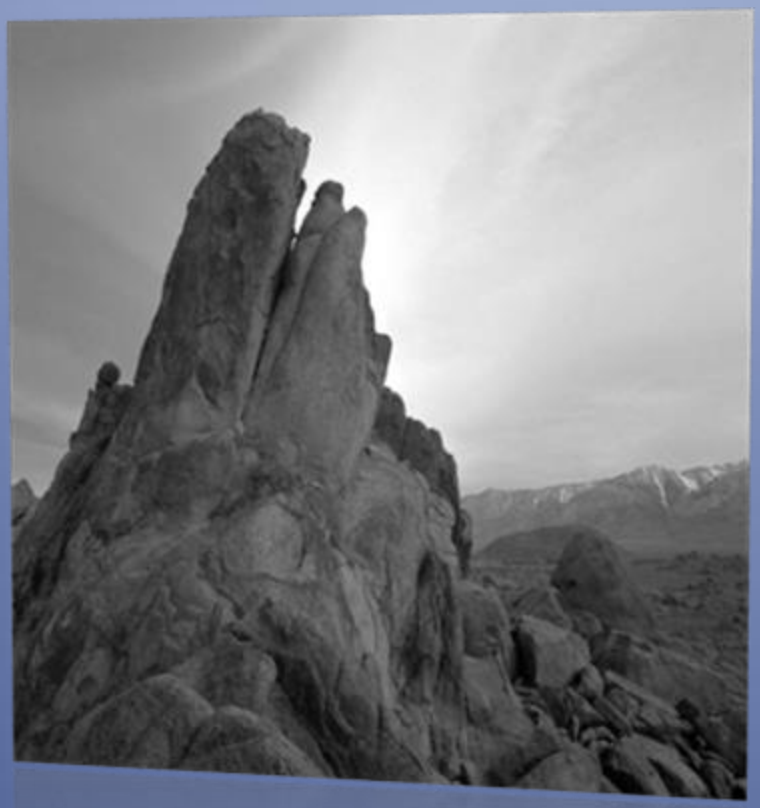


深入浅出的 GB28181

作者：DZ 先生

序言

曾经我对 GB 是个小白，后来的一次机会，我开始负责江阴市公安局的项目，那时候的我对监控是一脸懵逼的状态，随着项目烂摊子的起步，我便开始跟随着它一起茁壮成长，从第一次遇到国标，确认过眼神之后，我便开始遇见了对的人。我暗自给自己下目标一定要把国标给搞明白了，我打开万能的某宝网查询关于国标的书籍，发现除了一本《GBT 28181-2016 公共安全视频监控联网系统信息传输、交换、控制技术要求》便再无其他相关书籍。于是乎啃起了其电子版，从容易的到难的，从精简到复杂，就这样随着时间的逝去，我也逐渐的茁壮起来。最终运用国标知识，一次又一次的解决疑难杂症，建立起了强而稳定的监控系统平台。我曾对江阴市公安局 X 大队长夸下海口，我跟他说“如果哪天我离开这里了，一定会给你留下一个强壮而稳定的监控系统”，自豪的是我做到了。

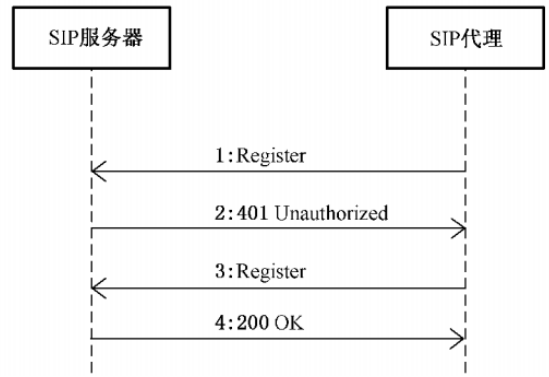
要想坚持的做一件事情，一个人肯定是很难做到的，我很幸运我遇到一群志同道合的朋友，在这里我要感谢他们（海康，大华，宇视，科达，深醒，大为，天行），感谢他们的支持和协同作战，最最要感谢的是一个叫金师傅的同志，没有他就没有如此多的案例，可以说他为整个监控系统奉献了自己的青春。也是他让我坚持完成了自己的作品。也是他帮我不断帮我不断宣传，圈粉，我才有了动力完成此书。

最后希望此书籍能够给更多从事监控系统的朋友们带来帮助，也真心的希望你们也能遇到这样的一起携手作战的朋友们。

目录

第一章 国标精选流程

1. 注册（IPC-平台）



国标注册消息流程详解

Step.1:

IPC（SIP 代理）向 SIP 服务器（中心服务器）发送 Register 注册消息

Step.2:

SIP 服务器 检查 IPC 带来信令中的 Authorization 字段（鉴权字段），发现 Register 信令中未带鉴权字段。回复 IPC：401 Unauthorized（注册未带鉴权）。注意，这不是异常报错，这是国标注册中的正常流程。

Step.3:

IPC 重新向 SIP 服务器发送 Register 注册消息，并带上鉴权字段（Register With Authorized）

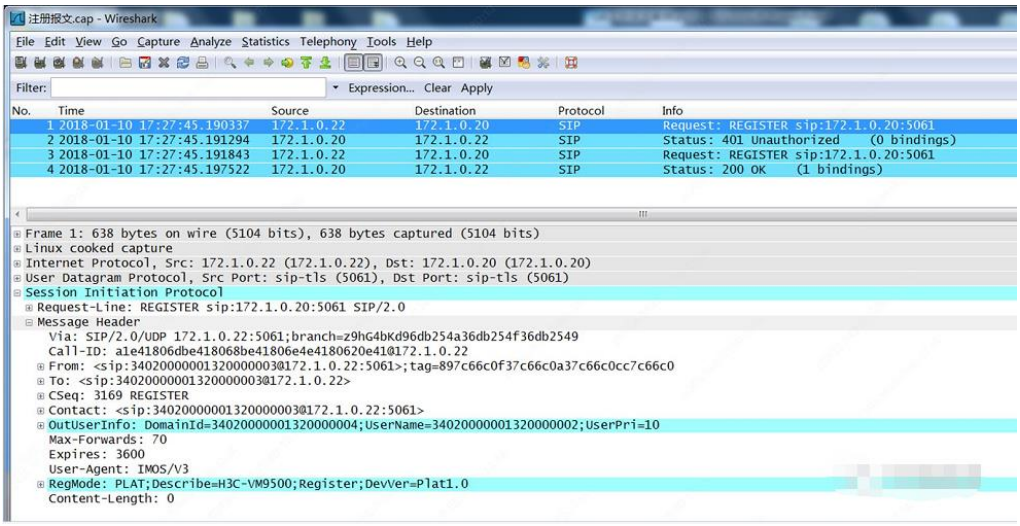
Step.4:

SIP 服务器 检查 Authorization 字段，如果该鉴权通过，则回复 200OK，设备在线。

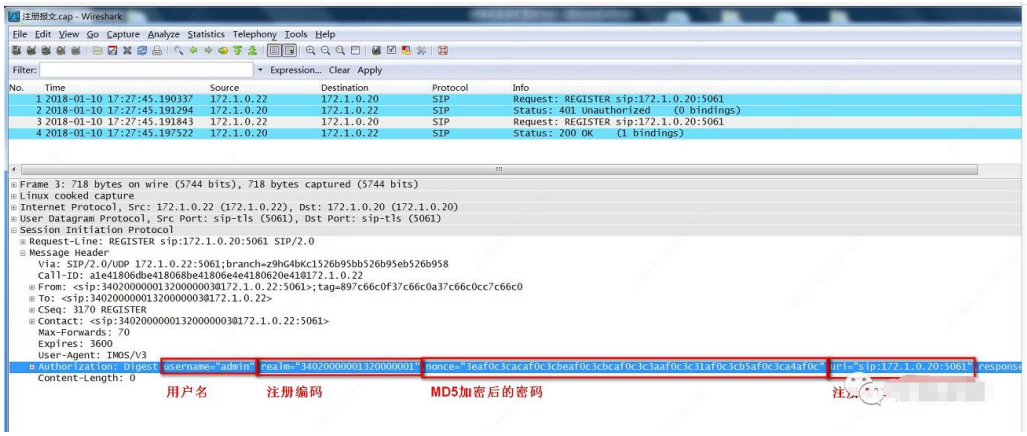
案例分析

No.	Time	Source	Destination	Protocol	Info
1	2018-01-10 17:27:45.190337	172.1.0.22	172.1.0.20	SIP	Request: REGISTER sip:172.1.0.20:5061
2	2018-01-10 17:27:45.191294	172.1.0.20	172.1.0.22	SIP	Status: 401 Unauthorized (0 bindings)
3	2018-01-10 17:27:45.191843	172.1.0.22	172.1.0.20	SIP	Request: REGISTER sip:172.1.0.20:5061
4	2018-01-10 17:27:45.197522	172.1.0.20	172.1.0.22	SIP	Status: 200 OK (1 bindings)

这是一个 22 下级域向 20 上级域注册的完整报文。小伙伴们可以参考上一页的流程来对照一下。



第一个注册信息：22 平台向 20 发送注册 Register 消息，没有带鉴权字段，20 平台收到后，比对鉴权字段发现异常，回复 401 Unauthorized，告诉下级域：你没有带鉴权消息哦！



第二个注册信息：可以看到我们第二次发送 Register 消息，带了鉴权字段，20 平台收到鉴权后，和数据库中的鉴权比对正确。OK，注册成功！ 我们可以看到这个鉴权字段包含：1.用户名 2.注册编码 3.MD5 加密的密码密文 4.注册端口的 URL 链接 等

知识拓展

我们观察到，注册消息里面有个 Expires 字段，这个字段为 3600 代表注册，字段为 0 则代表注销。

2. 保活（IPC-平台）

命令流程

国标保活消息流程详解

Step.1:

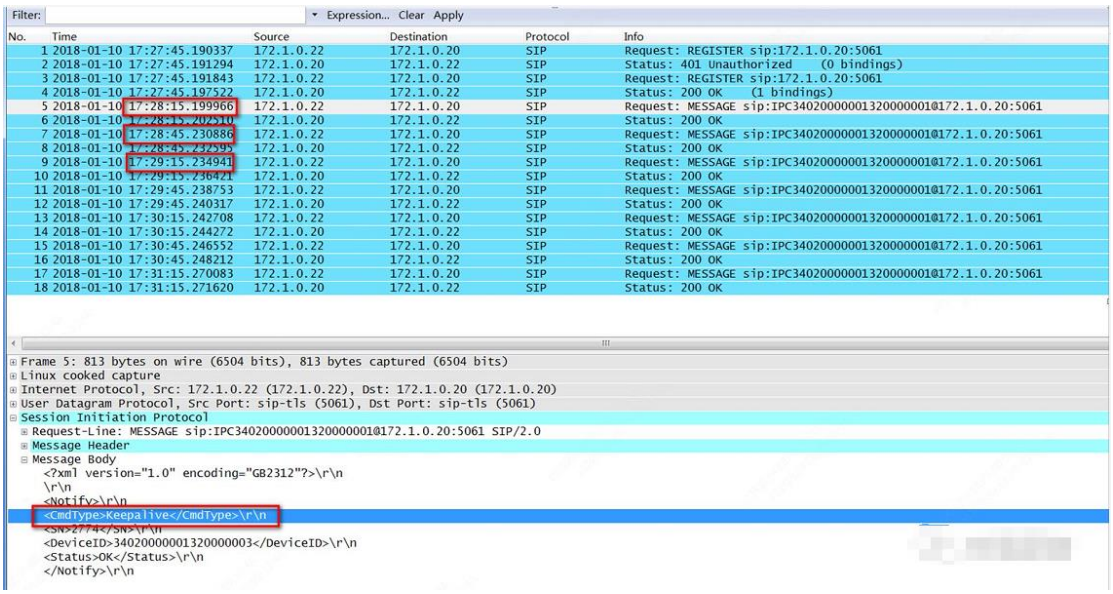
IPC（注册端）向平台（服务端）发送 MESSAGE 消息（30 秒一次），告知平台目前自身设备在平台上在线。

Step.2:

平台接收到 IPC 发来的保活消息，回复 200OK，表示收到。

注意：如果平台连续 3 次 MESSAGE 保活周期内（90 秒）没有收到保活消息，则平台认为设备离线。

实例分析



22 下级域在 20 上级域上注册成功后，22 下级域主动发送 MESSAGE 消息，平台收到消息后，回复 200OK。可以看到我们的保活消息有如下特点：

1.Cmdtype（命令类型）字段里面带的是 Keepalive(保活)；

2.每隔 30 秒发送一次；需要仔细分辨清楚哦。

3. 实况

命令流程

国标实况流程：

Step.1:

SIP 服务器发送 INVITE 消息到 XP，XP 返回 200 OK 并携带有 SDP1 字段，SIP 服务器再发送 INVITE 消息到 IPC 并携带有 SDP 消息，SDP 消息中含有收流者地址、收流者端口。

Step.2:

IPC 答复 200 OK，并携带有 SDP2 字段，SIP 答复 ACK 到 XP 也携带有 SDP2 字段，SDP 消息中含有发流者地址、发流者端口。在相机答复 200 OK 前，也可能答复 100trying。

Step.3:

SIP 答复 ACK 到 IPC，告知相机协商 ok，此后相机开始发流到 XP。

Step.4:

相机开始发流到 XP，发流需要遵循 SDP1 以及 SDP2 消息协商的 IP、端口；并且需要是国标规定是 RTP/PS 流。

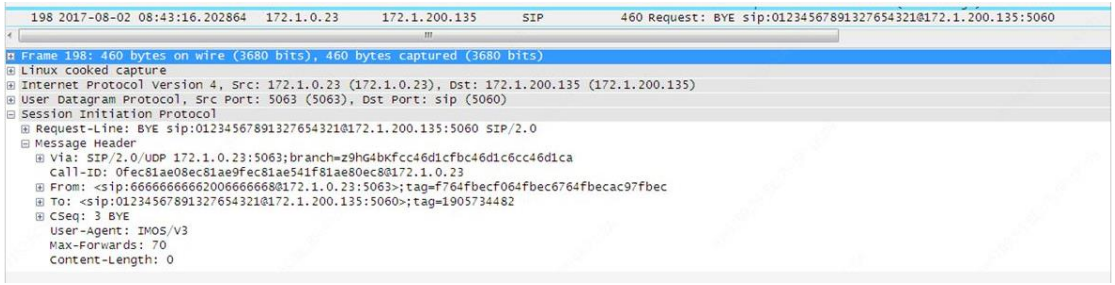
Step.5:

SIP 先发送 BYE 消息给 XP，再发送 BYE 消息到 IPC，拆除掉建立的监控关系，同时发流设备停止发流。

实例分析：

INVITE 消息中的 SDP 信息，描述了收流者地址和收流者端口。S 字段为 Play，代表实况请求。

200 OK 消息中的 SDP 消息，描述了发流者地址和发流者端口。另外 SDP 消息中的 S 字段、Y 字段，都需与 INVITE 中的相同。



发送了 BYE 消息，拆除监控关系，停止发流。

补充说明

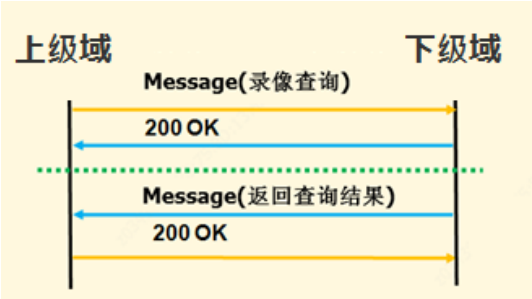
1、Y 字段的第一位为 0 代表实况，为 1 代表回放。

2、实况流程报文中的 Message Header 中的 Call-id，用于标识一个特定邀请以及与这个邀请相关的所有后续事务（即标识一个会话）。简单来说一个实况流程中的消息的 Call-id 都是要相同的，所以就可以通过 Call-id 来过滤出同一实况流程的报文。

注意：实况业务需要保活，同一个实况流程中的保活报文的 Call-id 也相同的。

4. 录像检索

国标录像检索流程图：

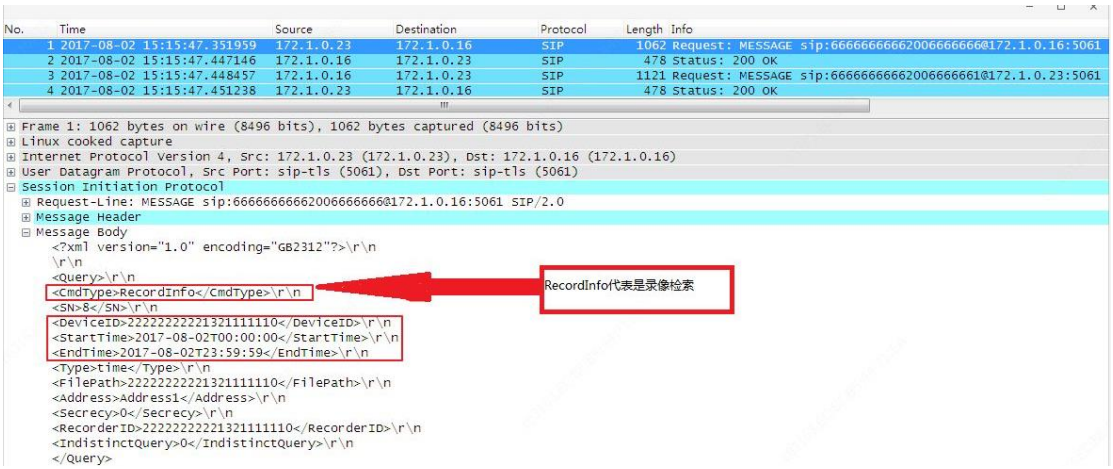


录像检索是国标外域对接后，上级域去查询下级域的录像，下级域把录像查询的结果上报给上级域，在上级域显示出录像的时间范围。录像检索是在上级域实现录像播放的前提条件。

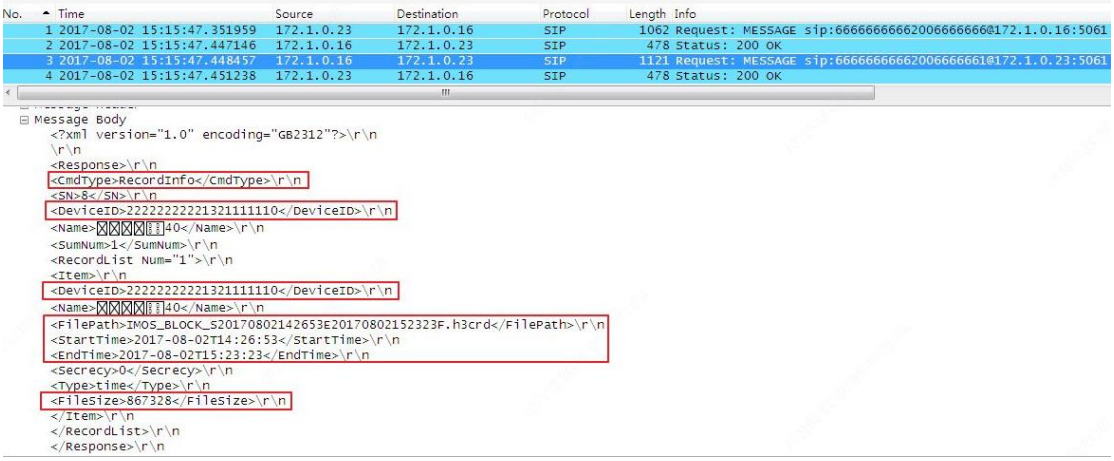
录像检索的信令流程描述：

Step.1:
目录检索方向目录拥有方发送目录查询请求 Message 消息，消息体中包含视音频文件检索条件。
Step.2:
目录拥有方向目录检索方发送 200 OK，无消息体。
Step.3:
目录拥有方向目录检索方发送查询结果，消息体中含文件目录，当一条 Message 消息无法传送完所有查询结果时，采用多条消息传送。
Step.4:
目录检索方向目录拥有方发送 200OK，无消息体。

实例分析
本例中 172.1.0.23 是上级域，172.1.0.16 下给域



首先，上级域发送 MESSAGE 消息，CmdType 字段是 RecordInfo 代表是录像检索，DeviceID 字段代表了要查询的设备的编码，StartTime 和 EndTime 字段分别代表了查询的开始时间和结束时间。随后下级域答复 200 OK，表示收到了这条录像查询的 MESSAGE 消息。



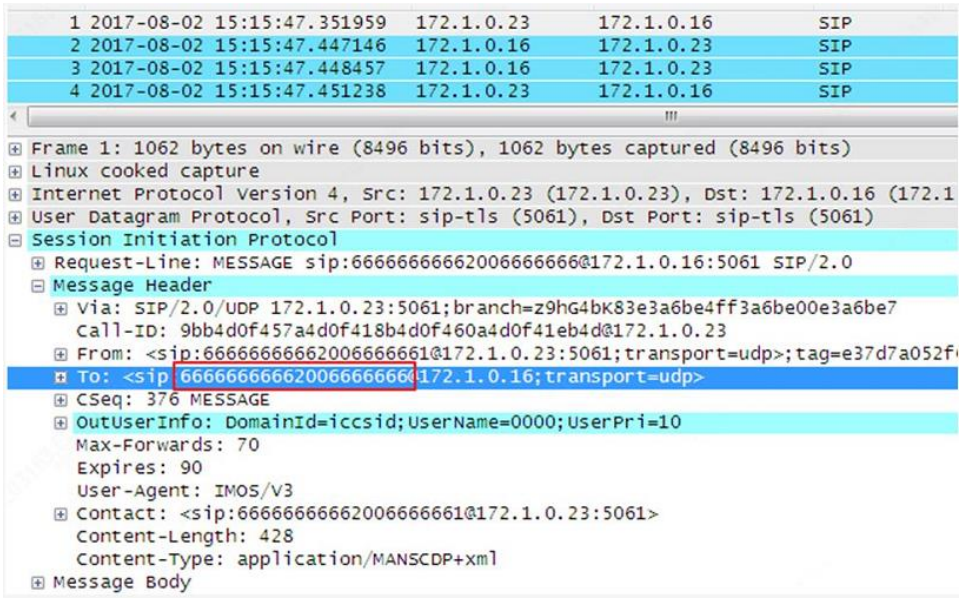
然后下级域向上级域发送查询结果，也是使用 MESSAGE 消息，其中 CmdType 字段是 RecordInfo 代表是录像检索，DeviceID 为查询的设备的编码，FilePath 表示文件路径名，StartTime 和 EndTime 表示查询到的录像的开始、结束时间，FileSize 代表查询到的录像文件的文件大小。随后上级域也答复了 200 OK，表示收到了这条查询结果的 MESSAGE 消息。

补充说明

1、目录查询请求中的 IndistinctQuery 字段代表模糊查询，缺省为 0。

值为 0 时：不进行模糊查询。此时根据 SIP 消息中 To 头域 URI 中的 ID 值确定查询录像位置，若 ID 值为本域系统 ID 则进行中心历史记录检索，若为前端设备 ID 则进行前端设备历史记录检索。

如下图中的 TO 头域的 URI 的 ID 值为域编码，所以本例是中心历史记录查询。



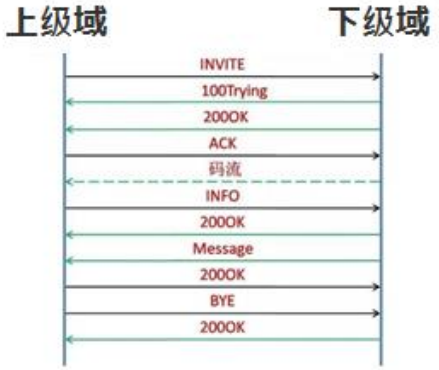
值为 1 时：进行模糊查询。此时设备所在域应同时进行中心检索（本域的录像）和前端检索（存储在前端的录像）并将结果统一返回。

2、FileSize 字段国标规定是可选字段。

3、目录查询结果响应 message Body 体中一定要有 RecordList 字段，否则对目录查询结果报错。

5. 国标域间回放、跳转流程

命令流程



Step1：首先上级域平台通过发送 INVITE 告诉下级域平台它需要看的录像的时间段、接收录像的地址和端口等信息；

Step2：下级平台收到 INVITE 之后，会先回复 100Trying，然后再回复 200OK，告诉上级域发送的录像的时间段、发送录像的地址和端口等信息；

Step3：上级域收到 200OK 后，会通过 ACK 信令告诉下级域我准备好了可以开始发流了，然后下级域就开始了发流过程；

Step4：在上级域看录像的时候，上级域如果做了暂停、快进、快退、拖动鼠标在进度条上移动等操作，那么上级域都会发送 INFO 信令告诉下级域它要做的一些操作（一条 INFO 信令对应一个操作）；

