

ICS 33.040.40

M 32

YD

中华人民共和国通信行业标准

YD/T 2040-2009

基于软交换的媒体网关安全技术要求

Security requirements of soft switch-based media-gateway

2009-12-11 发布

2010-01-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 媒体网关在软交换网络中的安全模型	2
6 信令面的安全	3
6.1 信令流通信安全要求	3
6.2 信令流通信安全机制	3
6.3 信令流通信 SA 建立	3
6.4 信令流通信安全协议及算法	4
6.5 信令流通信安全算法	4
6.6 信令流的 NAT 穿越（可选）	4
7 媒体面的安全	4
7.1 媒体流通信安全要求	4
7.2 媒体流通信安全机制	4
7.3 媒体流通信 SA 建立	5
7.4 媒体流通信安全协议	5
7.5 媒体流通信安全算法	5
8 网络管理安全要求	5
8.1 鉴别和认证	5
8.2 系统访问	5
9 常见网络攻击抵抗能力	7
10 可靠性要求	8
10.1 设备级故障管理	8
10.2 冗余备份要求	8
10.3 信令切换要求	9
附录 A（规范性附录）接入认证流程	10

前 言

本标准是“软交换网络安全”系列标准之一，该系列标准的结构和名称预计如下：

- 1) 软交换网络安全
- 2) 软交换设备安全技术要求和测试方法
- 3) 基于软交换的媒体网关安全技术要求
- 4) 基于软交换的媒体网关安全测试方法
- 5) 软交换业务接入控制设备安全技术要求和测试方法
- 6) 基于软交换的信令网关设备安全技术要求和测试方法
- 7) 基于软交换的媒体服务器设备安全技术要求和测试方法
- 8) 基于软交换的应用服务器设备安全技术要求和测试方法
- 9) IP 智能终端设备安全技术要求和测试方法
- 10) 软交换网络管理安全

本标准的附录 A 为规范性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院。

本标准主要起草人：段世惠、蒋晓琳。

基于软交换的媒体网关安全技术要求

1 范围

本标准给出了基于软交换的媒体网关安全模型，规定了信令层面与媒体层面的安全性要求，对媒体网关在网络管理安全、抵御常见网络攻击、可靠性等方面提出了安全要求。

本标准适用于基于软交换的媒体网关。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准。然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

	软交换网络安全
IETF RFC 2401	网络层安全架构
IETF RFC 3711	安全媒体流传输协议
IETF RFC 3948	IPSec ESP报文的UDP封装

3 术语和定义

下列术语和定义适用于本标准。

3.1

接入网关 access gateway

媒体网关的一种，用于实现用户侧语音、传真信号到分组网络媒体信息的转换，并将各种模拟终端用户接入到分组网络中。

3.2

认证中心 authentication center

提供对用户、终端和网络设备的认证、密钥分发和管理功能，在本标准中定义的是一个具有上述功能的逻辑功能实体。

3.3

媒体网关 media gateway

媒体网关将一种网络中的媒体转换成另一种网络所要求的媒体格式。例如：媒体网关能够在电路交换网的承载通道和分组网的媒体流之间进行转换，可以处理音频、视频或者 T.120，也可以具备处理这三者的任意组合的能力，能够进行全双工的媒体翻译，可以演示视频/音频消息，实现其他 IVR 功能，也可以进行媒体会议等。

3.4

媒体面 media plane

在本标准中特指媒体网关设备中负责处理媒体变换、转发的功能模块。

3.5

安全联盟 security association

通信双方建立的有关安全密钥、算法及通信双方地址标识信息的一个约定。

3.6

信令面 signalling plane

在本标准中特指媒体网关设备与软交换设备中负责处理信令解析、转发的功能模块。

3.7

软交换 soft switch

软交换网络的核心设备之一，它主要完成呼叫控制、媒体网关接入控制、资源分配、协议处理、路由、认证、计费等主要功能，并可以向用户提供基本话音业务、移动业务、多媒体业务以及多样化的第三方业务。

3.8

中继网关 trunk gateway

媒体网关的一种，跨接在 PSTN 网络和软交换网络之间，负责 TDM 中继电路和分组网络媒体信息之间的相互转换，此外中继网关也可以接入 PRI。

4 缩略语

下列缩略语适用于本标准。

ACL	Access Control List	访问控制列表
AG	Access Gateway	接入媒体网关
AH	Authentication Header	报文认证头协议
ESP	Encapsulation Security Payload	安全载荷封装协议
IAD	Integrated Access Device	综合接入设备
IKE	Internet Key Exchange	互联网密钥交换协议
IPSec	IP Security	网络层安全协议
OAM	Operation, Administration, Maintenance	操作管理维护
PSTN	Public Switch Telephone Network	公众电话交换网
QoS	Quality of Service	服务质量
TLS	Transport Layer Security	传输层安全协议
SA	Security Association	安全联盟
SP	Signaling Proxy	信令代理
SRTP	Security Real-time Transport Protocol	安全媒体流协议
SS	Soft Switch	软交换

