XFOCUS TEAM
From Internet,for Internet

VoIP network security threats and strategies

Liu lifeng

Beijing University of Posts and
Telecommunications Info-Security Center

X'CON 2004

X'con 2004

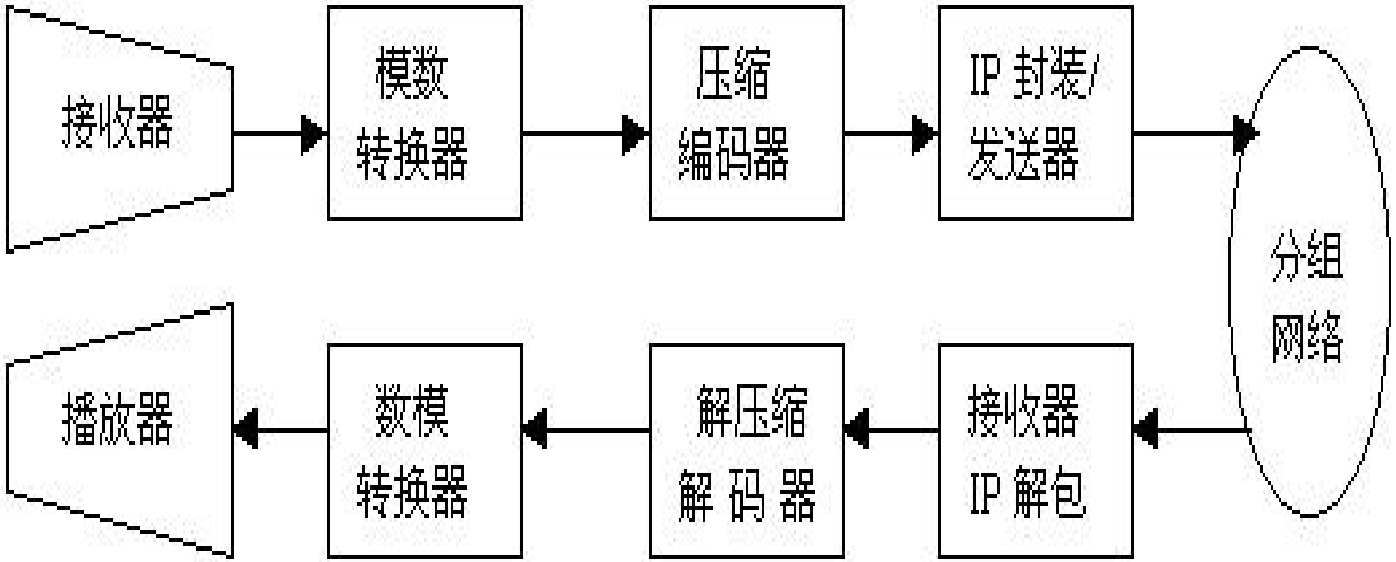
Agenda

- The development course of VoIP
- The future development tendency
- VoIP security issues
- The summary of the VoIP security mechanisms
- The Security defence proposings

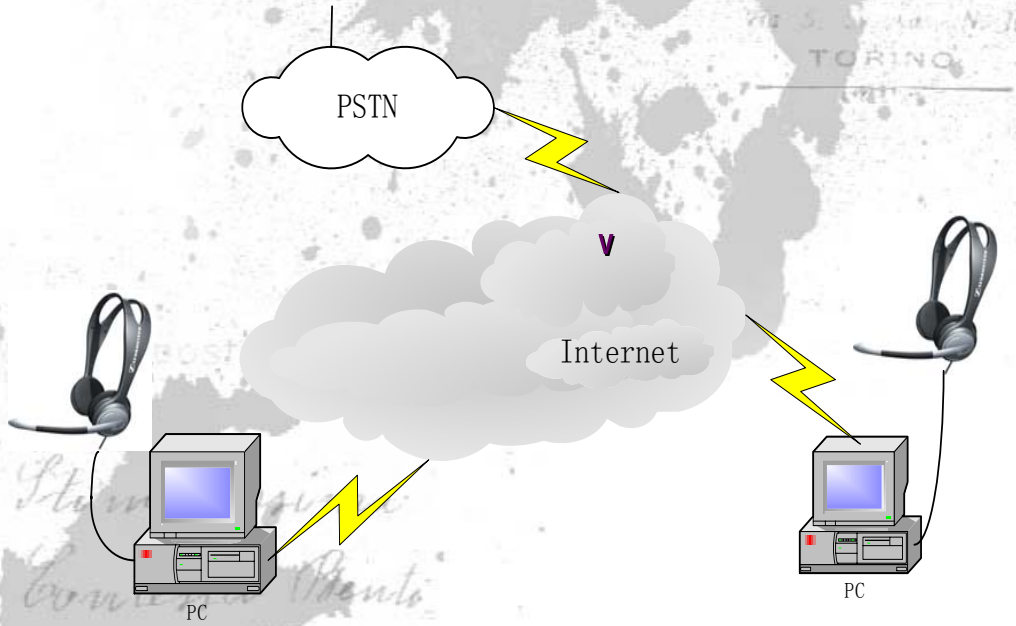
The development course of VoIP

- The initial application scene of VoIP
  - Forms: PC2PC ; PC2Phone
  - Characteristic: interpersonal communications; only realize partial calls from PC to telephone
  - Protocol: custom , without standard, without interpenetration, without interoperability and without the concept of operation

