# 1 通信链路

## MMS通信链路

|  |  |
| --- | --- |
| **需求** | MMS通信链路分类 |
| **编号** | D1 |
| **输入** | 1. 采集报文 |
| **处理逻辑** | 1. 在TCP报文中，按不区分次序的源和目的IP地址，以及IP协议是0x6进行链路分类 2. 在步骤1中，按不区分次序的源和目的TCP端口进行TCP连接分类 |
| **输出** | 1. MMS通信链路和该链路所包含TCP连接 |
| **说明** | 1. 报文结构参考附录D 2. 不区分次序的源和目的IP地址的举例：源地址10.1.1.1和目的地址10.1.1.2的报文与源地址10.1.1.2和目的地址10.1.1.1的报文分为一类 3. 不区分次序的源和目的TCP端口的举例：源端口12345和目的端口1234的报文与源端口1234和目的端口12345的报文分为一类 |
| **备注** | 实时 |

## SV通信链路

|  |  |
| --- | --- |
| **需求** | SV通信链路分类 |
| **编号** |  |
| **输入** | 1. 采集报文 |
| **处理逻辑** | 1. 相同APPID的报文分类为同一SV通信链路 2. 为每个报文进行当前时间标记，时间精度是1us |
| **输出** | 1. SV通信链路 |
| **说明** | 1. 报文结构参考附录E |
| **备注** | 实时 |

## GOOSE通信链路

|  |  |
| --- | --- |
| **需求** | GOOSE通信链路分类 |
| **编号** |  |
| **输入** | 1. 采集报文 |
| **处理逻辑** | 1. 相同APPID的报文分类为同一GOOSE通信链路 2. 为每个报文进行当前时间标记，时间精度是1us |
| **输出** | 1. GOOSE通信链路 |
| **说明** | 1. 报文结构参考附录F |
| **备注** | 实时 |

# MMS协议解析

## 2.1 MMS状态

### 2.1.1 TCP通信状态

|  |  |
| --- | --- |
| **需求** | TCP通信状态 |
| **编号** |  |
| **输入** | 1. 全部MMS通信链路的全部TCP连接的报文 |
| **处理逻辑** | 1. 各TCP连接在设定时间内未出现TCP头中未设置push标识的报文则异常，否则正常。默认设定时间：120S 2. 各MMS通信链路的TCP连接中，同一端口所建立的连接数大于或等于阈值则异常，否则正常，默认阈值：3 |
| **输出** | 1. MMS通信链路的该TCP连接通信超时消息 2. MMS通信链路的该端口TCP连接数超限消息 |
| **说明** | 1. 报文结构参考附录D |
| **备注** | 实时 |

## 2.2 MMS统计

### 2.2.1 TCP连接

|  |  |
| --- | --- |
| **需求** | TCP连接 |
| **编号** |  |
| **输入** | 1. 全部MMS通信链路的全部TCP连接 2. 指定统计周期 |
| **处理逻辑** | 1. 统计指定周期内已建立而未结束的TCP连接数量 2. 统计指定周期内由服务器端发起的的结束TCP连接的数量 3. 统计指定周期内由客户端发起的的结束TCP连接的数量 |
| **输出** | 1. 该统计周期内的TCP连接数量 |
| **说明** | 1. 报文结构参考附录D 2. 建立TCP连接是根据报文TCP头的标识信息，3次交互则创建完成，3次交互依序是syn->syn->acknowledgment，其中第一次syn的发起端是客户端 3. 结束TCP连接是根据报文TCP头的标识信息，4次交互则创建完成，4次交互依序是fin->acknowledgment->fin->acknowledgment，其中第一次fin是结束该TCP连接的发起端 |
| **备注** | 离线 |