5 媒体网关在软交换网络中的安全模型

从媒体网关来看，安全分为 2 个层面：信令面和媒体面。信令面主要负责媒体网关与软交换及认证中心之间的信令安全；媒体面主要负责媒体网关之间媒体流的安全。其安全模型如图 1 所示。

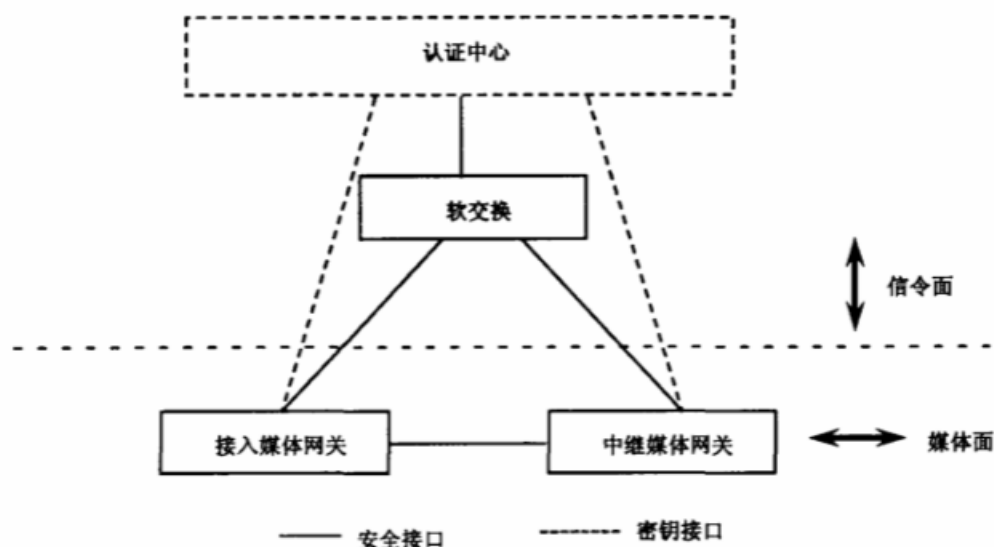


图1 媒体网关的安全模型

媒体网关的安全模型（如图1所示）的说明如下。

虚线：表示媒体网关与认证中心之间存在密钥交换；

实线：网络域中媒体网关与软交换、媒体网关与媒体网关之间的通信，提供媒体网关与软交换、媒体网关与媒体网关之间的通信安全，包括完整性保护、防重放、源认证以及可选的机密性保护；

除了信令层面和媒体层面的安全之外，媒体网关还应考虑自身的安全性，包括可靠性、抵抗常见网络攻击、安全管理等。

注1：媒体流是否需要保护可以根据用户或业务的需求以及运营商的安全策略来决定是否进行，同时具体保护方案上需要考虑电信监管和对媒体流服务质量的影响。

注2：在实际实现中，信令层面和媒体层面的安全性可以通过外部防火墙等安全设备来保障，如可以通过防火墙来建立IPSec VPN，在本标准中不考虑这种情况。

注3：图1仅仅针对媒体网关，对于软交换的密钥分发过程不予考虑。

6 信令面的安全

6.1 信令流通信安全要求

信令流通信安全要求应保证软交换网络域内媒体网关与软交换之间的信令报文的完整性、防重放、源认证以及可选的机密性保护。

6.2 信令流通信安全机制

要求媒体网关应支持与软交换设备之间的IPSec传输安全模式，通过IP层的安全保证媒体网关与软交换设备之间的通信是安全的，安全协议根据安全服务要求（完整性或机密性等）采用IPSec ESP或AH协议。