The process of the VoIP basic transmission



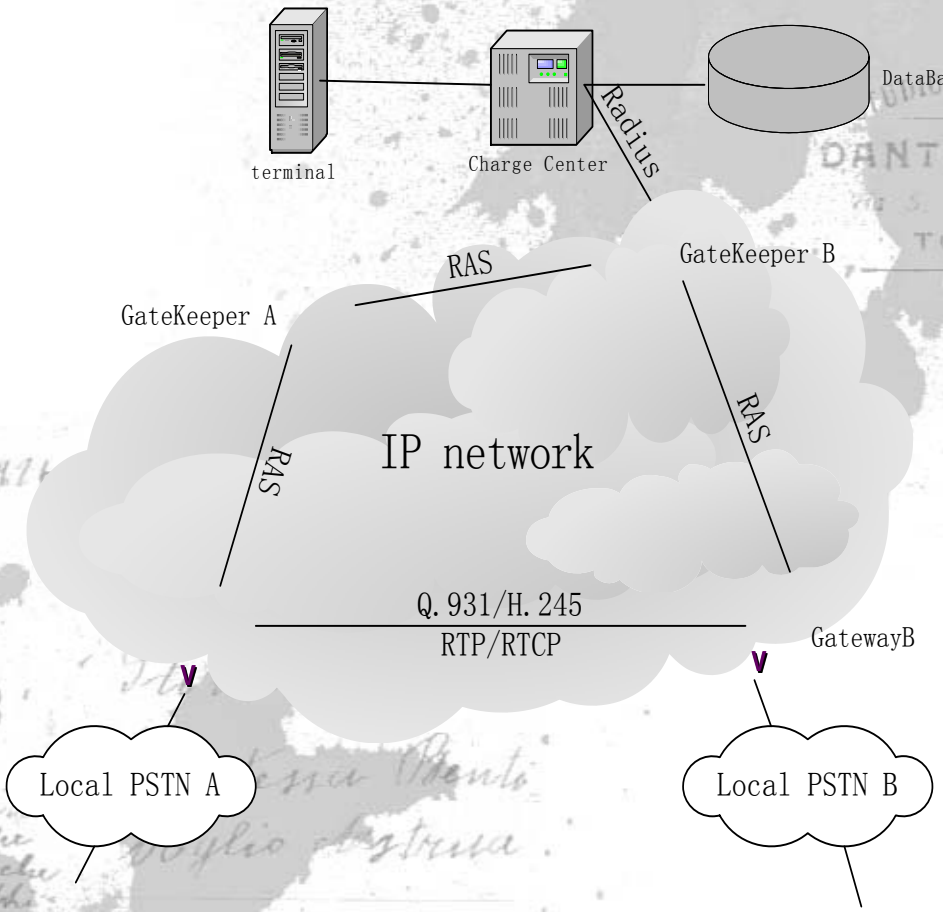
The initial application scene



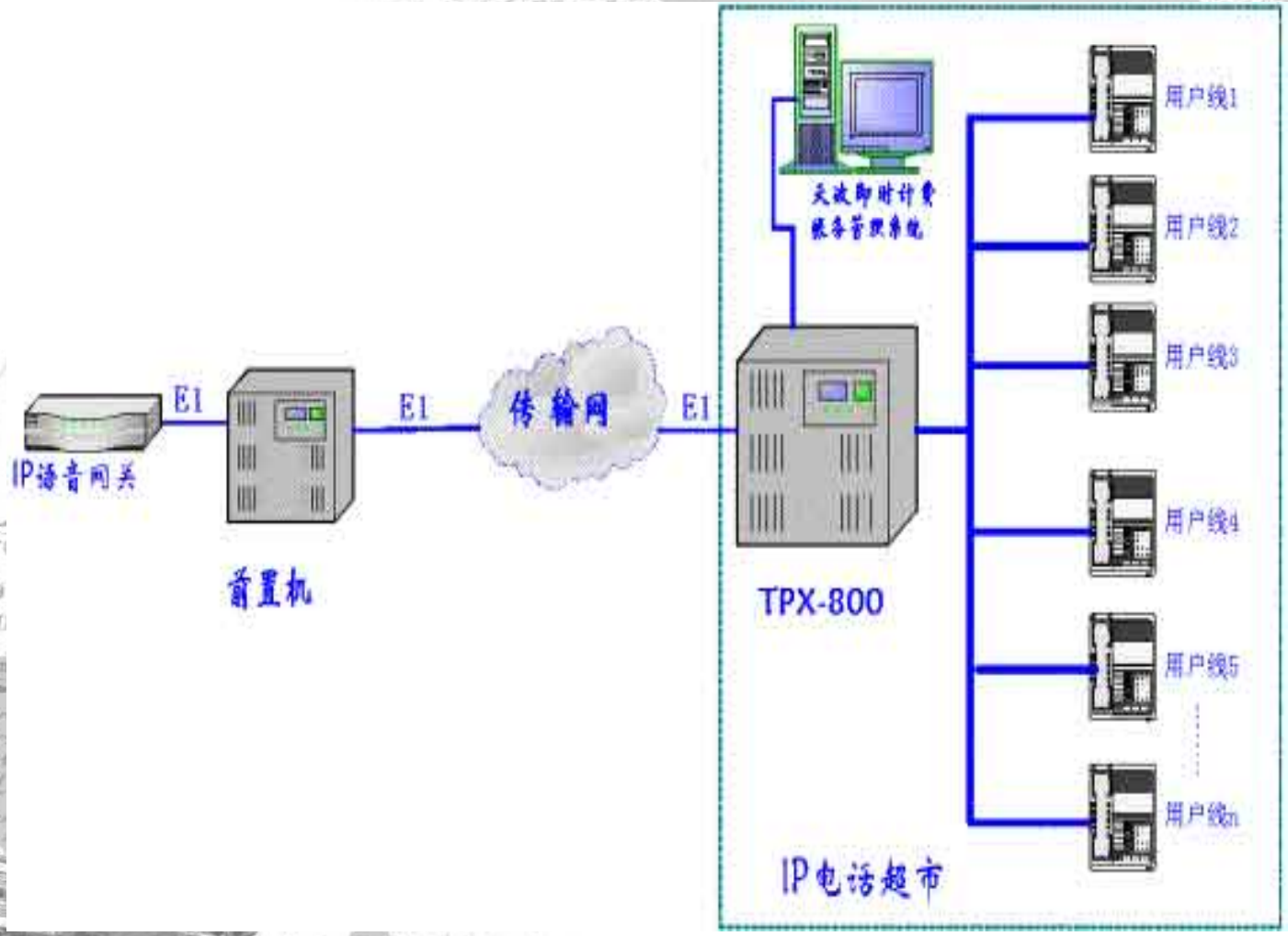
The development Course of VoIP

- The application Form of IP Phone
  - Form: phone to phone ; IP phone supermarket
  - Characteristic: The participation of carriers and enterprises ;Systematical application; Special network
  - Protocol: mainly use H.323
  - The network stucture:

