# （智能交通系统）

# 信息安全传输方案与实施

# 讨论稿

REL 2

2020.7.30

# 目 录

# 0. Changelog

Release 1:

Release 2:

增加了 2.1 之 GB/T 28059 部分；

完成了 4.（智能交通系统）传输安全实施方案；

增加了 5.网络调研之第二部分。

# 1. 介绍

智能交通系统中的信息采集、传输、存储、识别、检索等处理操作中，有两个明显涉及安全的环节：

- 信息传输。交通系统中的智能设备采集的数据如何安全地传输到控制中心。
- 隐私保护。在保护行人和车辆的活动轨迹等隐私的前提下，如何对信息进行识别、查询等处理。

本文以摄像头获得的视频流传输为代表，参照交通运输行业（或公共安全监控领域等）安全技术规范和要求，讨论安全传输的解决方法和方案。

现阶段只建立基本的思路和框架，等讨论达成共识后再进一步修改和细化。

## 1.1. 术语

交通、视频技术、安全等方面术语。

- 智能交通系统（Intelligent Traffic System，ITS）：运用传感器、计算机技术、通信技术、信息处理技术、电子自动控制等科技手段于道路、车辆、使用者以及环境，实现保障安全、提高效率、改善环境、节约能源的综合运输系统。
- H264/H265：当前/未来主要的视频编码标准，广泛应用在影视作品、安全监控摄像等场合。
- 安全协议：利用密码算法，针对一类通用安全需求制定的安全规程规范，并开发实现的安全程序系统，如 SSL、SSH、VPN 等。
- 端口映射：对网络协议数据单元进行转发的技术，一般为了实现访问可达、安全性而采用，通常在网络层或传输层实现。

# 2. 交通系统数据传输(简化)模型

以下仅以摄像头数据传输为关注点。

## 2.1. 相关规范与标准

查阅了两方面的相关规范和标准：

- 中国智能交通协会团体标准，如“道路交通智能摄像机通用技术要求”等。

  GB/T 28181-2011：《安全防范视频监控联网系统信息传输、交换、控制技术要求》
- 公共安全视频监控相关标准，如 GB 35114-2017 等。

部分具体标准列举如下，侧重安全。

### 1) 道路交通智能摄像机通用技术要求

《道路交通智能摄像机通用技术要求》征求意见稿 2019-11-08
http://www.its-china.org.cn/SvoteDao?CREMARKS=0&sid=1574148147

其安全相关部分，节选如下：

4 一般要求

4.1 分类

道路交通智能交通摄像机（以下简称摄像机）按功能分为Ⅰ、Ⅱ、Ⅲ三级，其中Ⅰ级摄像机具有图像处理功能，Ⅱ级摄像机具有图像分析处理、车辆检测分析功能，Ⅲ级摄像机具有图像分析处理、车辆检测分析和交通事件检测功能。

4.2 外观、结构和外壳防护能力

外观、结构和外壳防护能力应符合GA/T 1127的要求。

4.3 外部接口

摄像机应具备不少于1个RJ45网口、不少于1个RS485/232接口、不少于1个TTL电平或者IO输出接口、不少于1个SD卡或者USB接口，宜具备SYNC频率源同步接口。

4.4 视频数据传输

应符合GB/T 28181的要求。

4.5 信息安全技术要求

应符合GB 35114的A级要求。

5 技术要求

**2) 软件定义摄像机功能技术要求**

《软件定义摄像机功能技术要求》（征求意见稿 2019-11-08）

http://www.its-china.org.cn/SvoteDao?CREMARKS=0&sid=1574148258

无安全方面针对性要求。

**3) GB/T 28181：安全防范视频监控联网系统信息传输、交换、控制技术要求**

GB/T 28181-2011：《安全防范视频监控联网系统信息传输、交换、控制技术要求》

https://baike.baidu.com/item/GB/T28181-2011/6303912

http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=469659DC56B9B8187671FF08748CEC89

安全相关，节选如下：

## 8 传输、交换、控制安全性要求

### 8.1 设备身份认证

应对接入系统的所有设备进行统一的编码，设备编码规范见 6.1 中的规定。接入设备认证应根据不同情况采用不同的认证方式。对于非标准 SIP 设备，宜通过网关进行认证。

在低安全级别应用情况下，应采用基于口令的数字摘要认证方式对设备进行身份认证，认证流程见 9.1 和 IETF RFC 3261—2002 的第 22 章；在高安全级别应用情况下，应采用基于数字证书的认证方式对设备进行身份认证，认证流程见 9.1。

### 8.2 数据加密

在高安全级别应用情况下，宜在网络层采用 IPSec 或在传输层采用 TLS 对 SIP 消息实现逐跳安全加密；宜在应用层采用 S/MIME 机制的端到端加密（见 IETF RFC 3261—2002 的 23.3），传输过程中宜采用 RSA（1 024 位或 2 048 位）对会话密钥进行加密，传输内容宜采用 DES、3DES、AES（128）等算法加密。

在高安全级别应用情况下，数据存储宜采用 3DES、AES（128 位）、SM1 等算法进行加密。

### 8.3 SIP 信令认证

应对 SIP 信令做数字摘要认证，宜支持 MD5、SHA-1、SHA-256 等数字摘要算法。在 SIP 消息头域中，启用 Date 域，增加 Note 域。Note＝（Digest nonce＝""，algorithm＝），nonce 的值为数字摘要经过 BASE64 编码后的值，algorithm 的值为数字摘要的算法名称。信令认证的流程和方法规定见附录 H。当跨域访问时，若该信令是由本域的用户发起，则信令安全路由网关宜将发送到外域的信令添加 Monitor-User-Identity 头域，其取值为信令安全路由网关 ID 和用户的身份信息；若该信令不是由本域的用户发起，则只在原有 Monitor-User-Identity 域值前添加信令安全路由网关 ID；各段分隔符为“-”。用户的身份为用户 ID 以及用户身份属性信息（用户身份属性信息包括：用户隶属机构属性、用户类别属性和用户职级属性）。

### 8.4 数据完整性保护

联网系统宜采用数字摘要、数字时间戳及数字水印等技术防止信息的完整性被破坏，即防止恶意篡改系统数据。数字摘要宜采用信息摘要 5（MD5）、安全哈希算法 1（SHA-1）、安全哈希算法 256（SHA-256）等算法。

### 8.5 访问控制

联网系统应实现统一的用户管理和授权，在身份鉴别的基础上，系统宜采用基于属性或基于角色的访问控制模型对用户进行访问控制。当跨域访问时，宜采用信令 Monitor-User-Identity 携带的用户身份信息进行访问控制。

## 9 控制、传输流程和协议接口

### 9.1 注册和注销

#### 9.1.1 注册和注销基本要求

SIP 客户端、网关、SIP 设备、联网系统等 SIP 代理（SIP UA）使用 IETF RFC 3261 中定义的方法

Register 进行注册和注销。注册和注销时应进行认证，认证方式应支持数字摘要认证方式，高安全级别的宜支持数字证书的认证方式，数字证书的格式符合附录 I 中的规定。

SIP 代理在注册过期时间到来之前，应向注册服务器进行刷新注册，刷新注册消息流程应与 9.1.2.1 的流程描述一致，并遵循 IETF RFC 3261 对刷新注册的规定。

若注册失败，SIP 代理应间隔一定时间后继续发起注册过程，与上一次注册时间间隔应可调，一般情况下不应短于 60 s。

系统、设备注册过期时间应可配置，缺省值为 86 400 s(1 d)，应在注册过期时间到来之前发送刷新注册消息，为 SIP 服务器预留适当刷新注册处理时间，注册过期时间不应短于 3 600 s。

SIP 代理注册成功则认为 SIP 服务器为在线状态，注册失败则认为 SIP 服务器为离线状态；SIP 服务器在 SIP 代理注册成功后认为其为在线状态，SIP 代理注册过期则认为其为离线状态。