在可能的情况下，媒体网关与软交换之间的信令流也可以通过组网的方式在一定程度上保障安全性。

媒体网关必须以安全的方式接入到软交换，软交换应提供必要的接入认证机制，媒体网关与软交换之间的接入认证流程见附录A。

6.3 信令流通信SA建立

媒体网关与软交换设备之间的通信安全联盟（SA）建立遵循IETF RFC2401，其中给出了2种确立安全联盟（SA）的方法：

- 支持手工配置方式建立安全联盟；
- 支持通过IKE动态协商建立安全联盟对于软交换网络域安全联盟的建立。

要求手工配置方式为必选，IKE方式为可选。

媒体网关与软交换之间的密钥宜由软交换生成，并由软交换直接向媒体网关下发。

6.4 信令流通信安全协议及算法

根据不同的应用安全需求（完整性或机密性等），采用IPSec ESP协议。

媒体网关与软交换设备的完整性保护算法为HMAC-SHA-1-96算法（可选）。

媒体网关与软交换设备之间的加密算法待定。

媒体网关和认证中心之间的认证算法为HMAC-SHA-1-96算法（可选）。

6.5 信令流通信安全算法

完整性保护算法为HMAC-SHA-1-96算法（可选。）

加密算法待定。

6.6 信令流的 NAT 穿越（可选）

由于软交换经常位于NAT设备之后，因此需要考虑媒体网关与软交换设备之间的信令流，考虑IPSec协议如何穿越NAT。采用IPSec作为信令流安全保护协议时，当软交换网络中存在NAT设备时，需采用IPSec ESP协议，采用IPSec ESP报文UDP封装方式实现IPSec ESP穿越NAT（见IETF RFC 3948）。

如果在软交换网络中没有布置NAT设备，则无需考虑本节内容。

IPSec ESP报文将采用UDP封装方式完成，IPSec ESP报文采用UDP封装的指示及封装端口号后的交互流程见《软交换网络安全》附录D。

由于IPSec穿越NAT的复杂性，可考虑在密钥协商的注册认证过程中在支持安全算法协商的同时，支持安全协议的协商，如IPSec ESP作为保证互通的缺省安全协议，同时可以协商支持其他如TLS（基于TCP连接，无NAT问题），或其他自定义的应用层安全封装（不受NAT影响），在软交换网络安全中可以定义一种基于应用层（非网络层和传输层）的封装协议，确保网络的互通，传输层安全（TLS）或应用层安全协议可选，媒体网关和软交换设备之间可以通过协商来决定。

7 媒体面的安全

7.1 媒体流通信安全要求

媒体流通信安全要求保证通信双方媒体流的安全，包括媒体流的完整性、防重放、源认证以及机密性保护，同时这些安全服务的提供需要考虑多方面因素，包括用户或业务的安全需求以及运营商的安全策略等来决定是否实施，同时需要考虑电信网络监管和对媒体流服务质量的影响。

媒体流的安全性也可以选择通过外置防火墙等安全设备来保障。

对于综合接入媒体网关（AG）与综合接入设备（IAD），要求具备主叫号码显示功能。

7.2 媒体流通信安全机制

媒体流通信安全包括如下几个步骤。

主叫和被叫端设备安全联盟的建立：包括媒体流通信安全的密钥的分发，媒体流通信安全算法的协商（可选），当两端设备不支持媒体流保护安全算法协商时，需要支持本标准定义的缺省安全算法。

主叫和被叫端之间的媒体流安全通信：通过某种保护和加密格式对媒体流报文进行保护，即定义媒体流的安全协议。

7.3 媒体流通信 SA 建立

媒体网关设备之间的通信安全联盟(SA)建立遵循IETF RFC2401, 其中给出了2种确立安全联盟(SA)的方法:

