国 际 电 信 联 盟

ITU-T H.235.9

国际电信联盟
电信标准化部门

(09/2005)

H系列：视听和多媒体系统

视听业务的基础设施 — 系统概况

H.323安全性：H.323的安全网关支持

ITU-T H.235.9建议书

国际电信联盟

ITU-T H系列建议书

视听和多媒体系统

可视电话系统的特性	H.100-H.199
视听业务的基础设施	
概述	H.200-H.219
传输多路复用和同步	H.220-H.229
系统概况	**H.230-H.239**
通信规程	H.240-H.259
活动图像编码	H.260-H.279
相关系统概况	H.280-H.299
视听业务的系统和终端设备	H.300-H.349
视听和多媒体业务的号码簿业务体系结构	H.350-H.359
视听和多媒体业务的服务质量体系结构	H.360-H.369
多媒体的补充业务	H.450-H.499
移动性和协作程序	
移动性和协作、定义、协议和程序概述	H.500-H.509
H系列多媒体系统和业务的移动性	H.510-H.519
移动多媒体协作应用和业务	H.520-H.529
移动多媒体应用和业务的安全性	H.530-H.539
移动多媒体协作应用和业务的安全性	H.540-H.549
移动性互通程序	H.550-H.559
移动多媒体协作互通程序	H.560-H.569
宽带和三网合一多媒体业务	
在VDSL上传送宽带多媒体业务	H.610-H.619

欲了解更详细信息，请查阅*ITU-T*建议书目录。

ITU-T H.235.9建议书

H.323安全性：H.323的安全网关支持

摘　要

本建议书定义了一种方法，可用于在 H.323 实体之间通信用的信令通路中发现安全网关，还可用于在网守与安全网关 SG 间共享安全信息以保持信令的完整性和保密。

来　源

ITU-T 第 16 研究组（2005-2008）按照 ITU-T A.8 建议书规定的程序，于 2005 年 9 月 13 日批准了 ITU-T H.235.9 建议书。

关键词

网关，安全，信令。

前　言

国际电信联盟（ITU）是从事电信领域工作的联合国专门机构。ITU-T（国际电信联盟电信标准化部门）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定 ITU-T 各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA 第 1 号决议规定了批准建议书须遵循的程序。

属 ITU-T 研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联尚未收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能不是最新信息，因此大力提倡他们查询电信标准化局（TSB）的专利数据库。

目 录

引言

防火墙与/或网络地址解析设备的使用，是为处于不同管理控制下的网络区域当电话信令协议出现问题，务必通过交换网络地址来进行信令和媒体交换时提供业务安全。

ITU-T H.235.5 建议书引入了一种框架，通过这个框架，端点与它的网守或两个网守之间可以采用初始 RAS 消息对它们之间的一套强共享秘密进行协商，同时使用那些秘密来加密后续 RAS 的选定部分以及呼叫信令消息，并对这些消息加以认证。此方法仅适用于网守选路的信令方式。类似的方法和安全概要在 ITU-T H.235.1、H.235.2 和 H.235.3 建议书中进行了定义。此安全框架可能与应用层网关（ALG）产生冲突，应用层网关将网络域互连并对信令和由 H.225.0 RAS 与/或呼叫信令信息所携带的媒体传输地址进行操作。消息中的这些变化将导致在目的地的信息认证检查不成功。

本建议书描述了一个简单的手段，通过这个手段网守可以在一个信令通路中接到应用层网关（ALG）的通知，同时还能与那些应用层网关（ALG）共享协商后的信令认证密钥。这使得应用层网关（ALG）可在信令消息中操作非专用的数据，特别是传输地址，然后在将修改后的消息向前传递时对结果进行认证。在后面的正文中，上述装置指的是安全网关（SG）。这个技术保留了信令中的任何一个加密单元的端到端保密。

ITU-T H.235.9建议书

H.323安全性：H.323的安全网关支持

1 范围

本建议书适用于采用 H.225.0 RAS 协议的任何网守和端点，它们可能具有一个或多个指定行为的中间安全网关。

2 参考文献

2.1 规范性参考文献

下列 ITU-T 建议书和其他参考文献的条款，通过在本建议书中的引用而构成本建议书的条款。在出版时，所指出的版本是有效的。所有的建议书和其他参考文献都面临修订，使用本建议书的各方应探讨使用下列建议书和其他参考文献最新版本的可能性。当前有效的 ITU-T 建议书清单定期出版。本建议书中引用某个独立文件，并非确定该文件具备建议书的地位。

