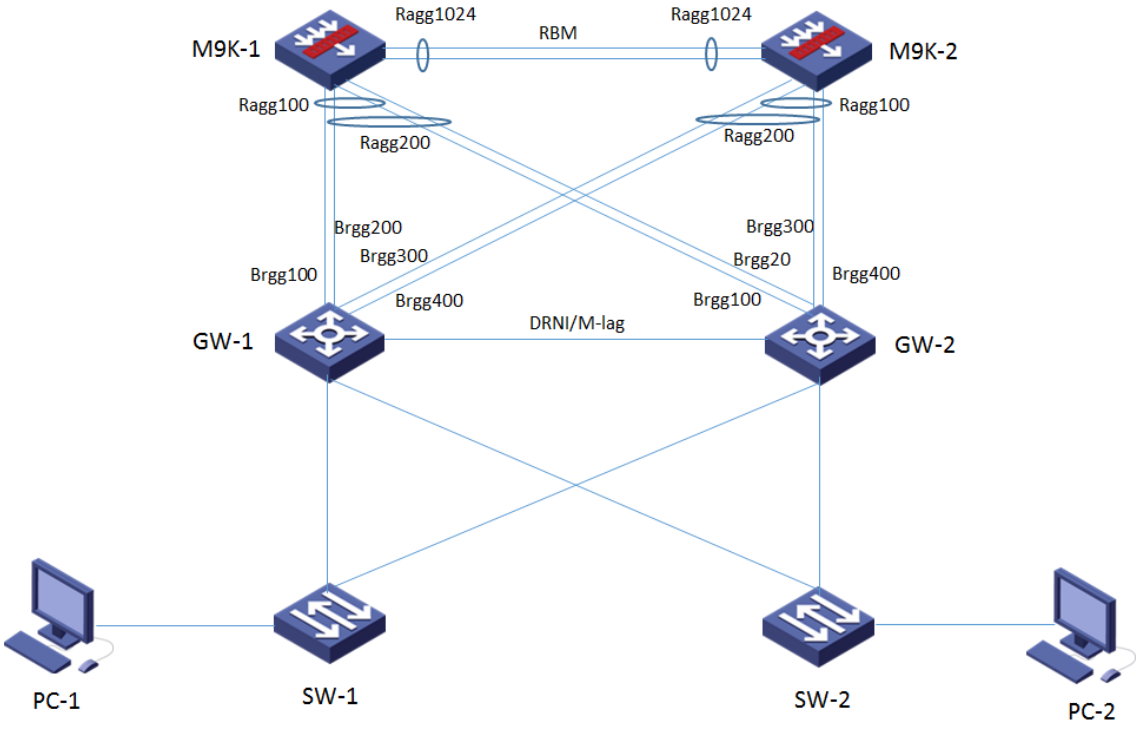
- 在配置之前确保内外网路由可达

5.13 M9000 RBM+context+VRRP+VRF主备配置举例

5.13.1 组网需求

如图 1 所示，Device 的上、下行业务接口均为三层接口，为提高业务稳定性，使用两台 Device 进行 RBM 双机热备组网，Device A 作为主设备，Device B 作为备设备。Host 访问 Internet 的流量正常情况下由 DeviceA 进行转发，当 Device A 或其链路发生故障时，由 Device B 接替 Device A 继续工作，保证业务不中断。

图5-13 RBM+context+VRRP+VRF 主备组网单租户图



5.13.2 配置思路

- 配置前确保设备的软硬件环境一致
- 本配置中仅以 2 个租户为例
- 配置安全域及安全策略保证网络可达

(1) 配置 Device A

RBM 接口配置

```
#
interface Route-Aggregation1024
 ip address 137.0.0.5 255.255.255.0
 link-aggregation mode dynamic
 ipv6 address 137::5/64
#
interface Ten-GigabitEthernet0/0/20
 port link-mode route
 port link-aggregation group 1024
#
interface Ten-GigabitEthernet1/0/20
 port link-mode route
 port link-aggregation group 1024
#
```

#业务聚合口配置

```
#
```

```
interface Route-Aggregation100
link-aggregation mode dynamic
#
interface Route-Aggregation200
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet0/0/23
 port link-mode route
port link-aggregation group 100
#
interface Ten-GigabitEthernet1/0/23
 port link-mode route
port link-aggregation group 100
#
interface Ten-GigabitEthernet0/0/24
 port link-mode route
 port link-aggregation group 200
#
interface Ten-GigabitEthernet1/0/24
 port link-mode route
 port link-aggregation group 200
#
```

Track 配置

```
track 1 interface Ten-GigabitEthernet0/0/23 physical
track 2 interface Ten-GigabitEthernet1/0/23 physical
track 3 interface Ten-GigabitEthernet0/0/24 physical
track 4 interface Ten-GigabitEthernet1/0/24 physical
```

使用两台 Device 进行 HA 组网，Device A 作为主设备，Device B 作为备设备。当 Device A 或其链路发生故障时，由 Device B 接替 Device A 继续工作，保证业务不中断。

```
#
remote-backup group
 data-channel interface Route-Aggregation1024
 undo configuration auto-sync enable            #与 H3C 控制器配合需加此命令
 configuration sync-check interval 1
 delay-time 30
 track 1
 track 2
 track 3
```

```
 track 4
 local-ipv6 137::5
 remote-ipv6 137::3
 device-role primary
#
```

#创建 context A

```
#
context VFW_4158082000 id 2
 context start
 location blade-controller-team 1
 allocate interface Route-Aggregation3 share
 allocate interface Route-Aggregation100 share
 allocate interface Route-Aggregation200 share
#
```

#配置 context A 下行口，vrid 一样

```
 #
 interface Route-Aggregation100.2000
  ip binding vpn-instance lwy_1_R1_123412
  ip address 33.1.1.3 255.255.255.254
  vrrp vrid 6 virtual-ip 5.1.1.3 255.255.255.254 active
  vlan-type dot1q vid 2000
  ipv6 address 33::1:3/127
  vrrp ipv6 vrid 6 virtual-ip FE80:2021::1:1 link-local active
  vrrp ipv6 vrid 6 virtual-ip 5::1:2 127
 #
 interface Route-Aggregation100.2005
  ip binding vpn-instance lwy_1_1_R4_112233
  ip address 34.1.1.20 255.255.255.254
  vrrp vrid 6 virtual-ip 6.1.1.13 255.255.255.254 active
  vlan-type dot1q vid 2005
  ipv6 address 34::1:15/127
  vrrp ipv6 vrid 6 virtual-ip FE80:2021::1:A link-local active
  vrrp ipv6 vrid 6 virtual-ip 6::1:D 127
 #
```

#配置 context A 上行口，vrid 一样

```
 #
 interface Route-Aggregation200.4016
  ip binding vpn-instance external_vpn_4016
  ip address 33.1.1.4 255.255.255.254
  vrrp vrid 5 virtual-ip 222.1.0.1 255.255.0.0 active
  vlan-type dot1q vid 4016
  ipv6 address 33::1:5/127
  vrrp ipv6 vrid 5 virtual-ip FE80:2021::1:2 link-local active
  vrrp ipv6 vrid 5 virtual-ip 222::2 96
 #
 interface Route-Aggregation200.4017
```

```
 ip binding vpn-instance external_vpn_4017
 ip address 34.1.1.10 255.255.255.254
 vrrp vrid 5 virtual-ip 223.1.0.5 255.255.0.0 active
 vlan-type dot1q vid 4017
 ipv6 address 34::1:A/127
 vrrp ipv6 vrid 5 virtual-ip FE80:2021::1:3 link-local active
 vrrp ipv6 vrid 5 virtual-ip 223::5 96
#
```

#配置 context A 路由

```
ip route-static vpn-instance lwy_1_1_R4_112233 0.0.0.0 0 vpn-instance external_vpn_4017
223.1.1.1
ip route-static vpn-instance external_vpn_4017 211.1.1.0 24 vpn-instance
lwy_1_1_R4_112233 6.1.1.12
ip route-static vpn-instance lwy_1_R1_123412 0.0.0.0 0 vpn-instance external_vpn_4016
222.1.1.1
ip route-static vpn-instance external_vpn_4016 111.1.1.0 24 vpn-instance lwy_1_R1_123412
5.1.1.2
```

#配置 contextA 安全域和安全策略

```
Name: Trust
Members:
  Route-Aggregation100.2000
  Route-Aggregation100.2005

Name: Untrust
Members:
  Route-Aggregation200.4016
  Route-Aggregation200.4017
```

#配置 contextA 安全策略

```
#
security-policy ip
 rule 0 name 0
  action pass
  vrf lwy_1_1_R4_112233
  source-zone local
  source-zone Trust
  source-zone Untrust
  destination-zone local
  destination-zone Trust
  destination-zone Untrust

 rule 1 name 1
  action pass
  vrf lwy_1_R1_123412
  source-zone local
  source-zone Trust
  source-zone Untrust
```

```
  destination-zone local
  destination-zone Trust
  destination-zone Untrust

 rule 2 name 2
  action pass
  vrf external_vpn_4016
  source-zone local
  source-zone Trust
  source-zone Untrust
  destination-zone local
  destination-zone Trust
  destination-zone Untrust

rule 65000 name 65000
  action pass
  service vrrp
```

(2) 配置 Device B

RBM 接口配置

```
#
interface Route-Aggregation1024
 ip address 137.0.0.3 255.255.255.0
 link-aggregation mode dynamic
 ipv6 address 137::3/64
#
interface Ten-GigabitEthernet0/0/20
 port link-mode route
 port link-aggregation group 1024
#
interface Ten-GigabitEthernet1/0/20
 port link-mode route
 port link-aggregation group 1024
#
```

#业务聚合口配置

```
#
interface Route-Aggregation100
link-aggregation mode dynamic
#
interface Route-Aggregation200
link-aggregation mode dynamic
#
interface Ten-GigabitEthernet0/0/23
 port link-mode route
```

```
port link-aggregation group 100
#
interface Ten-GigabitEthernet1/0/23
 port link-mode route
port link-aggregation group 100
#
interface Ten-GigabitEthernet0/0/24
 port link-mode route
 port link-aggregation group 200
#
interface Ten-GigabitEthernet1/0/24
 port link-mode route
 port link-aggregation group 200
#
```

Track 配置

```
track 1 interface Ten-GigabitEthernet0/0/23 physical
track 2 interface Ten-GigabitEthernet1/0/23 physical
track 3 interface Ten-GigabitEthernet0/0/24 physical
track 4 interface Ten-GigabitEthernet1/0/24 physical
```

使用两台 Device 进行 HA 组网，Device A 作为主设备，Device B 作为备设备。当 Device A 或其链路发生故障时，由 Device B 接替 Device A 继续工作，保证业务不中断。

```
#
remote-backup group
 data-channel interface Route-Aggregation1024
 undo configuration auto-sync enable            #与 H3C 控制器配合需加此命令
 configuration sync-check interval 1
 delay-time 30
 track 1
 track 2
 track 3
 track 4
 local-ipv6 137::3
 remote-ipv6 137::5
 device-role secondary
#
```

#创建 context A

```
#
context VFW_4158082000 id 2
 context start
```

```
 location blade-controller-team 1
 allocate interface Route-Aggregation3 share
 allocate interface Route-Aggregation100 share
 allocate interface Route-Aggregation200 share
#
```

#配置 context A 下行口，vrid 一样

```
#
interface Route-Aggregation100.2000
 ip binding vpn-instance lwy_1_R1_123412
 ip address 33.1.1.7 255.255.255.254
 vrrp vrid 6 virtual-ip 5.1.1.3 255.255.255.254 standby
 vlan-type dot1q vid 2000
 ipv6 address 33::1:7/127
 vrrp ipv6 vrid 6 virtual-ip FE80:2021::1:1 link-local standby
 vrrp ipv6 vrid 6 virtual-ip 5::1:2 127
#
interface Route-Aggregation100.2005
 ip binding vpn-instance lwy_1_1_R4_112233
 ip address 34.1.1.29 255.255.255.254
 vrrp vrid 6 virtual-ip 6.1.1.13 255.255.255.254 standby
 vlan-type dot1q vid 2005
 ipv6 address 34::1:19/127
 vrrp ipv6 vrid 6 virtual-ip FE80:2021::1:A link-local standby
 vrrp ipv6 vrid 6 virtual-ip 6::1:D 127
#
```

#配置 context A 上行口，vrid 一样

```
 #
 interface Route-Aggregation200.4016
 ip binding vpn-instance external_vpn_4016
  ip address 33.1.1.6 255.255.255.254
  vrrp vrid 5 virtual-ip 222.1.0.1 255.255.0.0 standby
 vlan-type dot1q vid 4016
  ipv6 address 33::1:6/127
  vrrp ipv6 vrid 5 virtual-ip FE80:2021::1:2 link-local standby
  vrrp ipv6 vrid 5 virtual-ip 222::2 96
 #
 interface Route-Aggregation200.4017
 ip binding vpn-instance external_vpn_4017
  ip address 34.1.1.12 255.255.255.254
 vrrp vrid 5 virtual-ip 223.1.0.5 255.255.0.0 standby
 vlan-type dot1q vid 4017
  ipv6 address 34::1:C/127
  vrrp ipv6 vrid 5 virtual-ip FE80:2021::1:3 link-local standby
  vrrp ipv6 vrid 5 virtual-ip 223::5 96
 #
```