### 9.1.2 信令流程

#### 9.1.2.1 基本注册

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，具体注册流程见图 8。

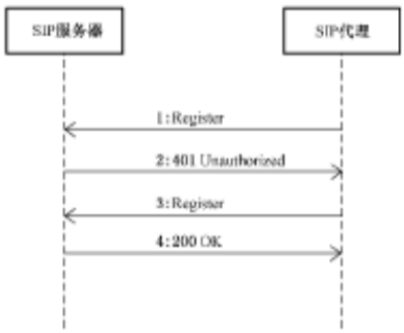



**图 8 基本注册流程示意图**

注册流程描述如下：

a) 1：SIP 代理向 SIP 服务器发送 Register 请求；

b) 2：SIP 服务器向 SIP 代理发送响应 401，并在响应的消息头 WWW_Authenticate 字段中给出适合 SIP 代理的认证体制和参数；

c) 3：SIP 代理重新向 SIP 服务器发送 Register 请求，在请求的 Authorization 字段给出信任书，包含认证信息；

d) 4：SIP 服务器对请求进行验证，如果检查出 SIP 代理身份合法，向 SIP 代理发送成功响应 200 OK，如果身份不合法则发送拒绝服务应答。

消息示范见 J.1。

#### 9.1.2.2 基于数字证书的双向认证注册

##### 9.1.2.2.1 基于数字证书的双向认证注册说明

SIP 代理和 SIP 服务器进行双向认证。对 IETF RFC 3261 中定义的方法 Register 进行如下头域扩展：

a) Authorization 的值增加 Capability 项用来描述编码器的安全能力。当 Authorization 的值为 Capability 时，只携带一个参数 algorithm，参数 algorithm 的值分为三部分，中间以逗号分割。第一部分为非对称算法描述，取值为 RSA；第二部分为摘要算法描述，取值为 MD5/SHA-1/SHA-256 中的一个或者多个；第三部分为对称算法的描述，取值为 DES/3DES/SM1 中的一个或者多个。

b) WWW-Authenticate 的值增加 Asymmetric 项用来携带验证 SIP 服务器身份的数据。当 WWW-Authenticate 的值为 Asymmetric 时，只携带参数 nonce 和 algorithm 。algorithm 的值取安全能力中指明的算法。

c) Authorization 的值增加 Asymmetric 项用来携带验证编码器的数据。当 Authorization 的值为 Asymmetric 时，携带 nonce、response、algorithm 三个参数。

#### 9.1.2.2.2 信令流程

基于数字证书的双向认证注册流程见图 9。

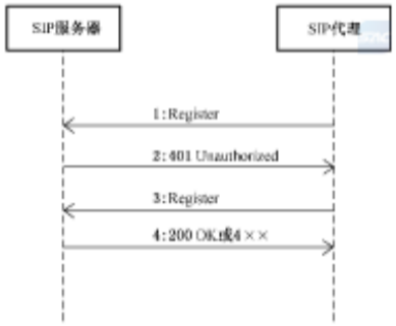



**图 9 基于数字证书的双向认证注册流程示意图**

信令流程描述如下：

a) 1:SIP UA 向 SIP 服务器发送 Register 请求，消息头域中携带 SIP UA 安全能力。增加 Authorization 头字段，Authorization 的值为 Capability，参数 algorithm 的值分为三部分，中间以逗号分割。第一部分为非对称算法描述，取值为 RSA；第二部分为摘要算法描述，取值为 MD5/SHA-1/SHA-256 中的一个或者多个；第三部分为对称算法的描述，取值为 DES/3DES/SM1 中的一个或者多个。

b) 2:SIP 服务器向 SIP UA 发送一个挑战响应 401，响应的消息头域 WWW-Authenticate 取值为 Asymmetric，参数 nonce 分为两部分 a 和 b 两部分，algorithm 的值取 SIP UA 安全能力中的算法。

c) 3:SIP UA 收到 401 响应后，得到 nonce 中的 a 和 b 两部分。首先用 SIP UA 私钥解密 b，得到结果 c，对结果 c 用 401 响应中 algorithm 指定的算法做摘要，得到结果 d，用 sip 服务器公钥解密 a，得到结果 d'，与结果 d 进行匹配，如果相匹配则信任该结果，否则丢弃。SIP UA 重新向 SIP 服务器发送 Register 请求，Authorization 取值为 Asymmetric，参数 nonce 的值与上面 b) 2:中的相同；response 的值为用本消息中 algorithm 指明的算法对[c+nonce]做摘要的结果。

d) 4:SIP 服务器对请求进行验证，如果检查 SIP UA 身份合法，向 SIP UA 发送成功响应 200 OK，如果身份不合法则发送拒绝服务应答。

消息示范见 J.2。

9.1.2.3 注销

注销流程见图 10。

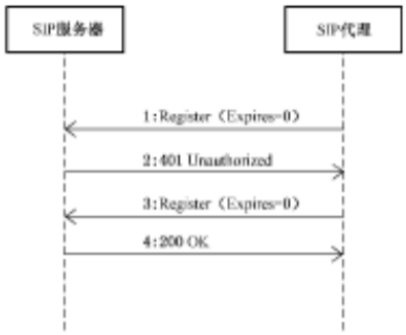



图 10 注销流程示意图

注销流程描述如下：

a) 1:SIP 代理向 SIP 服务器发送 Register 请求,Expires 字段的值为 0,表示 SIP 代理要注销；

b) 2:SIP 服务器向 SIP 代理发送响应 401,并在响应的消息头 WWW_Authenticate 字段中给出适合 SIP 代理的认证体制和参数；

c) 3:SIP 代理重新向 SIP 服务器发送 Register 请求,在请求的 Authorization 字段给出信任书,包含认证信息,Expires 字段的值为 0；

d) 4:SIP 服务器对请求进行验证,如果检查出 SIP 代理身份合法,向 SIP 代理发送成功响应 200 OK，如果身份不合法则发送拒绝服务应答。

消息示范见 J.3。

**4) GB 35114-2017：公共安全视频监控联网信息安全技术要求**

GB 35114-2017：公共安全视频监控联网信息安全技术要求

http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=B7F5589329EF98B32F0EB8ACEC341C81

该标准目录如下：

**5) 车路协同系统 应用层数据资源体系标准（征求意见稿 2019-12-24）**

http://www.its-china.org.cn/SvoteDao?CREMARKS=0&sid=1578643536

节选：

4.3 外部接口↵

摄像机应具备不少于1个RJ45网口、不少于1个RS485/232接口、不少于1个TTL电平或者IO输出接口、不少于1个SD卡或者USB接口，宜具备SYNC频率源同步接口。↵

4.4 视频数据传输↵

应符合GB/T 28181的要求。↵

4.5 信息安全技术要求↵

应符合GB 35114的A级要求。↵

**6) 公路网图像信息管理系统平台互联技术规范**

“GB/T 28059 公路网图像信息管理系统 平台互联技术规范”

http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=F8BB64F3C9C873033C6A9FF06FEC5935

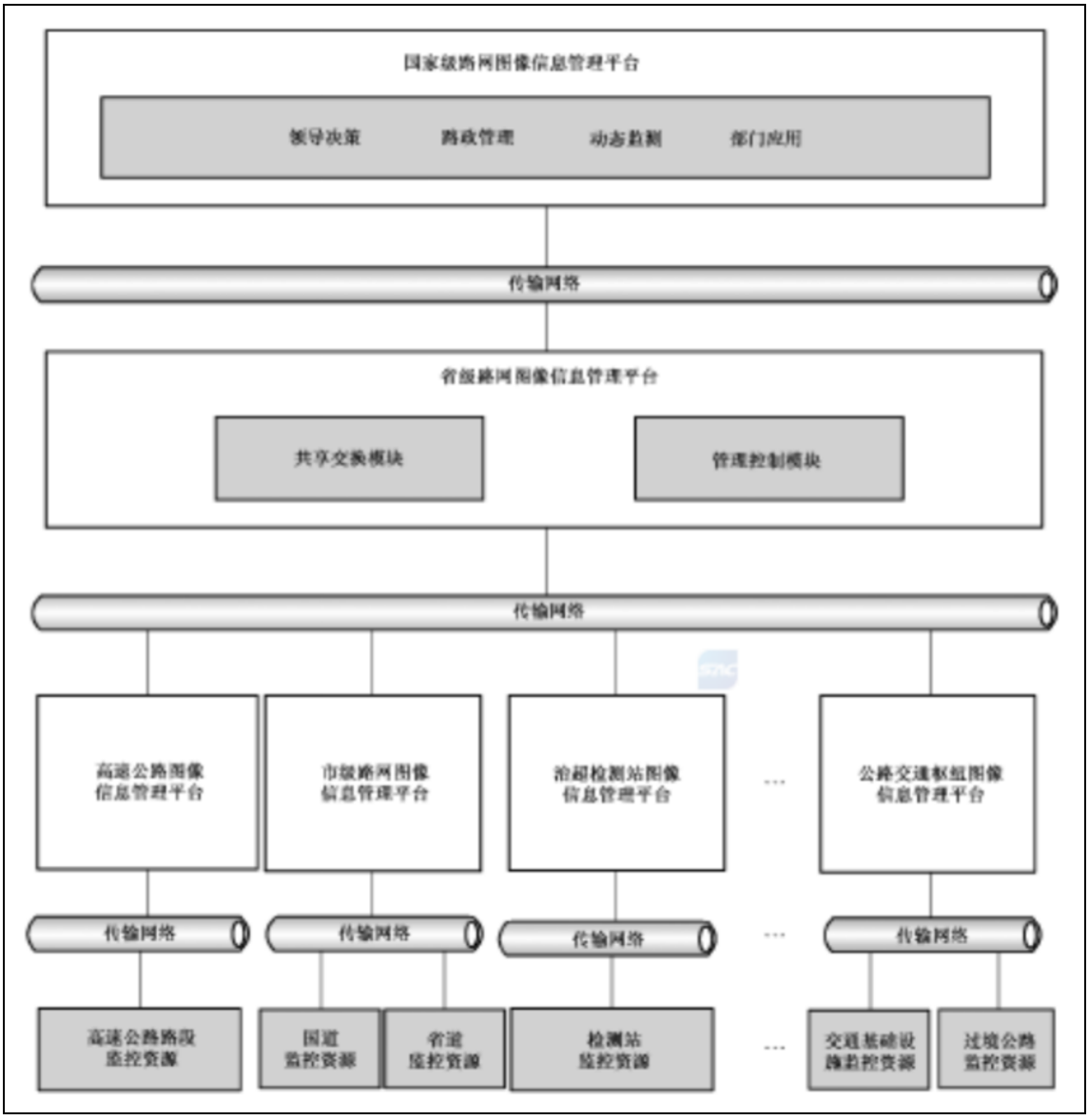
http://www.jianbiaoku.com/webarbs/book/62406/1171308.shtml

