UNIS R17900 核心路由器

日志信息参考

紫光恒越技术有限公司
www.unisyue.com

资料版本：6W100-20210120

目 录

1 简介

本文档介绍核心路由器日志信息，包含日志的参数介绍、产生原因、处理建议等，为用户进行系统诊断和维护提供参考。

本文假设您已具备数据通信技术知识，并熟悉 UNIS 网络产品。

1.1 日志格式说明

缺省情况下，日志信息根据输出方向不同，采用如下格式：

- 日志主机方向（RFC 3164 定义的格式）：

```
<PRI>TIMESTAMP Sysname %%vendorMODULE/severity/MNEMONIC: location; CONTENT
```

- 非日志主机方向：

```
Prefix TIMESTAMP Sysname MODULE/severity/MNEMONIC: CONTENT
```

表1-1 日志字段说明

字段	描述
<PRI>	优先级标识符，仅存在于输出方向为日志主机的日志信息。优先级的计算公式为：facility×8＋severity • facility 表示日志主机的记录工具，由 **info-center loghost** 命令设置，主要用于在日志主机端标志不同的日志来源，查找、过滤对应日志源的日志。 • severity 表示日志信息的严重等级，具体含义请参见表 1-2
Prefix	信息类型标识符，仅存在于输出方向为非日志主机方向的日志信息 • 百分号（%）：表示该日志信息为 Informational 级别及以上级别的日志 • 星号（*）：表示该日志信息为 Debug 级别的日志
TIMESTAMP	时间戳记录了日志信息产生的时间，方便用户查看和定位系统事件 • 日志主机方向：时间戳精确到秒，用户可以通过 **info-center timestamp loghost** 命令自定义时间显示格式 • 非日志主机方向：时间戳精确到毫秒，用户可以通过 **info-center timestamp** 命令自定义时间显示格式
Sysname	生成该日志信息的设备的名称或IP地址
%%vendor	厂家标志，%%10表示本日志信息由UNIS设备生成 只有发往日志主机的日志中携带该字段
MODULE	生成该日志信息的功能模块的名称
severity	日志信息的等级，具体说明请参见表1-2
MNEMONIC	助记符，本字段为该日志信息的概述，是一个不超过32个字符的字符串
location	定位信息，用来标识该日志信息的产生者。本字段为可选字段，只有在日志信息发往日志主机时才会存在，可能包含以下参数： • -MDC=XX，表示生成该日志的 MDC 的编号 • -DevIp=XXX.XXX.XXX.XXX，表示日志发送者的源 IP

字段	描述
	• -Chassis=XX-Slot=XX，表示生成该日志的 Chassis 编号和 Slot 编号 格式如下： -attribute1=x-attribute2=y…-attributeN=z 定位信息和日志描述之间用分号和空格“; ”分隔  说明 日志手册中以输出到非日志主机方向的日志为例，不提供 location 字段。
CONTENT	该日志的具体内容，包含事件或错误发生的详细信息 对于本字段中的可变参数域，本文使用表1-3定义的方式表示

日志信息按严重性可划分为如表 1-2 所示的八个等级，各等级的严重性依照数值从 0～7 依次降低。

表1-2 日志严重等级说明

级别	严重程度	描述
0	Emergency	表示设备不可用的信息，如系统授权已到期
1	Alert	表示设备出现重大故障，需要立刻做出反应的信息，如流量超出接口上限
2	Critical	表示严重信息，如设备温度已经超过预警值，设备电源、风扇出现故障等
3	Error	表示错误信息，如接口链路状态变化，存储卡拔出等
4	Warning	表示警告信息，如接口连接断开，内存耗尽告警等
5	Notification	表示正常出现但是重要的信息，如通过终端登录设备，设备重启等
6	Informational	表示需要记录的通知信息，如通过命令行输入命令的记录信息，执行ping命令的日志信息等
7	Debug	表示调试过程产生的信息

本文使用表 1-3 定义的方式表示日志描述字段中的可变参数域。

表1-3 可变参数域

参数标识	参数类型
INT16	有符号的16位整数
UINT16	无符号的16位整数
INT32	有符号的32位整数
UINT32	无符号的32位整数
INT64	有符号的64位整数
UINT64	无符号的64位整数
DOUBLE	有符号的双32位整数，格式为：[INT32].[INT32]
HEX	十六进制数

参数标识	参数类型
CHAR	字节类型
STRING	字符串类型
IPADDR	IP地址
MAC	MAC地址
DATE	日期
TIME	时间

1.2 如何获取日志信息

业务模块将生成的日志发送给信息中心模块，由信息中心模块统一管理。

缺省情况下，设备的信息中心功能处于开启状态，并允许向控制台（console）、监视终端（monitor）、日志缓冲区（logbuffer）、日志主机（loghost）和日志文件（logfile）方向输出日志信息。

通过 **info-center source** 命令可以设置日志信息的输出规则，通过输出规则可以指定日志的输出方向以及对哪些特性模块或信息等级的日志信息进行输出。所有信息等级高于或等于设置等级的日志信息都会被输出到指定的输出方向。例如，输出规则中如果指定允许等级为 6（informational）的信息输出，则等级 0～6 的信息均会被输出到指定的输出方向。

关于信息中心的详细描述请参见“网络管理和监控配置指导”中的“信息中心”。

1.2.1 通过控制台获取日志

用户通过 Console 接口登录设备后，可以在控制台上实时看到设备输出的日志。

1.2.2 通过监视终端获取日志

监视终端是指以 VTY 类型用户线登录的用户终端。使用监视终端登录设备后，如需在当前终端上显示日志，还需要进行以下配置：

- 执行 **terminal monitor** 命令打开终端显示功能
- 通过 **terminal logging level** 命令设置在当前终端上显示日志的级别。实际能够在终端上显示的日志级别由 **info-center source** 和 **terminal logging level** 命令共同决定。

terminal monitor 命令和 **terminal logging level** 命令只对当前登录生效，用户重新登录设备后，需要重新配置。

1.2.3 通过日志缓冲区获取日志

通过 **display logbuffer** 命令可以查看日志缓冲区中记录的日志。

1.2.4 通过日志文件获取日志

系统将日志保存到日志文件缓冲区后，用户可以通过以下方式将日志文件缓冲区中的日志保存到日志文件：

- 执行 **logfile save** 命令手动将日志文件缓冲区中的内容全部保存到日志文件。
- 系统周期性将日志文件缓冲区中的内容保存到日志文件。缺省情况下，系统自动保存日志文件的频率为 600 秒。用户可以通过 **info-center logfile frequency** 命令修改保存周期。

日志文件的缺省保存路径为存储设备根目录下的 logfile 目录。

通过 **more** 命令可以查看日志文件的内容。

1.2.5 通过日志主机获取日志

用户配置 **info-center loghost** 命令后，设备会向指定 IP 地址的日志主机发送日志，在日志主机上用户可以查看到设备的日志。如需指定多个日志主机，可多次执行 **info-center loghost** 命令。

请注意：设备上配置的日志主机接收日志信息的端口号必须和日志主机侧的设置一致，否则，日志主机将无法接收日志信息。这个端口号的缺省值为 514。

1.3 软件模块列表

表 1-4 列出了所有可能生成系统日志信息的软件模块。其中，“OPENSRC”代表所有开源软件模块的日志，本文使用“OPENSRC（开源软件名称）”表示不同开源软件模块输出的日志信息。

表1-4 软件模块列表

模块名	模块全称
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AFT	Address Family Translation
ARP	Address Resolution Protocol
ATK	ATK Detect and Defense
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BLS	Blacklist
CFD	Connectivity Fault Detection
CFGMAN	Configuration Management
CLKM	Clock Monitoring
DEV	Device Management
DHCP	Dynamic Host Configuration Protocol
DHCPR	IPv4 DHCP Relay

模块名	模块全称
DHCPS	IPv4 DHCP Server
DHCPS6	IPv6 DHCP Server
DHCPSP4	IPv4 DHCP snooping
DHCPSP6	IPv6 DHCP snooping
DIAG	Diagnosis
DLDP	Device Link Detection Protocol
EDEV	Extender Device Management
ETH	Ethernet
ETHOAM	Ethernet Operation, Administration and Maintenance
FIB	Forwarding Information Base
FILTER	Filter
FTP	File Transfer Protocol
gRPC	Google Remote Procedure Call
HA	High Availability
HTTPD	Hypertext Transfer Protocol Daemon
IFMON	Interface Monitor
IFNET	Interface Net Management
IKE	Internet Key Exchange
IP6ADDR	IPv6 address
IP6FW	IPv6 Forwarding
IPADDR	IP address
IPFW	IP Forwarding
IPSEC	IP Security
IRDP	ICMP Router Discovery Protocol
ISIS	Intermediate System-to-Intermediate System
ISSU	In-Service Software Upgrade
L2VPN	Layer 2 VPN
LAGG	Link Aggregation
LDP	Label Distribution Protocol
LIPC	Leopard Inter-process Communication
LLDP	Link Layer Discovery Protocol
LOAD	Load Management
LOCAL	Local
LOGIN	Login
LS	Local Server

模块名	模块全称
LSM	Label Switch Management
LSPV	LSP Verification
MAC	Media Access Control
MBFD	MPLS BFD
MBUF	Memory Buffer
MDC	Multitenant Device Context
MFIB	Multicast Forwarding Information Base
MGROUP	Mirroring group
MPLS	Multiprotocol Label Switching
MTLK	Monitor Link
MTP	Maintain Probe
NAT	Network Address Translate
ND	Neighbor Discovery
NETCONF	Network Configuration Protocol
NQA	Network Quality Analyzer
NTP	Network Time Protocol
OFP	OpenFlow Protocol
OPTMOD	Optical Module
OSPF	Open Shortest Path First
OSPFV3	Open Shortest Path First Version 3
PBR	Policy Based Route
PCE	Path Computation Element
PFILTER	Packet Filter
PIM	Protocol Independent Multicast
PING	Packet Internet Groper
PKI	Public Key Infrastructure
PKT2CPU	Packet to CPU
PKTCPT	Packet Capture
PPP	Point to Point Protocol
PTP	Precision Time Protocol
PWDCTL	Password Control
QOS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RIP	Routing Information Protocol
RIPNG	Routing Information Protocol Next Generation

模块名	模块全称
RM	Routing Management
RSVP	Resource Reservation Protocol
RTM	Real-Time Management
SCM	Service Control Manager
SCRLSP	Static CRLSP
SESSION	Session
SHELL	Shell
SLSP	Static LSP
SNMP	Simple Network Management Protocol
SSHC	Secure Shell Client
SSHS	Secure Shell Server
STP	Spanning Tree Protocol
STRUNK	Smart Trunk
SYSEVENT	System Event
SYSLOG	System Log
TACACS	Terminal Access Controller Access Control System
TE	Traffic Engineering
TELNETD	Telnet Daemon
UCM	User Connection Management
URPF	Unicast Reverse Path Forwarding
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
VSRP	Virtual Service Redundancy Protocol
VXLAN	Virtual eXtensible LAN
产品日志	产品日志

1.4 文档使用说明

本文将系统日志信息按照软件模块分类，每个模块以字母顺序排序。在每个模块中，系统日志信息按照助记符的名称，以字母顺序排序。在开源软件模块输出的日志信息中，助记符均为 SYSLOG，本文使用日志简要描述作为该类日志信息标题，不做特殊排序。

本文以表格的形式对日志信息进行介绍。有关表中各项的含义请参考表 1-5。

表1-5 日志信息表内容说明

表项	说明	举例
日志内容	显示日志信息的具体内容	ACL [UINT32] [STRING] [COUNTER64] packet(s).
参数解释	按照参数在日志中出现的顺序对参数进行解释 参数顺序用“$数字”表示，例如“$1”表示在该日志中出现的第一个参数	$1：ACL编号 $2：ACL规则的ID和内容 $3：与ACL规则匹配的数据包个数
日志等级	日志严重等级	6
举例	一个真实的日志信息举例。由于不同的系统设置，日志信息中的“<Int_16>TIMESTAMP HOSTNAME %%vendor”部分也会不同，本文表格中的日志信息举例不包含这部分内容	ACL/6/ACL_STATIS_INFO: ACL 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
日志说明	解释日志信息和日志生成的原因	匹配一条ACL规则的数据包个数。该日志会在数据包个数发生变化时输出
处理建议	建议用户应采取哪些处理措施。级别为6的“Informational”日志信息是正常运行的通知信息，用户无需处理	系统正常运行时产生的信息，无需处理

2 AAA

本节介绍 AAA 模块输出的日志信息。

2.1 AAA_FAILURE

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA failed.
参数解释	$1：AAA类型 $2：AAA方案 $3：服务 $4：用户名称
日志等级	5
举例	AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA failed.
日志说明	由于未收到服务器响应，用户名/密码错误，或其他原因（例如用户申请的服务类型不正确），用户的AAA请求被拒绝
处理建议	• 检查设备与服务器的连接 • 重新输入用户名和密码 • 检查服务器上的设置（例如服务类型）是否正确

2.2 AAA_LAUNCH

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA launched.
参数解释	$1：AAA类型 $2：AAA方案 $3：服务 $4：用户名称
日志等级	6
举例	AAA/6/AAA_LAUNCH: -AAAType=AUTHEN-AAADomain=domain1-Service=login-UserName=cwf@system; AAA launched.
日志说明	用户发送AAA请求
处理建议	无

2.3 AAA_SUCCESS

日志内容	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA succeeded.
参数解释	$1：AAA类型 $2：AAA方案 $3：服务 $4：用户名称
日志等级	6
举例	AAA/6/AAA_SUCCESS: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA succeeded.
日志说明	接受用户的AAA请求
处理建议	无

3 ACL

本节介绍 ACL 模块输出的日志信息。

3.1 ACL_ACCELERATE_NO_RES

日志内容	Failed to accelerate [STRING] ACL [UINT32]. The resources are insufficient.
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NO_RES: Failed to accelerate IPv6 ACL 2001. The resources are insufficient.
日志说明	因硬件资源不足，系统加速ACL失败
处理建议	删除一些规则或者关闭其他ACL的加速功能，释放硬件资源

3.2 ACL_ACCELERATE_NONCONTIGUOUSMASK

日志内容	Failed to accelerate ACL [UINT32]. ACL acceleration supports only contiguous wildcard masks.
参数解释	$1：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NONCONTIGUOUSMASK: Failed to accelerate ACL 2001. ACL acceleration supports only contiguous wildcard masks.
日志说明	因IPv4 ACL中的规则指定了非连续的掩码，导致ACL加速失败
处理建议	检查ACL规则并删除不支持的配置

3.3 ACL_ACCELERATE_NOT_SUPPORT

日志内容	Failed to accelerate [STRING] ACL [UINT32]. The operation is not supported.
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 ACL 2001. The operation is not supported.
日志说明	因系统不支持ACL加速而导致ACL加速失败
处理建议	无

3.4 ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP

日志内容	Failed to accelerate IPv6 ACL [UINT32]. ACL acceleration does not support the rules that contain the hop-by-hop keywords.
参数解释	$1：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP: Failed to accelerate IPv6 ACL 2001. ACL acceleration does not support the rules that contain the hop-by-hop keywords.
日志说明	因IPv6 ACL中的规则指定了hop-by-hop参数，导致ACL加速失败
处理建议	检查ACL规则并删除不支持的配置

3.5 ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG

日志内容	Failed to accelerate IPv6 ACL [UINT32]. ACL acceleration does not support specifying multiple TCP flags in one rule.
参数解释	$1：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG: Failed to accelerate IPv6 ACL 2001. ACL acceleration does not support specifying multiple TCP flags in one rule.
日志说明	因IPv6 ACL中的规则指定了多个Tcp Flag参数，导致ACL加速失败
处理建议	检查ACL规则并删除不支持的配置

3.6 ACL_ACCELERATE_UNK_ERR

日志内容	Failed to accelerate [STRING] ACL [UINT32].
参数解释	$1：ACL类型 $2：ACL编号
日志等级	4
举例	ACL/4/ACL_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 ACL 2001.
日志说明	因系统故障导致ACL加速失败
处理建议	无

3.7 ACL_IPV6_STATIS_INFO

日志内容	IPv6 ACL [UINT32] [STRING] [UINT64] packet(s).
参数解释	$1：ACL编号 $2：IPv6 ACL规则的ID及内容 $3：匹配上规则的报文个数
日志等级	6
举例	ACL/6/ACL_IPV6_STATIS_INFO: IPv6 ACL 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
日志说明	匹配上IPv6 ACL规则的报文数量发生变化
处理建议	无

3.8 ACL_NO_MEM

日志内容	Failed to configure [STRING] ACL [UINT] due to lack of memory
参数解释	$1：ACL类型 $2：ACL编号
日志等级	3
举例	ACL/3/ACL_NO_MEM: Failed to configure ACL 2001 due to lack of memory.
日志说明	内存不足导致配置ACL失败
处理建议	使用**display memory-threshold**命令检查内存使用情况

3.9 ACL_STATIS_INFO

日志内容	ACL [UINT32] [STRING] [UINT64] packet(s).
参数解释	$1：ACL编号 $2：IPv4 ACL规则的ID及内容 $3：匹配上规则的报文个数
日志等级	6
举例	ACL/6/ACL_STATIS_INFO: ACL 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
日志说明	匹配上IPv4 ACL规则的报文数量发生变化
处理建议	无

4 AFT

本节介绍 AFT 模块输出的日志信息。

4.1 AFT_ADDRESS_CONFLICT

日志内容	Address range (StartIp=[IPADDR];EndIp=[IPADDR]) assigned by the CP conflicts with an existing address group.
参数解释	$1：开始IPv4地址 $2：结束IPv4地址
日志等级	6
举例	AFT/6/AFT_ADDRESS_CONFLICT: Address range (StartIp=1.1.0.0;EndIp=1.1.0.255) assigned by the CP conflicts with an existing address group.
日志说明	转控分离组网环境，CP分配给UP的地址段与UP上已经配置地址段冲突时，生成该日志
处理建议	建议排查设备地址段配置，修改地址冲突配置

4.2 AFT_LOG_FLOW

日志内容	AFT PORTBLOCK was [STRING]: IPv6addr=[IPADDR]; VPNNameV6=[STRING]; ipv4addr=[IPADDR]; VPNNameV4=[STRING]; PortBlockSize=[UINT16]-[UINT16]; BeginTime_e=[STRING]; EndTime_e=[STRING].
参数解释	$1：事件类型 • allocated：端口块分配 • free：端口块释放 $2：IPv6地址 $3：IPv6所属VPN名称 $4：IPv4地址 $5：IPv4所属VPN名称 $6：分配的端口块中的起始值 $7：分配的端口块中的结束值 $8：端口块分配时间 $9：端口块释放时间
日志等级	6
举例	AFT/6/AFT_LOG_FLOW: AFT PORTBLOCK was free: IPv6addr=1000::1b; VPNNameV6=-; IPv4addr=10.0.0.140; VPNNameV4=-; PortBlockSize=1024-1535; BeginTime_e=03232017053558; EndTime_e=03232017065040.
日志说明	分配或释放端口块时生成该日志
处理建议	无

4.3 AFT_V6TOV4_FLOW

日志内容	Protocol(1001)= [STRING];SrcIPv6Addr(1036)= [IPADDR];SrcPort(1004)= [UINT16];NatSrcIPAddr(1005)= [IPADDR];NatSrcPort(1006)= [UINT16];DstIPv6Addr(1037)= [IPADDR];DstPort(1008)= [UINT16];NatDstIPAddr(1009)= [IPADDR];NatDstPort(1010)= [UINT16];InitPktCount(1044)= [UINT32];InitByteCount(1046)= [UINT32];RplyPktCount(1045)= [UINT32];RplyByteCount(1047)= [UINT32];RcvVPNInstance(1042)= [STRING];SndVPNInstance(1043)= [STRING];BeginTime_e(1013)= [STRING];EndTime_e(1014)= [STRING];Event(1048)= ([UNIT16])[STRING].
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：转换后的源IP地址 $5：转换后的源端口号 $6：目的IPv6地址 $7：目的端口号 $8：转换后的目的IP地址 $9：转换后的目的端口号 $10：入方向的报文总数 $11：入方向的字节总数 $12：出方向的报文总数 $13：出方向的字节总数 $14：源VPN名称 $15：目的VPN名称 $16：创建会话的时间 $17：会话删除时间 $18：日志类型 $19：日志类型描述信息 ○ Session created：AFT 会话创建 ○ Session ended：正常流结束，AFT 会话删除 ○ Session aged out：AFT 会话老化删除 ○ Session deleted through configuration：通过配置删除 AFT 会话 ○ Other：其他原因删除 AFT 会话，如由其他模块删除
日志等级	6
举例	AFT/6/AFT_V6TOV4_FLOW: Protocol(1001)=IPv6-ICMP;SrcIPv6Addr(1036)=1000::10;SrcPort(1004)=1;NatSrcIPAddr(1005)=9.9.9.9;NatSrcPort(1006)=1027;DstIPv6Addr(1037)=2000::201:102;DstPort(1008)=32768;NatDstIPAddr(1009)=2.1.1.2;NatDstPort(1010)=2048;InitPktCount(1044)=177411959;InitByteCount(1046)=2122604543;RplyPktCount(1045)=1895856127;RplyByteCount(1047)=30720;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=05052017134514;EndTime_e(1014)=;Event(1048)=(8)Session created.
日志说明	创建、删除IPv6侧发起的会话时生成该日志
处理建议	无

4.4 AFT_V4TOV6_FLOW

日志内容	Protocol(1001)= [STRING]; SrcIPAddr(1003)= [IPADDR];SrcPort(1004)= [UINT16]; NatSrcIPv6Addr(1038)= [IPADDR];NatSrcPort(1006)= [UINT16]; DstIPAddr(1003)= [IPADDR];DstPort(1008)= [UINT16]; NatDstIPv6Addr(1039)= [IPADDR];NatDstPort(1010)= [UINT16];InitPktCount(1044)= [UINT32];InitByteCount(1046)= [UINT32];RplyPktCount(1045)= [UINT32];RplyByteCount(1047)= [UINT32];RcvVPNInstance(1042)= [STRING];SndVPNInstance(1043)= [STRING];BeginTime_e(1013)= [STRING];EndTime_e(1014)= [STRING];Event(1048)= ([UNIT16])[STRING].
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $4：转换后的源IP地址 $5：转换后的源端口号 $6：目的IPv6地址 $7：目的端口号 $8：转换后的目的IP地址 $9：转换后的目的端口号 $10：入方向的报文总数 $11：入方向的字节总数 $12：出方向的报文总数 $13：出方向的字节总数 $14：源VPN名称 $15：目的VPN名称 $16：创建会话的时间 $17：会话删除时间 $18：日志类型 $19：日志类型描述信息 ○ Session created：AFT 会话创建 ○ Session ended：正常流结束，AFT 会话删除 ○ Session aged out：AFT 会话老化删除 ○ Session deleted through configuration：通过配置删除 AFT 会话 ○ Other：其他原因删除 AFT 会话，如由其他模块删除
日志等级	6
举例	AFT/6/AFT_V4TOV6_FLOW: Protocol(1001)=ICMP;SrcIPAddr(1003)=2.1.1.4;SrcPort(1004)=197;NatSrcIPv6Addr(1038)=2000::201:104;NatSrcPort(1006)=197;DstIPAddr(1003)=5.5.5.5;DstPort(1008)=2048;NatDstIPv6Addr(1039)=1000::;NatDstPort(1010)=32768;InitPktCount(1044)=2092588805;InitByteCount(1046)=1166331903;RplyPktCount(1045)=1895856127;RplyByteCount(1047)=30720;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=05052017152731;EndTime_e(1014)=;Event(1048)=(8)Session created.
日志说明	创建、删除IPv4侧发起的会话时生成该日志
处理建议	无

5 ARP

本节介绍 ARP 模块输出的日志信息。

5.1 ARP_ACTIVE_ACK_NO_REPLY

日志内容	No ARP reply from IP [STRING] was received on interface [STRING].
参数解释	$1：IP 地址 $2：接口名称
日志等级	6
举例	ARP/6/ARP_ACTIVE_ACK_NO_REPLY: No ARP reply from IP 192.168.10.1 was received on interface GigabitEthernet1/2/0/1.
日志说明	ARP主动确认功能检测到攻击 接口向所收到ARP报文的发送端IP发送ARP请求，未收到ARP应答
处理建议	**1.** 检查设备上学习到的 ARP 表项中的 IP 和 MAC 是否对应（如果网络部署中存在网关和服务器，优先检查网关和服务器的 IP 和 MAC 是否对应） **2.** 请联系系统支持

5.2 ARP_ACTIVE_ACK_NOREQUESTED_REPLY

日志内容	Interface [STRING] received from IP [STRING] an ARP reply that was not requested by the device.
参数解释	$1：接口名称 $2：IP地址
日志等级	4
举例	ARP/4/ARP_ACTIVE_ACK_NOREQUESTED_REPLY: Interface GigabitEthernet1/2/0/1 received from IP 192.168.10.1 an ARP reply that was not requested by the device.
日志说明	ARP主动确认功能检测到攻击 接口在未向ARP报文发送端IP地址发送ARP请求的情况下，收到ARP应答
处理建议	设备丢弃该ARP应答

5.3 ARP_BINDRULETOHW_FAILED

日志内容	Failed to download binding rule to hardware on the interface [STRING], SrcIP [IPADDR], SrcMAC [MAC], VLAN [UINT16], Gateway MAC [MAC].
参数解释	$1：接口名称. $2：源IP地址 $3：源MAC地址. $4：VLAN编号. $5：网关MAC地址.
日志等级	5
举例	ARP/5/ARP_BINDRULETOHW_FAILED: Failed to download binding rule to hardware on the interface Ethernet1/2/0/1, SrcIP 1.1.1.132, SrcMAC 0015-E944-A947, VLAN 1, Gateway MAC 00A1-B812-1108.
日志说明	由于硬件资源不足、内存不足或其他硬件错误导致绑定规则下发失败
处理建议	**3.** 使用 **`display qos-acl resource`** 查看硬件 ACL 资源是否充足 o 如果充足，则请执行步骤 2 o 如果不充足，则请取消部分 ACL 配置或接受当前结果 **4.** 使用 **`display memory`** 查看内存资源是否充足 o 如果充足，则请执行步骤 3 o 如果不充足，则请取消部分配置或接受当前结果 **5.** 硬件发生错误，请取消最后一次相关配置，并重新尝试

5.4 ARP_DUPLICATE_IPADDR_DETECT

日志内容	Detected an IP address conflict. The device with MAC address [STRING] connected to interface [STRING] in VSI [STRING] and the device with MAC address [STRING] connected to interface [STRING] in VSI [STRING] were using the same IP address [IPADDR].
参数解释	$1：MAC 地址 $2：接口名称（包括Tunnel口、三层接口和以太网服务实例等） $3：VSI名称 $4：冲突对端的源MAC地址 $5：冲突对端的源接口名称（包括Tunnel口、三层接口和以太网服务实例等） $6：冲突对端的VSI名称 $7：冲突的IP地址
日志等级	6
举例	ARP/6/ARP_DUPLICATE_IPADDR_DETECT: Detected an IP address conflict. The device with MAC address 00-00-01 connected to interface Ethernet1/2/0/1 service-instance 1000 in VSI vpna and the device with MAC address 00-00-02 connected to interface tunnel 10 in VSI vpna were using the same IP address 192.168.1.1.
日志说明	ARP检测到重复地址 接口收到ARP报文中发送端的IP地址，与本设备学习到的ARP表项中的IP地址冲突
处理建议	修改IP地址

5.5 ARP_DYNAMIC

日志内容	The maximum number of dynamic ARP entries for the device reached.
参数解释	无
日志等级	6
举例	ARP/6/ARP_DYNAMIC: The maximum number of dynamic ARP entries for the device reached.
日志说明	设备学到的ARP表项总数到达最大值，打印该提示日志
处理建议	无需处理

5.6 ARP_DYNAMIC_IF

日志内容	The maximum number of dynamic ARP entries for interface [STRING] reached.
参数解释	$1：接口名
日志等级	6
举例	ARP/6/ARP_DYNAMIC_IF: The maximum number of dynamic ARP entries for interface GigabitEthernet1/2/0/1 reached.
日志说明	接口学到的ARP表项总数到达最大值，打印该提示日志
处理建议	无需处理

5.7 ARP_DYNAMIC_SLOT

日志内容	形式一： The maximum number of dynamic ARP entries for slot [INT32] reached. 形式二： The maximum number of dynamic ARP entries for chassis [INT32] slot [INT32] reached.
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	6
举例	ARP/6/ARP_DYNAMIC_SLOT: The maximum number of dynamic ARP entries for slot 2 reached. ARP/6/ARP_DYNAMIC_SLOT: The maximum number of dynamic ARP entries for chassis 1 slot 2 reached.
日志说明	形式一： 指定slot学到的动态ARP表项数达到最大值 形式二： 指定chassis内slot上学到的动态ARP表项数达到最大值
处理建议	无需处理

5.8 ARP_ENTRY_CONFLICT

日志内容	The software entry for [STRING] on [STRING] and the hardware entry did not have the same [STRING].
参数解释	$1：IP地址 $2：VPN实例名。如果该ARP属于公网，显示为the public network $3：不一致的表项参数类型 • MAC address：MAC 地址 • output interface：ARP 表项的出接口 • output port ：ARP 表项的出端口 • outermost layer VLAN ID：第一层 VLAN 标签 • second outermost layer VLAN ID：第二层 VLAN 标签 • VSI index：VSI 索引 • link ID：VSI 出链路标识符
日志等级	6
举例	ARP/6/ARP_ENTRY_CONFLICT: The software entry for 1.1.1.1 on the VPN a and the hardware entry did not have the same MAC address, output port, VSI index, and link ID. ARP/6/ARP_ENTRY_CONFLICT: The software entry for 1.1.1.2 on the public network and the hardware entry did not have the same MAC address, output port, VSI index, and link ID.
日志说明	ARP软件表项与硬件表项不一致，比如ARP表项的出接口
处理建议	不需要处理，ARP会主动重刷硬件表项

5.9 ARP_HOST_IP_CONFLICT

日志内容	The host [STRING] connected to interface [STRING] cannot communicate correctly, because it uses the same IP address as the host connected to interface [STRING].
参数解释	$1：IP地址 $2：接口名 $3：接口名
日志等级	4
举例	ARP/4/ARP_HOST_IP_CONFLICT: The host 1.1.1.1 connected to interface GigabitEthernet1/2/0/1 cannot communicate correctly, because it uses the same IP address as the host connected to interface GigabitEthernet1/2/0/2.
日志说明	接口收到主机ARP报文中的源IP与其他接口连接的主机的IP地址冲突
处理建议	检查发送ARP报文的主机的合法性。如果非法，需要断开该主机网络

5.10 ARP_RATE_EXCEEDED

日志内容	The ARP packet rate ([UINT32] pps) exceeded the rate limit ([UINT32] pps) on interface [STRING] in the last [UINT32] seconds.
参数解释	$1：ARP报文速率 $2：ARP报文限速速率 $3：接口名称 $4：间隔时间
日志等级	4
举例	ARP/4/ARP_RATE_EXCEEDED: The ARP packet rate (100 pps) exceeded the rate limit (80 pps) on interface Ethernet1/2/0/1 in the last 10 seconds.
日志说明	接口接收ARP报文速率超过了接口的限速值
处理建议	检查ARP报文发送主机的合法性

5.11 ARP_RATELIMIT_NOTSUPPORT

日志内容	形式一： ARP packet rate limit is not support on slot [INT32]. 形式二： ARP packet rate limit is not support on chassis [INT32] slot [INT32].
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	6
举例	ARP/6/ARP_RATELIMIT_NOTSUPPORT: ARP packet rate limit is not support on slot 2.
日志说明	形式一： 指定slot不支持ARP报文限速功能 形式二： 指定chassis内slot不支持ARP报文限速功能
处理建议	无需处理

5.12 ARP_SENDER_IP_INVALID

日志内容	Sender IP [STRING] was not on the same network as the receiving interface [STRING].
参数解释	$1：IP地址 $2：接口名称
日志等级	6
举例	ARP/6/ARP_SENDER_IP_INVALID: Sender IP 192.168.10.2 was not on the same network as the receiving interface GigabitEthernet1/2/0/1.
日志说明	接口收到ARP报文中发送端IP与本接口不在同一网段
处理建议	检查发送端IP对应主机的合法性

5.13 ARP_SENDER_MAC_INVALID

日志内容	Sender MAC [STRING] was not identical to Ethernet source MAC [STRING] on interface [STRING].
参数解释	$1：MAC 地址 $2：MAC 地址 $3：接口名称
日志等级	4
举例	ARP/4/ARP_SENDER_MAC_INVALID: Sender MAC dc2d-cb14-0E00 was not identical to Ethernet source MAC dc2d-cb14-0E00 on interface GigabitEthernet1/2/0/1.
日志说明	接口收到ARP报文的以太网数据帧首部中的源MAC地址和ARP报文中的发送端MAC地址不同
处理建议	检查发送端MAC地址对应主机的合法性

5.14 ARP_SRC_MAC_FOUND_ATTACK

日志内容	An attack from MAC [STRING] was detected on interface [STRING].
参数解释	$1：MAC 地址 $2：接口名称
日志等级	6
举例	ARP/6/ARP_SRC_MAC_FOUND_ATTACK: An attack from MAC dc2d-cb14-0E00 was detected on interface GigabitEthernet1/2/0/1.
日志说明	源MAC地址固定的ARP攻击检测功能检测到攻击 5秒内，收到同一源MAC地址（源MAC地址固定）的ARP报文超过一定的阈值
处理建议	检查该源MAC地址对应主机的合法性

5.15 ARP_TARGET_IP_INVALID

日志内容	Target IP [STRING] was not the IP of the receiving interface [STRING].
参数解释	$1：IP 地址 $2：接口名称
日志等级	6
举例	ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.10.2 was not the IP of the receiving interface Ethernet1/2/0/1.
日志说明	接口收到ARP报文中的目标IP与本接口IP不一致
处理建议	检查发送ARP报文的主机的合法性

5.16 DUPIFIP

日志内容	Duplicate address [STRING] on interface [STRING], sourced from [STRING].
参数解释	$1：IP 地址 $2：接口名称 $3：MAC 地址
日志等级	6
举例	ARP/6/DUPIFIP: Duplicate address 1.1.1.1 on interface Ethernet1/2/0/1, sourced from 0015-E944-A947.
日志说明	ARP检测到重复地址 接口收到ARP报文的发送端IP地址与该接口的IP地址重复
处理建议	修改IP地址配置

5.17 DUPIP

日志内容	IP address [STRING] conflicted with global or imported IP address, sourced from [STRING].
参数解释	$1：IP 地址 $2：MAC 地址
日志等级	6
举例	ARP/6/DUPIP: IP address 30.1.1.1 conflicted with global or imported IP address, sourced from dc2d-cb00-0001.
日志说明	收到ARP报文中的发送端IP地址与全局或导入的IP地址冲突
处理建议	修改IP地址配置

5.18 DUPVRRPIP

日志内容	IP address [STRING] conflicted with VRRP virtual IP address on interface [STRING], sourced from [STRING].
参数解释	$1：IP 地址 $2：接口名称 $3：MAC 地址
日志等级	6
举例	ARP/6/DUPVRRPIP: IP address 1.1.1.1 conflicted with VRRP virtual IP address on interface Ethernet1/2/0/1, sourced from 0015-E944-A947.
日志说明	收到ARP报文中的发送端IP与VRRP虚拟IP地址冲突
处理建议	修改IP地址配置

5.19 L3_COMMON

日志内容	形式一： The Board on slot [INT32] doesn't support the ARP safe-guard function. 形式二： The Board on chassis t [INT32] slot [INT32] doesn't support the ARP safe-guard function.
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	4
举例	L3/4/L3_COMMON: -MDC=1-Slot=5; The Board on slot 5 doesn't support the ARP safe-guard function.
日志说明	形式一： 指定slot不支持ARP双向分离功能 形式二： 指定chassis内slot不支持ARP双向分离功能
处理建议	使用支持ARP双向分离功能的单板的接口

6 ATK

本节介绍 ATK 模块输出的日志信息。

6.1 ATK_ICMP_ADDRMASK_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ: IcmpType(1058)=17; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP地址掩码请求报文数超过1，聚合后触发日志
处理建议	无

6.2 ATK_ICMP_ADDRMASK_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW: IcmpType(1058)=17; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP地址掩码请求报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码请求报文触发一个日志
处理建议	无

6.3 ATK_ICMP_ADDRMASK_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW_SZ: IcmpType(1058)=17; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP地址掩码请求报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码请求报文触发一个日志
处理建议	无

6.4 ATK_ICMP_ADDRMASK_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_REQ_SZ: IcmpType(1058)=17; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP地址掩码请求报文数超过1，聚合后触发日志
处理建议	无

6.5 ATK_ICMP_ADDRMASK_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL: IcmpType(1058)=18; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP地址掩码应答报文数超过1，聚合后触发日志
处理建议	无

6.6 ATK_ICMP_ADDRMASK_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW: IcmpType(1058)=18; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP地址掩码应答报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码应答报文触发一个日志
处理建议	无

6.7 ATK_ICMP_ADDRMASK_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW_SZ: IcmpType(1058)=18; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP地址掩码应答报文首包触发日志；日志聚合开关关闭，每个ICMP地址掩码应答报文触发一个日志
处理建议	无

6.8 ATK_ICMP_ADDRMASK_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ADDRMASK_RPL_SZ: IcmpType(1058)=18; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP地址掩码应答报文数超过1，聚合后触发日志
处理建议	无

6.9 ATK_ICMP_ECHO_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ: IcmpType(1058)=8; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP请求回显报文数超过1，聚合后触发日志
处理建议	无

6.10 ATK_ICMP_ECHO_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1004)=[UINT16]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：目的端口 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW: IcmpType(1058)=8; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DstPort(1004)=22; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP请求回显报文首包触发日志；日志聚合开关关闭，每个ICMP请求回显报文触发一个日志
处理建议	无

6.11 ATK_ICMP_ECHO_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1004)=[UINT16]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：目的端口 $7：VPN名称 $8：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_RAW_SZ: IcmpType(1058)=8; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DstPort(1004)=22; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP请求回显报文首包触发日志；日志聚合开关关闭，每个ICMP请求回显报文触发一个日志
处理建议	无

6.12 ATK_ICMP_ECHO_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_REQ_SZ: IcmpType(1058)=8; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP请求回显报文数超过1，聚合后触发日志
处理建议	无

6.13 ATK_ICMP_ECHO_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL: IcmpType(1058)=0; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP回显应答报文数超过1，聚合后触发日志
处理建议	无

6.14 ATK_ICMP_ECHO_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW: IcmpType(1058)=0; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP回显应答报文首包触发日志；日志聚合开关关闭，每个ICMP回显应答报文触发一个日志
处理建议	无

6.15 ATK_ICMP_ECHO_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_RAW_SZ: IcmpType(1058)=0; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP回显应答报文首包触发日志；日志聚合开关关闭，每个ICMP回显应答报文触发一个日志
处理建议	无

6.16 ATK_ICMP_ECHO_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_ECHO_RPL_SZ: IcmpType(1058)=0; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP回显应答报文数超过1，聚合后触发日志
处理建议	无

6.17 ATK_ICMP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_ICMP_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的ICMP报文数超过阈值，触发日志
处理建议	无

6.18 ATK_ICMP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_ICMP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的ICMP报文数超过阈值，触发日志
处理建议	无

6.19 ATK_ICMP_INFO_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ: IcmpType(1058)=15; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP信息请求的报文数超过1，聚合后触发日志
处理建议	无

6.20 ATK_ICMP_INFO_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW: IcmpType(1058)=15; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP信息请求的报文首包触发日志；日志聚合开关关闭，每个ICMP信息请求的报文触发一个日志
处理建议	无

6.21 ATK_ICMP_INFO_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_RAW_SZ: IcmpType(1058)=15; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP信息请求的报文首包触发日志；日志聚合开关关闭，每个ICMP信息请求的报文触发一个日志
处理建议	无

6.22 ATK_ICMP_INFO_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_REQ_SZ: IcmpType(1058)=15; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP信息请求的报文数超过1，聚合后触发日志
处理建议	无

6.23 ATK_ICMP_INFO_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL: IcmpType(1058)=16; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP信息应答的报文数超过1，聚合后触发日志
处理建议	无

6.24 ATK_ICMP_INFO_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW: IcmpType(1058)=16; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP信息应答的报文首包触发日志；日志聚合开关关闭，每个ICMP信息应答的报文触发一个日志
处理建议	无

6.25 ATK_ICMP_INFO_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_RAW_SZ: IcmpType(1058)=16; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP信息应答的报文首包触发日志；日志聚合开关关闭，每个ICMP信息应答的报文触发一个日志
处理建议	无

6.26 ATK_ICMP_INFO_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_INFO_RPL_SZ: IcmpType(1058)=16; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP信息应答的报文数超过1，聚合后触发日志
处理建议	无

6.27 ATK_ICMP_LARGE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_LARGE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP超大报文数超过1，聚合后触发日志
处理建议	无

6.28 ATK_ICMP_LARGE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_LARGE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP超大报文首包触发日志；日志聚合开关关闭，每个ICMP超大报文触发一个日志
处理建议	无

6.29 ATK_ICMP_LARGE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_LARGE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP超大报文首包触发日志；日志聚合开关关闭，每个ICMP超大报文触发一个日志
处理建议	无

6.30 ATK_ICMP_LARGE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_LARGE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP超大报文数超过1，聚合后触发日志
处理建议	无

6.31 ATK_ICMP_PARAPROBLEM

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM: IcmpType(1058)=12; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP参数错误的报文数超过1，聚合后触发日志
处理建议	无

6.32 ATK_ICMP_PARAPROBLEM_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW: IcmpType(1058)=12; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP参数错误的报文首包触发日志；日志聚合开关关闭，每个ICMP参数错误的报文触发一个日志
处理建议	无

6.33 ATK_ICMP_PARAPROBLEM_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_RAW_SZ: IcmpType(1058)=12; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP参数错误的报文首包触发日志；日志聚合开关关闭，每个ICMP参数错误的报文触发一个日志
处理建议	无

6.34 ATK_ICMP_PARAPROBLEM_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_PARAPROBLEM_SZ: IcmpType(1058)=12; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP参数错误的报文数超过1，聚合后触发日志
处理建议	无

6.35 ATK_ICMP_PINGOFDEATH

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文数超过1，聚合后触发日志
处理建议	无

6.36 ATK_ICMP_PINGOFDEATH_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文首包触发日志；日志聚合开关关闭，每个标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文触发一个日志
处理建议	无

6.37 ATK_ICMP_PINGOFDEATH_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文首包触发日志；日志聚合开关关闭，每个标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文触发一个日志
处理建议	无

6.38 ATK_ICMP_PINGOFDEATH_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_PINGOFDEATH_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，标志位设置为最后一片并且(IP offset * 8) + (IP data lenth) > 65535 的ICMP报文数超过1，聚合后触发日志
处理建议	无

6.39 ATK_ICMP_REDIRECT

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT: IcmpType(1058)=5; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP重定向报文数超过1，聚合后触发日志
处理建议	无

6.40 ATK_ICMP_REDIRECT_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_RAW: IcmpType(1058)=5; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP重定向报文首包触发日志；日志聚合开关关闭，每个ICMP重定向报文触发一个日志
处理建议	无

6.41 ATK_ICMP_REDIRECT_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_RAW_SZ: IcmpType(1058)=5; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP重定向报文首包触发日志；日志聚合开关关闭，每个ICMP重定向报文触发一个日志
处理建议	无

6.42 ATK_ICMP_REDIRECT_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_REDIRECT_SZ: IcmpType(1058)=5; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP重定向报文数超过1，聚合后触发日志
处理建议	无

6.43 ATK_ICMP_SMURF

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文数超过1，聚合后触发日志
处理建议	无

6.44 ATK_ICMP_SMURF_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文首包触发日志 日志聚合开关关闭，符合上述条件的ICMP请求回显报文，每个报文触发一个日志
处理建议	无

6.45 ATK_ICMP_SMURF_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文首包触发日志 日志聚合开关关闭，符合上述条件的ICMP请求回显报文，每个报文触发一个日志
处理建议	无

6.46 ATK_ICMP_SMURF_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_SMURF_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP请求回显报文，目的IP为：(1)A、B、C类广播地址或者网络地址；D类或者E类地址；(2)入接口IP地址对应的广播地址或者网络地址特征的报文数超过1，聚合后触发日志
处理建议	无

6.47 ATK_ICMP_SOURCEQUENCH

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH: IcmpType(1058)=4; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP源端被关闭的报文数超过1，聚合后触发日志
处理建议	无

6.48 ATK_ICMP_SOURCEQUENCH_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW: IcmpType(1058)=4; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP源端被关闭的报文首包触发日志；日志聚合开关关闭，每个ICMP源端被关闭的报文触发一个日志
处理建议	无

6.49 ATK_ICMP_SOURCEQUENCH_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW_SZ: IcmpType(1058)=4; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP源端被关闭的报文首包触发日志；日志聚合开关关闭，每个ICMP源端被关闭的报文触发一个日志
处理建议	无

6.50 ATK_ICMP_SOURCEQUENCH_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_SOURCEQUENCH_SZ: IcmpType(1058)=4; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP源端被关闭的报文数超过1，聚合后触发日志
处理建议	无

6.51 ATK_ICMP_TIMEEXCEED

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED: IcmpType(1058)=11; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP超时的报文数超过1，聚合后触发日志
处理建议	无

6.52 ATK_ICMP_TIMEEXCEED_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW: IcmpType(1058)=11; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP超时的报文首包触发日志；日志聚合开关关闭，每个ICMP超时的报文触发一个日志
处理建议	无

6.53 ATK_ICMP_TIMEEXCEED_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_RAW_SZ: IcmpType(1058)=11; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP超时的报文首包触发日志；日志聚合开关关闭，每个ICMP超时的报文触发一个日志
处理建议	无

6.54 ATK_ICMP_TIMEEXCEED_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TIMEEXCEED_SZ: IcmpType(1058)=11; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP超时的报文数超过1，聚合后触发日志
处理建议	无

6.55 ATK_ICMP_TRACEROUTE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP类型为11且代码为0的报文数超过1，聚合后触发日志
处理建议	无

6.56 ATK_ICMP_TRACEROUTE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP类型为11且代码为0的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为11且代码为0的报文触发一个日志
处理建议	无

6.57 ATK_ICMP_TRACEROUTE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP类型为11且代码为0的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为11且代码为0的报文触发一个日志
处理建议	无

6.58 ATK_ICMP_TRACEROUTE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMP_TRACEROUTE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP类型为11且代码为0的报文数超过1，聚合后触发日志
处理建议	无

6.59 ATK_ICMP_TSTAMP_REQ

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ: IcmpType(1058)=13; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP时间戳请求的报文数超过1，聚合后触发日志
处理建议	无

6.60 ATK_ICMP_TSTAMP_REQ_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW: IcmpType(1058)=13; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP时间戳请求的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳请求的报文触发一个日志
处理建议	无

6.61 ATK_ICMP_TSTAMP_REQ_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW_SZ: IcmpType(1058)=13; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP时间戳请求的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳请求的报文触发一个日志
处理建议	无

6.62 ATK_ICMP_TSTAMP_REQ_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_REQ_SZ: IcmpType(1058)=13; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP时间戳请求的报文数超过1，聚合后触发日志
处理建议	无

6.63 ATK_ICMP_TSTAMP_RPL

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL: IcmpType(1058)=14; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP时间戳应答的报文数超过1，聚合后触发日志
处理建议	无

6.64 ATK_ICMP_TSTAMP_RPL_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW: IcmpType(1058)=14; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP时间戳应答的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳应答的报文触发一个日志
处理建议	无

6.65 ATK_ICMP_TSTAMP_RPL_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW_SZ: IcmpType(1058)=14; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP时间戳应答的报文首包触发日志；日志聚合开关关闭，每个ICMP时间戳应答的报文触发一个日志
处理建议	无

6.66 ATK_ICMP_TSTAMP_RPL_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TSTAMP_RPL_SZ: IcmpType(1058)=14; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP时间戳应答的报文数超过1，聚合后触发日志
处理建议	无

6.67 ATK_ICMP_TYPE

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE: IcmpType(1058)=38; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP用户自定义类型的报文数超过1，聚合后触发日志
处理建议	无

6.68 ATK_ICMP_TYPE_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_RAW: IcmpType(1058)=38; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMP用户自定义类型的报文触发一个日志
处理建议	无

6.69 ATK_ICMP_TYPE_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_RAW_SZ: IcmpType(1058)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMP用户自定义类型的报文触发一个日志
处理建议	无

6.70 ATK_ICMP_TYPE_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_TYPE_SZ: IcmpType(1058)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP用户自定义类型的报文数超过1，聚合后触发日志
处理建议	无

6.71 ATK_ICMP_UNREACHABLE

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE: IcmpType(1058)=3; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP目的不可达的报文数超过1，聚合后触发日志
处理建议	无

6.72 ATK_ICMP_UNREACHABLE_RAW

日志内容	IcmpType(1058)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW: IcmpType(1058)=3; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMP目的不可达的报文触发一个日志
处理建议	无

6.73 ATK_ICMP_UNREACHABLE_RAW_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_RAW_SZ: IcmpType(1058)=3; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMP目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMP目的不可达的报文触发一个日志
处理建议	无

6.74 ATK_ICMP_UNREACHABLE_SZ

日志内容	IcmpType(1058)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMP类型 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMP_UNREACHABLE_SZ: IcmpType(1058)=3; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011091319; EndTime_c(1012)=20131011091819; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP目的不可达的报文数超过1，聚合后触发日志
处理建议	无

6.75 ATK_ICMPV6_DEST_UNREACH

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH: Icmpv6Type(1059)=133; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6目的不可达的报文数超过1，聚合后触发日志
处理建议	无

6.76 ATK_ICMPV6_DEST_UNREACH_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW: Icmpv6Type(1059)=133; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMPV6目的不可达的报文触发一个日志
处理建议	无

6.77 ATK_ICMPV6_DEST_UNREACH_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW_SZ: Icmpv6Type(1059)=133; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6目的不可达的报文首包触发日志；日志聚合开关关闭，每个ICMPV6目的不可达的报文触发一个日志
处理建议	无

6.78 ATK_ICMPV6_DEST_UNREACH_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_DEST_UNREACH_SZ: Icmpv6Type(1059)=133; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6目的不可达的报文数超过1，聚合后触发日志
处理建议	无

6.79 ATK_ICMPV6_ECHO_REQ

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ: Icmpv6Type(1059)=128; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6请求回显的报文数超过1，聚合后触发日志
处理建议	无

6.80 ATK_ICMPV6_ECHO_REQ_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW: Icmpv6Type(1059)=128; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6请求回显的报文首包触发日志；日志聚合开关关闭，每个ICMPV6请求回显的报文触发一个日志
处理建议	无

6.81 ATK_ICMPV6_ECHO_REQ_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW_SZ: Icmpv6Type(1059)=128; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6请求回显的报文首包触发日志；日志聚合开关关闭，每个ICMPV6请求回显的报文触发一个日志
处理建议	无

6.82 ATK_ICMPV6_ECHO_REQ_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_REQ_SZ: Icmpv6Type(1059)=128; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6请求回显的报文数超过1，聚合后触发日志
处理建议	无

6.83 ATK_ICMPV6_ECHO_RPL

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL: Icmpv6Type(1059)=129; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6回显应答的报文数超过1，聚合后触发日志
处理建议	无

6.84 ATK_ICMPV6_ECHO_RPL_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW: Icmpv6Type(1059)=129; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6回显应答的报文首包触发日志；日志聚合开关关闭，每个ICMPV6回显应答的报文触发一个日志
处理建议	无

6.85 ATK_ICMPV6_ECHO_RPL_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW_SZ: Icmpv6Type(1059)=129; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6回显应答的报文首包触发日志；日志聚合开关关闭，每个ICMPV6回显应答的报文触发一个日志
处理建议	无

6.86 ATK_ICMPV6_ECHO_RPL_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_ECHO_RPL_SZ: Icmpv6Type(1059)=129; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6回显应答的报文数超过1，聚合后触发日志
处理建议	无

6.87 ATK_ICMPV6_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_ICMPV6_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPv6Addr(1007)=2002::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的ICMPV6报文数超过阈值，触发日志
处理建议	无

6.88 ATK_ICMPV6_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_ICMPV6_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1007)=2002::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的ICMPV6报文数超过阈值，触发日志
处理建议	无

6.89 ATK_ICMPV6_GROUPQUERY

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY: Icmpv6Type(1059)=130; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者查询的报文数超过1，聚合后触发日志
处理建议	无

6.90 ATK_ICMPV6_GROUPQUERY_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW: Icmpv6Type(1059)=130; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者查询的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者查询的报文触发一个日志
处理建议	无

6.91 ATK_ICMPV6_GROUPQUERY_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW_SZ: Icmpv6Type(1059)=130; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者查询的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者查询的报文触发一个日志
处理建议	无

6.92 ATK_ICMPV6_GROUPQUERY_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPQUERY_SZ: Icmpv6Type(1059)=130; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者查询的报文数超过1，聚合后触发日志
处理建议	无

6.93 ATK_ICMPV6_GROUPREDUCTION

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION: Icmpv6Type(1059)=132; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者Done的报文数超过1，聚合后触发日志
处理建议	无

6.94 ATK_ICMPV6_GROUPREDUCTION_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW: Icmpv6Type(1059)=132; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者Done的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者Done的报文触发一个日志
处理建议	无

6.95 ATK_ICMPV6_GROUPREDUCTION_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW_SZ: Icmpv6Type(1059)=132; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者Done的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者Done的报文触发一个日志
处理建议	无

6.96 ATK_ICMPV6_GROUPREDUCTION_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREDUCTION_SZ: Icmpv6Type(1059)=132; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者Done的报文数超过1，聚合后触发日志
处理建议	无

6.97 ATK_ICMPV6_GROUPREPORT

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT: Icmpv6Type(1059)=131; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者报告的报文数超过1，聚合后触发日志
处理建议	无

6.98 ATK_ICMPV6_GROUPREPORT_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW: Icmpv6Type(1059)=131; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者报告的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者报告的报文触发一个日志
处理建议	无

6.99 ATK_ICMPV6_GROUPREPORT_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW_SZ: Icmpv6Type(1059)=131; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6组播侦听者报告的报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6组播侦听者报告的报文触发一个日志
处理建议	无

6.100 ATK_ICMPV6_GROUPREPORT_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_GROUPREPORT_SZ: Icmpv6Type(1059)=131; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6组播侦听者报告的报文数超过1，聚合后触发日志
处理建议	无

6.101 ATK_ICMPV6_LARGE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6超长报文数超过1，聚合后触发日志
处理建议	无

6.102 ATK_ICMPV6_LARGE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6超长报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6超长报文触发一个日志
处理建议	无

6.103 ATK_ICMPV6_LARGE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6超长报文首包触发日志；日志聚合开关关闭，每个每个ICMPV6超长报文触发一个日志
处理建议	无

6.104 ATK_ICMPV6_LARGE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_LARGE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6超长报文数超过1，聚合后触发日志
处理建议	无

6.105 ATK_ICMPV6_PACKETTOOBIG

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG: Icmpv6Type(1059)=136; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6数据超长的报文数超过1，聚合后触发日志
处理建议	无

6.106 ATK_ICMPV6_PACKETTOOBIG_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW: Icmpv6Type(1059)=136; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6数据超长的报文首包触发日志；日志聚合开关关闭，每个ICMPV6数据超长的报文触发一个日志
处理建议	无

6.107 ATK_ICMPV6_PACKETTOOBIG_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW_SZ: Icmpv6Type(1059)=136; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6数据超长的报文首包触发日志；日志聚合开关关闭，每个ICMPV6数据超长的报文触发一个日志
处理建议	无

6.108 ATK_ICMPV6_PACKETTOOBIG_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_PACKETTOOBIG_SZ: Icmpv6Type(1059)=136; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6数据超长的报文数超过1，聚合后触发日志
处理建议	无

6.109 ATK_ICMPV6_PARAPROBLEM

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM: Icmpv6Type(1059)=135; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6参数问题的报文数超过1，聚合后触发日志
处理建议	无

6.110 ATK_ICMPV6_PARAPROBLEM_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW: Icmpv6Type(1059)=135; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6参数问题的报文首包触发日志；日志聚合开关关闭，每个ICMPV6参数问题的报文触发一个日志
处理建议	无

6.111 ATK_ICMPV6_PARAPROBLEM_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW_SZ: Icmpv6Type(1059)=135; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6参数问题的报文首包触发日志；日志聚合开关关闭，每个ICMPV6参数问题的报文触发一个日志
处理建议	无

6.112 ATK_ICMPV6_PARAPROBLEM_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_PARAPROBLEM_SZ: Icmpv6Type(1059)=135; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6参数问题的报文数超过1，聚合后触发日志
处理建议	无

6.113 ATK_ICMPV6_TIMEEXCEED

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED: Icmpv6Type(1059)=134; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6超时的报文数超过1，聚合后触发日志
处理建议	无

6.114 ATK_ICMPV6_TIMEEXCEED_RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW: Icmpv6Type(1059)=134; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6超时的报文首包触发日志；日志聚合开关关闭，每个ICMPV6超时的报文触发一个日志
处理建议	无

6.115 ATK_ICMPV6_TIMEEXCEED_RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW_SZ: Icmpv6Type(1059)=134; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6超时的报文首包触发日志；日志聚合开关关闭，每个ICMPV6超时的报文触发一个日志
处理建议	无

6.116 ATK_ICMPV6_TIMEEXCEED_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_TIMEEXCEED_SZ: Icmpv6Type(1059)=134; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6超时的报文数超过1，聚合后触发日志
处理建议	无

6.117 ATK_ICMPV6_TRACEROUTE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP类型为3的报文数超过1，聚合后触发日志
处理建议	无

6.118 ATK_ICMPV6_TRACEROUTE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435.
日志说明	日志聚合开关开启，ICMP类型为3的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为3的报文触发一个日志
处理建议	无

6.119 ATK_ICMPV6_TRACEROUTE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435.
日志说明	日志聚合开关开启，ICMP类型为3的报文首包触发日志；日志聚合开关关闭，每个ICMP类型为3的报文触发一个日志
处理建议	无

6.120 ATK_ICMPV6_TRACEROUTE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_ICMPV6_TRACEROUTE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMP类型为3的报文数超过1，聚合后触发日志
处理建议	无

6.121 ATK_ICMPV6_TYPE

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE: Icmpv6Type(1059)=38; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6用户自定义类型的报文数超过1，聚合后触发日志
处理建议	无

6.122 ATK_ICMPV6_TYPE _RAW

日志内容	Icmpv6Type(1059)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE_RAW: Icmpv6Type(1059)=38; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMPV6用户自定义类型的报文触发一个日志
处理建议	无

6.123 ATK_ICMPV6_TYPE _RAW_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE_RAW_SZ: Icmpv6Type(1059)=38; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，ICMPV6用户自定义类型的报文首包触发日志；日志聚合开关关闭，每个ICMPV6用户自定义类型的报文触发一个日志
处理建议	无

6.124 ATK_ICMPV6_TYPE_SZ

日志内容	Icmpv6Type(1059)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：ICMPv6类型 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_ICMPV6_TYPE_SZ: Icmpv6Type(1059)=38; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=5600::12; DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011100935; EndTime_c(1012)=20131011101435; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，ICMPV6用户自定义类型的报文数超过1，聚合后触发日志
处理建议	无

6.125 ATK_IP_OPTION

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IP_OPTION: IPOptValue(1057)=38; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，用户自定义IP选项的报文数超过1，聚合后触发日志
处理建议	无

6.126 ATK_IP_OPTION_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IP_OPTION_RAW: IPOptValue(1057)=38; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，用户自定义IP选项的报文首包触发日志；日志聚合开关关闭，每个用户自定义IP选项的报文触发一个日志
处理建议	无

6.127 ATK_IP_OPTION_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IP_OPTION_RAW_SZ: IPOptValue(1057)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，用户自定义IP选项的报文首包触发日志；日志聚合开关关闭，每个用户自定义IP选项的报文触发一个日志
处理建议	无

6.128 ATK_IP_OPTION_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IP_OPTION_SZ: IPOptValue(1057)=38; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，用户自定义IP选项的报文数超过1，聚合后触发日志
处理建议	无

6.129 ATK_IP4_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_ACK_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为ACK的IPV4报文数超过阈值，触发日志
处理建议	无

6.130 ATK_IP4_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_ACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为ACK的IPV4报文数超过阈值，触发日志
处理建议	无

6.131 ATK_IP4_DIS_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; TcpFlag(1074)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：TCP类型（仅在TCP报文中显示该字段） $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_DIS_PORTSCAN: RcvIfName(1023)=Ethernet1/2/0/2; Protocol(1001)=TCP; TcpFlag(1074)=[SYN]; DstIPAddr(1007)=6.1.1.5; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足分布式port scan时触发日志
处理建议	无

6.132 ATK_IP4_DIS_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：目的IP地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_DIS_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; DstIPAddr(1007)=6.1.1.5; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足分布式port scan时触发日志
处理建议	无

6.133 ATK_IP4_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_DNS_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送DNS Query的报文数超过阈值，触发日志发送
处理建议	无

6.134 ATK_IP4_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_DNS_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送DNS Query的报文数超过阈值，触发日志发送
处理建议	无

6.135 ATK_IP4_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_FIN_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的报文数超过阈值，触发日志发送
处理建议	无

6.136 ATK_IP4_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_FIN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的报文数超过阈值，触发日志发送
处理建议	无

6.137 ATK_IP4_FRAGMENT

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.138 ATK_IP4_FRAGMENT_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV4报文触发一个日志
处理建议	无

6.139 ATK_IP4_FRAGMENT_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV4报文触发一个日志
处理建议	无

6.140 ATK_IP4_FRAGMENT_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_FRAGMENT_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.141 ATK_IP4_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_HTTP_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送的HTTP的Get报文数超过阈值，触发日志发送
处理建议	无

6.142 ATK_IP4_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_HTTP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内向指定目的IP发送的HTTP的Get报文数超过阈值，触发日志发送
处理建议	无

6.143 ATK_IP4_IMPOSSIBLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.144 ATK_IP4_IMPOSSIBLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	无

6.145 ATK_IP4_IMPOSSIBLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	无

6.146 ATK_IP4_IMPOSSIBLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_IMPOSSIBLE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.147 ATK_IP4_IPSWEEP

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_IPSWEEP: RcvIfName(1023)=Ethernet1/2/0/2; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009060657.
日志说明	报文满足ip sweep时触发日志
处理建议	无

6.148 ATK_IP4_IPSWEEP_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_IPSWEEP_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009060657.
日志说明	报文满足ip sweep时触发日志
处理建议	无

6.149 ATK_IP4_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; DstIPAddr(1007)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：目的IP地址 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_PORTSCAN: RcvIfName(1023)=Ethernet1/2/0/2; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; DstIPAddr(1007)=6.1.1.5; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足port scan时触发日志
处理建议	无

6.150 ATK_IP4_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; DstIPAddr(1007)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：VPN名称 $6：目的IP地址 $7：动作类型 $8：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; DstIPAddr(1007)=6.1.1.5; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009052955.
日志说明	报文满足port scan时触发日志
处理建议	无

6.151 ATK_IP4_RST_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_RST_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV4报文数超过阈值，触发日志
处理建议	无

6.152 ATK_IP4_RST_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_RST_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV4报文数超过阈值，触发日志
处理建议	无

6.153 ATK_IP4_SYN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_SYN_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为SYN的IPV4报文数超过阈值，触发日志
处理建议	无

6.154 ATK_IP4_SYN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：VPN名称 $4：速率上限 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_SYN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为SYN的IPV4报文数超过阈值，触发日志
处理建议	无

6.155 ATK_IP4_SYNACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_SYNACK_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV4报文数超过阈值，触发日志
处理建议	无

6.156 ATK_IP4_SYNACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_SYNACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV4报文数超过阈值，触发日志
处理建议	无

6.157 ATK_IP4_TCP_ALLFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.158 ATK_IP4_TCP_ALLFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV4报文触发一个日志
处理建议	无

6.159 ATK_IP4_TCP_ALLFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV4报文触发一个日志
处理建议	无

6.160 ATK_IP4_TCP_ALLFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_ALLFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.161 ATK_IP4_TCP_FINONLY

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.162 ATK_IP4_TCP_FINONLY_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV4报文触发一个日志
处理建议	无

6.163 ATK_IP4_TCP_FINONLY_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV4报文触发一个日志
处理建议	无

6.164 ATK_IP4_TCP_FINONLY_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_FINONLY_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.165 ATK_IP4_TCP_INVALIDFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.166 ATK_IP4_TCP_INVALIDFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4 TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4 TCP报文触发一个日志
处理建议	无

6.167 ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4 TCP报文触发日志 日志聚合开关关闭，每个TCP标志位无效的IPv4 TCP报文触发一个日志
处理建议	无

6.168 ATK_IP4_TCP_INVALIDFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.169 ATK_IP4_TCP_LAND

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，IPV4源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	无

6.170 ATK_IP4_TCP_LAND_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV4源目的地址相同的TCP报文触发一个日志
处理建议	无

6.171 ATK_IP4_TCP_LAND_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV4源目的地址相同的TCP报文触发一个日志
处理建议	无

6.172 ATK_IP4_TCP_LAND_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_LAND_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，IPV4源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	无

6.173 ATK_IP4_TCP_NULLFLAG

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=4.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.174 ATK_IP4_TCP_NULLFLAG_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV4报文触发一个日志
处理建议	无

6.175 ATK_IP4_TCP_NULLFLAG_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV4报文触发一个日志
处理建议	无

6.176 ATK_IP4_TCP_NULLFLAG_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_NULLFLAG_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=4.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.177 ATK_IP4_TCP_SYNFIN

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.178 ATK_IP4_TCP_SYNFIN_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV4报文触发一个日志
处理建议	无

6.179 ATK_IP4_TCP_SYNFIN_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV4报文触发一个日志
处理建议	无

6.180 ATK_IP4_TCP_SYNFIN_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_SYNFIN_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.181 ATK_IP4_TCP_WINNUKE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=5.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.182 ATK_IP4_TCP_WINNUKE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文触发一个日志
处理建议	无

6.183 ATK_IP4_TCP_WINNUKE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文触发一个日志
处理建议	无

6.184 ATK_IP4_TCP_WINNUKE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TCP_WINNUKE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=5.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV4报文数超过1，聚合后触发日志
处理建议	无

6.185 ATK_IP4_TEARDROP

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，重叠偏移的报文数超过1，聚合后触发日志
处理建议	无

6.186 ATK_IP4_TEARDROP_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，重叠偏移的报文首包触发日志；日志聚合开关关闭，每个重叠偏移的报文触发一个日志
处理建议	无

6.187 ATK_IP4_TEARDROP_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，重叠偏移的报文首包触发日志；日志聚合开关关闭，每个重叠偏移的报文触发一个日志
处理建议	无

6.188 ATK_IP4_TEARDROP_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TEARDROP_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=3.
日志说明	日志聚合开关开启，重叠偏移的报文数超过1，聚合后触发日志
处理建议	无

6.189 ATK_IP4_TINY_FRAGMENT

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=6.
日志说明	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文数超过1，聚合后触发日志
处理建议	无

6.190 ATK_IP4_TINY_FRAGMENT_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文首包触发日志；日志聚合开关关闭，每个分片标志位IP_MF置位且IP数据包的长度小于68的报文触发一个日志
处理建议	无

6.191 ATK_IP4_TINY_FRAGMENT_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging.
日志说明	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文首包触发日志；日志聚合开关关闭，每个分片标志位IP_MF置位且IP数据包的长度小于68的报文触发一个日志
处理建议	无

6.192 ATK_IP4_TINY_FRAGMENT_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_TINY_FRAGMENT_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=TCP; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=6.
日志说明	日志聚合开关开启，分片标志位IP_MF置位且IP数据包的长度小于68的报文数超过1，聚合后触发日志
处理建议	无

6.193 ATK_IP4_UDP_BOMB

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文数超过1，聚合后触发日志
处理建议	无

6.194 ATK_IP4_UDP_BOMB_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文首包触发日志；日志聚合开关关闭，每个满足IP报文长度-IP首部>数据报长度的UDP报文触发一个日志
处理建议	无

6.195 ATK_IP4_UDP_BOMB_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文首包触发日志；日志聚合开关关闭，每个满足IP报文长度-IP首部>数据报长度的UDP报文触发一个日志
处理建议	无

6.196 ATK_IP4_UDP_BOMB_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_BOMB_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，满足IP报文长度-IP首部>数据报长度的UDP报文数超过1，聚合后触发日志
处理建议	无

6.197 ATK_IP4_UDP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定IPV4目的地址的UDP报文数超过阈值，触发日志
处理建议	无

6.198 ATK_IP4_UDP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IP地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPAddr(1007)=6.1.1.5; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009093351.
日志说明	单位时间内指定IPV4目的地址的UDP报文数超过阈值，触发日志
处理建议	无

6.199 ATK_IP4_UDP_FRAGGLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=11.
日志说明	日志聚合开关开启，满足IPV4源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	无

6.200 ATK_IP4_UDP_FRAGGLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	无

6.201 ATK_IP4_UDP_FRAGGLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	无

6.202 ATK_IP4_UDP_FRAGGLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_FRAGGLE_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=11.
日志说明	日志聚合开关开启，满足IPV4源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	无

6.203 ATK_IP4_UDP_SNORK

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	无

6.204 ATK_IP4_UDP_SNORK_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	无

6.205 ATK_IP4_UDP_SNORK_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV4源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	无

6.206 ATK_IP4_UDP_SNORK_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP4_UDP_SNORK_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131011074913; EndTime_c(1012)=20131011075413; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV4源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	无

6.207 ATK_IP6_ACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_ACK_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为ACK的IPV6报文数超过阈值，触发日志
处理建议	无

6.208 ATK_IP6_ACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_ACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为ACK的IPV6报文数超过阈值，触发日志
处理建议	无

6.209 ATK_IP6_DIS_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DIS_PORTSCAN: RcvIfName(1023)=Ethernet1/2/0/2; Protocol(1001)=UDP; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009100928.
日志说明	IPV6报文满足分布式port scan时触发日志
处理建议	无

6.210 ATK_IP6_DIS_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：目的IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DIS_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009100928.
日志说明	IPV6报文满足分布式port scan时触发日志
处理建议	无

6.211 ATK_IP6_DNS_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DNS_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送DNS Query的IPV6报文数超过阈值，触发日志发送
处理建议	无

6.212 ATK_IP6_DNS_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_DNS_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送DNS Query的IPV6报文数超过阈值，触发日志发送
处理建议	无

6.213 ATK_IP6_FIN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_FIN_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志发送
处理建议	无

6.214 ATK_IP6_FIN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_FIN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志发送
处理建议	无

6.215 ATK_IP6_FRAGMENT

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.216 ATK_IP6_FRAGMENT_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV6报文触发一个日志
处理建议	无

6.217 ATK_IP6_FRAGMENT_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文首包触发日志；日志聚合开关关闭，每个偏移量OffSet值在(0,5)之间的IPV6报文触发一个日志
处理建议	无

6.218 ATK_IP6_FRAGMENT_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_FRAGMENT_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，偏移量OffSet值在(0,5)之间的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.219 ATK_IP6_HTTP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_HTTP_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的HTTP的IPV6 Get报文数超过阈值，触发日志发送
处理建议	无

6.220 ATK_IP6_HTTP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_HTTP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内向指定目的IP发送的HTTP的IPV6 Get报文数超过阈值，触发日志发送
处理建议	无

6.221 ATK_IP6_IMPOSSIBLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，源目的地址相同的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.222 ATK_IP6_IMPOSSIBLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	无

6.223 ATK_IP6_IMPOSSIBLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议名称 $6：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging.
日志说明	日志聚合开关开启，源目的地址相同的IPV4报文首包触发日志；日志聚合开关关闭，每个源目的地址相同的IPV4报文触发一个日志
处理建议	无

6.224 ATK_IP6_IMPOSSIBLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：协议类型 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_IMPOSSIBLE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=1::1; RcvVPNInstance(1041)=--; Protocol(1001)=IPv6-ICMP; Action(1049)=logging; BeginTime_c(1011)=20131011103335; EndTime_c(1012)=20131011103835; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，源目的地址相同的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.225 ATK_IP6_IPSWEEP

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_IPSWEEP: RcvIfName(1023)=Ethernet1/2/0/2; Protocol(1001)=UDP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100639.
日志说明	IPV6报文满足ip sweep时触发日志
处理建议	无

6.226 ATK_IP6_IPSWEEP_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：动作类型 $6：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_IPSWEEP_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100639.
日志说明	IPV6报文满足ip sweep时触发日志
处理建议	无

6.227 ATK_IP6_PORTSCAN

日志内容	RcvIfName(1023)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：目的IPv6地址 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_PORTSCAN: RcvIfName(1023)=Ethernet1/2/0/2; Protocol(1001)=UDP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; DstIPv6Addr(1037)=2::2; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100455.
日志说明	IPV6报文满足port scan时触发日志
处理建议	无

6.228 ATK_IP6_PORTSCAN_SZ

日志内容	SrcZoneName(1025)=[STRING]; Protocol(1001)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：协议名称 $3：源IPv6地址 $4：VPN名称 $5：目的IPv6地址 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_PORTSCAN_SZ: SrcZoneName(1025)=Trust; Protocol(1001)=TCP; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; DstIPv6Addr(1037)=2::2; Action(1049)=logging,block-source; BeginTime_c(1011)=20131009100455.
日志说明	IPV6报文满足port scan时触发日志
处理建议	无

6.229 ATK_IP6_RST_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_RST_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV6报文数超过阈值，触发日志
处理建议	无

6.230 ATK_IP6_RST_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_RST_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为RST的IPV6报文数超过阈值，触发日志
处理建议	无

6.231 ATK_IP6_SYN_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_SYN_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	满足周期内指定目的地址的TCP标志位为SYN的IPV6报文数超过阈值，触发日志
处理建议	无

6.232 ATK_IP6_SYN_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_SYN_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	满足周期内指定目的地址的TCP标志位为SYN的IPV6报文数超过阈值，触发日志
处理建议	无

6.233 ATK_IP6_SYNACK_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_SYNACK_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志
处理建议	无

6.234 ATK_IP6_SYNACK_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_SYNACK_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定目的地址的TCP标志位为SYN+ACK的IPV6报文数超过阈值，触发日志
处理建议	无

6.235 ATK_IP6_TCP_ALLFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.236 ATK_IP6_TCP_ALLFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV6报文触发一个日志
处理建议	无

6.237 ATK_IP6_TCP_ALLFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位全置位的IPV6报文触发一个日志
处理建议	无

6.238 ATK_IP6_TCP_ALLFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_ALLFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位全置位的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.239 ATK_IP6_TCP_FINONLY

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.240 ATK_IP6_TCP_FINONLY_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV6报文触发一个日志
处理建议	无

6.241 ATK_IP6_TCP_FINONLY_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为FIN的IPV6报文触发一个日志
处理建议	无

6.242 ATK_IP6_TCP_FINONLY_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_FINONLY_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为FIN的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.243 ATK_IP6_TCP_INVALIDFLAGS

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.244 ATK_IP6_TCP_INVALIDFLAGS_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6 TCP报文首包触发日志 日志聚合开关关闭，每个TCP标志位为无效时的IPV6 TCP报文触发一个日志
处理建议	无

6.245 ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6 TCP报文首包触发日志 日志聚合开关关闭，每个TCP标志位为无效时的IPV6 TCP报文触发一个日志
处理建议	无

6.246 ATK_IP6_TCP_INVALIDFLAGS_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为无效（RST+FIN、RST+SYN、RST+FIN+SYN、PSH+RST+FIN、PSH+RST+SYN、PSH+RST+SYN+FIN、ACK+RST+FIN、ACK+RST+SYN、ACK+RST+SYN+FIN、ACK+PSH+SYN+FIN、ACK+PSH+RST+FIN、ACK+PSH+RST+SYN）时的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.247 ATK_IP6_TCP_LAND

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	无

6.248 ATK_IP6_TCP_LAND_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV6源目的地址相同的TCP报文触发一个日志
处理建议	无

6.249 ATK_IP6_TCP_LAND_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源目的地址相同的TCP报文首包触发日志；日志聚合开关关闭，每个IPV6源目的地址相同的TCP报文触发一个日志
处理建议	无

6.250 ATK_IP6_TCP_LAND_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_LAND_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源目的地址相同的TCP报文数超过1，聚合后触发日志
处理建议	无

6.251 ATK_IP6_TCP_NULLFLAG

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.252 ATK_IP6_TCP_NULLFLAG_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV6报文触发一个日志
处理建议	无

6.253 ATK_IP6_TCP_NULLFLAG_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位未置位的IPV6报文触发一个日志
处理建议	无

6.254 ATK_IP6_TCP_NULLFLAG_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_NULLFLAG_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位未置位的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.255 ATK_IP6_TCP_SYNFIN

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.256 ATK_IP6_TCP_SYNFIN_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV6报文触发一个日志
处理建议	无

6.257 ATK_IP6_TCP_SYNFIN_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=2000::1; DstIPv6Addr(1037)=2003::200; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP标志位为SYN+FIN的IPV6报文触发一个日志
处理建议	无

6.258 ATK_IP6_TCP_SYNFIN_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_SYNFIN_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP标志位为SYN+FIN的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.259 ATK_IP6_TCP_WINNUKE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.260 ATK_IP6_TCP_WINNUKE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文触发一个日志
处理建议	无

6.261 ATK_IP6_TCP_WINNUKE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文首包触发日志；日志聚合开关关闭，每个TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文触发一个日志
处理建议	无

6.262 ATK_IP6_TCP_WINNUKE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_TCP_WINNUKE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，TCP目的端口为139，标志位为URG且紧急指针非零的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.263 ATK_IP6_UDP_FLOOD

日志内容	RcvIfName(1023)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入接口名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FLOOD: RcvIfName(1023)=Ethernet1/2/0/2; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定IPV6目的地址的UDP报文数超过阈值，触发日志
处理建议	无

6.264 ATK_IP6_UDP_FLOOD_SZ

日志内容	SrcZoneName(1025)=[STRING]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1041)=[STRING]; UpperLimit(1048)=[UINT32]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING].
参数解释	$1：入域名称 $2：目的IPv6地址 $3：目的端口 $4：VPN名称 $5：速率上限 $6：动作类型 $7：攻击开始时间
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FLOOD_SZ: SrcZoneName(1025)=Trust; DstIPv6Addr(1037)=2::2; DstPort(1008)=22; RcvVPNInstance(1041)=--; UpperLimit(1048)=10; Action(1049)=logging; BeginTime_c(1011)=20131009100434.
日志说明	单位时间内指定IPV6目的地址的UDP报文数超过阈值，触发日志
处理建议	无

6.265 ATK_IP6_UDP_FRAGGLE

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	无

6.266 ATK_IP6_UDP_FRAGGLE_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	无

6.267 ATK_IP6_UDP_FRAGGLE_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7，目的端口为19的UDP报文触发一个日志
处理建议	无

6.268 ATK_IP6_UDP_FRAGGLE_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_FRAGGLE_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源端口为7，目的端口为19的UDP报文数超过1，聚合后触发日志
处理建议	无

6.269 ATK_IP6_UDP_SNORK

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	无

6.270 ATK_IP6_UDP_SNORK_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	无

6.271 ATK_IP6_UDP_SNORK_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文首包触发日志；日志聚合开关关闭，每个IPV6源端口为7、19或135，目的端口为135的UDP报文触发一个日志
处理建议	无

6.272 ATK_IP6_UDP_SNORK_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IP6_UDP_SNORK_SZ: SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关开启，IPV6源端口为7、19或135，目的端口为135的UDP报文数超过1，聚合后触发日志
处理建议	无

6.273 ATK_IPOPT_ABNORMAL

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011072002; EndTime_c(1012)=20131011072502; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，两个以上IP选项置位的报文数超过1，聚合后触发日志
处理建议	无

6.274 ATK_IPOPT_ABNORMAL_RAW

日志内容	RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入接口名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW: RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，两个以上IP选项置位的报文首包触发日志；日志聚合开关关闭，每个两个以上IP选项置位的报文触发一个日志
处理建议	无

6.275 ATK_IPOPT_ABNORMAL_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_RAW_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，两个以上IP选项置位的报文首包触发日志；日志聚合开关关闭，每个两个以上IP选项置位的报文触发一个日志
处理建议	无

6.276 ATK_IPOPT_ABNORMAL_SZ

日志内容	SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：入域名称 $2：源IP地址 $3：DS-Lite Tunnel对端地址 $4：目的IP地址 $5：VPN名称 $6：协议类型 $7：动作类型 $8：攻击开始时间 $9：攻击结束时间 $10：攻击次数
日志等级	3
举例	ATK/3/ATK_IPOPT_ABNORMAL_SZ: SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011072002; EndTime_c(1012)=20131011072502; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，两个以上IP选项置位的报文数超过1，聚合后触发日志
处理建议	无

6.277 ATK_IPOPT_LOOSESRCROUTE

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE: IPOptValue(1057)=131; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为131的报文数超过1，聚合后触发日志
处理建议	无

6.278 ATK_IPOPT_LOOSESRCROUTE_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW: IPOptValue(1057)=131; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为131的报文首包触发日志；日志聚合开关关闭，每个IP选项为131的报文触发一个日志
处理建议	无

6.279 ATK_IPOPT_LOOSESRCROUTE_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW_SZ: IPOptValue(1057)=131; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为131的报文首包触发日志；日志聚合开关关闭，每个IP选项为131的报文触发一个日志
处理建议	无

6.280 ATK_IPOPT_LOOSESRCROUTE_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)= [UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_LOOSESRCROUTE_SZ: IPOptValue(1057)=131; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为131的报文数超过1，聚合后触发日志
处理建议	无

6.281 ATK_IPOPT_RECORDROUTE

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE: IPOptValue(1057)=7; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为7的报文数超过1，聚合后触发日志
处理建议	无

6.282 ATK_IPOPT_RECORDROUTE_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW: IPOptValue(1057)=7; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为7的报文首包触发日志；日志聚合开关关闭，每个IP选项为7的报文触发一个日志
处理建议	无

6.283 ATK_IPOPT_RECORDROUTE_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_RAW_SZ: IPOptValue(1057)=7; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为7的报文首包触发日志；日志聚合开关关闭，每个IP选项为7的报文触发一个日志
处理建议	无

6.284 ATK_IPOPT_RECORDROUTE_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_RECORDROUTE_SZ: IPOptValue(1057)=7; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为7的报文数超过1，聚合后触发日志
处理建议	无

6.285 ATK_IPOPT_ROUTEALERT

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT: IPOptValue(1057)=148; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为148的报文数超过1，聚合后触发日志
处理建议	无