Step5:下级域收到上级域发送的 INFO 之后，会根据上级域的要求回复 200OK；

Step6：在录像放完的时候，下级域会发送 MESSAGE 消息告诉上级域录像已经放完了，可以结束了；

Step7:上级域收到 MESSAGE 信令后，先回复 200OK 表示知道了，然后再发送 BYE 消息告诉下级域我断开连接了；

Step8:下级域收到上级域的 BYE 消息之后，也会回复 200OK 表示知道了，至此回放结束。

案例分析

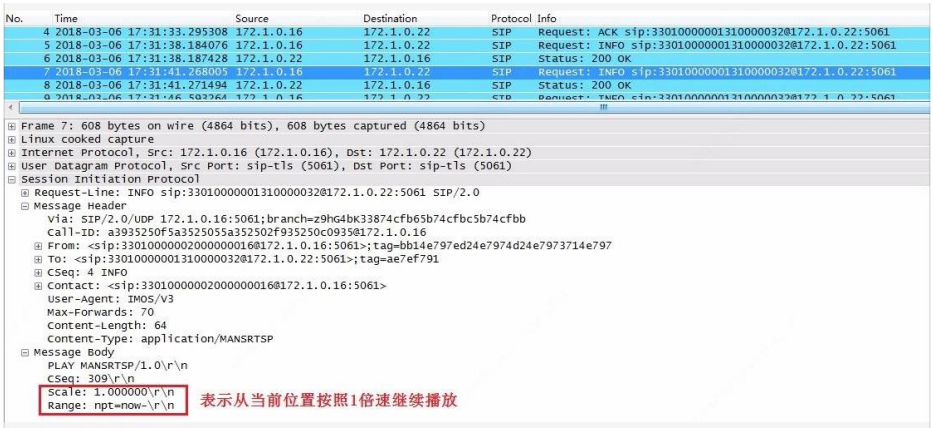
Step1：如下图，首先可以从上级域（172.1.0.16）发送给下级域（172.1.0.22）的 INVITE 消息里面看到有 s 字段是 Playback，这个 Playback 字段就表示请求的是录像回放；在 INVITE 消息中还携带了 Subject 字段，Subject 字段里面包含视频源 ID（此处表示的是要看录像的相机）和媒体流接收者 ID（此处是上级平台中心服务器 ID），o 字段表示媒体流接收者的地址（此处是 PC 电脑地址），t 字段表示要回放的录像的时间段，m 字段里面携带了媒体流接收端口，y 字段用来作为 SSRC 标识字段使用，需要下级域回复的报文也携带这个字段。

Step2:如下图，下级域回复的 200OK 中携带了媒体流发送地址和发送端口，回放的录像时间段（要和请求的时间段保持一致），y 字段（SSRC 值需要和请求时的 SSRC 值一样）

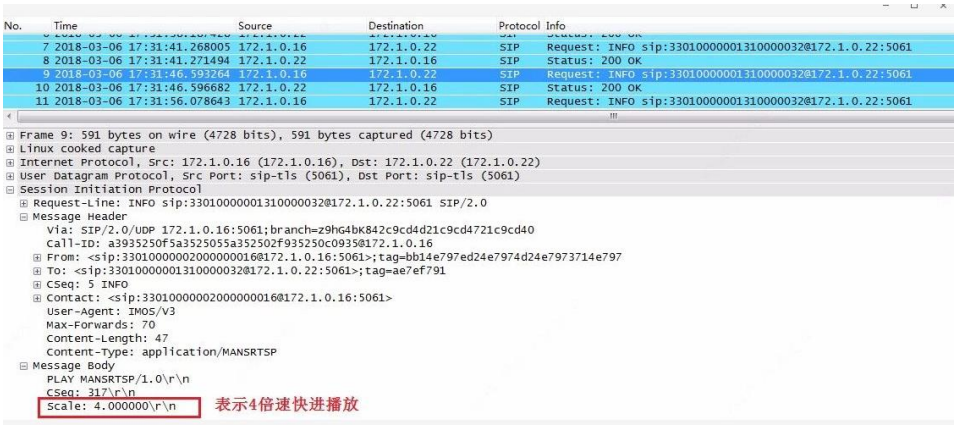
Step3: 录像播放开始之后，上级域会做一些操作，不同的操作发送的 INFO 消息里面会携带不同的字段，见下文描述。

1） 先暂停，字段 PauseTime 表示暂停，参数 now 代表从当前时间点暂停；

2） 然后继续播放，Scale 表示播放倍速，Range 为 now 表示从当前时间点开始播放。注意：如果没有 Scale 字段，那么默认是按照之前的倍速继续播放。



3） 接着 4 倍速快进播放



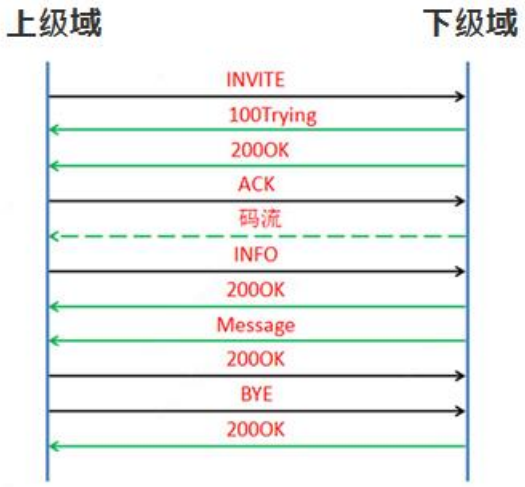
4） 最后再拖动鼠标跳转到 394 秒之后，Range 为 394 代表录像从第 394 秒开始播放。

注意：如果没有 Scale 字段，那么默认是按照之前的倍速继续播放。

Step4：录像播放完之后，下级域会发送 MESSAGE 信令告诉上级域历史媒体流发送完了，可以结束播放了。MESSAGE 字段里面 Mediastatus 字段表示媒体通知消息，DeviceID 表示媒体流发送设备的 ID（此处是相机 ID），NotifyType 表示通知的事件类型，参数为 121 代表历史媒体文件发送结束，即发流结束。随后上级域发送 BYE，整个回放流程结束。

6. 国标下载流程

命令流程



Step1: 首先上级域平台通过发送 INVITE 告诉下级域平台它需要下载的录像的时间段、接收录像的地址和端口等信息；

Step2：下级平台收到 INVITE 之后，会先回复 100 Trying，然后再回复 200 OK，告诉上级域发送录像的地址和端口等信息；

Step3：上级域收到 200 OK 后，会通过 ACK 信令告诉下级域我准备好了可以开始发流了，然后下级域就开始了发流过程；

Step4：在上级域下载录像的时候，上级域会发送 INFO 信令告诉下级域它下载的录像速率；

Step5:下级域收到上级域发送的 INFO 之后，会根据上级域的要求回复 200 OK；

Step6：在录像下载完成的时候，下级域会发送 MESSAGE 消息告诉上级域录像已经发送完了，可以结束了；

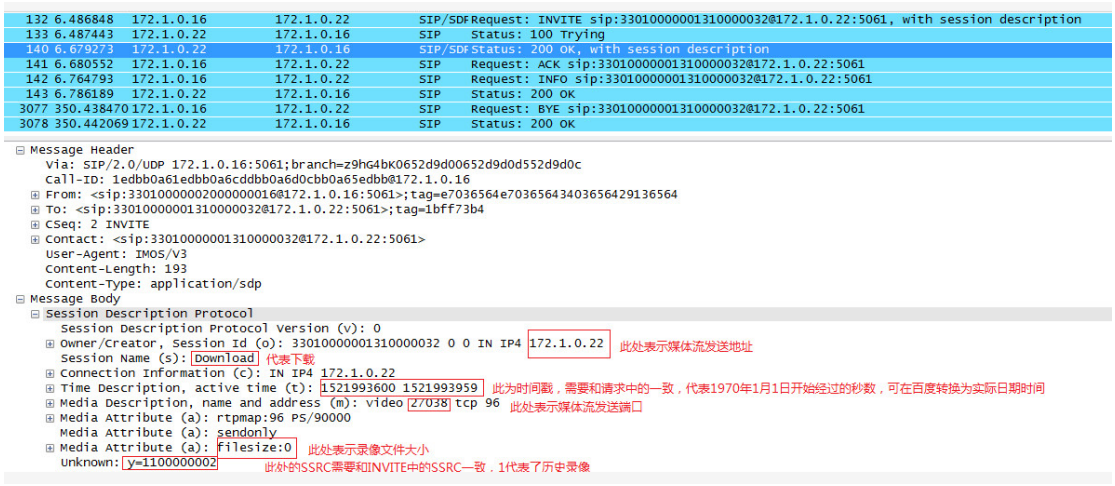
Step7:上级域收到 MESSAGE 信令后，先回复 200OK 表示知道了，然后再发送 BYE 消息告诉下级域我断开连接了；

Step8:下级域收到上级域的 BYE 消息之后，也会回复 200OK 表示知道了，至此下载结束。

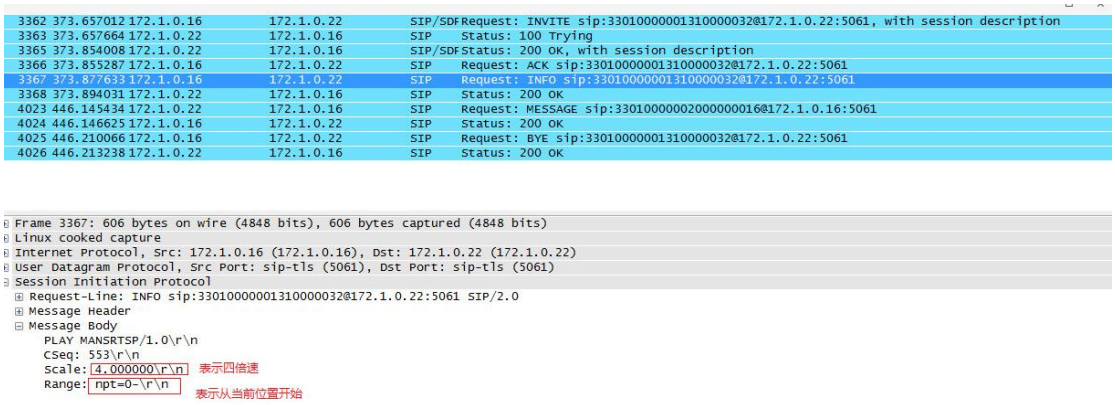
案例分析

Step1:如下图，首先可以从上级域（172.1.0.16）发送给下级域（172.1.0.22）的 INVITE 消息里面看到有 s 字段是 Download，这个 Download 字段就表示请求的是录像下载；在 INVITE 消息中还携带了 Subject 字段，Subject 字段里面包含视频源 ID（此处表示的是要下载录像的相机）和媒体流接收者 ID（此处是上级平台中心服务器 ID），c 字段表示媒体流接收者的地址（此处是媒体服务器地址），t 字段表示要下载的录像的时间段，m 字段里面携带了媒体流接收端口，y 字段用来作为 SSRC 标识字段使用，需要下级域回复的报文也携带这个字段；

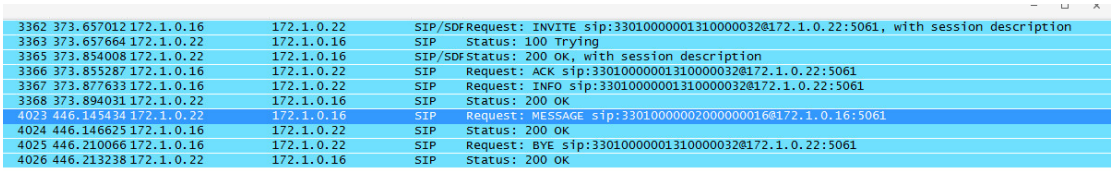
Step2:如下图，下级域回复的 200OK 中携带了媒体流发送地址和发送端口，y 字段（SSRC 值需要和请求时的 SSRC 值一样）

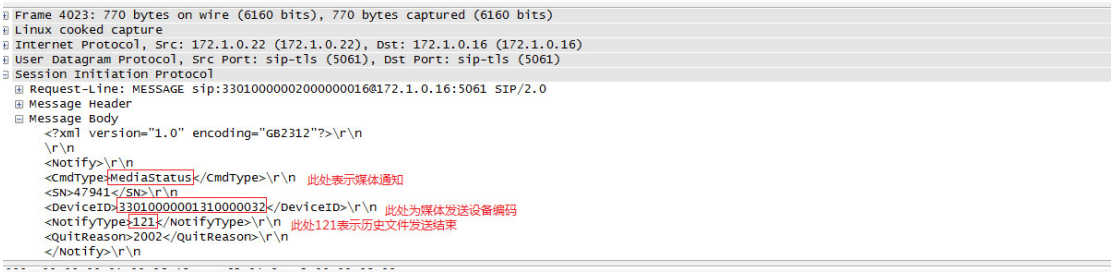


Step3: 录像下载开始之后，上级域会做一些操作，发送的 INFO 消息里面会携带一些的字段，如下图所示为四倍速下载



Step4：录像下载完之后，下级域会发送 MESSAGE 信令告诉上级域历史媒体流发送完了，可以结束播放了。MESSAGE 字段里面 Mediastatus 字段表示媒体通知消息，DeviceID 表示媒体流发送设备的 ID（此处是相机 ID），NotifyType 表示通知的事件类型，参数为 121 代表历史媒体文件发送结束，即发流结束。随后上级域发送 BYE，整个下载流程结束。

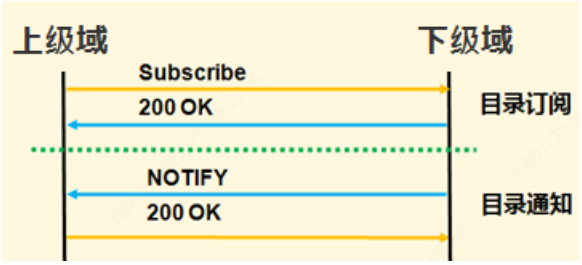




7. 目录订阅与通知

目录订阅，是指上下级域搭建完毕后，上级域要求下级域同步更新摄像机状态的过程。
目录通知：是指下级域获取到自身设备状态变更后，实时上报给上级域该状态变更的过程。
目录订阅以后，下级域一旦出现设备状态变更，就会上报推送消息，目录推送是一个长久持续的过程。

国标目录订阅与通知消息流程详解



目录订阅

Step.1:

上级域平台向下级域平台发送 Subscribe 消息，告诉下级域：我现在是你的上司啦，你这个域所有共享上来的设备，有啥状态变更（包括设备上线，下线，新增，删除），都要及时上报给我哦。

Step.2:

下级域收到 Subscribe 消息，答复 200OK：好的 BOSS，我这一发现状态变更，就向你上报消息！

目录通知

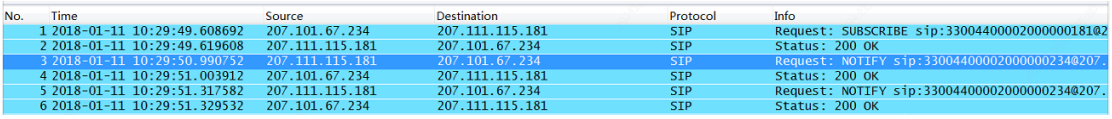
Step.3:

下级域接收到设备状态变更消息后，实时地向上级域发送 Notify 消息,告诉上级域：我下面的某某摄像机/某某 NVR 状态变为 在线/离线 了。

Step.4:

上级域收到 Notify 消息后，回复 200OK，实时更新该状态。

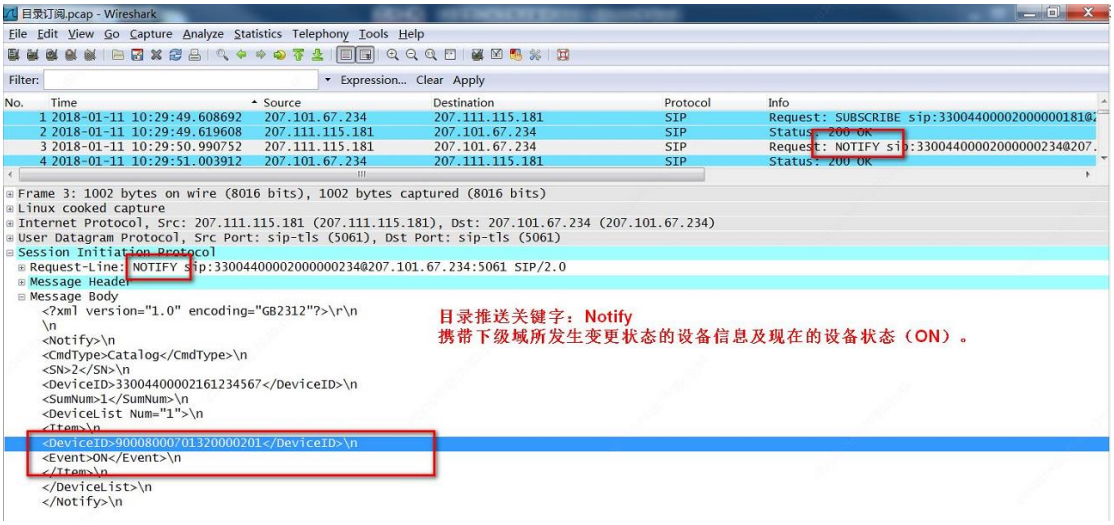
实例分析



No.	Time	Source	Destination	Protocol	Info
1	2018-01-11 10:29:49.608692	207.101.67.234	207.111.115.181	SIP	Request: SUBSCRIBE sip:33004400002000000181@2
2	2018-01-11 10:29:49.619608	207.111.115.181	207.101.67.234	SIP	Status: 200 OK
3	2018-01-11 10:29:50.990752	207.111.115.181	207.101.67.234	SIP	Request: NOTIFY sip:33004400002000000234@207.
4	2018-01-11 10:29:51.003912	207.101.67.234	207.111.115.181	SIP	Status: 200 OK
5	2018-01-11 10:29:51.317582	207.111.115.181	207.101.67.234	SIP	Request: NOTIFY sip:33004400002000000234@207.
6	2018-01-11 10:29:51.329532	207.101.67.234	207.111.115.181	SIP	Status: 200 OK

这是一个 234 上级域与 181 下级域进行目录订阅后的完整报文，我们来分步拆解解读一下。

上级域向下级域发送 Subscribe 消息，携带了消息主体：Catalog 以及下级域的国标外域共享编码。



目录订阅开启后，下级域检测到 201 这个共享编码的设备状态变更为在线（ON）了（可能本来这个设备已经离线了），向上级域上报 Notify 消息。上级域收到该消息后，将这条数据同步数据库。这样，我们就能实时地了解到下级域推送上来的资源状态信息了。

建议：

1、观察报文可发现，我们的目录订阅是从上级域的 5061 端口发送到下级域 5061 端口的，5061 是宇视的外域资源交互端口，其他厂商也有固定的类似端口，比如海康是 7100。

2、Catalog 字段用于在国标协议下级域给上级域上报资源目录和状态。

3、目录通知消息中，仔细观察，可看到有两个 DeviceID 字段，这是新国标规定的，前面一个 Device 字段表示设备的父组织编码，只有在 Item 字段之后的 Device,才代表是该设备的共享编码哦。

8. 设备目录查询与资源推送

在国标上下级域对接时，上级域需要能查看下级域的资源以及状态，第一步：操作人员在上级域界面对下级域进行外域资源检索操作（即设备目录查询），第二步：下级域接收了上级域的外域资源检索请求后会把已共享的资源推送上去（即资源推送）。

说明：

目录查询是查看下级域的资源以及初始状态，而后续需要实时更新下级域资源的状态变化时，需要上级域做目录订阅才可以。

如果订阅出现问题，可以在上级域对下级域进行资源查询，通过下级域上报所有已共享的资源，使上下级域已共享资源保持一致。

国标设备目录查询以及资源推送流程图

Step1：上级域发送 Message 信令给下级域，告诉下级域我需要看到你的资源；

Step2：下级域先回复 200OK，表示好的，我已收到你的命令；

Step3：下级域再发送 Message 信令（携带资源）给上级域。若上级域查询下级域组织下的共享资源共 N 个，需要根据每条报文上报的资源个数，分多条上报。上级域要根据报文中携带的资源总个数对查询资源进行接收。同一次查询响应报文的 SN 序号保持一致，标识一次查询响应上报的结果；

Step4：上级域会针对下级域发送的每一条 Message 报文回复 200OK，表示我已收到此资源的信息。

说明：

message 推送资源的报文一般都有很多条，每条一般携带的资源不能超过 4 个。

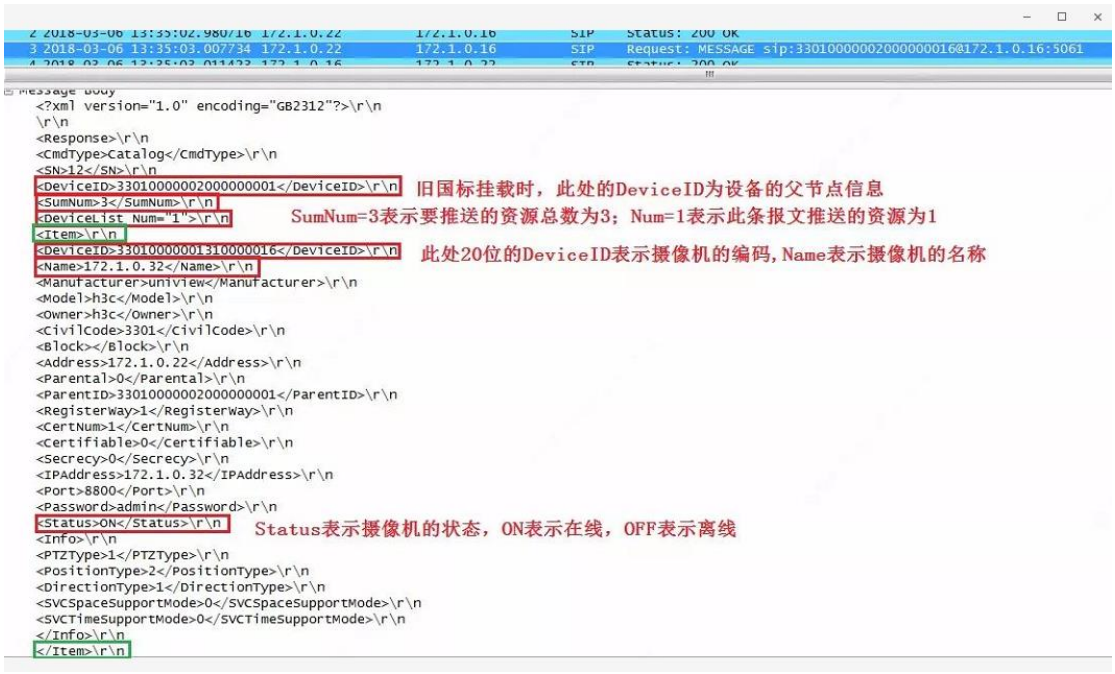
案例分析

如下图，其中 172.1.0.16 是上级域的 IP 地址，172.1.0.22 是下级域的 IP 地址，上下级域采用旧国标方式对接。

首先是上级域发送 Message 报文给下级域，Message 里面 Message Body 字段携带有 Catalog 表示目录查询的关键字段，DeviceID 表示下级域平台的设备 ID（国标是 20 位）。

如下图，此条 Message 是下级域推送的资源报文，首先从报文里面可以得到的主要信息如下：

SumNum(此处总共推送的资源数为 3)、Num(本次推送的资源数为 1)、DeviceID【摄像机挂在编码为 33010000002000000001（下级域平台编码）的父组织下】、Item 字段里面携带的有 DeviceID(推送的相机编码为 33010000001310000016)、Name（推送的相机名称为 172.1.0.32，）、Manufacturer（生产厂商为 uniview）、IPAddress（摄像机的地址 172.1.0.32）、Status（摄像机在线），还有其他一些信息，有些信息是资源推送必选的，有些可选可不选。



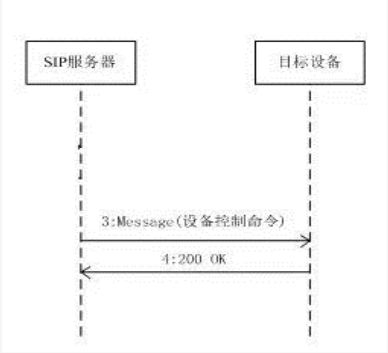
从资源推送报文中，可以清楚的知道一个名叫 172.1.0.32 的摄像机直接挂在了下级域的本域下面，且相机是在线的。

说明：

每一对 Item 表示一个资源，如果有对个资源，会有多个 Item，每个 Item 里面会携带推送的资源的编码和资源的名称等信息。

9. 云台控制流程

云台控制流程



命令流程描述如下：

1：SIP 服务器向目标设备发送设备控制命令，设备控制命令采用 MESSAGE 方法携带；

2：目标设备收到命令后返回 200 OK。

案例分析

云台控制命令码看四五六七字节，如图：

字节	位							
	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1	Bit0
字节 4	0	0	镜头变倍（Zoom）		云台垂直方向控制（Tilt）		云台水平方向控制(Pan)	
			缩小（OUT）	放大（IN）	上（Up）	下（Down）	左（Left）	右（Right）
字节 5	水平控制速度相对值							
字节 6	垂直控制速度相对值							
字节 7	变倍控制速度相对值				地址高 4 位			