“公路网图像信息管理系统 平台互联技术规范 第 1 部分”（GB/T 28059.1-2011）中提及其引用其他协议：

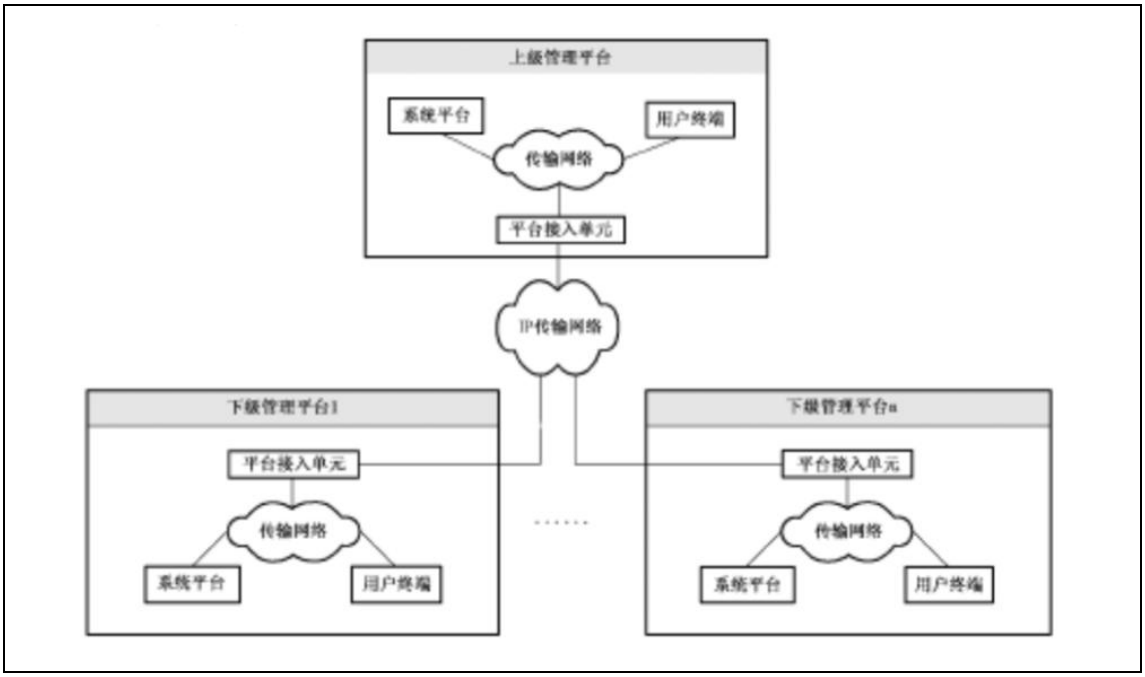
GB 50198 民用闭路监视电视系统工程技术规范
GB/T 28059.2 公路网图像信息管理系统 平台互联技术规范 第 2 部分:视频格式与编码
GB/T 28059.3 公路网图像信息管理系统 平台互联技术规范 第 3 部分:接口与通信控制协议
GB/T 28059.4 公路网图像信息管理系统 平台互联技术规范 第 4 部分:用户及设备管理
YD/T 1171 IP 网络技术要求 网络性能参数与指标
RFC 3261 会话初始协议(Session Initiation Protocol)
RFC 3265 SIP-特别事件通知(Session Initiation Protocol (SIP)-Specific Event Notification)

http://www.gb688.cn/bzgk/gb/std_list?p.p2=28059

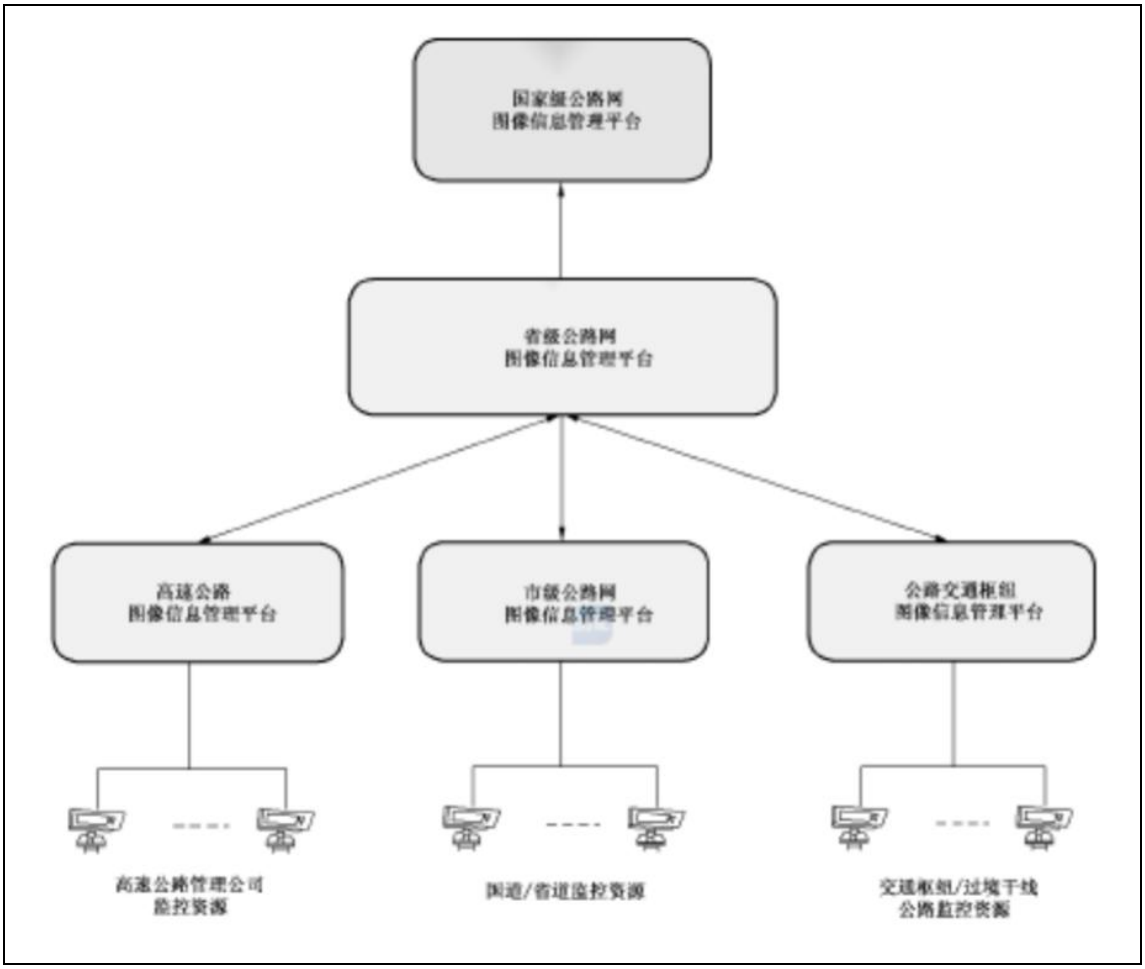
应用架构示意图：


国家级路网图像信息管理平台
领导决策
路政管理
动态监测
部门应用
传输网络
省级路网图像信息管理平台
共享交换模块
管理控制模块
传输网络
高速公路图像信息管理平台
市级路网图像信息管理平台
治超检测站图像信息管理平台
公路交通枢纽图像信息管理平台
传输网络
传输网络
传输网络
传输网络
高速公路路段监控资源
国道监控资源
省道监控资源
检测站监控资源
交通基础设施监控资源
过境公路监控资源