### 2.2.2 MMS性能

|  |  |
| --- | --- |
| **需求** | MMS性能 |
| **编号** |  |
| **输入** | 1. 指定MMS通信链路的全部TCP连接 2. 指定统计周期 |
| **处理逻辑** | 1. 统计指定周期和指定MMS通信链路中所有设置push标识的TCP报文帧数 2. 统计指定周期和指定MMS通信链路中全部设置push标识的TCP报文数据净荷字节数 3. 统计指定周期和指定MMS通信链路中所有由客户端发送设置push标识的TCP报文帧数 4. 统计指定周期和指定MMS通信链路中所有由客户端发送设置push标识的TCP报文据净荷字节数 5. 统计指定周期和指定MMS通信链路中所有由服务器端发送设置push标识的TCP报文帧数 6. 统计指定周期和指定MMS通信链路中所有由服务器端发送设置push标识的TCP报文据净荷字节数 |
| **输出** | 1. 该统计周期和MMS通信链路中的MMS帧数 2. 该统计周期和MMS通信链路中的MMS字节数 3. 该统计周期和MMS通信链路中的客户端发送MMS帧数 4. 该统计周期和MMS通信链路中的客户端发送MMS字节数 5. 该统计周期和MMS通信链路中的服务器端MMS帧数 6. 该统计周期和MMS通信链路中的服务器端MMS字节数 |
| **说明** | 1. 报文结构参考附录D 2. 建立TCP连接是根据报文TCP头的标识信息，3次交互则创建完成，3次交互依序是syn->syn->acknowledgment，其中第一次syn的发起端是客户端 |
| **备注** | 离线 |

# SV协议解析

## SV状态

### SV通信状态

|  |  |
| --- | --- |
| **需求** | SV通信状态 |
| **编号** |  |
| **输入** | 1. 全部SV通信链路 |
| **处理逻辑** | 1. 各SV通信链路在设定时间内未监测到报文则异常，否则正常。默认设定时间：1S |
| **输出** | 1. 该SV通信链路通信中断消息 |
| **说明** | 1. 报文结构参考附录E |
| **备注** | 实时 |

## SV统计

### SV性能

|  |  |
| --- | --- |
| **需求** | SV性能 |
| **编号** |  |
| **输入** | 1. 指定SV通信链路 2. 指定统计周期 |
| **处理逻辑** | 1. 统计指定周期和指定SV通信链路中所有报文帧数 2. 统计指定周期和指定SV通信链路中所有报文净荷字节数 3. 统计指定周期和指定SV通信链路中报文SV数据长度错误，APDU标识错误作为SV报文结构错误 |
| **输出** | 1. 该统计周期和SV通信链路中的SV帧数 2. 该统计周期和SV通信链路中的SV字节数 3. 该统计周期和SV通信链路中的SV结构错误报文帧数 |
| **说明** | 1. 报文结构参考附录E |
| **备注** | 离线 |

# GOOSE协议解析

## GOOSE状态

### 4.1.1 GOOSE通信状态

|  |  |
| --- | --- |
| **需求** | GOOSE通信状态 |
| **编号** |  |
| **输入** | 1. 全部GOOSE通信链路 |
| **处理逻辑** | 1. 各GOOSE通信链路在设定时间内未监测到报文则异常，否则正常。默认设定时间：4\*maxTime，maxTime由SCD文件定义，一般是5000ms |
| **输出** | 1. 该GOOSE通信链路通信中断消息 |
| **说明** | 1. 报文结构参考附录F |
| **备注** | 实时 |

## 4.2 GOOSE性能

### 4.2.1 GOOSE性能

|  |  |
| --- | --- |
| **需求** | GOOSE性能 |
| **编号** |  |
| **输入** | 1. 指定GOOSE通信链路 2. 指定统计周期 |
| **处理逻辑** | 1. 统计指定周期和指定GOOSE通信链路中所有报文帧数 2. 统计指定周期和指定GOOSE通信链路中所有报文净荷字节数 3. 统计指定周期和指定GOOSE通信链路中报文GOOSE数据长度错误，APDU标识错误作为GOOSE报文结构错误 |
| **输出** | 1. 该统计周期和GOOSE通信链路中的GOOSE帧数 2. 该统计周期和GOOSE通信链路中的GOOSE字节数 3. 该统计周期和GOOSE通信链路中的GOOSE结构错误报文帧数 |
| **说明** | 1. 报文结构参考附录F |
| **备注** | 离线 |