注 1：字节 4 中的 Bit5、Bit4 分别控制镜头变倍的缩小和放大，字节 4 中的 Bit3、Bit2、Bit1、Bit0 位分别控制云台上、下、左、右方向的转动，相应 Bit 位置 1 时，启动云台向相应方向转动，相应 Bit 位清 0 时，停止云台相应方向的转动。云台的转动方向以监视器显示图像的移动方向为准。

注 2：字节 5 控制水平方向速度，速度范围由慢到快为 00H-FFH；字节 6 控制垂直方向速度，速度范围由慢到快为 00H-FFH。

注 3：字节 7 的高 4 位为变焦速度，速度范围由慢到快为 0H-FH；低 4 位为地址的高 4 位。

Step1:

向右转动：服务器发送设备控制命令，控制设备向右转动，命令码 01 E0E0F0, 01 由十六进制转化成二进制是 0000 0001, 01 由十六进制转化成二进制是 0000 0001，bit0 位为 1，所以代表为向右转动。水平控制速度相对值为 E0，垂直控制速度相对值为 E0，变倍控制速度相对值 F0，由于垂直、变倍方向为 0，所以水平速度 E0 向右旋转。

```
Message Body
    <?xml version="1.0" encoding="GB2312"?>\r\n
    \r\n
    <Control>\r\n
    <CmdType>DeviceControl</CmdType>\r\n
    <SN>1</SN>\r\n
    <DeviceID>33010000001310000032</DeviceID>\r\n
    <PTZCmd>A50F0001E0E0F065</PTZCmd>\r\n
    </Control>\r\n
```

设备响应控制请求发送 200OK：

```
172.1.0.16      172.1.0.22      SIP     Request: MESSAGE sip:33010000001310000032@172.1.0.22:5061
172.1.0.22      172.1.0.16      SIP     Status: 200 OK
```

Step2:

向左转动：服务器发送设备控制命令，控制设备向左转动，命令码 02 FCFCF0，02 由十六进制转化成二进制是 0000 0010，bit1 位为 1，所以代表为向左转动。水平控制速度相对值为 FC，垂直控制速度相对值为 FC，变倍控制速度相对值 F0，由于垂直、变倍方向为 0，所以水平速度 FC 向左旋转。

```
<?xml version="1.0" encoding="GB2312"?>\r\n
\r\n
<Control>\r\n
<CmdType>DeviceControl</CmdType>\r\n
<SN>16</SN>\r\n
<DeviceID>33010000001310000032</DeviceID>\r\n
<PTZCmd>A50F0002FCFCF09E</PTZCmd>\r\n
</Control>\r\n
```

设备响应控制请求发送 200OK：

```
172.1.0.16      172.1.0.22      SIP     Request: MESSAGE sip:33010000001310000032@172.1.0.22:5061
172.1.0.22      172.1.0.16      SIP     Status: 200 OK
```

Step3:

向下转动：服务器发送设备控制命令，控制设备向下转动，命令码 04 E0E0F0，04 由十六进制转化成二进制是 0000 0100，bit2 位为 1，所以代表为向下转动。水平控制速度相对值为 E0，垂直控制速度相对值为 E0，变倍控制速度相对值 F0，由于水平、变倍方向为 0，所以垂直速度 E0 向下旋转。

```
<?xml version="1.0" encoding="GB2312"?>\r\n
\r\n
<Control>\r\n
<CmdType>DeviceControl</CmdType>\r\n
<SN>18</SN>\r\n
<DeviceID>33010000001310000032</DeviceID>\r\n
<PTZCmd>A50F0004E0E0F068</PTZCmd>\r\n
</Control>\r\n
```

设备响应控制请求发送 200OK：

```
172.1.0.16      172.1.0.22      SIP     Request: MESSAGE sip:33010000001310000032@172.1.0.22:5061
172.1.0.22      172.1.0.16      SIP     Status: 200 OK
```

Step4：

向上转动：服务器发送设备控制命令，控制设备向上转动，命令码 08 E0E0F0，08 由十六进制转化成二进制是 0000 1000，bit3 位为 1，所以代表为向上转动。水平控制速度相对值为 E0，垂直控制速度相对值为 E0，变倍控制速度相对值 F0，由于水平、变倍方向为 0，所以垂直速度 E0 向上旋转。

```
<?xml version="1.0" encoding="GB2312"?>\r\n
\r\n
<Control>\r\n
<CmdType>DeviceControl</CmdType>\r\n
<SN>20</SN>\r\n
<DeviceID>33010000001310000032</DeviceID>\r\n
<PTZCmd>A50F0008E0E0F06C</PTZCmd>\r\n
</Control>\r\n
```

设备响应控制请求发送 200OK：

```
172.1.0.16      172.1.0.22      SIP     Request: MESSAGE sip:33010000001310000032@172.1.0.22:5061
172.1.0.22      172.1.0.16      SIP     Status: 200 OK
```

Step5：

放大：服务器发送设备控制命令，控制设备放大，命令码 10 000040, 10 由十六进制转化成二进制是 0001 0000 , bit4 位为 1，所以代表为放大。水平控制速度相对值为 00，垂直控制速度相对值为 00，变倍控制速度相对值 40，由于水平、垂直方向为 0，所以变倍速度 40 放大。

```
<?xml version="1.0" encoding="GB2312"?>\r\n
\r\n
<Control>\r\n
<CmdType>DeviceControl</CmdType>\r\n
<SN>10</SN>\r\n
<DeviceID>33010000001310000032</DeviceID>\r\n
<PTZCmd>A50F001000004004</PTZCmd>\r\n
</Control>\r\n
```

设备响应控制请求发送 200OK：

```
172.1.0.16      172.1.0.22      SIP     Request: MESSAGE sip:33010000001310000032@172.1.0.22:5061
172.1.0.22      172.1.0.16      SIP     Status: 200 OK
```

Step6：

缩小：服务器发送设备控制命令，控制设备缩小，命令码 20 000040, 20 由十六进制转化成二进制是 0010 0000 , bit5 位为 1，所以代表为缩小。水平控制速度相对值为 00，垂直控制速度相对值为 00，变倍控制速度相对值 40，由于水平、垂直方向为 0，所以变倍速度 40 缩小。

```
<?xml version="1.0" encoding="GB2312"?>\r\n
\r\n
<Control>\r\n
<CmdType>DeviceControl</CmdType>\r\n
<SN>12</SN>\r\n
<DeviceID>33010000001310000032</DeviceID>\r\n
<PTZCmd>A50F002000004014</PTZCmd>\r\n
</Control>\r\n
```

设备响应控制请求发送 200OK：

```
172.1.0.16      172.1.0.22      SIP     Request: MESSAGE sip:33010000001310000032@172.1.0.22:5061
172.1.0.22      172.1.0.16      SIP     Status: 200 OK
```

Step7：

停止转动：服务器发送设备控制命令，控制设备向停止转动，命令码 00 0000F0,00 由十六进制转化成二进制是 0000 0000，所有位都是 0，水平控制速度相对值为 00，垂直控制速度相对值为 00，变倍控制速度相对值 F0，由于水平、垂直、变倍方向都为 0，所以控制设备向停止转动。

```
<?xml version="1.0" encoding="GB2312"?>\r\n
\r\n
<Control>\r\n
<CmdType>DeviceControl</CmdType>\r\n
<SN>2</SN>\r\n
<DeviceID>33010000001310000032</DeviceID>\r\n
<PTZCmd>A50F00000000F0A4</PTZCmd>\r\n
</Control>\r\n
```

设备响应控制请求发送 200OK：

```
172.1.0.16      172.1.0.22      SIP     Request: MESSAGE sip:33010000001310000032@172.1.0.22:5061
172.1.0.22      172.1.0.16      SIP     Status: 200 OK
```

注：不管服务器请求的是向哪个方向转动，或者是放大还是缩小，转动结束时，服务器都会向设备发送此停止转动指令。

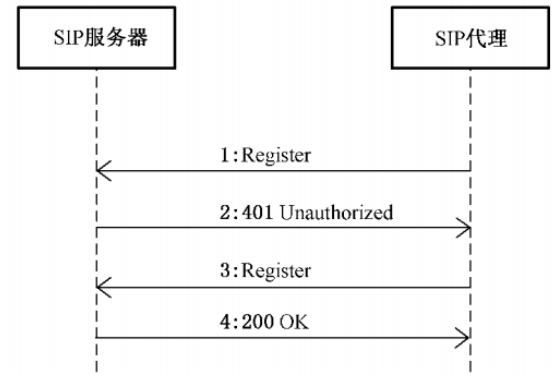
如上就是云台设备控制中方向控制和变倍控制的基本流程，是基于 SIP 信令的，MESSAGE 消息承载控制指令，200 OK 承载对控制指令的答复。

第二章 国标字段解释

1. 国标注册

1.1 注册流程

基本注册即采用 IETF RFC 3261 规定的基于数字摘要的挑战应答式安全技术进行注册，具体注册流程见下图



Step.1:
注册设备向对方中心服务器发送 Register 注册消息
Step.2:
中心服务器检查注册设备带来信令中的 Authorization 字段（鉴权字段），发现 Register 信令中未带鉴权字段。回复注册设备： 401 Unauthorized（注册未带鉴权）。注意，这不是异常报错，这是国标注册中的正常流程。
Step.3:
注册设备重新向中心服务器发送 Register 注册消息，并带上鉴权字段（Register With Authorized）
Step.4:
中心服务器检查 Authorization 字段，如果该鉴权通过，则回复 200OK，设备在线。

1.2 字段解释

REGISTER（前端注册到中心服务器为例）
REGISTER sip:32028100002000000000@3202810000 SIP/2.0---------方法：register；请求 URI 用户名@域 版本号
Via: SIP/2.0/UDP 46.10.1.66:5060;rport;branch=z9hG4bK111093174----------
Via 头域是标志了用于事务传输的传输设备，并且也标志了应答送回的地址。
branch 这个参数用于区分请求创建的事务
From: <sip:32028104561321000011@3202810000>;tag=1179799581
提交这个注册信息的用户的 address-ofrecord 资料 和 to 是一样的，后面要加个 tag，为什么请查看 RFC3261 的 19.3 章节

address-of-record 由注册用户 ID@域名组成 域名也可以是 ip 地址：端口 这种格式
To: <sip:32028104561321000011@3202810000>
Call-ID: 2033429411----------标志一组会话，
CSeq: 1 REGISTER----------和 method 对应一组会话，会递增
Contact: <sip:32028104561321000011@46.10.1.66:5060>-----提供了访问后续请求的特定 UA 实例的联系方法
Max-Forwards: 70----------最大跳转数（网络层）
User-Agent: IP Camera----------这边 UA 代理是一个摄像头
Expires: 3600----------注册有效期
Content-Length: 0----------文本字节

401
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 46.10.1.66:5060;branch=z9hG4bK111093174
Call-ID: 2033429411
From: <sip:32028104561321000011@3202810000>;tag=1179799581-------from and to 消息同上
To: <sip:32028104561321000011@3202810000>;tag=4dd866e7
CSeq: 1 REGISTER
User-Agent: IMOS/V3
WWW-Authenticate:Digest
realm="32028100002000000000",nonce="519c58b9519c58b9ac8c58b9a79c58b9d39c58b9009c58b9ac8c58b9198c58",algorithm=MD5----------告知没有填写认证，并给予认证方式
Content-Length: 0

REGISTER
REGISTER sip:32028100002000000000@3202810000 SIP/2.0
Via: SIP/2.0/UDP 46.10.1.66:5060;rport;branch=z9hG4bK132008081----同上
From: <sip:32028104561321000011@3202810000>;tag=1179799581
----------from and to 消息一致
To: <sip:32028104561321000011@3202810000>
Call-ID: 2033429411----------会话唯一标识符
Contact: <sip:32028104561321000011@46.10.1.66:5060>
Authorization: Digest username="32028104561321000011", realm="32028100002000000000", nonce="519c58b9519c58b9ac8c58b9a79c58b9d39c58b9009c58b9ac8c58b9198c58", uri="sip:32028100002000000000@3202810000", response="c990b63bfa21138bd724a467ec27b134", algorithm=MD5
知道这个怎么算吗？下文告诉你
Max-Forwards: 70
User-Agent: IP Camera
Expires: 3600
Content-Length: 0

200OK 消息

SIP/2.0 200 OK
Via: SIP/2.0/UDP 46.10.1.66:5060;branch=z9hG4bK132008081----------同上
Call-ID: 2033429411
From: <sip:32028104561321000011@3202810000>;tag=1179799581----------from and to 消息一致同上
To: <sip:32028104561321000011@3202810000>;tag=3129b066
CSeq: 2 REGISTER
Contact: <sip:32028104561321000011@46.10.1.66:5060>
Expires: 3600
User-Agent: IMOS/V3
Date: 2018-07-13T13:22:50.215----------回复消息这一时刻的时间，这个 date 头域必须存在
Content-Length: 0

REGISTER 认证加密计算

计算 Response 过程：
a. 下载 MD5 加解密工具。
b. 将 username,realm,password 依次组合获取 1 个字符串，并对这个字符串使用算法 H 来进行加密，获得密文 1.
c. 将 method,uri 依次组合获取 1 个字符串，并对这个字符串使用算法 H 来进行加密，获得密文 2.
d. 将密文 1，nonce 和密文 2 依次组合获取 1 个字符串，并对这个字符串使用算法 H 来进行加密，获得密文 3.
这个密文 3 就是最终的结果 Response。

步骤 1.
32028104561321000011:32028100002000000000:admin12345
MD5 加密后密文 ：
c9504793987d578e0640c26357fb1097

步骤 2：
REGISTER:sip:32028100002000000000@3202810000
MD5 加密后密文 ：
3e9f8eefefb80928175d2f3671f9b5e9

步骤 3：
密文 1+nonce+密文 2：
c9504793987d578e0640c26357fb1097:519c58b9519c58b9ac8c58b9a79c58b9d39c58b9009c58b9ac8c58b9198c58:3e9f8eefefb80928175d2f3671f9b5e9
MD5 加密后密文：
c990b63bfa21138bd724a467ec27b134
response = c990b63bfa21138bd724a467ec27b134

MD5 加密后密文 = response 所以注册校验成功,设备即成功上线。

2. 国标编码

编码规则 A

编码规则 A 由中心编码(8 位) 、 行业编码(2 位) 、 类型编码(3 位) 和序号(7 位) 四个码段共 20 位十进制数字字符构成, 即系统编码 = 中心编码 + 行业编码 + 类型编码 + 序号。

1）常用类型编码

200----中心服务器

111----DVR

118----NVR----不同厂家的编码不同，但不重要，查下 NVR 的本地国标编码便知

132----摄像机

注意：工作中一定要记住 20 位国标编码中的 11-13 位，看到就能分辨它代表什么？记住以上 4 种，足够你用。

2）中心编码

1，2 位-----省

3，4 位-----市

5，6 位-----区

7，8 位-----基层接入单位编码

举例：江苏 32 南京 02 江宁 81 湖熟街道 01

那么江苏南京江宁湖熟街道的国标 ID 可以为 32028101002000000000

3）行业编码

实际工作中，你可以自己定义 00 代表什么行业？一直到 99，可以自定义

如：

00------社会治安路面接入

01------社会治安社区接入

02------社会治安内部接入

……

4）序号

第 14 位为网络标识编码

0、1、2、3、4 为监控报警专网,5 为公安信息网,6 为政务 网,7 为 Internet 网,8 为 社 会 资源 接 入 网,9 预留

最后 6 位，用来表示数量的

3202810000132 0 000000 ~ 3202810000132 0 999999 999999+1=1 百万个摄像机编码

3202810000200 0 000000 ~ 3202810000200 0 999999 999999+1=1 百万个中心服务器编码

案例参考

现有一个项目，江苏省有一台服务器，13 个地市各一台服务器，要求你给江苏省，以及 13 个地市及地市的区域，做一套国标规划该怎么划分？在这里举一个例子，供大家参考，毕竟每个项目现实状况不同，这里仅供参考

省、市服务器 ID 划分
江苏省中心服务器 ID： 32000000 00 200 0 000001-----这里开头 2 位 32 代表江苏省
南京市中心服务器 ID： 32010000 00 200 0 000001-----这里 3201 代表江苏南京
镇江市中心服务器 ID： 32020000 00 200 0 000001-----这里 3202 代表江苏镇江
。。。。。。
南通市中心服务器 ID： 32130000 00 200 0 000001-----这里 3213 代表江苏南通

到这里为止 13 个地市的服务器国标 ID 已经完成，下面给南京市 11 个区做下服务器 ID 规划
市、区服务器 ID 划分（以南京江宁为例）
南京市江宁区服务器 ID：32010100 00 200 0000001----这里 320101 代表南京江宁

江宁区摄像机编码划分：
考虑现在国标上下级域之间推送一般采用”行政区划”的方式来推送。那么在建目录的时候，就按次序建立好，如下：
建一个目录编码为 320101 代表江宁区
建一个子目录为 32010101 代表湖熟街道----那么湖熟街道的摄像头编码为 32010101001320000001~999999
画图如下
320101
32010101 街道 1 目录下挂载摄像机编码 32010101001320000001~999999
32010102 街道 2 目录下挂载摄像机编码 32010102001320000001~999999
32010103 街道 3 目录下挂载摄像机编码 32010103001320000001~999999
32010104 街道 4 目录下挂载摄像机编码 32010104001320000001~999999
上图为江宁区目录结构

那么江宁区推送至南京市后，南京市目录结构会是什么样的？
南京市目录结构：
3201
320101---江宁区
32010101 街道 1 目录下挂载摄像机编码 32010101001320000001~999999
32010102 街道 2 目录下挂载摄像机编码 32010102001320000001~999999
32010103 街道 3 目录下挂载摄像机编码 32010103001320000001~999999
32010104 街道 4 目录下挂载摄像机编码 32010104001320000001~999999
320102---秦淮区
32010201 街道 1 目录下挂载摄像机编码 32010201001320000001~999999
32010202 街道 2 目录下挂载摄像机编码 32010202001320000001~999999
32010203 街道 3 目录下挂载摄像机编码 32010203001320000001~999999
32010204 街道 4 目录下挂载摄像机编码 32010204001320000001~999999
320103---其他区等等

南京市推往江苏省，江苏省结构图
32--江苏
3201--南京

320101---江宁区

32010101 街道 1 目录下挂载摄像机编码 32010101001320000001~999999

32010102 街道 2 目录下挂载摄像机编码 32010102001320000001~999999

32010103 街道 3 目录下挂载摄像机编码 32010103001320000001~999999

32010104 街道 4 目录下挂载摄像机编码 32010104001320000001~999999

320102---秦淮区

32010201 街道 1 目录下挂载摄像机编码 32010201001320000001~999999

32010202 街道 2 目录下挂载摄像机编码 32010202001320000001~999999

32010203 街道 3 目录下挂载摄像机编码 32010203001320000001~999999

32010204 街道 4 目录下挂载摄像机编码 32010204001320000001~999999

320103---其他区等等

3202--镇江

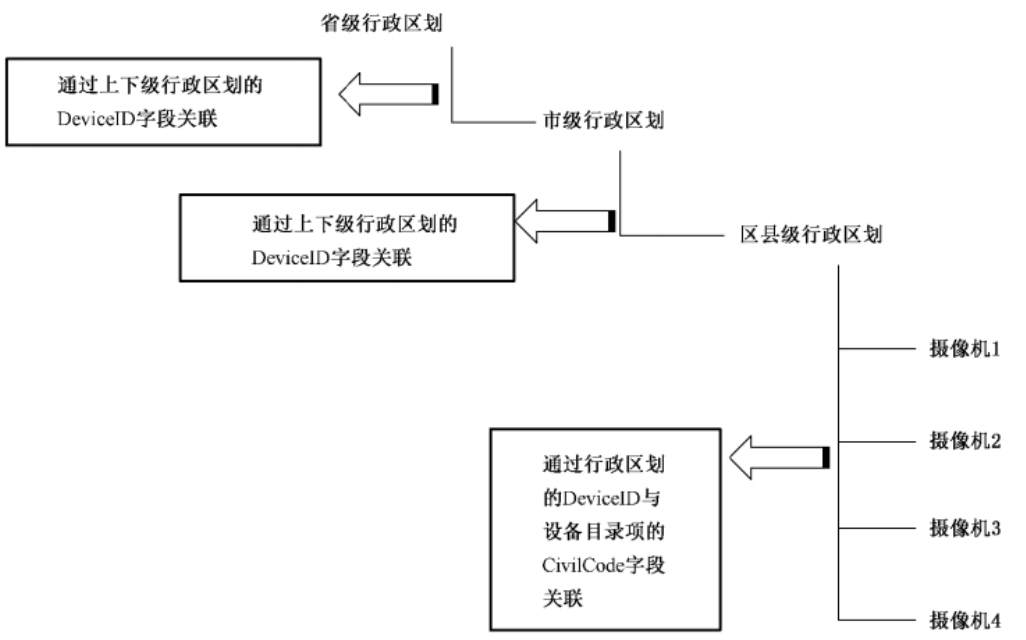
320201---润州区

32020101 街道 1 目录下挂载摄像机编码 32020101001320000001~999999

32020102 街道 2 目录下挂载摄像机编码 32020102001320000001~999999

3203--泰州。。。等等

行政区划结构示意图



业务分组和虚拟组织

215 and 216 初始定义：

附录 D（规范性附录）统一编码规则（第 84 页）

国标 28181-2016 下载地址

链接：https://pan.baidu.com/s/1bDRkdT1jehymevIpfv4WLA 密码：xzg4

类型编码	11、12、13	200～299 表示类型为平台设备	207	GIS 服务器编码
			208	管理服务器编码
			209	接入网关编码
			210	媒体存储服务器编码
			211	信令安全路由网关编码
			215	业务分组编码
			216	虚拟组织编码
			212～214，217～299	扩展的平台设备类型

附录 O（规范性目录）目录查询应答示例说明（第 199 页）

a. 业务分组，虚拟组织代表了摄像机的特定业务分组下的组织结构，用于特定业务设备树组织展示。

b. 业务分组根据特定的业务需求制定，一个业务分组包含一组特定的虚拟组织，虚拟组织下可划分子虚拟组织并可挂接设备，业务分组、 虚拟组织、 设备间为以业务分组为根节点，虚拟组织为分支节点，设备为叶节点的树状层次关系。

根据这句话的定义：215 下只能包含 216，216 下可以有 216，可以有 132，但不能有 215.