联网系统互联结构：




联网系统参考业务架构：




“第 2 部分：视频格式与编码”（GB/T 28059.2-2011）中规定：

http://www.gb688.cn/bzgk/gb/newGbInfo?hcno=4310504D53C4A327155D0C398E509F65

4.4 平台适配协议

4.4.1 网络适配方式

通信协议：TCP、UDP。
组播成员管理协议：IGMP V2。

4.4.2 视频流适配方式

视频码流封装在 RTP 中，通过管理配置协议可设置协议方式及端口。
使用 TCP 方式时，client/server 方式可设置。
最大数据包小于等于 16 K。
UDP 端口号：20000～20999。
TCP 端口号：20000～20999。

4.5 物理接口

传输接口：以太网接口。

5 视频接口

各级公路网图像信息管理平台之间的图像传输采用数字方式接口。
传输接口：以太网接口。
通信协议：TCP/IP。

**7) 其他参考规范及来源**

- 2020 年度中国智能交通协会团体标准公告

http://www.its-china.org.cn/SvoteDao?CREMARKS=0&sid=1595904249

- 全国团体标准信息平台

http://www.ttbz.org.cn/

## 2.2. 传输模型要素

下面总结和抽象摄像头使用环境中的网络各层，以及通信协议等各要素。

**1) 传输介质**

不做假设，只要能承载串口协议、以太帧、IP 协议之一即可。

**2) 物理接口**

智能设备可能拥有如下接口，或部分：

- 串口，RS232、485 等；
- RJ45
- USB

- SD 卡

**3) 通信协议**

以 IP 协议、TCP 协议（或 UDP 协议）为假设。

**4) 安全指标**

借鉴和遵循如下标准：

- GB/T 28181
- GB 35114

**5) 智能设备端系统**

假设能运行 TCP/IP 协议栈（或其他通信协议栈），其操作系统可能是：

- 嵌入式 Linux，包括安卓；
- Windows
- 其他 OS

其处理器可以是 x86、ARM 或其他微处理器。

**6) 应用通信模型**

如图 A 所示。

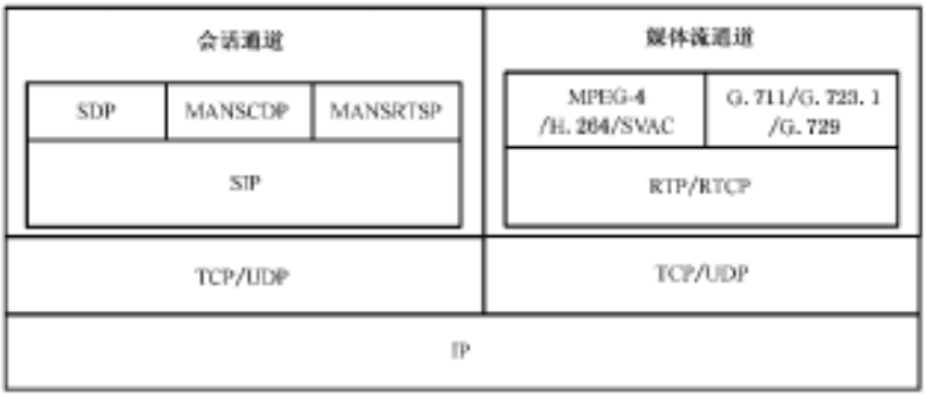



图 A 通信协议结构图（取自 GB/T 28181）

# 3. (智能交通系统)传输安全解决方案

结合图 A 所示的通信结构，以视频摄像头为智能设备即客户端代表，和服务器（控制中心）通信，假设：

- 数据通信发生在 TCP/IP 协议之上；
- 数据通信可能是单个或多个传输层(TCP 或 UDP)连接，也可能发生 TCP、UDP 之外的通信；
- 没有安全功能特性考虑；

现在需要在已有的系统之上实现安全特性，基本上可以使用外挂安全通信网关的方式实现。

## 3.1. 应用层通信模式抽象

根据应用程序的通信行为模式，抽象区分为两个模型：

- 基于 TCP 协议的通信模式
- 基于 IP 通信的通信模式

区别在于前者客户端通过一个固定的 IP 地址/TCP 端口（或事先已知的、或可临时配置的一个或多个 TCP 或 UDP 端口）与服务器通信，后者则适用于复杂的 IP 通信，可能需要发生 TCP、UDP 之外的通信的情况。


图 M1 基于 TCP 协议的通信模式

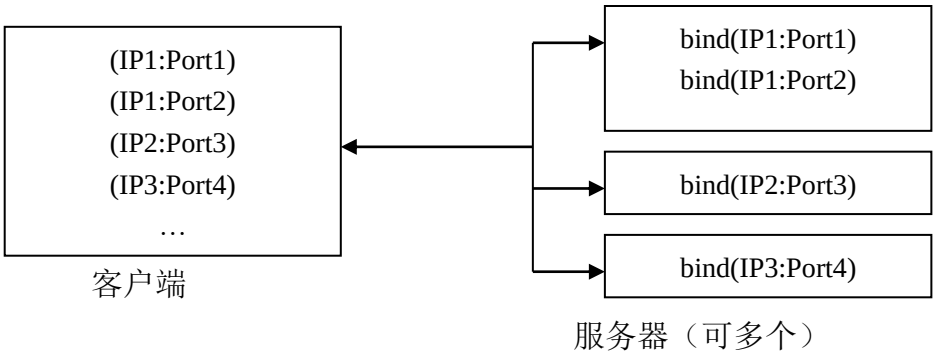



图 M2 基于 IP 协议的通信模式

## 3.2. M1 通信模式安全解决方案

使用传输层端口映射技术和方法解决 M1 模式，如图 S1 所示。

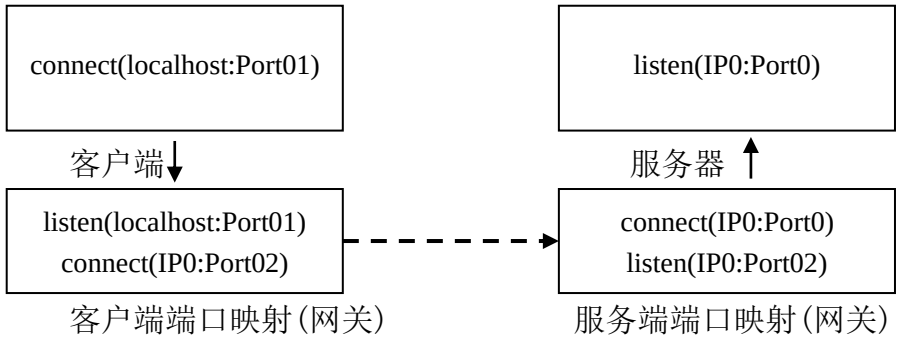



图 S1 针对 M1 通信模式的安全保护

客户端由连接 IP0:Port0 改为连接本机的 Port02，两个网关之间的安全通道连接（虚线）使用：

- SSH，其命令行参数-L、-R 可以高效地建立安全通道。也可以使用 ssh 库开发专门的网关代理程序。
- socat 工具程序。

客户端网关或服务端网关程序也可以安装在另一台机器上，只要保证内部连接（实线）的安全性即可。

## 3.3. M2 通信模式安全解决方案

使用 VPN 技术构造远程桥，解决 M2 模式的通信安全。该模式的优点不需要为每个传输层连接单独配置、建立安全通道，可以仅使用一个安全通道把两个局域网桥接起来（或把一个局域网先分为两个，再走安全通道桥接起来）。