typical structure of IP Phone network



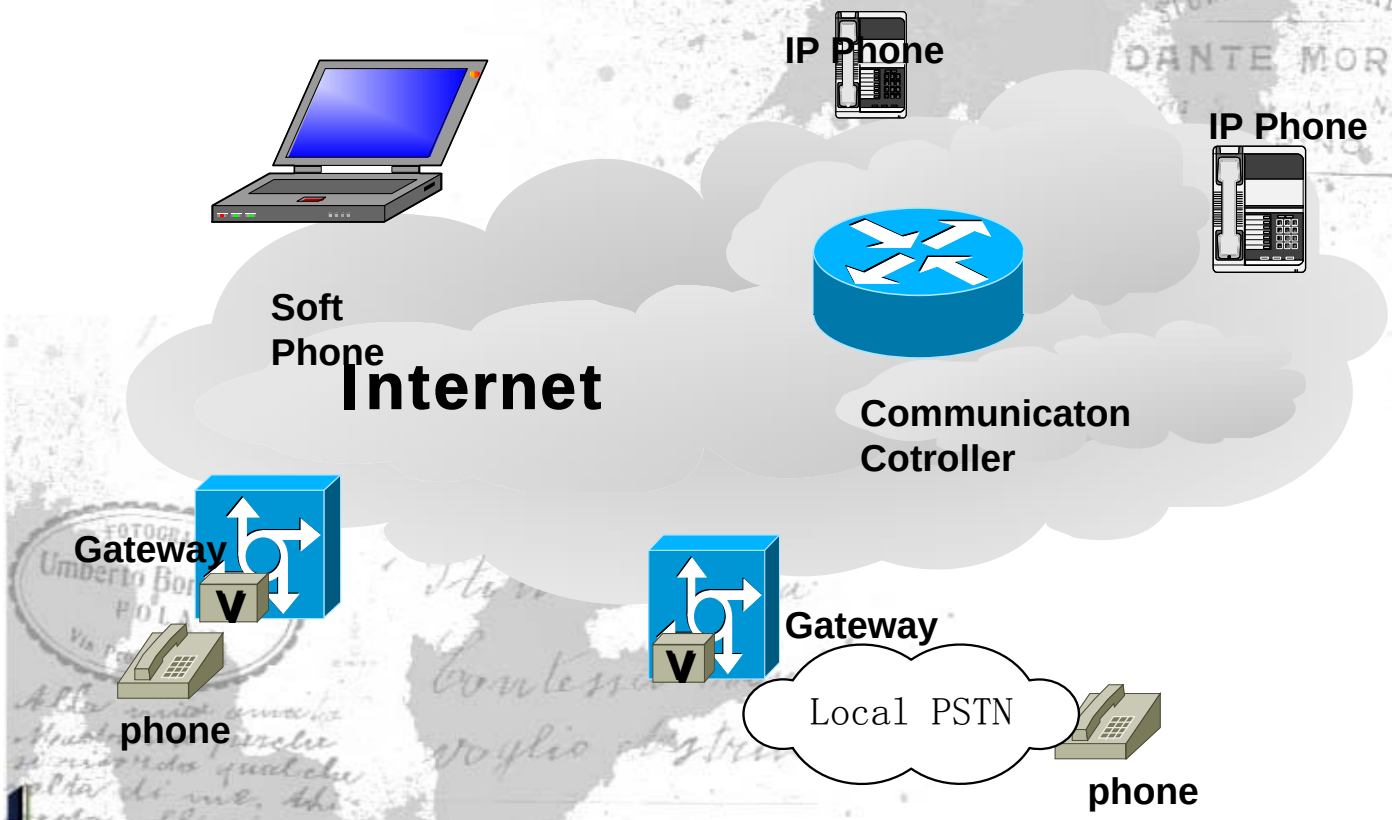
The IP Phone supermarket access



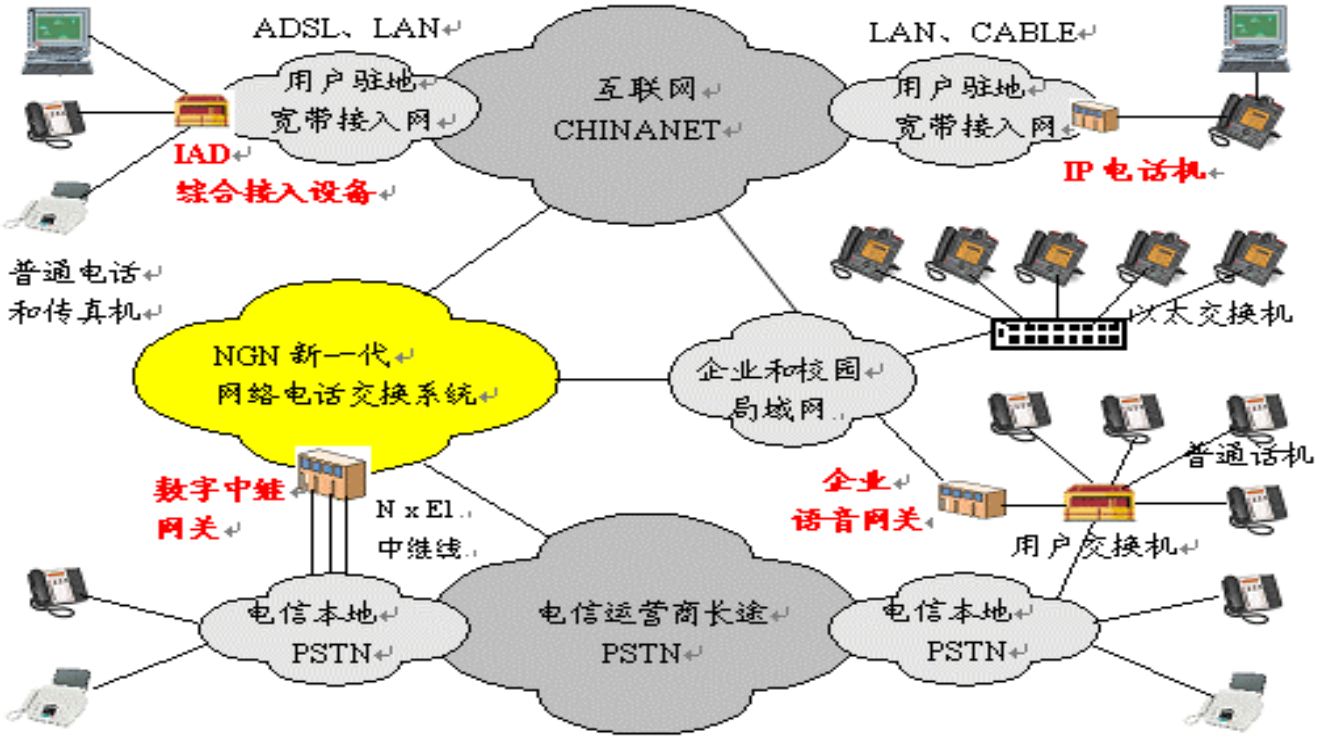
The development course of VoIP

- The application Form of network phone
  - Form: IP phone; wide-band phone
  - Characteristic: virtual carriers emergence ;traditional carriers provide service; internet access and transmission ; SMB deployment
  - Protocol: H.323 dominate continue; SIP show mighty tendency
  - The network structure:

The basic structure of Internet phone



Convergence network operating pattern

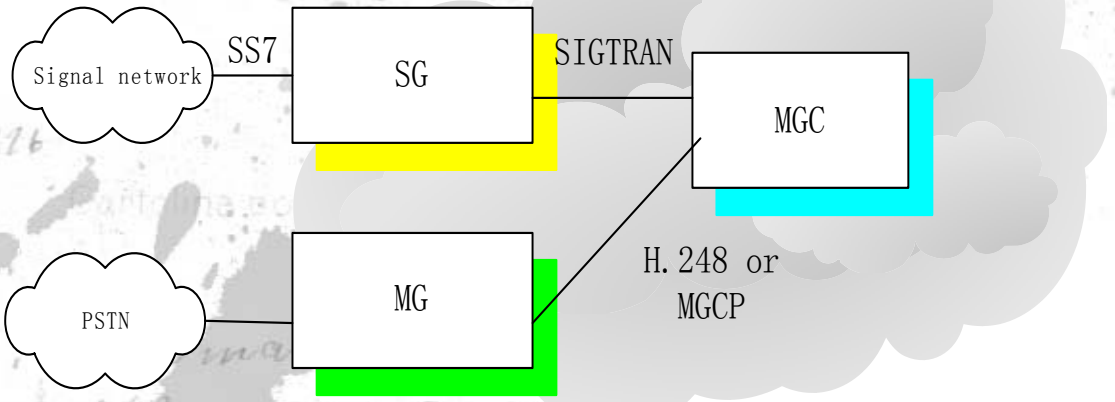


总体融合组网和网络电话用户接入模式

The development tendency of VoIP

- Make any transparent call, so do as the called
- Perfect convergence of PSTN and PLMN; the tendency of operation
- The Separation of media gateway and signal gateway
- The separation of control and service
- Converge with other services

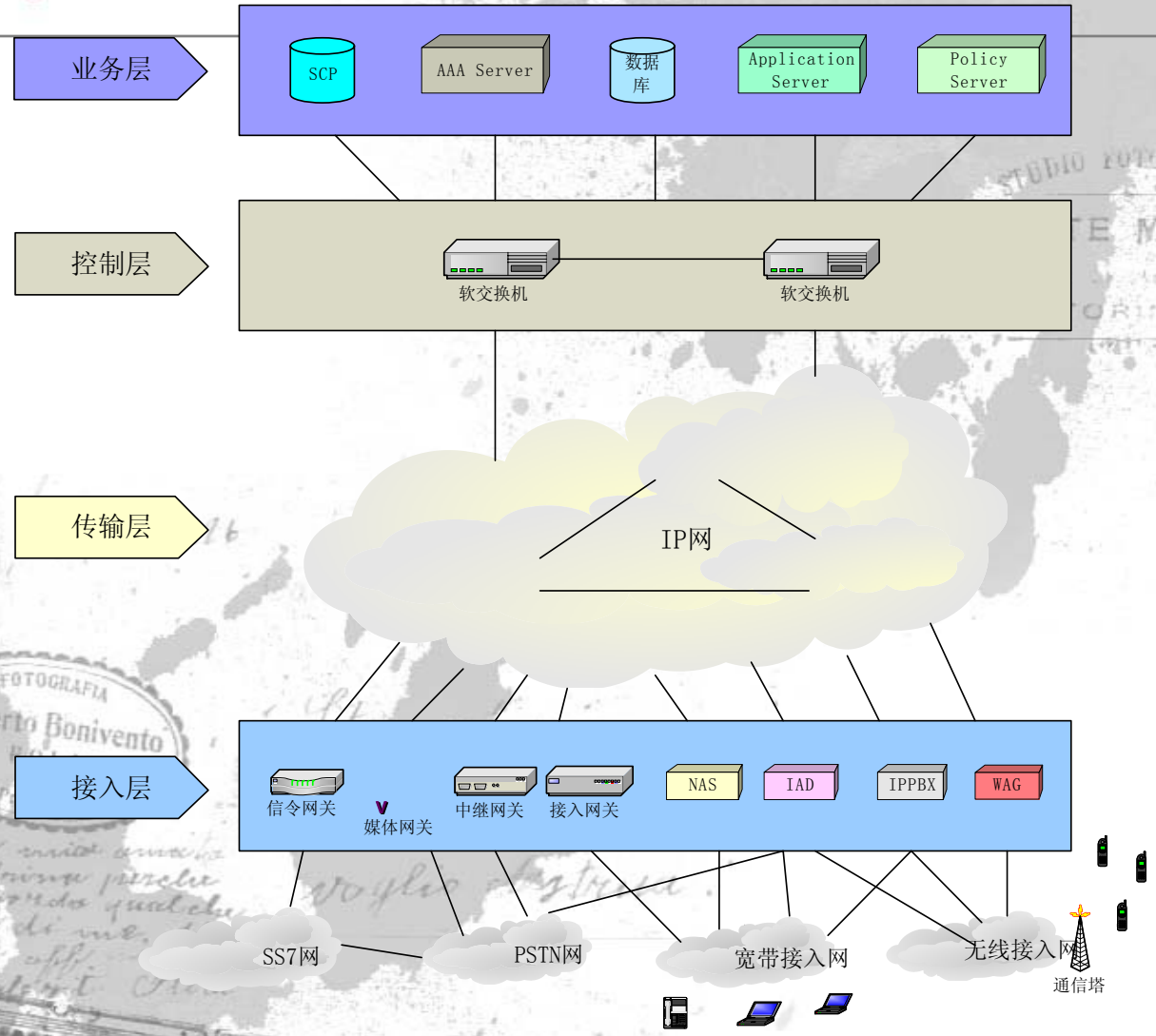
The sketch map of the gateway separation