# 5 网络异常监视

## 5.1 流量异常监视

|  |  |
| --- | --- |
| **需求** | 流量异常监视 |
| **编号** |  |
| **输入** | 1. 采集报文 |
| **处理逻辑** | 1. 当前一秒的流量相对上一秒突增50%或突减50% 2. 上一秒流量低于10Mbps时不进行流量异常监视 3. 初始时上一秒流量置0 |
| **输出** | 1. 流量突增或突减消息 |
| **说明** |  |
| **备注** | 实时 |

# 6 记录分析

## 6.1 过滤分析

|  |  |
| --- | --- |
| **需求** | 过滤分析 |
| **编号** |  |
| **输入** | 1. 指定GOOSE通信链路 2. 指定统计周期 |
| **处理逻辑** | 1. 统计指定周期和指定GOOSE通信链路中所有报文帧数 2. 统计指定周期和指定GOOSE通信链路中所有报文净荷字节数 3. 统计指定周期和指定GOOSE通信链路中报文GOOSE数据长度错误，APDU标识错误作为GOOSE报文结构错误 |
| **输出** | 1. 该统计周期和GOOSE通信链路中的GOOSE帧数 2. 该统计周期和GOOSE通信链路中的GOOSE字节数 3. 该统计周期和GOOSE通信链路中的GOOSE结构错误报文帧数 |
| **说明** | 1. 报文结构参考附录F |
| **备注** | 离线 |

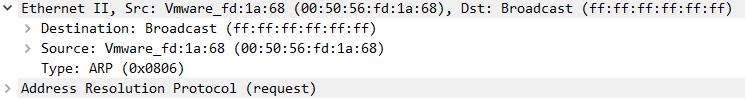
# 7 注意事项

## 7.1 镜像端口连接经验

* 1. 镜像端口连接主机时不能通过三层交换机，建议保持直连
  2. 主机网口型号和驱动及VLAN配置的不同，无法保证所采集报文完整。可能丢失VLAN信息

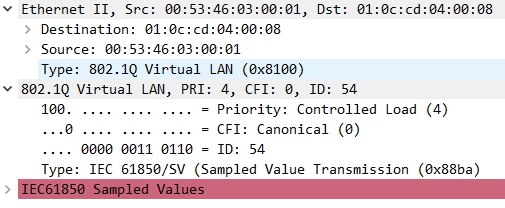
# 附录

## A以太网二层报文结构



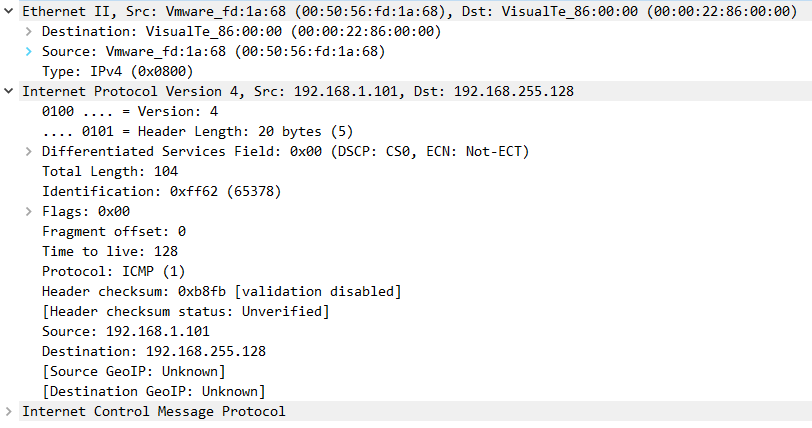
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **偏移(字节)** | **长度(字节)** | **名称** | **说明** | **备注** |
| 0 | 6 | 目的MAC地址 |  |  |
| 6 | 6 | 源MAC地址 |  |  |
| 12 | 2 | 以太网类型 |  |  |
| 14 | - | 数据 |  |  |