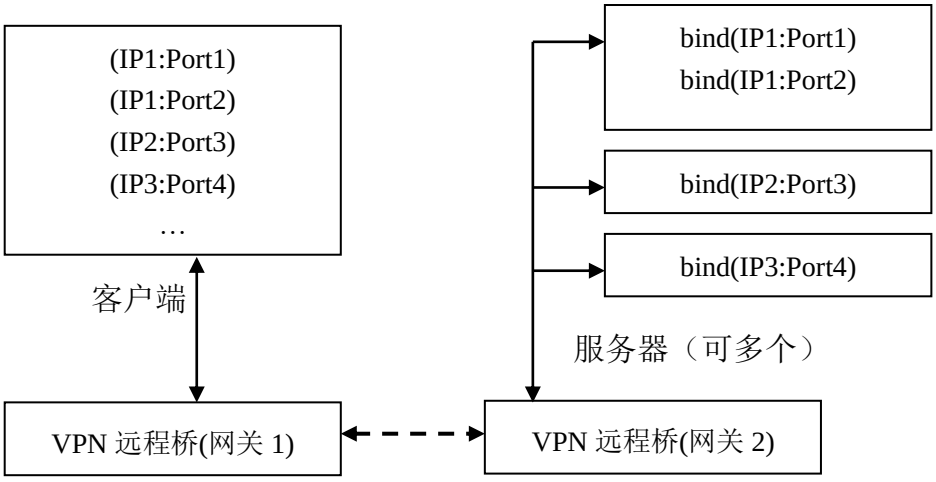



图 S2 针对 M2 通信模式的安全保护

网关之间的安全通道可以使用如下技术和工具，并配合桥接方法（比如 linux 的 brctl 命令）建立：

- OpenVPN 或 WireGuard 工具程序。
- VTun。

网关 1 或 2 也可以部署在单独的机器上。

## 3.4. 安全特性分析

使用如上的网关代理、VPN 方式解决安全传输问题，支持或满足如下安全特性或指标：

- 支持口令认证，可以使用摘要方法鉴别口令，从而保证口令安全。
- 支持公钥认证。
- 支持证书认证。以证书形式承载、发布的公钥更方便管理和使用，更利于支持大规模系统。

## 3.5. 独立网关形式的实现方法

使用单板机，比如树莓派（Raspberry Pi），安装 Linux 系统，部署 VPN 网关或运行端口映射程序。

# 4. (智能交通系统)传输安全实施方案

结合智能交通系统中监控视频等的数据传输特点，选用 VPN 方式实现智能交通系统中网络传输的安全解决方案，具体描述如下。

本方案参考了 GB/T 28059.1-2011 标准“公路网图像信息管理系统 平台互联技术规范”，相关术语和架构与之保持一致。

## 4.1. 路网图像信息传输架构

参照 GB/T 28059 中给出的 IP 互联架构“联网系统互联结构”图，如下图所示。

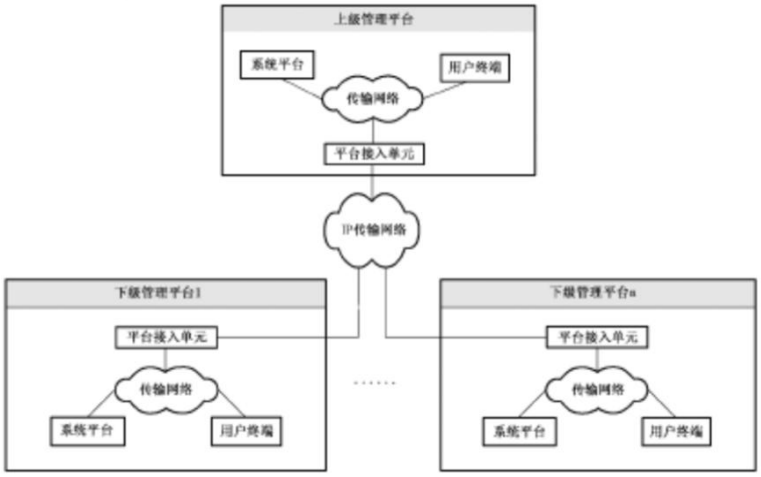



图 4-1 联网系统互联结构（GB/T 28059.1-2011）

平台内部“传输网络”和平台间一样，采用的也是“IP 传输网络”。所涉及的通信协议层次，如图 4-2 示。


图 4-2 通信协议结构（GB/T 28059.1-2011）

## 4.2. 路网 IP 传输网络中存在的安全问题和解决技术

IP 传输网络存在的安全问题、需要提供的安全特性和服务，以及实现技术、算法方法，如表 4-1 所示。

| | 安全特性 | 解决的问题 | 安全技术 | 相关算法和标准 | 技术方案 |
|---|---|---|---|---|---|
| 1 | 机密性 | 避免通信内容被窃听 | 加密和解密 | AES、SM4 | VPN |
| 2 | 完整性 | 防止明文，或密文数据被篡改 | MAC 码技术 | HMAC、SM3 | |
| 3 | 认证和抗抵赖 | 防止假冒用户身份，防止操作行为抵赖 | 证书和数字签名 | RSA、SM2 | |

表 4-1 安全特性对照表

## 4.3. 路网 IP 传输网络 VPN 安全网关

参照 GB/T 28059.1，路网 IP 传输网络中，接入 IP 网的核心部件是“平台接入单元”。简化的接入结构图，如图 4-3 所示。

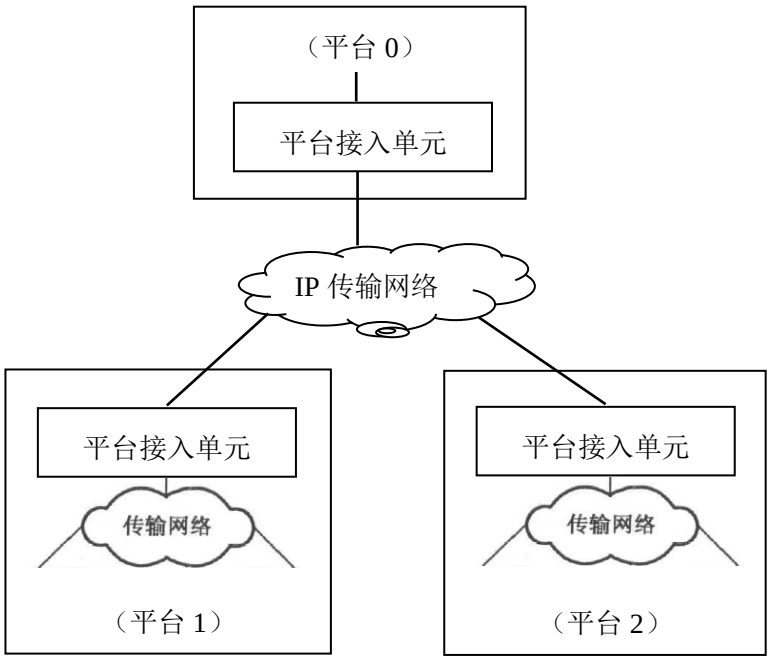



图 4-3 IP 传输网络结构（简化）：增加 VPN 安全网关前

平台接入单元所在位置是实施安全措施的关键点，在平台接入单元连接 IP 网络之前，部署 VPN 网关对上传数据进行安全保护。增加 VPN 网关后的结构示意图，如图 4-4 所示。

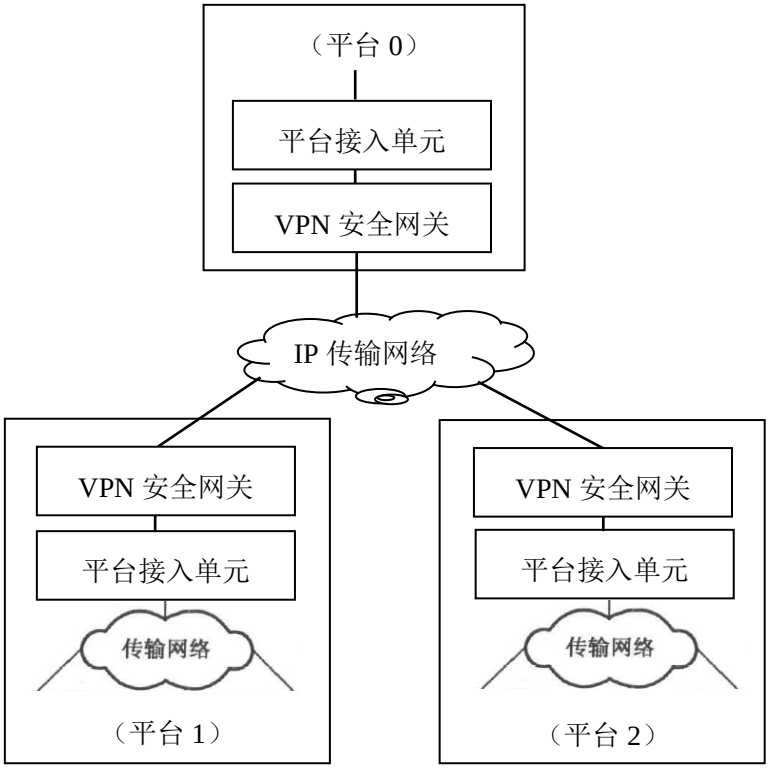



图 4-4 IP 传输网络结构：增加 VPN 安全网关后

注：

- VPN 安全网关之间的流量是受加密和认证保护的，因此可以在公共 IP 网络上传输；
- VPN 安全网关可以是可独立的设备形式，也可以内置平台接入单元中。

## 4.4. VPN 安全网关

独立设备形式的 VPN 安全网关，配置和参数：

- 硬件使用单板机树莓派（Raspberry Pi）；
- 操作系统安装 Linux 系统；
- 配置两个千兆网络接口，分别用于上行和下行；
- 使用 bridge-utils 软件工具包架设远程以太网桥。