6.286 ATK_IPOPT_ROUTEALERT_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW: IPOptValue(1057)=148; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为148的报文首包触发日志；日志聚合开关关闭，每个IP选项为148的报文触发一个日志
处理建议	无

6.287 ATK_IPOPT_ROUTEALERT_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_RAW_SZ: IPOptValue(1057)=148; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为148的报文首包触发日志；日志聚合开关关闭，每个IP选项为148的报文触发一个日志
处理建议	无

6.288 ATK_IPOPT_ROUTEALERT_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_ROUTEALERT_SZ: IPOptValue(1057)=148; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为148的报文数超过1，聚合后触发日志
处理建议	无

6.289 ATK_IPOPT_SECURITY

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY: IPOptValue(1057)=130; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131009091022; EndTime_c(1012)=20131009091522; AtkTimes(1050)=2.
日志说明	日志聚合开关打开，IP选项为130的报文数超过1，聚合后触发日志
处理建议	无

6.290 ATK_IPOPT_SECURITY_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY_RAW: IPOptValue(1057)=130; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为130的报文首包触发日志；日志聚合开关关闭，每个IP选项为130的报文触发一个日志
处理建议	无

6.291 ATK_IPOPT_SECURITY_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY_RAW_SZ: IPOptValue(1057)=130; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为130的报文首包触发日志；日志聚合开关关闭，每个IP选项为130的报文触发一个日志
处理建议	无

6.292 ATK_IPOPT_SECURITY_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_SECURITY_SZ: IPOptValue(1057)=130; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131009091022; EndTime_c(1012)=20131009091522; AtkTimes(1050)=2.
日志说明	日志聚合开关打开，IP选项为130的报文数超过1，聚合后触发日志
处理建议	无

6.293 ATK_IPOPT_STREAMID

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID: IPOptValue(1057)=136; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为136的报文数超过1，聚合后触发日志
处理建议	无

6.294 ATK_IPOPT_STREAMID_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID_RAW: IPOptValue(1057)=136; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为136的报文首包触发日志；日志聚合开关关闭，每个IP选项为136的报文触发一个日志
处理建议	无

6.295 ATK_IPOPT_STREAMID_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID_RAW_SZ: IPOptValue(1057)=136; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为136的报文首包触发日志；日志聚合开关关闭，每个IP选项为136的报文触发一个日志
处理建议	无

6.296 ATK_IPOPT_STREAMID_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STREAMID_SZ: IPOptValue(1057)=136; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为136的报文数超过1，聚合后触发日志
处理建议	无

6.297 ATK_IPOPT_STRICTSRCROUTE

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE: IPOptValue(1057)=137; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为137的报文数超过1，聚合后触发日志
处理建议	无

6.298 ATK_IPOPT_STRICTSRCROUTE_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW: IPOptValue(1057)=137; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为137的报文首包触发日志；日志聚合开关关闭，每个IP选项为137的报文触发一个日志
处理建议	无

6.299 ATK_IPOPT_STRICTSRCROUTE_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW_SZ: IPOptValue(1057)=137; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为137的报文首包触发日志；日志聚合开关关闭，每个IP选项为137的报文触发一个日志
处理建议	无

6.300 ATK_IPOPT_STRICTSRCROUTE_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_STRICTSRCROUTE_SZ: IPOptValue(1057)=137; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为137的报文数超过1，聚合后触发日志
处理建议	无

6.301 ATK_IPOPT_TIMESTAMP

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP: IPOptValue(1057)=68; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为68的报文数超过1，聚合后触发日志
处理建议	无

6.302 ATK_IPOPT_TIMESTAMP_RAW

日志内容	IPOptValue(1057)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入接口名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW: IPOptValue(1057)=68; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为68的报文首包触发日志；日志聚合开关关闭，每个IP选项为68的报文触发一个日志
处理建议	无

6.303 ATK_IPOPT_TIMESTAMP_RAW_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_RAW_SZ: IPOptValue(1057)=68; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging.
日志说明	日志聚合开关开启，IP选项为68的报文首包触发日志；日志聚合开关关闭，每个IP选项为68的报文触发一个日志
处理建议	无

6.304 ATK_IPOPT_TIMESTAMP_SZ

日志内容	IPOptValue(1057)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; DstIPAddr(1007)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Protocol(1001)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IP选项值 $2：入域名称 $3：源IP地址 $4：DS-Lite Tunnel对端地址 $5：目的IP地址 $6：VPN名称 $7：协议类型 $8：动作类型 $9：攻击开始时间 $10：攻击结束时间 $11：攻击次数
日志等级	5
举例	ATK/5/ATK_IPOPT_TIMESTAMP_SZ: IPOptValue(1057)=68; SrcZoneName(1025)=Trust; SrcIPAddr(1003)=9.1.1.1; DSLiteTunnelPeer(1040)=--; DstIPAddr(1007)=6.1.1.1; RcvVPNInstance(1041)=--; Protocol(1001)=RAWIP; Action(1049)=logging; BeginTime_c(1011)=20131011063123; EndTime_c(1012)=20131011063623; AtkTimes(1050)=3.
日志说明	日志聚合开关打开，IP选项为68的报文数超过1，聚合后触发日志
处理建议	无

6.305 ATK_IPV6_EXT_HEADER

日志内容	IPv6ExtHeader(1060)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IPv6 扩展头 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER: IPv6ExtHeader(1060)=43; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关打开，自定义扩展头的IPV6报文数超过1，聚合后触发日志
处理建议	无

6.306 ATK_IPV6_EXT_HEADER_ABNORMAL

日志内容	RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IPV6_EXT_HEADER_ABNORMAL: RcvIfName(1023)=Ethernet1/2/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
日志说明	日志聚合开关开启，扩展头个数超过配置的最大数目或者出现不允许重复扩展头的IPv6报文数超过1，触发一个日志
处理建议	无

6.307 ATK_IPV6_EXT_HEADER_ABNORMAL_RAW

日志内容	RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：入接口名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IPV6_EXT_HEADER_RAW: IPv6ExtHeader(1066)=43;RcvIfName(1023)=Ethernet1/2/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
日志说明	日志聚合开关关闭，扩展头个数超过配置的最大数目的每个IPv6报文触发一个日志
处理建议	无

6.308 ATK_IPV6_EXT_HEADER_ABNORMAL_RAW_SZ

日志内容	SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型
日志等级	3
举例	ATK/3/ATK_IPV6_EXT_HEADER_ABNORMAL_RAW_SZ: SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
日志说明	日志聚合开关关闭，扩展头个数超过配置的最大数目的每个IPv6报文触发一个日志
处理建议	无

6.309 ATK_IPV6_EXT_HEADER_ABNORMAL_SZ

日志内容	SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
参数解释	$1：入域名称 $2：源IPv6地址 $3：目的IPv6地址 $4：入接口VPN名称 $5：动作类型 $6：攻击开始时间 $7：攻击结束时间 $8：攻击次数
日志等级	3
举例	ATK/3/ATK_IPV6_EXT_HEADER_ABNORMAL_SZ: SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
日志说明	日志聚合开关开启，扩展头个数超过配置的最大数目或者出现不允许重复扩展头的IPv6报文数超过1，触发一个日志
处理建议	无

6.310 ATK_IPV6_EXT_HEADER_RAW

日志内容	IPv6ExtHeader(1060)=[UINT32]; RcvIfName(1023)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IPv6 扩展头 $2：入接口名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW: IPv6ExtHeader(1060)=43; RcvIfName(1023)=Ethernet1/2/0/2; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，自定义扩展头的IPV6报文首包触发日志；日志聚合开关关闭，每个自定义扩展头的IPV6报文触发一个日志
处理建议	无

6.311 ATK_IPV6_EXT_HEADER_RAW_SZ

日志内容	IPv6ExtHeader(1060)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING].
参数解释	$1：IPv6 扩展头 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：VPN名称 $6：动作类型
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER_RAW_SZ: IPv6ExtHeader(1060)=43; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging.
日志说明	日志聚合开关开启，自定义扩展头的IPV6报文首包触发日志；日志聚合开关关闭，每个自定义扩展头的IPV6报文触发一个日志
处理建议	无

6.312 ATK_IPV6_EXT_HEADER_SZ

日志内容	IPv6ExtHeader(1060)=[UINT32]; SrcZoneName(1025)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; DstIPv6Addr(1037)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Action(1049)=[STRING]; BeginTime_c(1011)=[STRING]; EndTime_c(1012)=[STRING]; AtkTimes(1050)=[UINT32].
参数解释	$1：IPv6 扩展头 $2：入域名称 $3：源IPv6地址 $4：目的IPv6地址 $5：入接口VPN名称 $6：动作类型 $7：攻击开始时间 $8：攻击结束时间 $9：攻击次数
日志等级	5
举例	ATK/5/ATK_IPV6_EXT_HEADER_SZ: IPv6ExtHeader(1060)=43; SrcZoneName(1025)=Trust; SrcIPv6Addr(1036)=1::1; DstIPv6Addr(1037)=2::11; RcvVPNInstance(1041)=--; Action(1049)=logging; BeginTime_c(1011)=20131009103631; EndTime_c(1012)=20131009104131; AtkTimes(1050)=2.
日志说明	日志聚合开关打开，自定义扩展头的IPV6报文数超过1，聚合后触发日志
处理建议	无

7 BFD

本节介绍 BFD 模块输出的日志信息。

7.1 BFD_CHANGE_FSM

日志内容	Sess[STRING], Ver, Sta: [STRING]->[STRING], Diag: [UINT32]
参数解释	$1：BFD会话的源地址、目的地址、接口、消息类型和MPLS FEC信息。LSP会话中包含LSP目的IP、掩码及下一跳IP；PW会话中包含Peer IP和PW ID；TE Tunnel会话中包含源IP、目的IP、Tunnel ID及LSP ID $2：变化前状态机的名称 $3：变化后状态机的名称 $4：诊断信息，包括 • 0 (No Diagnostic)：表示无诊断信息 • 1 (Control Detection Time Expired)：表示 Ctrl 会话本端检测时间超时，会话 down • 2 (Echo Function Failed)：表示 Echo 会话本端检测时间超时或 echo 报文的源 IP 地址被删除，会话 down • 3 (Neighbor Signaled Session Down)：表示对端通知本端 BFD 会话 down • 7 (Administratively Down)：表示本端系统阻止 BFD 会话的建立
日志等级	5
举例	BFD/5/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface:Vlan204, SessType:Ctrl, LinkType:INET], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic). BFD/5/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface: Vlan204, SessType: Ctrl, LinkType: LSP, FEC: LSP, 20.0.4.0/24/10.1.1.1], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic). BFD/5/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface: Vlan204, SessType: Ctrl, LinkType: LSP, FEC: PW FEC-128, 20.0.4.2/1], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic). BFD/5/BFD_CHANGE_FSM: Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface: Vlan204, SessType: Ctrl, LinkType: LSP, FEC: TE Tunnel, 20.0.4.2/20.0.4.1/100/100], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic).
日志说明	BFD会话的状态机发生变化。当BFD会话up或down时出现此信息。如果出现会话异常丢失的情况，可能由高错误率或高丢包率导致
处理建议	需要检查是否BFD配置的问题或网络出现拥塞

7.2 BFD_CHANGE_SESS

日志内容	Sess[STRING], Ver, Sta: [STRING], Diag: [UINT32]
参数解释	$1：BFD会话的源地址、目的地址、接口、消息类型和MPLS FEC信息。LSP会话中包含LSP目的IP、掩码及下一跳IP；PW会话中包含Peer IP和PW ID；TE Tunnel会话中包含源IP、目的IP、Tunnel ID及LSP ID $2：会话状态 $3：诊断码
日志等级	5
举例	BFD/5/BFD_CHANGE_SESS: Sess[17.1.1.2/17.1.1.1, LD/RD:1537/1537, Interface:GE1/2/0/1, SessType:Ctrl, LinkType:INET], Ver:1, Sta: Deleted, Diag: 7 (Administratively Down)
日志说明	当BFD会话删除时出现此信息
处理建议	请检查BFD会话配置

7.3 BFD_REACHED_UPPER_LIMIT

日志内容	The total number of BFD sessions [ULONG] reached the upper limit. Can’t create a new session.
参数解释	$1：BFD会话总数
日志等级	5
举例	BFD/5/BFD_REACHED_UPPER_LIMIT: The total number of BFD session 100 reached upper limit.
日志说明	BFD会话总数达到上限
处理建议	请检查BFD会话配置

8 BGP

本节介绍 BGP 模块输出的日志信息。

8.1 BGP_EXCEED_ROUTE_LIMIT

日志内容	BGP [STRING].[STRING]: The number of routes ([UINT32]) from peer [STRING] ([STRING]) exceeds the limit [UINT32].
参数解释	$1：BGP实例名称。 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：从对等体已接收到的路由前缀数量 $4：BGP对等体的IP地址 $5：BGP对等体的地址族 $6：允许从对等体接收的最大路由前缀数量
日志等级	4
举例	BGP/4/BGP_EXCEED_ROUTE_LIMIT: BGP default.vpn1: The number of routes (101) from peer 1.1.1.1 (IPv4-UNC) exceeds the limit 100.
日志说明	从对等体学到的路由数量超过了允许的最大路由数量
处理建议	检查是否是攻击导致，如果是，需要管理员找到问题原因，对攻击进行防御 否则，查看是否需要增大允许的最大路由数量

8.2 BGP_REACHED_THRESHOLD

日志内容	BGP [STRING].[STRING]: The ratio of the number of routes ([UINT32]) received from peer [STRING] ([STRING]) to the number of allowed routes ([UINT32]) has reached the threshold ([UINT32]%).
参数解释	$1：BGP实例名称。 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：从对等体已接收到的路由数量 $4：BGP对等体的IP地址 $5：BGP对等体的地址族 $6：允许从对等体接收的最大路由数量 $7：接收的路由数量占允许的最大路由数量百分比的阈值
日志等级	5
举例	BGP/5/BGP_REACHED_THRESHOLD: BGP default.vpn1: The ratio of the number of routes (3) received from peer 1.1.1.1 (IPv4-UNC) to the number of allowed routes (2) has reached the threshold (75%).
日志说明	接收的路由数量占允许的最大路由数量的百分比达到了阈值
处理建议	检查是否是攻击导致，如果是，需要管理员找到问题原因，对攻击进行防御 否则，查看是否需要增大以下数值： • 允许的最大路由数量 • 接收的路由数量占允许的最大路由数量百分比的阈值

8.3 BGP_LOG_ROUTE_FLAP

日志内容	BGP [STRING].[STRING]: The route [STRING] [STRING]/[UINT32] learned from peer [STRING] ([STRING]) flapped.
参数解释	$1：BGP实例名称。 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：BGP路由的RD值。不带RD的路由则显示为空 $4：BGP路由的前缀地址 $5：BGP路由的前缀掩码 $6：BGP对等体的IP地址 $7：BGP对等体的地址族
日志等级	4
举例	BGP/4/BGP_LOG_ROUTE_FLAP: BGP default.vpn1: The route 15.1.1.1/24 learned from peer 1.1.1.1 (IPv4-UNC) flapped.
日志说明	从对等体学到的路由发生抖动
处理建议	检查路由抖动是否不正常，如果是，需要管理员找到路由抖动的源头，并制定解决方案

8.4 BGP_LABEL_CONFLICT

日志内容	BGP egress-engineering incoming label [STRING] conflicts with current configuration.
参数解释	$1：标签值
日志等级	5
举例	BGP/5/BGP_LABEL_CONFLICT: BGP egress-engineering incoming label 3000 conflicts with current configuration.
日志说明	通过BGP-EPE功能为对等体分配的标签值已被占用
处理建议	检查配置BGP-EPE功能时指定的路由策略中应用的标签值是否与其他功能中使用的标签值相同

8.5 BGP_LABEL_OUTOFRANGE

日志内容	BGP egress-engineering incoming label [STRING] is out of range.
参数解释	$1：标签值
日志等级	5
举例	BGP/5/BGP_LABEL_OUTOFRANGE: BGP egress-engineering incoming label 1024 is out of range.
日志说明	通过BGP-EPE功能为对等体分配的标签值超出正常范围
处理建议	检查配置BGP-EPE功能时指定的路由策略中应用的标签取值是否合法

8.6 BGP_MEM_ALERT

日志内容	BGP [STRING] instance received system memory alert [STRING] event.
参数解释	$1：BGP实例名称。 $2：内存告警的类型，包括stop、start
日志等级	5
举例	BGP/5/BGP_MEM_ALERT: BGP default instance received system memory alert start event.
日志说明	BGP模块收到内存告警信息
处理建议	如果内存告警类型为start，请检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

8.7 BGP_PEER_LICENSE_REACHED

日志内容	BGP [STRING]: Number of peers in Established state reached the license limit.
参数解释	$1：BGP实例名称。
日志等级	5
举例	BGP/5/BGP_PEER_LICENSE_REACHED: BGP default: Number of peers in Established state reached the license limit.
日志说明	处于established状态的邻居数量已达到license规格限制
处理建议	检查license安装情况，判断是否需要安装新的license

8.8 BGP_ROUTE_LICENSE_REACHED

日志内容	BGP [STRING]: Number of [STRING] routes reached the license limit.
参数解释	$1：BGP实例名称。 $2：BGP地址族，取值包括： • IPv4-UNC public：表示公网 IPv4 单播路由 • IPv6-UNC public：表示公网 IPv6 单播路由 • IPv4 private：表示私网 IPv4 单播路由，VPNv4 路由和嵌套 VPN 路由 • IPv6 private：表示私网 IPv6 单播路由，VPNv6 路由
日志等级	5
举例	BGP/5/BGP_ROUTE_LICENSE_REACHED: BGP default: Number of IPv4-UNC public routes reached the license limit.
日志说明	指定类型的路由数量已达到license规格限制
处理建议	检查license安装情况，判断是否需要安装新的license 当指定类型的路由数量降低到License的规格限制以下或者License规格限制扩大时，之前被丢弃的路由不能自动恢复，需要用户手工配置，以便重新学习路由

8.9 BGP_STATE_CHANGED

日志内容	BGP [STRING].[STRING]: [STRING] state has changed from [STRING] to [STRING].
参数解释	$1：BGP实例名称。 $2：VPN实例名称。如果是公网内的日志信息，则显示为空 $3：BGP对等体的IP地址 $4：变化前的状态名称 $5：变化后的状态名称
日志等级	5
举例	BGP/5/BGP_STATE_CHANGED: BGP default.vpn1: 192.99.0.2 state has changed from ESTABLISHED to IDLE.
日志说明	BGP对等体的状态发生变化 此日志信息当BGP对等体从其他状态进入Established状态或者从Established状态进入其他状态时产生
处理建议	如果BGP对等体意外Down，请检查网络是否发生故障或丢包

9 BLS

本节介绍 BLS 模块输出的日志信息。

9.1 BLS_ENTRY_ADD

日志内容	SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; TTL(1051)=[STRING]; Reason(1052)=[STRING].
参数解释	$1：黑名单IP地址 $2：DS-Lite Tunnel 对端地址 $3：VPN名称 $4：老化时间 $5：添加原因
日志等级	5
举例	BLS/5/BLS_ENTRY_ADD: SrcIPAddr(1003)=1.1.1.6; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=; TTL(1051)=; Reason(1052)=Configuration. BLS/5/BLS_ENTRY_ADD: SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; TTL(1051)=10; Reason(1052)=Scan behavior detected.
日志说明	日志开关打开；手动配置一个黑名单；scan检测添加一个黑名单；触发日志发送
处理建议	无

9.2 BLS_ENTRY_DEL

日志内容	SrcIPAddr(1003)=[IPADDR]; DSLiteTunnelPeer(1040)=[STRING]; RcvVPNInstance(1041)=[STRING]; Reason(1052)=[STRING].
参数解释	$1：黑名单IP地址 $2：DS-Lite Tunnel对端地址 $3：VPN名称 $4：删除原因
日志等级	5
举例	BLS/5/BLS_ENTRY_DEL: SrcIPAddr(1003)=1.1.1.3; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=; Reason(1052)=Configuration. BLS/5/BLS_ENTRY_DEL: SrcIPAddr(1003)=9.1.1.5; DSLiteTunnelPeer(1040)=--; RcvVPNInstance(1041)=vpn1; Reason(1052)=Aging.
日志说明	日志开关打开；手动删除一个黑名单；老化删除一个黑名单；触发日志发送
处理建议	无

9.3 BLS_IPV6_ENTRY_ADD

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; TTL(1051)=[STRING]; Reason(1052)=[STRING].
参数解释	$1：黑名单IPv6地址 $2：VPN名称 $3：老化时间 $4：添加原因
日志等级	5
举例	BLS/5/BLS_IPV6_ENTRY_ADD: SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1041)=; TTL(1051)=; Reason(1052)=Configuration. BLS/5/BLS_IPV6_ENTRY_ADD: SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1041)=--; TTL(1051)=10; Reason(1052)=Scan behavior detected.
日志说明	日志开关打开；手动配置一个黑名单；scan检测添加一个黑名单；触发日志发送
处理建议	无

9.4 BLS_IPV6_ENTRY_DEL

日志内容	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1041)=[STRING]; Reason(1052)=[STRING].
参数解释	$1：黑名单IPv6地址 $2：VPN名称 $3：删除原因
日志等级	5
举例	BLS/5/BLS_IPV6_ENTRY_DEL: SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1041)=; Reason(1052)=Configuration.
日志说明	日志开关打开；手动删除一个黑名单；老化删除一个黑名单；触发日志发送
处理建议	无

10 CFD

本节介绍 CFD 模块输出的日志信息。

10.1 CFD_CROSS_CCM

日志内容	MEP [UINT16] in SI [INT32] received a cross-connect CCM. It's SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
参数解释	$1：服务实例的ID $2：本地MEP的ID $3：源MAC地址 $4：序列号 $5：远端MEP的ID $6：MD的ID。如果不存在，会显示“without ID” $7：MA的ID
日志等级	6
举例	CFD/6/CFD_CROSS_CCM: MEP 13 in SI 10 received a cross-connect CCM. Its SrcMAC is 0011-2233-4401, SeqNum is 78, RMEP is 12, MD ID is without ID, MA ID is 0.
日志说明	MEP收到交叉连接的CCM报文，该报文包含与本端不同的MA ID或MD ID
处理建议	检查两端MEP的配置。让MEP所属的MD和MA的配置一致，且两端MEP级别相同、方向都相同

10.2 CFD_ERROR_CCM

日志内容	MEP [UINT16] in SI [INT32] received an error CCM. It's SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
参数解释	$1：服务实例的ID $2：本地MEP的ID $3：源MAC地址 $4：序列号 $5：远端MEP的ID $6：MD的ID。如果不存在，会显示“without ID” $7：MA的ID
日志等级	6
举例	CFD/6/CFD_ERROR_CCM: MEP 2 in SI 7 received an error CCM. Its SrcMAC is 0011-2233-4401, SeqNum is 21, RMEP is 2, MD ID is 7, MA ID is 1.
日志说明	MEP收到错误的CCM报文，该报文包含错误的MEP ID或生存时间
处理建议	检查CCM配置。让两端的CC检测周期配置一致，并配置远端MEP ID在本端允许的MEP列表中

10.3 CFD_LOST_CCM

日志内容	MEP [UINT16] in SI [INT32] failed to receive CCMs from RMEP [UINT16].
参数解释	$1：本地MEP的ID $2：服务实例ID $3：远端MEP的ID
日志等级	6
举例	CFD/6/CFD_LOST_CCM: MEP 1 in SI 7 failed to receive CCMs from RMEP 2.
日志说明	MEP在3.5个CCM报文发送周期内没有收到CCM报文，可能的原因是链路故障或远端MEP在此期间没有发送CCM报文
处理建议	检查链路状态和远端MEP的配置。如果链路down了或有其它的故障，例如单通故障，则恢复此链路。如果远端配置了同一服务实例的MEP，则确认两端的CC发送周期是一致的

10.4 CFD_NO_HRD_RESOURCE

日志内容	Failed to start CCM on service instance [INT32] because of insufficient hardware frequency resources.
参数解释	$1：服务实例ID
日志等级	6
举例	CFD/6/CFD_NO_HRD_RESOURCE: -MDC=1; Failed to start CCM on service instance 7 because of insufficient hardware frequency resources.
日志说明	硬件频率资源不足，无法启动该服务实例的CCM检测
处理建议	请联系技术支持

10.5 CFD_REACH_LOWERLIMIT

日志内容	[STRING] reached or fell below the lower limit [STRING] on MEP [UINT16] in service instance [INT32].
参数解释	$1：检测事件： o Far-end frame loss ratio：表示目标 MEP 的帧丢失率 o Near-end frame loss ratio：表示源 MEP 的帧丢失率 o Frame delay：表示帧时延 $2：阈值 $3：本地MEP的ID $4：服务实例ID
日志等级	6
举例	CFD/6/ CFD_REACH_LOWERLIMIT: Far-end frame loss ratio reached or fell below the lower limit 4% on MEP 2 in service instance 3.
日志说明	检测结果达到或低于下限
处理建议	无

10.6 CFD_REACH_UPPERLIMIT

日志内容	[STRING] reached or exceeded the upper limit [STRING] on MEP [UINT16] in service instance [INT32].
参数解释	$1：检测事件： o Far-end frame loss ratio：表示目标 MEP 的帧丢失率 o Near-end frame loss ratio：表示源 MEP 的帧丢失率 o Frame delay：表示帧时延 $2：阈值 $3：本地MEP的ID $4：服务实例ID
日志等级	6
举例	CFD/6/ CFD_REACH_UPPERLIMIT: Far-end frame loss ratio reached or fell below the upper limit 80% on MEP 1 in service instance 3.
日志说明	检测结果达到或超过上限
处理建议	无

10.7 CFD_RECEIVE_CCM

日志内容	MEP [UINT16] in SI [INT32] received CCMs from RMEP [UINT16]
参数解释	$1：本地MEP的ID $2：服务实例ID $3：远端MEP的ID
日志等级	6
举例	CFD/6/CFD_RECEIVE_CCM: MEP 1 in SI 7 received CCMs from RMEP 2.
日志说明	MEP收到远端MEP发送的CCM报文
处理建议	无

11 CFGMAN

本节介绍配置管理模块输出的日志信息。

11.1 CFGMAN_CFGCHANGED

日志内容	-EventIndex=[INT32]-CommandSource=[INT32]-ConfigSource=[INT32]-ConfigDestination=[INT32]; Configuration changed.
参数解释	$1：事件索引，取值范围为1到2147483647 $2：引起配置变化的来源，取值为： • cli：表示引起配置变化的来源为命令行 • snmp：表示引起配置变化的来源为 SNMP 或者 SNMP 监控到配置数据库发生变化 • other：表示引起配置变化的来源为其它途径 $3：源配置，取值为： • erase：配置删除或重命名 • running：保存正在运行的配置 • commandSource：拷贝配置文件 • startup：保存运行配置到下次启动配置文件 • local：保存运行配置到本地文件 • networkFtp：通过 FTP 方式将网络上的某个配置文件保存到设备作为运行配置或者下次启动配置 • hotPlugging：热插拔板卡导致配置被删除或者失效 $4：目的配置，取值为： • erase：配置删除或重命名 • running：保存正在运行的配置 • commandSource：拷贝配置文件 • startup：保存运行配置到下次启动配置文件 • local：保存运行配置到本地文件 • networkFtp：通过 FTP 方式将网络上的某个配置文件保存到设备作为运行配置或者下次启动配置 • hotPlugging：热插拔板卡导致配置被删除或者失效
日志等级	5
举例	CFGMAN/5/CFGMAN_CFGCHANGED: -EventIndex=[6]-CommandSource=[snmp]-ConfigSource=[startup]-ConfigDestination=[running]; Configuration changed.
日志说明	如果配置在过去的十分钟内发生了变化，设备将记录事件索引、引起配置变化的来源、源配置以及目的配置
处理建议	无

11.2 CFGMAN_OPTCOMPLETION

日志内容	-OperateType=[INT32]-OperateTime=[INT32]-OperateState=[INT32]-OperateEndTime=[INT32]; Operation completed.
参数解释	$1：操作类型，取值为： • running2startup：将运行配置保存为下次启动配置 • startup2running：将下次启动配置设置为运行配置 • running2net：将运行配置保存到网络 • net2running：将网络上的配置文件上传到设备，并作为当前配置运行 • net2startup：将网络上的配置文件上传到设备，并保存为下次启动配置文件 • startup2net：将下次启动配置文件保存到网络 $2：操作时间 $3：操作状态，取值为： • InProcess：正在执行 • success：执行成功 • InvalidOperation：无效的操作 • InvalidProtocol：无效的协议 • InvalidSource：无效的源文件名 • InvalidDestination：无效的目的文件名 • InvalidServer：无效的服务器地址 • DeviceBusy：设备繁忙 • InvalidDevice：设备地址无效 • DeviceError：设备出错 • DeviceNotWritable：设备不可写 • DeviceFull：设备的存储空间不足 • FileOpenError：文件打开出错 • FileTransferError：文件传输出错 • ChecksumError：文件校验和错误 • LowMemory：没有内存 • AuthFailed：用户验证失败 • TransferTimeout：传输超时 • UnknownError：未知原因 • invalidConfig：无效配置 $4：操作结束时间
日志等级	5
举例	CFGMAN/5/CFGMAN_OPTCOMPLETION: -OperateType=[running2startup]-OperateTime=[248]-OperateState=[success]-OperateEndTime=[959983]; Operation completed.
日志说明	操作完成后记录操作的类型、状态以及时间
处理建议	请根据OperateState的值定位、处理问题

12 CLKM

本节介绍 CLKM（Clock Monitoring）模块输出的日志信息。

12.1 CLKM_ESMC_PKT_ALARM

日志内容	ESMC packets were lost. (PortName=[STRING])
参数解释	$1：接收ESMC报文的接口名称
日志等级	4
举例	CLKM/4/CLKM_ESMC_PKT_ALARM: ESMC packets were lost. (PortName=G1/2/0/1)
日志说明	ESMC报文丢失
处理建议	1. 查看本端和对端端口是否均配置 **esmc enable**，开启当前接口的 ESMC 功能 ○ 是：执行步骤 3 ○ 否：执行步骤 2 2. 在本段和对端端口补全 **esmc enable** 配置，查看设备是否继续打印该日志 ○ 是：执行步骤 3 ○ 否：问题解决 3. 收集告警、日志和配置信息，联系技术支持

12.2 CLKM_SOURCE_FREQDEVIATION_ALARM

日志内容	The frequency offset of the clock reference for [STRING] has crossed the threshold.
参数解释	$1：device或chassis编号
日志等级	4
举例	CLKM/4/CLKM_SOURCE_FREQDEVIATION_ALARM: The frequency offset of the clock reference for chassis 1 has crossed the threshold.
日志说明	时钟信号频偏值大于等于阈值
处理建议	查看时钟信号频偏检测的状态是否为告警状态

12.3 CLKM_SOURCE_FREQDEVIATION_NORMAL

日志内容	The frequency offset of the clock reference for [STRING] has dropped below the threshold and resumed to normal.
参数解释	$1：device或chassis编号
日志等级	4
举例	CLKM/4/CLKM_SOURC_FREQDEVIATION_NORMAL: The frequency offset of the clock reference for chassis 1 has dropped below the threshold and resumed to normal.
日志说明	时钟信号频偏值恢复到小于阈值
处理建议	无

12.4 CLKM_SOURCE_LOST

日志内容	[STRING] has lost signals from the clock reference.
参数解释	$1：Device或chassis编号
日志等级	4
举例	CLKM/4/CLKM_SOURCE_LOST: Chassis 1 has lost signals from the clock reference.
日志说明	时钟源信号丢失
处理建议	检查相关配置和参考源状态

12.5 CLKM_SOURCE_SSM_DEGRADE

日志内容	The SSM quality level of the clock reference for [STRING] has degraded from [STRING] to [STRING]. The SSM quality level threshold is [STRING].
参数解释	$1：device或chassis编号 $2：劣化前的SSM级别 $3：劣化后的SSM级别 $4：SSM级别劣化告警阈值
日志等级	4
举例	CLKM/4/CLKM_SOURCE_SSM_DEGRADE: The SSM quality level of the clock reference for chassis 1 has degraded from SSU-A to SEC. The SSM quality level threshold is SSU-A.
日志说明	时钟源SSM级别劣化，时钟源当前的SSM级别已经低于告警阈值
处理建议	检查相关配置和参考源状态

12.6 CLKM_SOURCE_SSM_RESUME

日志内容	The SSM quality level of the clock reference for [STRING] has risen from [STRING] to [STRING].The SSM quality level threshold is [STRING].
参数解释	$1：device或chassis编号 $2：劣化前的SSM级别 $3：劣化后的SSM级别 $4：SSM级别劣化告警阈值
日志等级	4
举例	CLKM/4/CLKM_SOURCE_SSM_RESUME: The SSM quality level of the clock reference for chassis 1 has risen from SEC to SSU-A. The SSM quality level threshold is SSU-A.
日志说明	时钟源SSM级别劣化恢复，时钟源当前的SSM级别已经达到告警阈值范围内
处理建议	无

12.7 CLKM_SOURCE_SWITCHOVER

日志内容	The clock reference of [STRING] has changed to [STRING].
参数解释	$1：device或chassis编号 $2：接口名，取值包括： • 实际的接口：时钟信号由上一级设备提供，通过指定的 WAN 接口输入，即线路时钟源的输入端口 • BITS0：由 BITS0 时钟设备产生的时钟信号 • BITS1：由 BITS1 时钟设备产生的时钟信号 • PTP：通过 PTP 协议获取的时钟信号 • local clock reference：时钟信号为本设备时钟扣板内部晶体震荡器产生的 38.88 MHz 信号
日志等级	4
举例	CLKM/4/CLKM_SOURCE_SSM_SWITCHOVER: The clock reference of chassis 1 has changed to BITS0.
日志说明	时钟源发生倒换
处理建议	无

13 DEV

本节介绍 DEV（设备管理）模块输出的日志信息。

13.1 BOARD_REBOOT

日志内容	Board is rebooting on [STRING].
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	DEV/5/BOARD_REBOOT: Board is rebooting on slot 1.
日志说明	用户在重启指定slot，或者指定slot因为异常而重启
处理建议	**1.** 检查是否有用户在重启指定 slot **2.** 如果没有用户重启，等待指定 slot 重新启动后，通过 display version 命令、对应指定 slot 信息中的 Last reboot reason 字段，查看重启原因 **3.** 如果重启原因为异常重启，请联系技术支持

13.2 BOARD_REMOVED

日志内容	Board was removed from [STRING], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：单板类型
日志等级	3
举例	DEV/3/BOARD_REMOVED: Board was removed from slot 1, type is LSQ1FV48SA.
日志说明	一块LPU或者备用MPU被拔出。设备退出集群
处理建议	**1.** 检查对应单板是否插紧 **2.** 检查对应单板是否损坏 **3.** 重新插入单板或更换单板 **4.** 重新将设备加入集群

13.3 BOARD_STATE_FAULT

日志内容	Board state changed to Fault on [STRING], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：单板类型
日志等级	2
举例	DEV/2/BOARD_STATE_FAULT: Board state changed to Fault on slot 1, type is LSQ1FV48SA.
日志说明	单板在以下情况会处于Fault（故障）状态： • 单板处于启动阶段（正在初始化或者加载软件版本），单板不可用 • 单板不能正常工作
处理建议	根据日志产生的情况，处理建议如下： • 对于第一种情况：单板型号不同，加载的软件版本不同，启动所需的时间不同。一般不超过 10 分钟，请以设备的实际情况为准 • 对于第二种情况：请联系技术支持

13.4 BOARD_STATE_NORMAL

日志内容	Board state changed to Normal on [STRING], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：单板类型
日志等级	5
举例	DEV/5/BOARD_STATE_NORMAL: Board state changed to Normal on slot 1, type is LSQ1FV48SA.
日志说明	一块新插入的LPU或者备用MPU完成了初始化
处理建议	无

13.5 CFCARD_FAILED

日志内容	CF card state changed to Fault in [STRING] [STRING].
参数解释	$1：the device或chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号（仅支持多个CF卡的产品支持该字段）
日志等级	3
举例	DEV/3/CFCARD_FAILED: CF card state changed to Fault in slot 1 CF card slot 1.
日志说明	CF卡故障
处理建议	**1.** 检查 CF 卡是否损坏 **2.** 重新安装 CF 卡或更换 CF 卡

13.6 CFCARD_INSERTED

日志内容	CF card was inserted in [STRING] [STRING].
参数解释	$1：the device或chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号（仅支持多个CF卡的产品支持该字段）
日志等级	4
举例	DEV/4/CFCARD_INSERTED: CF card was inserted in slot 1 CF card slot 1.
日志说明	CF卡安装到了指定槽位
处理建议	无

13.7 CFCARD_REMOVED

日志内容	CF card was removed from [STRING] [STRING].
参数解释	$1：the device或chassis编号+slot编号或slot编号 $2：CF卡所在的槽位号（仅支持多个CF卡的产品支持该字段）
日志等级	3
举例	DEV/3/CFCARD_REMOVED: CF card was removed from slot 1 CF card slot 1.
日志说明	CF卡被拔出
处理建议	**1.** 检查 CF 卡是否插紧 **2.** 检查 CF 卡是否损坏 **3.** 重新安装 CF 卡或更换 CF 卡

13.8 CHASSIS_REBOOT

日志内容	Chassis [STRING] is rebooting now.
参数解释	$1：chassis编号
日志等级	5
举例	DEV/5/CHASSIS_REBOOT: Chassis 1 is rebooting now.
日志说明	用户在重启成员设备，或者成员设备因为异常而重启
处理建议	**1.** 检查是否有用户在重启成员设备 **2.** 如果没有用户重启，等待成员设备重新启动后，通过 display version 命令、对应成员设备单板信息中的 Last reboot reason 字段，查看重启原因 **3.** 如果重启原因为异常重启，请联系技术支持

13.9 CPU_STATE_NORMAL

日志内容	Cpu state changed to Normal on [STRING].
参数解释	$1：chassis编号+slot编号+CPU编号或slot编号+CPU编号，只有slot支持多CPU时，才显示CPU编号
日志等级	5
举例	DEV/5/CPU_STATE_NORMAL: Cpu state changed to Normal on slot 1 cpu 1.
日志说明	CPU状态变成正常
处理建议	无

13.10 DEV_CLOCK_CHANGE

日志内容	-User=[STRING]-IPAddr=[IPADDR]; System clock changed from [STRING] to [STRING].
参数解释	$1：当前登录用户的用户名 $2：当前登录用户的IP地址 $3：老时间 $4：新时间
日志等级	5
举例	DEV/5/DEV_CLOCK_CHANGE: -User=admin-IPAddr=192.168.1.2; System clock changed from 15:49:52 01/02/2013 to 15:50:00 01/02/2013.
日志说明	系统时间发生了变更
处理建议	无

13.11 DEV_FAULT_TOOLONG

日志内容	Card in [STRING] is still in Fault state for [INT32] minutes.
参数解释	$1：chassis编号+slot编号或slot编号 $2：状态的持续时间
日志等级	4
举例	DEV/4/DEV_FAULT_TOOLONG: Card in slot 1 is still in Fault state for 60 minutes.
日志说明	单板长期处于Fault状态
处理建议	1. 重启单板尝试恢复 2. 联系工程师分析解决

13.12 DEV_REBOOT_UNSTABLE

日志内容	A reboot command was executed while the system status was not Stable.
参数解释	无
日志等级	5
举例	DEV/5/DEV_REBOOT_UNSTABLE: A reboot command was executed while the system status was not Stable.
日志说明	设备处于非稳定状态时，用户执行了**reboot**命令
处理建议	系统启动需要一定的时间，才能达到Stable状态。所以，在系统启动过程中请不要执行重启操作。如果系统长时间未能进入Stable状态，可通过**display system stable state**命令的显示信息找出未稳定的对象，根据其具体状态，采取进一步措施

13.13 DYINGGASP

日志内容	Power failure or manual power-off occurred.
参数解释	无
日志等级	0
举例	DYINGGASP/0/DYINGGASP: Power failure or manual power-off occurred.
日志说明	设备掉电，发送断电告警
处理建议	1. 检查设备电源连接是否正确 2. 如果为电源模块故障，请更换电源模块 3. 联系工程师定位解决

13.14 FAN_ABSENT

日志内容	形式一： Fan [INT32] is absent. 形式二： Chassis [STRING] fan [INT32] is absent.
参数解释	形式一： $1：风扇ID 形式二： $1：chassis编号 $2：风扇ID
日志等级	3
举例	DEV/3/FAN_ABSENT: Fan 2 is absent.
日志说明	指定位置没有风扇，或风扇被拔出
处理建议	**1.** 如果指定位置没有风扇，则可能因散热不好，引起设备温度升高，建议安装风扇 **2.** 如果有风扇，检查风扇框是否插紧 **3.** 检查风扇框是否损坏 **4.** 重新安装风扇框或更换风扇框

13.15 FAN_DIRECTION_NOT_PREFERRED

日志内容	Fan [INT32] airflow direction is not preferred on [STRING], please check it.
参数解释	$1：风扇ID $2：chassis编号+slot编号或slot编号
日志等级	1
举例	DEV/1/FAN_DIRECTION_NOT_PREFERRED: Fan 1 airflow direction is not preferred on slot 1, please check it.
日志说明	风扇的风道方向不是用户期望的方向。风扇方向配置出错或者插错风扇
处理建议	**1.** 根据机房通风系统的风向，选择风向一致的型号的风扇 **2.** 如果风扇风向和机房通风系统风向一致，请调整风扇风向的配置

13.16 FAN_FAILED

日志内容	形式一： Fan [INT32] failed. 形式二： Chassis [STRING] fan [INT32] failed.
参数解释	形式一： $1：风扇ID 形式二： $1：chassis编号 $2：风扇ID
日志等级	2
举例	DEV/2/FAN_FAILED: Fan 2 failed.
日志说明	风扇出现了故障，停止工作
处理建议	更换风扇

13.17 FAN_RECOVERED

日志内容	形式一： Fan [INT32] recovered. 形式二： Chassis [INT32] fan [INT32] recovered.
参数解释	形式一： $1：风扇ID 形式二： $1：chassis编号 $2：风扇ID
日志等级	5
举例	DEV/5/FAN_RECOVERED: Fan 2 recovered.
日志说明	插入风扇，稍后，风扇转入正常工作状态
处理建议	无

13.18 MAD_DETECT

日志内容	Multi-active devices detected, please fix it.
参数解释	无
日志等级	1
举例	DEV/1/MAD_DETECT: Multi-active devices detected, please fix it.
日志说明	当收到冲突消息的时候，检测到冲突，需要解决冲突问题
处理建议	1. 使用 **display cluster** 查看当前集群中有哪些成员设备，以便确定哪些成员设备分裂了 2. 查看集群链路信息，确认故障的集群链路 3. 手工修复状态为 DOWN 的集群链路

13.19 POWER_ABSENT

日志内容	形式一： Power [INT32] is absent. 形式二： Chassis [INT32] power [INT32] is absent.
参数解释	形式一： $1：电源模块ID 形式二： $1：chassis编号 $2：电源模块ID
日志等级	3
举例	DEV/3/POWER_ABSENT: Power 1 is absent.
日志说明	电源模块被拔出
处理建议	1. 检查电源是否插紧 2. 检查电源是否损坏 3. 重新安装电源或更换电源

13.20 POWER_FAILED

日志内容	形式一： Power [INT32] failed. 形式二： Chassis [INT32] power [INT32] failed.
参数解释	形式一： $1：电源模块ID 形式二： $1：chassis编号 $2：电源模块ID
日志等级	2
举例	DEV/2/POWER_FAILED: Power 1 failed.
日志说明	电源模块出现故障
处理建议	更换电源

13.21 POWER_MONITOR_ABSENT

日志内容	形式一： Power monitor unit [INT32] is absent. 形式二： Chassis [INT32] power monitor unit [INT32] is absent.
参数解释	形式一： $1：电源监控模块ID 形式二： $1：chassis编号 $2：电源监控模块ID
日志等级	3
举例	DEV/3/POWER_MONITOR_ABSENT: Power monitor unit 1 is absent.
日志说明	电源监控模块被拔出
处理建议	**1.** 检查电源监控模块是否插紧 **2.** 检查电源监控模块是否损坏 **3.** 重新安装电源监控模块或更换电源监控模块

13.22 POWER_MONITOR_FAILED

日志内容	形式一： Power monitor unit [INT32] failed. 形式二： Chassis [INT32] power monitor unit [INT32] failed.
参数解释	形式一： $1：电源监控模块ID 形式二： $1：chassis编号 $2：电源监控模块ID
日志等级	2
举例	DEV/2/POWER_MONITOR_FAILED: Power monitor unit 1 failed.
日志说明	电源监控模块出现故障
处理建议	更换电源监控模块

13.23 POWER_MONITOR_RECOVERED

日志内容	形式一： Power monitor unit [INT32] recovered. 形式二： Chassis [INT32] power monitor unit [INT32] recovered.
参数解释	形式一： $1：电源监控模块ID 形式二： $1：chassis编号 $2：电源监控模块ID
日志等级	5
举例	DEV/5/POWER_MONITOR_RECOVERED: Power monitor unit 1 recovered.
日志说明	电源监控模块插入后，状态从Failed或者Absent状态转换为OK
处理建议	无

13.24 POWER_RECOVERED

日志内容	形式一： Power [INT32] recovered. 形式二： Chassis [INT32] power [INT32] recovered.
参数解释	形式一： $1：电源模块ID 形式二： $1：chassis编号 $2：电源模块ID
日志等级	5
举例	DEV/5/POWER_RECOVERED: Power 1 recovered.
日志说明	电源模块插入后，状态从Failed或者Absent状态转换为OK
处理建议	无

13.25 RPS_ABSENT

日志内容	形式一： RPS [INT32] is absent. 形式二： Chassis [INT32] RPS [INT32] is absent.
参数解释	形式一： $1：冗余电源模块ID 形式二： $1：chassis编号 $2：冗余电源模块ID
日志等级	3
举例	DEV/3/RPS_ABSENT: RPS 1 is absent.
日志说明	冗余电源模块被拔出
处理建议	**1.** 检查冗余电源模块是否插紧 **2.** 检查冗余电源模块是否损坏 **3.** 重新安装冗余电源模块或更换冗余电源模块

13.26 RPS_NORMAL

日志内容	形式一： RPS [INT32] is normal. 形式二： Chassis [INT32] RPS [INT32] is normal.
参数解释	形式一： $1：冗余电源模块ID 形式二： $1：chassis编号 $2：冗余电源模块ID
日志等级	5
举例	DEV/5/RPS_NORMAL: RPS 1 is normal.
日志说明	冗余电源模块插入后，状态正常
处理建议	无

13.27 SUBCARD_FAULT

日志内容	Subcard state changed to Fault on [STRING] subslot [INT32], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号 $3：子卡类型
日志等级	2
举例	DEV/2/SUBCARD_FAULT: Subcard state changed to Fault on slot 1 subslot 1, type is MIM-1ATM-OC3SML.
日志说明	子卡重启，稍后，子卡状态转换为Fault，或者子卡故障
处理建议	**1.** 如果后续子卡状态可以变为 Normal，则无需处理 **2.** 如果子卡一直处于 Falut 状态，则子卡故障，更换子卡

13.28 SUBCARD_INSERTED

日志内容	Subcard was inserted in [STRING] subslot [INT32], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号 $3：子卡类型
日志等级	4
举例	DEV/4/SUBCARD_INSERTED: Subcard was inserted in slot 1 subslot 1, type is MIM-1ATM-OC3SML.
日志说明	一块子卡安装到了指定槽位
处理建议	无

13.29 SUBCARD_REBOOT

日志内容	Subcard is rebooting on [STRING] subslot [INT32].
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号
日志等级	5
举例	DEV/5/SUBCARD_REBOOT: Subcard is rebooting on slot 1 subslot 1.
日志说明	用户在重启子卡或者子卡因为运行异常自动重启
处理建议	如果子卡重启后能正常运行，则无需处理。如果您想进一步了解异常重启的原因或者子卡不断自动重启，请联系技术支持

13.30 SUBCARD_REMOVED

日志内容	Subcard was removed from [STRING] subslot [INT32], type is [STRING].
参数解释	$1：chassis编号+slot编号或slot编号 $2：子卡所在的子槽位号 $3：子卡类型
日志等级	3
举例	DEV/3/SUBCARD_REMOVED: Subcard was removed from slot 1 subslot 1, type is MIM-1ATM-OC3SML.
日志说明	一块子卡被拔出
处理建议	**1.** 检查子卡是否插紧 **2.** 检查子卡是否损坏 **3.** 重新安装子卡或更换子卡

13.31 SYSTEM_REBOOT

日志内容	System is rebooting now.
参数解释	无
日志等级	5
举例	DEV/5/SYSTEM_REBOOT: System is rebooting now.
日志说明	用户在重启系统，或者系统因为异常而重启
处理建议	**1.** 检查是否有用户在重启系统 **2.** 如果没有用户重启，等待系统重新启动后，通过 display version 命令显示信息中的 Last reboot reason 字段，查看重启原因 **3.** 如果重启原因为异常重启，请联系技术支持

13.32 TEMPERATURE_ALARM

日志内容	形式一： Temperature is greater than the high-temperature alarming threshold on sensor [STRING] [USHOT]. 形式二： Temperature is greater than the high-temperature alarming threshold on [STRING] sensor [STRING] [USHOT]. 形式三： Temperature is greater than the high-temperature alarming threshold on [STRING] [STRING] sensor [STRING] [USHOT].
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4
举例	DEV/4/TEMPERATURE_ALARM: Temperature is greater than the high-temperature alarming threshold on slot 1 sensor inflow 1.
日志说明	传感器温度超过严重级（Alarm）高温告警门限。环境温度太高或者风扇异常
处理建议	1. 检查环境温度是否过高，保持设备环境正常通风 2. **display fan** 命令检查风扇是否不在或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇

13.33 TEMPERATURE_LOW

日志内容	形式一： Temperature is less than the low-temperature threshold on sensor [STRING] [INT32]. 形式二： Temperature is less than the low-temperature threshold on [STRING] sensor [STRING] [INT32]. 形式三： Temperature is less than the low-temperature threshold on [STRING] [STRING] sensor [STRING] [INT32].
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4
举例	DEV/4/TEMPERATURE_LOW: Temperature is less than the low-temperature threshold on slot 1 sensor inflow 1.
日志说明	传感器温度低于低温告警门限
处理建议	环境温度过低，改善环境温度

13.34 TEMPERATURE_NORMAL

日志内容	形式一： Temperature changed to normal on sensor [STRING] [INT32]. 形式二： Temperature changed to normal on [STRING] sensor [STRING] [INT32]. 形式三： Temperature changed to normal on [STRING] [STRING] sensor [STRING] [INT32].
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	5
举例	DEV/5/TEMPERATURE_NORMAL: Temperature changed to normal on slot 1 sensor inflow 1.
日志说明	传感器温度指示正常（大于低温告警门限，小于一般级高温告警门限）
处理建议	无

13.35 TEMPERATURE_POWEROFF

日志内容	Powering off [STRING]: Temperature exceeded the shutdown threshold.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	5
举例	DEV/2/TEMPERATURE_POWEROFF: Powering off slot 1: Temperature exceeded the shutdown threshold.
日志说明	传感器温度指示正常（大于低温告警门限，小于一般级高温告警门限）
处理建议	1. 检查环境温度是否过高，保持设备环境通风正常 2. **display fan** 命令检查风扇是否拔出或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇 3. 手动给单板上电

13.36 TEMPERATURE_SHUTDOWN

日志内容	形式一： Temperature is greater than the high-temperature shutdown threshold on sensor [STRING] [INT32]. The slot will be powered off automatically. 形式二： Temperature is greater than the high-temperature shutdown threshold on [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically. 形式三： Temperature is greater than the high-temperature shutdown threshold on [STRING] [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically.
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	2
举例	DEV/2/TEMPERATURE_SHUTDOWN: Temperature is greater than the high-temperature shutdown threshold on slot 1 sensor inflow 1. The slot will be powered off automatically.
日志说明	传感器温度超过关断级高温告警门限。环境温度太高或者风扇异常
处理建议	1. 检查环境温度是否过高，保持设备环境通风正常 2. **display fan** 命令检查风扇是否不在或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇

13.37 TEMPERATURE_WARNING

日志内容	形式一： Temperature is greater than the high-temperature warning threshold on sensor [STRING] [INT32]. 形式二： Temperature is greater than the high-temperature warning threshold on [STRING] sensor [STRING] [INT32]. 形式三： Temperature is greater than the high-temperature warning threshold on [STRING] [STRING] sensor [STRING] [INT32].
参数解释	形式一： $1：传感器类型 $2：传感器ID 形式二： $1：slot编号 $2：传感器类型 $3：传感器ID 形式三： $1：chassis编号 $2：slot编号 $3：传感器类型 $4：传感器ID
日志等级	4
举例	DEV/4/TEMPERATURE_WARNING: Temperature is greater than the high-temperature warning threshold on slot 1 sensor inflow 1.
日志说明	传感器温度超过一般级高温告警门限。环境温度太高或者风扇异常
处理建议	1. 检查环境温度是否过高，保持设备环境通风正常 2. **display fan** 命令检查风扇是否不在或故障，以及检查风扇实际是否运转。如果风扇不在位，安装风扇；如果风扇故障，更换风扇

13.38 VCHK_VERSION_INCOMPATIBLE

日志内容	Software version of [STRING] is incompatible with that of the MPU.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	1
举例	DEV/1/VCHK_VERSION_INCOMPATIBLE: Software version of slot 1 is incompatible with that of the MPU.
日志说明	PEX在启动过程中，检测到自己的启动软件包和父设备上运行的软件包版本不兼容，PEX会打印该信息并重启
处理建议	请设置与父设备当前版本兼容的软件包作为该PEX的下次启动软件包/加载软件包

14 DHCP

本节介绍 DHCP（Dynamic Host Configuration Protocol）模块输出的日志信息。

14.1 DHCP_NORESOURCES

日志内容	Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
参数解释	无
日志等级	3
举例	DHCP/3/DHCP_NORESOURCES: Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
日志说明	配置DHCP功能需要针对DHCP报文下发报文过滤规则。由于设备硬件资源不足，导致设置DHCP报文过滤规则失败
处理建议	如果设备业务占用硬件资源过多，可能会导致资源不足，需要释放一些资源，重新配置DHCP功能

14.2 DHCP_NOTSUPPORTED

日志内容	Failed to apply filtering rules for DHCP packets because some rules are not supported.
参数解释	无
日志等级	3
举例	DHCP/3/DHCP_NOTSUPPORTED: Failed to apply filtering rules for DHCP packets because some rules are not supported.
日志说明	配置DHCP功能需要针对DHCP报文下发DHCP报文过滤规则。由于设备不支持某些报文过滤规则，导致设置DHCP报文过滤规则失败
处理建议	无

15 DHCPR

本节介绍 DHCPR（IPv4 DHCP Relay）模块输出的日志信息。

15.1 DHCPR_SERVERCHANGE

日志内容	Switched to the server of pool [STRING] at [IPADDR] because the current server did not respond. Switched to the server of interface [STRING] at [IPADDR] because the current server did not respond.
参数解释	$1：中继地址池名称 $2：切换到下一个DHCP服务器的IP地址 $3：开启中继功能的接口
日志等级	3
举例	DHCPR/3/DHCPR_SERVERCHANGE: -MDC=1; Switched to the server of pool 1 at *2.2.2.2* because the current server did not respond. DHCPR/3/DHCPR_SERVERCHANGE: -MDC=1; Switched to the server of interface GigabitEthernet1/2/0/1 at *2.2.2.2* because the current server did not respond.
日志说明	因为DHCP中继无法从当前的DHCP服务器得到应答，所以DHCP中继切换到下一台DHCP服务器申请IP地址
处理建议	无需处理

15.2 DHCPR_SWITCHMASTER

日志内容	Switched to the master DHCP server at [IPADDR].
参数解释	$1：主用DHCP服务器的IP地址
日志等级	3
举例	DHCPR/3/DHCPR_SWITCHMASTER: -MDC=1; Switched to the master DHCP server at 2.2.2.2.
日志说明	DHCP中继可以配置延迟回切时间，如果当时生效的为备用服务器，在经过延迟时间，DHCP中继会切换到主用DHCP服务器来执行申请IP地址的操作
处理建议	无需处理

16 DHCPS

本节介绍 DHCPS（ipv4 DHCP server）模块输出的日志信息。

16.1 DHCPS_ALLOCATE_IP

日志内容	DHCP server received a DHCP client's request packet on interface [STRING], and allocated an IP address [IPADDR](lease [UINT32] seconds) for the DHCP client(MAC [MAC]) from [STRING] pool.
参数解释	$1：IPv4 DHCP服务器所在接口的接口名 $2：分配给IPv4 DHCP客户端的IPv4地址 $3：分配给IPv4 DHCP客户端的IPv4地址租约时长 $4：IPv4 DHCP客户端的MAC地址 $5：IPv4 DHCP服务器地址池名
日志等级	5
举例	DHCPS/5/DHCPS_ALLOCATE_IP: DHCP server received a DHCP client's request packet on interface GigabitEthernet1/2/0/2, and allocated an IP address 1.0.0.91(lease 86400 seconds) for the DHCP client(MAC dc2d-cb00-905a) from p1 pool.
日志说明	IPv4 DHCP服务器为IPv4 DHCP客户端分配一个IPv4地址租约
处理建议	无

16.2 DHCPS_CONFLICT_IP

日志内容	A conflict IP [IPADDR] from [STRING] pool was detected by DHCP server on interface [STRING].
参数解释	$1：冲突的IPv4地址 $2：IPv4 DHCP服务器地址池名 $3：IPv4 DHCP服务器所在接口的接口名
日志等级	5
举例	DHCPS/5/DHCPS_CONFLICT_IP: A conflict IP 100.1.1.1 from p1 pool was detected by DHCP server on interface GigabitEthernet1/2/0/2.
日志说明	IPv4 DHCP服务器从地址池中删除一个冲突地址
处理建议	无

16.3 DHCPS_EXTEND_IP

日志内容	DHCP server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IP [IPADDR], MAC [MAC]).
参数解释	$1：IPv4 DHCP服务器所在接口的接口名 $2：IPv4 DHCP服务器地址池名 $3：分配给IPv4 DHCP客户端的IPv4地址 $4：IPv4 DHCP客户端的MAC地址
日志等级	5
举例	DHCPS/5/DHCPS_EXTEND_IP: DHCP server received a DHCP client's request packet on interface GigabitEthernet1/2/0/2, and extended lease from p1 pool for the DHCP client (IP 1.0.0.91, MAC dc2d-cb00-905a).
日志说明	IPv4 DHCP服务器为IPv4 DHCP客户端续约
处理建议	无

16.4 DHCPS_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPS/4/DHCPS_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCP server保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

16.5 DHCPS_RECLAIM_IP

日志内容	DHCP server reclaimed a [STRING] pool's lease(IP [IPADDR], lease [UINT32] seconds), which is allocated for the DHCP client (MAC [MAC]).
参数解释	$1：IPv4 DHCP服务器地址池名 $2：分配给IPv4 DHCP客户端的IPv4地址 $3：分配给IPv4 DHCP客户端的IPv4地址租约时长 $4：IPv4 DHCP客户端的MAC地址
日志等级	5
举例	DHCPS/5/DHCPS_RECLAIM_IP: DHCP server reclaimed a p1 pool's lease(IP 1.0.0.91, lease 86400 seconds), which is allocated for the DHCP client (MAC dc2d-cb00-905a).
日志说明	IPv4 DHCP服务器回收一个分配给IPv4 DHCP客户端的地址租约
处理建议	无

16.6 DHCPS_THRESHOLD_EXCEED

日志内容	The IP address utilization of the address pool [STRING] has exceeded the threshold.
参数解释	$1：地址池名称
日志等级	5
举例	The IP address utilization of the address pool 1 has exceeded the threshold.
日志说明	DHCP地址池中的地址使用率已经高于指定阈值
处理建议	管理员需要重新规划地址池中的地址资源

16.7 DHCPS_THRESHOLD_RECOVER

日志内容	The IP address usage of pool [STRING] has descended to 90% of the threshold.
参数解释	$1：地址池名称
日志等级	5
举例	DHCPS/5/DHCPS_THRESHOLD_RECOVER: The IP address usage of pool 1 has descended to 90% of the threshold.
日志说明	DHCP地址池中的地址使用率已经下降到指定阈值的90%
处理建议	无

16.8 DHCPS_VERIFY_CLASS

日志内容	Illegal DHCP client-PacketType=[STRING]-ClientAddress=[MAC];
参数解释	$1：报文类型 $2：IPv4 DHCP客户端的硬件地址
日志等级	5
举例	DHCPS/5/DHCPS_VERIFY_CLASS: Illegal DHCP client-PacketType= DHCPDISCOVER-ClientAddress=dc2d-cb01-0104;
日志说明	IPv4 DHCP服务器对客户端报文白名单验证不通过
处理建议	确认该DHCP客户端是否合法

16.9 DHCPS_WARNING_EXHAUSTION

日志内容	Address pool [STRING] has run out of IP addresses.
参数解释	$1：地址池名称
日志等级	5
举例	DHCPS/5/DHCPS_WARNING_EXHAUSTION: Address pool 1 has run out of IP addresses.
日志说明	DHCP地址池中的地址资源已耗尽
处理建议	管理员需要重新规划地址池中的地址资源

17 DHCPS6

本节介绍 DHCPS6（IPv6 DHCP server）模块输出的 日志信息。

17.1 DHCPS6_ALLOCATE_ADDRESS

日志内容	DHCPv6 server received a DHCPv6 client's request packet on interface [STRING], and allocated an IPv6 address [IPADDR] (lease [UINT32] seconds) for the DHCP client(DUID [HEX], IAID [HEX]) from [STRING] pool.
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：分配给IPv6 DHCP客户端的ipv6地址 $3：分配给IPv6 DHCP客户端的ipv6地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID $6：IPv6 DHCP服务器地址池名
日志等级	5
举例	DHCPS6/5/DHCPS6_ALLOCATE_ADDRESS: DHCPv6 server received a DHCPv6 client's request packet on interface Ethernet0/2, and allocated an IPv6 address 2000::3(lease 60 seconds) for the DHCP client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端分配一个IPv6地址租约
处理建议	无

17.2 DHCPS6_ALLOCATE_PREFIX

日志内容	DHCPv6 server received a DHCPv6 client's request packet on interface [STRING], and allocated an IPv6 prefix [IPADDR] (lease [UINT32] seconds) for the DHCP client(DUID [HEX], IAID [HEX]) from [STRING] pool.
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：分配给IPv6 DHCP客户端的IPv6前缀地址 $3：分配给IPv6 DHCP客户端的IPv6前缀地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID $6：IPv6 DHCP服务器地址池名
日志等级	5
举例	DHCPS6/5/DHCPS6_ALLOCATE_PREFIX: DHCPv6 server received a DHCPv6 client's request packet on interface Ethernet0/2, and allocated an IPv6 prefix 2000::(lease 60 seconds) for the DHCP client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端分配一个IPv6前缀地址租约
处理建议	无

17.3 DHCPS6_CONFLICT_ADDRESS

日志内容	A conflict IPv6 address [IPADDR] from [STRING] pool was detected by DHCPv6 server on interface [STRING].
参数解释	$1：冲突的IPv6地址 $2：IPv6 DHCP服务器地址池名 $3：IPv6 DHCP服务器所在接口的接口名
日志等级	5
举例	DHCPS6/5/DHCPS6_CONFLICT_ADDRESS: A conflict IPv6 address 33::1 from p1 pool was detected by DHCPv6 server on interface Ethernet0/2.
日志说明	IPv6 DHCP服务器从地址池删除一个冲突地址
处理建议	无

17.4 DHCPS6_EXTEND_ADDRESS

日志内容	DHCPv6 server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IPv6 address [IPADDR], DUID [HEX], IAID [HEX]).
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：IPv6 DHCP服务器地址池名 $3：分配给IPv6 DHCP客户端的IPv6地址 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_EXTEND_ADDRESS: DHCPv6 server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IPv6 address 2000::3, DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端地址续约
处理建议	无

17.5 DHCPS6_EXTEND_PREFIX

日志内容	DHCPv6 server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IPv6 prefix [IPADDR], DUID [HEX], IAID [HEX]).
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：IPv6 DHCP服务器地址池名 $3：分配给IPv6 DHCP客户端的IPv6前缀地址 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_EXTEND_PREFIX: DHCPv6 server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IPv6 prefix 2000::, DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
日志说明	IPv6 DHCP服务器为IPv6 DHCP客户端前缀地址续约
处理建议	无

17.6 DHCPS6_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPS6/4/DHCPS6_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCPv6 server保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

17.7 DHCPS6_RECLAIM_ADDRESS

日志内容	DHCPv6 server reclaimed a [STRING] pool's lease(IPv6 address [IPADDR], lease [UINT32] seconds), which is allocated for the DHCPv6 client (DUID [HEX], IAID [HEX]).
参数解释	$1：IPv6 DHCP服务器地址池名 $2：分配给IPv6 DHCP客户端的IPv6地址 $3：分配给IPv6 DHCP客户端的IPv6地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_RECLAIM_ADDRESS: DHCPv6 server reclaimed a p1 pool's lease(IPv6 address 2000::3, lease 60 seconds), which is allocated for the DHCPv6 client (DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
日志说明	IPv6 DHCP服务器回收一个分配给IPv6客户端的地址租约
处理建议	无

17.8 DHCPS6_RECLAIM_PREFIX

日志内容	DHCPv6 server reclaimed a [STRING] pool's lease(IPv6 prefix [IPADDR], lease [INTEGER] seconds), which is allocated for the DHCPv6 client (DUID [HEX], IAID [HEX]).
参数解释	$1：IPv6 DHCP服务器所在接口的接口名 $2：分配给IPv6 DHCP客户端的IPv6前缀地址 $3：分配给IPv6 DHCP客户端的IPv6前缀地址租约时长 $4：IPv6 DHCP客户端的DUID $5：IPv6 DHCP客户端的IAID
日志等级	5
举例	DHCPS6/5/DHCPS6_RECLAIM_PREFIX: DHCPv6 server reclaimed a p1 pool's lease(IPv6 prefix 2000::, lease 60 seconds), which is allocated for the DHCPv6 client (DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
日志说明	IPv6 DHCP服务器回收一个分配给IPv6客户端的前缀地址租约
处理建议	无

18 DHCPSP4

本节介绍 DHCPSP4 模块输出的 日志信息。

18.1 DHCPSP4_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPSP4/4/DHCPSP4_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCPv4 snooping保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

19 DHCPSP6

本节介绍 DHCPSP6 模块输出的日志信息。

19.1 DHCPSP6_FILE

日志内容	Failed to save DHCP client information due to lack of storage resources.
参数解释	无
日志等级	4
举例	DHCPSP6/4/DHCPSP6_FILE: Failed to save DHCP client information due to lack of storage resources.
日志说明	因为磁盘空间不足导致DHCPv6 snooping保存客户端信息到文件失败
处理建议	删除其他文件，使有空间保存此文件

20 DIAG

本节介绍 Diagnostic 模块输出的日志信息。

20.1 CPU_MINOR_RECOVERY

日志内容	CPU usage recovered to normal state.
参数解释	无
日志等级	5
举例	DIAG/5/CPU_MINOR_THRESHOLD: CPU usage recovered to normal state.
日志说明	当设备处于CPU低级别告警状态，并且采样值小于或等于恢复门限时，解除CPU低级别告警状态，CPU使用率恢复到正常
处理建议	根据提示信息操作设备，合理使用CPU资源

20.2 CPU_MINOR_THRESHOLD

日志内容	CPU usage is in minor alarm state. CPU usage: [UINT]% in last 1 minute. CPU usage thresholds: Minor: [UINT]% Severe: [UINT]% Recovery: [UINT]% Process info: JID PID PRI State FDs HH:MM:SS CPU Name [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR] Core states: ID Idle User Kernel Interrupt Busy CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]

参数解释	• 整个系统中 CPU 利用率的统计信息：
	  ○ $1：过去 1 分钟内统计的 CPU 利用率
	  ○ $2：低级别告警门限
	  ○ $3：高级别告警门限
	  ○ $4：告警恢复门限
	• 整个系统中 CPU 利用率最高的前 5 个进程的信息：
	  ○ $5：进程 JID
	  ○ $6：进程 PID
	  ○ $7：进程的优先级
	  ○ $8：进程的状态
	  ○ $9：进程文件句柄
	  ○ $10：进程启动时长
	  ○ $11：进程的 CPU 占用率
	  ○ $12：进程名
	• 整个系统中 CPU 利用率最高的前 5 个核的信息：
	  ○ $13：核 ID
	  ○ $14：空闲时间
	  ○ $15：用户态进程占用的时间
	  ○ $16：内核线程占用的时间
	  ○ $17：中断占用的时间
	  ○ $18：运行时间

日志等级	4
举例	DIAG/4/CPU_MINOR_THRESHOLD: CPU usage is in minor alarm state. CPU usage: 3% in last 1 minute. CPU usage thresholds: Minor: 1% Severe: 2% Recovery: 0% Process info: JID PID PRI State FDs HH:MM:SS CPU Name

日志内容	CPU usage is in minor alarm state. CPU usage: [UINT]% in last 1 minute. CPU usage thresholds: Minor: [UINT]% Severe: [UINT]% Recovery: [UINT]% Process info: JID PID PRI State FDs HH:MM:SS CPU Name [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR] Core states: ID Idle User Kernel Interrupt Busy CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]
	108398 108398120 S 36 00:00:0 12.58% snmpd 52 52 102 S 0 00:01:2 2.58% [DRV_FWD] 371 371 120 S 95 00:18:5 0.17% pppd 90 90 120 R 18 00:12:0 0.34% diagd 109 109 119 S 41 00:11:1 0.00% vbrd Core states: ID Idle User Kernel Interrupt Busy CPU0 98.61% 0.24% 0.62% 0.53% 1.39% CPU1 99.88% 0.00% 0.03% 0.09% 0.12%
日志说明	当CPU使用率的采样值从小于/等于变成大于低级别告警门限时，设备进入CPU低级别告警状态，并定期输出该日志，直到CPU低级别告警状态解除
处理建议	根据提示信息操作设备，合理使用CPU资源

20.3 CPU_SEVERE_RECOVERY

日志内容	CPU usage severe alarm removed.
参数解释	无
日志等级	5
举例	DIAG/5/CPU_RECOVERY: CPU usage severe alarm removed.
日志说明	当设备处于CPU高级别告警状态，并且采样值小于或等于低级别告警门限时，解除CPU高级别告警状态，输出该日志
处理建议	无

20.4 CPU_SEVERE_THRESHOLD

日志内容	CPU usage is in severe alarm state. CPU usage: [UINT]% in last 1 minute. CPU usage thresholds: Minor: [UINT]% Severe: [UINT]% Recovery: [UINT]% Process info: JID PID PRI State FDs HH:MM:SS CPU Name [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR] Core states: ID Idle User Kernel Interrupt Busy CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]

参数解释	• 整个系统中 CPU 利用率的统计信息：
	  ○ $1：过去 1 分钟内统计的 CPU 利用率
	  ○ $2：低级别告警门限
	  ○ $3：高级别告警门限
	  ○ $4：告警恢复门限
	• 整个系统中 CPU 利用率最高的前 5 个进程的信息：
	  ○ $5：进程 JID
	  ○ $6：进程 PID
	  ○ $7：进程的优先级
	  ○ $8：进程的状态
	  ○ $9：进程文件句柄
	  ○ $10：进程启动时长
	  ○ $11：进程的 CPU 占用率
	  ○ $12：进程名
	• 整个系统中 CPU 利用率最高的前 5 个核的信息：
	  ○ $13：核 ID
	  ○ $14：空闲时间
	  ○ $15：用户态进程占用的时间
	  ○ $16：内核线程占用的时间
	  ○ $17：中断占用的时间
	  ○ $18：运行时间

日志等级	3
举例	DIAG/3/CPU_THRESHOLD: CPU usage is in severe alarm state. CPU usage: 3% in last 1 minute. CPU usage thresholds: Minor: 1% Severe: 2% Recovery: 0% Process info: JID PID PRI State FDs HH:MM:SS CPU Name

日志内容	CPU usage is in severe alarm state. CPU usage: [UINT]% in last 1 minute. CPU usage thresholds: Minor: [UINT]% Severe: [UINT]% Recovery: [UINT]% Process info: JID PID PRI State FDs HH:MM:SS CPU Name [UINT] [UINT] [UINT] [CHAR] [UINT] [CHAR] [CHAR] [CHAR] Core states: ID Idle User Kernel Interrupt Busy CPU[UINT] [CHAR] [CHAR] [CHAR] [CHAR] [CHAR]
	108398 108398120 S 36 00:00:0 12.58% snmpd 52 52 102 S 0 00:01:2 2.58% [DRV_FWD] 371 371 120 S 95 00:18:5 0.17% pppd 90 90 120 R 18 00:12:0 0.34% diagd 109 109 119 S 41 00:11:1 0.00% vbrd Core states: ID Idle User Kernel Interrupt Busy CPU0 98.61% 0.24% 0.62% 0.53% 1.39% CPU1 99.88% 0.00% 0.03% 0.09% 0.12%
日志说明	当CPU使用率的采样值从小于/等于变成大于高级别告警门限时，设备进入CPU高级别告警状态，并定期输出该日志，直到CPU高级别告警状态解除
处理建议	请使用**display current-configuration | include "monitor cpu-usage"**命令查看CPU的告警门限，如果门限设置不合适，请使用**monitor cpu-usage**命令修改

20.5 CORE_EXCEED_THRESHOLD

日志内容	Usage of CPU [INT] core [INT] exceeded the threshold ([string]).
参数解释	$1：CPU号 $2：CPU核的编号
日志等级	3
举例	DIAG/3/CORE_EXCEED_THRESHOLD: Usage of CPU 0 core 2 exceeded the threshold (90%).
日志说明	CPU核利用率高于高级别告警门限值，进入高级别告警状态
处理建议	• 使用 **display process cpu**、**monitor thread** 命令显示所有进程的 CPU 使用率信息 • 请联系技术支持人员

20.6 CORE_MINOR_RECOVERY

日志内容	Core usage minor alarm CPU [INT] core [INT] removed.
参数解释	$1：CPU号 $2：CPU核的编号
日志等级	5
举例	DIAG/5/CORE_MINOR_RECOVERY: Core usage alarm CPU 0 core 1 removed.
日志说明	CPU核利用率低于或等于低级别告警门限值，CPU核从低级别告警状态恢复到正常状态
处理建议	无

20.7 CORE_MINOR_THRESHOLD

日志内容	Usage of CPU [INT] core [INT] exceeded the threshold ([string]).
参数解释	$1：CPU号 $2：CPU核的编号
日志等级	4
举例	DIAG/4/CORE_MINOR_THRESHOLD: Usage of CPU 0 core 2 exceeded the threshold (80%).
日志说明	CPU核利用率高于低级别告警门限值，进入低级别告警状态
处理建议	• 使用 **display process cpu**、**monitor thread** 命令显示所有进程的 CPU 使用率信息 • 请联系技术支持人员

20.8 CORE_RECOVERY

日志内容	Core usage alarm CPU [INT] core [INT] removed.
参数解释	$1：CPU号 $2：CPU核的编号
日志等级	5
举例	DIAG/5/CORE_RECOVERY: Core usage alarm CPU 0 core 1 removed.
日志说明	CPU核利用率低于或等于高级别告警门限值，高级别告警解除
处理建议	无

20.9 DIAG_STORAGE_BELOW_THRESHOLD

日志内容	The usage of [STRING] ([UINT32]%) was below or equal to the threshold of [UINT32]%.
参数解释	$1：存储介质的名称 $2：存储介质磁盘空间使用率 $3：存储介质使用率阈值
日志等级	1
举例	DIAG/1/DIAG_STORAGE_BELOW_THRESHOLD: The usage of flash (90%) was below or equal to the threshold of 95%.
日志说明	存储介质磁盘空间使用率小于或等于阈值
处理建议	无

20.10 DIAG_STORAGE_EXCEED_THRESHOLD

日志内容	The usage of [STRING] ([UINT32]%) exceeded the threshold of [UINT32]%.
参数解释	$1：存储介质的名称 $2：存储介质磁盘空间使用率 $3：存储介质使用率的阈值
日志等级	1
举例	DIAG/1/DIAG_STORAGE_EXCEED_THRESHOLD: The usage of flash (96%) exceeded the threshold of 95%.
日志说明	存储介质磁盘空间使用率大于阈值
处理建议	对长期不使用的文件，例如日志文件和历史版本的软件包，使用**delete**命令直接删除或者备份到PC后再删除

20.11 MEM_ALERT

日志内容	system memory info: total used free shared buffers cached Mem: ［ULONG］ ［ULONG］ ［ULONG］ ［ULONG］ ［ULONG］ ［ULONG］ -/+ buffers/cache: ［ULONG］ ［ULONG］ Swap: ［ULONG］ ［ULONG］ ［ULONG］ Lowmem: ［ULONG］ ［ULONG］ ［ULONG］

参数解释	• 整个系统中内存的统计信息：
	  ○ $1：系统可分配的物理内存的大小。设备总物理内存分为不可分配物理内存和可分配物理内存。其中，不可分配物理内存用于内核代码段存储、内核管理开销以及基本功能的运行等；可分配物理内存用于支撑业务模块的运行、文件存储等操作。不可分配内存的大小由设备根据系统运行需要自动计算划分，可分配物理内存的大小等于设备总物理内存减去不可分配内存的大小
	  ○ $2：整个系统已用的物理内存大小
	  ○ $3：整个系统可用的物理内存大小
	  ○ $4：多个进程共享的物理内存总额
	  ○ $5：已使用的文件缓冲区的大小
	  ○ $6：高速缓冲寄存器已使用的内存大小
	• 应用程序对内存的使用情况：
	  ○ $7：-/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached，表示应用程序已用的物理内存大小
	  ○ $8：-/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached，表示应用程序可用的物理内存大小
	• 交换分区的使用信息：
	  ○ $9：交换分区的总大小
	  ○ $10：已用的交换分区的大小
	  ○ $11：可用的交换分区的大小
	• Low memory 的使用情况：
	  ○ $12：Low memory 中内存的大小
	  ○ $13：Low memory 中已用内存的大小
	  ○ $14：Low memory 中可用内存的大小

日志等级	4
举例	DIAG/4/MEM_ALERT: system memory info: total used free shared buffers cached Mem: 1784424 920896 863528 0 0 35400 -/+ buffers/cache: 885496 898928 Swap: 0 0 0 Lowmem: 735848 637896 97952
日志说明	内存告警。当已使用的内存大于或等于一级、二级或三级内存告警门限时，系统会输出该信息，告知用户内存的具体使用情况
处理建议	1. 请使用 **display memory-threshold** 命令查看内存的一级、二级、三级告警门限。如果门限设置不合适，请使用 **memory-threshold** 命令修改

	2. 检查 ARP、路由表信息，排除设备受到非法攻击可能 3. 检查和优化组网，减少路由条目或者更换更高规格的设备

20.12 MEM_BELOW_THRESHOLD

日志内容	Memory usage has dropped below [STRING] threshold.
参数解释	$1：内存告警门限级别，包括： o minor：一级 o severe：二级 o critical：三级
日志等级	1
举例	DIAG/1/MEM_BELOW_THRESHOLD: Memory usage has dropped below critical threshold.
日志说明	内存告警解除。当系统剩余空闲内存大于内存恢复门限时，系统会输出该信息
处理建议	无

20.13 MEM_EXCEED_THRESHOLD

日志内容	Memory [STRING] threshold has been exceeded.
参数解释	$1：内存告警门限级别，包括： o minor：一级 o severe：二级 o critical：三级
日志等级	1
举例	DIAG/1/MEM_EXCEED_THRESHOLD: Memory minor threshold has been exceeded.
日志说明	内存告警。当已使用的内存大于或等于一级、二级或三级内存告警门限时，系统会输出该信息，并通知各业务模块进行自动修复：比如，不再申请新的内存或者释放部分内存
处理建议	1. 请使用 **display memory-threshold** 命令查看内存的一级、二级、三级告警门限。如果门限设置不合适，请使用 **memory-threshold** 命令修改 2. 检查 ARP、路由表信息，排除设备受到非法攻击可能 3. 检查和优化组网，减少路由条目或者更换更高规格的设备

21 DLDP

本节介绍 DLDP 模块输出的日志信息。

21.1 DLDP_AUTHENTICATION_FAILED

日志内容	The DLDP packet failed the authentication because of unmatched [STRING] field.
参数解释	$1：验证字段 ○ AUTHENTICATION PASSWORD：表示验证字不匹配 ○ AUTHENTICATION TYPE：表示验证类型不匹配 ○ INTERVAL：表示通告间隔不匹配
日志等级	5
举例	DLDP/5/DLDP_AUTHENTICATION_FAILED: The DLDP packet failed the authentication because of unmatched INTERVAL field.
日志说明	报文验证失败。可能的原因包括：验证类型不匹配、验证字不匹配、通告间隔不匹配
处理建议	检查DLDP验证类型、验证字和通告间隔是否与对端一致

21.2 DLDP_LINK_BIDIRECTIONAL

日志内容	DLDP detected a bidirectional link on interface [STRING].
参数解释	$1：接口名
日志等级	6
举例	DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a bidirectional link on interface Ethernet1/2/0/1.
日志说明	DLDP在接口上检测到双向链路
处理建议	无

21.3 DLDP_LINK_SHUTMODECHG

日志内容	DLDP automatically blocked the interface [STRING] because the port shutdown mode was changed to auto mode.
参数解释	$1：接口名
日志等级	5
举例	DLDP/5/DLDP_LINK_SHUTMODECHG: DLDP automatically blocked the interface Ethernet1/2/0/1 because the port shutdown mode was changed to auto mode.
日志说明	DLDP单通关闭模式由手动修改为自动，关闭端口
处理建议	无

21.4 DLDP_LINK_UNIDIRECTIONAL

日志内容	DLDP detected a unidirectional link on interface [STRING]. [STRING].
参数解释	$1：接口名 $2：接口关闭模式所指定的动作 o DLDP automatically blocked the interface：表示 DLDP 自动关闭了端口 o Please manually shut down the interface：表示需要用户手动关闭端口
日志等级	3
举例	DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a unidirectional link on interface Ethernet1/2/0/1. DLDP automatically blocked the interface.
日志说明	DLDP在接口上检测到单向链路
处理建议	检查线缆是否错接、脱落或者出现其他故障

