

H3C SecPath 负载均衡产品

虚拟化技术命令参考(V7)

新华三技术有限公司

<http://www.h3c.com>

资料版本：6W302-20201121

产品版本：

L5030/L5060/L5080/L5000-E	R8504
L5000-C/L5000-S	R8130
L5000-AK535	R8504
L1000-E/L1000-M/L1000-S	R8127
L1000-AK310/L1000-AK320/L1000-AK330	R8127
L100-C/L1000-C	R9510
LSU1ADECEA0	R8132
LSWM1ADED0/LSQM1ADEDSC0	R8522

Copyright © 2019-2020 新华三技术有限公司及其许可者 版权所有，保留一切权利。

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

除新华三技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。**H3C** 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，**H3C** 尽全力在本手册中提供准确的信息，但是 **H3C** 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前言

本命令参考主要介绍虚拟化技术相关的配置命令。

前言部分包含如下内容：

- [读者对象](#)
- [本书约定](#)
- [资料意见反馈](#)

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。
<i>斜体</i>	命令行参数（命令中必须由实际值进行替代的部分）采用 <i>斜体</i> 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择一个或者不选。
{ 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择一个、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
1.1 IRF 配置命令	1-1
1.1.1 display irf	1-1
1.1.2 display irf configuration	1-2
1.1.3 display irf link	1-3
1.1.4 display irf topology	1-4
1.1.5 display irf-port load-sharing mode	1-5
1.1.6 display mad	1-7
1.1.7 easy-irf	1-9
1.1.8 irf auto-update enable	1-12
1.1.9 irf domain	1-12
1.1.10 irf mac-address persistent	1-13
1.1.11 irf member description	1-14
1.1.12 irf member priority	1-15
1.1.13 irf member renumber	1-15
1.1.14 irf-port	1-16
1.1.15 irf-port global load-sharing mode	1-17
1.1.16 irf-port load-sharing mode	1-18
1.1.17 irf-port-configuration active	1-19
1.1.18 mad arp enable	1-20
1.1.19 mad bfd enable	1-21
1.1.20 mad enable	1-24
1.1.21 mad exclude interface	1-25
1.1.22 mad ip address	1-26
1.1.23 mad nd enable	1-27
1.1.24 mad restore	1-28
1.1.25 port group interface	1-28

1 IRF

1.1 IRF配置命令

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
L5030/L5060/L5080/L5000-E	支持
L5000-C/L5000-S	支持
L5000-AK535	支持
L1000-C/L1000-S/L1000-M/L1000-E	支持
L1000-AK310/L1000-AK320/L1000-AK330	支持
L100-C	不支持
LSU1ADECEA0/LSWM1ADED0/LSQM1ADEDSC0	支持

1.1.1 display irf

display irf 命令用来显示 IRF 的相关信息。

【命令】

```
display irf
```

【视图】

任意视图

【缺省用户角色】

```
network-admin  
network-operator
```

【举例】

显示 IRF 的相关信息。

```
<Sysname> display irf  
MemberID  Role      Priority  CPU-Mac      Description  
  1        Loading  1        00e0-fcbe-3102  F1Num001  
 *+2      Master   1        00e0-fcb1-ade2  F1Num002  
-----  
  
* indicates the device is the master.  
+ indicates the device through which the user logs in.  
  
The Bridge MAC of the IRF is: 00e0-fc00-1000  
Auto upgrade           : yes
```

Mac persistent : always
 Domain ID : 30

表1-1 display irf 命令显示信息描述表

字段	描述
MemberID	成员设备的编号： <ul style="list-style-type: none"> 如果编号前带“*”，表示该设备是主设备 如果编号前带“+”，表示该设备是用户当前登录的、正在操作的设备
Role	成员设备的角色，可能为： <ul style="list-style-type: none"> Standby: 从设备 Master: 主设备 Loading: 正在自动加载系统启动文件
Priority	成员设备的优先级
CPU-MAC	设备的CPU MAC地址
Description	设备的描述信息： <ul style="list-style-type: none"> 没有描述信息时，Description 字段显示为"-----" 如果描述信息较多，无法在一行中完全显示，则以“...”结尾，省略后面的信息。此时可以使用 display current-configuration 来查询完整的描述信息
Bridge MAC of the IRF is	IRF的桥MAC
Auto upgrade	是否开启自动加载系统启动文件功能： <ul style="list-style-type: none"> yes 表示开启 no 表示未开启
MAC persistent	是否开启IRF桥MAC保留功能： <ul style="list-style-type: none"> n min 表示 IRF 的桥 MAC 保留时间为 n 分钟 always 表示 IRF 的桥 MAC 永久保留不改变 no 表示立即改变 IRF 的桥 MAC
Domain ID	IRF的域编号，当网络中存在多个IRF时，用来唯一标识一个IRF

【相关命令】

- **display irf configuration**
- **display irf topology**

1.1.2 display irf configuration

display irf configuration 命令用来显示 IRF 中所有成员设备的 IRF 配置。

【命令】

display irf configuration

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【举例】

显示 IRF 中所有成员设备的 IRF 配置。

```
<Sysname> display irf configuration
MemberID  NewID      IRF-Port1                IRF-Port2
1          1          Ten-GigabitEthernet1/0/1  Ten-GigabitEthernet1/0/2
2          2          Ten-GigabitEthernet2/0/1  Ten-GigabitEthernet2/0/3
                Ten-GigabitEthernet2/0/2
```

表1-2 display irf configuration 命令显示信息描述表

字段	描述
MemberID	设备当前的成员编号
NewID	配置的成员编号，设备重启后将会生效
IRF-Port1	IRF端口1的配置 <ul style="list-style-type: none">如果显示信息中包含多个物理端口，则表示该 IRF 端口由多个 IRF 物理端口聚合而成如果显示为 disable，则表示该 IRF 端口还没有和 IRF 物理端口绑定
IRF-Port2	IRF端口2的配置 <ul style="list-style-type: none">如果显示信息中包含多个物理端口，则表示该 IRF 端口由多个 IRF 物理端口聚合而成如果显示为 disable，则表示该 IRF 端口还没有和 IRF 物理端口绑定

【相关命令】

- **display irf**
- **display irf topology**

1.1.3 display irf link

display irf link 命令用来显示 IRF 链路信息。

【命令】

```
display irf link
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator
context-admin
context-operator

【举例】

显示 IRF 链路信息。

```
<Sysname> display irf link
```

Member 1

IRF Port	Interface	Status
1	disable	--
2	Ten-GigabitEthernet1/0/1	UP
	Ten-GigabitEthernet1/0/2	ADM
	Ten-GigabitEthernet1/0/3	DOWN

Member 2

IRF Port	Interface	Status
1	Ten-GigabitEthernet2/0/1	UP
	Ten-GigabitEthernet2/0/2	DOWN
	Ten-GigabitEthernet2/0/3	ADM
2	disable	--

表1-3 display irf link 命令显示信息描述表

字段	描述
Member ID	成员编号
IRF Port	IRF端口号，其中： <ul style="list-style-type: none">• 1 表示 IRF 端口 1• 2 表示 IRF 端口 2
Interface	对应的IRF物理端口的名称 <ul style="list-style-type: none">• 如果显示信息中包含多个物理端口，则表示该 IRF 端口由多个 IRF 物理端口聚合而成• 如果显示为 disable，则表示该 IRF 端口还没有和 IRF 物理端口绑定
Status	IRF物理端口的链路状态 <ul style="list-style-type: none">• UP: 链路 up• DOWN: 链路 down• ADM: 表示该接口已经通过 shutdown 命令被关闭，即管理状态为关闭• ABSENT: 接口不存在，没有插入单板或接口模块扩展卡

1.1.4 display irf topology

display irf topology 命令用来查看 IRF 的拓扑信息。

【命令】

```
display irf topology
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示 IRF 的拓扑信息。

```
<Sysname> display irf topology
                        Topology Info
-----
      IRF-Port1          IRF-Port2
MemberID  Link      neighbor  Link      neighbor  Belong To
1         DOWN     ---          UP        2          000f-cbb8-1a82
2         UP       1           DIS       ---        000f-cbb8-1a82
```

表1-4 display irf topology 命令显示信息描述表

字段	描述
MemberID	成员编号
IRF-Port1	IRF-Port1的信息，包括Link和neighbor信息
IRF-Port2	IRF-Port2的信息，包括Link和neighbor信息
Link	IRF端口的链路状态，包括： <ul style="list-style-type: none">• UP: 链路 up• DOWN: 链路 down，可能因为物理链路没有连通，或者没有执行 irf-port-configuration active 命令激活 IRF 端口• DIS: 表示该 IRF 端口还没有和任何 IRF 物理端口绑定• TIMEOUT: IRF 报文超时• ISOLATE: 本设备处于隔离状态，原因可能为设备型号不符合加入 IRF 的要求，或当前 IRF 中成员设备已达到最大数量
neighbor	与该IRF端口直连的设备的成员编号（显示为“---”表示该端口没有连接其它成员设备）
Belong To	所属IRF，用IRF中当前主设备的CPU MAC地址表示

【相关命令】

- **display irf**
- **display irf configuration**

1.1.5 display irf-port load-sharing mode

display irf-port load-sharing mode 命令用来显示 IRF 链路的负载分担模式。

【命令】

```
display irf-port load-sharing mode [ irf-port [ member-id/irf-port-number ] ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

irf-port: 显示指定 IRF 链路的负载分担模式。不指定该参数时，显示全局 IRF 链路的负载分担模式。

member-id/irf-port-number: 表示 IRF 端口编号。其中，*member-id* 表示设备在 IRF 中的成员编号；*irf-port-number* 表示 IRF 端口索引，取值为 1 或 2。不指定该参数时，显示所有连通的 IRF 链路的负载分担模式，如果当前没有连通的 IRF 链路，则显示 “No IRF link exists.”。

【举例】

显示缺省情况下全局采用的 IRF 链路负载分担模式。

```
<Sysname> display irf-port load-sharing mode
irf-port Load-Sharing Mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

显示非缺省情况下全局采用的 IRF 链路负载分担模式。

```
<Sysname> display irf-port load-sharing mode
irf-port Load-Sharing Mode:
destination-mac address, source-mac address
```

显示缺省情况下 IRF 端口 1/2 下采用的负载分担模式。

```
<Sysname> display irf-port load-sharing mode irf-port 1/1
irf-port Load-Sharing Mode:
Layer 2 traffic: packet type-based sharing
Layer 3 traffic: packet type-based sharing
```

显示非缺省情况下 IRF 端口 1/2 下采用的负载分担模式。

```
<Sysname> display irf-port load-sharing mode irf-port 1/2
irf-port 1/2 Load-Sharing Mode:
destination-mac address, source-mac address
```

显示所有 IRF 端口下分别采用的负载分担模式。

```
<Sysname> display irf-port load-sharing mode irf-port
irf-port 1/2 Load-Sharing Mode:
destination-ip address, source-ip address
irf-port 2/1 Load-Sharing Mode:
Layer 2 traffic: destination-mac address, source-mac address
Layer 3 traffic: destination-ip address, source-ip address
```

表1-5 display irf-port load-sharing mode 命令显示信息描述表

字段	描述
irf-port Load-Sharing Mode	全局采用的IRF链路负载分担类型： <ul style="list-style-type: none">缺省情况下，为设备缺省的 IRF 链路负载分担类型非缺省情况下显示：用户配置后采用的 IRF 链路负载分担类型
irf-port1/2 Load-Sharing Mode	IRF端口1/2下采用的负载分担类型： <ul style="list-style-type: none">缺省情况下显示：全局采用的负载分担类型非缺省情况下显示：用户配置后采用的负载分担类型
Layer 2 traffic: destination-mac address, source-mac address	二层报文缺省采用的负载分担类型：按照源MAC地址和目的MAC地址进行负载分担

字段	描述
Layer 3 traffic: destination-ip address, source-ip address	三层报文缺省采用的负载分担类型：按照源IP地址和目的IP地址进行负载分担
MPLS traffic : mpls-label1, mpls-label2, mpls-label3	MPLS报文缺省采用的负载分担类型：按照第1~3层的MPLS标签进行负载分担
destination-mac address, source-mac address	用户配置后采用的负载分担类型：按照源MAC地址和目的MAC地址进行负载分担（此字段的显示内容与用户的配置相关）

1.1.6 display mad

display mad 命令用来显示 MAD 配置信息。

【命令】

```
display mad [ verbose ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
context-admin
context-operator
```

【参数】

verbose: 显示 MAD 详细配置信息。如果不指定该参数，则显示简要配置信息。

【举例】

显示 MAD 简要配置信息。

```
<Sysname> display mad
MAD ARP disabled.
MAD ND disabled.
MAD LACP enabled.
MAD BFD enabled.
```