案例

根据下例虚拟组织结构，来了解下报文字段结构：

外层大组织 65010200002000000001

业务分组 1（组织）65010200002150000001

虚拟组织 1（组织）65010200002160000001

子虚拟组织（组织）65010200002160000002

挂靠设备（相机）65010200001320000009

业务分组 2（组织）65010200002150000002

虚拟组织 1（组织）65010200002160000011

子虚拟组织（组织）65010200002160000012

挂靠设备（相机）65010200001320000010

```
<Item>
    < ！--业务分组标识，编码采用 D.1 中的 20 位 ID 格式，扩展 215 类型代表业务分组
-->
     <DeviceID>65010200002150000001</DeviceID>
     <Name> 业务分组名称</Name>
     <！--填写制定此业务分组所属的系统 ID-->
     <ParentID>65010200002000000001</ParentID>
</Item>
```

虚拟组织目录项

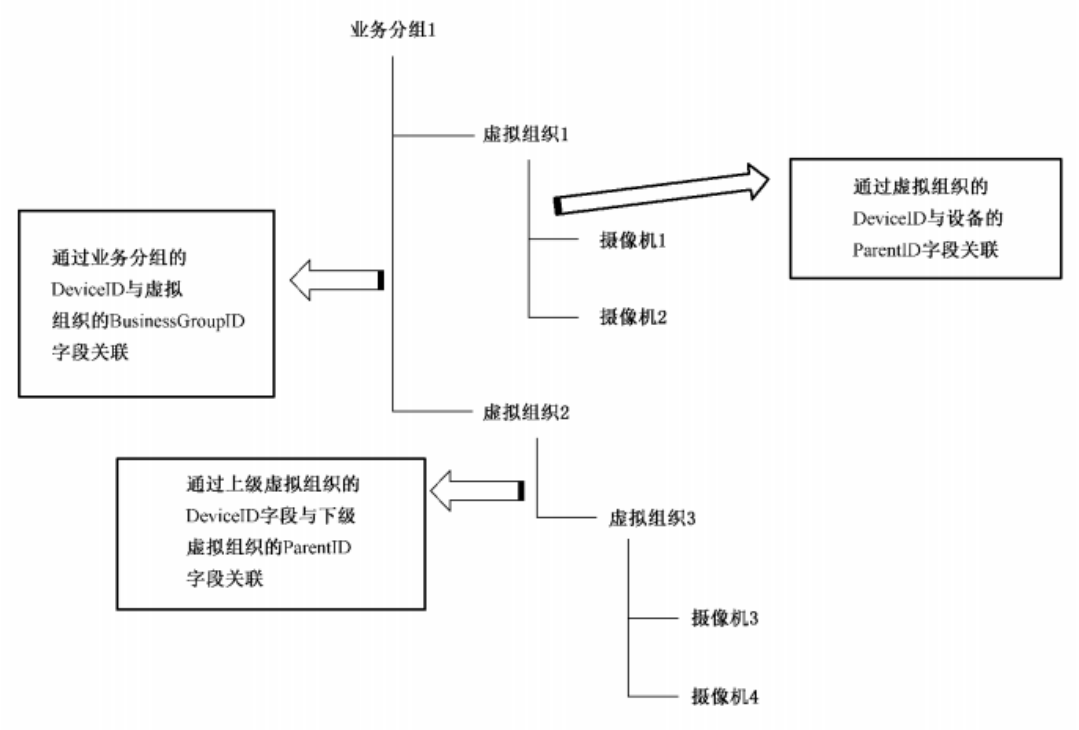
```
<Item>
    < ！--虚拟组织标识，编码采用 D.1 中的 20 位 ID 格式，扩展 216 类型代表虚拟组织
-->
```

<DeviceID>65010200002160000002</DeviceID>
<Name> 虚拟组织名称</Name>
< ！ --父节点虚拟组织 ID，用于标识虚拟组织间的层级关系，若有父节点虚拟组织则填写此字段-->
<ParentID>65010200002160000001</ParentID>
< ! --虚拟组织所属的业务分组 ID-->
<BusinessGroupID>65010200002150000001</BusinessGroupID>
</Item>

设备目录项

<Item>
<DeviceID>65010200001320000009</DeviceID>
<Name>IPC_天山视频</Name>
< Manufacturer> 设备厂商</Manufacturer>
< Model> 设备型号</Model>
<Owner> 设备归属</Owner>
<CivilCode>650102</CivilCode>
< ！ --若设备属于某组织机构下，应在 Block 字段中填写相应组织机构代码，组织机构代码应符合 GA/T380—2011 规定。 -->
<Block>650102000000</Block>
<Address> 设备安装地址</Address>
<Parental>0</Parental>
< ! --若上传目录中有此设备的父设备则应填写父设备 ID，若无父设备则应填写系统 ID；若设备属于某虚拟组织下，则应同时填写虚拟组织 ID；各个 ID 之间用“/”分隔。 -->
<ParentID> 摄像机父设备/虚拟组织</ParentID>
<RegisterWay>1</RegisterWay>
<Secrecy>0</Secrecy>
<Status>ON</Status>
</Item>

按照业务分组进行设备树展示使用业务分组、 虚拟组织、 设备目录类型，示例见图



3. SDP

SDP 定义

在这里有关 SDP 的定义，让我们来看下 RFC4566（扩展更新了 RFC2327）是如何定义的：
This memo defines the Session Description Protocol (SDP). SDP isintended for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation.
翻译：本规范定义了会话描述协议（SDP），SDP 是为了描述多媒体会话而设计的，主要用来描述会话通告，会话邀请或者其他形式的多媒体会话初始化。
简单解释 SDP 干嘛用的：不同的厂家，使用 GB 对接的时候，上级要能正常看下级推送过来的摄像头的视频，回放，以及球机控制等等的功能。

字段解释（符合 RFC4566）

在进行国标对接最多的工程中，如公安，交通，学校，水利等的行业，所用到的视频厂家一般有海康，大华，宇视，工程师在完成国标对接成功后，一般需要验证的两大块业务为实况和回放。在不能实现这两块业务功能时候，这个时候就需要抓包排查了，而需要看字段就是 SDP 的字段了。以下为 SDP 定义的常用字段：

Session Description
v=protocol version
o=(owner/creator and session identifier)
s=session name

u=*(URI of description)
c=*(connection information-not required if included in all media)

Time Desctiption
t= (time the session is active)

Media description
m= (media name and transport address)
c= * (connectioninformation-optionalifincludedatsession-level)
a= * (zero or more mediaattributelines)
y= * (SSRC)

f= * **(媒体描述)**

说明：
1) Session Description
v=0 "v="字段给出了 SDP 的版本，当前规范版本是 0，这个版本没有小号版本。
"o="源（发起者）<用户名><会话 ID><会话版本><网络类型><地址类型><单播地址>
如 32028100001320000001 0 0 IN IPV4 192.168.0.101
<用户名> 用户登录的源主机名字，如果不能提供则用"-"表示，用户名不能包含空格。这里一般是摄像机的国标 ID
<会话 ID> 是一个字符串，<用户名><会话 ID><网络类型><单播地址>这个组合形成该会话的唯一标识。用 0 标识的居多
<会话版本> 会话版本号，推荐使用 NTP 时间戳。用 0 标识的居多
<网络类型> 目前是 IN 代表 internet，未来可能会有其他值。
<地址类型> 目前只有 IPV4 和 IPV6 两种，目前主要是 IPV4,。
<单播地址> 创建会话的主机地址。一般为媒体服务器的地址。
注意：有时候处于某种原因，用户名和 IP 不想明确表示，只要保证 o 字段全球唯一，用户名和 IP 可以随机。
"s="请求媒体流的操作类型，play 代表实况；playback 代表回放。download 代表下载，Talk 代表语音。
"u=" 行应填写视音频文件的 URI。 该 URI 取值有两种方式: 简捷方式和普通方式。
简捷方式常用 摄像机 ID：其他参数格式。如 32028100001320000001:10111
普通方式采用 http://存储设备 ID[/文件夹]* /文件名, [/文件夹]* 为 0-N 级文件夹。
"c="<网络类型><地址裂类型><链接地址> 如 IN IPV4 192.168.0.100

2) Time Description
t 字段 在回放和下载时，t 行值为开始时间和结束时间。使用的时间为 UNIX 时间戳，需要用 UNIX 时间戳转为北京时间。

工具 UTCTime2.exe 下载链接：链接：https://pan.baidu.com/s/1LP8rD1U7qVOzaiSEGyPu-A 密码：iw52

3) Media description

m 字段 描述媒体类型，媒体端口，媒体协议，以及媒体负载方式

例：

m=video 6000 RTP/AVP 96------媒体类型视频或视音频，传输端口 6000，RTP over UDP，负载类型 96

m=video 6000 TCP/RTP/AVP 96------媒体类型视频或视音频，传输端口 6000，RTP over TCP，负载类型 96

m=audio 6000 RTP/AVP 8------媒体类型为音频，传输端口 6000，RTP over UDP，负载类型 8

a 字段：启用 IETF RFC 4566 中对 a 字段的定义 a=rtpmap: <payload type> <encoding name>/<clockrate> [/<encoding parameters>] 中的<encoding name> ，利用该属性携带编码器厂商名称(如:企业 1 或企业 2 编码名称 DAHUA 或 HIKVISION) 。 该属性表明该流为某厂商编码器编码且是不符

合本标准规定的媒体流，符合本标准规定的媒体流无需该属性。

例如:a=rtpmap:96 DAHUA/90000;

a=rtpmap:96 HIKVISION/90000。

a 字段有下列格式:

————a 字段可携带倍速参数，用于文件下载时控制下载进度。 格式如下:

a=downloadspeed: 下载倍速(取值为整型)

————a 字段可携带文件大小参数，用于下载时的进度计算。 格式如下:

a=filesize: 文件大小(单位:Byte)

————a 字段可携带 setup、connection 作为 TCP 连接协商参数，用于 TCP 方式传输媒体流服务端、

客户端的协商，协商机制参考 IETF RFC4571 的定义。 格式如下:

a=setup:TCP 连接方式(表示本 SDP 发送者在 RTP over TCP 连接建立时是主动还是被动发起 TCP 连接，“active”为主动，“passive”为被动)

a=connection:new (表示采用 RTP over TCP 传输时新建或重用原来的 TCP 连接，可固定采用新建 TCP 连接的方式)

a=recvonly 只接受（收流端）只用于媒体，不用于控制协议

a=sendonly 只发送 （发刘端）只用于媒体，不用于控制协议

y 字段：由 10 位十进制整数组成的字符串，表示 SSRC 值

第一位为 0 代表实况，为 1 则代表回放；

第二位至第六位由监控域 ID 的第 4 位到第 8 位组成；

最后 4 位为不重复的 4 个整数

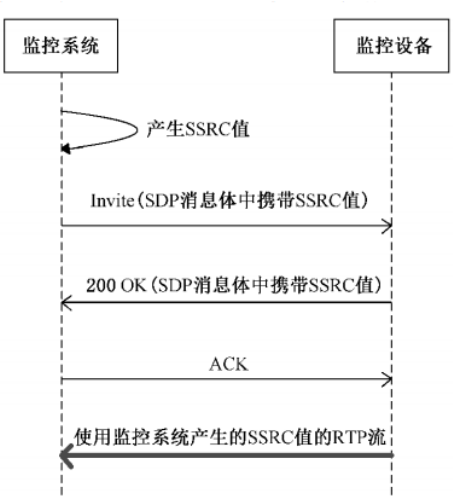
SSRC 的使用

SSRC 值由媒体流发送设备所在的 SIP 监控域产生，作为媒体流的标识使用。 点播域内设备、点播外域设备媒体流 SSRC 的处理方式分别说明如下:

a) 点播域内设备媒体流 SSRC 处理方式

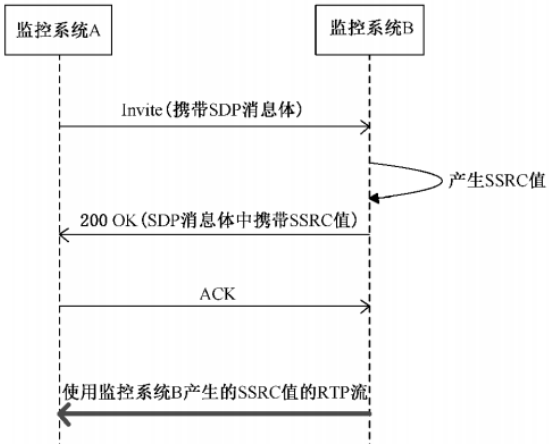
点播域内设备媒体流时,SSRC 值由本域监控系统产生并通过 Invite 请求发送给设备使用，设备在回复的 200OK 消息中携带此值，设备在发送的媒体流中使用此值作为 RTP 的 SSRC

值。 如下图所示



b) 点播外域设备媒体流 SSRC 处理方式

点播外域设备媒体流时,SSRC 由被点播域产生并在被点播域回复域发送的 RTP 码流使用该值作为 SSRC 值。 如下图所示



字段解释

UDP 回放流程分析

组网：上级平台（192.168.0.1）---国标----（192.168.1.1）下级平台

上级媒体设备：192.168.0.10
下级媒体设备：192.168.1.10

INVITE 消息如下：

v=0---协议版本为 0，唯一版本，目前没有比这更小的了

o=32028104001322015132 0 0 IN IP4 192.168.0.10-----用户名（即摄像头国标 ID），会话 ID 0，会话版本 0，网络类型 IN，创建会话的主机地址（即 SIP 服务器的 IP 地址）

s=Playback-----请求媒体流操作类型是回放

u=32028104001322015132:17895----URL 的简捷方式摄像头 ID：参数

c=IN IP4 192.168.0.10----------收流网络类型为 IN，地址类型为 IPV4，收流媒体设备 IP192.168.0.10

t=1529935740 1529965483----------转化成北京时间，开始时间为 2018/6/25 22:09:00；结束时间为 2018/6/26 06:24:43

m=video 14430 RTP/AVP 96----------媒体流类型为视音频，端口 14430，RTP 负载 UDP，负载类型 96

a=recvonly----------代表只接受模式（接受媒体流端）

a=rtpmap:96 PS/90000----------固定格式，负载类型 96，编码格式 PS，90000 是时钟

y=1281002378----------第一位为 1 代表回放，2-6 是来自监控域 ID 的 4-8 位，后 4 位随机不重复

200 OK 消息如下：
v=0---目前为 0，没有其他版本

o=32028104001322015132 0 0 IN IP4 192.168.0.10----上级访问的摄像头 ID，会话 ID，会话版本，网络类型，地址类型，会话创建主机的 IP，这边即为上级媒体流服务器 IP

s=Playback----------请求媒体流操作类型是回放

c=IN IP4 192.168.1.10----------下级发流端网络类型，地址类型和发流设备 IP

t=1529935740 1529965483----回放的开始和结束时间

m=video 5694 RTP/AVP 96-----媒体流类型，下级发流端口，RTP 负载 UDP，负载类型 96

a=rtpmap:96 PS/90000---------负载类型，编码格式，时钟

a=sendonly----------下级是发流，这边的只发送模式，可以理解为发送端

y=1100005694----------第一位为 1 代表回放，由于本组网类型属于上下级域的方式，所以这边的 SSRC 值由下级产生，和上级不一样。

TCP 实况流程分析
组网：摄像头 192.168.1.1----国标 TCP 接入-----192.168.0.1 SIP 服务器
平台媒体服务器 IP： 192.168.0.10

INVITE 消息分析：
v=0----协议版本

o=32028100002000000000 0 0 IN IP4 192.168.0.10---此组网方式，用户名为本 sip 监控域 ID，RFC4566 中提到，只要保证 o 字段保证会话唯一，那么用户名和 IP 地址可以随机（取决于开发取字段）。

s=Play------请求视频流操作类型为 play，代表是实况

c=IN IP4 192.168.0.10

t=0 0-------实况的开始时间和会话时间为 0 0，表示会话永恒，实况都是被动终止的，否则会话始终生效

m=video 20622 TCP/RTP/AVP 96-------TCP/RTP/AVP RTP 负载 TCP，即收流类型为 TCP

i=primary-----这边意义不大，可忽略，主要是为了方便阅读用的

a=recvonly

a=rtpmap:96 PS/90000

a=setup:active----------TCP 建立连接方式为主动接受

a=connection:new--------可固定采用新建 TCP 的方式

y=0281002257----------浏览本域上的摄像头，SSRC 值由本监控域产生

200Ok 消息分析：
v=0

o=32028104561321000011 4031 4031 IN IP4 192.168.1.1

s=Play

c=IN IP4 192.168.1.1

t=0 0

m=video 15064 TCP/RTP/AVP 96

a=setup:passive-----TCP 连接为被动，作为摄像机是被动发起实况连接的

a=sendonly

a=rtpmap:96 PS/90000

a=username:32028104561321000011----用户名（国标接入访问字段）

a=password:admin12345----------摄像机网页登录密码

a=filesize:0----------没有下载文件，文件大小为 0

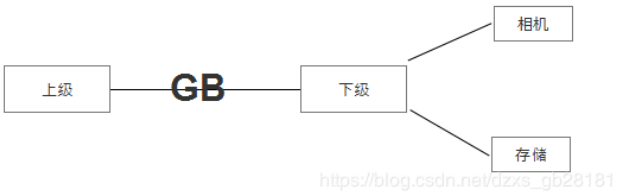
y=0281002257----------本组网方式，SSRC 值来自上级监控域的 SSRC 值

f=

4. 视音频文件检索

文件检索主要用区域、 设备、 录像时间段、 录像地点、 录像内容为条件进行查询, 用 Message 消息发送检索请求和返回查询结果, 传送结果的 Message 消息可以发送多条, 应支持附录 N 多响应消息传输的要求。

经典组网



命令流程

设备视音频文件检索消息流程如下图所示

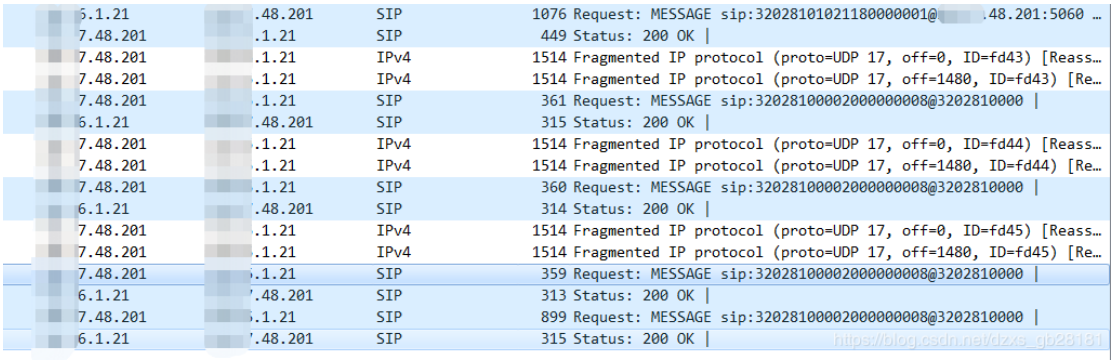
信令流程描述如下:
1: 目录检索方向目录拥有方发送目录查询请求 Message 消息, 消息体中包含视音频文件检索条件;
2: 目录拥有方向目录检索方发送 200 OK, 无消息体;
3: 目录拥有方向目录检索方发送查询结果, 消息体中含文件目录, 当一条 Message 消息无法传送完所有查询结果时, 采用多条消息传送;（GB28181 附录 N 多响应消息传输的要求）
4: 目录检索方向目录拥有方发送 200 OK, 无消息体。

字段解释

文件目录检索请求
< ! -- 命令类型: 文件目录检索(必选) -->
<element name="CmdType" fixed ="RecordInfo" />
< ! -- 命令序列号(必选) -->
<element name="SN" type="integer" minInclusive value = "1" />---多响应消息，这个 SN 值是相同的
< ! -- 目录设备/视频监控联网系统/区域编码(必选) -->
<element name="DeviceID" type="tg:deviceIDType" />
< ! -- 录像起始时间(必选)-->
<element name ="StartTime" type="dateTime"/>
< ! -- 录像终止时间(必选)-->
<element name ="EndTime" type="dateTime" />
< ! -- 文件路径名 (可选)-->
<element name=" FilePath" type="string"/>
< ! -- 录像地址(可选 支持不完全查询) -->
<element name="Address" type="string"/>
< ! -- 保密属性(可选) 缺省为 0;0: 不涉密,1: 涉密-->
<element name="Secrecy" type="integer" minInclusive value = "1"/>
< ! -- 录像产生类型(可选)time 或 alarm 或 manual 或 all-->
<element name="Type" type="string"/>
< ! -- 录像触发者 ID(可选)-->
<element name="RecorderID" type="string"/>
< ! --录像模糊查询属性(可选) 缺省为 0;0: 不进行模糊查询, 此时根据 SIP 消息中 To 头域
URI 中的 ID 值确定查询录像位置, 若 ID 值为本域系统 ID 则进行中心历史记录检索, 若为前
端设备 ID 则进行前端设备历史记录检索;1: 进行模糊查询, 此时 设备所在域应同时进行中心
检索和前端检索并将结果统一返回。 -->
<element name="IndistinctQuery" type="string"/>

案例结合

1. 上级向下级查询录像，抓包总体报文



第一条 message 是检索的报文，下面的 message 消息是下级给上级的回复。
如何确定是检索消息还是 keepalive 保活消息，可以查看 message body 体里的<cmdtype>字段

<CmdType>RecordInfo</CmdType>\n 这个表示是录像检索

<CmdType>Keepalive</CmdType>\r\n 这个表示保活

2. 检索消息体字段解释

<Query>
<CmdType>RecordInfo</CmdType>----------录像查询
<SN>10715</SN>----------命令序列号，多响应消息，此值相同
<DeviceID>32028101021320000009</DeviceID>----相机 ID
<StartTime>2018-12-06T00:00:00</StartTime>-------录像开始时间
<EndTime>2018-12-06T23:59:59</EndTime>---------录像结束时间
<Type>time</Type>----------根据时间查询
<FilePath>32028101021320000009</FilePath>------文件路径
<Address>Address1</Address>----------录像地址，支持不完全查询
<Secrecy>0</Secrecy>----------默认为 0 代表，不涉密
<RecorderID>32028101021320000009</RecorderID>-录像触发者 ID
<IndistinctQuery>0</IndistinctQuery>----------0：不进行模糊查询

3. 下级回复

<?xml version="1.0"?>
<Response>
<CmdType>RecordInfo</CmdType>
<SN>10715</SN>----------命令序列号同查询的相同
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<SumNum>31</SumNum>
<RecordList Num="10">----------10 条记录<item>项
<Item>
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>

<FilePath>1544024318_1544026472</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-05T23:38:38</StartTime>----回复的录像开始时间
<EndTime>2018-12-06T00:14:32</EndTime>--------录像的结束时间
<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
<Item>
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<FilePath>1544026472_1544028625</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-06T00:14:32</StartTime>--开始
<EndTime>2018-12-06T00:50:25</EndTime>------结束
<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
<Item>
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<FilePath>1544028625_1544030780</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-06T00:50:25</StartTime>--开始
<EndTime>2018-12-06T01:26:20</EndTime>------结束
<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
<Item>
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<FilePath>1544030780_1544032934</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-06T01:26:20</StartTime>---开始
<EndTime>2018-12-06T02:02:14</EndTime>-------结束
<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
<Item>
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<FilePath>1544032934_1544035087</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-06T02:02:14</StartTime>--开始
<EndTime>2018-12-06T02:38:07</EndTime>------结束

<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
<Item>
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<FilePath>1544035087_1544037242</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-06T02:38:07</StartTime>---开始
<EndTime>2018-12-06T03:14:02</EndTime>-------结束
<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
<Item>
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<FilePath>1544037242_1544039396</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-06T03:14:02</StartTime>--开始
<EndTime>2018-12-06T03:49:56</EndTime>------结束
<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
<Item>
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<FilePath>1544039396_1544041549</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-06T03:49:56</StartTime>--开始
<EndTime>2018-12-06T04:25:49</EndTime>------结束
<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
<Item>
<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<FilePath>1544041549_1544043703</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-06T04:25:49</StartTime>----开始
<EndTime>2018-12-06T05:01:43</EndTime>--------结束
<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
<Item>

<DeviceID>32028101021320000009</DeviceID>
<Name>....3</Name>
<FilePath>1544043703_1544045859</FilePath>
<Address>Address 1</Address>
<StartTime>2018-12-06T05:01:43</StartTime>----开始
<EndTime>2018-12-06T05:37:39</EndTime>--------结束
<Secrecy>0</Secrecy>
<Type>time</Type>
</Item>
</RecordList>
</Response>

这条 message 消息携带了 10 条，根据多响应消息的定义：
为缩短传输时间宜在每条响应消息中携带多条记录，每条响应消息携带记录上限为10000条
所以现在知道为啥可以一次性携带这么多条了吧，也知道为啥回复的 message 消息有多条了吧。
另外将所有回复的时间加在一起则为整段时间。

5. 联网系统实时流协议(MANSRTSP) 命令集

命令的名称和说明

媒体回放控制命令由客户端到服务器的请求消息和由服务器到客户端的应答消息完成，请求和应答引用 RTSP(IETF RFC2326) 协议中的部分请求和应答消息格式。
消息包括一起始行，一个或多个消息头(message header) 、 一个表示标题头结束的空行(即 CRLF 前没有内容的行) 和一个消息体(可选) 。 示例如下:
message=start-line
message header
CRLF
[message body]
消息有请求和应答两种，在每对请求—应答消息中，应包含相同的 CSeq 头域，具体描述如下:
a) 请求
请求消息的起始行格式为 Method SP RTSP-Version CRLF。
其中 Method: 请求命令; SP : 空白符;RTSP-Version: 协议版本号; CR: 回车; LF: 换行。
请求命令包括: **PLAY , PAUSE , TEARDOWN**。------记住这里，只有三种 播放---暂停---停止
b) 应答
应答消息的起始行格式为 Status-Line = RTSP-Version SP Status-Code SP Reason-PhraseCRLF。其中 RTSP-Version: 协议版本号;Status-Code :3 位状态码，用于回应请求时表示主机状态;Reason-Phrase: 是与状态码对应的文本解释。

命令定义

客户端发送 PLAY 请求消息，请求服务器发送媒体。应支持 Range 头，在 Range 头中给出播放时间范围，播放指定时间段的媒体,见 IETF RFC 2326—1998 的 12.29; 时间范围应支持 npt、smpte 相对时间戳范围。 服务器的响应消息中给出 RTP-Info 头信息, IETF RFC2326—1998 的 12.33。

Range 头取值为“ntp=now-”，不携带 Scale 头，表示从暂停位置以原倍速恢复播放。
示例:
PLAY RTSP/1.0
CSeq: 2
Range: npt=now

暂停播放命令
客户端发送 PAUSE 请求消息，请求服务器暂停发送媒体，但不释放资源。 见 IETF RFC 2326—1998 的 10.6。
PauseTime 取值固定为“now”，表示视频停止在当前位置。
示例:
PAUSE RTSP/1.0
CSeq: 1
PauseTime: now

