连接跟踪针对H323在数据包被分片的情况下的处理

- **现状描述**
  - Polycom软件版发送的包进行了分片处理，经过内核连接跟踪的h323模块时，解析不完整的协议包失败，无法对父子连接进行绑定，直接放通了。
- **直接影响**
  - 应用识别模块无法正确获取父连接，子连接最终识别失败。
- **改动思路**
  - 在内核解析H323时，对不完整的包做缓存，组装成完整的包，走完helper钩子的完整流程。
- **基本组件**
  - 包缓存
  - 定时器
- **处理流程**
  - 1. 如果包是完整的
    - a. 如果该方向上没有缓存包
      - 则不需要处理，走后续发送流程
    - b. 如果该方向上有缓存包
      - 则先发送缓存包，再发送本次的包
  - 2. 如果包是不完整的
    - a. 如果TPKT头部正确，但长度不完整
      - 缓存数据包
    - b. 如果TPKT头部不正确，（不是TPKT包）
      - 如果该方向上没有缓存包
        - 则放通处理
      - 如果该方向上有缓存包
        - 则组合包并重新走包校验流程1和2
  - 3. 定时器
    - 定时时间5ms
    - 如果缓存的包隔了一定的时间未处理，则发送出去
  - 4. 包缓存
    - 存在连接跟踪上，问题：如果定时驱动发送缓存包时，如何找到连接跟踪来发送？较为麻烦
    - 使用PerCPU，分方向，只存一个缓存包
  - 5. 组合包发送考虑
    - 如果申请新的skb，这需要记录nf_hook_state，且需要重注入到nf，目前helper回调，并没有传入nf_hook_state。需要扩展连接跟踪字段，提前存好nf_hook_state
    - 直接在当前skb扩容，将缓存的包合并到当前skb上，重走包校验流程。

XMind: ZEN | 试用模式