得益于第二层网桥对 IP 网络透明的优点，各个平台内的 IP 终端设备不需要额外的配置操作，即可使用 VPN 安全网关的通信服务。

## 4.5. 用户和证书中心

//暂略

//这个环节应该和原有的业务系统相结合，因为如果单独为了 VPN 网关建立证书中心的话，不仅冗余，而且安全审计粒度不够细，（在远程桥接 LAN 的模式下）无法记录和追踪到操作的具体用户。

# 5. 附件 1：网络调研汇编

网络调研关于交通摄像头等设备数据的处理和使用方法。

## 第 1 阶段

每个摄像头旁的路边桩上，都有一个铁盒子，里面就是储存卡。储存卡再被读卡器阅读后，通过专线将图像传到固定网络上。

有两种，一种是普通的同轴电缆，一种是光缆。监控摄像头连接的一般是 AV 线，传送的是模拟信号。

不是协议 是编码 （H.264 H.265 H.264+ H.265+这四种） 把监控的画面进行编码转为电信号或者光信号传输然后再解码显示。

监控摄像机中提到的三码流，指三种码率。一路高码率的码流用于本地高清存储,例如 h.264\D1 编码，一路低码率的码流用于网络传输,例如 D1/CIF 编码，另一路超低码流用于 3G\网络传输，手机观看，例如 QCIF,,同时兼顾本地存储和远程网络传输。三码流能实现本地传输和远程传输三种不同的带宽码流需要，本地传输采用高码流可以获得更高的高清录像存储，远程传输采用较低的码流以适应 CDMA/ADSL 等各种网络而获得更高的图像流畅度。

码流(Data Rate)是指视频文件在单位时间内使用的数据流量，也叫码率，是视频编码中画面质量控制中最重要的部分。同样分辨率下，视频文件的码流越大，压缩比就越小，画面质量就越好。和我们现在电脑 QQ 传输文件多少 KB 的指标差不多，录象机录象占用空间大小就是码流，直接点说就是看你录象机或者卡的软件在录象时的分辨率是多少，有 352*288 320*240 640*480 。即所谓的 CIF 或 D1。

多码流技术：通过在编码过程中同时产生多种不同码流及分辨率的流媒体数据，根据用户实际网络带宽条件为之自动分配相对最佳解码画质的解决方案。在实际网络直播应用中，由于位于不同网络位置的访问者所在网络环境存在差异，而仅以某种固定码流分辨率进行网络直播流媒体传送往往会导致网速较高的用户看到的画质仍不够清晰，网速较低的用户解码时间过长而使得画面不够流畅，

为解决二者的矛盾使访问者浏览到尽可能看到兼顾清晰和流畅的直播内容，采用多码流技术成为了一个最简单最有效的办法。

摄象机是没有码流可言的，码流是指视频压缩后图象占用空间的大小，通过远程浏览或者录象所传输的文件大小，和我们现在电脑 QQ 传输文件多少 KB 的指标差不多，录象机录象占用空间大小就是码流，直接点说就是看你录象机或者卡的软件在录象时的分辨率是多少，有 352*288 320*240 640*480 。即所谓的 CIF 或 D1。和摄象机是无关的

国际通用协议是 onvif 协议 一般都有协议版本号 像深圳施耐安的网络摄像机是支持 onvif2.0 以上的国际标准通用协议的 如果这个网络摄像机是今年的应该是支持国际标准协议的 这是对现在网络摄像机的基本要求

监控里的主码流和子码流是什么意思？主码流：是指视频文件在单位时间内使用的主要数据流量。子码流：是指视频文件在单位时间内使用的次要数据流量。

视频比特率与码流只是同一个问题两种叫法，比如一个 MPEG2 视频文件，一般不但包含视频信息还有音频信息，音频也有自己的比特率，这是音视信息复合在一起的文件，这个文件的码流是其音视码流的总和。

主码流：主码流用于本地存储。子码流：又称次码流，次码流用于网传。硬件逻辑单元在启动一次后同时产生 2 路码流，即一路主码流和一路次码流。主码流和次码流可以为不同的编码协议。次码流不能单独存在。

主码流较之次码流，码流大，压缩比小，图像质量高。

仅以某种固定码流分辨率进行网络直播流媒体传送往往会导致网速较高的用户看到的画质仍不够清晰，网速较低的用户解码时间过长而使得画面不够流畅，为解决二者的矛盾使访问者浏览到尽可能看到兼顾清晰和流畅的直播内容，采用多码流技术成为了一个最简单最有效的办法。

通过在编码过程中同时产生多种不同码流及分辨率的流媒体数据，根据用户实际网络带宽条件为之自动分配相对最佳解码画质的解决方案。在实际网络直播应用中，由于位于不同网络位置的访问者所在网络环境存在差异。

码流是指视频文件在单位时间内所使用的数据流，也称为码率，是视频编码中图像质量控制的重要组成部分。在相同分辨率下，码流越大，压缩比越小，图像质量越高。

视频监控中 d1 有几种参照标准？D1 是分辨率，分辨率还有 CIF，QCIF，2CIF，720P，1080P 等等。这些就是视频图像的分辨率呀，QCIF(176x144)、CIF(352x288)、2CIF（704x288）、4CIF(704x576)。像素越高，图像质量好，像

素越大越清楚呀

1．不同分辨率

4CIF：704＊576

2CIF：704＊288（HALFD1）

CIF：352＊288

QCIF：176＊144

2．不同码流

CIF：单码流

2CIF：双码流

4CIF，QCIF：多码流

CIF：即视频会议中通用的影像传输格式。分辨率为 352x288 像素，图像传输速率可达每秒 30 帧，符合 ITUH．261 视频会议数据传输协议。

QCIF：1／4CIF。可以简单地理解，水平和垂直像素的分辨率都是一半。

2CIF：双倍 CIF，这很少见。DCIF 的分辨率是视频图像通过奇、偶两个 HALFD 经过反隔行变换。形成 D1（720×576），D1 作为边界处理，变为 4CIF（704×576）。4CIF 水平减少 3／4，垂直减少 2／3，为 528×384。

4CIF：CIF 的四倍。可以简单地理解，在分辨率方面，水平和垂直像素都是 2 倍。

目前市场接受 CIF 分辨率主要有四点原因：

1．目前，数字监控要求视频码流不能太高；

2．视频传输带宽也有限；

3．使用 HALF 可以提高 D1 和 D1 的半分辨率，以满足高质量的要求，但代价是高码流。目前 D1 产品较多，但市场占有率很小；

4．CIF 分辨率，信噪比 32db 以上，一般用户可以接受，但视频图像质量不理想。目前，业内正在努力用 HALF D1 寻找 CIF 与 D1 之间的平衡点。

它们之间的关系是：4CIF＝2 个 2CIF＝4 个 CIF＝16 个 QCIF，其中 DCIF 是 4CIF 经水平 3/4 缩小、垂直 2/3 缩小，转换成 528×384 的，528×384 的像素数正好是 CIF 像素数的两倍，所以 DCIF 也叫 DOUBLE CIF。