#配置 context A 路由

```
ip route-static vpn-instance lwy_1_1_R4_112233 0.0.0.0 0 vpn-instance external_vpn_4017
223.1.1.1
```

```
ip route-static vpn-instance external_vpn_4017 211.1.1.0 24 vpn-instance
lwy_1_1_R4_112233 6.1.1.12
ip route-static vpn-instance lwy_1_R1_123412 0.0.0.0 0 vpn-instance external_vpn_4016
222.1.1.1
ip route-static vpn-instance external_vpn_4016 111.1.1.0 24 vpn-instance lwy_1_R1_123412
5.1.1.2
```

#配置 contextA 安全域和安全策略

```
Name: Trust
Members:
  Route-Aggregation100.2000
  Route-Aggregation100.2005

Name: Untrust
Members:
  Route-Aggregation200.4016
  Route-Aggregation200.4017
```

#配置 contextA 安全策略

```
#
security-policy ip
 rule 0 name 0
  action pass
  vrf lwy_1_1_R4_112233
  source-zone local
  source-zone Trust
  source-zone Untrust
  destination-zone local
  destination-zone Trust
  destination-zone Untrust

 rule 1 name 1
  action pass
  vrf lwy_1_R1_123412
  source-zone local
  source-zone Trust
  source-zone Untrust
  destination-zone local
  destination-zone Trust
  destination-zone Untrust

 rule 2 name 2
  action pass
  vrf external_vpn_4016
  source-zone local
  source-zone Trust
  source-zone Untrust
  destination-zone local
  destination-zone Trust
```

```
  destination-zone Untrust

rule 65000 name 65000
  action pass
  service vrrp
```

(3) 配置 Gateway 1

与 FW 下行口连接的接口配置

```
#
interface Vlan-interface2000
 ip binding vpn-instance lwy_1_R1_123412
 ip address 5.1.1.2 255.255.255.254
 ipv6 address 5::1:3/127
#
interface Vlan-interface2005
 ip binding vpn-instance lwy_1_1_R4_112233
 ip address 6.1.1.12 255.255.255.254
 ipv6 address 6::1:C/127
#
interface Bridge-Aggregation100
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2000 2005
 link-aggregation mode dynamic
 port drni group 100
#
interface Bridge-Aggregation300
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2000 2005
 link-aggregation mode dynamic
 port drni group 300
#
```

与 FW 上行口连接的接口配置

```
#
interface Vlan-interface4016
 ip binding vpn-instance external_vpn_4016
 ip address 222.1.1.1 255.255.0.0
 ipv6 address 222::1/96
#
interface Vlan-interface4017
 ip binding vpn-instance external_vpn_4017
 ip address 223.1.1.1 255.255.0.0
 ipv6 address 223::1/96
#
interface Bridge-Aggregation200
 port link-type trunk
 undo port trunk permit vlan 1
```

```
 port trunk permit vlan 4016 4017
 link-aggregation mode dynamic
 port drni group 200
#
interface Bridge-Aggregation400
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4016 4017
 link-aggregation mode dynamic
 port drni group 400
#
```

静态路由配置

```
ip route-static vpn-instance lwy_1_R1_123412 0.0.0.0 0 5.1.1.3
ip route-static vpn-instance lwy_1_1_R4_112233 0.0.0.0 0 6.1.1.13
ip route-static vpn-instance external_vpn_4016 111.1.1.0 24 222.1.0.1
ip route-static vpn-instance external_vpn_4017 211.1.1.0 24 223.1.0.5
```

(4) 配置 Gateway 2

与 FW 下行口连接的接口配置

```
#
interface Vlan-interface2000
 ip binding vpn-instance lwy_1_R1_123412
 ip address 5.1.1.2 255.255.255.254
 ipv6 address 5::1:3/127
#
interface Vlan-interface2005
 ip binding vpn-instance lwy_1_1_R4_112233
 ip address 6.1.1.12 255.255.255.254
 ipv6 address 6::1:C/127
#
interface Bridge-Aggregation100
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2000 2005
 link-aggregation mode dynamic
 port drni group 100
#
interface Bridge-Aggregation300
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2000 2005
 link-aggregation mode dynamic
 port drni group 300
#
```

与 FW 上行口连接的接口配置

```
#
interface Vlan-interface4016
 ip binding vpn-instance external_vpn_4016
```

```
 ip address 222.1.1.1 255.255.0.0
 ipv6 address 222::1/96
#
interface Vlan-interface4017
 ip binding vpn-instance external_vpn_4017
 ip address 223.1.1.1 255.255.0.0
 ipv6 address 223::1/96
#
interface Bridge-Aggregation200
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4016 4017
 link-aggregation mode dynamic
 port drni group 200
#
interface Bridge-Aggregation400
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 4016 4017
 link-aggregation mode dynamic
 port drni group 400
#
```

静态路由配置

```
ip route-static vpn-instance lwy_1_R1_123412 0.0.0.0 0 5.1.1.3
ip route-static vpn-instance lwy_1_1_R4_112233 0.0.0.0 0 6.1.1.13
ip route-static vpn-instance external_vpn_4016 111.1.1.0 24 222.1.0.1
ip route-static vpn-instance external_vpn_4017 211.1.1.0 24 223.1.0.5
```

5.13.3 配置注意事项

- 在配置之前确保内外网路由可达

5.14 RBM组网使用系统要求

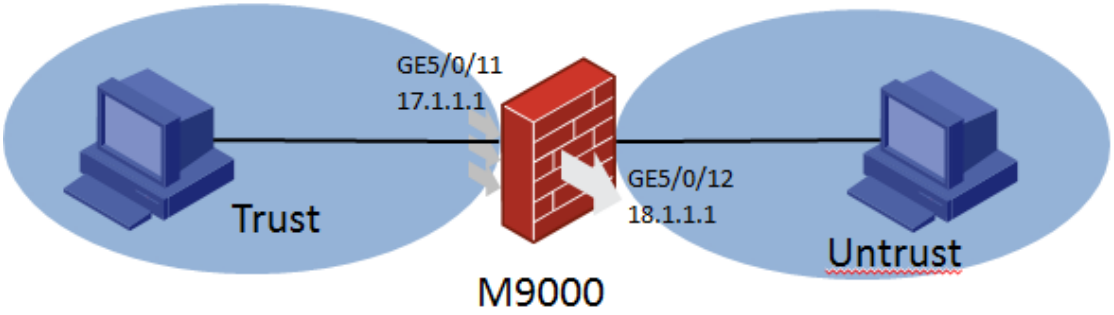
- 要求组成 RBM 双机的两台设备主控板的数量相同，接口板的位置、类型和数量都相同，业务板的数量和位置相同，否则会出现主用设备备份过去的信息，与备用设备的物理配置无法兼容，导致主备切换后出现问题。
- 建议两台设备的 RBM 心跳接口带宽为(N+3)*10G，其中 N 为业务卡数量（数据通道接口默认使用心跳线接口）。
- 要求主备设备的 HASH 选板模式、HASH 因子配置一致。
- 配置同步功能只在主上生效，即：在配置主上敲的命令可以同步到配置备，在配置备上敲命令的话不会往主上同步。
- RBM 回切时间建议根据局点情况进行调整。

6 M9000 的安全策略基本配置

6.1 组网需求

某公司以 Device 作为网络边界安全防护设备，配置安全策略，使得 Trust 域的用户可以访问 Untrust 域内的用户，但 Untrust 内的用户不能访问 Trust 内用户。

图6-1 安全策略基本功能组网图



6.2 配置思路

- 配置接口地址，分别将接口加入 Trust 和 Untrust 域
- 配置地址对象组
- 配置服务对象组
- 配置安全策略，安全策略中引用地址对象组和服务对象组

6.3 配置步骤

配置接口 GigabitEthernet 5/0/11 的地址。

```
[M9K]interface GigabitEthernet 5/0/11
[M9K-GigabitEthernet5/0/11]ip address 17.1.1.1 24
```

配置接口 GigabitEthernet 5/0/12 的地址

```
[M9K]interface GigabitEthernet 5/0/12
[M9K-GigabitEthernet5/0/12]ip address 18.1.1.1 24
```

在命令行下将接口 GigabitEthernet 5/0/11 加入 Trust 域。

```
[M9K]security-zone name Trust
[M9K-security-zone-Trust]import interface GigabitEthernet 5/0/11
```

在命令行下将接口 GigabitEthernet 5/0/12 加入 Untrust 域。

```
[M9K]security-zone name Untrust
[M9K-security-zone-Untrust]import interface GigabitEthernet 5/0/12
```

创建名称为 trust-untrust 的地址对象组，IP 地址范围从 17.1.1.2~17.1.1.200

```
[M9K]object-group ip address trust-
untrust
[M9K-obj-grp-ip-trust-untrust]network range 17.1.1.2 17.1.1.200
```

创建名称为 untrust-trust 的地址对象组，IP 地址范围从 18.1.1.2~18.1.1.200

```
[M9K]object-group ip address untrust-trust
[M9K-obj-grp-ip-untrust-trust]network range 18.1.1.2 18.1.1.200
```
创建名称为 tcp 的服务对象组，并定义其支持的服务为 tcp
```
[M9K]object-group service tcp
[M9K-obj-grp-service-tcp]service tcp source gt 1023 destination gt 79
```
创建安全策略 trust-untrust，过滤条件为：源 IP 地址为 trust-untrust 的地址对象组，目的地址为 untrust-trust 地址对象组，服务对象组为 tcp；开启命中策略计数功能。
```
[M9K]security-policy ip
[M9K-security-policy-ip]rule 0 name trust-untrust
[M9K-security-policy-ip-0-trust-untrust]source-ip trust-untrust
[M9K-security-policy-ip-0-trust-untrust]destination-ip untrust-trust
[M9K-security-policy-ip-0-trust-untrust]action pass
[M9K-security-policy-ip-0-trust-untrust]service tcp
[M9K-security-policy-ip-0-trust-untrust]counting enable
```

6.4 注意事项

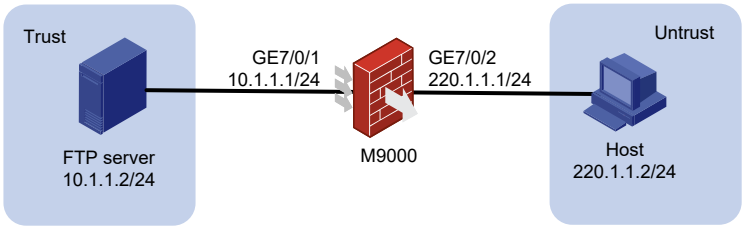
- 当安全策略与包过滤同时配置时，因为安全策略对报文的处理在包过滤之前，报文与安全策略规则匹配成功后，不再进行包过滤处理，所以请合理配置安全策略和包过滤，否则可能会导致配置的包过滤不生效。
- 配置安全策略时，请按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

7 M9000 的 NAT 基本功能

7.1 组网需求

如图 7-1 所示，M9000 连接内网和外网，FTP Server 处于内网，IP 地址为 10.1.1.2，Host 在外网，IP 地址为 220.1.1.2。现在 Host 以公网地址 220.1.1.1 访问 FTP Server，需要对 Host 地址进行 NAT Outbound 转换，转换地址池地址为 10.1.1.100～10.1.1.102。

图7-1 NAT 基本功能组网图



7.2 配置思路

- 配置接口地址。
- 配置 NAT Server，Host 主动访问 FTP Server 时转换目的地址。
- 配置 NAT Outbound，Host 主动访问 FTP Server 时转换源地址。

- 将接口加入安全域，配置安全策略。

7.3 配置步骤

配置接口地址。

```
<Sysname> System-view
[Sysname]interface GigabitEthernet 7/0/2
[Sysname-GigabitEthernet7/0/2]ip address 10.1.1.1 24
[Sysname]interface GigabitEthernet 7/0/2
[Sysname-GigabitEthernet7/0/2]ip address 220.1.1.1 24
```

在接口 GigabitEthernet7/0/2 上配置 NAT server。

```
[Sysname-GigabitEthernet7/0/2]nat server protocol tcp global 220.1.1.1 ftp inside
10.1.1.2 ftp
```

创建 NAT 地址池。

```
[Sysname]nat address-group 0
[Sysname-address-group-0]address 10.1.1.100 10.1.1.102
```

配置需要地址转换的 ACL。

```
[Sysname]acl basic 2999
[Sysname-acl-ipv4-basic-2999]rule 0 permit source 220.1.1.0 0.0.0.255
```

在内网端口上配置 NAT Outbound。

```
[Sysname]interface GigabitEthernet 7/0/1
[Sysname-GigabitEthernet7/0/1]nat outbound 2999 address-group 0
```

将接口 GigabitEthernet7/0/1 加入到 Trust 域。

```
[Sysname]security-zone name trust
[Sysname-security-zone-Trust]import interface GigabitEthernet 7/0/1
```

将接口 GigabitEthernet7/0/2 加入到 Untrust 域。

```
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust]import interface GigabitEthernet 7/0/2
[Sysname-security-zone-Untrust]quit
```