显示 MAD 详细配置信息。

```
<Sysname> display mad verbose
Multi-active recovery state: No
Excluded ports (user-configured):
  GigabitEthernet1/0/1
  GigabitEthernet2/0/1
Excluded ports (system-configured):
  GigabitEthernet1/0/2
  GigabitEthernet2/0/2
MAD ARP disabled.
MAD ND disabled.
MAD LACP enabled interface: Route-Aggregation2
```

```

MAD status                : Normal
Member ID      Port      MAD status
1              GigabitEthernet1/0/3    Normal
2              GigabitEthernet2/0/3    Normal
MAD BFD enabled interface: Route-Aggregation2
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

```

表1-6 display mad 命令显示信息描述表

字段	描述
MAD ARP disabled.	ARP MAD检测功能未开启 如本功能已开启，则显示为MAD ARP enabled
MAD ND disabled.	ND MAD检测功能未开启 如本功能已开启，则显示为MAD ND enabled
MAD LACP enabled.	LACP MAD检测功能已开启 如本功能未开启，则显示为MAD LACP disabled
MAD BFD enabled.	BFD MAD检测功能已开启 如本功能未开启，则显示为MAD BFD disabled
Multi-active recovery state	当前IRF是否被MAD功能设置为Recovery状态： <ul style="list-style-type: none"> • Yes: IRF 处于 Recovery 状态，当一个 IRF 分裂为多个 IRF 后，将发生多 Active 冲突，选举失败的 IRF 进入 Recovery 状态，该状态下的 IRF 会自动关闭所有非保留的业务接口 • No: IRF 没有处于 Recovery 状态
Excluded ports (user-configured)	用户配置的保留接口
Excluded ports (system-configured)	系统默认保留的接口（不需要用户配置，自动保留），包括： <ul style="list-style-type: none"> • IRF 物理端口 • 系统自动保留的二层聚合接口的成员接口。当用户将二层聚合接口配置为保留接口时，其成员接口自动为系统保留接口 • 系统自动保留的三层聚合接口的成员接口。当用户将三层聚合接口配置为保留接口时，其成员接口自动为系统保留接口
MAD ARP enabled interface:	开启了ARP MAD检测功能的接口 如ARP MAD检测功能未开启，则显示为MAD ARP disabled.
MAD ND enabled interface:	开启了ND MAD检测功能的接口 如ND MAD检测功能未开启，则显示为MAD ND disabled.
MAD LACP enabled interface	开启了LACP MAD检测功能的接口 如LACP MAD检测功能未开启，则显示为MAD LACP disabled.

字段	描述
MAD status	LACP MAD的工作状态： <ul style="list-style-type: none"> • Normal: LACP MAD 工作状态正常 • Faulty: LACP MAD 工作状态不正常，需要检查接口状态、中间设备是否支持 LACP MAD、以及聚合接口的成员端口是否分布到所有成员设备上
Member ID Port MAD status	LACP MAD详细信息： <ul style="list-style-type: none"> • Member ID: IRF 中的成员设备编号 • Port: 开启了 LACP MAD 的聚合组中的成员端口 • MAD status: 该成员端口的 LACP MAD 工作状态，Normal 表示正常，Faulty 表示不正常
MAD BFD enabled interface:	开启了BFD MAD的三层接口 如BFD MAD检测功能未开启，则显示为MAD BFD disabled.
MAD status	BFD MAD的工作状态： <ul style="list-style-type: none"> • Normal: BFD MAD 工作状态正常 • Faulty: BFD MAD 工作状态不正常，需要检查 BFD MAD 链路的连通状态 • N/A: 无法判断 BFD MAD 工作状态，在使用管理以太网口实现 BFD MAD 检测时可能出现此信息
Member ID MAD IP address Neighbor MAD status	BFD MAD详细信息： <ul style="list-style-type: none"> • Member ID: IRF 中的成员设备编号 • MAD IP address: 各成员设备对应的 MAD IP 地址 • Neighbor: 邻居设备的成员编号 • MAD status: IRF 设备成员到邻居成员的 BFD MAD 工作状态，Normal 表示正常，Faulty 表示不正常

1.1.7 easy-irf

easy-irf 命令用于快速配置 IRF。

【命令】

```

easy-irf [ member member-id [ renumber new-member-id ] domain domain-id
[ priority priority ] [ irf-port1 interface-list1 ] [ irf-port2
interface-list2 ] ]

```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member *member-id*: 表示设备当前的成员编号，取值范围为 1~2。

renumber new-member-id: 表示新成员编号，取值范围为 1~2。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。如果不指定该参数，则表示不修改成员编号。

domain domain-id: 表示设备所属的 IRF 域编号，*domain-id* 的取值范围为 0~4294967295。同一 IRF 中的成员设备应配置相同的域编号。

priority priority: 表示 IRF 成员的优先级，*priority* 的取值范围为 1~32。优先级值越大表示优先级越高，优先级高的设备竞选时成为主设备的可能性越大。

irf-port1 interface-list1: 表示与 IRF 端口 1 绑定的 IRF 物理端口。表示方式为 *interface-list1* = { *interface-type interface-number* }&<1-2>。其中 *interface-type interface-number* 表示接口类型和接口编号。&<1-2>表示前面的参数最多可以输入 2 次。

irf-port2 interface-list2: 表示与 IRF 端口 2 绑定的 IRF 物理端口。表示方式为 *interface-list2* = { *interface-type interface-number* }&<1-2>。其中 *interface-type interface-number* 表示接口类型和接口编号。&<1-2>表示前面的参数最多可以输入 2 次。一个物理端口只能与一个 IRF 端口绑定。

设备各款型对于本节所描述的参数支持情况有所不同，详细差异信息如下：

型号	参数	描述
L5030/L5060/L5080/L5000-E	n	8
L5000-C/L5000-S		8
L5000-AK535		8
L1000-C/L1000-S/L1000-M/L1000-E		8
L1000-AK310/L1000-AK320/L1000-AK330		8
L100-C		不支持
LSU1ADECEA0/LSWM1ADED0/LSQM1ADEDSC0		LSU1ADECEA0/LSWM1ADED0: 2 LSQM1ADEDSC0: 1

【使用指导】

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。

多次执行本命令时，生效情况如下：

- 多次执行本命令来修改域编号或优先级时，最近一次执行的命令生效。
- 多次执行本命令来修改 IRF 物理端口时，本次配置的端口会与之前已配置的端口同时生效。

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，逗号前后不能有空格。

如需删除现有的 IRF 物理端口配置，需要在 IRF 端口视图下，执行 **undo port group interface** 命令。

更多配置要求，请参见“虚拟化技术配置指导”中的“IRF”。

【举例】

通过非交互模式配置成员设备 2 的新成员编号为 1，域编号为 10，优先级为 10，IRF 端口 1 和 Ten-GigabitEthernet2/0/1 和 Ten-GigabitEthernet2/0/2 绑定。

```
<Sysname> system-view
[Sysname] easy-irf member 2 renumber 1 domain 10 priority 10 irf-port1 ten-gigabitethernet
2/0/1 ten-gigabitethernet 2/0/2
*****
Configuration summary for member 2
IRF new member ID: 1
IRF domain ID      : 10
IRF priority       : 10
IRF-port 1        : Ten-GigabitEthernet2/0/1, Ten-GigabitEthernet2/0/2
IRF-port 2        : Disabled
*****
Are you sure to use these settings to set up IRF? [Y/N] y
Starting to configure IRF...
Configuration succeeded.
The device will reboot for the new member ID to take effect. Continue? [Y/N] y
```

通过交互模式配置成员设备 2 的新编号为 1，域编号为 10，优先级为 10，IRF 端口 1 和 Ten-GigabitEthernet2/0/1 和 Ten-GigabitEthernet2/0/2 绑定。

```
<Sysname> system-view
[Sysname] easy-irf
*****
Welcome to use easy IRF.
To skip the current step, enter a dot sign (.).
To return to the previous step, enter a minus sign (-).
To use the default value (enclosed in []) for each parameter, press Enter without entering a value.
To quit the setup procedure, press CTRL+C.
*****
Select a member by its ID <2> [2]:2
Specify a new member ID <1~10> [1]: 1
Specify a domain ID <0~4294967295> [0]: 10
Specify a priority <1~32> [1]: 10
Specify IRF-port 1 bindings (a physical interface or a comma-separated physical interface list)[Disabled]: ten-gigabitethernet2/0/1,ten-gigabitethernet2/0/2
Specify IRF-port 2 bindings (a physical interface or a comma-separated physical interface list)[Disabled]:
*****
Configuration summary for member 2
IRF new member ID: 1
IRF domain ID      : 10
```

```
IRF priority      : 10
IRF-port 1       : Ten-GigabitEthernet2/0/1, Ten-GigabitEthernet2/0/2
IRF-port 2       : Disabled
*****
Are you sure to use these settings to set up IRF? [Y/N] y
Starting to configure IRF...
Configuration succeeded.
The device will reboot for the new member ID to take effect. Continue? [Y/N] y
```

1.1.8 irf auto-update enable

irf auto-update enable 命令用来开启 IRF 启动文件自动加载功能。

undo irf auto-update enable 命令用来关闭 IRF 启动文件自动加载功能。

【命令】

```
irf auto-update enable
undo irf auto-update enable
```

【缺省情况】

IRF 启动文件的自动加载功能处于开启状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启启动文件自动加载功能后，当新加入 IRF 的设备和主设备的软件版本不同时，新加入的设备会自动同步主设备的软件版本，再重新加入 IRF。为了能够成功进行自动加载，请确保从设备存储介质上有足够的空闲空间用于存放 IRF 的启动文件。如果从设备存储介质上空闲空间不足，该设备将自动删除当前启动文件来再次尝试加载；如果空闲空间仍然不足，该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 **BootWare** 菜单，删除一些不重要的文件后，再将设备重新加入 IRF。

【举例】

```
# 开启启动文件自动加载功能。
<Sysname> system-view
[Sysname] irf auto-update enable
```

1.1.9 irf domain

irf domain 命令用来配置 IRF 域编号。

undo irf domain 命令用来恢复缺省情况。

【命令】

```
irf domain domain-id
undo irf domain
```

【缺省情况】

IRF 的域编号为 0。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

domain-id: IRF 的域编号，取值范围为 0~4294967295。

【使用指导】

为了适应各种组网应用，同一个网络里可以部署多个 IRF。多个 IRF 之间使用不同的域编号以示区别。

如果 LACP MAD、ARP MAD、或 ND MAD 组网的中间设备本身也是一个 IRF 系统，则必须配置该命令确保 IRF 和中间设备的 IRF 域编号不同，否则可能造成检测异常，甚至导致业务中断。

IRF 中的所有成员设备都共用这个 IRF 域编号。在 IRF 设备上使用 **irf domain**、**mad enable**、**mad arp enable**、**mad nd enable** 命令均可修改全局 IRF 域编号，最新的配置生效。请按照网络规划来修改 IRF 域编号，不要随意修改。

【举例】

```
# 配置 IRF 的域编号为 10。  
<Sysname> system-view  
[Sysname] irf domain 10
```

1.1.10 irf mac-address persistent

irf mac-address persistent 命令用来配置 IRF 桥 MAC 的保留时间。

undo irf mac-address persistent 命令用来配置 IRF 桥 MAC 不保留，立即变化。

【命令】

```
irf mac-address persistent { always | timer }  
undo irf mac-address persistent
```

【缺省情况】

IRF 桥 MAC 保留 6 分钟。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

always: 配置 IRF 桥 MAC 永久保留。如果配置了 MAC 地址永久保留，则无论 IRF 桥 MAC 拥有者是否离开 IRF，IRF 桥 MAC 始终保持不变。

timer: 配置 IRF 桥 MAC 的保留时间为 6 分钟。如果配置了桥 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 分钟内不变化。如果 IRF 桥 MAC 拥有者在 6 分钟内重新又加入 IRF，则 IRF 桥 MAC 不会变化。如果 6 分钟后 IRF 桥 MAC 拥有者没有回到 IRF，则会使用 IRF 当前主设备的桥 MAC 作为 IRF 桥 MAC。

【使用指导】

IRF 桥 MAC 保留时间是指在桥 MAC 拥有者离开 IRF 后，IRF 可以继续使用当前桥 MAC 的时间。如果配置了 MAC 地址不保留，立即变化，当 IRF 桥 MAC 拥有者离开 IRF 时，系统立即会使用 IRF 中当前主设备的桥 MAC 做 IRF 桥 MAC。

