H3C SecPath 入侵防御系统

虚拟化技术配置指导(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W204-20190429
产品版本：

T5010/T5020	R8514
T5030/T5060/T5080/T5000-S/T5000-C	R8501
T1020/T1030/T1050/T1060/T1080	R8514
T1000-AK340/AK350	R8514
LSWM1IPSD0/LSQM1IPSDSC0/IM-IPSX-IV	R8512

前 言

本配置指导主要介绍 IRF 和 Context 相关的特性。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

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

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

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

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 IRF

1.1 IRF简介

IRF（Intelligent Resilient Framework，智能弹性架构）是 H3C 自主研发的软件虚拟化技术。它的核心思想是将多台设备连接在一起，进行必要的配置后，虚拟化成一台设备。使用这种虚拟化技术可以集合多台设备的硬件资源和软件处理能力，实现多台设备的协同工作、统一管理和不间断维护。为了便于描述，这个“虚拟设备”也称为 IRF。所以，本文中的 IRF 有两层意思，一个是指 IRF 技术，一个是指 IRF 设备。

1.1.1 IRF的优点

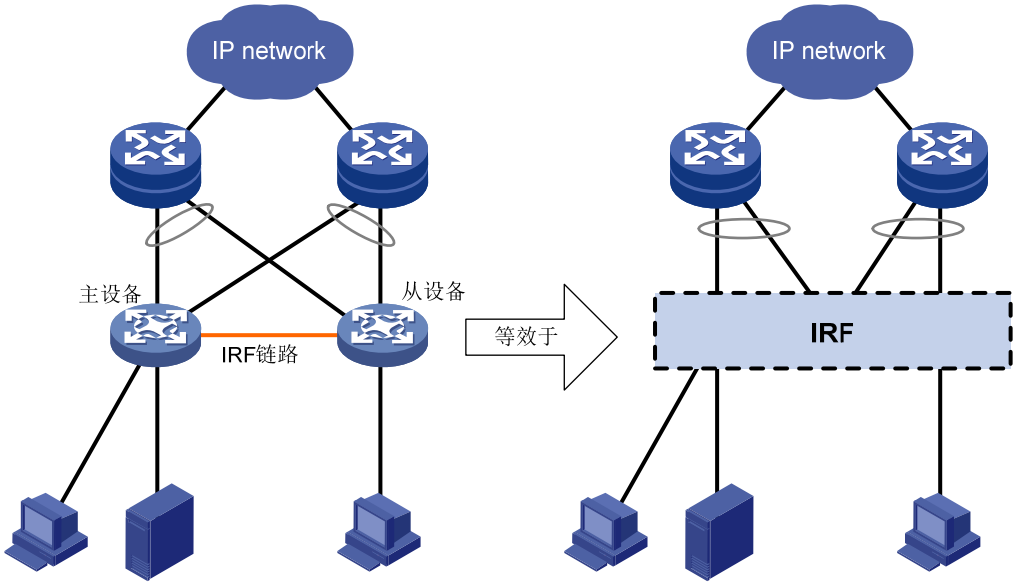
IRF 主要具有以下优点：

- 简化管理。IRF 形成之后，用户通过任意成员设备的任意端口都可以登录 IRF 系统，对 IRF 内所有成员设备进行统一管理。
- 1:N 备份。IRF 由多台成员设备组成，其中，主设备负责 IRF 的运行、管理和维护，从设备在作为备份的同时也可以处理业务。一旦主设备故障，系统会迅速自动选举新的主设备，以保证业务不中断，从而实现了设备的 1:N 备份。
- 跨成员设备的链路聚合。IRF 和上、下层设备之间的物理链路支持聚合功能，并且不同成员设备上的物理链路可以聚合成一个逻辑链路，多条物理链路之间可以互为备份也可以进行负载分担，当某个成员设备离开 IRF，其它成员设备上的链路仍能收发报文，从而提高了聚合链路的可靠性。
- 强大的网络扩展能力。通过增加成员设备，可以轻松自如的扩展 IRF 的端口数、带宽。因为各成员设备都有 CPU，能够独立处理协议报文、进行报文转发，所以 IRF 还能轻松自如的扩展处理能力。

1.1.2 IRF的应用

如 图 1-1 所示，主设备和从设备组成IRF，对上、下层设备来说，它们就是一台设备——IRF。

图1-1 IRF 组网应用示意图



1.1.3 IRF基本概念

1. 角色

IRF 中每台设备都称为成员设备。成员设备按照功能不同，分为两种角色：

- 主用设备（简称为主设备）：负责管理和控制整个 IRF。
- 从属设备（简称为从设备）：处理业务、转发报文的同时作为主设备的备份设备运行。当主设备故障时，系统会自动从从设备中选举一个新的主设备接替原主设备工作。

主设备和从设备均由角色选举产生。一个IRF中同时只能存在一台主设备，其它成员设备都是从设备。关于设备角色选举过程的详细介绍请参见“1.2.3 角色选举”。

2. IRF端口

一种专用于 IRF 成员设备之间进行连接的逻辑接口，每台成员设备上可以配置两个 IRF 端口，分别为 IRF-Port1 和 IRF-Port2。它需要和物理端口绑定之后才能生效。

IRF 端口采用二维编号，分为 IRF-Port*n*/1 和 IRF-Port*n*/2，其中 *n* 为设备的成员编号。

为简洁起见，本文描述时统一使用 IRF-Port1 和 IRF-Port2。

3. IRF物理端口

与 IRF 端口绑定，用于 IRF 成员设备之间进行连接的物理接口。

通常情况下，电口或者光口负责向网络中转发业务报文，将它们与 IRF 端口绑定后就作为 IRF 物理端口，可转发的报文包括 IRF 相关协商报文以及需要跨成员设备转发的业务报文。

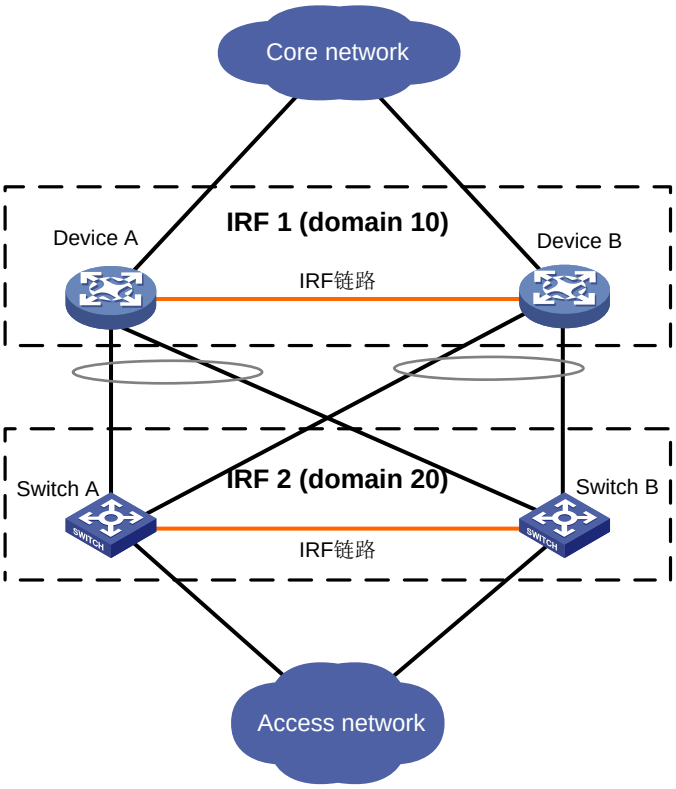
由于 IRF 物理端口上不能开启 STP 或其它环路控制协议，IRF 成员设备需要根据接收和发送报文的端口以及 IRF 的当前拓扑，来判断报文在发送后是否会产生环路。如果判断结果为会产生环路，设备将在位于环路路径上的发送端口处将报文丢弃。该方式会造成大量广播报文在 IRF 物理端口上被丢弃，此为正常现象。在使用 SNMP 工具监测设备端口的收发报文记录时，取消对 IRF 物理端口的监测，可以避免收到大量丢弃报文的告警信息。

4. IRF域

域是一个逻辑概念，一个 IRF 对应一个 IRF 域。

为了适应各种组网应用，同一个网络里可以部署多个IRF，IRF之间使用域编号（DomainID）来以示区别。如 图 1-2 所示，Device A和Device B组成IRF 1，Switch A和Switch B组成IRF 2。如果IRF 1 和IRF 2 之间有MAD检测链路，则两个IRF各自的成员设备间发送的MAD检测报文会被另外的IRF接收到，从而对两个IRF的MAD检测造成影响。这种情况下，需要给两个IRF配置不同的域编号，以保证两个IRF互不干扰。

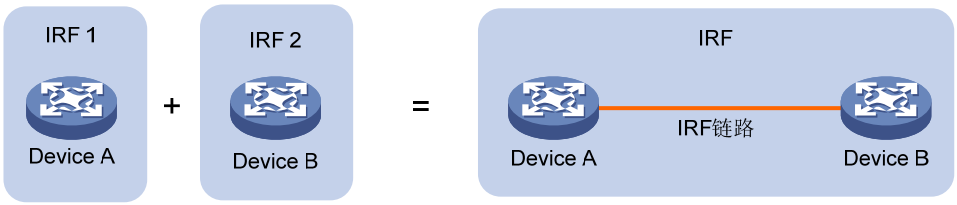
图1-2 多 IRF 域示意图



5. IRF合并

如 图 1-3 所示，两个IRF各自已经稳定运行，通过物理连接和必要的配置，形成一个IRF，这个过程称为IRF合并。

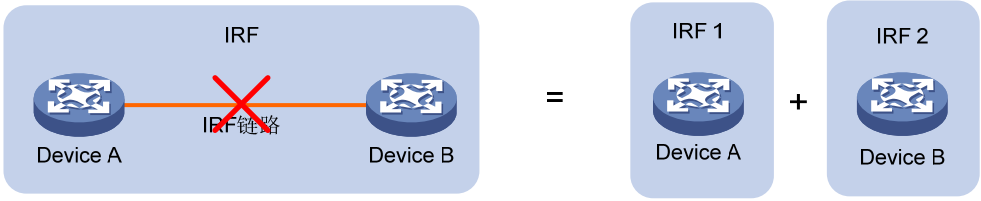
图1-3 IRF 合并示意图



6. IRF分裂

如 图 1-4 所示，一个IRF形成后，由于IRF链路故障，导致IRF中两相邻成员设备不连通，一个IRF变成两个IRF，这个过程称为IRF分裂。

图1-4 IRF 分裂示意图



7. 成员优先级

成员优先级是成员设备的一个属性，主要用于角色选举过程中确定成员设备的角色。优先级越高当选为主设备的可能性越大。

设备的缺省优先级均为 1，如果想让某台设备当选为主设备，则在组建 IRF 前，可以通过命令行手工提高该设备的成员优先级。

1.2 IRF工作原理

IRF系统将经历 物理连接、拓扑收集、角色选举、IRF的管理与维护四个阶段。成员设备之间需要先建立IRF物理连接，然后会自动进行拓扑收集和角色选举，完成IRF的建立，此后进入IRF管理和维护阶段。

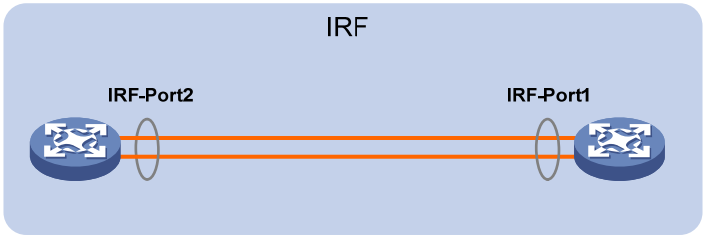
1.2.1 物理连接

要形成一个 IRF，需要先连接成员设备的 IRF 物理端口。

1. 连接要求

本设备上与IRF-Port1 口绑定的IRF物理端口只能和邻居成员设备IRF-Port2 口上绑定的IRF物理端口相连，本设备上与IRF-Port2 口绑定的IRF物理端口只能和邻居成员设备IRF-Port1 口上绑定的IRF物理端口相连，如 图 1-5 所示。否则，不能形成IRF。

图1-5 IRF 物理连接示意图



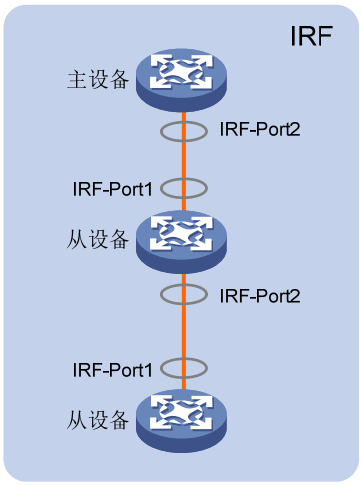
- 设备出厂时没有将 IRF 端口与 IRF 物理端口绑定，需要用户通过命令行手工配置后才能用于 IRF。
- 一个 IRF 端口可以与一个或多个 IRF 物理端口绑定，以提高 IRF 链路的带宽以及可靠性。

2. 连接拓扑

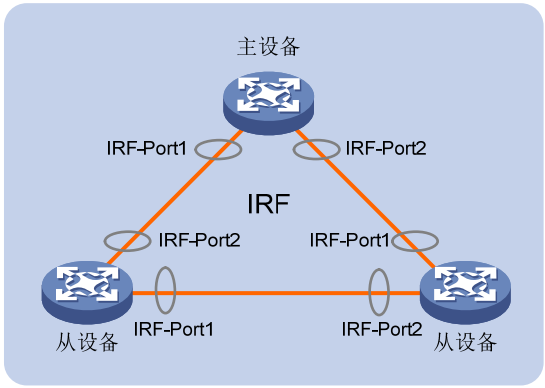
IRF的连接拓扑有两种：链形连接和环形连接，如 图 1-6 所示。

- 链形连接对成员设备的物理位置要求比环形连接低，主要用于成员设备物理位置分散的组网。
- 环形连接比链形连接更可靠。因为当链形连接中出现链路故障时，会引起 IRF 分裂；而环形连接中某条链路故障时，会形成链形连接，IRF 的业务不会受到影响。

图1-6 IRF 连接拓扑示意图



链形连接



环形连接

说明

目前，设备仅支持链形连接。

1.2.2 拓扑收集

每个成员设备和邻居成员设备通过交互 IRF Hello 报文来收集整个 IRF 的拓扑。IRF Hello 报文会携带拓扑信息，具体包括 IRF 端口连接关系、成员设备编号、成员设备优先级、成员设备的桥 MAC 等内容。

每个成员设备在本地记录自己已知的拓扑信息。设备刚启动时只记录了自身的拓扑信息。当 IRF 端口状态变为 up 后，设备会将已知的拓扑信息周期性的从 up 状态的 IRF 端口发送出去；邻居收到该信息后，会更新本地记录的拓扑信息；如此往复，经过一段时间的收集，所有成员设备都会收集到完整的拓扑信息。

此时会进入角色选举阶段。

1.2.3 角色选举

确定成员设备角色为主设备或从设备的过程称为角色选举。角色选举会在以下情况下进行：IRF 建立、主设备离开或者故障、两个 IRF 合并等。其中，IRF 合并包括合并前独立运行的两个 IRF 合并为一个 IRF 和 IRF 分裂后重新合并两种情况。

IRF 建立、主设备离开或者故障、独立运行的两个 IRF 合并为一个 IRF 时，角色选举规则如下：

(1) 当前主设备优先，IRF 不会因为有新的成员设备加入而重新选举主设备。不过，当 IRF 形成时，因为没有主设备，所有加入的设备都认为自己是主设备，则继续下一条规则的比较。

(2) 成员优先级大的优先。如果优先级相同，则继续下一条规则的比较。

(3) 系统运行时间长的优先。在 IRF 中，成员设备启动时间间隔精度为 10 分钟，即 10 分钟之内启动的设备，则认为它们是同时启动的，则继续下一条规则的比较。