– ITU-T Recommendation H.225.0 (2003), *Call signalling protocols and media stream packetization for packet-based multimedia communication systems.*
– ITU-T Recommendation H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.
– ITU-T Recommendation H.235.1 (2005), *H.323 security: Baseline security profile*.
– ITU-T Recommendation H.235.2 (2005), *H.323 security: Signature security profile.*
– ITU-T Recommendation H.235.3 (2005), *H.323 security: Hybrid security profile.*
– ITU-T Recommendation H.235.5 (2005), *H.323 security: Framework for secure authentication in RAS using weak shared secrets*.
– ITU-T Recommendation H.245 (2005), *Control protocol for multimedia communication.*
– ITU-T Recommendation H.323 (2003), *Packet-based multimedia communications systems.*

2.2 资料性参考文献

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0.*
– IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.
– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol.*

3 定义

本建议书对以下术语进行了定义：

3.1 application level gateway 应用层网关：是一个协议知觉设备，将两个或多个网络区域互连，能够解释并修改应用层协议以提供传输地址解析及其他功能。一个 ALG 可提供内部的传输层网络地址解析（NAT）和防火墙功能，也可以从外部来控制它们。

3.2 local address 本地地址：在内部地址域内的传输地址。

3.3 media gateway 媒体网关：将两个或多个网络域互连的设备，可以被其他设备（如一个安全网关 SG）所控制以在域之间提供受控的媒体流。媒体网关 MG 是一个在传输层及以下有效工作的可编程的 NAT/防火墙。

3.4 network address translation 网络地址解析：将网络传输地址从一个网络域映射到另一个域的操作。

3.5 pinhole 针孔：一个可穿过网关 SG（或一个其控制下的媒体网关）的流量通路。针孔通常以 4 个传输地址（域 A 的源地址、网关 SG 域 A 地址、网关 SG 域 B 地址、域 B 的目的地地址）为特征，其他特性还有传输协议及方向性。源地址可能未指定，例如一个监听端口。

3.6 realm 域：一个共享公用网络地址空间的网络区域；假定不同的域采用不兼容的，冲突的或专用的地址空间。

3.7 security gateway 安全网关：安装在两个或多个 IP 网络区域间，用于提供安全功能如确认或限制数据流量并在网络区域间映射传输地址的设备。在本建议书中，假定安全网关是一个了解 H.323 信令协议的应用层网关 ALG。

4 缩写

本建议书使用以下缩写：

ALG 应用层网关

GCF GatekeeperConfirm

GK 网守

GRJ GatekeeperReject

LCF LocationConfirm

LRQ LocationRequest

MG 媒体网关

NAT 网络地址解析

OID 对象标识符

RAS 注册、许可和状态协议

SG 安全网关

UDP 用户数据报协议

5 惯例

本建议书定义了信令安全性能、程序或安全算法的各种对象标识符（OID）。这些 OID 与指定值的序列树相关，这些值可能来自外部源或是 ITU-T 保持的 OID 树的一部分。特别地，与 ITU-T H.235 建议书相关的那些 OID 在文本中有下列表述：

“OID” = {itu-t（0）recommendation（0）h（8）235 version（0）**V N**}，其中 **V** 象征性地代表一个十进制的数字，它指示 ITU-T H.235 建议书的对应版本；如 1、2、3 或 4。**N** 象征性地代表一个十进制的数字，它惟一地标识 OID 实例，因而标识程序、算法或安全性能。

因此，ASN.1 编码 OID 由数字序列组成。为方便起见，每个 OID 的电文助记速写串符号在报文中使用，如“OID”。给出每个 OID 串与 ASN.1 数字序列相关的映射。遵循 ITU-T H.235 建议书的实施必须仅使用 ASN.1 编码数字。