当使用 ARP MAD/ND MAD 和 MSTP 组网时，需要将 IRF 配置为 MAC 地址立即改变，即配置 **undo irf mac-address persistent** 命令，以避免流量中断。

当使用链型拓扑搭建 IRF，且 IRF 与其他设备之间有聚合链路存在时，如果需要重启主设备，请不要使用 **undo irf mac-address persistent** 命令配置 IRF 的桥 MAC 立即变化，否则可能会导致数据传输的延时甚至丢包。

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。

缺省情况下，IRF 的桥 MAC 为 IRF 中当前主设备的桥 MAC。

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。

【举例】

```
# 配置 IRF 的桥 MAC 保留时间为永久保留。
<Sysname> system-view
[Sysname] irf mac-address persistent always
```

1.1.11 irf member description

irf member description 命令用来配置 IRF 中成员设备的描述信息。

undo irf member description 命令用来恢复缺省情况。

【命令】

```
irf member member-id description text
undo irf member member-id description
```

【缺省情况】

未配置成员设备的描述信息。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member-id: 表示设备在 IRF 中的成员编号。

text: 设备的描述信息，为 1~127 个字符的字符串。

【举例】

```
# 配置成员设备 1 的描述信息为 F1Num001。  
<Sysname> system-view  
[Sysname] irf member 1 description F1Num001
```

1.1.12 irf member priority

irf member priority 命令用来配置 IRF 中成员设备的优先级。
undo irf member priority 命令用来恢复缺省情况。

【命令】

```
irf member member-id priority priority  
undo irf member member-id priority
```

【缺省情况】

设备的成员优先级均为 1。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member-id: 表示设备在 IRF 中的成员编号，取值范围是 1~2。

priority: 表示优先级，取值范围为 1~32。优先级值越大表示优先级越高，优先级高的设备竞选时成为主设备的可能性越大。

【使用指导】

本命令的配置会影响成员设备在下次选举中的角色，但不会触发选举。

【举例】

```
# 配置 IRF 中成员编号为 2 的设备的优先级为 32。  
<Sysname> system-view  
[Sysname] irf member 2 priority 32
```

1.1.13 irf member renumber

irf member renumber 命令用来配置设备的成员编号。
undo irf member renumber 命令用来取消成员编号的设置。

【命令】

```
irf member member-id renumber new-member-id  
undo irf member member-id renumber
```

【缺省情况】

设备的成员编号是 1。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member-id: 表示设备在 IRF 中的成员编号，取值范围是 1~2。

new-member-id: 表示修改后的成员编号，取值范围 1~2。

【使用指导】



注意

在 IRF 中以设备编号标志设备，配置 IRF 端口和优先级也是根据设备编号来配置的，所以，修改设备成员编号可能导致设备配置发生变化或者丢失，请慎重处理。

当新加入的设备的编号和 IRF 中已有成员设备的编号相同时，设备不能加入 IRF。此时，请使用该命令修改设备的成员编号后，重新加入 IRF。

H3C 建议您修改成员设备编号时勿配置两台成员设备编号互换。这样配置可能带来非预期的配置互换或数据丢失。例如配置成员设备 2 和 3 编号互换会引起对应接口下的配置也发生互换。

该配置需要重启 *member-id* 标识的设备才能生效。

undo irf member renumber 命令只能取消本次运行过程中配置的成员编号。设备重启后，设备的成员编号就变为 *new-member-id*，不能再取消，只能重新配置。

【举例】

配置 IRF 中设备（原成员编号为 1）的成员编号为 2。

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

```
[Sysname] irf member 1 renumber 2
```

```
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]y
```

如果要取消以上配置，使设备的成员编号仍然是 1，则可以执行以下命令：

```
[Sysname] undo irf member 1 renumber
```

```
Renumbering the member ID may result in configuration change or loss. Continue?[Y/N]y
```

如果配置 **irf member 1 renumber 2** 后，重启设备，则设备的成员编号会变为 2。此时，不能使用 **undo irf member 1 renumber** 恢复到编号 1，只能使用 **irf member 2 renumber 1** 重新配置。

1.1.14 irf-port

irf-port 命令用来进入 IRF 端口视图。

undo irf-port 用来取消 IRF 端口上的所有配置。

【命令】

```
irf-port member-id/irf-port-number
```

```
undo irf-port member-id/irf-port-number
```

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

member-id: 表示设备在 IRF 中的成员编号。

irf-port-number 表示 IRF 端口索引，取值为 1 时表示 IRF-port1，为 2 时表示 IRF-port2。

【使用指导】

在组建 IRF 前，必须进入 IRF 端口视图，并绑定 IRF 物理端口才能开启该 IRF 端口，从而进行 IRF 连接。

【举例】

进入 IRF 端口 2/1。

```
<Sysname> system-view
[Sysname] irf-port 2/1
[Sysname-irf-port2/1]
```

【相关命令】

- **port group interface**

1.1.15 irf-port global load-sharing mode

irf-port global load-sharing mode 命令用来配置全局 IRF 链路的负载分担模式。

undo irf-port global load-sharing mode 命令用来恢复缺省情况。

【命令】

```
irf-port global load-sharing mode { destination-ip | destination-mac |
source-ip | source-mac } *
undo irf-port global load-sharing mode
```

【缺省情况】

IRF 链路基于源目的 IP 来进行负载分担。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

destination-ip: 表示按报文的目的地 IP 地址进行负载分担。

destination-mac: 表示按报文的目的地 MAC 地址进行负载分担。

source-ip: 表示按报文的源 IP 地址进行负载分担。

source-mac: 表示按报文的源 MAC 地址进行负载分担。

【使用指导】

用户可以通过本命令配置全局的 IRF 链路负载分担模式，也可以通过 `irf-port load-sharing mode` 命令配置指定 IRF 端口的负载分担模式：

- 在系统视图的配置对所有 IRF 链路生效；
- 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 链路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。

多次执行本命令，最后一次执行的命令生效。

对于设备不支持的负载分担模式，系统将提示用户不支持。

【举例】

配置全局按照报文目的 MAC 地址进行负载分担。

```
<Sysname> system-view
[Sysname] irf-port global load-sharing mode destination-mac
```

【相关命令】

- `irf-port load-sharing mode`

1.1.16 irf-port load-sharing mode

`irf-port load-sharing mode` 命令用来配置端口下 IRF 链路的负载分担模式。

`undo irf-port load-sharing mode` 命令用来恢复缺省情况。

【命令】

```
irf-port load-sharing mode { destination-ip | destination-mac | source-ip |
source-mac } *
undo irf-port load-sharing mode
```

【缺省情况】

IRF 链路基于源目的 IP 来进行负载分担。

【视图】

IRF 端口视图

【缺省用户角色】

network-admin

【参数】

destination-ip: 表示按报文的目 IP 地址进行负载分担。

destination-mac: 表示按报文的目 MAC 地址进行负载分担。

source-ip: 表示按报文的源 IP 地址进行负载分担。

source-mac: 表示按报文的源 MAC 地址进行负载分担。

【使用指导】

在配置负载分担模式前，请先将 IRF 端口和 IRF 物理端口绑定。否则，负载分担模式将配置失败。用户可以通过本命令配置指定 IRF 端口的负载分担模式，也可以通过 `irf-port global load-sharing mode` 命令配置全局的 IRF 链路负载分担模式：

- 在系统视图的配置对所有 IRF 链路生效；
 - 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 链路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。
- 多次执行本命令，最后一次执行的命令生效。
- 对于设备不支持的负载分担模式，系统将提示用户不支持。

【举例】

配置按报文目的 MAC 地址实现 IRF 端口 1/2 下 IRF 链路的负载分担模式。

```
<Sysname> system-view
[Sysname] irf-port 1/2
[Sysname-irf-port1/2] irf-port load-sharing mode destination-mac
```

【相关命令】

- `irf-port global load-sharing mode`

1.1.17 irf-port-configuration active

`irf-port-configuration active` 命令用于来激活设备上所有 IRF 端口的配置。

【命令】

`irf-port-configuration active`

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

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。

系统启动，通过配置文件将 IRF 物理端口加入 IRF 端口，或者 IRF 形成后再加入新的 IRF 物理端口时，IRF 端口下的配置会自动激活不再需要使用该命令来激活。

【举例】

在 IRF 端口 1/2 状态为 DIS 的情况下，激活 IRF 端口的配置。

- IRF 端口状态为 DIS 表示 IRF 端口还没有与任何 IRF 物理端口绑定，所以，先配置绑定关系。绑定前需要先将 IRF 物理端口关闭，绑定后再将 IRF 物理端口激活。

```
<Sysname> system-view
[Sysname] interface ten-gigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] irf-port 1/2
[Sysname-irf-port1/2] port group interface Ten-GigabitEthernet 1/0/1
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
```

```

[Sysname-irf-port1/2] quit
[Sysname] interface ten-gigabitEthernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] undo shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
• 将当前配置保存到下次启动配置文件，以便 IRF 端口的配置在设备重启后能继续生效。
[Sysname] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/startup.cfg exists, overwrite? [Y/N]:y
Validating file. Please wait.....
Saved the current configuration to mainboard device successfully.
• 激活 IRF 端口的配置。
[Sysname] irf-port-configuration active

```

1.1.18 mad arp enable

mad arp enable 命令用来开启 ARP MAD 检测功能。

undo mad arp enable 用来关闭 ARP MAD 检测功能。

【命令】

```

mad arp enable
undo mad arp enable

```

【缺省情况】

ARP MAD 检测功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

```

network-admin
context-admin

```

【使用指导】

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

配置 ARP MAD 检测时，请注意表 1-7 所列配置注意事项。

表1-7 ARP MAD 检测配置注意事项

注意事项类别	使用限制和注意事项
ARP MAD检测VLAN	<ul style="list-style-type: none"> • 不允许在 Vlan-interface1 接口上开启 ARP MAD 检测功能 • 如果使用中间设备，需要进行如下配置： <ul style="list-style-type: none"> ◦ 在 IRF 设备和中间设备上，创建专用于 ARP MAD 检测的 VLAN ◦ 在 IRF 设备和中间设备上，将用于 ARP MAD 检测的物理接口添加到 ARP MAD 检测专用 VLAN 中 ◦ 在 IRF 设备上创建 ARP MAD 检测 VLAN 的 VLAN 接口 • 建议勿在 ARP MAD 检测 VLAN 上运行其它业务
ARP MAD配置指导	<p>如果使用中间设备，请确保满足如下要求：</p> <ul style="list-style-type: none"> • 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。关于生成树功能的详细介绍请参见“二层技术-以太网交换配置指导”中的“生成树” • 配置 IRF 的桥 MAC 地址保留时间为立即改变 • 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

执行 **mad arp enable** 命令时，系统会要求用户输入 IRF 域编号。如果继续使用当前编号，则直接按回车即可。

IRF 域编号是一个全局变量，在 IRF 设备上使用 **irf domain**、**mad enable**、**mad arp enable**、**mad nd enable** 命令均可修改全局 IRF 域编号，最新的配置生效。

【举例】

```
# 在 VLAN 接口 3 上启用 ARP MAD 检测功能。
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad arp enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

【相关命令】

- **irf domain**

1.1.19 mad bfd enable

mad bfd enable 命令用来开启 BFD MAD 检测功能。

undo mad bfd enable 用来关闭 BFD MAD 检测功能。

【命令】