21.5 DLDP_NEIGHBOR_AGED

日志内容	A neighbor on interface [STRING] was deleted because the neighbor was aged. The neighbor's system MAC is [MAC], and the port index is [UINT16].
参数解释	$1：接口名 $2：MAC地址 $3：接口索引
日志等级	5
举例	DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface Ethernet1/2/0/1 was deleted because the neighbor was aged. The neighbor's system MAC is dc2d-cb69-5f21, and the port index is 1.
日志说明	接口删除了一个已老化的邻居
处理建议	无

21.6 DLDP_NEIGHBOR_CONFIRMED

日志内容	A neighbor was confirmed on interface [STRING]. The neighbor's system MAC is [MAC], and the port index is [UINT16].
参数解释	$1：接口名 $2：MAC地址 $3：接口索引
日志等级	6
举例	DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface Ethernet1/2/0/1. The neighbor's system MAC is dc2d-cb69-5f21, and the port index is 1.
日志说明	接口检测到一个处于确定状态的邻居
处理建议	无

21.7 DLDP_NEIGHBOR_DELETED

日志内容	A neighbor on interface [STRING] was deleted because a [STRING] packet arrived. The neighbor's system MAC is [MAC], and the port index is [UINT16].
参数解释	$1：接口名 $2：报文类型 ○ DISABLE：表示收到了 Disable 报文 ○ LINKDOWN：表示收到了 LinkDown 报文 $3：MAC地址 $4：接口索引
日志等级	5
举例	DLDP/5/DLDP_NEIGHBOR_DELETED: A neighbor on interface Ethernet1/2/0/1 was deleted because a DISABLE packet arrived. The neighbor's system MAC is dc2d-cb69-5f21, and the port index is 1.
日志说明	由于收到了Disable报文或LinkDown报文，因此接口删除一个处于确定状态的邻居
处理建议	无

22 DOMAIN

本节介绍 DOMAIN 模块输出的日志信息。

22.1 DOMAIN_IP_LOWTHR_ALM

日志内容	-Domain=[STRING]-IPUsage=[STRING]-IPPoolLowerValue=[STRING]; IP resource usage reached or dropped below the lower threshold.
参数解释	$1：ISP域名称 $2：IP地址使用率 $3：IP地址使用率下限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_IP_LOWTHR_ALM: -Domain=abc-IPUsage=10%-IPPoolLowerValue=20%; IP resource usage reached or dropped below the lower threshold.
日志说明	当域下授权IP地址池/IP地址池组中的IP地址使用率达到或低于告警下限阈值，生成下限告警
处理建议	无

22.2 DOMAIN_IP_LOWTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-IPUsage=[STRING]-IPPoolLowerValue=[STRING]; Low IP resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：IP地址使用率 $3：IP地址使用率下限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_IP_LOWTHR_ALM_REMOVE: -Domain=dom1-IPUsage=50%-IPPoolLowerValue=20%; Low IP resource usage alarm condition cleared.
日志说明	当域下授权IP地址池/IP地址池组中的IP地址使用率>=（下限阈值+告警差值）时，生成使用率下限恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

22.3 DOMAIN_IP_UPTHR_ALM

日志内容	-Domain=[STRING]-IPUsage=[STRING]-IPPoolUpperValue=[STRING]; IP resource usage reached or exceeded the upper threshold.
参数解释	$1：ISP域名称 $2：IP地址使用率 $3：IP地址使用率上限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_IP_UPTHR_ALM: -Domain=dom1-IPUsage=90%-IPPoolUpperValue=80%; IP resource usage reached or exceeded the upper threshold.
日志说明	当域下授权IP地址池/IP地址池组中的IP地址使用率达到或超过告警上限阈值，生成上限告警
处理建议	及时调整用户授权IP地址池可用资源

22.4 DOMAIN_IP_UPTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-IPUsage=[STRING]-IPPoolUpperValue=[STRING]; High IP resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：IP地址使用率 $3：IP地址使用率上限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_IP_UPTHR_ALM_REMOVE: -Domain=dom1-IPUsage=50%-IPPoolUpperValue=80%; High IP resource usage alarm condition cleared.
日志说明	当域下授权IP地址池/IP地址池组中的IP地址使用率<=（上限阈值–告警差值）时，生成使用率上限恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

22.5 DOMAIN_IPV6_LOWTHR_ALM

日志内容	-Domain=[STRING]-IPv6Usage=[STRING]-IPv6PoolLowerValue=[STRING]; IPv6 address resource usage reached or dropped below the lower threshold.
参数解释	$1：ISP域名称 $2：IPv6地址使用率 $3：IPv6地址使用率下限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_IPV6_LOWTHR_ALM: -Domain=abc-IPv6Usage=10%-IPv6PoolLowerValue=20%; IPv6 address resource usage reached or dropped below the lower threshold.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的IPv6地址使用率达到或低于告警下限阈值，生成下限告警
处理建议	无

22.6 DOMAIN_IPV6_LOWTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-IPv6Usage=[STRING]-IPv6PoolLowerValue=[STRING]; Low IPv6 address resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：IPv6地址使用率 $3：IPv6地址使用率下限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_IPV6_LOWTHR_ALM_REMOVE: -Domain=dom1-IPv6Usage=50%-IPv6PoolLowerValue=20%; Low IPv6 address resource usage alarm condition cleared.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的IPv6地址使用率>=（下限阈值+告警差值）<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

22.7 DOMAIN_IPV6_UPTHR_ALM

日志内容	-Domain=[STRING]-IPv6Usage=[STRING]-IPv6PoolUpperValue=[STRING]; IPv6 address resource usage reached or exceeded the upper threshold.
参数解释	$1：ISP域名称 $2：IPv6地址使用率 $3：IPv6地址使用率上限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_IPV6_UPTHR_ALM: -Domain=abc-IPv6Usage=90%-IPv6PoolUpperValue=80%; IPv6 address resource usage reached or exceeded the upper threshold.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的IPv6地址使用率达到或超过告警上限阈值，生成上限告警
处理建议	及时调整用户授权IPv6地址池可用资源

22.8 DOMAIN_IPV6_UPTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-IPv6Usage=[STRING]-IPv6PoolUpperValue=[STRING]; High IPv6 address resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：IPv6地址使用率 $3：IPv6地址使用率上限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_IPV6_UPTHR_ALM_REMOVE: -Domain=dom1-IPv6Usage=50%-IPv6PoolUpperValue=80%; High IPv6 address resource usage alarm condition cleared.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的IPv6地址使用率<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

22.9 DOMAIN_ND_PREF_LOWTHR_ALM

日志内容	-Domain=[STRING]-NDPrefixUsage=[STRING]-IPv6PoolLowerValue=[STRING]; ND prefix resource usage reached or dropped below the lower threshold.
参数解释	$1：ISP域名称 $2：ND前缀使用率 $3：IPv6前缀使用率下限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_ND_PREF_LOWTHR_ALM: -Domain=abc-NDPrefixUsage=10%-IPv6PoolLowerValue=20%; ND prefix resource usage reached or dropped below the lower threshold.
日志说明	当域下授权ND前缀池/ND前缀地址池组中的ND前缀使用率达到或低于告警下限阈值，生成下限告警
处理建议	无

22.10 DOMAIN_ND_PREF_LOWTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-NDPrefixUsage=[STRING]-IPv6PoolLowerValue=[STRING]; Low ND prefix resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：ND前缀使用率 $3：IPv6前缀使用率下限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_ND_PREF_LOWTHR_ALM_REMOVE: -Domain=abc-NDPrefixUsage=50%-IPv6PoolLowerValue=20%; Low ND prefix resource usage alarm condition cleared.
日志说明	当域下授权ND前缀池/ND前缀地址池组中的ND前缀使用率>=（下限阈值+告警差值）<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

22.11 DOMAIN_ND_PREF_UPTHR_ALM

日志内容	-Domain=[STRING]-NDPrefixUsage=[STRING]-IPv6PoolUpperValue=[STRING]; ND prefix resource usage reached or exceeded the upper threshold.
参数解释	$1：ISP域名称 $2：ND前缀使用率 $3：IPv6前缀使用率上限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_ND_PREF_UPTHR_ALM: -Domain=abc-NDPrefixUsage=90%-IPv6PoolUpperValue=80%; ND prefix resource usage reached or exceeded the upper threshold.
日志说明	当域下授权ND前缀池/ND前缀地址池组中的ND前缀使用率达到或超过告警上限阈值，生成上限告警
处理建议	及时调整用户授权ND前缀池/ND前缀地址池可用资源

22.12 DOMAIN_ND_PREF_UPTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-NDPrefixUsage=[STRING]-IPv6PoolUpperValue=[STRING]; High ND prefix resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：ND前缀使用率 $3：IPv6前缀使用率上限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_ND_PREF_UPTHR_ALM_REMOVE: -Domain=abc-NDPrefixUsage=50%-IPv6PoolUpperValue=80%; High ND prefix resource usage alarm condition cleared.
日志说明	当域下授权ND前缀池/ND前缀地址池组中的ND前缀使用率<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

22.13 DOMAIN_PD_PREF_LOWTHR_ALM

日志内容	-Domain=[STRING]-PDPrefixUsage=[STRING]-IPv6PoolLowerValue=[STRING]; PD prefix resource usage reached or dropped below the lower threshold.
参数解释	$1：ISP域名称 $2：PD前缀地址使用率 $3：IPv6前缀使用率下限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_PD_PREF_LOWTHR_ALM: -Domain=abc-PDPrefixUsage=10%-IPv6PoolLowerValue=20%; PD prefix resource usage reached or dropped below the lower threshold.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的PD前缀使用率达到或低于下限阈值，生成下限告警
处理建议	无

22.14 DOMAIN_PD_PREF_LOWTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-PDPrefixUsage=[STRING]-IPv6PoolLowerValue=[STRING]; Low PD prefix resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：PD前缀地址使用率 $3：IPv6前缀使用率下限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_PD_PREF_LOWTHR_ALM_REMOVE: -Domain=abc-PDPrefixUsage=50%-IPv6PoolLowerValue=20%; Low PD prefix resource usage alarm condition cleared.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的PD前缀使用率>=（下限阈值+告警差值）<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

22.15 DOMAIN_PD_PREF_UPTHR_ALM

日志内容	-Domain=[STRING]-PDPrefixUsage=[STRING]-IPv6PoolUpperValue=[STRING]; PD prefix resource usage reached or exceeded the upper threshold.
参数解释	$1：ISP域名称 $2：PD前缀地址使用率 $3：IPv6前缀使用率上限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_PD_PREF_UPTHR_ALM: -Domain=abc-PDPrefixUsage=90%-IPv6PoolUpperValue=80%; PD prefix resource usage reached or exceeded the upper threshold.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的PD前缀使用率达到或超过上限阈值，生成上限告警
处理建议	及时调整用户授权IPv6地址池可用资源

22.16 DOMAIN_PD_PREF_UPTHR_ALM_REMOVE

日志内容	-Domain=[STRING]-PDPrefixUsage=[STRING]-IPv6PoolUpperValue=[STRING]; High PD prefix resource usage alarm condition cleared.
参数解释	$1：ISP域名称 $2：PD前缀地址使用率 $3：IPv6前缀使用率上限阈值
日志等级	5
举例	DOMAIN/5/DOMAIN_PD_PREF_UPTHR_ALM_REMOVE: -Domain=abc-PDPrefixUsage=50%-IPv6PoolUpperValue=80%; High PD prefix resource usage alarm condition cleared.
日志说明	当域下授权IPv6地址池/IPv6地址池组中的PD前缀使用率<=（上限阈值-告警差值）时，生成使用率恢复告警 其中，告警差值=（上限阈值–下限阈值）*10%
处理建议	无

23 EDEV

本节介绍扩展设备管理模块输出的日志信息。

23.1 EDEV_FAILOVER_GROUP_STATE_CHANGE

日志内容	Status of stateful failover group [STRING] with ID [UINT32] changed to [STRING].
参数解释	$1：备份组的名字 $2：备份组的ID $2：备份组的状态： ○ primary 表示备份组中 primary 节点处理业务 ○ secondary 表示备份组中 secondary 节点处理业务
日志等级	5
举例	EDEV/5/EDEV_FAILOVER_GROUP_STATE_CHANGE: -MDC=1; Status of stateful failover group 123 with ID 0 changed to primary.
日志说明	备份组的状态发生了变化
处理建议	无

24 ETH

本节介绍以太网模块输出的日志信息。

24.1 ETH_VLAN_TERMINATION_FAILED

日志内容	The vlan-type dot1q configuration on [STRING] failed.
参数解释	$1：接口名称
日志等级	4
举例	ETH/4/ETH_VLAN_TERMINATION_FAILED: -MDC=1; The vlan-type dot1q configuration on GigabitEthernet1/2/0/1.1 failed.
日志说明	接口下发**vlan-type dot1q**系列命令的配置时失败，可能由硬件资源不足引起
处理建议	联系UNIS技术支持

24.2 ETH_VLAN_TERMINATION_NOT_SUPPORT

日志内容	The vlan-type dot1q configuration on [STRING] is not supported.
参数解释	$1：接口名称
日志等级	4
举例	ETH/4/ETH_VLAN_TERMINATION_NOT_SUPPORT: -MDC=1; The vlan-type dot1q configuration on GigabitEthernet1/2/0/1.1 is not supported.
日志说明	接口不支持**vlan-type dot1q**系列命令
处理建议	检查接口所在单板是否支持VLAN终结功能

24.3 ETH_VMAC_INEFFECTIVE

日志内容	Interface [STRING] failed to add a virtual MAC: [STRING].
参数解释	$1：接口名称 $2：接口添加虚拟MAC地址失败的原因
日志等级	3
举例	ETH/3/ETH_VMAC_INEFFECTIVE: Interface GigabitEthernet1/2/0/1 failed to add a virtual MAC: Insufficient hardware resources.
日志说明	添加虚拟MAC地址失败
处理建议	确定操作失败的根因并解决，例如接口上的VRRP的虚拟MAC地址数量达到上限，导致没有足够的硬件资源来添加新的虚拟MAC地址，此时可以删除空闲的VRRP备份组，释放部分硬件资源

25 ETHOAM

本节介绍 ETHOAM 模块输出的日志信息。

25.1 ETHOAM_CONNECTION_FAIL_DOWN

日志内容	The link is down on interface [string] because a remote failure occurred on peer interface.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ETHOAM_CONNECTION_FAIL_DOWN: The link is down on interface Ethernet1/2/0/1 because a remote failure occurred on peer interface.
日志说明	对端接口发生故障，链路down
处理建议	检查链路状态或对端的OAM状态

25.2 ETHOAM_CONNECTION_FAIL_TIMEOUT

日志内容	Interface [string] removed the OAM connection because it received no Information OAMPDU before the timer times out.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ETHOAM_CONNECTION_FAIL_TIMEOUT: Interface Ethernet1/2/0/1 removed the OAM connection because it received no Information OAMPDU before the timer times out.
日志说明	接口在超时时间内没有收到信息OAMPDU，所以删除OAM连接
处理建议	检查链路状态或对端的OAM状态

25.3 ETHOAM_CONNECTION_FAIL_UNSATISF

日志内容	Interface [string] failed to establish an OAM connection because the peer doesn’t match the capacity of the local interface.
参数解释	$1：接口名称
日志等级	3
举例	ETHOAM/3/ETHOAM_CONNECTION_FAIL_UNSATISF: Interface Ethernet1/2/0/1 failed to establish an OAM connection because the peer doesn’t match the capacity of the local interface.
日志说明	对端与本端接口的OAM协议状态不匹配，建立OAM连接失败
处理建议	分析两端发出的OAM报文中的协议状态字段

25.4 ETHOAM_CONNECTION_SUCCEED

日志内容	An OAM connection is established on interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_CONNECTION_SUCCEED: An OAM connection is established on interface Ethernet1/2/0/1.
日志说明	OAM连接建立成功
处理建议	无

25.5 ETHOAM_DISABLE

日志内容	Ethernet OAM is now disabled on interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_DISABLE: Ethernet OAM is now disabled on interface Ethernet1/2/0/1.
日志说明	以太网OAM功能已关闭
处理建议	无

25.6 ETHOAM_DISCOVERY_EXIT

日志内容	OAM interface [string] quit the OAM connection..
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_DISCOVERY_EXIT: OAM interface Ethernet1/2/0/1 quit the OAM connection.
日志说明	本端接口退出OAM连接
处理建议	无

25.7 ETHOAM_ENABLE

日志内容	Ethernet OAM is now enabled on interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_ENABLE: Ethernet OAM is now enabled on interface Ethernet1/2/0/1.
日志说明	以太网OAM功能已使能
处理建议	无

25.8 ETHOAM_ENTER_LOOPBACK_CTRLLED

日志内容	The local OAM entity enters remote loopback as controlled DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ ETHOAM_ENTER_LOOPBACK_CTRLLED: The local OAM entity enters remote loopback as controlled DTE on OAM interface Ethernet1/2/0/1.
日志说明	对端使能OAM远端环回功能后，本端OAM实体作为被控制DTE进入远端环回
处理建议	无

25.9 ETHOAM_ENTER_LOOPBACK_CTRLLING

日志内容	The local OAM entity enters remote loopback as controlling DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ ETHOAM_ENTER_LOOPBACK_CTRLLING: The local OAM entity enters remote loopback as controlling DTE on OAM interface Ethernet1/2/0/1.
日志说明	接口使能OAM远端环回功能后，本端OAM实体作为控制DTE进入远端环回
处理建议	无

25.10 ETHOAM_LOCAL_DYING_GASP

日志内容	A local Dying Gasp event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOCAL_DYING_GASP: A local Dying Gasp event occurred on interface Ethernet1/2/0/1.
日志说明	重启设备或关闭接口导致本端产生致命故障（Dying Gasp）事件
处理建议	链路恢复之前不能使用

25.11 ETHOAM_LOCAL_ERROR_FRAME

日志内容	An errored frame event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME: An errored frame event occurred on local interface Ethernet1/2/0/1.
日志说明	本地接口产生错误帧事件
处理建议	本端收到错误报文，检查一下本端和对端之间的链路是否正常

25.12 ETHOAM_LOCAL_ERROR_FRAME_PERIOD

日志内容	An errored frame period event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_PERIOD: An errored frame period event occurred on local interface Ethernet1/2/0/1.
日志说明	本地接口产生错误帧周期事件
处理建议	本端收到错误报文，检查一下本端和对端之间的链路是否正常

25.13 ETHOAM_LOCAL_ERROR_FRAME_SECOND

日志内容	An errored frame seconds event occurred on local interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_SECOND: An errored frame seconds event occurred on local port Ethernet1/2/0/1.
日志说明	本地接口产生错误帧秒事件
处理建议	本端收到错误报文，检查一下本端和对端之间的链路是否正常

25.14 ETHOAM_LOCAL_LINK_FAULT

日志内容	A local Link Fault event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOCAL_LINK_FAULT: A local Link Fault event occurred on interface Ethernet1/2/0/1.
日志说明	本地链路down，产生链路故障事件
处理建议	重新连接本地接口的光纤接收端

25.15 ETHOAM_LOOPBACK_EXIT

日志内容	OAM interface [string] quit remote loopback.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOOPBACK_EXIT: OAM interface Ethernet1/2/0/1 quit remote loopback.
日志说明	远端环回连接建立未完成时，接口关闭远端环回或OAM连接断开后，OAM接口退出远端环回
处理建议	无

25.16 ETHOAM_LOOPBACK_EXIT_ERROR_STATU

日志内容	OAM interface [string] quit remote loopback due to incorrect multiplexer or parser status.
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_LOOPBACK_EXIT_ERROR_STATU: OAM interface Ethernet1/2/0/1 quit remote loopback due to incorrect multiplexer or parser status.
日志说明	复用器或解析器状态错误，OAM接口Ethernet1/2/0/1退出远端环回
处理建议	在OAM实体上关闭并重新使能以太网OAM

25.17 ETHOAM_LOOPBACK_NO_RESOURCE

日志内容	OAM interface [string] can’t enter remote loopback due to insufficient resources.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOOPBACK_NO_RESOURCE: OAM interface Ethernet1/2/0/1 can’t enter remote loopback due to insufficient resources.
日志说明	当在本端或对端OAM实体上运行**oam remote-loopback start**命令时，OAM接口由于资源不足而无法进入远端环回
处理建议	端口上使能远端环回，需要设置端口的硬件转发资源，如果配置的端口过多，可能会导致资源不足，需要关闭一下其他端口的远端环回功能，再在本端口上重新运行**oam remote-loopback start**命令

25.18 ETHOAM_LOOPBACK_NOT_SUPPORT

日志内容	OAM interface [string] can’t enter remote loopback because the operation is not supported.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_LOOPBACK_NOT_SUPPORT: OAM interface Ethernet1/2/0/1 can’t enter remote loopback because the operation is not supported.
日志说明	由于设备不支持，OAM接口无法进入远端环回
处理建议	无

25.19 ETHOAM_NO_ENOUGH_RESOURCE

日志内容	The configuration failed on OAM interface [string] because of insufficient resources.
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ ETHOAM_NO_ENOUGH_RESOURCE: The configuration failed on OAM interface Ethernet1/2/0/1 because of insufficient resources.
日志说明	系统内存资源不足导致OAM接口上的配置失败
处理建议	减少一下系统的无用配置，释放部分内存资源后，再重新配置

25.20 ETHOAM_NOT_CONNECTION_TIMEOUT

日志内容	Interface [string] quit Ethernet OAM because it received no Information OAMPDU before the timer times out.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_NOT_CONNECTION_TIMEOUT: Interface Ethernet1/2/0/1 quit Ethernet OAM because it received no Information OAMPDU before the timer times out.
日志说明	本地端口在超时时间内没有收到信息OAMPDU，所以退出以太网OAM
处理建议	对端发送OAM报文不及时，检查本地和对端的链路状态是否正常，以及对端的OAM功能是否使能了

25.21 ETHOAM_QUIT_LOOPBACK_CTRLLED

日志内容	The local OAM entity quit remote loopback as controlled DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ ETHOAM_QUIT_LOOPBACK_CTRLLED: The local OAM entity quit remote loopback as controlled DTE on OAM interface Ethernet1/2/0/1.
日志说明	当本端作为远端环回的被控端时，由于对端关闭了远端环回功能，本端也会退出远端环回
处理建议	无

25.22 ETHOAM_QUIT_LOOPBACK_CTRLLING

日志内容	The local OAM entity quit remote loopback as controlling DTE on OAM interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_QUIT_LOOPBACK_CONTROLLING: The local OAM entity quit remote loopback as controlling DTE on OAM interface Ethernet1/2/0/1.
日志说明	在接口上使能远端环回，当再将端口上的远端环回功能关闭后，本端会退出远端环回
处理建议	无

25.23 ETHOAM_REMOTE_CRITICAL

日志内容	A remote Critical event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_REMOTE_CRITICAL: A remote Critical event occurred on interface Ethernet1/2/0/1.
日志说明	发生远端紧急事件
处理建议	链路恢复之前不能使用

25.24 ETHOAM_REMOTE_DYING_GASP

日志内容	A remote Dying Gasp event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_REMOTE_DYING_GASP: A remote Dying Gasp event occurred on interface Ethernet1/2/0/1.
日志说明	重启远端设备或关闭接口导致远端产生致命故障（Dying Gasp）事件
处理建议	链路恢复之前不能使用

25.25 ETHOAM_REMOTE_ERROR_FRAME

日志内容	An errored frame event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME: An errored frame event occurred on the peer interface Ethernet1/2/0/1.
日志说明	对端产生错误帧事件
处理建议	对端收到错误报文，检查一下本端和对端之间的链路是否正常

25.26 ETHOAM_REMOTE_ERROR_FRAME_PERIOD

日志内容	An errored frame period event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_PERIOD: An errored frame period event occurred on the peer interface Ethernet1/2/0/1.
日志说明	对端产生错误帧周期事件
处理建议	对端收到错误报文，检查一下本端和对端之间的链路是否正常

25.27 ETHOAM_REMOTE_ERROR_FRAME_SECOND

日志内容	An errored frame seconds event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_SECOND: An errored frame seconds event occurred on the peer interface Ethernet1/2/0/1.
日志说明	对端产生错误帧秒事件
处理建议	对端收到错误报文，检查一下本端和对端之间的链路是否正常

25.28 ETHOAM_REMOTE_ERROR_SYMBOL

日志内容	An errored symbol event occurred on the peer interface [string].
参数解释	$1：接口名称
日志等级	6
举例	ETHOAM/6/ETHOAM_REMOTE_ERROR_SYMBOL: An errored symbol event occurred on the peer interface Ethernet1/2/0/1.
日志说明	对端产生错误信号事件
处理建议	对端收到错误信号，检查一下本端和对端之间的链路是否正常

25.29 ETHOAM_REMOTE_EXIT

日志内容	OAM interface [string] quit OAM connection because Ethernet OAM is disabled on the peer interface.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_REMOTE_EXIT: OAM interface Ethernet1/2/0/1 quit OAM connection because Ethernet OAM is disabled on the peer interface.
日志说明	对端接口关闭以太网OAM功能导致本端接口退出OAM连接
处理建议	无

25.30 ETHOAM_REMOTE_FAILURE_RECOVER

日志内容	Peer interface [string] recovered.
参数解释	$1：接口名称
日志等级	5
举例	ETHOAM/5/ ETHOAM_REMOTE_FAILURE_RECOVER: Peer interface Ethernet1/2/0/1 recovered.
日志说明	对端接口链路故障清除，OAM连接恢复
处理建议	无

25.31 ETHOAM_REMOTE_LINK_FAULT

日志内容	A remote Link Fault event occurred on interface [string].
参数解释	$1：接口名称
日志等级	4
举例	ETHOAM/4/ETHOAM_REMOTE_LINK_FAULT: A remote Link Fault event occurred on interface Ethernet1/2/0/1.
日志说明	远端链路down，产生远端链路故障事件
处理建议	重新连接远端接口的光纤接收端

26 FIB

本节包含 FIB 日志消息。

26.1 FIB_FILE

日志内容	Failed to save the IP forwarding table due to lack of storage resources.
参数解释	无
日志等级	4
举例	FIB/4/FIB_FILE: -MDC=1; Failed to save the IP forwarding table due to lack of storage resources.
日志说明	存储介质剩余空间不足，保存IP FIB信息失败
处理建议	删除其它无用文件，释放存储介质的存储空间

27 FILTER

本节介绍 FILTER 模块输出的日志信息。

27.1 FILTER_EXECUTION_ICMP

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];IcmpType(1062)=[STRING]([UINT16]);IcmpCode(1063)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IP地址 $7：目的IP地址 $8：ICMP类型 $9：ICMP代码 $10：命中次数 $11：事件信息
日志等级	6
举例	FILTER/6/FILTER_EXECUTION_ICMP: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1067)=inbound;AclType(1064)=ACL;Acl(1065)=3000;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;DstIPAddr(1007)=200.1.1.1;IcmpType(1059)=Echo(8);IcmpCode(1060)=0;MatchAclCount(1066)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送ICMP报文过滤日志，之后定时发送该日志
处理建议	无

27.2 FILTER_EXECUTION_ICMPV6

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];Icmpv6Type(1064)=[STRING]([UINT16]);Icmpv6Code(1065)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IPv6地址 $7：目的IPv6地址 $8：ICMPV6类型 $9：ICMPV6代码 $10：命中次数 $11：事件信息
日志等级	6
举例	FILTER/6/FILTER_EXECUTION_ICMPV6: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1067)=inbound;AclType(1064)=ACL;Acl(1065)=3000;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=3001::1;Icmpv6Type(1064)=Echo(128);Icmpv6Code(1065)=0;MatchAclCount(1066)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送ICMPV6报文过滤日志，之后定时发送该日志
处理建议	无

27.3 FILTER_IPV4_EXECUTION

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IP地址 $7：源端口号 $8：目的IP地址 $9：目的端口号 $10：命中次数 $11：事件信息
日志等级	6
举例	FILTER/6/FILTER_IPV4_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;AclType(1067)=ACL;Acl(1068)=3000;Protocol(1001)=TCP;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchAclCount(1069)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送报文过滤日志，之后定时发送该日志
处理建议	无

27.4 FILTER_IPV6_EXECUTION

日志内容	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];AclType(1067)=[STRING];Acl(1068)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];MatchAclCount(1069)=[UINT32];Event(1048)=[STRING];
参数解释	$1：接口名称 $2：方向 $3：ACL类型 $4：ACL编号或者名称 $5：四层协议名称 $6：源IPv6地址 $7：源端口号 $8：目的IPv6地址 $9：目的端口号 $10：命中次数 $11：事件信息
日志等级	6
举例	FILTER/6/FILTER_IPV6_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;AclType(1067)=ACL;Acl(1068)=3000;Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3001::1;DstPort(1008)=1026;MatchAclCount(1069)=1000;Event(1048)=Permit;
日志说明	首次命中包过滤时发送报文过滤日志，之后定时发送该日志
处理建议	无

28 FTP

本节介绍 FTP（File Transfer Protocol）模块输出的日志信息。

28.1 FTP_ACL_DENY

日志内容	The FTP Connection [IPADDR]([STRING]) request was denied according to ACL rules.
参数解释	$1：FTP客户端IP地址 $2：FTP客户端IP地址所在VPN
日志等级	5
举例	FTP/5/FTP_ACL_DENY: The FTP Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
日志说明	FTP ACL规则限制登录IP地址。该日志在FTP服务端检测到非法客户端尝试登录时输出
处理建议	无

28.2 FTP_REACH_SESSION_LIMIT

日志内容	FTP client [STRING] failed to log in. The current number of FTP sessions is [NUMBER]. The maximum number allowed is ([NUMBER]).
参数解释	$1：FTP客户端IP地址 $2：当前的FTP会话数 $3：设备允许建立的FTP会话数
日志等级	6
举例	FTP/6/FTP_REACH_SESSION_LIMIT: FTP client 1.1.1.1 failed to log in. The current number of FTP sessions is 10. The maximum number allowed is (10).
日志说明	FTP登录用户达到上限。该日志在FTP服务端检测到登录客户端数达到上限时输出
处理建议	• 请使用 **display current-configuration | include sesion-limit** 命令查看设备当前允许的 FTP 最大登录用户数（如果执行该 **display** 命令后没有显示，则表示使用的是缺省配置） • 根据需要使用 **aaa session-limit** 命令配置允许的 FTP 最大登录用户数

29 gRPC

本节介绍 gRPC 模块输出的日志信息。

29.1 GRPC_ENABLE_WITHOUT_TLS

日志内容	PKI domain [STRING] isn't associated with a valid local certificate. The gRPC process will start without the PKI domain.
参数解释	$1：PKI域名
日志等级	4
举例	GRPC/4/GRPC_ENABLE_WITHOUT_TLS: PKI domain xxx isn't associated with a valid local certificate. The gRPC process will start without the PKI domain.
日志说明	由于PKI域中没有包含有效的本地证书，gRPC功能启动后将不会引用该PKI域进行加密通信，设备和采集器仍将采用非加密方式建立gRPC连接
处理建议	无

29.2 GRPC_LOGIN

日志内容	[STRING] logged in from [STRING], session id [INT32].
参数解释	$1：用户名 $2：客户端地址 $3：会话ID
日志等级	6
举例	GRPC/6/GRPC_LOGIN: user logged in from 127.0.0.1, session id 1.
日志说明	用户登录成功
处理建议	无

29.3 GRPC_LOGIN_FAILED

日志内容	[STRING] from [STRING] login failed. 或 [STRING] from [STRING] login failed. [STRING]
参数解释	$1：用户名 $2：客户端地址 $3：失败原因，取值为Number of the gRPC sessions reached the limit.
日志等级	4
举例	GRPC/4/GRPC_LOGIN_FAILED: user from 127.0.0.1 login failed. GRPC/4/GRPC_LOGIN_FAILED: user from 127.0.0.1 login failed. Number of the gRPC sessions reached the limit.
日志说明	用户登录失败
处理建议	**1.** 如果未显示失败原因，请检查是否已配置用户，以及用户名和密码是否正确 **2.** 如果显示 gRPC 会话到达数量上限，请减少 gRPC 客户端连接数

29.4 GRPC_LOGOUT

日志内容	[STRING] logged out, session id [INT32].
参数解释	$1：用户名 $2：会话ID
日志等级	6
举例	GRPC/6/GRPC_LOGOUT: user logged out, session id 1.
日志说明	用户正常登出
处理建议	无

29.5 GRPC_SERVER_FAILED

日志内容	Failed to enable gRPC server.
参数解释	无
日志等级	4
举例	GRPC/4/GRPC_SERVER_FAILED: Failed to enable gRPC server.
日志说明	因端口冲突，无法和gRPC服务器建立连接
处理建议	检查是否端口号被占用

29.6 GRPC_SUBSCRIBE_EVENT_FAILED

日志内容	Failed to subscribe event [STRING].
参数解释	$1：事件名
日志等级	4
举例	GRPC/4/GRPC_SUBSCRIBE_EVENT_FAILED: Failed to subscribe event syslog.
日志说明	订阅事件失败
处理建议	无

29.7 GRPC_RECEIVE_SUBSCRIPTION

日志内容	Received a subscription of module [STRING].
参数解释	$1：模块名
日志等级	6
举例	GRPC/6/GRPC_RECEIVE_SUBSCRIPTION: Received a subscription of module syslog.
日志说明	收到某个模块的一个订阅事件
处理建议	无

30 HA

本节介绍 HA 模块输出的日志信息。

30.1 HA_BATCHBACKUP_FINISHED

日志内容	Batch backup of standby board in [STRING] has finished.
参数解释	$1：当slot仅支持单CPU时，表示slot所在位置；当slot支持多CPU时，表示CPU所在位置
日志等级	5
举例	HA/5/HA_BATCHBACKUP_FINISHED: Batch backup of standby board in slot 1 CPU 0 has finished.
日志说明	指定slot/CPU的批量备份完成
处理建议	无

30.2 HA_BATCHBACKUP_STARTED

日志内容	Batch backup of standby board in [STRING] started.
参数解释	$1：当slot仅支持单CPU时，表示slot所在位置；当slot支持多CPU时，表示CPU所在位置
日志等级	5
举例	HA/5/HA_BATCHBACKUP_STARTED: Batch backup of standby board in slot 1 CPU 0 started.
日志说明	指定slot/CPU的批量备份开始
处理建议	无

30.3 HA_STANDBY_NOT_READY

日志内容	Standby board in [STRING] is not ready, reboot ...
参数解释	$1：当slot仅支持单CPU时，表示slot所在位置；当slot支持多CPU时，表示CPU所在位置
日志等级	4
举例	HA/4/HA_STANDBY_NOT_READY: Standby board in slot 1 CPU 0 is not ready, reboot ...
日志说明	主备倒换时，如果备用slot/CPU未准备好，则不会进行主备倒换，而是重启备用slot/CPU和主用slot/CPU，并在备用slot/CPU上打印该信息
处理建议	建议备用slot/CPU批量备份完成前不要进行主备倒换

30.4 HA_STANDBY_TO_MASTER

日志内容	Standby board in [STRING] changed to the master.
参数解释	$1：当slot仅支持单CPU时，表示slot所在位置；当slot支持多CPU时，表示CPU所在位置
日志等级	5
举例	HA/5/HA_STANDBY_TO_MASTER: Standby board in slot 1 CPU 0 changed to the master.
日志说明	发生主备倒换，备用slot/CPU成为主用slot/CPU
处理建议	无

31 HTTPD

本节介绍 HTTPD（HTTP daemon）模块输出的日志信息。

31.1 HTTPD_CONNECT

日志内容	[STRING] client [STRING] connected to the server successfully.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_CONNECT: HTTP client 192.168.30.117 connected to the server successfully.
日志说明	HTTP/HTTPS服务器接受了客户端的请求，HTTP/HTTPS连接成功建立
处理建议	无

31.2 HTTPD_CONNECT_TIMEOUT

日志内容	[STRING] client [STRING] connection idle timeout.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_CONNECT_TIMEOUT: HTTP client 192.168.30.117 connection to server idle timeout.
日志说明	HTTP/HTTPS连接因空闲时间太长而断开
处理建议	无

31.3 HTTPD_DISCONNECT

日志内容	[STRING] client [STRING] disconnected from the server.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_DISCONNECT: HTTP client 192.168.30.117 disconnected from the server.
日志说明	HTTP/HTTPS客户端断开了到服务器的连接
处理建议	无

31.4 HTTPD_FAIL_FOR_ACL

日志内容	[STRING] client [STRING] failed the ACL check and could not connect to the server.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_FAIL_FOR_ACL: HTTP client 192.168.30.117 failed the ACL check and cannot connect to the server.
日志说明	HTTP/HTTPS客户端没有通过ACL检查，无法建立连接
处理建议	无

31.5 HTTPD_FAIL_FOR_ACP

日志内容	[STRING] client [STRING] was denied by the certificate access control policy and could not connect to the server.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_FAIL_FOR_ACP: HTTP client 192.168.30.117 was denied by the certificate attribute access control policy and could not connect to the server.
日志说明	HTTP/HTTPS客户端没有通过证书接入控制策略检查，无法建立连接
处理建议	无

31.6 HTTPD_REACH_CONNECT_LIMIT

日志内容	[STRING] client [STRING] failed to connect to the server, because the number of connections reached the upper limit.
参数解释	$1：连接类型，HTTP或HTTPS $2：客户端IP地址
日志等级	6
举例	HTTPD/6/HTTPD_REACH_CONNECT_LIMIT: HTTP client 192.168.30.117 failed to connect to the server, because the number of connections reached the upper limit.
日志说明	已达到最大连接数，无法建立新的连接
处理建议	请根据需要使用命令**aaa session-limit**配置允许的Web最大登录用户数

32 IFMON

本节介绍接口告警模块输出的日志信息。

32.1 BGTRAFFIC_SEND_BEGIN

日志内容	Interface [STRING] began sending background traffic.
参数解释	$1：接口名称
日志等级	6
举例	IFMON/6/BGTRAFFIC_SEND_BEGIN: Interface GigabitEthernet1/2/0/1 began sending background traffic.
日志说明	接口出方向业务流量不足100Mbps时，接口开始发送背景流量
处理建议	无

32.2 BGTRAFFIC_SEND_END

日志内容	Interface [STRING] stopped sending background traffic.
参数解释	$1：接口名称
日志等级	6
举例	IFMON/6/BGTRAFFIC_SEND_END: Interface GigabitEthernet1/2/0/1 stopped sending background traffic.
日志说明	接口出方向业务流量大于300Mbps时，接口停止发送背景流量
处理建议	无

33 IFNET

本节介绍接口管理模块输出的日志信息。

33.1 IF_JUMBOFRAME_WARN

日志内容	The specified size of jumbo frames on the aggregate interface [STRING] is not supported on the member port [STRING].
参数解释	$1：聚合接口名称 $2：成员端口名称
日志等级	3
举例	IFNET/3/IF_JUMBOFRAME_WARN: -MDC=1-Slot=3; The specified size of jumbo frames on the aggregate interface Bridge-Aggregation1 is not supported on the member port GigabitEthernet1/2/0/1.
日志说明	聚合接口修改**jumboframe enable** [*size*]配置，部分成员端口不支持
处理建议	确认成员端口支持配置的*size*范围，将聚合接口的*size*配置在该范围内

33.2 INTERFACE_NOTSUPPRESSED

日志内容	Interface [STRING] is not suppressed.
参数解释	$1：接口名称
日志等级	6
举例	IFNET/6/INTERFACE_NOTSUPPRESSED: Interface GigabitEthernet1/2/0/1 is not suppressed.
日志说明	接口由抑制状态变为非抑制状态，此时上层业务可以感知接口UP/DOWN状态变化
处理建议	无

33.3 INTERFACE_SUPPRESSED

日志内容	Interface [STRING] was suppressed.
参数解释	$1：接口名称
日志等级	5
举例	IFNET/5/INTERFACE_SUPPRESSED: Interface GigabitEthernet1/2/0/1 was suppressed.
日志说明	当接口状态频繁变化时，接口被抑制。抑制期间，上层业务不能感知端口UP/DOWN状态变化
处理建议	1. 检查接口（本端或对端）连线是否被频繁插拔 2. 通过配置以太网接口物理连接状态抑制功能调整抑制参数

33.4 LINK_UPDOWN

日志内容	Line protocol state on the interface [STRING] changed to [STRING].
参数解释	$1：接口名称 $2：协议状态，up、down
日志等级	5
举例	IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/2/0/1 changed to down.
日志说明	接口的链路层协议状态发生变化
处理建议	链路层状态为down时，请使用**display interface**命令查看链路层状态，进一步定位链路层状态为down的原因

33.5 PFC_WARNING

日志内容	On interface [STRING], the rate of [STRING] PFC packets of 802.1p priority [INTEGER] exceeded the PFC early-warning threshold [INTEGER] pps. The current rate is [INTEGER].
参数解释	$1：接口名称 $2：告警方向，input、output $3：指定的802.1p优先级 $4：指定接口每秒接收的PFC帧数量，单位为pps $5：当前接口接收PFC报文的速率，单位为pps
日志等级	4
举例	IFNET/4/PFC_WARNING: On interface GigabitEthernet1/2/0/1, the rate of input PFC packets of 802.1p priority 1 exceeded the PFC early-warning threshold 50 pps. The current rate is 60.
日志说明	接口接收或者发送PFC报文的速率达到预警门限
处理建议	无

33.6 PHY_UPDOWN

日志内容	Physical state on the interface [STRING] changed to [STRING].
参数解释	$1：接口名称 $2：链路状态，up、down
日志等级	3
举例	IFNET/3/PHY_UPDOWN: Physical state on the GigabitEthernet1/2/0/1 changed to down.
日志说明	接口的链路状态发生变化
处理建议	物理层状态为down时，请检查是否没有物理连线或者链路故障

33.7 PROTOCOL_UPDOWN

日志内容	Protocol [STRING] state on the interface [STRING] changed to [STRING].
参数解释	$1：协议名称 $2：接口名称 $3：协议状态，up、down
日志等级	5
举例	IFNET/5/PROTOCOL_UPDOWN: Protocol IPX state on the interface GigabitEthernet1/2/0/1 changed to up.
日志说明	接口上一个协议的状态发生变化
处理建议	网络层状态为down时，请检查网络层协议配置

33.8 STORM_CONSTRAIN_BELOW

日志内容	[STRING] is in controlled status, [STRING] flux falls below its lower threshold [STRING].
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制下限 • *lowerlimit*% • *lowerlimit* pps • *lowerlimit* kbps
日志等级	1
举例	IFNET/1/STORM_CONSTRAIN_BELOW: GigabitEthernet1/2/0/1 is in controlled status, BC flux falls below its lower threshold 90%.
日志说明	端口处于受控状态，该端口下任意类型的流量从超上限回落到小于下限阈值
处理建议	无

33.9 STORM_CONSTRAIN_CONTROLLED

日志内容	[STRING] turned into controlled status, port status is controlled, packet type is [STRING], upper threshold is [STRING].
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制上限 • *upperlimit*% • *upperlimit* pps • *upperlimit* kbps
日志等级	1
举例	IFNET/1/STORM_CONSTRAIN_CONTROLLED: GigabitEthernet1/2/0/1 turned into controlled status, port status is controlled, packet type is BC, upper threshold is 90%.
日志说明	端口处于受控状态，该端口下任意类型的流量超过配置的上限阈值
处理建议	无

33.10 STORM_CONSTRAIN_EXCEED

日志内容	[STRING] is in controlled status, [STRING] flux exceeds its upper threshold [STRING].
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制上限 • *upperlimit*% • *upperlimit* pps • *upperlimit* kbps
日志等级	1
举例	IFNET/1/STORM_CONSTRAIN_EXCEED: GigabitEthernet1/2/0/1 is in controlled status, BC flux exceeds its upper threshold 90%.
日志说明	端口处于受控状态，该端口下任意类型的流量超过配置的上限阈值
处理建议	无

33.11 STORM_CONSTRAIN_NORMAL

日志内容	[STRING] returned to normal status, port status is [STRING], packet type is [STRING], lower threshold is [STRING].
参数解释	$1：接口名称 $2：报文类型，BC、MC、UC $3：抑制下限 • *lowerlimit*% • *lowerlimit* pps • *lowerlimit* kbps
日志等级	1
举例	IFNET/1/STORM_CONSTRAIN_NORMAL: GigabitEthernet1/2/0/1 returned to normal status, port status is normal, packet type is BC, lower threshold is 10%.
日志说明	端口处于正常状态，该端口下任意类型的流量从超上限回落到小于下限阈值
处理建议	无

33.12 VLAN_MODE_CHANGE

日志内容	Dynamic VLAN [INT32] has changed to a static VLAN.
参数解释	$1：VLANID
日志等级	5
举例	IFNET/5/VLAN_MODE_CHANGE: Dynamic VLAN 20 has changed to a static VLAN.
日志说明	创建VLAN接口导致动态VLAN转换成静态VLAN
处理建议	无

34 IKE

本节介绍 IKE 模块输出的日志信息。

34.1 IKE_P1_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 1 SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：失败原因，显示为no matching proposal、invalid ID information、unavailable certificate、unsupported DOI、unsupported situation、invalid proposal syntax、invalid SPI、invalid protocol ID、invalid certificate、authentication failure、invalid message header、invalid transform ID、malformed payload、retransmission timeout、或incorrect configuration $2：源地址 $3：目的地址
日志等级	6
举例	IKE/6/IKE_P1_SA_ESTABLISH_FAIL: Failed to establish phase 1 SA for the reason of no matching proposal. The SA's source address is 1.1.1.1 and its destination address is 2.2.2.2.
日志说明	IKE建立第一阶段SA失败以及失败原因
处理建议	检查本端和对端设备的IKE配置

34.2 IKE_P2_SA_ESTABLISH_FAIL

日志内容	Failed to establish phase 2 SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：失败原因，显示为invalid key information、invalid ID information、unavailable proposal、unsupported DOI、unsupported situation、invalid proposal syntax、invalid SPI、invalid protocol ID、invalid hash information、invalid message header、malformed payload、retransmission timeout、或incorrect configuration $2：源地址 $3：目的地址
日志等级	6
举例	IKE/6/IKE_P2_SA_ESTABLISH_FAIL: Failed to establish phase 2 SA for the reason of invalid key information. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	IKE建立第二阶段SA失败以及失败原因
处理建议	检查本端和对端设备的IKE和IPsec配置

34.3 IKE_P2_SA_TERMINATE

日志内容	The IKE phase 2 SA was deleted for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：删除SA的原因，显示为SA expiration $2：源地址 $3：目的地址
日志等级	6
举例	IKE/6/IKE_P2_SA_TERMINATE: The IKE phase 2 SA was deleted for the reason of SA expiration. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	第二阶段SA由于过期失效而删除
处理建议	无

35 INTRACE

本节介绍 INPCB（协议栈控制块）模块输出的日志信息。

35.1 WHITELIST

日志内容	-[STRING]; Failed to add ACL rule [STRING]:[UINT16] -> [STRING]:[UINT16] to the whitelist, VRF: [UINT16], error code: 0x[UINT32].
参数解释	$1：板号 $2：本地地址 $3：本地端口号 $4：远端地址 $5：远端端口号 $6：私网索引 $7：错误码，包括： • 0x22010002：ACL 规则已存在 • 0x22010008：白名单规则已达上限 • 0x40010001：其他异常，比如 MDC 控制块不存在 • 0x4001000B：资源不足
日志等级	3
举例	INTRACE/3/WHITELIST: -Chassis=2-Slot=3; Failed to add ACL rule 1.1.1.1:36523 -> 1.1.1.2:179 to the whitelist, VRF: 0, error code: 0x22010002.
日志说明	TCP业务添加ACL白名单失败
处理建议	检查该TCP连接状态，查看该连接业务是否正常

日志内容	-[STRING]; Failed to delete ACL rule [STRING]:[UINT16] -> [STRING]:[UINT16] from the whitelist, VRF: [UINT16], error code: 0x[UINT32].
参数解释	$1：板号 $2：本地地址 $3：本地端口号 $4：远端地址 $5：远端端口号 $6：私网索引 $7：错误码，包括： • 0x40010001：其他异常，比如 MDC 控制块不存在 • 0x40010008：传入参数错误 • 0x4001000B：资源不足
日志等级	3
举例	INTRACE/3/WHITELIST:-Chassis=2-Slot=3; Failed to delete ACL rule 1.1.1.1:36523 -> 1.1.1.2:179 from the whitelist, VRF: 0, error code: 0x22010001.
日志说明	TCP业务删除ACL白名单失败
处理建议	检查TCP和ACL白名单，查看是否出现内存残留或业务异常

36 IP6ADDR

本节介绍 IPv6 地址模块输出的日志信息。

36.1 IP6ADDR_ADDLINKLOCAL_FAIL

日志内容	Failed to add a link-local address of interface [STRING] to driver. Reason: [STRING].
参数解释	$1：接口名 $2：下发链路本地地址失败的原因： ○ Deploying link-local addresses to driver is not supported：设备不支持下发链路本地地址到驱动 ○ Insufficient resources：资源不足 ○ Unknown error：未知错误
日志等级	4
举例	IP6ADDR/4/IP6ADDR_ADDLINKLOCAL_FAIL: Failed to add a link-local address of interface GigabitEthernet1/2/0/1 to driver. Reason: Insufficient resources.
日志说明	接口通过有状态或无状态方式获取IPv6地址时，或手工指定接口的IPv6地址时，设备会自动生成链路本地地址，并下发给驱动。如果将链路本地地址下发给驱动失败，则打印此日志
处理建议	• 如果是设备不支持下发链路本地地址到驱动，不必处理 • 如果是因为资源不足，可清理设备内存以释放资源，然后重新执行操作 • 如果是未知错误，请联系技术支持

36.2 IP6ADDR_CREATEADDRESS_CONFLICT

日志内容	Failed to create an address by the prefix. Reason: [STRING] on [STRING] conflicts with SRv6 locator [STRING].
参数解释	$1：IPv6地址 $2：接口名 $3：Locator段
日志等级	4
举例	IP6ADDR/4/IP6ADDR_CREATEADDRESS_CONFLICT: Failed to create an address by the prefix. Reason: 2000::1234:0:0:1/80 on GigabitEthernet1/2/0/1 conflicts with SRv6 locator 2000::1/64.
日志说明	接口上生成的IPv6地址不能和SRv6视图下配置的Locator段冲突。如果使用**ipv6 address** *prefix-number*命令为接口配置IPv6地址，但是地址被包含于在SRv6视图下配置的Locator段中，则输出本日志
处理建议	取消冲突配置，重新为接口配置新的IPv6地址

36.3 IP6ADDR_CREATEADDRESS_ERROR

日志内容	Failed to create an address by the prefix. Reason: [STRING] on [STRING] and [STRING] on [STRING] overlap.
参数解释	$1：IPv6地址前缀 $2：接口名 $3：IPv6地址前缀 $4：接口名
日志等级	4
举例	IP6ADDR/4/IP6ADDR_CREATEADDRESS_ERROR: Failed to create an address by the prefix. Reason: 2001::/64 on GigabitEthernet1/2/0/2 and 2001::/64 on GigabitEthernet1/2/0/1 overlap.
日志说明	当配置接口通过引用前缀生成IPv6地址时，可能由于同一台设备的不同接口前缀覆盖，导致IPv6地址生成失败，此时输出本日志
处理建议	取消冲突接口上的通过前缀生成IPv6地址的配置，重新配置其他前缀的IPv6地址

36.4 IP6ADDR_CREATEADDRESS_INVALID

日志内容	Can't configure the unspecified address or loopback address on [STRING] by using a prefix with all zeros.
参数解释	$1：接口名
日志等级	4
举例	IP6ADDR/4/IP6ADDR_CREATEADDRESS_INVALID: Can't configure the unspecified address or loopback address on GigabitEthernet1/2/0/1 by using a prefix with all zeros.
日志说明	接口上的IPv6地址不能是未指定地址或者环回地址。如果使用**ipv6 prefix**命令配置了全零的IPv6地址前缀，并通过**ipv6 address** *prefix-number*命令引用全零的IPv6地址前缀为接口配置了未指定地址或者环回地址，则输出本日志
处理建议	取消无效配置，重新为接口配置新的IPv6地址

36.5 IP6ADDR_FUNCTION_FAIL

日志内容	Failed to enable IPv6 on interface [STRING]. Reason: [STRING].
参数解释	$1：接口名 $2：使能IPv6功能失败的原因，取值包括： • Insufficient resources：资源不足 • IPv6 is not supported：由于设备不支持 IPv6，接口上不支持配置 IPv6 地址 • Unknown error：未知错误
日志等级	4
举例	IP6ADDR/4/IP6ADDR_FUNCTION_FAIL: Failed to enable IPv6 on interface GigabitEthernet1/2/0/1. Reason: Insufficient resources.
日志说明	接口通过有状态或无状态方式获取IPv6地址时，或手工指定接口的IPv6地址时，会使能IPv6功能。如果为接口配置IPv6地址失败，即使能IPv6功能失败，则打印此日志。使能IPv6功能失败的原因一般有：资源不足、设备不支持IPv6、未知错误等
处理建议	• 如果是因为资源不足，可清理设备内存以释放资源，然后重新执行操作 • 如果是未知错误，请联系技术支持

37 IP6FW

本节包含 IP6FW（IPv6 Forwarding）日志信息。

37.1 IP6FW_ABNORMAL_HEADERS

日志内容	Received an IPv6 packet with repeated extension headers.
参数解释	无
日志等级	6
举例	IP6FW/6/IP6FW_ABNORMAL_HEADERS: Received an IPv6 packet with repeated extension headers.
日志说明	收到一个包含重复扩展头的IPv6报文
处理建议	检查报文源的合法性

37.2 IP6FW_FAILED_TO_SET_MTU

日志内容	Failed to set MTU [UINT32] on interface [STRING] for IPv6 packets.
参数解释	$1：MTU值 $2：接口名称
日志等级	5
举例	IP6FW/5/IP6FW_FAILED_TO_SET_MTU: Failed to set MTU 9600 on interface GigabitEthernet6/3/8 for IPv6 packets.
日志说明	在接口上配置MTU值失败
处理建议	修改接口下MTU值

38 IPADDR

本节介绍 IP 地址模块输出的日志信息。

38.1 IPADDR_HA_EVENT_ERROR

日志内容	A process failed HA upgrade because [STRING].

日志内容	A process failed HA upgrade because [STRING].
参数解释	$1：进程HA升级失败原因： • IPADDR failed the smooth upgrade：板间平滑失败 • IPADDR failed to reupgrade to the master process：重新升级为主失败 • IPADDR stopped to restart the timer：重启定时器停止 • IPADDR failed to upgrade to the master process：升级为主进程失败 • IPADDR failed to restart the upgrade：重新尝试升级失败 • IPADDR failed to add the unicast object to the master task epoll：将 sync 单播对象挂主任务 epoll 失败 • IPADDR failed to create an unicast object：创建单播失败 • IPADDR role switchover failed when the standby process switched to the master process：备升主时角色转换失败 • IPADDR switchover failed when the master process switched to the standby process：主变备时降级失败 • IPADDR HA upgrade failed：HA 升级失败 • IPADDR failed to set the interface filtering criteria：设置接口选择句柄失败 • IPADDR failed to register interface events：注册接口事件失败 • IPADDR failed to subscribe port events：订阅端口事件失败 • IPADDR failed to add a VPN port event to the master epoll：添加 VPN 的端口事件到主 Epoll 失败 • IRDP failed to open DBM：打开 DBM 数据库失败 • IRDP failed to initiate a connection to the device management module：向设备管理建立连接失败 • IRDP failed to add the master task epoll with the handle used to connect to the device management module ：与设备管理建立连接的句柄加 Epoll 失败 • IRDP failed to register device management events：注册设备管理事件失败 • IRDP failed to subscribe port events：订阅协议使能端口事件失败 • IRDP failed to add the master task epoll with the handle used to subscribe port events：订阅协议使能端口事件的句柄加 Epoll 失败 • IRDP failed to set the interface filtering criteria：设置接口选择句柄失败 • IRDP failed to register interface events：注册接口事件失败 • IRDP failed to register network events：注册网络事件失败 • IRDP failed to create the interface control block storage handle：创建接口控制块存储句柄失败 • IRDP failed to create the timer：创建定时器失败 • IRDP failed to add the master task epoll with the handle used to create the timer：创建定时器的句柄加 Epoll 失败 • IRDP failed to set the schedule time for the timer：设置定时器调度时间失败 • IRDP failed to set the timer to unblocked status：设置定制器为非阻塞失败 • IRDP failed to create a timer instance：创建定时器实例失败

日志内容	A process failed HA upgrade because [STRING].
日志等级	4
举例	IPADDR/4/IPADDR_HA_EVENT_ERROR: A process failed HA upgrade because IPADDR failed the smooth upgrade.
日志说明	进程HA升级失败，原因是板间平滑失败，重新升级为主失败等
处理建议	请联系技术支持

38.2 IPADDR_HA_STOP_EVENT

日志内容	The device received an HA stop event.
参数解释	无
日志等级	4
举例	IPADDR/4/IPADDR_HA_STOP_EVENT: The device received an HA stop event.
日志说明	设备收到HA STOP事件
处理建议	请联系技术支持

39 IPFW

本节包含 IPFW（IP Forwarding）日志信息。

39.1 IP_ADD_FLOW_ANTITCPSYNFLD

日志内容	Add a flow-based entry: Packet type=[STRING]; SrcIP=[IPADDR]; DstPort=[UINT16]; VPN=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：攻击报文的源IP地址 $3：被攻击的目的端口号 $4：VPN实例名称，公网取值为the public network，获取名称失败时取值N/A
日志等级	4
举例	IPFW/4/IP_ADD_FLOW_ANTITCPSYNFLD: Add a flow-based entry: Packet type=IP; SrcIP=2000::1; DstPort=23; VPN=the public network
日志说明	检测到可能是基于流的TCP SYN Flood攻击，添加一条基于该流的TCP SYN Flood攻击防范表项
处理建议	检查攻击来源

39.2 IP_ADD_FLOW_ANTIUDPFLD

日志内容	Add a flow-based entry: Packet type=[STRING]; SrcIP=[IPADDR]; DstPort=[UINT16]; VPN=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：攻击报文的源IP地址 $3：被攻击的目的端口号 $4：VPN实例名称，公网取值为the public network，获取名称失败时取值N/A
日志等级	4
举例	IPFW/4/IP_ADD_FLOW_ANTIUDPFLD: Add a flow-based entry: Packet type=IP; SrcIP=2000::1; DstPort=69; VPN=the public network.
日志说明	检测到可能是基于流的UDP Flood攻击，添加一条基于该流的UDP Flood攻击防范表项
处理建议	检查攻击来源

39.3 IP_ADD_INTERFACE_ANTITCPSYNFLD

日志内容	Add an interface-based entry: Packet type=[STRING]; Interface=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：接口名称
日志等级	4
举例	IPFW/4/IP_ADD_INTERFACE_ANTITCPSYNFLD: Add an interface-based entry: Packets type=MPLS; Interface=GigabitEthernet1/2/0/1.
日志说明	检测到可能是基于接口的TCP SYN Flood攻击，添加一条基于该接口的TCP SYN Flood攻击防范表项
处理建议	检查攻击来源

39.4 IP_ADD_INTERFACE_ANTIUDPFLD

日志内容	Add an interface-based entry: Packet type=[STRING]; Interface=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：接口名称
日志等级	4
举例	IPFW/4/IP_ADD_INTERFACE_ANTIUDPFLD: Add an interface-based entry: Packets type=MPLS; Interface=GigabitEthernet1/2/0/1.
日志说明	检测到可能是基于接口的UDP Flood攻击，添加一条基于该接口的UDP Flood攻击防范表项
处理建议	检查攻击来源

39.5 IP_DEL_FLOW_ANTITCPSYNFLD

日志内容	Delete a flow-based entry: Packet type=[STRING]; SrcIP=[IPADDR]; DstPort=[UINT16]; VPN=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：攻击报文的源IP地址 $3：被攻击的端口号 $4：VPN实例名称，公网取值为the public network，获取名称失败时取值N/A
日志等级	4
举例	IPFW/4/IP_DEL_FLOW_ANTITCPSYNFLD: Delete a flow-based entry: Packet type=MPLS; SrcIP=192.168.1.2; DstPort=80; VPN=vpn1.
日志说明	在私网中，删除一条基于流的TCP SYN Flood攻击防范表项，该表项的报文类型是MPLS，源IP地址是192.168.1.2，目的端口号是80，VPN实例名称是vpn1
处理建议	无需处理

39.6 IP_DEL_FLOW_ANTIUDPFLD

日志内容	Delete a flow-based entry: Packet type=[STRING]; SrcIP=[IPADDR]; DstPort=[UINT16]; VPN=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：攻击报文的源IP地址 $3：被攻击的端口号 $4：VPN实例名称，公网取值为the public network，获取名称失败时取值N/A
日志等级	4
举例	IPFW/4/IP_DEL_FLOW_ANTIUDPFLD: Delete a flow-based entry: Packet type=MPLS; SrcIP=192.168.1.2; DstPort=80; VPN=vpn1.
日志说明	在私网中，删除一条基于流的UDP Flood攻击防范表项，该表项的报文类型是MPLS，源IP地址是192.168.1.2，目的端口号是80，VPN实例名称是vpn1
处理建议	无需处理

39.7 IP_DEL_INTERFACE_ANTITCPSYNFLD

日志内容	Delete an interface-based entry: Packet type=[STRING]; Interface=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：接口名称
日志等级	4
举例	IPFW/4/IP_DEL_INTERFACE_ANTITCPSYNFLD: Delete an interface-based entry: Packets type=IP, Interface=GigabitEthernet1/2/0/1.
日志说明	删除一条基于接口的TCP SYN Flood攻击防范表项，该表项的报文类型是IP，接口名称是GigabitEthernet1/2/0/1
处理建议	无需处理

39.8 IP_DEL_INTERFACE_ANTIUDPFLD

日志内容	Delete an interface-based entry: Packet type=[STRING]; Interface=[STRING].
参数解释	$1：报文类型，取值包括： • MPLS • IP $2：接口名称
日志等级	4
举例	IPFW/4/IP_DEL_INTERFACE_ANTIUDPFLD: Delete an interface-based entry: Packets type=IP, Interface=GigabitEthernet1/2/0/1.
日志说明	删除一条基于接口的UDP Flood攻击防范表项，该表项的报文类型是IP，接口名称是GigabitEthernet1/2/0/1
处理建议	无需处理

39.9 IP_INSERT_FAILED_ANTITCPSYNFLD

日志内容	Insert into AVL tree failed for flow-based entry: Family=[UINT32]; DstPort=[UINT16]; VPN=[UINT16].
参数解释	$1：协议簇编号 $2：目的端口号 $3：VPN名称
日志等级	5
举例	IPFW/5/IP_INSERT_FAILED_ANTITCPSYNFLD: Insert into AVL tree failed for flow-based entry : Family=2; DstPort=80; VPN=2.
日志说明	基于流的TCP SYN Flood攻击防范的攻击表项插入AVL树失败，协议簇号是2，目的端口号是80，显示VPN名称
处理建议	无需处理

39.10 IP_INSERT_FAILED_ANTIUDPFLD

日志内容	Insert into AVL tree failed for flow-based entry: Family=[UINT32]; DstPort=[UINT16]; VPN=[UINT16].
参数解释	$1：协议簇编号 $2：目的端口号 $3：VPN名称
日志等级	5
举例	IPFW/5/IP_INSERT_FAILED_ANTIUDPFLD: Insert into AVL tree failed for flow-based entry : Family=2; DstPort=80; VPN=2.
日志说明	基于流的UDP Flood攻击防范的攻击表项插入AVL树失败，协议簇号是2，目的端口号是80，显示VPN名称
处理建议	无需处理

39.11 IP_NOTSUPPORT_ANTITCPSYNFLD

日志内容	TCP SYN flood attack prevention is not supported.
参数解释	无
日志等级	6
举例	IPFW/6/IP_NOTSUPPORT_ANTITCPSYNFLD: TCP SYN flood attack prevention is not supported.
日志说明	不支持TCP SYN Flood攻击防范功能
处理建议	无需处理

39.12 IP_NOTSUPPORT_ANTIUDPFLD

日志内容	UDP flood attack prevention is not supported.
参数解释	无
日志等级	6
举例	IPFW/6/IP_NOTSUPPORT_ANTIUDPFLD: UDP flood attack prevention is not supported.
日志说明	不支持UDP Flood攻击防范功能
处理建议	无需处理

39.13 IP_SETTING_FAILED_ANTITCPSYNFLD

日志内容	Setting entry to drive failed. Total failures=[UINT32].
参数解释	$1：下驱动失败的TCP SYN Flood攻击防范的攻击表项总个数
日志等级	5
举例	IPFW/5/IP_SETTING_FAILED_ANTITCPSYNFLD: Setting entry to drive failed. Total failures = 12345.
日志说明	表项下驱动失败，下驱动失败的TCP SYN Flood攻击防范的攻击表项总个数为12345
处理建议	无需处理

39.14 IP_SETTING_FAILED_ANTIUDPFLD

日志内容	Setting entry to drive failed. Total failures=[UINT32].
参数解释	$1：下驱动失败的UDP Flood攻击防范的攻击表项总个数
日志等级	5
举例	IPFW/5/IP_SETTING_FAILED_ANTIUDPFLD: Setting entry to drive failed. Total failures = 12345.
日志说明	表项下驱动失败，下驱动失败的UDP Flood攻击防范的攻击表项总个数为12345
处理建议	无需处理

39.15 IP_CLEARDRVSTAT_ANTITCPSYNFLD

日志内容	Failed to clear drive's statistics.
参数解释	无
日志等级	4
举例	IPFW/4/IP_CLEARDRVSTAT_ANTITCPSYNFLD: Failed to clear drive's statistics.
日志说明	清除驱动的TCP SYN Flood攻击防范的报文统计信息失败
处理建议	无需处理

39.16 IP_CLEARDRVSTAT_ANTIUDPFLD

日志内容	Failed to clear drive's statistics.
参数解释	无
日志等级	4
举例	IPFW/4/IP_CLEARDRVSTAT_ANTIUDPFLD: Failed to clear drive's statistics.
日志说明	清除驱动的UDP Flood攻击防范的报文统计信息失败
处理建议	无需处理

39.17 IPFW_BPA_NORESOURCE

日志内容	Not enough resources are available on [STRING] to enable BGP policy accounting for interface [STRING].
参数解释	$1:chassis编号+slot编号或slot编号 $2: 接口名
日志等级	6
举例	IPFW/6/IPFW_BPA_NORESOURCE: -MDC=1-Slot=2; Not enough resources are available on slot2 to enable BGP policy accounting for interface Route-Aggregation1.
日志说明	配置**bgp-policy accounting**命令时，由于slot资源不足导致接口开启BGP策略计费功能失败
处理建议	无

39.18 IPFW_INFO

日志内容	The specified IP load sharing mode is not supported on this slot.
参数解释	无
日志等级	6
举例	IPFW/6/IPFW_INFO: -MDC=1-Slot=2; The specified IP load sharing mode is not supported on this slot.
日志说明	用户配置的IP负载均衡模式在此单板上不支持
处理建议	确认单板支持的模式，重新配置

日志内容	Failed to configure IP load sharing mode on this slot.
参数解释	无
日志等级	6
举例	IPFW/6/IPFW_INFO: -MDC=1-Slot=2; Failed to configure IP load sharing mode on this slot.
日志说明	用户配置的IP负载均衡模式在此单板上配置失败
处理建议	确认单板支持的模式，重新配置

39.19 IPFW_FAILED_TO_SET_MTU

日志内容	Failed to set MTU [UINT32] on interface [STRING] for IPv4 packets.
参数解释	$1：MTU值 $2：接口名称
日志等级	5
举例	IPFW/5/IPFW_FAILED_TO_SET_MTU: Failed to set MTU 9600 on interface GigabitEthernet6/3/8 for IPv4 packets.
日志说明	在接口上配置MTU值失败
处理建议	修改接口下MTU值

40 IPSEC

本节介绍 IPsec 模块输出的日志信息。

40.1 IPSEC_FAILED_ADD_FLOW_TABLE

日志内容	Failed to add flow-table due to [STRING].
参数解释	$1：失败原因
日志等级	4
举例	IPSEC/4/IPSEC_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
日志说明	添加流表失败，可能原因包括硬件资源不足等
处理建议	对于硬件资源不足情况，请联系技术支持

40.2 IPSEC_PACKET_DISCARDED

日志内容	IPsec packet discarded, Src IP:[STRING], Dst IP:[STRING], SPI:[UINT32], SN:[UINT32], Cause:[STRING].
参数解释	$1：报文的源IP地址 $2：报文的目的IP地址 $3：SPI（Security Parameter Index，安全参数索引） $4：报文的序列号 $5：报文丢弃的原因： • 抗重放检测失败，显示为：Anti-replay checking failed. • AH 认证失败，显示为：AH authentication failed. • ESP 认证失败，显示为：ESP authentication failed. • SA 无效，显示为：Invalid SA. • ESP 解密失败，显示为：ESP decryption failed. • 报文的源地址匹配不上 SA，显示为：Source address of packet does not match the SA. • 没有匹配的 ACL 规则，显示为：No ACL rule matched.
日志等级	6
举例	IPSEC/6/IPSEC_PACKET_DISCARDED: IPsec packet discarded, Src IP:1.1.1.2, Dest IP:1.1.1.4, SPI:1002, SN:0, Cause:ah authentication failed
日志说明	IPsec报文被丢弃
处理建议	无

40.3 IPSEC_SA_ESTABLISH

日志内容	Established IPsec SA. The SA’s source address is [STRING], destination address is [STRING], protocol is [STRING], and SPI is [UINT32].
参数解释	$1：IPsec SA的源IP地址 $2：IPsec SA的目的IP地址 $3：IPsec SA使用的安全协议 $4：IPsec SA的SPI
日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH: Established IPsec SA. The SA’s source address is 1.1.1.1, destination address is 2.2.2.2, protocol is AH, and SPI is 2435.
日志说明	IPsec SA创建成功
处理建议	无

40.4 IPSEC_SA_ESTABLISH_FAIL

日志内容	Failed to establish IPsec SA for the reason of [STRING]. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：IPsec SA创建失败的原因： • 隧道创建失败，显示为：Tunnel establishment failure. • 配置不完整，显示为：Incomplete configuration. • 配置的安全提议无效，显示为：Unavailable transform set. $2：源IP地址 $3：目的IP地址
日志等级	6
举例	IPSEC/6/IPSEC_SA_ESTABLISH_FAIL: Failed to establish IPsec SA for the reason of creating tunnel failure. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	IPsec SA创建失败。触发该日志的原因可能有：隧道创建失败、配置不完整、或者配置的安全提议无效
处理建议	检查本端和对端设备上的IPsec配置

40.5 IPSEC_SA_INITINATION

日志内容	Began to establish IPsec SA. The SA's source address is [STRING], and its destination address is [STRING].
参数解释	$1：IPsec SA的源IP地址 $2：IPsec SA的目的IP地址
日志等级	6
举例	IPSEC/6/IPSEC_SA_INITINATION: Began to establish IPsec SA. The SA's source address is 1.1.1.1, and its destination address is 2.2.2.2.
日志说明	开始创建IPsec SA
处理建议	无

40.6 IPSEC_SA_TERMINATE

日志内容	The IPsec SA was deleted for the reason of [STRING]. The SA's source address is [STRING], destination address is [STRING], protocol is [STRING], and SPI is [UINT32].
参数解释	$1：IPsec SA被删除的原因： • SA 空闲超时，显示为：SA idle timeout. • 执行了 reset 命令，显示为：reset command executed. $2：源IP地址 $3：目的IP地址 $4：使用的安全协议 $5：SPI
日志等级	6
举例	IPSEC/6/IPSEC_SA_TERMINATE: The IPsec SA was deleted for the reason of SA idle timeout. The SA's source address is 1.1.1.1, destination address is 2.2.2.2, protocol is ESP, and SPI is 34563.
日志说明	IPsec SA被删除。触发该日志的原因可能有：SA空闲超时或者执行了reset命令
处理建议	无

41 IRDP

本节介绍 IRDP 模块输出的日志信息。

41.1 IRDP_EXCEED_ADVADDR_LIMIT

日志内容	The number of advertisement addresses on interface [STRING] exceeded the limit 255.
参数解释	$1：接口名称
日志等级	6
举例	IRDP/6/IRDP_EXCEED_ADVADDR_LIMIT: The number of advertisement addresses on interface GigabitEthernet1/2/0/1 exceeded the limit 255.
日志说明	接口上待通告的地址数超过了上限值
处理建议	删除接口上不需要的地址

42 ISIS

本节介绍 IS-IS 模块输出的日志信息。

42.1 ISIS_LSP_CONFLICT

日志内容	IS-IS [UINT16], [STRING] LSP, LSPID=[STRING], SeqNum=[HEX], system ID conflict might exist.
参数解释	$1：进程ID $2：IS类型，值为Level-1或Level-2 $3：LSP ID $4：LSP序列号
日志等级	5
举例	ISIS/5/ISIS_LSP_CONFLICT: -MDC=1; IS-IS 1, Level-1 LSP, LSPID=1111.1111.1111.00-00, SeqNum=0x000045bf, system ID conflict might exist.
日志说明	网络中可能存在System ID冲突
处理建议	检查产生该LSP的设备的System ID是否和其他设备的System ID冲突

42.2 ISIS_MEM_ALERT

日志内容	ISIS Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	ISIS/5/ISIS_MEM_ALERT: ISIS Process received system memory alert start event.
日志说明	IS-IS模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

42.3 ISIS_NBR_CHG

日志内容	IS-IS [UINT16], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING], Reason: [STRING].
参数解释	$1：IS-IS进程ID $2：IS-IS邻居等级 $3：邻居ID $4：接口名称 $5：邻居状态 $6：邻居状态变化原因
日志等级	5
举例	ISIS/5/ISIS_NBR_CHG: IS-IS 1, Level-1 adjacency 0000.0000.0001 (GigabitEthernet1/2/0/1), state changed to DOWN, Reason: circuit data clean.
日志说明	邻居状态发生变化
处理建议	需要关注邻居状态变化原因。当邻居状态变为down时，检查IS-IS配置正确性和网络连通性

43 ISSU

本节介绍 ISSU 模块输出的日志信息。

43.1 ISSU_PROCESSWITCHOVER

日志内容	Switchover completed. The standby process became the active process.
参数解释	无
日志等级	5
举例	ISSU/5/ISSU_PROCESSWITCHOVER: Switchover completed. The standby process became the active process.
日志说明	用户执行**issu run switchover**进行主备倒换完成，备进程已升级为主进程
处理建议	无

43.2 ISSU_ROLLBACKCHECKNORMAL

日志内容	The rollback might not be able to restore the previous version for [STRING] because the status is not normal.
参数解释	$1：chassis编号+slot编号或slot编号
日志等级	4
举例	ISSU/4/ISSU_ROLLBACKCHECKNORMAL: The rollback might not be able to restore the previous version for chassis 1 slot 2 because the state is not normal.
日志说明	ISSU升级，ISSU状态处理Switching，用户执行**issu rollback**回滚或ISSU回滚定时器超时自动回滚，如果有升级过的板状态不为Normal，会输出该日志
处理建议	无

44 L2VPN

本节介绍 L2VPN 模块输出的日志信息。

44.1 L2VPN_BGPVC_CONFLICT_LOCAL

日志内容	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with local site.
参数解释	$1：冲突的远端Site ID $2：引发冲突的远端Site的IP地址 $3：引发冲突的远端Site的Route Distinguisher
日志等级	5
举例	L2VPN/5/L2VPN_BGPVC_CONFLICT_LOCAL: Remote site ID 1 (From 1.1.1.1, route distinguisher 1:1) conflicts with local site.
日志说明	本端Site ID和另一个远端Site ID冲突。触发该日志的原因可能有： • 新接收到一个远端 Site ID 和本端 Site ID 相同 • 新配置本端 Site ID 和已接收到的一个远端 Site ID 相同
处理建议	更改远端或本端Site ID，或者修改配置使得远端Site不引入到本端Site所在实例

44.2 L2VPN_BGPVC_CONFLICT_REMOTE

日志内容	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with another remote site.
参数解释	$1：冲突的远端Site ID $2：引发冲突的远端Site的IP地址 $3：引发冲突的远端Site的Route Distinguisher
日志等级	5
举例	L2VPN/5/L2VPN_BGPVC_CONFLICT_REMOTE: Remote site ID 1 (From 1.1.1.1, route distinguisher 1:1) conflicts with another remote site.
日志说明	两个远端的Site ID冲突。触发该日志的原因可能为：在已经接收一个远端Site的情况下，接收到另一个远端Site，两者的Site ID相同
处理建议	更改其中一个远端Site ID，或者修改配置使得两个远端不引入到同一个实例中

44.3 L2VPN_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for L2VPN.
参数解释	无
日志等级	4
举例	L2VPN/4/L2VPN_HARD_RESOURCE_NOENOUGH: No enough hardware resource for L2VPN.
日志说明	L2VPN硬件资源不足
处理建议	请检查是否生成了当前业务不需要的VSI、PW或AC，是则删除对应配置

44.4 L2VPN_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for L2VPN are restored.
参数解释	无
日志等级	6
举例	L2VPN/6/L2VPN_HARD_RESOURCE_RESTORE: Hardware resources for L2VPN are restored.
日志说明	L2VPN硬件资源恢复
处理建议	无

44.5 L2VPN_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for a static PW in [STRING] [STRING] is duplicate.
参数解释	$1：入标签值 $2：L2VPN类型，交叉连接组或者VSI $3：交叉连接组或者VSI的名称
日志等级	4
举例	L2VPN/4/L2VPN_LABEL_DUPLICATE: Incoming label 1024 for a static PW in Xconnect-group aaa is duplicate.
日志说明	交叉连接组或者VSI的静态PW的入标签被静态LSP或者静态CRLSP占用。触发该日志的原因可能有： • 在 MPLS 已使能的情况下，配置了一条入标签被静态 LSP 或者静态 CRLSP 占用的静态 PW • 在入标签被静态 LSP 或静态 CRLSP 占用的静态 PW 存在的情况下，使能 MPLS
处理建议	删除该静态PW，重新配置一条静态PW，并指定新的入标签值

44.6 L2VPN_MACLIMIT_FALL_AC

日志内容	The number of MAC address entries on the AC fell below the upper limit. (VSI name=[STRING], link ID=[UINT32], max-mac-entries=[UINT32], current-mac-entries=[UINT32])
参数解释	$1：AC关联的VSI的名称 $2：AC的Link ID $3：AC的最大MAC地址学习数，取值为unlimited时，表示不对学习的最大MAC地址数进行限制 $4：AC当前学习到的MAC地址数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_FALL_AC: -MDC=1-Slot=5; The number of MAC address entries on the AC fell below the upper limit. (VSI name=aaa, link ID=1, max-mac-entries=100, current-mac-entries=80)
日志说明	AC上学习到的MAC地址数量回落到上限值的90%以下
处理建议	无

44.7 L2VPN_MACLIMIT_FALL_PW

日志内容	The number of MAC address entries on the PW fell below the upper limit. (VSI name=[STRING], link ID=[UINT32], max-mac-entries=[UINT32], current-mac-entries=[UINT32])
参数解释	$1：PW所在的VSI的名称 $2：PW的Link ID $3：PW的最大MAC地址学习数，取值为unlimited时，表示不对学习的最大MAC地址数进行限制 $4：PW当前学习到的MAC地址数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_FALL_PW: -MDC=1-Slot=5; The number of MAC address entries on the PW fell below the upper limit. (VSI name=aaa, link ID=100, max-mac-entries=50, current-mac-entries=30)
日志说明	PW上学习到的MAC地址数量回落到上限值的90%以下
处理建议	无

44.8 L2VPN_MACLIMIT_FALL_VSI

日志内容	The number of MAC address entries on the VSI fell below the upper limit. (VSI name=[STRING], max-mac-entries=[UINT32], current-mac-entries=[UINT32])
参数解释	$1：VSI的名称 $2：VSI的最大MAC地址学习数 $3：VSI当前学习到的MAC地址数，取值为unlimited时，表示不对学习的最大MAC地址数进行限制
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_FALL_VSI: -MDC=1-Slot=5; The number of MAC address entries on the VSI fell below the upper limit. (VSI name=aaa, max-mac-entries=200, current-mac-entries=150)
日志说明	VSI内学习到的MAC地址数量回落到上限值的90%以下
处理建议	无

44.9 L2VPN_MACLIMIT_MAX_AC

日志内容	The number of MAC address entries on the AC reached the upper limit. (VSI name=[STRING], link ID=[UINT32], max-mac-entries=[UINT32])
参数解释	$1：AC关联的VSI的名称 $2：AC的Link ID $3：AC的最大MAC地址学习数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_MAX_AC: -MDC=1-Slot=5; The number of MAC address entries on the AC reached the upper limit. (VSI name=aaa, link ID=1, max-mac-entries=100)
日志说明	AC上学习到的MAC地址数量达到上限
处理建议	无

44.10 L2VPN_MACLIMIT_MAX_PW

日志内容	The number of MAC address entries on the PW reached the upper limit. (VSI name=[STRING], link ID=[UINT32], max-mac-entries=[UINT32])
参数解释	$1：PW所在的VSI的名称 $2：PW的Link ID $3：PW的最大MAC地址学习数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_MAX_PW: -MDC=1-Slot=5; The number of MAC address entries on the PW reached the upper limit. (VSI name=aaa, link ID=100, max-mac-entries=50)
日志说明	PW上学习到的MAC地址数量达到上限
处理建议	无

44.11 L2VPN_MACLIMIT_MAX_VSI

日志内容	The number of MAC address entries on the VSI reached the upper limit. (VSI name=[STRING], max-mac-entries=[UINT32])
参数解释	$1：VSI的名称 $2：VSI的最大MAC地址学习数
日志等级	4
举例	L2VPN/4/L2VPN_MACLIMIT_MAX_VSI: -MDC=1-Slot=5; The number of MAC address entries on the VSI reached the upper limit. (VSI name=aaa, max-mac-entries=200)
日志说明	VSI内学习到的MAC地址数量达到上限
处理建议	无

45 LAGG

本节介绍 LAGG 模块输出的日志信息。

45.1 LAGG_ACTIVE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the active state.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_ACTIVE: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the active state.
日志说明	聚合组内某成员端口成为激活端口
处理建议	无

45.2 LAGG_INACTIVE_AICFG

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the member port and the aggregate interface have different attribute configurations.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_AICFG: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the member port and the aggregate interface have different attribute configurations.
日志说明	由于聚合组内某成员端口的属性类配置与聚合接口属性类配置不同，该成员端口成为去激活端口
处理建议	修改该成员端口的属性类配置，使其与聚合接口属性类配置一致

45.3 LAGG_INACTIVE_BFD

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the BFD session state of the port was down.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_BFD: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the BFD session state of the port is down.
日志说明	聚合成员端口上的BFD会话down时，该成员端口变为去激活状态
处理建议	排查链路故障、检查该非选中状态的成员端口的操作key和属性类配置是否与参考端口一致

