目 录

1 IP Accounting 配置命令

1.1 IP Accounting 配置命令

1.1.1 display ip count

【命令】

display ip count { **inbound-packets** | **outbound-packets** } { **exterior** | **firewall-denied** | **interior** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

inbound-packets：显示接收的 IP 报文的统计信息。

outbound-packets：显示发送的 IP 报文的统计信息。

exterior：显示 exterior 表中的 IP 报文统计信息，exterior 表用来记录不符合规则的合法 IP 报文的统计信息。

firewall-denied：显示被防火墙拒绝的 IP 报文的统计信息。

interior：显示 interior 表中的 IP 报文统计信息，interior 表用来记录符合规则的合法 IP 报文的统计信息。

说明

当接口上没有配置防火墙时，合法报文是指所有进出接口的 IP 报文；当接口上配置了防火墙时，合法报文是指通过了防火墙的 IP 报文。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ip count 命令用来显示 IP Accounting 统计的 IP 报文信息。

【举例】

显示接收的合法 IP 报文中，不符合规则的 IP 报文的统计信息。

```
<Sysname> display ip count inbound-packets exterior
6 Inbound streams information in exterior list:
  SrcIP            DstIP              Protocol  Pkts        Bytes
  0.0.0.0          255.255.255.255    UDP       28          9502
  10.153.72.181    10.153.73.255      UDP       174         38034
  10.153.72.137    239.255.255.250    UDP       4           644
  10.153.72.141    224.0.0.2          IGMP      4           128
  10.153.72.141    224.0.0.9          UDP       4           208
  10.153.72.141    224.0.0.9          IGMP      4           128
```

表1-1 display ip count 命令显示信息描述表

字段	描述
SrcIP	报文源 IP 地址
DstIP	报文目的 IP 地址
Protocol	报文的协议类型
Pkts	报文个数
Bytes	报文字节数

1.1.2 display ip count rule

【命令】

display ip count rule [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ip count rule 命令用来显示用户配置的 IP Accounting 统计规则。

【举例】

显示用户配置的 IP Accounting 统计规则。

```
<Sysname> display ip count rule
  IP Count rule list:
          IP address      address mask
             1.1.1.0     255.255.255.0
             2.0.0.0         255.0.0.0
  -----------------------------------
  Total: 2 rules
```

表1-2 display ip count rule 命令显示信息描述表

字段	描述
IP address	网段地址
address mask	网络掩码

1.1.3 ip count enable

【命令】

ip count enable

undo ip count enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

ip count enable 命令用来启动 IP Accounting 报文统计功能。**undo ip count enable** 命令用来取消 IP Accounting 报文统计功能。

缺省情况下，没有启动 IP Accounting 报文统计功能。

【举例】

启动 IP Accounting 报文统计功能。

```
<Sysname> system-view
[Sysname] ip count enable
```

1.1.4 ip count exterior-threshold

【命令】

ip count exterior-threshold *number*

undo ip count exterior-threshold

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

number：exterior 表中流记录个数，取值范围为 0～8192。

【描述】

ip count exterior-threshold 命令用来设置 exterior 统计表中流记录个数的最大值。**undo ip count exterior-threshold** 用来将 exterior 统计表中流记录个数的最大值恢复为缺省值（如果该表中已经存在流记录，则系统会提示用户清空此表后再设置）。

缺省情况下，exterior 统计表中流记录个数的最大值为 0，即系统不统计不符合 IP Accounting 统计规则的合法 IP 报文的信息。

【举例】

设置 exterior 统计表中流记录个数的最大值为 100。

```
<Sysname> system-view
[Sysname] ip count exterior-threshold 100
```

1.1.5 ip count firewall-denied

【命令】

ip count firewall-denied { **inbound-packets** | **outbound-packets** }

undo ip count firewall-denied { **inbound-packets** | **outbound-packets** }

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

inbound-packets：统计在当前接口上被防火墙拒绝接收的 IP 报文信息。

outbound-packets：统计在当前接口上被防火墙拒绝发送的 IP 报文信息。

【描述】

ip count firewall-denied 命令用来配置对当前接口上被防火墙拒绝的 IP 报文信息进行统计。**undo ip count firewall-denied** 命令用来恢复缺省情况。

缺省情况下，不统计被防火墙拒绝的 IP 报文信息。

通过在接口上使用上述命令，可以使 IP Accounting 特性对被防火墙拒绝接收或者发送的 IP 报文信息进行统计。对于统计的接收和发送的 IP 报文信息，统一存放在 firewall-denied table 中。

【举例】

启动对接口 Ethernet1/1 上被防火墙拒绝发送的 IP 报文信息的统计。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ip count firewall-denied outbound-packets
```

取消对接口 Ethernet1/1 上被防火墙拒绝发送的 IP 报文信息的统计。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] undo ip count firewall-denied outbound-packets
```

1.1.6 ip count inbound-packets

【命令】

ip count inbound-packets

undo ip count inbound-packets

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

ip count inbound-packets 命令用来配置对当前接口接收的合法 IP 报文信息进行统计。**undo ip count inbound-packets** 命令用来恢复缺省情况。