配置地址对象。

```
[Sysname]object-group ip address testSouAddr
[Sysname-obj-grp-ip-testSouAddr]network host address 220.1.1.2
[Sysname]object-group ip address testDestAddr
[Sysname-obj-grp-ip-testDestAddr]network host address 10.1.1.2
```

配置安全策略

```
[Sysname]security-policy ip
[Sysname-security-policy-ip]rule name testObjPol
[Sysname-security-policy-ip-0-testObjPol]source-ip testSouAddr
[Sysname-security-policy-ip-0-testObjPol]destination-ip testDestAddr
[Sysname-security-policy-ip-0-testObjPol]service ftp
[Sysname-security-policy-ip-0-testObjPol]source-zone untrust
[Sysname-security-policy-ip-0-testObjPol]destination-zone trust
[Sysname-security-policy-ip-0-testObjPol]action pass
```

7.4 注意事项

- 对于 NAT Server 来说，在安全策略中规则匹配的目的地址为 NAT Server 转换后的私网地址。
- 对于 NAT Outbound 来说，在安全策略中，规则匹配的源地址为转换前的地址。
- 每个接口下可以配置的 NAT server，最多可支持 2048 个。
- 每个接口下配置 nat outbound，最多可支持 2048 个。
- NAT 地址池个数，最多可支持 256 个。
- 每个 NAT 地址池中的地址总数，最多可支持 65535 个。
- 每个地址池中地址条目，最多可支持 64 个。
- NAT 地址池配置注意事项

地址池的地址尽量配成一个完整的掩码地址，配置地址尽量为 0～2^n 或者 2^n～2^(n+1)-1，其中 n>0。

下面的地址段配置是正常最优的：

10.1.1.0~10.1.1.255

11.1.1.4~ 11.1.1.17

下面的地址段配置不可取：10.1.1.3~10.1.1.255

也就是说最好按照子网掩码去划分最优(要求包含子网的全零和全 1 地址)，如：

10.1.1.4-10.1.1.7(10.1.1.4/30)

10.1.1.8-10.1.1.11(10.1.1.8/30)

10.1.1.8-10.1.1.15(10.1.1.8/29)

10.1.1.16-10.1.1.31(10.1.1.16/28)

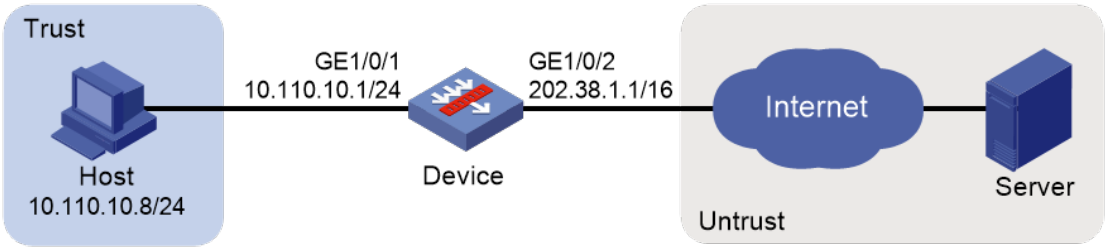
10.1.1.32-10.1.1.63(10.1.1.32/27)

8 内网用户通过 NAT 访问外网（静态地址转换）

8.1 组网需求

如图 8-1 所示，内部网络用户 10.110.10.8/24 使用外网地址 202.38.1.100 访问 Internet。

图8-1 NAT 基本功能组网图



8.2 配置思路

- 配置接口地址。
- 配置一对一静态地址转换规则。
- 出接口使能静态 NAT 转换功能。
- 将接口加入安全域，配置安全策略。

8.3 配置步骤

配置接口地址。

```
<Sysname>System-view
[Sysname]interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2]ip address 202.38.1.1 16
[Sysname]interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1]ip address 10.110.10.1 24
```

#配置内网 IP 地址 10.110.10.8 到外网地址 202.38.1.100 之间的一对一静态转换映射。

```
[Sysname]nat static outbound 10.110.10.8 202.38.1.100
```

#使配置的静态地址转换在接口 GigabitEthernet1/0/2 上生效。

```
[Sysname]interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1]nat static enable
```

将接口 GigabitEthernet1/0/1 加入到 Trust 域。

```
[Sysname]security-zone name Trust
[Sysname-security-zone-Trust]import interface GigabitEthernet 1/0/1
```

将接口 GigabitEthernet1/0/2 加入到 Untrust 域。

```
[Sysname]security-zone name Untrust
[Sysname-security-zone-Untrust]import interface GigabitEthernet 1/0/2
```

配置安全策略。

```
[Sysname]security-policy ip
[Sysname-security-policy-ip]rule name Trust-Untrust
[Sysname-security-policy-ip-Trust-Untrust]action pass
```

9 SSL VPN

9.1 SSL VPN简介

SSL VPN 目前主要有如下几种：

- Web 接入方式：使用户能够通过 Web 接入方式访问企业内网资源。
- TCP 接入方式：使用户能够通过 TCP 接入方式访问企业内网资源。
- IP 接入方式：使用户能够通过 IP 接入方式访问企业内网资源。

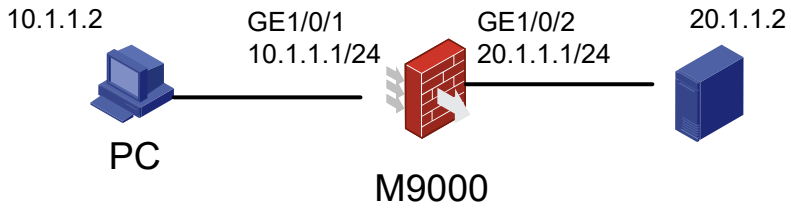
说明：目前 M9000 系列暂不支持 Web 和 TCP 的接入方式。

9.2 配置IP接入方式

9.2.1 组网需求

PC 通过 SSL VPN 网关设备安全地访问服务器端的特定 IP 资源。

图9-1 组网图



9.2.2 配置思路

- 配置接口地址，安全域及安全策略
- 配置 PKI domain。
- 导入 CA 证书和服务器证书。
- 配置 ssl 服务器端策略。
- 配置 SSL VPN 网关。
- 配置 SSL VPN 的 AC 口，以及地址池。
- 配置 SSL VPN 访问实例，并在实例下创建路由表项和策略组。
- 配置本地用户。

9.2.3 配置步骤

配置接口地址

```
<System>system-view
[System]interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1]ip address 10.1.1.1 255.255.255.0
[System] interface GigabitEthernet1/0/2
```

```
[Sysname-GigabitEthernet1/0/2]ip address 20.1.1.1 255.255.255.0
```

配置 PKI 域 sslvpn

```
[System]pki domain sslvpn
[System-pki-domain-sslvpn]public-key rsa general name sslvpn
[System-pki-domain-sslvpn]undo crl check enable
```

导入 CA 证书 ca.cer 和服务器证书 server.pfx。

```
[System]pki import domain sslvpn der ca filename ca.cer
[System]pki import domain sslvpn p12 local filename server.pfx
```

配置 SSL 服务器端策略 ssl。

```
[System]ssl server-policy ssl
[System-ssl-server-policy-ssl]pki-domain sslvpn
```

配置 SSL VPN 网关 gw。

```
[System]sslvpn gateway gw
[System-sslvpn-gateway-gw]ip address 10.1.1.1 port 2000
[System-sslvpn-gateway-gw]ssl server-policy ssl
[System-sslvpn-gateway-gw]service enable
```

创建 SSL VPN AC 接口 1，并创建地址池 ippool

```
[System]interface sslvpn-ac 1
[System-SSLVPN-AC1]ip address 1.1.1.100 24
[System-SSLVPN-AC1]quit
[System]sslvpn ip address-pool ippool 1.1.1.1 1.1.1.10
```

将 AC 口加入安全域

```
[System]security-zone name trust
[System-security-zone-Trust]import interface SSLVPN-AC 1
```

配置 SSL VPN 访问实例 ctx1，在实例下创建路由表项和策略组，开启服务。

```
[System] sslvpn context ctx1
[System-sslvpn-context-ctx1]gateway gw
[System-sslvpn-context-ctx1]ip-tunnel interface sslvpn-ac 1
[System-sslvpn-context-ctx1]ip-route-list rtlist
[System-sslvpn-context-ctx1-route-list-rtlist]include 2.1.1.0 255.255.255.0
[System-sslvpn-context-ctx1-route-list-rtlist]quit
[System-sslvpn-context-ctx1]policy-group pgroup
[System-sslvpn-context-ctx1-policy-group-pgroup]ip-tunnel address-pool ippool mask
255.255.255.0
[System-sslvpn-context-ctx1-policy-group-pgroup]ip-tunnel access-route ip-route-list
rtlist
[System-sslvpn-context-ctx1-policy-group-pgroup]filter  ip-tunnel acl 3000
[System-sslvpn-context-ctx1-policy-group-pgroup]quit
[System-sslvpn-context-ctx1]service enable
[System-sslvpn-context-ctx1]quit
[System]acl advanced 3000
[System-acl-ipv4-adv-3000]rule permit ip
[System-acl-ipv4-adv-3000]quit
```

创建高级 ACL，配置出方向 NAT 地址转换。

```
[System]nat address-group 1
[System -nat-address-group-1]address 20.1.1.10 20.1.1.20
[System]interface GigabitEthernet1/0/2
```

```
[System-GigabitEthernet1/0/2]nat outbound 3000 address-group 1
```

创建本地 SSL VPN 用户 h3c，密码为 admin123456，授权用户的 SSL VPN 策略组为 pgroup。

```
[System]local-user h3c class network
[System-luser-network-h3c]password simple admin123456
[System-luser-network-h3c]service-type sslvpn
[System-luser-network-h3c]authorization-attribute sslvpn-policy-group pgroup
```

9.2.4 登录和注意事项

1. 登录

IP 接入方式需要在相应的客户端登录：

图9-2 iNode 客户端

2. 注意事项

- AC 地址与 address-pool 不能有地址冲突，否则不能访问资源。
- 将接口 G1/0/1 和 G1/0/2 放入安全域。
- 配置安全策略为放行。
- 设备与 SSL VPN 客户端、Server 之间路由可达。
- Server 端有到 1.1.1.0/24 网段的路由。
- CA 证书 ca.cer 和服务器证书 server.pfx 须有效，且提前导入设备。
- 修改 sslvpn 配置后，需要在 sslvpn context 视图下先 undo service enable 再 service enable
- 需要在接口配置 nat outbound，M9K 设备当业务板数量大于等于 2 时连接服务器端的接口下需要配合使用 nat 来保证报文来回路径一致

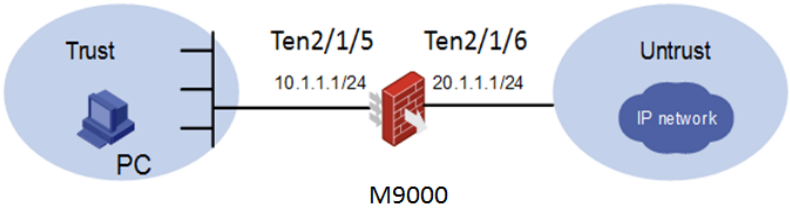
- IP 接入方式时，AC 接口需要加入安全域并放通策略，地址池到内网资源的

PC 上需要安装 SSL VPN IP 接入的客户端，如 iNode 客户端（客户端的下载可以通过 web 访问网关去下载客户端）；

10 串行部署- IPS 模式基本功能

10.1 组网需求

图10-1 M9000 的三层 IPS 基本功能组网图



公司内部网络通过 Device 与 Internet 互连。内部网络属于 Trust 安全域，外部网络属于 Untrust 安全域。要求正确配置安全策略，使内外网所有流量都经 IPS 策略防护。

10.2 配置思路

- 配置接口 IP 并加入安全域。
- 创建 IPS 策略。
- 配置安全策略。

10.3 配置步骤

配置接口 Ten-GigabitEthernet2/1/5 的地址。

```
[Sysname]interface Ten-GigabitEthernet 2/1/5
[Sysname-Ten-GigabitEthernet2/1/5]ip address 10.1.1.1 24
```

配置接口 Ten-GigabitEthernet2/1/6 的地址。

```
[Sysname]interface Ten-GigabitEthernet 2/1/6
[Sysname-Ten-GigabitEthernet2/1/6]ip address 20.1.1.1 24
```

将接口 Ten-GigabitEthernet 2/1/5 加入 Trust 域。

```
[Sysname]security-zone name trust
[Sysname-security-zone-Trust]import interface Ten-GigabitEthernet 2/1/5
```

在命令行下将接口 Ten-GigabitEthernet2/1/6 加入 Untrust 域。

```
[Sysname]security-zone name untrust
[Sysname-security-zone-Untrust]import interface Ten-GigabitEthernet 2/1/6
```

创建 IPS 策略

```
[Sysname]ips policy ips
[Sysname-ips-policy-ips]quit
```

创建 app-profile ips，在 profile 中引用 ips 策略。

```
[Sysname]app-profile ips
[Sysname-profile-ips]ips apply policy ips mode protect
[Sysname-app-profile-ips]quit
```

