目 录

1 Flow日志

1.1 Flow日志简介

1.1.1 Flow日志概述

设备根据报文的 5 元组（源 IP 地址、目的 IP 地址、源端口、目的端口、协议号）对用户访问网络的流进行分类统计，并生成用户流（Flow）日志。Flow 日志目前主要用来记录用户访问网络所产生的 NAT 会话相关信息，包括 5 元组和发送、接收的字节数等。网络管理员利用这些信息可以实时跟踪、记录、分析用户访问网络的情况。

Flow 日志可以封装成 UDP 报文直接发送到日志主机，也可以发送到信息中心封装成系统日志，但由用户访问网络时会产生大量 NAT 会话日志，且系统日志传输格式为 ASCII 码，相比 Flow 日志的二进制格式传输效率低，为了满足用户需求，因此开发出 Flow 日志。

1.1.2 Flow日志的版本

Flow日志根据日志信息所包含字段多少分为Flow1.0 和Flow3.0 两个版本。两种Flow日志的内容稍有不同，具体差别请参见 表 1-1 和 表 1-2。

下表中介绍的字段是设备向日志主机方向发送的原始信息所包含的字段，可能与用户最终看到的信息格式有差异，最终显示格式与用户使用的日志解析工具有关，请以实际情况为准。

表1-1 Flow1.0 日志信息包含的字段

字段	描述
SrcIP	NAT转换前的源IP地址
DestIP	NAT转换前的目的IP地址
SrcPort	NAT转换前的TCP/UDP源端口号
DestPort	NAT转换前的TCP/UDP目的端口号
StartTime	流起始时间，以秒为单位，从1970/1/1 0:0开始计算
EndTime	流结束时间，以秒为单位，从1970/1/1 0:0开始计算 当Operator字段取值为6时，该字段为0
Protocol	IP承载的协议类型

字段	描述
Operator	操作字，记录生成Flow日志的原因： • 0：保留不用 • 1：正常流结束 • 2：定时器超时老化 • 3：清除配置/配置变动引起的流老化 • 4：资源不足带来的流老化 • 5：保留不用 • 6：活跃流定期记录其连接情况 • 7：新的流创建触发强制删除原有流 • 8：流创建 • FE：其他 • 10~FE-1：以后扩充用
Reserved	保留

表1-2 Flow3.0 日志信息包含的字段

字段	描述
Protocol	IP承载的协议类型
Operator	操作字，记录生成Flow日志的原因： • 0：保留不用 • 1：正常流结束 • 2：定时器超时老化 • 3：清除配置/配置变动引起的流老化 • 4：资源不足带来的流老化 • 5：保留不用 • 6：活跃流定期记录其连接情况 • 7：新的流创建触发强制删除原有流 • 8：流创建 • FE：其他 • 10~FE-1：以后扩充用
IPVersion	IP报文版本
TosIPv4	IPv4报文的Tos字段
SourceIP	NAT转换前的源IP地址
SrcNatIP	NAT转换后的源IP地址
DestIP	NAT转换前的目的IP地址
DestNatIP	NAT转换后的目的IP地址
SrcPort	NAT转换前的TCP/UDP源端口号

字段	描述
SrcNatPort	NAT转换后的TCP/UDP源端口号
DestPort	NAT转换前的TCP/UDP目的端口号
DestNatPort	NAT转换后的TCP/UDP目的端口号
StartTime	流起始时间，以秒为单位，从1970/01/01 00:00开始计算
EndTime	流结束时间，以秒为单位，从1970/01/01 00:00开始计算 当Operator字段取值为6时，该字段为0
InTotalPkg	接收的报文包数
InTotalByte	接收的报文字节数
OutTotalPkg	发出的报文包数
OutTotalByte	发出的报文字节数
InVPNID	入VPN ID
OutVPNID	出VPN ID
Reserved1、2、3	保留