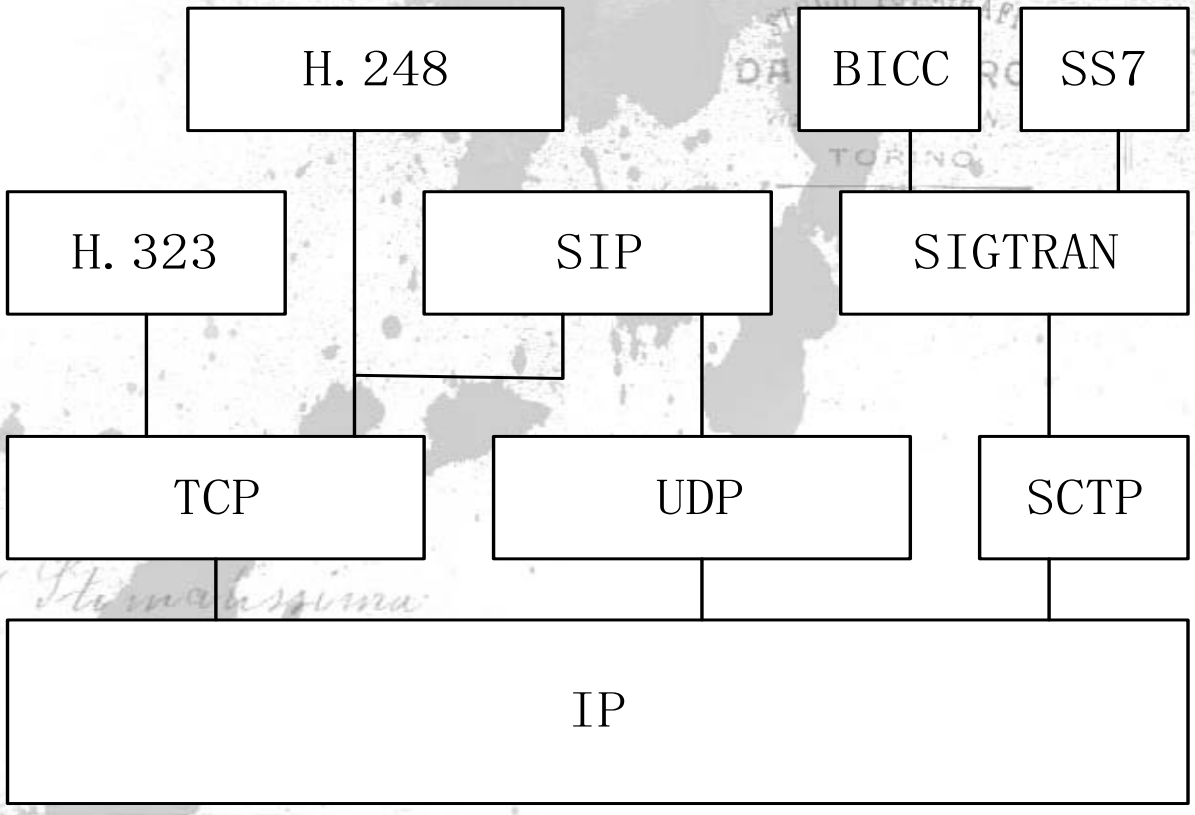
The development tendency of VoIP

- NGN
  - Form: NGN terminal; IAD
  - Characteristic: network convergence; multi-service support (including voice service); carrier –level operation
  - Protocol: H.248 and SIP
  - Network structure: soft switch structure

NGN structure

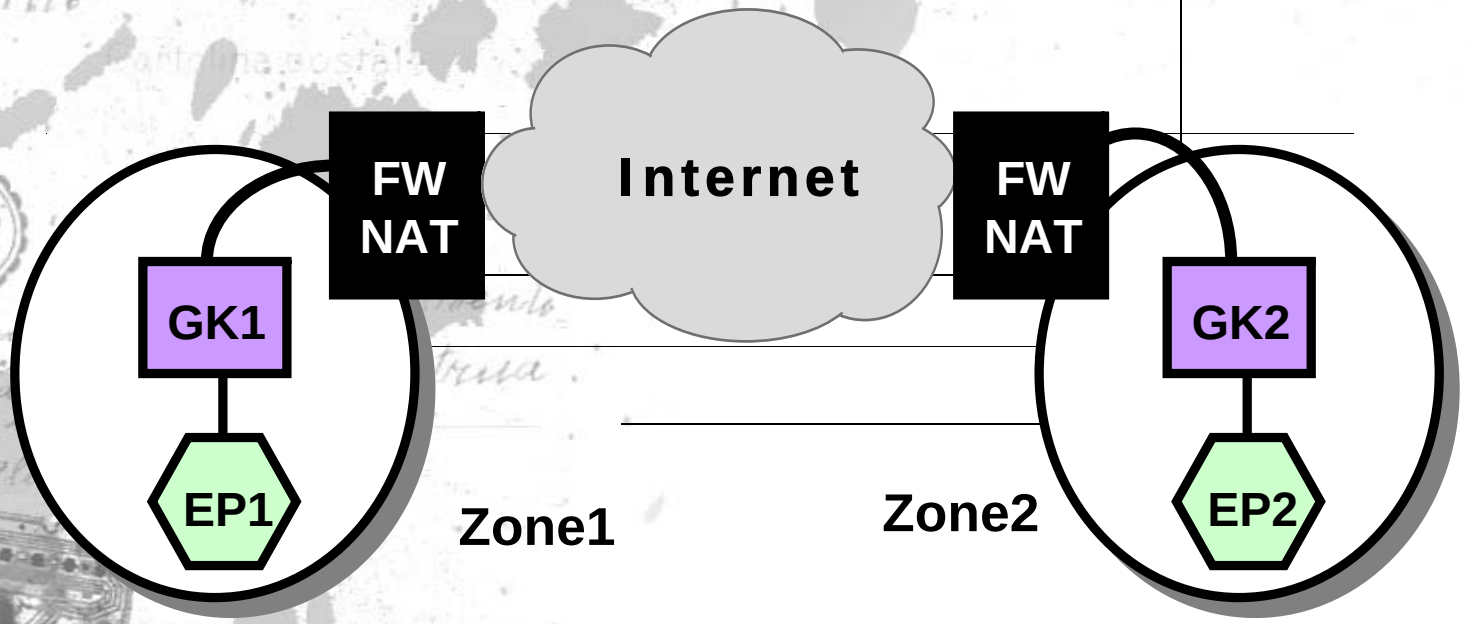


The call and control protocol system of NGN



VoIP and Firewalls/NATs (1)

- Firewalls cannot open/close holes for addresses/ports embedded in payload without application level proxy
- NATs cannot translate addresses/ports in the payload unless it has Application Level Gateway (ALG)



VoIP and Firewalls/NATs (2)

- End-to-end encryption/authentication at IP or TCP layer will not work through firewalls/NATs
- Timeout issues in UDP
  - Call Control channel may be closed while media channels are active
  - NAT address binding has a lifetime equal to that of TCP connection, So NAT will terminate the media streams as soon as TCP is closed
- Multicast does not run through NAT
  - Devices behind NAPT will not receive multicast since attached networks ca appear like a single end station
- H.323 is harder to handle since it uses ASN.1 encoding compared to SIP using text-based encoding

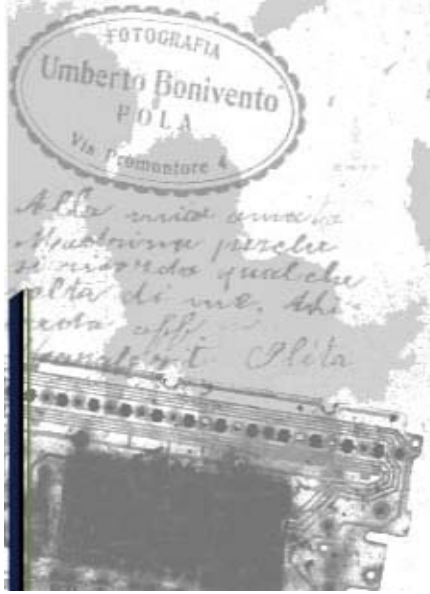
The solutions of the FW/NAT tarversal

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

The vulnerabilities of the existing VoIP network

Info-Vulnerability :

- obtain security by isolation (for example special network)
- Only access authentication (for example Network Phone)
- SMB VoIP systems take little security measures
- Security is option
- Protocol only difines a security mechanism



The vulnerabilities of the existing VoIP network

network vulnerability :

- Realization exists a lot of holes (especially H.323)
- Without any specific dependency measure
- Real system will exist some specific problems
- Deployment exist problems (perhaps bring data network security problems)