(4) CPU MAC 小的优先。

通过以上规则选出的最优成员设备即为主设备，其它成员设备则均为从设备。

IRF 分裂后重新合并时，原 Recovery 状态 IRF 中所有成员设备重启后以从设备身份加入原正常工作状态的 IRF，原正常工作状态的 IRF 的主设备作为合并后 IRF 的主设备。

在角色选举完成后，IRF 形成，进入 IRF 管理与维护阶段。

说明

- IRF 合并的情况下（分裂后重新合并的情况除外），每个 IRF 的主设备间会进行竞选，竞选仍然遵循角色选举的规则，竞选失败方的所有成员设备重启后均以从设备的角色加入获胜方，最终合并为一个 IRF。合并过程中的重启是设备自动完成的。
- 不管设备与其它设备一起形成 IRF，还是加入已有 IRF，如果该设备被选为从设备，则该设备会使用主设备的配置重新启动，以保证和主设备上的配置一致，本设备上的配置文件还在，但不再生效。

1.2.4 IRF的管理与维护

角色选举完成之后，IRF 形成，所有的成员设备组成一台虚拟设备存在于网络中，所有成员设备上的资源归该虚拟设备拥有并由主设备统一管理。

1. 成员编号

在运行过程中，IRF 使用成员编号来标识成员设备，以便对其进行管理。例如，IRF 中接口的编号会加入成员编号信息：当设备独立运行时，接口编号第一维参数的值通常为 1，加入 IRF 后，接口编号第一维参数的值会变成成员编号的值。所以，在 IRF 中必须保证所有设备成员编号的唯一性。

如果建立 IRF 时存在编号相同的成员设备，则不能建立 IRF；如果新设备加入 IRF，但是该设备与已有成员设备的编号冲突，则该设备不能加入 IRF。请在建立 IRF 前，请统一规划各成员设备的编号，并逐一进行手工配置，以保证各设备成员编号的唯一性。

2. IRF拓扑维护

如果某成员设备 A 故障或者 IRF 链路故障，其邻居设备会立即将“成员设备 A 离开”的信息广播通知给 IRF 中的其它设备。获取到离开消息的成员设备会根据本地维护的 IRF 拓扑信息表来判断离开的是主设备还是从设备，如果离开的是主设备，则触发新的角色选举，再更新本地的 IRF 拓扑；如果离开的是从设备，则直接更新本地的 IRF 拓扑，以保证 IRF 拓扑能迅速收敛。

说明

IRF 端口的状态由与它绑定的 IRF 物理端口的状态决定。与 IRF 端口绑定的所有 IRF 物理端口状态均为 down 时，IRF 端口的状态才会变成 down。

3. MAD功能

IRF 链路故障会导致一个 IRF 变成多个新的 IRF。这些 IRF 拥有相同的 IP 地址等三层配置，会引起地址冲突，导致故障在网络中扩大。为了提高系统的可用性，当 IRF 分裂时我们就需要一种机制，能够检测出网络中同时存在多个 IRF，并进行相应的处理，尽量降低 IRF 分裂对业务的影响。MAD（Multi-Active Detection，多 Active 检测）就是这样一种检测和处理机制。它主要提供以下功能：

(1) 分裂检测

通过LACP（Link Aggregation Control Protocol，链路聚合控制协议）、BFD（Bidirectional Forwarding Detection，双向转发检测）、ARP（Address Resolution Protocol，地址解析协议）或者ND（Neighbor Discovery，邻居发现）来检测网络中是否存在多个IRF。同一IRF中可以配置一个或多个检测机制，详细信息，请参考“1.8.8 MAD配置”。

(2) 冲突处理

IRF 分裂后，通过分裂检测机制 IRF 会检测到网络中存在其它正常工作的 IRF。

- 对于 LACP MAD 和 BFD MAD 检测，冲突处理会先比较两个 IRF 中成员设备的数量，数量多的 IRF 继续工作；数量少的迁移到 Recovery 状态（即禁用状态）；如果成员数量相等，则主设备成员编号小的 IRF 继续正常工作；其它 IRF 迁移到 Recovery 状态（即禁用状态）。
- 对于 ARP MAD 和 ND MAD 检测，冲突处理会直接让主设备成员编号小的 IRF 继续正常工作；其它 IRF 迁移到 Recovery 状态（即禁用状态）。

IRF 迁移到 Recovery 状态后会关闭该 IRF 中所有成员设备上除保留端口以外的其它所有物理端口（通常为业务接口），以保证该 IRF 不能再转发业务报文。缺省情况下，只有 IRF 物理端口是保留端口，可通过 **mad exclude interface** 命令配置。

(3) MAD 故障恢复

IRF 链路故障导致 IRF 分裂，从而引起多 Active 冲突。因此修复故障的 IRF 链路，让冲突的 IRF 重新合并为一个 IRF，就能恢复 MAD 故障。

- 如果出现故障的是继续正常工作的 IRF，则在进行 MAD 故障恢复前，可以通过命令行先启用 Recovery 状态的 IRF，让它接替原 IRF 工作，以便保证业务尽量少受影响，再恢复 MAD 故障。
- 如果在 MAD 故障恢复前，处于 Recovery 状态的 IRF 也出现了故障，则需要将故障 IRF 和故障链路都修复后，才能让冲突的 IRF 重新合并为一个 IRF，恢复 MAD 故障。

关于 LACP 的详细介绍请参见“二层技术-以太网交换配置指导”中的“以太网链路聚合”；关于 BFD 的详细介绍请参见“可靠性配置指导”中的“BFD”；关于 ARP 的详细介绍请参见“三层技术-IP 业务配置指导”中的“ARP”。

1.3 配置限制和指导

1. 组建IRF时的注意事项

- 通常情况下，必须是同一型号的产品才能组成 IRF。
- 一个 IRF 中允许加入的成员设备的数量存在上限。如果超过上限，则不允许新的成员设备加入。设备最多支持 2 个成员设备。
- IRF 中所有成员设备的软件版本必须相同，如果有软件版本不同的设备要加入 IRF，请确保 IRF 的启动文件同步加载功能处于开启状态。
- 如果两台物理设备的桥 MAC 相同，则它们不能合并为一个 IRF。IRF 的桥 MAC 不受此限制，只要成员设备自身桥 MAC 唯一即可。
- 在组成 IRF 的所有设备上，ACL 硬件模式的相关配置都必须相同，否则这些设备将无法组成 IRF。有关 ACL 硬件模式的详细介绍，请参见“ACL 和 QoS 配置指导”中的“ACL”。
- 在组成 IRF 的所有成员设备上，确保 IRF 端口绑定的物理端口类型、数量一致。
- 设备仅支持 IRF 物理端口直连组建 IRF，不支持跨中间设备。

2. IRF形成后的配置限制和指导

- 以太网接口作为 IRF 物理端口与 IRF 端口绑定后，只支持接口配置命令，包括 **shutdown**、**description** 和 **flow-interval**，这些命令的详细介绍，请参见“接口管理命令参考”中的“以太网接口”。
- 因为 LACP MAD 和 ARP MAD、ND MAD 冲突处理的原则不同，请不要同时配置。BFD MAD 和 ARP MAD、ND MAD 冲突处理的原则不同，并且 BFD MAD 和生成树协议互斥，ARP MAD、ND MAD 需要开启生成树协议，因此 BFD MAD 和 ARP MAD、ND MAD 无法同时配置。
- 在 LACP MAD、ARP MAD 和 ND MAD 检测组网中，如果中间设备本身也是一个 IRF 系统，则必须通过配置确保其 IRF 域编号与被检测的 IRF 系统不同，否则可能造成检测异常，甚至导致业务中断。在 BFD MAD 检测组网中，IRF 域编号为可选配置。
- IRF 域编号是一个全局变量，IRF 中的所有成员设备都共用这个 IRF 域编号。因此，请按照网络规划来修改 IRF 域编号，不要随意修改。
- IRF 迁移到 Recovery 状态后会关闭该 IRF 中所有成员设备上除保留端口以外的其它所有物理端口（通常为业务接口），保留端口可通过 **mad exclude interface** 命令配置。
- 如果接口因为多 Active 冲突被关闭，则只能等 IRF 恢复到正常工作状态后，接口才能自动被激活，不能通过 **undo shutdown** 命令来激活。
- 当使用 ARP MAD + MSTP 或 ND MAD + MSTP 组网时，需要将 IRF 配置为桥 MAC 地址立即改变，即配置 **undo irf mac-address persistent** 命令。
- 当 IRF 设备上存在跨成员设备的聚合链路时，请不要使用 **undo irf mac-address persistent** 命令配置 IRF 的桥 MAC 立即变化，否则可能会导致流量中断。
- 请确保 IRF 中各成员设备上安装的特性 License 一致，否则，可能会导致这些 License 对应的特性不能正常运行。

1.4 IRF配置任务简介

成员编号、成员优先级、IRF 端口配置方式不同，时效不同。建议用户使用以下步骤来建立 IRF：

(1) 进行网络规划，明确使用哪台设备作为主设备、各成员设备的编号以及成员设备之间的物理连接；

(2) 将当前配置保存到设备的下次启动配置文件，以便设备重启后，IRF 配置能够继续生效。

(3) 连接 IRF 物理接口，确保 IRF 链路处于 up 状态；

(4) 访问 IRF；

(5) 根据需要，在 IRF 模式下快速配置 IRF 或者使用多条命令逐个配置 IRF 参数，比如原 IRF 物理端口故障需要绑定其它 IRF 物理端口等。

表1-1 IRF 配置任务简介

配置任务		说明	详细配置
将当前配置保存到设备的下次启动配置文件		必选	1.5
访问IRF		必选	1.6
IRF模式下快速配置IRF		和“IRF模式下配置IRF”二者选其一	1.7
IRF模式下配置IRF	配置成员编号	必选	1.8.1
	配置成员优先级	可选	1.8.2
	配置IRF端口	必选	1.8.3
	配置成员设备的描述信息	可选	1.8.4
	配置IRF链路的负载分担类型	可选	1.8.5
	配置IRF的桥MAC保留时间	可选	1.8.6
	开启IRF系统启动文件的自动加载功能	可选	1.8.7
	MAD配置	可选	1.8.8

1.5 将当前配置保存到设备的下次启动配置文件

表1-2 将当前配置保存到设备的下次启动配置文件

操作	命令	说明
将当前配置保存到存储介质的根目录下，并将该文件设置为下次启动配置文件	**save** [**safely**] [**backup** | **main**] [**force**]	该命令可在任意视图下执行

1.6 访问IRF

IRF 的访问方式如下：

- 本地登录：通过任意成员设备的 Console 口登录。
- 远程登录：给任意成员设备的任意三层接口配置 IP 地址，并且路由可达，就可以通过 Telnet、WEB、SNMP 等方式进行远程登录。

不管使用哪种方式登录 IRF，实际上登录的都是主设备。主设备是 IRF 系统的配置和控制中心，在主设备上配置后，主设备会将相关配置同步给从设备，以便保证主设备和从设备配置的一致性。

1.7 IRF模式下快速配置IRF

使用该功能，用户可以通过一条命令配置 IRF 的基本参数，包括新成员编号、域编号、绑定物理端口，简化了配置步骤，达到快速配置 IRF 的效果。

在配置该功能时，有两种方式：

- 交互模式：用户输入 **easy-irf**，回车，在交互过程中输入具体参数的值。
- 非交互模式，在输入命令行时直接指定所需参数的值。

两种方式的配置效果相同，如果用户对本功能不熟悉，建议使用交互模式。

配置时，需要注意的是：

- 如果给成员设备指定新的成员编号，该成员设备会立即自动重启，以使新的成员编号生效。
- 多次使用该功能，修改域编号/优先级/IRF 物理端口时，域编号和优先级的新配置覆盖旧配置，IRF 物理端口的配置会新旧进行叠加。如需删除旧的 IRF 物理端口配置，需要在 IRF 端口视图下，执行 **undo port group interface** 命令。
- 不同型号的设备支持绑定的最大 IRF 物理端口数请参见命令手册。
- 在交互模式下，为 IRF 端口指定物理端口时，请注意：
  - 接口类型和接口编号间不能有空格。
  - 不同物理接口之间用英文逗号分隔。

表1-3 快速配置 IRF

操作	命令	说明
进入系统视图	**system-view**	-
快速配置IRF	**easy-irf** [**member** *member-id* [**renumber** *new-member-id*] **domain** *domain-id* [**priority** *priority*] [**irf-port1** *interface-list1*] [**irf-port2** *interface-list2*]]	若在多成员设备的IRF环境中使用该命令，请确保配置的新成员编号与当前IRF中的成员编号不冲突

1.8 IRF模式下配置IRF

1.8.1 配置成员编号

注意

在 IRF 中以成员编号标识设备，IRF 端口和成员优先级的配置也和成员编号紧密相关。所以，修改设备成员编号可能导致配置发生变化或者失效，请慎重使用。

配置成员编号时，请确保该编号在 IRF 中唯一。如果存在相同的成员编号，则不能建立 IRF。如果新设备加入 IRF，但是该设备与已有成员设备的编号冲突，则该设备不能加入 IRF。

- 修改成员编号后，但是没有重启本设备，则原编号继续生效，各物理资源仍然使用原编号来标识。
- 修改成员编号后，如果保存当前配置，重启本设备，则新的成员编号生效，需要用新编号来标识物理资源；配置文件中，只有 IRF 端口的编号以及 IRF 端口下的配置、成员优先级会继续生效，其它与成员编号相关的配置（比如普通物理接口的配置等）不再生效，需要重新配置。

表1-4 配置成员编号

操作	命令	说明
进入系统视图	**system-view**	-
配置成员编号	**irf member** *member-id* **renumber** *new-member-id*	缺省情况下，设备的成员编号均为1

1.8.2 配置成员优先级

在主设备选举过程中，优先级数值大的成员设备将优先被选举成为主设备。

表1-5 配置成员优先级

操作	命令	说明
进入系统视图	**system-view**	-
配置IRF中指定成员设备的优先级	**irf member** *member-id* **priority** *priority*	缺省情况下，设备的成员优先级均为1

1.8.3 配置IRF端口

表1-6 配置 IRF 端口

操作	命令	说明
进入系统视图	**system-view**	-
进入IRF物理端口视图	**interface** *interface-type interface-number*	-
关闭接口	**shutdown**	如果允许关闭当前端口，则直接在该接口视图下执行**shutdown**命令即可；如果不能关闭该端口，请根据系统提示信息关闭该端口直连的邻居设备上的端口
退回系统视图	**quit**	-
进入IRF端口视图	**irf-port** *member-id/irf-port-number*	-
将IRF端口和IRF物理端口绑定	**port group interface** *interface-type interface-number*	缺省情况下，IRF端口没有和任何IRF物理端口绑定 多次执行该命令，可以将IRF端口与多个IRF物理端口绑定，以实现IRF链路的备份或负载分担，从而提高IRF链路的带宽和可靠性。当绑定的物理端口数达到上限时，该命令将执行失败，不同型号的设备支持绑定的最大IRF物理端口数请参见命令手册

操作	命令	说明
退回到系统视图	**quit**	-
进入IRF物理端口视图	**interface** *interface-type interface-number*	-
激活接口	**undo shutdown**	-
退回系统视图	**quit**	-
保存当前配置	**save**	激活IRF端口会引起IRF合并，进而设备需要重启。为了避免重启后配置丢失，请在激活IRF端口前先将当前配置保存到下次启动配置文件
激活IRF端口下的配置	**irf-port-configuration active**	IRF物理线缆连接好，并将IRF物理端口添加到IRF端口后，必须通过该命令手工激活IRF端口的配置才能形成IRF

1.8.4 配置成员设备的描述信息

当网络中存在多个 IRF 或者同一 IRF 中存在多台成员设备且物理位置比较分散（比如在不同楼层甚至不同建筑）时，为了确认成员设备的物理位置，在组建 IRF 时可以将物理位置设置为成员设备的描述信息，以便后期维护。

