



VoIP网络安全威胁和对策

刘利锋
北京邮电大学信息安全中心

X'con 2004 概要

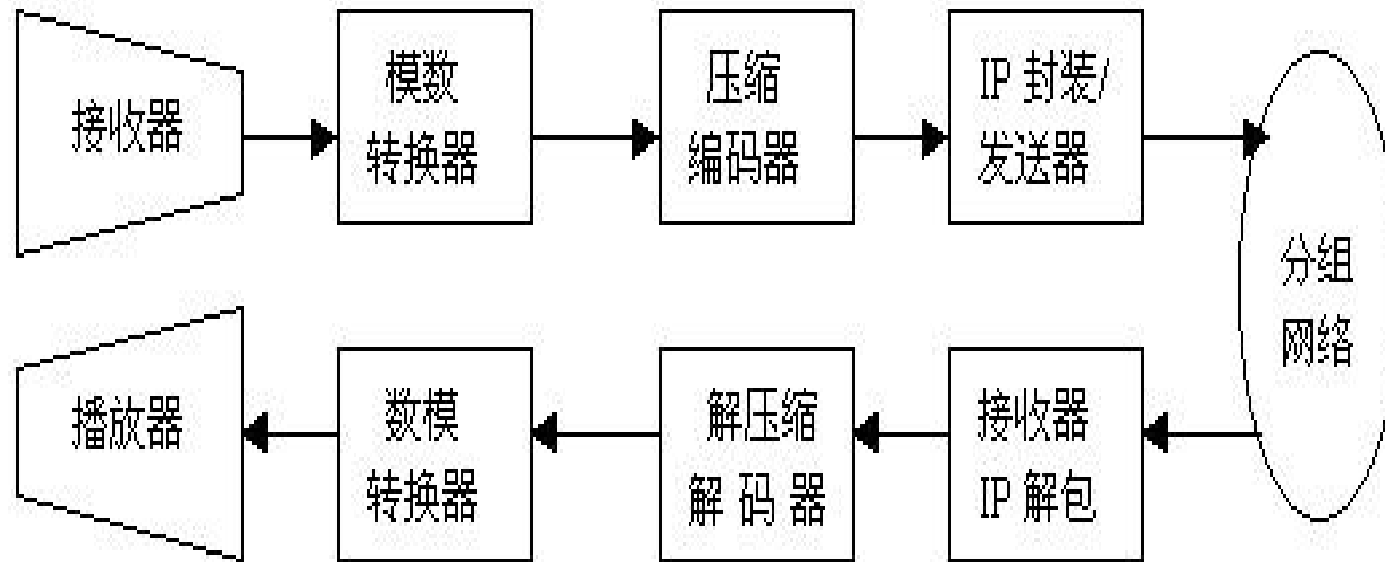
- VoIP技术应用发展历程
- VoIP未来发展趋向
- 安全威胁和问题
- VoIP安全机制概述
- 防御建议