The vulnerabilities of the existing VoIP network

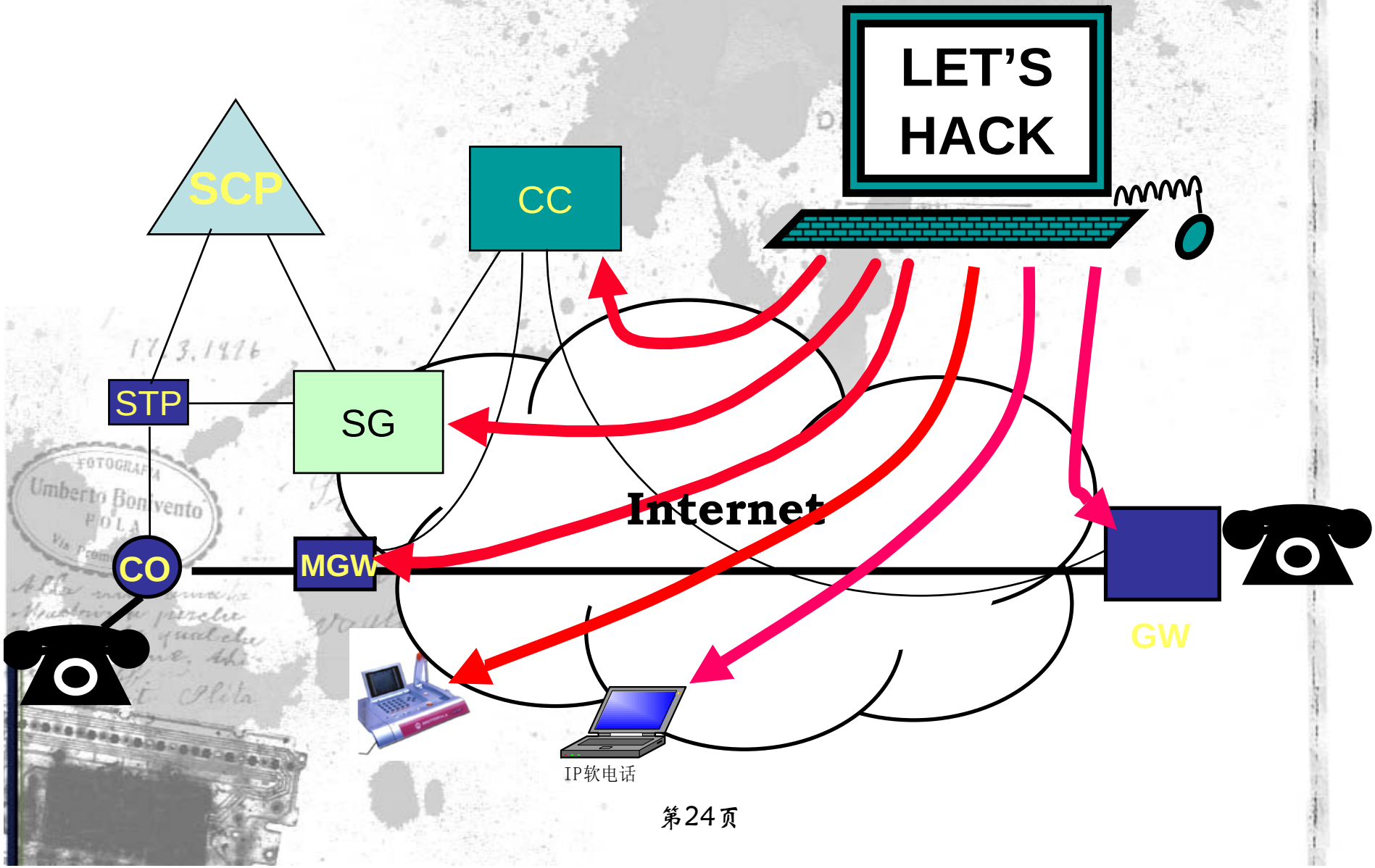
Protocol vulnerability

- Exist a universal problem of RTP DoS
- May be affected UDP Flood attack (especially adopt relatively complicated security mechanism)
- Security protocol holes

The possibility of vulnerability change into security threats

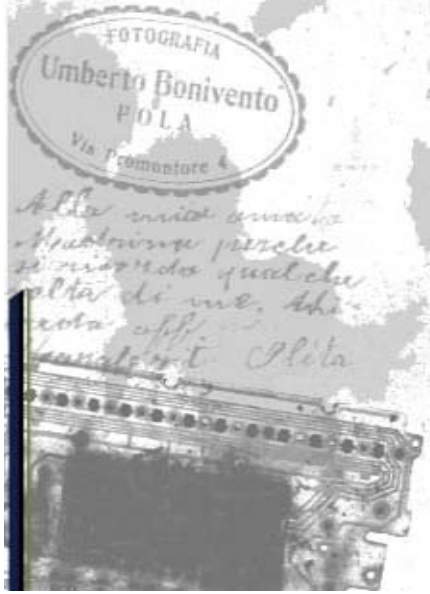
- Carrier system public access
- The transmission of the enterprise VoIP system through Internet
- Virtual operating system is based of Internet
- PSTN faces threats

The sketch map of security threats



Security threats

- Denial of Service
- unauthorize access
- Trace to telephone
- Attack to media (disturb and insert)
- eavesdrop
- Session hijack
- intrusion control
- The telephone fee swindling
- Telephone leaflet
- Other threats



Security threat

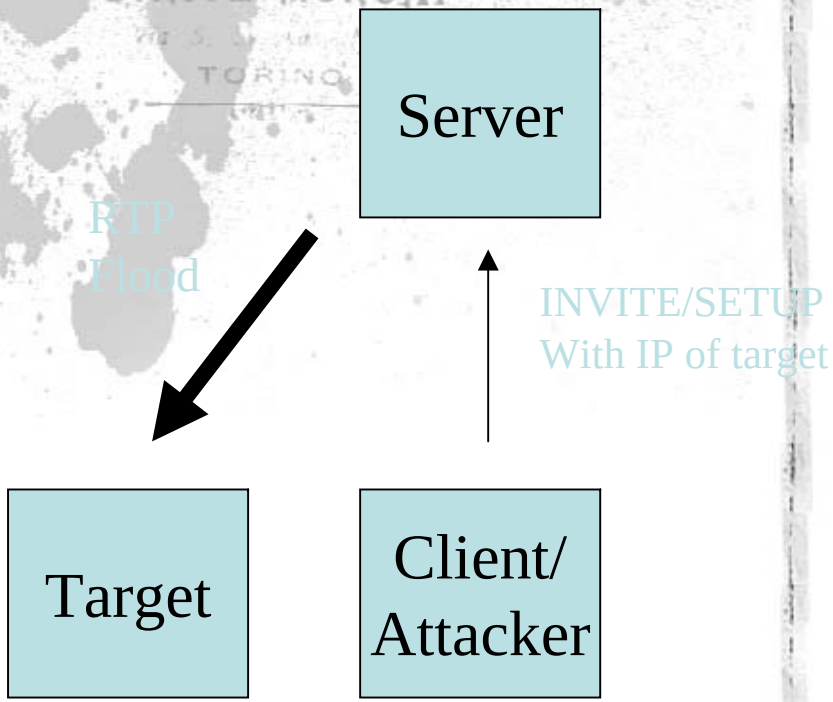
DoS

- consuming system resources
- A lot of service requested DoS attack
- Make use of system holes DoS attack

  Especially RTP DoS attack and H.323 protocol realize holes

The DoS Problem

- Attacker sends SIP INVITE or RTSP SETUP to server
- IP for RTP is target
  - Source IP in RTSP
  - SDP in SIP
- Server sends media to target



Security threats

- The realize holes of H.323 protocol

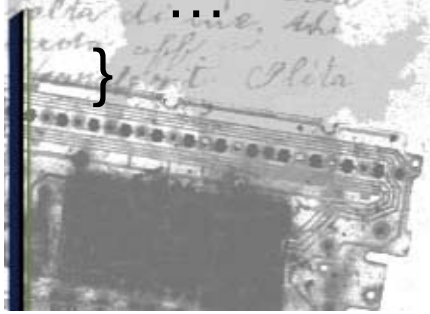
  Principle: Network protocol described in ASN.1 is judged as the second of ten security hidden trouble ; SNMP and H.323 protocol is among them;

  There are already a lot of VoIP manufacturers who have announced some relevant hole-information .Microsoft have announced 3 relative holes from the early of this year until now.（MS04-001，MS04-07，MS04-10）