快进/慢进命令
在客户端发送的 PLAY 请求消息中，应使用 Scale 头来控制播放的快慢，见 IETF RFC2326—1998 的 12.34。 Scale 为 1，正常播放;不等于 1，为正常播放速率的倍数; 负数为倒放。快进/ 慢进命令应只携带 Scale 头，表示从当前位置开始以指定的倍速播放，不携带 Range 头。
示例:
PLAY RTSP/1.0
CSeq: 3
Scale: 2.0

随机拖放命令
在客户端发送的 PLAY 请求消息中，应支持 Range 头域，使用 smpte 相对时间戳范围，实现随机拖放播放，表示按当前播放速度跳转到 Range 头指定的时间点，不携带 Scale 头。
示例:
PLAY RTSP/1.0
CSeq: 4
Range: npt=100-

停止命令
客户端发送 TEARDOWN 请求消息，停止发送指定流，结束会话，并释放资源。

应答命令

客户端、 服务器端应支持应答命令的状态码 200、4xx 以及 5xx。 见 IETF RFC2326。

Scale 和 Range 头域取值范围

Scale 头应支持的基本取值为 0.25、0.5、1、2、4。

Range 头的值为播放录像起点的相对值, 取值范围为 0 到播放录像的终点时间, 参数以 s 为单位,**不能为负值。 如 Range 头的值为 0, 则表示从起点开始播放,Range 头的值为 100, 则表示从录像起点后的 100 s 处开始播放,Range 头的取值为 now 表示从当前位置开始播放。**

6. 目录查询

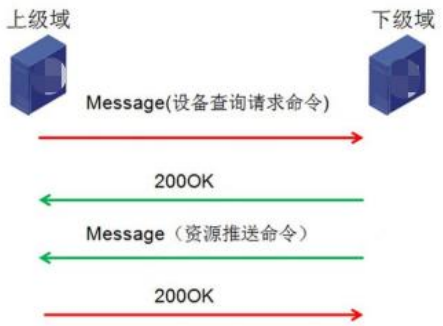
各位广大的视频监控的朋友，你什么时候需要做“目录查询”这个动作？以下几点原因仅供参考

1） 平台国标对接后，通过目录查询将下级推送的资源查询出来

2）排错（如在线状态状态不对，前端设备数量问题，设备类型不对，目录结构不对等等）

这两个原因应该是广大监控工程师最常用的两个，没有之一，有莫有？

命令流程



说明：

1）上级首先向下级发送 message 进行设备查询请求

2） 下级收到请求后，给上级回复好的，马上发送资源过来

3） 下级发送资源，每一条携带的资源不超过 4 个，且 SN 序列号相同，标识一次响应查询的结果

4）下级每发送一条消息，上级都要回复一条收到的消息，这样才算一个完整的流程

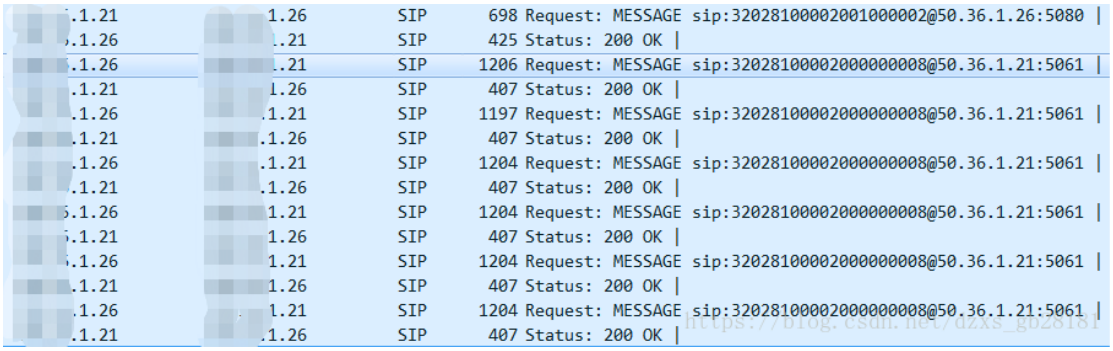
案例结合

1）组网介绍

上级 宇视平台 50.36.X.21 平台国标 ID 32028100002000000008

下级 科达平台 50.36.X.26 平台国标 ID 32028100002001000002

2）报文分析



除了第一条 message 消息为命令请求外，其余的 message 消息都为响应消息

说明

1)第一条 message 字段结构分析

<?xml version="1.0" encoding="GB2312"?>

<Query>----------查询

<CmdType>Catalog</CmdType>----------命令类型

<SN>86</SN>----------序列号

<DeviceID>32028100002001000002</DeviceID>----------下级设备 ID

</Query>

2) 第二条 message 字段结构分析

<?xml version="1.0"?>

<Response>

<CmdType>Catalog</CmdType>

<SN>86</SN>----------与第一条 SN 号相同，表明同一批会话

<DeviceID>32028100002001000002</DeviceID>-------本设备国标编码

<SumNum>259</SumNum>----------推送数量 259

<DeviceList Num="1">----------本次推送数量

<Item>

<DeviceID>32028100002160000002</DeviceID>------设备 ID（这边是目录，如果 11-13 是 132 则为摄像机），216 可以看出是通过虚拟分组推送的

<Name>Surveillance system</Name>----------设备名称

<Manufacturer>QX</Manufacturer>----------厂商

<Model>QX</Model>----------型号

<Owner>QX</Owner>----------设备归属

<CivilCode>320281</CivilCode>----------行政区划编码

<Block></Block>----------警区

<Address></Address>----------设备安装地址，国标没具体说，应该是前端配置的 IP 地址

<Parental>1</Parental>----------存在子设备，这里表明有子目录存在

<ParentID>32028100002001000002</ParentID>---父设备 ID

<RegisterWay>1</RegisterWay>----------符合 IETF RFC 3261 标准的认证注册模式

<Secrecy>0</Secrecy>----------0 表示不涉密

<Status>ON</Status>----------ON 表示在线

<Longitude>0.000000</Longitude>----------经度

<Latitude>0.000000</Latitude>----------纬度

<Info></Info>----------info 消息，这边没有，容易产生一个问题，设备类型是枪机还是球机，在做目录查询的时候，你会发现要么全部球机，要么全部枪机

</Item>

</DeviceList>

</Response>

3) 第三条 message 字段结构分析

<?xml version="1.0"?>

<Response>

<CmdType>Catalog</CmdType>

<SN>86</SN>

<DeviceID>32028100002001000002</DeviceID>

<SumNum>259</SumNum>

<DeviceList Num="1">

<Item>

<DeviceID>32028100002160000003</DeviceID>---推送的设备 ID，可以看出这边也是一个目录

<Name>…….</Name>

<Manufacturer>QX</Manufacturer>

<Model>QX</Model>

<Owner>QX</Owner>

<CivilCode>320281</CivilCode>

<Block></Block>

<Address></Address>

<Parental>1</Parental>----------有子设备,说明这个目录下有相机或者目录，看下一条 message 消息就知道

<ParentID>32028100002160000002</ParentID>---父目录 ID

<RegisterWay>1</RegisterWay>

<Secrecy>0</Secrecy>

<Status>ON</Status>

<Longitude>0.000000</Longitude>

<Latitude>0.000000</Latitude>

<Info></Info>

</Item>

</DeviceList>

4）第四条 message 字段分析

<?xml version="1.0"?>

<Response>

<CmdType>Catalog</CmdType>

<SN>86</SN>

<DeviceID>32028100002001000002</DeviceID>

<SumNum>259</SumNum>

<DeviceList Num="1">

<Item>

<DeviceID>32028101001320000071</DeviceID>--------目录下的摄像头

<Name>.....B2135.._1</Name>

<Manufacturer>QX</Manufacturer>

<Model>QX</Model>

<Owner>QX</Owner>

<CivilCode>320281</CivilCode>

<Block></Block>

<Address></Address>

<Parental>0</Parental>----------------------------没有子设备，说明该目录下没有子目录

<ParentID>32028100002160000003</ParentID>---父目录 ID

```
<RegisterWay>1</RegisterWay>
<Secrecy>0</Secrecy>
<Status>ON</Status>
<Longitude>0.000000</Longitude>
<Latitude>0.000000</Latitude>
<Info></Info>
</Item>
</DeviceList>
</Response>
```


总结：该组织结构如下图所示

目录（32028100002001000002）----------------------系统设备 ID

子目录（32028100002160000002）----------------虚拟目录

子目录（32028100002160000003）----------虚拟目录

子设备（32028101001320000071）----摄像机

子设备（32028101001320000072）----摄像机

。。。。。。。。。。。。。。。。。。。。。。。。。 -----摄像机

字段解释

```
<complexType name="itemType">
<sequence>
<!-- 设备/区域/系统编码（必选） -->
<element name="DeviceID" type="tg:deviceIDType"/>
<!-- 设备/区域/系统名称（必选） -->
<element name="Name" type="string"/>
<!-- 当为设备时，设备厂商（必选） -->
<element name=" Manufacturer" type="string"/>
<!-- 当为设备时，设备型号（必选） -->
<element name=" Model" type="string"/>
<!-- 当为设备时，设备归属（必选） -->
<element name=" Owner" type="string"/>
<!-- 行政区域（必选） -->
<element name="CivilCode" type="string"/>
<!-- 警区（可选） -->
```

<element name="Block" type="string"/>
<!-- 当为设备时，安装地址（必选） -->
<element name="Address" type="string"/>
<!-- 当为设备时，是否有子设备（必选） 1 有， 0 没有 -->
<element name="Parental" type="integer" minInclusive value = "0"/>
<!-- 父设备/区域/系统 ID（ 可必选，有父设备需要填写） -->
<element name="ParentID" type="string"/>
<!-- 信令安全模式（可选）缺省为 0； 0：不采用； 2： S/MIME 签名方式； 3：S/MIME 加密签名同时采用方式； 4：数字摘要方式-->
<element name=" SafetyWay " type="integer" minInclusive value = "0"/>
<!-- 注册方式（必选）缺省为 1； 1： 符合 sip3261 标准的认证注册模式； 2：基于口令的双向认证注册模式； 3： 基于数字证书的双向认证注册模式-->
<element name="RegisterWay" type="integer" minInclusive value = "1"/>
<!-- 证书序列号（有证书的设备必选） -->
<element name="CertNum" type="string"/>
<!-- 证书有效标识（有证书的设备必选）缺省为 0；证书有效标识： 0：无效 1：有效-->
<element name="Certifiable" type="integer" minInclusive value = "0"/>
<!-- 无效原因码（有证书切且证书无效的设备必选） -->
<element name="ErrCode" type="integer" minInclusive value = "1"/>
<!-- 证书终止有效期（有证书的设备必选） -->
<element name="EndTime" type="dateTime"/>
<!-- 保密属性（必选）缺省为 0； 0：不涉密， 1：涉密-->
<element name="Secrecy" type="integer" minInclusive value = "1"/>
<!-- 设备/区域/系统 IP 地址（可选） -->
<element name="IPAddress" type="string"/>
<!-- 设备/区域/系统端口（可选） -->
<element name="Port" type="integer"/>
<!-- 设备口令（可选） -->
<element name="Password" type="string"/>
<!-- 设备状态（必选） -->
<element name="Status" type=" tg:statusType"/>
<!-- 经度（可选） -->
<element name="Longitude" type="double" minOccurs= "0"/>
<!-- 纬度（可选） -->
<element name="Latitude" type="double" minOccurs= "0"/>
<Info>
<!--摄像机类型扩展，标识摄像机类型： 1-球机； 2-半球； 3-固定枪机；4-遥控枪机。当目录项为摄像机时可选。 -->
<element name="PTZType" type="integer" minInclusive value = "1"/>
<!--摄像机位置类型扩展。 1-省际检查站、 2-党政机关、 3-车站码头、 4-中心广场、 5-体育场馆、 6-商业中心、 7-宗教场所、 8-校园周边、 9-治安复杂区域、 10-交通干线。当目录项为摄像机时可选。 -->
<element name="PositionType" type="integer" minInclusive value ="1"/>
<!--摄像机安装位置室外、室内属性。 1-室外、 2-室内 。当目录项为摄像机时可选，缺省

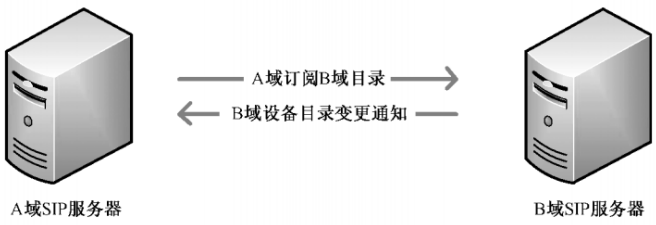
```
为 1。 -->
<element name="RoomType" type="integer" minInclusive value = "1"/>
<!--摄像机用途属性。 1-治安、 2-交通、 3-重点。当目录项为摄像机时可选。 -->
<element name="UseType" type="integer" minInclusive value = "1"/>
<!--摄像机补光属性。 1-无补光、 2-红外补光、 3-白光补光。当目录项为摄像机时可选，缺省为 1。 -->
<element name="SupplyLightType" type="integer" minInclusive value= "1"/>
<!--摄像机监视方位属性。 1-东、 2-西、 3-南、 4-北、 5-东南、 6-东北、7-西南、 8-西北。当目录项为摄像机时且为固定摄像机或设置看守位摄像机时可选。 -->
<element name="DirectionType" type="integer" minInclusive value ="1"/>
<!--摄像机支持的分辨率，可有多个分辨率值，各个取值见以“/” 分隔。分辨率取值参见国标附录 F 中 SDPf 字段规定。当目录项为摄像机时可选。-->
<element name="Resolution" type="string" minInclusive value ="1"/>
<!--虚拟组织所属的业务分组 ID，业务分组根据特定的业务需求制定，一
个业务分组包含一组特定的虚拟组织。 -->
<element name="BusinessGroupID" type="tg:deviceIDType"/>
</Info>
</sequence>
</complexType>
```

7. 目录订阅与通知

联网系统间采用订阅通知机制实现状态变化的设备信息的传送，用于提供联网系统间设备状态一致性的维护机制。 SIP 域可通过订阅方式订阅其他 SIP 域的全部或部分目录的离线、上线、增加、删除、更新等变更信息；被订阅域在目录变更后，应将变更事件通知订阅域。订阅通知消息使用 IETF RFC3265 规定的 SUBSCRIBE、NOTIFY 方法实现。

某一 SIP 域可进行其他多个 SIP 域目录信息的订阅，也可接受其他多个 SIP 域的订阅。 本域保存订阅目录、被订阅目录列表，在本域被订阅目录变更后向订阅域发送通知消息，订阅域接收到通知消息后进行相应更新处理。

订阅方式



小伙伴们根据你的工作经验，你认为 A 域订阅 B 域，有几种订阅方式？

根据 DZ 君的工作经验，目前 DZ 君只遇到了 A 域订阅 B 域的系统 ID，因为 DZ 君遇到的平台还不可以订阅下级域的目录，也没有操作过其他的订阅方式。

没关系，那就跟 DZ 君一起学习下国标 28181-2016 里的定义吧，咱一起学习一起进步。
国标标准定义了以下几种订阅方式：

1）A 订阅 B 的系统 ID------最常用的
释：B 域检测到直属目录和下级域的目录变更事件时应向 A 域发送通知消息;

2）A 订阅 B 的下级域系统 ID
释：B 域检测到对应此 ID 的下级系统范围内的目录变更事件时应向 A 域发送通知消息;

3）A 订阅 B 的行政区划编码
释：B 域检测到属于此行政区划的目录变更事件时应向 A 域发送通知消息

4）A 订阅 B 的设备 ID
释：B 域检测到该设备及其下属子设备发生目录变更事件时应向 A 域发送通知消息;

5）A 订阅 B 的上报业务分组 ID，虚拟组织 ID
释：B 域检测到该业务分组、虚拟组织下属虚拟组织、设备发生目录变更事件时应向 A 域发送通知消息

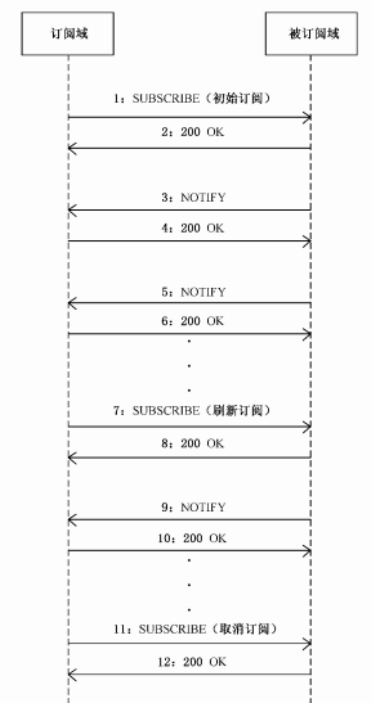
刷新订阅

A 域在初始订阅成功之后，应在过期之前向 B 域发送刷新订阅消息，进行订阅状态维护。
刷新订阅消息与初始订阅消息属于同一会话，并且 Expire 头域值大于 0.
初始化订阅时，Expire 头域值国标定义可以配置，默认为 600s。

取消订阅

（两种方式：主动和被动）
主动： A 订阅 B，A 主动取消订阅。取消订阅请求应与初始订阅请求属于同一会话，并且 Expire 头域值为 0
被动： A 订阅 B，B 域可通过发送 subscription-state 头域为 terminated 的 NOTIFY 消息主动结束订阅，NOTIFY 消息体可为空，订阅方接收到该消息后回复 200 OK 响应。

命令流程



命令流程描述如下:

1: 订阅域向被订阅域发送初始订阅 SUBSCRIBE 消息，订阅目的域的目录变更事件，消息头域中使用 Event 头域描述订阅事件，消息体中携带订阅的详细参数，使用 Expire 头域指定订阅过期时间;

2: 被订阅域设备收到订阅消息后，向订阅域发送 200 OK 响应;

3: 对于初始订阅操作，被订阅域立即发送 NOTIFY 消息携带离线及其他异常状态设备目录，消息头域中使用 Event 头域描述订 阅事件;

4: 订阅域收到 NOTIFY 消息后回复 200 OK 响应;

5: 被订阅域目录变更后，通过 NOTIFY 消息将变更事件通知订阅域，消息头域中使用 Event 头域描述订阅事件;

6: 订阅域收到 NOTIFY 消息后回复 200 OK 响应;

7: 订阅域在过期之前向被订阅域发送刷新订阅 SUBSCRIBE 消息，订阅目的域的目录变更事件，消息头域中使用 Event 头域描述订 阅事件，消息体中携带订阅的详细参数，使用 Expire 头域指定订阅过期时间;

8: 被订阅域设备收到订阅消息后，向订阅域发送 200 OK 响应;

9: 被订阅域目录变更后，通过 NOTIFY 消息将变更事件通知订阅域，消息头域中使用 Event 头域描述订阅事件;

10: 订阅域收到 NOTIFY 消息后回复 200 OK 响应;

11: 订阅域向被订阅域发送取消订阅 SUBSCRIBE 消息，消息头域中使用 Event 头域描述订阅事件，消息体中携带订阅的详细参数,Expire 头域值为 0;

12: 被订阅域设备收到订阅消息后，向订阅域发送 200 OK 响应，取消向订阅域发送目录变更通知消息。

案例结合

第一步：SUBSCRIBE 消息

第三步：NOTIFY 消息，初始订阅上报离线及异常设备状态

第五步： NOTIFY 消息暂时没抓，后期补上

第七步：刷新订阅是比较难抓的，有机会抓来展示

第九步：后期补上

第十一步：来看下主动取消吧，被动取消有机会可以的话，补上，因为 DZ 在做的时候是先取消的订阅，在订阅的，所以这边的 CALL-id 和订阅的 CALL-ID 不一致

字段解释

订阅消息与通知消息体（国标规范）

订阅消息消息体示例如下:

```
< ? xml version="1.0" ?>
<Query>
    < ! -- 命令类型: 目录订阅(必选) -->
    <CmdType>Catalog</CmdType>
    < ! -- 命令序列号(必选) -->
    <SN> 命令序列号</SN>
    < ! -- 订阅的系统/行政区划/设备/业务分组/虚拟组织编码(必选) -->
    <DeviceID> 订阅编码</ DeviceID>
</Query>
```

通知消息消息体示例如下，增加/更新目录通知消息中 Item 的字段参数应遵循 A.2.1g) 的规定:

```
< ? xml version="1.0" ?>
<Notify>
    < ! -- 命令类型: 目录订阅(必选) -->
    <CmdType>Catalog</CmdType>
    < ! -- 命令序列号(必选) -->
    <SN> 命令序列号</SN>
    < ! -- 订阅的系统/行政区划/设备/业务分组/虚拟组织编码(必选) -->
    <DeviceID> 订阅编码</DeviceID>
    < ! -- 通知消息中 SumNum 取值与 DeviceList 中 Num 取值相同(必选) -->
    <SumNum>2</SumNum>
    <DeviceList Num="2">
```

```
        <Item>
            <!-- 状态改变的系统/设备/行政区划编码(必选) -->
            <DeviceID> 编码 1</DeviceID>
            <!-- 状态改变事件 ON: 上线, OFF: 离线, VLOST: 视频丢失,DEFECT: 故障,
            ADD: 增加,DEL: 删除,UPDATE: 更新(必选) -->
            <Event>OFF</Event>
        </Item>

        <Item>
            <!-- 状态改变的系统/设备/行政区划编码(必选) -->
            <DeviceID> 编码 n</DeviceID>
            <!-- 状态改变事件 ON: 上线, OFF: 离线, VLOST: 视频丢失,DEFECT: 故障,
            ADD: 增加,DEL: 删除,UPDATE: 更新(必选) -->
            <Event>ADD</Event>
            <Name>IPC_天山视频</Name>
            < Manufacturer>XXX</Manufacturer>
            < Model>1.0</Model>
            <Owner>0</Owner>
            <CivilCode>650102</CivilCode>
            <Address>axy</Address>
            <Parental>0</Parental>
            <RegisterWay>1</RegisterWay>
            <Secrecy>0</Secrecy>
            <Status>ON</Status>
        </Item>
    </DeviceList>
</Notify
```

8. 多响应消息传输

多响应介绍

目录查询响应、 文件查询响应、 订阅后的通知消息会出现响应、 通知消息需发送多条记录的情况, 此时可通过多条响应、 通知消息对记录进行分批传送, 各响应消息的 SN 值需与请求消息相同。 为了保证多条响应、 通知消息传输的稳定可靠, 多条响应、 通知消息发送时宜采用串行发送方式, 记录发送方需收到上一条 SIP Message 消息的 SIP 响应后再进行后续发送处理。 待发送记录条数达到百条级别时, 为缩短传输时间宜在每条响应消息中携带多条记录, 每条响应息携带记录上限为 10000 条。

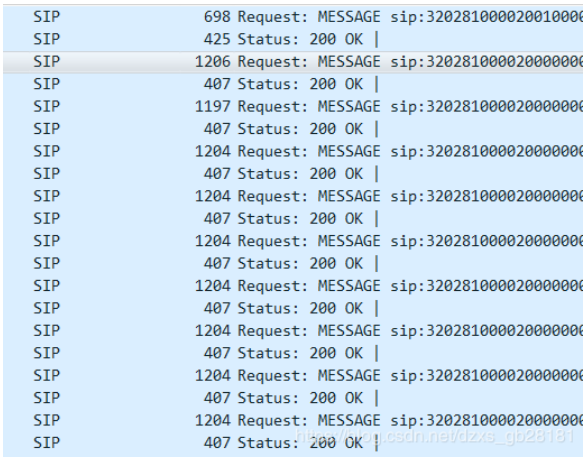
SIP 协议栈应支持 TCP 方式的 SIP 消息收发处理，处理机制应符合 IETF RFC 3261—2002 中第 18 章“Transport”的规定。
目录查询、 文件查询未查询出结果情况下返回响应中 SumNum 应取值为 0，且不携带记录列表。
以文件查询响应作为示例如下:

```
< ? xml version="1.0" ?>
<Response>
<CmdType> RecordInfo </CmdType>
<SN>17430</SN>
<DeviceID>64010000001310000001</DeviceID>
<Name>Camera1</Name>
<SumNum>0</SumNum>
</Response>
```