缺省情况下，不统计接口接收到的合法 IP 报文信息。

通过在接口上使用 **ip count inbound-packets** 命令，可以使 IP Accounting 特性对接口接收到的合法 IP 报文信息进行统计，对于接收到的合法 IP 报文信息，根据是否匹配 IP Accounting 统计规则，将 IP 报文信息存储在 interior 表或者 exterior 表中。

说明

当接口上没有配置防火墙时，合法报文是指所有进出接口的 IP 报文；当接口上配置了防火墙时，合法报文是指通过了防火墙的 IP 报文。

【举例】

启动对 Ethernet1/1 接收的合法 IP 报文信息的统计。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ip count inbound-packets
```

取消对 Ethernet1/1 接收的合法 IP 报文信息的统计。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] undo ip count inbound-packets
```

1.1.7 ip count interior-threshold

【命令】

ip count interior-threshold *number*

undo ip count interior-threshold

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

number：interior 表中流记录个数，取值范围为 0～16384。

【描述】

ip count interior-threshold 命令用来设置 interior 统计表中流记录个数的最大值。**undo ip count interior-threshold** 命令用来将 interior 统计表中流记录个数的最大值恢复为缺省值（如果表中已经存在的流记录个数大于缺省值，则提示用户清空此表后再设置）。

缺省情况下，interior 统计表中流记录个数的最大值为 512。

【举例】

设置 interior 统计表中流记录个数的最大值为 1000。

```
<Sysname> system-view
[Sysname] ip count interior-threshold 1000
```

1.1.8 ip count outbound-packets

【命令】

ip count outbound-packets

undo ip count outbound-packets

【视图】

接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

ip count outbound-packets 命令用来配置对当前接口发送的合法 IP 报文信息进行统计。**undo ip count outbound-packets** 命令用来恢复缺省情况。

缺省情况下，不统计接口发送的合法 IP 报文信息。

通过在接口上使用本命令，可以使 IP Accounting 特性对接口发送的合法 IP 报文信息进行统计。对于发送的合法 IP 报文信息，根据是否匹配规则，将 IP 报文信息存储在 interior 表或者 exterior 表中。

【举例】

启动对 Ethernet1/1 发送的合法 IP 报文信息的统计。

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ip count outbound-packets
```

1.1.9 ip count rule

【命令】

ip count rule *ip-address* { *mask* | *mask-length* }

undo ip count rule [*ip-address* { *mask* | *mask-length* }]

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

ip-address：IP 地址。

mask：网络掩码。

mask-length：网络掩码的长度，取值范围为 0～32。

【描述】

ip count rule 命令用来配置 IP Accounting 统计的匹配规则。**undo ip count rule** 命令用来删除已经配置的匹配规则，如果不带参数则删除所有已经配置的 IP Accounting 统计规则。

用户配置的规则由一个 IP 地址和相应的掩码组成，规则表中记录的是 IP 地址和其掩码相“与”的结果，即网段的地址。对于通过了接口（当接口没有配置防火墙时）或者接口上防火墙（当接口配置了防火墙时）的 IP 报文，如果 IP 报文的源 IP 地址或目的 IP 地址中只要有一个匹配规则中的网段地址，就将该报文信息记录在“符合规则的报文统计表（interior table）”中，否则就记录在“不符合规则的报文统计表（exterior table）”中。

需要注意的是：

- 用户最多可以配置 32 条规则。
- 如果不配置规则，则认为当前流都是用户不关心的，统计到 exterior 表里。

【举例】

配置 IP Accounting 统计的匹配规则。

```
<Sysname> system-view
[Sysname] ip count rule 169.254.10.1 255.255.0.0
```

1.1.10 ip count timeout

【命令】

ip count timeout *minutes*

undo ip count timeout

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

minutes：统计表中流记录的老化时间，取值范围为 60～10080，单位为分钟。

【描述】

ip count timeout 命令用来配置 IP Accounting 统计表中流记录的老化时间。**undo ip count timeout** 命令用来恢复老化时间为缺省值。

缺省情况下，IP Accounting 统计表中流记录的老化时间为 720 分钟（即 12 小时）。

如果某一统计表中流记录信息在老化时间内没有更新，则 IP Accounting 特性认为该信息已经超时，将其删除。

【举例】

设置 IP Accounting 表中流记录的老化时间为 100 分钟。

```
<Sysname> system-view
[Sysname] ip count timeout 100
```

1.1.11 reset ip count

【命令】

reset ip count { **all** | **exterior** | **firewall** | **interior** }

【视图】

用户视图

【缺省级别】

2：系统级

【参数】

all：清除所有的统计信息。

firewall：清除 firewall-denied 表中的 IP 报文统计信息。

exterior：清除 exterior 表中的 IP 报文统计信息。

interior：清除 interior 表中的 IP 报文统计信息。

【描述】

reset ip count 命令用来清除 IP Accounting 已有的 IP 报文统计信息。

【举例】

清除所有的 IP 报文统计信息。

```
<Sysname> reset ip count all
```