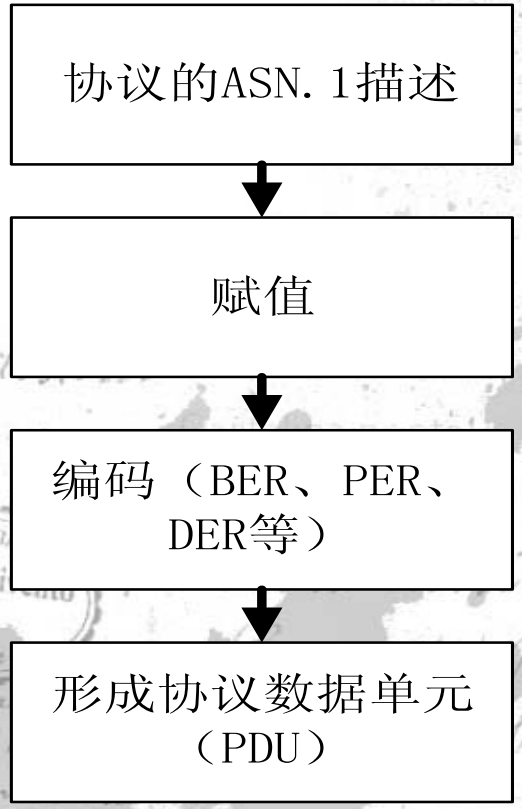
  Risk: system may be intruded.

An example of ASN.1

```
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,
    ...
}
```



The procedure of the ASN.1 application



- The smart protocol notation language
- Protocol defined by ASN.1 may be much complicated
- Buffer Overflow holes show up during the realization of coding mode frequently
- Network protocol holes make remote attacks possible

Security threats

- media attack threat

  An attack threats based on eavesdrop and network packet disguising technology

  Include media eavesdrop,interrupt , audio insert and so on .

Security threats

- The call following and hijack attack

  Through sniffing talk signaling data packet and protocol analysis ,pick up the call-status information of a phone

  Attacker may hijack or teardown this session

Security Threat

- The access technology without authentication and cheat in call fee

  The breakthroughs of Some authentication algorithms

  Replay attack

  Man-in-the-middle attack

Security Threat

- Telephone flexlet
  - telephone flexlet just to alert
  - telephone flexlet in order to issue information

In other words, they are harassing calls. It is an active attack and meanwhile it will result in serious social issues if matching with anounymous call and other masquerading technologies.

Security Threat

- other threats
  - Threats in data network
  - Special threats to VoIP network deploy

For example threats to AAA server or Proxy Server to solve NAT traversal and so on

VoIP Security Mechanisms

- Security Mechanisms
  - Security mechanisms
  - Security Protocol
    - SEG, TLS
    - MIKEY
    - IUS, Diameter
  - Built-in security
    - existing security
    - stream encryption
    - Secure RTP

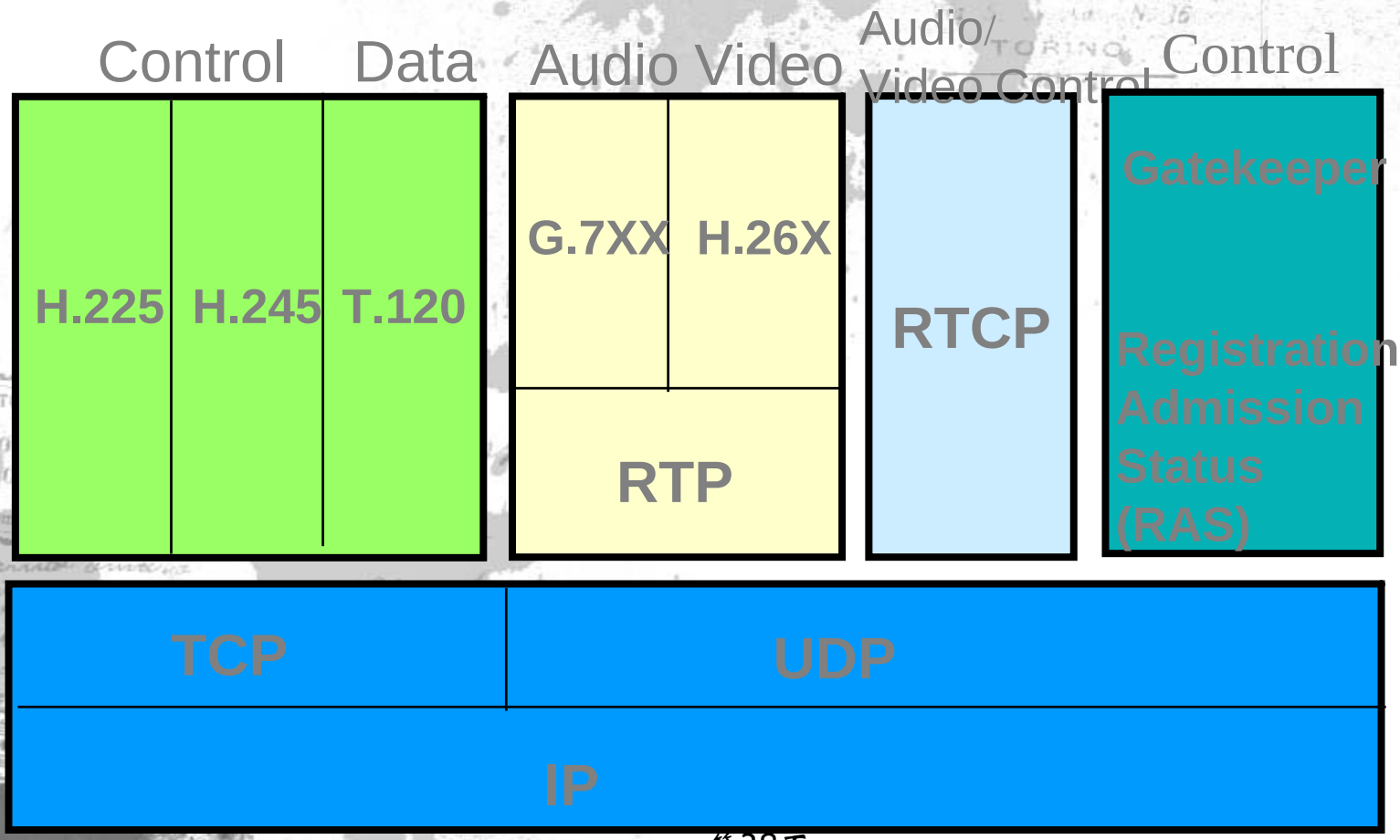
Security in VoIP Systems

- **Security mechanisms**
  - **Key management schemes**
  - **User authentication for billing/accounting**
  - **Message encryption and authentication**