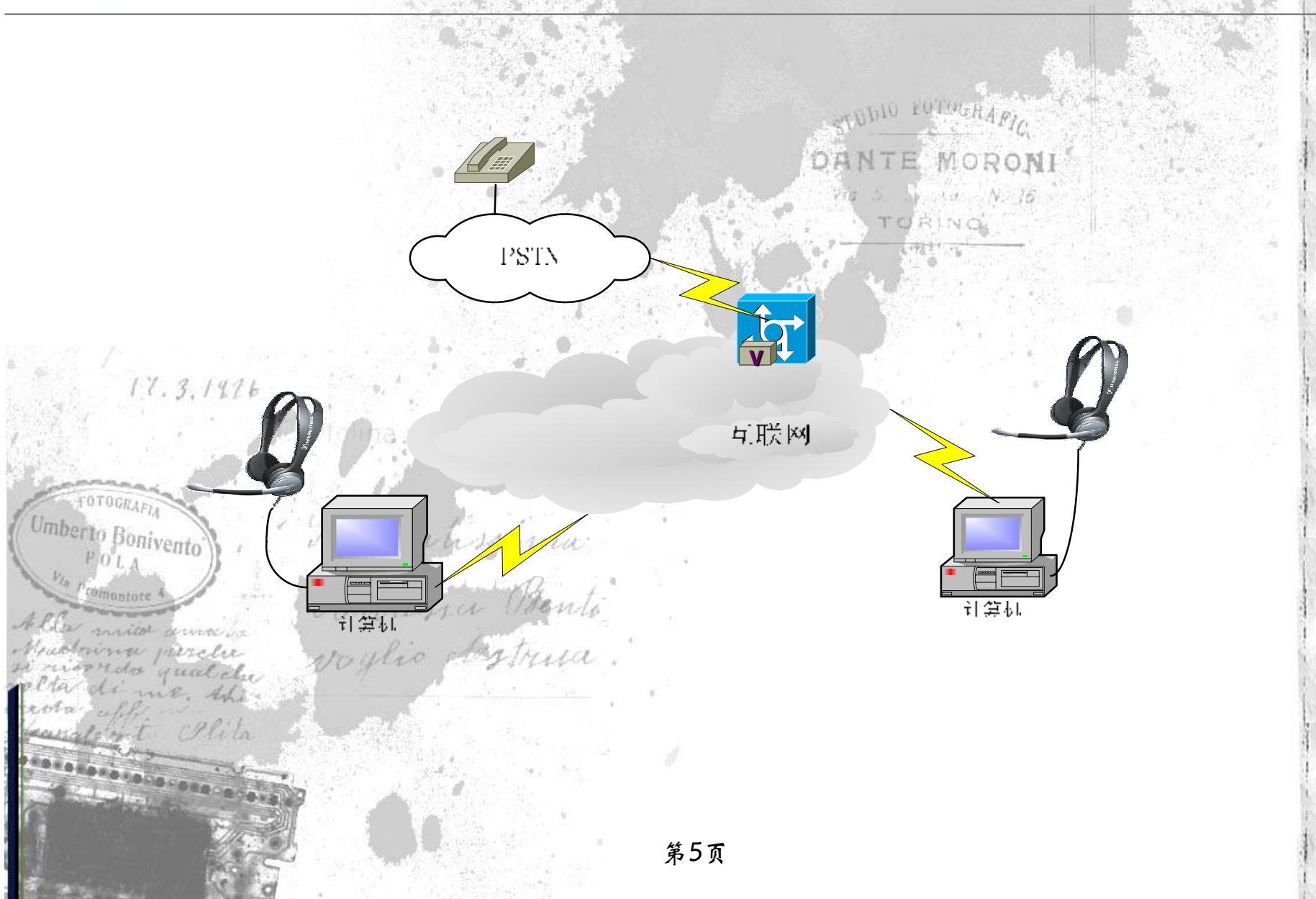
- 最初的VoIP应用

形式：PC2PC和一定PC2PHONE

特点：零散的个人行为。可实现部分的PC到电话的呼叫。

协议：自定义的没标准。没有互联互通性。还没有可运营的概念





- IP电话应用

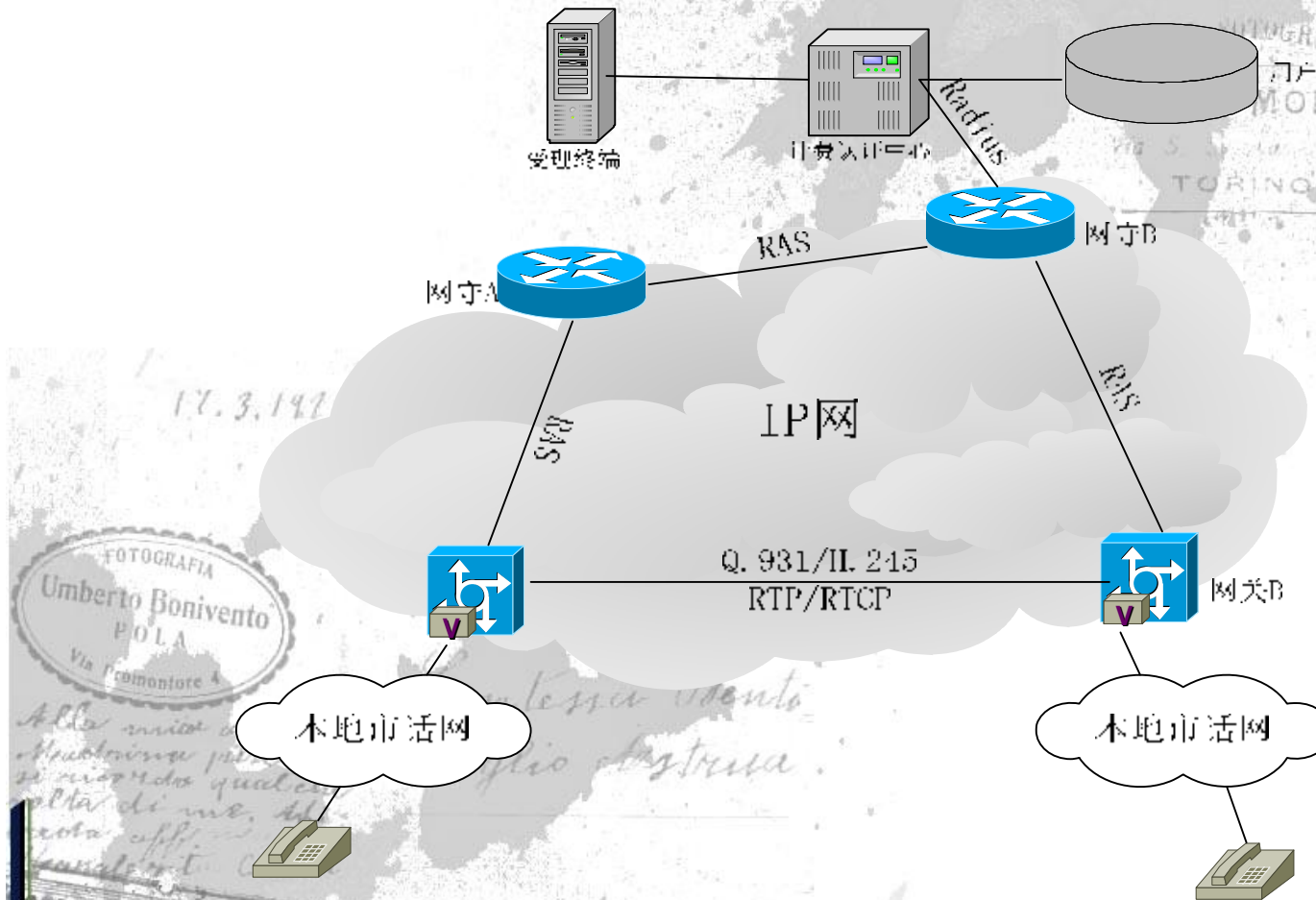
形式：电话到电话；IP电话超市

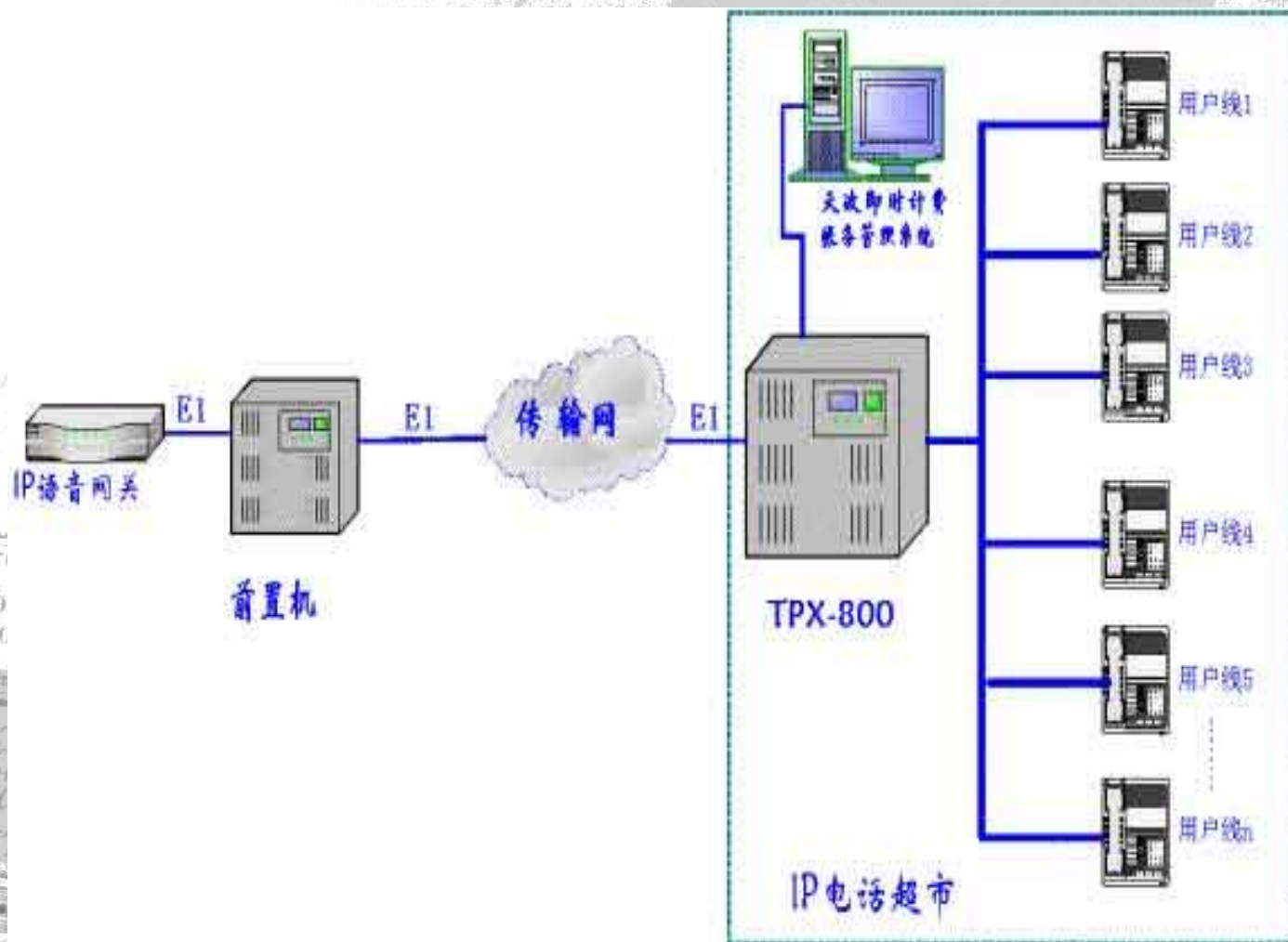
特点：运营商和大企业的参与；有组织的应用；专网

协议：H.323占主流

网络结构：

IP电话网络构架图





- 网络电话应用

形式：IP电话机；宽带电话

特点：虚拟运营商出现；传统运营商提供服务；互联网接入和传输；SMB部署

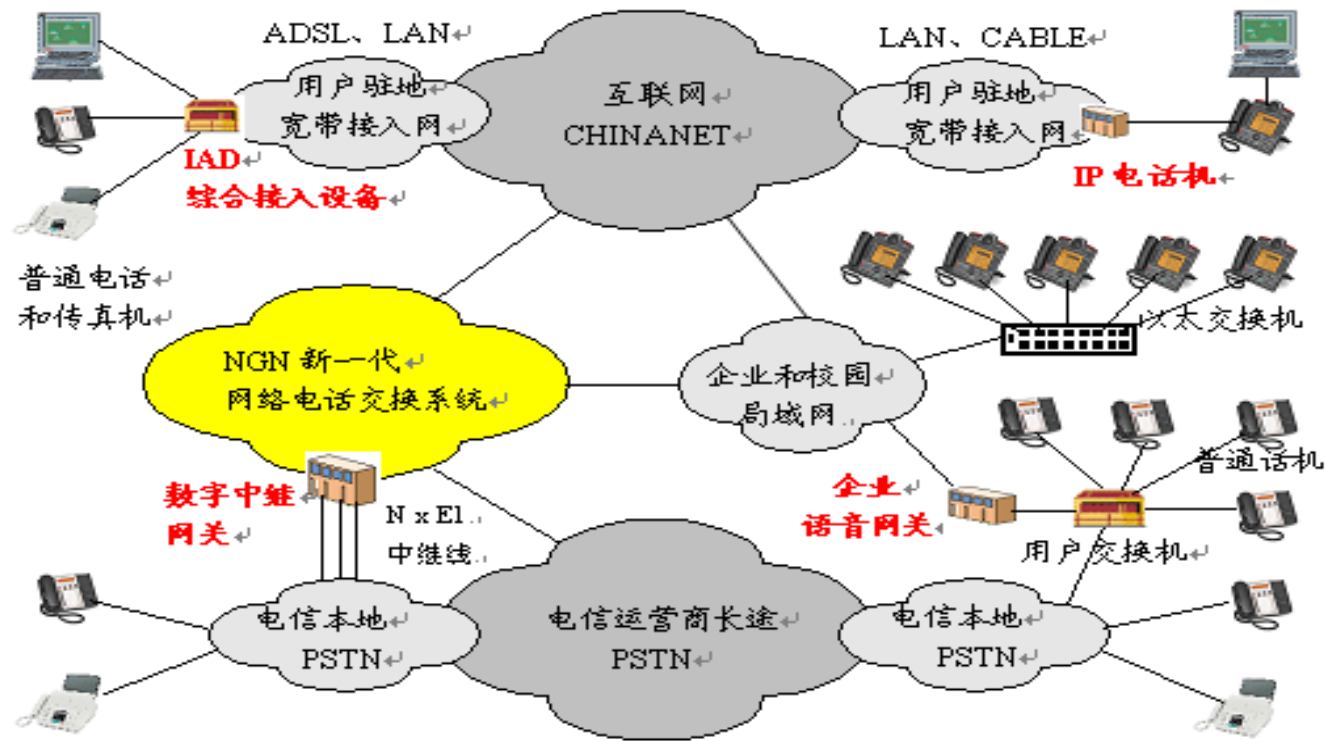
协议：H.323继续优势；SIP表现出强劲发展