表1-7 配置成员设备的描述信息

操作	命令	说明
进入系统视图	**system-view**	-
配置IRF中指定成员设备的描述信息	**irf member** *member-id* **description** *text*	缺省情况下，未配置成员设备的描述信息

1.8.5 配置IRF链路的负载分担类型

提示

在配置负载分担模式前，IRF 端口必须至少和一个 IRF 物理端口绑定。否则，负载分担模式将配置失败。

当 IRF 端口与多个 IRF 物理端口绑定时，成员设备之间就会存在多条 IRF 链路。通过改变 IRF 链路负载分担的类型，可以灵活地实现成员设备间流量的负载分担。用户既可以指定系统按照报文携带的 IP 地址、MAC 地址等信息之一或其组合来选择所采用的负载分担类型。

用户可以通过全局配置（系统视图下）和端口下（IRF 端口视图下）配置的方式设置 IRF 链路的负载分担模式：

- 在系统视图下的配置对所有 IRF 端口生效；
- 在 IRF 端口视图下的配置只对当前 IRF 端口下的 IRF 链路生效；
- IRF 端口会优先采用端口下的配置。如果端口下没有配置，则采用全局配置。

表1-8 全局配置 IRF 链路的负载分担类型

操作	命令	说明
进入系统视图	**system-view**	-
配置IRF链路的负载分担模式	**irf-port global load-sharing mode { destination-ip | destination-mac | source-ip | source-mac } ***	多次执行该命令配置不同负载分担模式时，以最新的配置为准

表1-9 端口下配置 IRF 链路的负载分担类型

操作	命令	说明
进入系统视图	**system-view**	-
进入IRF端口视图	**irf-port** *member-id/irf-port-number*	-
配置IRF链路的负载分担模式	**irf-port load-sharing mode { destination-ip | destination-mac | source-ip | source-mac } ***	多次执行该命令配置不同负载分担模式时，以最新的配置为准

1.8.6 配置IRF的桥MAC保留时间

注意

- 桥 MAC 变化可能导致流量短时间中断，请谨慎配置。
- 如果两台物理设备的桥 MAC 相同，则它们不能合并为一个 IRF。IRF 的桥 MAC 不受此限制，只要成员设备自身桥 MAC 唯一即可。
- 当使用 ARP MAD 和 MSTP 或 ND MAD 和 MSTP 组网时，需要将 IRF 配置为桥 MAC 地址立即改变，即配置 **undo irf mac-address persistent** 命令。
- 当 IRF 设备上存在跨成员设备的聚合链路时，请不要使用 **undo irf mac-address persistent** 命令配置 IRF 的桥 MAC 立即变化，否则可能会导致流量中断。

桥 MAC 是设备作为网桥与外界通信时使用的 MAC 地址。一些二层协议（例如 LACP）会使用桥 MAC 标识不同设备，所以网络上的桥设备必须具有唯一的桥 MAC。如果网络中存在桥 MAC 相同的设备，则会引起桥 MAC 冲突，从而导致通信故障。

IRF 作为一台虚拟设备与外界通信，也具有唯一的桥 MAC，称为 IRF 桥 MAC。IRF 会选用某台成员设备的桥 MAC 作为 IRF 的桥 MAC，这台成员设备被称为 IRF 桥 MAC 拥有者。通常情况下，IRF 使用主设备的桥 MAC 作为 IRF 桥 MAC。

因为桥 MAC 冲突会引起通信故障，桥 MAC 的切换又会导致流量中断。因此，用户需要根据网络实际情况配置 IRF 桥 MAC 的保留时间：

- 如果配置了 IRF 桥 MAC 保留时间为 6 分钟，则当 IRF 桥 MAC 拥有者离开 IRF 时，IRF 桥 MAC 在 6 分钟内保持不变化；如果 6 分钟后 IRF 桥 MAC 拥有者没有回到 IRF，则使用新选举的主设备的桥 MAC 作为 IRF 桥 MAC。该配置适用于 IRF 桥 MAC 拥有者短时间内离开又回到 IRF 的情况（比如设备重启或者链路临时故障等），可以减少不必要的桥 MAC 切换导致的流量中断。

- 如果配置了 IRF 桥 MAC 保留时间为永久，则无论 IRF 桥 MAC 拥有者是否离开 IRF，IRF 桥 MAC 始终保持不变。
- 如果配置了 IRF 桥 MAC 不保留，则当 IRF 桥 MAC 拥有者离开 IRF 时，系统会立即使用 IRF 中当前主设备的桥 MAC 做 IRF 桥 MAC。

表1-10 配置 IRF 的桥 MAC 保留时间

操作	命令	说明
进入系统视图	**system-view**	-
配置IRF的桥MAC会永久保留	**irf mac-address persistent always**	缺省情况下IRF桥MAC保留时间为6分钟
配置IRF的桥MAC的保留时间为6分钟	**irf mac-address persistent timer**	
配置IRF的桥MAC不保留，会立即变化	**undo irf mac-address persistent**	

1.8.7 开启启动文件的自动加载功能

注意

加载启动软件包需要一定时间，在加载期间，请不要手工重启处于加载状态的从设备，否则，会导致该从设备加载启动软件包失败而不能启动。用户可打开日志信息显示开关，并根据日志信息的内容来判断加载过程是否开始以及是否结束。

如果新设备加入 IRF，并且新设备的软件版本和主设备的软件版本不一致，则新加入的设备不能正常启动。此时：

- 如果没有开启启动文件的自动加载功能，则需要用户手工升级新设备后，再将新设备加入 IRF。或者在主设备上开启启动文件的自动加载功能，重启新设备，让新设备重新加入 IRF。
- 如果已经开启了启动文件的自动加载功能，则新设备加入 IRF 时，会与主设备的软件版本号进行比较，如果不一致，则自动从主设备下载启动文件，然后使用新的系统启动文件重启，重新加入 IRF。如果新下载的启动文件的文件名与设备上原有启动文件文件名重名，则原有启动文件会被覆盖。

为了能够自动加载成功，请确保从设备存储介质上有足够的空闲空间用于存放新的启动文件。如果从设备存储介质上空闲空间不足，系统会自动删除从设备的当前启动文件来完成加载。如果删除从设备的当前启动文件后空间仍然不足，从设备将无法进行自动加载。此时，需要管理员重启从设备并进入从设备的 Boot ROM 菜单，删除一些不重要的文件后，再让从设备重新加入 IRF。

表1-11 开启 IRF 系统启动文件的自动加载功能

操作	命令	说明
进入系统视图	**system-view**	-
开启IRF系统启动文件的自动加载功能	**irf auto-update enable**	缺省情况下，IRF系统启动文件的自动加载功能处于开启状态

1.8.8 MAD配置

设备支持的 MAD 检测方式有：LACP MAD 检测、BFD MAD 检测、ARP MAD 检测和 ND MAD 检测。四种 MAD 检测机制各有特点，用户可以根据现有组网情况进行选择。

LACP MAD 和 ARP MAD、ND MAD 冲突处理的原则不同，请不要同时配置。

BFD MAD 和 ARP MAD、ND MAD 冲突处理的原则不同，并且 BFD MAD 和生成树协议互斥，ARP MAD、ND MAD 需要开启生成树协议，因此 BFD MAD 和 ARP MAD、ND MAD 无法同时配置。

表1-12 MAD 检测机制的比较

MAD 检测方式	优势	限制
LACP MAD	检测速度快，利用现有聚合组网即可实现，无需占用额外接口，利用聚合链路同时传输普通业务报文和MAD检测报文（扩展LACP报文）	组网中需要使用H3C设备作为中间设备，每个成员设备都需要连接到中间设备
BFD MAD	检测速度较快，组网形式灵活，对其它设备没有要求	配置专用三层接口，这些接口不能再传输普通业务流量 • 如果不使用中间设备，则要求成员设备间是全链接，即每个成员设备都必须和其它所有成员设备相连。该链路专用于 MAD 检测，不能再传输普通业务流量。该方式适用于成员设备少，并且物理距离比较近的组网环境 • 如果使用中间设备，组网时每个成员设备都需要连接到中间设备，这些 BFD 链路专用于 MAD 检测
ARP MAD	非聚合的IPv4组网环境，和MSTP配合使用，无需占用额外端口。在使用中间设备的组网中对中间设备没有要求	检测速度慢于前两种
ND MAD	非聚合的IPv6组网环境，和MSTP配合使用，无需占用额外端口。在使用中间设备的组网中对中间设备没有要求	检测速度慢于前两种

1. LACP MAD检测

(1) LACP MAD 检测原理

LACP MAD 检测是通过扩展 LACP 协议报文内容实现的，即在 LACP 协议报文的扩展字段内定义一个新的 TLV（Type/Length/Value，类型/长度/值）数据域——用于交互 IRF 的 DomainID（域编号）和 ActiveID（等于主设备的成员编号）。

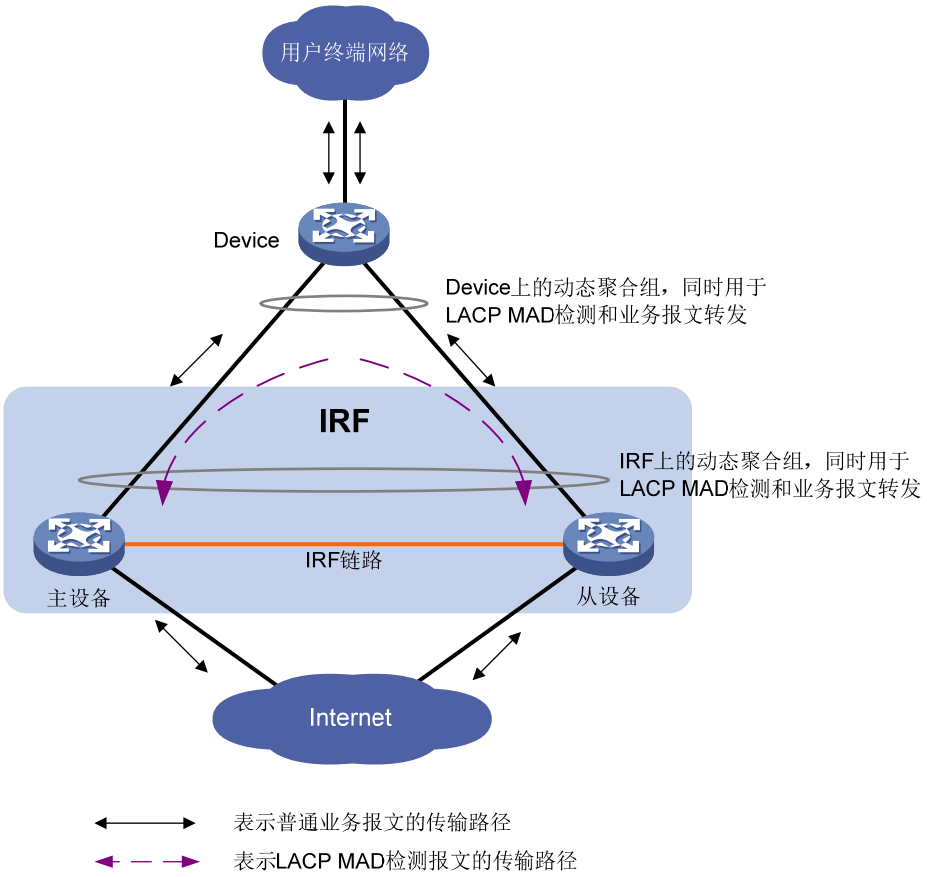
开启 LACP MAD 检测后，成员设备通过 LACP 协议报文和其它成员设备交互 DomainID 和 ActiveID 信息。

- 当成员设备收到 LACP 协议报文后，先比较 DomainID。如果 DomainID 相同，再比较 ActiveID；如果 DomainID 不同，则认为报文来自不同 IRF，不再进行 MAD 处理。
- 如果 ActiveID 相同，则表示 IRF 正常运行，没有发生多 Active 冲突；如果 ActiveID 值不同，则表示 IRF 分裂，检测到多 Active 冲突。

(2) LACP MAD 检测组网要求

LACP MAD检测方式组网中需要使用H3C设备作为中间设备。通常采用如 图 1-7 所示的组网：成员设备之间通过Device交互LACP扩展报文。

图1-7 LACP MAD 检测组网示意图



(3) 配置 LACP MAD 检测

LACP MAD 检测的配置步骤为：

- 配置 IRF 域编号；
- 创建聚合接口；（中间设备上也需要进行该项配置）
- 将聚合接口的工作模式配置为动态聚合模式；（中间设备上也需要进行该项配置）
- 在动态聚合接口下开启 LACP MAD 检测功能；
- 给聚合组添加成员端口。（中间设备上也需要进行该项配置）

表1-13 配置 LACP MAD 检测

操作		命令	说明
进入系统视图		**system-view**	-
配置IRF域编号		**irf domain** *domain-id*	缺省情况下，IRF的域编号为0
创建并进入聚合接口视图	进入二层聚合接口视图	**interface bridge-aggregation** *interface-number*	二者选其一
	进入三层聚合	**interface route-aggregation**	

操作	命令	说明
接口视图	*interface-number*	
配置聚合组工作在动态聚合模式下	**link-aggregation mode dynamic**	缺省情况下，聚合组工作在静态聚合模式下
开启LACP MAD检测功能	**mad enable**	缺省情况下，LACP MAD检测功能处于关闭状态
退回系统视图	**quit**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
将以太网接口加入聚合组	**port link-aggregation group** *group-id*	-

2. BFD MAD检测

说明

配置 BFD MAD 检测时，需要将 BFD MAD 检测功能的三层接口加入安全域，并配置该安全域与系统缺省 Local 安全域之间的安全策略。

(1) BFD MAD 检测原理

BFD MAD 检测是通过 BFD 协议来实现的。要使 BFD MAD 检测功能正常运行，除在三层接口下开启 BFD MAD 检测功能外，还需要在该接口上配置 MAD IP 地址。MAD IP 地址与普通 IP 地址不同的地方在于：MAD IP 地址与成员设备是绑定的，IRF 中的每个成员设备上都需要配置，且所有成员设备的 MAD IP 必须属于同一网段。

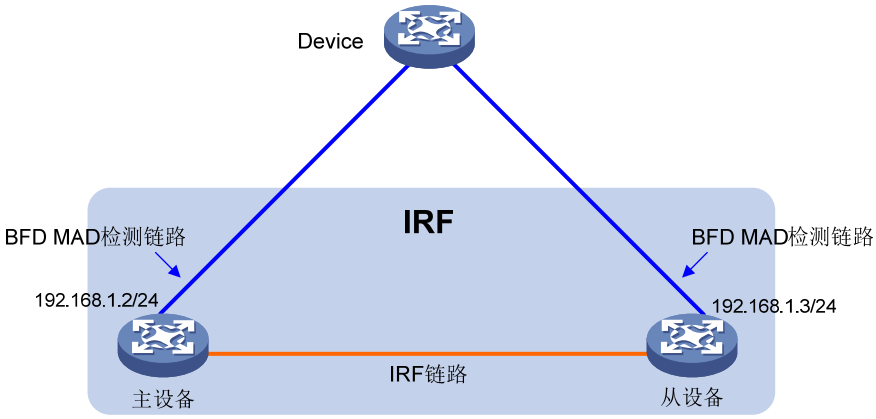
- 当 IRF 正常运行时，只有主设备上配置的 MAD IP 地址生效，从设备上配置的 MAD IP 地址不生效，BFD 会话处于 down 状态；（使用 **display bfd session** 命令查看 BFD 会话的状态。如果 Session State 显示为 Up，则表示激活状态；如果显示为 Down，则表示处于 down 状态）
- 当 IRF 分裂形成多个 IRF 时，不同 IRF 中主设备上配置的 MAD IP 地址均会生效，BFD 会话被激活，此时会检测到多 Active 冲突。