1.2 Flow日志配置任务简介

在配置 Flow 日志前需要通过 **nat log enable** 命令使能 NAT 日志功能，并根据用户需求选择开启 NAT 新建、删除会话日志和活跃流日志功能，关于命令的详细介绍，请参见“三层技术-IP 业务”中的“NAT”。

表1-3 Flow 日志配置任务简介

配置任务		说明	详细配置
配置Flow日志的版本		可选	1.3
配置Flow日志的源地址		可选	1.4
配置Flow日志的负载分担		可选	1.5
配置Flow日志输出方式	配置Flow日志输出到日志主机	二者必选其一	1.7.1
	配置Flow日志输出到信息中心		1.7.2

1.3 配置Flow日志的版本

请根据日志接收设备的实际能力配置 Flow 日志的版本。

设备支持 Flow1.0 和 Flow3.0 两个版本，但同一时刻只能使用一个版本。所以，如果多次使用该命令配置版本，则最新的配置生效。

表1-4 配置 Flow 日志的版本

操作	命令	说明
进入系统视图	**system-view**	-
配置Flow日志报文的版本号	**userlog flow export version** *version-number*	缺省情况下，Flow日志报文的版本号为1.0

1.4 配置Flow日志报文的源地址

Flow 日志可以使用源地址来唯一标识报文的发送者，以便对 Flow 日志进行过滤。指定源地址后，当设备向日志主机发送 Flow 日志时，就使用这个唯一 IP 地址作为报文的源 IP 地址，而不是使用报文出接口的地址。

推荐将 Flow 日志报文的源地址配置为设备上 Loopback 接口的地址，以屏蔽某个物理接口状态改变对 Flow 日志报文的影响。

表1-5 配置 Flow 日志报文的源地址

操作	命令	说明
进入系统视图	**system-view**	-
配置Flow日志报文的源地址	**userlog flow export source-ip** *ip-address*	缺省情况下，Flow日志报文的源地址为发送该报文的出接口IP地址

1.5 配置Flow日志的负载分担

缺省情况下，每一条 Flow 日志会复制输出给所有已配置的 Flow 日志主机。

配置了 Flow 日志负载分担功能后，Flow 日志按照会话源 IP 进行逐流负载分担，即源 IP 相同的会话对应的 Flow 日志始终发送到特定的一台日志主机。这样可以降低用户日志发送的压力，并减少冗余日志的处理。

在配置负载分担功能时，需要注意如果配置的日志主机不可达时，日志主机仍会参与 Flow 日志的负载分担，但负载分担到不可达的日志主机的 Flow 日志会直接被丢弃。

表1-6 配置 Flow 日志的负载分担

操作	命令	说明
进入系统视图	**system-view**	-
配置Flow日志的负载分担	**userlog flow export load-balancing**	缺省情况下，Flow日志输出到所有已配置的日志主机

1.6 配置Flow日志的时间戳

Flow 日志支持两种时间戳，分别是 UTC 时间（Coordinated Universal Time，国际协调时间）和本地时间。其中：

- UTC 时间指的是标准的格林威治时间。
- 本地时间指的是格林威治时间加上时区偏移的时间。用户可以使用命令 clock timezone 来配置需要偏移的时间。关于 clock timezone 的详细介绍，请参见“基础配置”中的“设备管理”。

表1-7 配置 Flow 日志的时间戳

操作	命令	说明
进入系统视图	**system-view**	-
配置Flow日志的时间戳使用本地时间	**userlog flow export timestamp localtime**	缺省情况下，Flow日志的时间戳使用UTC时间。 同一时刻只能使用一种时间戳

1.7 配置Flow日志输出方式

Flow 日志有两种输出方式：

- 将 Flow 日志封装成 UDP 报文直接发送给网络中的日志主机。日志主机可以对 Flow 日志进行解析和分类显示，以达到远程监控的目的。
- 将 Flow 日志输出到本设备的信息中心模块，再通过设置信息中心的输出参数，最终决定 Flow 日志的输出方向。关于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”。