- 支持手工配置方式建立安全联盟;
- 支持通过IKE动态协商建立安全联盟对于软交换网络域安全联盟的建立。

要求手工配置方式为必选, IKE方式为可选。

7.4 媒体流通信安全协议

媒体流通信安全协议采用IETF RFC 3711, 保证媒体面的互通。SRTP的报文格式如图2所示。

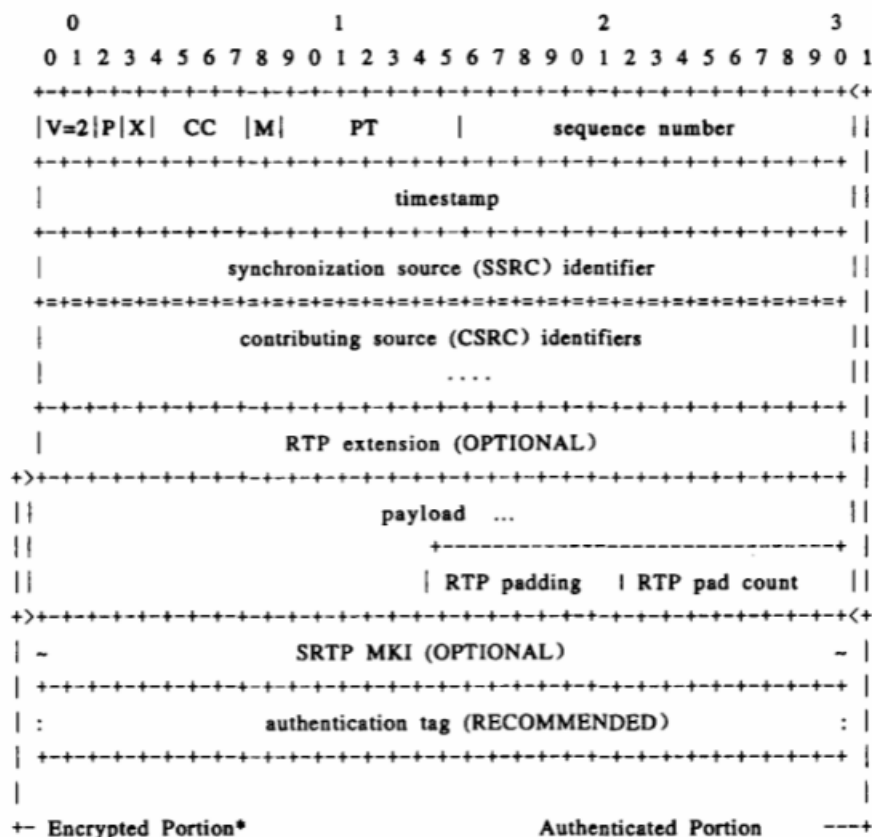


图2 SRTP的报文格式

图2中的报文格式中给出了对RTP报文加密和进行完整性校验时, 报文加密和完整性保护的

7.5 媒体流通信安全算法

完整性保护算法为HMAC-SHA-1-96算法(可选)。

加密算法待定。

8 网络管理安全要求

8.1 鉴别和认证

对设备的管理用户都需要鉴别和认证, 鉴别和认证是系统访问的基础, 对有关SNMP管理、Web管理、远程登录管理中用户认证的要求见8.2节。与管理相关的安全数据应得到妥善的保护。

用户进行网络管理时所使用的登录口令的长度应不少于8个字符, 并且应由数字、字符或特殊符号组成, 媒体网关应提供检查机制, 保证每个口令至少是由前述的三类符号中的两类组成。

8.2 系统访问

系统访问可以考虑采取带内/带外管理方式。由于带内管理面临潜在的安全问题, 媒体网关可通过如

独立的管理端口、VPN虚接口等方式支持专用的管理网络，将管理通信流和其他通信流量隔离。媒体网关可提供关闭带内接口的能力，以实现只通过专用管理网络管理设备。

系统访问可以通过SNMP访问、Telnet访问、串口访问、SSH访问、Web访问等方式实现。

(1) SNMP访问

SNMP是一种应用非常广泛的网络管理协议，主要用于设备的监控和配置的更改等，目前使用的SNMP协议有3个版本，分别是SNMPv1、SNMPv2c和SNMPv3。

媒体网关可支持SNMPv1、v2c，但是应提供禁用功能，并且缺省应该是禁用的。提供SNMPv1和SNMPv2c应可以和访问控制列表相结合，控制非法网管接入设备，同时不使用public/private作为缺省团体名，缺省只读团体名和读写团体名称不能够相同，并且在适当的时机提示管理员修改团体名。

媒体网关应支持安全性较好的SNMPv3作为网管协议，支持USM等安全机制。

此外，建议媒体网关实现对网管站的访问控制，限定用户通过哪些IP地址使用SNMP对设备进行访问。

(2) Telnet访问

Telnet协议用于通过网络对设备进行远程登录。在媒体网关中，如果为用户提供Telnet服务，则建议满足下列约定：

- 用户应提供用户名/口令才能进行后续的操作，用户地址和操作应记入日志；
- Telnet访问时应提供对用户账号的分级管理机制，提供对Telnet用户权限的控制功能；
- 应限制同时访问的用户数目；
- 在设定的时间内不进行交互，用户应自动被注销，提供终端超时锁定功能；
- 可限定用户通过哪些IP地址使用Telnet服务对设备进行访问；
- 能够针对Telnet的密码试探攻击进行防范，可对同一个IP地址使用延时响应机制，也可利用限定来自同一个IP地址的登录尝试次数；
- 必要时可关闭Telnet服务。