势头

网络结构：

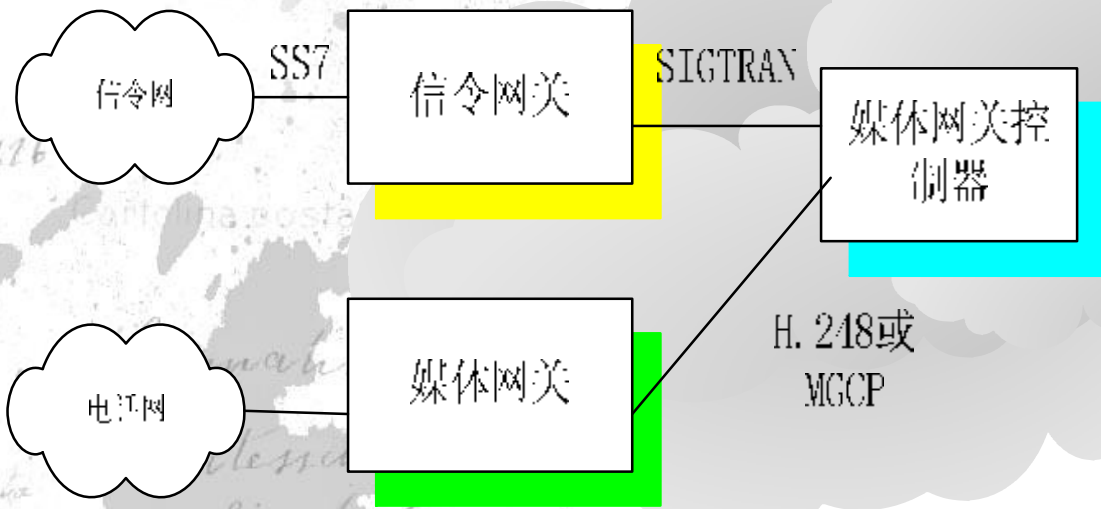
网络基本架构





➤ 总体融合组网和网络电话用户接入模式

- 即可透明的呼叫任何电话，也可作为被叫
- 与PSTN和PLMN的完美融合，可运营的发展方向。
- 媒体网关和信令网关分离
- 控制和业务分离
- 与其他业务融合



- 下一代网络

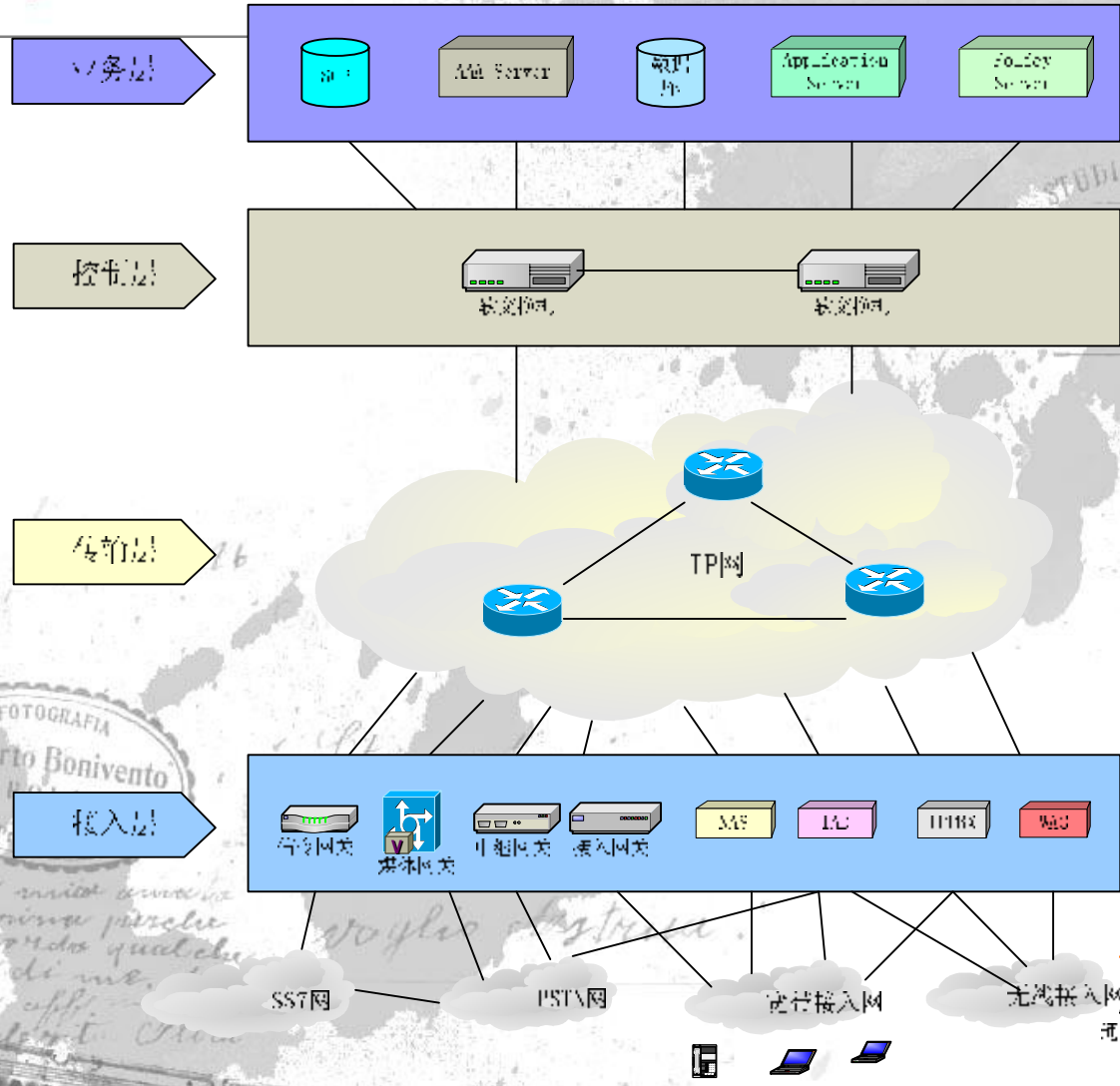
形式：**NGN终端；IAD**

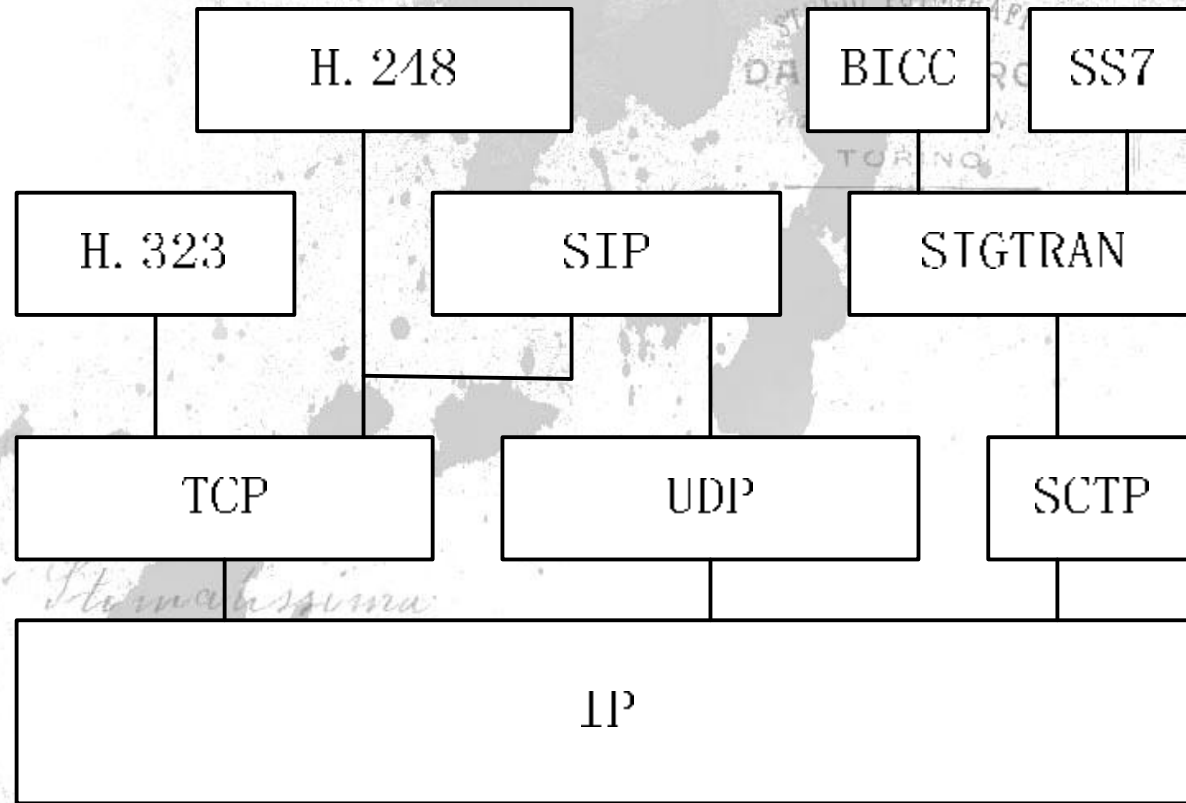
特点：**多网融合；多业务支持（包括话音业务）；电信级运营**

协议：**H.248和SIP**

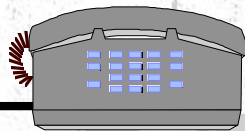
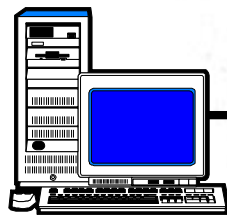
网络结构：**软交换架构**