45.4 LAGG_INACTIVE_CONFIGURATION

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the aggregation configuration of the port is incorrect.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_CONFIGURATION: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the aggregation configuration of the port is incorrect.
日志说明	由于聚合组内某成员端口配置限制，该成员端口变为去激活状态
处理建议	无

45.5 LAGG_INACTIVE_DUPLEX

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the duplex mode is different between the member port and the reference port.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_DUPLEX: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the duplex mode is different between the member port and the reference port.
日志说明	由于聚合组内某成员端口的双工模式与参考端口不一致，该成员端口变为去激活状态
处理建议	修改该端口双工模式，使其与参考端口一致

45.6 LAGG_INACTIVE_HARDWAREVALUE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because of the port's hardware restirction.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_HARDWAREVALUE: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because of the port's hardware restirction.
日志说明	聚合组内某成员端口因硬件限制与参考端口不一致，该成员端口变为去激活状态
处理建议	无

45.7 LAGG_INACTIVE_LINKQUALITY_LOW

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the member port has low link quality.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_LINKQUALITY_LOW: Member port FGE1/2/0/5 of aggregation group BAGG1 changed to the inactive state, because the member port has low link quality.
日志说明	聚合组内成员端口因为链路质量低，无法满足正常的业务转发需求，端口变为去激活状态
处理建议	检查网线是否老化，接口模块是否故障等

45.8 LAGG_INACTIVE_LOWER_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of active ports is below the lower limit.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_LOWER_LIMIT: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the number of active ports is below the lower limit.
日志说明	因聚合组内激活端口数量未达到配置的最小激活端口数，聚合组内某成员端口变为去激活状态
处理建议	增加激活端口数量，使其达到最小激活端口数

45.9 LAGG_INACTIVE_PARTNER

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the aggregation configuration of its peer port is incorrect.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_PARTNER: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the aggregation configuration of its peer port is incorrect.
日志说明	动态聚合组内，由于对端端口聚合配置不正确变为去激活状态，本端端口变为去激活状态
处理建议	无

45.10 LAGG_INACTIVE_PHYSTATE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the physical state of the port is down.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_PHYSTATE: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the physical state of the port is down.
日志说明	聚合组内某成员端口处于down状态，该成员端口变为去激活状态
处理建议	使该端口处于UP状态

45.11 LAGG_INACTIVE_RESOURCE_INSUFICIE

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because all aggregate resources are occupied.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_RESOURCE_INSUFICIE: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because all aggregate resources are occupied.
日志说明	聚合资源不足导致聚合组内成员端口变为去激活端口
处理建议	无

45.12 LAGG_INACTIVE_SECONDARY

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because it was the secondary member port in the aggregation group in 1+1 backup mode.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_SECONDARY: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because it was the secondary member port in the aggregation group in 1+1 backup mode.
日志说明	接口为1:1主备模式聚合组的备份端口，切换为inactive状态
处理建议	无

45.13 LAGG_INACTIVE_SPEED

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the speed configuration of the port is incorrect.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_SPEED: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the speed configuration of the port is incorrect.
日志说明	聚合组内某成员端口速率与参考端口不一致，该端口变为去激活状态
处理建议	修改该端口速率，使其与参考端口一致

45.14 LAGG_INACTIVE_STRUNK_DOWN

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the role of the aggregate interface is secondary in a smart trunk.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_STRUNK_DOWN: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the role of the aggregate interface is secondary in a smart trunk.
日志说明	聚合接口在S-Trunk组中的角色影响该聚合组中成员端口选中情况，当聚合接口在S-Trunk组中的角色为Secondary时，该聚合组中成员接口不选中
处理建议	无

45.15 LAGG_INACTIVE_UPPER_LIMIT

日志内容	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of active ports has reached the upper limit.
参数解释	$1：端口名称 $2：聚合组类型及ID
日志等级	6
举例	LAGG/6/LAGG_INACTIVE_UPPER_LIMIT: Member port GE1/2/0/1 of aggregation group BAGG1 changed to the inactive state, because the number of active ports has reached the upper limit.
日志说明	动态聚合组内激活端口数量已达到上限。后加入的成员端口成为激活端口，致使某成员端口变为去激活状态
处理建议	无

46 LDP

本节介绍 LDP 模块输出的日志信息。

46.1 LDP_SESSION_CHG

日志内容	Session ([STRING], [STRING]) is [STRING] ([STRING]). ([STRING])

参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0
	$2：VPN实例名。如果该会话属于公网，显示为public instance
	$3：会话状态，up或者down
	$4：会话失败的原因，仅在会话状态为down时显示
	$5：会话信息。仅在会话状态为down时，显示会话相关信息：
	• LocalTransportAddr：本地传输地址
	• PeerTransportAddr：对端传输地址
	• SessionRole：本地 LSR 在会话中的角色，取值为：
	  ○ Active：主动方
	  ○ Passive：被动方
	• SessionUpTime：会话处于 Operational 状态的持续时间，格式为 DD:HH:MM
	• KeepaliveTime：协商出来的 Keepalive 时间值，单位为秒
	• KeepaliveSentCount：本地发送的 Keepalive 消息的总数
	• KeepaliveRcvdCount：本地接收的 Keepalive 消息的总数
	• GracefulRestart：对等体上是否使能了 LDP GR 功能：
	  ○ On：表示使能
	  ○ Off：表未使能
	• SocketID：会话的套接字 ID
	• WaitSendMsgCount：等待发送的 TCP 消息数量
	• CPUusage：会话 down 时的 CPU 使用率
	• MemoryState：会话 down 时内存门限状态，取值包括：
	  ○ Normal：正常
	  ○ Minor：一级门限
	  ○ Severe：二级门限
	  ○ Critical：三级门限

日志等级	5
举例	LDP/5/LDP_SESSION_CHG: Session (22.22.22.2:0, public instance) is up. LDP/5/LDP_SESSION_CHG: Session (22.22.22.2:0, VPN instance: vpn1) is down (hello hold timer expired). (LocalTransportAddr=11.1.1.1, PeerTransportAddr=22.2.2.2, SessionRole=Passive, SessionUpTime=0000:00:35, KeepaliveTime=45s, KeepaliveSentCount=143, KeepaliveRcvdCount=148, GracefulRestart=Off, SocketID=35, WaitSendMsgCount=0, CPUUsage=19%, MemoryState=Normal)
日志说明	会话状态改变了
处理建议	当会话状态是up时，无 当会话状态是down时，根据会话失败原因检查接口状态，链路状态和其他相关配置 会话失败原因包括： • interface not operational：接口不可用 • MPLS disabled on interface：接口上关闭 MPLS 功能 • LDP disabled on interface：接口上关闭 LDP 功能

	• LDP auto-configure disabled on interface：接口上关闭 LDP 自动配置功能 • VPN instance changed on interface：接口所属的 VPN 实例已更改 • LDP instance deleted：LDP 实例已删除 • targeted peer deleted：手工删除 LDP 对等体 • L2VPN disabled targeted peer：L2VPN 注销 targeted peer • TE tunnel disabled targeted peer：TE 隧道注销 targeted peer • session protection disabled targeted peer：会话保护注销 targeted peer • OSPF Remote LFA disabled targeted peer：OSPF Remote LFA 注销 targeted peer • IS-IS Remote LFA disabled targeted peer：IS-IS Remote LFA 注销 targeted peer • process deactivated：LDP 进程降级 • failed to receive the initialization message：未收到初始化信息 • graceful restart reconnect timer expired：平滑重启重连时间超时 • failed to recover adjacency by NSR：NSR 恢复邻接关系失败 • failed to upgrade session by NSR：NSR 升级会话失败 • closed the GR session：GR 会话关闭 • keepalive hold timer expired：keepalive 保持时间超时 • hello hold timer expired：Hello 保持时间超时 • session reset：重启会话 • TCP connection down：TCP 连接断开 • received a fatal notification message ：收到致命的通知信息 • internal error：内部错误 • memory in critical state：内存达到 critical 状态 • transport address changed on interface：接口上的传输地址更改 • MD5 password changed：会话 MD5 密码变化

46.2 LDP_SESSION_GR

日志内容	Session ([STRING], [STRING]): ([STRING]).
参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0 $2：VPN实例名。如果该会话属于公网，显示为public instance $3：会话平滑重启的状态，取值包括： • Start reconnection：启动会话重连 • Reconnection failed：会话重连失败 • Start recovery：会话重连成功，进入标签通告恢复过程 • Recovery completed：会话恢复全过程完成
日志等级	5
举例	LDP/5/LDP_SESSION_GR: Session (22.22.22.2:0, VPN instance: vpn1): Start reconnection.
日志说明	当已协商支持对端设备LDP平滑重启的LDP会话down时，触发该日志。日志显示会话平滑重启过程的状态变化
处理建议	从LDP_SESSION_CHG 日志消息可以查看会话平滑重启的原因 当会话平滑重启状态显示为Reconnection failed时，根据会话失败原因检查接口状态，链路状态和其他相关配置，其他情况无需处理

46.3 LDP_SESSION_SP

日志内容	Session ([STRING], [STRING]): ([STRING]).
参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0 $2：VPN实例名。如果该会话属于公网，显示为public instance $3：会话保护状态，取值包括： • Hold up the session：保持会话，等待 Link hello 邻接关系恢复 • Session recovered successfully：Link hello 邻接关系恢复成功 • Session recovery failed：Link hello 邻接关系恢复失败
日志等级	5
举例	LDP/5/LDP_SESSION_SP: Session (22.22.22.2:0, VPN instance: vpn1): Hold up the session.
日志说明	当会话的最后一个Link hello邻接关系丢失时，触发该日志。日志显示会话保护过程的状态变化
处理建议	检查接口状态和链路状态

46.4 LDP_ADJACENCY_DOWN

日志内容	ADJ ([STRING], [STRING], [STRING]) is down [STRING]. ([STRING])

参数解释	$1：对等体的LDP ID。如果无法获得对等体的LDP ID，显示为0.0.0.0:0
	$2：VPN实例名。如果该会话属于公网，显示为public instance
	$3：接口名称。如果是Target Hello，该字段不显示
	$4：邻接体down的原因
	$5：邻接体相关信息：
	• Type：邻接体类型，取值包括：
	  ○ Link：表示 Link Hello 邻接关系
	  ○ Target：表示 Target Hello 邻接关系
	• SourceAddr：邻接体的源地址
	• DestinationAddr：邻接体的目的地址
	• TransportAddr：邻接体的传输地址
	• ADJUpTime：邻接体建立的持续时间，格式为 DD:HH:MM
	• HelloHoldTime：Hello 保持时间，单位为秒
	• HelloSentCount：本地发送 Hello 消息的总数
	• HelloRcvdCount：本地接收 Hello 消息的总数

日志等级	5
举例	LDP/5/LDP_ADJACENCY_DOWN: ADJ (10.200.0.60:0, public instance, GE2/0/1) is down (Hello timer expired). (Type=Link, SourceAddr=100.12.1.2, DestinationAddr=224.0.0.2, TransportAddr=22.2.2.2, ADJUpTime=0000:00:02, HelloHoldTime=15s, HelloSentCount=27, HelloRcvdCount=25)
日志说明	LDP邻接体状态为down的原因及相关信息
处理建议	当LDP邻接体状态是down时，根据邻接体down的原因检查接口状态、链路状态和其他相关配置 LDP邻接体down的原因包括： • VPN instance changed on interface：接口所属的 VPN 实例已更改 • LDP disabled on interface：接口上关闭 LDP 功能 • LDP auto-configure disabled on interface：接口上关闭 LDP 自动配置功能 • MPLS disabled on interface：接口上关闭 MPLS • interface not operational：接口不可用 • targeted peer deleted：手工删除 targeted peer • L2VPN disabled targeted peer：L2VPN 注销 targeted peer • TE tunnel disabled targeted peer：TE 隧道注销 targeted peer • session protection disabled targeted peer：会话保护注销 targeted peer • OSPF Remote LFA disabled targeted peer：OSPF Remote LFA 注销 targeted peer • IS-IS Remote LFA disabled targeted peer：ISIS Remote LFA 注销 targeted peer • process deactivated：LDP 进程降级 • LDP instance deleted：LDP 实例已删除 • hello hold timer expired：Hello 保持时间超时

	• no IPv6 transport address：没有 IPv6 传输地址

47 LIPC

本节包含 LIPC（Leopard Inter-process Communication，Leopard 版本进程间通信）模块的日志消息。

47.1 PORT_CHANGE

日志内容	STCP: Node where the listening port number [INTGER] (MDC: [INTGER] VRF: [INTGER]) resides changed from LIP [INTGER] to LIP [INTGER].
参数解释	$1：LIPC全局端口号 $2：LIPC全局端口号所在的MDC $3：LIPC全局端口号所在的VRF $4：LIPC全局端口号侦听位置变化之前所在的节点 $5：LIPC全局端口号侦听位置变化之后所在的节点
日志等级	5
举例	LIPC/5/PORT_CHANGE: STCP: Node where the listening port number 620 (MDC: 1 VRF: 1) resides changed from LIP 1 to LIP 3.
日志说明	STCP模块根据业务模块的请求，为作为服务端的业务模块分配全局端口号，业务模块侦听该端口号。通常情况下，业务模块只能在申请成功的节点上侦听该端口号，如果业务模块在其他节点上同时侦听该端口号时，输出该日志。STCP会将侦听端口从原节点迁移到新侦听的节点上
处理建议	无

48 LLDP

本节介绍 LLDP 模块输出的日志信息。

48.1 LLDP_CREATE_NEIGHBOR

日志内容	[STRING] agent neighbor created on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：邻居的设备号 $5：邻居的端口号
日志等级	6
举例	LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent neighbor created on port GigabitEthernet1/2/0/1 (IfIndex 599), neighbor's chassis ID is dc2d-cb66-ba00, port ID is GigabitEthernet1/2/0/2.
日志说明	端口收到新邻居发来的LLDP报文
处理建议	无

48.2 LLDP_DELETE_NEIGHBOR

日志内容	[STRING] agent neighbor deleted on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：邻居的设备号 $5：邻居的接口号
日志等级	6
举例	LLDP/6/LLDP_DELETE_NEIGHBOR: Nearest bridge agent neighbor deleted on port GigabitEthernet1/2/0/1 (IfIndex 599), neighbor's chassis ID is dc2d-cb66-ba00, port ID is GigabitEthernet1/2/0/2.
日志说明	当邻居被删除时，接口收到删除消息
处理建议	无

48.3 LLDP_LESS_THAN_NEIGHBOR_LIMIT

日志内容	The number of [STRING] agent neighbors maintained by port [STRING] (IfIndex [UINT32]) is less than [UINT32], and new neighbors can be added.
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：接口可以维护的最大邻居数
日志等级	6
举例	LLDP/6/LLDP_LESS_THAN_NEIGHBOR_LIMIT: The number of nearest bridge agent neighbors maintained by port GigabitEthernet1/2/0/1 (IfIndex 599) is less than 5, and new neighbors can be added.
日志说明	接口邻居数未达到最大值，还可以为接口增加新邻居
处理建议	无

48.4 LLDP_NEIGHBOR_AGE_OUT

日志内容	[STRING] agent neighbor aged out on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：邻居的设备号 $5：邻居的接口号
日志等级	5
举例	LLDP/5/LLDP_NEIGHBOR_AGE_OUT: Nearest bridge agent neighbor aged out on port GigabitEthernet1/2/0/1 (IfIndex599), neighbor's chassis ID is dc2d-cb66-ba00, port ID is GigabitEthernet1/2/0/2.
日志说明	当接口在一段时间内没有收到邻居发来的LLDP报文时，打印本信息
处理建议	检查链路状态，或者检查对端LLDP的接收和发送状态

48.5 LLDP_PVID_INCONSISTENT

日志内容	PVID mismatch discovered on [STRING] (PVID [UINT32]), with [STRING] [STRING] (PVID [STRING]).
参数解释	$1：接口名称 $2：VLAN ID $3：系统名称 $4：接口名称 $5：VLAN ID
日志等级	5
举例	LLDP/5/LLDP_PVID_INCONSISTENT: MDC=1; PVID mismatch discovered on GigabitEthernet1/2/0/1 (PVID 1), with Ten-GigabitEthernet0/2/7 (PVID 500).
日志说明	当邻居的PVID信息与接口本地的PVID不同时，打印本信息
处理建议	修改邻居两端的PVID，使其一致

48.6 LLDP_REACH_NEIGHBOR_LIMIT

日志内容	The number of [STRING] agent neighbors maintained by the port [STRING] (IfIndex [UINT32]) has reached [UINT32], and no more neighbors can be added.
参数解释	$1：代理类型 $2：接口名称 $3：接口索引 $4：接口可以维护的最大邻居数
日志等级	5
举例	LLDP/5/LLDP_REACH_NEIGHBOR_LIMIT: The number of nearest bridge agent neighbors maintained by the port GigabitEthernet1/2/0/1 (IfIndex 599) has reached 5, and no more neighbors can be added.
日志说明	当邻居数达到最大值的接口收到LLDP报文时，打印本信息
处理建议	无

49 LOAD

本节介绍 LOAD 模块输出的日志信息。

49.1 BOARD_LOADING

日志内容	Board in chassis [INT32] slot [INT32] is loading software images.
参数解释	$1：chassis编号 $2：slot编号
日志等级	4
举例	LOAD/4/BOARD_LOADING: Board in chassis 1 slot 5 is loading software images.
日志说明	单板启动过程中，加载启动软件包
处理建议	无

49.2 LOAD_FAILED

日志内容	Board in chassis [INT32] slot [INT32] failed to load software images.
参数解释	$1：chassis编号 $2：slot编号
日志等级	3
举例	LOAD/3/LOAD_FAILED: Board in chassis 1 slot 5 failed to load software images.
日志说明	单板在启动过程中，加载启动软件包失败
处理建议	1. 使用 **display boot-loader** 命令查看单板使用的下次启动软件包 2. 使用 **dir** 命令查看启动软件包是否存在。如果不存在或者损坏，请重新获取启动软件包或者设置其它软件包作为该单板的下次启动软件包 3. 如果仍不能解决，请联系工程师

49.3 LOAD_FINISHED

日志内容	Board in chassis [INT32] slot [INT32] has finished loading software images.
参数解释	$1：chassis编号 $2：slot编号
日志等级	5
举例	LOAD/5/LOAD_FINISHED: Board in chassis 1 slot 5 has finished loading software images.
日志说明	单板完成文件加载
处理建议	无

50 LOCAL

本节介绍 LOCAL 模块输出的日志信息。

50.1 LOCAL_CMDDENY

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for visiting user [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：本地用户名
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for visiting user admin.
日志说明	因操作者访问权限不足，执行进入本地用户视图的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for adding user [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：本地用户名
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for adding user admin.
日志说明	因操作者访问权限不足，执行添加本地用户的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for deleting user [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：本地用户名
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for deleting user admin.
日志说明	因操作者访问权限不足，执行删除本地用户的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for configuring user [STRING]'s [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：本地用户名 $5：配置的用户属性项，包括以下取值： • password：密码 • state：用户状态 • service-type：服务类型 • authorization-attribute：授权属性 • bind-attribute：绑定属性 • group：用户组 • access-limit：最大用户数
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for configuring user admin's access-limit.
日志说明	因操作者访问权限不足，执行配置本地用户属性的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for visiting group [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：用户组名称
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for visiting group system.
日志说明	因操作者访问权限不足，执行进入用户组的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for adding group [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：用户组名称
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for adding group system.
日志说明	因操作者访问权限不足，执行添加用户组的命令失败
处理建议	无

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Permission denied for deleting group [STRING].
参数解释	$1：用户线名称（如果不涉及该参数，则显示为**） $2：操作者的IP地址（如果不涉及该参数，则显示为**） $3：操作者的用户名（如果不涉及该参数，则显示为**） $4：用户组名称
日志等级	5
举例	LOCAL/5/LOCAL_CMDDENY: -Line=vty0-IPAddr=111.8.10.111-User=opt; Permission denied for deleting group system.
日志说明	因操作者访问权限不足，执行删除用户组的命令失败
处理建议	无

51 LOGIN

本节介绍 LOGIN（登录管理）模块输出的日志信息。

51.1 LOGIN_AUTHENTICATION_FAILED

日志内容	Authentication failed for [STRING] from [STRING] because of [STRING].
参数解释	$1：用户名 $2：用户线名或IP地址 $3：失败原因： ○ no AAA response from any server during the authentication：AAA 服务器无响应 ○ invalid username or password or service type mismatch：用户名、密码错误或服务类型不匹配 ○ configuration error or other errors：配置错误或其它错误
日志等级	5
举例	LOGIN/5/LOGIN_AUTHENTICATION_FAILED: Authentication failed for Usera from console0 because of no AAA response from any server during the authentication.
日志说明	用户登录时认证失败
处理建议	请根据错误原因进行相应的处理

51.2 LOGIN_FAILED

日志内容	[STRING] failed to log in from [STRING].
参数解释	$1：用户名 $2：用户线名和IP地址
日志等级	5
举例	LOGIN/5/LOGIN_FAILED: TTY failed to log in from console0. LOGIN/5/LOGIN_FAILED: usera failed to log in from 192.168.11.22.
日志说明	用户登录失败
处理建议	无

51.3 LOGIN_INVALID_USERNAME_PWD

日志内容	Invalid username or password from [STRING].
参数解释	$1：用户线名和IP地址
日志等级	5
举例	LOGIN/5/LOGIN_INVALID_USERNAME_PWD: Invalid username or password from console0. LOGIN/5/LOGIN_INVALID_USERNAME_PWD: Invalid username or password from 192.168.11.22.
日志说明	用户输入无效的用户名或密码
处理建议	无

52 LS

本节包含本地服务器日志信息。

52.1 LOCALSVR_PROMPTED_CHANGE_PWD

日志内容	Please change the password of [STRING] [STRING], because [STRING].
参数解释	$1：密码类型 ○ device management user：设备管理用户 ○ user line：用户线 ○ user line class：用户线类 $2：用户名/用户线编号/用户线类型 $3：提醒修改密码原因 ○ the current password is a weak-password：密码是弱密码 ○ the current password is the default password：密码是缺省密码 ○ it is the first login of the current user or the password had been reset：首次登录或者密码已被重置 ○ the password had expired：密码已经老化
日志等级	6
举例	LOCALSVR/6/LOCALSVR_PROMPTED_CHANGE_PWD: Please change the password of device management user hhh, because the current password is a weak password.
日志说明	如果用户使用不符合密码策略的密码登录设备，系统会在该用户登录后每隔24小时输出一条日志信息提醒该用户修改当前密码
处理建议	根据用户登录时采用的认证方式不同，处理建议如下： • 认证方式为 scheme 时，请修改用户的本地密码 • 认证方式为 password 时，请修改用户所在用户线/用户线类的认证密码

52.2 LS_ADD_USER_TO_GROUP

日志内容	Admin [STRING] added user [STRING] to group [STRING].
参数解释	$1：管理员名 $2：用户名 $3：用户组名
日志等级	4
举例	LS/4/LS_ADD_USER_TO_GROUP: Admin admin added user user1 to group group1.
日志说明	管理员添加一个用户到一个用户组
处理建议	无

52.3 LS_AUTHEN_FAILURE

日志内容	User [STRING] from [STRING] failed authentication. [STRING]
参数解释	$1：用户名 $2：IP地址 $3：失败原因 • 用户没有找到 • 密码认证失败 • 用户未上线 • 接入类型不匹配 • 绑定属性失败 • 用户在黑名单
日志等级	5
举例	LS/5/LS_AUTHEN_FAILURE: User cwf@system from 192.168.0.22 failed authentication. “User not found.”
日志说明	本地服务器拒绝了一个用户的认证请求
处理建议	无

52.4 LS_AUTHEN_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
参数解释	$1：用户名 $2：IP地址
日志等级	6
举例	LS/6/LS_AUTHEN_SUCCESS: User cwf@system from 192.168.0.22 was authenticated successfully.
日志说明	本地服务器接受了一个用户的认证请求
处理建议	无

52.5 LS_DEL_USER_FROM_GROUP

日志内容	Admin [STRING] delete user [STRING] from group [STRING].
参数解释	$1：管理员名 $2：用户名 $3：用户组名
日志等级	4
举例	LS/4/LS_DEL_USER_FROM_GROUP: Admin admin delete user user1 from group group1.
日志说明	管理员将用户从用户组里删除
处理建议	无

52.6 LS_DELETE_PASSWORD_FAIL

日志内容	Failed to delete the password for user [STRING].
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_DELETE_PASSWORD_FAIL: Failed to delete the password for user abcd.
日志说明	删除用户密码失败
处理建议	检查文件系统

52.7 LS_PWD_ADDBLACKLIST

日志内容	User [STRING] was added to the blacklist due to multiple login failures, [STRING].
参数解释	$1：用户名 $2：结果 • 但是可以做其他的尝试 • 被永久阻塞 • 被临时阻塞指定时间（单位：分钟）
日志等级	4
举例	LS/4/LS_PWD_ADDBLACKLIST: user1 was added to the blacklist due to multiple login failures, but could make other attempts.
日志说明	用户多次登录失败后被加入了黑名单
处理建议	检查用户的密码

52.8 LS_PWD_CHGPWD_FOR_AGEDOUT

日志内容	User [STRING] changed the password because it was expired.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_AGEDOUT: aaa changed the password because it was expired.
日志说明	用户由于密码已过期而修改了密码
处理建议	无

52.9 LS_PWD_CHGPWD_FOR_AGEOUT

日志内容	User [STRING] changed the password because it was about to expire.
参数解释	$1：用户名 $2：老化时间
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_AGEOUT: aaa changed the password because it was about to expire.
日志说明	用户由于密码即将过期而修改了密码
处理建议	无

52.10 LS_PWD_CHGPWD_FOR_COMPOSITION

日志内容	User [STRING] changed the password because it had an invalid composition.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_COMPOSITION: aaa changed the password because it had an invalid composition.
日志说明	用户由于密码组合错误而修改了密码
处理建议	无

52.11 LS_PWD_CHGPWD_FOR_FIRSTLOGIN

日志内容	User [STRING] changed the password at the first login.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_FIRSTLOGIN: aaa changed the password at the first login.
日志说明	用户首次登录修改了密码
处理建议	无

52.12 LS_PWD_CHGPWD_FOR_LENGTH

日志内容	User [STRING] changed the password because it was too short.
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_PWD_CHGPWD_FOR_LENGTH: aaa changed the password because it was too short.
日志说明	用户因为密码太短而修改了密码
处理建议	无

52.13 LS_PWD_FAILED2WRITEPASS2FILE

日志内容	Failed to write the password records to file.
参数解释	无
日志等级	4
举例	LS/4/LS_PWD_FAILED2WRITEPASS2FILE: Failed to write the password records to file.
日志说明	把密码记录写到文件失败
处理建议	无

52.14 LS_PWD_MODIFY_FAIL

日志内容	Admin [STRING] from [STRING] could not modify the password for user [STRING], because [STRING].
参数解释	$1：管理员名 $2：IP地址 $3：用户名 $4：原因： • 密码不匹配 • 不能写密码历史 • 密码无法验证
日志等级	4
举例	LS/4/LS_PWD_MODIFY_FAIL: Admin admin from 1.1.1.1 could not modify the password for user user1, because passwords do not match.
日志说明	修改用户密码失败
处理建议	无

52.15 LS_PWD_MODIFY_SUCCESS

日志内容	Admin [STRING] from [STRING] modify the password for user [STRING] successfully.
参数解释	$1：管理员名 $2：IP地址 $3：用户名
日志等级	6
举例	LS/6/LS_PWD_MODIFY_SUCCESS: Admin admin from 1.1.1.1 modify the password for user abc successfully.
日志说明	管理员成功修改了用户密码
处理建议	无

52.16 LS_REAUTHEN_FAILURE

日志内容	User [STRING] from [STRING] failed reauthentication.
参数解释	$1：用户名 $2：IP地址
日志等级	5
举例	LS/5/LS_REAUTHEN_FAILURE: User abcd from 1.1.1.1 failed reauthentication.
日志说明	用户再次认证失败
处理建议	检查旧密码

52.17 LS_UPDATE_PASSWORD_FAIL

日志内容	Failed to update the password for user [STRING].
参数解释	$1：用户名
日志等级	4
举例	LS/4/LS_UPDATE_PASSWORD_FAIL: Failed to update the password for user abc.
日志说明	为用户更新密码失败
处理建议	检查文件系统

52.18 LS_USER_CANCEL

日志内容	User [STRING] from [STRING] cancelled inputting the password.
参数解释	$1：用户名 $2：IP地址
日志等级	5
举例	LS/5/LS_USER_CANCEL: User 1 from 1.1.1.1 cancelled inputting the password.
日志说明	用户取消输入密码或者没有在90秒内输入密码
处理建议	无

52.19 LS_USER_PASSWORD_EXPIRE

日志内容	User [STRING]'s login idle timer timed out.
参数解释	$1：用户名
日志等级	5
举例	LS/5/LS_USER_PASSWORD_EXPIRE: User 1's login idle timer timed out.
日志说明	用户登录空闲时间超时
处理建议	无

52.20 LS_USER_ROLE_CHANGE

日志内容	Admin [STRING] [STRING] the user role [STRING] for [STRING].
参数解释	$1：管理员名 $2：添加/删除 $3：用户角色 $4：用户名
日志等级	4
举例	LS/4/LS_USER_ROLE_CHANGE: Admin admin add user role network-admin for user abcd.
日志说明	管理员修改了用户的用户角色
处理建议	无

53 LSM

本节介绍 LSM 模块输出的日志信息。

53.1 LSM_SR_LABEL_CONFLICT

日志内容	Protocol [STRING] assigned label ([STRING]) for prefix ([STRING]), which already has label ([STRING]) assigned by protocol [STRING].
参数解释	$1：路由协议1 $2：标签值1 $3：前缀地址及掩码 $4：标签值2 $3：路由协议2
日志等级	5
举例	LSM/5/LSM_SR_LABEL_CONFLICT: Protocol ISIS assigned label (16000) to prefix (5.5.5.5/32), which already has label (17000) assigned by protocol OSPF.
日志说明	在同一SR节点上不同路由协议为同一前缀地址分配不同的标签
处理建议	• 不同路由协议为同一前缀地址分配相同标签 • 在 SR 节点上删除未被使用的路由协议进程，保证仅一个路由协议为前缀地址分配标签

53.2 LSM_SR_PREFIX_CONFLICT

日志内容	Label ([STRING]) for prefix ([STRING]) has been used by prefix ([STRING]).
参数解释	$1：标签值 $2：前缀地址1及掩码 $3：前缀地址2及掩码
日志等级	5
举例	LSM/5/LSM_SR_PREFIX_CONFLICT: The label(16700) for prefix(8.8.8.8/32) has been used by prefix(5.5.5.5/32).
日志说明	前缀地址标签分配冲突，同一个标签被分配给两个不同的前缀地址
处理建议	给新前缀地址分配不同标签

54 LSPV

本节介绍 LSP 验证模块输出的日志信息。

54.1 LSPV_PING_STATIS_INFO

日志内容	Ping statistics for [STRING]: [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packets loss, round-trip min/avg/max = [UINT32]/[UINT32]/[UINT32] ms.
参数解释	$1：FEC $2：发出的请求数 $3：收到的应答数 $4：未收到应答的次数占发送请求总数的比例 $5：最小往返延迟时间 $6：平均往返延迟时间 $7：最大往返延迟时间
日志等级	6
举例	LSPV/6/LSPV_PING_STATIS_INFO: Ping statistics for FEC 192.168.1.1/32: 5 packets transmitted, 5 packets received, 0.0% packets loss, round-trip min/avg/max = 1/2/5 ms.
日志说明	执行**ping mpls**命令，触发该日志。日志显示ping的统计信息
处理建议	如果没有收到应答报文，检测到LSP隧道或者PW的连通性

55 MAC

本节介绍 MAC 模块输出的日志信息。

55.1 MAC_TABLE_FULL_GLOBAL

日志内容	The number of MAC address entries exceeded the maximum number [UINT32].
参数解释	$1：最大MAC地址数量
日志等级	4
举例	MAC/4/MAC_TABLE_FULL_GLOBAL: The number of MAC address entries exceeded the maximum number 1024.
日志说明	全局MAC地址表中的表项数量超过了允许的最大数量
处理建议	无

55.2 MAC_TABLE_FULL_PORT

日志内容	The number of MAC address entries exceeded the maximum number [UINT32] for interface [STRING].
参数解释	$1：最大MAC地址数量 $2：接口名称
日志等级	4
举例	MAC/4/MAC_TABLE_FULL_PORT: The number of MAC address entries exceeded the maximum number 1024 for interface GigabitEthernet1/2/0/2.
日志说明	接口对应的MAC地址表中的表项数量超过了允许的最大数量
处理建议	无

55.3 MAC_TABLE_FULL_VLAN

日志内容	The number of MAC address entries exceeded the maximum number [UINT32] in VLAN [UINT32].
参数解释	$1：最大MAC地址数量 $2：VLAN ID
日志等级	4
举例	MAC/4/MAC_TABLE_FULL_VLAN: The number of MAC address entries exceeded the maximum number 1024 in VLAN 2.
日志说明	VLAN对应的MAC地址表中的表项数量超过了允许的最大数量
处理建议	无

56 MBFD

本节介绍 MPLS BFD 模块输出的日志信息。

56.1 MBFD_TRACEROUTE_FAILURE

日志内容	[STRING] is failed. ([STRING].)
参数解释	$1：LSP信息 $2：LSP失败原因
日志等级	5
举例	MBFD/5/MBFD_TRACEROUTE_FAILURE: LSP (LDP IPv4: 22.22.2.2/32, nexthop: 20.20.20.2) is failed. (Replying router has no mapping for the FEC.) MBFD/5/MBFD_TRACEROUTE_FAILURE: TE tunnel (RSVP IPv4: Tunnel1) is failed. (No label entry.)
日志说明	通过周期性Traceroute功能检测LSP或MPLS TE隧道时，如果收到带有不合法返回代码的应答，则打印本日志信息，说明LSP或者MPLS TE隧道出现了故障
处理建议	检查LSP或者MPLS TE隧道的配置情况

57 MBUF

本节介绍 MBUF 模块输出的日志信息。

57.1 MBUF_DATA_BLOCK_CREATE_FAIL

日志内容	Failed to create an MBUF data block because of insufficient memory. Failure count: [UINT32].
参数解释	$1：失败次数
日志等级	2
举例	MBUF/2/MBUF_DATA_BLOCK_CREATE_FAIL: Failed to create an MBUF data block because of insufficient memory. Failure count: 128.
日志说明	当申请MBUF数据块失败时，输出该日志。为避免该日志输出过于频繁，本次申请MBUF数据块失败距上次申请MBUF数据块失败间隔大于等于一分钟时，才会输出该日志
处理建议	1. 在 Probe 视图下执行 **display system internal kernel memory pool | include mbuf** 命令查询已申请的 MBUF 数据块的数量 2. 在系统视图下执行 **display memory** 命令查询系统内存总量 3. 将“已申请的 MBUF 数据块的数量”和“系统内存总量”比较，判断是否已申请的 MBUF 数据块过多导致申请失败 • 如果不是，则通过其他内存管理命令查询出占用内存较多的模块 • 如果是，则继续通过 Probe 视图下的 **display system internal mbuf socket statistics** 命令查询 Socket 申请的 MBUF 数据块的数量，对比已申请的 MBUF 数据块的数量，判断是否某个进程缓存在 Socket 缓冲区中的 MBUF 数据块过多 o 如果是，则进一步分析进程不能及时释放 Socket 缓冲区中的 MBUF 数据块的原因 o 如果不是，则需要通过其他手段找出申请大量 MBUF 数据块的真正原因

58 MDC

本节介绍 MDC（Multitenant Device Context，多租户设备环境）模块输出的日志信息。

58.1 MDC_CREATE

日志内容	MDC [UINT16] was created.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_CREATE: MDC 2 was created.
日志说明	MDC成功创建
处理建议	无

58.2 MDC_CREATE_ERR

日志内容	Failed to create MDC [UINT16] for insufficient resources.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_CREATE_ERR: -Slot=1; Failed to create MDC 2 for insufficient resources.
日志说明	备用主控板启动时会从主用主控板获取所有已创建的MDC的信息，并在备用主控板创建同样的MDC。如果备用主控板因为资源限制无法创建该MDC，则输出此日志信息。MDC进驻备用主控板失败，无法在该备用主控板上提供服务
处理建议	1. 使用 **display mdc resource** 命令查询新插入的备用主控板的 CPU、内存空间和磁盘空间 2. 增加备用主控板的内存或减少磁盘使用，以保证新 MDC 可创建 3. 使用 **undo mdc** 命令删除该 MDC，或者换一块资源足够的主控板作为备用主控板

58.3 MDC_DELETE

日志内容	MDC [UINT16] was deleted.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_DELETE: MDC 2 was deleted.
日志说明	MDC成功删除
处理建议	无

58.4 MDC_EVENT_ERROR

日志内容	Function [STRING] returned [STRING] when handling event [UINT32] on virtual OS [UINT32]. Reason: [STRING].
参数解释	$1：函数的地址 $2：函数的处理结果 $3：事件的编号 $4：MDC的编号 $5：函数处理结果出现的原因，取值为： ○ Not enough resources available for this MDC：资源不足导致处理失败 ○ Not enough memory space to complete the operation：内存不足导致处理失败 ○ Other reason：其他原因导致的处理失败
日志等级	4
举例	MDC/4/MDC_EVENT_ERROR: -MDC=1; Function 0xfacd26b1 returned 0x40010001 when handling event 1 on virtual OS 2. Reason: Other reason.
日志说明	MDC相关事件处理失败
处理建议	联系工程师分析解决

58.5 MDC_KERNEL_EVENT_TOOLONG

日志内容	[STRING] [UINT32] kernel event in sequence [STRING] function [STRING] failed to finish within [UINT32] minutes.
参数解释	$1：取值为MDC或Context $2：MDC或Context的编号 $3：内核事件的阶段 $4：内核事件阶段对应的函数的地址 $5：所用时间
日志等级	4
举例	MDC/4/MDC_KERNEL_EVENT_TOOLONG: -slot=1; MDC 2 kernel event in sequence 0x4fe5 function 0xff245e failed to finish within 15 minutes.
日志说明	某内核事件在长时间内未完成
处理建议	**1.** 重启单板，尝试恢复 **2.** 联系工程师分析解决

58.6 MDC_LICENSE_EXPIRE

日志内容	The MDC feature's license will expire in [UINT32] days.
参数解释	$1：天数，取值范围为1到30天
日志等级	5
举例	MDC/5/MDC_LICENSE_EXPIRE: The MDC feature’s license will expire in 5 days.
日志说明	MDC License将在指定天数后失效
处理建议	安装新的License

58.7 MDC_NO_FORMAL_LICENSE

日志内容	The feature MDC has no formal license.
参数解释	无
日志等级	5
举例	MDC/5/MDC_NO_FORMAL_LICENSE: The feature MDC has no formal license.
日志说明	备用主控板变为主用主控板了，但是新主用主控板没有安装MDC License。系统会给新主用主控板一个MDC试用期。试用期过期，如果用户还没有给新主用主控板安装License，则不能继续使用MDC特性
处理建议	安装正式MDC License

58.8 MDC_NO_LICENSE_EXIT

日志内容	The MDC feature is being disabled, because it has no license.
参数解释	无
日志等级	5
举例	MDC/5/MDC_NO_LICENSE_EXIT: The MDC feature is being disabled, because it has no license.
日志说明	MDC特性被禁用，因为MDC License过期或者被卸载了
处理建议	安装MDC License

58.9 MDC_OFFLINE

日志内容	MDC [UINT16] is offline now.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_OFFLINE: MDC 2 is offline now.
日志说明	MDC停用了
处理建议	无

58.10 MDC_ONLINE

日志内容	MDC [UINT16] is online now.
参数解释	$1：MDC的编号
日志等级	5
举例	MDC/5/MDC_ONLINE: MDC 2 is online now.
日志说明	MDC启用了
处理建议	无

58.11 MDC_STATE_CHANGE

日志内容	MDC [UINT16] status changed to [STRING].
参数解释	$1：MDC的编号 $2：MDC的状态： ○ updating 表示正在给 MDC 分配接口板，即对 MDC 执行 **location** 命令 ○ stopping 表示 MDC 正在停止，即 MDC 正在执行 **undo mdc start** 命令 ○ inactive 表示 MDC 处于未启动状态 ○ starting 表示 MDC 正在启动中，即对 MDC 正在执行 **mdc start** 命令 ○ active 表示 MDC 正常运行
日志等级	5
举例	MDC/5/MDC_STATE_CHANGE: MDC 2 state changed to active.
日志说明	MDC状态发生了变化
处理建议	无

59 MFIB

本节介绍组播转发模块输出的日志信息。

59.1 MFIB_CFG_NOT_SUPPORT

日志内容	Failed to apply [STRING] configuration because the operation is not supported.
参数解释	$1：组播模块的命令行
日志等级	4
举例	MFIB/4/MFIB_OIF_NOT_SUPPORT: Failed to apply multicast rpf-fail-pkt flooding configuration because the operation is not supported.
日志说明	因硬件不支持对应配置而导致配置失败
处理建议	无

59.2 MFIB_MTI_NO_ENOUGH_RESOURCE

日志内容	Failed to create [STRING] because of insufficient resources.
参数解释	$1：MTunnel隧道的名称
日志等级	4
举例	MFIB/4/MFIB_MTI_NO_ENOUGH_RESOURCE: Failed to create MTunnel1 because of insufficient resources.
日志说明	因硬件资源不足而导致MTunnel隧道创建失败
处理建议	使用**undo group** *group-address* **source** *source-address*命令删除暂时不用的组播隧道，释放组播隧道资源

59.3 MFIB_OIF_NOT_SUPPORT

日志内容	Failed to add oif to entry ([[STRING], [STRING]) because some oifs are not supported.
参数解释	$1：组播表项源地址 $2：组播表项组地址
日志等级	4
举例	MFIB/4/MFIB_OIF_NOT_SUPPORT: Failed to add oif to entry (1.1.1.1, 225.0.0.1) because some oifs are not supported.
日志说明	硬件不支持向组播表项添加某些出接口
处理建议	检查生成该日志的板卡上各接口是否配置了如下命令： • **igmp static-group** *group-address* [**source** *source-address*] { **dot1q vid** *vlan-list* | **dot1q vid** *vlan-id* **second-dot1q** *vlan-list* } • **igmp user-vlan-aggregation dot1q vid** *vlan-id* [**second-dot1q** *vlan-id*] • **mld static-group** *ipv6-group-address* [**source** *ipv6-source-address*] { **dot1q vid** *vlan-list* | **dot1q vid** *vlan-id* **second-dot1q** *vlan-list* } • **mld user-vlan-aggregation dot1q vid** *vlan-id* [**second-dot1q** *vlan-id*] 如果配置了上述命令，则删除相关配置

60 MGROUP

本节主要介绍与镜像组相关的日志消息。

60.1 MGROUP_APPLY_SAMPLER_FAIL

日志内容	Failed to apply the sampler for mirroring group [UINT16], because the sampler resources are insufficient.
参数解释	$1：镜像组编号
日志等级	3
举例	MGROUP/3/MGROUP_APPLY_SAMPLER_FAIL: Failed to apply the sampler for mirroring group 1, because the sampler resources are insufficient.
日志说明	采样器资源不足时，新镜像组引用采样器失败
处理建议	无

60.2 MGROUP_RESTORE_CPUCFG_FAIL

日志内容	Failed to restore configuration for mirroring CPU of [STRING] in mirroring group [UINT16], because [STRING]
参数解释	$1：单板所在的槽位号 $2：镜像组编号 $3：恢复源CPU配置失败的原因
日志等级	3
举例	MGROUP/3/MGROUP_RESTORE_CPUCFG_FAIL: Failed to restore configuration for mirroring CPU of chassis 1 slot 2 in mirroring group 1, because the type of the monitor port in the mirroring group is not supported.
日志说明	当单板上的CPU用作镜像组的源CPU时，在单板拔出阶段，配置发生变化，单板再插入时，可能会引起镜像组源CPU的配置恢复失败
处理建议	排查配置恢复失败的原因，如果是由于系统不支持变化的配置，删除不支持的配置，重新配置镜像组的源CPU

60.3 MGROUP_RESTORE_IFCFG_FAIL

日志内容	Failed to restore configuration for interface [STRING] in mirroring group [UINT16], because [STRING]
参数解释	$1：接口名称 $2：镜像组编号 $3：恢复源端口配置失败的原因
日志等级	3
举例	MGROUP/3/MGROUP_RESTORE_IFCFG_FAIL: Failed to restore configuration for interface Ethernet1/2/0/2 in mirroring group 1, because the type of the monitor port in the mirroring group is not supported.
日志说明	当单板上的接口用作镜像组的源端口时，在单板拔出阶段，配置发生变化，单板再插入时，可能会引起镜像组源端口的配置恢复失败
处理建议	排查配置恢复失败的原因，如果是由于系统不支持变化的配置，删除不支持的配置，重新配置镜像组的源端口

60.4 MGROUP_SYNC_CFG_FAIL

日志内容	Failed to restore configuration for mirroring group [UINT16] in [STRING], because [STRING]
参数解释	$1：镜像组编号 $2：单板所在的槽位号 $3：恢复镜像组配置失败的原因
日志等级	3
举例	MGROUP/3/MGROUP_SYNC_CFG_FAIL: Failed to restore configuration for mirroring group 1 in chassis 1 slot 2, because monitor resources are insufficient.
日志说明	当向单板同步完整的镜像组配置时，由于单板资源不足，引起配置恢复失败
处理建议	删除配置恢复失败的镜像组

61 MPLS

本节介绍 MPLS 模块输出的日志信息。

61.1 MPLS_HARD_RESOURCE_NOENOUGH

日志内容	No enough hardware resource for MPLS.
参数解释	无
日志等级	4
举例	MPLS/4/MPLS_HARD_RESOURCE_NOENOUGH: No enough hardware resource for MPLS.
日志说明	MPLS硬件资源不足
处理建议	请检查是否生成了当前业务不需要的大量LSP，是则配置获调整标签分发协议的LSP触发策略、标签通告策略、标签接受策略，以过滤掉不需要的LSP

61.2 MPLS_HARD_RESOURCE_RESTORE

日志内容	Hardware resources for MPLS are restored.
参数解释	无
日志等级	6
举例	MPLS/6/MPLS_HARD_RESOURCE_RESTORE: Hardware resources for MPLS are restored.
日志说明	MPLS硬件资源恢复
处理建议	无

62 MSDP

本节介绍 MSDP 模块输出的日志信息。

62.1 MSDP_PEER_START

日志内容	Started a session with peer [STRING].
参数解释	$1：MSDP对等体的IP地址
日志等级	5
举例	MSDP/5/MSDP_PEER_START: Started a session with peer 192.168.0.1.
日志说明	MSDP对等体会话状态变为established
处理建议	无

62.2 MSDP_PEER_START

日志内容	NSR start a session with peer [STRING].
参数解释	$1：MSDP对等体的IP地址
日志等级	5
举例	MSDP/5/MSDP_PEER_START: NSR started a session with peer 192.168.0.1.
日志说明	MSDP对等体会话状态通过NSR恢复为established
处理建议	无

62.3 MSDP_PEER_CLOSE

日志内容	Stopped a session with peer [STRING].
参数解释	$1：MSDP对等体的IP地址
日志等级	5
举例	MSDP/5/MSDP_PEER_CLOSE: Stopped a session with peer 192.168.0.1.
日志说明	MSDP对等体会话状态从established变为disabled
处理建议	检查MSDP配置是否错误以及检查网络是否发生故障

62.4 MSDP_SA_LIMIT

日志内容	SA from peer [STRING] for ([STRING], [STRING]) exceeded sa-limit of [ULONG].
参数解释	$1：MSDP对等体的IP地址 $2：SA报文中携带的组播源地址 $3：SA报文中携带的组播组地址 $4：指定MSDP对等体可缓存的（S，G）表项的最大值
日志等级	5
举例	MSDP/5/MSDP_SA_LIMIT: SA from peer 192.168.0.1 for (1.1.1.1, 225.0.0.1) exceeded sa-limit of 1000.
日志说明	已缓存的SA报文中的（S，G）表项数量已经达到设置的允许缓存的最大值
处理建议	通过**peer sa-cache-maximum**命令将可缓存的（S，G）表项的最大数量调大或调整组网以减少（S，G）表项数目

63 MTLK

本节介绍 Monitor Link 模块输出的日志信息。

63.1 MTLK_UPLINK_STATUS_CHANGE

日志内容	The uplink of monitor link group [UINT32] is [STRING].
参数解释	$1：Monitor Link组ID $2：Monitor Link组状态 ○ down：故障 ○ up：正常
日志等级	6
举例	MTLK/6/MTLK_UPLINK_STATUS_CHANGE: The uplink of monitor link group 1 is up.
日志说明	Monitor Link组上行链路up或down
处理建议	检查故障链路

64 MTP

本节介绍接口 MTP 模块输出的日志信息。

64.1 MTP_PING_INFO

日志内容	Ping information, (Base: [STRING]), (Result: [STRING]).
参数解释	$1：Ping的基本信息，包括Ping的时间、目的IP地址、VRF索引、协议模块信息、发送Ping包的数量。协议模块信息包含模块名和实例名，若无实例名，则为空 $2：Ping的结果信息，包括发送Ping包成功数以及各Ping包结果信息。Ping包结果信息包含Ping包长度、Ping包发送顺序以及结果
日志等级	6
举例	MTP/6/MTP_PING_INFO: Ping information, (Base: Time = 09:39:18, Destination IP = 10.11.1.1, VrfIndex = 0, Protocol Module = BGP (default), Packet Number = 9), (Result: Success = 9, Length 100 ping 1 success, Length 100 ping 2 success, Length 100 ping 3 success, Length 1000 ping 4 success, Length 1000 ping 5 success, Length 1000 ping 6 success, Length 4000 ping 7 success, Length 4000 ping 8 success, Length 4000 ping 9 success).
日志说明	开启MTP功能后，当与邻居间的路由协议报文超时时，设备会向超时的邻居发起Ping操作并记录Ping结果
处理建议	根据Ping结果信息，检查相应链路是否存在故障

64.2 MTP_TRACERT_INFO

日志内容	Tracert information, (Base: [STRING]), (Result: [STRING]).
参数解释	$1：Tracert的基本信息，包括Tracert的时间、目的IP地址、VRF索引、最大跳数、每跳发送探测报文数、协议模块信息。协议模块信息包含模块名和实例名，若无实例名，则为空 $2：Tracert的结果信息，包括每一跳探测的回应IP地址、回应IP地址所属AS号（若不存在则不显示）以及探测成功的次数。若该跳探测无回应，则不显示该跳结果信息
日志等级	6
举例	MTP/6/MTP_TRACERT_INFO: Tracert information, (Base: Time = 10:39:18, Destination IP = 10.11.1.1, VrfIndex = 0, MaxHop = 30, Packet Number = 3, Protocol Module = BGP (default)), (Result: TTL 1 Response IP = 10.2.1.1 Success = 3, TTL 2 Response IP = 10.11.1.1 [AS 100] Success = 3).
日志说明	开启MTP功能后，当与邻居间的路由协议报文超时时，设备会向超时的邻居发起Tracert操作并记录Tracert结果
处理建议	根据Tracert结果信息，检查相应链路是否存在故障

65 NAT

本节介绍 NAT 模块输出的日志信息。

65.1 EIM_MODE_PORT_USAGE_ALARM

日志内容	[STRING] Port usage reaches [STRING]%; SrcIPAddr=[IPADDR]; VPNInstance=[STRING]; NATIPAddr=[IPADDR]; ConnectCount=[UINT16].
参数解释	$1：协议类型 $2：百分比 $3：源IP地址 $4：源VPN名称 $5：转换后的源IP地址 $6：分配端口数
日志等级	6
举例	NAT/6/EIM_MODE_PORT_USAGE_ALARM: UDP Port usage reaches 40%; SrcIPAddr=1.1.1.211; VPNInstance=-; NATIPAddr=198.1.1.16; ConnectCount=40.
日志说明	当NAT端口块中端口的使用率大于或等于通过命令**nat log port-block port-usage threshold**配置的告警阈值，且PAT方式出方向动态地址转换模式为Endpoint-Independent Mapping时，才会发送该日志
处理建议	无

65.2 IP_EXHAUST_ALARM

日志内容	The IP addresses in NAT IP pool [STRING] ran out.
参数解释	$1：地址池名称
日志等级	4
举例	NAT/6/IP_EXHAUST_ALARM: The IP addresses in NAT IP pool1 ran out.
日志说明	NAT地址池内地址资源耗尽时会发送该日志
处理建议	无

65.3 IP_EXHAUST_ALARM_RECOVER

日志内容	IP addresses in NAT IP pool [STRING] became available.
参数解释	$1：地址池名称
日志等级	4
举例	NAT/6/IP_EXHAUST_ALARM_RECOVER: IP addresses in NAT IP pool pool1 became available.
日志说明	NAT地址池内地址使用率降低至87.5%或以下时会发送该日志，提示用户地址资源恢复
处理建议	无

65.4 IP_USAGE_ALARM

日志内容	NAT IP pool [STRING], total IP count [UINT16], active IP count [UINT16], exceeding the upper limit.
参数解释	$1：地址池名称 $2：地址池内地址总数 $3：地址池内生效地址数
日志等级	4
举例	NAT/6/IP_USAGE_ALARM: NAT IP pool 1, total IP count 100, active IP count 100, exceeding the upper limit.
日志说明	NAT地址池内地址的使用率大于或等于设置的阈值时会发送该日志
处理建议	无

65.5 IP_USAGE_ALARM_RECOVER

日志内容	NAT IP pool [STRING], total IP count [UINT16], active IP count [UINT16], recovering from a usage alarm.
参数解释	$1：地址池名称 $2：地址池内地址总数 $3：地址池内生效地址数
日志等级	4
举例	NAT/6/IP_USAGE_ALARM_RECOVER: NAT IP pool 1, total IP count 100, active IP count 87, recovering from a usage alarm.
日志说明	NAT地址池内地址的使用率小于等于设置的阈值的87.5%时会发送该日志，提示用户资源恢复
处理建议	无

65.6 NAT_ADDR_BIND_CONFLICT

日志内容	Failed to activate NAT configuration on interface [STRING], because global IP addresses already bound to another service card.
参数解释	$1：接口名称
日志等级	4
举例	NAT/4/NAT_ADDR_BIND_CONFLICT: Failed to activate NAT configuration on interface GigabitEthernet1/2/0/1, because global IP addresses already bound to another service card.
日志说明	配置中的外网地址绑定指定业务板时发现其已经绑定到其他业务板上，则触发该日志
处理建议	如果有多个接口引用了相同的外网地址，则这些接口必须指定同一块业务板进行NAT处理。请使用**display nat all**命令检查配置，并修改配置使引用相同外网地址的接口绑定相同的业务板。另外，由于该绑定冲突，失效配置需要先删除，再重新进行配置

65.7 NAT_BANDWIDTH_EXCEED

日志内容	Bandwidth usage of the CGN card reached [UINT32]%.
参数解释	$1：带宽使用率告警阈值
日志等级	4
举例	NAT/4/NAT_BANDWIDTH_EXCEED: Bandwidth usage of the CGN card reached 90%.
日志说明	CGN板带宽使用率达到告警阈值时，会发送该日志
处理建议	无

65.8 NAT_BANDWIDTH_RECOVERY

日志内容	Bandwidth usage of the CGN card dropped below alarm threshold([UINT32]%).
参数解释	$1：带宽使用率告警阈值
日志等级	6
举例	NAT/6/NAT_BANDWIDTH_RECOVERY: Bandwidth usage of the CGN card dropped below alarm threshold(90%).
日志说明	CGN板带宽使用率低于告警阈值时会发送该日志，提示用户资源恢复
处理建议	无

65.9 NAT_EIM

日志内容	Protocol(1001)=[STRING];LocalIPAddr(1003)=[IPADDR];LocalPort(1004)=[UINT16];GlobalIPAddr(1005)=[IPADDR];GlobalPort(1006)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=[STRING];
参数解释	$1：协议类型 $2：源IP地址 $3：源端口号 $4：转换后的源IP地址 $5：转换后的源端口号 $6：源VPN名称 $7：目的VPN名称 $8：源DS-Lite Tunnel $9：创建EIM表项的时间 $10：EIM表项删除时间 $11：日志类型描述信息，包括： • NAT EIM entry created：NAT EIM 表项创建日志 • NAT EIM entry deleted：NAT EIM 表项删除日志
日志等级	6
举例	NAT/6/NAT_EIM: -Protocol(1001)=UDP;LocalIPAddr(1003)=1.1.1.2;LocalPort(1004)=1024;GlobalIPAddr(1005)=30.3.1.231;GlobalPort(1006)=1026;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;BeginTime_e(1013)=10261971001739;EndTime_e(1014)=;Event(1048)=Nat eim created;
日志说明	创建、删除NAT EIM表项时会发送该日志
处理建议	无

65.10 NAT_FAILED_ADD_FLOW_RULE

日志内容	Failed to add flow-table due to: [STRING].
参数解释	$1：失败原因
日志等级	4
举例	NAT/4/NAT_FAILED_ADD_FLOW_RULE: Failed to add flow-table due to: Not enough resources are available to complete the operation.
日志说明	添加流表失败，可能原因包括硬件资源不足、内存不足等
处理建议	请联系技术支持

65.11 NAT_FAILED_ADD_FLOW_TABLE

日志内容	Failed to add flow-table due to [STRING].
参数解释	$1：失败原因
日志等级	4
举例	NAT/4/NAT_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
日志说明	添加流表失败，可能原因包括硬件资源不足、NAT配置地址存在重叠等
处理建议	对于硬件资源不足情况，请联系技术支持 对于NAT配置地址存在重叠情况，请尽量避免出现部分地址重叠，如果不可避免，请将重叠部分地址和不重叠地址分开，单独配置

65.12 NAT_FLOW

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
参数解释	$1：协议类型 $2：应用层协议 $3：源IP地址 $4：源端口号 $5：转换后的源IP地址 $6：转换后的源端口号 $7：目的IP地址 $8：目的端口号 $9：转换后的目的IP地址 $10：转换后的目的端口号 $11：入方向的报文总数 $12：入方向的字节总数 $13：出方向的报文总数 $14：出方向的字节总数 $15：源VPN名称 $16：目的VPN名称 $17：源DS-Lite Tunnel $18：目的DS-Lite Tunnel $19：创建会话的时间 $20：会话删除时间 $22：日志类型 $22：日志类型描述信息，包括： • Session created：NAT 会话创建日志 • Active data flow timeout：流量或时间阈值日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • Aged for reset or config-change：通过配置删除会话日志 • Other：其他原因删除会话日志，如由其他模块删除
日志等级	6
举例	NAT/6/NAT_FLOW: Protocol(1001)=UDP;Application(1002)=other;SrcIPAddr(1003)=1.1.1.2;SrcPort(1004)=1024;NatSrcIPAddr(1005)=30.3.1.231;NatSrcPort(1006)=1026;DstIPAddr(1007)=2.1.1.2;DstPort(1008)=1024;NatDstIPAddr(1009)=2.1.1.2;NatDstPort(1010)=1024;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=03232017091640;EndTime_e(1014)=;Event(1048)=(8)Session created;

日志内容	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
日志说明	创建、删除NAT会话时会发送该日志 NAT会话过程中会定时发送该日志 NAT会话的流量或时间达到指定的阈值时会发送该日志
处理建议	无

65.13 NAT_INSTANCE_SERVER_INVALID

日志内容	The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server in the same instance.
参数解释	无
日志等级	4
举例	NAT/4/NAT_INSTANCE_SERVER_INVALID: The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server in the same instance.
日志说明	Easy IP方式的NAT服务器配置生效时，当同一个实例下存在其他NAT服务器配置也包含相同的外网信息，则触发该日志
处理建议	同一个实例下配置的NAT服务器，其协议类型、外网地址和外网端口号的组合必须是唯一的。请修改相应实例的NAT服务器配置

65.14 NAT_RESOURCE_MEMORY_WARNING

日志内容	Insufficient memory to alloc nat resource pool.
参数解释	无
日志等级	4
举例	NAT/4/NAT_RESOURCE_MEMORY_WARNING:Insufficient memory to alloc nat resource pool.
日志说明	内存不足的情况下由EIM模式切换到CDM模式时会发送该日志
处理建议	无

65.15 NAT_SERVER_INVALID

日志内容	The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server on this interface.
参数解释	无
日志等级	4
举例	NAT/4/NAT_SERVER_INVALID: The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server on this interface.
日志说明	Easy IP方式的NAT服务器配置生效时发现同一个接口下存在其他NAT服务器配置也包含相同的外网信息，则触发该日志
处理建议	同一个接口下配置的NAT服务器，其协议类型、外网地址和外网端口号的组合必须是唯一的。请修改相应接口的NAT服务器配置

65.16 NAT_SERVICE_CARD_RECOVER_FAILURE

日志内容	形式一： Failed to recover the configuration of binding the service card on slot [UINT16] to interface [STRING], because [STRING]. 形式二： Failed to recover the configuration of binding the service card on chassis [UINT16] slot [UINT16] to interface [STRING], because [STRING].
参数解释	形式一： $1：slot编号 $2：接口名称 $3：指定接口绑定业务板配置恢复失败的原因 • NAT addresses already bound to another service card：NAT 地址已经绑定到其他业务板 • NAT service is not supported on this service card：指定业务板不支持 NAT 业务 • the hardware resources are not enough：硬件资源不足 • unknown error：未知错误 形式二： $1：chassis编号 $2：slot编号 $3：接口名称 $4：指定接口绑定业务板配置恢复失败的原因 • NAT addresses already bound to another service card：NAT 地址已经绑定到其他业务板 • NAT service is not supported on this service card：指定业务板不支持 NAT 业务 • the hardware resources are not enough：硬件资源不足 • unknown error：未知错误
日志等级	4
举例	NAT/4/NAT_SERVICE_CARD_RECOVER_FAILURE: Failed to recover the configuration of binding the service card on slot 3 to interface GigabitEthernet1/2/0/2, because NAT service is not supported on this service card.
日志说明	恢复接口绑定业务板配置失败时触发该日志
处理建议	• 如果提示 NAT 地址已经绑定到其他业务板，则使用 **display nat all** 检查配置，并修改配置使引用相同外网地址的接口绑定相同的业务板 • 如果提示业务板不支持 NAT 业务、硬件资源不足或者未知错误，请排查业务板的硬件问题

65.17 NAT444_SYSLOG

日志内容	All port block resources ran out in address group [UINT 16].
参数解释	$1：地址组名称
日志等级	6
举例	NAT/6/ NAT444_SYSLOG: All port block resources ran out in address group 1.
日志说明	地址组内端口块资源耗尽时会发送该日志
处理建议	无

65.18 PORT_USAGE_ALARM

日志内容	Port usage reaches [STRING]%; SrcIPAddr=[IPADDR]; VPNInstance=[STRING]; NATIPAddr=[IPADDR]; ConnectCount=[UINT16].
参数解释	$1：百分比 $2：源IP地址 $3：源VPN名称 $4：转换后的源IP地址 $5：分配端口数
日志等级	6
举例	NAT/6/PORT_USAGE_ALARM: Port usage reaches 40%; SrcIPAddr=1.1.1.211; VPNInstance=-; NATIPAddr=16.1.1.198; ConnectCount=40.
日志说明	当NAT端口块中端口的使用率大于或等于通过命令**nat log port-block port-usage threshold**配置的告警阈值，且PAT方式出方向动态地址转换模式为Connection-Dependent Mapping时，才会发送该日志
处理建议	无

65.19 PORTBLOCK_ALARM

日志内容	Address group [UINT16]; total port blocks [UINT16]; active port blocks [UINT16]; usage over [UINT16]%.
参数解释	$1：地址组名称 $2：端口块总数 $3：分配了的端口块数 $4：端口块使用率
日志等级	6
举例	NAT/6/PORTBLOCK_ALARM: Address group 3; total port blocks 16575; active port blocks 6630; usage over 40%.
日志说明	NAT端口块的使用率大于或等于通过命令**nat log port-block usage threshold**配置的告警阈值时会发送该日志
处理建议	无

65.20 PORTBLOCKGRP_MEMORY_WARNING

日志内容	Insufficient memory caused by excessive public addresses in port block group [UINT16]. Please reconfigure the public address space.
参数解释	$1：NAT端口块组的编号
日志等级	4
举例	NAT/4/PORTBLOCKGRP_MEMORY_WARNING: Insufficient memory caused by excessive public addresses in port block group 1. Please reconfigure the public address space.
日志说明	端口块组内配置的公网地址成员的地址范围太大，导致内存不足，会发送该日志
处理建议	用户需要重新配置公网地址成员的地址范围

66 ND

本节介绍 ND 模块输出的日志信息。

66.1 ND_CONFLICT

日志内容	[STRING] is inconsistent.
参数解释	$1：配置类型 • M_FLAG：被管理地址配置标志位 • O_FLAG：其他信息配置标志位 • CUR_HOP_LIMIT：跳数限制 • REACHABLE TIME：保持邻居可达状态的时间 • NS INTERVAL：邻居请求消息间隔 • MTU：发布链路的 MTU • PREFIX VALID TIME：前缀的有效存活时间 • PREFIX PREFERRED TIME：前缀用于无状态地址配置的优选项的存活时间
日志等级	6
举例	ND/6/ND_CONFLICT：PREFIX VALID TIME is inconsistent.
日志说明	设备收到一个路由通告消息，导致与邻居路由器上的配置不一致
处理建议	检查并保证设备与邻居路由器上的配置一致

66.2 ND_DUPADDR

日志内容	Duplicate address: [STRING] on the interface [STRING].
参数解释	$1：将要分配的IPv6地址 $2：接口名称
日志等级	6
举例	ND/6/ND_DUPADDR: Duplicate address: 33::8 on interface Vlan-interface9.
日志说明	分配给该接口的地址已经被其他设备使用
处理建议	分配一个新的IPv6地址

66.3 ND_HOST_IP_CONFLICT

日志内容	The host [STRING] connected to interface [STRING] cannot communicate correctly, because it uses the same IPv6 address as the host connected to interface [STRING].
参数解释	$1：IPv6地址 $2：接口名 $3：接口名
日志等级	4
举例	ND/4/ND_HOST_IP_CONFLICT: The host 2::2 connected to interface GigabitEthernet1/2/0/1 cannot communicate correctly, because it uses the same IPv6 address as the host connected to interface GigabitEthernet1/2/0/1.
日志说明	分配给该接口的地址已经被其他设备使用
处理建议	分配一个新的IPv6地址。如果非法，需要断开该主机网络

66.4 ND_MAC_CHECK

日志内容	Packet received on interface [STRING] was dropped because source MAC [STRING] was inconsistent with link-layer address [STRING].
参数解释	$1：接收ND报文的接口名 $2：ND报文中的源MAC地址 $3：ND报文的链路层源MAC地址
日志等级	6
举例	ND/6/ND_MAC_CHECK: Packet received on interface Ethernet2/0/2 was dropped because source MAC 0002-0002-0001 was inconsistent with link-layer address 0002-0002-0002.
日志说明	**ipv6 nd mac-check enable**命令用来在网关设备上开启ND协议报文源MAC地址一致性检查功能。在网关开启此功能后，会对接收的ND协议报文进行检查，如果ND协议报文中的源MAC地址和源链路层选项地址中的MAC地址不同，则丢弃该报文。若使用**ipv6 nd check log enable**命令来开启ND日志信息功能，会有相关的log信息输出
处理建议	检查链路层源MAC对应主机的合法性

66.5 ND_MAXNUM_DEV

日志内容	The number of dynamic neighbor entries for the device has reached the maximum.
参数解释	无
日志等级	6
举例	The number of dynamic neighbor entries for the device has reached the maximum.
日志说明	设备学到的动态邻居表项总数到达最大值，打印该提示日志
处理建议	无

66.6 ND_MAXNUM_IF

日志内容	The number of dynamic neighbor entries on interface [STRING] has reached the maximum.
参数解释	$1：接口名
日志等级	6
举例	The number of dynamic neighbor entries on interface GigabitEthernet1/2/0/1 has reached the maximum.
日志说明	接口学到的动态邻居表项总数到达最大值，打印该提示日志
处理建议	无

66.7 ND_RAGUARD_DROP

日志内容	Dropped RA messages with the source IPv6 address [STRING] on interface [STRING]. [STRING] messages dropped in total on the interface.
参数解释	$1：被丢弃报文的源IPv6地址 $2：丢弃报文的端口名 $3：该端口已丢弃的报文总数
日志等级	4
举例	ND/6/ND_RAGUARD_DROP: Dropped RA messages with the source IPv6 address FE80::20 on interface GigabitEthernet1/2/0/1. 20 RA messages dropped in total on the interface.
日志说明	RA Guard检测到攻击，丢弃相应的报文并提示日志信息
处理建议	检查发送报文的设备是否合法

66.8 ND_SET_PORT_TRUST_NORESOURCE

日志内容	Not enough resources to complete the operation.
参数解释	无
日志等级	6
举例	ND/6/ND_SET_PORT_TRUST_NORESOURCE: Not enough resources to complete the operation.
日志说明	下发端口规则失败，原因是驱动资源不足
处理建议	释放设备驱动资源，重新下发

66.9 ND_SET_VLAN_REDIRECT_NORESOURCE

日志内容	Not enough resources to complete the operation.
参数解释	无
日志等级	6
举例	ND/6/ND_VLAN_REDIRECT_NORESOURCE: Not enough resources to complete the operation.
日志说明	下发VLAN规则失败，原因是驱动资源不足
处理建议	释放设备驱动资源，重新下发

67 NETCONF 日志

本节介绍 NETCONF 模块输出的日志信息。

67.1 CLI

日志内容	User ([STRING], [STRING][STRING]) performed an CLI operation: [STRING] operation result=[STRING][STRING]
参数解释	$1：用户名或用户线类型 • 如果用户使用 Scheme 方式登录设备，该值为用户名 • 如果用户使用无认证或 Password 方式登录设备，该值为用户线的类型，例如 VTY $2：用户IP地址或用户线类型及相对编号 • 用户通过 Telnet 或 SSH 登录设备时，该字段取值为用户的 IP 地址 • 用户通过 Console 或 AUX 登录设备时，该字段取值为用户线的类型及相对编号，例如 CON0 $3：NETCONF会话的编号（Web和RESTful类型会话无此字段） $4：NETCONF请求中的message-id（Web和RESTful类型会话无此字段） $5：CLI的执行成功，取值为Succeeded；CLI的执行失败，取值为Failed $6：CLI执行失败的原因（仅已知失败原因的情况显示该信息）
日志等级	6
举例	XMLSOAP/6/CLI: -MDC=1; User (test, 169.254.5.222, session ID=1) performed an CLI operation:message ID=101, operation result=Succeeded.
日志说明	CLI配置执行完毕后，输出CLI的执行结果
处理建议	无

67.2 EDIT-CONFIG

日志内容	User ([STRING], [STRING][STRING])[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. No attributes. 或 User ([STRING], [STRING],[STRING]),[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. Attributes: [STRING].
参数解释	$1：用户名或用户线类型 • 如果用户使用 Scheme 方式登录设备，该值为用户名 • 如果用户使用无认证或 Password 方式登录设备，该值为用户线的类型，例如 VTY $2：用户IP地址或用户线类型及相对编号 • 用户通过 Telnet 或 SSH 登录设备时，该字段取值为用户的 IP 地址 • 用户通过 Console 或 AUX 登录设备时，该字段取值为用户线的类型及相对编号，例如 console0 $3：NETCONF会话的编号，没有则不显示 $4：NETCONF请求中的message-id，没有则不显示 $5：NETCONF行操作名称 $6：模块和表名称 $7：索引信息。仅下发索引时显示，用括号包围；如果日志中包含多个索引，则索引之间用逗号分隔 $8：NETCONF行操作的处理结果，NETCONF行操作执行成功时，取值为Succeeded；执行失败时，取值为Failed $9：属性列信息。仅配置属性列时显示该信息
日志等级	6
举例	XMLSOAP/6/EDIT-CONFIG: -MDC=1; User (test, 192.168.200.220, session ID 1), message ID=101, operation=merge DHCP/DHCPServerPoolStatic (PoolIndex=1, Ipv4Address=1.1.1.1), result=Failed. Attributes: CID="aaaaa", HType=1.
日志说明	按NETCONF行操作输出日志，用户下发一次NETCONF操作，设备输出该操作中每个请求行操作的日志 仅action和set操作支持输入该日志
处理建议	无

67.3 NETCONF_MSG_DEL

日志内容	A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
参数解释	无
日志等级	7
举例	NETCONF/7/NETCONF_MSG_DEL: A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
日志说明	来自NETCONF over SSH客户端或XML视图的NETCONF请求报文由于其大小超过设备支持的上限而被丢弃
处理建议	1. 减小发往设备的单个 NETCONF 请求报文的大小，例如删除报文中的空格、换行、制表符等占位字符 2. 如果报文仍然过大，可以拆分 NETCONF 请求并分别封装后再发送给设备，建议联系技术支持

67.4 REPLY

日志内容	Sent a NETCONF reply to the client: Session ID=[UINT16], Content=[STRING]. 或 Sent a NETCONF reply to the client: Session ID=[UINT16], Content (partial)=[STRING].
参数解释	$1：NETCONF会话ID，建立会话前，该字段显示为“-” $2：设备发送到客户端的NETCONF报文
日志等级	7
举例	XMLSOAP/7/REPLY: -MDC=1; Sent a NETCONF reply to the client: Session ID=1, Content=</env:Body></env:Envelope>.
日志说明	设备发送到客户端的NETCONF报文，用于调试NETCONF工作是否正常 如果一条日志中的NETCONF报文内容太多，则分多条日志输出，每条日志添加“partial”标识
处理建议	无

67.5 THREAD

日志内容	Maximum number of NETCONF threads already reached.
参数解释	无
日志等级	3
举例	XMLCFG/3/THREAD: -MDC=1; Maximum number of NETCONF threads already reached.
日志说明	NETCONF线程数达到上限
处理建议	NETCONF线程数达到上限，请稍后重试

68 NQA

本节介绍 NQA 模块输出的日志信息。

68.1 NQA_BATCH_START_FAILURE

日志内容	Failed to batch start the [STRING] operation. Reason: [STRING]
参数解释	$1：NQA测试类型，取值为Y.1564 $3：错误类型 ○ Invalid configuration：非法配置 ○ Not enough resources：资源不足
日志等级	6
举例	NQA/6/NQA_BATCH_START_FAILURE: Failed to batch start the Y.1564 operation. Invalid configuration.
日志说明	Y.1564测试启动过程中，服务性能测试批量启动失败，失败原因可能是参数配置不正确或者硬件资源不足，此时提示此日志
处理建议	• 检查配置参数进行修改并重新启动测试 • 联系技术支持

68.2 NQA_LOG_UNREACHABLE

日志内容	Server [STRING] unreachable.
参数解释	$1：NQA服务器的IP地址
日志等级	6
举例	NQA/6/NQA_LOG_UNREACHABLE: Server 192.168.30.117 unreachable.
日志说明	NQA客户端检测到NQA服务器不可达
处理建议	检查网络环境

68.3 NQA_PACKET_OVERSIZE

日志内容	NQA entry ([STRING]-[STRING]): The payload size exceeds 65503 bytes, and all IPv6 UDP probe packets will be dropped by the NQA server.
参数解释	$1：NQA测试组的管理员名称 $2：测试操作的标签
日志等级	6
举例	NQA/6/NQA_PACKET_OVERSIZE: NQA entry (1-1): The payload size exceeds 65503 bytes, and all IPv6 UDP probe packets will be dropped by the NQA server.
日志说明	NQA客户端发送了使用UDP协议、目的地址为IPv6地址、且数据段长度超过65503字节的探测报文，这样的探测报文将在服务器端被丢弃
处理建议	检查设备配置，修改NQA测试的**`data-size`**数据字段大小

68.4 NQA_REFLECTOR_START_FAILURE

日志内容	NQA reflector [UINT32]: Failed to start the NQA reflector. Please check the parameters.
参数解释	$1：反射会话的ID
日志等级	6
举例	NQAS/6/NQA_REFLECTOR_START_FAILURE: NQA reflector 1: Failed to start the NQA reflector, Please check the parameters.
日志说明	启动NQA服务器端的反射功能失败，提示用户检查配置参数
处理建议	配置NQA服务器端的反射参数时，**`nqa reflector`**命令缺少参数必配项，根据当前网络环境判断参数的必配项，并检查参数配置并重新将参数配置完整

68.5 NQA_REFRESH_FAILURE

日志内容	Failed to refresh the [STRING] operation. Reason: [STRING]
参数解释	$1：NQA测试类型，取值为RFC2544 $3：错误类型 o Invalid configuration.：非法配置 o Not enough resources.：资源不足
日志等级	6
举例	NQA/6/NQA_REFRESH_FAILURE: Failed to refresh the RFC2544 operation. Invalid configuration.
日志说明	对于路径服务质量测试（即RFC2544）：连续启动多个路径服务质量测试操作失败，失败原因可能是参数配置不正确或者硬件资源不足，此时提示此日志，且已启动的路径服务质量测试结果均删除，所有路径服务质量测试均停止
处理建议	• 检查配置参数进行修改并重新启动测试 • 联系技术支持

68.6 NQA_REFRESH_START

日志内容	Start to refresh the [STRING] operation and reset the result.
参数解释	$1：NQA测试类型，取值为RFC2544
日志等级	6
举例	NQA/6/NQA_REFRESH_START: Start to refresh the RFC2544 operation and reset the result.
日志说明	路径服务质量测试（即RFC2544）测试进行过程中，还可以再次执行**start**命令启动新一个路径服务质量测试，此时会清除当前正在进行的路径服务质量测试的测试结果，并将所有的路径服务质量测试并行启动，此时提示该日志
处理建议	无

68.7 NQA_SCHEDULE_FAILURE

日志内容	NQA entry ([STRING]- [STRING]): Failed to start the scheduled NQA operation because port [STRING] used by the operation is not available.
参数解释	$1：NQA测试组的管理员名称 $2：测试操作的标签 $3：端口号
日志等级	6
举例	NQA/6/NQA_SCHEDULE_FAILURE: NQA entry (admin-tag): Failed to start the scheduled NQA operation because port 10000 used by the operation is not available.
日志说明	由于端口被其他服务占用，导致NQA客户端的测试调度失败
处理建议	调度失败的情况下，用户需要修改NQA测试中被占用的端口或是关闭已占用端口的服务

68.8 NQA_SEVER_FAILURE

日志内容	Failed to enable the NQA server because listening port [STRING] is not available.
参数解释	$1：端口号
日志等级	6
举例	NQA/6/NQA_SEVER_FAILURE: Failed to enable the NQA server because listening port 10000 is not available.
日志说明	由于端口被其他服务占用，导致NQA服务器功能开启失败
处理建议	服务器功能开启失败的情况下，用户需要修改被占用的端口或是关闭已占用端口的服务

68.9 NQA_START_FAILURE

日志内容	NQA entry ([STRING]-[STRING]): [STRING]
参数解释	$1：NQA测试组的管理员名称 $2：测试操作的标签 $3：NQA测试下发驱动执行时失败，失败的原因包括： • Operation failed due to configuration conflicts：配置冲突导致下发驱动失败 • Operation failed because the driver was not ready to perform the operation：驱动未准备就绪导致下发驱动失败 • Operation not supported：驱动不支持该操作 • Not enough resources to complete the operation：资源不足导致下发驱动失败 • Operation failed due to an unknown error：其他情况导致下发驱动操作失败
日志等级	6
举例	NQA/6/NQA_START_FAILURE: NQA entry 1-1: Operation failed due to configuration conflicts.
日志说明	NQA测试下发驱动执行时，失败
处理建议	• 检查配置参数进行修改并重新启动测试 • 联系技术支持

68.10 NQA_TWAMP_LIGHT_PACKET_INVALID

日志内容	NQA TWAMP Light test session [UINT32] index [UINT32]: The number of packets captured for statistics collection is invalid.
参数解释	$1：测试会话ID $2：统计数据的序列号
日志等级	6
举例	NQA/6/ NQA_TWAMP_LIGHT_PACKET_INVALID: NQA TWAMP Light test session 1 index 7: The number of packets captured for statistics collection is invalid.
日志说明	统计的探测帧数量异常，本次探测统计结果不计入统计计数
处理建议	检查NQA TWAMP-light测试配置，可能原因为：配置的统计周期小于发送报文的周期

68.11 NQA_TWAMP_LIGHT_REACTION

日志内容	NQA TWAMP Light test session [UINT32] reaction entry [UINT32]: Detected continual violation of the [STRING] [STRING] threshold for a threshold violation monitor time of [UINT32] ms.
参数解释	$1：测试会话的ID $2：阈值告警组编号 $3：阈值告警类型，取值包括： o two-way delay：双向时延阈值告警 o two-way loss：双向丢包率阈值告警 o two-way jitter：双向抖动阈值告警 $4：阈值动作，取值包括： o upper：大于等于阈值告警的上限阈值 o lower：小于等于阈值告警的下限阈值 $5：日志告警周期
日志等级	6
举例	NQA/6/NQA_TWAMP_LIGHT_REACTION: NQA TWAMP Light test session 1 reaction entry 1: Detected continual violation of the two-way loss upper threshold for a threshold violation monitor time of 2000 ms.
日志说明	监测NQA TWAMP-light测试的探测结果，从测试统计的第一个结果大于等于阈值告警的上限阈值或者从大于阈值告警的下限阈值恢复到小于等于该下限阈值开始计时，若在监控时间内测试结果持续不变，打印该日志。
处理建议	无

68.12 NQA_TWAMP_LIGHT_START_FAILURE

日志内容	NQA TWAMP Light test session [UINT32]: Failed to start the test session. Please check the parameters.
参数解释	$1：测试会话的ID
日志等级	6
举例	NQAS/6/NQA_TWAMP_LIGHT_START_FAILURE: NQA TWAMP Light test session 1: Failed to start the test session, Please check the parameters.
日志说明	启动TWAMP-light Responder端的测试会话失败，提示用户检查配置参数
处理建议	配置TWAMP-light Responder端测试会话的反射参数时，**test-session**命令TWAMP-light Responder端缺少参数必配项，根据当前网络环境判断参数的必配项，并检查参数配置并重新将参数配置完整

69 NTP

本节介绍 NTP 模块输出的日志信息。

69.1 NTP_CLOCK_CHANGE

日志内容	System clock changed from [STRING] to [STRING], the NTP server's IP address is [STRING].
参数解释	$1：起始时间 $2：同步后时间 $3：IP地址
日志等级	5
举例	NTP/5/NTP_CLOCK_CHANGE: System clock changed from 02:12:58:345 12/28/2012 to 02:29:12:879 12/28/2012, the NTP server's IP address is 192.168.30.116.
日志说明	NTP客户端的时间已经和NTP服务器同步
处理建议	无