(3) 串口访问

媒体网关如果支持串口访问功能，在终端与主机进行交互的过程中应提供与Telnet访问方式相同的安全保护能力。

(4) SSH访问（可选）

SSH是在不安全的网络上为远程登录会话和其他网络服务提供安全性的一种协议，对SSH服务的要求如下：

- 应支持SSHv1和SSHv2两种版本；
- 用户应通过身份认证才能进行后续的操作，用户地址和操作记入日志，媒体网关应支持口令认证，宜支持公钥认证，可实现基于主机认证；
- SSH服务器宜采用认证超时机制，在超时范围内没有通过认证应断开连接，建议限制客户端在一个会话上认证尝试的次数；
- SSHv2应支持用于会话的加密密钥和认证密钥的动态管理，支持Diffie-Hellman组14的密钥交换，在密钥交换过程中协商密钥交换算法、对称加密算法和认证算法等，并对服务器端进行主机认证；
- 应支持HMAC-SHA1认证算法，建议支持HMAC-SHA1-96认证算法，可实现HMAC-MD5、HMAC-MD5-96等认证算法；

— 应支持3DES-CBC对称加密算法，可实现Blowfish-CBC、IDEA-CBC、CAST128-CBC、AES256-CBC、AES128-CBC等对称加密算法；

- 对于非对称加密算法，应支持SSH-DSS，建议实现SSH-RSA；
- 可限定用户通过哪些IP地址使用SSH服务对设备进行访问；
- 应支持必要时关闭SSH服务。

(5) Web管理

Web管理基于HTTP协议，媒体网关宜支持Web管理，建议满足下列约定：

- 用户应提供用户名/口令才能进行后续的操作，用户地址和操作应记入日志；
- 可限定用户通过哪些IP地址使用HTTP对设备进行访问；
- 必要时可关闭HTTP服务；
- 应支持SSL/TLS安全协议，实现对管理用户数据的完整性保护。

(6) 软件升级

媒体网关可以使用FTP/TFTP协议实现设备的软件升级，软件升级包括软件版本、设备配置等，有本地和远程两种途径。软件升级通过建立FTP/TFTP服务器和客户端的连接来实现，FTP/TFTP协议应支持口令认证功能。

对于远程软件升级，建议支持SSHv2，实现文件的安全传送。

9 常见网络攻击抵抗能力

针对已知的各种攻击，媒体网关设备应能够进行处理，并且不影响媒体网关正常的数据发送。当媒体网关检测到攻击发生，应该生成告警。下面几种常见的攻击，媒体网关应也能够处理。

(1) 抗大流量攻击能力

媒体网关设备在网络中运行的过程中，经常会遇到某些大流量攻击，这些攻击主要包括2种形式。一种大流量是属于路过流量，远远超过了正常业务流量，占用媒体网关大量的资源。另外一种大流量更具有危害性，这些流量的目的地址就是媒体网关设备本身，这样通常会导致媒体网关设备无法处理这样庞大的流量，导致整个媒体网关设备陷于瘫痪或者崩溃，进一步地导致用户业务受到影响。

对于第一种情况，媒体网关设备应能够处理，媒体网关的端口宜线速转发流量，不能进行线速转发时，可按一定的比率丢弃报文，但是应确保媒体网关的信令报文和管理报文（如TELNET和SNMP等）的正常发送和接收。

对于第二种情况，媒体网关应能够处理这些异常攻击流量，采取丢弃报文策略，同时生成告警日志，媒体网关在这种情况下应保证能够继续为用户提供服务，不能出现崩溃现象。同时媒体网关还应能够完成正常的信令协议和管理报文的正常发送和接收处理。

(2) 抗畸形包处理

媒体网关应该具有完整的协议检测功能，防止非法报文的攻击，媒体网关设备应能够具有如下良好的畸形报文处理能力：

- 媒体网关应能够检测超短/长报文并采取丢弃策略，同时对这种报文提供统计数据；
- 媒体网关设备应能够检测网络层报文错误并采取丢弃策略，同时必须提供错误报文统计数据；
- 媒体网关设备不能由于错误报文/畸形报文而崩溃；
- 媒体网关设备本身不应发出错误报文/畸形报文。

(3) 定向广播报文攻击防范

媒体网关应该具有防DoS攻击能力，应该至少支持以下几种防DoS攻击的机制：

- TCP SYN Flood攻击；
- ping超大包攻击；
- Smurf攻击；
- ICMP攻击；
- IP分片攻击；
- 分布式DoS攻击。

(4) IP地址欺骗防范

媒体网关应该具有一定的IP地址欺骗防范能力。

10 可靠性要求

10.1 设备级故障管理

媒体网关应提供网关内部的故障检测、通知、隔离和业务恢复功能。

媒体网关应检测出以下故障并对其进行管理：

- 模块故障；
- 机框管理模块故障/冗余机架管理；
- 主系统控制模块故障/备系统控制模块故障/主系统控制模块切换；
- 链路/信道故障；
- 供电故障；
- 风扇故障；
- 模块温度过高；
- 数据总线故障；
- TDM端口/IP端口故障；
- 时钟卡故障；
- 外部TDM时钟源；
- 其他。