下一代网络体系结构





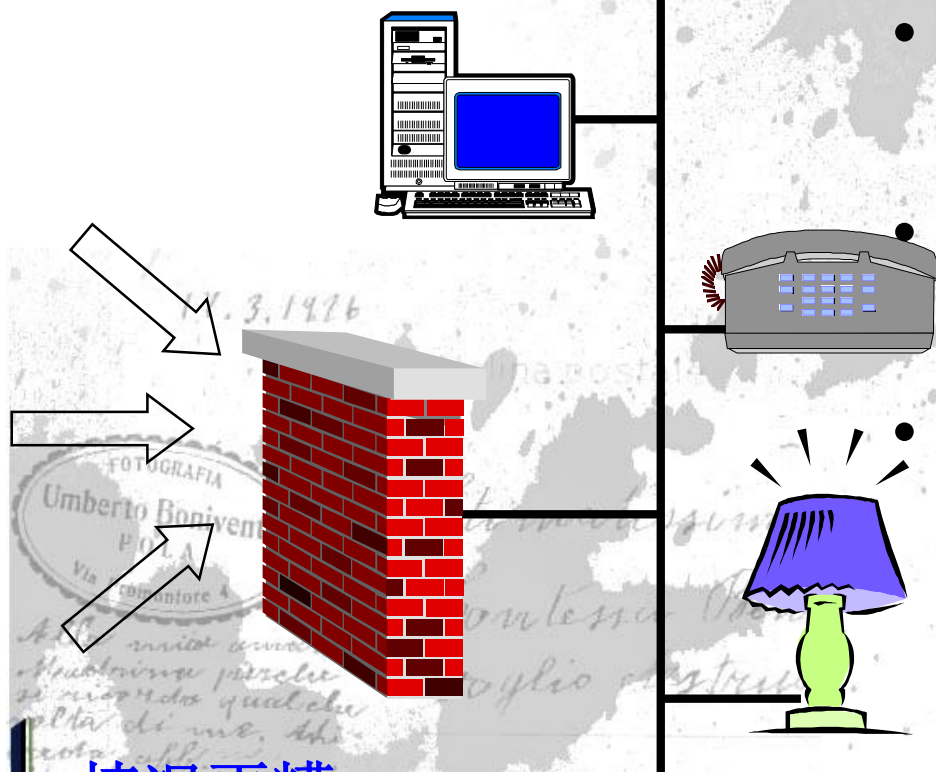
Firewall 问题:



- 有不请自来的呼叫
 - - 可以打开一些知名端口来解决 (5060、1720)，但是...
- 媒体流动态分配端口
 - - 防火墙将阻隔！

即使内部具有公网地址

NAT & PAT 问题:



情况更糟，
为私网地址

- 发布自己的位置
 - - 网守注册
- 信令消息中的是私网地址
 - - 必须修改为可寻址
- 媒体流地址和端口必须重写
 - - **NAT**应当转换以后的公网地址应当可获得

- ALG (Application Layer Gateway)
- MidCom
- STUN(Simple Traversal of UDP Through NAT)
- TURN(Traversal Using Relay NAT)
- ICE(Interactive Connectivity Establishment)
- Full Proxy
- Tunnelling

信息脆弱性

- 用隔离来实现安全（专网）
- 只有接入认证（网络电话）
- 中小企业VoIP应用基本没有安全考虑
- 安全是一个可选项
- 协议只是提出一种机制

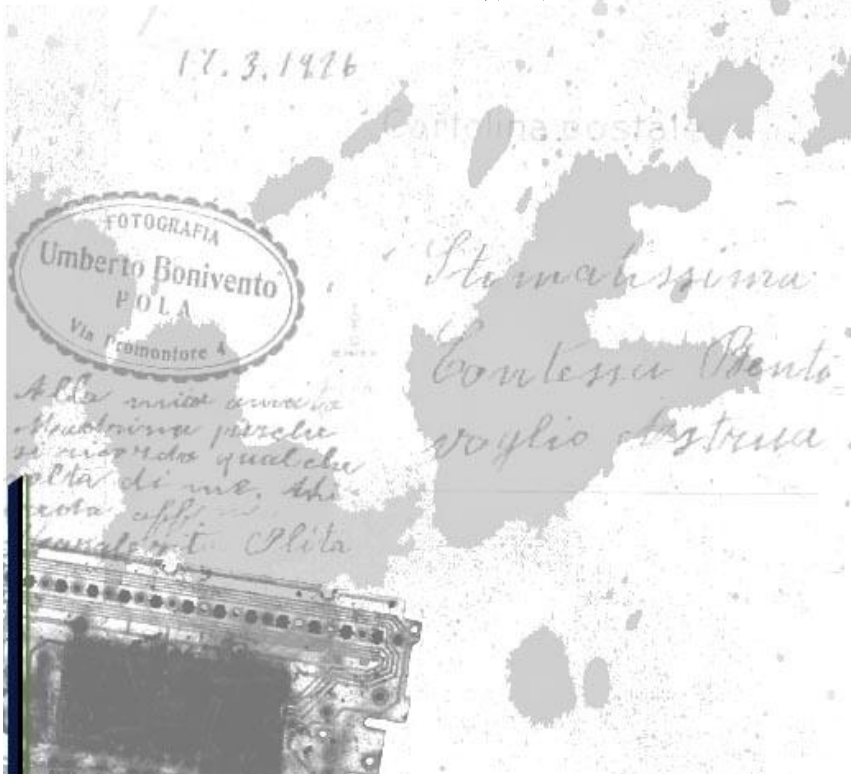
网络脆弱性

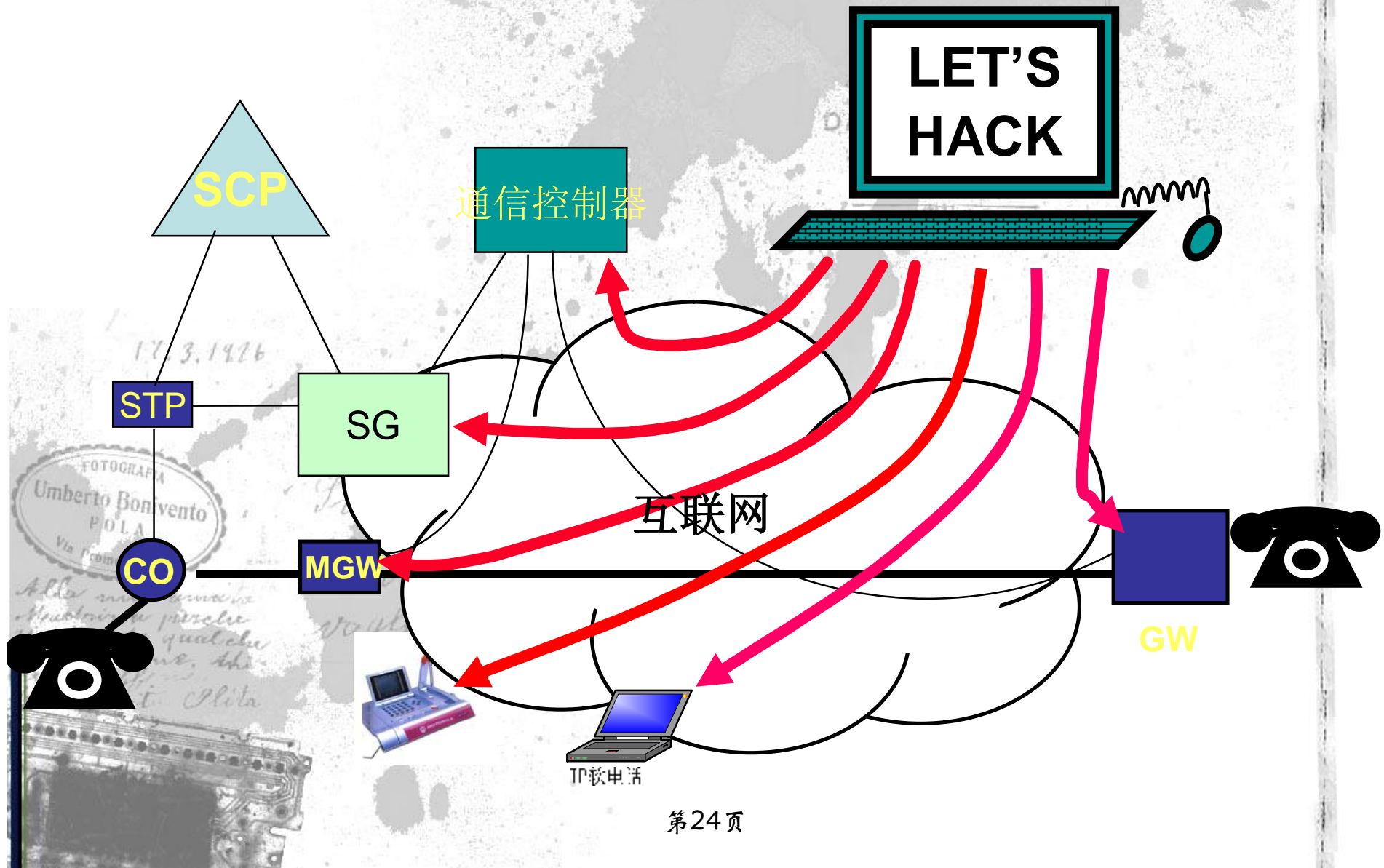
- 实现存在很多漏洞（尤其是H.323）
- 没有任何特意防范 措施
- 真实系统会存在某些特定的问题
- 部署存在问题（还可能带来数据网安全问题）