```
mad bfd enable
undo mad bfd enable
```

【缺省情况】

BFD MAD 检测功能处于关闭状态。

【视图】

VLAN 接口视图

三层聚合接口视图

管理以太网口视图

【缺省用户角色】

network-admin

【使用指导】

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

使用 VLAN 接口进行 BFD MAD 检测时，请注意[表 1-8](#)所列配置注意事项。

表1-8 使用 VLAN 接口进行 BFD MAD 检测

注意事项类别	使用限制和注意事项
BFD MAD检测VLAN	<ul style="list-style-type: none">• 不允许在 Vlan-interface1 接口上开启 BFD MAD 检测功能• 如果使用中间设备，需要进行如下配置：<ul style="list-style-type: none">◦ 在 IRF 设备和中间设备上，创建专用于 BFD MAD 检测的 VLAN◦ 在 IRF 设备和中间设备上，将用于 BFD MAD 检测的物理接口添加到 BFD MAD 检测专用 VLAN 中◦ 在 IRF 设备上，创建 BFD MAD 检测 VLAN 的 VLAN 接口• 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 作为 BFD MAD 检测专用 VLAN• 用于 BFD MAD 检测的 VLAN 接口对应的 VLAN 中只能包含 BFD MAD 检测链路上的端口，请不要将其它端口加入该 VLAN。当某个业务端口需要使用 port trunk permit vlan all 命令允许所有 VLAN 通过时，请使用 undo port trunk permit 命令将用于 BFD MAD 的 VLAN 排除
BFD MAD检测VLAN的特性限制	<p>开启BFD检测功能的VLAN接口及VLAN内的物理端口只能专用于BFD检测，不允许运行其它业务</p> <ul style="list-style-type: none">• 开启 BFD 检测功能的 VLAN 接口只能配置 mad bfd enable 和 mad ip address 命令。如果用户配置了其它业务，可能会影响该业务以及 BFD 检测功能的运行• BFD MAD 检测功能与生成树功能互斥，在开启了 BFD MAD 检测功能的 VLAN 接口对应 VLAN 内的端口上，请不要开启生成树协议
BFD MAD IP地址	<ul style="list-style-type: none">• 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• 为不同成员设备配置同一网段内的不同 MAD IP 地址

使用管理用以太网口进行 BFD MAD 检测时，请注意[表 1-9](#)所列配置注意事项。

表1-9 使用管理用以太网口进行 BFD MAD 检测

注意事项类别	使用限制和注意事项
管理用以太网口	将IRF中所有成员设备的管理用以太网口连接到同一台中间设备的普通以太网端口上
BFD MAD检测VLAN	<ul style="list-style-type: none"> • 将中间设备上与 IRF 成员设备相连的端口配置在一个 VLAN 内（IRF 设备的管理以太网口不需要此配置） • 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 作为 BFD MAD 检测专用 VLAN • 请确保中间设备上 BFD MAD 检测 VLAN 中仅包含用于 BFD 检测的端口
MAD IP地址	<ul style="list-style-type: none"> • 在管理用以太网口使用 mad ip address 命令配置 MAD IP 地址，请勿使用 ip address 命令配置 • 为不同成员设备配置同一网段内的不同 MAD IP 地址

使用三层聚合接口进行 BFD MAD 检测时，请注意[表 1-10](#)所列配置注意事项。

表1-10 使用三层聚合接口进行 BFD MAD 检测

注意事项类别	使用限制和注意事项
三层聚合接口配置	<ul style="list-style-type: none"> • 必须使用静态聚合模式的三层聚合接口（聚合接口缺省工作在静态聚合模式） • 如果网络中存在多个 IRF，在配置 BFD MAD 时，各 IRF 必须使用不同的三层聚合接口做 BFD MAD 检测专用的三层接口 • 聚合成员端口的个数不能超过聚合组最大选中端口数。否则，由于超出聚合组最大选中端口数的成员端口无法成为选中端口，会使 BFD MAD 无法正常工作，工作状态显示为 Faulty
BFD MAD检测VLAN	如果使用中间设备，请将中间设备上用于BFD MAD检测的物理接口添加到同一个VLAN中。中间设备上的端口不用加入聚合组
BFD MAD检测VLAN的特性限制	开启BFD检测功能的接口只能配置 mad bfd enable 和 mad ip address 命令。如果用户配置了其它业务，可能会影响该业务以及BFD检测功能的运行
MAD IP地址	<ul style="list-style-type: none"> • 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 • 为不同成员设备配置同一网段内的不同 MAD IP 地址

【举例】

在三层聚合接口 3 上启用 BFD MAD 检测功能。

```
<Sysname> system-view
[Sysname] interface route-aggregation 3
[Sysname-Route-Aggregation 3] mad bfd enable
```

1.1.20 mad enable

mad enable 命令用来开启 LACP MAD 方式检测功能。

undo mad enable 用来关闭 LACP MAD 方式检测功能。

【命令】

mad enable

undo mad enable

【缺省情况】

LACP MAD 检测功能处于关闭状态。

【视图】

聚合接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

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

LACP MAD 检测方式需要使用 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。请在动态聚合接口下开启 LACP MAD 方式检测功能。聚合接口创建后，可使用 **link-aggregation mode dynamic** 命令将该接口配置为动态接口。

在 LACP 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。

为了防止 IRF 级联组网时，本 IRF 的 MAD 检测报文转发到邻居 IRF 中影响邻居 IRF 的 MAD 检测，执行 **mad enable** 命令时，系统会要求用户输入 IRF 域编号。如果继续使用当前编号，则直接按回车即可。

IRF 域编号是一个全局变量，在 IRF 设备上使用 **irf domain**、**mad enable**、**mad arp enable**、**mad nd enable** 命令均可修改全局 IRF 域编号，最新的配置生效。

【举例】

在二层动态聚合接口 1 下启用 LACP MAD 方式检测功能。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
[Sysname-Bridge-Aggregation1] link-aggregation mode dynamic
[Sysname-Bridge-Aggregation1] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
MAD LACP only enable on dynamic aggregation interface.
```

在三层动态聚合接口 1 下启用 LACP MAD 方式检测功能。

```
<Sysname> system-view
[Sysname] interface route-aggregation 1
[Sysname-Route-Aggregation1] link-aggregation mode dynamic
```

```
[Sysname-Route-Aggregation1] mad enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
MAD LACP only enable on dynamic aggregation interface.
```

【相关命令】

- `irf domain`

1.1.21 mad exclude interface

`mad exclude interface` 命令用来配置保留接口。

`undo mad exclude interface` 命令用来将接口配置为非保留接口。

【命令】

```
mad exclude interface interface-type interface-number  
undo mad exclude interface interface-type interface-number
```

【缺省情况】

缺省情况下，设备进入 **Recovery** 状态时会自动关闭本设备上除了系统保留接口以外的所有业务接口。

【视图】

系统视图

【缺省用户角色】

```
network-admin  
context-admin
```

【参数】

`interface-type interface-number`: 表示接口类型和接口编号。

【使用指导】

设备进入 **Recovery** 状态时会自动关闭本设备上除系统保留接口外的所有的业务接口。如果希望 **Recovery** 状态 IRF 上有特殊用途的接口（比如 **Telnet** 登录接口）保持 **UP** 状态，可以将其配置为保留接口。建议您仅将 **Telnet** 登录接口配置为保留接口。

当分裂的 IRF 恢复时，处于 **Recovery** 状态的设备重启后重新加入 IRF，被 **MAD** 关闭的接口会自动恢复到正常状态。

在 **MAD** 故障未修复，接口没有自动恢复时，如果需要让 **Recovery** 状态 IRF 中的成员设备及其接口恢复到正常状态（原因可能是 **Active** 状态的 IRF 出现故障），可以在 **Recovery** 状态 IRF 上执行 `mad restore` 命令。

【举例】

配置 **GigabitEthernet1/0/1** 为保留接口，即当设备进入 **Recovery** 状态时，该接口不会被关闭。

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

【相关命令】

- `mad restore`

1.1.22 mad ip address

`mad ip address` 命令用来为成员设备配置 MAD IP 地址。

`undo mad ip address` 命令用来删除成员设备的 MAD IP 地址。

【命令】

```
mad ip address ip-address { mask | mask-length } member member-id
```

```
undo mad ip address ip-address { mask | mask-length } member member-id
```

【缺省情况】

没有为成员设备配置 MAD IP 地址。

【视图】

VLAN 接口视图

三层聚合接口视图

管理用以太网口视图

【缺省用户角色】

network-admin

【参数】

ip-address: 接口的 IP 地址，为点分十进制格式。

mask: 接口 IP 地址相应的子网掩码，为点分十进制格式。

mask-length: 子网掩码长度，即掩码中连续“1”的个数，取值范围为 0~32。

member *member-id*: 表示成员在 IRF 中的成员编号。

【使用指导】

当使用 BFD MAD 检测时，IRF 中的所有成员设备都需要配置 MAD IP 地址，这些 IP 地址与成员编号绑定，且必须为同一网段。只有主设备的 MAD IP 地址生效，从设备的 MAD IP 地址不生效。当 IRF 链路分裂时，IRF 中的原从设备变为主设备，配置的 MAD IP 地址生效，BFD 会话被激活，设备将认为在网络中检测到存在配置冲突的 IRF。

在用于 BFD MAD 检测的接口不要配置其它 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。

【举例】

配置三层聚合接口 3 在成员设备 1 上的 MAD IP 地址。

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

```
[Sysname] interface route-aggregation 3
```

```
[Sysname-Route-Aggregation 3] mad ip address 192.168.0.1 255.255.255.0 member 1
```

配置三层聚合接口 3 在成员设备 2 上的 MAD IP 地址。

```
[Sysname-Route-Aggregation 3] mad ip address 192.168.0.2 255.255.255.0 member 2
```


【相关命令】

- `mad bfd enable`

1.1.23 mad nd enable

`mad nd enable` 命令用来开启 ND MAD 检测功能。

`undo mad nd enable` 用来关闭 ND MAD 检测功能。

【命令】

`mad nd enable`

`undo mad nd enable`

【缺省情况】

ND MAD 检测功能处于关闭状态。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

context-admin

【使用指导】

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

VLAN 1 不能用于 MAD 检测，因此，不能在 VLAN 接口 1 下开启 ND MAD 检测功能。

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。

为了防止 IRF 级联组网时，本 IRF 的 MAD 检测报文转发到邻居 IRF 中影响邻居 IRF 的 MAD 检测，执行 `mad nd enable` 命令时，系统会要求用户输入 IRF 域编号。如果继续使用当前编号，则直接按回车即可。

IRF 域编号是一个全局变量，在 IRF 设备上使用 `irf domain`、`mad enable`、`mad arp enable`、`mad nd enable` 命令均可修改全局 IRF 域编号，最新的配置生效。

【举例】

在 VLAN 接口 3 上启用 ND MAD 检测功能。

```
<Sysname> system-view
[Sysname] interface vlan-interface 3
[Sysname-Vlan-interface3] mad nd enable
You need to assign a domain ID (range: 0-4294967295)
[Current domain is: 0]: 1
The assigned domain ID is: 1
```

【相关命令】

- `irf domain`

1.1.24 mad restore

mad restore 命令用来将设备从 **Recovery** 状态恢复到正常状态。

【命令】

```
mad restore
```

【视图】

系统视图

【缺省用户角色】

```
network-admin
```

【使用指导】

当 IRF 链路故障会导致多 **Active** 冲突，原 IRF 分裂为多个 IRF，为了防止网络中配置冲突，IRF 系统会通过多 **Active** 检测机制，让其中一个 IRF 继续正常工作，其它 IRF 的状态修改为 **Recovery**（处于该状态的 IRF 不能处理业务报文）。如果继续正常工作的 IRF 也发生故障不能工作，此时可以通过本命令将处于 **Recovery** 状态的 IRF 恢复到正常工作状态接替原 IRF 工作，以便保证业务尽量少受影响。

【举例】

将 IRF 从 **Recovery** 状态恢复到正常状态。

```
<Sysname> system-view
[Sysname] mad restore
This command will restore the device from multi-active conflict state. Continue? [Y/N]:Y
Restoring from multi-active conflict state, please wait...
```

1.1.25 port group interface

port group interface 命令用来绑定设备的 IRF 端口和 IRF 物理端口，在 IRF 端口上第一次绑定 IRF 物理端口的同时相当于开启了 IRF 端口的 IRF 功能。

undo port group interface 命令用来取消设备的 IRF 端口和 IRF 物理端口的绑定关系。

【命令】

```
port group interface interface-type interface-number [ mode { enhanced |
extended | normal } ]
undo port group interface interface-name
```

【缺省情况】

IRF 端口创建后未与任何物理端口绑定。

【视图】

IRF 端口视图

【缺省用户角色】

```
network-admin
```

【参数】

interface-type interface-number: 表示 IRF 物理端口的类型和编号。

interface-name: IRF 物理端口的名称, 格式为 *interface-type+interface-number*, *interface-type* 与 *interface-number* 之间没有空格。

【使用指导】

多次执行该命令可以将同一 IRF 端口与多个 IRF 物理端口绑定, 具体数值如下。

设备各款型对于本节所描述的参数支持情况有所不同, 详细差异信息如下:

型号	参数	描述
L5030/L5060/L5080/L5000-E	IRF可绑定的 最多物理端口 数	8
L5000-C/L5000-S		8
L5000-AK535		8
L1000-C/L1000-E/L1000-M/L1000-S		8
L1000-AK310/L1000-AK320/L1000-AK330		8
L100-C		不支持
LSU1ADECEA0/LSWM1ADED0/LSQM1ADEDSC0		LSU1ADECEA0/LSWM1ADED0: 2 LSQM1ADEDSC0: 1

需要先使用 **shutdown** 命令关闭相应的物理端口, 才能将 IRF 端口与物理端口绑定或解绑定。在绑定或解绑定的操作完成后, 需要执行 **undo shutdown** 命令开启物理端口。