## B 携带VLAN以太网二层报文结构



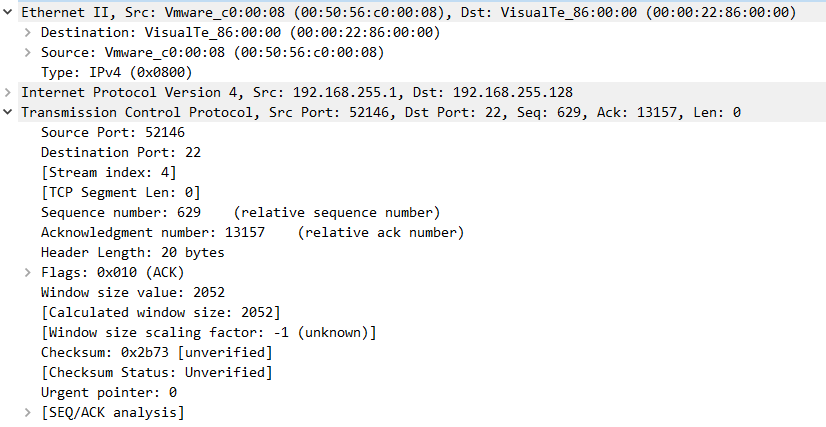
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **偏移(字节)** | **长度(字节)** | **名称** | **说明** | **备注** |
| 0 | 6 | 目的MAC地址 |  |  |
| 6 | 6 | 源MAC地址 |  |  |
| 12 | 2 | 以太网类型1 | 0x8100 |  |
| 14 | 2 | VLAN |  | 2字节共16位：0~2位是VLAN优先级；3位是CFI；4~15位是VLAN ID |
| 16 | 2 | 以太网类型2 |  |  |
| 18 | - | 数据 |  |  |

## C IP报文结构



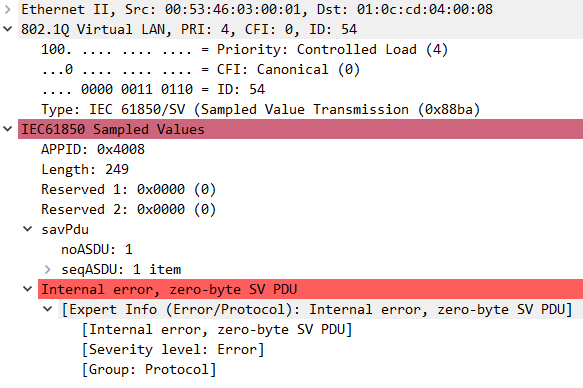
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **偏移(字节)** | **长度(字节)** | **名称** | **说明** | **备注** |
| - | 14或18 | 二层报文帧头 | 参考附录A或B | 以太网类型或以太网类型2是0x0800 |
| 0 | 20 | IP头 | 0字节是版本及IP头长度，IP头长度由4~7位决定（左移2位计算）；1字节是DSCP；2~3字节是IP报文总长度；4~5字节是标识符；6~7字节是标记和段偏移；8字节是生存时间；9字节是IP协议；10~11字节是校验和；12~15是源IP地址；16~19是目的IP地址 |  |
| 20 | - | 数据 |  |  |

## D TCP报文结构



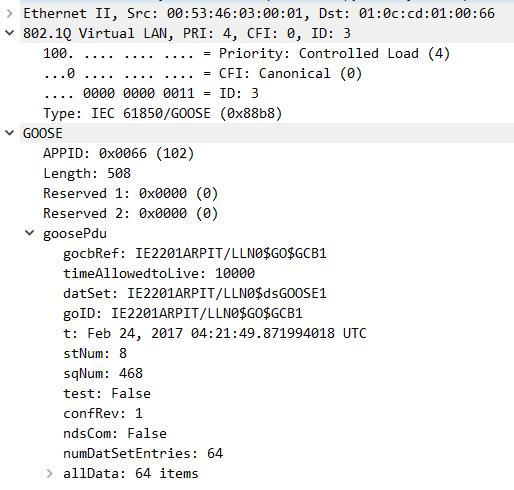
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **偏移(字节)** | **长度(字节)** | **名称** | **说明** | **备注** |
| - | 14或18 | 二层报文帧头 | 参考附录A或B | 以太网类型或以太网类型2是0x0800 |
| - | 20 | IP头 | 参考附录C | IP协议是0x6 |
| 0 | - | TCP头 | 0~1字节是源端口；2~3字节是目的端口；4~7字节是序号；8~11字节是确认序号；12~13字节是TCP头长度和标记；14~15字节是窗口尺寸；16~17字节是校验和；18~19字节是紧急指针;20~?字节是option，由12字节0~3位决定（左移2位计算） | 12~13字节共16位： 第9位是ECN-echo；第10位是urgent；第11位是Acknowledgment；第12位是push；第13位是Reset；第14位是Syn；第15位是FIN |
| 20 | - | 数据 |  |  |