创建安全策略,，并应用创建的 profile。

```
[Sysname]security-policy ip
[Sysname-security-policy-ip]rule 1 name ips
[Sysname-security-policy-ip-1-1]profile ips
[Sysname-security-policy-ip-1-1]source-zone trust
[Sysname-security-policy-ip-1-1]destination-zone untrus
[Sysname-security-policy-ip-1-1]action pass
```

Web 界面配置

创建 IPS 策略：对象——应用安全——入侵防御——配置文件——新建

在安全策略中应用 profile：策略—安全策略—新建—新建策略—内容安全中，IPS 策略中应用创建的 ips 策略。


新建安全策略
名称
ips
自动命名
源安全域
Trust
[多选]
目的安全域
Untrust
[多选]
类型
IPv4
IPv6
所属策略组
请选择策略组
描述信息
(1-127字符)
动作
允许
拒绝
内容安全
Web应用防护配置文件
--NONE--
入侵防御配置文件
ips
[配置]
数据过滤配置文件
--NONE--
文件过滤配置文件
--NONE--
防病毒配置文件
--NONE--
URL过滤配置文件
--NONE--
记录日志
开启
关闭
开启策略匹配统计
开启
关闭
会话老化时间
启用
长连接老化时间
启用
启用策略
开启
关闭
策略冗余分析
确定
取消

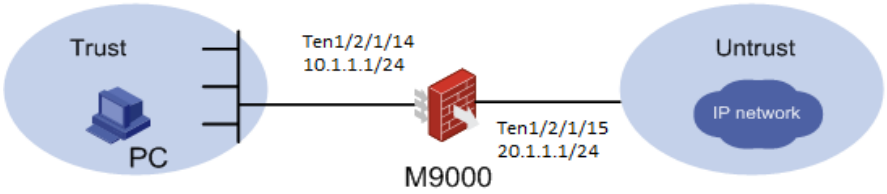
10.4 注意事项

默认情况下，创建自定义的 ips 策略同 default 策略中开启的特征状态保持一致，自定义策略中可以通过 override 命令改写具体特征的使能情况及动作。

11 AV 病毒防护基本功能

11.1 组网需求

图11-1 M9000 的 AV 基本功能组网图



公司内部网络通过 Device 与 Internet 互连。内部网络属于 Trust 安全域，外部网络属于 Untrust 安全域。要求正确配置安全策略，使内外网所有流量都经病毒防护。

11.2 配置思路

- 配置接口地址并加入安全域。
- 创建 AV 策略。
- 创建 app-profile。
- 创建安全策略。

11.3 配置步骤

配置接口 Ten-GigabitEthernet1/2/1/14 的地址。

```
[Sysname]interface Ten-GigabitEthernet1/2/1/14
[Sysname-Ten-GigabitEthernet1/2/1/14]ip address 10.1.1.1 24
```

配置接口 Ten-GigabitEthernet1/2/1/15 的地址。

```
[Sysname]interface Ten-GigabitEthernet1/2/1/15
[Sysname-Ten-GigabitEthernet1/2/1/15]ip address 20.1.1.1 24
```

将接口 Ten-GigabitEthernet1/2/1/14 加入 Trust 域。

```
[Sysname] security-zone name Trust
[Sysname-security-zone-Trust]import interface Ten-GigabitEthernet 1/2/1/14
```

在命令行下将接口 Ten-GigabitEthernet1/2/1/15 加入 Untrust 域。

```
[Sysname]security-zone name Untrust
[Sysname-security-zone-Untrust]import interface Ten-GigabitEthernet 1/2/1/15
```

创建病毒策略 AV。

```
[Sysname]anti-virus policy AV
```

```
[Sysname-anti-virus-policy-av]quit
```

创建 app-profile AV，在 profile 中引用 AV 策略。

```
[Sysname]app-profile AV
[Sysname-app-profile-AV]anti-virus apply policy AV mode protect
[Sysname-app-profile-AV]quit
```

创建安全策略,，并应用创建的 profile。

```
[Sysname]security-policy ip
[Sysname-security-policy-ip]rule 0 name 1
[Sysname-security-policy-ip-0-1]profile AV
[Sysname-security-policy-ip-0-1]source-zone trust
[Sysname-security-policy-ip-0-1]destination-zone untrust
[Sysname-security-policy-ip-0-1]action pass
```

Web 界面配置

创建 AV 策略：对象——应用安全——防病毒——创建 AV 策略

在安全策略中应用 profile：策略—安全策略—新建—新建策略—内容安全中，防病毒配置文件中应用 AV 策略。

11.4 注意事项

默认情况下，创建自定义的 AV 策略同 anti-virus default 策略中开启的应用检测状态保持一致，自定义策略中可以自定义需要检测的协议及方向，并且可以配置例外策略，用户可以根据实际使用情况进行开启关闭。

12 日志

12.1 日志简介

M9000 当前支持的日志主要有如下几种：

- Syslog 日志：Syslog 日志用来记录系统产生的日志，Syslog 日志包括普通日志、诊断日志、安全日志、隐藏日志、调试跟踪日志。系统日志传输格式为 ASCII 码，通过防火墙的信息中心模块进行分类管理和输出。
- Flow 日志：Flow 日志用来记录会话信息，主要包括用户访问网络的五元组信息（源 IP 地址、目的 IP 地址、源端口、目的端口、协议号）、发送和接收的统计信息等。NAT 日志、会

话日志、AFT 日志可以通过流日志发送，其格式为二进制格式，其中 NAT 的流日志也可以发送到信息中心封装成 Syslog 日志。但 Syslog 日志相比 Flow 日志传输效率低，当日志量大时强烈不建议将 Flow 日志封装为 Syslog 日志发送。

- Customlog 日志：Customlog 日志用户快速地将用户关心的日志发送至日志主机，配置该功能后，业务模块生成的日志通过快速输出通道直接发送至日志主机，不经过信息中心模块处理，该方式可以节省 系统资源，更高效快捷。Customlog 日志主要包括 NAT444 日志、Session 日志、DPI 日志、攻击防范日志、AFT 日志等。

12.2 配置发送Syslog日志

假定我们的日志服务器地址为：192.168.96.40，发送日志到该服务器上的配置如下：

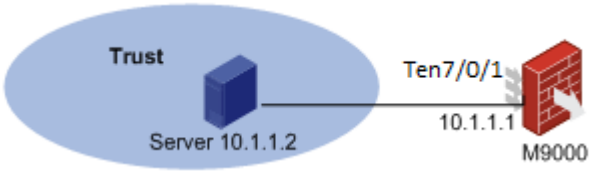
```
<Sysname>system-view
[Sysname]info-center enable
[Sysname]info-center loghost 192.168.96.40
```

12.3 配置发送NAT的Customlog日志

12.3.1 配置需求

如图 12-1 所示，开启 NAT 日志功能，并设置以 Customlog 格式发送 NAT444 日志到日志服务器。

图12-1 发送 customlog 日志组网图



12.3.2 配置思路

- 配置接口地址并加入安全域、配置安全策略，此步骤略。
- 开启 NAT 日志功能。
- 配置 Customlog 日志格式及主机。

12.3.3 配置步骤

开启 NAT 日志功能。

```
<Sysname>system-view
[Sysname]nat log enable
```

配置分配端口块日志。

```
[Sysname]nat log port-block-assign
```

配置回收端口块日志。

```
[Sysname]nat log port-block-withdraw
```

配置流创建时产生日志。

```
[Sysname]nat log flow-begin
```

配置流结束时产生日志。

```
[Sysname]nat log flow-end
```

配置日志格式为电信格式 NAT444 日志。

```
[Sysname]customlog format nat telecom
```

配置以电信格式将日志输出到日志服务器 10.1.1.2。

```
[Sysname]customlog host 10.1.1.2 export telecom-userlog telecom-sessionlog
```

12.3.4 日志结果分析

#端口块日志格式如下

```
Jan 05 15:50:39 192.168.210.20  1 Jan 05 15:48:17 - Sysname - NAT444:userbasedA [0
45.0.0.10 - 200.0.2.202 - 6025 6536]
```

#回收端口块日志格式

```
Jan 05 15:51:09 192.168.210.20  1 Jan 05 15:48:47 - Sysname - NAT444:userbasedW [0
45.0.0.10 - 200.0.2.202 - 6025 6536]
```

#流开始日志格式如下

```
Jan 05 15:50:39 192.168.210.20  1 Jan 05 15:48:17 - Sysname - NAT444:sessionbasedA [17
45.0.0.10 - 200.0.2.202 4097 6025 -]
Jan 05 15:50:39 192.168.210.20  1 Jan 05 15:48:17 - Sysname - NAT444:sessionbasedA [17
45.0.0.10 - 200.0.2.202 4096 6026 -]
```

#流束日志格式如下

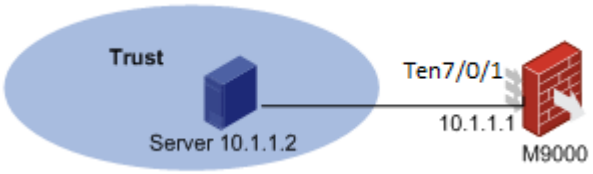
```
Jan 05 15:51:05 192.168.210.20  1 Jan 05 15:48:43 - Sysname - NAT444:sessionbasedW [17
45.0.0.10 - 200.0.2.202 4096 6026 -]
Jan 05 15:51:05 192.168.210.20  1 Jan 05 15:48:43 - Sysname - NAT444:sessionbasedW [17
45.0.0.10 - 200.0.2.202 4097 6025 -]
```

12.4 配置发送IPS的Customlog日志

12.4.1 配置需求

如图 12-2 所示，开启 IPS 日志功能，并设置以 Customlog 格式发送至日志服务器。

图12-2 发送 customlog 日志组网图



12.4.2 配置思路

- 配置接口地址并加入安全域、配置安全策略，此步骤略。
- 配置 Customlog 日志格式及主机。

12.4.3 配置步骤

开启日志格式为 IPS 日志。

```
<Sysname>system-view
[Sysname]customlog format dpi ips
```

配置将 IPS 日志输出到日志服务器 10.1.1.2。

```
[Sysname]customlog  host 10.1.1.2 export dpi ips
```

12.4.4 日志结果分析

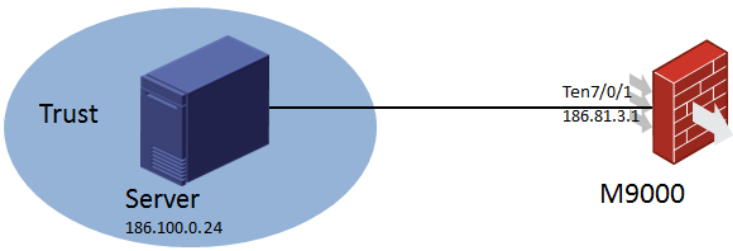
```
Sep 16 09:19:51 2020 Sysname %%10IPS/4/IPS_IPV4_INTERZONE: -Slot=1.1;
Protocol(1001)=TCP; Application(1002)=http; SrcIPAddr(1003)=3.1.0.1;
SrcPort(1004)=12009; DstIPAddr(1007)=3.1.120.1; DstPort(1008)=80;
RcvVPNInstance(1042)=management; SrcZoneName(1025)=Untrust; DstZoneName(1035)=Trust;
UserName(1113)=3.1.0.1; PolicyName(1079)=default;
AttackName(1088)=Generic_Cross_Site_Scripting_(Mouse_Event_Handlers);
AttackID(1089)=23423; Category(1090)=Vulnerability; Protection(1091)=WebServer;
SubProtection(1092)=Any; Severity(1087)=MEDIUM; Action(1053)=Permit & Logging;
CVE(1075)=--; BID(1076)=--; MSB(1077)=--; HitDirection(1115)=original; RealSrcIP(1100)=;
SubCategory(1124)=XSS; LoginUserName(1177)=; LoginPwd(1178)=; CapturePktName(1116)=;
HttpHost(1117)= QhXCXMIjIFvnkTuHb; HttpFirstLine(1118)=/cgi-
bin/activecalendar/data/mysqlevents.php?css=%22%3e%3c%3ca/ll%20%3d%22%3e%27%3e%20%22b%3d
%27%3e%22%27OnMouSEOver%3d%22%09alert%28%27jibpfcphrjt%27%29%22%09%3e%3e;
PayLoad(1135)=css="><<a/ll ="">'> "b='>"'OnMouSEOver="\...
```

12.5 配置发送NAT的Flow日志

12.5.1 组网需求

如图 12-3 所示，开启 NAT 日志功能，并发送 Userlog 日志到日志服务器 186.100.0.24 中。Userlog 日志用来发送 NAT 转换的日志。