配置本命令后, 即便热插拔接口板导致绑定的 IRF 物理端口不存在了, 但绑定关系仍然存在, 使用 **undo port group interface** 命令可以取消绑定关系。

有些接口板出厂时已将接口分组, 同一组内的接口只能都作为 IRF 物理端口, 或者都不作为 IRF 物理端口。当将某组中的一个接口和 IRF 端口绑定时, 系统要求先将该组中的所有接口都关闭, 否则, 绑定失败; 当绑定后, 将其中一个接口激活时, 系统会判断该组中的其它接口是否已经和 IRF 端口绑定 (可以绑定到同一 IRF 端口, 也可以绑定到不同 IRF 端口), 如果未绑定, 则不允许激活。

更多配置要求, 请参见“虚拟化技术配置指导”中的“IRF”。

【举例】

将成员设备 1 的 IRF 物理端口 Ten-GigabitEthernet1/0/1 和 IRF 端口 IRF-port1/2 绑定。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] shutdown
[Sysname-Ten-GigabitEthernet1/0/1] quit
[Sysname] irf-port 1/2
[Sysname-irf-port1/2] port group interface ten-gigabitethernet 1/0/1
[Sysname-irf-port1/2] quit
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] undo shutdown
```

【相关命令】

- **irf-port**

目 录

1 Context	1-1
1.1 Context 命令	1-1
1.1.1 allocate interface	1-1
1.1.2 allocate vlan	1-2
1.1.3 capability security-policy-rule maximum	1-3
1.1.4 capability session maximum	1-4
1.1.5 capability session rate	1-5
1.1.6 capability throughput	1-6
1.1.7 context	1-6
1.1.8 context start	1-7
1.1.9 context-capability inbound broadcast single	1-8
1.1.10 context-capability inbound broadcast total	1-9
1.1.11 context-capability inbound drop-logging enable	1-10
1.1.12 context-capability inbound multicast single	1-10
1.1.13 context-capability inbound multicast total	1-11
1.1.14 context-capability inbound unicast single	1-12
1.1.15 context-capability inbound unicast total	1-13
1.1.16 description	1-14
1.1.17 display context	1-14
1.1.18 display context capability	1-15
1.1.19 display context capability inbound broadcast	1-17
1.1.20 display context capability inbound multicast	1-18
1.1.21 display context capability inbound unicast	1-19
1.1.22 display context configuration	1-20
1.1.23 display context interface	1-21
1.1.24 display context online-users sslvpn	1-22
1.1.25 display context resource	1-23
1.1.26 display context statistics	1-24
1.1.27 display context vlan	1-26
1.1.28 hardware fast-forwarding vpc enable	1-27
1.1.29 limit-resource cpu	1-28
1.1.30 limit-resource disk	1-28
1.1.31 limit-resource memory	1-29

1.1.32 reset context capability inbound broadcast	1-30
1.1.33 reset context capability inbound multicast.....	1-30
1.1.34 reset context capability inbound unicast	1-31
1.1.35 switchto context	1-31
1.1.36 tar context log	1-32

1 Context

本特性的支持情况与设备型号有关，请以设备的实际情况为准。

型号	说明
L5030/L5060/L5080/L5000-E	支持
L5000-C/L5000-S	支持
L5000-AK535	支持
L1000-C/L1000-S/L1000-M/L1000-E	支持
L1000-AK310/L1000-AK320/L1000-AK330	支持
L100-C	不支持
LSU1ADECEA0/LSWM1ADED0/LSQM1ADEDSC0	支持

1.1 Context命令

对于本文列出的命令，缺省 Context 均支持，非缺省 Context 只支持 **display context interface**、**context-capability inbound broadcast single**、**context-capability inbound broadcast single**、**context-capability inbound unicast single** 命令。

1.1.1 allocate interface

allocate interface 命令用来为 Context 分配接口。

undo allocate interface 命令用来取消为 Context 分配的接口。

【命令】

```
allocate interface { interface-type interface-number }&<1-24> [ share ]  
undo allocate interface { interface-type interface-number }&<1-24>  
allocate interface interface-type interface-number1 to interface-type interface-number2 [ share ]  
undo allocate interface interface-type interface-number1 to interface-type interface-number2
```

【缺省情况】

设备上的所有接口都属于缺省 Context，不属于任何非缺省 Context。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

`{ interface-type interface-number }<1-24>`: 表示给 Context 分配非连续的接口。
`interface-type interface-number` 表示接口类型和编号, <1-24>表示前面的参数最多可以输入 24 次。

`interface-type interface-number1 to interface-type interface-number2`: 表示给 Context 分配一组连续的接口。其中, `interface-type` 表示接口类型, `interface-number1` 表示起始接口的编号, `interface-number2` 表示结束接口的编号。起始接口和结束接口的类型必须相同, 并且处于同一接口板上, 否则将配置失败。

share: 表示接口是否共享。不指定该参数表示独占。

【使用指导】

- 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)。使用该方式分配的接口归多个 Context 所有、使用。在缺省 Context 内仍然存在该接口, 可执行接口支持的所有命令; 在分配给的非缺省 Context 内, 会新建同名接口, 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。



- 当设备运行在 IRF 模式时, 禁止将 IRF 物理端口分配给自定义 Context。
 - 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。
 - 逻辑接口仅支持共享方式分配, 物理接口支持独占和共享两种方式分配。
-

【举例】

将接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/3 以共享的方式分配给 context sub1。

```
<Sysname> system-view
[Sysname] context sub1
[Sysname-context-2-sub1] allocate interface gigabitethernet 1/0/1 gigabitethernet 1/0/3
share
```

1.1.2 allocate vlan

allocate vlan 命令用来为 Context 分配 VLAN。

undo allocate vlan 命令用来取消为 Context 分配的 VLAN。

【命令】

```
allocate vlan vlan-id<1-24>
undo allocate vlan vlan-id<1-24>
allocate vlan vlan-id1 to vlan-id2
undo allocate vlan vlan-id1 to vlan-id2
```

【缺省情况】

没有为 Context 分配 VLAN。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

vlan-id&<1-24>: 表示给 Context 分配非连续的 VLAN。*vlan-id* 表示 VLAN 的编号, &<1-24> 表示前面的参数最多可以输入 24 次。

vlan-id1 to vlan-id2: 表示给 Context 分配一组连续的 VLAN。其中, *vlan-id1* 表示起始 VLAN 的编号, *vlan-id2* 表示结束 VLAN 的编号。

【使用指导】

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, 可以通过本命令将设备上存在的除 VLAN 1 以外的静态 VLAN 分配给非缺省 Context。共享 VLAN 由多个 Context 共同所有。VLAN 被分配后, 用户须在缺省 Context 内对该 VLAN 配置, 非缺省 Context 内不能配置该 VLAN, 只能查看该 VLAN 的相关信息。
- 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。

【举例】

将 VLAN100 分配给 context sub1。

```
<Sysname> system-view
[Sysname] context sub1
[Sysname-context-2-sub1] allocate vlan 100
```

【相关命令】

- **display context vlan**

1.1.3 capability security-policy-rule maximum

capability security-policy-rule maximum 命令用来设置 Context 的安全策略规则总数限制。

undo capability security-policy-rule maximum 命令用来恢复缺省情况。

【命令】

```
capability security-policy-rule maximum max-number
undo capability security-policy-rule maximum
```

【缺省情况】

未对 Context 的安全策略规则总数进行限制。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

max-number: 表示 Context 内可配置的安全策略规则最大数目，取值范围为 1~4294967295。

【使用指导】

一个 Context 内可以配置多个安全策略规则。如果不加限制，会出现大量规则占用过多的内存的情况，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。

如果设置的最大值比当前存在的规则总数小，配置仍会成功，多出的规则不会删除，但不能新增规则。

【举例】

配置 Context 的安全策略规则数最多为 1000 条。

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability security-policy-rule maximum 1000
```

【相关命令】

- **display security-policy ip** (安全命令参考/安全策略)

1.1.4 capability session maximum

capability session maximum 命令用来设置 Context 的单播会话并发数限制。

undo capability session maximum 命令用来恢复缺省情况。

【命令】

```
capability session maximum max-number
undo capability session maximum
```

【缺省情况】

未对 Context 允许的单播会话并发数进行限制。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

max-number: 允许同时存在的最大单播会话数目，取值范围为 1~4294967295。

【使用指导】

如果一个 Context 建立了太多会话会导致其他 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 建立会话的数量，当会话总数达到限制值时，后续不能新建会话。

如果设置的最大值比当前存在的会话总数小，配置仍会成功，但不允许新建会话，且已经创建的会话不会被删除，直到已建立的会话通过老化机制使得会话总数低于配置的最大值后，系统才允许新建会话。

Context 会话并发数限制对本机流量不生效，例如：FTP、Telnet、SSH、HTTP 和 HTTP 类型的七层负载均衡等业务。

【举例】

配置 Context cnt2 上的单播会话并发数为 1000000。

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] capability session maximum 1000000
```

【相关命令】

- **context**
- **display session statistics**（安全命令参考/会话管理）

1.1.5 capability session rate

capability session rate 命令用来设置 Context 的会话新建速率限制。

undo capability session rate 命令用来恢复缺省情况。

【命令】

```
capability session rate max-value
undo capability session rate
```

【缺省情况】

未对 Context 允许的会话新建速率进行限制。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

max-value: 允许的会话新建速率最大值，单位为每秒会话个数。

【使用指导】

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，当会话新建速率达到限制值时，后续不能新建会话。

Context 会话新建速率限制对本机流量不生效，例如：FTP、Telnet、SSH、HTTP 和 HTTP 类型的七层负载均衡等业务。

【举例】

配置 Context cnt2 上的会话新建速率最大值为每秒 20000 个会话数。

```
<Sysname> system-view
[Sysname] context cnt2
```

```
[Sysname-context-2-cnt2] capability session rate 20000
```

【相关命令】

- **context**
- **display session statistics** (安全命令参考/会话管理)

1.1.6 capability throughput

capability throughput 命令用来设置 Context 出方向的吞吐量限制。

undo capability throughput 命令用来恢复缺省情况。

【命令】

```
capability throughput { kbps | pps } threshold  
undo capability throughput
```

【缺省情况】

各 Context 出方向不做吞吐量限制，按实际能力转发。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

kbps: 表示出方向吞吐量按每秒千比特计算。

pps: 表示出方向吞吐量按每秒报文数计算。

threshold: 表示吞吐量限制值，取值范围为 1000~100000000。

【举例】

配置名称为 cnt2 的 Context 的出方向吞吐量为 100000bps。

```
<Sysname> system-view  
[Sysname] context cnt2  
[Sysname-context-2-cnt2] capability throughput kbps 100000
```

配置名称为 cnt3 的 Context 的出方向吞吐量为 10000pps。

```
<Sysname> system-view  
[Sysname] context cnt3  
[Sysname-context-3-cnt3] capability throughput pps 10000
```

1.1.7 context

context 命令用来创建 Context，并进入 Context 视图。如果指定的 Context 已经存在，则直接进入 Context 视图。

undo context 命令用来删除指定 Context。

【命令】

```
context context-name [ id context-id ] [ vlan-unshared ]  
undo context context-name
```

【缺省情况】

存在缺省 Context，名称为 Admin，编号为 1。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

context-name: Context 的名称，为 1~15 个字符的字符串，区分大小写。

context-id: Context 的编号。不指定该参数时，系统会自动给 Context 分配一个当前空闲的最小编号。

vlan-unshared: 不和其它 Context 共享 VLAN。不指定该参数时，表示和其它 Context 共享 VLAN。

【使用指导】

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。
- 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 1~VLAN 4094。Context 各自使用和管理 VLAN，互不干扰。

【举例】

创建一个名称为 test 的 Context。

```
<Sysname> system-view
[Sysname] context test
[Sysname-context-2-test]
```

创建一个名称为 test，ID 为 2 的 Context。

```
<Sysname> system-view
[Sysname] context test id 2
[Sysname-context-2-test]
```

1.1.8 context start

context start 命令用来启动 Context。

undo context start 命令用来停止该 Context。

【命令】

```
context start [ force ]
undo context start [ force ]
```

【缺省情况】

未启动 Context。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

force: 强制启动/停止 Context。不指定该参数时，表示按正常程序启动 Context。

【使用指导】



停止 Context 会导致该 Context 的业务中断，以及登录该 Context 的用户自动退出，请谨慎使用。为避免 Context 的当前配置丢失，停止 Context 前请保存 Context 的配置。

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。

【举例】

```
# 启动 Context cnt2。
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] context start
```

1.1.9 context-capability inbound broadcast single

context-capability inbound broadcast single 命令用来配置单个 Context 入方向广播报文的速率限制。

undo context-capability inbound broadcast single 命令用来恢复缺省情况。

【命令】