基本假定

本建议书认为 IP 网络模型中，多个被称为域的网络区域是通过被称为安全网关（SG）的设备互连的，这些设备知道 H.323 协议，而且是被设计成能够在它们互连的网络域之间控制信息流量的。预期网关设备（SG）能够检查域之间的信令消息流，确保它们的有效性，提取交换过的传输地址信息，使用该传输信息来构建域之间的适当的流通路，并修改传输地址使它对于消息转发的域而言是正确的。当然网关设备（SG）务必确保信令通路流量从它们自身流过，但是它们也可以控制其他设备以支持任何一种已经建立的媒体流。网关设备 SG 之间的控制协议和“媒体网关”在本建议书中并未述及。

为了使某个域中的网守能够为端点或其他域中的网守所使用，如果 SG 所服务的域中没有已知的网守，则应该为每个域都提供一个网守发现地址。这样经过执行所有必要的 H.323 消息操作后，SG 可以将从某个地址接收到的发现信息转发到实际的网守。配置的示例图见图 1，图中显示了一个网守服务于多个网络域中的端点。

实际上，安全网关务必代表它们所服务的每一个域的网守（当然，网守所驻守的域除外，如图中的域 A 中的网守 A）。SG B 为图中的两个网守都提供了发现地址，这样它为 LRQ/LCF 信令提供了一个网守到网守的通路。还应注意的是 SG 并不需要为每个域的每个网守提供接入。例如，图 1 中的 SG A 可以配置成仅为域 B 提供网守 A 的发现地址。

假定每个网守知道系统中的每个 SG 的惟一名字，同时网守和每个 SG 之间共享一个可用于它们之间安全通信的已加密码的强秘密。这些实体以及相应的密钥的协商和交换方式将在下文中讨论，但并不是本建议书的主题。共享的秘密对每个 SG/网守对必须是惟一的。还假定 SG 将修改 RAS 和已交换的呼叫信令地址，以确保 RAS 和呼叫信令经过它们传递。