当出现以上故障时，媒体网关可有以下几种反应：

- 关闭故障板卡；
- 重新设置板卡；
- 通知模块切换至背板上的一条激活数据、TDM或串行管理总线上。

将通信重新路由至以IP接口上的备份端口处或备份TDM链路上

10.2 冗余备份要求

媒体网关应考虑对以下部件进行冗余备份和容错管理：

- 备份总线（可选）；
- 备份外部时钟源；
- 备份电源；
- 备份信令链路；

- 备份数据链路;
- 备份风扇;
- 其他。

主要单板均采用1:1或1:N热备份方式,所有单板均支持热插拔,可以在线更换,支持异常保护功能和数据备份功能。

10.3 信令切换要求

如果媒体网关的主系统控制模块发生故障,媒体网关应能够自动切换至备用系统控制模块,随后备用系统控制模块就自动开始与软交换进行通信,同时不会影响当前呼叫的状态。

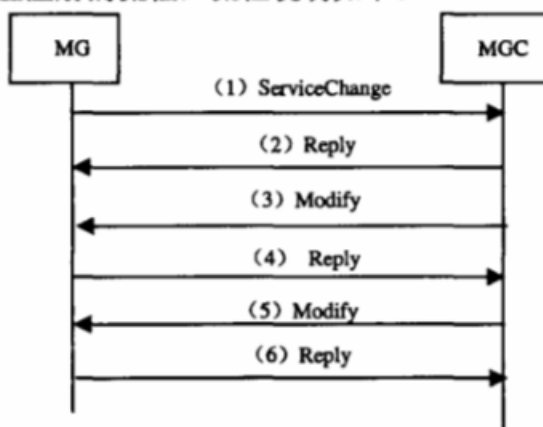
在具有双归宿的软交换网络环境下,如果工作中的软交换发生故障,媒体网关能够主动识别软交换所发生的故障并向备用软交换建立工作关系。

附录 A
(规范性附录)
接入认证流程

本附录所描述的接入认证流程仅仅在 MGC/软交换与媒体网关之间进行，不涉及到其他的功能实体。

A.1 H.248 协议接入认证注册流程

图 A.1 是 H.248 协议接入认证注册的流程，流程说明如下。



图A.1 H.248协议接入认证注册流程

(1) MG 向 MGC 发送 ServiceChange 进行注册，ServiceChange 中的 TerminationId 设置为 Root, Method 项为必选，设置为 Restart, ServiceChangeReason 项为必选，version 项为可选。命令中还带有 4 个用于认证的 X 字段：一个用于数字签名的数字串 MG_{AUTH} 、算法 ID 和随机数 Rand；还带有用于 DH 交换的 A。

MG 事先产生一个随机数 Rand，同时 MG 再产生一个用于 DH 交换的私人数字 a，计算得到 $A=g^a \bmod (P)$ 。通过计算得到 MG 的数字签名：

$$MG_{AUTH}=MD5(Ki + MGID + A + Rand);$$

(2) MGC 收到 ServiceChange 命令后，首先计算：

$$MG_{RES}=MD5(Ki + MGID + A + Rand)。$$

如果 $MG_{AUTH} = MG_{RES}$ ，则说明是合法的 MG 发过来的信息，认证通过；否则拒绝。同时接入控制器再产生一个用于 DH 交换的私人数字 b，计算 $B=g^b \bmod (P)$ 得到共享的鉴权密钥 $KEY-MGC=A^b \bmod (P)=g^{ab} \bmod (P)$ ，再生成一随机数 Rand，进而计算得到 $MGC_{AUTH}=MD5(KEY-MGC + Ki + B + Rand)$ 。

(3) MGC 向 MG 发送 Modify 消息，同时 MGC 把 B、 MGC_{AUTH} 、算法 ID（实验中采用 MD5）和随机数 Rand 下传给 MG。

(4) MG 得到 B 和 MGC_{AUTH} 后，计算得到共享密钥 $KEY-MG=B^a \bmod (P)=g^{ab} \bmod (P)$

进而计算 $MGC_{RES}=MD5(KEY-MG + Ki + B + Rand)$ ，如果 $MGC_{AUTH} = MGC_{RES}$ ，则说明是一个合法的 MGC 发过来的信息，MG 向 MGC 回送 Reply 响应。