```
context-capability inbound broadcast single pps threshold
undo context-capability inbound broadcast single
```

【缺省情况】

单个 Context 入方向广播报文限速速率的缺省值为广播报文总速率阈值除以使用共享接口 Context 的总数。

【视图】

系统视图

Context 视图

【缺省用户角色】

network-admin

【参数】

pps threshold: 入方向广播报文的速率阈值，取值范围为 1000~100000，单位为 pps。

【使用指导】

此功能仅对使用共享接口且处于 Active 状态的 Context 生效。

在系统视图下执行此命令是用来配置缺省 Context 入方向广播报文限速速率的阈值；在 Context 视图下执行此命令式用来配置非缺省 Context 入方向广播报文限速速率的阈值。

当广播报文总速率和单个 Context 入方向广播报文速率均达到各自的阈值后，发往此 Context 的广播报文会被设备丢弃，否则不会被丢弃。广播报文总速率限制由 **context-capability inbound broadcast total** 命令设置。

【举例】

配置缺省 Context 入方向广播报文的速率最大值为 10000pps。

```
<Sysname> system-view
[Sysname] context-capability inbound broadcast single pps 10000
```

配置 Context ctx1 入方向广播报文的速率最大值为 10000pps。

```
<Sysname> system-view
[Sysname] context ctx1
[Sysname-context-1-ctx1] context-capability inbound broadcast single pps 10000
```

【相关命令】

- **context-capability inbound broadcast total**

1.1.10 context-capability inbound broadcast total

context-capability inbound broadcast total 命令用来配置所有 Context 入方向广播报文的总速率限制。

undo context-capability inbound broadcast total 命令用来恢复缺省情况。

【命令】

```
context-capability inbound broadcast total pps threshold
undo context-capability inbound broadcast total
```

【缺省情况】

所有 Context 入方向广播报文总速率限制为 20000pps。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pps threshold: 入方向广播报文的总速率阈值，取值范围为 0，1000~100000，单位为 pps。取值为 0 时表示不限速。

【使用指导】

此功能仅对使用共享接口且处于 Active 状态的 Context 生效。

所有 Context 入方向广播报文总速率是指所有使用共享接口的 Context 接收广播报文的速率之和，简称“广播报文总速率”。

当广播报文总速率和单个 Context 入方向广播报文速率均达到各自的阈值后，发往此 Context 的广播报文会被设备丢弃，否则不会被丢弃。单个 Context 入方向广播报文速率由 **context-capability inbound broadcast single** 命令设置。

【举例】

配置所有 Context 入方向广播报文的总速率最大值为 10000pps。

```
<Sysname> system-view
[Sysname] context-capability inbound broadcast total pps 10000
```

【相关命令】

- **context-capability inbound broadcast single**

1.1.11 context-capability inbound drop-logging enable

context-capability inbound drop-logging enable 命令用来开启 Context 入方向报文限速丢包日志功能。

undo context-capability inbound drop-logging enable 命令用来关闭 Context 入方向报文限速丢包日志功能。

【命令】

```
context-capability inbound drop-logging enable
undo context-capability inbound drop-logging enable
```

【缺省情况】

Context 入方向报文限速丢包日志功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

开启此功能后，当 Context 接收到的广播报文或组播报文因达到系统设置的阈值而被丢弃时，设备将会对丢弃的报文生成日志信息。此日志信息将会被输出到信息中心模块处理，信息中心模块的配置将决定日志信息的发送规则和发送方向。有关信息中心的详细介绍，请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

开启 Context 入方向报文限速丢包日志功能。

```
<Sysname> system-view
[Sysname] context-capability inbound drop-logging enable
```

1.1.12 context-capability inbound multicast single

context-capability inbound multicast single 命令用来配置单个 Context 入方向组播报文的速率限制。

undo context-capability inbound multicast single 命令用来恢复缺省情况。

【命令】

```
context-capability inbound multicast single pps threshold
undo context-capability inbound multicast single
```

【缺省情况】

单个 Context 入方向组播报文限速速率的缺省值为组播报文总速率阈值除以使用共享接口 Context 的总数。

【视图】

系统视图
Context 视图

【缺省用户角色】

network-admin

【参数】

pps threshold: Context 入方向组播报文的速率阈值，取值范围为 1000~100000，单位为 pps。

【使用指导】

此功能仅对使用共享接口且处于 Active 状态的 Context 生效。

在系统视图下执行此命令是用来配置缺省 Context 入方向组播报文限速速率的阈值；在 Context 视图下执行此命令式用来配置非缺省 Context 入方向组播报文限速速率的阈值。

当组播报文总速率和单个 Context 入方向组播报文速率均达到各自的阈值后，发往此 Context 的组播报文会被设备丢弃，否则不会被丢弃。组播报文总速率限制由 **context-capability inbound multicast total** 命令设置。

【举例】

配置缺省 Context 入方向组播报文的限速速率是 10000pps。

```
<Sysname> system-view
[Sysname] context-capability inbound multicast single pps 10000
```

配置 Context ctx1 入方向组播报文的限速速率是 10000pps。

```
<Sysname> system-view
[Sysname] context ctx1
[Sysname-context-1-ctx1] context-capability inbound multicast single pps 10000
```

【相关命令】

- **context-capability inbound multicast total**

1.1.13 context-capability inbound multicast total

context-capability inbound multicast total 命令用来配置所有 Context 入方向组播报文的总速率限制。

undo context-capability inbound multicast total 命令用来恢复缺省情况。

【命令】

```
context-capability inbound multicast total pps threshold
undo context-capability inbound multicast total
```


【缺省情况】

所有 Context 入方向组播报文总速率限制为 0pps。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pps threshold: 入方向组播报文的总速率阈值，取值范围为 0，1000~100000，单位为 pps。取值为 0 时表示不限速。

【使用指导】

此功能仅对使用共享接口且处于 Active 状态的 Context 生效。

所有 Context 入方向组播报文总速率是指所有使用共享接口的 Context 接收组播报文的速率之和，简称“组播报文总速率”。

当组播报文总速率和单个 Context 入方向组播报文速率均达到各自的阈值后，发往此 Context 的组播报文会被设备丢弃，否则不会被丢弃。单个 Context 入方向组播报文速率由 **context-capability inbound multicast single** 命令设置。

【举例】

```
# 配置所有 Context 入方向组播报文的总速率最大值为 10000pps。  
<Sysname> system-view  
[Sysname] context-capability inbound multicast total pps 10000
```

【相关命令】

- **context-capability inbound multicast single**

1.1.14 context-capability inbound unicast single

context-capability inbound unicast single 命令用来配置单个 Context 入方向单播报文的 CPU 消耗率限制。

undo context-capability inbound unicast single 命令用来恢复缺省情况。

【命令】

```
context-capability inbound unicast single cpu-usage threshold  
undo context-capability inbound unicast single
```

【缺省情况】

单个 Context 入方向单播报文的 CPU 消耗率为单播报文的总 CPU 消耗率除以设备上所有 Context 的总数。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

cpu-usage threshold: 入方向单播报文的 CPU 消耗率阈值，取值范围为 1~100，单位为百分比。

【使用指导】

此功能对使用共享接口和独占接口且处于 Active 状态的 Context 均生效。

在系统视图下执行此命令是用来配置缺省 Context 入方向单播报文的 CPU 消耗率阈值；在 Context 视图下执行此命令式用来配置非缺省 Context 入方向单播报文的 CPU 消耗率阈值。

当单播报文的总 CPU 消耗率和单个 Context 入方向单播报文的 CPU 消耗率均达到各自的阈值后，发往此 Context 的单播报文会被设备丢弃，否则不会被丢弃。单播报文的总 CPU 消耗率由 **context-capability inbound unicast total** 命令设置。

【举例】

配置缺省 Context 入方向单播报文的 CPU 消耗率为 70%。

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

```
[Sysname] context-capability inbound unicast single cpu-usage 70
```

【相关命令】

- **context-capability inbound unicast total**

1.1.15 context-capability inbound unicast total

context-capability inbound unicast total 命令用来配置所有 Context 入方向单播报文的总 CPU 消耗率限制。

undo context-capability inbound unicast total 命令用来恢复缺省情况。

【命令】

```
context-capability inbound unicast total cpu-usage threshold
```

```
undo context-capability inbound unicast total
```

【缺省情况】

所有 Context 入方向单播报文的总 CPU 消耗率是 100%。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

cpu-usage threshold: 入方向单播报文的总 CPU 消耗率阈值，取值范围为 1~100，单位为百分比。

【使用指导】

此功能对使用共享接口和独占接口且处于 Active 状态的 Context 均生效。

所有 Context 入方向单播报文的总 CPU 消耗率是指一个安全引擎组中所有使用共享接口和独占接口的 Context 处理单播报文所消耗 CPU 百分比之和，简称“单播报文的总 CPU 消耗率”。

当单播报文的总 CPU 消耗率和单个 Context 入方向单播报文的 CPU 消耗率达到各自的阈值后，发往此 Context 的单播报文会被设备丢弃，否则不会被丢弃。单个 Context 入方向单播报文的 CPU 消耗率由 `context-capability inbound unicast single` 命令设置。

【举例】

```
# 配置所有 Context 入方向单播报文的总 CPU 消耗率为 70%。  
<Sysname> system-view  
[Sysname] context-capability inbound unicast total cpu-usage 70
```

【相关命令】

- `context-capability inbound unicast single`

1.1.16 description

`description` 命令用来配置 Context 的描述信息。

`undo description` 命令用来恢复缺省情况。

【命令】

```
description text  
undo description
```

【缺省情况】

缺省 Context 描述信息为 DefaultContext。非缺省 Context 没有配置描述信息。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

text: Context 的描述信息，为 1~255 个字符的字符串，区分大小写。

【使用指导】

当设备上配置的 Context 较多时，用户可以为 Context 配置特定的描述信息，以便记忆和管理 Context。

【举例】

```
# 将 Context 的描述信息配置为 test。  
<Sysname> system-view  
[Sysname] context cnt2  
[Sysname-context-2-cnt2] description test
```

1.1.17 display context

`display context` 命令用来显示已经创建的 Context 的信息，包括编号和状态等。

【命令】

```
display context [ name context-name ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name: Context 的名称，为 1~15 个字符的字符串，区分大小写。

【使用指导】

在缺省 Context 中，可使用 **name context-name** 参数查看指定 Context 的信息。不指定 **name context-name** 参数时，则显示设备上创建的所有 Context 的信息。

【举例】

显示已经创建的 Context 的信息。

```
<Sysname> display context
ID      Name      Status      Description
1       cnt1      active      context1
2       cnt2      inactive    context2
3       cnt3      inactive    context3
```

表1-1 display context 命令显示信息描述表

字段	描述
ID	Context的编号
Name	Context的名称
Status	Context的状态： <ul style="list-style-type: none">• active: 表示 Context 正常运行• inactive: 表示 Context 处于未启动状态• starting: 表示 Context 正在启动• stopping: 表示 Context 正在停止
Description	Context描述信息

1.1.18 display context capability

display context capability 命令用来显示 Context 内可分配业务资源的使用情况。

【命令】

```
display context [ name context-name ] capability [ security-policy | session ]  
[ slot slot-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name: 显示指定 Context 内可分配业务资源的使用情况，context-name 是 Context 的名称，为 1~15 个字符的字符串，区分大小写。若不指定该参数，则表示显示所有 Context 内可分配业务资源的使用情况。

security-policy: 显示可分配安全策略规则资源的使用情况。

session: 显示可分配会话资源的使用情况。

slot slot-number: 显示指定成员设备上的 Context 内可分配会话资源的使用情况，slot-number 表示设备在 IRF 中的成员编号。若不指定该参数，则表示显示所有成员设备上的 Context 内可分配会话资源的使用情况。

【使用指导】

此命令仅支持在缺省 Context 中使用。

【举例】

显示所有 Context 内可分配业务资源的使用情况。