- **Signaling security**
  - **H.323, SIP**
- **Media security**
  - **RTP**

The VoIP security mechanisms （H.323）

- H.323 Protocol Stack

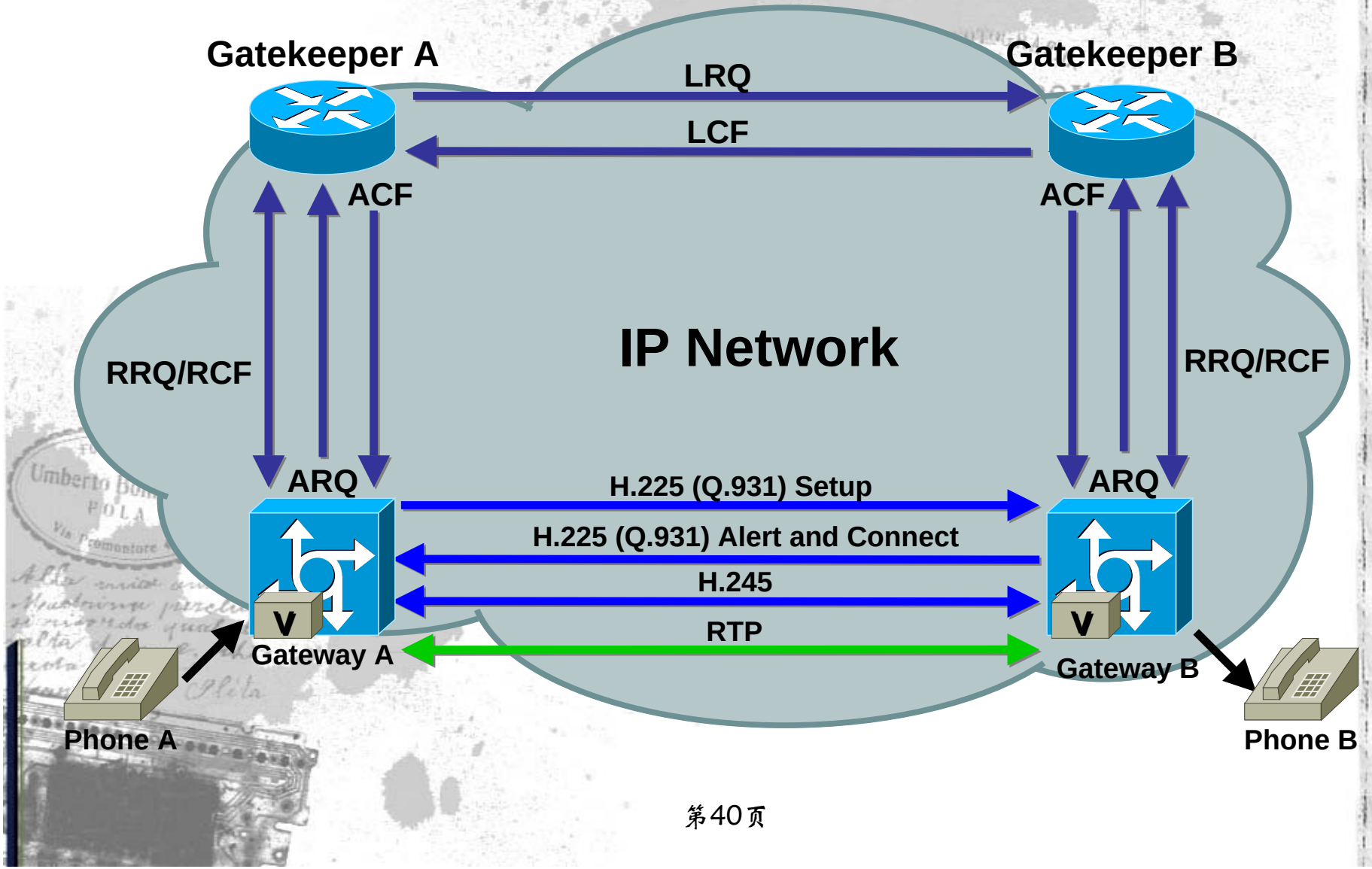


The VoIP security mechanisms （H.323）

Basic H.323 call procedure

1. Gatekeeper discovery
2. Gateway register
3. Address resolution
4. Call establishment
5. Conversation course
6. Tearing down

The basic H.323 call scope



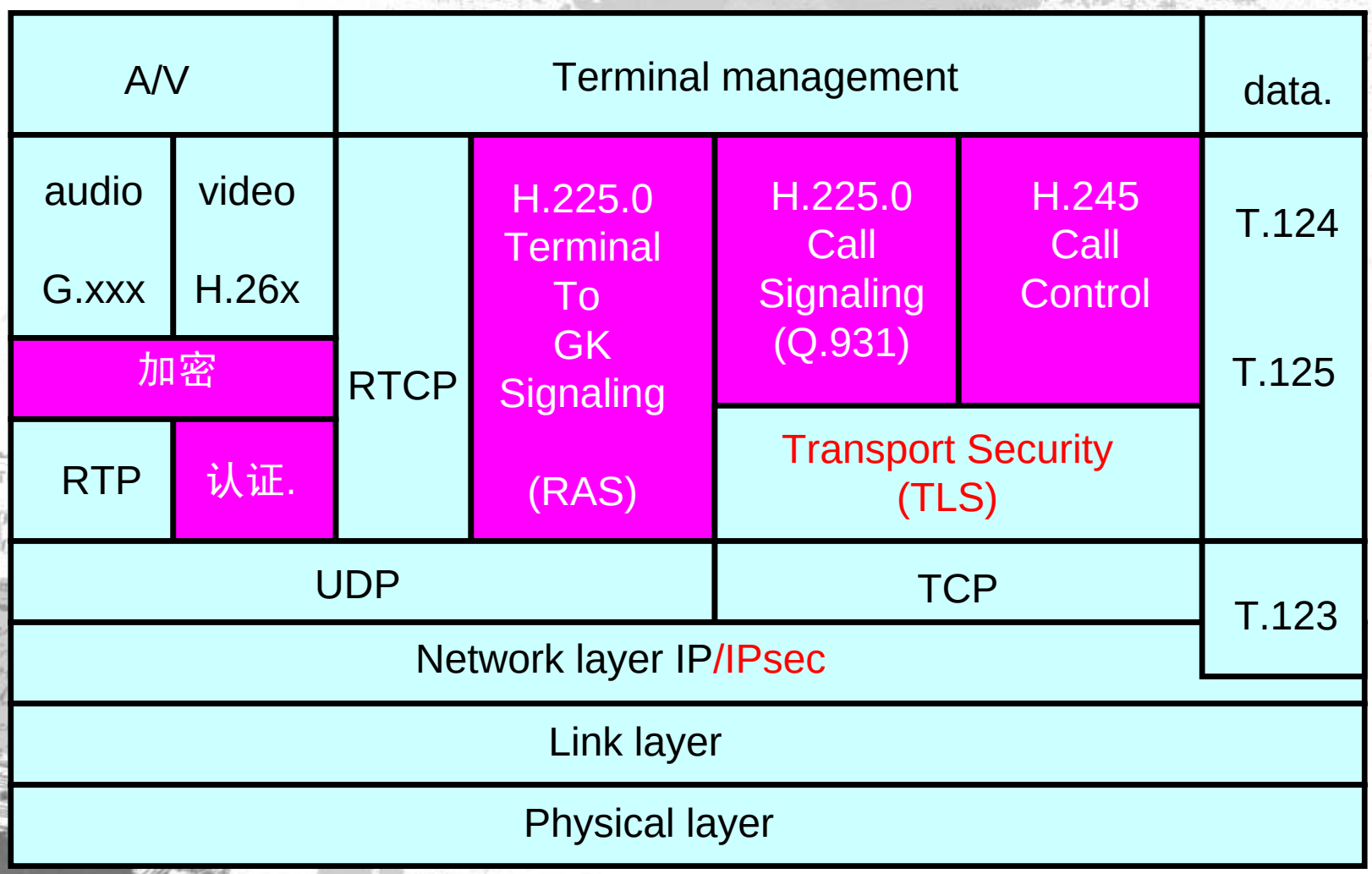
The VoIP security mechanisms （H.323）

- The machanisms in H.323 security
  - ICV；
  - Diffie-Hellman；
  - password with symmetric encryption；
  - password with hashing ；
  - Certificate with signature ；
  - something else ；

H.235 - Security for H.323

- **"Security and encryption for H.323 and other H.245-based multimedia terminals"**
  - Provides cryptographic protection of control protocols (RAS, H.225.0 & H.245) and multimedia data stream
  - Negotiation of security services, algorithms/keys and capabilities
  - Password/certificate-based user authentication and access control
  - Integrated key management
  - Anti-spamming against denial of service attacks
  - Relies on well-established security standards from ISO & IETF
  - Provides baseline and signature security profiles