协议脆弱性

- 存在RTP DoS(普遍存在的一个问题)
- 易受到UDP Flood攻击（尤其采用了比较复杂的安全机制以后）
- 安全协议漏洞

- 电信运营系统的公网接入
- 企业VoIP系统的互联网传输
- 虚拟运营系统基于互联网运营
- PSTN面临威胁





- 拒绝服务
- 非授权接入
- 电话跟踪
- 媒体干扰和插音技术
- 媒体窃听技术
- 会话劫持
- 入侵控制技术
- 话费欺诈
- 电话传单
- 其他威胁

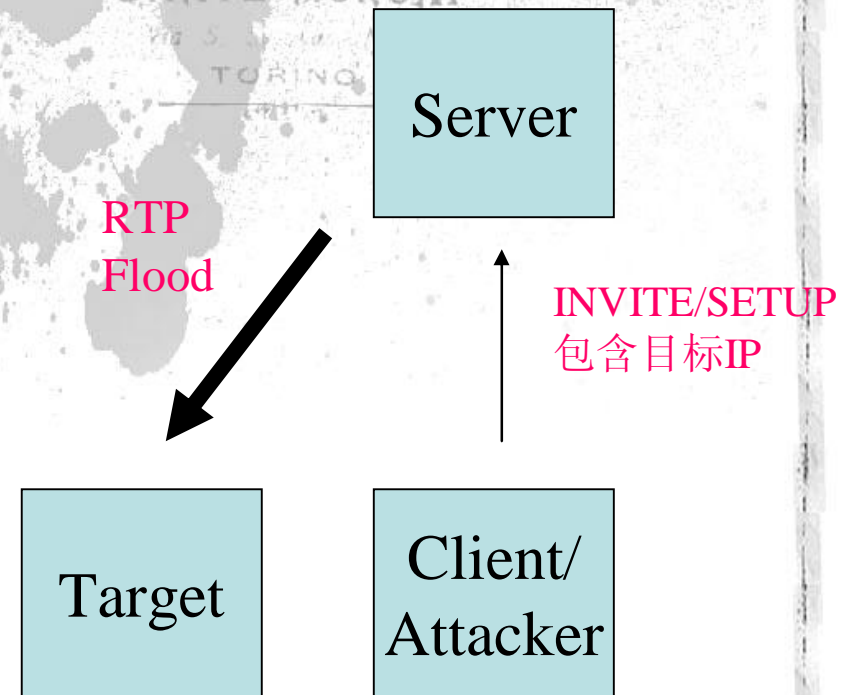
拒绝服务攻击

- 耗费系统资源的DoS攻击
- 大量服务请求式DoS攻击
- 利用系统漏洞式的DoS攻击

特别指出RTP DoS攻击和H.323协议实现漏洞

RTP DoS

- 攻击者发送INVITE或SETUP
- 包含攻击目标IP
- SERVER将发送RTP流给目标



- H.323协议实现漏洞威胁

原理：用ASN.1语言描述的网络协议被评为十大安全隐患之第二。SNMP协议即为其中之一。H323也不例外。

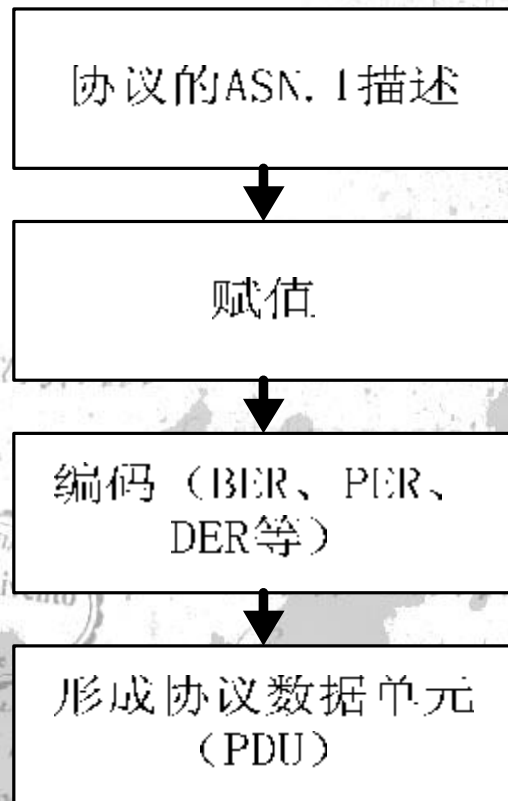
已经有很多VoIP厂商公布漏洞信息。微软从年初到现在已经公布两个了相关漏洞。（MS04-001，MS04-07，MS04-10）

危害：可造成系统入侵。

H323-UserInformation ::= SEQUENCE – root for all
Q.931 related ASN.1

```
{  
  h323-uu-pdu H323-UU-PDU,  
  user-data SEQUENCE {  
    protocol- discriminator INTEGER(0..255),  
    user-information OCTET STRING(SIZE  
      (1..131)),
```

```
  } OPTIONAL,  
}
```