```
<Sysname> display context capability
Session usage and establishment rate:
Slot 1 CPU 0:
  ID   Name      Maximum   Used    Free   Total(/s)  Rate(/s)  Usage(%)
  ---  ---      -
  1    Admin      NA        500    NA     NA         1000      NA
  2    conetxt1  10000    300    9700   1000       100       10
  3    context2  2000     1000   1000   2000       1000      50
Security policy rule usage:
  ID   Name      Maximum   Used    Free
  ---  ---      -
  1    Admin      NA        500    NA
  2    conetxt1  10000    300    9700
  3    context2  2000     1000   1000
```

表1-2 display context capability 命令显示信息描述表

字段	描述
Session usage	表示可分配会话连接数的使用情况
Session establishment rate	表示可分配会话新建速率的使用情况
Security policy rule usage	表示可分配安全策略规则资源的使用情况
ID	表示Context的ID
Name	表示Context的名称
Maximum	表示当前Context内可分配资源的最大值
Used	表示当前Context内可分配资源已被使用的数量
Free	表示当前Context内可分配资源未被使用的数量

Total	表示当前Context内会话新建速率的最大值，单位为每秒连接数
Rate	表示当前Context内会话的当前新建速率，单位为每秒连接数
Usage	表示当前Context内会话新建速率所占的百分比

【相关命令】

- **capability security-policy-rule maximum**
- **capability session maximum**
- **capability session rate**

1.1.19 display context capability inbound broadcast

display context capability inbound broadcast 命令用来显示 Context 入方向广播报文的速率限制的统计信息。

【命令】

```
display context name context-name capability inbound broadcast slot
slot-number
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name *context-name*: 显示指定 Context 上入方向广播报文的速率限制的统计信息。
context-name 表示 Context 的名称，为 1~15 个字符的字符串，区分大小写。

slot *slot-number*: 显示指定成员设备上的入方向广播报文的速率限制的统计信息，
slot-number 表示设备在 IRF 中的成员编号。

【举例】

显示 Context abc 在指定 Slot 上的入方向广播报文的速率限制的统计信息。

```
<Sysname> display context name abc capability inbound broadcast slot 1
Context name: abc
Context ID: 2
Drop Rate: 1000 pps
Inbound throughput limit: 8000 pps
Total inbound throughput limit: 10000 pps
```

表1-3 display context capability inbound broadcast 命令显示信息描述表

字段	描述
Context name	表示Context的名称

Context id	表示Context的ID
Drop Rate	表示此Context丢弃广播报文的速率，单位为pps
Inbound throughput limit	表示此Context入方向广播报文的总速率阈值，单位为pps
Total inbound throughput limit	表示所有Context入方向广播报文的速率阈值，单位为pps

1.1.20 display context capability inbound multicast

display context capability inbound multicast 命令用来显示 Context 入方向组播报文的速率限制的统计信息。

【命令】

```
display context name context-name capability inbound multicast slot slot-number
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name：显示指定 Context 上入方向组播报文的速率限制的统计信息。
context-name 表示 Context 的名称，为 1~15 个字符的字符串，区分大小写。

slot slot-number：显示指定成员设备上的入方向组播报文的速率限制的统计信息，
slot-number 表示设备在 IRF 中的成员编号。

【举例】

显示 Context abc 在指定 Slot 上的入方向组播报文的速率限制的统计信息。

```
<Sysname> display context name abc capability inbound multicast slot 1
Context name: abc
Context ID: 2
Drop Rate: 1000 pps
Inbound throughput limit: 8000 pps
Total inbound throughput limit: 10000 pps
```

表1-4 display context capability inbound multicast 命令显示信息描述表

字段	描述
Context name	表示Context的名称
Context id	表示Context的ID
Drop Rate	表示此Context丢弃组播报文的速率，单位为pps
Inbound throughput limit	表示此Context入方向组播报文的总速率阈值，单位为pps

Total inbound throughput limit	表示所有Context入方向组播报文的速率阈值，单位为pps
--------------------------------	--------------------------------

1.1.21 display context capability inbound unicast

display context capability inbound unicast 命令用来显示 Context 入方向单播报文的速率限制的统计信息。

【命令】

```
display context name context-name capability inbound unicast slot
slot-number
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name：显示指定 Context 上入方向单播报文的速率限制的统计信息。
context-name 表示 Context 的名称，为 1~15 个字符的字符串，区分大小写。

slot slot-number：指定成员设备。*slot-number* 为设备在 IRF 中的成员编号。

【举例】

显示 Context abc 在指定 Slot 上的入方向单播报文的速率限制的统计信息。

```
<Sysname> display context name abc capability inbound unicast slot 1
Context Name: abc
Context ID: 2
The Total Threshold is 0
The Context Threshold is 100
The Total Drop Num is 0
CPUID   Pper   Dper   Prate  Pcycle   Drate  Dcycle   Hdrate  TotalDrate
CPU0    0.0%  0.0%   0/s    0         0/s    0         0/s     0/s
CPU1    0.0%  0.0%   0/s    0         0/s    0         0/s     0/s
```

表1-5 display context capability inbound unicast 命令显示信息描述表

字段	描述
Context name	表示Context的名称
Context ID	表示Context的ID
The Total Threshold	表示所有Context入方向单播报文的总cpu消耗阈值百分比
The Context Threshold	表示此Context入方向单播报文的cpu消耗阈值百分比
The Total Drop Num	单播限速丢包数
CPUID	CPUID

Pper	通过报文消耗的cycle数的百分比
Dper	丢弃报文消耗的cycle数的百分比
Prate	通过报文速率
Pcycle	通过报文消耗的cycle数
Drate	丢弃报文速率
Dcycle	丢弃报文消耗的cycle数
HDrate	硬件丢包速率
TotalDrate	总丢包速率

1.1.22 display context configuration

display context configuration 命令用来显示各 Context 的配置信息。

【命令】

```
display context [ name context-name ] configuration [ file filename ]
```

【视图】

任意视图

【缺省用户角色】

```
network-admin
network-operator
```

【参数】

name *context-name*: 显示指定 Context 的配置信息, *context-name* 是 Context 的名称, 为 1~15 个字符的字符串, 区分大小写。若不指定该参数, 则表示显示所有 Context 的配置信息。

file *filename*: 表示将显示的配置信息保存到指定文件。 *filename* 表示文件的名称, 为 1~255 个字符的字符串 (含后缀), 不区分大小写, 文件名不能为 “.” 或 “..”, 不能包含 “|”、“/”、“:”、“\”、“?”、“\”、“<”、“>”、“|”、“*”, 首字符不能为 “-”, 且后缀必须为 “.tar.gz”, 后缀不区分大小写。不指定该参数时, 用户可根据提示信息选择将配置信息保存到指定文件或直接将配置信息导出到终端显示。

【使用指导】

此命令仅支持在缺省 Context 中使用。

执行该命令, 相当于在所有 Context 中一次性执行 **display current-configuration** 命令。

在缺省 Context 中, 无法对处于未启动状态的自定义 Context 进行配置信息收集。

【举例】

显示所有 Context 的配置信息。

```
<Sysname> display context configuration
Save or display context configuration(Y=save, N=display)? [Y/N]:n
=====inner configuration of context Admin=====
```

```

=====
display current-configuration
#
  version 7.1.064, Feature 9321
#
sysname Sysname
#
context Admin id 1
#
context cnt1 id 2
#
return
<Sysname>

=====inner configuration of context cnt1=====

=====
display current-configuration
#
  version 7.1.064, Feature 9321
#
sysname Sysname
#
context Admin id 1
#
context cnt1 id 2
---- More ----
# 在交互信息时选择将配置信息保存到指定文件，并输入文件名为 test.tar.gz。
<Sysname> display context configuration
Save or display context configuration (Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag.tar.gz]: test.tar.gz
Saving context configuration to flash:/test.tar.gz. Please wait...
# 在命令行中直接通过参数指定将配置信息保存到文件 test.tar.gz。
<Sysname> display context configuration file test.tar.gz
Saving context configuration to flash:/test.tar.gz. Please wait...

```

1.1.23 display context interface

display context interface 命令用来显示 Context 的接口列表。

【命令】

```
display context [ name context-name ] interface
```

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

name context-name: Context 的名称，为 1~15 个字符的字符串，区分大小写。

【使用指导】

在缺省 Context 中，可使用 **name context-name** 参数查看指定 Context 的接口列表；不指定 **name context-name** 参数时，则显示设备上创建的所有 Context 的接口列表。

【举例】

```
# 显示所有 Context 的接口列表。
<Sysname> display context interface
Context stub1's interfaces:
  GigabitEthernet1/0/2
Context stub2's interfaces:
  GigabitEthernet1/0/3
```

【相关命令】

- **allocate interface**

1.1.24 display context online-users sslvpn

display context online-users sslvpn 命令用来显示所有 Context 内 SSL VPN 在线用户数。

【命令】

```
display context online-users sslvpn
```

【视图】

任意视图

【缺省用户角色】

network-admin
context-admin

【使用指导】

本命令仅支持在缺省 Context 中使用。

此功能统计的 SSL VPN 在线用户数指的是当前在线的 SSL VPN 会话数。

【举例】

```
# 显示所有 Context 内 SSL VPN 在线用户数。
<Sysname> display context online-users sslvpn
Total number of SSL VPN online users: 50
```

表1-6 display context online-users sslvpn 命令显示信息描述表

字段	描述
Total number of SSL VPN online users	所有Context内SSL VPN在线用户总数

1.1.25 display context resource

display context resource 命令用来显示 Context 对 CPU/磁盘/内存资源的使用情况。

【命令】

```
display context [ name context-name ] resource [ cpu | disk | memory ] [ slot slot-number cpu cpu-number ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name *context-name*: 显示指定 Context 对 CPU/磁盘/内存资源的使用情况。*context-name* 表示 Context 的名称，为 1~15 个字符的字符串，区分大小写。不指定该参数时，显示所有 Context 对 CPU/磁盘/内存资源的使用情况。

cpu: 显示 Context 对 CPU 的使用情况。

disk: 显示 Context 对磁盘的使用情况。

memory: 显示 Context 对内存的使用情况。

slot *slot-number* **cpu** *cpu-number*: 显示 Context 对指定成员设备上的 CPU/磁盘/内存资源的使用情况，*slot-number* 表示设备在 IRF 中的成员编号，*cpu-number* 表示 CPU 的编号。不指定该参数时，显示 Context 对所有成员设备的 CPU/磁盘/内存资源的使用情况。

【使用指导】

若不指定 **cpu**、**disk** 和 **memory** 参数，则显示 Context 对 CPU、磁盘和内存的使用情况。

【举例】

显示 Context 对所有成员设备上 CPU 资源的使用情况。

```
<Sysname> display context resource cpu
```

```
CPU usage:
```

```
Slot 1 CPU 0:
```

ID	Name	Weight	Usage(%)
1	cnt1	10	24
2	cnt2	10	0

```
Slot 2 CPU 0:
```

ID	Name	Weight	Usage(%)
1	cnt3	10	0
2	cnt4	10	0

表1-7 display context resource 命令显示信息描述表

字段	描述
Memory	表示下面显示的是内存的使用情况

字段	描述
CPU	表示下面显示的是CPU的使用情况
Disk	表示下面显示的是磁盘的使用情况
Used 238.1MB, Free 249.3MB, Total 487.4MB	内存的使用情况, Used 表示内存已使用空间的大小(单位为MB), Free 表示当前空闲内存的大小(单位为MB), Total 表示整个内存大小(单位为MB)。如果Context没有启动,则Used会显示为0
Cfa0: Used 0MB, Free 61MB, Total 61MB	Cfa0表示磁盘的名称, Used 表示整个磁盘已使用空间的大小(单位为MB), Free 表示整个磁盘当前空闲空间的大小(单位为MB), Total 表示整个磁盘空间大小(单位为MB)。如果Context没有启动,则Used会显示为0
ID	Context的编号
name	Context的名称
Weight	Context使用CPU的权重值
Usage(%)	Context对CPU的实际占用率, 用百分比表示
Quota(MB)	Context使用磁盘/内存的限制值, 单位为MB
Used(MB)	Context当前已使用的磁盘/内存空间的大小, 单位为MB
Free(MB)	Context还可以使用的磁盘/内存空间的大小, 单位为MB

【相关命令】

- `limit-resource cpu`
- `limit-resource disk`
- `limit-resource memory`

1.1.26 display context statistics

`display context statistics` 命令用来显示 Context 内资源的统计信息。

【命令】

```
display context [ name context-name ] statistics [ file filename ]
```

【视图】

任意视图

【缺省用户角色】

network-admin
network-operator

【参数】

name context-name: 显示指定 Context 内资源的统计信息, *context-name* 是 Context 的名称, 为 1~15 个字符的字符串, 区分大小写。若不指定该参数, 则表示显示所有 Context 内资源的统计信息。

file filename: 表示将收集到的资源统计信息保存到指定文件。 *filename* 表示文件的名称, 为 1~255 个字符的字符串(含后缀), 不区分大小写, 文件名不能为“.”或“..”, 不能包含“”、

“/”、“:”、“\”、“?”、“\”、“<”、“>”、“|”、“*”，首字符不能为“-”，且后缀必须为“.tar.gz”，后缀不区分大小写。不指定该参数时，用户可根据提示信息选择将资源的统计信息保存到指定文件或直接将资源的统计信息导出到终端显示。

【使用指导】

此命令仅支持在缺省 Context 中使用。

执行该命令，相当于一次性执行如下命令：

- **display context capability**
- **display counters inbound interface**
- **display counters outbound interface**
- **display counters rate inbound interface**
- **display counters rate outbound interface**
- **display interface**
- **display ip statistics**
- **display ipv6 statistics**
- **display session statistics**
- **display nat statistics**

有关此命令显示信息的详细介绍，请参考各个命令显示信息的介绍。

【举例】

显示所有 Context 内资源的统计信息。