69.2 NTP_LEAP_CHANGE

日志内容	System Leap Indicator changed from [UINT32] to [UINT32] after clock update.
参数解释	$1：起始闰秒标识 $2：当前闰秒标识
日志等级	5
举例	NTP/5/NTP_LEAP_CHANGE: System Leap Indicator changed from 00 to 01 after clock update.
日志说明	• NTP 闰秒标识是一个二位码，预报当天最近的分钟里要被插入的闰秒秒数 • 比特值在闰秒秒数插入当天 23:59 前或次日 00:00 后设置。因此秒数会比插入当天的时间提前或推后 1 秒 • 系统的闰秒标识会发生变化。例如，NTP 状态会从未同步状态变为已同步状态
处理建议	无

69.3 NTP_SOURCE_CHANGE

日志内容	NTP server's IP address changed from [STRING] to [STRING].
参数解释	$1：起始时钟源的IP地址 $2：新时钟源的IP地址
日志等级	5
举例	NTP/5/NTP_SOURCE_CHANGE: NTP server's IP address changed from 1.1.1.1 to 1.1.1.2.
日志说明	系统改变了时钟源
处理建议	无

69.4 NTP_SOURCE_LOST

日志内容	Lost synchronization with NTP server with IP address [STRING].
参数解释	$1：IP 地址
日志等级	5
举例	NTP/5/NTP_SOURCE_LOST: Lost synchronization with NTP server with IP address 1.1.1.1.
日志说明	NTP交互中的时钟源处于未同步状态或不可达
处理建议	检查NTP服务器及网络连接，若NTP服务器故障，请在客户端配置新的服务器作为时钟源

69.5 NTP_STRATUM_CHANGE

日志内容	System stratum changed from [UINT32] to [UINT32] after clock update.
参数解释	$1：起始层 $2：当前层
日志等级	5
举例	NTP/5/NTP_STRATUM_CHANGE: System stratum changed from 6 to 5 after clock update.
日志说明	系统的层数已发生变化
处理建议	无

70 OFP

本节介绍 OpenFlow 模块输出的日志信息。

70.1 OFC_DATAPATH_CHANNEL_CONNECT

日志内容	OpenFlow Controller datapath [STRING], channel with IP address [STRING] connected
参数解释	$1：OpenFlow实例的Datapath ID $2：和控制器连接的OpenFlow交换机的IP地址
日志等级	5
举例	OFC/5/OFC_DATAPATH_CHANNEL_CONNECT: OpenFlow Controller datapath 0x174258ae43182, channel with IP address 169.28.25.123 connected
日志说明	控制器建立了一个新的连接
处理建议	无

70.2 OFC_DATAPATH_CHANNEL_DISCONNECT

日志内容	OpenFlow Controller datapath [STRING], channel with IP address [STRING] disconnected
参数解释	$1：OpenFlow实例的Datapath ID $2：和控制器连接的OpenFlow交换机的IP地址
日志等级	5
举例	OFC/6/OFC_DATAPATH_CHANNEL_DISCONNECT:OpenFlow Controller datapath 0x174258ae43182, channel with IP address 169.28.25.123 disconnected
日志说明	OpenFlow交换机与控制器的安全通道连接断开
处理建议	无

70.3 OFC_FLOW_ADD

日志内容	App [CHAR] added flow entry: [STRING].
参数解释	$1：App ID $2：流表项内容，其中match的内容为匹配域，action的内容为动作集
日志等级	5
举例	OFC/5/OFC_FLOW_ADD：App 1 added flow entry: match(context 0x12a56, ipaddr 1.1.1.1, vxlan id 1), action(set svlan 2, set cvlan 3, modify destination mac 0-0-5, output 11).
日志说明	控制器上的App向OpenFlow交换机下发增加流表项的信息
处理建议	无

70.4 OFC_FLOW_DEL

日志内容	App [CHAR] deleted flow entry: [STRING].
参数解释	$1：App ID $2：流表项内容，其中match的内容为匹配域，action的内容为动作集
日志等级	5
举例	OFC/5/OFC_FLOW_DEL：App 1 deleted flow entry: match(context 0x12a56, ipaddr 1.1.1.1, vxlan id 1), action(set svlan 2, set cvlan 3, modify destination mac 0-0-5, output 11).
日志说明	控制器上的App向OpenFlow交换机下发删除流表项的信息
处理建议	无

70.5 OFC_FLOW_MOD

日志内容	App [CHAR] modified flow entry: [STRING].
参数解释	$1：App ID $2：流表项内容，其中match的内容为匹配域，action的内容为动作集
日志等级	5
举例	OFC/5/OFC_FLOW_MOD：App 1 modified flow entry: match(context 0x12a56, ipaddr 1.1.1.1, vxlan id 1), action(set svlan 2, set cvlan 3, modify destination mac 0-0-5, output 11).
日志说明	控制器上的App向OpenFlow交换机下发修改流表项的信息
处理建议	无

70.6 OFP_ACTIVE

日志内容	Activate openflow instance [UINT16]
参数解释	$1：实例ID
日志等级	5
举例	OFP/5/OFP_ACTIVE: Activate openflow instance 1.
日志说明	收到激活OpenFlow实例的命令
处理建议	无

70.7 OFP_ACTIVE_FAILED

日志内容	Failed to activate instance [UINT16].
参数解释	$1：实例ID
日志等级	4
举例	OFP/4/OFP_ACTIVE_FAILED: Failed to activate instance 1.
日志说明	激活OpenFlow实例失败
处理建议	无

70.8 OFP_ACTIVE_MAC_LEARN_FORBIDDEN_F

日志内容	Failed to execute the mac-learning forbidden command when activating instance [UINT16]
参数解释	$1：实例ID
日志等级	4
举例	OFP/4/OFP_ACTIVE_MAC_LEARN_FORBIDDEN_F: Failed to execute the mac-learning forbidden command when activating instance 1.
日志说明	激活OpenFlow实例时，该实例下配置的**mac-learning forbidden**命令下发失败，可能是因为设备硬件不支持。同时，下发失败的配置将被自动删除
处理建议	联系技术支持

70.9 OFP_CONNECT

日志内容	Openflow instance [UINT16], controller [CHAR] is [STRING].
参数解释	$1：实例ID $2：控制器ID $3：连接状态，显示为connected或disconnected
日志等级	5
举例	OFP/5/OFP_CONNECT: Openflow instance 1, controller 0 is connected.
日志说明	控制器连接状态变化
处理建议	无

70.10 OFP_FAIL_OPEN

日志内容	Openflow instance [UINT16] is in fail [STRING] mode.
参数解释	$1：实例ID $2：连接中断模式，显示为secure或standalone
日志等级	5
举例	OFP/5/OFP_FAIL_OPEN: Openflow instance 1 is in fail secure mode.
日志说明	实例激活后无法连接控制器或者从所有控制器断开，显示连接中断模式
处理建议	无

70.11 OFP_FLOW_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add flow entry [UINT32], xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：XID $5：流表项cookie $6：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_ADD: Openflow instance 1 controller 0: add flow entry 1, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（增加操作）并通过报文检查。即将添加流表项
处理建议	无

70.12 OFP_FLOW_ADD_DUP

日志内容	Openflow instance [UINT16] controller [CHAR]: add duplicate flow entry [UINT32], xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：XID $5：Cookie $6：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_ADD_DUP: Openflow instance 1 controller 0: add duplicate flow entry 1, xid 0x1, cookie 0x1, table id 0.
日志说明	表项重复添加
处理建议	无

70.13 OFP_FLOW_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add flow entry [UINT32], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：规则ID $4：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_ADD_FAILED: Openflow instance 1 controller 0: failed to add flow entry 1, table id 0.
日志说明	添加流表项失败
处理建议	无

70.14 OFP_FLOW_ADD_TABLE_MISS

日志内容	Openflow instance [UINT16] controller [CHAR]: add table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_ADD_TABLE_MISS: Openflow instance 1 controller 0: add table miss flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（增加操作）并通过报文检查。即将添加miss规则
处理建议	无

70.15 OFP_FLOW_ADD_TABLE_MISS_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add table miss flow entry, table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_ADD_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to add table miss flow entry, table id 0.
日志说明	添加miss规则失败
处理建议	无

70.16 OFP_FLOW_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete flow entry, xid 0x[HEX], cookie 0x[HEX], table id [STRING].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_DEL: Openflow instance 1 controller 0: delete flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（删除操作）并通过报文检查。即将删除对应的流表项
处理建议	无

70.17 OFP_FLOW_DEL_TABLE_MISS

日志内容	Openflow instance [UINT16] controller [CHAR]: delete table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [STRING].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_DEL_TABLE_MISS: Openflow instance 1 controller 0: delete table miss flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（删除操作）并通过报文检查。即将删除对应的miss规则
处理建议	无

70.18 OFP_FLOW_DEL_TABLE_MISS_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to delete table miss flow entry, table id [STRING].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_DEL_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to delete table miss flow entry, table id 0.
日志说明	删除miss规则失败
处理建议	无

70.19 OFP_FLOW_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_MOD: Openflow instance 1 controller 0: modify flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（修改操作）并通过报文检查。即将修改对应的流表项
处理建议	无

70.20 OFP_FLOW_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify flow entry, table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_MOD_FAILED: Openflow instance 1 controller 0: failed to modify flow entry, table id 0.
日志说明	修改流表项失败
处理建议	控制器重试修改操作或直接删除流表项

70.21 OFP_FLOW_MOD_TABLE_MISS

日志内容	Openflow instance [UINT16] controller [CHAR]: modify table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：XID $4：流表项cookie $5：流表ID
日志等级	5
举例	OFP/5/OFP_FLOW_MOD_TABLE_MISS: Openflow instance 1 controller 0: modify table miss flow entry, xid 0x1, cookie 0x0, table id 0.
日志说明	收到修改流表信息（修改操作）并通过报文检查。即将修改对应的miss规则
处理建议	无

70.22 OFP_FLOW_MOD_TABLE_MISS_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify table miss flow entry, table id [CHAR].
参数解释	$1：实例ID $2：控制器ID $3：流表ID
日志等级	4
举例	OFP/4/OFP_FLOW_MOD_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to modify table miss flow entry, table id 0.
日志说明	修改miss规则失败
处理建议	控制器重试修改操作或直接删除miss规则

70.23 OFP_FLOW_RMV_GROUP

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted with a group_mod message.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_RMV_GROUP: The flow entry 1 in table 0 of instance 1 was deleted with a group_mod message.
日志说明	Group删除导致的表项删除
处理建议	无

70.24 OFP_FLOW_RMV_HARDTIME

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted because of an hard-time expiration.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_RMV_HARDTIME: The flow entry 1 in table 0 of instance 1 was deleted because of an hard-time expiration.
日志说明	Hard-time超时导致的表项删除
处理建议	无

70.25 OFP_FLOW_RMV_IDLETIME

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted because of an idle-time expiration.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_RMV_IDLETIME: The flow entry 1 in table 0 of instance 1 was deleted because of an idle-time expiration.
日志说明	Idle-time超时导致的表项删除
处理建议	无

70.26 OFP_FLOW_RMV_METER

日志内容	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted with a meter_mod message.
参数解释	$1：规则ID $2：流表ID $3：实例ID
日志等级	5
举例	OFP/5/OFP_FLOW_RMV_GROUP: The flow entry 1 in table 0 of instance1 was deleted with a meter_mod message.
日志说明	Meter删除导致的表项删除
处理建议	无

70.27 OFP_FLOW_UPDATE_FAILED

日志内容	OpenFlow instance [UINT16] table [CHAR]: failed to update or synchronize flow entry [UINT32].
参数解释	$1：实例ID $2：流表ID $3：流表项ID
日志等级	4
举例	OFP/4/OFP_FLOW_UPDATE_FAILED: OpenFlow instance 1 table 0: failed to update or synchronize flow entry 10000.
日志说明	主备倒换时，新主用主控板更新流表项失败 设备插入新接口板时，接口板同步主控板的流表项失败 集群中主从设备倒换时，新主设备更新流表项失败 集群中加入新成员设备时，成员设备同步主设备的流表项失败
处理建议	删除下发失败的流表项

70.28 OFP_GROUP_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add group [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_GROUP_ADD: Openflow instance 1 controller 0: add group 1, xid 0x1.
日志说明	收到修改group表信息（增加操作）并通过报文检查。即将添加group表项
处理建议	无

70.29 OFP_GROUP_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add group [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID
日志等级	4
举例	OFP/4/OFP_GROUP_ADD_FAILED: Openflow Instance 1 controller 0: failed to add group 1.
日志说明	添加group表项失败
处理建议	无

70.30 OFP_GROUP_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete group [STRING], xid [HEX].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_GROUP_DEL: Openflow instance 1 controller 0: delete group 1, xid 0x1.
日志说明	收到修改group表信息（删除操作）并通过报文检查。即将删除对应group表项
处理建议	无

70.31 OFP_GROUP_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify group [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_GROUP_MOD: Openflow instance 1 controller 0: modify group 1, xid 0x1.
日志说明	收到修改group表信息（修改操作）并通过报文检查。即将修改对应group表项
处理建议	无

70.32 OFP_GROUP_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify group [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Group表项ID
日志等级	4
举例	OFP/4/OFP_GROUP_MOD_FAILED: Openflow instance 1 controller 0: failed to modify group 1.
日志说明	修改group表项失败
处理建议	控制器重试修改操作或直接删除group表项

70.33 OFP_METER_ADD

日志内容	Openflow instance [UINT16] controller [CHAR]: add meter [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_METER_ADD: Openflow instance 1 controller 0: add meter 1, xid 0x1.
日志说明	收到修改meter表信息（增加操作）并通过报文检查。即将添加meter表项
处理建议	无

70.34 OFP_METER_ADD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to add meter [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID
日志等级	4
举例	OFP/4/OFP_METER_ADD_FAILED: Openflow Instance 1 controller 0: failed to add meter 1.
日志说明	添加meter表项失败
处理建议	无

70.35 OFP_METER_DEL

日志内容	Openflow instance [UINT16] controller [CHAR]: delete meter [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_METER_DEL: Openflow instance 1 controller 0: delete meter 1, xid 0x1.
日志说明	收到修改meter表信息（删除操作）并通过报文检查。即将删除指定的meter表项
处理建议	无

70.36 OFP_METER_MOD

日志内容	Openflow instance [UINT16] controller [CHAR]: modify meter [STRING], xid 0x[HEX].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID $4：XID
日志等级	5
举例	OFP/5/OFP_METER_MOD: Openflow Instance 1 controller 0: modify meter 1, xid 0x1.
日志说明	收到修改meter表信息（修改操作）并通过报文检查。即将修改指定的meter表项
处理建议	无

70.37 OFP_METER_MOD_FAILED

日志内容	Openflow instance [UINT16] controller [CHAR]: failed to modify meter [STRING].
参数解释	$1：实例ID $2：控制器ID $3：Meter表项ID
日志等级	4
举例	OFP/4/OFP_METER_MOD_FAILED: Openflow instance 1 controller 0: failed to modify meter 1.
日志说明	修改meter表项失败
处理建议	控制器重试修改操作或直接删除meter表项

70.38 OFP_MISS_RMV_GROUP

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted with a group_mod message.
参数解释	$1：流表ID $2：实例ID
日志等级	5
举例	OFP/5/OFP_MISS_RMV_GROUP: The table-miss flow entry in table 0 of instance 1 was deleted with a group_mod message.
日志说明	Group删除导致的table-miss表项删除
处理建议	无

70.39 OFP_MISS_RMV_HARDTIME

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted because of an hard-time expiration.
参数解释	$1：流表ID $2：实例ID
日志等级	5
举例	OFP/5/OFP_MISS_RMV_HARDTIME: The table-miss flow entry in table 0 of instance 1 was deleted because of an hard-time expiration.
日志说明	Hard-time超时导致的table-miss表项删除
处理建议	无

70.40 OFP_MISS_RMV_IDLETIME

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted because of an idle-time expiration.
参数解释	$1：流表ID $2：实例ID
日志等级	5
举例	OFP/5/OFP_MISS_RMV_IDLETIME: The table-miss flow entry in table 0 of instance 1 was deleted because of an idle-time expiration.
日志说明	Idle-time超时导致的table-miss表项删除
处理建议	无

70.41 OFP_MISS_RMV_METER

日志内容	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted with a meter_mod message.
参数解释	$1：流表ID $2：实例ID
日志等级	5
举例	OFP/5/OFP_MISS_RMV_METER: The table-miss flow entry in table 0 of instance 1 was deleted with a meter_mod message.
日志说明	Meter删除导致的table-miss表项删除
处理建议	无

71 OPTMOD

本节介绍 OPTMOD 模块输出的日志信息。

71.1 BIAS_HIGH

日志内容	[STRING]: Bias current is high.
参数解释	$1：端口类型和编号
日志等级	2
举例	OPTMOD/2/BIAS_HIGH: GigabitEthernet1/2/0/1: Bias current is high.
日志说明	光模块的偏置电流超过上限
处理建议	1. **display transceive diagnosis interface** 命令查看当前偏置电流值是否已经超过高告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有偏置电流值高的告警 3. 如果确实超过门限了，模块有问题，更换模块。

71.2 BIAS_LOW

日志内容	[STRING]: Bias current is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/BIAS_LOW: GigabitEthernet1/2/0/1: Bias current is low.
日志说明	光模块的偏置电流低于下限
处理建议	1. **display transceive diagnosis interface** 命令查看当前偏置电流值是否已经超过低告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有偏置电流高的告警 3. 如果低于低告警门限，模块有问题，更换模块

71.3 BIAS_NORMAL

日志内容	[STRING]: Bias current is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/BIAS_NORMAL: GigabitEthernet1/2/0/1: Bias current is normal.
日志说明	光模块的偏置电流恢复至正常范围
处理建议	无

71.4 CFG_ERR

日志内容	[STRING]: Transceiver type and port configuration mismatched.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/CFG_ERR: GigabitEthernet1/2/0/1: Transceiver type and port configuration mismatched.
日志说明	光模块类型与端口配置不匹配
处理建议	检查端口当前配置与光模块类型，如果确实不匹配，则更换匹配模块，或更新配置

71.5 CHKSUM_ERR

日志内容	[STRING]: Transceiver information checksum error.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/CHKSUM_ERR: GigabitEthernet1/2/0/1: Transceiver information checksum error .
日志说明	光模块寄存器信息校验失败
处理建议	更换光模块，或联系工程师解决

71.6 FIBER_SFP MODULE_INVALID

日志内容	[STRING]: This transceiver module is not compatible with the interface card. HP does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in [UINT32] days. Please replace it with a compatible one as soon as possible.
参数解释	$1：端口类型和编号 $2：光模块失效天数
日志等级	4
举例	OPTMOD/4/FIBER_SFPMODULE_INVALID: GigabitEthernet1/2/0/1: This transceiver module is not compatible with the interface card. HP does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in 3 days. Please replace it with a compatible one as soon as possible.
日志说明	光模块与接口卡不匹配
处理建议	更换光模块

71.7 FIBER_SFPMODULE_NOWINVALID

日志内容	[STRING]: This is not a supported transceiver for this platform. HP does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the HP web site or contact your HP sales rep for a list of supported transceivers.
参数解释	$1：端口类型和编号
日志等级	4
举例	OPTMOD/4/FIBER_SFPMODULE_NOWINVALID: GigabitEthernet1/2/0/1: This is not a supported transceiver for this platform. HP does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the HP web site or contact your HP sales rep for a list of supported transceivers.
日志说明	不支持该光模块
处理建议	更换光模块

71.8 IO_ERR

日志内容	[STRING]: The transceiver information I/O failed.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/IO_ERR: GigabitEthernet1/2/0/1: The transceiver information I/O failed.
日志说明	设备读取光模块寄存器信息失败
处理建议	执行**display transceive diagnosis interface**或者**display transceive alarm interface**命令，如果都显示fail，则表示光模块故障，请更换

71.9 MOD_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	$1：端口类型和编号 $2：故障类型
日志等级	5
举例	OPTMOD/5/MOD_ALM_OFF: GigabitEthernet1/2/0/1: Module_not_ready was removed.
日志说明	光模块的某故障被清除
处理建议	无

71.10 MOD_ALM_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	$1：端口类型和编号 $2：故障类型
日志等级	5
举例	OPTMOD/5/MOD_ALM_ON: GigabitEthernet1/2/0/1: Module_not_ready wasdetected.
日志说明	检测到光模块一故障
处理建议	执行**display transceive alarm interface**命令，如果仍然显示Module not ready，则表示光模块有问题，请更换

71.11 MODULE_IN

日志内容	[STRING]: The transceiver is [STRING].
参数解释	$1：端口类型和编号 $2：光模块类型
日志等级	4
举例	OPTMOD/4/MODULE_IN: GigabitEthernet1/2/0/1: The transceiver is 1000_BASE_T_AN_SFP.
日志说明	光模块类型。当一光模块插入某端口时，设备生成此日志信息
处理建议	无

71.12 MODULE_OUT

日志内容	[STRING]: Transceiver absent.
参数解释	$1：端口类型和编号
日志等级	4
举例	OPTMOD/4/MODULE_OUT: GigabitEthernet1/2/0/1: The transceiver is absent.
日志说明	光模块被拔出
处理建议	无

71.13 PHONY_MODULE

日志内容	[STRING]: This transceiver is not sold by UNIS. UNIS does not guarantee the correct operation of the module or assume maintenance responsibility.
参数解释	$1：端口类型和编号
日志等级	4
举例	OPTMOD/4/PHONY_MODULE: GigabitEthernet1/2/0/1: This transceiver is not sold by UNIS. UNIS does not guarantee the correct operation of the module or assume maintenance responsibility.
日志说明	光模块非UNIS生产
处理建议	更换光模块

71.14 RX_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	$1：端口类型和编号 $2：RX故障类型
日志等级	5
举例	OPTMOD/5/RX_ALM_OFF: GigabitEthernet1/2/0/1: RX_not_ready was removed.
日志说明	光模块RX故障被清除
处理建议	无

71.15 RX_ALM_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	$1：端口类型和编号 $2：RX故障类型
日志等级	5
举例	OPTMOD/5/RX_ALM_ON: GigabitEthernet1/2/0/1: RX_not_ready was detected.
日志说明	检测到光模块RX故障
处理建议	使用**display transceive alarm interface**命令可查看到这个故障，确认是模块问题，更换模块

71.16 RX_POW_HIGH

日志内容	[STRING]: RX power is high.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/RX_POW_HIGH: GigabitEthernet1/2/0/1: RX power is high.
日志说明	光模块RX功率超过上限
处理建议	1. **display transceive diagnosis interface** 命令查看功率是否已经超过高告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有功率高的告警 3. 如果确实超过门限了，模块有问题，更换模块

71.17 RX_POW_LOW

日志内容	[STRING]: RX power is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/RX_POW_LOW: GigabitEthernet1/2/0/1: RX power is low.
日志说明	光模块RX功率低于下限
处理建议	1. **display transceive diagnosis interface** 命令查看功率是否已经低于低告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有功率低告警 3. 如果确实低于门限了，模块有问题，更换模块

71.18 RX_POW_NORMAL

日志内容	[STRING]: RX power is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/RX_POW_NORMAL: GigabitEthernet1/2/0/1: RX power is normal.
日志说明	光模块RX功率恢复至正常范围
处理建议	无

71.19 TEMP_HIGH

日志内容	[STRING]: Temperature is high.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TEMP_HIGH: GigabitEthernet1/2/0/1: Temperature is high.
日志说明	光模块温度超过上限
处理建议	检查设备风扇是否工作正常，安装风扇或更换故障风扇 检查环境温度，如果温度确实过高就调节温度 如果设备风扇正常，且环境温度正常，则模块故障，更换模块

71.20 TEMP_LOW

日志内容	[STRING]: Temperature is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TEMP_LOW: GigabitEthernet1/2/0/1: Temperature is low.
日志说明	光模块温度低于下限
处理建议	检查环境温度，如果温度确实过低高就调节温度，如果环境温度正常，就是模块故障，更换模块

71.21 TEMP_NORMAL

日志内容	[STRING]: Temperature is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TEMP_NORMAL: GigabitEthernet1/2/0/1: Temperature is normal.
日志说明	光模块温度恢复至正常范围
处理建议	无

71.22 TX_ALM_OFF

日志内容	[STRING]: [STRING] was removed.
参数解释	$1：端口类型和编号 $2：TX故障类型
日志等级	5
举例	OPTMOD/5/TX_ALM_OFF: GigabitEthernet1/2/0/1: TX_fault was removed.
日志说明	光模块TX故障被清除
处理建议	无

71.23 TX_ALM_ON

日志内容	[STRING]: [STRING] was detected.
参数解释	$1：端口类型和编号 $2：TX故障类型
日志等级	5
举例	OPTMOD/5/TX_ALM_ON: GigabitEthernet1/2/0/1: TX_fault was detected.
日志说明	检测到光模块TX故障
处理建议	使用**display transceive alarm interface**命令可查看到这个故障，确认是模块问题，更换模块

71.24 TX_POW_HIGH

日志内容	[STRING]: TX power is high.
参数解释	$1：端口类型和编号
日志等级	2
举例	OPTMOD/2/TX_POW_HIGH: GigabitEthernet1/2/0/1: TX power is high.
日志说明	光模块TX功率超过上限
处理建议	1. **display transceive diagnosis interface** 命令查看功率是否已经超过高告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有功率高告警 3. 如果确实超过门限了，模块有问题，更换模块

71.25 TX_POW_LOW

日志内容	[STRING]: TX power is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TX_POW_LOW: GigabitEthernet1/2/0/1: TX power is low.
日志说明	光模块TX功率低于下限
处理建议	1. **display transceive diagnosis interface** 命令查看功率是否已经低于低告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有功率低告警 3. 如果确实低于门限了，模块有问题，更换模块

71.26 TX_POW_NORMAL

日志内容	[STRING]: TX power is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/TX_POW_NORMAL: GigabitEthernet1/2/0/1: TX power is normal.
日志说明	光模块TX功率恢复至正常范围
处理建议	无

71.27 TYPE_ERR

日志内容	[STRING]: The transceiver type is not supported by port hardware.
参数解释	$1：端口类型和编号
日志等级	3
举例	OPTMOD/3/TYPE_ERR: GigabitEthernet1/2/0/1: The transceiver type is not supported by port hardware.
日志说明	端口硬件不支持光模块类型
处理建议	更换光模块

71.28 VOLT_HIGH

日志内容	[STRING]: Voltage is high.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/VOLT_HIGH: GigabitEthernet1/2/0/1: Voltage is high.
日志说明	光模块电压超过上限
处理建议	1. **display transceive diagnosis interface** 命令查看电压是否已经超过高告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有电压高告警 3. 如果确实超过门限了，模块有问题，更换模块

71.29 VOLT_LOW

日志内容	[STRING]: Voltage is low.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/VOLT_LOW: GigabitEthernet1/2/0/1: Voltage is low.
日志说明	光模块电压低于下限
处理建议	1. **display transceive diagnosis interface** 命令查看电压是否已经超过低告警门限 2. **display transceive alarm interface** 命令查看当前是否确实有电压低告警 3. 如果确实超过门限了，模块有问题，更换模块

71.30 VOLT_NORMAL

日志内容	[STRING]: Voltage is normal.
参数解释	$1：端口类型和编号
日志等级	5
举例	OPTMOD/5/VOLT_NORMAL: GigabitEthernet1/2/0/1: Voltage is normal!
日志说明	光模块电压恢复至正常范围
处理建议	无

72 OSPF

本节介绍 OSPF 模块输出的日志信息。

72.1 OSPF_DUP_RTRID_NBR

日志内容	OSPF [UINT16] Duplicate router ID [STRING] on interface [STRING], sourced from IP address [IPADDR].
参数解释	$1：OSPF进程ID $2：路由器ID $3：接口名称 $4：IP地址
日志等级	6
举例	OSPF/6/OSPF_DUP_RTRID_NBR: OSPF 1 Duplicate router ID 11.11.11.11 on interface GigabitEthernet1/2/0/3, sourced from IP address 11.2.2.2.
日志说明	检测到两台直连设备配置了相同的路由器ID
处理建议	修改其中一台设备的路由器ID，并使用**reset ospf process**命令使新的路由器ID生效

72.2 OSPF_IP_CONFLICT_INTRA

日志内容	OSPF [UINT16] Received newer self-originated network-LSAs. Possible conflict of IP address [IPADDR] in area [STRING] on interface [STRING].
参数解释	$1：OSPF进程ID $2：IP地址 $3：OSPF区域ID $4：接口名称
日志等级	6
举例	OSPF/6/OSPF_IP_CONFLICT_INTRA: OSPF 1 Received newer self-originated network-LSAs. Possible conflict of IP address 11.1.1.1 in area 0.0.0.1 on interface GigabitEthernet1/2/0/3.
日志说明	同一OSPF区域内两台设备的接口上可能配置了相同的主IP地址，其中至少一台设备是DR
处理建议	在确保同一OSPF区域内不存在Router ID冲突的情况下，修改IP地址配置

72.3 OSPF_LAST_NBR_DOWN

日志内容	OSPF [UINT32] Last neighbor down event: Router ID: [STRING] Local address: [STRING] Remote address: [STRING] Reason: [STRING]
参数解释	$1：OSPF进程ID $2：路由器ID $3：本地IP地址 $4：邻居IP地址 $5：原因
日志等级	6
举例	OSPF/6/OSPF_LAST_NBR_DOWN: OSPF 1 Last neighbor down event: Router ID: 2.2.2.2 Local address: 10.1.1.1 Remote address: 10.1.1.2 Reason: Dead Interval timer expired.
日志说明	最近一次OSPF邻居down事件
处理建议	检查OSPF邻居down事件的原因，根据具体原因进行处理： • 如果是配置相关命令导致邻居 down，如接口参数变化等，请检查配置是否正确 • 如果是超时邻居 down，检查网络状况或者配置的超时时间是否合理 • 如果是 BFD 检测导致的邻居 down ，检查网络状况或者 BFD 检测时间配置是否合理 • 如果是接口状态变化导致的邻居 down，检查网络连接情况

72.4 OSPF_MEM_ALERT

日志内容	OSPF Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	OSPF/5/OSPF_MEM_ALERT: OSPF Process received system memory alert start event.
日志说明	OSPF模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存，对占用内存较多的模块进行调整，尽量释放可用内存

72.5 OSPF_NBR_CHG

日志内容	OSPF [UINT32] Neighbor [STRING] ([STRING]) changed from [STRING] to [STRING]
参数解释	$1：OSPF进程ID $2：邻居路由器ID $3：接口名称 $4：旧邻接状态 $5：新邻接状态
日志等级	5
举例	OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 2.2.2.2 (Vlan-interface100) changed from Full to Down.
日志说明	接口OSPF邻接状态改变
处理建议	当某接口与邻居邻接状态从Full变为其他状态时，检查OSPF配置正确性和网络连通性

72.6 OSPF_NBR_CHG_REASON

日志内容	OSPF [UINT32] Area [STRING] Router [STRING]([STRING]) CPU usage: [STRING], VPN name: [STRING], IfMTU: [UINT32], Neighbor address: [STRING], NbrID [STRING] changed from [STRING] to [STRING] at [STRING]. Last 4 hello packets received at: [STRING] Last 4 hello packets sent at: [STRING]
参数解释	$1：OSPF进程ID $2：区域ID $3：路由ID $4：接口简名 $5：CPU使用率 $6：VPN名称 $7：接口MTU大小 $8：邻居的IP地址 $9：邻居的路由器ID $10：变化前的邻居状态 $11：变化后的邻居状态和状态变化原因 $12：邻居状态改变的时间 $13：邻居状态改变前接收的4个Hello报文的时间 $14：邻居状态改变前发送的4个Hello报文的时间
日志等级	5
举例	OSPF/5/OSPF_NBR_CHG_REASON: OSPF 1 Area 0.0.0.0 Router 2.2.2.2(GE1/2/0/1) CPU usage:3.80%, VPN name: a, IfMTU:1500, Neighbor address:10.1.1.2, NbrID:1.1.1.1 changed from Full to Down because OSPF interface parameters changed at 2019-04-01 15:20:57:034. Last 4 hello packets received at: 2019-09-01 15:19:46:225 2019-09-01 15:19:56:224 2019-09-01 15:20:06:225 2019-09-01 15:20:16:225 Last 4 hello packets sent at: 2019-09-01 15:20:22:033 2019-09-01 15:20:32:033 2019-09-01 15:20:42:032 2019-09-01 15:20:52:033
日志说明	接口OSPF邻居状态改变原因
处理建议	当某接口与邻居的状态发生回退时发送该日志，请检查OSPF配置正确性和网络连通性

72.7 OSPF_RT_LMT

日志内容	OSPF [UINT32] route limit reached.
参数解释	$1：OSPF进程ID
日志等级	4
举例	OSPF/4/OSPF_RT_LMT: OSPF 1 route limit reached.
日志说明	OSPF进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

72.8 OSPF_RTRID_CHG

日志内容	OSPF [UINT32] New router ID elected, please restart OSPF if you want to make the new router ID take effect.
参数解释	$1：OSPF进程ID
日志等级	5
举例	OSPF/5/OSPF_RTRID_CHG: OSPF 1 New router ID elected, please restart OSPF if you want to make the new router ID take effect.
日志说明	用户更改了router ID或者是使用的接口IP发生变化而改变了OSPF路由器ID。需要手动重启OSPF使新的路由器ID生效
处理建议	使用**reset ospf process**命令使新的路由器ID生效

72.9 OSPF_RTRID_CONFLICT_INTER

日志内容	OSPF [UINT16] Received newer self-originated ase-LSAs. Possible conflict of router ID [STRING].
参数解释	$1：OSPF进程ID $2：路由器ID
日志等级	6
举例	OSPF/6/OSPF_RTRID_CONFILICT_INTER: OSPF 1 Received newer self-originated ase-LSAs. Possible conflict of router ID 11.11.11.11.
日志说明	同一OSPF域内非直连的两台设备可能配置了相同的路由器ID，其中一台设备为ASBR
处理建议	修改其中一台设备的路由器ID，并使用**reset ospf process**命令使新的路由器ID生效

72.10 OSPF_RTRID_CONFLICT_INTRA

日志内容	OSPF [UINT16] Received newer self-originated router-LSAs. Possible conflict of router ID [STRING] in area [STRING].
参数解释	$1：OSPF进程ID $2：路由器ID $3：OSPF区域ID
日志等级	6
举例	OSPF/6/OSPF_RTRID_CONFLICT_INTRA: OSPF 1 Received newer self-originated router-LSAs. Possible conflict of router ID 11.11.11.11 in area 0.0.0.1.
日志说明	同一OSPF区域内非直连的两台设备可能配置了相同的路由器ID
处理建议	修改其中一台设备的路由器ID，并使用**`reset ospf process`**命令使新的路由器ID生效

72.11 OSPF_VLINKID_CHG

日志内容	OSPF [UINT32] Router ID changed, reconfigure Vlink on peer
参数解释	$1：OSPF进程ID
日志等级	5
举例	OSPF/5/OSPF_VLINKID_CHG:OSPF 1 Router ID changed, reconfigure Vlink on peer
日志说明	新的OSPF路由器ID生效。需要根据新的路由器ID检查并修改对端路由器的虚连接配置
处理建议	根据新的路由器ID检查并修改对端路由器的虚连接配置

73 OSPFV3

本节介绍 OSPFv3 模块输出的日志信息。

73.1 OSPFV3_LAST_NBR_DOWN

日志内容	OSPFv3 [UINT32] Last neighbor down event: Router ID: [STRING] Local interface ID: [UINT32] Remote interface ID: [UINT32] Reason: [STRING].
参数解释	$1：OSPFv3进程ID $2：路由器ID $3：本地接口ID $4：对端接口ID $5：原因
日志等级	6
举例	OSPFV3/6/OSPFV3_LAST_NBR_DOWN: OSPFv3 1 Last neighbor down event: Router ID: 2.2.2.2 Local interface ID: 1111 Remote interface ID: 2222 Reason: Dead Interval timer expired.
日志说明	最近一次OSPFv3邻居down事件
处理建议	检查OSPFV3邻居down事件的原因，根据具体原因进行处理： • 如果是配置相关命令导致邻居 down，如接口参数变化等，请检查配置是否正确 • 如果是超时邻居 down，检查网络状况或者配置的超时时间是否合理 • 如果是 BFD 检测导致的邻居 down ，检查网络状况或者 BFD 检测时间配置是否合理 • 如果是接口状态变化导致的邻居 down，检查网络连接情况

73.2 OSPFV3_MEM_ALERT

日志内容	OSPFV3 Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	OSPFV3/5/OSPFV3_MEM_ALERT: OSPFV3 Process received system memory alert start event.
日志说明	OSPFv3模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

73.3 OSPFV3_NBR_CHG

日志内容	OSPFv3 [UINT32] Neighbor [STRING] ([STRING]) received [STRING] and its state changed from [STRING] to [STRING].
参数解释	$1：OSPFv3进程ID $2：邻居路由器ID $3：接口名称 $4：邻居事件 $5：旧邻接状态 $6：新邻接状态
日志等级	5
举例	OSPFV3/5/OSPFV3_NBR_CHG: OSPFv3 1 Neighbor 2.2.2.2 (Vlan100) received 1-Way and its state changed from Full to Init.
日志说明	接口OSPFv3邻接状态改变
处理建议	当某接口与邻居邻接状态从Full变为其他状态时，检查OSPFv3配置正确性和网络连通性

73.4 OSPFV3_RT_LMT

日志内容	OSPFv3 [UINT32] route limit reached.
参数解释	$1：OSPFv3进程ID
日志等级	5
举例	OSPFV3/5/OSPFV3_RT_LMT:OSPFv3 1 route limit reached.
日志说明	OSPFv3进程的路由数达到了上限值
处理建议	检查是否受到攻击或者减少网络路由数

74 PBR

本节介绍 PBR 模块输出的日志信息。

74.1 PBR_HARDWARE_BIND_ERROR

日志内容	Failed to apply the policy [STRING] to interface [STRING] because of [STRING]..
参数解释	$1：策略名 $2：接口名 $3：硬件处理失败的原因，包括以下三种类型： • insufficient hardware resources：资源不足 • unsupported operations：系统不支持该操作 • insufficient hardware resources and unsupported operations：硬件资源不足且系统不支硬件持
日志等级	4
举例	PBR/4/PBR_HARDWARE_BIND_ERROR: Failed to apply the policy abc to interface GigabitEthernet1/2/0/1 because of unsupported operations.
日志说明	接口配置单播策略路由发生错误
处理建议	根据错误原因修改策略中的配置

74.2 PBR_HARDWARE_ERROR

日志内容	Failed to update policy [STRING] due to [STRING].
参数解释	$1：策略名 $2：硬件处理失败的原因，包括以下三种类型： • insufficient hardware resources：资源不足 • unsupported operations：系统不支持该操作 • insufficient hardware resources and unsupported operations：硬件资源不足且系统不支硬件持
日志等级	4
举例	PBR/4/PBR_HARDWARE_ERROR: Failed to update policy aaa due to insufficient hardware resources and not supported operations.
日志说明	更新单播策略路由配置失败
处理建议	根据失败原因修改策略中的配置

74.3 PBR_NEXTHOP_CHANGE

日志内容	The link to next hop [IPADDR] of policy [STRING] (node ID: [STRING], VPN instance: [STRING]) changed due to [STRING].
参数解释	$1：下一跳地址 $2：策略名称 $3：节点名称 $4：VPN名称，如果是公网，则取值为Public network $5：下一跳发生变化的原因，包括以下五种类型： • FIB change ：FIB 信息发生变化 • reachable status ：下一跳地址从不可达到可达 • unreachable status ：下一跳地址从可达到不可达 • direct change ：配置下一跳动作带不带 direct 参数时直连下一跳路由发生变化 • track change ：track 项状态发生变化
日志等级	4
举例	PBR/4/PBR_NEXTHOP_CHANGE: The link to next hop 1.1.1.1 of policy a (node ID: 0, VPN instance: Public network) changed due to FIB change..
日志说明	公网中的节点编号为0的策略路由a，由于FIB表发生改变下一跳链路发生变化
处理建议	提示用户具体的下一跳链路发生改变，方便用户定位问题并解决问题

75 PCE

本节介绍 PCE 模块输出的日志信息

75.1 PCE_PCEP_SESSION_CHG

日志内容	Session ([STRING], [STRING]) is [STRING].
参数解释	$1：会话对端IP地址 $2：会话所在VPN实例名称，如果无法获取则显示为unknown $3：会话的状态变更，up或者down，如果状态变更为down，则一并显示会话down的原因
日志等级	5
举例	PCE/5/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is up. PCE/5/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is down (dead timer expired).

日志说明	显示会话的状态变化以及会话down的原因
	down 的原因可能包括：
	• TCP connection down：TCP 连接断开
	• received a close message：在如下五种情况下会收到对端的关闭消息
	  ○ No explanation provided：未提供详细原因（当会话空闲超过 3 分钟，会以此种形式关闭会话）
	  ○ DeadTimer expired：deadtimer 定时器超时
	  ○ Reception of a malformed PCEP message：消息格式错误或者收到畸形消息
	  ○ Reception of an unacceptable number of unknown requests/replies：收到超过限制的未知计算请求/计算应答
	  ○ Reception of an unacceptable number of unrecognized PCEP messages：收到超过限制的未知消息
	• reception of a malformed PCEP message：收到非法消息
	• internal error：内部错误
	• memory in critical state：内存不足
	• dead timer expired：会话超时
	• process deactivated：PCE 进程去激活
	• remote peer unavailable/untriggered：对等体失效
	• reception of an unacceptable number of unrecognized PCEP messages：收到超过限制的未知消息
	• reception of an unacceptable number of unknown requests/replies：收到超过限制的未知计算请求/计算应答
	• PCE address changed：PCE 地址变化
	• initialization failed：初始化失败

处理建议	如果会话的状态变更为up，不需要进行其它操作 如果会话的状态变更为down，请根据提示原因检查网络环境或者配置

76 PFILTER

本节介绍报文过滤模块输出的日志信息。

76.1 PFILTER_GLB_RES_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction globally. [STRING] ACL [UINT] has already been applied globally.
参数解释	$1：ACL版本 $2：ACL编号 $3：流量方向 $4：ACL类型 $5：ACL编号
日志等级	3
举例	PFILTER/3/PFILTER_GLB_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction globally. IPv6 ACL 3000 has already been applied globally.
日志说明	IPv4、IPv6、MAC类型的ACL在某方向上全局应用了，系统无法在此方向上全局应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

76.2 PFILTER_GLB_IPV4_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally. The resources are insufficient.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新IPv4缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.3 PFILTER_GLB_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新IPv4缺省动作
处理建议	无

76.4 PFILTER_GLB_IPV6_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally. The resources are insufficient.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新IPv6缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.5 PFILTER_GLB_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新IPv6缺省动作
处理建议	无

76.6 PFILTER_GLB_MAC_DACT_NO_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction globally. The resources are insufficient.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新MAC缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.7 PFILTER_GLB_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction globally.
参数解释	$1：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新MAC缺省动作
处理建议	无

76.8 PFILTER_GLB_NO_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The resources are insufficient.
参数解释	$1：ACL版本 $2：ACL编号 $3：规则的ID及内容 $4：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在某个方向上全局应用或更新ACL规则
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.9 PFILTER_GLB_NOT_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The ACL is not supported.
参数解释	$1：ACL版本 $2：ACL编号 $3：规则的ID及内容 $4：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The ACL is not supported.
日志说明	因系统不支持ACL规则而导致无法在某个方向上全局应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

76.10 PFILTER_GLB_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向
日志等级	3
举例	PFILTER/3/PFILTER_GLB_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally.
日志说明	因故障导致系统无法在某个方向上全局应用或更新ACL
处理建议	无

76.11 PFILTER_IF_IPV4_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 1/2/0/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新IPv4缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.12 PFILTER_IF_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING].
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 1/2/0/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新IPv4缺省动作
处理建议	无

76.13 PFILTER_IF_IPV6_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 1/2/0/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新IPv6缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.14 PFILTER_IF_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING].
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 1/2/0/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新IPv6缺省动作
处理建议	无

76.15 PFILTER_IF_MAC_DACT_NO_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 1/2/0/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新MAC缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.16 PFILTER_IF_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING].
参数解释	$1：流量方向 $2：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 1/2/0/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新MAC缺省动作
处理建议	无

76.17 PFILTER_IF_NO_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The resources are insufficient.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 1/2/0/2. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在接口的某个方向上应用或更新ACL规则
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.18 PFILTER_IF_NOT_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The ACL is not supported.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 1/2/0/2. The ACL is not supported.
日志说明	因系统不支持ACL规则而导致无法在接口的某个方向上应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

76.19 PFILTER_IF_RES_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction of interface [STRING]. [STRING] ACL [UINT] has already been applied to the interface.
参数解释	$1：ACL版本 $2：ACL编号 $3：流量方向 $4：接口名称 $5：ACL类型 $6：ACL编号
日志等级	3
举例	PFILTER/3/PFILTER_IF_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction of interface Ethernet 1/2/0/2. IPv6 ACL 3000 has already been applied to the interface.
日志说明	IPv4、IPv6、MAC类型的ACL在接口某方向上应用了，系统无法在此方向上应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

76.20 PFILTER_IF_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING].
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：接口名称
日志等级	3
举例	PFILTER/3/PFILTER_IF_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 1/2/0/2.
日志说明	因故障系统无法在接口的某个方向上应用或更新ACL规则
处理建议	无

76.21 PFILTER_IPV6_STATIS_INFO

日志内容	[STRING] ([STRING]): Packet-filter IPv6 [UINT32] [STRING] [STRING] [UINT64] packet(s).
参数解释	$1：ACL应用目的地 $2：流量方向 $3：ACL编号 $4：ACL规则的ID及内容 $5：匹配上规则的报文个数
日志等级	6
举例	PFILTER/6/PFILTER_IPV6_STATIS_INFO: Ethernet1/2/0/1 (inbound): Packet-filter IPv6 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
日志说明	匹配上报文过滤中的IPv6 ACL规则的报文数量发生变化
处理建议	无

76.22 PFILTER_STATIS_INFO

日志内容	[STRING] ([STRING]): Packet-filter [UINT32] [STRING] [UINT64] packet(s).
参数解释	$1：ACL应用目的地 $2：流量方向 $3：ACL编号 $4：ACL规则的ID及内容 $5：匹配上规则的报文个数
日志等级	6
举例	PFILTER/6/PFILTER_STATIS_INFO: Ethernet1/2/0/1 (inbound): Packet-filter 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
日志说明	匹配上报文过滤中的IPv4 ACL规则的报文数量发生变化
处理建议	无

76.23 PFILTER_VLAN_IPV4_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction of VLAN 1. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新IPv4缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.24 PFILTER_VLAN_IPV4_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv4 default action to the [STRING] direction of VLAN [UINT16].
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction of VLAN 1.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新IPv4缺省动作
处理建议	无

76.25 PFILTER_VLAN_IPV6_DACT_NO_RES

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction of VLAN 1. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新IPv6缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.26 PFILTER_VLAN_IPV6_DACT_UNK_ERR

日志内容	Failed to apply or refresh the IPv6 default action to the [STRING] direction of VLAN [UINT16].
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction of VLAN 1.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新IPv6缺省动作
处理建议	无

76.27 PFILTER_VLAN_MAC_DACT_NO_RES

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction of VLAN 1. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新MAC缺省动作
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.28 PFILTER_VLAN_MAC_DACT_UNK_ERR

日志内容	Failed to apply or refresh the MAC default action to the [STRING] direction of VLAN [UINT16].
参数解释	$1：流量方向 $2：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction of VLAN 1.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新MAC缺省动作
处理建议	无

76.29 PFILTER_VLAN_NO_RES

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of VLAN 1. The resources are insufficient.
日志说明	因硬件资源不足，系统无法在VLAN的某个方向上应用或更新ACL规则
处理建议	使用**display qos-acl resource**命令检查硬件资源使用情况

76.30 PFILTER_VLAN_NOT_SUPPORT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16]. The ACL is not supported.
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_NOT_SUPPORT: Failed to apply or refresh ACL 2000 rule 1 to the inbound direction of VLAN 1. The ACL is not supported.
日志说明	因系统不支持ACL规则而导致无法在VLAN的某个方向上应用或更新ACL规则
处理建议	检查ACL规则并删除不支持的配置

76.31 PFILTER_VLAN_RES_CONFLICT

日志内容	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction of VLAN [UINT16]. [STRING] ACL [UINT] has already been applied to the VLAN.
参数解释	$1：ACL版本 $2：ACL编号 $3：流量方向 $4：VLAN ID $5：ACL类型 $6：ACL编号
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction of VLAN 1. IPv6 ACL 3000 has already been applied to the VLAN.
日志说明	IPv4、IPv6、MAC类型的ACL已经在VLAN的某方向上应用了，系统无法在此方向上应用或更新相同类型的ACL规则
处理建议	删除相同类型的ACL

76.32 PFILTER_VLAN_UNK_ERR

日志内容	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16].
参数解释	$1：ACL版本 $2：ACL编号 $3：ACL规则的ID及内容 $4：流量方向 $5：VLAN ID
日志等级	3
举例	PFILTER/3/PFILTER_VLAN_UNK_ERR: Failed to apply or refresh ACL 2000 rule 1 to the inbound direction of VLAN 1.
日志说明	因故障系统无法在VLAN的某个方向上应用或更新ACL规则
处理建议	无

77 PIM

本节介绍 PIM 模块输出的日志信息。

77.1 PIM_NBR_DOWN

日志内容	[STRING] Neighbor [STRING] ([STRING]) is down.
参数解释	$1：公网侧PIM邻居down时，该参数为空；私网侧PIM邻居down时，该参数为VPN实例的名称 $2：PIM邻居的IP地址 $3：接口名称
日志等级	5
举例	PIM/5/PIM_NBR_DOWN: Neighbor 10.1.1.1(Vlan-interface10) is down.
日志说明	PIM邻居的状态变为down
处理建议	检查PIM配置是否错误以及检查网络是否发生故障

77.2 PIM_NBR_UP

日志内容	[STRING] Neighbor [STRING] ([STRING]) is up.
参数解释	$1：公网侧PIM邻居up时，该参数为空；私网侧PIM邻居up时，该参数为VPN实例的名称 $2：PIM邻居的IP地址 $3：接口名称
日志等级	5
举例	PIM/5/PIM_NBR_UP: Neighbor 10.1.1.1(Vlan-interface10) is up.
日志说明	PIM邻居的状态变为up
处理建议	无

78 PING

本节介绍 ping 模块输出的日志信息。

78.1 PING6_SRV6_STATISTICS

日志内容	Ping6 SRv6 statistics: [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packet loss.
参数解释	$1：发送的回显请求数量 $2：接收的回显应答数量 $3：没有回复的报文占总请求报文比
日志等级	6
举例	PING/6/PING6_SRV6_STATISTICS: Ping6 SRv6 statistics: 5 packets transmitted, 5 packets received, 0.0% packet loss.
日志说明	用户执行**ping ipv6-sid**命令查看SRv6转发路径的连通性
处理建议	如果没有收到报文，请检查SRv6转发路径上各设备的路由和SID情况。关于SRv6的相关介绍请参考“Segment Routing配置指导”中的“IPv6 SR”

78.2 PING_STATISTICS

日志内容	[STRING] statistics for [STRING]: [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
参数解释	$1：Ping或Ping6 $2：目的IP地址，IPv6地址，或主机名 $3：发送的回显请求数量 $4：接收的回显应答数量 $5：没有回复的报文占总请求报文比 $6：最小往返时间 $7：平均往返时间 $8：最大往返时间 $9：往返时间标准差
日志等级	6
举例	PING/6/PING_STATISTICS: Ping statistics for 192.168.0.115: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
日志说明	用户执行**ping**命令查看公网中对端是否可达
处理建议	如果没有收到报文，请检查接口是否DOWN，并查找路由表，看是否存在有效路由

78.3 PING_VPN_STATISTICS

日志内容	[STRING] statistics for [STRING] in VPN instance [STRING] : [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
参数解释	$1：Ping或Ping6 $2：目的IP地址，IPv6地址，或主机名 $3：VPN实例名 $3：发送的回显请求数量 $4：接收的回显应答数量 $5：没有回复的报文占总请求报文比 $6：最小往返时间 $7：平均往返时间 $8：最大往返时间 $9：往返时间标准差
日志等级	6
举例	PING/6/PING_VPN_STATISTICS: Ping statistics for 192.168.0.115 in VPN instance vpn1: 5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
日志说明	用户执行**ping**命令查看VPN中的对端是否可达
处理建议	如果没有收到报文，请检查接口是否DOWN，并查找路由表，看是否存在有效路由

79 PKG

本节介绍包管理模块输出的日志信息。

79.1 PKG_VERSION_CONSISTENT

日志内容	形式一： Software images on slot [STRING] are not consistent with those on the active MPU. The slot will reboot to reload the images of the active MPU. 形式二： Software images on chassis [STRING] slot [STRING] are not consistent with those on the local active MPU. The slot will reboot to reload the images of the local active MPU.
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	5
举例	形式一： PKG/5/PKG_VERSION_CONSISTENT: Software images on slot 2 are not consistent with those on the active MPU. The slot will reboot to reload the images of the active MPU. 形式二： PKG/5/PKG_VERSION_CONSISTENT: Software images on chassis 2 slot 2 are not consistent with those on the local active MPU. The slot will reboot to reload the images of the local active MPU.
日志说明	建议在设备稳定的情况下，才对软件包进行安装、卸载、升级操作。如果用户没有遵循以上建议，在业务板启动过程中，通过**install**命令安装/卸载Feature/Patch包或者增量升级Boot/System/Feature包，此时升级的软件包不能同步给正在启动的业务板，会导致业务板启动完成后，运行的软件版本和主用主控板上当前运行的软件版本不一致。系统会自动重启这些业务板以便这些业务板能自动加载新的软件包，保持和主用主控板的版本一致。业务板重启前，会打印该日志
处理建议	执行安装、卸载以及升级操作前，请使用**display system stable**命令显示系统的稳定状态，如果System State未处于Stable状态，不能进行安装、卸载以及升级软件包操作

80 PKI

本节包含 PKI 日志消息。

80.1 REQUEST_CERT_FAIL

日志内容	Failed to request certificate of domain [STRING].
参数解释	$1：PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_FAIL: Failed to request certificate of domain abc.
日志说明	为PKI域申请证书失败
处理建议	检查设备和CA服务器的配置和其间的网络

80.2 REQUEST_CERT_SUCCESS

日志内容	Request certificate of domain [STRING] successfully.
参数解释	$1：PKI域名
日志等级	5
举例	PKI/5/REQUEST_CERT_SUCCESS: Request certificate of domain abc successfully.
日志说明	为PKI域申请证书成功
处理建议	无

81 PKT2CPU

本节包含 PKT2CPU 日志消息。

81.1 PKT2CPU_NO_RESOURCE

日志内容	-Interface=[STRING]-ProtocolType=[UINT32]-MacAddr=[STRING]; The resources are insufficient. -Interface=[STRING]-ProtocolType=[UINT32]-SrcPort=[UINT32]-DstPort=[UINT32]; The resources are insufficient.
参数解释	$1：接口名 $2：协议类型 $3：MAC地址或源端口 $4：目的端口
日志等级	4
举例	PKT2CPU/4/PKT2CPU_NO_RESOURCE: -Interface=Ethernet1/2/0/2-ProtocolType=21-MacAddr=0180-c200-0014; The resources are insufficient.
日志说明	硬件资源不足
处理建议	取消配置

82 PKTCPT

本节介绍 PKTCPT（Packet Capture）模块输出的日志信息。

82.1 PKTCPT_AP_OFFLINE

日志内容	Failed to start packet capture. Reason: AP was offline.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_AP_OFFLINE: Failed to start packet capture. Reason: AP was offline.
日志说明	指定报文捕获的AP没有上线，报文捕获启动失败
处理建议	检查配置，AP上线后再次开启报文捕获

82.2 PKTCPT_AREADY_EXIT

日志内容	Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_AREADY_EXIT: Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
日志说明	AC/FIT AP组网，当AC上的报文捕获功能先停止时，AP还在上传捕获的报文。此时用户再次开启报文捕获功能，报文捕获功能会启动失败
处理建议	请稍后重新开启报文捕获功能

82.3 PKTCPT_CONN_FAIL

日志内容	Failed to start packet capture. Reason: Failed to connect to the FTP server.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_CONN_FAIL: Failed to start packet capture. Reason: Failed to connect to the FTP server.
日志说明	无法连接到与设备在同一网段的FTP服务器，报文捕获功能启动失败
处理建议	• 检查 URL 是否合法。可能情况包括：指定的 FTP 服务器的 IP 地址不存在；指定的 IP 地址不是 FTP 服务器的地址；指定的 FTP 服务器的接口处于关闭状态 • 检查 URL 中域名解析是否成功 • 检查开启报文捕获服务设备与 FTP 服务器是否可达 • 检查 FTP 服务器是否上线

82.4 PKTCPT_INVALID_FILTER

日志内容	Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_INVALD_FILTER: Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
日志说明	捕获过滤规则非法，启动报文捕获功能失败
处理建议	修改捕获过滤规则

82.5 PKTCPT_LOGIN_DENIED

日志内容	Packet capture aborted. Reason: FTP server login failure.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_LOGIN_DENIED: Packet capture aborted. Reason: FTP server login failure.
日志说明	登录FTP服务器失败，报文捕获退出
处理建议	检查用户名密码是否正确

82.6 PKTCPT_MEMORY_ALERT

日志内容	Packet capture aborted. Reason: Memory threshold reached.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_MEMORY_ALERT: Packet capture aborted. Reason: Memory threshold reached.
日志说明	设备达到内存门限时，报文捕获功能退出
处理建议	无

82.7 PKTCPT_OPEN_FAIL

日志内容	Failed to start packet capture. Reason: File for storing captured frames not opened.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_OPEN_FAIL: Failed to start packet capture. Reason: File for storing captured frames not opened.
日志说明	将报文文件保存到FLASH时，文件路径无法打开，报文捕获功能启动失败
处理建议	• 若用户不具有写文件权限，请配置写权限 • 若指定的文件名是已经存在并被其它程序占用，请使用其它文件名

82.8 PKTCPT_OPERATION_TIMEOUT

日志内容	Failed to start or continue packet capture. Reason: Operation timed out.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_OPERATION_TIMEOUT: Failed to start or continue packet capture. Reason: Operation timed out.
日志说明	由于指定的与设备在不同网段的FTP服务器不可达，连接超时导致报文捕获启动失败；由于指定的与设备在不同网段的FTP服务器不在线，上传捕获的报文超时，导致报文捕获退出
处理建议	• 检查 FTP 服务器是否可达 • 检查 FTP 服务器是否在线

82.9 PKTCPT_SERVICE_FAIL

日志内容	Failed to start packet capture. Reason: TCP or UDP port binding faults.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_SERVICE_FAIL: Failed to start packet capture. Reason: TCP or UDP port binding faults.
日志说明	由于TCP或者UDP端口绑定冲突等原因导致报文捕获功能启动失败
处理建议	• 如果之前打开的报文捕获客户端（第三方软件 wireshark）没有关闭，请关闭后重新启动报文捕获功能 • 绑定新的端口号，重新启动报文捕获功能

82.10 PKTCPT_UNKNOWN_ERROR

日志内容	Failed to start or continue packet capture. Reason: Unknown error.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_UNKNOWN_ERROR: Failed to start or continue the packet capture. Reason: Unknown error.
日志说明	其它未知原因导致服务启动失败或者退出
处理建议	无

82.11 PKTCPT_UPLOAD_ERROR

日志内容	Packet capture aborted. Reason: Failed to upload captured frames.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_UPLOAD_ERROR: Packet capture aborted. Reason: Failed to upload captured frames.
日志说明	由于上传捕获的数据报文失败，导致报文捕获退出
处理建议	• 检查是否试图改变 FTP 的工作目录 • 检查指定 FTP 服务器上文件是否有写权限 • 检查 FTP 服务器是否下线 • 检查与 FTP 服务器是否可达 • 检查 FTP 服务器是否已满 • 检查报文捕获服务是否退出

82.12 PKTCPT_WRITE_FAIL

日志内容	Packet capture aborted. Reason: Not enough space to store captured frames.
参数解释	无
日志等级	6
举例	PKTCPT/6/PKTCPT_WRITE_FAIL: Packet capture aborted. Reason: Not enough space to store captured frames.
日志说明	报文文件保存到FLASH时，FLASH已满，报文捕获功能退出
处理建议	删除无用文件释放磁盘空间

83 PPP

本节介绍 PPP 模块输出的日志信息。

83.1 PPP_SESSIONS_LOWER_THRESHOLD

日志内容	The PPP session number is below the lower warning threshold (LowerThreshold=[INT32]).
参数解释	$1：在线PPP会话数目的下限告警阈值
日志等级	4
举例	PPP/4/PPP_SESSIONS_LOWER_THRESHOLD: The PPP session number is below the lower warning threshold (LowerThreshold=20).
日志说明	在线PPP会话数目已低于配置的下限告警阈值
处理建议	1. 执行 **display access-user** 命令查看当前在线接入 PPP 用户总数 2. 确认 PPP 用户是否非正常大量下线

83.2 PPP_SESSIONS_RECOVER_NORMAL

日志内容	The PPP session number has recovered to normal state.
参数解释	无
日志等级	5
举例	PPP/5/PPP_SESSIONS_RECOVER_NORMAL: The PPP session number has recovered to normal state.
日志说明	在线PPP会话数目重新恢复到设定的正常范围内
处理建议	无

83.3 PPP_SESSIONS_UPPER_THRESHOLD

日志内容	The PPP session number is above the upper warning threshold (UpperThreshold=[INT32]).
参数解释	$1：在线PPP会话数目的上限告警阈值
日志等级	4
举例	PPP/4/ PPP_SESSIONS_UPPER_THRESHOLD: The PPP session number is above the upper warning threshold (UpperThreshold=20).
日志说明	在线PPP会话数目已高于配置的上限告警阈值
处理建议	1. 执行 **display access-user** 命令查看当前在线接入 PPP 用户总数 2. 确认是否存在大量非法 PPP 用户上线

83.4 PPPOES_LIMIT

日志内容	Maximum number of PPPoE sessions already reached.
参数解释	无
日志等级	6
举例	PPPOES/6/PPPOES_LIMIT: Maximum number of PPPoE sessions already reached.
日志说明	PPPoE用户上线已达到系统允许上线的最大数目，新用户无法上线
处理建议	1. 确认 **pppoe-server session-limit total** 配置 2. 执行 **display pppoe-server session summary slot** 命令查看当前单板上的 PPPoE 会话数是否已达到系统允许创建的最大数目 3. 如果非上述原因导致新用户无法上线，请联系 UNIS 技术支持

83.5 PPPOES_LIMIT_VLAN

日志内容	Maximum number of PPPoE sessions for the VLAN already reached.
参数解释	无
日志等级	6
举例	PPPOES/6/PPPOES_LIMIT_VLAN: Maximum number of PPPoE sessions for the VLAN already reached.
日志说明	PPPoE用户上线已达到每个VLAN创建会话最大数目，新用户无法上线
处理建议	1. 确认 **pppoe-server session-limit per-vlan** 配置 2. 执行 **display pppoe-server session summary interface** 命令查看当前接口上的 PPPoE 会话数是否已达到 VLAN 允许创建的最大数目 3. 如果非上述原因导致新用户无法上线，请联系 UNIS 技术支持

83.6 PPPOES_LIMIT_IF

日志内容	Maximum number of PPPoE sessions for the interface already reached.
参数解释	无
日志等级	6
举例	PPPOES/6/PPPOES_LIMIT_IF: Maximum number of PPPoE sessions for the interface already reached.
日志说明	PPPoE用户上线已达到接口创建会话最大数目，新用户无法上线
处理建议	1. 确认 **pppoe-server session-limit** 配置 2. 执行 **display pppoe-server session summary interface** 命令查看当前接口上的 PPPoE 会话数是否已达到接口允许创建的最大数目 3. 如果非上述原因导致新用户无法上线，请联系 UNIS 技术支持

83.7 PPPOES_LIMIT_MAC

日志内容	Maximum number of PPPoE sessions for the user already reached.
参数解释	无
日志等级	6
举例	PPPOES/6/PPPOES_LIMIT_MAC: Maximum number of PPPoE sessions for the user already reached.
日志说明	PPPoE用户上线已达到每个用户创建会话最大数目，新用户无法上线
处理建议	1. 确认 **pppoe-server session-limit per-mac** 配置 2. 执行 **display pppoe-server session summary interface** 命令查看当前接口上的 PPPoE 会话数是否已达到用户允许创建的最大数目 3. 如果非上述原因导致新用户无法上线，请联系 UNIS 技术支持

83.8 PPPOES_MAC_THROTTLE

日志内容	The MAC [STRING] triggered MAC throttle on interface [STRING].
参数解释	$1：MAC 地址 $2：接口名称
日志等级	5
举例	PPPOES/5/PPPOES_MAC_THROTTLE: -MDC=1; The MAC 001b-21a8-0949 triggered MAC throttle on interface GigabitEthernet1/2/0/1.
日志说明	在监视时间段内某PPPoE用户建立会话请求数目已达到接入接口允许每个用户会话请求数目的最大值，在扼制时间内接入接口直接丢弃该用户的会话请求
处理建议	1. 确认 **pppoe-server throttle per-mac** 配置 2. 执行 **display pppoe-server throttled-mac** 命令查看用户接入接口上被扼制用户的剩余扼制时间 3. 如果非上述原因导致新用户无法上线，请联系 UNIS 技术支持

83.9 PPPOES_SESSION_ADD_DRIVER_FAILED

日志内容	Failed to add a PPPoE session Ifname=[STRING], SessionID=[UINT16]. Cause: Not enough hardware resources.
参数解释	$1：PPPoE用户上线接口名称 $2：PPPoE会话ID
日志等级	4
举例	PPPOES/4/PPPOES_SESSION_ADD_DRIVER_FAILED: Failed to add a PPPoE session: Ifname=GigabitEthernet1/2/0/1, SessionID=100. Cause: Not enough hardware resources.
日志说明	驱动硬件资源不足导致添加PPPoE会话失败
处理建议	请联系技术支持

83.10 PPPOES_SESSIONS_LOWER_THRESHOLD

日志内容	形式一： The PPPoE session number is below the lower warning threshold (LowerThreshold=[INT32]). 形式二： The PPPoE session number on slot [INT32] is below the lower warning threshold (LowerThreshold=[INT32]). 形式三： The PPPoE session number on chassis [INT32] slot [INT32] is below the lower warning threshold (LowerThreshold=[INT32]).
参数解释	形式一： $1：在线PPPoE会话数目的下限告警阈值 形式二： $1：slot编号 $2：在线PPPoE会话数目的下限告警阈值 形式三： $1：chassis编号 $2：slot编号 $3：在线PPPoE会话数目的下限告警阈值
日志等级	4
举例	PPPOES/4/PPPOES_SESSIONS_LOWER_THRESHOLD: The PPPoE session number is below the lower warning threshold (LowerThreshold=20).
日志说明	形式一： 在线PPPoE会话数目已低于配置的下限告警阈值 形式二： 指定slot上在线PPPoE会话数目已低于配置的下限告警阈值 形式三： 指定chassis内slot上在线PPPoE会话数目已低于配置的下限告警阈值
处理建议	1. 执行 **display pppoe-server session summary** 命令查看 PPPoE 会话摘要信息 2. 确认 PPPoE 用户是否非正常大量下线

83.11 PPPOES_SESSIONS_RECOVER_NORMAL

日志内容	形式一： The PPPoE session number has recovered to normal state. 形式二： The PPPoE session number on slot [INT32] has recovered to normal state. 形式三： The PPPoE session number on chassis [INT32] slot [INT32] has recovered to normal state.
参数解释	无
日志等级	5
举例	PPPOES/5/PPPOES_SESSIONS_RECOVER_NORMAL: The PPPoE session number has recovered to normal state.
日志说明	形式一： 在线PPPoE会话数目重新恢复到设定的正常范围内 形式二： 指定slot上在线PPPoE会话数目从告警状态重新恢复到设定的正常范围 形式三： 指定chassis内slot上在线PPPoE会话数目从告警状态重新恢复到设定的正常范围
处理建议	无

83.12 PPPOES_SESSIONS_UPPER_THRESHOLD

日志内容	形式一： The PPPoE session number is above the upper warning threshold (UpperThreshold=[INT32]). 形式二： The PPPoE session number on slot [INT32] is above the upper warning threshold (UpperThreshold=[INT32]). 形式三： The PPPoE session number on chassis [INT32] slot [INT32] is above the upper warning threshold (UpperThreshold=[INT32]).
参数解释	形式一： $1：在线PPPoE会话数目的上限告警阈值 形式二： $1：slot编号 $2：在线PPPoE会话数目的上限告警阈值 形式三： $1：chassis编号 $2：slot编号 $3：在线PPPoE会话数目的上限告警阈值
日志等级	4
举例	PPPOES/4/ PPPOES_SESSIONS_UPPER_THRESHOLD: The PPPoE session number is above the upper warning threshold (UpperThreshold=20).
日志说明	形式一： 在线PPPoE会话数目已高于配置的上限告警阈值 形式二： 指定slot上在线PPPoE会话数目已高于配置的上限告警阈值 形式三： 指定chassis内slot上在线PPPoE会话数目已高于配置的上限告警阈值
处理建议	1. 执行 **display pppoe-server session summary** 命令查看 PPPoE 会话摘要信息 2. 确认是否存在大量非法 PPPoE 用户上线

84 PTP

本节介绍 PTP 模块输出的日志信息。

84.1 PTP_EXT_TIME_PORT_DISCONNECT

日志内容	The external time port became disconnect. (ExtTimePortType=[STRING])
参数解释	$1：外部时钟源的接口类型，取值包括： ○ ToD0：第一路 ToD 时钟 ○ ToD1：第一路 ToD 时钟
日志等级	4
举例	PTP/4/PTP_EXT_TIME_PORT_DISCONNECT: The external time port became disconnect. (ExtTimePortType=ToD0)
日志说明	设备无法接收到外部时钟源的时钟信号或外部时钟源断开与本端设备的连接
处理建议	请确认连接外部时钟源的PTP接口是否UP： • PTP 接口 UP，则收集告警、日志和配置信息，联系技术支持 • PTP 接口 DOWN，则表示链路故障或接口 DOWN，排除故障恢复链路

84.2 PTP_EXT_TIME_PORT_RECOVER

日志内容	The external time port status resumed. (ExtTimePortType=[STRING])
参数解释	$1：外部时钟源的端口类型，取值包括： ○ ToD0：第一路 ToD 时钟 ○ ToD1：第一路 ToD 时钟
日志等级	4
举例	PTP/4/PTP_EXT_TIME_PORT_RECOVER: The external time port status resumed. (ExtTimePortType=ToD0)
日志说明	设备重新接收到外部时钟源的时钟信号，外部时钟源与本设备相连的物理链路恢复连接
处理建议	无

84.3 PTP_FREQUENCY_LOCK

日志内容	Clock frequency resumed to locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_FREQUENCY_LOCK: Clock frequency resumed to locked state.
日志说明	时钟从频率失锁状态中恢复为正常
处理建议	无

84.4 PTP_FREQUENCY_NOT_LOCK

日志内容	Clock frequency not in locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_FREQUENCY_NOT_LOCK: Clock frequency not in locked state.
日志说明	时钟频率失锁告警，原因包括： • 以太频率同步模式下，参考源频偏过大 • 1588v2 频率同步模式下，时间戳异常 • 系统时钟的输出频率频偏超过+/-10ppm

处理建议	设备打印该告警以后，是否打印了PTP_FREQUENCY_LOCK日志
	• 若查看到 PTP_FREQUENCY_LOCK 日志，则表示设备刚启动或者频率发生震荡，正常告警
	• 若未查看到此日志，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

84.5 PTP_MASTER_CLOCK_CHANGE

日志内容	PTP master clock property changed. (OldMasterClockId=[STRING], CurrentMasterClockId=[STRING], NewSourceIfIndex=[UINT16], OldSourcePortNum=[UINT16], CurrentSourcePortNum=[UINT16], OldSourcePortName=[STRING], CurrentSourcePortName=[STRING])
参数解释	$1：原来主时钟ID $2：当前主时钟ID $3：新的时钟源索引 $4：曾为本设备提供时钟源的接口编号 $5：当前为本设备提供时钟源的接口编号 $6：曾为本设备提供时钟源的接口名称 $7：当前为本设备提供时钟源的接口名称
日志等级	4
举例	PTP/4/PTP_MASTER_CLOCK_CHANGE: PTP master clock property changed. (OldMasterClockId=000FE2-FFFE-FF0000, CurrentMasterClockId=000FE2-FFFE-FF0000, NewSourceIfIndex=1, OldSourcePortNum=2, CurrentSourcePortNum=1, OldSourcePortName=G1/2/0/2, CurrentSourcePortName=G1/2/0/1)
日志说明	主时钟源属性发生改变，原因包括： • PTP 域内的时钟设备属性发生变化，导致出现了优先级更高的时钟源或获取时钟源的路径发生了改变 • 接入了优先级更高的时钟源 • 接收时钟源信号的 PTP 接口所在链路故障或者 PTP 接口 DOWN

处理建议	使用**display ptp interface brief**命令查看是否存在PTP接口处于Disabled状态
	• 若存在接口处于 Disabled 状态，则表示该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文；收集告警、日志和配置信息，联系技术支持
	• 若不存在接口处于 Disabled 状态，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

84.6 PTP_PKT_ABNORMAL

日志内容	Received an abnormal PTP packet.
参数解释	无
日志等级	6
举例	PTP/6/PTP_PKT_ABNORMAL: Received an abnormal PTP packet.
日志说明	设备收到的PTP报文有缺陷，可能因为PTP报文中的TimeSource、TimeTraceable、FreqencyTraceable字段不符合规定
处理建议	**1.** 查看对端设备是否配置 PTP 特殊技术标准 ○ 是：执行步骤 3 ○ 否：执行步骤 2 **2.** 为对端设备配置 PTP 特殊技术标准，等待 20min，查看是否打印 PTP_PKT_ABNORMALCOUNT 日志 ○ 是：执行步骤 4 ○ 否：问题解决 **3.** 等待 20min，查看是否打印 PTP_PKT_ABNORMALCOUNT 日志 ○ 是：执行步骤 4 ○ 否：问题解决 **4.** 收集告警、日志和配置信息，联系技术支持

84.7 PTP_PKT_ABNORMALCOUNT

日志内容	Received [ULONG] abnormal PTP packets in the last 10 minutes.
参数解释	$1：最近十分钟内PTP缺陷报文个数
日志等级	6
举例	PTP/6/PTP_PKT_ABNORMALCOUNT: Received 300 abnormal PTP packets in the last 10 minutes.
日志说明	接收到的PTP缺陷报文数量
处理建议	**1.** 查看对端设备是否配置 PTP 特殊技术标准 ○ 是：执行步骤 3 ○ 否：执行步骤 2 **2.** 为对端设备配置 PTP 特殊技术标准，等待 20min，查看是否继续打印 PTP_PKT_ABNORMALCOUNT 日志 ○ 是：执行步骤 4 ○ 否：问题解决 **3.** 等待 20min，查看是否继续打印 PTP_PKT_ABNORMALCOUNT 日志 ○ 是：执行步骤 4 ○ 否：问题解决 **4.** 收集告警、日志和配置信息，联系技术支持

84.8 PTP_PKTLOST

日志内容	PTP packets were lost. (PktType=[STRING])
参数解释	$1：PTP报文类型，取值包括： ○ Delay_Resp：PTP Delay_Resp 报文 ○ Announce：PTP Announce 报文 ○ Sync：PTP Sync 报文 ○ Pdelay_Resp：PTP Pdelay_Resp 报文
日志等级	4
举例	PTP/4/PTP_PKTLOST: PTP packets were lost. (PktType=Announce)
日志说明	Slave端口检测Announce、Delay_Resp、Sync报文，超过检测时间没有收到报文，则认为报文丢失
处理建议	在打印该日志的PTP从时钟设备上使用**display ptp statistics**命令查看接收报文统计计数是否增长 • 若增长，则表示链路延时过长导致的超时，无须处理 • 若不增长，则在 PTP 主时钟设备使用 **display ptp statistics** 命令查看发送报文统计计数是否增长 ○ 若增长，则表示链路故障导致对端超时没收到报文，排除故障恢复链路 ○ 若不增长，则收集告警、日志和配置信息，联系技术支持

84.9 PTP_PKTLOST_RECOVER

日志内容	PTP packets lost were recovered. (PktType=[STRING])
参数解释	$1：PTP报文类型，取值包括： ○ Delay_Resp：PTP Delay_Resp 报文 ○ Announce：PTP Announce 报文 ○ Sync：PTP Sync 报文 ○ Pdelay_Resp：PTP Pdelay_Resp 报文
日志等级	4
举例	PTP/4/PTP_PKTLOST_RECOVER: PTP packets lost were recovered. (PktType =Announce)
日志说明	从PTP报文丢失告警状态中恢复正常。只有当Slave端口检测Announce、Delay_Resp、Sync报文超时后又重新收到Announce、Delay_Resp报文或者超时时间过长设备自身由从时钟转变为主时钟时，才会打印此日志
处理建议	无

84.10 PTP_PORT_BMCINFO_CHANGE

日志内容	The BMC info for port [UINT16] changed. (PortName=[STRING], PortSourceId=[STRING], PortSourcePortNum=[UINT16], PortSourceStepsRemoved=[UINT16], CurrentMasterClockId=[STRING])
参数解释	$1：PTP接口索引 $2：PTP接口名称 $3：PTP接口接收到的时钟源ID $4：PTP接口接收到的时钟源端口号 $5：PTP接口接收到的时钟源跳数 $6：设备当前主时钟ID
日志等级	5
举例	PTP/5/PTP_PORT_BMCINFO_CHANGE: The BMC info for port 1 changed. (PortName=G1/2/0/1, PortSourceId=000FE2-FFFE-FF0001, PortSourcePortNum=1, PortSourceStepsRemoved=5, CurrentMasterClockId=000FE2-FFFE-FF0000)
日志说明	PTP接口收到的时钟源ID、时钟源端口号或时钟源跳数等时钟源信息发生变化
处理建议	无

84.11 PTP_PORT_STATE_CHANGE

日志内容	PTP port state changed. (IfIndex=[UINT16], PortName=[STRING], PortState=[STRING], OldPortState=[STRING])
参数解释	$1：PTP接口索引 $2：PTP接口名称 $3：PTP接口当前的状态，取值包括： o Master：接口状态为 Master，对外发布时间信息 o Slave：接口状态为 Slave，跟踪外部时间信息 o Passive：接口状态为 Passive（接口收到对端的 Announce 报文后，计算出的状态），不跟踪外部时间信息，也不对外发布时间信息 o Listening：接口状态为 Listening（接口初始化后，即进入 Listening 状态），不跟踪外部时间信息，也不对外发布时间信息 o Faulty：接口状态为 Faulty，该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文 o Initializing：接口状态为 Initializing，接口位于初始化状态，接口不处理协议报文 o Premaster：接口状态为 Premaster，Master 状态前的临时状态 o Disable：接口状态为Disabled，接口上PTP协议未运行，接口不处理协议报文 o Uncalibrated：接口状态为 Uncalibrated，Slave 状态前的临时状态 o $4：PTP 接口变化前的状态，取值包括： o Master：接口状态为 Master，对外发布时间信息 o Slave：接口状态为 Slave，跟踪外部时间信息 o Passive：接口状态为 Passive（接口收到对端的 Announce 报文后，计算出的状态），不跟踪外部时间信息，也不对外发布时间信息 o Listening：接口状态为 Listening（接口初始化后，即进入 Listening 状态），不跟踪外部时间信息，也不对外发布时间信息 o Faulty：接口状态为 Faulty，该状态为 PTP 协议的错误状态（即检测到错误），接口不处理 PTP 协议报文 o Initializing：接口状态为 Initializing，接口位于初始化状态，接口不处理协议报文 o Premaster：接口状态为 Premaster，Master 状态前的临时状态 o Disable：接口状态为Disabled，接口上PTP协议未运行，接口不处理协议报文 o Uncalibrated：接口状态为 Uncalibrated，Slave 状态前的临时状态
日志等级	5
举例	PTP/5/PTP_PORT_STATE_CHANGE: PTP port state changed. (IfIndex=1, PortName=G1/2/0/1, PortState=Slave, OldPortState=Master)
日志说明	PTP接口状态发生改变，原因包括： • PTP 域内的时钟设备属性发生变化，比如优先级、时钟等级、时钟精度、接口的 NotSlave 属性等 • 接入了优先级更高的时钟源 • PTP 接口所在链路故障或者 PTP 接口 DOWN
处理建议	使用**display ptp interface brief**命令查看是否存在PTP接口处于Fault状态 • 若存在接口处于 Fault 状态，则表示链路故障或接口 DOWN，排除故障恢复链路

	• 若不存在接口处于 Fault 状态，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

84.12 PTP_SRC_CHANGE

日志内容	Clock source property changed. (SourceName=[STRING], Priority1=[UCHAR], Priority2=[UCHAR], ClockClass=[UINT16], ClockAccuracy=[UINT16]], ClockSourceType=[STRING])

参数解释	$1：时钟源，取值包括：
	  ○ Local：本地时钟
	  ○ Tod1：第一路 ToD 时钟
	  ○ Tod2：第二路 ToD 时钟
	$2：第一优先级
	$3：第二优先级
	$4：时钟源的时间等级
	$5：时钟源的时间精度
	$6：最优时钟的时钟类别，取值包括：
	  ○ Atomic clock：原子时钟
	  ○ GPS：Global Positioning System，全球定位系统
	  ○ Handset：手持设备
	  ○ Internal oscillator：内部震荡器
	  ○ NTP：Network Time Protocol，网络时间协议
	  ○ Other：其他
	  ○ PTP：Precision Time Protocol，精确时间协议
	  ○ Terrestrial radio：陆基无线电
	  ○ Unknown：未知

日志等级	5
举例	PTP/5/PTP_SRC_CHANGE: Clock source property changed. (SourceName=Tod1, Priority1=1, Priority2=2, ClockClass=6, ClockAccuracy=20, ClockSourceType=Atomic clock)
日志说明	时钟源属性发生改变，原因包括： • 用户通过命令行改变时钟源属性 • 接收到了精度更高的外接时钟源
处理建议	无