(2) BFD MAD 检测组网要求

BFD MAD检测方式可以使用中间设备来进行连接，也可以不使用中间设备。在使用中间设备时，典型组网如 图 1-8 所示。用于BFD MAD检测的以太网端口需要属于同一三层聚合接口或VLAN，在该三层聚合接口视图下或VLAN接口视图下为不同成员设备配置同一网段内的不同MAD IP地址。

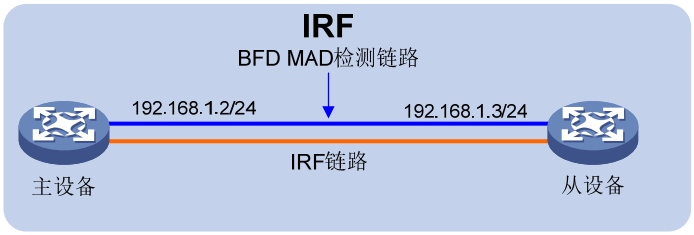
使用中间设备实现 BFD MAD 检测组网示意图：

图1-8 使用中间设备实现 BFD MAD 检测组网示意图



在没有中间设备时，需要采用如 图 1-9 所示的组网方式：每台成员设备必须和其它所有成员设备之间使用以太网端口建立BFD MAD检测链路（即成员设备之间是全连接组网）。这些链路连接的接口必须属于同一VLAN或三层聚合接口，在该VLAN接口或三层聚合接口视图下给不同成员设备配置同一网段下的不同IP地址。

图1-9 不使用中间设备实现 BFD MAD 检测组网示意图



提示

开启 BFD MAD 检测功能的三层接口只能专用于 BFD MAD 检测，这些接口下建议只配置 **mad bfd enable** 和 **mad ip address** 命令。如果用户配置了其它命令，可能会影响该业务以及 BFD MAD 检测功能的运行。

(3) 配置 BFD MAD 检测

配置 BFD MAD 检测时，请遵循以下要求：

- 如果网络中存在多个 IRF，在配置 BFD MAD 时，各 IRF 必须使用不同的 VLAN 或三层聚合接口作为 BFD MAD 检测专用 VLAN 或三层聚合接口。
- 开启 BFD MAD 检测功能的 VLAN 接口或三层聚合接口以及成员接口上不支持包括 ARP 的所有的二层或三层协议应用。
- 不允许在 Vlan-interface1 接口上开启 BFD MAD 检测功能。
- BFD MAD 检测功能与生成树功能互斥，在开启了 BFD MAD 检测功能 VLAN 接口绑定的二层以太网接口上，请关闭生成树协议。

- 在用于 BFD MAD 检测的接口下必须使用 **mad ip address** 命令配置 MAD IP 地址，而不要配置其它 IP 地址（包括使用 **ip address** 命令配置的普通 IP 地址、VRRP 虚拟 IP 地址等），以免影响 MAD 检测功能。

使用以太网端口进行 BFD MAD 检测功能的配置顺序为：

- 创建一个新 VLAN 或三层聚合口，专用于 BFD MAD 检测；（对于使用中间设备的组网，中间设备上也需要进行该项配置）
- 确定哪些物理端口用于 BFD MAD 检测，并将这些端口都添加到 BFD MAD 检测专用 VLAN 或三层聚合口中；（如果用到中间设备组网，中间设备上也需要进行该项配置）
- 为 BFD MAD 检测专用 VLAN 创建 VLAN 接口或创建三层聚合接口专用于 BFD MAD 检测，在接口下开启 BFD MAD 检测功能，并配置 MAD IP 地址。

表1-14 配置使用 VLAN 口进行 BFD MAD 检测

操作		命令	说明
进入系统视图		**system-view**	-
（可选）配置IRF域编号		**irf domain** *domain-id*	缺省情况下，IRF的域编号为0
创建一个新VLAN专用于BFD MAD检测		**vlan** *vlan-id*	缺省情况下，只存在VLAN 1 VLAN 1不能用于BFD MAD检测
退回系统视图		**quit**	-
进入以太网接口视图		**interface** *interface-type interface-number*	-
将端口加入BFD MAD检测专用VLAN	Access端口	**port access vlan** *vlan-id*	请根据端口的当前链路类型选择对应的配置命令 BFD MAD检测对检测端口的链路类型没有要求，不需要刻意修改端口的当前链路类型。缺省情况下，端口端的链路类型为Access端口
	Trunk端口	**port trunk permit vlan** *vlan-id*	
	Hybrid端口	**port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	
退回系统视图		**quit**	-
进入VLAN接口视图		**interface vlan-interface** *interface-number*	-
开启BFD MAD检测功能		**mad bfd enable**	缺省情况下，BFD MAD检测功能处于关闭状态
给指定成员设备配置MAD IP地址		**mad ip address** *ip-address* { *mask* | *mask-length* } **member** *member-id*	缺省情况下，未配置成员设备的MAD IP地址

表1-15 配置三层聚合接口 BFD MAD 检测

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置IRF域编号	**irf domain** *domain-id*	缺省情况下，IRF的域编号为0
创建一个三层聚合接口专用于BFD MAD检测	**interface route-aggregation** *interface-number*	-

操作	命令	说明
退回系统视图	**quit**	-
进入以太网接口视图	**interface** *interface-type interface-number*	-
将端口加入BFD MAD检测专用聚合组	**port link-aggregation group** *group-number*	-
退回系统视图	**quit**	-
进入三层聚合接口视图	**interface route-aggregation** *interface-number*	-
开启BFD MAD检测功能	**mad bfd enable**	缺省情况下，BFD MAD检测功能处于关闭状态
给指定成员设备配置MAD IP地址	**mad ip address** *ip-address* { *mask* | *mask-length* } **member** *member-id*	缺省情况下，未配置成员设备的MAD IP地址

3. ARP MAD检测

(1) ARP MAD 检测原理

ARP MAD 检测是通过扩展 ARP 协议报文内容实现的，即使用 ARP 协议报文中未使用的字段来交互 IRF 的 DomainID 和 ActiveID。

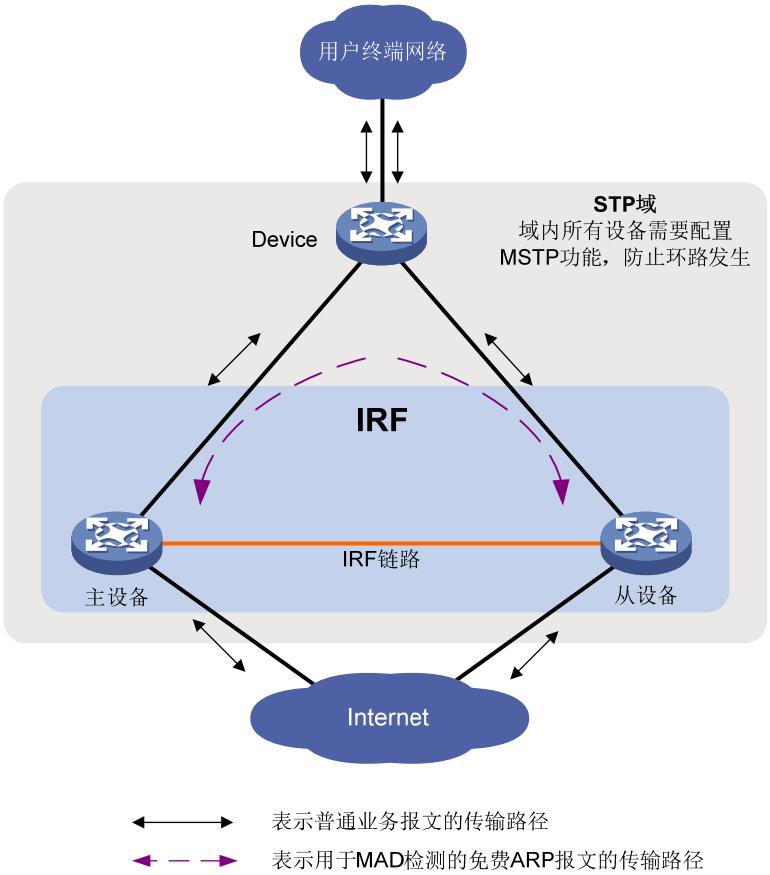
开启 ARP MAD 检测后，成员设备可以通过 ARP 协议报文和其它成员设备交互 DomainID 和 ActiveID 信息。

- 当成员设备收到ARP协议报文后，先比较DomainID。如果DomainID相同，再比较ActiveID；如果 DomainID 不同，则认为报文来自不同 IRF，不再进行 MAD 处理。
- 如果 ActiveID 相同，则表示 IRF 正常运行，没有发生多 Active 冲突；如果 ActiveID 值不同，则表示 IRF 分裂，检测到多 Active 冲突。

(2) ARP MAD 检测组网要求

ARP MAD检测方式可以使用中间设备来进行连接，也可以不使用中间设备。通常采用如 图 1-10 所示的组网：成员设备之间通过Device交互ARP报文，Device、主设备和从设备上都要配置生成树功能，以防止形成环路。

图1-10 ARP MAD 检测组网示意图



(3) 配置 ARP MAD 检测

配置 ARP MAD 检测时，请遵循以下要求：

- 当 ARP MAD 检测组网使用中间设备进行连接时，可使用普通的数据链路作为 ARP MAD 检测链路；当不使用中间设备时，需要在所有的成员设备之间建立两两互联的 ARP MAD 检测链路。
- 如果使用中间设备组网，在 IRF 和中间设备上均需配置生成树功能。并确保配置生成树功能后，只有一条 ARP MAD 检测链路处于转发状态，能够转发 ARP MAD 检测报文。

ARP MAD 检测功能的配置顺序为：

- 创建一个新 VLAN，专用于 ARP MAD 检测；（对于使用中间设备的组网，中间设备上也需要进行该项配置）
- 确定哪些物理端口用于 ARP MAD 检测，并将这些端口都添加到 ARP MAD 检测专用 VLAN 中；（如果用到中间设备组网，中间设备上也需要进行该项配置）
- 为 ARP MAD 检测专用 VLAN 创建 VLAN 接口，在接口下开启 ARP MAD 检测功能，并配置 IP 地址。

表1-16 配置 ARP MAD 检测

操作	命令	说明
进入系统视图	**system-view**	-

操作		命令	说明
配置IRF域编号		**irf domain** *domain-id*	缺省情况下，IRF的域编号为0
将IRF配置为MAC地址立即改变		**undo irf mac-address persistent**	缺省情况下，IRF的桥MAC会保留6分钟
创建一个新VLAN专用于ARP MAD检测		**vlan** *vlan-id*	缺省情况下，只存在VLAN 1 VLAN 1不能用于ARP MAD检测
退回系统视图		**quit**	-
进入以太网接口视图		**interface** *interface-type interface-number*	-
端口加入ARP MAD检测专用VLAN	Access端口	**port access vlan** *vlan-id*	请根据端口的当前链路类型选择对应的配置命令 ARP MAD检测对检测端口的链路类型没有要求，不需要刻意修改端口的当前链路类型。缺省情况下，端口端的链路类型为Access端口
	Trunk端口	**port trunk permit vlan** *vlan-id*	
	Hybrid端口	**port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	
退回系统视图		**quit**	-
进入VLAN接口视图		**interface vlan-interface** *interface-number*	-
配置IP地址		**ip address** *ip-address* { *mask* | *mask-length* }	缺省情况下，未配置VLAN接口的IP地址
开启ARP MAD检测功能		**mad arp enable**	缺省情况下，ARP MAD检测功能处于关闭状态

4. ND MAD检测

(1) ND MAD 检测原理

ND MAD 检测是通过扩展 ND 协议报文内容实现的，即使用 ND 的 NS 协议报文携带扩展选项数据来交互 IRF 的 DomainID 和 ActiveID。

开启 ND MAD 检测后，成员设备可以通过 ND 协议报文和其它成员设备交互 DomainID 和 ActiveID 信息。

- 当成员设备收到 ND 协议报文后，先比较 DomainID。如果 DomainID 相同，再比较 ActiveID；如果 DomainID 不同，则认为报文来自不同 IRF，不再进行 MAD 处理。
- 如果 ActiveID 相同，则表示 IRF 正常运行，没有发生多 Active 冲突；如果 ActiveID 值不同，则表示 IRF 分裂，检测到多 Active 冲突。

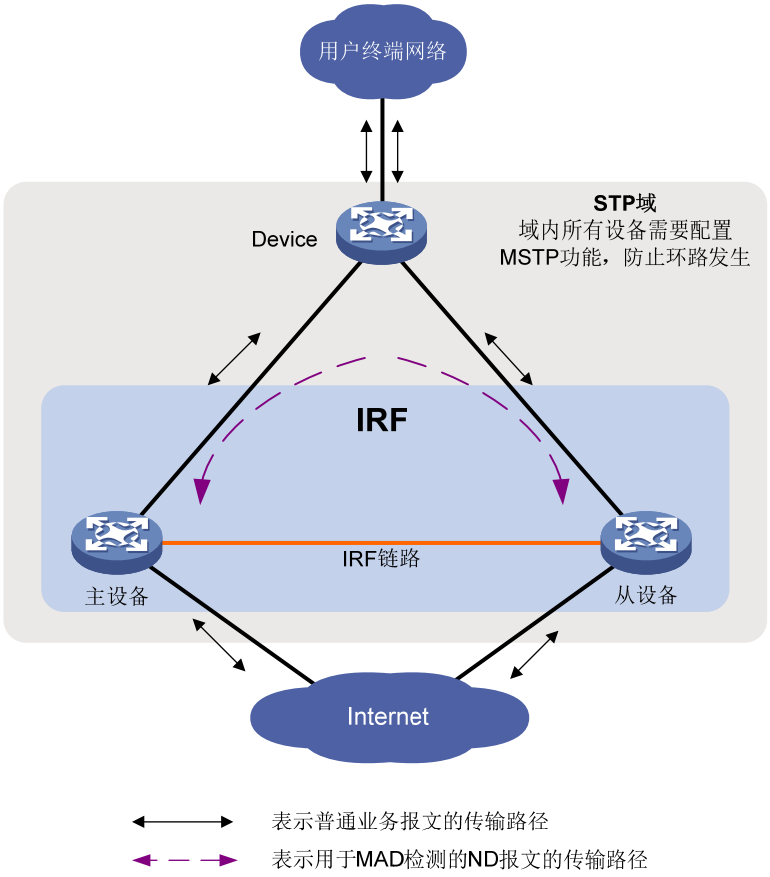
(2) ND MAD 检测组网要求

注意

在 ND MAD 检测组网中，如果中间设备本身也是一个 IRF 系统，则必须通过配置确保其 IRF 域编号与被检测的 IRF 系统不同，否则可能造成检测异常，甚至导致业务中断。

ND MAD检测方式可以使用中间设备来进行连接，也可以不使用中间设备。通常采用如 图 1-11 所示的组网：成员设备之间通过Device交互ND报文，Device、主设备和从设备上都要配置生成树功能，以防止形成环路。

图1-11 ND MAD 检测组网示意图



(3) 配置 ND MAD 检测

配置 ND MAD 检测时，请遵循以下要求：

- 当 ND MAD 检测组网使用中间设备进行连接时，可使用普通的数据链路作为 ND MAD 检测链路；当不使用中间设备时，需要在所有的成员设备之间建立两两互联的 ND MAD 检测链路。
- 如果使用中间设备组网，在 IRF 和中间设备上均需配置生成树功能。并确保配置生成树功能后，只有一条 ND MAD 检测链路处于转发状态，能够转发 ND MAD 检测报文。