图12-3 发送 NAT 日志组网图



12.5.2 配置思路

- 配置接口地址并加入安全域、配置安全策略，此步骤略。
- 开启 NAT 日志功能。
- 配置 Userlog 日志主机。

12.5.3 配置步骤

开启 NAT 日志功能。

```
<Sysname>System-view
[Sysname]nat log enable
```

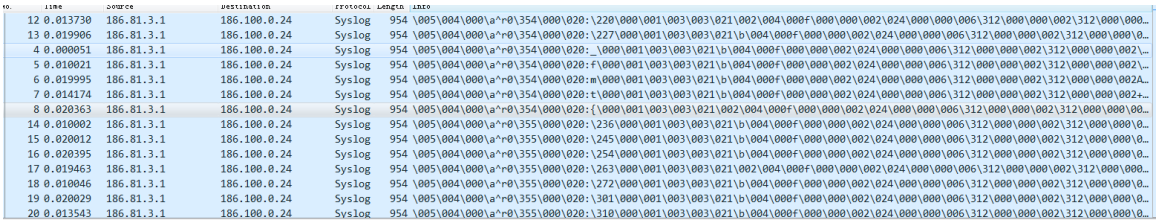
```
[Sysname]nat log flow-begin
[Sysname]nat log flow-end
```

配置 Userlog 日志主机。

```
[Sysname]userlog flow export host 186.100.0.24 port 514
```

12.5.4 日志结果及分析

如下是 Userlog 以二进制方式产生的日志：



No.	Time	Source	Destination	Protocol	Length	Info
12	0.013730	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:\220\000\001\003\003\021\002\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000…
13	0.019906	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:\227\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
4	0.000051	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:_\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\002\…
5	0.010021	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:f\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\002\…
6	0.019995	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:m\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\002A…
7	0.014174	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:t\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\002+…
8	0.020363	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:{\000\001\003\003\021\002\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\00…
14	0.010002	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\236\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
15	0.020012	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\245\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
16	0.020395	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\254\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
17	0.019463	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\263\000\001\003\003\021\002\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000…
18	0.010046	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\272\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
19	0.020029	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\301\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
20	0.013543	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\310\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…

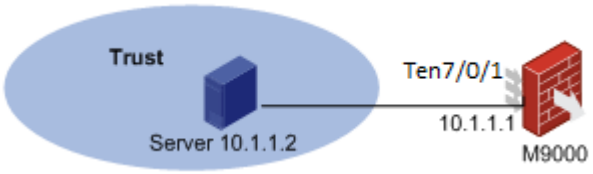
将 userlog 直接以二进制的方式输出到流日志主机上，在日志主机 wireshark 抓包，可观察到相关消息，但因为是二进制，无法直观查看消息内容(\005\004\000\a 代表日志类型为 5.0，\003\004\000\016 代表 3.0，\001\004\000$代表 1.0)

12.6 配置发送Session的Flow日志

12.6.1 组网需求

如图 12-4 所示，配置在会话建立时，产生会话日志，并发送到日志服务器 10.1.1.2。

图12-4 发送 Session 日志组网图



12.6.2 配置思路

- 配置接口地址并加入安全域、配置安全策略，此步骤略。
- 接口开启会话日志功能。
- 全局开启新建会话、删除会话的日志功能。
- 配置 Userlog 日志主机。

12.6.3 配置步骤

在接口下配置会话日志。

```
[Sysname]interface ten-gigabitethernet7/0/1
[Sysname-Ten-GigabitEthernet7/0/1]session log enable ipv4 inbound
[Sysname-Ten-GigabitEthernet7/0/1]session log enable ipv4 outbound
```

配置会话产生的时间阈值。

```
[Sysname]session log flow-begin
[Sysname]session log flow-end
```

#配置 Userlog 日志主机。

```
[Sysname]userlog flow export host 10.1.1.2 port 514
```

12.6.4 日志结果及分析

如下是 Session 日志显示信息：

```
Jan  7 10:48:17 2014 Sysname %%10SESSION/6/SESSION_IPV4_FLOW: -Slot=3.1;
Protocol(1001)=UDP;SrcIPAddr(1003)=10.1.1.2;SrcPort(1004)=1701;NatSrcIPAddr(1005)=10.1.1
.65;NatSrcPort(1006)=5003;DstIPAddr(1007)=10.1.1.1;DstPort(1008)=1701;NatDstIPAddr(1009)
=10.1.1.1;NatDstPort(1010)=1701;InitPktCount(1044)=137;InitByteCount(1046)=6576;RplyPktC
ount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=re10;RcvDS
LiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=01072014093531;EndTim
e_e(1014)=;Event(1048)=(6)Active data flow timeout;
```

12.7 注意事项

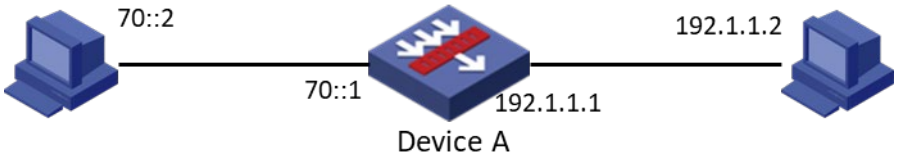
- 如果要把日志发送到日志服务器，要确保有去往服务器的路由可达。
- 配置接口板上业务口作为日志发送口，禁止使用主控管理口作为日志发送口。
- 对于同一个模块，同时配置了 Custmlog 和 Userlog 主机时，Customlog 日志优先级更高。

13 M9000 AFT 支持静态端口块特性

13.1 组网需求

如图 1 组网所示，验证 AFT 支持静态端口块特性。

图13-1 组网图



13.2 配置思路

- 配置安全域及安全策略保证网络可达
- 将物理口加入到安全域

13.3 配置步骤

配置 FW 的上下行接口地址，并在接口下使能 aft 功能。

```
[M9K100]interface Ten-GigabitEthernet2/0/15
[M9K100-Ten-GigabitEthernet2/0/15]ipv6 address 70::1 64
```

```
[M9K100-Ten-GigabitEthernet2/0/15]aft enable
[M9K100-Ten-GigabitEthernet2/0/15]quit
[M9K100]interface Ten-GigabitEthernet2/0/16
[M9K100-Ten-GigabitEthernet2/0/16]ip address 192.1.1.1 24
[M9K100-Ten-GigabitEthernet2/0/16]aft enable
[M9K100-Ten-GigabitEthernet2/0/16]quit
```

#配置安全策略及安全域保证网络可达。

```
[M9K100]security-zone name Trust
[M9K100-security-zone-Trust]import interface Ten-GigabitEthernet 2/0/15
[M9K100-security-zone-Trust]quit
[M9K100]security-zone name Untrust
[M9K100-security-zone-Untrust]import interface Ten-GigabitEthernet 2/0/16
[M9K100-security-zone-Untrust]quit
[M9K100]security-policy ip
[M9K100-security-policy-ip]rule 0 name ap
[M9K100-security-policy-ip-0-ap]action pass
[M9K100-security-policy-ip-0-ap]quit
[M9K100]security-policy ipv6
[M9K100-security-policy-ipv6]rule 0 name ap
[M9K100-security-policy-ipv6-0-ap]action pass
[M9K100-security-policy-ipv6-0-ap]quit
```

Nat64 相关配置，IPv6 发起访问：静态端口块转 IPv6 源，Nat64 前缀转 IPv6 目的。

```
[M9K100]aft port-block-group 1
[M9K100-aft-port-block-group-1]ipv6-prefix 72:: 72:: 64
[M9K100-aft-port-block-group-1]ip-address 202.1.1.2 202.1.1.5
[M9K100-aft-port-block-group-1]block-size 10000
[M9K100-aft-port-block-group-1]port-range 10000 30000
[M9K100-aft-port-block-group-1]quit
[M9K100]aft v6tov4 source port-block-group 1
[M9K100]aft prefix-general AF01:: 96
```

#开启会话引流

```
[M9K100]session flow-redirect enable
[M9K100]session flow-redirect hardware-fast-forwarding
```

13.4 注意事项

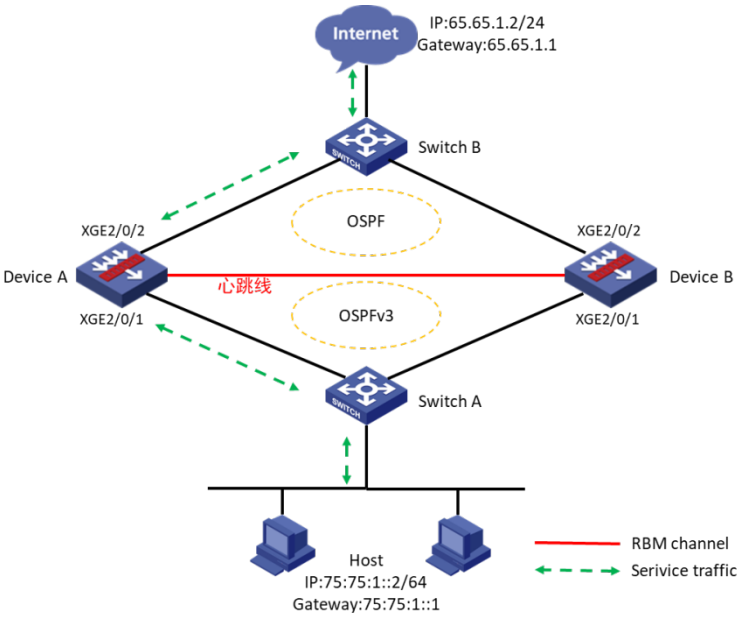
- 只有在连接 IPv4 网络和 IPv6 网络的接口上都开启 AFT 功能后，才能实现 IPv4 报文和 IPv6 报文之间的相互转换。

14 M9000 AFT 支持动态端口块热备特性

14.1 组网需求

如图 1 所示，本文仅以 RBM 组网为例，验证 AFT 支持动态端口块热备特性。

图14-1 组网图



14.2 配置思路

- 配置设备的 RBM 主备组网
- 配置安全域及安全策略保证网络可达
- 将物理口加入到安全域

14.3 配置步骤

1.配置 Device A

#配置 RBM 主备组网-略

配置 ospf 动态路由。

```
RBM_P[M9K200]ospfv3 75
RBM_P[M9K200-ospfv3-75]router-id 2.2.2.75
RBM_P[M9K200-ospfv3-75]default-route-advertise always type 1
RBM_P[M9K200-ospfv3-75]area 0
RBM_P[M9K200-ospfv3-75-area-0.0.0.0]quit
RBM_P[M9K200-ospfv3-75]quit
RBM_P[M9K200]ospf 75 router-id 1.1.1.75
RBM_P[M9K200-ospf-75]default-route-advertise always type 1
RBM_P[M9K200-ospf-75]area 0
RBM_P[M9K200-ospf-75-area-0.0.0.0]quit
RBM_P[M9K200-ospf-75]quit
```

配置 FW 的上下行接口地址，并在接口下使能 aft 功能和 OSPFv3/v2 功能。

```
RBM_P[M9K200]interface Ten-GigabitEthernet2/0/1
RBM_P[M9K200-Ten-GigabitEthernet2/0/1]ospfv3 75 area 0.0.0.0
RBM_P[M9K200-Ten-GigabitEthernet2/0/1]aft enable
RBM_P[M9K200-Ten-GigabitEthernet2/0/1]ipv6 address 75:1::2/64
```

```
RBM_P[M9K200-Ten-GigabitEthernet2/0/1]quit
RBM_P[M9K200]interface Ten-GigabitEthernet2/0/2
RBM_P[M9K200-Ten-GigabitEthernet2/0/2]ospf 75 area 0.0.0.0
RBM_P[M9K200-Ten-GigabitEthernet2/0/2]aft enable
RBM_P[M9K200-Ten-GigabitEthernet2/0/2]ip address 65.1.1.2 24
RBM_P[M9K200-Ten-GigabitEthernet2/0/2]quit
```

#配置安全策略及安全域保证网络可达。

```
RBM_P[M9K200]security-zone name Trust
RBM_P[M9K200-security-zone-Trust]import interface Ten-GigabitEthernet 2/0/1
RBM_P[M9K200-security-zone-Trust]quit
RBM_P[M9K200]security-zone name Untrust
RBM_P[M9K200-security-zone-Untrust]import interface Ten-GigabitEthernet 2/0/2
RBM_P[M9K200-security-zone-Untrust]quit
RBM_P[M9K200]security-policy ip
RBM_P[M9K200-security-policy-ip]rule 0 name ap
RBM_P[M9K200-security-policy-ip-0-ap]action pass
RBM_P[M9K200-security-policy-ip-0-ap]quit
RBM_P[M9K200-security-policy-ip]quit
RBM_P[M9K200]security-policy ipv6
RBM_P[M9K200-security-policy-ipv6]rule 0 name ap
RBM_P[M9K200-security-policy-ipv6-0-ap]action pass
RBM_P[M9K200-security-policy-ipv6-0-ap]quit
RBM_P[M9K200-security-policy-ipv6]quit
```

Nat64 相关配置，IPv6 发起访问：动态端口块转 IPv6 源，Nat64 前缀转 IPv6 目的。

```
RBM_P[M9K200]acl ipv6 advanced 3000
RBM_P[M9K200-acl-ipv6-adv-3000]rule permit ipv6 source 75:75:1:: 64
RBM_P[M9K200-acl-ipv6-adv-3000]quit
RBM_P[M9K200]aft address-group 1
RBM_P[M9K200-aft-address-group-1]address 223.1.1.2 223.1.1.5
RBM_P[M9K200-aft-address-group-1]quit
RBM_P[M9K200]aft v6tov4 source  acl ipv6 number 3000 address-group 1 port-block-
size 100 extended-block-number 2 port-range 1024 2023
RBM_P[M9K200]aft prefix-nat64 af10:: 96
```