84.13 PTP_SRC_CLASS_BELOW_THRESHOLD

日志内容	The clock source class fell below the threshold.
参数解释	无
日志等级	4
举例	PTP/4/PTP_SRC_CLASS_BELOW_THRESHOLD: The clock source class fell below the threshold.
日志说明	时钟源劣化告警阈值，原因包括： • 当设备通过 PTP 输入接口中分组报文获取时钟源时，当前选用 PTP 本地时钟源的时钟等级低于时钟等级阈值，且 PTP 时钟源的 stepsRemoved 值为 0 • 当设备通过 TOD 输入接口获取时钟源时，当前选用 TOD 外接时钟源的时钟等级低于时钟等级阈值
处理建议	使用**display ptp clock**命令，查看Class字段显示当前时钟源等级是否低于告警阈值 • 若低于告警阈值，在时钟源所在设备上调高时钟等级或者切换时钟源为时钟等级更高的时钟源，查看告警是否打印 PTP_SRC_CLASS_RECOVER 日志 o 若查看到 PTP_SRC_CLASS_RECOVER 日志，正常告警 o 若未查看到此日志，则收集告警、日志和配置信息，联系技术支持 • 若高于告警阈值，收集告警、日志和配置信息，联系技术支持

84.14 PTP_SRC_CLASS_RECOVER

日志内容	The clock source class crossed the threshold.
参数解释	无
日志等级	4
举例	PTP/4/PTP_SRC_CLASS_RECOVER: The clock source class crossed the threshold.
日志说明	时钟源输入时钟等级高于或者等于劣化告警阈值
处理建议	无

84.15 PTP_SRC_SWITCH

日志内容	Clock source switched. (LastClockID=[STRING], CurrentClockID=[STRING])
参数解释	$1：原来的时钟源ID $2：当前的时钟源ID
日志等级	4
举例	PTP/4/PTP_SRC_SWITCH: Clock source switched.(LastSource=000FE2-FFFE-FF0000, CurrentSource=000FE2-FFFE-FF0001)
日志说明	新的更好的时钟源加入PTP域，设备跟踪的时钟源发生切换
处理建议	无

84.16 PTP_TIME_LOCK

日志内容	Time resumed to locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIME_LOCK: Time resumed to locked state.
日志说明	时钟从失锁状态中恢复为正常
处理建议	无

84.17 PTP_TIME_NOT_LOCK

日志内容	Time not in locked state.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIME_NOT_LOCK: Time not in locked state.
日志说明	时钟失锁告警，原因包括： • 频率失锁 • 子卡逻辑或者时钟扣板硬件故障 • DSP 收到的时间戳不变或者时戳错误

处理建议	检查PTP Slave接口是否链路故障或接口DOWN
	• 若链路故障或接口 DOWN，排除故障恢复链路
	• 接口正常，则查看 PTP 配置信息是否发生改变
	  ○ 若 PTP 配置信息发生改变，则恢复配置
	  ○ 若 PTP 配置信息未发生改变，则收集告警、日志和配置信息，联系技术支持

84.18 PTP_TIME_OFFSET_EXCEED_THRESHOLD

日志内容	The PTP time offset exceeded the threshold. (TimeOffset=[UINT16], AlarmThresholdTimeOffset=[UINT16])
参数解释	$1：源绝对时间差 $2：源绝对时间差告警阈值
日志等级	4
举例	PTP/4/PTP_TIME_OFFSET_EXCEED_THRESHOLD: The PTP time offset exceeded the threshold. (TimeOffset=500, AlarmThresholdTimeOffset=400)
日志说明	PTP源绝对时间差超过阈值。比较外部基准参考时间和PTP时间，获取两者时间差值，差值超过时间偏差告警阈值，则打印此信息
处理建议	使用**ptp asymmetry-correction**命令配置非对称延迟校正时间，调整当前设备的PTP时钟源时间，使与外部基准时间一致，查看设备是否打印PTP_TIME_OFFSET_RECOVER日志 • 若查看到 PTP_TIME_OFFSET_RECOVER 日志，则问题解决 • 若未查看到此日志，则收集告警、日志和配置信息，联系技术支持

84.19 PTP_TIME_OFFSET_RECOVER

日志内容	The PTP standard time offset resumed. (TimeOffset=[UINT16], AlarmThresholdTimeOffset=[UINT16])
参数解释	$1：源绝对时间差 $2：源绝对时间差告警阈值
日志等级	4
举例	PTP/4/PTP_STANDARD_TIME_OFFSET_RECOVER: The PTP standard time offset resumedl. (TimeOffset=300, AlarmThresholdTimeOffset=400)
日志说明	PTP源绝对时间差恢复为正常状态
处理建议	无

84.20 PTP_TIME_SYNC

日志内容	Time resumed to synchronized state.
参数解释	无
日志等级	4
举例	PTP/4/PTP_TIME_SYNC: Time resumed to synchronized state.
日志说明	设备恢复到时钟同步的正常状态
处理建议	无

84.21 PTP_TIME_UNSYNC

日志内容	Time changed to unsynchronized state.
参数解释	无
日志等级	4
举例	PTP/4/PTP_TIME_UNSYNC: Time changed to unsynchronized state.
日志说明	设备处于无法进行时钟同步的状态，原因包括： • 链路故障或者接口 DOWN 导致设备没有跟踪的时钟源 • 本设备时钟源优先级配置得太高，使得本设备处于 local 状态，无法同步其他设备的时间信号
处理建议	1. 使用 **displsy ptp interface brief** 命令查看设备是否存在 PTP Slave 接口 o 是：请联系技术支持 o 否：执行步骤 2 2. 使用 **display ptp clock** 命令，查看 Clock type 字段显示是否为 ToD 外接时钟源类型 o 是：执行步骤 3 o 否：设备没有时钟源可以同步，正常打印 3. 检查是否通过 **ptp { tod0 | tod1 } input** 命令配置了 ToD 时钟信号的入方向接收延迟校正时间 o 是：请联系技术支持 o 否：执行步骤 4 4. 执行 **ptp { tod0 | tod1 } input** 命令校正 ToD 时钟信号为入方向接收延迟校正时间，查看设备是否打印 PTP_TIME_SYNC 日志 o 是：问题解决 o 否：收集告警、日志和配置信息，联系技术支持

84.22 PTP_TIMESTAMP_CHANGE

日志内容	The timestamp state turned to normal.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIMESTAMP_CHANGE: The timestamp state turned to normal.
日志说明	本设备接收到的报文中携带的时间戳恢复为持续变化，时间戳状态正常 正常情况下设备接收到的PTP报文中的时间戳是持续变化的，当时间戳不变化时表示状态异常，只有时间戳从异常状态恢复到正常状态时，才会输出该日志
处理建议	无

84.23 PTP_TIMESTAMP_UNCHANGE

日志内容	The timestamp state turned to abnormal.
参数解释	无
日志等级	3
举例	PTP/3/PTP_TIMESTAMP_UNCHANGE: The timestamp state turned to abnormal.
日志说明	本设备接收到的报文中携带的时间戳不变化，时间戳状态异常 正常情况下设备接收到的PTP报文中的时间戳是持续变化的，当时间戳不变化时表示状态异常

处理建议	使用**display ptp statistics**命令查看Sync报文统计计数是否增长
	• 若增长，则收集告警、日志和配置信息，并联系技术支持
	• 若不增长，则检查链路是否故障，并待链路故障解除后，查看设备是否打印PTP_TIMESTAMP_CHANGED 日志
	  ○ 若查看到 PTP_TIMESTAMP_CHANGED 日志，则表示时间戳状态恢复正常
	  ○ 若未查看到此日志，则收集告警、日志和配置信息，联系技术支持

84.24 PTP_TIMOFFSUM_PK-PK_ALARM

日志内容	The PTP time offset sum exceeded the threshold. (TimeOffsetSum=[UINT16], TimeOffsetSumAlarmThreshold=[UINT16])
参数解释	$1：PTP时间偏差累加和峰峰值 $2：PTP时间偏差累加和峰峰值的告警阈值
日志等级	4
举例	PTP/4/PTP_TIMOFFSUM_PK-PK_ALARM: The PTP time offset sum exceeded the threshold. (TimeOffsetSum=500, TimeOffsetSumAlarmThreshold=400)
日志说明	PTP时间偏差累加和峰峰值超过阈值

处理建议	**1.** 查看当前时间是否处于锁定状态
	  ○ 是：执行步骤 3
	  ○ 否：执行步骤 2
	2. 等待 15 分钟，当前时间是否处于锁定状态
	  ○ 是：执行步骤 3
	  ○ 否：执行步骤 4
	3. 等待 15 分钟，查看告警是否恢复（是否打印 PTP_TIMOFFSUM_RECOVER 日志）
	  ○ 是：问题解决
	  ○ 否：执行步骤 4
	4. 收集告警、日志和配置信息，联系技术支持

84.25 PTP_TIMOFFSUM_PK-PK_RECOVER

日志内容	The PTP time offset sum resumed. (TimeOffsetSum=[UINT16], TimeOffsetSumAlarmThreshold=[UINT16])
参数解释	$1：PTP时间偏差累加和峰峰值 $2：PTP时间偏差累加和峰峰值的告警阈值
日志等级	4
举例	PTP/4/PTP_TIMOFFSUM_PK-PK_RECOVER: The PTP time offset sum resumedl. (TimeOffsetSum=300, TimeOffsetSumAlarmThreshold=400)
日志说明	PTP时间偏差累加和峰峰值恢复为正常状态
处理建议	无

85 PWDCTL

本节介绍 Password control 模块输出的日志信息。

85.1 PWDCTL_ADD_BLACKLIST

日志内容	[STRING] was added to the blacklist for failed login attempts.
参数解释	$1：用户名
日志等级	6
举例	PWDCTL/6/PWDCTRL_ADD_BLACKLIST: hhh was added to the blacklist for failed login attempts.
日志说明	因为用户输入密码错误，用户登录设备失败，被加入密码控制黑名单
处理建议	无

85.2 PWDCTL_CHANGE_PASSWORD

日志内容	[STRING] changed the password because [STRING].
参数解释	$1：用户名 $2：更改密码原因 o it was the first login of the account：用户首次登录 o the password had expired：密码已经过期 o the password was too short：密码长度过短 o the password was not complex enough：密码复杂度不满足要求 o the password was default password：密码是缺省密码
日志等级	6
举例	PWDCTL/6/PWDCTL_CHANGE_PASSWORD: hhh changed the password because It is the first login of the account.
日志说明	由于某种原因，用户改变用户密码。例如该用户的账户第一次登录设备
处理建议	无

85.3 PWDCTL_FAILED_TO_OPENFILE

日志内容	Failed to create or open the password file.
参数解释	无
日志等级	3
举例	PWDCTL/3/PWDCTL_FAILED_TO_OPENFILE: Failed to create or open the password file.
日志说明	因文件系统异常导致创建或打开*.dat文件失败
处理建议	请检查设备文件系统存储空间是否充足

85.4 PWDCTL_FAILED_TO_WRITEPWD

日志内容	Failed to write the password records to file.
参数解释	无
日志等级	3
举例	PWDCTL/3/PWDCTL_FAILED_TO_WRITEPWD: Failed to write the password records to file.
日志说明	设备无法将用户密码写入密码记录文件
处理建议	请检查设备文件系统存储空间是否充足

85.5 PWDCTL_NOENOUGHSPACE

日志内容	Not enough free space on the storage media where the file is located.
参数解释	无
日志等级	3
举例	PWDCTL/3/PWDCTL_NOENOUGHSPACE: Not enough free space on the storage media where the file is located.
日志说明	配置失败，因为*.dat文件所在介质（Flash或CF卡等）存储空间不足
处理建议	请检查设备文件系统存储空间是否充足

85.6 PWDCTL_NOTFOUNDUSER

日志内容	Can't find the username in the file.
参数解释	无
日志等级	3
举例	PWDCTL/3/PWDCTL_NOTFOUNDUSER: Can't find the username in the file.
日志说明	本地用户密码设置失败，因为在*.dat文件中获取不到该用户信息
处理建议	重新创建一个本地用户或关闭Password Control功能后再重新开启Password Control功能

85.7 PWDCTL_UPDATETIME

日志内容	Last login time updated after clock update.
参数解释	无
日志等级	6
举例	PWDCTL/6/ PWDCTL_UPDATETIME: Last login time updated after clock update.
日志说明	用户最近登录时间已同步更新
处理建议	无

86 QOS

本节介绍 QoS 模块输出的日志信息。

86.1 EDSG_CONFIG_CONFLICT

日志内容	Failed to activate EDSG service policy [UINT32] on user [UINT32]. The EDSG service policy conflicts with existing configurations in the [STRING] direction.
参数解释	$1：EDSG业务策略ID $2：User ID $3：下发方向
日志等级	3
举例	QOS/3/EDSG_ CONFIG_CONFLICT: Failed to activate EDSG service policy 1 on user 0x30000072. The EDSG service policy conflicts with existing configurations in the outbound direction.
日志说明	• EDSG 业务策略与 User-profile 视图下的 QMProfile、GTS 或 qos queue 两两互斥 • EDSG 业务策略与用户上线接口上配置的 HQoS 互斥
处理建议	• 如果 User-profile 视图下存在 QMProfile、GTS 或 qos queue 的配置，请调整这部分配置 • 如果用户上线接口视图下存在 HQoS 配置，请调整 HQoS 配置

86.2 EDSG_EXCEED_LIMIT

日志内容	Failed to activate EDSG service policy [UINT32] on user [UINT32]. The EDSG service policy ID is out of range.
参数解释	$1：EDSG业务策略ID $2：User ID
日志等级	3
举例	QOS/3/EDSG_ EXCEED_LIMIT: Failed to activate EDSG service policy 1 on user 0x30000072. The EDSG service policy ID is out of range.
日志说明	EDSG业务策略应用失败，原因是：RADIUS服务器下发的EDSG业务策略ID不在设备支持的范围内
处理建议	请根据业务板类型确认设备是否支持在同一用户上激活多个EDSG业务策略： • 同一用户上仅支持激活一个 EDSG 业务策略，则策略 ID 取值必须为 1 • 同一用户上支持激活 N 个 EDSG 业务策略，则策略 ID 取值范围为 1～N 修改RADIUS服务器下发的EDSG业务策略ID为设备支持的合理范围

86.3 EDSG_LRMODE_CONFLICT

日志内容	Failed to activate EDSG service policy [UINT32] on user [UINT32]. The rate limit mode for the EDSG service policy is different from the rate limit mode for an existing EDSG service policy.
参数解释	$1：EDSG业务策略ID $2：User ID
日志等级	3
举例	QOS/3/EDSG_LRMODE_CONFLICT: Failed to activate EDSG service policy 1 on user 0x30000072. The rate limit mode for the EDSG service policy is different from the rate limit mode for an existing EDSG service policy.
日志说明	EDSG业务策略应用失败，原因是：RADIUS服务器下发EDSG业务策略的流量限速模式不一致，后下发的EDSG业务策略应用失败
处理建议	请修改RADIUS服务器下发的EDSG业务策略的流量限速模式

86.4 EDSG_MODE_CONFLICT

日志内容	Failed to activate EDSG service policy [UINT32] on user [UINT32]. The status of the separate rate limiting function for the EDSG service policy is different from the status of this function for an existing EDSG service policy.
参数解释	$1：EDSG业务策略ID $2：User ID
日志等级	3
举例	QOS/3/EDSG_ EXCEED_LIMIT: Failed to activate EDSG service policy 1 on user 0x30000072. The status of the separate rate limiting function for the EDSG service policy is different from the status of this function for an existing EDSG service policy.
日志说明	EDSG业务策略应用失败，原因是：RADIUS服务器下发EDSG业务策略的双栈业务流量独立限速功能状态不一致，后下发的EDSG业务策略应用失败
处理建议	无

86.5 EDSG_NOT_SUPPORT

日志内容	Failed to activate service [UINT32] on user [UINT32]. The EDSG service policy is not supported.
参数解释	$1：EDSG业务策略ID $2：User ID
日志等级	3
举例	QOS/3/EDSG_NOT_SUPPORT: Failed to activate service 1 on user 0x30000072. The EDSG service policy is not supported.
日志说明	EDSG业务策略应用失败，原因是：不支持EDSG业务限速（together模式下的带内带宽）下发
处理建议	建议用户从其他类型接口上线

86.6 QOS_CAR_APPLYIF_FAIL

日志内容	[STRING]; Failed to apply the [STRING] CAR in [STRING] profile [STRING] to interface [STRING]. Reason: [STRING].

参数解释	$1：CAR应用的端口信息
	$2：CAR应用方向
	• inbound：表示入方向
	• outbound：表示出方向
	$3：Profile类型，取值为user
	$4：Profile名称
	$5：接口名称
	$6：失败原因
	  ○ The CAR is not supported：不支持 CAR
	  ○ The resources are insufficient：资源不足

日志等级	4
举例	QOS/4/QOS_CAR_APPLYIF_FAIL: Port=GigabitEthernet1/2/0/1; Failed to apply the inbound CAR in user profile a to interface GigabitEthernet1/2/0/1. Reason: The resources are insufficient.
日志说明	• 接口下应用 user profile 时，下发配置的 CAR 信息失败 • 接口下已经应用 user profile，在该 user profile 下增加或修改 CAR 配置失败
处理建议	删除profile下的CAR配置或修改CAR的相关参数

86.7 QOS_CAR_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] CAR in [STRING] profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：CAR应用方向 $3：Profile类型 $4：Profile名称 $5：失败原因
日志等级	4
举例	QOS/4/QOS_CAR_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN=”N/A”-Port=GigabitEthernet1/2/0/5; Failed to apply the inbound CAR in user profile a to the user. Reason: The resources are insufficient.
日志说明	• 用户上线，下发配置的 CAR 信息失败 • 用户已经上线，修改 CAR 信息或者增加 CAR 应用失败
处理建议	取消CAR在profile下的应用或者修改CAR的相关参数信息

86.8 QOS_CBWFQ_REMOVED

日志内容	CBWFQ is removed from [STRING].
参数解释	$1：接口名称
日志等级	3
举例	QOS/3/QOS_CBWFQ_REMOVED: CBWFQ is removed from GigabitEthernet1/2/0/1.
日志说明	因接口最大带宽或接口速率更改后低于接口上原来配置的CBWFQ要求的带宽或速率，系统从接口上删除CBWFQ
处理建议	增大接口最大带宽或接口速率后重新应用被删除的CBWFQ

86.9 QOS_DIFFSERV_CFG_FAIL

日志内容	Failed to configure the MPLS Diffserv mode in VPN instance [STRING]. Reason: [STRING].
参数解释	$1：VPN实例名称 $2：失败原因： ○ 业务板不支持配置 MPLS 的差分服务模式：The card does not support MPLS Diffserv mode
日志等级	4
举例	QOS/4/QOS_DIFFSERV_CFG_FAIL: -MDC=1-Chassis=1-Slot=5; Failed to configure the MPLS Diffserv mode in VPN instance vpn1. Reason: The card does not support MPLS Diffserv mode.
日志说明	在VPN实例中配置MPLS的差分服务模式失败
处理建议	无

86.10 QOS_GTS_APPLYIF_FAIL

日志内容	[STRING]; Failed to apply the [STRING] GTS in [STRING] profile [STRING] to interface [STRING]. Reason: [STRING].
参数解释	$1：用户标识信息 $2：GTS应用方向 • inbound：表示入方向 • outbound：表示出方向 $3：Profile类型，取值为user $4：User profile名称 $5：接口名称 $6：失败原因 ○ The resources are insufficient.：资源不足 ○ The configuration in the user profile to be applied conflicts with the existing configuration on the interface.：与接口上的 GTS 配置冲突
日志等级	4
举例	QOS/4/QOS_GTS_APPLYIF_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet1/2/0/5; Failed to apply the inbound GTS in user profile u1 to interface GigabitEthernet1/2/0/5. Reason: The resources are insufficient.
日志说明	• 接口下应用 User Profile，User Profile 中配置的 GTS 下发失败 • 接口下已经应用 User Profile，修改 GTS 配置或者增加 GTS 应用失败
处理建议	取消GTS在user profile下的应用或者修改GTS的相关参数信息

86.11 QOS_GTS_APPLYINT_FAIL

日志内容	Failed to apply the gts configuration to the interface [STRING]. [STRING]
参数解释	$1：接口名称 $2：失败原因
日志等级	4
举例	QOS/4/QOS_GTS_APPLYINT_FAIL; Failed to apply the gts configuration to the interface Route-Aggregation1. The operation is not supported.
日志说明	单板上的接口不支持应用GTS
处理建议	无

86.12 QOS_GTS_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] GTS to the traffic of user profile a in [STRING] in [STRING] profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：GTS应用方向 $3：GTS应用范围 $4：Profile类型 $5：User profile名称 $6：失败原因 ○ The resources are insufficient.：资源不足 ○ The GTS configuration conflicts with the CAR configuration in an EDSG service policy.：在同一个 EDSG 业务策略中，流量整形与流量监管冲突
日志等级	4
举例	QOS/4/QOS_GTS_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet1/2/0/5; Failed to apply the inbound GTS to the traffic of session group profile a in queue 0. Reason: The GTS configuration conflicts with the CAR configuration in an EDSG service policy.
日志说明	• 用户上线，下发配置的 GTS 失败 • 用户已经上线，修改 GTS 配置或者增加 GTS 应用失败 • 用户已经上线，GTS 的配置与 EDSG 业务流量监管配置冲突
处理建议	取消GTS在user profile下的应用或者修改GTS的相关参数信息

86.13 QOS_ITACAR_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the ITA CAR at level [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：ITA CAR的级别 $3：失败原因
日志等级	4
举例	QOS/4/QOS_ITACAR_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-SVLAN=100-Port=GigabitEthernet1/2/0/5; Failed to apply the ITA CAR at level 7 to the user. Reason: The ITA CAR is not supported.
日志说明	• 通过 COA 消息，RADIUS 服务器为已上线用户授权 ITA 业务策略，ITA 业务策略中流量计费级别的流量监管应用失败 • 通过 COA 消息，RADIUS 服务器修改已上线用户 ITA 业务策略，ITA 业务策略中流量计费级别的流量监管参数修改失败
处理建议	RADIUS服务器取消应用ITA业务策略或者修改ITA业务策略中流量计费级别的流量监管参数

86.14 QOS_LR_APPLYIF_CONFIGFAIL

日志内容	Failed to apply the rate limiting configuration to the [STRING] direction of the interface [STRING]. [STRING].
参数解释	$1：流量方向 $2：接口名称 $3：失败原因
日志等级	4
举例	QOS/4/QOS_LR_APPLYIF_CONFIGFAIL: Failed to apply the rate limiting configuration to the outbound direction of the interface Bridge-Aggregation 1. The operation is not supported.
日志说明	LR限速配置应用到接口上，某些板可能会下发失败
处理建议	请根据失败原因，修改限速配置

86.15 QOS_LR_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] rate limit to the traffic of user profile [STRING] in all queues. Reason: [STRING]
参数解释	$1：用户标识信息 $2：限速应用方向 $3：User profile名称 $5：失败原因 ○ The resources are insufficient.：资源不足 ○ The rate limit is not supported.：不支持对用户配置限速 ○ The rate limit configuration conflicts with the CAR configuration in a EDSG service policy.：限速配置与 EDSG 业务流量监管配置冲突
日志等级	4
举例	QOS/4/QOS_LR_APPLYUSER_FAIL: -MDC=1-Slot=3; -MAC=0010-9400-1f38-VPN=N/A-SVLAN=4008-CVLAN=992-Port=Route-Aggregation1024.4093; Failed to apply the outbound rate limit to the traffic of user profile u1 in all queues. Reason: The resources are insufficient.
日志说明	通过**qos user-queue**命令配置的限速： • 用户上线，下发配置的限速失败 • 用户已经上线，修改限速配置或者增加限速应用失败 • 用户已经上线，限速配置与 EDSG 业务流量监管配置冲突
处理建议	取消限速在user profile下的应用或者修改限速的相关参数信息

86.16 QOS_MEMORY_WARNING

日志内容	The system does not have enough memory.
参数解释	无
日志等级	4
举例	QOS/4/QOS_MEMORY_WARNING: The system does not have enough memory.
日志说明	QoS响应系统内存门限告警
处理建议	等待系统内存恢复

86.17 QOS_NOT_ENOUGH_BANDWIDTH

日志内容	Policy [STRING] requested bandwidth [UINT32](kbps). Only [UINT32](kbps) is available on [STRING].
参数解释	$1：QoS策略名称 $2：CBWFQ需要的带宽 $3：接口可用带宽 $4：接口名称
日志等级	3
举例	QOS/3/QOS_NOT_ENOUGH_BANDWIDTH: Policy d requested bandwidth 10000(kbps). Only 80(kbps) is available on GigabitEthernet1/2/0/1.
日志说明	因CBWFQ要求的带宽大于接口最大带宽，CBWFQ配置失败
处理建议	增大接口最大带宽值或减小CBWFQ要求的带宽值

86.18 QOS_POLICY_APPLYCOPP_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of control plane slot [UINT32]. [STRING].
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：槽位号 $5：失败原因 ○ The behavior is empty：流行为为空 ○ Only one rate-limiting action is supported in one behavior to be applied to the control plane：一个流行为中仅支持配置一个限速动作
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYCOPP_CBFAIL: Failed to apply classifier-behavior d in policy b to the inbound direction of control plane slot 3. The behavior is empty.
日志说明	系统在控制平面的某个方向上应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

86.19 QOS_POLICY_APPLYCOPP_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of control plane slot [UINT32]. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：槽位号 $4：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYCOPP_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of control plane slot 3. The operation is not supported.
日志说明	系统在控制平面的某个方向上应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

86.20 QOS_POLICY_APPLYGLOBAL_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction globally. [STRING].
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYGLOBAL_CBFAIL: Failed to apply classifier-behavior a in policy b to the outbound direction globally. The behavior is empty.
日志说明	系统在某个方向上全局应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

86.21 QOS_POLICY_APPLYGLOBAL_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction globally. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYGLOBAL_FAIL: Failed to apply or refresh QoS policy b to the inbound direction globally. The operation is not supported.
日志说明	系统在某个方向上全局应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

86.22 QOS_POLICY_APPLYIF_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of interface [STRING]. [STRING].
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：接口名称 $5：失败原因 ○ The behavior is empty.：流行为为空，未配置任何动作 ○ Only one service class marking action is supported for the same EXP value on the same interface and the service class value can't be modified except that the old value has been deleted.：对于同一个 EXP 值，同一接口上仅支持配置一个重新标记报文的 MPLS TE 隧道转发类值的动作；且仅支持通过删除并重新配置的方式进行修改
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYIF_CBFAIL: Failed to apply classifier-behavior b in policy b to the inbound direction of interface Ethernet1/2/0/2. The behavior is empty.
日志说明	系统在接口的某个方向上应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

86.23 QOS_POLICY_APPLYIF_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of interface [STRING]. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：接口名称 $4：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYIF_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of interface Ethernet1/2/0/2. The operation is not supported.
日志说明	系统在接口的某个方向上应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

86.24 QOS_POLICY_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] QoS policy [STRING] in user profile [STRING] to the user.Reason: [STRING].
参数解释	$1：用户标识信息 $2：QoS policy应用方向 $3：QoS policy名称 $4：User profile名称 $5：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet1/2/0/5; Failed to apply the inbound QoS policy p in user profile a to the user.Reason: The QoS policy is not supported.
日志说明	• 用户上线，下发配置的 QoS policy 信息失败 • 用户已经上线，修改 QoS Policy 信息或者增加 QoS Policy 应用失败
处理建议	取消QoS policy在User profile下的应用或者修改QoS Profile的信息

86.25 QOS_POLICY_APPLYVLAN_CBFAIL

日志内容	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of VLAN [UINT32]. [STRING].
参数解释	$1：CB对名称 $2：QoS策略名称 $3：流量方向 $4：VLAN ID $5：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYVLAN_CBFAIL: Failed to apply classifier-behavior b in policy b to the inbound direction of VLAN 2. The behavior is empty.
日志说明	系统在VLAN的某个方向上应用或更新QoS策略中的某个CB对失败
处理建议	请根据失败原因，修改策略中的配置

86.26 QOS_POLICY_APPLYVLAN_FAIL

日志内容	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of VLAN [UINT32]. [STRING].
参数解释	$1：QoS策略名称 $2：流量方向 $3：VLAN ID $4：失败原因
日志等级	4
举例	QOS/4/QOS_POLICY_APPLYVLAN_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of VLAN 2. The operation is not supported.
日志说明	系统在VLAN的某个方向上应用或更新QoS策略失败
处理建议	请根据失败原因，修改策略中的配置

86.27 QOS_PRIORITY_APPLYUSER_FAIL

日志内容	Failed to identify the [STRING] priority of the user. Reason: [STRING].
参数解释	$1：流量方向 $2：失败原因
日志等级	4
举例	QOS/4/QOS_PRIORITY_APPLYUSER_FAIL: Failed to identify the inbound priority of the user. Reason: The priority type is not supported.
日志说明	根据用户的优先级在入方向修改该用户对应报文的优先级失败或者根据用户优先级入队列失败
处理建议	取消根据用户优先级入队列或者修改该用户对应报文的优先级

86.28 QOS_PROFILE_AUTHOR_FAIL

日志内容	[STRING]; Failed to authorize the QoS configuration to the user. Reason: [STRING]
参数解释	$1：用户标识信息 $2：失败原因 ○ The session group profile conflicts with the user profile configured with user queue settings.：已配置用户队列的 User Profile 和 Session Group Profile 冲突
日志等级	4
举例	QOS/4/QOS_PROFILE_AUTH_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN=”N/A”-Port=GigabitEthernet1/2/0/5; Failed to authorize the QoS configuration to the user. Reason: The session group profile conflicts with the user profile configured with user queue settings.
日志说明	对上线用户同时授权已配置用户队列的User Profile和Session Group Profile时会冲突，导致User Profile、Session Group Profile及其他相关QoS配置均授权失败
处理建议	• 通过 **display access-user** 命令查看接入用户的信息，定位到授权失败（inactive）的Profile • 修改冲突配置，不要对上线用户同时授权已配置用户队列的 User Profile 和 Session Group Profile

86.29 QOS_PROFILE_NOTEXIST

日志内容	[STRING]; The [STRING] profile [STRING] doesn't exist.
参数解释	$1：用户标识信息 $2：Profile类型 ○ user ○ session group $3：Profile名称
日志等级	4
举例	QOS/4/QOS_PROFILE_NOTEXIST: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN=”N/A”-Port=GigabitEthernet1/2/0/5; The user profile a doesn't exist.
日志说明	授权的User Profile或Session Group Profile不存在
处理建议	创建对应的User Profile或Session Group Profile

86.30 QOS_QMPROFILE_APPLYIF_FAIL

日志内容	[STRING]; Failed to apply the [STRING] queue scheduling profile [STRING] in [STRING] profile [STRING] to the interface [STRING]. Reason: [STRING].
参数解释	$1：用户标识信息 $2：QMProfile方向 • inbound：表示入方向 • outbound：表示出方向 $3：QMProfile名称 $4：Profile类型，取值为user $5：Profile名称 $6：接口名称 $7：失败原因 • The QMProfile is not supported.：不支持 • The configuration in the user profile to be applied conflicts with the existing configuration on the interface.：应用的 User Profile 与接口上已存在的配置冲突
日志等级	4
举例	QOS/4/QOS_QMPROFILE_APPLYIF_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-SVLAN=100-Port=GigabitEthernet1/2/0/5; Failed to apply the inbound queue scheduling profile b in user profile a to interface GigabitEthernet1/2/0/5. Reason: The QMProfile is not supported. QOS/4/QOS_QMPROFILE_APPLYIF_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet1/2/0/5; Failed to apply the inbound queue scheduling profile b in user profile a to interface GigabitEthernet1/2/0/5. Reason: The configuration in the user profile to be applied conflicts with the existing configuration on the interface.
日志说明	• 接口下应用 User Profile，User Profile 中配置的 QMProfile 下发失败 • 接口下已经应用 User Profile，修改 QMProfile 配置或者增加 QMProfile 应用失败
处理建议	取消QMProfile在profile下的应用或者修改QMProfile的相关信息

86.31 QOS_QMPROFILE_APPLYINT_FAIL

日志内容	Failed to apply the queue management profile to the [STRING] direction of interface [STRING]. [STRING]
参数解释	$1：流量方向，包括： • inbound • outbound $2：接口名称 $3：失败原因，包括： • 单板上的接口不支持应用队列调度策略 • 资源不足导致接口应用队列调度策略失败
日志等级	4
举例	QOS/4/QOS_QMPROFILE_APPLYINT_FAIL: Failed to apply the queue management profile to the outbound direction of interface Route-Aggregation1. The operation is not supported.
日志说明	单板上的接口不支持应用队列调度策略
处理建议	设备资源不足时，请删除部分已应用的ACL规则，释放部分资源

86.32 QOS_QMPROFILE_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply queue management profile [STRING] in [STRING] profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：Queue management Profile名称 $3：Profile类型 $4：Profile名称 $5：失败原因
日志等级	4
举例	QOS/4/QOS_QMPROFILE_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-SVLAN=100-Port=GigabitEthernet1/2/0/5; Failed to apply queue management profile b in session group profile a to the user. Reason: The QMProfile is not supported. QOS/4/QOS_QMPROFILE_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet1/2/0/5; Failed to apply queue scheduling profile b in session group profile a to the user. Reason: The queue scheduling profile configuration conflicts with the CAR configuration in an EDSG service policy.
日志说明	• 用户上线，下发配置的 QMProfile 信息失败 • 用户已经上线，修改 QMProfile 信息或者增加 QMProfile 应用失败 • 用户已经上线，修改后的 QMProfile 信息或者增加 QMProfile 与 EDSG 业务流量限速配置冲突
处理建议	取消QMProfile在profile下的应用或者修改QMProfile的相关信息

86.33 QOS_QMPROFILE_MODIFYQUEUE_FAIL

日志内容	Failed to configure queue [UINT32] in queue management profile [STRING]. [STRING].
参数解释	$1：队列编号 $2：Profile名称 $3：失败原因
日志等级	4
举例	QOS/4/QOS_QMPROFILE_MODIFYQUEUE_FAIL: Failed to configure queue 1 in queue management profile myqueue. The value is out of range.
日志说明	qmprofile成功应用到端口后，再对某队列进行修改，新的参数超出端口能力范围
处理建议	取消此profile在对应板的应用再修改队列参数

86.34 QOS_QMPROFILE_RESTORE_FAIL

日志内容	Failed to restore the configuration of queue scheduling profile [STRING] on interface [STRING], because [STRING].
参数解释	$1：队列调度策略名称 $2：接口名称 $3：失败原因 ○ the minimum guaranteed bandwidth exceeds the interface bandwidth.：队列调度策略中配置的队列最小保证带宽超过了接口带宽上限 ○ the queue-based GTS configuration conflicts with the maximum bandwidth setting in the queue scheduling profile.：基于队列配置的 GTS 和队列调度策略中配置的队列最大带宽冲突
日志等级	4
举例	QOS/4/QOS_QMPROFILE_RESTORE_FAIL: -MDC=1; Failed to restore the configuration of queue scheduling profile abc on interface GigabitEthernet1/2/0/3, because the minimum guaranteed bandwidth exceeds the interface bandwidth.
日志说明	通过预配置方式配置接口下GTS和队列调度策略后，再插入对应单板使配置生效： • 队列调度策略中最小保证带宽超过了接口带宽上限 • 同时配置了基于队列的 GTS 和队列调度策略中的队列最大带宽
处理建议	修改或删除错误配置

86.35 QOS_WEIGHT_APPLYUSER_FAIL

日志内容	[STRING]; Failed to apply the [STRING] weight in [STRING] profile [STRING] to the user. Reason: [STRING].
参数解释	$1：用户标识信息 $2：Weight应用方向 $3：Profile类型 $4：Profile名称 $5：失败原因
日志等级	4
举例	QOS/4/QOS_WEIGHT_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet1/2/0/5; Failed to apply the outbound weight in user profile a to the user. Reason: The resources are insufficient. QOS/4/QOS_WEIGHT_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet1/2/0/5; Failed to apply the outbound weight in user profile a to the user. Reason: The weight configuration conflicts with the CAR configuration in an EDSG service policy.
日志说明	1.用户上线，下发配置的Weight信息失败 2.用户已经上线，修改Weight信息或者增加Weight应用失败 3.用户已经上线，修改后的Weight信息或者增加Weight与EDSG业务流量限速配置冲突
处理建议	取消Weight在profile下的应用或者修改Weight的相关参数信息

87 RADIUS

本节介绍 RADIUS 模块输出的日志信息。

87.1 RADIUS_AUTH_FAILURE

日志内容	User [STRING] from [STRING] failed authentication.
参数解释	$1：用户名称 $2：IP地址
日志等级	5
举例	RADIUS/5/RADIUS_AUTH_FAILURE: User abc@system from 192.168.0.22 failed authentication.
日志说明	RADIUS服务器了拒绝用户的认证请求
处理建议	无

87.2 RADIUS_AUTH_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
参数解释	$1：用户名称 $2：IP地址
日志等级	6
举例	RADIUS/6/RADIUS_AUTH_SUCCESS: User abc@system from 192.168.0.22 was authenticated successfully.
日志说明	RADIUS服务器接收了用户的认证请求
处理建议	无

87.3 RADIUS_DELETE_HOST_FAIL

日志内容	Failed to delete servers in scheme [STRING].
参数解释	$1：方案名称
日志等级	4
举例	RADIUS/4/RADIUS_DELETE_HOST_FAIL: Failed to delete servers in scheme abc.
日志说明	删除RADIUS方案中的服务器失败
处理建议	无

88 RIP

本节介绍 RIP 模块输出的日志信息。

88.1 RIP_MEM_ALERT

日志内容	RIP Process received system memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	RIP/5/RIP_MEM_ALERT: RIP Process received system memory alert start event.
日志说明	RIP模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

89 RIPNG

本节介绍 RIPng 模块输出的日志信息。

89.1 RIPNG_MEM_ALERT

日志内容	RIPng Process receivedsystem memory alert [STRING] event.
参数解释	$1：内存告警类型
日志等级	5
举例	RIPNG/5/RIPNG_MEM_ALERT: RIPNG Process received system memory alert start event.
日志说明	RIPng模块收到内存告警信息
处理建议	当超过各级内存门限时，检查系统内存占用情况，对占用内存较多的模块进行调整，尽量释放可用内存

90 RM

本节介绍 RM 模块输出的日志信息。

90.1 RM_ACRT_REACH_LIMIT

日志内容	Max active [STRING] routes [UINT32] reached in URT of [STRING]
参数解释	$1：IPv4或IPv6 $2：最大激活路由数 $3：VPN实例名
日志等级	4
举例	RM/4/RM_ACRT_REACH_LIMIT: Max active IPv4 routes 100000 reached in URT of VPN1
日志说明	VPN实例单播路由表中的激活路由数达到了上限值
处理建议	检查所有的路由并删除不需要的路由

90.2 RM_ACRT_REACH_THRESVALUE

日志内容	Threshold value [UINT32] of max active [STRING] routes reached in URT of [STRING]
参数解释	$1：最大激活路由数告警百分比 $2：IPv4或IPv6 $3：VPN实例名
日志等级	4
举例	RM/4/RM_ACRT_REACH_THRESVALUE: Threshold value 50% of max active IPv4 routes reached in URT of vpn1
日志说明	VPN实例单播路由表中的激活路由数达到了最大路由数告警百分比
处理建议	修改最大路由数告警百分比或路由数上限值

90.3 RM_THRESHLD_VALUE_REACH

日志内容	Threshold value [UINT32] of active [STRING] routes reached in URT of [STRING]
参数解释	$1：最大激活路由数 $2：IPv4或IPv6 $3：VPN实例名
日志等级	4
举例	RM/4/RM_THRESHLD_VALUE_REACH: Threshold value 10000 of active IPv4 routes reached in URT of vpn1
日志说明	VPN实例单播路由表中的激活路由数达到了上限值
处理建议	修改路由数上限值

90.4 RM_TOTAL_THRESHLD_VALUE_REACH

日志内容	Threshold value [UINT32] reached for active [STRING] routes in all URTs.
参数解释	$1：最大激活路由数 $2：IPv4或IPv6
日志等级	4
举例	RM/4/RM_TOTAL_THRESHLD_VALUE_REACH: Threshold value 1000 reached for active IPv4 routes in all URTs.
日志说明	公网和所有VPN实例的IPv4/IPv6激活路由总数达到了上限值
处理建议	检查路由表，确认是否需要配置路由策略，减少路由表条目

91 RSVP

本节介绍 RSVP 模块输出的日志信息。

91.1 RSVP_FRR_SWITCH

日志内容	Session ([STRING]): FRR is [STRING].
参数解释	$1：被保护隧道信息 $2：会话保护状态，如果有备份隧道信息，同时输出备隧道信息，取值包括： ready：绑定了快速重路由的旁路隧道，此时未进行切换 used：绑定了快速重路由的旁路隧道，此时已切换 disabled：解绑定快速重路由的旁路隧道
日志等级	5
举例	RSVP/5/RSVP_FRR_SWITCH: Session (DIP 2.2.2.2, SIP 1.1.1.1, TID 3, LSPID 5): FRR is ready. Bypass tunnel is Tunnel5.
日志说明	当隧道FRR保护成功、保护取消或发生切换时，触发该日志
处理建议	无

91.2 RSVP_P2MP_FRR_SWITCH

日志内容	Session ([STRING]): FRR is [STRING].
参数解释	$1：被保护隧道信息 $2：会话保护状态，如果有备份隧道信息，同时输出备隧道信息，取值包括： ready：绑定了快速重路由的旁路隧道，此时未进行切换 used：绑定了快速重路由的旁路隧道，此时已切换 disabled：解绑定快速重路由的旁路隧道
日志等级	5
举例	RSVP/5/RSVP_P2MP_FRR_SWITCH: P2MP session (DIP 2.2.2.2, SIP 1.1.1.1, P2MPID 0x1010101, TID 3, LSPID 5): FRR is ready. Bypass tunnel is Tunnel5.
日志说明	当隧道FRR保护成功、保护取消或发生切换时，触发该日志
处理建议	无

92 RTM

本节介绍 EAA 的 RTM（Real-Time Management）模块输出的日志信息。

92.1 RTM_ENVIRONMENT

日志内容	Can't find environment variable [STRING].
参数解释	$1：环境变量的名字
日志等级	4
举例	RTM/4/RTM_ENVIRONMENT: Can't find environment variable TestEnv.
日志说明	CLI监控策略替换环境变量时没有找到对应的环境变量，CLI监控策略执行失败
处理建议	请先定义环境变量再使用环境变量

92.2 RTM_TCL_LOAD_FAILED

日志内容	Failed to load the Tcl script file of policy [STRING].
参数解释	$1：Tcl监控策略的名称
日志等级	4
举例	RTM/4/RTM_TCL_LOAD_FAILED: Failed to load the Tcl script file of policy [STRING].
日志说明	Tcl监控策略对应的文件加载到内存失败
处理建议	无

92.3 RTM_TCL_MODIFY

日志内容	Failed to execute Tcl-defined policy [STRING] because the policy's Tcl script file had been modified.
参数解释	$1：Tcl监控策略的名称
日志等级	4
举例	RTM/4/RTM_TCL_MODIFY: Failed to execute Tcl-defined policy aaa because the policy's Tcl script file had been modified.
日志说明	Tcl监控策略触发执行时，对应的文件被修改
处理建议	确保Tcl监控策略对应的文件与注册文件相同或者重新创建Tcl监控策略

92.4 RTM_TCL_NOT_EXIST

日志内容	Failed to execute Tcl-defined policy [STRING] because the policy's Tcl script file was not found.
参数解释	$1：Tcl监控策略的名称
日志等级	4
举例	RTM/4/RTM_TCL_NOT_EXIST: Failed to execute Tcl-defined policy aaa because the policy's Tcl script file was not found.
日志说明	Tcl监控策略触发执行时对应的文件不存在
处理建议	确保Tcl监控策略对应的文件存在或者重新创建Tcl监控策略

93 SAVA

本节介绍 SAVA（Source Address Validation Architecture）模块输出的日志信息。

93.1 SAVA_SET_DRV_FAILED

日志内容	Failed to set the driver for enabling IPv6 SAVA on interface [STRING].
参数解释	$1: 接口名称
日志等级	5
举例	SAVA/5/SAVA_SET_DRV_FAILED: Failed to set the driver for enabling IPv6 SAVA on interface GigabitEthernet1/2/0/1.
日志说明	在接口上开启IPv6 SAVA功能，功能下硬件驱动失败
处理建议	• 请稍后重新执行一遍本命令

93.2 SAVA_SPOOFING_DETECTED

日志内容	Spoofing packet detected: Spoofing packet detected : source IP 2000::1, destination IP 3000::2, protocol 6, source port 200, destination port 3000 on interface GigabitEthernet1/2/0/1.
参数解释	$1：仿冒的源IP地址 $2：目的IP地址 $3：IP报文协议号 $4：源端口号 $5：目的端口号 $6：接口名称
日志等级	6
举例	SAVA/6/SAVA_SPOOFING_DETECTED: Spoofing packet detected : source IP 2000::1, destination IP 3000::2, protocol 6, source port 200, destination port 3000 on interface GigabitEthernet1/2/0/1.
日志说明	设备检测到非法主机仿冒合法用户IP
处理建议	检查报文发送者的合法性

93.3 SAVA_SET_DRV_FAILED

日志内容	Failed to set the driver for enabling IPv6 SAVA on interface [STRING].
参数解释	$1: 接口名称
日志等级	5
举例	SAVA/5/SAVA_SET_DRV_FAILED: Failed to set the driver for enabling IPv6 SAVA on interface GigabitEthernet1/2/0/1.
日志说明	在接口上开启IPv6 SAVA功能，功能下硬件驱动失败
处理建议	请稍后重新执行一遍本命令

94 SCMD

本节介绍 SCMD（服务控制管理）模块输出的日志信息。

94.1 PROCESS_ABNORMAL

日志内容	The process [STRING] exited abnormally. ServiceName=[STRING], ExitCode=[STRING], KillSignal=[STRING], StartTime=[STRING], StopTime=[STRING].
参数解释	$1：进程名 $2：进程脚本里定义的服务名 $3：进程退出码，取值为： • 数字表示进程退出码 • NA 表示无退出码，进程被信号关闭 $4：关闭进程的信号，取值为： • 数字表示关闭进程的信号的数值 • NA 表示没有关闭信号，进程主动退出，并非被信号关闭 $5：进程的创建时间 $6：进程的关闭时间
日志等级	4
举例	SCMD/4/PROCESS_ABNORMAL: The process diagd exited abnormally. ServiceName=DIAG, ExitCode=1, KillSignal=NA, StartTime=2019-03-06 14:18:06, StopTime=2019-03-06 14:35:25.
日志说明	服务异常退出，输出进程异常退出的相关参数，以便定位
处理建议	1. 通常情况下，进程异常退出后，会立即自动重启。可使用 display process 命令查看进程是否存在。如果进程存在，则进程已恢复 2. 如果进程未恢复，请搜集以下信息： o 在 probe 视图下，执行 view /var/log/trace.log > trace.log，然后将设备存储目录下的 trace.log 文件通过 FTP 或 TFTP 功能，上传到服务器 o 联系工程师，将上述文件，发送给工程师进行分析，并保留现场，以便工程师进行进一步分析定位 3. 如果进程已恢复，但仍需要定位进程异常退出的原因，请执行（2） 备注：当使用FTP功能将文件上传到服务器时，请使用binary传输模式

94.2 PROCESS_ACTIVEFAILED

日志内容	The standby process [STRING] failed to switch to the active process due to uncompleted synchronization, and was restarted.
参数解释	$1：进程名
日志等级	4
举例	SCMD/4/PROCESS_ACTIVEFAILED: The standby process diagd failed to switch to the active process due to uncompleted synchronization, and was restarted.
日志说明	备用进程还未完成同步时主进程意外退出，导致备进程倒换成主进程失败。进程重启
处理建议	无

94.3 PROCESS_CORERECORD

日志内容	Exceptions occurred with process [STRING]. A core dump file was generated.
参数解释	$1：进程名
日志等级	4
举例	SCMD/4/PROCESS_CORERECORD: Exceptions occurred with process diagd. A core dump file was generated.
日志说明	进程异常退出产生了core文件。core文件用于记录进程异常退出时的相关信息，以便定位
处理建议	1. 请使用 **display exception context** 命令搜集进程异常信息，并将该异常信息保存到一个文件中 2. 通过 **display exception filepath** 命令查看 core 文件目录，并通过 FTP 或 TFTP 功能，将 core 文件和记载了异常信息的文件上传到服务器 3. 联系工程师，将上述文件，发送给工程师进行分析，并保留现场，以便工程师进一步分析定位 当使用FTP功能将文件上传到服务器时，请使用binary传输模式

94.4 SCM_ABNORMAL_REBOOT

日志内容	形式一： The process [STRING] can't be restored. Reboot now. 形式二： The process [STRING] can't be restored. Reboot [STRING] now.
参数解释	形式一： $1：进程名 形式二： $1：进程名 $2：chassis编号+slot编号或slot编号
日志等级	3
举例	SCMD/3/SCM_ABNORMAL_REBOOT: The process ipbased can't be restored. Reboot slot 2 now.
日志说明	形式一： 进程在设备启动过程中，异常退出，尝试自动重启多次后，仍不能恢复，则自动重启设备。 形式二： 进程在指定slot启动过程中，异常退出，尝试自动重启多次后，仍不能恢复，则系统会自动重启指定slot。
处理建议	1. 等单板重启后，使用 **display process** 命令查看进程是否恢复 2. 若多次重启后仍不能恢复，联系工程师解决

94.5 SCM_ABNORMAL_REBOOTMDC

日志内容	The process [STRING] in [STRING] [UINT16] can't be restored. Reboot [STRING] [UINT16] now.
参数解释	$1：进程名 $2：取值为MDC或Context $3：MDC或Context的编号 $4：取值为MDC或Context $5：MDC或Context的编号
日志等级	3
举例	SCMD/3/SCM_ABNORMAL_REBOOTMDC: The process ipbased in MDC 2 can't be restored. Reboot MDC 2 now.
日志说明	在主用主控板上的用户MDC的在启动过程中，或者在引擎组中主引擎上的Context启动过程中，进程异常退出，尝试自动重启多次后，仍不能恢复，则重启此MDC或Context。此日志在MDC 1或Context 1中输出
处理建议	1. 等单板重启后，使用 **display process** 命令查看进程是否恢复 2. 若多次重启后仍不能恢复，联系工程师解决

94.6 SCM_ABORT_RESTORE

日志内容	The process [STRING] can't be restored, abort it.
参数解释	$1：进程名
日志等级	3
举例	SCMD/3/SCM_ABORT_RESTORE: The process ipbased can't be restored, abort it.
日志说明	进程在系统运行中异常退出，尝试自动重启多次后，仍不能恢复，系统放弃恢复该进程
处理建议	1. 任意视图下执行 **display process log** 命令查看进程退出详细信息 2. 重启异常进程所在单板或 MDC，尝试恢复 3. 提供 **display process log** 命令的显示信息，联系工程师解决

94.7 SCM_INSMOD_ADDON_TOOLONG

日志内容	Failed to finish loading [STRING] in [UINT32] minutes.
参数解释	$1：内核文件的名称 $1：已加载时间
日志等级	4
举例	SCMD/4/SCM_INSMOD_ADDON_TOOLONG: Failed to finish loading addon.ko in 30 minutes.
日志说明	设备启动过程中加载内核文件超时
处理建议	**1.** 重启单板，尝试恢复 **2.** 联系工程师解决

94.8 SCM_KERNEL_INIT_TOOLONG

日志内容	Kernel init in sequence [STRING] function [STRING] failed to finish in [UINT32] minutes.
参数解释	$1：内核事件的阶段 $2：内核事件阶段对应的函数的地址 $3：所用时间
日志等级	4
举例	SCMD/4/SCM_KERNEL_INIT_TOOLONG: Kernel init in sequence 0x25e7 function 0x6645ffe2 failed to finish in 15 minutes.
日志说明	内核初始化时，某个阶段某函数运行时间过长
处理建议	**1.** 重启单板，尝试恢复 **2.** 联系工程师解决

94.9 SCM_PROCESS_STARTING_TOOLONG

日志内容	The process [STRING] on [STRING] [UINT16] has not finished starting in [UINT32] hours.
参数解释	$1：进程名 $2：取值为MDC或Context（不支持MDC或者Context的设备，不会输出该信息） $3：MDC或Context的编号（不支持MDC或者Context的设备，不会输出该信息） $4：所用时间
日志等级	4
举例	SCMD/4/ SCM_PROCESS_STARTING_TOOLONG: The process ipbased on MDC 2 has not finished starting in 1 hours.
日志说明	进程长时间未启动完成。可能是因为配置太多导致进程启动慢，也可能是进程异常
处理建议	1. 大量配置的情况下，设备启动需要较长时间，如果等待 6 小时后，仍提示进程未完成启动，则可以认为进程已经异常 2. 重启单板/MDC/Context，尝试恢复。等单板/MDC/Context 重启后，使用 **display process** 命令查看进程是否恢复 3. 联系工程师解决

94.10 SCM_PROCESS_STILL_STARTING

日志内容	The process [STRING] on [STRING] [UINT16] is still starting for [UINT32] minutes.
参数解释	$1：进程的名称 $2：取值为MDC或Context（不支持MDC或者Context的设备，不会输出该信息） $3：MDC或Context编号（不支持MDC或者Context的设备，不会输出该信息） $4：所用时间
日志等级	6
举例	SCMD/6/SCM_PROCESS_STILL_STARTING: The process ipbased on MDC 2 is still starting for 20 minutes.
日志说明	某进程一直处于启动状态
处理建议	正常提示，无须处理

94.11 SCM_SKIP_PROCESS

日志内容	The process [STRING] was skipped because it failed to start within 6 hours.
参数解释	$1：进程名
日志等级	4
举例	SCMD/4/SCM_SKIP_PROCESS: The process ipbased was skipped because it failed to start within 6 hours.
日志说明	单板/MDC/Context启动过程中，有进程超过6小时未启动完成，跳过该进程继续启动
处理建议	1. 重启单板/MDC/Context 尝试恢复。等单板/MDC/Context 重启后，使用 **display process** 命令查看进程是否恢复 2. 联系工程师解决

94.12 SCM_SKIP_PROCESS

日志内容	The process [STRING] on [STRING] [UINT16] was skipped because it failed to start within 6 hours.
参数解释	$1：进程名 $2：取值为MDC或Context $3：MDC或Context的编号
日志等级	3
举例	SCMD/3/SCM_SKIP_PROCESS: The process ipbased on MDC 2 was skipped because it failed to start within 6 hours.
日志说明	某进程超过6小时未启动完成，系统跳过该进程，继续启动
处理建议	1. 重启单板/MDC/Context，尝试恢复。等单板/MDC/Context 重启后，使用 **display process** 命令查看进程是否恢复 2. 联系工程师解决

95 SCRLSP

本节介绍静态 CRLSP 模块输出的日志信息。

95.1 SCRLSP_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for static CRLSP [STRING] is duplicate.
参数解释	$1：入标签值 $2：静态CRLSP名称
日志等级	4
举例	SCRLSP/4/SCRLSP_LABEL_DUPLICATE: Incoming label 1024 for static CRLSP aaa is duplicate.
日志说明	静态CRLSP的入标签被静态PW或者静态LSP占用。触发该日志的原因可能有： 1. 在 MPLS 已使能的情况下，配置了一条入标签被静态 PW 或者静态 LSP 占用的静态 CRLSP 2. 在入标签被静态 PW 或静态 LSP 占用的静态 CRLSP 存在的情况下，使能 MPLS
处理建议	删除该CRLSP，重新配置一条静态CRLSP，并指定一个新的入标签

96 SESSION

本节介绍 SESSION 模块输出的日志信息。

96.1 SESSION_DRV_EXCEED

日志内容	The number of session entries ([UINT32]) supported by hardware already reached.
参数解释	$1：产品硬件支持的最大会话表项的数目
日志等级	6
举例	SESSION/6/SESSION_DRV_EXCEED: The number of session entries (65535) supported by hardware already reached.
日志说明	会话表项数目达到硬件支持的最大规格时会发送该日志
处理建议	无

96.2 SESSION_DRV_RECOVERY

日志内容	Session resources supported by hardware had been released.
参数解释	无
日志等级	6
举例	SESSION/6/SESSION_DRV_RECOVERY: Session resources supported by hardware had been released.
日志说明	会话表项资源从用尽状态恢复时会发送该日志
处理建议	无

96.3 SESSION_IPV4_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
参数解释	$1：协议类型 $2：源IP地址 $3：源端口号 $4：转换后的源IP地址 $5：转换后的源端口号 $6：目的IP地址 $7：目的端口号 $8：转换后的目的IP地址 $9：转换后的目的端口号 $10：入方向的报文总数 $11：入方向的字节总数 $12：出方向的报文总数 $13：出方向的字节总数 $14：源VPN名称 $15：目的VPN名称 $16：源DS-Lite Tunnel $17：目的DS-Lite Tunnel $18：创建会话的时间 $19：会话删除时间 $20：日志类型 $21：日志类型描述信息，包括： • Session created：会话创建日志 • Active flow threshold：流量或时间阈值日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • Aged for reset or config-change：通过配置删除会话日志 • Other：其他原因删除会话日志，如由其他模块删除
日志等级	6
举例	SESSION/6/SESSION_IPV4_FLOW: Protocol(1001)=UDP;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=10.10.10.1;NATSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;NATDstIPAddr(1009)=20.20.20.1;NATDstPort(1010)=21;InitPktCount(1044)=1;InitByteCount(1046)=50;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=03182024082546;EndTime_e(1014)=;Event(1048)=(8)Session created;

日志说明	创建、删除IPv4会话时会发送该日志 IPv4会话过程中会定时发送该日志 IPv4会话的流量或时间达到指定的阈值时会发送该日志
处理建议	无

96.4 SESSION_IPV6_FLOW

日志内容	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
参数解释	$1：协议类型 $2：源IPv6地址 $3：源端口号 $3：目的IPv6地址 $4：目的端口号 $5：入方向的报文总数 $6：入方向的字节总数 $7：出方向的报文总数 $8：出方向的字节总数 $9：源VPN名称 $10：目的VPN名称 $11：创建会话的时间 $12：会话删除时间 $13：日志类型 $14：日志类型描述信息，包括： • Session created：会话创建日志 • Active flow threshold：流量或时间阈值日志 • Normal over：正常流结束，会话删除日志 • Aged for timeout：会话老化删除日志 • Aged for reset or config-change：通过配置删除会话日志 • Other：其他原因删除会话日志，如由其他模块删除
日志等级	6
举例	SESSION/6/SESSION_IPV6_FLOW: Protocol(1001)=UDP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=1024;DstIPv6Addr(1037)=3001::2;DstPort(1008)=53;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1047)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=03182024082901;EndTime_e(1014)=;Event(1048)=(8)Session created;
日志说明	创建、删除IPv6会话时会发送该日志 IPv6会话过程中会定时发送该日志 IPv6会话的流量或时间达到指定的阈值时会发送该日志
处理建议	无

97 SHELL

本节介绍 SHELL 模块输出的日志信息。

97.1 SHELL_CMD

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command is [STRING]
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**） $4：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CMD: -Line=aux0-IPAddr=**-User=**; Command is quit
日志说明	记录设备执行过的命令
处理建议	无

97.2 SHELL_CMD_CONFIRM

日志内容	Confirm option of command [STRING] is [STRING].
参数解释	$1：命令字符串 $2：确认选项
日志等级	6
举例	SHELL/6/SHELL_CMD_CONFIRM: Confirm option of command save is no.
日志说明	记录需要用户确认命令的用户选项操作结果
处理建议	无

97.3 SHELL_CMD_EXECUTEFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be executed.
参数解释	$1：用户名 $2：IP地址 $3：命令字符串 $4：当前命令模式
日志等级	4
举例	SHELL/4/SHELL_CMD_EXECUTEFAIL: -User=**-IPAddr=192.168.62.138; Command save in view system failed to be executed.
日志说明	后台程序下发的命令执行失败
处理建议	定位命令执行失败的具体原因

97.4 SHELL_CMD_INPUT

日志内容	Input string for the [STRING] command is [STRING].
参数解释	$1：命令字符串 $2：输入字符串
日志等级	6
举例	SHELL/6/SHELL_CMD_INPUT: Input string for the save command is startup.cfg. SHELL/6/SHELL_CMD_INPUT: Input string for the save command is CTRL_C. SHELL/6/SHELL_CMD_INPUT: Input string for the save command is the Enter key.
日志说明	当用户执行命令时，如果需要输入相关信息以进行下一步操作，则输入的字符内容将被记录，并产生日志信息 例如： • 在执行 **save** 命令保存配置时，需要用户输入配置文件名和路径，用户输入的该信息将被记录 • 在执行 **save** 命令保存配置时，需要用户输入配置文件名和路径，用户输入 CTRL_C 取消了保存配置操作，则该信息将被记录 • 在执行 **save** 命令保存配置时，需要用户输入配置文件名和路径，用户输入回车，则该信息将被记录
处理建议	无

97.5 SHELL_CMD_INPUT_TIMEOUT

日志内容	Operation timed out: Getting input for the [STRING] command.
参数解释	$1：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CMD_INPUT_TIMEOUT: Operation timed out: Getting input for the fdisk command.
日志说明	当用户执行命令时，如果需要输入额外信息确认操作，而用户在一定时间内未输入信息，则产生输入超时的日志信息
处理建议	无

97.6 SHELL_CMD_LOCKEDBYOTHER

日志内容	SHELL/6/SHELL_CMD_LOCKEDBYOTHER: The system has been locked by [STRING].
参数解释	$1：配置会话的类型
日志等级	6
举例	SHELL/6/SHELL_CMD_LOCKEDBYOTHER: The system has been locked by NETCONF.
日志说明	其他用户占有全局配置锁，导致命令行命令下发失败
处理建议	等待其他用户释放全局配置锁后再配置

97.7 SHELL_CMD_MATCHFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be matched.
参数解释	$1：用户名 $2：IP地址 $3：命令字符串 $4：当前命令模式
日志等级	4
举例	SHELL/4/SHELL_CMD_MATCHFAIL: -User=**-IPAddr=192.168.62.138; Command description 10 in view system failed to be matched.
日志说明	由于命令输入错误，或者当前模式错误等，造成命令匹配错误
处理建议	定位命令匹配失败的具体原因

97.8 SHELL_CMDDENY

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command=[STRING] is denied.
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**） $4：命令字符串
日志等级	5
举例	SHELL/5/SHELL_CMDDENY: -Line=vty0-IPAddr=192.168.62.138-User=**; Command vlan 10 is permission denied.
日志说明	命令执行失败。用户权限不够
处理建议	无

97.9 SHELL_CMDFAIL

日志内容	The [STRING] command failed to restore the configuration.
参数解释	$1：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CMDFAIL: The “vlan 1024” command failed to restore the configuration.
日志说明	文本配置恢复操作失败
处理建议	无

97.10 SHELL_COMMIT_FAIL

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Failed to commit the target configuration.
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**）
日志等级	4
举例	SHELL/4/SHELL_COMMIT_FAIL: -Line=aux0-IPAddr=**-User=**; Failed to commit the target configuration.
日志说明	私有模式或独占模式下，下发目标配置失败
处理建议	无

97.11 SHELL_COMMIT_ROLLBACK

日志内容	The configuration commit delay is overtime, a configuration rollback will be performed.
参数解释	无
日志等级	5
举例	SHELL/5/ SHELL_COMMIT_ROLLBACK: The configuration commit delay is overtime, a configuration rollback will be performed.
日志说明	下发目标配置时指定了超时回滚时间，设备达到超时回滚时间进行配置回滚，配置回滚开始的提示
处理建议	无

97.12 SHELL_COMMIT_ROLLBACKDONE

日志内容	The configuration rollback has been performed.
参数解释	无
日志等级	5
举例	SHELL/5/ SHELL_COMMIT_ROLLBACKDONE: The configuration rollback has been performed.
日志说明	下发目标配置时指定了超时回滚时间，设备达到超时回滚时间，配置回滚完成的提示
处理建议	无

97.13 SHELL_COMMIT_ROLLBACKFAIL

日志内容	Failed to roll back the configuration from the uncommitted changes.
参数解释	无
日志等级	5
举例	SHELL/5/ SHELL_COMMIT_ROLLBACKFAIL: Failed to roll back the configuration from the uncommitted changes.
日志说明	下发目标配置时指定了超时回滚时间，设备达到超时回滚时间进行配置回滚时，回滚失败
处理建议	请根据需要手工处理

97.14 SHELL_COMMIT_SUCCESS

日志内容	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Target configuration successfully committed.
参数解释	$1：用户线名（如果不涉及该参数，显示为**） $2：IP地址（如果不涉及该参数，显示为**） $3：用户名（如果不涉及该参数，显示为**）
日志等级	5
举例	SHELL/5/SHELL_COMMIT_SUCCESS: -Line=aux0-IPAddr=**-User=**; Target configuration successfully committed.
日志说明	私有模式或独占模式下，下发目标配置成功
处理建议	无

97.15 SHELL_CRITICAL_CMDFAIL

日志内容	-User=[STRING]-IPAddr=[STRING]; Command=[STRING] .
参数解释	$1：用户名 $2：IP地址 $3：命令字符串
日志等级	6
举例	SHELL/6/SHELL_CRITICAL_CMDFAIL: -User=admin-IPAddr=169.254.0.7; Command is save.
日志说明	命令执行失败
处理建议	无

97.16 SHELL_LOGIN

日志内容	[STRING] logged in from [STRING].
参数解释	$1：用户名 $2：用户线名
日志等级	5
举例	SHELL/5/SHELL_LOGIN: Console logged in from console0.
日志说明	用户成功登录 用户线名为“local”时，表示用户登录到备用主控板自身
处理建议	无

97.17 SHELL_LOGOUT

日志内容	[STRING] logged out from [STRING].
参数解释	$1：用户名 $2：用户线名
日志等级	5
举例	SHELL/5/SHELL_LOGOUT: Console logged out from console0.
日志说明	用户退出登录 用户线名为“local”时，表示用户从备用主控板自身退出登录
处理建议	无

97.18 SHELL_SAVE_FAILED

日志内容	Failed to save running configuration to configuration file for configuration rollback.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVE_FAILED: Failed to save running configuration to configuration file for configuration rollback.
日志说明	系统保存下发目标配置前的配置到配置文件失败，无法进行配置回滚。系统保存下发目标配置前的配置到配置文件的时机有： • 执行 **commit** 命令后下发目标配置失败 • 执行 **commit confirmed** 命令指定了超时回滚时间，但在超时回滚时间内没有再次执行 **commit** 命令确认下发目标配置
处理建议	如需将当前配置回滚到下发目标配置前的配置，请手动恢复

97.19 SHELL_SAVE_SUCCESS

日志内容	Saved running configuration to configuration file for configuration rollback.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVE_SUCCESS: Saved running configuration to configuration file for configuration rollback.
日志说明	系统成功地保存下发目标配置前的配置到配置文件，以进行配置回滚。系统保存下发目标配置前的配置到配置文件的时机有： • 执行 **commit** 命令后下发目标配置失败 • 执行 **commit confirmed** 命令指定了超时回滚时间，但在超时回滚时间内没有再次执行 **commit** 命令确认下发目标配置
处理建议	无

97.20 SHELL_SAVEPOINT_EXIST

日志内容	The running configuration at this rollback point is the same as the configuration at the previous rollback point.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVEPOINT_EXIST: The running configuration at this rollback point is the same as the configuration at the previous rollback point.
日志说明	新创建的配置回滚点与上次创建的配置回滚点对应的配置相同
处理建议	无

97.21 SHELL_SAVEPOINT_FAILED

日志内容	Failed to create a new rollback point.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVEPOINT_FAILED: Failed to create a new rollback point.
日志说明	创建新配置回滚点失败
处理建议	如需保留对应配置回滚点，可以手动恢复回滚点对应配置，然后检查文件系统（例如文件系统剩余存储空间是否充足），再执行**commit**命令

97.22 SHELL_SAVEPOINT_SUCCESS

日志内容	Created a new rollback point.
参数解释	N/A
日志等级	5
举例	SHELL/5/SHELL_SAVEPOINT_SUCCESS: Created a new rollback point.
日志说明	成功创建一个新配置回滚点
处理建议	无

98 SLSP

本节介绍静态 LSP 模块输出的日志信息。

98.1 SLSP_LABEL_DUPLICATE

日志内容	Incoming label [INT32] for static LSP [STRING] is duplicate.
参数解释	$1：入标签值 $2：静态LSP名称
日志等级	4
举例	SLSP/4/SLSP_LABEL_DUPLICATE: Incoming label 1024 for static LSP aaa is duplicate.
日志说明	静态LSP的入标签被静态PW或者静态CRLSP占用。触发该日志的原因可能有： • 在 MPLS 已使能的情况下，配置了一条入标签被静态 PW 或静态 CRLSP 占用的静态 LSP • 在入标签被静态 PW 或静态 CRLSP 占用的静态 LSP 存在的情况下，使能 MPLS
处理建议	删除该LSP，重新配置一条静态LSP，并指定一个新的入标签

99 SNMP

本节介绍 SNMP 模块输出的日志信息。

99.1 SNMP_ACL_RESTRICTION

日志内容	SNMP [STRING] from [STRING] is rejected due to ACL restriction.
参数解释	$1：SNMP团体名/用户名/组名 $2：NMS的IP地址
日志等级	3
举例	SNMP/3/SNMP_ACL_RESTRICTION: SNMP community public from 192.168.1.100 is rejected due to ACL restrictions.
日志说明	当SNMP报文因ACL限制被拒绝通过时，打印系统日志
处理建议	检查SNMP agent上的ACL配置，及agent是否被攻击

99.2 SNMP_AUTHENTICATION_FAILURE

日志内容	Failed to authenticate SNMP message.
参数解释	无
日志等级	4
举例	SNMP/4/SNMP_AUTHENTICATION_FAILURE: Failed to authenticate SNMP message.
日志说明	NMS向Agent发起SNMP请求，当认证失败时，Agent记录此日志信息
处理建议	无

99.3 SNMP_GET

日志内容	-seqNO=[UINT32]-srcIP=[STRING]-op=GET-node=[STRING]-value=[STRING]; The agent received a message.
参数解释	$1：SNMP操作日志的序列号 $2：NMS的IP 地址 $3：Get操作的MIB节点名及对应的OID $4：请求报文的取值字段
日志等级	6
举例	SNMP/6/SNMP_GET: -seqNO=1-srcIP=192.168.28.28-op=GET-node=sysLocation(1.3.6.1.2.1.1.6.0)-value=; The agent received a message.
日志说明	NMS向Agent发送Get请求报文。如果SNMP日志功能开启，SNMP模块将记录Get请求相关信息
处理建议	无

99.4 SNMP_INFORM_LOST

日志内容	Inform failed to reach NMS [STRING]: Inform [STRING][STRING].
参数解释	$1：NMS主机地址及端口号 $2：告警名称及对应的OID $3：告警携带的MIB节点名称、OID及相应的值 o 如果告警未携带 MIB 节点，此参数部分不会出现 o 如果告警携带有 MIB 节点，此参数部分以“ with ”（空格 with 空格）开头，节点间以“;”（分号）作为分隔符
日志等级	3
举例	SNMP/3/SNMP_INFORM_LOST: Inform failed to reach NMS 192.168.111.222(163): Inform coldStart(1.3.6.1.6.3.1.1.5.1).
日志说明	当NMS路由不可达，或者设备给NMS发送Inform报文超时仍未收到响应时，设备会将发送失败的Inform报文以日志的方式保存下来，以便用户查询 当日志携带多个参数导致日志超长时，系统会自动将当前日志拆分为多条日志发送，且添加定位符标识“-PART=xx”，xx表示拆分后生成的日志的序号
处理建议	检查设备与NMS之间是否路由可达

99.5 SNMP_NOTIFY

日志内容	Notification [STRING][STRING].
参数解释	$1：告警名称及对应的OID $2：告警携带的MIB节点名称、OID及相应的值 o 如果告警未携带 MIB 节点，此参数部分不会出现 o 如果告警携带有 MIB 节点，此参数部分以“ with ”（空格 with 空格）开头，节点间以“;”（分号）作为分隔符
日志等级	6
举例	未拆分的日志举例： SNMP/6/SNMP_NOTIFY: Notification unisLogIn(1.3.6.1.4.1.10519.256.2.2.1.1.3.0.1) with unisTerminalUserName(1.3.6.1.4.1.10519.256.2.2.1.1.2.1.0)=;unisTerminalSource(1.3.6.1.4.1.10519.256.2.2.1.1.2.2.0)=Console. 被拆分的日志举例： SNMP/6/SNMP_NOTIFY: -MDC=1; -PART=1; Notification syslogMsgNotification(1.3.6.1.2.1.192.0.1) with syslogMsgFacility(1.3.6.1.2.1.192.1.2.1.2.1)=23;syslogMsgSeverity(1.3.6.1.2.1.192.1.2.1.3.1)=6;syslogMsgVersion(1.3.6.1.2.1.192.1.2.1.4.1)=1;syslogMsgTimeStamp(1.3.6.1.2.1.192.1.2.1.5.1)=07-e2-04-12-12-26-35-00-00-00-2d-00-00[hex];syslogMsgHostName(1.3.6.1.2.1.192.1.2.1.6.1)=UNIS;syslogMsgAppName(1.3.6.1.2.1.192.1.2.1.7.1)=SHELL;syslogMsgProcID(1.3.6.1.2.1.192.1.2.1.8.1)=-;syslogMsgMsgID(1.3.6.1.2.1.192.1.2.1.9.1)=SHELL_CMD;syslogMsgSDParams(1.3.6.1.2.1.192.1.2.1.10.1)=4;syslogMsgMsg(1.3.6.1.2.1.192.1.2.1.11.1)= Command is snmp-agent trap enable syslog;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.1.12.83.121.115.76.111.99.64.50.53.53.48.54.3.77.68.67)=1;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.2.12.65.112.112.76.111.99.64.50.53.53.48.54.4.76.105.110.101)=con0. SNMP/6/SNMP_NOTIFY: -MDC=1; -PART=2; Notification syslogMsgNotification(1.3.6.1.2.1.192.0.1) with syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.3.12.65.112.112.76.111.99.64.50.53.53.48.54.6.73.80.65.100.100.114)=**;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.4.12.65.112.112.76.111.99.64.50.53.53.48.54.4.85.115.101.114)=**.
日志说明	Agent发送告警给NMS。如果SNMP告警日志功能开启，Agent将记录SNMP告警信息 当日志携带多个参数导致日志超长时，系统会自动将当前日志拆分为多条日志发送，且添加定位符标识“-PART=xx”，xx表示拆分后生成的日志的序号
处理建议	无

99.6 SNMP_SET

日志内容	-seqNO=[UINT32]-srcIP=[STRING]-op=SET-errorIndex=[UINT32]-errorStatus=[STRING]-node=[STRING]-value=[STRING]; The agent received a message.
参数解释	$1：SNMP操作日志的序列号 $2：NMS的IP地址 $3：Set操作的差错索引 $4：Set操作的差错状态 $5：Set操作的MIB节点名及对应的OID $6：Set操作设置的MIB节点的值
日志等级	6
举例	SNMP/6/SNMP_SET: -seqNO=3-srcIP=192.168.28.28-op=SET-errorIndex=0-errorStatus=noError-node=sysLocation(1.3.6.1.2.1.1.6.0)-value=Beijing China; The agent received a message.
日志说明	NMS向Agent发送Set请求。如果SNMP日志功能开启，SNMP模块将记录Set操作
处理建议	无

99.7 SNMP_USM_NOTINTIMEWINDOW

日志内容	-User=[STRING]-IPAddr=[STRING]; SNMPv3 message is not in the time window.
参数解释	$1：用户名 $2：NMS的IP地址
日志等级	4
举例	SNMP/4/SNMP_USM_NOTINTIMEWINDOW: -User=admin-IPAddr=169.254.0.7; SNMPv3 message is not in the time window.
日志说明	SNMPv3消息不在时间窗
处理建议	无

100 SSHC

本节介绍 SSHC（SSH client，SSH 客户端）模块输出的日志信息。

100.1 SSHC_ALGORITHM_MISMATCH

日志内容	Failed to log in to SSH server [STRING] because of [STRING] algorithm mismatch.
参数解释	$1：SSH服务端IP地址 $2：算法类型:encryption（加密）、key exchange（密钥交换）、MAC（message authentication code）或者public key（公钥）
日志等级	6
举例	SSHC/6/SSHC_ALGORITHM_MISMATCH: Failed to log in to SSH server 192.168.30.11 because of encryption algorithm mismatch.
日志说明	算法不匹配，SSH客户端登录服务器失败
处理建议	修改算法，使SSH客户端和服务器使用相同算法

101 SSHS

本节介绍 SSHS（SSH server，SSH 服务器）模块输出的日志信息。

101.1 SSHS_ACL_DENY

日志内容	The SSH Connection [IPADDR]([STRING]) request was denied according to ACL rules.
参数解释	$1：SSH客户端IP地址 $2：SSH客户端IP地址所在VPN
日志等级	5
举例	SSHS/5/SSH_ACL_DENY: The SSH Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
日志说明	SSH ACL规则限制登录IP地址。该日志在SSH服务端检测到非法客户端尝试登录时输出
处理建议	无

101.2 SSHS_ALGORITHM_MISMATCH

日志内容	SSH client [STRING] failed to log in because of [STRING] algorithm mismatch.
参数解释	$1：SSH客户端IP地址 $2：算法类型，encryption（加密）、key exchange（密钥交换）、MAC（message authentication code）或者public key（公钥）
日志等级	6
举例	SSHS/6/SSHS_ALGORITHM_MISMATCH: SSH client 192.168.30.117 failed to log in because of encryption algorithm mismatch.
日志说明	算法不匹配，SSH客户端登录失败
处理建议	修改算法，使SSH客户端和服务器使用相同算法

101.3 SSHS_AUTH_EXCEED_RETRY_TIMES

日志内容	SSH user [STRING] (IP: [STRING]) failed to log in, because the number of authentication attempts exceeded the upper limit.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_AUTH_EXCEED_RETRY_TIMES: SSH user David (IP: 192.168.30.117) failed to log in, because the number of authentication attempts exceeded the upper limit.
日志说明	SSH用户登录失败，认证尝试次数达到了最大值
处理建议	请SSH用户确认登录信息，并尝试重新登录

101.4 SSHS_AUTH_FAIL

日志内容	SSH user [STRING] (IP: [STRING]) didn't pass public key authentication for [STRING].
参数解释	$1：用户名 $2：SSH客户端IP地址 $3：失败原因： • wrong public key algorithm （公钥算法错误） • wrong public key（公钥错误） • wrong digital signature（数字签名错误）
日志等级	5
举例	SSHS/5/SSHS_AUTH_FAIL: SSH user David (IP: 192.168.30.117) didn't pass public key authentication for wrong public key algorithm.
日志说明	SSH用户没有通过公钥认证
处理建议	请SSH用户重新登录

101.5 SSHS_AUTH_TIMEOUT

日志内容	Authentication timed out for [IPADDR].
参数解释	$1：用户IP地址
日志等级	6
举例	SSHS/6/SSHS_AUTH_TIMEOUT: Authentication timed out for 1.1.1.1.
日志说明	SSH用户认证超时。该日志在SSH服务端检测到用户认证超时时输出
处理建议	建议用户检查是否没有及时输入认证信息

101.6 SSHS_CONNECT

日志内容	SSH user [STRING] (IP: [STRING]) connected to the server successfully.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_CONNECT: SSH user David (IP: 192.168.30.117) connected to the server successfully.
日志说明	SSH用户成功登录服务器
处理建议	无

101.7 SSHS_DECRYPT_FAIL

日志内容	The packet from [STRING] failed to be decrypted with [STRING].
参数解释	$1：SSH客户端IP地址 $2：加密算法（比如aes256-cbc）
日志等级	5
举例	SSHS/5/SSHS_DECRYPT_FAIL: The packet from 192.168.30.117 failed to be decrypted with aes256-cbc.
日志说明	来自SSH客户端的报文解密失败
处理建议	无

101.8 SSHS_DISCONNECT

日志内容	SSH user [STRING] (IP: [STRING]) disconnected from the server.
参数解释	$1：用户名 $2：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_DISCONNECT: SSH user David (IP: 192.168.30.117) disconnected from the server.
日志说明	SSH用户退出登录
处理建议	无

101.9 SSHS_ENCRYPT_FAIL

日志内容	The packet to [STRING] failed to be encrypted with [STRING].
参数解释	$1：SSH客户端IP地址 $2：加密算法（比如aes256-cbc）
日志等级	5
举例	SSHS/5/SSHS_ENCRYPT_FAIL: The packet to 192.168.30.117 failed to be encrypted with aes256-cbc.
日志说明	发往SSH客户端的报文加密失败
处理建议	无

101.10 SSHS_LOG

日志内容	Authentication failed for [STRING] from [STRING] port [INT32] because of invalid username or wrong password.
参数解释	$1：SSH客户端IP地址 $2：用户名 $3：端口号
日志等级	6
举例	SSHS/6/SSHS_LOG: Authentication failed for David from 140.1.1.46 port 16266 because of invalid username or wrong password.
日志说明	SSH用户密码认证失败
处理建议	无

101.11 SSHS_MAC_ERROR

日志内容	SSH server received a packet with wrong message authentication code (MAC) from [STRING].
参数解释	$1：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_MAC_ERROR: SSH server received a packet with wrong message authentication code (MAC) from 192.168.30.117.
日志说明	SSH服务器从客户端收到一个MAC错误的报文
处理建议	无

101.12 SSHS_REACH_SESSION_LIMIT

日志内容	SSH client [STRING] failed to log in. The current number of SSH sessions is [NUMBER]. The maximum number allowed is [NUMBER].
参数解释	$1：SSH客户端IP地址 $2：当前的SSH会话数 $3：设备允许建立的SSH会话数
日志等级	6
举例	SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 192.168.30.117 failed to log in. The current number of SSH sessions is 10. The maximum number allowed is 10.
日志说明	SSH客户端登录失败，SSH会话数达到了最大值
处理建议	无

101.13 SSHS_REACH_USER_LIMIT

日志内容	SSH client [STRING] failed to log in, because the number of users reached the upper limit.
参数解释	$1：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_REACH_USER_LIMIT: SSH client 192.168.30.117 failed to log in, because the number of users reached the upper limit.
日志说明	SSH客户端登录失败，SSH用户数达到了最大值
处理建议	无

101.14 SSHS_SCP_OPER

日志内容	User [STRING] at [IPADDR] requested operation: [STRING].
参数解释	$1：用户名称. $2：用户IP地址. $3：用户请求内容，包括文件操作信息 • get file "*name*"：下载名为 *name* 的文件 • put file "*name*"：上传名为 *name* 的文件
日志等级	6
举例	SSHS/6/SSHS_SCP_OPER: -MDC=1; User user1 at 1.1.1.1 requested operation: put file "aa".
日志说明	SCP服务器收到SCP用户请求执行相关操作
处理建议	无