远程监控 DVR 一般设为 4CIF

监控 720p 码率是多少 监控摄像头的码率怎么算？1280X720 分辨率，如果要计算，海康威视有全套计算工具，你可以去官网下载后自己计算

海康的占内存一天 42G 不到。海康网络摄像头 200 万像素，存储一天需要的空间容量跟编码技术有关，smart265 编码技术。

如果采用 H.264 压缩标准的话，4~6MB 每秒的码流也就够用了，这么计算的话每天 42GB~63GB；不过现在海康采用的是 H.265 压缩标准也就是 2~4MB 的码流就可以存储 200 万像素的设备了，这么计算的话每天 21GB~42GB。

200w264 监控头一天一宿容量大约 20 个 g 左右 4 个头 1t 硬盘存储容量大约 13 天左右,265 官方号称存储减半那就是一天一宿 10 个 g 左右,由于国内惯例 官方夸大其效果， 265 头一天一宿应该在 13 个 g 左右。

### 第 2 阶段

IPC（IP 摄像机，IP Camera）通过 IP 网络传输网络视频信号。高清的分辨率在 720P 以及 720P 以上。除了 IPC，也有纯数字非压缩式摄像机，通过光纤 FC 接口或者 HDMI 接口或者 HD-SDI 接口传输视频信号。NVR 是用来接入 IPC 的录像机，DVR 是用来接入模拟摄像机的录像机。

如果所有摄像机网络化，那么必经之路就是有一个集中管理核心出现。NVR（Network Video Recorder 网络硬盘录像机）的功能是通过网络接收 IPC 设备传输的数字视频码流，并进行存储、管理，从而实现网络化带来的分布式架构优势。通过 Nvr，可以同时观看、浏览、回放、管理、存储多个网络摄像机，摆脱了电脑硬件的牵绊。NVR 需要与前端的 IP 摄像机或 DVS 配合使用。

DVR（Digital Video Recorder 数字视频录像机），区别于传统的模拟视频录像机，采用硬盘录像，故常常被称为硬盘录像机。DVR 是一套进行图像计算存储处理的计算机系统，具有对图像/语音和动态帧等进行长时间录像、录音、远程监视和控制的功能，集合了录像机、画面分割器、云台镜头控制、报警控制、网络传输等功能于一身，用一台设备就能取代模拟监控系统一大堆设备的功能。

网络视频服务器（DVS,digital video server)数字视频编码器是压缩、处理音视频数据的专业网络传输设备，由音视频压缩编解码器芯片、输入输出通道、网络接口、音视频接口、RS485 串行接口控制、协议接口控制、系统软件管理等构成，主要是提供视频压缩或解压功能，完成图象数据的采集或复原等，比较流行的基于 MPEG-4 或 H.264 的图像数据压缩通过 Internet 网络传输数据以及音频数据的处理。

## 6. 附录 2：密码算法、安全协议概念介绍

网络传输安全基本上关心两个问题：

- 登录认证，是鉴别用户的登录过程。

- 传输加密，是把数据加密成为密文后传输，避免被偷听、篡改等。

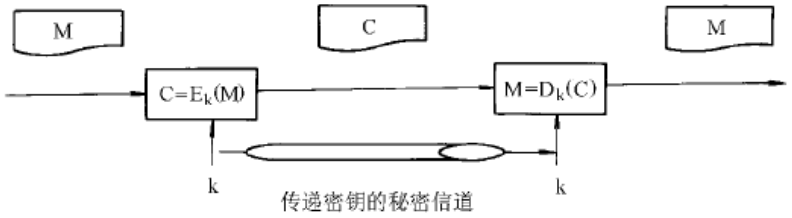
为了解决这些问题，需要使用到：

- 密码算法，包括对称加密、非对称加密、Hash 算法等几类函数。
- 安全协议，有(通信)多方参与的交互式过程，比如 SSL、SSH、IPSec、等。

安全协议使用密码算法作为基本安全要素，并根据应用场合需求形成不同的安全程序系统，比如 HTTP/SSL、SSH、VPN/IPSec 等

**1) 对称密码算法**

对称密码加密也称常规密码加密、单钥密码加密、秘密密钥加密，它包括许多数据加密方法。对称密码系统的基本模型如图所示：




其基本特征是：数据加密和解密使用同一个密钥；在算法公开的前提下所有秘密都在密钥中，因此密钥本身应该通过另外的秘密信道传递。对称密码系统的安全性依赖于两个因素：其一，加密算法强度至少应该满足：当敌手已知算法，通过截获密文不能导出明文或者发现密钥。更高的要求是当敌手即使拥有部分密文以及相应明文段落也不能导出明文或者发现密钥系统。其二，发送方和接收方必须以安全的方式传递和保存密钥副本，对称加密的安全性取决于密钥的保密性而不是算法的机密性。

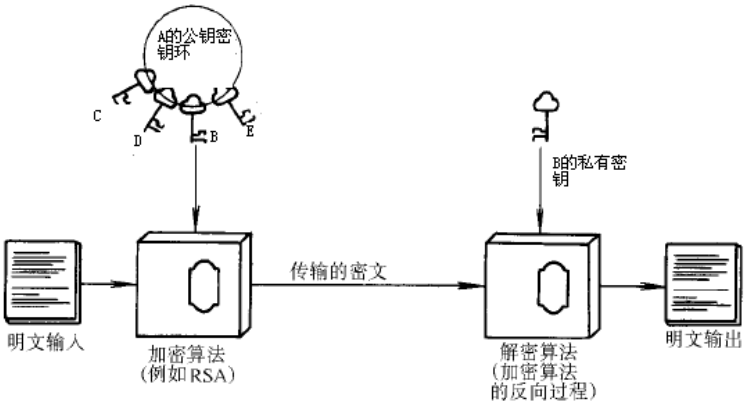
目前对称加密算法的国际标准是 AES，国内是 SM4 等。

**2) 公开密钥算法（非对称密码算法）**

公钥密码也称为非对称密码，公钥密码系统的核心是信源端对明文加密和信宿端对密文解密时分别使用两个相互对应，但计算上只能单向推导的一对密钥。根据应用的需要，将其中一个称为公钥，另一个称为私钥。

传统的对称密码系统主要是建立在位操作基础之上，而公钥密码算法和密钥生成则是建立在数学函数基础之上。目前，公钥密码理论中大量使用数论等数学理论和方法，对现代密码学产生了深远的影响。公钥加密方法的安全性主要基于复杂数学问题的难解性假设，根据所基于的数学难题来分类，以下三类系统目前被认为是安全和有效的：基于大整数因子分解的公钥密码系统（RSA）、离散对数

系统（DSA）、椭圆曲线离散对数系统（ECC）。




在数据保密通信中，加密钥匙是公开的，解密私钥原则上不传递，因此密钥的分配和管理较对称密码系统简单。公开密钥加密系统还能够很容易地实现数字签名。因此，公钥密码技术适应了电子商务应用需要。

为了充分发挥各自的优点，在实践中可以混合使用对称算法和非对称算法。对称算法速度快，但是需要额外的安全渠道协商对称密钥，而非对称算法速度极慢却拥有公钥。因此，一般使用公钥加密传递对称会话密钥，然后继续用对称算法加密批量数据。

### 3) HASH 函数

HASH 函数，又称杂凑函数，是在信息安全领域有广泛和重要应用的密码算法，它有一种类似于指纹的应用。在网络安全协议中，杂凑函数用来处理电子签名，将冗长的签名文件压缩为一段独特的数字信息，像指纹鉴别身份一样保证原来数字签名文件的合法性和安全性。SHA-1 和 MD5 曾经最常用的杂凑函数。经过这些算法的处理，原始信息即使只更动一个字母，对应的压缩信息也会变为截然不同的“指纹”，这就保证了经过处理信息的唯一性。为电子商务等提供了数字认证的可能性。

HASH 函数，又称杂凑函数，是在信息安全领域有广泛和重要应用的密码算法，它有一种类似于指纹的应用。在网络安全协议中，杂凑函数用来处理电子签名，将冗长的签名文件压缩为一段独特的数字信息，像指纹鉴别身份一样保证原来数字签名文件的合法性和安全性。SHA-1 和 MD5 是目前最常用的杂凑函数。经过这些算法的处理，原始信息即使只更动一个字母，对应的压缩信息也会变为截然不同的“指纹”，这就保证了经过处理信息的唯一性。为电子商务等提供了数字认证的可能性。

设有散列函数 h＝H（M），这里 M是可变长度消息， h 是固定长度的函数值。散列函数值行的作用是对消息 M产生一个“摘要”，使得接收方能够对消息 M的完整性进行检验。散列方法本身并不需要保密。