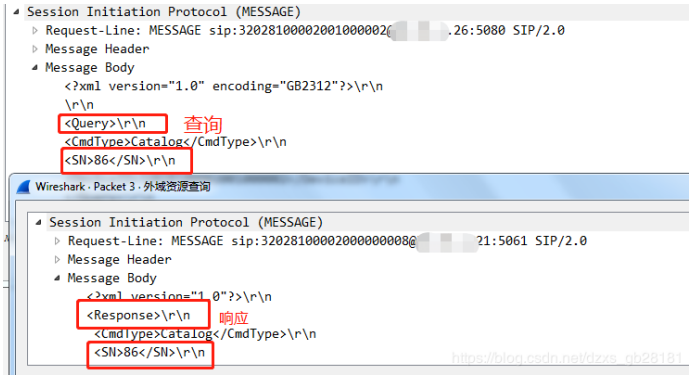
From : GB/T 28181 —2016 附录 N 定义，第 198 页

多响应应用

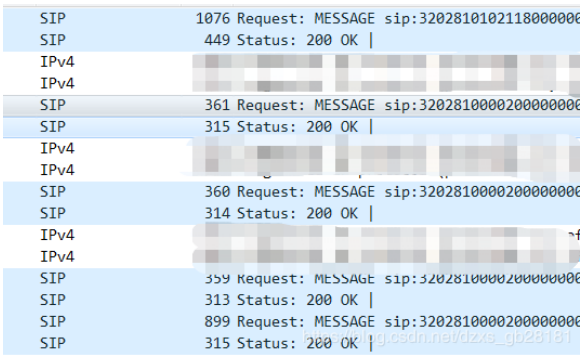
1. 目录查询多响应应用：



这是一个目录查询的报文，我们可以看到很多 message and 200Ok 的报文，第一个报文是查询，后面的 message 是响应报文，根据多响应消息的请求可以看到每条报文的 SN 值都是相同的。每条响应消息携带记录上限位 10000 条，这边是 1 条。如下：



2. 文件查询多响应消息应用

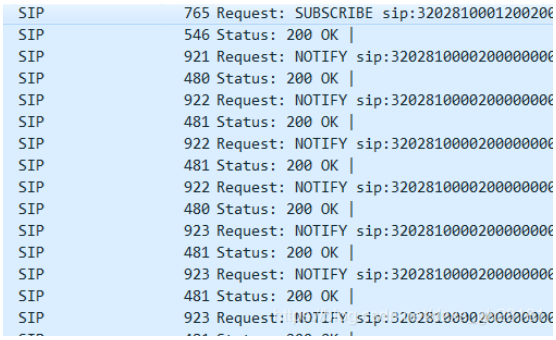


这是一个录像文件查询的报文，我们可以看到很多 message and 200Ok 的报文，第一个报文是查询，后面的 message 是响应报文，根据多响应消息的请求可以看到每条报文的 SN 值都是相同的。每条响应消息携带记录上限位 10000 条，这边是多条。如下：

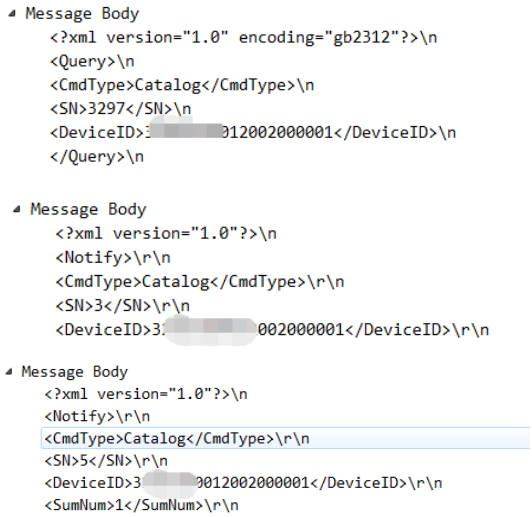
(查询)

（响应）

3. 订阅后通知消息应用



根据国标 2016 的定义，却发现订阅后的通知消息的 SN 值居然不同？打算找个时间发个邮件问问官方啥情况？



注意：三张图的 SN 值都是不同的哦!!! ----我已经给技术委员会发了邮件，等待给答复中。

总结：多响应消息关注以下三点

1. 目录查询响应、 文件查询响应、 订阅后的通知消息（待国标委员会验证）
2. SN 值
3. 携带多条记录不超过 10000 条

9. 基于 RTP 的视音频封装

基于 RTP 的视音频数据 PS 封装

基于 RTP 的 PS 封装首先按照 ISO/IEC13818-1:2000 将视音频流封装成 PS 包，再将 PS 包以负载的方式封装成 RTP 包。

进行 PS 封装时，应将每个视频帧封装为一个 PS 包，且每个关键帧的 PS 包中应包含系统头(System Header)和 PSM(Program Stream Map)，系统头和 PSM 放置于 PS 包头之后、 第一个 PES 包之前。

典型的视频关键帧 PS 包结构如图 C.1 所示，其中 PESV 为视频 PES 包,PESA 为音频 PES 包，视频非关键帧的 PS 包结构中一般不包含系统头和 PSM。PS 包中各部分的具体数据结构参见 ISO/IEC13818-1: 2000 中的相关描述。

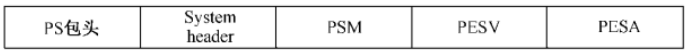


图 C.1　典型的视频关键帧 PS 包结构

系统头应包含对 PS 包中码流种类的描述，其中视频和音频的流 ID(stream_id) 取值如下:

a) 视频流 ID:0xE0;

b) 音频流 ID:0xC0。

针对本文档规定的几种视音频格式,PSM 中流类型(stream_type) 的取值如下:

a) MPEG-4 视频流:0x10;

b) H.264 视频流:0x1B;

c) SVAC 视频流:0x80;

d) G.711 音频流:0x90;

e) G.722.1 音频流:0x92;

f) G.723.1 音频流:0x93;

g) G.729 音频流:0x99;

h) SVAC 音频流:0x9B。

PS 包封装的其他具体技术规范详见 ISO/IEC13818-1:2000。

PS 包的 RTP 封装格式参照 IETF RFC2250,RTP 的主要参数设置如下:

a) 负载类型(payloadtype) :96;

b) 编码名称(encoding name) :PS;

c) 时钟频率(clockrate) :90 kHz;

d) SDP 描述中“m”字段的“media”项:video。

基于 RTP 的视音频基本流封装

该方式直接将视音频数据以负载的方式封装成 RTP 包。

C.2.1 MPEG-4 视频流的 RTP 封装

MPEG-4 视频流的 RTP 封装格式应符合 IETF RFC3016 协议中的相关规定。

MPEG-4 视频流 RTP 包的负载类型(Payload Type) 标识号选定: 从 IETF RFC 3551—2003 表 5 中的动态范围(96~127) 中选择，建议定为 97。

C.2.2 H.264 视频流的 RTP 封装

H.264 的 RTP 载荷格式应符合 IETF RFC3984 中的相关规定。

H.264 视频流 RTP 包的负载类型(Payload Type) 标识号选定: 从 IETF RFC3551—2003 表 5 中的动态范围(96~127) 中选择，建议定为 98。

C.2.3 SVAC 视频流的 RTP 封装

SVAC 视频流的 RTP 载荷格式可参照 IETF RFC3984 中的相关规定。

SVAC 视频流 RTP 包的负载类型(Payload Type) 标识号选定: 从 IETF RFC 3551—2003 表 5 中的动态范围(96~127) 中选择，建议定为 99。

C.2.4 音频流的 RTP 封装

语音比特流宜采用标准的 RTP 协议进行打包。

在一个 RTP 包中，音频载荷数据应为整数个音频编码帧，且时间长度在 20 ms~180 ms 之间。

音频载荷数据的 RTP 封装参数如下:

a) G.711 的主要参数

G.711 A 律语音编码 RTP 包的负载类型(Payload Type) 的参数规定如下(见 IETF RFC3551—2003 中的表 4) :

1) 负载类型(PT) :8;

2) 编码名称(encoding name) :PCMA;

3) 时钟频率(clockrate) :8 kHz;

4) 通道数:1;

5) SDP 描述中“m”字段的“media”项:audio。

b) SVAC 音频的主要参数

SVAC 语音编码 RTP 包的负载类型(Payload Type) 的参数规定如下:

1) 负载类型(PT) :20;

2) 编码名称(encoding name) :SVACA;

3) 时钟频率(clockrate) :8 kHz;

4) 通道数:1;

5) SDP 描述中“m”字段的“media”项:audio。

c) G.723.1 的主要参数

G.723.1 语音编码 RTP 包的负载类型(Payload Type) 的参数规定参照 IETF RFC3551—2003 表 4 中的 G.723, 具体如下:

1) 负载类型(PT) :4;

2) 编码名称(encoding name) :G723;

3) 时钟频率(clockrate) :8 kHz;

4) 通道数:1;

5) SDP 描述中“m”字段的“media”项:audio。

d) G.729 的主要参数

G.729 语音编码 RTP 包的负载类型(Payload Type) 的参数规定如下(见 IETF RFC 3551—2003 中的表 4) :

1) 负载类型(PT) :18;

2) 编码名称(encoding name) :G729;

3) 时钟频率(clockrate) :8 kHz;

4) 通道数:1;

5) SDP 描述中“m”字段的“media”项:audio。

e) G.722.1 的主要参数

G.722.1 语音编码 RTP 包的负载类型(Payload Type) 的参数规定参照 IETF RFC3551—2003 表 4 中的 G.722, 具体如下:

1) 负载类型(PT) :9;

2) 编码名称(encoding name) :G722;

3) 时钟频率(clockrate) :8 kHz;

4) 通道数:1;

5) SDP 描述中“m”字段的“media”项:audio。

第三章 Trouble Shooting

1. 捣鬼的网闸

案发背景

曾经某局点“尸地”为了增强打僵尸的能力，以及提高整体作战的能力，增加了两台“大炮”（流媒体），并配置了两个导火芯（IP 地址为 192.168.1.99 和 101），当天白日里，DZ 君冒死完成了炮台的搭建，且大炮已经开始自动攻击僵尸（流媒体正常转发，业务正常），完美保障了“作战指挥中心”。当晚，卫兵报出指挥中心遭到攻击的消息，说大炮已经不发射炮弹了（流媒体不转发了）。警报响起，各级领导找到我，要求我立即找出原因，恢复大炮的工作。于是 DZ 君首先就找到了白天了的大炮部署线路图（组网），查看到底是哪里的问题？

大炮部署线路图（组网图）

污染区A　　A和B之间的时空隧道　　污染区B

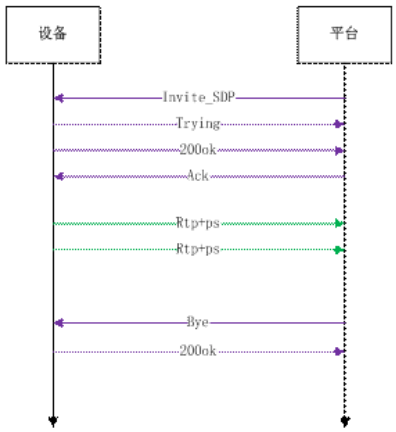
下级平台（192.168.1.1）------（192.168.1.254）网闸（192.168.2.254）-----（192.168.2.1）上级平台

下级平台大炮M1（流媒体）=192.168.1.99　　上级平台大炮M1（流媒体）=192.168.2.4

下级平台大炮M2（流媒体）=192.168.1.101　　下级平台大炮M2（流媒体）=192.168.2.5

在污染区 B（上级平台）看大炮打僵尸（实况），发现污染区 B 和污染区 A 之间时空隧道门被关闭了（信令通道建立失败），为了确定是时空隧道门的问题，DZ 君开启了透视镜（A 区和 B 区互抓）。但在透视之前，我们要先做一件事，那就是大炮攻击僵尸的正常流程是啥？

大炮正常工作流程（实况信令流程）



透视图（抓包分析）

1） 污染区 B 发给时空隧道门的 INVITE 消息

v=0

o=32028100002000000008 0 0 IN IP4 192.168.2.5

s=Play

c=IN IP4 192.168.2.5-----收流地址

t=0 0

m=video 18314 RTP/AVP 96----收流端口 18314 and 使用 UDP 传输

i=primary
a=recvonly
a=rtpmap:96 PS/90000
y=0281001908

2） 时空隧道门转发给污染区 A 的 INVITE 消息

v=0
o=32028100002000000008 0 0 IN IP4 192.168.1.254
s=Play
c=IN IP4 192.168.1.254----收流地址
t=0 0
m=video 14163 RTP/AVP 96---收流端口，使用 UDP 传输
i=primary
a=recvonly
a=rtpmap:96 PS/90000
y=0281001908

3） 污染区 A 转发给时空隧道门的 200Ok 消息

v=0
o=32028104001322004425 0 0 IN IP4 192.168.1.101
s=Play
c=IN IP4 192.168.1.101---发流地址
t=0 0
m=video 25950 RTP/AVP 96--发流端口
a=rtpmap:96 PS/90000
a=sendonly
y=0100005110
f=v/2/4/25/1/2000a/1/8/1

4） 时空隧道门转给污染区 B 的 200OK 消息

v=0
o=32028104001322004425 0 0 IN IP4 192.168.2.2501--纳尼，什么鬼，这什么 IPV4 地址？
s=Play
c=IN IP4 192.168.2.2501---纳尼，发流地址这就不存在啊
t=0 0
m=video 14163 RTP/AVP 96
a=rtpmap:96 PS/90000
a=sendonly
y=0100005110
f=v/2/4/25/1/2000a/1/8/1

甩锅

报告领导，我开启透视图分析过后，发现是时空隧道门转发出问题了，需要时空隧道门的厂家来处理。需要我的地方，我帮忙处理。虽然甩锅了，但是态度还是要给力的。

2. 流媒体双网卡绑定之超实用绑定法

案发背景

曾经 DZ 君刚入职不久，接下某个大盘，信通大队长是个高富帅的牛逼的人物，某日 call me：这边政务网的视频怎么那么卡的啊，经常顿啊顿的，刚开始的时候平台只有两台媒体服务器，还是千兆单网卡，那个时候 DZ 君也不是很懂，二线给的方案是做双网卡绑定，那个时候还没有具体步骤方案，就知道百度找方法做。后来发现绑定模式有 7 种之多，DZ 君找了其中一种方式做了，刚开始是好的，业务也正常，丫丫的，第二天业务就不正常了，发现同网段的居然 ping 不通了，有时候通，有时候又不通，真是蓝瘦香菇呀！

于是痛定思痛，经过几天的实验，DZ 君终于找到了超实用，有效的方法。第二天高富帅就在群里说，视频丝滑的一米。果断 666 啊。今天 DZ 君就把这种方法分享给广大的监控朋友们！一起丝滑！

原理：

在监控系统中，由于流媒体服务器可能存在大量转发要求，双网卡聚合成为一种选择，实现负载均衡、线路冗余功能。下面就流媒体上采用异或策略调度模式的双网卡聚合方式配置方法介绍如下（其他服务器配置方法类似）：

采用异或策略时有两种方式，

xmit_hash_policy=0 表示根据 Layer2，(源 MAC 地址 XOR 目标 MAC 地址) % slave 数量。

xmit_hash_policy=1 表示 Layer3+4，（(源 IP XOR 目的 IP）XOR（源端口 XOR 目的端口)）% slave 数量

如果流媒体流量转发的接收者与流媒体不在同一个网络，则需要使用 xmit_hash_policy=1 ——使用这种方式是比较优质的方式

双网卡配置方法

系统： Centos x64 位 可以用命令 cat /etc/issue 查看 (32 位和 64 位都可以）

绑定模式： lay3+4(1) 同时交换机上也要配置这种模式

绑定网卡名：eth1 and eth2 or eth3 and eth4 最好不要用管理口 eth0

1) 网卡 bond0 的配置

```
DEVICE=bond0
BOOTPROTO=static
TYPE=Ethernet
BROADCAST=192.168.1.255
IPADDR=192.168.1.1
NETWORK=192.168.1.0
NETMASK=255.255.255.0
NM_CONTROLLED=no
ONBOOT=yes
```

BONDING_OPTS="mode=2 xmit_hash_policy=1 miimon=100"

2) 网卡 eth1 的配置
DEVICE=eth1
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
USERCTL=no
SLAVE=yes

3） 网卡 eth2 的配置
DEVICE=eth2
BOOTPROTO=none
ONBOOT=yes
MASTER=bond0
USERCTL=no
SLAVE=yes

4）默认情况下，内核已支持 bonding，只需要简单修改/etc/modprobe.conf（如果没有，则在/etc/modprobe.d/手动创建 modprobe.conf 这个文件） 这个配置文档就可以了：
vi /etc/modprobe.d/modprobe.conf
添加一行 alias bond0 bonding

5）重启网卡 service network restart

6）查看是否生效
命令： cat /proc/net/bonding/bond0

Bonding Mode: load balancing (xor)--------xor 模式
Transmit Hash Policy: layer3+4 (1) --------3+4
MII Status: up----------up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0
Slave Interface: eth1----------网卡 eth1
MII Status: up----------网卡状态 up

Speed: 1000 Mbps----------速率 1000M
Duplex: full----------全双工
Link Failure Count: 1
Permanent HW addr: 48:ea:63:67:b1:bd
Slave queue ID: 0

Slave Interface: eth2----------网卡 eth2

MII Status: up----------网卡状态 up
Speed: 1000 Mbps----------速率 1000M
Duplex: full----------全双工
Link Failure Count: 1
Permanent HW addr: 48:ea:63:67:b1:be

Slave queue ID: 0

7） 查看 bond0 and eth1 and eth2 的硬件 mac 地址是否一致
[root@localhost ~]# ifconfig
bond0 Link encap:Ethernet HWaddr **48:EA:63:67:B1:BD**
inet addr:173.200.2.99 Bcast:173.200.3.255 Mask:255.255.254.0
inet6 addr: fe80::4aea:63ff:fe67:b1bd/64 Scope:Link
UP BROADCAST RUNNING MASTER MULTICAST MTU:1500 Metric:1
RX packets:656079838493 errors:135 dropped:26668095 overruns:0 frame:134
TX packets:276199894685 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:150000
RX bytes:650473453115237 (591.6 TiB) TX bytes:311169287987543 (283.0 TiB)

eth1 Link encap:Ethernet HWaddr **48:EA:63:67:B1:BD**
UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
RX packets:235935232796 errors:135 dropped:5002535 overruns:0 frame:134
TX packets:139210339998 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:150000
RX bytes:234400026297441 (213.1 TiB) TX bytes:156523007539641 (142.3 TiB)
Interrupt:18 Memory:cb400000-cb420000

eth2 Link encap:Ethernet HWaddr **48:EA:63:67:B1:BD**
UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
RX packets:420144605699 errors:0 dropped:21665560 overruns:0 frame:0
TX packets:136989554700 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:150000
RX bytes:416073426820456 (378.4 TiB) TX bytes:154646280461524 (140.6 TiB)
Interrupt:20 Memory:ce500000-ce520000

查看网卡流量
[root@localhost ~]# sar -n DEV 1 5--------命令后面 1 5 意思是：每一秒钟取一次值，取 5 次。

Average:	IFACE	rxpck/s	txpck/s	rxkB/s	txkB/s	rxcmp/s	txcmp/s	rxmcst/s
Average:	lo	2.00	2.00	0.14	0.14	0.00	0.00	0.00
Average:	eth2	9075.40	6597.80	9479.70	7732.77	0.00	0.00	0.00
Average:	slot0_GE4	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average:	slot0_GE3	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average:	slot0_GE2	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average:	slot0_GE1	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average:	eth1	4660.40	4596.00	5745.49	5019.62	0.00	0.00	0.00
Average:	eth0	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Average:	bond0	13735.80	11193.40	15225.19	12751.82	0.00	0.00	0.00

说明

IFACE：LAN 接口

rxpck/s：每秒钟接收的数据包

txpck/s：每秒钟发送的数据包

rxbyt/s：每秒钟接收的字节数----通过它可以算出网卡目前速率

txbyt/s：每秒钟发送的字节数----通过它可以算出网卡目前速率

rxcmp/s：每秒钟接收的压缩数据包

txcmp/s：每秒钟发送的压缩数据包

rxmcst/s：每秒钟接收的多播数据包

到这里为止，你已经距离丝滑已经更近了一步，因为让视频丝滑的影响原因有很多像丢包啊，乱序啊，服务器性能啊，显卡性能啊，网速啊等等，当然主要原因还是丢包，乱序和带宽

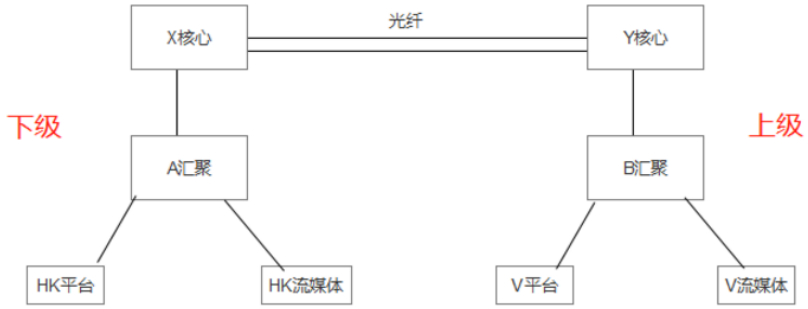
3. 隐形杀手之经典丢包乱序

最近很火的一款游戏吃鸡游戏，DZ 君也是跟着时代潮流走，曾经一次 DZ 君我背着一把 98K，一把 M24，在决赛圈躲在一颗树的后面，让人感到不可思议的是，最后就剩余我和敌人，不论我在树的什么位置他总能打到我，不过我 DZ 君也不是好欺负的，通过扫射，终于找到了地上的吉利服，成功吃鸡。我已经算是老阴 B 了，对手比我还阴。所以所以说隐形杀手是最可怕的。因为不容易发现，悄无声息的到来。

监控售后实施真的是一件很辛苦的事情，我们往往都是把握大方向，很多细节往往也容易忽略，我们经常只管搭建平台，吧业务实现即可，如能看实况和回放便可以了，其中还有一些隐患往往都是运行一段时间才能发现，如视频卡顿，因为卡顿的原因很多，但往往网络造成的原因是占 90%的，下面我们就来看一个大平台视频卡顿的案例。

案例分析

1）组网图



2）卡顿问题描述

电脑登录 V 平台看下级 HK 的视频卡顿，视频流是 UDP，请问你的排查步骤是什么？

3）可能原因

卡顿的原因嫌疑最大的两个原因：丢包和乱序

4） 排查步骤

（1）电脑直连 Y 核心，V 平台实况策略改为直接让下级 HK 流媒体发流过来。抓包分析发现无丢包有乱序。第一步就先暂时排除了自己的嫌疑

（2）电脑直连 A 汇聚，V 平台实况策略改为直接让下级 HK 流媒体发流过来，抓包分析发现，无乱序无丢包。第二部排除了 HK 流媒体发出来有问题

（3）电脑直连 X 核心，V 平台实况策略改为直接让下级 HK 流媒体发流过来，抓包分析发现，无乱序无丢包。第三部排除了 A 到 X 之间的网络乱序

（4）X 核心上抓到 Y 的视频报文，抓包分析发现，无乱序无丢包，第四部排除了 X 核心发出来有乱序的可能性

（5）Y 核心上抓接收的报文，抓包分析发现，无丢包有乱序，那就是 Y 核心存在问题

（6）经过某厂家的排查，发现是 Y 核心自身防火墙压力过大导致

排查口诀

去自己，查丢包，查乱序，无问题，查自己

4. 一倍速回放，前几秒倍速播放

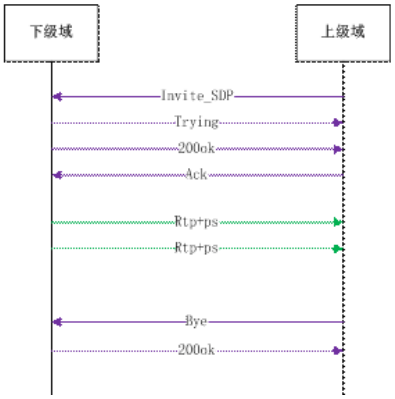
某日 DZ 君我正忙着新项目的各种测试，以及其他问题的处理，突然一个电话来了，显示周 XX，DZ 君第一反应，哎呀又啥事，喂，周兄，咋啦，他说我这边派出所点播回放，前 1 秒左右视频好像是在以 16 倍速播放，1 秒后就正常了，DZ 君由于忙着其他问题，先暂时放着了，没有处理，就在上周升级完某平台后，我发现了此问题，随后往其下级平台在看了下，仍然还是有这个问题，于是 DZ 君就开始了排查之路。下面 DZ 君就教下大家如何来排查？