(5) MGC 定期向 MG 发送 Modify 命令进行鉴权，命令中带有 MGC 产生的随机数 Rand 及用共享密钥 KEY-MGC 加密生成的结果。同时命令中还带有算法 ID。如采用 MD5 加密，则加密方法为 MD5 (KEY-MG + Rand)。

(6) MG 在 Reply 的应答中用 Signal 描述符带有用共享密钥 KEY-MG 加密的两项：MGID 及随机数 Rand（为 MGC 所带的）。如采用 MD5 加密，则加密方法为：MD5 (KEY-MG + MGID + Rand)。

上述流程中：

(1) 在初次注册成功后，马上发送 MODIFY 消息以生成共享密钥。

(2) 后续通过 modify 重复 (5) ~ (6) 步定期进行安全检测，Modify 时间间隔由 MGC 控制，建议不大于 10min。

(3) 推荐加密算法采用 MD5。

按照正文的描述，计算 MD5 的表达式如下：

$DIGET = MD5 (Param1 + Param2 + Param3 + Param4)$

DIGIT: MD5 的输出，为 128bit 长的数据块；

Parami: 表示一个一定长度的以 byte 为单位的 bit 数值串；

加号 (+) 表示：将各个 Param 的 bit 数值串从左到右按照数值从高位到低位排列后形成一个 bit 数值串作为入参输入 MD5 进行计算。

(4) 用于 Differ-Hellman 交换质数 p 及底数 g 网关上就应根据 MGC 的要求进行配置或生成，对 MG 和 MGC 公开。

(5) 用户初始安装时，在 MGC 和 MG 中设置一个共享密钥 K_i ，密钥长度是 128bit；

(6) 每个 MG 都有一个数字标示 (MGID)：MGID 为 16 个 byte 数字标识，包含厂家和设备信息，该信息不在其他地方公开传送，只有 MG 本身和管理该 MG 的 MGC 知道。

(7) 计算值与信令的相互转化：

a) 将 DH 值、随机数值、MD5 摘要等用于认证计算的二进制 bit 数值编码组装成信令时，对这些数值从高位到低位以字节为单位逐字节转换 (bit 数值的长度保证为字节的整数倍)，每个字节按从高位到低位转换成 2 个十六进制字符，从左到右顺序组装成信令文本字符串。

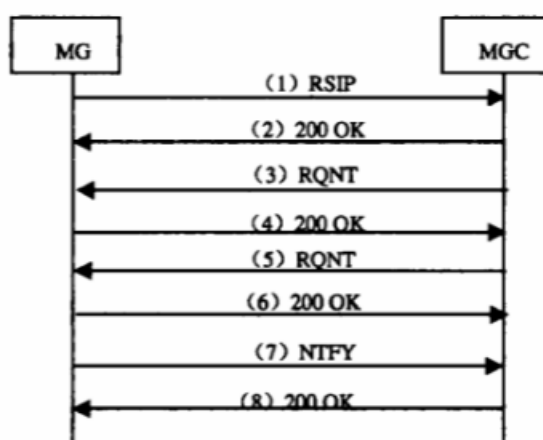
b) 对于算法，由数字转换为十进制字符串，组装成信令。

c) 对于 DH 值、随机数值、MD5 摘要等，如果是从信令上获得对方的这些值，应该将十六进制字符串格式的信令文本，按从左到右按顺序转换为二进制 bit 数值。转换时每两个字符按从左到右顺序转换成一个字节的高 4 位和低 4 位长度，将所有字节按数值的从高位到低位的顺序排列形成二进制数值，用于本地计算。

(8) 随机数：长度为 byte 的整数倍。

B.2 MGCP 协议接入认证注册流程

图A.2是MGCP协议接入认证注册的流程，流程说明如下。



图A.2 MGCP协议接入认证注册流程

(1) MG 向 MGC 发送 RSIP 命令进行注册, RSIP 中的 EndpointId 参数使用通配值 "*", RestartMethod 项为必选, 设置为 Restart, 命令中还带有 4 个用于认证的 X 字段: 一个用于数字签名的数字串 MG_{AUTH}、算法 ID 和随机数 Rand₁; 还带有用于 DH 交换的 A。

MG 事先产生一个随机数 Rand, 同时 MG 再产生一个用于 DH 交换的私人数字 a, 计算得到 $A = g^a \bmod (P)$ 。通过计算得到 MG 的数字签名: $MG_{AUTH} = MD5(Ki + MGID + A + Rand_1)$;