101.15 SSHS_SFTP_OPER

日志内容	User [STRING] at [IPADDR] requested operation: [STRING].
参数解释	$1：用户名称. $2：用户IP地址. $3：用户请求内容，包括文件操作和目录操作等信息 • open dir "*path*"：打开目录 *path* • open "*file*" (attribute code *code*) in *MODE* mode：在 *MODE* 模式下，打开文件 *file*，该文件的属性代码为 *code* • remove file "*path*"：删除文件 *path* • mkdir "*path*" (attribute code *code*)：创建新目录 *path*，该目录的属性代码为 *code* • rmdir "*path*"：删除目录 *path* • rename old "*old-name*" to new "*new-name*"：改变旧文件或文件夹的名称 *old-name* 为 *new-name*
日志等级	6
举例	SSHS/6/SSHS_SFTP_OPER: User user1 at 1.1.1.1 requested operation: open dir "flash:/".
日志说明	SFTP用户请求相关操作信息。该日志在SFTP服务端收到用户请求执行相关命令时输出
处理建议	无

101.16 SSHS_SRV_UNAVAILABLE

日志内容	The [STRING] server is disabled or the [STRING] service type is not supported.
参数解释	$1：服务类型，包括Stelnet、SCP、SFTP、NETCONF
日志等级	6
举例	SSHS/6/SSHS_SRV_UNAVAILABLE: The SCP server is disabled or the SCP service type is not supported.
日志说明	Stelnet/SCP/SFTP/NETCONF over SSH服务不可用，服务器正在断开连接
处理建议	检查服务状态或用户配置

101.17 SSHS_VERSION_MISMATCH

日志内容	SSH client [STRING] failed to log in because of version mismatch.
参数解释	$1：SSH客户端IP地址
日志等级	6
举例	SSHS/6/SSHS_VERSION_MISMATCH: SSH client 192.168.30.117 failed to log in because of version mismatch.
日志说明	SSH客户端和服务器的SSH版本号不匹配
处理建议	修改版本，使SSH客户端和服务器使用相同SSH版本

102 STP

本节介绍生成树模块输出的日志信息。

102.1 STP_BPDU_PROTECTION

日志内容	BPDU-Protection port [STRING] received BPDUs.
参数解释	$1：接口名
日志等级	4
举例	STP/4/STP_BPDU_PROTECTION: BPDU-Protection port GigabitEthernet1/2/0/1 received BPDUs.
日志说明	使能了BPDU保护功能的接口收到BPDU报文
处理建议	检查下行设备是否是用户终端，是否存在恶意攻击

102.2 STP_BPDU_RECEIVE_EXPIRY

日志内容	Instance [UINT32]'s port [STRING] received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	5
举例	STP/5/STP_BPDU_RECEIVE_EXPIRY: Instance 0's port GigabitEthernet1/2/0/1 received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
日志说明	非指定端口因在BPDU超时之前没有收到任何BPDU报文，端口状态发生改变
处理建议	检查上行设备的STP状态及是否存在恶意攻击

102.3 STP_CONSISTENCY_RESTORATION

日志内容	Consistency restored on VLAN [UINT32]'s port [STRING].
参数解释	$1：VLAN ID $2：接口名
日志等级	6
举例	STP/6/STP_CONSISTENCY_RESTORATION: Consistency restored on VLAN 10's port GigabitEthernet1/2/0/1.
日志说明	接口类型不一致或者PVID不一致的保护状态解除
处理建议	无

102.4 STP_DETECTED_TC

日志内容	[STRING] [UINT32]'s port [STRING] detected a topology change.
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	6
举例	STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet1/2/0/1 detected a topology change.
日志说明	接口所在生成树实例或VLAN拓扑发生变化，本端设备检测到拓扑变化
处理建议	检查拓扑变化的原因。如果是有链路down了，就恢复此故障链路

102.5 STP_DISABLE

日志内容	STP is now disabled on the device.
参数解释	无
日志等级	6
举例	STP/6/STP_DISABLE: STP is now disabled on the device.
日志说明	设备全局去使能了生成树特性
处理建议	无

102.6 STP_DISCARDING

日志内容	Instance [UINT32]'s port [STRING] has been set to discarding state.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	6
举例	STP/6/STP_DISCARDING: Instance 0's port GigabitEthernet1/2/0/1 has been set to discarding state.
日志说明	MSTP在计算实例内端口状态，该接口被置为discarding状态
处理建议	无

102.7 STP_ENABLE

日志内容	STP is now enabled on the device.
参数解释	无
日志等级	6
举例	STP/6/STP_ENABLE: STP is now enabled on the device.
日志说明	设备全局使能了生成树特性
处理建议	无

102.8 STP_FORWARDING

日志内容	Instance [UINT32]'s port [STRING] has been set to forwarding state.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	6
举例	STP/6/STP_FORWARDING: Instance 0's port GigabitEthernet1/2/0/1 has been set to forwarding state.
日志说明	STP在计算实例内端口状态，该接口被置为forwarding状态
处理建议	无

102.9 STP_LOOP_PROTECTION

日志内容	Instance [UINT32]'s LOOP-Protection port [STRING] failed to receive configuration BPDUs.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	4
举例	STP/4/STP_LOOP_PROTECTION: Instance 0's LOOP-Protection port GigabitEthernet1/2/0/1 failed to receive configuration BPDUs.
日志说明	使能了环路保护功能的接口不能接受BPDU配置报文
处理建议	检查上行设备的STP状态及是否存在恶意攻击

102.10 STP_NOT_ROOT

日志内容	The current switch is no longer the root of instance [UINT32].
参数解释	$1：生成树实例编号
日志等级	5
举例	STP/5/STP_NOT_ROOT: The current switch is no longer the root of instance 0.
日志说明	本设备某生成树实例配置为根桥，但它收到比自身更优的BPDU报文后，就不再是此实例的根桥
处理建议	检查桥优先级配置及是否存在恶意攻击

102.11 STP_NOTIFIED_TC

日志内容	[STRING] [UINT32]'s port [STRING] was notified a topology change.
参数解释	$1：生成树实例或VLAN $2：生成树实例编号或VLAN ID $3：接口名
日志等级	6
举例	STP/6/STP_NOTIFIED_TC: Instance 0's port GigabitEthernet1/2/0/1 was notified a topology change.
日志说明	远端相连设备通知本设备某接口所在生成树实例或VLAN的拓扑发生变化
处理建议	检查拓扑变化的原因。如果是有链路down了，就恢复此故障链路

102.12 STP_PORT_TYPE_INCONSISTENCY

日志内容	Access port [STRING] in VLAN [UINT32] received PVST BPDUs from a trunk or hybrid port.
参数解释	$1：接口名 $2：VLAN ID
日志等级	4
举例	STP/4/STP_PORT_TYPE_INCONSISTENCY: Access port GigabitEthernet1/2/0/1 in VLAN 10 received PVST BPDUs from a trunk or hybrid port.
日志说明	Access接口收到了对端Trunk或Hybrid接口发出的PVST报文
处理建议	检查两端的接口类型配置是否一致

102.13 STP_PVID_INCONSISTENCY

日志内容	Port [STRING] with PVID [UINT32] received PVST BPDUs from a port with PVID [UINT32].
参数解释	$1：接口名 $2：VLAN ID $3：VLAN ID
日志等级	4
举例	STP/4/STP_PVID_INCONSISTENCY: Port GigabitEthernet1/2/0/1 with PVID 10 received PVST BPDUs from a port with PVID 20.
日志说明	接口收到了PVID不一致的报文
处理建议	检查两端的接口PVID配置是否一致

102.14 STP_PVST_BPDU_PROTECTION

日志内容	PVST BPDUs were received on port [STRING], which is enabled with PVST BPDU protection.
参数解释	$1：接口名
日志等级	4
举例	STP/4/STP_PVST_BPDU_PROTECTION: PVST BPDUs were received on port GigabitEthernet1/2/0/1, which is enabled with PVST BPDU protection.
日志说明	在MSTP模式下，设备上使能了PVST报文保护功能的端口收到了PVST报文
处理建议	检查其他设备是否发出了PVST BPDU

102.15 STP_ROOT_PROTECTION

日志内容	Instance [UINT32]'s ROOT-Protection port [STRING] received superior BPDUs.
参数解释	$1：生成树实例编号 $2：接口名
日志等级	4
举例	STP/4/STP_ROOT_PROTECTION: Instance 0's ROOT-Protection port Ethernet1/2/0/2 received superior BPDUs.
日志说明	使能了根保护功能的接口收到了比自身BPDU报文更优的BPDU报文
处理建议	检查桥优先级配置及是否存在恶意攻击

102.16 STP_STG_NUM_DETECTION

日志内容	STG count [UINT32] is smaller than the MPU's STG count [UINT32].
参数解释	$1：指定单板STG个数 $2：主控板STG个数
日志等级	4
举例	STP/4/STP_STG_NUM_DETECTION: STG count 64 is smaller than the MPU's STG count 65.
日志说明	检测到指定单板上的STG个数小于主控板上的STG个数
处理建议	配置的STP实例个数不能大于所有单板的STG个数的最小值。例如：配置STP实例数是m，所有单板中，STG个数最小的一块单板的STG数是n，m不能大于n

103 STRUNK

本节介绍 STRUNK 模块输出的日志信息。

103.1 STRUNK_DROPPACKET_INCONSISTENCY

日志内容	Smart trunk [UINT32] dropped the S-Trunk protocol packet because [STRING].
参数解释	$1：S-Trunk组编号 $2：丢弃报文原因： • the source and destination IP addresses or VPN instance of S-Trunk protocol packets are not configured on the local device：本端未配置 S-Trunk 协议报文的 IP 地址或本端不存在 S-Trunk 协议报文中的 VPN 实例 • the packet's source or destination IP address does not match the local configuration：S-Trunk 协议报文的 IP 地址和本端配置的 S-Trunk 协议报文的 IP 地址不匹配 • the VPN instance of S-Trunk protocol packets is different from the local VPN instance：S-Trunk 协议报文的 VPN 实例和接口绑定的 VPN 实例不一致 • the sequence number check failed：序列号校验失败 • key verification failed：密钥验证失败
日志等级	4
举例	STRUNK/4/STRUNK_DROPPACKET_INCONSISTENCY: Smart trunk 10 dropped the S-Trunk protocol packet because key verification failed.
日志说明	本端和对端设备S-Trunk配置不一致
处理建议	**1.** 检查部署 S-Trunk 的设备上 S-Trunk 相关配置是否一致 **2.** 如果配置一致，检查是否存在非法用户报文攻击

103.2 STRUNK_MEMBER_ROLE_CHANGE

日志内容	Smart trunk member role changed: Interface type=[STRING], interface number=[UINT32], previous role (trigger)=[STRING] ([STRING]), new role (trigger)=[STRING] ([STRING])
参数解释	$1：S-Trunk组中成员接口类型，包括BAGG和RAGG $2：成员接口编号 $3：成员接口原有的状态： o Primary：成员接口处于主用状态 o Secondary：成员接口处于备用状态 $4：成员接口处于原有状态的原因： o MANUAL_SECONDARY：成员接口在 S-Trunk 中的工作模式是强制为备用状态 o MANUAL_PRIMARY：成员接口在 S-Trunk 中的工作模式是强制为主用状态 o STRUNK_INIT：S-Trunk 正在初始化 o AUTO_SECONDARY：S-Trunk 组中本端设备为备用状态 o AUTO_PRIMARY：S-Trunk 组中本端设备为主用状态 o PEER_MEMBER_DOWN：对端成员接口变为 down o PEER_MEMBER_UP：对端成员接口变为 up $5：成员接口当前状态： o Primary：成员接口处于主用状态 o Secondary：成员接口处于备用状态 $6：成员接口处于当前状态的原因： o MANUAL_SECONDARY：成员接口在 S-Trunk 中的工作模式是强制为备用状态 o MANUAL_PRIMARY：成员接口在 S-Trunk 中的工作模式是强制为主用状态 o STRUNK_INIT：S-Trunk 正在初始化 o AUTO_SECONDARY：S-Trunk 组中本端设备为备用状态 o AUTO_PRIMARY：S-Trunk 组中本端设备为主用状态 o PEER_MEMBER_DOWN：对端成员接口变为 down o PEER_MEMBER_UP：对端成员接口变为 up
日志等级	5
举例	STRUNK/5/STRUNK_MEMBER_ROLE_CHANGE: Smart trunk member role changed: Interface type=BAGG, interface number=1, previous role (trigger)=Secondary (STRUNK_INIT), new role (trigger)=Primary (MANUAL_PRIMARY)
日志说明	S-Trunk组成员接口的状态变化
处理建议	• 检查本端或对端设备是否故障 • 检查本端或对端成员接口是否处于 down 状态

103.3 STRUNK_RECEIVE_TIMEOUT

日志内容	Hello timeout timer expired on smart trunk [UINT32].
参数解释	$1：S-Trunk组编号
日志等级	4
举例	STRUNK/4/STRUNK_RECEIVE_TIMEOUT: Hello timeout timer expired on smart trunk 1.
日志说明	在S-Trunk报文超时定时器超时前，未收到对端的S-Trunk协议报文，协商失败
处理建议	• 请查看 S-Trunk 链路是否为 up 状态 • 请查看 CPU 占有率是否过高

103.4 STRUNK_ROLE_CHANGE

日志内容	The role of the device changed in a smart trunk: Smart trunk ID=[UINT32], previous role (trigger)=[STRING] ([STRING]), new role (trigger)=[STRING] ([STRING])
参数解释	$1：S-Trunk组编号 $3：S-Trunk组的原有状态： o Init：S-Trunk 组处于初始化状态 o Primary：S-Trunk 组处于主用状态 o Secondary：S-Trunk 组处于备用状态 $4：S-Trunk组处于原有状态的原因： o INIT：S-Trunk 组正在初始化 o PRIORITY：根据优先级确定的主备状态变化 o TIMEOUT：本端在定时器超时后没有收到对端协议报文，从备用状态转为主用状态 o PEER_TIMEOUT：对端在定时器超时后没有收到本端协议报文，从备用状态转为主用状态 o BFD_DOWN：本端通过 BFD 检测到本端与对端间的链路 down o PEER_BFD_DOWN：对端通过 BFD 检测到对端与本端间的链路 down $5：S-Trunk组当前状态： o Init：S-Trunk 组处于初始化状态 o Primary：S-Trunk 组处于主用状态 o Secondary：S-Trunk 组处于备用状态 $6：S-Trunk组处于当前状态的原因： o INIT：S-Trunk 组正在初始化 o PRIORITY：根据优先级确定的主备状态变化 o TIMEOUT：本端在定时器超时后没有收到对端协议报文，从备用状态转为主用状态 o PEER_TIMEOUT：对端在定时器超时后没有收到本端协议报文，从备用状态转为主用状态 o BFD_DOWN：本端通过 BFD 检测到本端与对端间的链路 down o PEER_BFD_DOWN：对端通过 BFD 检测到对端与本端间的链路 down
日志等级	5
举例	STRUNK/5/STRUNK_ROLE_CHANGE: The role of the device changed in a smart trunk: Smart trunk ID=1, previous role (trigger)=Init (INIT), new role (trigger)=Secondary (PRIORITY)
日志说明	S-Trunk组状态变化
处理建议	检查加入S-Trunk组的两台设备间链路是否三层可达，排查设备故障

103.5 STRUNK_PDUINTERVAL_MISMATCH

日志内容	Smart trunk [UINT32] has a packet transmission interval different than the peer device.
参数解释	$1：S-Trunk组编号
日志等级	5
举例	STRUNK/5/STRUNK_PDUINTERVAL_MISMATCH: Smart trunk 1 has a packet transmission interval different than the peer device.
日志说明	两端设备某个S-Trunk组的Strunk报文发送周期配置的不一致，导致一端S-Trunk组快速超时，出现误检测
处理建议	将S-Trunk两端设备对应组的S-Trunk报文发送周期设置为相同

104 SYSEVENT

本节介绍系统事件模块输出的日志信息。

104.1 EVENT_TIMEOUT

日志内容	Module [UINT32]'s processing for event [UINT32] timed out. Module [UINT32]'s processing for event [UINT32] on [STRING] timed out.
参数解释	$1：模块ID $2：事件ID $3：MDC *MDC-ID*或Context *Context-ID*
日志等级	6
举例	SYSEVENT/6/EVENT_TIMEOUT: -MDC=1; Module 0x1140000's processing for event 0x20000010 timed out. SYSEVENT/6/EVENT_TIMEOUT: -Context=1; Module 0x33c0000's processing for event 0x20000010 on Context 16 timed out.
日志说明	应用模块处理事件超时 非缺省MDC/Context上打印的日志信息不包含MDC *MDC-ID*或Context *Context-ID* 缺省MDC/Context上打印的本MDC/Context的日志信息不包含MDC *MDC-ID*或Context *Context-ID* 缺省MDC/Context上打印的其它MDC/Context的日志信息包含MDC *MDC-ID*或Context *Context-ID*
处理建议	无

105 SYSLOG

本节包含 syslog 日志消息。

105.1 SYSLOG_FILE_DECOMPRESS_ERROR

日志内容	Failed to decompress [STRING].
参数解释	$1：待解压的日志文件的名称和路径
日志等级	4
举例	SYSLOG/4/SYSLOG_FILE_DECOMPRESS_ERROR: Failed to decompress flash:/logfile/logfile1.log.gz.
日志说明	解压日志文件失败
处理建议	1. 在用户视图下，通过 **dir** 命令查看存储介质是否空间不足，如果空间不足则使用 **delete /unreserved** 命令删除部分不再使用的文件 2. 其它情况请联系技服人员解决

105.2 SYSLOG_LOGBUFFER_FAILURE

日志内容	Log cannot be sent to the logbuffer because of communication timeout between syslog and DBM processes.
参数解释	无
日志等级	4
举例	SYSLOG/4/SYSLOG_LOGBUFFER_FAILURE: Log cannot be sent to the logbuffer because of communication timeout between syslog and DBM processes.
日志说明	日志无法输出到日志缓冲区，因为Syslog进程和DBM进程通信超时
处理建议	请联系技术支持人员

105.3 SYSLOG_LOGFILE_FULL

日志内容	Log file space is full.
参数解释	无
日志等级	4
举例	SYSLOG/4/SYSLOG_LOGFILE_FULL: Log file space is full.
日志说明	日志空间已满
处理建议	备份日志文件后将其删除，然后根据需要使能端口

105.4 SYSLOG_RESTART

日志内容	System restarted -- [STRING] [STRING] Software.
参数解释	$1：公司名称 $2：软件名称
日志等级	6
举例	SYSLOG/6/SYSLOG_RESTART: System restarted -- UNIS Uniware Software
日志说明	系统重启日志
处理建议	无

105.5 SYSLOG_RTM_EVENT_BUFFER_FULL

日志内容	In the last minute, [String] syslog logs were not monitored because the buffer was full.
参数解释	$1：过去1分钟内SYSLOG模块没有发送给EAA模块的日志的条数
日志等级	5
举例	SYSLOG/5/SYSLOG_RTM_EVENT_BUFFER_FULL: In the last minute, 100 syslog logs were not monitored because the buffer was full.
日志说明	设备在短时间内产生大量日志，导致EAA监控的日志缓冲区被占满，有多条日志没来得及匹配便被丢弃了
处理建议	• 找到日志的来源，减少日志的生成 • 使用 **rtm event syslog buffer-size** 命令增大 EAA 监控的日志缓冲区的大小

106 TACACS

本节介绍 TACACS 模块输出的日志信息。

106.1 TACACS_AUTH_FAILURE

日志内容	User [STRING] from [STRING] failed authentication.
参数解释	$1：用户名称 $2：IP地址
日志等级	5
举例	TACACS/5/TACACS_AUTH_FAILURE: User cwf@system from 192.168.0.22 failed authentication.
日志说明	TACACS服务器了拒绝用户的认证请求
处理建议	无

106.2 TACACS_AUTH_SUCCESS

日志内容	User [STRING] from [STRING] was authenticated successfully.
参数解释	$1：用户名称 $2：IP地址
日志等级	6
举例	TACACS/6/TACACS_AUTH_SUCCESS: User cwf@system from 192.168.0.22 was authenticated successfully.
日志说明	TACACS服务器接收了用户的认证请求
处理建议	无

106.3 TACACS_DELETE_HOST_FAIL

日志内容	Failed to delete servers in scheme [STRING].
参数解释	$1：方案名称
日志等级	4
举例	TACACS/4/TACACS_DELETE_HOST_FAIL: Failed to delete servers in scheme abc.
日志说明	删除TACACS方案中的服务器失败
处理建议	无

107 TE

本节介绍 TE 模块输出的日志信息。

107.1 TE_BACKUP_SWITCH

日志内容	Tunnel [UNIT] ([STRING]): [STRING]. [STRING]
参数解释	$1：主隧道信息 $2：LSP信息 $3：会话保护状态，取值包括： • Backup tunnel ready：热备隧道保护状态，此时未进行切换 • Backup tunnel used：热备隧道保护使用状态，此时已切换 • Backup tunnel disabled：不需要保护 • Main tunnel recovered：主链路恢复，切换回主链路 $4：LSP路径信息，包括LSP经过的LSR节点的接口IP地址、LSR ID或使用的标签值。仅当状态为Backup tunnel used或Main tunnel recovered时打印
日志等级	5
举例	TE/5/TE_BACKUP_SWITCH: Tunnel 5 (IngressLsrID=1.1.1.8 EgressLsrID=2.2.2.8 LSPID=100 Bandwidth=1000kbps): Backup tunnel used. Current LSP path is 10.1.1.1/32(flag=0x00) - 10.1.1.2/32(flag=0x00) - 1151(flag=0x01) - 2.2.2.8/32(flag=0x20).
日志说明	当热备隧道或Segment Routing隧道建立、取消和热备切换时，触发该日志
处理建议	无

107.2 TE_MBB_SWITCH

日志内容	Tunnel [STRING] ([STRING]): Make before break triggered by [STRING]. [STRING]
参数解释	$1：主隧道信息 $2：LSP信息 $3：Make-before-break重建隧道，取值包括： • configuration change：配置变化，触发重建隧道 • FRR used：FRR 主隧道已切换，触发重建主隧道 • reoptimize timer expiration：重优化时间到，触发重建隧道 • automatic bandwidth adjustment: 自动带宽调整，触发重建隧道 • stateful PCE updated：接收 Stateful PCE PCUpd 消息，触发重建隧道 $4：LSP路径信息
日志等级	5
举例	TE/5/TE_MBB_SWITCH: Tunnel 5 (IngressLsrID=1.1.1.8 EgressLsrID=2.2.2.8 LSPID=100 Bandwidth=1000kbps): Make-before-break triggered by configuration change. Current LSP path is 10.1.1.1/32(flag=0x00) - 10.1.1.2/32(flag=0x00) - 1151(flag=0x01) - 2.2.2.8/32(flag=0x20).
日志说明	当make-before-break重建隧道时，触发该日志
处理建议	无

107.3 TE_TUNNEL_NESTING

日志内容	Tunnel [STRING] had the nesting issue.
参数解释	$1：隧道的ID
日志等级	4
举例	TE/4/TE_TUNNEL_NESTING: -MDC=1; Tunnel1002 had the nesting issue.
日志说明	由于错误配置**nextsid**引起隧道出现嵌套

处理建议	隧道存在嵌套，即隧道引用的显式路径中配置的**nextsid** [**index** *index-number*] **label** *label-value* **type binding-sid**为一条隧道。错误的隧道嵌套，会导致报文转发失败。当隧道存在错误嵌套时，处理建议如下：
	• 删除当前隧道引用的显示路径中配置的 **nextsid** [**index** *index-number*] **label** *label-value* **type binding-sid**，防止隧道错误嵌套
	• 检查是否存在如下错误嵌套
	  ○ 自身嵌套，即当前隧道引用的显示路径中 **binding-sid** 对应的标签值标识的 MPLS TE 隧道为当前隧道
	  ○ 多层嵌套，目前只支持一层嵌套
	  ○ 循环嵌套，例如：隧道 A 嵌套隧道 B，隧道 B 又嵌套隧道 A

107.4 TE_LABEL_DUPLICATE

日志内容	Binding SID label [STRING] for tunnel [STRING] is duplicate.
参数解释	$1：隧道绑定的SID标签值 $2：隧道的ID
日志等级	4
举例	TE/4/TE_LABEL_DUPLICATE: -MDC=1; Binding SID label 1200 for tunnel 1 is duplicate.
日志说明	为MPLS TE隧道指定的BSID标签已被占用
处理建议	• 继续使用该标签。通过 **display mpls label** 命令查看该标签被哪个协议占用，执行相关配置释放该标签。然后删除隧道下配置的 **mpls te binding-sid** 命令，再重新执行该命令为 MPLS TE 隧道指定 BSID • 使用其他未被占用的标签

108 TELNETD

本节介绍 TELNETD（Telnet Daemon）模块输出的日志信息。

108.1 TELNETD_ACL_DENY

日志内容	The Telnet Connection [IPADDR]([STRING]) request was denied according to ACL rules.
参数解释	$1：Telnet客户端IP地址 $2：Telnet客户端IP地址所在VPN
日志等级	5
举例	TELNETD/5/TELNETD_ACL_DENY: The Telnet Connection 1.2.3.4(vpn1) request was denied according to ACL rules.
日志说明	Telnet ACL规则限制登录IP地址。该日志在Telnet服务端检测到非法客户端尝试登录时输出
处理建议	无

108.2 TELNETD_REACH_SESSION_LIMIT

日志内容	Telnet client [STRING] failed to log in. The current number of Telnet sessions is [NUMBER]. The maximum number allowed is ([NUMBER]).
参数解释	$1：Telnet客户端IP地址 $2：当前的Telnet会话数 $3：设备允许建立的Telnet会话数
日志等级	6
举例	TELNETD/6/TELNETD_REACH_SESSION_LIMIT: Telnet client 1.1.1.1 failed to log in. The current number of Telnet sessions is 10. The maximum number allowed is (10).
日志说明	Telnet登录用户达到上限。该日志在Telnet服务端检测到登录客户端数达到上限时输出
处理建议	请根据需要使用命令**aaa session-limit**配置允许的Telnet最大登录用户数

109 UCM

本节介绍 UCM 模块输出的日志信息。

109.1 UCM_SESSIONS_LOWER_THRESHOLD

日志内容	The access user session number is below the lower warning threshold (LowerThreshold=[INT32]).
参数解释	$1：在线接入用户会话数目的下限告警阈值
日志等级	4
举例	UCM/4/UCM_SESSIONS_LOWER_THRESHOLD: The access user session number is below the lower warning threshold (LowerThreshold=20).
日志说明	在线接入用户会话数目已低于配置的下限告警阈值
处理建议	1. 执行 **display access-user** 命令查看接入用户总数信息 2. 确认接入用户是否非正常大量下线

109.2 UCM_SESSIONS_RECOVER_NORMAL

日志内容	The access user session number has recovered to normal state.
参数解释	无
日志等级	5
举例	UCM/5/UCM_SESSIONS_RECOVER_NORMAL: The access user session number has recovered to normal state.
日志说明	在线接入用户会话数目重新恢复到设定的正常范围内
处理建议	无

109.3 UCM_SESSIONS_UPPER_THRESHOLD

日志内容	The access user session number is above the upper warning threshold (UpperThreshold=[INT32]).
参数解释	$1：在线接入用户会话数目的上限告警阈值
日志等级	4
举例	UCM/4/ UCM_SESSIONS_UPPER_THRESHOLD: The access user session number is above the upper warning threshold (UpperThreshold=20).
日志说明	在线接入用户会话数目已高于配置的上限告警阈值
处理建议	1. 执行 **display access-user** 命令查看接入用户总数信息 2. 确认是否存在大量非法接入用户上线

109.4 USER_LOGON_SUCCESS

日志内容	-UserName=[STRING]-IPv4Addr=[IPADDR]-IPv6Addr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-RemoteTunnelIPAddr=[STRING]-RemoteTunnelName=[STRING]; The user came online successfully.
参数解释	$1：用户名 $2：用户IPv4地址 $3：用户IPv6地址 $4：接口名称 $5：外层VLAN ID $6：内层VLAN ID $7：MAC地址 $8：远端隧道地址 $9：远端隧道名称
日志等级	6
举例	UCM/6/USER_LOGON_SUCCESS: -UserName=user1-IPv4Addr=1.1.0.1-IPv6Addr=N/A-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF-RemoteTunnelIPAddr=123.1.1.2-RemoteTunnelName=LAC; The user came online successfully.
日志说明	用户上线成功
处理建议	无

109.5 USER_LOGON_FAILED

日志内容	-UserName=[STRING]-IPv4Addr=[IPADDR]-IPv6Addr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-RemoteTunnelIPAddr=[STRING]-RemoteTunnelName=[STRING]-Reason=[STRING]; The user failed to come online.
参数解释	$1：用户名 $2：用户IPv4地址 $3：用户IPv6地址 $4：接口名称 $5：外层VLAN ID $6：内层VLAN ID $7：MAC地址 $8：远端隧道IP地址 $9：远端隧道名称 $10：上线失败原因，取值请参见表108-1
日志等级	6
举例	UCM/6/USER_LOGON_FAILED: -UserName=user1-IPv4Addr=N/A-IPv6Addr=N/A-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF-RemoteTunnelIPAddr=123.1.1.2-RemoteTunnelName=LNS1-Reason= Invalid username or password ; The user failed to come online.
日志说明	用户上线失败
处理建议	具体处理建议请见表108-1

表109-1 上线失败原因列表

上线失败原因	说明	处理建议
The number of users on this interface has reached the upper limit	上线用户数达到接口允许接入的最大用户数	按根据需要，使用**access-limit**命令用调整接口允许接入的最大用户数
The number of users on this device has reached the upper limit	上线用户数达到整机允许接入的最大用户数	请根据需要，购买能够满足接入用户数需求的License
The VPN bound to the IPoE static user and the authorized VPN are different	静态用户绑定的VPN实例与AAA为静态用户授权VPN实例不一致时不允许用户上线	如果需要静态用户绑定VPN实例的同时也授权VPN实例，请保证两个VPN实例相同

109.6 USER_LOGOFF

日志内容	-UserName=[STRING]-IPv4Addr=[IPADDR]-IPv6Addr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-RemoteTunnelIPAddr=[STRING]-RemoteTunnelName=[STRING]-Reason=[STRING]; The user logged off.
参数解释	$1：用户名 $2：用户IPv4地址 $3：用户IPv6地址 $4：接口名称 $5：外层VLAN ID $6：内层VLAN ID $7：MAC地址 $8：远端隧道IP地址 $9：远端隧道名 $10：下线原因，取值请参见表108-2
日志等级	6
举例	UCM/6/USER_LOGOFF: -UserName=user1-IPv4Addr=1.1.0.1-IPv6Addr=N/A-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF-RemoteTunnelIPAddr=123.1.1.2-RemoteTunnelName=LNS1-Reason=user logoff; The user logged off.
日志说明	用户正常下线
处理建议	无

表109-2 正常下线原因列表

下线原因	说明
Re-DHCP for IPoE Web authentication	在二次地址分配MAC无感知应用中，用户走普通Web流程在Web阶段认证成功上线后，当设备收到AAA服务器的计费应答报文后，强制DHCP用户下线，以便用户可以重新走MAC无感知流程上线

109.7 USER_LOGOFF_ABNORMAL

日志内容	-UserName=[STRING]-IPv4Addr=[IPADDR]-IPv6Addr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-RemoteTunnelIPAddr=[STRING]-RemoteTunnelName=[STRING]-Reason=[STRING]; The user logged off abnormally.
参数解释	$1：用户名 $2：用户IPv4地址 $3：用户IPv6地址 $4：接口名称 $5：外层VLAN ID $6：内层VLAN ID $7：MAC地址 $8：远端隧道IP地址 $9：远端隧道名 $10：下线原因，具体原因请见表108-3
日志等级	6
举例	UCM/6/USER_LOGOFF_ABNORMAL: -UserName=user1-IPv4Addr=1.1.0.1-IPv6Addr=N/A-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF-RemoteTunnelIPAddr=123.1.1.2-RemoteTunnelName=LNS1-Reason=session time out; The user logged off abnormally.
日志说明	用户异常下线
处理建议	具体处理建议请见表108-3

表109-3 异常下线原因列表

下线原因	说明	处理建议
Logged out by the RADIUS proxy	在RADIUS代理组网中，对于通过无线方式上线的802.1X和IPoE用户，当802.1X用户下线时，会同时将IPoE用户下线	请排查802.1X用户的下线原因
UP switchover	在UP备份组网中，主备UP切换导致用户下线	请联系技术支持

UP switchover without backup interface	在UP热备或温备组网中，主备UP切换时，没有备接口导致用户下线	• 温备模式下：
		  ◦ 请检查是否执行 **backup-interface** 命令配置了备接口
		  ◦ 若是子接口接入，请继续检查用户上线子接口是否存在对应的备份子接口。若存在备份子接口，还需要检查该备份子接口是否正常
		• 热备模式下，请继续检查用户上线子接口是否存在对应的备份子接口。若存在备份子接口，还需要检查该备份子接口是否正常

UP backup status change	模块（例UP备份模块）进程重启、UP迁移或主备倒换等原因引起UP备份组状态变化时导致用户下线	请检查当前UP备份组的状态是否正常；如不正常请继续检查最近是否修改了UP备份的配置，确保配置正确
UP backup configuration change	UP备份的配置变化导致用户下线	请检查最近修改的配置

110 URPF

本节介绍 uRPF 模块输出的日志信息。

110.1 URPF_CONFIG

日志内容	形式一： Failed to enable uRPF. uRPF is not supported. 形式二： Failed to enable uRPF on [STRING]. uRPF is not supported on [STRING]. 形式三： Failed to enable uRPF on [STRING] slot [INT32]. uRPF is not supported on [STRING] slot [INT32]. 形式四： Failed to enable uRPF on [STRING] slot [INT32] cpu [INT32]. uRPF is not supported on [STRING] slot [INT32] cpu [INT32]. 形式五： Failed to enable uRPF on [STRING] chassis [INT32] slot [INT32]. uRPF is not supported on [STRING] chassis [INT32] slot [INT32]. 形式六： Failed to enable uRPF on [STRING] chassis [INT32] slot [INT32] cpu [INT32]. uRPF is not supported on [STRING] chassis [INT32] slot [INT32] cpu [INT32]
参数解释	形式二： $1：接口 形式三： $1：接口或安全域 $2：Slot编号 形式四： $1：接口或安全域 $2：Slot编号 $3：CPU编号 形式五： $1：接口或安全域 $2：Chassis编号 $3：Slot编号 形式六： $1：接口或安全域 $2：Chassis编号 $3：Slot编号 $4：CPU编号
日志等级	4
举例	URPF/4/URPF_CONFIG: -MDC=1-Chassis=2-Slot=2; Failed to enable uRPF on Vlan-interface2 chassis 2 slot 2.
日志说明	形式一： 全局开启IPv4 uRPF功能失败。

	设备不支持全局开启IPv4 uRPF功能。 形式二： 在指定接口或安全域上开启IPv4 uRPF功能失败。 设备不支持在指定接口或安全域上开启IPv4 uRPF功能。 形式三： 在指定Slot指定接口或安全域上开启IPv4 uRPF功能失败。 设备不支持在指定Slot指定接口或安全域上开启IPv4 uRPF功能。 形式四： 在指定Slot指定CPU指定接口或安全域上开启IPv4 uRPF功能失败。 设备不支持在指定Slot指定CPU指定接口或安全域上开启IPv4 uRPF功能。 形式五： 在指定Chassis指定Slot指定接口或安全域上开启IPv4 uRPF功能失败。 设备不支持在指定Chassis指定Slot指定接口或安全域上开启IPv4 uRPF功能。 形式四： 在指定Chassis指定Slot指定CPU指定接口或安全域上开启IPv4 uRPF功能失败。 设备不支持在指定Chassis指定Slot指定CPU指定接口或安全域上开启IPv4 uRPF功能。
处理建议	无

110.2 URPF6_CONFIG

日志内容	形式一： Failed to enable IPv6 uRPF. IPv6 uRPF is not supported. 形式二： Failed to enable IPv6 uRPF on [STRING]. IPv6 uRPF is not supported on [STRING]. 形式三： Failed to enable IPv6 uRPF on [STRING] slot [INT32]. IPv6 uRPF is not supported on [STRING] slot [INT32]. 形式四： Failed to enable IPv6 uRPF on [STRING] slot [INT32] cpu [INT32]. IPv6 uRPF is not supported on [STRING] slot [INT32] cpu [INT32]. 形式五： Failed to enable IPv6 uRPF on [STRING] chassis [INT32] slot [INT32]. IPv6 uRPF is not supported on [STRING] chassis [INT32] slot [INT32]. 形式六： Failed to enable IPv6 uRPF on [STRING] chassis [INT32] slot [INT32] cpu [INT32]. IPv6 uRPF is not supported on [STRING] chassis [INT32] slot [INT32] cpu [INT32]
参数解释	形式二： $1：接口或安全域 形式三： $1：接口或安全域 $2：Slot编号 形式四： $1：接口或安全域 $2：Slot编号 $3：CPU编号 形式五： $1：接口或安全域 $2：Chassis编号 $3：Slot编号 形式六： $1：接口或安全域 $2：Chassis编号 $3：Slot编号 $4：CPU编号
日志等级	4
举例	URPF/4/URPF6_CONFIG: -MDC=1-Chassis=2-Slot=2; Failed to enable IPv6 uRPF on Vlan-interface2 chassis 2 slot 2.
日志说明	形式一： 全局开启IPv6 uRPF功能失败。

	设备不支持全局开启IPv6 uRPF功能。 形式二： 在指定接口或安全域上开启IPv6 uRPF功能失败。 设备不支持在指定接口或安全域上开启IPv6 uRPF功能。 形式三： 在指定Slot指定接口或安全域上开启IPv6 uRPF功能失败。 设备不支持在指定Slot指定接口或安全域上开启IPv6 uRPF功能。 形式四： 在指定Slot指定CPU指定接口或安全域上开启IPv6 uRPF功能失败。 设备不支持在指定Slot指定CPU指定接口或安全域上开启IPv6 uRPF功能。 形式五： 在指定Chassis指定Slot指定接口或安全域上开启IPv6 uRPF功能失败。 设备不支持在指定Chassis指定Slot指定接口或安全域上开启IPv6 uRPF功能。 形式四： 在指定Chassis指定Slot指定CPU指定接口或安全域上开启IPv6 uRPF功能失败。 设备不支持在指定Chassis指定Slot指定CPU指定接口或安全域上开启IPv6 uRPF功能。
处理建议	无

111 USER

本节介绍业务跟踪模块输出的日志信息。

111.1 USER_RECOVER_NORMAL

日志内容	形式一： The user number on slot [INT32] has recovered to normal state. 形式二： The user number on chassis [INT32] slot [INT32] has recovered to normal state.
参数解释	形式一： $1：slot编号 形式二： $1：chassis编号 $2：slot编号
日志等级	5
举例	USER/5/ USER_RECOVER_NORMAL: The user number on slot 1 has recovered to normal state.
日志说明	指定slot上接入用户数从上限阈值重新恢复到设定的正常范围
处理建议	无

111.2 USER_TRACEINFO

日志内容	[objectID=[UINT16]][slotID=[UINT16]][STRING][user info: [STRING]][trace info:[STRING]]
参数解释	$1：业务跟踪对象的编号 $2：接入用户所属的槽位号 $3：业务跟踪阶段，目前有PPPoE、L2TP、PPP、IPoE、Portal、UCM和AAA等多个阶段 $4：用户信息。各用户信息含义请参见表110-1被跟踪用户信息描述表 $5：跟踪详细信息。各业务跟踪阶段的详细跟踪信息如下： ○ 各 PPPoE 阶段的详细信息请参见表 110-2 被跟踪详细信息描述表（PPPoE） ○ 各 L2TP 阶段的详细信息请参见表 110-3 被跟踪详细信息描述表（L2TP） ○ 各 PPP 阶段的详细信息请参见表 110-4 被跟踪详细信息描述表（PPP） ○ 各 IPoE 阶段的详细信息请参见表 110-5 被跟踪详细信息描述表（IPoE） ○ 各 Portal 阶段的详细信息请参见表 110-6 被跟踪详细信息描述表（Portal） ○ 各 UCM 阶段的详细信息请参见表 110-7 被跟踪详细信息描述表（UCM） ○ 各 AAA 阶段的详细信息请参见表 110-8 被跟踪详细信息描述表（AAA） ○ 各 DHCP 阶段的信息请参见表 110-9 被跟踪详细信息描述表（DHCP） ○ 各 ARP 阶段的详细信息请参见表 110-10 被跟踪详细信息描述表（ARP） ○ 各 ND 阶段的详细信息请参见表 110-11 被跟踪详细信息描述表（ND） ○ 各 IGMP 阶段的详细信息请参见表 110-12 被跟踪详细信息描述表（IGMP） ○ 各 MLD 阶段的详细信息请参见表 110-13 被跟踪详细信息描述表（MLD）
日志等级	7
举例	USER/7/USER_TRACEINFO:[objectID=1][slotID=0][UCM][user info: MAC address: dc2d-cb00-0020 IP address: 2.2.2.8 Access interface: GigabitEthernet1/2/0/1 User name: 2.2.2.8 Access mode: IPoE] [trace info:[Adapt State]UserID:4, ConnectID:0, Receive MODIFY event, current state is ADDED]
日志说明	编号为1业务跟踪对象在UCM阶段，从1号槽位的GigabitEthernet1/2/0/1接口收到一个MODIFY事件消息
处理建议	无

1. 被跟踪用户信息描述表

表111-1 被跟踪用户信息描述表

字段	描述
MAC address	接入用户的MAC地址
Access interface	接入用户接入接口
Service VLAN	接入用户的外层VLAN ID

字段	描述
Customer VLAN	接入用户的内层VLAN ID
Tunnel ID	接入用户的L2TP隧道ID
Username	接入用户的用户名
IP address	接入用户的IP地址
Access mode	业务跟踪对象的接入模式

2. 被跟踪详细信息描述表

(1) PPPoE

表111-2 被跟踪详细信息描述表（PPPoE）

字段	描述
Received a PADI packet	PPPoE Sever收到PPPoE Client的PADI报文
Sent a PADO packet	PPPoE Server向PPPoE Client发送PADO报文
Received a PADR packet	PPPoE Sever收到PPPoE Client的PADR报文
Established a PPPoE session successfully. Notified PPP to create session (session ID=*sessionid*)	建立PPPoE会话，通知PPP创建会话.。其中session ID表示PPP会话ID
Sent a PADS packet	PPPoE Server向PPPoE Client发送PADS报文
Established a PPPoE session successfully. Notified PPP to start session negotiation (session ID=*sessionid*)	建立PPPoE会话，通知PPP开始会话协商。其中session ID表示PPP会话ID
Received a PADT packet	PPPoE Sever收到PPPoE Client的PADT报文
Deleted the PPPoE session successfully.	删除PPPoE会话
Sent a PADT packet	PPPoE Sever向PPPoE Client发送PADT报文

(2) L2TP

表111-3 被跟踪详细信息描述表（L2TP）

字段	描述
PPP notified LAC up and L2TP started a tunnel establishment process	PPP通知LAC up事件，LAC端发起L2TP隧道协商
PPP notified LAC up and L2TP started establishing a session within a middle state L2TP tunnel	PPP通知LAC up事件，LAC端在一个中间状态的L2TP隧道中发起L2TP会话协商
PPP notified LAC up and L2TP started establishing a session within an L2TP tunnel	PPP通知LAC up事件，LAC端在一个已经建立的L2TP隧道中发起L2TP会话协商
Sent an ICRQ packet to LNS, TunnelID=*tunnelid*, SessionID=*sessionid*	LAC端向LNS端发送ICRQ报文。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID

字段	描述
Received an ICRP packet, TunnelID=*tunnelid*, SessionID=*sessionid*	LAC端收到ICRP报文。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID
Sent an ICCN packet to LNS, TunnelID=*tunnelid*, SessionID=*sessionid*	LAC端向LNS端发送ICCN报文。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID
Received an ICCN packet and processed successfully, TunnelID=*tunnelid*, SessionID=*sessionid*	LNS端收到ICCN报文，处理成功。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID
Received an invalid ICCN packet and failed to process it, TunnelID=*tunnelid*, SessionID=*sessionid*	LNS端收到非法ICCN报文，处理失败。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID
Received an ICCN packet but failed to allocate resources, TunnelID=*tunnelid*, SessionID=*sessionid*	LNS端收到ICCN报文，资源不足处理失败。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID
Received an ICCN packet but failed to process it, TunnelID=*tunnelid*, SessionID=*sessionid*	LNS端收到ICCN报文，但处理失败。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID
An L2TP session on LAC was going offline, TunnelID=*tunnelid*, SessionID=*sessionid*	LAC端L2TP会话正在下线。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID
An L2TP session on LNS was going offline, TunnelID=*tunnelid*, SessionID=*sessionid*	LNS端L2TP会话正在下线。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID
Sent a CDN packet to the peer, TunnelID=*tunnelid*, SessionID=*sessionid*	本端向对端发送CDN报文。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID
Received a CDN packet, TunnelID=*tunnelid*, SessionID=*sessionid*	本端收到对端发送的CDN报文
Deleted an L2TP session, TunnelID=*tunnelid*, SessionID=*sessionid*	删除本地L2TP会话。其中： • TunnelID：表示 L2TP 隧道 ID • SessionID：表示 L2TP 会话 ID

(3) PPP

表111-4 被跟踪详细信息描述表（PPP）

字段	描述
Received interface up event	PPP收到接口up事件
LCP FSM open event	PPP LCP状态机open事件
Determined negotiation parameters during LCP initialization	LCP初始化，确定LCP需要协商参数
LCP FSM up event	PPP LCP状态机up事件
Sent an LCP Configuration Request packet	PPP发送LCP Configure-Request报文
Received an LCP negotiation packet or Echo keepalive packet	PPP收到LCP协商报文或echo保活报文
Received an LCP Configuration Request packet	PPP收到LCP Configure-Request报文
Sent an LCP Configuration Ack packet	PPP发送LCP Configure-Ack报文
Received an LCP Configuration Ack packet	PPP收到LCP Configure-Ack报文
LCP up event	PPP LCP 协商成功
LCP FSM down event	PPP LCP状态机down事件
LCP down event	PPP收到LCP down事件
LCP FSM close event	PPP LCP状态机close事件
Started authentication after LCP negotiation succeeded	PPP LCP 协商阶段成功，进入认证阶段
Sent a CHAP Challenge packet	PPP CHAP认证阶段发送Challenge报文
Received a CHAP authentication packet in authentication phase	PPP在认证阶段收到CHAP认证类型报文
Received a CHAP Request packet	PPP收到CHAP认证请求报文
Sent an authentication request to UCM	PPP向UCM发送认证请求，进行认证
Received a CHAP authentication success message from AAA	PPP收到AAA的CHAP认证成功消息
Sent a CHAP Ack packet	PPP向客户端发送CHAP认证成功报文
CHAP authentication succeeded	PPP CHAP认证成功
Received a CHAP authentication failure message from AAA	PPP收到AAA的CHAP认证失败消息
Sent a CHAP Nak packet	PPP向客户端发送CHAP认证失败报文
Received a PAP authentication packet in authentication phase	PPP在认证阶段收到PAP认证类型报文
Received a PAP Request packet	PPP收到PAP认证请求报文
Received a PAP authentication success message from AAA	PPP收到AAA的PAP认证成功消息
Sent a PAP Ack packet	PPP向客户端发送PAP认证成功报文
PAP authentication succeeded	PPP PAP认证成功

字段	描述
PAP authentication failed	PPP PAP认证失败
Received a PAP authentication failure message from AAA	PPP收到AAA的PAP认证失败消息
Sent a PAP Nak packet	PPP向客户端发送PAP认证失败报文
Received an LCP Termination Request packet	PPP收到LCP Terminate-Request报文
Sent an LCP Termination Ack packet	PPP发送LCP Terminate-Ack报文
Started NCP negotiation	PPP 进入NCP协商阶段
IPCP FSM open event	PPP IPCP状态机open事件
Determined negotiation parameters during IPCP initialization	初始化IPCP协商选项
IPCP FSM up event	PPP IPCP状态机up事件
Sent an IPCP Configuration Request packet	PPP发送IPCP Configure-Request报文
Received an IPCP negotiation packet in IPCP negotiation phase	PPP在IPCP协商阶段收到IPCP协商报文
Received an IPCP Configuration Request packet	PPP收到IPCP Configure-Request报文
Received an IPCP Configuration Ack packet	PPP收到IPCP Configure-Ack报文
Sent an IPCP Configuration Nak packet	PPP发送IPCP Configure-Nak报文
Sent an IPCP Configuration Ack packet	PPP发送IPCP Configure-Ack报文
IPCP negotiation succeeded	PPP IPCP 协商成功
Sent an LCP Echo Request packet	PPP发送Echo-Request报文
Received an LCP Echo Reply packet	PPP收到Echo-Reply报文
Received interface down event	PPP收到接口down事件
IPCP FSM down event	PPP IPCP状态机down事件
IPCP down event	PPP收到IPCP down事件
IPCP FSM close event	PPP IPCP状态机close事件
Notify NCP down	LCP通知上层协议NCP down
PPP L2TP prenego started	PPP L2TP预协商开始
PPP L2TP prenego finished	PPP L2TP预协商结束
Mandatory-lcp, LCP renego started	强制LCP重协商，开始LCP重协商
Mandatory-chap, CHAP renego started	强制CHAP验证，开始CHAP验证
L2TP mandatory-chap needed the authentication mode of CHAP on VT	配置强制CHAP验证，但VT口上没有配置CHAP认证方式
LCP prenego for L2TP failed	LCP预协商失败
PPP L2TP prenego CHAP started	CHAP认证预协商开始

字段	描述
PPP L2TP prenego CHAP finished	CHAP认证预协商结束
PPP L2TP prenego PAP started	PAP认证预协商开始
PPP L2TP prenego PAP finished	PAP认证预协商结束
PPP L2TP prenego MSCHAP started	MSCHAP认证预协商开始
PPP L2TP prenego MSCHAP finished	MSCHAP认证预协商结束
PPP L2TP prenego authentication failed	PPP L2TP认证预协商失败
Received an LCP Configuration Nak packet	PPP收到LCP Configure-Nak报文
Sent an LCP Configuration Nak packet	PPP发送LCP Configure-Nak报文
Received an LCP Configuration Reject packet	PPP收到LCP Configure-Reject报文
Sent an LCP Configuration Reject packet	PPP发送LCP Configure-Reject报文
Received an LCP Termination Ack packet	PPP收到LCP Termination-Ack报文
Sent an LCP Termination Request packet	PPP发送LCP Termination-Request报文
Received an LCP Code Reject packet	PPP收到LCP Code-Reject报文
Sent an LCP Code Reject packet	PPP发送LCP Code-Reject报文
Received an LCP Protocol Reject packet	PPP收到LCP Protocol-Reject报文
Sent an LCP Protocol Reject packet	PPP发送LCP Protocol-Reject报文
Received an LCP Echo Request packet	PPP收到LCP Echo-Request报文
Sent an LCP Echo Reply packet	PPP发送LCP Echo-Reply报文
Received an LCP Identification packet	PPP收到LCP Identification报文
Sent an LCP Identific packet	PPP发送LCP Identific报文
Received an IPCP Configuration Nak packet	PPP收到IPCP Configure-Nak报文
Sent an IPCP Configuration Reject packet	PPP发送IPCP Configure-Reject报文
Received an IPCP Configuration Reject packet	PPP收到IPCP Configure-Reject报文
Sent an IPCP Termination Request packet	PPP发送IPCP Termination-Request报文
Received an IPCP Termination Request packet	PPP收到IPCP Termination-Request报文
Sent an IPCP Termination Ack packet	PPP发送IPCP Termination-Ack报文
Received an IPCP Termination Ack packet	PPP收到IPCP Termination-Ack报文
Sent an IPCP Code Reject packet	PPP发送IPCP Code-Reject报文
Received an IPCP Code Reject packet	PPP收到IPCP Code-Reject报文
Sent a CHAP Request packet	PPP发送CHAP Request报文
Received a CHAP Challenge packet	PPP收到CHAP Challenge报文
Received a CHAP Ack packet	PPP收到CHAP Ack报文

字段	描述
Received a CHAP Nak packet	PPP收到CHAP Nak报文
Sent a MS-CHAP-V2 CHGPWD packet	PPP发送MS-CHAP-V2 CHGPWD报文
Received a PAP Ack packet	PPP收到PAP Ack报文
Received a PAP Nak packet	PPP收到PAP Nak报文
Sent a PAP Request packet	PPP发送PAP Request报文
Authentication failed	认证失败
Authentication succeeded	认证成功
CHAP authentication failed	CHAP认证失败
Received an authentication failure message from UCM	PPP从UCM接收到认证失败消息
Received an authentication success message from UCM	PPP从UCM接收到认证成功消息
Sent a conn request to UCM	PPP向UCM发送连接请求
Sent a conn-down request to UCM	PPP向UCM发送连接down请求
Sent a conn-up request to UCM	PPP向UCM发送连接up请求
Sent an MP bundle request to UCM	PPP向UCM发送MP捆绑请求
Sent an offline request to UCM	PPP向UCM发送下线请求

(4) IPoE

表111-5 被跟踪详细信息描述表（IPoE）

字段	描述
Received an IP packet, VPN=*vpn*	IPoE收到用户IP报文。其中，VPN表示用户所属VPN实例，如果用户属于公网，则不显示VPN字段
Sent a packet to UCM for authentication, VPN=*vpn*	IPoE发送报文到UCM进行认证。其中，VPN表示用户所属VPN实例，如果用户属于公网，则不显示VPN字段
Received a Reject message from UCM, VPN=*vpn*	IPoE从UCM收到拒绝用户连接的通知。其中，VPN表示用户所属VPN实例，如果用户属于公网，则不显示VPN字段

(5) Portal

表111-6 被跟踪详细信息描述表（Portal）

字段	描述
Sent logon request to UCM	Portal向UCM发送认证请求消息
Received logon success message from UCM	Portal收到UCM发送的上线成功消息
Received logon failure message from UCM	Portal收到UCM发送的上线失败消息
Sent logoff request to UCM	Portal向UCM发送下线请求消息

字段	描述
Received logoff response from UCM	Portal收到UCM发送的下线应答消息
Received forced-logoff message from UCM	Portal收到UCM发送的强制用户下线消息
Received message for user informaiton transparent transmission from UCM	Portal收到UCM发送的待透传的用户信息
Received MAC binding query request from IPoE	Portal收到IPoE发送的MAC地址绑定查询消息
Sent MAC binding query response to IPoE	Portal向IPoE发送MAC地址绑定查询应答消息
Received MAC-trigger user online message from UCM	Portal收到UCM发送的MAC地址绑定用户上线通知消息
Received MAC-trigger user offline message from UCM.	Portal收到UCM发送的MAC地址绑定用户下线通知消息
Received user roaming message from UCM	Portal收到UCM发送的用户漫游消息
Received authentication-continue message from UCM	Portal收到UCM发送的认证持续消息
Received packet from portal server newpt	接收到Portal服务器newpt发送的报文
Sent packet to portal server newpt	已发送报文给Portal服务器newpt
Ver	Portal协议报文的版本号，取值包括： • 1.0：版本 1 • 2.0：版本 2 • 3.0：版本 2
Type	Portal协议报文类型： • REQ_CHALLENGE • ACK_CHALLENGE • REQ_AUTH • ACK_AUTH • REQ_LOGOUT • ACK_LOGOUT • AFF_ACK_AUTH • NTF_LOGOUT • REQ_INFO • ACK_INFO • NTF_USER_DISCOVER • NTF_USER_IP_CHANGE • AFF_NTF_USER_IP_CHANGE • ACK_NTF_LOGOUT • NTF_HEART • NTF_USER_HEART • ACK_NTF_USER_HEART • NTF_CHALLENGE • NTF_USER_NOTIFY

字段	描述
	• AFF_NTF_USER_NOTIFY • REQ_MACBIND_INFO • ACK_MACBIND_INFO • NTF_USER_LOGON • NTF_USER_LOGOUT • REQ_USER_OFFLINE • UNKNOWN
Method	Portal的认证方法： • EAP：EAP 认证方法 • CHAP：CHAP 认证方法 • PAP：PAP 认证方法
SerialNo	Portal报文序列号
ReqID	Portal报文的请求ID
UserIP	Portal用户的IP地址
ErrCode	错误码
AttrNum	Portal报文携带的属性个数

(6) UCM

表111-7 被跟踪详细信息描述表（UCM）

字段	描述
Failed to send *msgtype*.	UCM向PAM发送msgtype消息失败。其中*msgtype*取值包括： • UCM_UIA_PAM_MSG_COA：表示 COA（Change of Authorization）Messages，用于更改用户授权信息 • UCM_UIA_PAM_MSG_DM：表示 DMs（Disconnect Messages），用于强制用户下线

UserID: userid, VASID: *vasid*, Received AAA reply (MsgType: *msgtype*)	UCM收到AAA的回应消息。其中：
	• UserID：表示用户 ID
	• VASID：表示增值业务 ID，即 ITA 业务计费级别或 EDSG 业务 ID
	• MsgType：表示消息类型。取值包括：
	  ○ AUTH_REQ_ACK：认证请求通过
	  ○ AUTH_REQ_REJ：认证请求拒绝
	  ○ AUTH_REQ_CONTINUE：持续认证
	  ○ AUTHOR_REQ_ACK：授权请求通过
	  ○ AUTHOR_REQ_REJ：授权请求拒绝
	  ○ ACCT_START_ACK：计费开始请求通过
	  ○ ACCT_START_REJ：计费开始请求拒绝
	  ○ ACCT_START_BROADCAST_ACK：计费开始请求广播通过
	  ○ ACCT_UPDATE_ACK：计费更新通过

字段	描述
	◦ ACCT_UPDATE_REJ：计费更新拒绝 ◦ ACCT_UPDATE_BROADCAST_ACK：计费更新广播通过 ◦ ACCT_STOP_ACK：计费停止通过 ◦ ACCT_STOP_REJ：计费停止拒绝 ◦ ACCT_STOP_BROADCAST_ACK：计费停止广播通过 ◦ DM_REQ：设备下线请求 ◦ COA_REQ：更改用户业务参数请求 ◦ DOMAIN_CUT：根据 Domain 让用户下线 ◦ GET_DATA：获取数据请求
UserID: *userid*, Sent account start request to AAA	UCM向AAA发计费开始请求
UserID: *userid*, Sent account update request to AAA	UCM向AAA发计费更新请求
UserID: userid, ConnectID: *connectid*, Received msgname from *accessname*.	从*accessname*收到*msgname*消息。其中： • UserID：表示用户 ID • ConnectID：表示 UCM 连接类型对应 ID 值。取值包括： ◦ 0：LAC 端上自动拨号的 L2TP 和 LNS 端上的 L2TP 连接 ◦ 1：DHCP、IPoE 和 ARP 等连接 ◦ 2：DHCPv6、IPoEv6 和 ND 等连接 ◦ 3：PPP、IP6CP 和 ND 连接 • accessname：表示接入方式名称。取值包括： ◦ PPP：表示 PPP 接入 ◦ IPOE4：表示 IPv4 IPoE 接入 ◦ DHCP4：表示 DHCPv4 接入 ◦ IPOE6：表示 IPv6 IPoE 接入 ◦ DHCP6：表示 DHCPv6 接入 ◦ ARP：表示 ARP 接入 ◦ NDRS：表示 NDRS 接入 ◦ NDNS：表示 NDNS 接入 ◦ IPOEWEB：表示 IPoE Web 接入 ◦ L2IFLEASE：表示二层 IPoE 接口专线接入 ◦ L3IFLEASE：表示三层 IPoE 接口专线接入 ◦ L3SUBLEASE：表示三层 IPoE 子网专线接入 ◦ L2VPNLEASE：表示 IPoE L2VPN 专线接入 ◦ PAM：表示 PAM 接入 • msgname：表示消息名称。取值包括： ◦ UCM_UIA_PPP_MSG_AUTH_REQ：PPP 认证请求 ◦ UCM_UIA_PPP_MSG_CONN_REQ：PPP 连接请求 ◦ UCM_UIA_PPP_MSG_CONN-UP_REQ：PPP 连接 UP 请求 ◦ UCM_UIA_PPP_MSG_CONN-DOWN_REQ：PPP 连接 DOWN 请求

字段	描述
	○ UCM_UIA_PPP_MSG_OFFLINE_REQ：PPP 下线请求 ○ UCM_UIA_PPP_MSG_OFFLINE_INF：PPP 下线信息 ○ UCM_UIA_IPOEIP4_MSG_CONN_REQ：IPv4 IPoE 连接请求 ○ UCM_UIA_IPOEIP6_MSG_CONN_REQ：IPv6 IPoE 连接请求 ○ UCM_UIA_IPOEIP6_MGG_CONN_MODIFYUSR_NTF：IPv6 IPoE 修改用户通知 ○ UCM_UIA_DHCP_MSG_CONN_REQ：DHCPv4 连接请求 ○ UCM_UIA_DHCP_MSG_CONN-UP_REQ：DHCPv4 连接 UP 请求 ○ UCM_UIA_DHCP_MSG_RENEW_REQ：DHCPv4 刷新请求 ○ UCM_UIA_DHCP_MSG_CONN-DOWN_REQ：DHCPv4 连接 DOWN 请求 ○ UCM_UIA_DHCP_MSG_DISCONN_INF：DHCPv4 断开连接信息 ○ UCM_UIA_DHCP6_MSG_CONN_REQ：DHCPv6 连接请求 ○ UCM_UIA_DHCP6_MSG_CONN-UP_REQ：DHCPv6 连接 UP 请求 ○ UCM_UIA_DHCP6_MSG_RENEW_REQ：DHCPv6 连接更新请求 ○ UCM_UIA_DHCP6_MSG_CONN-DOWN_REQ：DHCPv6 连接 DOWN 请求 ○ UCM_UIA_DHCP6_MSG_DISCONN_INF：DHCPv6 断开连接信息 ○ UCM_UIA_ARP_MSG_CONN_REQ：ARP 连接请求 ○ UCM_UIA_ARP_MSG_CONN-UP_REQ：ARP 连接 UP 请求 ○ UCM_UIA_ARP_MSG_DTC_TIMEOUT：ARP 探测超时 ○ UCM_UIA_NDRS_MSG_CONN_REQ：NDRS 连接请求 ○ UCM_UIA_NDRS_MSG_CONN-UP_REQ：NDRS 连接 UP 请求 ○ UCM_UIA_NDRS_MSG_MODIFYUSRIP_REQ：NDRS 修改用户 IP 请求 ○ UCM_UIA_NDNSNA_MSG_CONN_REQ：NDNS 连接请求 ○ UCM_UIA_NDNSNA_MSG_CONN-UP_REQ：NDNS 连接 UP 请求 ○ UCM_UIA_ND_MSG_DTC_TIMEOUT：NDNS 探测超时 ○ UCM_UIA_PORTAL_MSG_AUTH_REQ：IPoE Web 认证请求 ○ UCM_UIA_PORTAL_MSG_AUTH_REQ_CONTINUE：IPoE Web 持续认证请求 ○ UCM_UIA_PORTAL_MSG_DISCONN_REQ：IPoE Web 认证关闭连接请求 ○ UCM_UIA_PORTAL_MSG_DISCONN_INF：IPoE Web 认证关闭连接信息 ○ UCM_UIA_PORTAL_MSG_SERVERINFO：IPoE Web 认证服务器信息 ○ UCM_UIA_PORTAL_MSG_ROAM：IPoE Web 用户漫游 ○ UCM_UIA_PORTAL_MSG_MT_ONLINE：IPoE Web 用户上线消息 ○ UCM_UIA_PORTAL_MSG_MT_OFFLINE：IPoE Web 用户下线消息 ○ UCM_UIA_LEASE_MSG_CONN_REQ：IPoE 专线连接请求 ○ UCM_UIA_LEASE_MSG_CONN-UP_REQ：IPoE 专线连接 UP 请求 ○ UCM_UIA_LEASE_MSG_CONDOWN_REQ：IPoE 专线连接 DOWN 请求 ○ UCM_UIA_PAM_MSG_AUTH_REQ：PAM 认证请求 ○ UCM_UIA_PAM_MSG_ACCT_START_REQ：PAM 计费开始请求 ○ UCM_UIA_PAM_MSG_ACCT_UPDATE_REQ：PAM 计费更新请求 ○ UCM_UIA_PAM_MSG_ACCT_STOP_REQ：PAM 计费停止请求 ○ UCM_UIA_PAM_MSG_USER_DELETE：PAM 用户删除

字段	描述
	○ UCM_UIA_PAM_MSG_USER_RECOVER：PAM 用户恢复 ○ UCM_UIA_PAM_MSG_GETDATA_ACK：PAM 获取数据回应 ○ UCM_UIA_PAM_MSG_SMOOTH_USERDELETE：PAM 用户删除
[Adapt State]UserID: *userid*, ConnectID: *connectid*, Received event *event*, current state is *state*.	Adapter状态机，接收到*event*事件，当前状态是*state*。其中： • UserID：表示用户 ID • ConnectID：表示 UCM 连接类型对应 ID 值。取值包括： ○ 0：LAC 端上自动拨号的 L2TP 和 LNS 端上的 L2TP 连接 ○ 1：DHCP、IPoE 和 ARP 等连接 ○ 2：DHCPv6、IPoEv6 和 ND 等连接 ○ 3：PPP、IP6CP 和 ND 连接 • *event*：表示 Adapter 状态机事件。取值包括： ○ ADD：添加 ○ MODIFY：修改信息 ○ DEL：删除 ○ TRAFFIC_DELCOMPLETE：流量删除完成 ○ PROXY_DELCOMPLETE：下接口板删除完成 ○ FWD-DELCOMPLETE：下内核删除完成 ○ FWD-SUCC：下内核成功 ○ FWD-FAIL：下内核失败 ○ PROXY-SUCC：下接口板成功 ○ PROXY-FAIL：下接口板失败 • *state*：表示当前状态。取值包括： ○ INIT：初始化 ○ FWD：下内核 ○ FWD-MODIFY：下内核修改信息 ○ PROXY：下接口板和备用接口板 ○ PROXY-MODIFY：下接口板修改信息 ○ ADDED：添加成功 ○ DELETING：正在删除
[Adapt State]UserID: *userid*, ConnectID: *connectid*, Received *event* event, State changed from *oldstate* to *newstate*	Adapter状态机，接收到*event*事件，状态从*oldstate*切换为*newstate*。其中： • UserID：表示用户 ID • ConnectID：表示 UCM 连接类型对应 ID 值。取值同上一条信息中 ConnectID • *event*：表示 Adapter 状态机事件。取值同上一条信息中 *event* • *oldstate*：表示状态机切换前状态。取值同上一条信息中 *state* • *newstate*：表示状态机切换后状态。取值同上一条信息中 *state*
[Conn state]UserID: *userid*, ConnectID: *connectid*, Received *event* event, Current state is *state*.	连接状态机，收到*event*事件，当前状态是*state*。其中： • UserID：表示用户 ID • ConnectID：表示 UCM 连接类型对应 ID 值。取值包括： ○ 0：LAC 端上自动拨号的 L2TP 和 LNS 端上的 L2TP 连接 ○ 1：DHCP、IPoE 和 ARP 等连接

字段	描述
	○ 2：DHCPv6、IPoEv6 和 ND 等连接 ○ 3：PPP、IP6CP 和 ND 连接 • *event*：表示连接状态机事件。取值包括： ○ USER-AUTH-PASSED：用户认证通过 ○ CONNREQ-PASSED：连接请求通过 ○ ADDR-REQ-ACK：地址请求通过 ○ CONN-UP-WITH-NAT：连接 UP 需要 NAT 事件 ○ CONN-UP-WITHOUT-NAT：连接 UP 不需要 NAT 事件 ○ NAT-REQ-ACK：NAT 请求通过 ○ USER-ADD-ACK：用户添加请求通过 ○ USER-DEL-ACK：用户删除请求通过 ○ CLOSE：连接关闭 ○ DOWN ：连接断开 ○ EXTRA-CONNREQ：附加连接请求 ○ EXTRA-CONN-UP：附加连接 UP 请求 ○ RENEW：更新连接信息（租约更新等） • *state*：表示当前状态。取值包括： ○ INIT：初始化 ○ ADDR-REQ-SENT：地址请求发送 ○ AUTHED：已认证 ○ NAT-REQ-SENT：NAT 请求发送 ○ USER-ADDING：正在添加用户 ○ OPEN：连接建立 ○ DELETING：正在删除 ○ DELETED：已经删除
[Conn State]UserID: *userid*, Received *event* event, State changed from *oldstate* to *newstate*.	连接状态机，收到*event*事件，状态从*oldstate*切换到*newstate*。其中： • UserID：表示用户 ID • *event*：表示连接状态机事件。取值同上一条信息中 *event* • *oldstate*：表示状态机切换前状态。取值同上一条信息中 *state* • *newstate*：表示状态机切换后状态。取值同上一条信息中 *state*
[LOGOUT State]UserID: *userid*, Received *event* event, Current state is *state*.	• LOGOUT 状态机，收到 *event* 事件，当前状态为 *state*。其中： • UserID：表示用户 ID • *event*：表示 LOGOUT 状态机事件。取值包括： ○ AUTHREQ：认证请求 ○ AUTHSUCC：认证成功 ○ USER_MODIFYACK：用户修改成功 • *state*：表示当前状态。取值包括： ○ INIT：初始化 ○ AUTHING：正在认证 ○ USER_UPDATE：用户更新

字段	描述
[LOGOUT State]UserID: *userid*, Received *event* event, State changed from *oldstate* to *newstate*.	LOGOUT状态机，收到*event*事件，状态从*oldstate*切换为*newstate*。其中： • UserID：表示用户 ID • *event*：表示 LOGOUT 状态机事件。取值同上一条信息中 *event* • *oldstate*：表示状态机切换前状态。取值同上一条信息中 *state* • *newstate*：表示状态机切换后状态。取值同上一条信息中 *state*

[Reauth State]UserID: *userid*, Received *event* event, Current state is *state*.	• 重认证状态机，收到 *event* 事件，当前状态为 *state*。其中：
	• UserID：表示用户 ID
	• *event*：表示重认证状态机事件。取值包括：
	  ○ AUTHREQ：认证请求
	  ○ AUTHSUCC：认证成功
	  ○ AUTHCONTINUE：用户持续认证
	  ○ AUTH-FAIL：认证失败
	  ○ USER_MODIFYACK：用户业务参数修改成功
	  ○ USER_MODIFYREJ：用户业务参数修改拒绝
	  ○ WEB_AUTHACK_RESP：Web 认证 ACK 回应
	  ○ MACAUTH_ACK：MAC 认证成功
	  ○ DOWN：UCM 收到用户的连接断开请求
	• *state*：表示当前状态。取值包括：
	  ○ INIT：初始化
	  ○ AUTHING：正在认证
	  ○ USER_UPDATE：用户数据更新
	  ○ WAIT_WEBRESP_ACK：等待 Web 回应 ACK
	  ○ WAIT_MACAUTH_ACK：等待 MAC 认证 ACK

[Reauth State]UserID: *userid*, Received *event* event, State changed from *oldstate* to *newstate*.	重认证状态机，收到*event*事件，状态从*oldstate*切换到*newstate*。其中： • UserID：表示用户 ID • *event*：表示重认证状态机事件。取值同上一条信息中 *event* • *oldstate*：表示状态机切换前状态。取值同上一条信息中 *state* • *newstate*：表示状态机切换后状态。取值同上一条信息中 *state*

[Shell Phase]UserID: *userid*, ConnectID: *connectid*, Received event *event*, Current phase is *phase*.	Shell状态机，收到*event*事件，当前状态为*phase*。其中：
	• UserID：表示用户 ID
	• ConnectID：表示 UCM 连接类型对应 ID 值。取值包括：
	  ○ 0：LAC 端上自动拨号的 L2TP 和 LNS 端上的 L2TP 连接
	  ○ 1：DHCP、IPoE 和 ARP 等连接
	  ○ 2：DHCPv6、IPoEv6 和 ND 等连接
	  ○ 3：PPP、IP6CP 和 ND 连接
	• *event*：表示 Shell 状态机事件。取值包括：
	  ○ AUTH-REQ：认证请求
	  ○ CONN-REQ：UCM 收到接入的连接请求
	  ○ CONN-UP：连接 UP 请求
	  ○ CONN-DOWN：断开连接请求

字段	描述
	○ RENEW-REQ：更新连接请求（如租约等） ○ MODIFY-USERIP：修改用户 IP ○ DISCONN-REQ：断开连接请求 ○ MPBIND-REQ：MP 绑定请求 ○ ACCT-START-REQ：计费开始请求 ○ ACCT-UPDATE-REQ：计费更新请求 ○ ACCT-STOP-REQ：计费停止请求 ○ RECOVER-REQ：恢复请求 ○ GETDATA-ACK：处理 GetData 回应 ○ WEB-AUTHREQ：Web 认证请求 ○ WEB-AUTHACK-RESPONSE：Web 认证 ACK 回应 ○ DOWN-REQ：下线请求 ○ STOP-MT：停止 MAC 无感知 ○ MAC-AUTH：MAC 认证 ○ TERMINATE：下线用户 ○ GROUPID-CHG：组 ID 修改 ○ AUTH-SUCC：认证成功 ○ AUTH-FAIL：认证失败 ○ AUTH-CONTINUE：用户持续认证 ○ ACC-START-SUCC：开始计费成功 ○ ACC-START-FAIL：开始计费失败 ○ ACC-UPDATE-SUCC：计费更新成功 ○ ACC-STOP-FAIL：计费停止失败 ○ ACCESS-MSG-PASS：接入消息通过 ○ MPBIND-SUCCESS：MP 绑定成功 ○ MPBIND-FAILURE：MP 绑定失败 ○ PAM-AUTH-SUCC：PAM 认证成功 ○ PAM-AUTH-FAIL：PAM 认证失败 ○ PAM-AUTH-CONTINUE：PAM 持续认证 ○ PAM-ACCT-START-SUCC：PAM 计费开始成功 ○ PAM-ACCT-START-FAIL：PAM 计费开始失败 ○ PAM-ACCT-UPDATE-SUCC：PAM 计费更新成功 ○ PAM-ACCT-UPDATE-FAIL：PAM 计费更新失败 ○ PAM-ACCT-STOP-SUCC：PAM 计费停止成功 ○ PAM-ACCT-STOP-FAIL：PAM 计费停止失败 ○ COA：修改认证信息 ○ MODIFY-ACK：修改成功 ○ NEGSLOTCHG：用户协商板切换 ○ TERMINATE：下线 ○ ADDRREQ-ACK：地址请求成功 ○ ADDRREQ-REJ：地址请求失败 ○ NATREQ-ACK：NAT 事件请求成功

字段	描述
	○ NATREQ-REJ：NAT 事件请求失败 ○ FWD-SYNC-SUCC：添加转发表项成功 ○ FWD-SYNC-FAIL：添加转发表项失败 ○ PROXY-SYNC-SUCC：通知接口板添加转发表项成功 ○ PROXY-SYNC-FAIL：通知接口板添加转发表项失败 ○ FWD-SYNC-DELCOMPLETE：内核删除用户完成 ○ PROXY-SYNC-DELCOMPLETE：接口板删除用户完成 ○ AUTH-PASS：认证完成 ○ ADAPT-ADD-ACK：用户添加成功 ○ ADAPT-ADD-REJ：用户添加拒绝 ○ ADAPT-MODIFY-ACK：用户修改成功 ○ ADAPT-MODIFY-REJ：用户修改拒绝 ○ UP：用户上线 ○ ADAPT-DEL-ACK：用户删除成功 ○ DEL-COMPLETE：删除完成 ○ REAUTH-AUTH-PASS：重认证通过 ○ REAUTH-AUTH-CONTINUE：重认证持续认证 ○ REAUTH-AUTH-FAIL：重认证失败 ○ REAUTH-MACAUTH-SUCC：重认证成功 ○ REAUTH-COMPLETE：重认证完成 ○ REAUTH-DOWN：重认证停止 ○ WEB-CLOSE：Web 连接断开请求 ○ LOGOUT-AUTH-PASS：IPoE Web 用户从 Web 认证阶段退回到认证前域阶段时，认证成功 ○ LOGOUT-COMPLETE：IPoE Web 用户在 Web 认证阶段上线成功 ○ USER-MODIFY-ACK：用户修改成功 ○ OPEN：连接完成 • *phase*：表示当前状态。取值包括： ○ INITIAL：初始阶段 ○ AUTHENTICATION：认证阶段（认证阶段向 AAA 请求认证，还没收到回应） ○ AUTHED：认证完成阶段（收到 AAA 认证回应通过消息） ○ NETWORK：网络协商阶段（已经申请地址且开始下内核和接口板及备用接口板） ○ ONLINE：用户上线完成，用户在线 ○ TERMINATE：用户下线 ○ REAUTH：重认证阶段（IPoE Web 用户在 Web 认证阶段进行认证） ○ LOGOUT：退出（IPoE Web 用户从 Web 认证阶段退回到认证前域阶段）
[Shell Phase]UserID: *userid*, ConnectID: *connectid*, Received *event* event, Phase changed from *oldphase* to *newphase*.	Shell状态机，收到*event*事件，状态从*oldphase*切换到*newphase*。其中： • UserID：表示用户 ID • ConnectID：表示 UCM 连接类型对应 ID 值。取值同上一条信息中 ConnectID • *event*：表示 Shell 状态机事件。取值同上一条信息中 *event* • *oldphase*：表示状态机切换前状态。取值同上一条信息中 *phase*

字段	描述
	• *newphase*：表示状态机切换后状态。取值同上一条信息中 *phase*

[User State]UserID: *userid*, Received *event* event, Current state is *state*.	用户状态机，收到*event*事件，当前状态为*state*。其中：
	• UserID：表示用户 ID
	• *event*：表示用户状态机事件。取值包括：
	  ○ AUTHREQ：UCM 收到接入的认证请求
	  ○ AUTHSUCC：UCM 收到 AAA 的认证成功事件
	  ○ AUTHSUCC-ADMIN：管理用户认证成功
	  ○ AUTH-FAIL：UCM 收到 AAA 的认证失败事件
	  ○ AUTH-CONTINUE：UCM 收到 AAA 的用户持续认证事件
	  ○ CONNREQ：UCM 收到接入的连接请求
	  ○ CONN-UP：UCM 收到接入的连接完成
	  ○ USERADD-ACK：用户添加成功
	  ○ USERDEL-ACK：用户删除成功
	  ○ CLOSE：UCM 内部原因引起的下线
	  ○ DOWN：接入发起的下线
	  ○ MPBINDREQ：MP 绑定请求
	  ○ MPBINDSUCCESS：MP 绑定成功
	  ○ MPBINDFAILURE：MP 绑定失败
	  ○ PAM_AUTHREQ：PAM 认证请求
	  ○ PAM_ACCTSTARTREQ：PAM 计费开始请求
	  ○ PAM_ACCTUPDATEREQ：PAM 计费更新请求
	  ○ PAM_ACCTSTOPREQ：PAM 计费停止请求
	  ○ PAM_AUTHSUCCESS：PAM 认证成功
	  ○ PAM_AUTHFAILURE：PAM 认证失败
	  ○ PAM_AUTHCONTINUE：PAM 用户持续认证
	  ○ PAM_USERDELETE：PAM 用户删除
	  ○ REAUTH：IPoE Web 前域用户重认证
	  ○ REAUTH_SUCC：重认证成功
	  ○ REAUTH_FAIL：重认证失败
	  ○ LOGOUT：IPoE Web 退出后域
	  ○ LOGOUT_SUCC：IPoE Web 退出后域成功
	  ○ MODIFY：用户修改
	  ○ MODIFY-ACK：用户修改成功
	• *state*：表示当前状态。取值包括：
	  ○ INIT：初始化
	  ○ AUTHING：正在认证
	  ○ ALLOC：认证失败和用户下线的中间状态（只有 PPP 有这个状态）
	  ○ AUTHED：已认证
	  ○ USER-ADDING：下内核和通知备用接口板，等待结果的中间状态
	  ○ UP：上线成功
	  ○ DELETING：正在删除

字段	描述
	○ DELETED：删除完成 ○ BINDING：绑定阶段（PPP MP 才有） ○ REAUTH：重认证阶段（IPoE Web 用户在 Web 认证阶段进行认证） ○ LOGOUT：退出（IPoE Web 用户从 Web 认证阶段退回到认证前域阶段） ○ MODIFY：更新用户信息（COA）
[User State]UserID: *userid*, Received *event* event, State changed from *oldstate* to *newstate*	用户状态机，收到*event*事件，状态从*oldstate*状态切换到*newstate*。其中： • UserID：表示用户 ID • *event*：表示用户状态机事件。取值同上一条信息中 *event* • *oldstate*：表示状态机切换前状态。取值同上一条信息中 *state* • *newstate*：表示状态机切换后状态。取值同上一条信息中 *state*
UserID *userid* group ID changed.	用户的用户组ID发生改变
UserID: *userid*, Received assigned IP address *ipaddr* from AM.	用户收到AM分配的IP地址是*ipaddr*
UserID *userid* will be terminated, the cause is *cause*.	用户将被终止连接，原因是*cause*.
UserID: *userid*, Sent authentication request to AAA, the access user type is *type*.	UCM向AAA发送认证请求。其中： • UserID：表示用户 ID • type：表示用户接入类型。取值包括： ○ PPPoE：PPP over Ethernet 用户 ○ PPPoA：PPP over ATM 用户 ○ PPPoFR：PPP over FR 用户 ○ PPPoPhy：物理链路直接承载 PPP 用户 ○ VPPP：LAC 端上自动拨号的 L2TP 用户 ○ LNS：LNS 端上 L2TP 用户 ○ MAC auth：MAC 地址认证用户 ○ Dot1x：802.1X 用户 ○ Web auth：Web 认证用户 ○ Telnet：Telnet 用户 ○ FTP：FTP 用户 ○ Terminal：从 Console 口、AUC 口、Asyn 口登录用户 ○ SSH：SSH 用户 ○ Portal：Portal 用户 ○ PAD：PAD 用户 ○ Command：命令行授权和计费用户 ○ Super：切换用户角色的用户 ○ IPoE L2VPN leased：IPoE L2VPN 专线用户 ○ NETCONF SOAP HTTP：HTTP web 用户 ○ NETCONF RESTful HTTP：NETCONF over SOAP over HTTP 用户