- 协议应用非常灵活
- 协议描述比较复杂
- 编码方式实现容易出现缓存去溢出漏洞
- 网络协议描述可造成远程攻击

- 媒体攻击威胁

基于嗅探技术和网络伪装技术而形成的一种攻击方式。

包括窃听，干扰，插音，阻塞等几种攻击技术。

- 电话跟踪与劫持

通过对通话信令数据包的嗅探和协议分析，提取目标电话状态信息。

在一定的的时候可以劫持该通话链路或者随时终止该会话。

- 非授权接入技术和话费欺诈
- 突破某些认证的算法
- 重放攻击
- 中间人攻击

- 电话传单

午夜凶铃式传单

发布信息式传单

或者叫骚扰电话，这是一种主动式攻

击，如果和非授权入侵攻击和其他伪装技术配合将产生严重的社会问题。

- 其他威胁

一般数据网络中的安全威胁

针对VoIP网络部署特别的威胁

比如对AAA服务器或为解决NAT穿透而引入代理服务器等。

- TLS/SSL
- IPSec

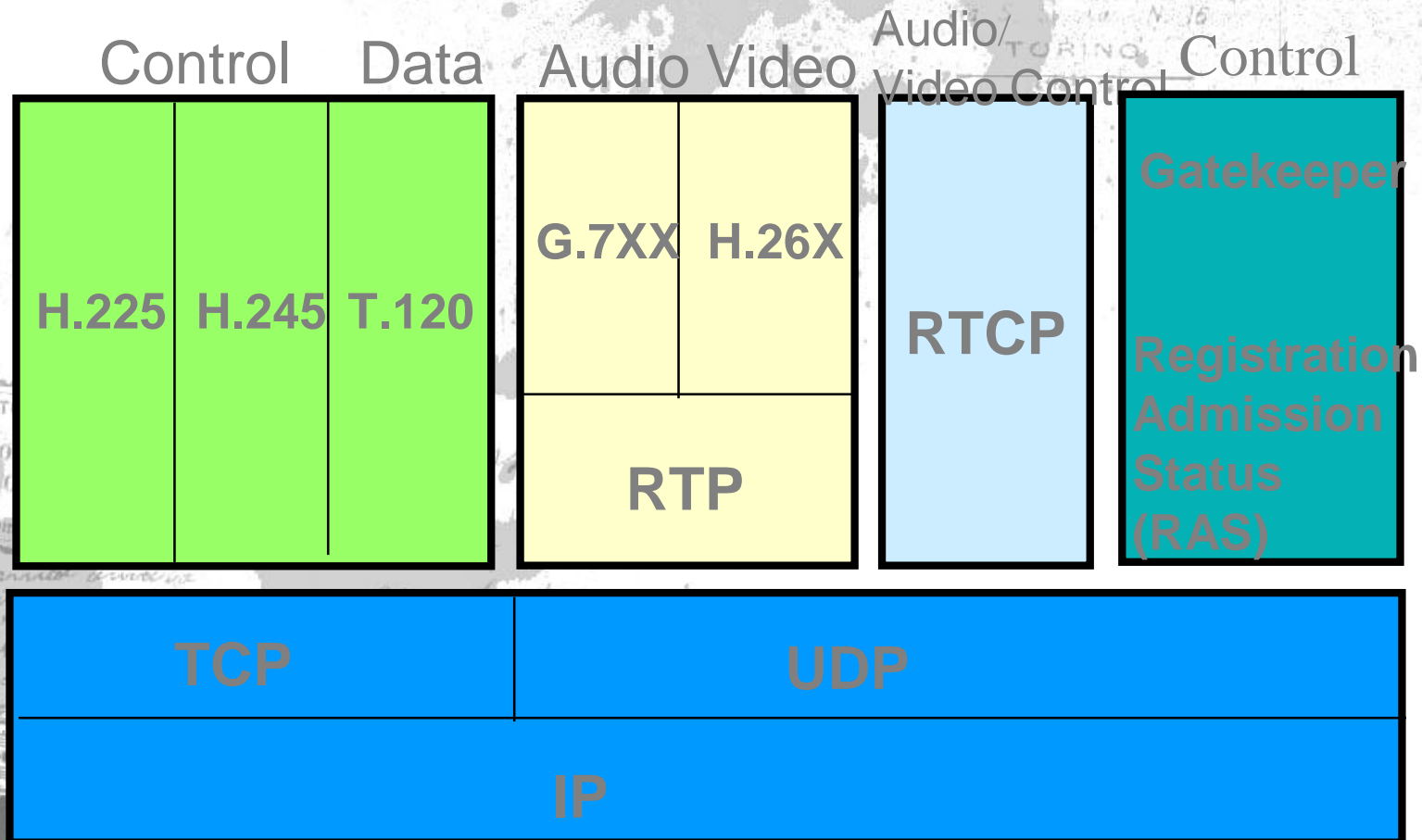
以上两种安全机制在数据网络中使用非常普遍

- 应用层安全机制

在不同的体系结构下采取不同的安全机制

- Radius

- H.323的协议体系



基本的H.323流程

网守寻找

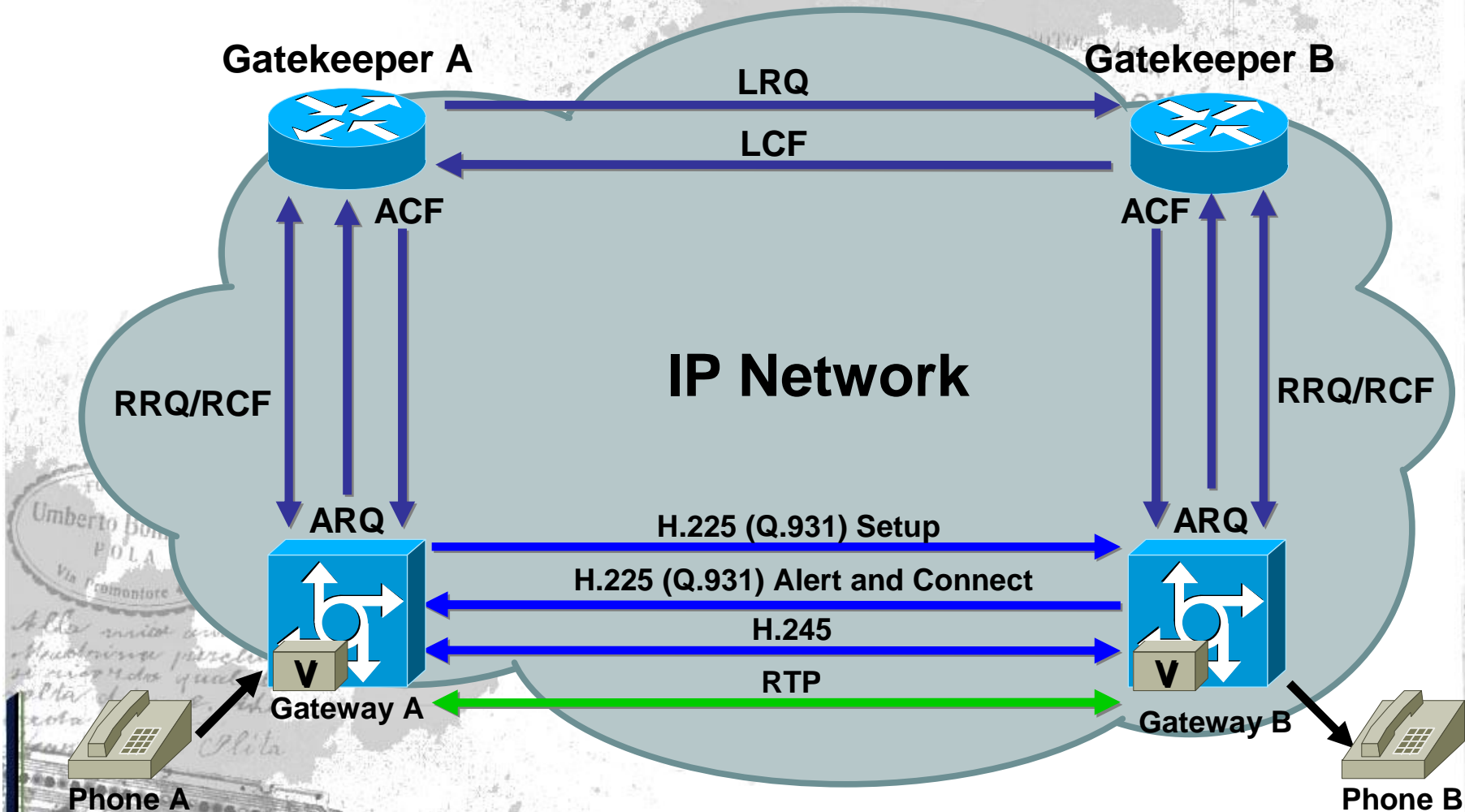
网关注册

地址解析

呼叫建立

通话过程

链路拆除



- H.323安全方面的策略

ICV;

Diffie-Hellman;

password with symmetric encryption;

password with hashing ;

Certificate with signature ;

something else ;