排查思路

默认回放流程 invite ， 100try ， 200OK，ACK 这 4 个报文信令完成后，下级平台默认应以 1 倍速发流出来；

若鼠标点击录像进度条上的某个时刻，则录像默认还是以 1 倍速从那个点开始播放。

1） 回放流程



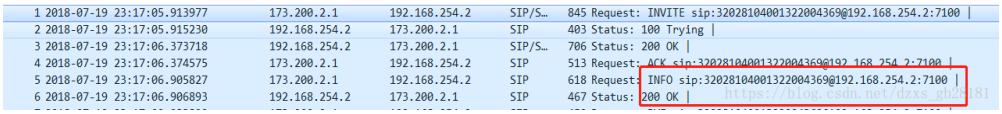
正常点击回放流程是 INVITE，100TRY，200OK 和 ACK。

2） INFO 消息

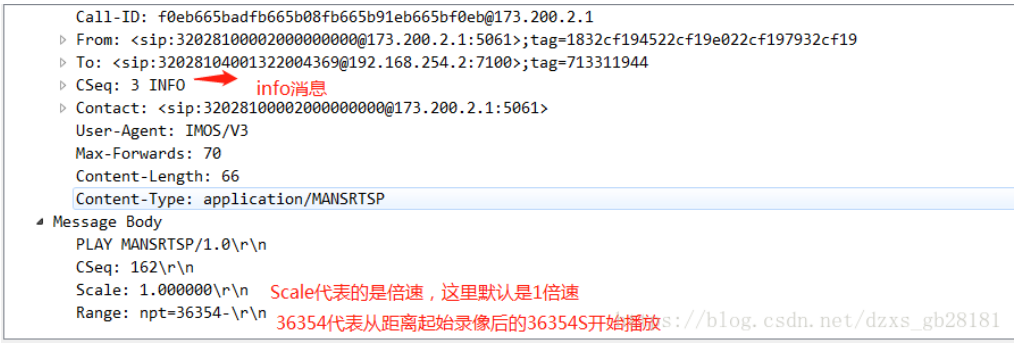
在进行点播的时候，如对检索出来的某一段录像，点击鼠标从某一刻开始看录像，那么这个时候，上级就会往下级平台发送 info 消息，下级平台往上级平台回复 200Ok 消息。

抓包分析

1） 抓信令



点开 INFO 消息看具体信息



下级平台从收到 ACk 开始就开始以高倍速的流发出来了，收到上级平台的 info 消息后，开始正常播放。

2） 抓媒体流

建议不经过本地流媒体，由下级平台的流媒体直接发送至电脑，这样比较有说服力，电脑上抓 10s 报文，看下第一个 UDP 报文和最后衹UDP 报文之间相差几秒，将报文转化成视频，发现视频流在以 1 倍速正常播放，但是总视频却是 5 分钟，说明什么？说明下级平台疯狂发流。10s 钟发了 5 分钟的视频。

谁的锅？下级平台的锅！

总结：回放信令流程走完，应以 1 倍速播放，除非收到上级平台的命令 INFO 消息，改变发流速率。

5. 刷新订阅是否存在？

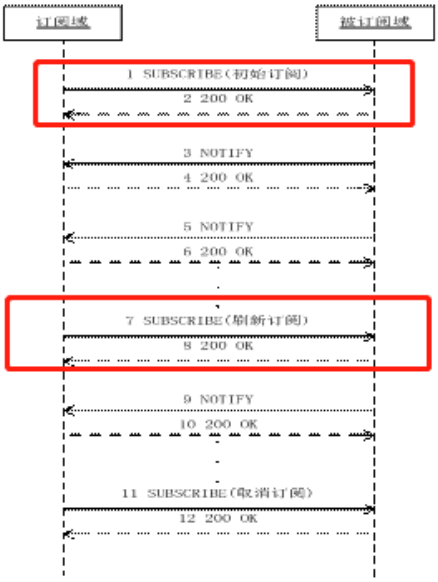
这是一个困扰我很久的问题，为了解决这个问题，DZ 先生曾把订阅相关的详细文档看了一遍，发现订阅缺乏保活机制，就是因为缺乏这个机制，在测试发现下级不上报状态后，下级平台是有理由说订阅是否仍然有效，刷新订阅是否有发。这边我们主要解决的问题是-刷新订阅是否存在？

测试平台组网搭建

上级平台（173.200.3.213）-----国标对接---下级平台（173.200.3.212）

注意：上下级平台所使用的软件及补丁一定要和真实平台一致，这很重要

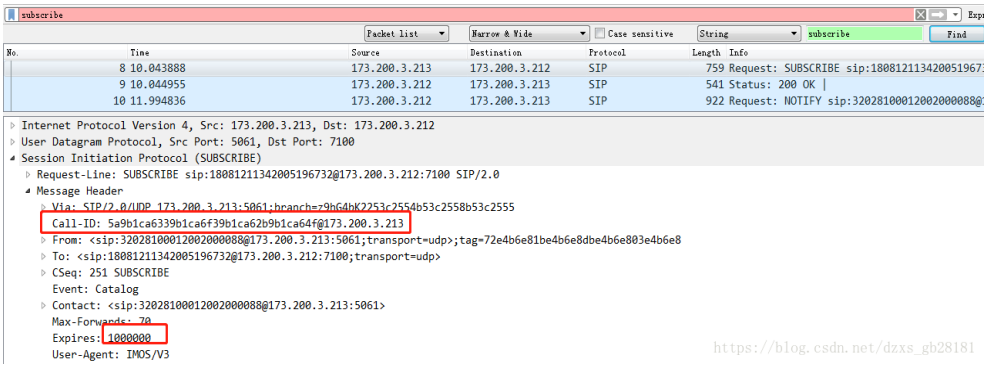
订阅流程介绍



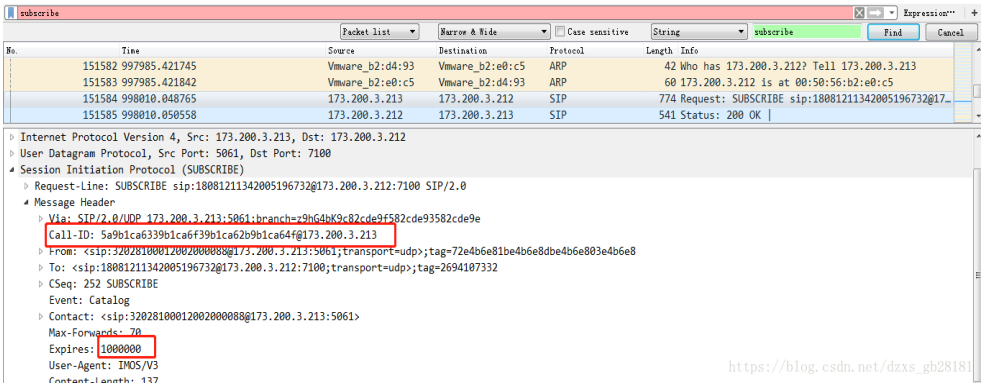
在这里我们要注意两点，第一点，首次订阅；第二点，刷新订阅。RFC3625 中定义，刷新订阅的 CALL-ID 和首次的订阅的 CALL-ID 是一致的。因此后面抓包，我们需要对比这两个 CALL-ID。

抓包分析

首次订阅报文



第二次的刷新报文



通过对比 CALL-ID 一致，表示第二次的订阅是刷新订阅。

总结：

上级成功订阅下级域，且刷新订阅通过抓包分析是存在的，那么下级平台过段时间不上报状态为下级平台的问题。

6. 国标网络标准

A 和 B 是邻居，AB 今年都挣到了钱，于是都决定建一栋楼房，A 和 B 于是各自叫了一只工程队 C 和 D。C 和 D 做事风格不一样，C 建楼房时从打地基开始，地基打的特别牢靠，而且一钻一瓦都严严实实，房子因此非常稳定。D 建房子时不打地基，从平地上直接盖，石头间距，瓦的间距也没有控制好。但粉刷过后，也能达到能住和好看的效果。A 和 B 验房子时都没有注意太多。于是都验收通过了。过了一段时间，B 发现房子不是漏水，就是有房子老鼠打洞。B 经常责怪天气糟糕，老鼠成灾，却没有想过房子的地基和盖房子的砖瓦控制达标问题。

同样的问题，**视频是建立在网络之上，没有好的网络质量就没有好的视频质量。**

视频网络标准

GB/T 28181 —2016（第 11 页 5.5 网络传输质量）

联网系统 IP 网络的传输质量(如传输时延、 包丢失率、 包误差率、 虚假包率等) 应符合如下要求:

a) 网络时延上限值为 400 ms
b) 时延抖动上限值为 50 ms
c) 丢包率上限值为 1×10-3----------丢包率是千分之一
d) 包误差率上限值为 1×10-4--------错报率的上限是万分之一
C and D 是视频质量的主要杀手

7. 论国标视频流端口奇偶性

今天 DZ 先生主讲的案例是关于国标视频流端口奇偶性的，DZ 先生在处理这个问题之前已经知道国标视频流端口定义为偶数，只是在我所负责大平台中，网闸把我的视频流端口改为了奇数，虽然业务一直正常，直到这次遇到严格规范的视频流端口的架构，网闸导致了我的平台信令报错。DZ 先生我曾经多次与网闸交锋，虽然保持着**的记录，但他们的言行，和服务态度让我决定利用这次机会再战一回。说问题之前想给大家介绍下国标 RTP 视频流端口奇偶数定义：
在 RFC 1889 的第 10 章中讲述到
10. RTP over Network and Transport Protocols
RTP relies on the underlying protocol(s) to provide demultiplexing of RTP data and RTCP control streams. For UDP and similar protocols, **RTP uses an even port number(RTP 使用一个偶数端口)** and the corresponding RTCP stream uses the next higher (odd) port number. **If an application is supplied with an odd number for use as the RTP port, it should replace this number with the next lower (even) number.（如果一个应用提供的 RTP 端口为奇数，它应该被替换掉用比它低一点的偶数，这边应该是相当于奇数-1 后的偶数）**

组网架构
上级平台（192.168.1.1）-----（192.168.1.254）网闸（10.1.1.254）----（10.1.1.1）下级平台

问题描述：
上级平台浏览下级平台的录像信令报错。

回放信令抓包分析（上下级平台互抓）
上级抓下级 invite 报文：
v=0
o=32028159031327200061 0 0 IN IP4 192.168.1.2
s=Playback
u=32028159031327200061:17577
c=IN IP4 192.168.1.2----------媒体收流地址
t=1541738382 1541743573
m=video 24930 RTP/AVP 96-------24930 为收流端口偶数

下级抓上级 invite 报文：
v=0
o=32028159031327200061 0 0 IN IP4 192.168.1.2
s=Playback

u=32028159031327200061:17577
c=IN IP4 10.1.1.254----------媒体收流地址
t=1541738382 1541743573
m=video 17413 RTP/AVP 96-------17413 为收流端口奇数

分析总结：
上级平台浏览录像向下级发送 invite 报文，告知下级平台的收流端口为偶数端口，网闸在进行转发 invite 报文的时候，将收流端口改为了奇数端口。此时需要网闸按照国标定义将收流端口改为偶数。（现实中，经过网闸整改后，业务恢复正常）

8. 海康国标错误码 1807

背景
人物：DZ 先生，金兄（楼长），貌兄（海康兄弟），X 市的坤兄（海康兄弟）
时间：2018 年 11 月 13 日
地点：A 市公安局 11 楼会议室
事件：将宇视两大大平台接入 X 市对应的大平台

对的没错，那一天我们讨论了很短的时间，因为海康兄弟比较专业，在进行一番专业的指点江山后，我们的坤兄很快推进了下一波工作，就在周四的傍晚，由我们的金兄和坤兄开始了对接。

国标对接
还记得前面案例 DZ 先生多次提到的国标对接的四大要素吗？不记得也没关系，DZ 先生在说一次，四大要素如下：
SIP 端口： 平台间对接的信令端口
服务地址：平台间对接的信令地址
中心国标 ID：20 位国标编码
鉴权账号和密码：可用可不用

我们的金兄和坤兄互相把自己平台的 sip 端口，SIP IP 及中心平台 20 位国标编码给了对方。双方都是成熟的大平台，都是操作老手了，按理说也不会有什么问题。然后意外发生了。对接失败，没有显示在线。坤兄经过抓包后分析，发现报错码为 1807,
Error-Info: <sip:0.0.0.0:5060;user=phone>;IMOS_AS_ERRORCODE=1807
DZ 先生随意对宇视国标错误码展开了排查，发现宇视没有 1807 这个错误码

1801	ERR_XP_WINDOW_ALREADY_SET	通道已被注册
1802	ERR_XP_EXCEED_MAX_PLAY_PORT_NUM	注册的播放通道数已超过了最大支持的播放通道数
1803	ERR_XP_NOT_SUPPORT	不支持该功能
1804	ERR_XP_UNKNOWN_ERROR	未知错误
1824	ERR_XP_DLL_NOT_EXIST	指定的动态库不存在
1825	ERR_XP_FAIL_TO_LOAD_DLL	加载动态库失败

海康兄弟查了海康的国标错误码：

1805	查询到的录像文件数为 0	无录像文件
1806	录像分页查询开始序号大于文件总数	
1807	查询超时，超过 30 秒 VRM 或者平台无结果返回	
1901	查询点播 url，对应文件列表不存在	查询超时，需重新查询录像文件列表
1902	查询点播 url，对应文件列表查询失败	
1903	查询点播 url，该文件在对应文件列表中	

找到了原因，针对这种错误码，一般接下来的处理是交给研发了，但好在我们的坤兄比较机智，检查了一下中心国标编码，发现自己给金兄的国标编码给错了。导致此错误。

分析

如果下级填写了错误的国标 ID，而注册的服务 ip 和 sip 端口是正确的，那么上级平台收到下级平台发送的注册报文后，发现 sip ip and port 都没有问题，但是 ID 在自己的平台里并没有这个 ID，这个时候我是不能给他注册的，因此返回这样一个报错给下级。

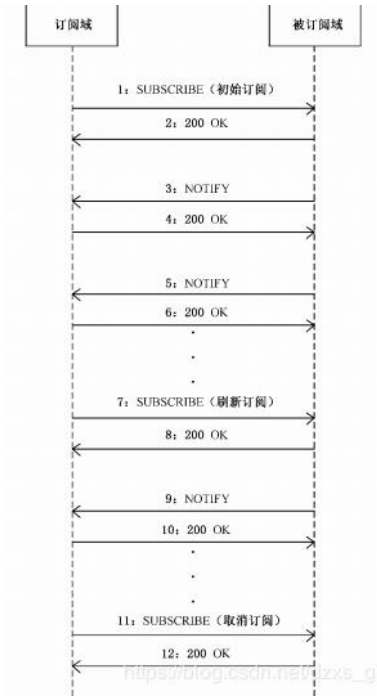
总结

1. 国标对接注意四大对接要素，一定多核对自己给别人的信息不能有错，不能因为小事而浪费更多精力来排错。
2. 下级平台注册上级海康平台，在 sip ip 和 port 没有问题的状态下，如果平台 ID 填错，海康会有报 1807 错误（各家平台不一样）。

9. 你真的订阅成功了吗？

2017 年，我和海康工程师貌貌先生相识，从此我们结下了缘分，因为在这里，我是他的上级，而他是我的下级，他有两个大平台，一个是 X1 小区出入口，一个是 X2 海康平台，且这两个平台的点位不可替代。某天我们的金师傅发现了上下级状态不一致，那一天是我们的烦恼的开始，而且这个问题已经拖了将近快大半年了，直到上周四晚上，终于解决了我们平台和 X1 小区出入口平台的状态不一致的问题。还剩余一个最大的平台 X2 待解决中。虽然待解决，但我们已经有了思路，最近我们也会很快将其解决。现在 DZ 先生用这个案例来谈谈关于这个状态不一致的问题。我们先来看下跟状态同步的订阅流程：

订阅流程



命令流程描述如下:

1: 订阅域向被订阅域发送初始订阅 SUBSCRIBE 消息，订阅目的域的目录变更事件，消息头域中使用 Event 头域描述订阅事件，消息体中携带订阅的详细参数，使用 Expire 头域指定订阅过期时间;

2: 被订阅域设备收到订阅消息后，向订阅域发送 200 OK 响应;

3: 对于初始订阅操作，被订阅域立即发送 NOTIFY 消息携带离线及其他异常状态设备目录，消息头域中使用 Event 头域描述订阅事件;

4: 订阅域收到 NOTIFY 消息后回复 200 OK 响应;

5: 被订阅域目录变更后，通过 NOTIFY 消息将变更事件通知订阅域，消息头域中使用 Event 头域描述订阅事件;

6: 订阅域收到 NOTIFY 消息后回复 200 OK 响应;

7: 订阅域在过期之前向被订阅域发送刷新订阅 SUBSCRIBE 消息，订阅目的域的目录变更事件，消息头域中使用 Event 头域描述订阅事件，消息体中携带订阅的详细参数，使用 Expire 头域指定订阅过期时间;

8: 被订阅域设备收到订阅消息后，向订阅域发送 200 OK 响应;

9: 被订阅域目录变更后，通过 NOTIFY 消息将变更事件通知订阅域，消息头域中使用 Event 头域描述订阅事件;

10: 订阅域收到 NOTIFY 消息后回复 200 OK 响应;

11: 订阅域向被订阅域发送取消订阅 SUBSCRIBE 消息，消息头域中使用 Event 头域描述订阅事件，消息体中携带订阅的详细参数,Expire 头域值为 0;

12: 被订阅域设备收到订阅消息后，向订阅域发送 200 OK 响应，取消向订阅域发送目录变更通知消息。

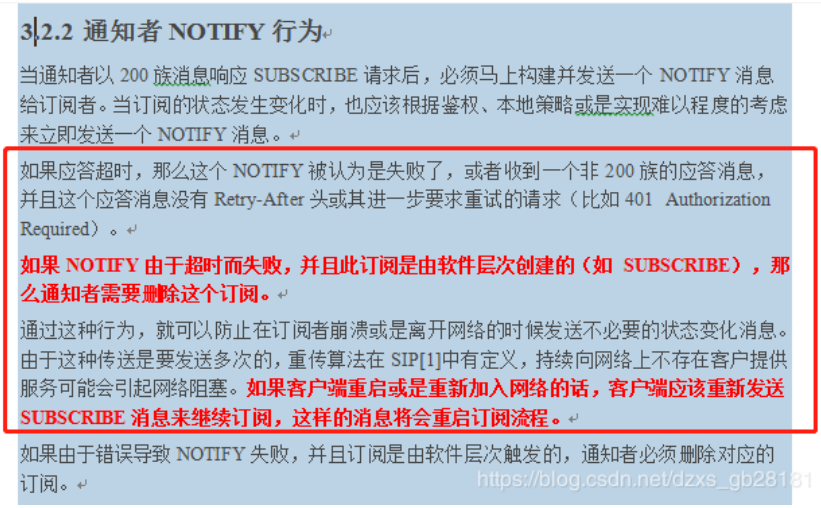
前期排查问题过程：

根据订阅的流程，订阅成功需要有 subscribe 和 200OK 消息。于是我们从开始订阅开始抓包，然后找一个摄像头离线看是否有 notify 消息，经过多次发现，subscribe 和 200Ok 是有的是没有问题，但 notify 消息有时候上报有时候不上报。接下来我们又扯到了刷新订阅，为了验

证这个问题，我们搭建了测试平台，由于我们的订阅有效期是 11 天，我们特地抓了 11 天的报文，发现刷新订阅存在，在这些证据的确凿的情况下，我们认为是下级海康在订阅成功的状态下，设备上下线不发 notify 消息。

后期排查问题过程：

1. 经过貌貌的多次排查和海康研发的查看，发现了通道关闭，也就是说 subscribe 订阅成功后，后面的上报 notify 消息流程没有完毕，导致通道关闭，最终后面下级不在发送 notify 消息。为了证明正确性，我们查看了 rfc 3265 文档，文档里是这样解释的



3.2.2 通知者 NOTIFY 行为

当通知者以 200 族消息响应 SUBSCRIBE 请求后，必须马上构建并发送一个 NOTIFY 消息给订阅者。当订阅的状态发生变化时，也应该根据鉴权、本地策略或是实现难以程度的考虑来立即发送一个 NOTIFY 消息。

如果应答超时，那么这个 NOTIFY 被认为是失败了，或者收到一个非 200 族的应答消息，并且这个应答消息没有 Retry-After 头或其进一步要求重试的请求（比如 401 Authorization Required）。

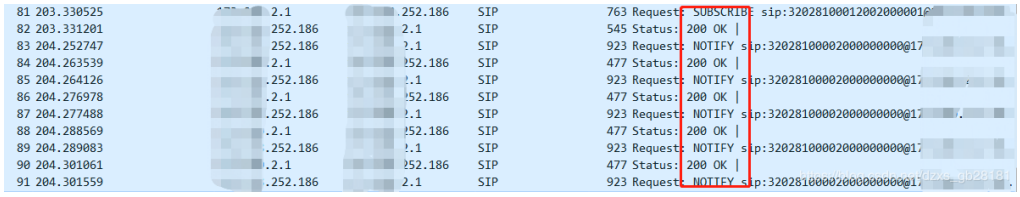
如果 NOTIFY 由于超时而失败，并且此订阅是由软件层次创建的（如 SUBSCRIBE），那么通知者需要删除这个订阅。

通过这种行为，就可以防止在订阅者崩溃或是离开网络的时候发送不必要的状态变化消息。由于这种传送是要发送多次的，重传算法在 SIP[1]中有定义，持续向网络上不存在客户提供服务可能会引起网络阻塞。**如果客户端重启或是重新加入网络的话，客户端应该重新发送 SUBSCRIBE 消息来继续订阅，这样的消息将会重启订阅流程。**

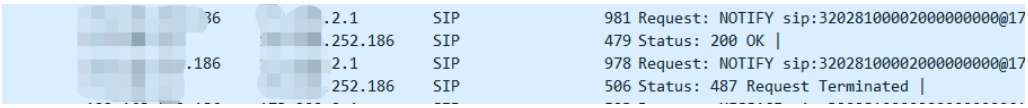
如果由于错误导致 NOTIFY 失败，并且订阅是由软件层次触发的，通知者必须删除对应的订阅。

文档下载地址：
链接：https://pan.baidu.com/s/1twq8i5BqPuNXZi-suMNUng
提取码：kz73

我们再来看下报文：



81	203.330525	[redacted] 2.1	[redacted].252.186	SIP	763 Request: SUBSCRIBE sip:32028100012002000001[redacted]
82	203.331201	[redacted]252.186	[redacted]2.1	SIP	545 Status: 200 OK |
83	204.252747	[redacted]252.186	[redacted]2.1	SIP	923 Request: NOTIFY sip:32028100002000000000@17[redacted]
84	204.263539	[redacted].2.1	[redacted]252.186	SIP	477 Status: 200 OK |
85	204.264126	[redacted].252.186	[redacted]2.1	SIP	923 Request: NOTIFY sip:32028100002000000000@17[redacted]
86	204.276978	[redacted].2.1	[redacted]252.186	SIP	477 Status: 200 OK |
87	204.277488	[redacted].252.186	[redacted]2.1	SIP	923 Request: NOTIFY sip:32028100002000000000@17[redacted]
88	204.288569	[redacted].2.1	[redacted]252.186	SIP	477 Status: 200 OK |
89	204.289083	[redacted].252.186	[redacted]2.1	SIP	923 Request: NOTIFY sip:32028100002000000000@17[redacted]
90	204.301061	[redacted].2.1	[redacted]252.186	SIP	477 Status: 200 OK |
91	204.301559	[redacted].252.186	[redacted]2.1	SIP	923 Request: NOTIFY sip:32028100002000000000@17[redacted]



[redacted]36	[redacted].2.1	SIP	981 Request: NOTIFY sip:32028100002000000000@17
[redacted]	[redacted].252.186	SIP	479 Status: 200 OK |
[redacted].186	[redacted]2.1	SIP	978 Request: NOTIFY sip:32028100002000000000@17
[redacted]	[redacted]252.186	SIP	506 Status: 487 Request Terminated |

notify 消息突然收到 487 这样的请求终止报文，而不是 200Ok，这个时候下级通道被关闭，不会再上报状态变化的 notify 消息。此时我们需要解决这个报错。

根据这个报错，我们在解决错误问题时发现了以下问题：
1）海康在删除此编码组织后，还会继续发送此 notify 消息的 update 事件。后来海康经过数据里里删除后，即解决问题。
2）上级平台如果本地没有 32 这个编码，但是网外推送了 32 编码，那么下级推送过来时将不会再接收，会认为本地有此编码。
海康貌貌先生把数据里的编码删除后，此时重启服务后，订阅成功，notify 消息流程走完，没有一个报错。此时取消一个点位的共享后，进行了 notify 消息上报。

接下来，我们参照此方法解决和 X2 平台的订阅问题，发现了另外一个奇葩的问题，DZ 先生将在另外一个案例里说明。

总结：

订阅的过程报文是 subscribe 和 200ok，真正成功是 notify 和 200Ok 全部走完且没有报错。

10. 多余的录像&缺失的录像

今天金师傅告诉我昨天他加了一个下级平台，下级是海康的 NVR，他今早告诉我，为什么我查下级海康的 NVR 今天的录像，它是从昨天的录像开始的？遇到这种问题，我们首先的第一反应是问：“平台时间同步否？”，金师傅告诉我，时间已经同步。接下来该怎么解？让我们看下文