#开启端口块同步(默认开启)

```
[H3C] aft port-block synchronization enable
```

配置路由保证网络可达。

2.配置 Device B 略

#功能验证：

```
RBM_P[M9K200]dis aft  port-block dynamic
CPU 0 on slot 4:
Total entries found: 0
CPU 0 on slot 5:
Total entries found: 0
CPU 1 on slot 7:
Total entries found: 0
CPU 1 on slot 8:
IPv6 Address: 75:75:1::2
IPv4 Address: 223.1.1.5
Port block  : [1324 - 1423]
Port-block mapping state : Backed Up

Total entries found: 1
```

```
RBM_S[M9K100]dis aft port-block dynamic
CPU 0 on slot 4:
Total entries found: 0
CPU 0 on slot 5:
Total entries found: 0
CPU 1 on slot 7:
Total entries found: 0
CPU 1 on slot 8:
IPv6 Address: 75:75:1::2
IPv4 Address: 223.1.1.5
Port block  : [1324 - 1423]
Port-block mapping state : Restored

Total entries found: 1
```

14.4 注意事项

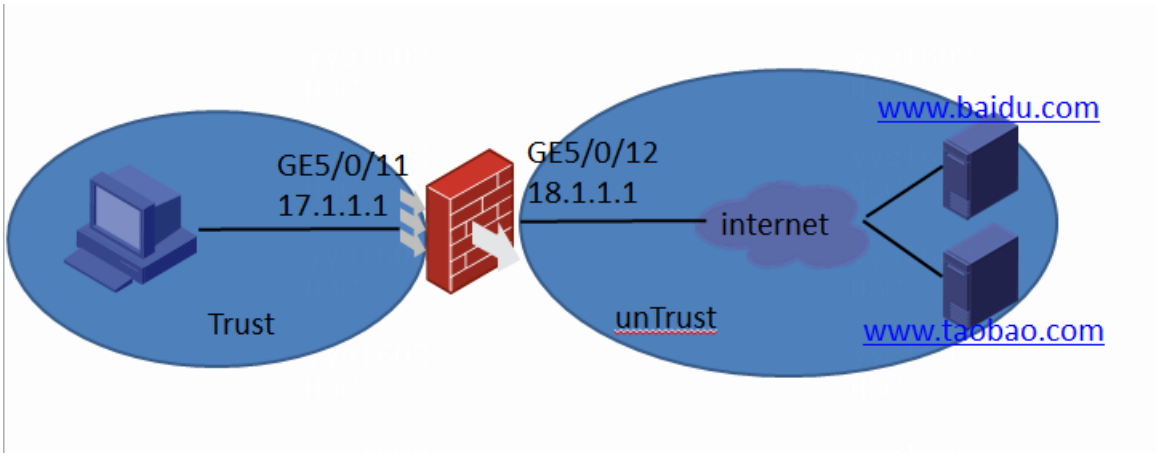
- 只有在连接 IPv4 网络和 IPv6 网络的接口上都开启 AFT 功能后，才能实现 IPv4 报文和 IPv6 报文之间的相互转换。

15 M9000 的安全策略支持 URL 分类管控的配置

15.1 组网需求

某公司以 Device 作为网络边界安全防护设备，配置安全策略，使得 Trust 域的用户可以访问 Untrust 域内的 www.baidu.com 网站，但能访问淘宝网站。

图15-1 安全策略基本功能组网图



15.2 配置思路

- 配置接口地址，分别将接口加入 Trust 和 Untrust 域
- 配置地址对象组
- 配置 URL 分类
- 配置安全策略，安全策略中引用地址对象组和安全域和 URL 分类

15.3 配置步骤

配置接口 GigabitEthernet 5/0/11 的地址。

```
[Device]interface GigabitEthernet
5/0/11
[Device-GigabitEthernet5/0/11]ip address 17.1.1.1 24
```

配置接口 GigabitEthernet 5/0/12 的地址

```
[Device]interface GigabitEthernet 5/0/12
[Device-GigabitEthernet5/0/12]ip address 18.1.1.1 24
```

在命令行下将接口 GigabitEthernet 5/0/11 加入 Trust 域。

```
[Device]security-zone name Trust
[Device-security-zone-Trust]import interface GigabitEthernet 5/0/11
```

在命令行下将接口 GigabitEthernet 5/0/12 加入 Untrust 域。

```
[Device]security-zone name Untrust
[Device-security-zone-Untrust]import interface GigabitEthernet 5/0/12
```

创建名称为 trust-untrust 的地址对象组，IP 地址范围从 17.1.1.2~17.1.1.200

```
[Device]object-group ip address trust-untrust
[Device-obj-grp-ip-trust-untrust]network range 17.1.1.2 17.1.1.200
```

#创建名称为百度和淘宝的 URL 分类

```
[Device] url-filter category baidu severity 5001
[Device-url-filter-category-baidu] rule 1 host text *baidu.com
[Device] url-filter category taobao severity 5002
[Device-url-filter-category-baidu] rule 1 host text *taobao.com
```

创建安全策略 trust-untrust，过滤条件为：源 IP 地址为 trust-untrust 的地址对象组，源安全域 trust，目的安全域 untrust，url 分类为 baidu，动作放行；开启日志记录和命中策略计数功能。

```
[Device]security-policy ip
[Device-security-policy-ip]rule 0 name trust-untrust
[Device-security-policy-ip-0-trust-untrust]source-ip trust-untrust
[Device-security-policy-ip-0-trust-untrust]source-zone trust
[Device-security-policy-ip-0-trust-untrust]destination-zone untrust
[Device-security-policy-ip-0-trust-untrust]action pass
[Device-security-policy-ip-0-trust-untrust]url-category baidu
[Device-security-policy-ip-0-trust-untrust]counting enable
```

创建安全策略 drop-taobao，过滤条件为：源 IP 地址为 trust-untrust 的地址对象组，源安全域 trust，目的安全域 untrust，url 分类为 taobao，动作拒绝；开启日志记录和命中策略计数功能。

```
[Device]security-policy ip
[Device-security-policy-ip]rule 1 name drop-taobao
[Device-security-policy-ip-1-drop-taobao]source-ip trust-untrust
[Device-security-policy-ip-1-drop-taobao]source-zone trust
[Device-security-policy-ip-1-drop-taobao]destination-zone untrust
[Device-security-policy-ip-1-drop-taobao]action drop
[Device-security-policy-ip-1-drop-taobao]url-category taobao
[Device-security-policy-ip-1-drop-taobao]counting enable
```

15.4 注意事项

- 由于网络环境中一些知名网站中存在多个域名，当访问其网站时也需要放行相关联的 URL 域名地址，不然网站可能会打不开，可将与主 URL 相关的域名加到同一个 URL 分类下。
- URL 分类配置项不支持安全策略加速。
- 自定义 URL 不需要升级 URL 特征库。
- 配置安全策略时，请按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

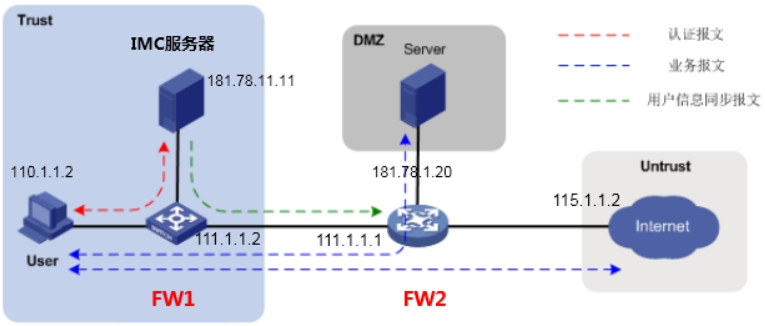
H3C FW 与 EIA 组件对接开局指导

16 FW 与 EIA 组件对接基本功能

16.1 组网需求

如图 19_1 所示，可以通过 IMC 直接导入信息到 FW 设备。

图16-1 FW 与 EIA 组件组网图



16.2 配置思路

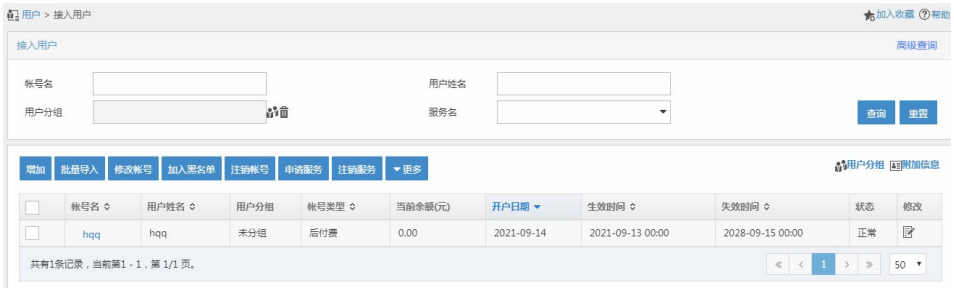
- IMC 上添加设备
- 在 FW 上开启身份识别功能，开启 restful 服务
- FW 上配置 imc 服务器信息
- FW 上配置用户导入策略

16.3 配置步骤

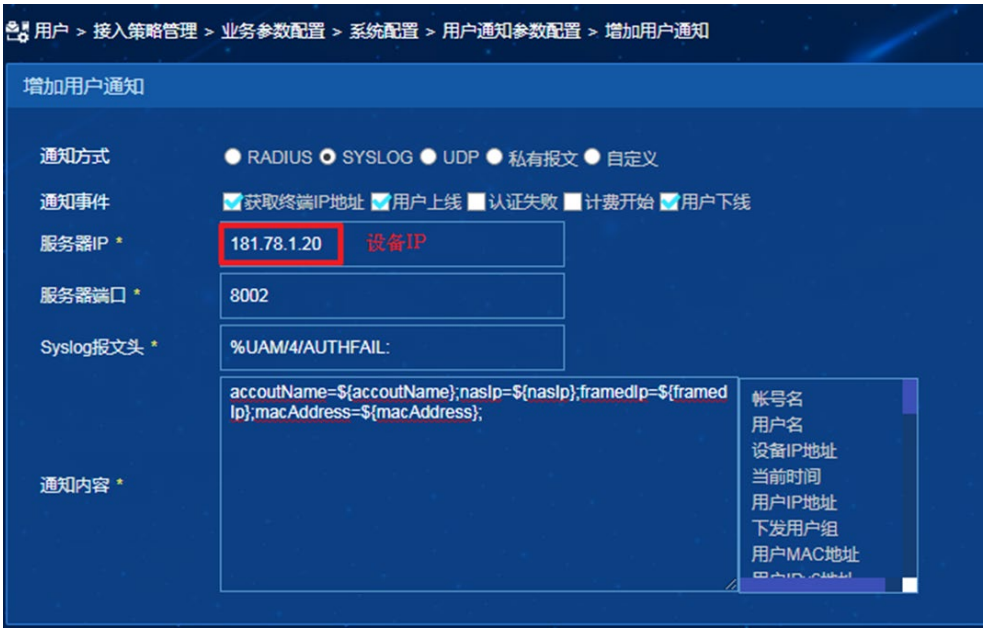
16.3.1 IMC 配置

添加设备

查看接入用户



用户-接入策略管理-业务参数配置-系统配置-用户通知参数配置-增加用户通知：



注意：此处的服务器 ip 为被同步用户信息的 fw 设备，端口与设备侧配置的保持一致

点击用户-接入策略管理-业务参数配置-系统配置手动生效

16.3.2 设备配置

接口加入安全域，配置安全策略

```
<H3C> System-view
[H3C]interface Ten-GigabitEthernet2/0/7
[H3C-GigabitEthernet7/0/2]ip address 181.78.1.20 16
将接口 Ten-GigabitEthernet2/0/7 加入 Trust 域
[H3C] security-zone name Trust
[H3C-security-zone-Trust]import interface Ten-GigabitEthernet 2/0/7
```

开启 restful 的 http 和 https 服务：

```
[H3C]restful http enable
[H3C]restful https enable
```

开启身份识别用户开关

user-identity enable

注意：如果只是要导入接入用户，以上命令可不用开启

配置 restful 服务器（即 IMC 服务器）参数：

```
[H3C]user-identity restful-server imc
[H3C-restfulserver-imc] login-name admin password simple 1qaz!QAZ
[H3C-restfulserver-imc] uri get-user-database http://181.78.11.11:8080/imcr
s/uam/acmUser/acmUserList
[H3C-restfulserver-imc] connection-detect enable
```

配置 sec-manage 服务器信息：

```
[H3C]user-identity security-manage-server imc
[H3C-identity-sec-manage-server-imc] ip 181.78.11.11
[H3C-identity-sec-manage-server-imc] listen-port 8002
```

配置用户导入策略

```
[H3C]user-identity user-import-policy imc
[H3C-identity-user-impt-policy-imc] restful-server imc
```

导入身份识别用户：

```
[H3C]user-identity user-account import policy imc
```

此时 FW2 已导入 user 的身份用户信息

配置安全策略，允许 user 用户访问公网 115.1.1.2

```
[H3C]security-policy ip
[H3C-security-policy-ip]rule 3 name 1
[H3C-security-policy-ip-3-1]action pass
[H3C-security-policy-ip-3-1]user user
```