## E SV报文结构(IEC61850-9-2)



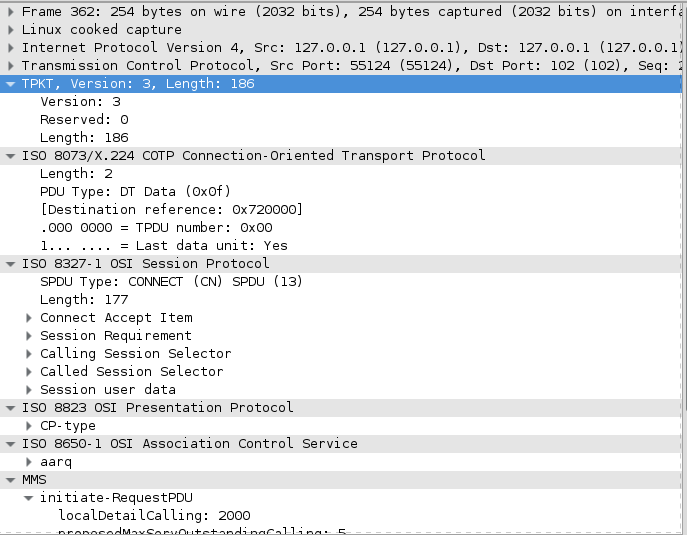
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **偏移(字节)** | **长度(字节)** | **名称** | **说明** | **备注** |
| - | 14或18 | 二层报文帧头 | 参考附录A或B | 以太网类型或以太网类型2是0x88BA |
| 0 | 2 | APPID | 0x4000~0x7FFF |  |
| 2 | 2 | SV数据长度 |  |  |
| 4 | 4 | 保留 | 0x0 |  |
| 8 | 1 | APDU标识 | 0x60 |  |
| 9 | 1 | APDU长度 |  |
| 10 | 1 | ASDU数目标识 | 0x80 | ASDU数目值长度由ASDU数目长度决定 |
| - | 1 | ASDU数目长度 |  |
| - | - | ASDU数目值 |  |
| - | 1 | ASDU序列标识 | 0xA2 |  |
| - | 1 | ASDU序列长度 |  |
| - | 1 | ASDU标识 | 0x30 |  |
| - | 1 | ASDU长度 |  |
| - | 1 | ASDU pad标识 |  | pad值长度由pad长度决定 |
| - | 1 | ASDU pad长度 |  |
| - | - | ASDU pad值 |  |
| - | - | 更多的ASDU pad |  | 数值字段是big endian，x86体系处理前需转换为little endian |

## F GOOSE报文结构



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **偏移(字节)** | **长度(字节)** | **名称** | **说明** | **备注** |
| - | 14或18 | 二层报文帧头 | 参考附录A或B | 以太网类型或以太网类型2是0x88B8 |
| 0 | 2 | APPID | 0x0000~0x3FFF |  |
| 2 | 2 | GOOSE数据长度 |  |  |
| 4 | 4 | 保留 | 0x0 |  |
| 8 | 1 | APDU标识 | 0x61 |  |
| - | - | APDU长度 |  | 字段第一字节的0位是0，指该字段为APDU的长度值；否则1~7位表示APDU长度值使用的字节数 |
| - | - | APDU长度值（option） |  | 由APDU长度决定 |
| - | 1或2 | ASDU pad标识 |  |  |
| - | - | ASDU pad长度 |  |  |
| - | - | ASDU pad值 |  | 由pad长度决定 |
| - | - | 更多的ASDU pad |  | 数值字段是big endian，x86体系处理前需转换为little endian |

## G MMS报文结构



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **偏移(字节)** | **长度(字节)** | **名称** | **说明** | **备注** |
| - | 14或18 | 二层报文帧头 | 参考附录A或B | 以太网类型或以太网类型2是0x0800 |
| - | 20 | IP头 | 参考附录C | IP协议是0x6 |
| - | - | TCP头 | 参考附录D |  |
| 20 | - | 数据 |  |  |