通常情况下，用户访问网络会在短时间内产生大量 NAT 会话日志。系统日志传输格式为 ASCII 码，相比 Flow 日志的二进制格式传输效率低。所以，建议在日志量较小的情况下，使用输出到信心中心的方式。

Flow 日志的两种输出方式互斥，同一时刻只能选择一种输出方式。如果同时配置了两种输出方式，则系统会自动选择输出到信息中心，而不会发送到日志主机。

1.7.1 配置Flow日志输出到日志主机

表1-8 配置 Flow 日志输出到指定的日志主机

操作	命令	说明
进入系统视图	**system-view**	-
配置Flow日志输出到日志主机	**userlog flow export** [**vpn-instance** *vpn-instance-name*] **host** { *hostname* | *ipv4-address* | **ipv6** *ipv6-address* } **port** *udp-port*	缺省情况下，没有配置Flow日志主机的IP地址和UDP端口号

1.7.2 配置Flow日志输出到信息中心

Flow 日志输出至信息中心时，优先级为 informational，即作为设备的一般提示信息。

表1-9 配置 Flow 日志输出到信息中心

操作	命令	说明
进入系统视图	**system-view**	-
配置Flow日志输出到信息中心	**userlog flow syslog**	缺省情况下，Flow日志采用输出到日志主机的方式

1.8 Flow日志显示和维护

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 Flow 日志的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 Flow 日志信息。

表1-10 Flow 日志显示和维护

操作	命令
查看日志的配置和统计信息	**display userlog export**
清除Flow日志的统计信息	**reset userlog flow export**

1.9 Flow日志典型配置举例

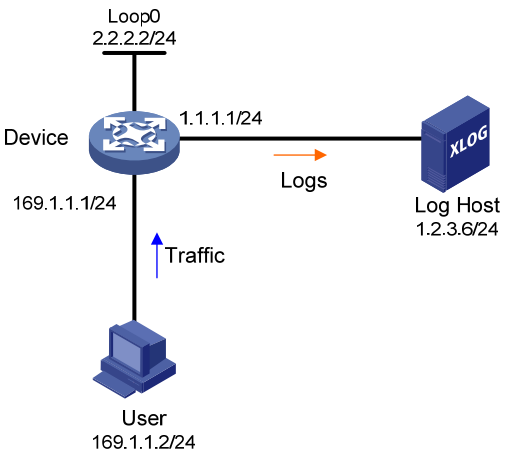
1.9.1 Flow日志配置举例

1. 组网需求

如 图 1-1 所示，用户通过在设备Device上的配置，从而实现在日志主机上（Log Host）对用户User的上网活动进行监控。

2. 组网图

图1-1 配置 Flow 日志组网图



3. 配置步骤

说明

按组网图所示配置各接口的 IP 地址，并确保 Device 与 User、Log Host 之间路由可达。

开启 NAT 日志功能。

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

开启 NAT 新建、删除会话和活跃流的日志功能。

```
[Device] nat log flow-begin
[Device] nat log flow-end
[Device] nat log flow-active 10
```

将 Flow 日志报文版本号设为 3.0。

```
[Device] userlog flow export version 3
```

将 Flow 日志信息发送给 Flow 日志主机（地址为 1.2.3.6:2000）。

```
[Device] userlog flow export host 1.2.3.6 port 2000
```

将 2.2.2.2 配置为承载 Flow 日志的 UDP 报文的源 IP 地址。

```
[Device] userlog flow export source-ip 2.2.2.2
[Device] quit
```

4. 验证结果

查看 Flow 日志的配置和统计信息。

```
<Device> display userlog export
Flow:
  Export flow log as UDP Packet.
  Version: 3.0
  Source address: 2.2.2.2
  Log load balance function: Disabled
  Log host numbers: 1

  Log host 1:
    IP address/Port: 1.2.3.6/2000
    Total logs/UDP packets exported: 112/87
```