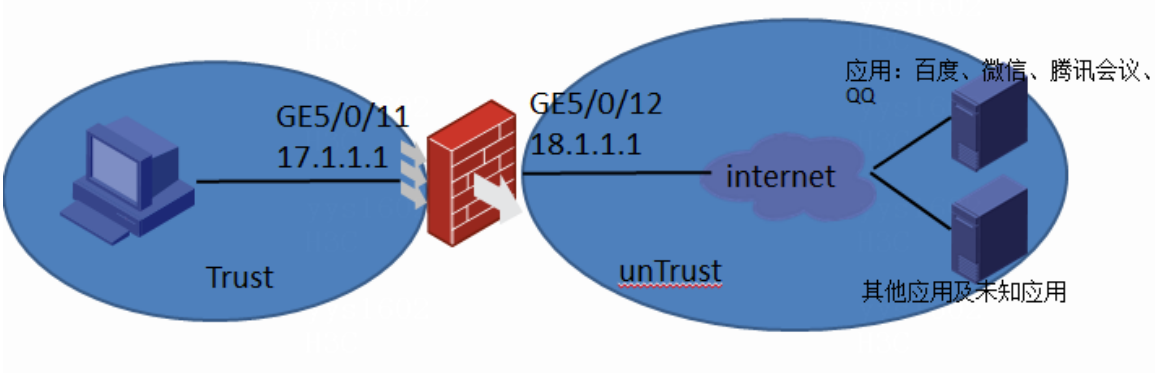
以上配置完成用户登陆之后无需再次在防火墙上进行验证就可以通过防火墙访问外网

17 M9000 支持安全策略对未知应用识别管控的配置

17.1 组网需求

某公司以 Device 作为网络边界安全防护设备，配置安全策略，使得 Trust 域的用户可以访问百度应用、微信、QQ、腾讯会议；拒绝访问其他任何应用软件，包括特征库中识别不出的未知应用。

图17-1 功能组网图



17.2 配置思路

- 配置接口地址，分别将接口加入 Trust 和 Untrust 域
- 配置地址对象组
- 安装 License，升级官网最新 APR 特征库
- 配置安全策略，安全策略中引用地址对象组、安全域和应用

17.3 配置步骤

配置接口 GigabitEthernet 5/0/11 的地址。

```
[Device]interface GigabitEthernet 5/0/11
[Device-GigabitEthernet5/0/11]ip address 17.1.1.1 24
```

配置接口 GigabitEthernet 5/0/12 的地址

```
[Device]interface GigabitEthernet 5/0/12
[Device-GigabitEthernet5/0/12]ip address 18.1.1.1 24
```

在命令行下将接口 GigabitEthernet 5/0/11 加入 Trust 域。

```
[Device]security-zone name Trust
[Device-security-zone-Trust]import interface GigabitEthernet 5/0/11
```

在命令行下将接口 GigabitEthernet 5/0/12 加入 Untrust 域。

```
[Device]security-zone name Untrust
[Device-security-zone-Untrust]import interface GigabitEthernet 5/0/12
```

创建名称为 trust-untrust 的地址对象组，IP 地址范围从 17.1.1.2~17.1.1.200

```
[Device]object-group ip address trust-untrust
[Device-obj-grp-ip-trust-untrust]network range 17.1.1.2 17.1.1.200
```

#安装 License，先有授权码，由授权码生成激活文件,将 ak 激活文件导入设备 flash 中，进行加载安装。

```
[Device]license activation-file install flsh:/xxxxxxxxxxxxxxxxx.ak
```

#从 h3c 官网下载最新 APR 特征库文件导入设备 flash 中，手动离线升级应用识别特征库库。

```
[Device]apr signature update V7-APR-1.0.120.dat
```

创建安全策略 basic-app，过滤条件为：源安全域 trust，目的安全域 untrust，应用项为应用识别的基础协议应用，为了能够识别出更上层应用，动作放行。

```
[Device]security-policy ip
[Device-security-policy-ip]rule 0 name basic-app
[Device-security-policy-ip-0-trust-untrust]source-zone trust
[Device-security-policy-ip-0-trust-untrust]destination-zone untrust
[Device-security-policy-ip-0-trust-untrust]action pass
[Device-security-policy-ip-0-trust-untrust]application dns
[Device-security-policy-ip-0-trust-untrust]application http
[Device-security-policy-ip-0-trust-untrust]application https
[Device-security-policy-ip-0-trust-untrust]application general_udp
[Device-security-policy-ip-0-trust-untrust]application general_tcp
```

创建安全策略 trust-untrust，过滤条件为：源 IP 地址为 trust-untrust 的地址对象组，源安全域 trust，目的安全域 untrust，应用项为需要访问的应用，动作为放行。

```
[Device]security-policy ip
[Device-security-policy-ip]rule 1 name trust-untrust
[Device-security-policy-ip-1-trust-untrust]source-ip trust-untrust
[Device-security-policy-ip-1-trust-untrust]source-zone trust
[Device-security-policy-ip-1-trust-untrust]destination-zone untrust
[Device-security-policy-ip-1-trust-untrust]action pass
[Device-security-policy-ip-1-trust-untrust]application WeChat
[Device-security-policy-ip-1-trust-untrust]application QQ
[Device-security-policy-ip-1-trust-untrust]application BaiDu
[Device-security-policy-ip-1-trust-untrust]application TencentMeeting
[Device-security-policy-ip-1-trust-untrust]counting enable
```

创建安全策略 drop-app，过滤条件为：源 IP 地址为 trust-untrust 的地址对象组，源安全域 trust，目的安全域 untrust，应用为其他应用，动作拒绝。

```
[Device]security-policy ip
[Device-security-policy-ip]rule 2 name drop-app
[Device-security-policy-ip-2-drop-app]source-ip trust-untrust
[Device-security-policy-ip-2-drop-app]source-zone trust
[Device-security-policy-ip-2-drop-app]destination-zone untrust
[Device-security-policy-ip-2-drop-app]action drop
[Device-security-policy-ip-2-drop-app]application http_other
[Device-security-policy-ip-2-drop-app]application https_other
[Device-security-policy-ip-2-drop-app]application tcp_other
[Device-security-policy-ip-2-drop-app]application udp_other
[Device-security-policy-ip-2-drop-app]counting enable
```

17.4 注意事项

- 上层应用的识别需要依赖基础协议应用，为使安全策略中配置的应用可以被识别，就必须允许应用所依赖的基础协议的报文通过。

- 设备在一定阈值的载荷报文之后，如果依然无法识别更高层的应用，这条流即不再识别应用，而其七层应用设置为 xxx 其它应用。为了体现已经识别出是基于 xxx 协议并且其上层应用是未知的。
- 有的应用允许访问时需要放行其关联的应用，否则此应用软件或者网站可能会访问不了或者页面打不开，根据需求进行放行应用。
- 配置安全策略时，请按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

18 Qos 优化配置—硬件限速

18.1 Qos 简介

QoS 策略由如下部分组成：

- 类，定义了对报文进行识别的规则。
- 流行为，定义了一组针对类识别后的报文所做的 QoS 动作。

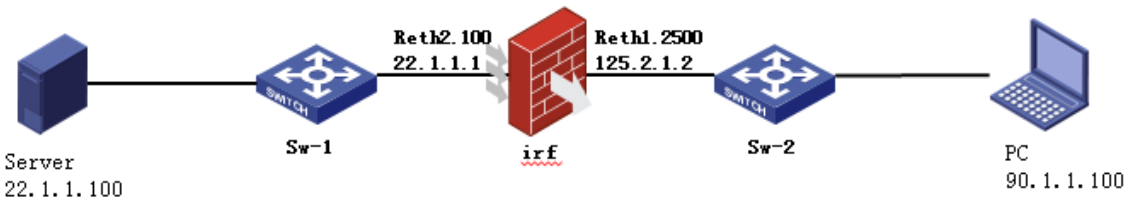
通过将类和流行为关联起来，QoS 策略可对符合分类规则的报文执行流行为中定义的动作。

用户可以在一个策略中定义多个类与流行为的绑定关系。

18.2 配置内网至外网的qos限速（outbound）

18.2.1 配置组网

如图所示：



18.2.2 配置思路

- 私网用户 server ip 经防火墙后，对外显示已是 nat 后的地址，所以从内外到外网进行限速通过匹配源 ip 来实现，源 ip 为浮动 ip 地址；

18.2.3 配置步骤

配置 ACL，匹配源 ip。

```
[H3C]acl advanced name out-car1
[H3C-acl-ipv4-adv-out-car1] rule 0 permit ip source 125.2.1.100 0
```

配置出方向 qos 全局 car。

```
[H3C]qos car out-car1 aggregative cir 2048 cbs 1024
```

配置出方向 qos 流分类。

```
[H3C]traffic classifier out-car1
[H3C-classifier-out-car1] if-match acl name out-car1
```

配置出方向 qos 流行为。

```
[H3C]traffic behavior out-car1
[H3C-behavior-out-car1] car name out-car1
```

配置出方向 qos 策略。

```
[H3C]qos policy out-car1
[H3C-qospolicy-out-car1] classifier out-car1 behavior out-car1
```

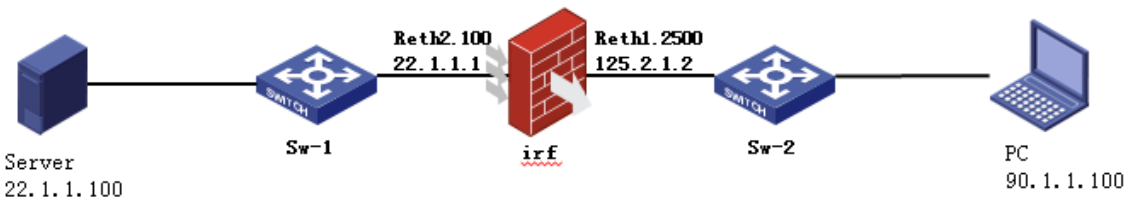
在 reth1 接口应用出方向 qos 策略。（不支持在子接口应用，直接在主接口进行应用，主接口对应的子接口皆可生效）

```
[H3C]int Reth 1
[H3C-Reth1] qos apply policy out-car1 outbound enhancement
```

18.3 配置外网至内网的qos限速（inbound）

18.3.1 配置组网

如图所示：



18.3.2 配置思路

- 外网用户 PC 直接访问 nat 后的地址，所以从外网到内网进行限速通过匹配目的 ip 来实现，源 ip 为浮动 ip 地址；

18.3.3 配置步骤

配置 ACL，匹配目的 ip。

```
[H3C]acl advanced name in-car1
[H3C-acl-ipv4-adv-in-car1] rule 0 permit ip destination 125.2.1.100 0
```

配置入方向 qos 全局 car。

```
[H3C]qos car in-car1 aggregative cir 2048 cbs 1024
```

配置入方向 qos 流分类。

```
[H3C]traffic classifier in-car1
[H3C-classifier-in-car1] if-match acl name in-car1
```

配置入方向 qos 流行为。

```
[H3C]traffic behavior in-car1
[H3C-behavior-in-car1] car name in-car1
```

配置入方向 qos 策略。

```
[H3C]qos policy in-car1
[H3C-qospolicy-in-car1] classifier in-car1 behavior in-car1
```

在 reth1 接口应用出方向 qos 策略。（不支持在子接口应用，直接在主接口进行应用，主接口对应的子接口皆可生效）

```
[H3C]int Reth 1
[H3C-Reth1] qos apply policy in-car1 inbound enhancement
```

18.3.4 注意事项

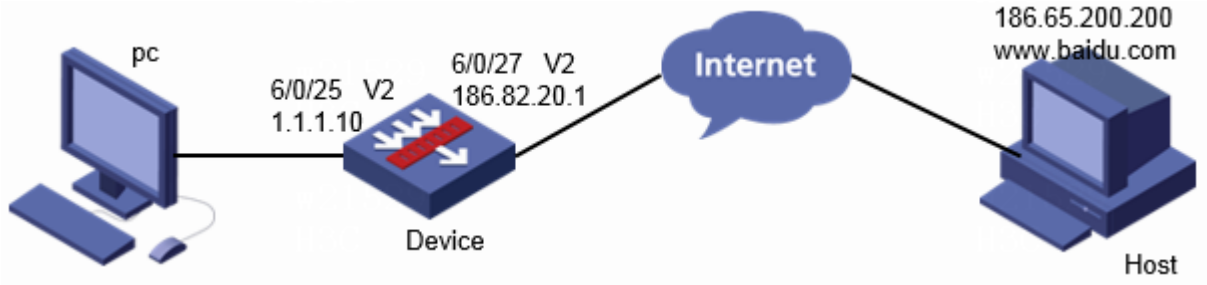
1. 不推荐多 context 场景；
2. 流分类下的 ACL 只能引用一个，且 ACL 中只支持配置 ip 和端口，不支持引用对象组；
3. QoS car 全局 car 不可以被多个流行为共用，否则设置的限速值会成命中各流行为限速流量的被限速总值
4. 内存门限后重启进程会导致 openflow 表项下刷失败，门限下不要进行进程重启等操作；
5. 冗余口下成员口为聚合子接口，该组网不支持，不建议配置；
6. 聚合口下物理成员口建议单块接口卡出单一接口，NSQM1CGQ4TG24SHA0 接口卡支持配置 2k 限速，若聚合口下两个物理成员口为同块接口卡接口，则 outbound 方向限速规格支持配置 1.5k，inbound 方向支持配置 2k，同板接口成员越多，outbound 方向支持配置限速规格越低；
7. v6 qos 配置全局 car 限速会影响 v4 的限速规格；