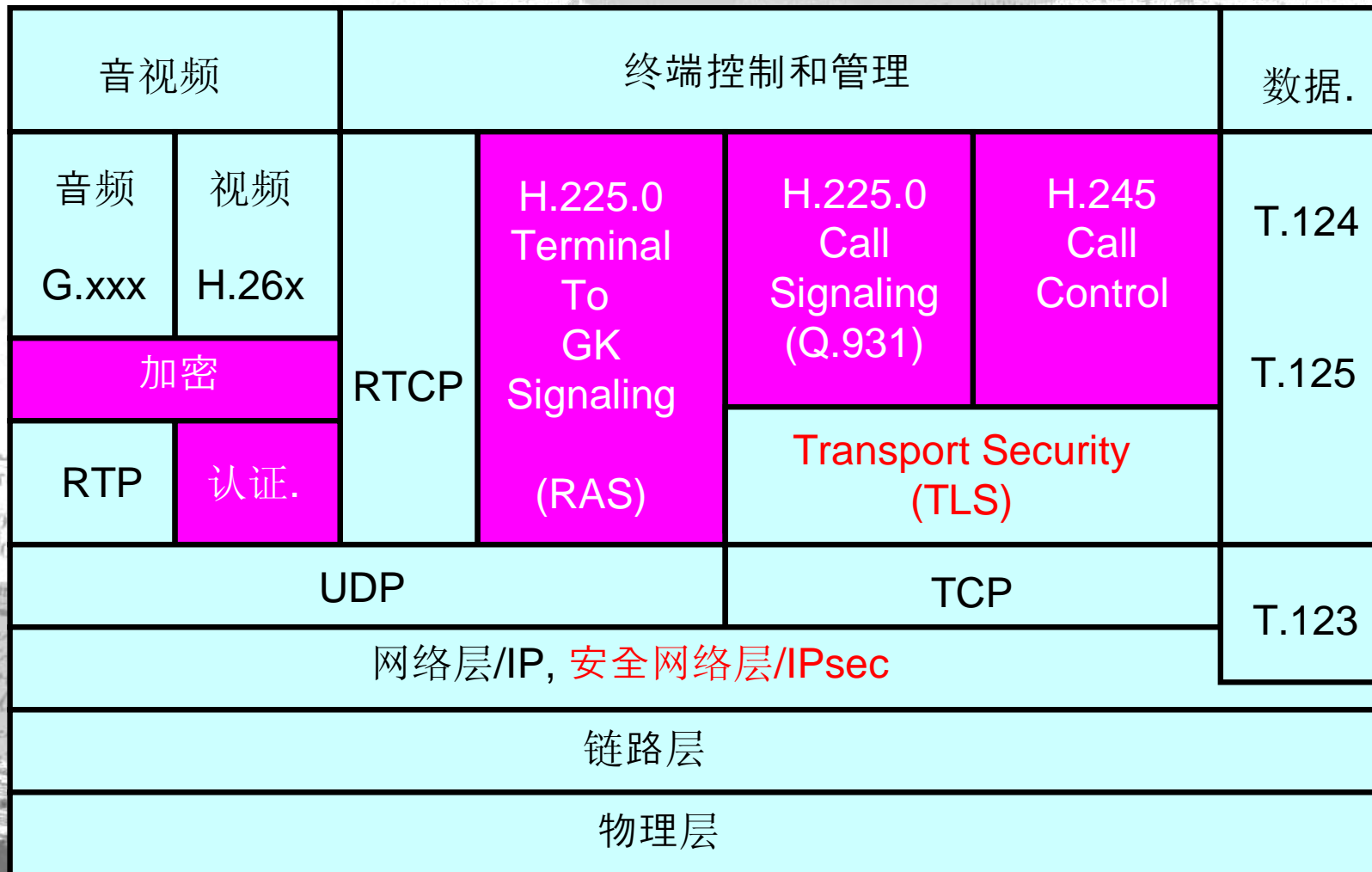
- 实现方法

tokens

cryptoTokens

两字段承载所有安全信息。H.235详细定义了它们的具体的用法。

H.235作用域



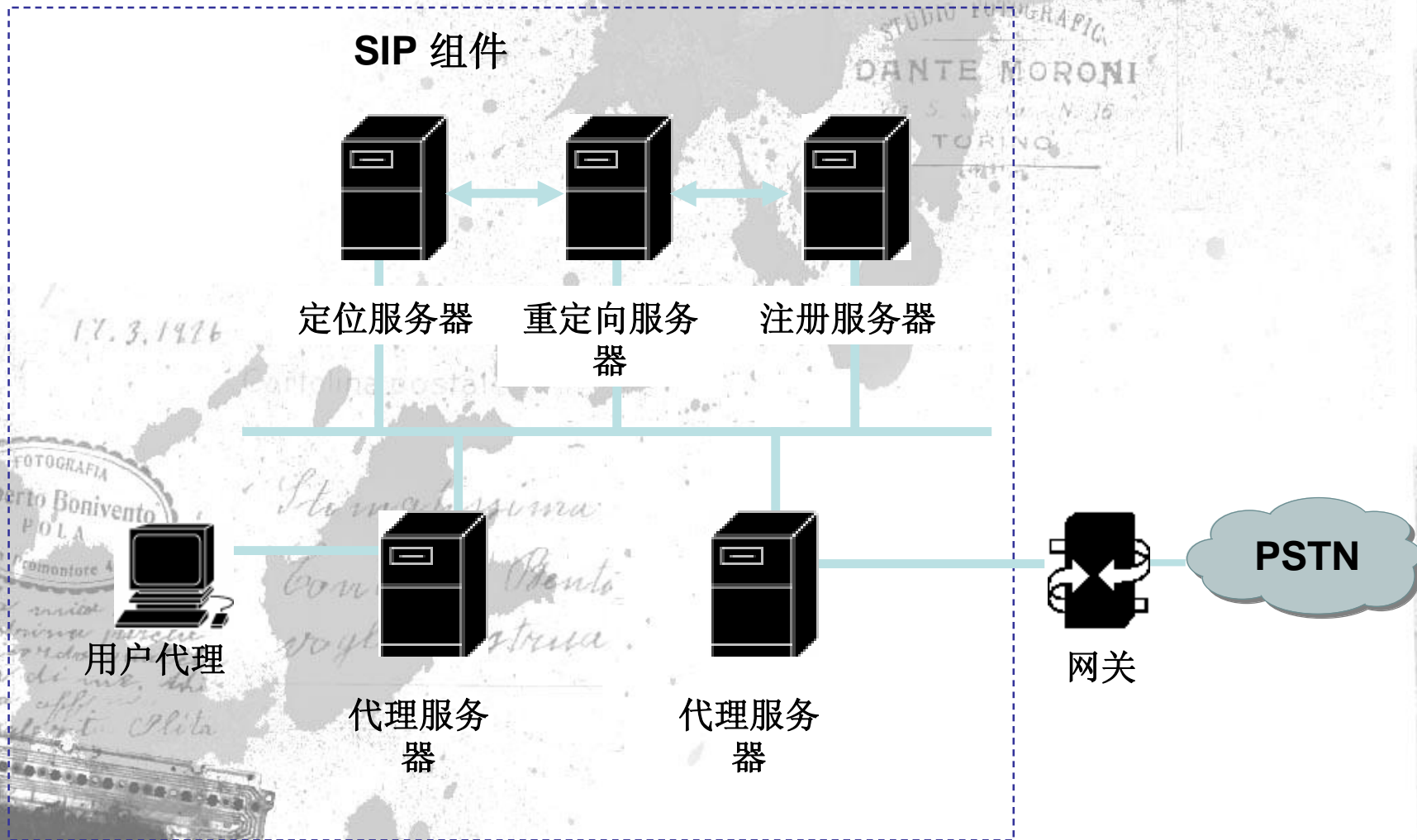
- 基于SIP协议的网络

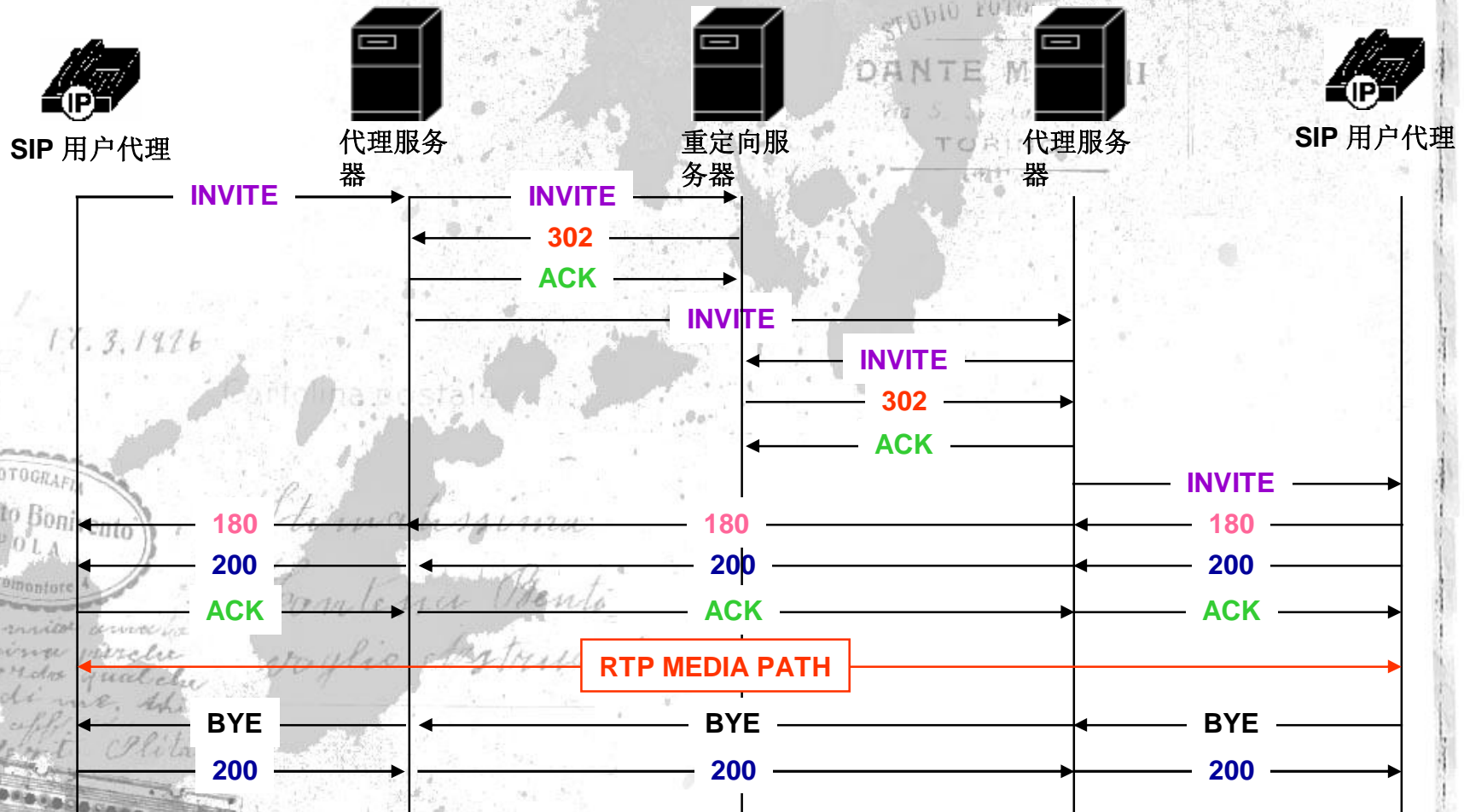
信令简单

格式简单

组网灵活

3G支持





- SIP体系中的安全机制

Basic认证（新的RFC中不采用）

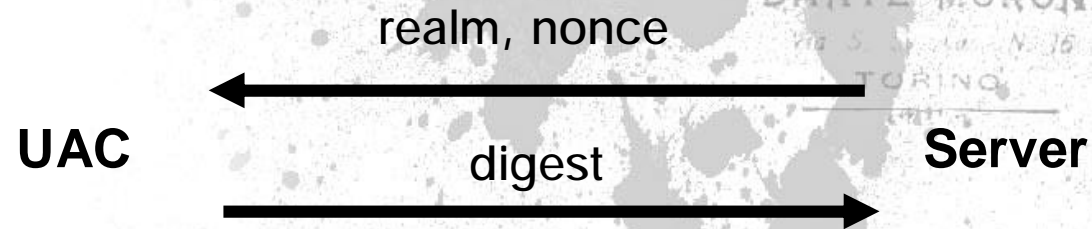
Digest 认证（类似于HTTP Digest）

S/MIME机制

PGP机制（在新RFC中已经不在建议采用）

SIPS Url Scheme（属于传输层范畴）

- Digest认证



$\text{digestedPW} = H(\text{username}:\text{realm}:\text{password})$

$\text{Digest} = H(\text{digestedPW}:\text{nonce}:H(\text{method}:\text{URI}))$

特点: 1、挑战-响应机制
2、没有提供完整性检测和保

密性

- S/MIME机制
- 1、完整性、保密性和认证
- 2、需要公钥证书和PKI



```
INVITE sip:u@h SIP/2.0
From: sip:bob@foo
To: sip:a@c