ND MAD 检测功能的配置顺序为：

- 创建一个新 VLAN，专用于 ND MAD 检测；（对于使用中间设备的组网，中间设备上也需要进行该项配置）
- 确定哪些物理端口用于 ND MAD 检测，并将这些端口都添加到 ND MAD 检测专用 VLAN 中；（如果用到中间设备组网，中间设备上也需要进行该项配置）
- 为 ND MAD 检测专用 VLAN 创建 VLAN 接口，在接口下开启 ND MAD 检测功能，并配置 IP 地址。

表1-17 配置 ND MAD 检测

操作		命令	说明
进入系统视图		**system-view**	-
配置IRF域编号		**irf domain** *domain-id*	缺省情况下，IRF的域编号为0
将IRF配置为MAC地址立即改变		**undo irf mac-address persistent**	缺省情况下，IRF的桥MAC会保留6分钟
创建一个新VLAN专用于ND MAD检测		**vlan** *vlan-id*	缺省情况下，只存在VLAN 1 VLAN 1不能用于ND MAD检测
退回系统视图		**quit**	-
进入以太网接口视图		**interface** *interface-type interface-number*	-
端口加入ND MAD检测专用VLAN	Access端口	**port access vlan** *vlan-id*	请根据端口的当前链路类型选择对应的配置命令 ND MAD检测对检测端口的链路类型没有要求，不需要刻意修改端口的当前链路类型。缺省情况下，端口端的链路类型为Access端口
	Trunk端口	**port trunk permit vlan** *vlan-id*	
	Hybrid端口	**port hybrid vlan** *vlan-id* { **tagged** | **untagged** }	
退回系统视图		**quit**	-
进入VLAN接口视图		**interface vlan-interface** *interface-number*	-
配置IP地址		**ipv6 address** { *ipv6-address/prefix-length* | *ipv6-address prefix-length* }	缺省情况下，未配置VLAN接口的IPv6地址
开启ND MAD检测功能		**mad nd enable**	缺省情况下，ND MAD检测功能处于关闭状态

5. 配置保留接口

IRF 系统在进行多 Active 处理的时候，缺省情况下，会关闭 Recovery 状态设备上的所有业务接口。如果接口有特殊用途需要保持 up 状态（比如 Telnet 登录接口等），则用户可以通过命令行将这些接口配置为保留接口。

需要注意的是：

- 使用 VLAN 接口进行远程登录时，需要将该 VLAN 接口及其对应的以太网端口都配置为保留接口。但如果在正常工作状态的 IRF 中该 VLAN 接口也处于 UP 状态，则在网络中会产生 IP 地址冲突。
- 请勿将用于 MAD 检测的聚合接口及其成员接口、VLAN 接口及其对应的以太网端口、管理用以太网口配置为保留接口。

表1-18 配置保留接口

操作	命令	说明
进入系统视图	**system-view**	-
配置保留接口，当设备进入	**mad exclude interface**	缺省情况下，设备进入Recovery状态时会自动关

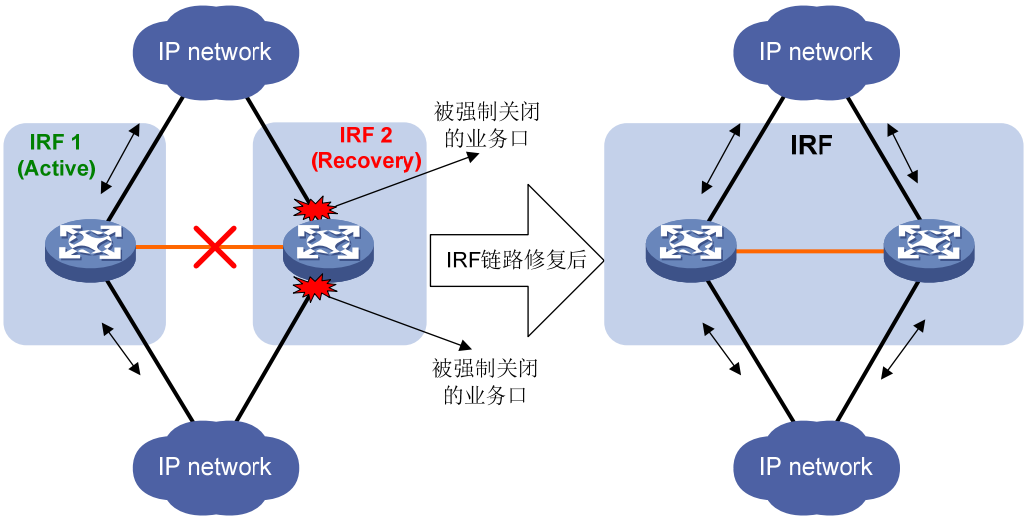
操作	命令	说明
Recovery状态时，该接口不会被关闭	*interface-type interface-number*	闭本设备上所有的业务接口 IRF物理端口自动作为保留接口，不需要配置

6. MAD故障恢复

IRF 链路故障将一个 IRF 分裂为两个 IRF，从而导致多 Active 冲突。当系统检测到多 Active 冲突后，两个冲突的 IRF 会进行竞选，主设备成员编号小的获胜，继续正常运行，失败的 IRF 会转入 Recovery 状态，暂时不能转发业务报文。此时通过修复 IRF 链路可以恢复 IRF 系统（设备会尝试自动修复 IRF 链路，如果修复失败的话，则需要用户手工修复）。

IRF链路修复后，处于正常工作状态的IRF和处于Recovery状态的IRF会自动合并为一个IRF：原Recovery状态IRF中所有成员设备以从设备身份加入原正常工作状态的IRF，原Recovery状态IRF中被强制关闭的业务接口自动恢复到真实的物理状态，整个IRF系统恢复，如 图 1-12 所示。

图1-12 MAD 故障恢复（IRF 链路故障）



如果MAD故障还没来得及修复而处于正常工作状态的IRF也故障了（原因可能是设备故障或者上下行线路故障），如 图 1-13 所示。此时可以在IRF 2（处于Recovery状态的IRF）上执行**mad restore**命令，让IRF 2 恢复到正常状态，先接替IRF 1 工作。然后再修复IRF 1 和IRF链路，修复后，两个IRF发生合并，整个IRF系统恢复。

图1-13 MAD 故障恢复（IRF 链路故障+正常工作状态的 IRF 故障）

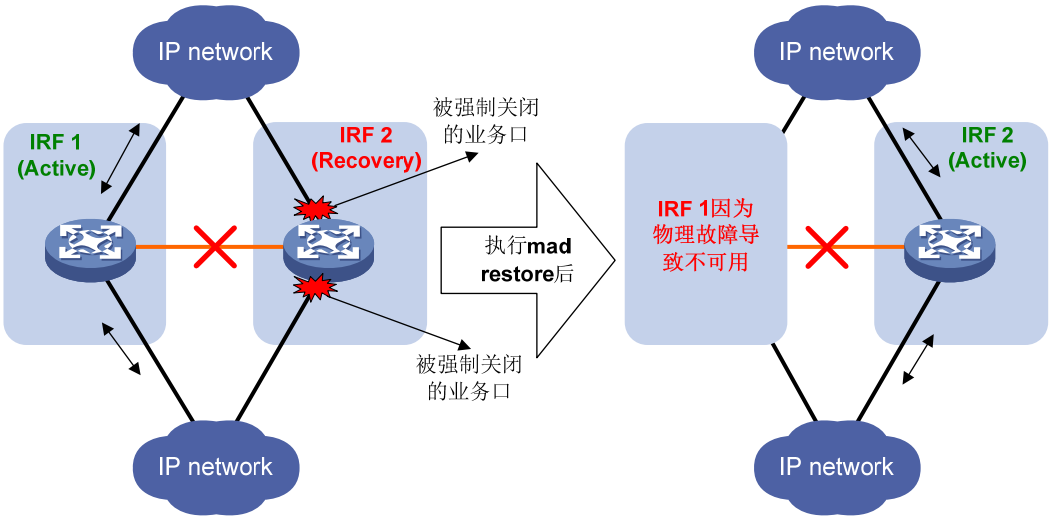


表1-19 手动恢复处于 Recovery 状态的设备

操作	命令	说明
进入系统视图	**system-view**	-
将IRF从Recovery状态恢复到正常工作状态	**mad restore**	-

1.9 IRF显示和维护

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

表1-20 IRF 显示和维护

操作	命令
显示IRF中所有成员设备的相关信息	**display irf**
查看IRF的拓扑信息	**display irf topology**
显示IRF链路信息	**display irf link**
显示IRF配置信息	**display irf configuration**
显示IRF链路的负载分担模式	**display irf-port load-sharing mode** [**irf-port** [*member-id*/*irf-port-number*]]
显示MAD配置信息	**display mad** [**verbose**]

1.10 IRF典型配置举例

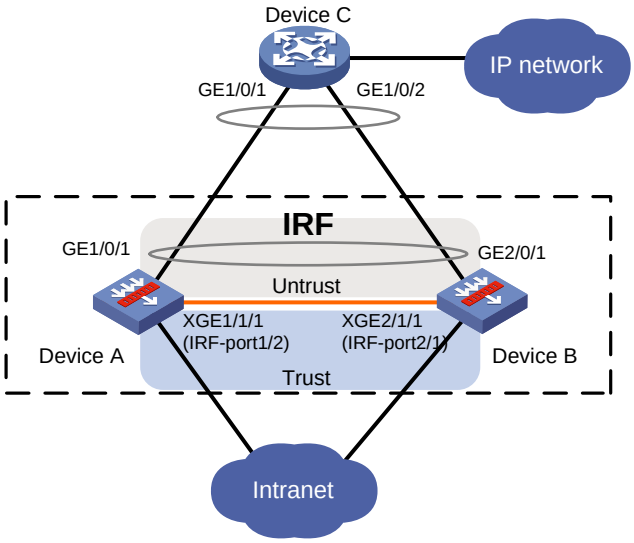
1.10.1 IRF典型配置举例（LACP MAD检测方式）

1. 组网需求

由于公司业务量激增，网络规模迅速扩大，当前中心设备（Device A）转发能力已经不能满足需求。现需要在保护现有投资的基础上将网络转发能力提高一倍，并要求网络易管理、易维护。

2. 组网图

图1-14 IRF 典型配置组网图（LACP MAD 检测方式）



3. 配置思路

- Device A 提供的安全业务处理能力已经不能满足网络需求，需要另外增加一台设备 Device B。
- 鉴于 IRF 技术具有管理简便、网络扩展能力强、可靠性高等优点，所以本例使用 IRF 技术构建接入层（即在 Device A 和 Device B 上配置 IRF 功能）。
- 为了防止 IRF 链路故障导致 IRF 分裂，网络中存在两个配置冲突的 IRF，需要启用 MAD 检测功能。因为网络中有一台中间设备 Device C，支持 LACP 协议，所以我们采用 LACP MAD 检测。

4. 配置步骤

(1) 配置 Device A

配置接口 IP 地址、路由、安全域及域间安全策略保证网络可达，具体配置步骤略。

设备成员编号 1 的设备的优先级为 32。

```
<DeviceA> system-view
[DeviceA] irf member 1 priority 32
```

配置 IRF 端口 1/2，并将它与物理端口 Ten-GigabitEthernet1/1/2 绑定，并保存配置。

```
[DeviceA] interface ten-gigabitethernet 1/1/2
[DeviceA-Ten-GigabitEthernet1/1/2] shutdown
[DeviceA-Ten-GigabitEthernet1/1/2] quit
[DeviceA] irf-port 1/2
```

```
[DeviceA-irf-port1/2] port group interface ten-gigabitethernet 1/1/2
[DeviceA-irf-port1/2] quit
[DeviceA] interface ten-gigabitethernet 1/1/2
[DeviceA-Ten-GigabitEthernet1/1/2] undo shutdown
[DeviceA-Ten-GigabitEthernet1/1/2] quit
[DeviceA] save
```

激活 IRF 端口下的配置。

```
[DeviceA] irf-port-configuration active
```

(2) 配置 Device B

配置接口 IP 地址、路由、安全域及域间安全策略保证网络可达，具体配置步骤略。

将 Device B 的成员编号配置为 2，并重启设备使新编号生效。

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[DeviceB] quit
<DeviceB> reboot
```

参照 图 1-14 进行物理连线。

重新登录到设备，配置 IRF 端口 2/1，并将它与物理端口 Ten-GigabitEthernet2/1/1 绑定，并保存配置。

```
<DeviceB> system-view
[DeviceB] interface ten-gigabitethernet 2/1/1
[DeviceB-Ten-GigabitEthernet2/1/1] shutdown
[DeviceB-Ten-GigabitEthernet2/1/1] quit
[DeviceB] irf-port 2/1
[DeviceB-irf-port2/1] port group interface ten-gigabitethernet 2/1/1
[DeviceB-irf-port2/1] quit
[DeviceB] interface ten-gigabitethernet 2/1/1
[DeviceB-Ten-GigabitEthernet2/1/1] undo shutdown
[DeviceB-Ten-GigabitEthernet2/1/1] quit
[DeviceB] save
```

激活 IRF 端口下的配置。

```
[DeviceB] irf-port-configuration active
```

(3) Device A 和 Device B 间将会进行主设备竞选，竞选失败的一方将重启（Device B），重启完成后，IRF 形成。

(4) 配置 LACP MAD 检测

设置 IRF 域编号为 1。

```
[DeviceA] irf domain 1
```

创建一个动态聚合接口，并开启 LACP MAD 检测功能。

```
[DeviceA] interface route-aggregation 2
[DeviceA-Route-Aggregation2] link-aggregation mode dynamic
[DeviceA-Route-Aggregation2] mad enable
 You need to assign a domain ID (range: 0-4294967295)
 [Current domain is: 1]:
 The assigned  domain ID is: 1
```

```
MAD LACP only enable on dynamic aggregation interface.
[DeviceA-Route-Aggregation2] quit
```

在聚合接口中添加成员端口 GigabitEthernet1/0/2 和 GigabitEthernet2/0/1，用于 Device A 和 Device B 实现 LACP MAD 检测。

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] port link-aggregation group 2
[DeviceA-GigabitEthernet1/0/2] quit
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] port link-aggregation group 2
[DeviceA-GigabitEthernet2/0/1] quit
```

(5) 配置中间设备 Device C

提示

如果中间设备是一个 IRF 系统，则必须通过配置确保其 IRF 域编号与被检测的 IRF 系统不同。

Device C 作为中间设备来转发、处理 LACP 协议报文，协助 Device A 和 Device B 进行多 Active 检测。从节约成本的角度考虑，使用一台支持 LACP 协议扩展功能的设备即可。

配置接口 IP 地址、路由保证网络可达，具体配置步骤略。

创建一个动态聚合接口。

```
<DeviceC> system-view
[DeviceC] interface route-aggregation 2
[DeviceC-Route-Aggregation2] link-aggregation mode dynamic
[DeviceC-Route-Aggregation2] quit
```

在聚合接口中添加成员端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2，用于帮助 LACP MAD 检测。

```
[DeviceC] interface gigabitethernet 1/0/1
[DeviceC-GigabitEthernet1/0/1] port link-aggregation group 2
[DeviceC-GigabitEthernet1/0/1] quit
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] port link-aggregation group 2
[DeviceC-GigabitEthernet1/0/2] quit
```

5. 验证配置

(1) IRF 链路正常情况下查看相关配置

查看 IRF 相关信息，可见 IRF 成功建立，且 DeviceA 为主设备。

```
[DeviceA] display irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  32        487a-da95-93b5  ---
   2        Standby 1         3897-d6a8-1b1a  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 487a-da95-93b3
 Auto upgrade               : yes
```

```
 Mac persistent              : 6 min
 Domain ID                   : 1
```

查看 LACP MAD 状态，状态正常。

```
[DeviceA] display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  Ten-Gigabitethernet1/1/2
  Ten-GigabitEthernet2/1/1
MAD ARP disabled.
MAD ND disabled.
MAD LACP enabled interface: Route-Aggregation2
  MAD status              : Normal
  Member ID   Port                                MAD status
  1           GigabitEthernet1/0/2                Normal
  2           GigabitEthernet2/0/1                Normal
MAD BFD disabled.
```