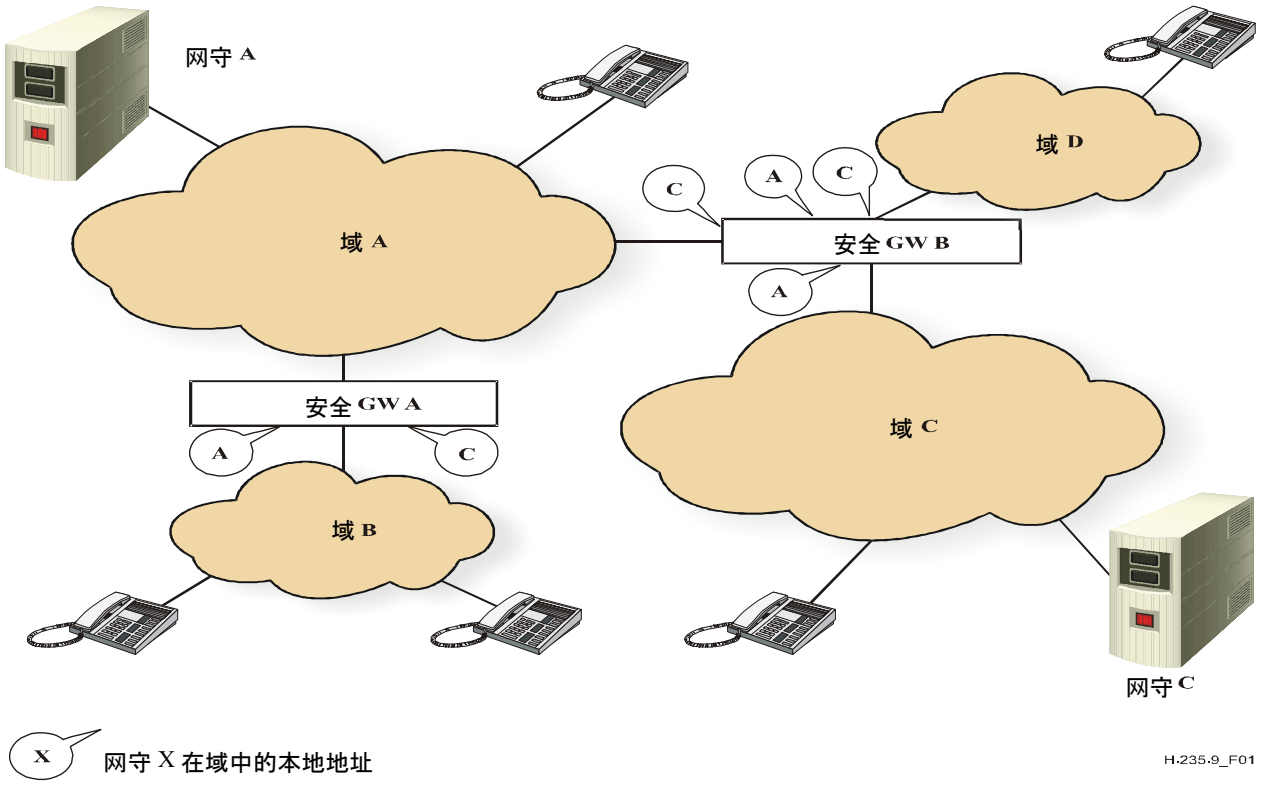


图 1/H.235.9－安全网关配置图

除此之外，对已建立的初始发现过程进行选路和/或地址解析的方法也不是本建议书的主题，但下文中仍有论述。后续的地址建立，伴随着所有必需的解析，也假定是 SG 应进行的操作的一部分。

6 基本操作

以下的叙述假定出现在系统中的每个 SG 已与每个预期它会为之服务的网守注册。如何实现的细节将稍后讨论。对于基本的操作，假设 SG 已经被每个网守识别，并与每个网守共享了一个惟一的强秘密，并为每一个网守提供了一个或多个“本地”网守发现地址。SG 注册的细节将在后面的章节中讨论。下面将描述 SG 如何参与端点的注册以便获得 GK 与端点之间进行端到端认证密钥协商的途径。

6.1 端点网守发现

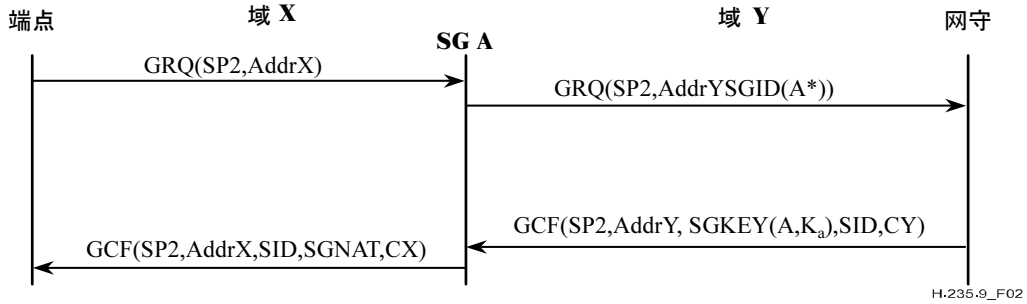
当端点发送 GRQ 到网守发现地址，GRQ 途经 SG 继续传递到一个或多个网守时，SG 可以在 GRQ 内操作地址时在 GRQ.**token** 单元上增加 **ClearToken**。这个 ClearToken 将被标识为 SG-id token（通过它的 **tokenOID**），并将包含一个能够惟一代表这个 SG 的标识串。这个 SG 应该从 GRQ 的 **authenticationCapability** 概要中移走所有的特殊 **AuthenticationMechanism**（例如，RFC 2246 和 RFC 3546 中的 TLS 或 RFC 2401 中的 IPsec），那都是它所不能支持的信息认证进程。这将确保网守选择与 SG 兼容的概要。第一个接收到 GRQ 的 SG 必须包含标识着发现地址的单元，SG 就是在这个地址从端点接收到 GRQ 的。

不容置疑的假定是每个 SG 为了进行地址处理，将在 GRQ 内操作所有的信令地址字段以及后续的 RAS 消息，以确保所有经过的信令消息能流过 SG。

6.2 端点认证密钥分发

当 GRQ 到达网守（GK），网守将对 GRQ，包括 SG-id 标记，进行处理。假定 GK 将作为端点的网守，它将准备发送 GCF 回端点。于是 GK 将在 GCF 消息中加入已选的 **AuthenticationMechanism**，伴随着 SG 密钥 **ClearToken**（由它的 **tokenOID** 所标识）给由收到的 SG-id 标记所标识的 SG。这个密钥标记将包含 SG 的标识、GK 的标识、一个初始化矢量、使用初始化矢量 IV 加密的对话认证密钥以及 SG 与网守之间的共享秘密。加密算法必须在 SG 注册时进行协商，或加以预设。