Content-Type: multipart
```

SDP

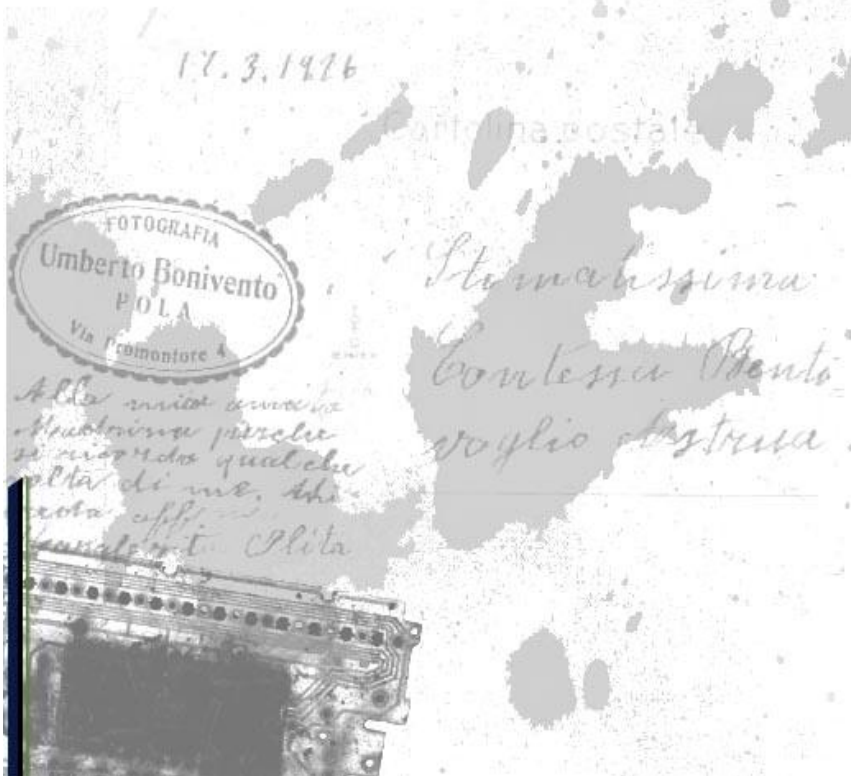
```
INVITE sip:u@h SIP/2.0
From: sip:bob@foo
To: sip:a@c
Content-Type: SDP
```

SDP text

signature

certificate

- 目前的RTP/RTCP
 - 内嵌利用PEM-style-CBC加密的安全机制；
 - 没有包认证机制（期望底层协议提供）；



- 安全RTP (SRTP)

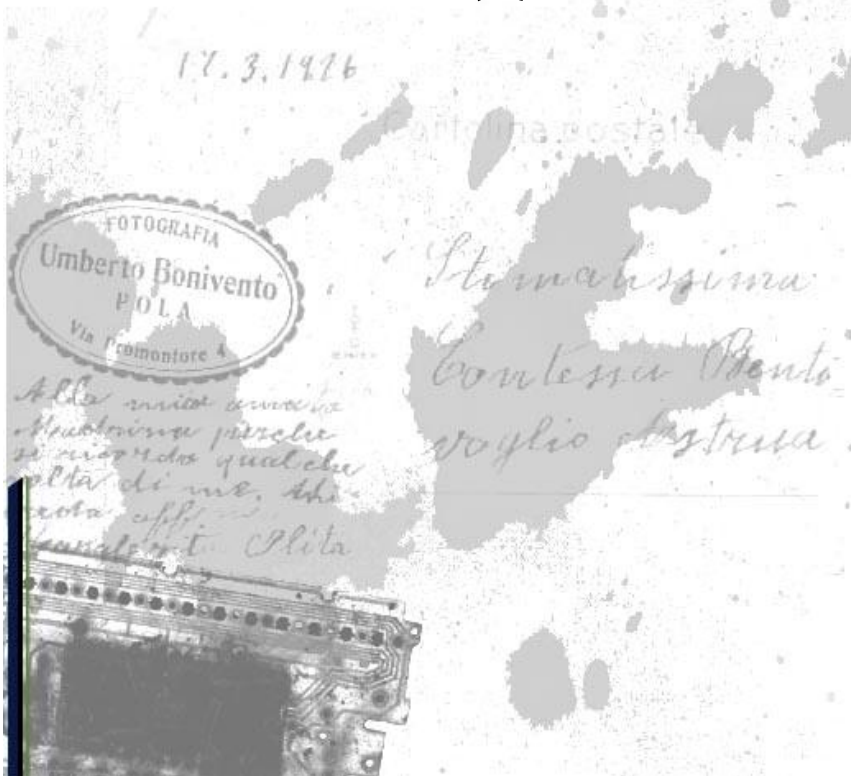
已经作为一种草案提出；
内置保密和认证的RTP协议安全机制；
加密：AES, AES f8mode
认证：HMAC-SHA1
还没形成标准；

- 会话密钥管理

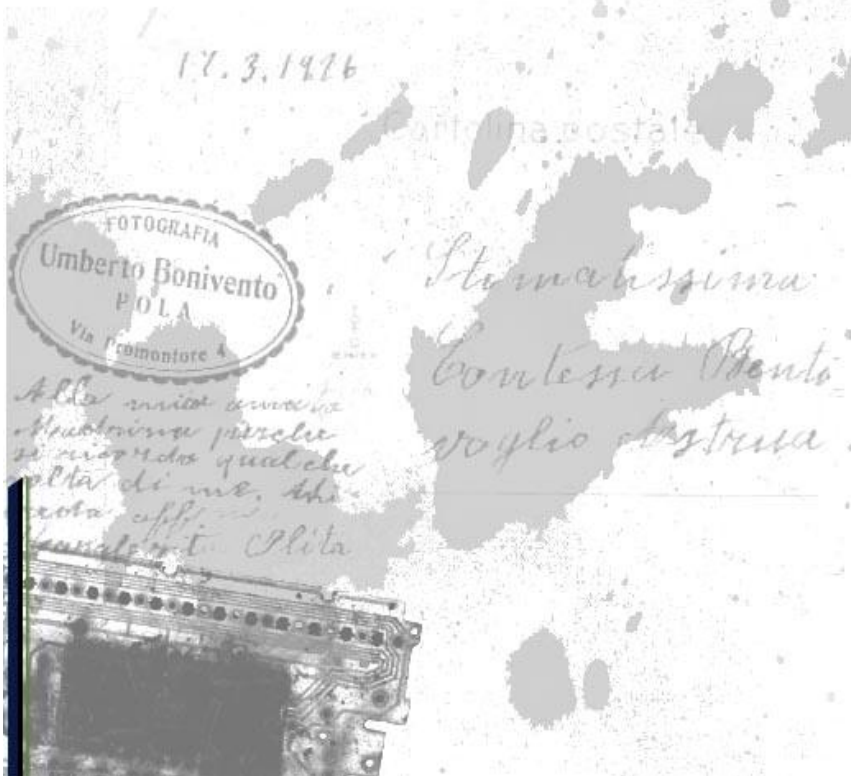
前期安全信令中传输 (SDP或SETUP) ;

Diffie Helman key exchange ;

IKE或Kerberos



- 只能解决部分安全问题
- 也会带来新的安全问题
- 有些脆弱性是本身的问题



- 关掉不必要的服务
- 增加接入的强身份认证
- 数据包认证
- 媒体加密
- 媒体源认证
- 研究与数据网络共存的安全体系
- 其他的安全措施

希望能够给予指导
欢迎提出宝贵建议

E-mail: hyperfeng@163.com

QQ : 106810831

电话 : 13691007935