(2) MGC 收到 RSIP 命令后, 首先计算: $MG_{RES} = MD5(Ki + MGID + A + Rand)$

如果 $MG_{AUTH} = MG_{RES}$, 则说明是合法的 MG 发过来的注册信息, 认证通过, MGC 向 MG 发送 200 OK 消息; 否则拒绝。

认证通过后, MGC 再产生一个用于 DH 交换的私人数字 b, 计算 $B = g^b \bmod (P)$ 得到共享的鉴权密钥 $KEY-MGC = A^b \bmod (P) = g^{ab} \bmod (P)$, 再生成一个随机数 Rand₂, 进而计算得到 $MGC_{AUTH} = MD5(KEY-MGC + Ki + B + Rand_2)$ 。

(3) MGC 向 MG 发送 RQNT 消息, 同时 MGC 把 B、MGC_{AUTH}、算法 ID (例如 MD5) 和随机数 Rand₂ 下传给 MG。

(4) MG 得到 B 和 MGC_{AUTH} 后, 计算得到共享密钥 $KEY-MG = B^a \bmod (P) = g^{ab} \bmod (P)$, 进而计算 $MGC_{RES} = MD5(KEY-MG + Ki + B + Rand)$ 。如果 $MGC_{AUTH} = MGC_{RES}$, 则说明是一个合法的 MGC 发过来的命令消息, MG 返回 200 OK 响应命令。

(5) MGC 定期向 MG 发送 RQNT 命令进行鉴权, 命令中带有 MGC 产生的随机数 Rand 及用共享密钥 KEY-MGC 加密生成的结果。同时命令中还带有算法 ID。如采用 MD5 加密, 则加密方法为 MD5 (KEY-MGC + Rand)。

(6) MG 回送 200 OK 响应。

(7) MG 向 MGC 发送 NTFY 命令, 其中 ObservedEvents 参数带有用共享密钥 KEY-MG 加密的两项: MGID 及随机数 Rand (为 MGC 在上一步中以 RQNT 发送的)。同时, 命令还携带算法 ID, 如采用 MD5 加密, 则加密方法为: MD5 (KEY-MG + MGID + Rand)。

(8) MGC 回送 200 OK。

上述流程中:

(1) 在初次注册成功后, 马上发送 RQNT 消息以生成共享密钥。

(2) 后续通过 RQNT 重复 (5) ~ (6) 步定期进行安全检测。RQNT 时间间隔由 MGC 控制, 建议不大于 10min。

(3) 推荐加密算法采用 MD5。

按照以上描述, 计算 MD5 的表达式如下: $DIGET = MD5(Param1 + Param2 + Param3 + Param4)$

DIGIT: MD5 的输出, 为 128bit 长度的数据块;

Parami: 表示一个一定长度的以 byte 为单位的 bit 数值串;

加号 (+) 表示: 将各个 Param 的 bit 数值串从左到右按照数值从高位到低位排列后形成一个 bit 数值串作为入参输入 MD5 进行计算。

(4) 用于 Differ-Hellman 交换质数 p 及底数 g, 网关应根据 MGC 的要求进行配置或生成, 对 MG 和 MGC 公开。

(5) 用户初始安装时, 在 MGC 和 MG 中设置一个共享密钥 Ki, 密钥长度是 128bit;

(6) 每个 MG 都有一个数字标示 (MGID): MGID 为 16 个 byte 数字标识, 包含厂家和设备信息, 该信息不在其他地方公开传送, 只有 MG 本身和管理该 MG 的 MGC 知道。

(7) 计算值与信令的相互转化:

a) 将 DH 值、随机数值、MD5 摘要等用于认证计算的二进制 bit 数值编码组装成信令时, 对这些数值从高位到低位以字节为单位逐字节转换 (bit 数值的长度保证为字节的整数倍), 每个字节按从高位到低位转换成 2 个十六进制字符, 从左到右顺序组装成信令文本字符串。

b) 对于算法, 由数字转换为十进制字符串, 组装成信令。

c) 对于 DH 值、随机数值、MD5 摘要等, 如果是从信令上获得对方的这些值, 应该将十六进制字符串格式的信令文本, 按从左到右按顺序转换为二进制 bit 数值。转换时每两个字符按从左到右顺序转换成一个字节的高 4 位和低 4 位长度, 将所有字节按数值的从高位到低位的顺序排列形成二进制数值, 用于本地计算。

(8) 随机数: 长度为 byte 的整数倍, 不小于 16byte 长度。