```
<Sysname> display context statistics
Save or display context statistics (Y=save, N=display)? [Y/N]:n
=====
===== display session statistics =====
Slot 1:
Current sessions: 0
      TCP sessions:          0
      UDP sessions:          0
      ICMP sessions:         0
      ICMPv6 sessions:       0
      UDP-Lite sessions:     0
      SCTP sessions:         0
      DCCP sessions:         0
      RAWIP sessions:        0
---- More ----
```

将资源统计信息保存到指定文件，并输入文件名为 test.tar.gz。

```
<Sysname> display context statistics
Save or display context statistics(Y=save, N=display)? [Y/N]:y
Please input the file name(*.tar.gz)[flash:/diag.tar.gz]: test.tar.gz
Saving context statistics to flash:/test.tar.gz. Please wait....
```

将资源统计信息保存到文件 test.tar.gz。

```
<Sysname> display context statistics file test.tar.gz
Saving context statistics to flash:/test.tar.gz. Please wait...
```

【相关命令】

- **display context capability**
- **display counters inbound interface** (接口管理命令参考/以太网接口)
- **display counters outbound interface** (接口管理命令参考/以太网接口)
- **display counters rate inbound interface** (接口管理命令参考/以太网接口)
- **display counters rate outbound interface** (接口管理命令参考/以太网接口)
- **display interface** (接口管理命令参考/以太网接口)
- **display ip statistics** (三层技术-IP 业务命令参考/IP 性能优化)
- **display ipv6 statistics** (三层技术-IP 业务命令参考/IPv6 基础)
- **display session statistics** (安全命令参考/会话管理)
- **display nat statistics** (三层技术-IP 业务命令参考/NAT)

1.1.27 display context vlan

display context vlan 命令用来显示 Context 的 VLAN 列表。

【命令】

```
display context [ name context-name ] vlan
```

【视图】

任意视图

【缺省用户角色】

```
network-admin  
network-operator
```

【参数】

name *context-name*: Context 的名称, 为 1~15 个字符的字符串, 区分大小写。

【使用指导】

在缺省 Context 中, 可使用 **name** *context-name* 参数查看指定 Context 的 VLAN 列表; 不指定 **name** *context-name* 参数时, 则显示设备上创建的所有 Context 的 VLAN 列表。

【举例】

显示所有 Context 的 VLAN 列表。

```
<Sysname> display context vlan  
Context stub1's VLAN(s):
```

```
Context stub2's VLAN(s):  
 2,4094
```

```
Context stub3's VLAN(s):  
 5,6,800-3000,3400
```

显示 Context sub1 的 VLAN 列表。

```
<Sysname> display context name sub1 vlan  
Context stub1's VLAN(s):  
 5,6,11-23,3400
```

【相关命令】

- `allocate vlan`

1.1.28 hardware fast-forwarding vpc enable

`hardware fast-forwarding vpc enable` 命令用来开启跨 VPC（Virtual Private Cloud，虚拟私有云）的硬件快速转发功能。

`undo hardware fast-forwarding vpc enable` 命令用来关闭跨 VPC 的硬件快速转发功能。

【命令】

```
hardware fast-forwarding vpc enable [ slot slot-number [ cpu cpu-number ] ]  
undo hardware fast-forwarding vpc enable [ slot slot-number [ cpu  
cpu-number ] ]
```

```
hardware fast-forwarding vpc enable [ chassis chassis-number slot  
slot-number [ cpu cpu-number ] ]  
undo hardware fast-forwarding vpc enable [ chassis chassis-number slot  
slot-number [ cpu cpu-number ] ]
```

【缺省情况】

跨 VPC 的硬件快速转发功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

slot slot-number: 表示单板所在的槽位号。不指定该参数时，则表示所有成员设备。

chassis chassis-number slot slot-number 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。不指定该参数时，则表示 IRF 中的所有单板。

cpu cpu-number: *cpu-number* 表示 CPU 的编号。只有指定的 **slot** 支持多 CPU 时，才能配置该参数。

【使用指导】

开启硬件快速转发功能后（即执行 `hardware fast-forwarding enable` 命令）本功能才能生效，此功能可以提高跨 VPC 报文转发的性能。有关 `hardware fast-forwarding enable` 命令的详细信息，请参见“三层技术-IP 业务命令参考”中的“快速转发”。

配置此功能后，设备上的所有 Context 均生效。

此功能与 GRE 和 MPLS 功能互斥不能同时使用。

【举例】

```
# 开启跨 VPC 的硬件快速转发功能。
```



```
<Sysname> system-view
[Sysname] hardware fast-forwarding vpc enable
```

【相关命令】

- **hardware fast-forwarding enable**（三层技术-IP 业务命令参考/快速转发）

1.1.29 limit-resource cpu

limit-resource cpu 命令用来配置 Context 的 CPU 权重。

undo limit-resource cpu 命令用来恢复缺省情况。

【命令】

```
limit-resource cpu weight weight-value
undo limit-resource cpu
```

【缺省情况】

各 Context 的 CPU 权重均为 10。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

weight weight-value: 配置指定 Context 的 CPU 权重，取值范围为 1~10。系统根据 Context 的权重为 Context 分配 CPU 时间。

【举例】

配置 Context 的 CPU 权重为 2。

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] limit-resource cpu weight 2
```

1.1.30 limit-resource disk

limit-resource disk 命令用来配置 Context 可使用的磁盘空间上限（用百分比表示）。

undo limit-resource disk 命令用来恢复缺省情况。

【命令】

```
limit-resource disk slot slot-number cpu cpu-number ratio limit-ratio
undo limit-resource disk slot slot-number cpu cpu-number
```

【缺省情况】

Context 可以使用物理设备上的所有空闲磁盘空间。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number* **cpu** *cpu-number*: 配置 Context 在指定成员设备上可使用的磁盘空间上限。
slot-number 表示设备在 IRF 中的成员编号, *cpu-number* 表示 CPU 的编号。

ratio *limit-ratio*: 表示 Context 在设备上最多可使用的磁盘空间大小与该设备整个磁盘空间大小的百分比, 取值范围为 1~100。

【使用指导】

为了防止单个 Context 过多的占用磁盘而影响其它 Context, 特别是为防止异常情况下对磁盘的占用, 可以为指定的 Context 配置磁盘上限, 当 Context 占用磁盘空间达到限制值时, 后续不能申请新的磁盘空间。

请在 Context 启动后配置磁盘上限。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。

如果设备上有多块磁盘, 该命令对所有磁盘生效。

【举例】

配置 Context cnt2 最多可使用 1 号成员设备上磁盘空间的 30%。

```
<Sysname> system-view
[Sysname] context cnt2
[Sysname-context-2-cnt2] limit-resource disk slot 1 cpu 0 ratio 30
```

1.1.31 limit-resource memory

limit-resource memory 命令用来配置 Context 可使用的内存空间上限 (用百分比表示)。

undo limit-resource memory 命令用来恢复到缺省情况。

【命令】

```
limit-resource memory slot slot-number cpu cpu-number ratio limit-ratio
undo limit-resource memory slot slot-number cpu cpu-number
```

【缺省情况】

所有 Context 共享物理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。

【视图】

Context 视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number* **cpu** *cpu-number*: 配置 Context 在指定成员设备上可使用的内存空间上限。
slot-number 表示设备在 IRF 中的成员编号, *cpu-number* 表示 CPU 的编号。

ratio limit-ratio: 表示 Context 在设备上最多可使用的内存大小与该设备整个内存大小的百分比，取值范围为 1~100。

【使用指导】

为了防止单个 Context 过多的占用内存而影响其它 Context，特别是为防止异常情况下对内存的占用，可以为指定的 Context 配置内存上限，当 Context 占用内存达到限制值时，后续不能申请新的内存。

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而引起功能异常。

【举例】

```
# 配置 Context cnt2 最多可使用 1 号成员设备内存的 30%。  
<Sysname> system-view  
[Sysname] context cnt2  
[Sysname-context-2-cnt2] limit-resource memory slot 1 cpu 0 ratio 30
```

1.1.32 reset context capability inbound broadcast

reset context capability inbound broadcast 命令用来清除 Context 入方向广播报文的速率限制的统计信息。

【命令】

```
reset context name context-name capability inbound broadcast slot slot-number
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

name context-name: 清除指定 Context 上入方向广播报文的速率限制的统计信息。
context-name 表示 Context 的名称，为 1~15 个字符的字符串，区分大小写。

slot slot-number: 清除 Context 在指定成员设备上的入方向广播报文的速率限制的统计信息，
slot-number 表示设备在 IRF 中的成员编号。

【举例】

```
# 清除 Context abc 在指定 Slot 上的广播限速统计信息。  
<Sysname> reset context name abc capability inbound broadcast slot 1
```

1.1.33 reset context capability inbound multicast

reset context capability inbound multicast 命令用来清除 Context 入方向组播报文的速率限制的统计信息。

【命令】

```
reset context name context-name capability inbound multicast slot  
slot-number
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

name *context-name*: 清除指定 Context 上入方向组播报文的速率限制的统计信息。
context-name 表示 Context 的名称，为 1~15 个字符的字符串，区分大小写。

slot *slot-number*: 清除 Context 在指定成员设备上的入方向组播报文的速率限制的统计信息，
slot-number 表示设备在 IRF 中的成员编号。

【举例】

清除 Context abc 在指定 Slot 上的组播限速统计信息。

```
<Sysname> reset context name abc capability inbound multicast slot 1
```

1.1.34 reset context capability inbound unicast

reset context capability inbound unicast 命令用来清除 Context 入方向单播报文的速率限制的统计信息。

【命令】

```
reset context name context-name capability inbound unicast slot slot-number
```

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

name *context-name*: 清除指定 Context 上入方向单播报文的速率限制的统计信息。
context-name 表示 Context 的名称，为 1~15 个字符的字符串，区分大小写。

slot *slot-number*: 指定成员设备。*slot-number* 为设备在 IRF 中的成员编号。

【举例】

清除 Context abc 在指定 Slot 上的单播限速统计信息。

```
<Sysname> reset context name abc capability inbound unicast slot 1
```

1.1.35 switchto context

switchto context 命令用来登录到指定的 Context。

【命令】

```
switchto context context-name
```

【视图】

系统视图

【缺省用户角色】

```
network-admin  
network-operator
```

【参数】

context-name: 已启动的 Context 的名称。

【使用指导】

只要用户和物理设备之间路由可达，就能使用该命令，通过物理设备和 Context 的内联接口，登录 Context。

【举例】

```
# 切换到 Context test2。  
<Sysname> system-view  
[Sysname] switchto context test2  
*****  
* Copyright (c) 2004-2018 New H3C Technologies Co., Ltd. All rights reserved.*  
* Without the owner's prior written consent, *  
* no decompiling or reverse-engineering shall be allowed. *  
*****  
  
<Context2>
```

1.1.36 tar context log

tar context log 命令用来收集各 Context 的日志信息。

【命令】

```
tar context [ name context-name ] log file filename
```

【视图】

用户视图

【缺省用户角色】

```
network-admin
```

【参数】

name context-name: 收集指定 Context 的日志信息，*context-name* 是 Context 的名称，为 1~15 个字符的字符串，区分大小写。若不指定该参数，则表示收集所有 Context 的日志信息。

file filename: 表示将收集到的日志信息保存到指定文件。*filename* 表示文件的名称，为 1~255 个字符的字符串（含后缀），不区分大小写，文件名不能为“.”或“..”，不能包含“”、“/”、

“:”、“\”、“?”、“\”、“<”、“>”、“|”、“*”，首字符不能为“-”，且后缀必须为“.tar.gz”，后缀不区分大小写。

【使用指导】

此命令仅支持在缺省 Context 中使用。

执行该命令会收集 logfile 文件夹和 diagfile 文件夹下的所有文件。

在缺省 Context 中，无法对从未启动过的自定义 Context 进行日志信息收集。

【举例】

收集各 Context 的日志信息，并指定保存文件的名称为 test.tar.gz。

```
<Sysname> tar context log file test.tar.gz
```