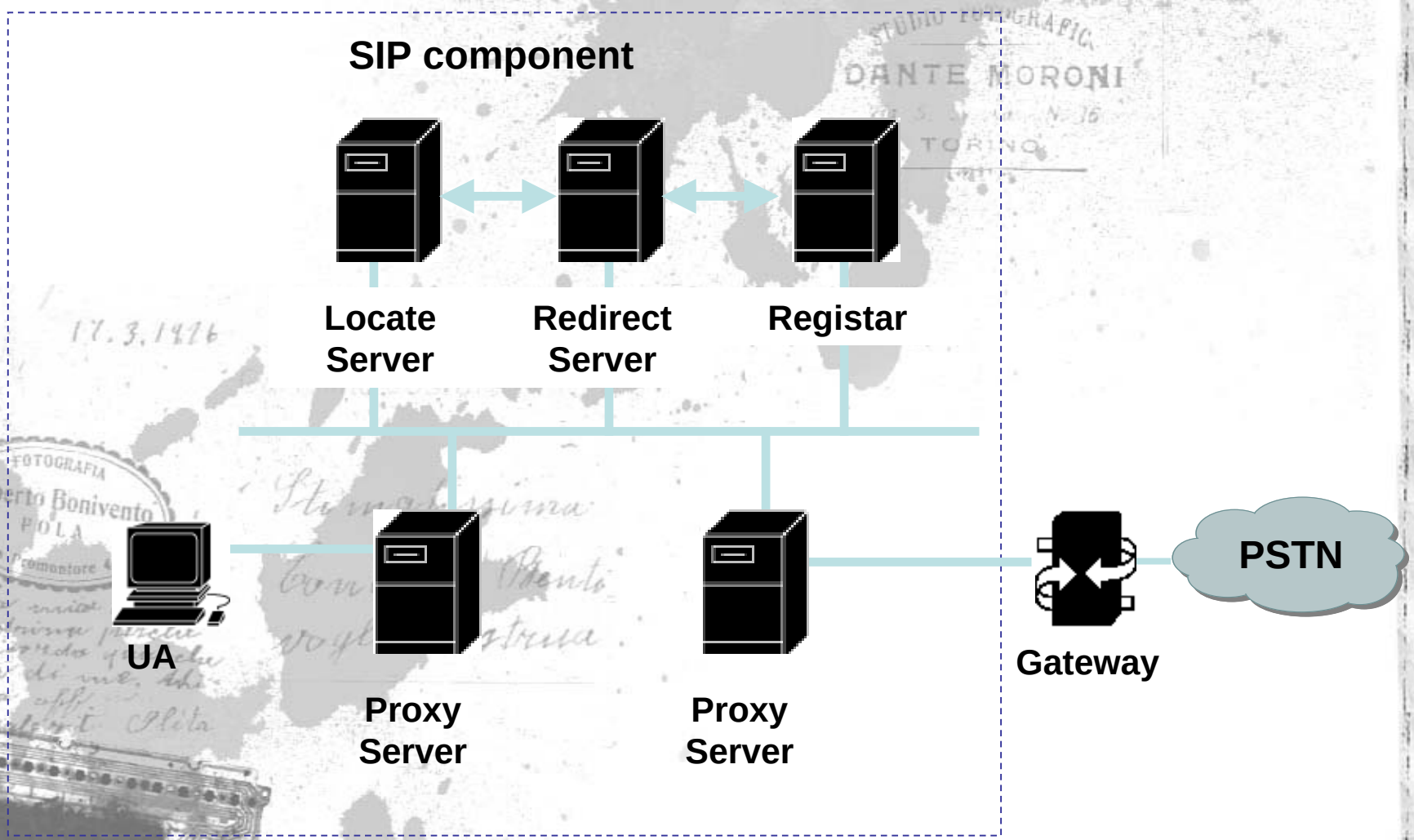
Scope of H.235



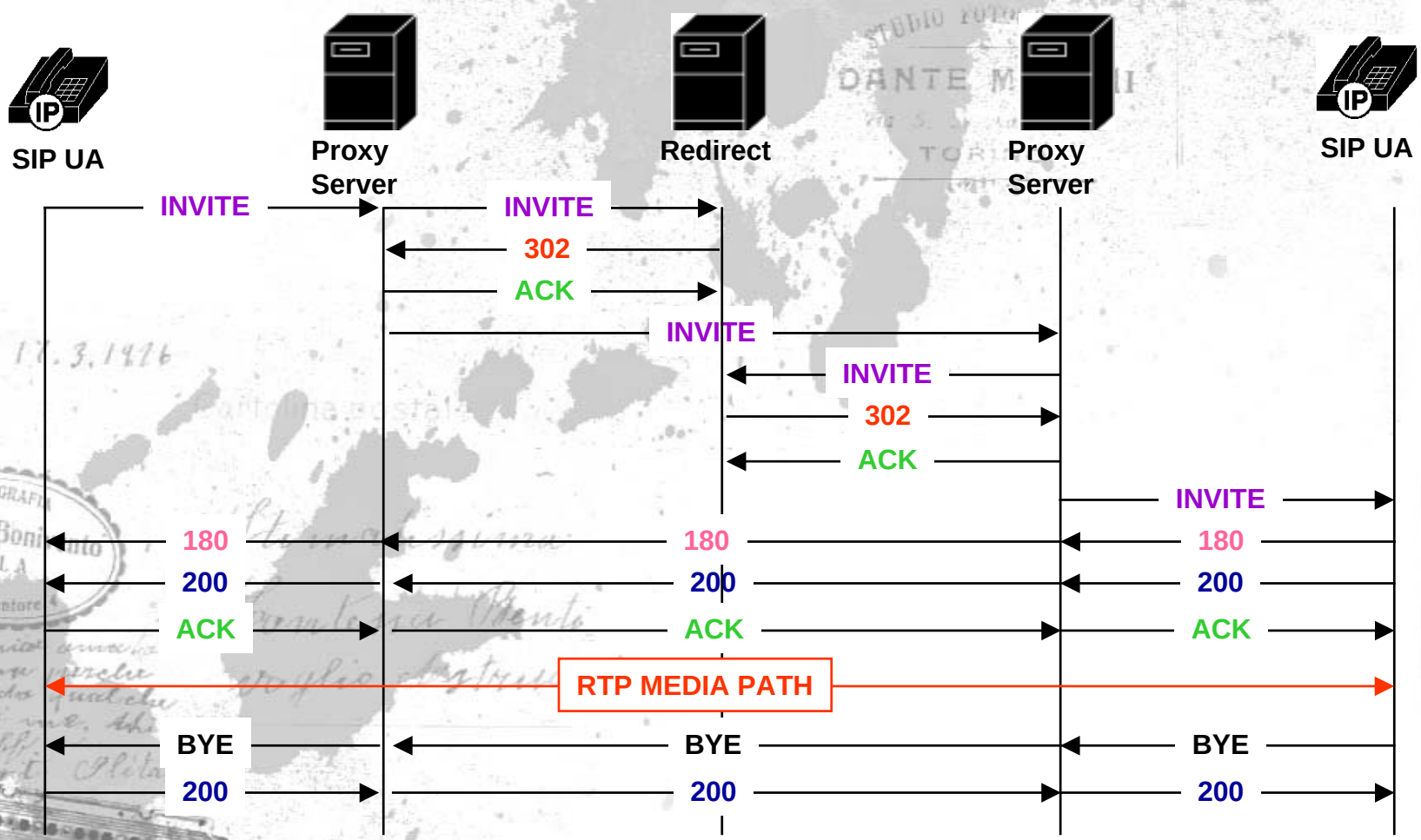
The VoIP security mechanisms （SIP）

- SIP protocol-based network
  - simple signaling
  - simple format
  - Group's network is flexible
  - 3G support

SIP distribution system



A intact SIP call



The VoIP security mechanisms （SIP）

- The security mechanisms in SIP

  Basic authentication (deprecated in new RFC)

  Digest authentication (the similar with HTTP Digest)

  S/MIME mechanism

  PGP mechanism (deprecated in new RFC)

  SIPS Url Scheme

SIP Security – HTTP Digest Auth.

- [illegible] proxy challenge/response [illegible]
- [illegible]nt authentication and re[illegible]
- [illegible]nd confidentiality
- [illegible] public servi[illegible]
- [illegible]tication

digestedPW = H(username:realm:password)

Digest = H(digestedPW:nonce:H(method:URI))

SIP Security – S/MIME

```
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

The VoIP security mechanisms （RTP）

- Current RTP/RTCP
  - Built-in security mechanism using PEM-style DES-CBC encryption
  - Packet authentication not defined, expected to be provided by lower-layer protocols

- Problems
  - TLS not applicable; possibly use IPSEC
  - Problems with IPSEC: multicast traffic & header compression
  - RTP/UDP/IP header : 12 + 8 + 20 = 40 bytes overhead
  - Compressed RTP can reduce this to 2 or 4 bytes

The VoIP security mechanisms （RTP）

- Secure RTP (SRTP): Internet Draft
  - A profile of RTP with built-in privacy/authentication mechanisms considering 3G networks
  - Requirements:
    - efficiency
    - no error propagation
    - no message expansion
    - random access property (fast-forward/rewind)
    - selective payload encryption
    - header compression capable, unequal error protection
  - Encryption: Counter mode AES, AES in f8-mode
  - Authentication: HMAC-SHA1

The VoIP security mechanisms （RTP）

- Session key management
  - Send session key in SDP k line
    - Must encrypt and authenticate SIP messages
    - Relies on PGP/SMIME for encryption and authentication
    - Requirements:
  - Diffie Helman key exchange in SDP
    - Must encrypt and authenticate SIP messages
    - MUST authenticate SIP messages
    - Relies on PGP/SMIME for authentication only
  - Use IKE or Kerberos

The Security defence proposing

- close unused service
- add access identifier authentication
- data packet authentication
- media encryption
- media-source authentication
- Study coexisting security system of data network and VoIP
- Other security strategies

Thanks!!!

E-mail:hyperfeng@163.com

QQ : 106810831

电话： 13691007935