目前最常用的 Hash 算法是 SHA-2。

**4) MAC 函数**

MAC 函数也称密码校验和，它由如下形式的函数 C 产生：MAC=CK（M），其中 M 是一个变长消息，K 是收发双方共享的密钥，CK（M）是定长的认证符。在假定或已知消息正确时，将 MAC 附于发送方的消息后；接收方可通过计算 MAC 来认证该消息。

目前常用的 MAC 算法是 HMAC（RFC 2104）。

**5) 数字签名**

在收发双方不能完全信任的情况下，数字签名是解决该问题的最好方法。其作用相当于手写签名。数字签名满足：必须能验证签名者、签名日期和时间；能认证被签的消息内容；应能由第三方仲裁，以解决争议。

数字签名必须是与消息相关的二进制位串，签名必须使用发送方某些独有的信息，以防止伪造和否认，产生数字签名比较容易，识别和验证签名比较容易，伪造数字签名在计算上是不可行的，保存数字签名的拷贝是可行的。

基于密码技术的数字签名一般采用具有数字签名功能的公开钥密码算法，如 RSA、DSA 等。其基本原理是使用秘密钥加密实现数字签名，使用公开钥解密实现签名验证。在实际应用中，数字签名包括两个步骤：（1）对待签名信息计算 HASH 值（2）对 HASH 值采用秘密钥加密得到数字签名值；验证过程是首先将数字签名值用对应的公开钥解密，并和重新计算的信息的 HASH 值进行比较，如果相同，证明验证签名正确，否则认为是错误。

**6) 数字证书**

数字证书是指利用数字签名技术实现的经由第三方可信的、权威的机构 CA 签发的，将被认证对象（用户）的身份信息和其公开钥进行有效捆绑而编码形成的数字认证信息。通过验证者对数字证书的验证，确保用户身份和用户公开钥的一一对应性，从而确认用户对该公开钥的合法拥有，从而利用该公钥进行安全的信息加密。

X509 标准是数字证书的主要标准之一。在一个标准的数字证书中，包含证书版本号、证书序列号、证书签发者身份信息、证书拥有者（用户）身份信息、证书有效期、证书拥有者公钥信息、某些扩展信息、签名方法以及证书签发者用自己的私钥对以上信息所做的签名产生的签名信息。证书的验证主要包括验证数字签名是否正确（确认证书是否被修改）、证书有效期是否有效、证书签发者是否可信、证书中其他信息是否符合政策、证书是否已经被注销等，在证书链中，还应验证证书链中所有的证书是否符合信任链关系等。

关于证书注销列表（黑名单）。数字证书在有效期内因各种原因（对应秘密钥丢失、身份信息变更等）可能变得不安全，需要申请注销。证书注销列表是由可信的、权威的第三方机构 CA 审核签发的所有在证书有效期内，但是被注销的证书的列表。该列表经由 CA 机构签名保证可信。用户通过定期下载，在验证证书有效性时使用。

**7) CA 中心**

CA 中心（Certificate Authority）即数字证书认证机构，是一个可信的、权威的第三方机构，其主要功能就是为用户（包括人和设备等）签发数字证书，并实施相应的管理。

CA 的核心功能就是发放和管理数字证书，具体描述如下：

（1）接收验证最终用户数字证书的申请。

（2）确定是否接受最终用户数字证书的申请—证书的审批。

（3）向申请者颁发、拒绝颁发数字证书—证书的发放。

（4）接收、处理最终用户的数字证书更新请求—证书的更新。

（5）接收最终用户数字证书的查询、撤销。

（6）产生和发布证书注销列表（CRL）。

（7）数字证书的归档。

（8）密钥归档。

（9）历史数据归档。

CA 的数字签名保证了证书的合法性和权威性。主体的公钥可有两种产生方式：（1）用户自己生成密钥对，然后将公钥以安全的方式传给 CA，该过程必须保证用户公钥的可验证性和完整性。（2）CA 替用户生成密钥对，然后将其以安全的方式传送给用户，该过程必须确保密钥的机密性、完整性和可验证性。该方式下由于用户的私钥为 CA 所产生，故对 CA 的可信性有更高的要求。

RA（Registry Authority，注册中心），是数字证书注册审批机构。RA 系统是 CA 的证书发放、管理的延伸。它负责证书申请者的信息录入、审核等工作；同时，对发放的证书完成相应的管理功能。

RA 系统是整个 CA 中心得以正常运营不可缺少的一部分。但有的系统中，将 RA 合并在 CA 中。一般说来，注册机构控制注册、证书传递、其他密钥和证书生命周期管理过程中主体、最终实体和 PKI 间的交换。

**8) PKI**

公钥基础设施（Public Key Infrastructure,PKI）是一个用公开钥密码算法原理和技术实现并提供安全服务的具有通用性的安全基础设施。PKI 是一种遵循标准的利用公钥加密技术为电子商务、电子政务的开展提供一整套安全的基础

设施。用户利用 PKI 平台提供的安全服务进行安全通信。PKI 这种遵循标准的密钥管理平台，能够为所有网络应用透明地提供采用加密和数字签名等密码服务所需要的密码和证书管理。使用基于公开密钥技术平台的用户建立安全通信信任机制的基础是，网上进行的任何需要提供安全服务的通信都是建立在公钥的基础之上的，而与公钥成对的私钥只掌握在他们与之通信的对方。这个信任的基础是通过公钥证书的使用来实现的。公钥证书就是用户的身份与之所持有的公钥的结合，在结合之前，由一个可信任的权威机构———认证机构（CA）来证实用户的身份。然后由可信任的 CA 对该用户身份及对应公钥相结合的证书进行数字签名，用来证明证书的有效性。PKI 首先必须具有可信任的认证机构，在公钥加密技术基础上实现证书的产生、管理、存档、发放以及证书撤销管理等功能，并包括实现这些功能的硬件、软件、人力资源、相关政策和操作规范以及为 PKI 体系中的各成员提供全部的安全服务，例如，身份认证、数据保密性、完整性以及不可否认性服务等。

构建实施一个 PKI 系统主要包括以下内容：

（1）认证机构证书的签发机构，它是 PKI 的核心，是 PKI 应用中权威的、可信任的、公正的第三方机构。

（2）证书库证书的集中存放地，提供公众查询。

（3）密钥备份及恢复系统对用户的解密密钥进行备份，当丢失时进行恢复，而签名密钥不能备份和恢复。

（4）证书撤销处理系统证书由于某种原因需要作废，终止使用，将通过证书撤销列表 CRL 来实现。

（5）PKI 应用接口系统

综上所述，PKI 是一种新的安全技术，它基于公开密钥密码技术，通过数字证书建立信任关系。PKI 是利用公钥技术实现电子商务安全的一种体系，是一种基础设施，可以保证网络通信、网上交易的安全。

**9) SSL**

Secure Sockets Layer，又 Transport Layer Security，TLS

结合使用了对称加密算法、非对称算法、数字证书等技术，为保护网络数据在线传输而设计的安全传输协议。早先是针对 http 传输而设计，即浏览器普遍使用的 HTTPS，后来扩展适用于传输层协议的安全保护，可以提供身份鉴别、机密性、完整性保护。

SSL 使用 X.509 认证，利用非对称加密算法对通信方做身份认证，协商生成会话密钥（Session key）用来将通信两方交换的数据做加密，保证双方通信的保密性和可靠性，使客户与服务器应用之间的通信不被攻击者窃听。

使用 SSL 协议一般需要在程序系统中集成一个 SSL 实现库（比如 OpenSSL），

实现在发送数据之前对数据进行加密。

**10) SSH**

Secure Shell

SSH 一种加密的网络传输协议，通过在网络中创建安全隧道来实现网络双方之间连接安全。在设计上，SSH 是 Telnet 和非安全 shell 的替代品，因此 ssh 常见的用途是远程登录系统。不过，SSH 协议拥有灵活的机制，允许原先没有考虑安全的程序可以通过 SSH 增加安全特性，满足新的安全需求，而不用修改原有程序。

SSH 可以使用公钥证书进行登录和加密，从而提高安全性，且简化了维护和管理工作。

**11) VPN**

Virtual Private Network 虚拟私有网络

VPN 是一种利用隧道协议（Tunneling Protocol）来实现网络通信中认证、消息保密与完整性保护等功能的安全协议和程序系统，常用于连接中大型企业、团体间的通信保护。

VPN 的优点是工作在网络层或更低层，因此对上层的应用是透明的，即不需要修改现有程序就可以给现有程序增加安全保护。

可以借助 SSL 或 SSH 技术构建 VPN 系统。常用的虚拟专用网协议有：PPTP、L2TP、IPSec、SSL、GRE 等。

# 7. End