19 M9000 的接口绑定 VPN 的情况下支持配置基于域名的地址组对象

19.1 组网需求

某公司以 Device 作为网络边界安全防护设备，配置路由，对象组可以配置带 VPN 的主机名对象，获取不同 vpn 下主机名对应的 IP 地址信息。本文以域名为 www.baidu.com 的网站为例。

图19-1 基本组网组网图



19.2 配置思路

- 配置接口地址，将接口绑定 vpn
- 配置路由
- 配置地址对象组绑定 vpn
- 配置安全策略，安全策略中引用包含主机名的地址对象组

19.3 配置步骤

配置 VPN

```
[Device]ip vpn-instance v2
```

配置接口 GigabitEthernet6/0/25 的地址。

```
[Device]interface GigabitEthernet 6/0/25
[Device-GigabitEthernet5/0/11]ip address 1.1.1.10 24
```

#配置接口 GigabitEthernet6/0/25 绑定 VPN

```
[Device]interface GigabitEthernet 6/0/25
[Device-GigabitEthernet6/0/25] ip binding vpn-instance v2
```

配置接口 GigabitEthernet6/0/27 的地址。

```
[Device]interface GigabitEthernet 6/0/27
[Device-GigabitEthernet5/0/11]ip address 186.82.20.1 16
```

#配置接口 GigabitEthernet6/0/27 绑定 VPN

```
[Device]interface GigabitEthernet 6/0/27
[Device-GigabitEthernet6/0/27] ip binding vpn-instance v2
```

在命令行下将接口 GigabitEthernet 6/0/25 加入 Trust 域。

```
[Device]security-zone name Trust
[Device-security-zone-Trust]import interface GigabitEthernet 6/0/25
```

在命令行下将接口 GigabitEthernet t6/0/27 加入 Trust 域。

```
[Device]security-zone name trust
[Device-security-zone-trust]import interface GigabitEthernet 6/0/27
```

创建名称为 baidu 的绑定 VPN 的地址对象组

```
[Device]object-group ip address baidu
[Device-obj-grp-ip-baidu] network host name www.baidu.com vpn-instance v2
```

创建安全策略 yuming，过滤条件为：VRF 为 v2

```
[Device]security-policy ip
[Device-security-policy-ip]rule 0 name yuming
[Device-security-policy-ip-0-yuming]source-zone trust
[Device-security-policy-ip-0-yuming]source-zone untrust
```

```
[Device-security-policy-ip-0-yuming]destination-zone trust
[Device-security-policy-ip-0-yuming]destination-zone untrust
[Device-security-policy-ip-0-yuming]action pass
[Device-security-policy-ip-0-yuming] vrf v2
[Device-security-policy-ip-0-yuming] destination-ip baidu
```

#功能实现验证

```
[Device]ping -vpn-instance v2 www.baidu.com
Ping www.baidu.com (186.65.200.200): 56 data bytes, press CTRL+C to break
56 bytes from 186.65.200.200: icmp_seq=0 ttl=127 time=1.464 ms
56 bytes from 186.65.200.200: icmp_seq=1 ttl=127 time=0.959 ms
56 bytes from 186.65.200.200: icmp_seq=2 ttl=127 time=0.955 ms
56 bytes from 186.65.200.200: icmp_seq=3 ttl=127 time=0.959 ms
56 bytes from 186.65.200.200: icmp_seq=4 ttl=127 time=1.085 ms

--- Ping statistics for www.baidu.com in VPN instance v2 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 0.955/1.084/1.464/0.196 ms
```

19.4 注意事项

- 当安全策略与包过滤同时配置时，因为安全策略对报文的处理在包过滤之前，报文与安全策略规则匹配成功后，不再进行包过滤处理，所以请合理配置安全策略和包过滤，否则可能会导致配置的包过滤不生效。
- 配置安全策略时，请按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

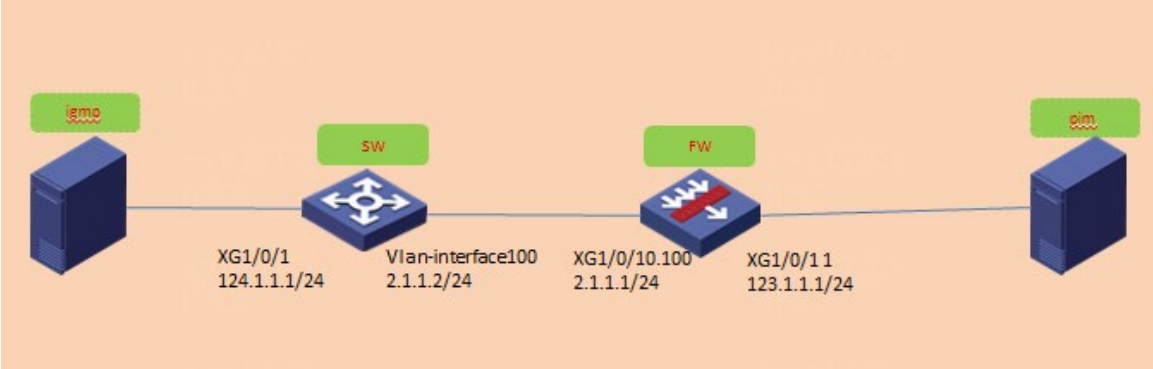
20 跨 VPN 组播配置

20.1 组播简介

组播 VPN（Virtual Private Network，虚拟专用网络）用于在 VPN 网络中实现组播传输。

20.2 配置ipv4 跨VPN组播转发

20.2.1 配置组网



20.2.2 配置思路

防火墙配置跨 VPN 组播路由使组播可以跨 VPN 转发

20.2.3 配置步骤

#配置内外网 VPN

```
[H3C]ip vpn-instance external_vpn
[H3C]ip vpn-instance siwang_vpn
```

配置 ospf 动态路由，用于发布和学习组播 rp 信息

```
[H3C]ospf 100 router-id 2.2.2.2 vpn-instance external_vpn  OSPF
 area 0.0.0.0
```

#接口配置：

```
[H3C]interface Ten-GigabitEthernet 1/0/10.100
 ip binding vpn-instance external_vpn
 ip address 2.1.1.1 255.255.255.0
 ospf 100 area 0.0.0.0
 pim sm
 vlan-type dot1q vid 100
#
[H3C]interface Ten-GigabitEthernet 1/0/11
 ip binding vpn-instance siwang_vpn
 ip address 123.1.1.1 255.255.255.0
 pim sm
```

配置 rp，rp 也可以放置在交换机中，防火墙上不是必须配置

```
interface LoopBack0
 ip binding vpn-instance siwang_vpn
```

```
 ip address 1.1.1.1 255.255.255.255
 pim sm
#
interface LoopBack1
 ip binding vpn-instance external_vpn
 ip address 2.2.2.2 255.255.255.255
 ospf 100 area 0.0.0.0
 pim sm
#
pim vpn-instance external_vpn
 c-bsr 2.2.2.2
 c-rp 2.2.2.2
#
pim vpn-instance siwang_vpn
 static-rp 1.1.1.1
```

配置跨 VPN 组播路由

```
multicast routing vpn-instance external_vpn
multicast extranet select-rpf vpn-instance siwang_vpn source 2.2.2.0 24 group 226.0.0.0
24
multicast extranet select-rpf vpn-instance siwang_vpn source 123.1.1.0 24 group 226.0.0.0
24
```

#配置安全域，必须把对端 vpn 也要加到安全域中，不然会被 aspf 丢弃

```
security-zone name Trust
 import interface LoopBack0
 import interface LoopBack1
 import interface Ten-GigabitEthernet 1/0/10.100
 import interface Ten-GigabitEthernet 1/0/11
 import ip 123.1.1.0 24 vpn-instance siwang_vpn
import ip 123.1.1.0 24 vpn-instance external_vpn
```

配置安全策略

```
security-policy ip
 rule 0 name 0
  action pass
 rule 1 name 1
  action pass
  vrf external_vpn
 rule 2 name 2
  action pass
```

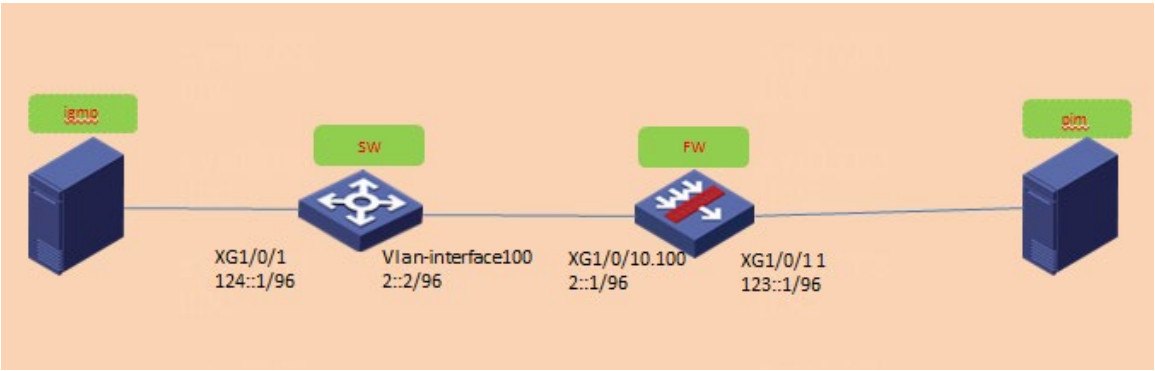
```
  vrf siwang_vpn
#
```

配置交换机：

```
ospf 100 router-id 2.2.2.1
 area 0.0.0.0
#
interface Vlan-interface100
 ip address 2.1.1.2 255.255.255.0
 ospf 100 area 0.0.0.0
 pim sm
#
interface Ten-GigabitEthernet1/0/1
 port link-mode route
 flow-interval 5
 ip address 124.1.1.1 255.255.255.0
 igmp enable
```

20.3 配置ipv6 跨VPN组播转发

20.3.1 配置组网



20.3.2 配置思路

防火墙配置跨 VPN 组播路由使组播可以跨 VPN 转发

20.3.3 配置步骤

#配置内外网 VPN：

```
[H3C]ip vpn-instance external_vpn
[H3C]ip vpn-instance siwang_vpn
```

#配置 ospf 动态路由，用于发布和学习组播 rp 信息

```
ospfv3 100 vpn-instance external_vpn
```

```
 router-id 3.3.3.3
 area 0.0.0.0
```

#接口配置：

```
[H3C]interface Ten-GigabitEthernet 1/0/10.100
 ip binding vpn-instance external_vpn
 ospfv3 100 area 0.0.0.0
 ipv6 pim sm
 vlan-type dot1q vid 100
 ipv6 address 2::1/96
#
interface Ten-GigabitEthernet 1/0/11
 ip binding vpn-instance siwang_vpn
 ipv6 pim sm
 ipv6 address 123::1/96
```

#配置 rp，rp 也可以放置在交换机中，防火墙上不是必须配置

```
interface LoopBack0
 ip binding vpn-instance siwang_vpn
 ipv6 pim sm
 ipv6 address 1::1/128
#
interface LoopBack1
 ip binding vpn-instance external_vpn
 ospfv3 100 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2:2:2::2/128
#
ipv6 pim vpn-instance siwang_vpn
 static-rp 1::1
#
ipv6 pim vpn-instance external_vpn
 c-bsr 2:2:2::2
 c-rp 2:2:2::2
```

#配置跨 VPN 组播路由

```
ipv6 multicast routing vpn-instance external_vpn              跨 VPN 转发策略
 ipv6 multicast extranet select-rpf vpn-instance a source 2:2:2:: 96 group FF1E:
: 96
 ipv6 multicast extranet select-rpf vpn-instance a source 123:: 96 group FF1E::
96
```

#配置安全域，必须把对端 vpn 也要加到安全域中，不然会被 aspf 丢弃

```
security-zone name Trust
 import interface LoopBack0
 import interface LoopBack1
 import interface Ten-GigabitEthernet 1/0/10.100
 import interface Ten-GigabitEthernet 1/0/11
 import ipv6 123:: 64 vpn-instance siwang_vpn
import ipv6 123:: 64 vpn-instance external_vpn
```

#配置安全策略

```
security-policy ipv6
 rule 0 name 0
  action pass
 rule 1 name 1
  action pass
  vrf siwang_vpn
 rule 2 name 2
  action pass
  vrf external_vpn
```

配置交换机：

```
ospfv3 100
 router-id 3.3.3.1
 area 0.0.0.0
#
interface Vlan-interface200
 ospfv3 100 area 0.0.0.0
 ipv6 pim sm
 ipv6 address 2::2/96
#
interface Ten-GigabitEthernet1/0/3
 port link-mode route
 flow-interval 5
 ipv6 address 124::1/96
 mld enable
```