(2) IRF 链路异常情况下查看相关配置

查看 LACP MAD 状态，状态异常，表示 IRF 分裂。

```
[DeviceA] display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  Ten-GigabitEthernet1/1/2
MAD ARP disabled.
MAD ND disabled.
MAD LACP enabled interface: Route-Aggregation2
  MAD status              : Faulty
  Member ID   Port                                MAD status
  1           GigabitEthernet1/0/2                Faulty
MAD BFD disabled.
```

查看 Device B 上的非保留端口全部被置为 Down，显示信息略。

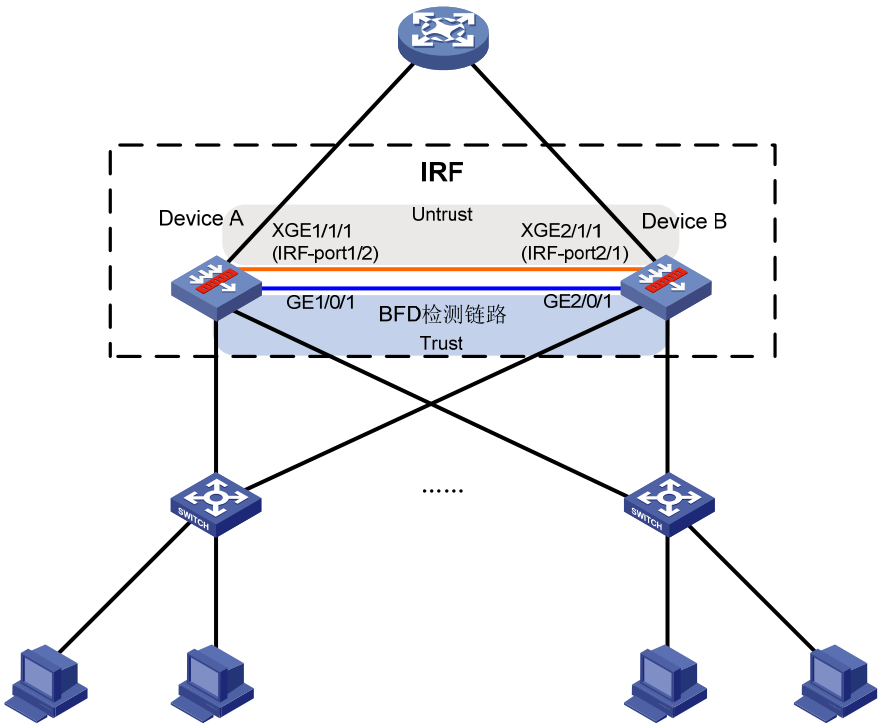
1.10.2 IRF典型配置举例（BFD MAD检测方式）

1. 组网需求

由于网络规模迅速扩大，当前中心设备（Device A）转发能力已经不能满足需求，现需要在保护现有投资的基础上将网络转发能力提高一倍，并要求网络易管理、易维护。

2. 组网图

图1-15 IRF 典型配置组网图（BFD MAD 检测方式）



3. 配置思路

- Device A 处于局域网的汇聚层，为了将汇聚层的安全业务处理能力提高一倍，需要另外增加一台设备 Device B。
- 鉴于 IRF 技术具有管理简便、网络扩展能力强、可靠性高等优点，所以本例使用 IRF 技术构建网络汇聚层（即在 Device A 和 Device B 上配置 IRF 功能），接入层设备通过聚合双链路上行。
- 为了防止 IRF 链路故障导致 IRF 分裂，网络中存在两个配置冲突的 IRF，需要启用 MAD 检测功能。因为成员设备比较少，我们采用 BFD MAD 检测方式来监测 IRF 的状态。

4. 配置步骤

(1) 配置 Device A

配置接口 IP 地址、路由、安全域及域间安全策略保证网络可达，具体配置步骤略。

```
<DeviceA> system-view
```

设备成员编号 1 的设备的优先级为 32。

```
[DeviceA] irf member 1 priority 32
```

配置 IRF 端口 1/2，并将它与物理端口 Ten-GigabitEthernet1/1/2 绑定，并保存配置。

```
[DeviceA] interface ten-gigabitethernet 1/1/2
[DeviceA-Ten-GigabitEthernet1/1/2] shutdown
[DeviceA-Ten-GigabitEthernet1/1/2] quit
[DeviceA] irf-port 1/2
[DeviceA-irf-port1/2] port group interface ten-gigabitethernet 1/1/2
```

```
[DeviceA-irf-port1/2] quit
[DeviceA] interface ten-gigabitethernet 1/1/2
[DeviceA-Ten-GigabitEthernet1/1/2] undo shutdown
[DeviceA-Ten-GigabitEthernet1/1/2] quit
[DeviceA] save
```

激活 IRF 端口下的配置。

```
[DeviceA] irf-port-configuration active
```

(2) 配置 Device B

配置接口 IP 地址、路由、安全域及域间安全策略保证网络可达，具体配置步骤略。

将 Device B 的成员编号配置为 2，并重启设备使新编号生效。

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[DeviceB] quit
<DeviceB> reboot
```

参照 图 1-15 进行物理连线。

重新登录到设备，配置 IRF 端口 2/1，并将它与物理端口 Ten-GigabitEthernet2/1/1 绑定，并保存配置。

```
<DeviceB> system-view
[DeviceB] interface ten-gigabitethernet 2/1/1
[DeviceB-Ten-GigabitEthernet2/1/1] shutdown
[DeviceB-Ten-GigabitEthernet2/1/1] quit
[DeviceB] irf-port 2/1
[DeviceB-irf-port2/1] port group interface ten-gigabitethernet 2/1/1
[DeviceB-irf-port2/1] quit
[DeviceB] interface ten-gigabitethernet 2/1/1
[DeviceB-Ten-GigabitEthernet2/1/1] undo shutdown
[DeviceB-Ten-GigabitEthernet2/1/1] quit
[DeviceB] save
```

激活 IRF 端口下的配置。

```
[DeviceB] irf-port-configuration active
```

(3) Device A 和 Device B 间将会进行主设备竞选，竞选失败的一方将重启（Device B），重启完成后，IRF 形成。

(4) 配置 BFD MAD 检测

创建三层聚合接口 3。

```
[DeviceA] interface route-aggregation 3
[DeviceA-Route-Aggregation3] quit
```

分别将 Device A(成员编号为 1)上的接口 GE1/0/1 和 Device B(成员编号为 2)上的接口 GE2/0/1 加入聚合组 3 中。

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-aggregation group 3
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface gigabitethernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] port link-aggregation group 3
```

```
[DeviceA-GigabitEthernet2/0/1] quit
```

配置三层聚合接口 3 的 MAD IP 地址。

```
[DeviceA] interface route-aggregation 3
[DeviceA-Route-Aggregation3] mad bfd enable
[DeviceA-Route-Aggregation3] mad ip address 192.168.2.1 24 member 1
[DeviceA-Route-Aggregation3] mad ip address 192.168.2.2 24 member 2
[DeviceA-Route-Aggregation3] quit
```

5. 验证配置

(1) IRF 链路正常情况下查看相关配置

查看 IRF 相关信息，可见 IRF 成功建立，且 DeviceA 为主设备。

```
[DeviceA] display irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  32        487a-da95-93b5  ---
   2        Standby 1         3897-d6a8-1b1a  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 487a-da95-93b3
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 0
```

查看 BFD MAD 状态，状态正常。

```
[DeviceA] display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  Ten-GigabitEthernet1/1/2
  Ten-GigabitEthernet2/1/1
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
MAD BFD enabled interface: Route-Aggregation3
  MAD status                : Normal
  Member ID   MAD IP address       Neighbor   MAD status
  1           192.168.1.1/24       2          Normal
  2           192.168.1.2/24       1          Normal
```

(2) IRF 链路异常情况下查看相关配置

查看 BFD MAD 状态，状态异常，表示 IRF 分裂。

```
[DeviceA] display mad verbose
Excluded ports (user-configured):
Excluded ports (system-configured):
  Ten-GigabitEthernet1/1/2
MAD ARP disabled.
MAD ND disabled.
MAD LACP disabled.
```

```
MAD BFD enabled interface: Route-Aggregation3
  MAD status                  : Faulty
  Member ID   MAD IP address       Neighbor   MAD status
  1           192.168.1.1/24       2          Faulty
```

查看 Device B 上的非保留端口全部被置为 Down，显示信息略。

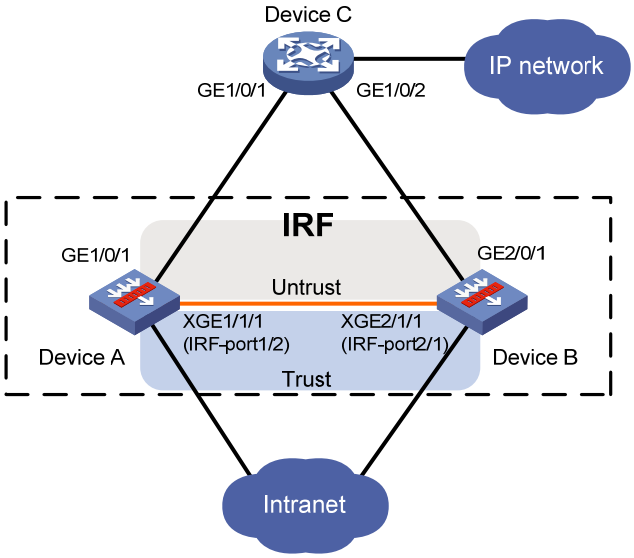
1.10.3 IRF典型配置举例（ARP MAD检测方式）

1. 组网需求

由于网络规模迅速扩大，当前中心设备（Device A）转发能力已经不能满足需求，现需要在保护现有投资的基础上将网络转发能力提高一倍，并要求网络易管理、易维护。

2. 组网图

图1-16 IRF 典型配置组网图（ARP MAD 检测方式）



3. 配置思路

- Device A 处于局域网的汇聚层，为了将汇聚层的安全业务处理能力提高一倍，需要另外增加一台设备 Device B。
- 鉴于 IRF 技术具有管理简便、网络扩展能力强、可靠性高等优点，所以本例使用 IRF 技术构建网络接入层（即在 Device A 和 Device B 上配置 IRF 功能），IRF 通过双链路上行。
- 为了防止 IRF 链路故障导致 IRF 分裂，网络中存在两个配置冲突的 IRF，需要启用 MAD 检测功能。因为成员设备比较少，我们采用 ARP MAD 检测方式来监测 IRF 的状态，复用链路上行传递 ARP MAD 报文。为防止环路发生，在 IRF 和 Device C 上启用生成树功能。

4. 配置步骤

(1) 配置 Device A

配置接口 IP 地址、路由、安全域及域间安全策略保证网络可达，具体配置步骤略。

```
<DeviceA> system-view
```

设备成员编号 1 的设备的优先级为 32。

```
[DeviceA] irf member 1 priority 32
```

配置 IRF 端口 1/2，并将它与物理端口 Ten-GigabitEthernet1/1/2 绑定，并保存配置。

```
[DeviceA] interface ten-gigabitethernet 1/1/2
[DeviceA-Ten-GigabitEthernet1/1/2] shutdown
[DeviceA-Ten-GigabitEthernet1/1/2] quit
[DeviceA] irf-port 1/2
[DeviceA-irf-port1/2] port group interface ten-gigabitethernet 1/1/2
[DeviceA-irf-port1/2] quit
[DeviceA] interface ten-gigabitethernet 1/1/2
[DeviceA-Ten-GigabitEthernet1/1/2] undo shutdown
[DeviceA-Ten-GigabitEthernet1/1/2] quit
[DeviceA] save
```

激活 IRF 端口下的配置。

```
[DeviceA] irf-port-configuration active
```

(2) 配置 Device B

配置接口 IP 地址、路由、安全域及域间安全策略保证网络可达，具体配置步骤略。

将 Device B 的成员编号配置为 2，并重启设备使新编号生效。

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[DeviceB] quit
<DeviceB> reboot
```

参照 图 1-16 进行物理连线，Device A和Device B组成IRF。

重新登录到设备，配置 IRF 端口 2/1，并将它与物理端口 Ten-GigabitEthernet2/1/1 绑定，并保存配置。

```
<DeviceB> system-view
[DeviceB] interface ten-gigabitethernet 2/1/1
[DeviceB-Ten-GigabitEthernet2/1/1] shutdown
[DeviceB-Ten-GigabitEthernet2/1/1] quit
[DeviceB] irf-port 2/1
[DeviceB-irf-port2/1] port group interface ten-gigabitethernet 2/1/1
[DeviceB-irf-port2/1] quit
[DeviceB] interface ten-gigabitethernet 2/1/1
[DeviceB-Ten-GigabitEthernet2/1/1] undo shutdown
[DeviceB-Ten-GigabitEthernet2/1/1] quit
[DeviceB] save
```

激活 IRF 端口下的配置。

```
[DeviceB] irf-port-configuration active
```

(3) Device A 和 Device B 间将会进行主设备竞选，竞选失败的一方将重启（Device B），重启完成后，IRF 形成。

(4) 配置 ARP MAD 检测

在 IRF 上全局开启生成树协议，并配置 MST 域，以防止环路的发生。

```
[DeviceA] stp global enable
[DeviceA] stp region-configuration
```

```
[DeviceA-mst-region] region-name arpmad
[DeviceA-mst-region] instance 1 vlan 3
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

将 IRF 配置为桥 MAC 立即改变。

```
[DeviceA] undo irf mac-address persistent
```

设置 IRF 域编号为 1。

```
[DeviceA] irf domain 1
```

创建 VLAN 3，并将 Device A（成员编号为 1）上的端口 GigabitEthernet1/0/1 和 Device B（成员编号为 2）上的端口 GigabitEthernet2/0/1 加入 VLAN 3 中。

```
[DeviceA] vlan 3
[DeviceA-vlan3] quit
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-mode bridge
[DeviceA-GigabitEthernet1/0/1] port access vlan 3
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] port link-mode bridge
[DeviceA-GigabitEthernet2/0/1] port access vlan 3
[DeviceA-GigabitEthernet2/0/1] quit
```

创建 VLAN-interface3，并配置 IP 地址，开启 ARP MAD 检测功能。

```
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] ip address 192.168.2.1 24
[DeviceA-Vlan-interface3] mad arp enable
 You need to assign a domain ID (range: 0-4294967295)
 [Current domain is: 1]:
 The assigned  domain ID is: 1
```

(5) 配置中间设备 Device C

提示

如果中间设备是一个 IRF 系统，则必须通过配置确保其 IRF 域编号与被检测的 IRF 系统不同。

Device C 作为中间设备来转发、处理 ARP 报文，协助 Device A 和 Device B 进行多 Active 检测。从节约成本的角度考虑，使用一台支持 ARP 功能的设备即可。

配置接口 IP 地址、路由保证网络可达，具体配置步骤略。

在全局开启生成树协议，并配置 MST 域，以防止环路的发生。

```
<DeviceC> system-view
[DeviceC] stp global enable
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name arpmad
[DeviceC-mst-region] instance 1 vlan 3
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

创建 VLAN 3，并将端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 加入 VLAN 3 中，用于转发 ARP MAD 报文。

```
[DeviceC] vlan 3
[DeviceC-vlan3] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[DeviceC-vlan3] quit
```

5. 验证配置

(1) IRF 链路正常情况下查看相关配置

查看 IRF 相关信息，可见 IRF 成功建立，且 DeviceA 为主设备。

```
[DeviceA] display irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  32        487a-da95-93b5  ---
   2        Standby 1         3897-d6a8-1b1a  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 487a-da95-93b3
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 1
```

查看 ARP MAD 状态，状态正常。