字段	描述
	○ HTTP Web：HTTP web 用户 ○ NETCONF SOAP HTTPS：NETCONF over SOAP over HTTPS 用户 ○ NETCONF RESTful HTTPS：NETCONF over RESTful over HTTPS 用户 ○ HTTPS Web：HTTPS web 用户 ○ L2 IPoE dynamic：二层 IPoE 动态接入用户 ○ L2 IPoE static：二层 IPoE 静态接入用户 ○ L2 IPoE interface leased：二层 IPoE 接口专线用户 ○ L2 IPoE leased subuser：二层专线子用户 ○ L3 IPoE dynamic：三层 IPoE 动态接入用户 ○ L3 IPoE static：三层 IPoE 静态用户 ○ L3 IPoE interface leased：三层 IPoE 接口专线用户 ○ L3 IPoE subnet leased：三层子网专线用户 ○ IKE：IKE 用户 ○ SSLVPN：SSL VPN 用户 ○ DVPN：DVPN 用户
UserID: *userid*, session key: *key*, New SocketPAM (*usertype*) user is created.	• 新创建 SocketPAM 类型的用户。其中： • UserID：表示用户 ID • session key：表示 PAM 接入用户索引 • *usertype*：表示用户类型。取值包括： ○ Telnet：Telnet 用户 ○ FTP：FTP 用户 ○ Terminal：从 Console 口、AUC 口、Asyn 口登录用户 ○ SSH：SSH 用户 ○ PAD：PAD 用户 ○ Command：命令行授权和计费用户 ○ Super：切换用户角色的用户
UserID: *userid*, session key: *key*, New SessionPAM (*usertype*) user is created.	• 新创建 SessionPAM 类型的用户。其中： • UserID：表示用户 ID • session key：表示 PAM 接入用户索引 • *usertype*：表示用户类型。取值包括： ○ NETCONF SOAP HTTPS：NETCONF over SOAP over HTTPS 用户 ○ NETCONF RESTful HTTP：NETCONF over SOAP over HTTP 用户 ○ HTTP Web：HTTP web 用户 ○ NETCONF SOAP HTTPS：NETCONF over SOAP over HTTPS 用户 ○ NETCONF RESTful HTTPS：NETCONF over RESTful over HTTPS 用户 ○ HTTPS Web：HTTPS web 用户 ○ IKE：IKE 用户 ○ SSLVPN：SSL VPN 用户 ○ DVPN：DVPN 用户
UserID: *userid*, session Key: *key*, New Portal	新创建Portal用户。其中：

字段	描述
user is created	• UserID：表示用户 ID • session key：表示 PAM 接入用户索引

UserID: *userid*, ConnectID: *connectid*, New PPP user is created	新创建PPP用户。其中：
	• UserID：表示用户 ID
	• ConnectID：表示 UCM 连接类型对应 ID 值。取值包括：
	  ○ 0：LAC 端上自动拨号的 L2TP 和 LNS 端上的 L2TP 连接
	  ○ 1：DHCP、IPoE 和 ARP 等连接
	  ○ 2：DHCPv6、IPoEv6 和 ND 等连接
	  ○ 3：PPP、IP6CP 和 ND 连接

UserID: *userid*, ConnectID: *connectid*, New IPoE4 user is created	新创建IPv4 IPoE用户。其中：
	• UserID：表示用户 ID
	• ConnectID：表示 UCM 连接类型对应 ID 值。取值包括：
	  ○ 0：LAC 端上自动拨号的 L2TP 和 LNS 端上的 L2TP 连接
	  ○ 1：DHCP、IPoE 和 ARP 等连接
	  ○ 2：DHCPv6、IPoEv6 和 ND 等连接
	  ○ 3：PPP、IP6CP 和 ND 连接

UserID: *userid*, ConnectID: *connectid*, New IPoE6 user is created.	新创建IPv6 IPoE用户。其中：
	• UserID：表示用户 ID
	• ConnectID：表示 UCM 连接类型对应 ID 值。取值包括：
	  ○ 0：LAC 端上自动拨号的 L2TP 和 LNS 端上的 L2TP 连接
	  ○ 1：DHCP、IPoE 和 ARP 等连接
	  ○ 2：DHCPv6、IPoEv6 和 ND 等连接
	  ○ 3：PPP、IP6CP 和 ND 连接

UserID: *userid*, ConnectID: *connectid*, New leased user is created.	新创建IPoE专线用户。其中：
	• UserID：表示用户 ID
	• ConnectID：表示 UCM 连接类型对应 ID 值。取值包括：
	  ○ 0：LAC 端上自动拨号的 L2TP 和 LNS 端上的 L2TP 连接
	  ○ 1：DHCP、IPoE 和 ARP 等连接
	  ○ 2：DHCPv6、IPoEv6 和 ND 等连接
	  ○ 3：PPP、IP6CP 和 ND 连接

(7) AAA

表111-8 被跟踪详细信息描述表（AAA）

字段	描述
Domain *domain-name* rejected the user.	域*domain-name*拒绝此用户接入
Domain *domain-name* is in blocked state.	域*domain-name*的状态为block
The user failed to access domain *domain-name* because the maximum number of users already reached.	*domain-name*域内允许接入的用户数已达到上限，此用户不能接入

字段	描述
Received an authentication request.	AAA收到UCM的用户认证请求消息
Received an accounting-start request.	AAA收到UCM的用户开始计费请求消息
Received an accounting-update request.	AAA收到UCM的用户实时计费请求消息
Received an accounting-stop request.	AAA收到UCM的用户结束计费请求消息
Received a get-data reply.	AAA收到UCM的数据获取响应消息
Received an LDAP authentication response.	AAA收到LDAP认证应答报文
Received an LDAP authorization response.	AAA收到LDAP授权应答报文
RADIUS authentication: Request initiated.	RADIUS认证：初始化请求报文
RADIUS accounting start: Request initiated.	RADIUS开始计费：初始化请求报文
RADIUS accounting update: Request initiated.	RADIUS实时计费：初始化请求报文
RADIUS accounting stop: Request initiated.	RADIUS结束计费：初始化请求报文
RADIUS accounting start: Failed. Reason: *reason*.	RADIUS开始计费：失败 失败原因是*reason*
RADIUS accounting update: Failed. Reason: *reason*.	RADIUS实时计费：失败 失败原因是*reason*
RADIUS accounting stop: Failed. Reason: *reason*.	RADIUS结束计费：失败 失败原因是*reason*
RADIUS authentication: Succeeded.	RADIUS认证：成功
RADIUS accounting start: Succeeded.	RADIUS开始计费：成功
RADIUS accounting update: Succeeded.	RADIUS实时计费：成功
RADIUS accounting stop: Succeeded.	RADIUS结束计费：成功
RADIUS authentication: Failed. Reason: *reason*.	RADIUS认证：失败 失败原因是*reason*，包括以下取值： • Server rejected：服务器拒绝
RADIUS authorization: Failed. Reason: *reason*.	RADIUS授权：失败 失败原因是*reason*，包括以下取值： • Data error：授权属性数据错误
TACACS authentication: Request initiated.	TACACS认证：初始化请求报文
TACACS continue authentication: Request initiated.	TACACS获取数据：初始化请求报文
TACACS accounting start: Request initiated.	TACACS开始计费：初始化请求报文
TACACS accounting update: Request initiated.	TACACS实时计费：初始化请求报文
TACACS accounting stop: Request initiated.	TACACS结束计费：初始化请求报文
TACACS authentication: Failed. Reason: *reason*.	TACACS认证：失败 失败原因是*reason*

字段	描述
TACACS continue authentication: Failed. Reason: *reason*.	TACACS获取数据：失败 失败原因是*reason*
TACACS authorization: Failed. Reason: *reason*.	TACACS授权：失败 失败原因是*reason*
TACACS accounting start: Failed. Reason: *reason*.	TACACS开始计费：失败 失败原因是*reason*
TACACS accounting update: Failed. Reason: *reason*.	TACACS实时计费：失败 失败原因是*reason*
TACACS accounting stop: Failed. Reason: *reason*.	TACACS结束计费：失败 失败原因是*reason*
TACACS authentication: Succeeded.	TACACS认证：成功
TACACS continue authentication: Succeeded.	TACACS获取数据：成功
TACACS accounting start: Succeeded.	TACACS开始计费：成功
TACACS accounting update: Succeeded.	TACACS实时计费：成功
TACACS accounting stop: Succeeded.	TACACS结束计费：成功

(8) DHCP

表111-9 被跟踪详细信息描述表（DHCP）

字段	描述
DHCPACC received a message *type*, DHCPACCIndex *index*, state *state*	DHCP接入模块收到UCM发送的DHCP客户端消息*type*，DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *type*取值包括： • UCM_UIA_DHCP_MSG_CONN_REQ_ACK：建立连接成功 • UCM_UIA_DHCP_MSG_CONN_REQ_REJ：拒绝建立连接 • UCM_UIA_DHCP_MSG_CONNUP_REQ_ACK：DHCP 客户端上线请求成功 • UCM_UIA_DHCP_MSG_CONNUP_REQ_REJ：拒绝 DHCP 客户端的上线请求 • UCM_UIA_DHCP_MSG_DISCONN_INF：用户下线成功 *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：DHCP 接入模块等待 UCM 回应建立连接请求消息 • DHCPACC_WAIT_UCM_UP_ACK：DHCP 接入模块等待 UCM 回应用户上线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：DHCP 接入模块等待 UCM 回应用户下线请求

字段	描述
DHCPACC sent a message *type*, DHCPACCIndex *index*, state *state*.	DHCP接入模块向UCM发送DHCP客户端消息*type*，DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *type*取值包括： • UCM_UIA_DHCP_MSG_CONNUP_REQ：DHCP客户端上线 • UCM_UIA_DHCP_MSG_CONNDOWN_REQ：DHCP 客户端下线 *state*的取值包括： • DHCPACC_WAIT_SERVER_ACK：等待 DHCP 服务器回应 DHCP-ACK 报文 • DHCPACC_WORKING：DHCP 客户端上线成功
DHCPACC would change to state *after-state*, DHCPACCIndex *index*, current state *before-state*.	DHCP接入模块的状态将要切换为*after-state*，DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*before-state* *after-state*和*before-state*的取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求确定消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUEST 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC sent a DHCP-DISCOVER packet to AM. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*.	DHCP接入模块将DHCP-DISCOVER报文转发给AM模块。DHCP-DISCOVER报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文

字段	描述
	• DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC received a DHCP-OFFER packet from AM. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*.	DHCP接入模块收到AM模块应答的DHCP-OFFER报文。DHCP-OFFER报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC received a DHCP-NAK packet from AM. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*.	DHCP接入模块收到AM模块发送的DHCP-NAK报文。DHCP-NAK报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求

字段	描述
	• DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC sent a DHCP-OFFER packet to client. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*	DHCP接入模块将DHCP-OFFER报文转发给DHCP客户端。DHCP-OFFER报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 DHCP 服务器应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC sent a DHCP-NAK packet to client. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*	DHCP接入模块将DHCP-NAK报文转发给DHCP客户端。DHCP-NAK报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模

字段	描述
	块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC received a DHCP-REQUEST packet from client. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*	DHCP接入模块收到DHCP客户端发送的DHCP-REQUEST报文。DHCP-REQUEST报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC sent a DHCP-REQUEST packet to AM. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*	DHCP接入模块将DHCP-REQUEST报文转发给AM模块。DHCP-REQUEST报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM

字段	描述
	应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC receive a DHCP-ACK packet from AM. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*.	DHCP接入模块收到AM模块发送的DHCP-ACK报文。DHCP-REQUEST报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC sent a DHCP-ACK packet to client. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*	DHCP接入模块将DHCP-ACK报文转发给DHCP客户端。DHCP-ACK报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM

字段	描述
	模块应答 DHCP-RENEW 报文
DHCPACC received a DHCP-REQUEST packet from client. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*.	DHCP接入模块收到DHCP客户端发送的DHCP-REQUEST报文。DHCP-REQUEST报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC sent a DHCP-REQUEST packet to AM. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*.	DHCP接入模块将DHCP-REQUEST报文转发给AM模块。DHCP-REQUEST报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文

字段	描述
DHCPACC received a DHCP-ACK packet from AM. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*.	DHCP接入模块收到AM发送的DHCP-ACK报文。 DHCP-ACK报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC sent a DHCP-ACK packet to CLIENT. Giaddr *giaddr*, Yiaddr *yiaddr*, DHCPACCIndex *index*, state *state*.	DHCP接入模块将DHCP-ACK报文转发给DHCP客户端。 DHCP-ACK报文中的Giaddr字段为*giaddr*，Yiaddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCP客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 DHCP-OFFER 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCP 客户端发送 DHCP-REQUSET 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 DHCP-ACK 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCP 客户端上线请求 • DHCPACC_WORKING：DHCP 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCP 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCP 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 DHCP-RENEW 报文
DHCPACC sent a solicit packet to AM.	DHCPv6接入模块将Solicit报文转发给AM模块，Solicit报文中IAAddr字段为*IAAddr*。DHCPv6客户端的本地索引为

字段	描述
IAAddr *IAAddr*, DHCPACCIndex *index*, state *state*.	*index*，DHCPv6客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 Advertise 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCPv6 客户端发送 Request 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 Reply 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCPv6 客户端上线请求 • DHCPACC_WORKING：DHCPv6 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCPv6 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCPv6 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 Renew 报文
DHCPACC received an advertise packet from AM. IAAddr *IAAddr*, DHCPACCIndex *index*, state *state*.	DHCPv6接入模块收到AM发送的Advertise报文，Advertise报文中的IAAddr字段为*yiaddr*。DHCP客户端的本地索引为*index*，DHCPv6客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 Advertise 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCPv6 客户端发送 Request 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 Reply 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCPv6 客户端上线请求 • DHCPACC_WORKING：DHCPv6 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCPv6 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCPv6 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 Renew 报文
DHCPACC sent a advertise packet to client. IAAddr *IAAddr*, DHCPACCIndex *index*, state *state*.	DHCPv6接入模块将Advertise报文转发给DHCPv6客户端，Advertise报文中的IAAddr字段为*IAAddr*。DHCPv6客户端的本地索引为*index*，DHCPv6客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM

字段	描述
	应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 Advertise 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCPv6 客户端发送 Request 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 Reply 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCPv6 客户端上线请求 • DHCPACC_WORKING：DHCPv6 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCPv6 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCPv6 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 Renew 报文
DHCPACC received a reply packet from AM. IAAddr *IAAddr*, DHCPACCIndex *index*, state *state*.	DHCPv6接入模块收到AM模块发送的Reply报文，Reply报文中的IAAddr字段为*IAAddr*。DHCPv6客户端的本地索引为*index*，DHCPv6客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 Advertise 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCPv6 客户端发送 Request 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 Reply 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCPv6 客户端上线请求 • DHCPACC_WORKING：DHCPv6 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCPv6 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCPv6 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 Renew 报文
DHCPACC sent a reply packet to client. IAAddr *IAAddr*, DHCPACCIndex *index*, state *state*.	DHCPv6接入模块将Reply报文转发给DHCP客户端，Reply报文中的IAAddr字段为*IAAddr*。DHCPv6客户端的本地索引为*index*，DHCPv6客户端当前的状态为*state* *state*取值包括： • DHCPACC_WAIT_UCM_REQ_ACK：等待 UCM 应答建立连接请求消息 • DHCPACC_WAIT_AM_OFFER：等待 AM 模块应答 Advertise 报文 • DHCPACC_WAIT_CLIENT_REQ：等待 DHCPv6

字段	描述
	客户端发送 Request 报文 • DHCPACC_WAIT_AM_ACK：等待 AM 模块应答 Reply 报文 • DHCPACC_WAIT_UCM_UP_ACK：等待 UCM 应答 DHCPv6 客户端上线请求 • DHCPACC_WORKING：DHCPv6 客户端上线成功 • DHCPACC_WAIT_AM_DOWN_ACK：等待 AM 模块应答 DHCPv6 客户端下线请求 • DHCPACC_WAIT_UCM_DOWN_ACK：等待 UCM 应答 DHCPv6 客户端下线请求 • DHCPACC_RENEW_WAIT_SERACK：等待 AM 模块应答 Renew 报文

(9) ARP

表111-10 被跟踪详细信息描述表（ARP）

字段	描述
Add user	UCM通知ARP添加用户
Modify user by UID *uid*	根据UID修改ARP用户的会话参数，UID为*uid*
Modify user	修改ARP用户的会话参数
Delete user	UCM通知ARP删除用户
Receive a connection ACK message from UCM	ARP收到UCM发送的连接确认消息
Receive a connection reject message from UCM	ARP收到UCM发送的连接拒绝消息
Work slot has been changed to the local slot, start ARP user detection through	发起ARP用户在线探测的板切换至本板，本板开始ARP用户在线探测
Work slot has been changed to slot *slot-number*, stop ARPuser detection	发起ARP用户在线探测的板切换至板*slot-number*，本板停止ARP用户在线探测
Receive an ARP *type* packet: DstIP: *dst-ip*, DstMAC: *dst-mac*, SrcIP: *src-ip*, SrcMAC: *src-mac*	收到ARP报文，报文类型为*type*，目的IP地址为*dst-ip*，目的MAC地址为*dst-mac*，发送端IP地址为*src-ip*，发送端MAC地址为*src-mac*
Send an ARP reply to user	向用户发送一个ARP应答报文
[DetectTimer] Create ARP user detection timer	创建ARP用户在线探测定时器
[DetectTimer] ARP user detection timer timed out	ARP用户在线探测定时器超时
[DetectTimer] ARP request successfully sent	在ARP用户在线探测过程中，发送ARP请求报文成功
[DetectTimer] User detection attempts reached. Send cut message to UCM	ARP用户在线探测次数达到上限，向UCM发送用户下线请求
[DetectTimer] Set ARP user detection flag	设置ARP用户在线探测的标记位
[DetectTimer] The detection configuration has been changed. Ifindex: *ifindex*, Retries: *retries*, Interval: *interval*	ARP用户在线探测配置发生变化，发起探测的接口为*ifindex*，探测失败后允许重复尝试的最大次数为*retries*，探测的时间间隔为*interval*秒

(10) ND

表111-11 被跟踪详细信息描述表（ND）

字段	描述
Add user with IPv6 prefix *prefix*	UCM通知ND添加用户，UCM给ND用户分配IPv6前缀*prefix*
Modify user by UID *uid*	根据UID修改ND用户的会话参数，UID为*uid*
Modify user	修改ND用户的会话参数
Delete user	UCM通知ND删除用户
Receive a connection ACK message from UCM	ND收到UCM发送的连接确认消息
Receive a connection reject message from UCM	ND收到UCM发送的连接拒绝消息
Forbid to renew link-local address	ND禁止用户更新其Linklocal地址
Work slot has been changed to the local slot, start ND user detection	ND用户所在端口切换至本板，且需要开始ND用户在线探测
Work slot has been changed to slot *slot-number*, stop ND user detection	ND用户所在端口切换至板*slot_number*，同时停止本板的ND用户在线探测
Send an RA message. User MAC: *mac_address,* IPv6 prefix: *prefix*	发送RA报文，ND用户MAC地址为*mac_address*，分配给ND用户的IPv6前缀是*prefix*
[DetectTimer] Create ND user detection timer	创建ND用户在线探测定时器
[DetectTimer] ND user detection timer timed out	ND用户在线探测定时器超时
[DetectTimer] NS message successfully sent	在ND用户在线探测过程中，发送NS请求报文成功
[DetectTimer] User detection attempts reached. Send cut message to UCM	ND用户在线探测次数达到上限，向UCM发送用户下线请求
[DetectTimer] Set ND user detection flag	设置ND用户在线探测的标记位
[DetectTimer] The detection configuration has been changed. Ifindex: *ifindex*, Retries: *retries*, Interval: *interval*	ND用户在线探测配置发生变化，接口索引为*ifindex*，探测失败后允许重复尝试的最大次数为*retries*，探测时间间隔为*interval*
[DetectTimer] Invalid user IPv6 address. Detection failed	用户IPv6地址无效，ND用户在线探测失败

(11) IGMP

表111-12 被跟踪详细信息描述表（IGMP）

字段	描述
Multicast user comes online.	IGMP收到UCM的组播用户上线报文
Multicast user goes offline.	IGMP收到UCM的组播用户下线报文
Multicast authentication information change.	组播认证信息发生变化

(12) MLD

表111-13 被跟踪详细信息描述表（MLD）

字段	描述
Multicast user comes online.	MLD收到UCM的组播用户上线报文
Multicast user goes offline.	MLD收到UCM的组播用户下线报文
Multicast authentication information change.	组播认证信息发生变化

111.3 USER_UPPER_THRESHOLD

日志内容	形式一： The user number on slot [INT32] is above the upper warning threshold (UpperThreshold=[INT32]). 形式二： The user number on chassis [INT32] slot [INT32] is above the upper warning threshold (UpperThreshold=[INT32]).
参数解释	形式一： $1：slot编号 $2：接入用户数告警阈值 形式二： $1：chassis编号 $2：slot编号 $3：接入用户数告警阈值
日志等级	4
举例	USER/4/USER_UPPER_THRESHOLD: The user number on slot 1 is above the upper warning threshold (UpperThreshold=20).
日志说明	指定slot上接入用户数超过上限阈值
处理建议	确认是否存在大量非法IPoE和PPPoE用户上线

112 VLAN

本节介绍接口 VLAN 模块输出的日志信息。

112.1 VLAN_FAILED

日志内容	Failed to add interface [STRING] to the default VLAN.
参数解释	$1：接口名称
日志等级	4
举例	VLAN/4/VLAN_FAILED: Failed to add interface S-Channel4/2/0/19:100 to the default VLAN.
日志说明	在硬件资源不足的时候创建一个S-Channel接口，此S-Channel接口不能加入到缺省VLAN
处理建议	无

112.2 VLAN_VLANMAPPING_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
参数解释	$1：接口名称
日志等级	4
举例	VLAN/4/VLAN_VLANMAPPING_FAILED: The configuration failed because of resource insufficiency or conflicts on Ethernet1/2/0/1.
日志说明	因本接口硬件资源不足或者接口加入或离开二层聚合组，所以部分或全部VLAN映射配置丢失
处理建议	无

112.3 VLAN_VLANTRANSPARENT_FAILED

日志内容	The configuration failed because of resource insufficiency or conflicts on [STRING].
参数解释	$1：接口名称
日志等级	4
举例	VLAN/4/VLAN_VLANTRANSPARENT_FAILED: The configuration failed because of resource insufficiency or conflicts on Ethernet1/2/0/1.
日志说明	因本接口硬件资源不足或者接口加入或离开二层聚合组，所以部分或全部VLAN透传配置丢失
处理建议	无

113 VRRP

本节介绍 VRRP 模块输出的日志信息。

113.1 VRRP_STATUS_CHANGE

日志内容	The status of [STRING] virtual router [UINT32] (configured on [STRING]) changed from [STRING] to [STRING]: [STRING].
参数解释	$1：VRRP协议版本 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：先前状态 $5：当前状态 $6：状态变化原因： • Interface event received：收到接口事件 • IP address deleted：虚地址删除 • The status of the tracked object changed：Track 对象状态变化 • VRRP packet received：收到 VRRP 报文 • Current device has changed to IP address owner：当前设备成为地址拥有者 • Master-down-timer expired：Master down 定时器超时 • Zero priority packet received：收到 0 优先级的报文 • Preempt：发生了抢占 • Master group drove：管理备份组驱动
日志等级	6
举例	VRRP/6/VRRP_STATUS_CHANGE: The status of IPv4 virtual router 10 (configured on Ethernet1/2/0/1) changed (from Backup to Master): Master-down-timer expired.
日志说明	VRRP备份组中的Master或Backup路由器状态发生变化。可能的原因包括：收到接口事件、虚地址删除、Track对象状态变化、收到VRRP报文、当前设备成为地址拥有者、Master down定时器超时、收到0优先级的报文、发生了抢占或者管理备份组驱动
处理建议	检查VRRP备份组中的Master或Backup路由器状态，确保备份组工作正常

113.2 VRRP_VF_STATUS_CHANGE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) virtual forwarder [UINT32] detected status change (from [STRING] to [STRING]): [STRING].
参数解释	$1：VRRP协议版本 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：VF ID $5：VF先前状态 $6：VF当前状态 $7：状态变化原因
日志等级	6
举例	VRRP/6/VRRP_VF_STATUS_CHANGE: The IPv4 virtual router 10 (configured on GigabitEthernet5/1) virtual forwarder 2 detected status change (from Active to Initialize): Weight changed.
日志说明	虚拟转发器状态发生改变。可能的原因包括权重变化、定时器超时、VRRP备份组Down
处理建议	检查Track项的状态

113.3 VRRP_VMAC_INEFFECTIVE

日志内容	The [STRING] virtual router [UINT32] (configured on [STRING]) failed to add virtual MAC: [STRING].
参数解释	$1：VRRP协议版本 $2：VRRP备份组号 $3：VRRP备份组所在接口的名称 $4：出现错误的原因
日志等级	3
举例	VRRP/3/VRRP_VMAC_INEFFECTIVE: The IPv4 virtual router 10 (configured on Ethernet1/2/0/1) failed to add virtual MAC: Insufficient hardware resources.
日志说明	添加虚拟MAC地址失败
处理建议	确定操作失败的根因并解决

114 VXLAN

本节介绍 VXLAN 模块输出的日志信息。

114.1 VXLAN_LICENSE_UNAVAILABLE

日志内容	The VXLAN feature is disabled, because no licenses are valid.
参数解释	无
日志等级	3
举例	VXLAN/3/VXLAN_LICENSE_UNAVAILABLE: The VXLAN feature is disabled, because no licenses are valid.
日志说明	因为没有有效的License，VXLAN特性被禁用
处理建议	检查VXLAN的License，若要使用VXLAN特性，请安装有效的License

115 组播

115.1 FAPMC_EXHAUST

日志内容	The hardware resources were exhausted.
参数解释	无
日志等级	4
举例	LSWMON/4/FAPMC_EXHAUST: -Chassis=1-Slot=2; The hardware resources were exhausted.
日志说明	FAP芯片上组播出接口过多导致硬件资源耗尽
处理建议	建议不要在此芯片上配置太多组播出接口

115.2 HWFWDRESOURCE_ALARM

日志内容	The hardware resource usage on chip [UINT16] in slot [UINT16] reached or exceeded 95%. Reason: Too many multicast outgoing interfaces exist on the chip.
参数解释	$1：硬件芯片号 $2：槽位号
日志等级	4
举例	MC/4/HWFWDRESOURCE_ALARM: The hardware resource usage on chip 3 in slot 2 reached or exceeded 95%. Reason: Too many multicast outgoing interfaces exist on the chip.
日志说明	硬件芯片上组播出接口过多导致硬件资源使用率大于等于95%，打印此log告警
处理建议	建议不要在此芯片上再配置出接口

115.3 HWFWDRESOURCE_EXHAUST

日志内容	The hardware resources on chip [UINT16] in slot [UINT16] were exhausted. Reason: Too many multicast outgoing interfaces exist on the chip.
参数解释	$1：硬件芯片号 $2：槽位号
日志等级	2
举例	MC/2/HWFWDRESOURCE_EXHAUST: The hardware resources on chip 3 in slot 2 were exhausted. Reason: Too many multicast outgoing interfaces exist on the chip.
日志说明	硬件芯片上组播出接口过多导致硬件资源耗尽
处理建议	在此硬件芯片上减少组播出接口的配置

115.4 HWFWDRESOURCE_RECOVER

日志内容	The hardware resource usage on chip [UINT16] in slot [UINT16] dropped below 95%.
参数解释	$1：硬件芯片号 $2：槽位号
日志等级	4
举例	MC/4/HWFWDRESOURCE_RECOVER: The hardware resource usage on chip 3 in slot 2 dropped below 95%.
日志说明	硬件芯片上的硬件资源从耗尽或者使用率超过95%首次降低到95%以内打印
处理建议	无

116 功率管理

本节介绍功率管理模块输出的日志信息。

116.1 OVERLOAD

日志内容	System power required is [UINT32] w, more than total system power [UINT32] w. Please install additional power modules.
参数解释	$1：使用总功率 $2：系统总功率
日志等级	2
举例	PWRM/2/OVERLOAD: System power required is 6875 w, more than total system power 6000 w. Please install additional power modules.
日志说明	系统的使用总功率大于当前总功率，提示用户安装更多的电源模块，打印此log信息
处理建议	电源功率不足，需要增加电源

116.2 REDUNDANT_NUM_DECREASE

日志内容	Chassis [STRING]: Not enough power. The number of redundant power supplies changed from [UINT32] to [UINT32].
参数解释	$1：框号 $2：原冗余电源数量 $3：现冗余电源数量
日志等级	5
举例	PWRM/5/REDUNDANT_NUM_DECREASE: Chassis 1: Not enough power. The number of redundant power supplies changed from 1 to 0.
日志说明	功率不足，冗余电源数量变化
处理建议	插入电源

116.3 REDUNDANT_NUM_INCREASE

日志内容	Chassis [STRING]:Power has become sufficient.The number of redundant power supplies changed from [UINT32] to [UINT32].
参数解释	$1：框号 $2：原冗余电源数量 $3：现冗余电源数量
日志等级	5
举例	PWRM/5/REDUNDANT_NUM_INCREASE: Chassis 1: Power has become sufficient.The number of redundant power supplies changed from 0 to 1.
日志说明	功率足够，冗余电源数量变化
处理建议	无

116.4 REDUNDANT_POWERSUPPLY_INSTALLED

日志内容	The first redundant power supply in chassis [STRING] was installed.
参数解释	$1：框号
日志等级	5
举例	PWRM/5/REDUNDANT_POWERSUPPLY_INSTALLED: The first redundant power supply in chassis 1 was installed.
日志说明	第一个冗余电源安装，打印此log信息，提示用户有冗余电源
处理建议	无

116.5 REDUNDANT_POWERSUPPLY_REMOVED

日志内容	The last redundant power supply in chassis [STRING] was removed.
参数解释	$1：框号
日志等级	4
举例	PWRM/4/REDUNDANT_POWERSUPPLY_REMOVED: The last redundant power supply in chassis 1 was removed.
日志说明	最后一个冗余电源拔出，打印此log信息，提示用户所有冗余电源都已经拔出，后续拔出电源可能会导致功率不足
处理建议	建议不要再拔出电源

116.6 SETTING_PRIORITY_FAILED

日志内容	Chassis [STRING] Slot [UINT16] : The slot is not an LPU slot. Setting priority is not supported.
参数解释	$1：框号 $2：槽位号
日志等级	5
举例	PWRM/5/SETTING_PRIORITY_FAILED: Chassis 2 Slot 2 : The slot is not an LPU slot. Setting priority is not supported.
日志说明	该槽位不是线卡，无法设定功率优先级
处理建议	只对线卡设定功率优先级

116.7 UNDER_POWER

日志内容	Not enough power to power on board in chassis [STRING] slot [UINT16]. Required power is [UINT32] W, available power is [UINT32] W.
参数解释	$1：框号 $2：槽位号 $3：单板需求功率 $4：系统可用功率
日志等级	4
举例	PWRM/4/UNDER_POWER: Not enough power to power on board in chassis 1 slot 2. Required power is 1000 W, available power is 200 W.
日志说明	功率不足以给单板上电，打印此log信息
处理建议	电源功率不足，需要增加电源

116.8 UNSUPPORTED_BOARD

日志内容	[STRING] at chassis [UINT16] slot [UINT16] can not be supported.
参数解释	$1：单板名称 $2：框号 $3：槽位号
日志等级	4
举例	PWRM/4/UNSUPPORTED_BOARD: CR-LPU-XP20CC02 at chassis 1 slot 14 can not be supported.
日志说明	单板为不支持的类型
处理建议	当前模式下不支持该单板，请检查或更换单板

117 风扇管理

本节介绍风扇管理模块输出的日志信息。

117.1 FAN_ERROR

日志内容	Fan [UINT32]/[UNIT32] error.
参数解释	$1：风扇框编号 $2：风扇模块编号
日志等级	2
举例	FAN/2/FAN_ERROR: -MDC=1-Chassis=1-Slot=1; Fan 1/2 error.
日志说明	风扇模块处于异常状态
处理建议	请更换风扇模块

117.2 FAN_OEM_NOIDENTIFY

日志内容	The fan tray [UINT16] is not compatible with the system.
参数解释	$1：风扇模块号
日志等级	2
举例	FAN/2/FAN_OEM_NOIDENTIFY: The fan tray 1 is not compatible with the system.
日志说明	风扇模块与系统不配套
处理建议	拔掉此不配套风扇，换用配套风扇

117.3 FAN_SPEED_ERROR

日志内容	The speed of fan [UINT32]/[UNIT32] is too low.
参数解释	$1：风扇框编号 $2：风扇模块编号
日志等级	2
举例	FAN/2/FAN_SPEED_ERROR: -MDC=1-Chassis=1-Slot=1; The speed of fan 1/1 is too low.
日志说明	如果风扇模块转速低于全速的15%时，则打印该日志信息
处理建议	请更换风扇模块

118 电源管理

本节介绍电源管理模块输出的日志信息。

118.1 BACKPLANE_3V3_ABNORMAL

日志内容	Backplane 3.3V output voltage became abnormal.
参数解释	无
日志等级	4
举例	POWER/4/BACKPLANE_3V3_ABNORMAL: -MDC=1-Chassis=1-Slot=20; Backplane 3.3V output voltage became abnormal.
日志说明	背板输出3.3V电压处于异常状态。仅R17900-20设备打印该日志信息
处理建议	请联系技术支持

118.2 BACKPLANE_3V3_RESTORE

日志内容	Backplane 3.3V output voltage restored to normal.
参数解释	无
日志等级	5
举例	POWER/5/BACKPLANE_3V3_RESTORE: -MDC=1-Chassis=1-Slot=20; Backplane 3.3V output voltage restored to normal.
日志说明	背板输出3.3V电压正常状态。仅R17900-20设备打印该日志信息
处理建议	无

118.3 BACKPLANE_LOWER_12V_ABNORMAL

日志内容	12V output voltage of the lower backplane became abnormal.
参数解释	无
日志等级	4
举例	POWER/4/BACKPLANE_LOWER_12V_ABNORMAL: -MDC=1-Chassis=1-Slot=20; 12V output voltage of the lower backplane became abnormal.
日志说明	下背板输出12V电压处于异常状态。仅R17900-20设备打印该日志信息
处理建议	请联系技术支持

118.4 BACKPLANE_LOWER_12V_RESTORE

日志内容	12V output voltage of the lower backplane restored to normal.
参数解释	无
日志等级	5
举例	POWER/5/BACKPLANE_LOWER_12V_RESTORE: -MDC=1-Chassis=1-Slot=20; 12V output voltage of the lower backplane restored to normal.
日志说明	下背板输出12V电压处于正常状态。仅R17900-20设备打印该日志信息
处理建议	无

118.5 BACKPLANE_UPPER_12V_ABNORMAL

日志内容	12V output voltage of the upper backplane became abnormal.
参数解释	无
日志等级	4
举例	POWER/4/BACKPLANE_UPPER_12V_ABNORMAL: -MDC=1-Chassis=1-Slot=20; 12V output voltage of the upper backplane became abnormal.
日志说明	上背板输出12V电压处于异常状态。仅R17900-20设备打印该日志信息
处理建议	请联系技术支持

118.6 BACKPLANE_UPPER_12V_RESTORE

日志内容	12V output voltage of the upper backplane restored to normal.
参数解释	无
日志等级	5
举例	POWER/5/BACKPLANE_UPPER_12V_RESTORE: -MDC=1-Chassis=1-Slot=20; 12V output voltage of the upper backplane restored to normal.
日志说明	上背板输出12V电压处于正常状态。仅R17900-20设备打印该日志信息
处理建议	无

118.7 POWER_FAILED

日志内容	Output power of chassis [STRING] module [UINT32] does not match the input voltage of the module, Please identify whether the power module is operating correctly. If not, replace the module.
参数解释	$1：框号 $2：电源模块ID
日志等级	3
举例	POWER/3/POWER_FAILED: Output power of chassis 1 module 1 does not match the input voltage of the module. Please identify whether the power module is operating correctly. If not, replace the module.
日志说明	电源模块功率与输入电压不匹配
处理建议	**1.** 检查电源是否损坏 **2.** 更换电源

118.8 POWER_INCOMPATIBLE

日志内容	Incompatible power supply detected.
参数解释	无
日志等级	2
举例	POWER/2/POWER_INCOMPATIBLE: -MDC=1; Incompatible power supply detected.
日志说明	电源模块不兼容
处理建议	提示用户有不兼容的电源模块插入，检查电源是否混插，将电源换成统一型号电源

118.9 POWER_OEM_NOIDENTIFY

日志内容	The power supply [UINT16] is not compatible with the system.
参数解释	$1：电源模块号
日志等级	2
举例	POWER/2/POWER_OEM_NOIDENTIFY: The power supply 2 is not compatible with the system.
日志说明	电源模块与系统不配套
处理建议	拔掉此不配套电源，换用配套电源

118.10 POWER_SWITCH_ABNORMAL

日志内容	Only one power switch turned on. Please turn on the other power switch.
参数解释	无
日志等级	4
举例	POWER/4/POWER_SWITCH_ABNORMAL: -MDC=1-Chassis=1-Slot=20; Only one power switch turned on. Please turn on the other power switch.
日志说明	两个电源开关，只有一个处于ON状态，请将另一个也设置为ON状态。仅R17900-20设备打印该日志信息
处理建议	将另一个电源开关也设置为 ON 状态

118.11 POWER_SWITCH_RESTORE

日志内容	Both power switches turned on.
参数解释	无
日志等级	5
举例	POWER/5/POWER_SWITCH_RESTORE: -MDC=1-Chassis=1-Slot=20; Both power switches turned on.
日志说明	两个电源开关均处于ON状态，设备供电正常。仅R17900-20设备打印该日志信息
处理建议	无

119 温度管理

119.1 TEMPERATURE_CHIP_FAULTY

日志内容	Slot [UINT16] [STRING] temperature chip became faulty.
参数解释	$1：槽位号 $2：温度芯片位置
日志等级	4
举例	TEMP/4/TEMPERATURE_CHIP_FAULTY: -MDC=1-Chassis=1-Slot=1; Slot 1 Inflow 1 temperature chip became faulty.
日志说明	温度监控芯片处于异常状态
处理建议	请联系技术支持

119.2 TEMPERATURE_CHIP_RESTORE

日志内容	Slot [UINT16] [STRING] temperature chip restored to normal.
参数解释	$1：槽位号 $2：温度芯片位置
日志等级	5
举例	TEMP/5/TEMPERATURE_CHIP_RESTORE: -MDC=1-Chassis=1-Slot=1; Slot 1 Inflow 1 temperature chip restored to normal.
日志说明	温度监控芯片处于正常状态
处理建议	无

120 交换监控

120.1 CLUSTER_FIBER_CONNECTION

日志内容	Bundle port [STRING] subport [STRING] connected to the incorrect subport,please check.
参数解释	$1：BundlePort号 $2：Subport号
日志等级	3
举例	LSWMON/3/CLUSTER_FIBER_CONNECTION: Chassis=1-Slot=25; Bundle port 1 subport 1 connected to the incorrect subport,please check.
日志说明	集群网板级联光纤端口连接到错误的端口上，接口被shutdown防止交换网故障
处理建议	请检查告警端口级联光纤，连接到正确的集群网板端口上，当光纤有拔走动作时，接口自动恢复shutdown动作

120.2 CLUSTERPORT_DIFFERENCE

日志内容	Number of system maximum uplink ports is [UINT16]. Chassis [UINT16] slot [UINT16] has only [UINT16] uplink ports. The difference between the numbers must be equal to or less than two.
参数解释	$1：集群端口数 $2：框号 $3：槽位号 $4：集群端口数
日志等级	3
举例	LSWMON/3/CLUSTERPORT_DIFFERENCE: -Chassis=1-Slot=13; Number of system maximum uplink ports is 6. Chassis 1 slot 10 has only 3 uplink ports. The difference between the numbers must be equal to or less than two.
日志说明	R17900-08集群系统多个集群网板时，集群光模块UP的数目，两个网板之间的数目差值，必须小于等于2
处理建议	补齐缺少集群光模块连接的平面，或者把UP的光模块的平均到各个网板

120.3 CLUSTERPORT_REQUIRE

日志内容	Only port [UINT32] is up. At least two ports in up state are required.
参数解释	$1：集群端口号
日志等级	3
举例	LSWMON/3/CLUSTERPORT_REQUIRE: -Chassis=1-Slot=13; Only port 1 is up. At least two ports in up state are required.
日志说明	R17900-08集群每个槽位上至少有两个up端口，若up端口数量少于两个，则输出日志提示信息
处理建议	R17900-08集群请连接up端口，保证每个槽位至少有两个up端口

120.4 CLUSTERPORTCRC_CRIT

日志内容	Cluster control port [UINT32] was disable. Reason: A port on the ipc chip received packets with CRC errors.
参数解释	$1：集群控制通道端口号
日志等级	2
举例	LSWMON/2/CLUSTERPORT_CRIT: -Chassis=1-Slot=20; Cluster control port 1 was disable. Reason: A port on the ipc chip received packets with CRC errors.
日志说明	集群控制通道接口有CRC，防止控制协议报文超时，会进行主动shutdown进行控制通道切换，需要用户尽快排查光纤和光模块
处理建议	更换集群控制通道光纤或者光模块进行排查

120.5 FABRIC_CONNECTION_ERR

日志内容	Fabric port [STRING] connected to an unexpected port [STRING] ,please check.
参数解释	$1：端口号 $2：端口号
日志等级	3
举例	LSWMON/3/FABRIC_CONNECTION_ERR: -MDC=1-Chassis=1-Slot=25; Fabric port 1/25/3/5 connected to an unexpected port 1/25/3/5 ,please check.
日志说明	网板上面的link因为硬件连机器损坏等故障导致对接，则输出日志提示信息
处理建议	请排查连接的两个端口连机器物理是否损伤，进行更换

120.6 ILKNCRC_CRIT

日志内容	Chip [UINT32] was isolated. Reason: A port on the chip received packets with CRC errors.
参数解释	$1：芯片号
日志等级	2
举例	LSWMON/2/ILKNCRC_CRIT: -Chassis=1-Slot=2; Chip 1 was isolated. Reason: A port on the chip received packets with CRC errors.
日志说明	转发芯片上的端口出现CRC故障，该芯片已被隔离
处理建议	请联系技术支持

120.7 ILKNFAULT_CRIT

日志内容	Chip [UINT32] was isolated. Reason: A port on the chip failed.
参数解释	$1：芯片号
日志等级	2
举例	LSWMON/2/ILKNFAULT_CRIT: -Chassis=1-Slot=2; Chip 2 was isolated. Reason: A port on the chip failed.
日志说明	转发芯片上的端口出现故障，该芯片已被隔离
处理建议	请联系技术支持

120.8 LOOSECONN_CRIT

日志内容	Chip [UINT32] port [UINT32] went down or flapped. Please secure the cards in chassis [UINT16] slot [UINT16] and chassis [UINT16] slot [UINT16] firmly.
参数解释	$1：芯片号 $2：端口号 $3：框号 $4：槽位号 $5：框号 $6：槽位号
日志等级	2
举例	LSWMON/2/LOOSECONN_CRIT: -Chassis=1-Slot=2; Chip 0 port 6 went down or flapped. Please secure the cards in chassis 1 slot 17 and chassis 1 slot 22 firmly.
日志说明	线卡或者网板插入后，检查到链路有down，提示用户排查是否插紧单板
处理建议	发现单板没有插紧，重新插拔告警单板，把单板插到位

120.9 MODULE_WARN

日志内容	Bundle port [UINT16] subport [UINT16].warning. Reason: RX power low.
参数解释	$1：bundleport号 $2：subport号
日志等级	1
举例	LSWMON/1/MODULE_WARN: -Chassis=1-Slot=22; Bundle port 1 subport 1 warning. Reason: RX power low.
日志说明	R17900-20集群光纤对应的bundleport subport的接收光功率不满足要求
处理建议	通过专业光纤擦除工具，擦拭光纤和光接口，如果问题仍然存在，更换新的光纤

120.10 SFIFAULT_CRIT

日志内容	Chip [UINT32] was isolated. Reason: Link failures occurred on all ports of the chip.
参数解释	$1：芯片号
日志等级	2
举例	LSWMON/2/SFIFAULT_CRIT: -Chassis=1-Slot=2; Chip 0 was isolated. Reason: Link failures occurred on all ports of the chip.
日志说明	数据通道端口全部出现链路故障，该FAP上的两个转发芯片已被隔离
处理建议	请确认本框内是否有网板，如果有请联系技术支持

120.11 SFIRECOVER_CRIT

日志内容	Chip [UINT32] was released from isolation. Reason: A switching fabric was inserted.
参数解释	$1：芯片号
日志等级	2
举例	LSWMON/2/SFIRECOVER_CRIT: -Chassis=1-Slot=2; Chip 0 was released from isolation. Reason: A switching fabric was inserted.
日志说明	网板插入，线卡侧解除数据通道端口隔离，该FAP上的转发芯片隔离被解除
处理建议	无

121 端口镜像

本节介绍端口镜像模块输出的日志信息。

121.1 MIRRORING-PORT_LIMIT

日志内容	Nps not support Cpupacket.
参数解释	无
日志等级	4
举例	QACL/4/MIRRORING-PORT_LIMIT: -Chassis=1 -Slot=2; Nps not support Cpupacket.
日志说明	nps不支持只镜像协议报文的功能
处理建议	无

122 MPLS TE 带宽资源

本节介绍入 MPLS TE 带宽资源模块的输出日志信息。

122.1 MPLSTE_FLOWID_NORESOURCE

日志内容	Insufficient bandwidth resources for MPLS TE tunnel [UINT32].
参数解释	$1：TE隧道ID
日志等级	4
举例	MPLS/4/MPLSTE_FLOWID_NORESOURCE: Insufficient bandwidth resources for MPLS TE tunnel 143.
日志说明	该TE隧道出接口的带宽资源已耗尽，申请带宽资源失败
处理建议	无

122.2 MPLS_SRLSP_FLOWID_NORESOURCE

日志内容	Insufficient bandwidth resources for SRLSP:nid = [UINT32].
参数解释	$1：SRLSP的nid.
日志等级	4
举例	MPLS/4/MPLS_SRLSP_FLOWID_NORESOURCE: Insufficient bandwidth resources for SRLSP:nid = 143.
日志说明	该SRLSP出接口的带宽资源已耗尽，申请带宽资源失败
处理建议	无

123 入方向队列

本节介绍入方向队列模块的输出日志信息。

123.1 QACL_CONFIGURATION_FAILURE

日志内容	Failed to apply the inbound queuing configuration on the interface. Reason: Not enough hardware resources.
参数解释	无
日志等级	4
举例	QACL/4/QACL_CONFIGURATION_FAILURE: -Chassis=1-Slot=2; Failed to apply the inbound queuing configuration on the interface. Reason: Not enough hardware resources.
日志说明	硬件资源不足，导致入方向队列配置不生效
处理建议	根据需要减少相关的配置

124 QACL

124.1 BPA_APPLY_RESOURCE_FAIL

日志内容	Failed to request hardware resources for BGP policy accounting.
参数解释	无
日志等级	4
举例	QACL/4/BPA_APPLY_RESOURCE_FAIL: -MDC=1-Chassis=1-Slot=2; Failed to request hardware resources for BGP policy accounting.
日志说明	BPA业务申请硬件资源失败
处理建议	联系技术人员

124.2 BPA_IN_RESOURCE_EXHAUSTED

日志内容	Hardware resource exhaustion. Reason: Too many inbound BPA services have been deployed to the chips.
参数解释	无
日志等级	4
举例	QACL/4/BPA_IN_RESOURCE_EXHAUSTED : -MDC=1-Slot=2; Hardware resource exhaustion. Reason: Too many inbound BPA services have been deployed to the chips.
日志说明	芯片入方向BPA业务下发过多，导致硬件资源耗尽
处理建议	在此芯片上减少入方向BPA业务的配置

124.3 BPA_OUT_RESOURCE_EXHAUSTED

日志内容	Hardware resource exhaustion. Reason: Too many outbound BPA services have been deployed to the chips.
参数解释	无
日志等级	4
举例	QACL/4/BPA_OUT_RESOURCE_EXHAUSTED: -MDC=1-Slot=2; Hardware resource exhaustion. Reason: Too many outbound BPA services have been deployed to the chips.
日志说明	芯片出方向BPA业务下发过多，导致硬件资源耗尽
处理建议	在此芯片上减少出方向BPA业务的配置

124.4 MEMORY_ALERT_CRITICAL

日志内容	Failed to configure the command because the critical free-memory threshold was exceeded.
参数解释	无
日志等级	4
举例	QACL/4/MEMORY_ALERT_CRITICAL: Failed to configure the command because the critical free-memory threshold was exceeded.
日志说明	在配置QoS和ACL模块命令时，系统达到三级内存门限，配置不生效
处理建议	等待内存恢复正常之后再配置

124.5 MEMORY_ALERT_MINOR

日志内容	The minor free-memory threshold was exceeded, but the configuration took effect.
参数解释	无
日志等级	4
举例	QACL/4/MEMORY_ALERT_MINOR: The minor free-memory threshold was exceeded, but the configuration took effect.
日志说明	在配置QoS和ACL模块命令时，系统达到一级内存门限，配置生效
处理建议	建议停止配置QoS和ACL模块命令

124.6 MEMORY_ALERT_SEVERE

日志内容	Failed to configure the command because the severe free-memory threshold was exceeded.
参数解释	无
日志等级	4
举例	QACL/4/MEMORY_ALERT_SEVERE: Failed to configure the command because the severe free-memory threshold was exceeded.
日志说明	在配置QoS和ACL模块命令时，系统达到二级内存门限，配置不生效
处理建议	等待内存恢复正常之后再配置

125 集群

125.1 CHASSIS_CONFLICT

日志内容	Port [UINT32] and port [UINT32] were connected to chassis that have the same chassis number (chassis [STRING]).
参数解释	$1：端口号 $2：端口号 $3：框号
日志等级	5
举例	CCRP/5/CHASSIS_CONFLICT: Port 1 and port 2 were connected to chassis that have the same chassis number (chassis 1).
日志说明	两个不同端口所连接的框框号发生冲突
处理建议	请检查并修改框号

125.2 CHASSIS_CONFLICT_WITH_SELF

日志内容	Port [UINT32] was connected to a chassis that has the same chassis number (chassis [STRING]) as this chassis.
参数解释	$1：端口号 $2：框号
日志等级	5
举例	CCRP/5/CHASSIS_CONFLICT_WITH_SELF: Port 1 was connected to a chassis that has the same chassis number (chassis 1) as this chassis.
日志说明	端口所连接的框与本框存在框号冲突
处理建议	请检查并修改框号

125.3 CHASSIS_NUMBER_CONFLICT

日志内容	Chassis [STRING] on port [UINT32] is conflict with another chassis.
参数解释	$1：连接端的框号 $2：端口号
日志等级	5
举例	CCRP/5/CHASSIS_NUMBER_CONFLICT: Chassis 1 on port 2 is conflict with another chassis.
日志说明	连接端与拓扑中其他框的框号相同
处理建议	**1.** 根据信息中的端口号，找到连接设备的设备 **2.** 连接串口，修改框号

125.4 FLUSH_MCAST_ENTRY_FAIL

日志内容	Failed to flush a multicast entry: chassis=[STRING], operation=[UINT32], upstream number=[UINT32], downstream-count=[UINT32].
参数解释	$1：框号 $2：操作类型 $3：上游端口号 $4：下游端口数目
日志等级	5
举例	CCRP/5/FLUSH_MCAST_ENTRY_FAIL: Failed to flush a multicast entry: chassis=1, operation=1, upstream number=2, downstream-count=4.
日志说明	组播表项下刷失败
处理建议	请联系技术人员

125.5 FLUSH_UCAST_ENTRY_FAIL

日志内容	Failed to flush a unicast entry: chassis=[STRING], operation=[UINT32], old-port=[UINT32], new-port=[UINT32].
参数解释	$1：框号 $2：操作类型 $3：旧端口号 $4：新端口号
日志等级	5
举例	CCRP/5/FLUSH_UCAST_ENTRY_FAIL: Failed to flush a unicast entry: chassis=1, operation=2, old-port=1, new-port=2.
日志说明	单播表项下刷失败
处理建议	请联系技术人员

125.6 MESH_STATE_ABNORMAL

日志内容	Control plane has not been in fully meshed state for over [UINT64] minutes. Please examine the connections.
参数解释	$1：时间
日志等级	4
举例	CCRP/4/MESH_STATE_ABNORMAL: -MDC=1; Control plane has not been in fully meshed state for over 60 minutes. Please examine the connections.
日志说明	集群处于非全互联状态，请检查连接
处理建议	背靠背环境：每个主控都要与其他主控有连接 多框环境： 每个主控都要与所有MCCU有连接，每个MCCU都要与其他所有MCCU有连接

125.7 MESH_STATE_RESTORE

日志内容	Control plane changed into fully-meshed state.
参数解释	无
日志等级	4
举例	CCRP/4/MESH_STATE_RESTORE: -MDC=1; Control plane changed into fully-meshed state.
日志说明	集群控制平台进入全互联状态
处理建议	无

125.8 MULTIPLE_MASTER

日志内容	The master (chassis [STRING] slot [UINT16]) recognized by port [UINT32] is not the current master (chassis [STRING] slot [UINT16]) in the system.
参数解释	$1：框号 $2：槽位号 $3：端口号 $4：框号 $5：槽位号
日志等级	5
举例	CCRP/5/MULTIPLE_MASTER: The master (chassis 2 slot 20) recognized by port 1 is not the current master (chassis 1 slot 20) in the system.
日志说明	系统中存在多主冲突
处理建议	请检查并修改集群相关配置

125.9 NEIGHBOR_UP

日志内容	Neighbor chassis [UINT32] slot [UINT32] on port [UINT32] changed from Init to Up.
参数解释	$1：框号 $2：槽位号 $3：端口号
日志等级	5
举例	CCRP/5/NEIGHBOR_UP: Neighbor chassis 1 slot 20 on port 1 changed from Init to Up.
日志说明	集群控制通道邻居从INIT状态变为UP状态
处理建议	无

125.10 NEIGHBOR_UP_TO_DOWN

日志内容	Neighbor chassis [UINT32] slot [UINT32] on port [UINT32] changed from Up to Down.
参数解释	$1：框号 $2：槽位号 $3：端口号
日志等级	5
举例	CCRP/5/NEIGHBOR_UP_TO_DOWN: Neighbor chassis 1 slot 20 on port 1 changed from Up to Down.
日志说明	集群控制通道邻居从UP状态变为DOWN状态
处理建议	请检查状态变化是否与人为操作相关，若无任何操作，请检查相应连接

125.11 NEIGHBOR_UP_TO_INIT

日志内容	Neighbor chassis [UINT32] slot [UINT32] on port [UINT32] changed from Up to Init.
参数解释	$1：框号 $2：槽位号 $3：端口号
日志等级	5
举例	CCRP/5/NEIGHBOR_UP_TO_INIT: Neighbor chassis 1 slot 20 on port 1 changed from Up to Init.
日志说明	集群控制通道邻居从UP状态变为INIT状态
处理建议	无

125.12 PORT_LINK_CHANGE

日志内容	PORT_LINK_UP: The link of control channel port [UINT32] came up. PORT_LINK_DOWN: The link of control channel port [UINT32] link went down.
参数解释	$1：端口号
日志等级	5
举例	CCRP/5/PORT_LINK_DOWN: The link of control channel port 1 went down.
日志说明	集群控制通道端口link状态发生变化
处理建议	请检查端口状态变化是否与人为操作相关，若无任何操作，请检查相应端口

125.13 PORT_LINK_FAULT

日志内容	Port [UINT32] was connected to [STRING].
参数解释	$1： 端口号 $2：对端与本身关系 • itself • a port on the same MPU • a port on the same CCU • a port on the other MPU in the same chassis
日志等级	5
举例	CCRP/5/PORT_LINK_FAULT: Port 1 was connected to a port on the same MPU.
日志说明	集群控制端口物理连线错误
处理建议	请根据日志，检查相关连线

125.14 PORT_LINK_UDC_MISMATCH

日志内容	Port [UINT32] received packets with mismatched sequence numbers from port [UINT32] of chassis [STRING] slot [UINT16]. Please check the port connection.
参数解释	$1：端口号 $2：端口号 $3：框号 $4：槽位号
日志等级	5
举例	CCRP/5/PORT_LINK_ UDC_MISMATCH: Port 1 received packets with mismatched sequence numbers from port 2 of chassis 2 slot 20. Please check the port connection.
日志说明	端口接收到的对端报文序列号有误
处理建议	请检查连接是否正常

125.15 PORT_LINK_UDC_MISMATCH_ISSU

日志内容	Port [UINT32] received packets with mismatched sequence numbers. Please check the port connection.
参数解释	$1：端口号
日志等级	5
举例	CCRP/5/PORT_LINK_UDC_MISMATCH_ISSU: Port 1 received packets with mismatched sequence numbers. Please check the port connection.
日志说明	端口收到的报文序列号有误
处理建议	请检查控制通道连接并联系技术人员

125.16 PORT_LINK_UDC_TIMEOUT

日志内容	Port [UINT32] has problem in receiving packets from its peer.
参数解释	$1：端口号
日志等级	5
举例	CCRP/5/PORT_LINK_UDC_TIMEOUT: Port 1 has problem in receiving packets from its peer.
日志说明	集群端口发生单通，接收对端报文出现问题
处理建议	请检查连线及单板是否正常

125.17 PORT_RXPOWER_LOW

日志内容	Bundle port [UINT16] subport [UINT16] warning. Reason: RX power low.
参数解释	$1：集群互联口号 $2：集群互联口子端口号
日志等级	3
举例	CLUSTER/3/PORT_RXPOWER_LOW: -Chassis=1–Slot=22; Bundle port 1 subport 1 warning. Reason: RX power low.
日志说明	集群互联口接收光功率低
处理建议	请检查光模块及集群互联口连线是否有误,如果无误,请联系技术支持人员

125.18 PORTFAULT_ALERT

日志内容	Link flapped up and down in the past 5 seconds on bundle port [UINT32]. Please check for cabling errors.
参数解释	$1：集群互联口号
日志等级	1
举例	CLUSTER/1/ PORTFAULT_ALERT: -Chassis=1-Slot =22; Link flapped up and down in the past 5 seconds on bundle port 1. Please check for cabling errors.
日志说明	集群互联口频繁up/down
处理建议	请检查光模块及集群互联口连线是否有误，如果无误，请联系技术支持人员

126 FIP

126.1 TEMPERATURE_OFF

日志内容	Board in chassis [STRING] slot [UINT16] was powered off for temperature was greater than high-temperature shutdown threshold.
参数解释	$1：框号 $2：槽位号
日志等级	4
举例	FIP/4/TEMPERATURE_OFF: -MDC=1; Board in chassis fcc1 slot 2 was powered off for temperature was greater than high-temperature shutdown threshold.
日志说明	单板由于温度高于高温关断门限而下电
处理建议	**1.** 检查环境温度是否过高，保持设备环境通风正常 **2.** 检查风扇是否存在且正常工作

127 JIGGLE

127.1 OFF

日志内容	Ejector levers closed. The module is operating correctly.
参数解释	无
日志等级	5
举例	JIGGLE/5/OFF: Ejector levers closed. The module is operating correctly.
日志说明	网板的把手已扣上，板子恢复正常工作
处理建议	无

127.2 ON

日志内容	Ejector levers opened. The module can be pulled out safely.
参数解释	无
日志等级	5
举例	JIGGLE/5/ON: Ejector levers opened. The module can be pulled out safely.
日志说明	网板的把手已打开，板子可以被拔出
处理建议	无

127.3 TRIGGER

日志内容	Chassis [STRING] slot [UINT16]: OFL button pressed. The module can be pulled out safely.
参数解释	$1：框号 $2：槽位号
日志等级	5
举例	JIGGLE/5/TRIGGER: Chassis 1 slot 22: OFL button pressed. The module can be pulled out safely.
日志说明	网板的OFL按钮已按下，板子可以被拔出
处理建议	无

128 MPUM

128.1 FAULTY_CHASSIS_CCU

日志内容	The faulty chassis [STRING] still has CCU Cards in the control-channel connections. Please check the connections for potential risks that might cause a system failure.
参数解释	$1：故障框（分裂出去的FCC框）的框号
日志等级	4
举例	MPUM/4/FAULTY_CHASSIS_CCU: -MDC=1; The faulty chassis fcc1 still has CCU Cards in the control-channel connections. Please check the connections for potential risks that might cause a system failure.
日志说明	集群控制通道分裂，FCC框已经分裂出去，但是避免引起更严重的故障，分裂出去的FCC框的CCU仍然在系统中正常使用，打印此日志
处理建议	**1.** 检查控制通道连接，将控制通道线路连接好 **2.** 断开故障框的 CCU 连接,或重启故障框

128.2 FCC1_FOUND

日志内容	The chassis has been connected to FCC1.
参数解释	无
日志等级	4
举例	MPUM/4/FCC1_FOUND: The chassis has been connected to FCC1.
日志说明	框启动时没有与FCC1互连，打印WAIT_FCC1信息；然后，连接上FCC1之后，串口会打印此日志
处理建议	无

128.3 MASTER_LOST

日志内容	Please check the control-channel connections, and then press the ESC and eshell keys to enter eshell view to execute the reboot command.
参数解释	无
日志等级	4
举例	MPUM/4/MASTER_LOST: Please check the control-channel connections, and then press the ESC and eshell keys to enter eshell view to execute the reboot command.
日志说明	集群控制通道分裂，与Master失去联系的主控串口打印此日志
处理建议	**1.** 首先，检查控制通道连接，将控制通道线路连接好 **2.** 然后，打开每个与 Master 失联的主控串口，进入 eshell 重启；或直接将失联框断电重启

128.4 MULTIPLE_MASTER

日志内容	More than one master was found in the system. Please check the control-channel connections, and then press the ESC and eshell keys to enter eshell view to execute the reboot command.
参数解释	无
日志等级	4
举例	MPUM/4/MULTIPLE_MASTER: More than one master was found in the system. Please check the control-channel connections, and then press the ESC and eshell keys to enter eshell view to execute the reboot command.
日志说明	本框连接到了两个或多个集群系统中，串口会打印此日志
处理建议	检查控制通道连接，让本框只与一个系统连接，然后进入eshell视图重启

128.5 NEIGHBORS_LOST

日志内容	Please check the control-channel connections, and then execute the reboot command.
参数解释	无
日志等级	4
举例	MPUM/4/NEIGHBORS_LOST: -MDC=1-Chassis=fcc1-Slot=14; Please check the control-channel connections, and then execute the reboot command.
日志说明	集群控制通道分裂，本框是Master，但是因本框优先级低而被隔离了
处理建议	**1.** 首先，检查控制通道连接，将控制通道线路连接好 **2.** 然后，执行 reboot force 重启

128.6 ONE_MASTER_FOUND

日志内容	One master has been found in the system and no other master exists.
参数解释	无
日志等级	4
举例	MPUM/4/ONE_MASTER_FOUND: One master has been found in the system and no other master exists.
日志说明	系统中已有一主用主控，并且无其它主用主控
处理建议	无

128.7 WAIT_FCC1

日志内容	Please connect the chassis to FCC1, or press the ESC and eshell keys to enter eshell view to modify the cluster mode and chassis number and then reboot.
参数解释	无
日志等级	4
举例	MPUM/4/WAIT_FCC1: Please connect the chassis to FCC1, or press the ESC and eshell keys to enter eshell view to modify the cluster mode and chassis number and then reboot.
日志说明	多框模式下，如果本框不是FCC1且没有与FCC1互联，则串口打印
处理建议	**1.** 检查本框与 FCC1 主控之间是否存在控制通道通路 **2.** 进入 eshell 视图，执行 summary 检查集群模式和框号是否正确

129 NP 芯片

129.1 DEADLOCK_ALERT

日志内容	Chip [UINT16] was isolated. Reason: Deadlock error occurred on the chip.
参数解释	$1：NP芯片号
日志等级	1
举例	NP/1/DEADLOCK_ALERT: -Chassis=1-Slot=2; Chip 1 was isolated. Reason: Deadlock error occurred on the chip.
日志说明	NP芯片出现死锁错误，该芯片已被隔离
处理建议	请联系技术支持

129.2 ECC_ALERT

日志内容	Chip [UINT16] was isolated. Reason: Irreparable ECC error occurred.
参数解释	$1：NP芯片号
日志等级	1
举例	NP/1/ECC_ALERT: -Chassis=1-Slot=2; Chip 1 was isolated. Reason: Irreparable ECC error occurred.
日志说明	NP芯片出现无法纠正的ECC错误，该芯片已被隔离
处理建议	请联系技术支持

129.3 ILKN_ALERT

日志内容	Chip [UINT16] was isolated. Reason: Interlaken on the chip failed.
参数解释	$1：NP芯片号
日志等级	1
举例	NP/1/ILKN_ALERT: -Chassis=1-Slot=2; Chip 2 was isolated. Reason: Interlaken on the chip failed.
日志说明	NP芯片上的Interlakent通道出现故障，该芯片已被隔离
处理建议	请联系技术支持

129.4 NPS_ALERT

日志内容	Chip [UINT8] was isolated because of [STRING].
参数解释	$1：NPS芯片号 $2：隔离原因，取值包含： • a deadlock error：芯片出现死锁错误 • a PCI_OFFLOAD exception：PCI_OFFLOAD 模块异常 • an uncorrectable ECC error：芯片出现无法纠正的 ECC 错误
日志等级	1
举例	NP/1/NPS_ALERT: -MDC=1-Chassis=1-Slot=2; Chip 1 was isolated because of a deadlock error.
日志说明	因为硬件问题，导致当前NPS芯片被隔离
处理建议	请联系技术支持

129.5 NP_TCAM_ERROR

日志内容	A NP chip error event of type [HEX] occurred on the chip [UINT16].
参数解释	$1：错误事件的类型 $2：NP芯片号
日志等级	4
举例	NPTCAM/4/NP_TCAM_ERROR: -Chassis=1-Slot=2; A NP chip error event of type 0x2 occurred on the chip 0.
日志说明	NP芯片读写TCAM时产生错误
处理建议	请联系技术支持

130 VXLAN 统计资源

本节介绍 VXLAN 模块输出的统计资源不足的提示日志信息。

130.1 VXLAN_STATISTIC_NORESOURCE

日志内容	Not enough resources for VXLAN statistics.
参数解释	无
日志等级	4
举例	VXLAN/4/VXLAN_STATISTIC_NORESOURCE: -MDC=1-Slot=2; Not enough resources for VXLAN statistics.
日志说明	在绑定隧道到vsi时，vsi下开启了隧道统计且统计资源不足，申请统计资源失败
处理建议	等待统计资源足够之后再配置

131 PTP

131.1 PTP_ALERT

日志内容	Failed to issue the PTP command. Reason: Clock daughter card is absent.
参数解释	无
日志等级	3
举例	PTP/3/PTP_ALERT: -MDC=1-Slot=2; Failed to issue the PTP command. Reason: Clock daughter card is absent.
日志说明	PTP驱动命令下发失败；可能原因：时钟扣板不在位或出现故障
处理建议	请检查时钟扣板是否在位，若时钟扣板已在位，请联系技术支持

132 IP FIB 前缀硬件资源

本节介绍 IP FIB 前缀包括 IPv4、IPv6 硬件 TCAM 表项资源不足的提示日志信息。

132.1 IPUC_FTN_NORESOURCE

日志内容	[STRING] FTN does not have sufficient TCAM resources.
参数解释	$1：FTN表类型，IPv4或IPv6
日志等级	4
举例	L3/4/IPUC_FTN_NORESOURCE: -MDC=1-Slot=2; IPv4 FTN does not have sufficient TCAM resources. L3/4/IPUC_FTN_NORESOURCE: -MDC=1-Slot=2; IPv6 FTN does not have sufficient TCAM resources.
日志说明	IPv4或IPv6的FTN表资源不足，NP芯片下发FTN表失败
处理建议	请删除超出规格的路由

133 IPC 拓扑故障日志

133.1 IETH_PORT_SWITCH

日志内容	No port available for IPC switchover from [UINT16]. IPC switchover from [UINT16] to [UINT16] failed. Reason: [STRING]. IPC switchover from [UINT16] to [UINT16] succeeded.

参数解释	• 无可切换的端口
	  ○ $1：故障端口号
	• 故障端口切换时，由于某些原因切换失败
	  ○ $1：故障端口号 $2：切换端口号 $3：切换失败原因
	• 故障端口成功切换到可用端口
	  ○ $1：故障端口号 $2：切换端口号

日志等级	3
举例	IPC/3/IETH_PORT_SWITCH: -MDC=1-Slot=2; IPC switchover from 4 to 5 failed. Reason: no enough vlan resources.
日志说明	CPU与交换芯片相连的端口故障发生切换时，打印该日志
处理建议	根据日志确认是否切换成功。若失败，查看端口信息，确认切换失败原因

133.2 STATE_FAULT

日志内容	The channel for IPC can't transmit packets. The channel for IPC to slot [UINT16] CPU [UINT16] can't transmit packets.
参数解释	$1：槽位号 $2：CPU号
日志等级	3
举例	IBC/3/STATE_FAULT: -MDC=1-Slot=2; The channel for IPC to slot1.CPU 2 can't transmit packets.
日志说明	检测到端口故障时，输出该日志
处理建议	根据ping诊断或者查看端口信息定位端口故障原因

134 CARD

134.1 CARD_PROCESSING

日志内容	Processing the subcard in chassis [UINT16] slot [UINT16] subslot [UINT16]. Please wait.
参数解释	$1：框号 $2：槽位号 $3：子槽位号
日志等级	6
举例	CARD/6/CARD_PROCESSING: -MDC=1-Slot=2; Processing the subcard in chassis 1 slot 2 subslot 1. Please wait.
日志说明	前面的子卡插拔操作还未完成，请稍后
处理建议	请耐心等待，若30分钟后仍未处理完请将子卡拔出重新插入，若仍有问题请联系技术支持

134.2 MODULE_WARNING

日志内容	Unrecognized or unsupported subcard in chassis [UINT16] slot [UINT16] subslot [UINT16].
参数解释	$1：框号 $2：槽位号 $3：子槽位号
日志等级	4
举例	MODULE/4/MODULE_WARNING: -MDC=1-Slot=2; Unrecognized or unsupported subcard in chassis 1 slot 2 subslot 1.
日志说明	子卡类型未识别，或不支持该子卡
处理建议	1. 首先请确认所插子卡是否支持 2. 若支持请检查子卡插入是否到位 3. 请将子卡拔出重新插入 4. 若仍有问题请联系技术支持

135 业务板

135.1 TUNNEL_REDIRECTION_FAILURE

日志内容	Failed to redirect traffic from tunnel [UINT32] to the Service Board. Reason: Not enough ACL resources.
参数解释	$1：隧道ID
日志等级	4
举例	TUNNEL/4/TUNNEL_REDIRECTION_FAILURE: -MDC=1-Chassis=1-Slot=2; Failed to redirect traffic from tunnel 10 to the Service Board. Reason: Not enough ACL resources.
日志说明	ACL资源不足，导致ACL功能从隧道10引流到业务板不生效
处理建议	根据需要减少ACL相关的配置

136 ARP 防攻击日志

本节介绍 ARP 防攻击模块输出的日志信息。

136.1 ANTI-ATTACK_ALARM_CLEAR

日志内容	The rate of [STRING] traffic on [STRING] dropped to or below the alarm threshold.
参数解释	$1：协议名称 $2：接口名称
日志等级	5
举例	RXTX/5/ANTI-ATTACK_ALARM_CLEAR: -MDC=1-Slot=2; The rate of ARP_Request_Local/ARP_Request_Proxy traffic on GigabitEthernet1/2/0/1 dropped to or below the alarm threshold.
日志说明	当前协议的传输速率恢复到所在接口的限速阈值以内，告警消除
处理建议	提示用户当前协议传输速率恢复到了该接口速率阈值内，恢复正常

136.2 ANTI-ATTACK_ALARM_THRESHOLD

日志内容	The rate of [STRING] traffic on [STRING] exceeded the alarm threshold.
参数解释	$1：协议名称 $2：接口名称
日志等级	4
举例	RXTX/4/ANTI-ATTACK_ALARM_THRESHOLD: -MDC=1-Slot=2; The rate of ARP_Request_Local/ARP_Request_Proxy traffic on GigabitEthernet1/2/0/1 exceeded the alarm threshold.
日志说明	当前协议的传输速率超过所在接口的限速阈值
处理建议	提示用户降低所在接口上对应的协议速率

137 MPLS 标签索引资源

137.1 MPLS_LABELINDEX_NORESOURCE

日志内容	Not enough label index resources for nid [UINT32].
参数解释	$1：NHLFE ID
日志等级	4
举例	MPLS/4/ MPLS_ LABELINDEX _NORESOURCE: Not enough label index resources for nid 143.
日志说明	标签索引资源已耗尽，申请标签索引资源失败
处理建议	无

138 内部控制通道

138.1 ERR_EXCEED_THRESHOLD

日志内容	Number of errors on the link [STRING] reached or exceeded the fault threshold.
参数解释	$1：链路名称，包含如下取值： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP *n*：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot *n*：连接 slot n 的链路，n 为 slot 号 • to NP *n*：连接 NP n 的链路，n 为 NP 号，取值为 0～5
日志等级	3
举例	IBC/3/ERR_EXCEED_THRESHOLD: Number of errors on the link used for IBD to CPU 1 reached or exceeded the fault threshold.
日志说明	内部控制通道链路上的错误包到达故障门限
处理建议	连接到槽位的端口链路down，需要检查单板是否插紧；通常为硬件故障

138.2 ERR_RECOVERY

日志内容	Number of errors on the link [STRING] dropped below the fault threshold.
参数解释	$1：链路名称，包含如下取值： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP *n*：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot *n*：连接 slot n 的链路，n 为 slot 号 • to NP *n*：连接 NP n 的链路，n 为 NP 号，取值为 0～5
日志等级	3
举例	IBC/3/ERR_RECOVERY: Number of errors on the link used for IBD to CPU 1 dropped below the fault threshold.
日志说明	内部控制通道链路上的错误包恢复到故障门限以下
处理建议	无

138.3 LINK_DOWN

日志内容	The link [STRING] went down.
参数解释	$1：链路名称，包含如下取值： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP *n*：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot *n*：连接 slot n 的链路，n 为 slot 号 • to NP *n*：连接 NP n 的链路，n 为 NP 号，取值为 0～5
日志等级	3
举例	IBC/3/LINK_DOWN: The link used for IBD to CPU 1 went down.
日志说明	内部控制通道链路处于down状态
处理建议	连接到槽位的端口链路down，需要检查单板是否插紧；通常为硬件故障

138.4 LINK_UP

日志内容	The link [STRING] came up.
参数解释	$1：链路名称，包含如下取值： • used for IPC：用于 IPC 的链路 • used for IBD：用于 IBD 的链路 • used for MGE：用于管理以太网接口的内部链路 • used for NP *n*：用于 NP n 的链路，n 为 NP 号，n 为 0～5 的数字 • used for IPC to CPU 1：连接 CPU1 的 IPC 链路 • used for IBD to CPU 1：连接 CPU1 的 IBD 链路 • to slot *n*：连接 slot n 的链路，n 为 slot 号 • to NP *n*：连接 NP n 的链路，n 为 NP 号，取值为 0～5
日志等级	3
举例	IBC/3/LINK_UP: The link used for IBD to CPU 1 came up.
日志说明	内部控制通道链路恢复到up状态
处理建议	无

139 DEVM

139.1 MPU_INCOMPATIBLE

日志内容	Inconsistent MPU models.
参数解释	无
日志等级	2
举例	DEVM/2/MPU_INCOMPATIBLE: Inconsistent MPU models.
日志说明	本机框插入了不同型号的主控板
处理建议	请更换为本机框支持的相同型号主控板

140 NQA

140.1 NQA_RTC_OCCUPIED

日志内容	Failed to configure the NQA operation. Reason: RTC [UINT64] on chip [UINT8] is being used by an NQA operation.
参数解释	$1：rtc号 $2：NP芯片号
日志等级	4
举例	NP/4/NQA_RTC_OCCUPIED: -Chassis=1-Slot=2; Failed to configure the NQA operation. Reason: RTC 1 on chip 1.is being used by an NQA operation.
日志说明	当前NP芯片的定时器已用于路径服务质量测试
处理建议	请不要在同一个NP芯片上，启动多个路径服务质量测试

141 ISOLATE

141.1 FORWARDING_FAILURE_OCCURRED

日志内容	Forwarding failure [HEX] occurred on all ports of NP [UINT16].
参数解释	$1：故障类型 $2：NP芯片号
日志等级	4
举例	ISOLATE/4/FORWARDING_FAILURE_OCCURRED: -MDC=1-Chassis=1-Slot=2; Forwarding failure 0x10 occurred on all ports of NP 2.
日志说明	当前NP芯片上所有数据端口出现转发故障
处理建议	• 对于 0x10 类型的故障，请先确保本机框内的网板处于正常运行状态。如果本机框内的网板处于正常运行状态，但故障未恢复，请联系技术支持 • 对于其他类型的故障，请直接联系技术支持

141.2 FORWARDING_FAILURE_RECOVERED

日志内容	Forwarding failure has been cleared on all ports of NP [UINT16].
参数解释	$1：NP芯片号
日志等级	5
举例	ISOLATE/5/FORWARDING_FAILURE_RECOVERED: -MDC=1-Chassis=1-Slot=2; Forwarding failure has been cleared on all ports of NP 2.
日志说明	当前NP芯片上所有数据端口的转发故障已解除
处理建议	无

142 DMON

142.1 INTERFACE_DOWN

日志内容	[STRING] went down. Reason: [STRING].
参数解释	$1：接口名称 $2：接口处于DOWN状态的原因，取值如下： o Interface being powered up：接口正在处于上电状态，暂时无法正常工作 o Interface has been shut down by using the **shutdown** command：接口已经通过 **shutdown** 命令被关闭 o Interface MAC exception：MAC 硬件异常 o Interface physical exception：接口物理芯片处于异常状态 o Interface transceiver module exception：接口光模块读写寄存器数值时，出现异常 o Invalid interface configuration：接口配置信息无效 o MAC became down. Probably because of local fault：MAC 芯片处于 DOWN 状态，可能是本端故障 o MAC became down. Probably because of remote fault：MAC 芯片处于 DOWN 状态，可能是远端故障 o Operating mode has been changed：接口工作模式发生变化 o Physical status became down. Probably because of link fault：接口物理芯片处于 DOWN 状态，可能因为没有物理连线或者线路故障 o Rx loss of signal occurred on the transceiver module：光模块收光侧信号丢失 o SDH AU-AIS alarm occurred：接口出现 AU-AIS（Administration Unit Alarm Indication Signal，管理单元告警指示信号）告警 o SDH LOF alarm occurred：接口出现 LOF（Loss Of Frame，帧丢失）告警 o SDH LOP alarm occurred：接口出现 LOP（Loss Of Pointer，指针丢失）告警 o SDH LOS alarm occurred：接口出现 LOS（Loss Of Signal，接收端收不到发送端传过来的信号）告警 o SDH MS-AIS alarm occurred：接口出现 MS-AIS（Mutiplex Section-Alarm Indication Signal，复用段告警指示信号）告警 o SDH MS-RDI alarm occurred：接口出现 MS_RDI（Multiplex Section-Remote Defect Indication，复用段远端缺陷指示）告警 o SDH SDBER alarm occurred：接口出现 SD（Signal Degrade，信号衰减）告警 o SDH SFBER alarm occurred：接口出现 SF（Signal Fail，信号失败）告警 o SDH TU-AIS alarm occurred：接口出现 TU-AIS（Tributary Unit Alarm Indication Signal，支路单元告警指示信号）告警 o Subcard is absent：接口子卡不在位 o Transceiver module is absent：光模块不在位
日志等级	5
举例	DMON/5/INTERFACE_DOWN: -Chassis=1-Slot=2; GE1/2/0/1 went down. Reason: Interface has been shut down by using the shutdown command.
日志说明	接口处于DOWN状态的原因
处理建议	**1.** 如果接口已经通过 **shutdown** 命令被关闭，请使用 **undo shutdown** 命令进行恢复

2. 如果接口工作模式发生变化，请根据实际业务情况，使用 **port link-mode** 命令进行工作模式切换
3. 请检查光功率，调至正常范围
4. 请检查物理链路连接情况
5. 请重新插入光模块
6. 请更换光模块
7. 请重新插入接口子卡
8. 请更换单板
9. 请收集告警信息，联系新华三技术支持工程师

142.2 INTERFACE_UP

日志内容	[STRING] came up. Reason: [STRING].
参数解释	$1：接口名称 $2：接口已恢复至UP状态的原因，取值如下： o Interface has been brought up by using the **undo shutdown** command：接口已经通过 **undo shutdown** 命令进行恢复 o MAC became up because local fault was removed：MAC 芯片已恢复至 UP 状态，本端故障已解除 o MAC became up because remote fault was removed：MAC 芯片已恢复至 UP 状态，远端故障已解除 o Operating mode has been changed：接口工作模式发生变化 o Physical status became up：接口物理芯片已恢复至正常状态 o Rx signal loss was recovered on the transceiver module：光模块收光侧信号已恢复至正常状态 o SDH AU-AIS alarm was removed：接口已消除 AU-AIS（Administration Unit Alarm Indication Signal，管理单元告警指示信号）告警 o SDH LOF alarm was removed：接口已消除 LOF（Loss Of Frame，帧丢失）告警 o SDH LOP alarm was removed：接口已消除 LOP（Loss Of Pointer，指针丢失）告警 o SDH LOS alarm was removed：接口已消除 LOS（Loss Of Signal，接收端收不到发送端传过来的信号）告警 o SDH MS-AIS alarm was removed：接口已消除 MS-AIS（Mutiplex Section-Alarm Indication Signal，复用段告警指示信号）告警 o SDH MS-RDI alarm was removed：接口已消除 MS-RDI（Multiplex Section-Remote Defect Indication，复用段远端缺陷指示）告警 o SDH SDBER alarm was removed：接口已消除 SD（Signal Degrade，信号衰减）告警 o SDH SFBER alarm was removed：接口已消除 SF（Signal Fail，信号失败）告警 o SDH TU-AIS alarm was removed：接口已消除 TU-AIS（Tributary Unit Alarm Indication Signal，支路单元告警指示信号）告警 o Subcard is present：接口子卡已恢复至在位状态 o Transceiver module status is present：光模块已恢复至在位状态
日志等级	5
举例	DMON/5/INTERFACE_UP: -Chassis=1-Slot=2; GE1/2/0/1 came up. Reason: Interface has been brought up by using the undo shutdown command.
日志说明	接口已恢复至UP状态的原因
处理建议	无