

VOS2000 加密规范

(V1.1)

南京昆石网络技术有限公司

2007 年 10 月

前言

VOS2000 加密规范是由南京昆石网络技术有限公司提出的一套加密协议，其目的是针对终端、对接平台以及中继落地与 VOS2000 软交换之间的通信进行加密，防止对软交换平台的封杀、干扰，保证通信的安全性与完整性。

本文档是 VOS2000 加密规范的 1.1 版本，在 1.0 版本的基础上增加了在 SIP 协议中使用本加密规范的说明。

本规范版权及解释权属于南京昆石网络技术有限公司，任何第三方厂商可以免费使用。

1 加密规范说明

1.1 对除 RTP 以外的协议过程，如 H323 中的 RAS、Q931、H245 和 SIP 中的数据包采用以下加密规范：

加密的数据包分为首部与数据两部分。

首部	数据
----	----

首部长度为 8 个字节，格式如下：

0	1	2	3	4	5	6	7
协议标识	保留		算法		数据长度		

- **协议标识** (2 个字节)：加密数据包的标识，第一个字节值固定为 0x4b，第二个字节值固定为 0x53
- **保留** (2 个字节)：保留字段，值为 0
- **算法** (2 个字节)：数据部分采用的加密算法，目前只支持 0x01 (RC4)
- **数据长度** (2 个字节)：加密数据包中数据部分的长度，长度不包括首部中的 8 个字节

数据部分的格式根据首部中算法字段的值而定，目前只支持 RC4 算法。

算法字段的值为 0x01 时，表示采用 RC4 加密算法，数据格式如下：

标识类型	标识长度	标识数据...
加密数据...		

- **标识类型** (1 个字节)：标识数据部分包含的数据类型，其值的对应内容如下：
 - 0 呼叫方为终端，标识数据中为话机号码（终端包括话机和SIP语音网关）
 - 1 呼叫方为网关，标识数据中为网关标识（网关包括对接的软交换平台、中继网关和以前缀方式注册的语音网关）
- **标识长度** (1 个字节)：标识数据字段的长度
- **标识数据** (可选)：由标识类型标记的数据，若为终端，该字段填写对应的话机号码 (E164 号码)；若为网关，该字段填写网关标识 (H323ID)；长度由标识长度表示，如标识长度为 0，该字段不存在。
- **加密数据**：经 RC4 算法加密后的数据 (RAS、Q931、H245、SIP)，若为 H323 终端，加密密钥为终端的 H323ID；若为 SIP 终端，加密密钥为话机的密码；若为网关，加密密钥为网关上设置的加密密钥。

* 为配合加密，需要在网关设置中添加用作加密密钥的密码。

* 对于 H323 中的 Q931 和 H245，加密数据中不包含原数据包中的 TPKT 部分。

1.2 针对 RTP 语音包，采用如下加密：

算法	长度	RTP数据
填充数据		

- **算法**（1 个字节）：标识所使用的加密算法，目前只支持 0x00
- **长度**（1 个字节）：将原 RTP 数据包的第一个字节 0x80 替换成原 RTP 包的实际长度
- **RTP 数据**：对原 RTP 包除首字节以外的部分，使用加密密钥进行异或运算产生的数据填写在该字段
- **填充数据**：在数据包的尾部添加随机长度的填充数据

* RTP 加密密钥的选择：对于 H323 协议，使用当前通话的 CallReferenceValue 的低字节；对于 SIP 协议，使用当前通话的 Call-ID 的首字节。

2 使用说明

2.1 H323 终端注册，号码为 9000，H323id 为 reg9000

构造一个 UDP 数据包，按照上述协议说明填写首部信息，

0x4b	0x53	0x00	0x01	数据长度
数据				

数据部分，标识类型为 0；标识长度为话机号码的长度，此处为 4；标识数据中为话机的号码，此处为 '9000'；对 RRQ 消息使用 H323id (reg9000) 为密钥，进行加密，将加密后的数据放入报文的加密数据部分。

0	1	2	3	4	5	6	7
0	4	'9'	'0'	'0'	'0'	加密数据...	
加密数据（加密的RRQ）							

VOS2000 接收到加密的注册包，将使用话机 9000 的 h323id 为密钥 (reg9000) 对加密数据部分进行解密，并对注册信息校验，如果注册成功，则返回加密的 RCF，如下

0	1	2	3	4	5	6	7
0	4	'9'	'0'	'0'	'0'	加密数据...	
加密数据（加密的RCF）							

2.2 H323 网关发起呼叫，对接网关 H323ID 为 duijie，网关的密钥为 passwd

首部省略。

数据部分，标识类型为 1；标识长度为网关的加密标识长度，此处为 6；标识数据中为网关的 H323ID，此处为 'duijie'；对 Setup 消息使用密钥 (passwd) 进行加密，将加密后的数据放入报文的加密数据部分。

0	1	2	3	4	5	6	7
1	6	'd'	'u'	'i'	'j'	'i'	'e'
加密数据（加密的Setup）							

VOS2000 接收到加密的 Setup 包，将使用网关的密钥 (passwd) 对加密数据部分进行解密。

2.3 SIP 终端发起呼叫，号码为 123456，话机密码为 pass

首部省略。

数据部分，标识类型为 0；标识长度为话机的号码长度，此处为 6；标识数据中为话机号码，此处为 ‘123456’；对 INVITE 消息使用 (passwd) 为密钥，进行加密，将加密后的数据放入报文的加密数据部分。

0	1	2	3	4	5	6	7
0	6	‘1’	‘2’	‘3’	‘4’	‘5’	‘6’
加密数据（加密的INVITE）							

VOS2000 接收到加密的 INVITE 包，将使用话机的密码 (passwd) 为密钥对加密数据部分进行解密。