```
[DeviceA] display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  Ten-GigabitEthernet1/1/2
  Ten-GigabitEthernet2/1/1
MAD ARP enabled interface:
  Vlan-interface3
MAD ND disabled.
MAD LACP disabled.
MAD BFD disabled.
```

(2) IRF 链路异常情况下查看相关配置

查看 ARP MAD 状态，状态异常，表示 IRF 分裂。

```
[DeviceA] display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  Ten-GigabitEthernet1/1/2
MAD ARP enabled interface:
  Vlan-interface3
MAD ND disabled.
MAD LACP disabled.
MAD BFD disabled.
```

查看 Device B 上的非保留端口全部被置为 Down，显示信息略。

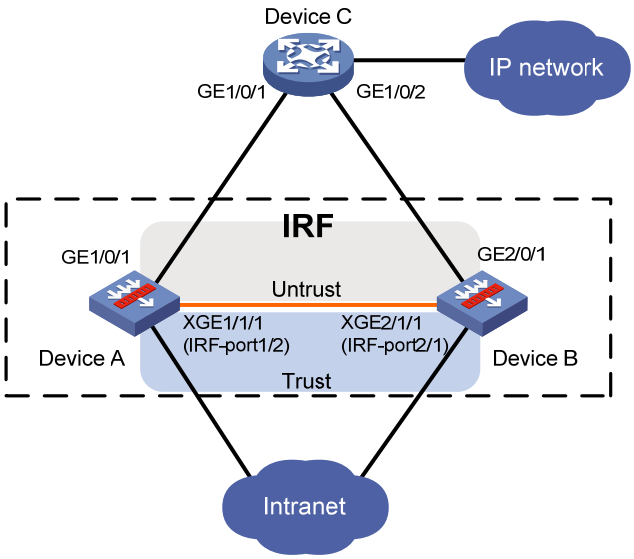
1.10.4 IRF典型配置举例（ND MAD检测方式）

1. 组网需求

IPv6 网络中，由于网络规模迅速扩大，当前中心设备（Device A）转发能力已经不能满足需求，现需要在保护现有投资的基础上将网络转发能力提高一倍，并要求网络易管理、易维护。

2. 组网图

图1-17 IRF 典型配置组网图（ND MAD 检测方式）



3. 配置思路

- Device A 处于局域网的汇聚层，为了将汇聚层的安全业务处理能力提高一倍，需要另外增加一台设备 Device B。
- 鉴于 IRF 技术具有管理简便、网络扩展能力强、可靠性高等优点，所以本例使用 IRF 技术构建网络接入层（即在 Device A 和 Device B 上配置 IRF 功能），IRF 通过双链路上行。
- 为了防止 IRF 链路故障导致 IRF 分裂，网络中存在两个配置冲突的 IRF，需要启用 MAD 检测功能。在 IPv6 环境我们采用 ND MAD 检测方式来监测 IRF 的状态，复用链路上行传递 ND MAD 报文。为防止环路发生，在 IRF 和 Device C 上启用生成树功能。

4. 配置步骤

(1) 配置 Device A

配置接口 IP 地址、路由、安全域及域间安全策略保证网络可达，具体配置步骤略。

```
<DeviceA> system-view
```

设备成员编号 1 的设备的优先级为 32。

```
[DeviceA] irf member 1 priority 32
```

配置 IRF 端口 1/2，并将它与物理端口 Ten-GigabitEthernet1/1/2 绑定，并保存配置。

```
[DeviceA] interface ten-gigabitethernet 1/1/2
[DeviceA-Ten-GigabitEthernet1/1/2] shutdown
[DeviceA-Ten-GigabitEthernet1/1/2] quit
[DeviceA] irf-port 1/2
```

```
[DeviceA-irf-port1/2] port group interface ten-gigabitethernet 1/1/2
[DeviceA-irf-port1/2] quit
[DeviceA] interface ten-gigabitethernet 1/1/2
[DeviceA-Ten-GigabitEthernet1/1/2] undo shutdown
[DeviceA-Ten-GigabitEthernet1/1/2] quit
[DeviceA] save
```

激活 IRF 端口下的配置。

```
[DeviceA] irf-port-configuration active
```

(2) 配置 Device B

配置接口 IP 地址、路由、安全域及域间安全策略保证网络可达，具体配置步骤略。

将 Device B 的成员编号配置为 2，并重启设备使新编号生效。

```
<DeviceB> system-view
[DeviceB] irf member 1 renumber 2
Warning: Renumbering the member ID may result in configuration change or loss. Continue?
[Y/N]:y
[DeviceB] quit
<DeviceB> reboot
```

参照 图 1-17 进行物理连线，Device A和Device B组成IRF。

重新登录到设备，配置 IRF 端口 2/1，并将它与物理端口 Ten-GigabitEthernet2/1/1 绑定，并保存配置。

```
<DeviceB> system-view
[DeviceB] interface ten-gigabitethernet 2/1/1
[DeviceB-Ten-GigabitEthernet2/1/1] shutdown
[DeviceB-Ten-GigabitEthernet2/1/1] quit
[DeviceB] irf-port 2/1
[DeviceB-irf-port2/1] port group interface ten-gigabitethernet 2/1/1
[DeviceB-irf-port2/1] quit
[DeviceB] interface ten-gigabitethernet 2/1/1
[DeviceB-Ten-GigabitEthernet2/1/1] undo shutdown
[DeviceB-Ten-GigabitEthernet2/1/1] quit
[DeviceB] save
```

激活 IRF 端口下的配置。

```
[DeviceB] irf-port-configuration active
```

(3) Device A 和 Device B 间将会进行主设备竞选，竞选失败的一方将重启（Device B），重启完成后，IRF 形成。

(4) 配置 ND MAD 检测

在 IRF 上全局开启生成树协议，并配置 MST 域，以防止环路的发生。

```
[DeviceA] stp global enable
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name ndmad
[DeviceA-mst-region] instance 1 vlan 3
[DeviceA-mst-region] active region-configuration
[DeviceA-mst-region] quit
```

将 IRF 配置为桥 MAC 立即改变。

```
[DeviceA] undo irf mac-address persistent
```

设置 IRF 域编号为 1。

```
[DeviceA] irf domain 1
```

创建 VLAN 3，并将 Device A（成员编号为 1）上的端口 GigabitEthernet1/0/1 和 Device B（成员编号为 2）上的端口 GigabitEthernet2/0/1 加入 VLAN 3 中。

```
[DeviceA] vlan 3
[DeviceA-vlan3] quit
[DeviceA] interface GigabitEthernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] port link-mode bridge
[DeviceA-GigabitEthernet1/0/1] port access vlan 3
[DeviceA-GigabitEthernet1/0/1] quit
[DeviceA] interface GigabitEthernet 2/0/1
[DeviceA-GigabitEthernet2/0/1] port link-mode bridge
[DeviceA-GigabitEthernet2/0/1] port access vlan 3
[DeviceA-GigabitEthernet2/0/1] quit
```

创建 VLAN-interface3，并配置 IPv6 地址，开启 ND MAD 检测功能。

```
[DeviceA] interface vlan-interface 3
[DeviceA-Vlan-interface3] ipv6 address 2001::1 64
[DeviceA-Vlan-interface3] mad nd enable
 You need to assign a domain ID (range: 0-4294967295)
 [Current domain is: 1]:
 The assigned  domain ID is: 1
```

(5) 配置中间设备 Device C

提示

如果中间设备是一个 IRF 系统，则必须通过配置确保其 IRF 域编号与被检测的 IRF 系统不同。

Device C 作为中间设备来转发、处理 ND 报文，协助 Device A 和 Device B 进行多 Active 检测。从节约成本的角度考虑，使用一台支持 ND 功能的设备即可。

配置接口 IP 地址、路由保证网络可达，具体配置步骤略。

在全局开启生成树协议，并配置 MST 域，以防止环路的发生。

```
<DeviceC> system-view
[DeviceC] stp global enable
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name ndmad
[DeviceC-mst-region] instance 1 vlan 3
[DeviceC-mst-region] active region-configuration
[DeviceC-mst-region] quit
```

创建 VLAN 3，并将端口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 加入 VLAN 3 中，用于转发 ND MAD 报文。

```
[DeviceC] vlan 3
[DeviceC-vlan3] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[DeviceC-vlan3] quit
```

5. 验证配置

(1) IRF 链路正常情况下查看相关配置

查看 IRF 相关信息，可见 IRF 成功建立，且 DeviceA 为主设备。

```
[DeviceA] display irf
MemberID    Role    Priority  CPU-Mac         Description
 *+1        Master  32        487a-da95-93b5  ---
   2        Standby 1         3897-d6a8-1b1a  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 487a-da95-93b3
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 1
```

查看 ND MAD 状态，状态正常。

```
[DeviceA] display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  Ten-GigabitEthernet1/1/2
  Ten-GigabitEthernet2/1/1
MAD ARP disabled.
MAD ND enabled interface:
  Vlan-interface3
MAD LACP disabled.
MAD BFD disabled.
```

(2) IRF 链路异常情况下查看相关配置

查看 ND MAD 状态，状态异常，表示 IRF 分裂。