多余的录像排查思路

1. 首先我们确定时间已经同步
2. 确定组网

   上级平台（X.X.1.21）----------GB---------下级海康平台（X.X.48.201）
3. 确定录像查询报文流程

图 18 设备视音频文件检索消息流程示意图

注：

1）流程中第一条 Message 中包含了目录检索方要查询录像的开始时间和结束时间

2）流程中第二条 Message 中包含了目录拥有方给目录检索方的录像开始时间和结束时间

抓包分析如下：

上级给下级发查询报文

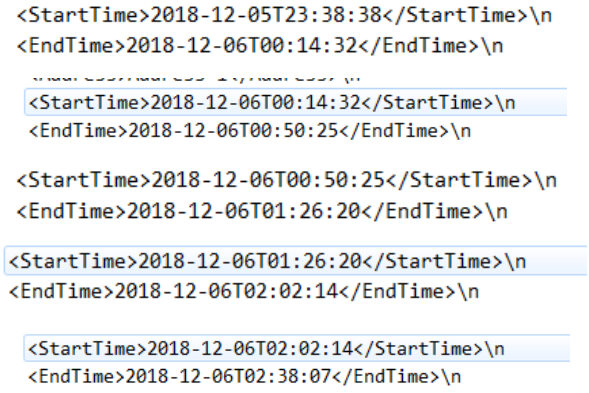
```
Message Body
    <?xml version="1.0" encoding="GB2312"?>\r\n
    \r\n
    <Query>\r\n
    <CmdType>RecordInfo</CmdType>\r\n
    <SN>10715</SN>\r\n
    <DeviceID>32028101021320000009</DeviceID>\r\n
    <StartTime>2018-12-06T00:00:00</StartTime>\r\n
    <EndTime>2018-12-06T23:59:59</EndTime>\r\n
    <Type>time</Type>\r\n
    <FilePath>32028101021320000009</FilePath>\r\n
    <Address>Address1</Address>\r\n
    <Secrecy>0</Secrecy>\r\n
    <RecorderID>32028101021320000009</RecorderID>\r\n
    <IndistinctQuery>0</IndistinctQuery>\r\n
    </Query>
```

上级发给下级的查询录像的开始时间和结束时间

上级查的是 2018-12-06 00:00:00~23:59:59 这段时间的录像。

如果想知道其他字段的意思可以看**第二章第 4 节视音频文件检索**。

下级给上级回复录像开始时间和录像时间



and ~~~~~~~~~~等等

由于下级 NVR 是多响应消息，分段发的，我就不一一截图了，从下级给上级回复的报文中，我们已经可以看出下级最开始的回复报文中，录像开始时间为 2018-12-06 23:38:38~2018-12-06 00:14:32 。并没有正确的回复。正确的应该为 2018-12-06 00:00:00 开始。

总结：查询的录像结果正确否，在时间同步的情况下，看上级查询录像的开始时间、结束时间是否和下级的回复的开始和结束时间一致。

缺失的录像排查思路

总结：请保持前端相机 & 存储时间 & 平台时间一致。前端相机和存储时间如果小于平台时间，会导致查询录像时，录像有丢失。

11. 国标对接内功大法—彰显专家气质

“如何通过国标对接的谈判，来彰显你专家的气质”，国标对接绝对不是一个你所认为的简单的活，对于大部分的工程师，他们所认为的国标对接就是简单的国标对接，推送资源。这就大错特错了。你再好好想想，你真的就只需要考虑这点事？学完本课，在国标对接方面，你将思维缜密，考虑周到，事半功倍。绝对可以在对接会议上秒杀 X 康、X 视、X 达等工程师，彰显你专家的气质。

国标对接注意事项（重点）

1. **了解人员架构（记得留下联系方式，电话或者微信）**

   客户负责人、自己、我方集成商负责人，对方对接工程师、对方集成商负责人、网络工程师（可能含双方）；这里 DZ 先生推荐拉微信群，所有相关人员都在内，方便及时沟通处理。

2. **网络组网架构**

   组网架构图一定要有，如果当时没有，后期也要准备一份；网络方面主要了解以下重点信息

   （1）两个平台网络打通是通过路由，还是网闸（对接填写对方的地址因组网不同而不同）

（2）网络放行双方的信令端口和视频流端口（根据业务需要，可能还有其他端口，自行评估）

（3）组网节点中不能存在百兆节点，如果有要尽快替换成千兆（即使当时问题没表现出来，也不能保留这颗雷）

3. 国标编码

国标编码不容小觑，因为中心编码一旦修改，这是个工程量巨大的工作，没人愿意去承担这样巨大的工作量。所以我们要从源头就保证好不会需要修改。

（1）规定中心服务器国标编码。

是否有专人指定，还是自行规定？如果有专人指定这是最好的，但也要提醒规划者，一旦使用，就不能更改，告知他一旦修改，需要承担巨大工作量修改工作以及业务暂停使用的风险，需要他在这方面多些谨慎。如果是自行指定，也需要告知客户，并告知客户相关风险性。（牢记：修改中心服务器国标编码存在巨大修改性的工作量）

（2）资源推送

资源推送主要考虑，推送的目录结构，推送资源的目录编码及资源编码

a）下级往上级推送资源，下级需要以什么目录结构方式往上级推送，这个需要提前沟通好，否则要承担重新推送的风险。

b）关于推送资源的目录编码，首先要确定客户方面是否有规划，如果没有，还需要和上级工程师沟通，因为胡乱定义编码，可能造成上级数据库存在相同编码，而没法接收下级推送过来的资源。

c）推送资源建议以行政区划的方式推送，以下举个列子，实际使用需要灵活使用。

目录 A（总目录）：组织编码 3202

子目录 B1：组织编码 320201

B1 下的资源：资源编码 320201000001320000001。。。。。

子目录 B2：组织编码 320202

B2 子目录 C1：组织编码 32020201

C1 的资源：资源编码 320202010001320000001.。。。。。

4. 对接协议

对接协议主要考虑：统一新旧国标、国标 UDP 还是 TCP、H.264 还是 H.265，关于这三点，要全方位考虑，并给予对接方案，否则会出现令人头痛的事情。这里就需要工程师有大局观了。

（1）H.264 or H.265

下级域的工程师首先要考虑这一点，因为现在 H.265 还没有统一，厂家各家开发各家的不能互相解码，如果是 H.265 则需要改成 H.264。这里会有一个问题，因为 H.264 所需的存储是 H.265 的两倍，如果改了，原来可以存 30 天，改为 H.264 之后就只有 15 天录像了，需要你评估当前存储是否可以保持原有的录像天数，如果不能则需要告知客户，需要客户同意才可以。

（2）国标 UDP 还是 TCP

针对国标对接，是使用国标 UDP 还是 TCP？你需要从以下几点进行评估

a. 首先确定级域，看最顶级上级域是想要 UDP 流还是 TCP 流，如某省 X 公安厅 X 康平台只能接受 UDP 流，那么自上往下都得要使用 UDP 传输。

b. 下级平台相机接入是 TCP 还是 UDP，如果是 TCP 还得要改 UDP，这个都是需要提前告知客户的，当然你首先要提前评估。

（3）统一新旧国标

不同的平台，不同的版本，所支持的新旧国标是不一样的，所以在对接的时候，我们需要首先统一国标是使用旧国标还是新国标，保持统一，以避免信令交互中可能存在的问题。只要不是需要传输 TCP 视频流，旧国标是完全可以支撑视频业务的。

5. 对接鉴权

为什么提到鉴权，也许很多工程师知道但是从来没有涉及到过，请记住，凡是涉及到国家私密安全的单位业务，请记得加上鉴权。不要偷懒！要有责任心！

6. 时间

请不要小看的这个时间，只要客户稍微严格一点，都会要求时间统一，一定要问客户或者集成商，是否有 NTP 服务器，如果有请一定使用它们的 NTP 服务器，即使时间不对，只要客户认可即可。

如果没有 NTP 服务器，可以和上级或者集成商搭建一个 NTP 服务器，以此来完成时间统一。

时间不统一不是小事，纠结起来够你以及上级域工程师喝一壶！（一次性解决，避免后患）

7. 订阅

订阅的作用是只要下级有目录或者资源状态变更，下级会向上级进行上报，上级收到通知到后进行变更，以保持目录结构和在线状态一致。请记得让上级工程师订阅你的平台，否则状态不一致，群里@你，也够你和上级进行扯皮了的！

8. 经纬度

DZ 先生向来都是一次性提出，经纬度也不例外，你优先提出可以体现出你很专业，你为客户考虑周到。如果客户需要，你需要测试当前版本是否支持传递经纬度信息。

9. 下级或者上级流媒体传输性能

当进行国标对接后，我们需要了解上级调用下级的视频是否会非常多。我们需要同时考虑上级和下级的流媒体性能是否能满足当前的业务需求，DZ 先生建议流媒体都做上双网卡聚合。确保带宽。这还需要你和集成商以及网络工程师沟通，交换机是否有空余口，聚合模式等。

检查项（主要上级检查，如果你是下级也要督促上级检查）

1. 实况：流畅性，时间一致性
2. 录像：检索录像，回放流畅性，下载可否
3. 设备状态一致性：在线数一致性
4. 设备状态上报：上下线设备，看是否上级变更状态
5. 设备类型一致性：枪球机是否一致，抽查
6. 网络质量：实况和录像播放时，抓包，检查网络质量，重点（以防止后面一点卡段都找你麻烦，不怕麻烦可以不检查）

丢包率上限值为 1×10-3----------丢包率是千分之一
包误差率上限值为 1×10-4--------错报率的上限是万分之一
7. 经纬度：下级录入经纬度，上级查询外域资源是否可以收到
8.时间：上下级实况时间是否一致

12. 视频倍速拖影之三角定位法则

“利用三角定位法则，排查视频倍速播放拖影问题”，在说这个问题之前，DZ 先生想和大家说一个简单的道理，这儿有一条水渠，渠道里装了水，正常情况下，在无外力的干扰下，水面就是一面镜子，当你照镜子时，你长的漂亮，照出来就漂亮，当然如果长得丑那也不能怪镜子。如果渠道突然倾斜，或者抖动，那将会怎样？水面将会波澜起伏。如果在外力的作用下，同样，水面也会波澜起伏。在这里：

第一角：网络环境比作渠道环境
第二角：水面比作视频流
第三角：自身解码比作外力

三角定位法则：第一角决定第二角的完整性，第三角决定第二角的呈现性。

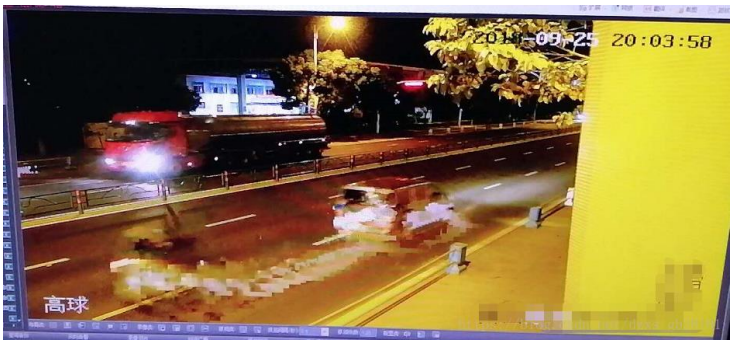
案例结合
组网：
前端----国标 UDP 接入---平台，一路视频流到实况，一路视频流到中心存储。

问题描述：
集成商反馈：回放录像，4 倍速，暂停再播放，会出现拖影
DZ 查看后总结：　　回放存在拖影

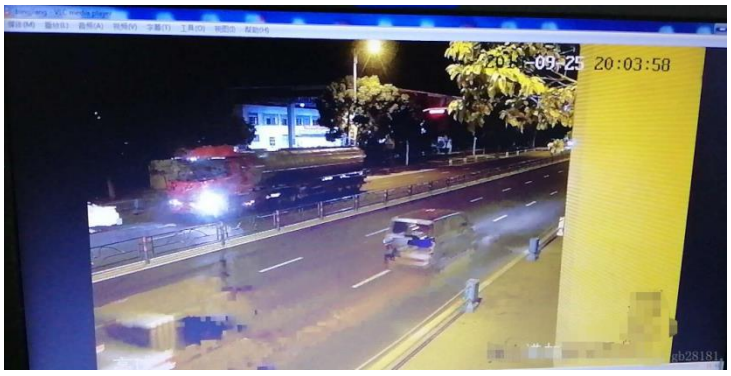
原因分析：
首先这个问题描述是比较绝对的，经过 DZ 查看，并不是 100%出现，DZ 先生发现，在 4 倍速播放出现拖影的时候，以正常的速度播放，还是会在相同的时间点出现拖影。由于这个点位出现的频率是比较高的，这就好排查了。

咱先排查第一角，网络环境。DZ 先生切身体会，建议抓 30 分钟的报文，分 3 个包，每个包 10 分钟，如果一次抓的时间太长，在把视频流转换成视频的时候，解码等待时间太长。**转换成视频流后播放视频，看拖影的时间点和平台回放录像拖影的时间点是否一致？**

抓包分析结果：
录像拖影时间点



视频流播放拖影时间点：



报文分析

Analysing stream from ort 15060 to port 24966 SSRC = 0x10BFDC34

Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps	Marker	Status
1	18284	0.00	0.00	0.00	3.01		[Ok]
2	18285	0.00	0.00	0.00	14.53		[Ok]
3	18286	0.00	0.00	0.00	26.05		[Ok]
4	18287	0.00	0.00	0.00	37.57		[Ok]
5	18288	0.00	0.00	0.00	49.09		[Ok]
6	18289	0.00	0.00	0.00	60.61		[Ok]
7	18290	0.00	0.00	0.00	72.13		[Ok]
8	18291	0.00	0.00	0.00	83.65		[Ok]

Max delta = 0.00 ms at packet no. 0
Max jitter = 0.00 ms. Mean jitter = 0.00 ms.
Max skew = 0.00 ms.
Total RTP packets = 275451 (expected 275451) Lost RTP packets = 18 (0.01%) Sequence errors = 245
Duration 701.96 s (0 ms clock drift, corresponding to 1 Hz (+0.00%)

丢包率满足千分之一，乱序没有满足万分之一，拖影为乱序造成，请排查网络

总结：

利用三角定位法则：第一角决定第二角的完整性，第三角决定第二角的呈现性。无论是卡顿，还是拖影，基本 99%都是第一角造成的，只有 1%是第三角造成的。

友情提示：说不要跟我扯网络的都是耍流氓!!

13. NAT 组网国标对接经典组网一（下级 单一 NVR）

注：NAT 组网国标对接——不到万不得已不要用

都说安防行业竞争激烈，如果某个厂家能挣得一个大平台权，基本上后面的项目设备都是以此厂家为主。但是往往突入行的一个大平台，由于集成商未对现场情况了解清楚。会造成国标对接困难重重，以下为 DZ 先生遇到的一个情况：

现场情况：有多台 NVR，但是出口只有一个专网地址。怎么办？ 我们作为安防工程师都知道，国标对接第一步，打通网络，网络要避开 NAT，最好以路由或者用网闸打通网络。在这种情况下集成商会考虑到成本及地址问题，不愿意更改，那怎么办？这个时候我们只能用 NAT 方式。

国标对接注册流程四大要素

SIP 端口：平台间对接的信令端口
服务地址：平台间对接的信令地址
中心国标 ID
鉴权账号和密码

说明： 一般服务主要跟端口有关，跟地址无关，所以 NAT 对接时，下级的信令端口一定要不一致，地址相同不受影响

NAT 组网国标对接下级主要更改项

a. 一个局域网里的 NVR 每台设备的 SIP 端口不能重复（NVR 支持更改 sip 端口）
b. 平台在进行国标对接时，需要将 NAT 方式改为，外域在 NAT 内，否则上级浏览视频取不到流，还会有奇怪现象如下：
b.1 取不到流时会有奇怪现象，流媒体业务表的发流地址是私有地址
b.2 私有地址和上级平台的流媒体地址网络不通，按理说不应该取到流
b.3 上级流媒收到了下级流媒体发来的包，通过收流端口可以收到视频流，且可以用 VLC 播放
b.4 上级流媒体不往 PC 端发视频流，流媒体抓发流端口无流
b.5 这会造成一个业务问题的错觉，平台上将对接改为外域在 nat 内后即恢复正常

二级 NAT

用此方式可以完成二级 NAT 的对接，可以对接成功和业务正常，但建议二级 NAT 尽量不要用，因为后期出问题很难排查，不要给自己埋雷。

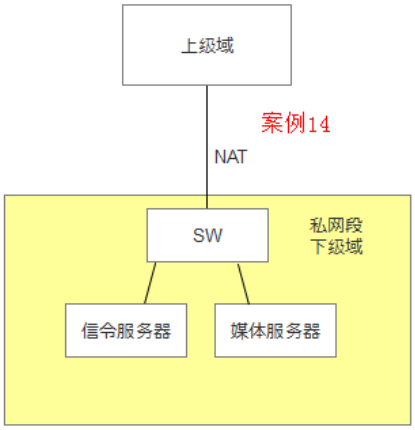
NAT 组网缺点：

1）排查问题困难，在只知道地址和没有端口的情况下，抓包有时候会无从下手
2）NAT 会存在映射表，映射表是有有效期的，在 NAT 出现问题时，会造成串流现象
3）维护困难

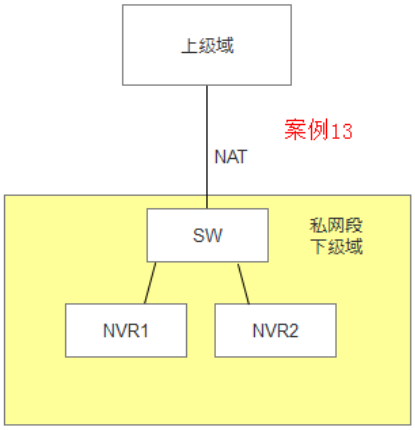
14. NAT 组网国标对接经典组网二（下级 平台+流媒体）

注：NAT 组网国标对接——不到万不得已不要用

NVR 是信令和媒体的合体，而这次案例是将这个合体拆开。且现实案例中，信令服务器+媒体服务器这种架构居多。组网架构图如下：



下级为信令服务器+媒体服务器



下级仅为NVR

国标对接注册流程四大要素

SIP 端口： 平台间对接的信令端口

服务地址：平台间对接的信令地址

中心国标 ID

鉴权账号和密码

可行性分析

1）根据国标对接注册流程以及案例 13 的成功，这边毫无疑问信令服务器映射出去进行对接是可以成功的。

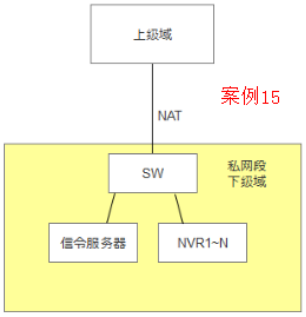
2）但是在调用实况和录像的时候，下级视频的发流地址为媒体服务器，媒体服务器在没有映射的情况下肯定和上级媒体服务器网络之间是不通的，这会导致上级取不到视频流，从而黑屏无码流。

3）根据案例 13 的成功，媒体服务器也可进行 NAT 映射，从而打通上下级媒体之间的通信。DZ 先生个人认为应该可行，但还没有实施过，DZ 先生曾在某局遇到此种组网，因种种原因最后没有做此种架构，最后将信令和媒体进行了合一。在以后的组网中，如果遇到此种架构可以再做一番实验，再证明下可行性。

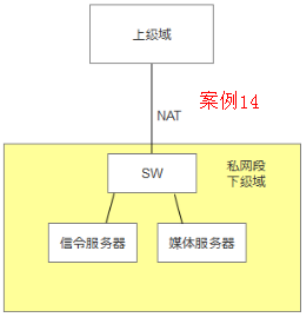
15. NAT 组网国标对接经典组网三（下级 平台+NVR）

注：NAT 组网国标对接——不到万不得已不要用

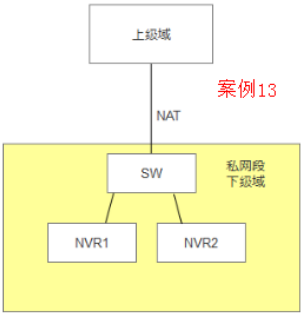
我们先来看下案例 12 这种组网架构，然后再做分析



下级为信令服务器+NVR



下级为信令服务器+媒体服务器



下级仅为NVR

国标对接注册流程四大要素

SIP 端口： 平台间对接的信令端口

服务地址：平台间对接的信令地址

中心国标 ID

鉴权账号和密码

可行性分析

1. 在私网里，NVR 以私有协议或者国标的方式加入到平台

2. 这边先将信令服务器 NAT 映射出去，国标对接成功，我们看下浏览实况或者录像的信令流程

3. 上级发送 invite 消息至信令服务器，信令服务器再将 invite 消息给 NVR，NVR->信令服务器->上级，信令流程无问题。

4. 我们再来看下发流情况，发流为 NVR，由于 NVR 没有映射出去导致 NVR 和上级流媒体网络不通，导致上级黑屏无码流

5. 将 NVR 映射出去即可打通网络（**未实施过，待验证**）

友情提醒：

1）案例 15 中，如果 NVR 非常多，做这种架构就是给自己埋雷，最好增加一台流媒体，然后将平台和媒体合一

2）根据案例 13，案例 14，及案例 15 这三种经典组网架构，在后期遇到这种组网时可以套用这三种公式

3）案例永远只是案例，一定要根据现场情况制定最可靠可行的方案，一定不要给自己埋雷。

附 监控 linux 基础

作为一个监控工程师，DZ 君用工作经验告诉你，任何东西不会都不要紧，只要有百度，只要有二线，只要有研发，没有什么东西是搞不定的，监控工程师最好还是懂点 Linux 比较好，因为修改网络配置，查看服务状态等是我们必须掌握的技能之一，今天 DZ 君在这里给刚入门的监控工程师一点小小的知识库，希望对你有用。

文件操作类

1）vi 编辑器的使用

[root@vmserver home]# vi a.txt

按键 i 是进入编辑状态

按键 esc 是退出编辑状态

在退出编辑状态下，：q！是不保存退出，：wq 是保存退出

2）将文件从服务器 A 拷贝至服务器 B

在 A 服务器/var 下的文件 a.txt 拷贝至 192.168.0.1 服务器上/home 目录下

scp /var/a.txt root@192.168.0.1:/home

3）如何查看文件

cat /vat/a.txt

4）删除文件 a.txt 和文件夹 A
rm -rf a.txt
rm -rf A

5）查找命令 find 用法
find / -name a.log　查找/目录下名叫 a.log 的文件

网络类常用命令
1）　网卡编辑和查看网址
vi /etc/sysconfig/network-script/ifcfg-eth0　编辑完保存
DEVICE=eth0
BOOTPROTO=static
BROADCAST=192.168.0.255
IPADDR=192.168.0.10
NETMASK=255.255.255.0
METWORK=192.168.0.0
GATEWAY=192.168.0.1
NM_CONTROLLED=no
ONBOOT=yes

重启网络 service network restart
ifconfig 是查看网卡地址

2）如何查看网卡双工和速率
ethtool eth1 即可查看

系统类常用命令
uname -a　查看系统位数 i686 是 32 位，x64 是 64 位
cat /etc/issue　查看系统版本
vi /etc/selinux/config 修改 selinux 类型
top 查看 cpu，内存使用率

```
[root@localhost /]#top

op - 19:35:41 up 47 min,  2 users,  load average: 0.05, 0.01, 0.00
Tasks: 156 total,   1 running, 151 sleeping,   4 stopped,   0 zombie
Cpu(s):  1.9%us,  0.8%sy,  0.0%ni, 97.1%id,  0.0%wa,  0.2%hi,  0.0%si,  0.0%st
Mem:   2071192k total,   371264k used,  1699928k free,    24904k buffers
Swap:  4161528k total,        0k used,  4161528k free,   171784k cached

us表示用户空间占用cpu百分比

sy表示内核空间占用cpu百分比

id表示cpu空间空间所占的百分比

Mem表示内存的情况  total表示内存总共有多少kb  used表示已经使用的内存

Free表示现在空闲的内存大小
```


vi /etc/sysconfig/network　修改主机名字
date -s "2018-07-07 00:00:00" 修改系统时间

hwclock -w --systohc　同步到硬件

关闭防火墙

```
A：可以用service iptables stop表示临时关闭防火墙，可以用chkconfig命令永久关闭防火墙服务。

临时关闭防火墙命令：

[root@localhost /]# service iptables stop
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Setting chains to policy ACCEPT: filter          [  OK  ]
iptables: Unloading modules:                               [  OK  ]

永久关闭防火墙命令：

[root@localhost ~]# chkconfig --level 3 iptables off
[root@localhost ~]# chkconfig --level 5 iptables off


检查结果：输入 /etc/intit.d/iptables staus 查看防火墙状态，确认防火墙关闭

[root@localhost ~]# /etc/init.d/iptables status
iptables: Firewall is not running.
```


抓包

tcpdump -s 0 -i bond0 host 192.168.0.1 -w qqq.cap -v　　针对地址抓包

tcpdump -s 0 -i bond0 port 5060 or 5061 -w qqq.cap -v　针对端口抓包

init 6 重启，　init 0 关机

磁盘类常用命令

du -sh /home　查看文件夹大小

du -sh /home/a.log　查看文件大小

df -h　查看硬盘空间使用率