```
[DeviceA] display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
Excluded ports (system-configured):
  Ten-GigabitEthernet1/1/2
MAD ARP disabled.
MAD ND enabled interface:
  Vlan-interface3
MAD LACP disabled.
MAD BFD disabled.
```

查看 Device B 上的非保留端口全部被置为 Down，显示信息略。

目 录

1 Context

1.1 Context简介

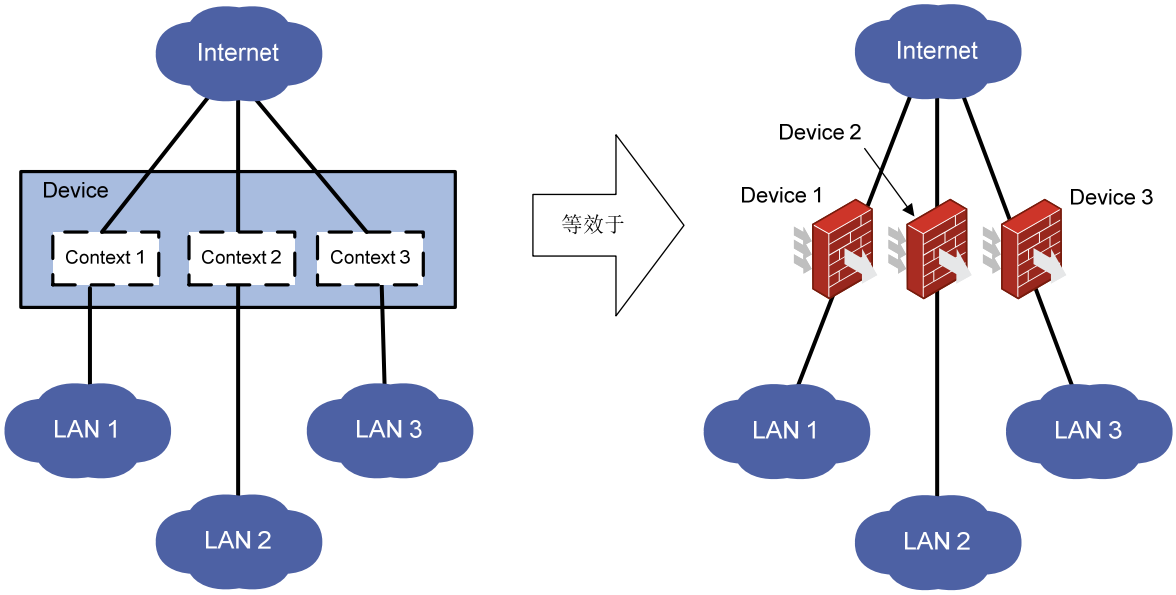
通过虚拟化技术将一台物理设备划分成多台逻辑设备，每台逻辑设备就称为一个 Context。每个 Context 拥有自己专属的软硬件资源，独立运行。

对于用户来说，每个 Context 就是一台独立的设备，方便管理和维护；对于管理者来说，可以将一台物理设备虚拟成多台逻辑设备供不同的分支机构使用，可以保护现有投资，提高组网灵活性。

1.1.1 Context的应用

如 图 1-1 所示，LAN 1、LAN 2 和LAN 3 是三个不同的局域网，它们通过同一台设备连接到外网。通过虚拟化技术，能让一台设备当三台设备使用。具体做法是，在Device上创建三个Context（Context 1、Context 2、Context 3），分别负责LAN 1、LAN 2、LAN 3 的安全接入。LAN 1、LAN 2、LAN 3 的网络管理员可以（也只能）分别登录到自己的设备进行配置、保存、重启等操作，不会影响其它网络的使用，其效果等同于LAN 1、LAN 2 和LAN 3 分别通过各自的设备Device 1、Device 2、Device 3 接入Internet。

图1-1 Context 组网示意图



1.1.2 缺省Context和非缺省Context

- 设备支持Context功能后，整台物理设备就是一个Context，称为缺省Context，如 图 1-1 中的Device。当用户登录物理设备时，实际登录的就是缺省Context。用户在物理设备上的配置实质就是对缺省Context的配置。缺省Context的名称为Admin，编号为 1。缺省Context不需要创建，不能删除。

- 与缺省Context相对应的是非缺省Context，如 图 1-1 中的Context 1、Context 2、Context 3。非缺省Context是管理员在设备上通过命令行创建的，可分配给不同的接入网络使用。
- 缺省 Context 拥有对整台物理设备的所有权限，它可以使用和管理设备所有的资源。缺省 Context 下可以创建/删除非缺省 Context，给非缺省 Context 分配 CPU 资源/磁盘/内存空间、接口、VLAN，没有分配的 CPU 资源/磁盘/内存空间、接口、VLAN 由缺省 Context 使用和管理。
- 非缺省 Context 下不可再创建/删除非缺省 Context，它只能使用缺省 Context 分配给自己的资源，并在缺省 Context 指定的资源限制范围内工作，不能抢占其他 Context 或者系统剩余的资源。
- 非缺省 Context 下不支持共享口的报文捕获功能，关于报文捕获功能的详细描述请参见“网络管理和监控配置指导”中的“报文捕获配置”。

1.2 Context配置限制和指导

非缺省 Context 中的 DPI 业务功能使用缺省 Context 中的应用层检测引擎对报文进行匹配，当创建、删除、关闭和重启非缺省 Context 时，缺省 Context 中的应用层检测引擎会重新激活，激活期间设备上的所有 Context 均不能对报文进行 DPI 业务处理。

1.2.1 分配VLAN时的注意事项

- 对于共享 VLAN，请先在缺省 Context 内创建 VLAN，再通过 **allocate vlan** 命令将指定 VLAN 分配给指定的 Context 使用。
- VLAN 1 不能被共享。
- 端口的缺省 VLAN 不能被共享。
- 已经创建了 VLAN 接口的 VLAN 不能被共享。

1.2.2 分配接口时的注意事项

(1) 有些接口可以创建子接口，这样的接口我们称为父接口。分配父接口与子接口时：

- 不能将子接口独占分配给 Context。
- 如果子接口已经被分配，则不能再分配其父接口。
- 如果父接口已经被分配，则不能再分配其子接口。

(2) 分配聚合接口与成员接口时：

- 聚合接口只能共享分配给 Context。
- 不能将成员接口共享分配给 Context。

(3) 如果接口已经被共享分配，则不能再独占分配。需将共享分配配置取消后，才能独占分配。

(4) 不允许独占分配逻辑接口。

(5) 禁止将 IRF 物理端口分配给自定义 Context。

(6) 当三层物理子接口与聚合子接口作为冗余口的成员端口时，禁止把其主接口共享给自定义 Context。

1.3 Context配置任务简介

表1-1 Context 配置任务简介

配置任务		说明	详细配置
创建Context		必选	1.4
为Context分配资源	为Context分配CPU/磁盘/内存资源	必选	1.5.1
	为Context分配接口	必选	1.5.2
	为Context分配VLAN	可选	1.5.3
	限制Context的吞吐量	可选	1.5.4
	限制Context安全策略规则总数	可选	1.5.5
	限制Context会话并发数	可选	1.5.6
	限制Context会话新建速率	可选	1.5.7
启动Context		必选	1.6
访问和管理Context		必选	1.7

1.4 创建Context

创建 Context 相当于构造了一台新的设备。

创建 Context 时，通过 **vlan-unshared** 参数可选择是否和其它 Context 共享 VLAN：

- 如果选择和其它 Context 共享 VLAN，需要在缺省 Context 内创建并配置 VLAN，再分配给非缺省 Context。共享 VLAN 由多个 Context 共同所有。VLAN 1 为系统缺省 VLAN，由缺省 Context 独有，不能分配给非缺省 Context。
- 如果选择不和其它 Context 共享 VLAN，请登录该 Context，并使用 **vlan** 命令创建 VLAN 2～VLAN 4094。VLAN 1 为缺省 VLAN，用户不能手工创建和删除。Context 各自使用和管理 VLAN，互不干扰。

表1-2 创建 Context

操作	命令	说明
进入系统视图	**system-view**	-
创建Context，并进入Context视图	**context** *context-name* [**id** *context-id*] [**vlan-unshared**]	缺省情况下，设备上存在缺省Context，名称为Admin，编号为1
配置Context的描述信息	**description** *text*	缺省情况下，缺省Context描述信息为DefaultContext。非缺省Context没有配置描述信息

1.5 为Context分配资源

1.5.1 为Context分配CPU/磁盘/内存资源

如果设备上创建了多个 Context，这些 Context 会共享设备的 CPU/磁盘/内存资源，为了防止一个 Context 过多的占用 CPU/磁盘/内存，而导致其它 Context 无法运行，需要限制 Context 对 CPU/磁盘/内存资源的使用。

(1) CPU 权重

当 CPU 无法满足所有 Context 的处理需求时，系统将按照 CPU 权重值为每个 Context 分配处理时间。通过调整 Context 的权重，可以使指定的 Context 获得更多的 CPU 资源，保证关键业务的运行。例如：在三个 Context 中，将处理关键业务的 Context 的 CPU 权重设置为 2，其余两个 Context 的 CPU 权重设置为 1，则当 CPU 处理能力不足时，将为关键业务 Context 提供 2 倍于其它 Context 的处理时间。

(2) 磁盘空间上限

执行 **limit-resource disk** 命令前，请使用 **display context resource** 命令查看 Context 当前实际已经使用的磁盘空间大小。配置值应大于 Context 当前实际已经使用的磁盘空间大小，否则，会导致 Context 申请新的磁盘空间失败，从而无法进行文件夹创建、文件拷贝和保存等操作。

请在 Context 启动后，配置磁盘上限。因为，Context 创建后，如果没有启动，磁盘使用值为 0，此时如果配置磁盘上限，请尽量不要配置过小的上限，否则，可能导致 Context 启动不了。

(3) 内存空间上限

执行 **limit-resource memory** 命令前，请使用 **display context resource** 命令查看 Context 当前实际已经使用的内存空间大小。配置值应大于 Context 当前实际已经使用的内存空间大小，否则，会导致 Context 申请内存失败引起功能异常。

请在 Context 启动后，再配置内存上限，并且配置的上限值不应过小，以免 Context 内业务申请不到内存后引起功能不正常。

表1-3 为 Context 分配 CPU/磁盘/内存资源

操作	命令	说明
进入系统视图	**system-view**	-
进入Context视图	**context** *context-name*	-
指定Context的CPU权重	**limit-resource cpu weight** *weight-value*	缺省情况下，Context的CPU权重为10
配置Context可使用的磁盘空间上限	**limit-resource disk slot** *slot-number* **cpu** *cpu-number* **ratio** *limit-ratio*	缺省情况下，Context可以使用其所在成员设备上的所有磁盘空间 如果设备上有多块磁盘，该命令对所有磁盘生效
配置Context可使用的内存空间上限	**limit-resource memory slot** *slot-number* **cpu** *cpu-number* **ratio** *limit-ratio*	缺省情况下，Context可以使用其所在成员设备上的所有内存空间，每个Context可使用的内存空间上限为空闲内存空间值

1.5.2 为Context分配接口

设备上的所有接口都属于缺省Context，不属于任何非缺省Context。请给非缺省Context分配接口，它才能和网络中的其它设备通信。

为了提高设备接口的利用率，在给 Context 分配接口时，可以选择：

- 独占方式分配（不带 **share** 参数）。使用该方式分配的接口仅归该 Context 所有、使用。用户登录该 Context 后，能查看到该接口，并执行接口支持的所有命令。
- 共享方式分配（带 **share** 参数）：表示将一个接口分配给多个 Context 使用，这些 Context 共享这个物理接口，但是在各个 Context 内会创建一个同名的虚接口，这些虚接口具有不同的 MAC 地址和 IP 地址。设备从共享的物理接口接收报文后交给对应的虚拟接口处理；出方向，虚拟接口处理完报文后，会交给共享的物理接口发送。使用该方式，可以提高设备接口的利用率。通过共享方式分配的接口：
  - 在缺省 Context 内仍然存在该接口，该接口可执行接口支持的所有命令；
  - 在非缺省 Context 内，会新建一个同名接口，用户登录这些 Context 后，能查看到该接口，但只能执行 **shutdown**、**description** 以及网络/安全相关的命令。

注意

- 当三层子接口作为冗余口的成员端口时，禁止把其主接口共享给自定义 Context。
- 不允许独占分配逻辑接口

表1-4 为 Context 分配接口

操作	命令	说明
进入系统视图	**system-view**	-
进入Context视图	**context** *context-name*	-
为Context分配接口	**allocate interface** { *interface-type interface-number* }&<1-24> [**share**]	二者选其一 缺省情况下，设备上的所有接口都属于缺省Context，不属于任何非缺省Context
	allocate interface *interface-type interface-number1* **to** *interface-type interface-number2* [**share**]	

1.5.3 为Context分配VLAN

创建 Context 时，如果不选择 **vlan-unshared** 参数，则表示和其它 Context 共享 VLAN。对于共享 VLAN，请先在缺省 Context 内创建 VLAN，再通过 **allocate vlan** 命令将指定 VLAN 分配给指定的 Context 使用。

表1-5 为 Context 分配 VLAN

操作	命令	说明
进入系统视图	**system-view**	-
进入Context视图	**context** *context-name*	-

操作	命令	说明
为Context分配VLAN	**allocate vlan** *vlan-id*&<1-24>	二者选其一 缺省情况下，没有为Context分配VLAN
	allocate vlan *vlan-id1* **to** *vlan-id2*	

1.5.4 限制Context的吞吐量

为了防止一个 Context 的报文过多而导致其它 Context 的报文被丢弃，需要限制 Context 的吞吐量当启用吞吐量限制时，系统优先处理协议报文，对于超过限制值的业务报文会被丢弃。。

表1-6 限制 Context 的吞吐量

操作	命令	说明
进入系统视图	**system-view**	-
进入Context视图	**context** *context-name*	-
设置Context的吞吐量限制	**capability throughput** { **kbps** | **pps** } *value*	缺省情况下，各Context不做吞吐量限制，按实际能力转发

1.5.5 限制Context安全策略规则总数

一个 Context 内可以配置多条安全策略规则。如果不加限制，会出现大量规则占用过多内存的情况，影响 Context 的其它功能正常运行。所以，请根据需要为 Context 设置安全策略规则总数限制。当规则总数达到限制值时，后续不能新增规则。关于安全策略的详细描述请参见“安全配置指导”中的“安全策略”。

表1-7 限制 Context 安全策略规则总数

操作	命令	说明
进入系统视图	**system-view**	-
进入Context视图	**context** *context-name*	-
设置Context的安全策略规则总数限制	**capability security-policy-rule maximum** *max-value*	缺省情况下，不限制Context的安全策略规则总数

1.5.6 限制Context会话并发数

如果一个 Context 建立了太多会话表会导致其他 Context 的会话由于内存不够而无法建立，为了防止这种情况，需要限制 Context 建立会话表的数量。

需要注意的是：Context 会话并发数限制对本机流量不生效，例如：FTP、Telnet、SSH 和 HTTP 等业务。

表1-8 为 Context 限制会话并发数

操作	命令	说明
进入系统视图	**system-view**	-
进入Context视图	**context** *context-name*	-
设置Context的单播会话并发数限制	**capability session maximum** *max-number*	缺省情况下，不限制该Context允许的单播会话并发数

1.5.7 限制Context会话新建速率

如果一个Context的会话新建速率过快会导致其他Context由于CPU处理能力不够而无法建立会话，为了防止这种情况，需要限制 Context 的会话新建速率。

需要注意的是：Context 会话新建速率限制对本机流量不生效，例如：FTP、Telnet、SSH 和 HTTP 等业务。

表1-9 为 Context 限制会话新建速率

操作	命令	说明
进入系统视图	**system-view**	-
进入Context视图	**context** *context-name*	-
设置Context的会话新建速率限制	**capability session rate** *max-value*	缺省情况下，不限制该Context允许的会话新建速率

1.6 启动Context

Context 创建后需要执行 **context start** 命令，才能完成新 Context 的初始化，相当于上电启动。启动后，用户可以登录到该 Context 执行配置。

正常程序启动 Context 时，设备会先做一些检查（比如 Context 的主、备进程能否正常启动），满足条件后，才启动 Context，该命令会保证主备的 Context 状态一致，如果某成员设备上的 Context 启动失败，则会导致所有该 Context 进程启动失败。正常程序启动的 Context 能更好的保证 Context 的业务正常运行，所以，通常情况下，使用 **context start** 命令启动 Context 即可。**force** 参数用于以下场景：在 IRF 环境，如果主备倒换或者配置恢复过程中出现内存不足，会导致部分 Context 虽然可以处理业务，但因为它们的主、备进程状态不一致，这些 Context 一直停留在 updating 或者 inactive 状态。当内存资源恢复后，执行 **context start force** 命令，设备会在不中断业务的情况下，尽可能修复不正常的 Conext 进程，让这些 Context 恢复到正常状态。

提示

在使用 **context start force** 前，用户可以通过 **display context**、**display system internal context configuration-status**、**display system internal context id** *contex-id* **running-status** 命令查看 Context 的运行情况。

表1-10 启动 Context

操作	命令	说明
进入系统视图	**system-view**	-
进入Context视图	**context** *context-name*	-
启动Context	**context start** [**force**]	-

1.7 访问和管理Context

只要用户和设备之间路由可达，就能使用 **switchto context** 命令，通过设备和 Context 的内部连接，登录 Context。

表1-11 登录 Context

操作	命令	说明
进入系统视图	**system-view**	-
登录Context	**switchto context** *context-name*	必选

用户登录 Context 后，可以在 Context 的用户视图执行 **quit** 命令来退出登录。此时，命令视图将从当前 Context 的用户视图返回到缺省 Context 的系统视图。

除了上述方式，用户还可以通过 Context 上的接口，使用该 Context 的 IP 地址进行 Telnet/SSH 登录。

1.8 Context显示和维护

在完成 Context 相关配置后，在任意视图下执行 **display** 命令，可以显示配置后 Context 的运行情况，通过查看显示信息，来验证配置的效果。

在用户视图下，用户可以执行 **reset** 命令清除相关数据信息。

表1-12 Context 显示和维护

操作	命令
显示Context的相关信息	**display context** [**name** *context-name*]
显示Context的接口列表	**display context** [**name** *context-name*] **interface**
显示Context对CPU/磁盘/内存资源的使用情况	**display context** [**name** *context-name*] **resource** [**cpu** | **disk** | **memory**] [**slot** slot-number **cpu** *cpu-number*]
显示Context的VLAN列表	**display context** [**name** *context-name*] **vlan**

1.9 Context典型配置举例

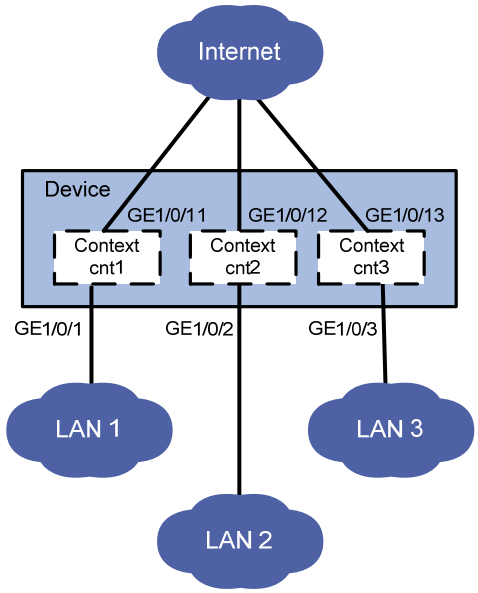
1. 组网需求

将设备 Device 虚拟成三台独立的设备：Context cnt1、Context cnt2、Context cnt3，并分给三个不同的用户网络用作接入设备。

- LAN 1 的用户多，业务需求复杂，因此需要给 Context cnt1 提供较大的磁盘/内存空间使用上限，以便保存配置文件、启动文件和系统信息等；Context cnt2 使用系统缺省的磁盘空间；LAN 3 人员规模小，上网流量比较少，对接入设备的配置及性能要求较低，因此对 Context cnt3 提供较低的 CPU 权重。
- GigabitEthernet1/0/1 和 GigabitEthernet1/0/11 分配给 Context cnt1、GigabitEthernet1/0/2 和 GigabitEthernet1/0/12 分配给 Context cnt2、GigabitEthernet1/0/3 和 GigabitEthernet1/0/13 分配给 Context cnt3。

2. 组网图

图1-2 Context 典型配置组网图



3. 配置步骤

(1) 配置 Context cnt1

创建 Context cnt1，设置描述信息。

```
[Sysname] context cnt1
[Sysname-context-2-cnt1] description context-1
```

配置 Context cnt1 的磁盘使用上限为 60%。

```
[Sysname-context-2-cnt1] limit-resource disk slot 1 cpu 0 ratio 60
```

配置 Context cnt1 的内存使用上限为 60%。

```
[Sysname-context-2-cnt1] limit-resource memory slot 1 cpu 0 ratio 60
```

配置 Context cnt1 的 CPU 权重为 8。

```
[Sysname-context-2-cnt1] limit-resource cpu weight 8
```

启动 Context cnt1。

```
[Sysname-context-2-cnt1] context start
It will take some time to start the context...
Context started successfully.
```

将接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/11 分配给 Context cnt1。

```
[Sysname-context-2-cnt1] allocate interface gigabitethernet 1/0/1 gigabitethernet 1/0/11
[Sysname-context-2-cnt1] quit
```

(2) 配置 Context cnt2

创建 Context cnt2，设置描述信息

```
[Sysname] context cnt2
[Sysname-context-3-cnt2] description context-2
```

启动 Context cnt2。

```
[Sysname-context-3-cnt2] context start
It will take some time to start the context...
Context started successfully.
```

将接口 GigabitEthernet1/0/2 和 GigabitEthernet1/0/12 分配给 Context cnt2。

```
[Sysname-context-3-cnt2] allocate interface gigabitethernet 1/0/2 gigabitethernet 1/0/12
[Sysname-context-3-cnt2] quit
```

(3) 配置 Context cnt3

创建 Context cnt3，设置描述信息

```
[Sysname] context cnt3
[Sysname-context-4-cnt3] description context-3
```

#配置 Context cnt3 的 CPU 权重为 2。

```
[Sysname-context-4-cnt3] limit-resource cpu weight 2
```

启动 Context cnt3。

```
[Sysname-context-4-cnt3] context start
It will take some time to start the context...
Context started successfully.
```

将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/13 分配给 Context cnt3。

```
[Sysname-context-4-cnt3] allocate interface gigabitethernet 1/0/3 gigabitethernet 1/0/13
[Sysname-context-4-cnt3] quit
```

完成上述配置后，可使用 **switchto context** 命令登录到指定的 Context，进行业务相关的配置。