由于 GCF 沿着到端点的通路传递回来，它经过了提供 SG-id 标记的 SG。此 SG 必须对消息进行分解以获得对话 ID 以及它自己的密钥令牌。它必须对对话认证密钥进行解密并使用它来认证收到的消息。如果消息是可信的，SG 将对所有传输地址进行适当的操作，然后去掉自己 SG-key 标记、插入一个 SG-NAT 标记（如果这个标记还没出现过）来重建消息，再对重建后的消息进行认证并发出。对话 ID 和认证密钥必须保留给后续的 RAS 和会议所用的呼叫信令信息使用。通过单个 SG 的基本顺序在图 2 中给出了图示。还应注意的是 SG 务必准备从 GCF 推断出的所有针孔（如 RAS 针孔以及供替换的 GK 地址针孔等）。



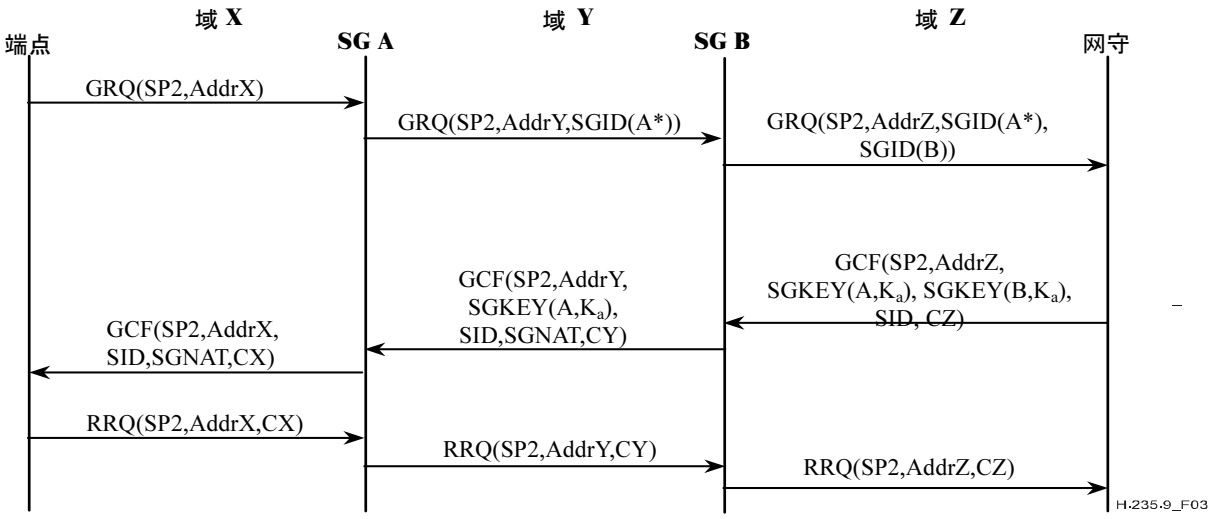
SP2=H.235.5安全概要
Addrx=x域中的地址
SGID（ A*）=SG-id ClearToken标识SG A的出现
（ *表示SGID包含GRQ所使用的发现地址。）
SID=对话ID（ 由网守指派）
K_a=SID的消息认证密钥
SGKEY （ A, K_a）=SG-key ClearToken 用A的秘密密钥加密的K_a
SGNAT=SG-NAT ClearToken
CX=域 x 内的消息校验和（ 使用协商的 K_a 进行计算）

图 2/H.235.9－基本的SG遍历交换

此方案很容易就可扩展到端点和网守之间有一系列的 SG 的情形。每个 SG 在 GRQ 通过时加入它自己的 ClearToken，在 GCF 从网守返回到端点时去掉它自己应答的 ClearToken。通路中的第一个返回到端点的

SG 必须在 GCF 内插入 SG-NAT 标记。图 3 显示了此操作过程。对后续 RAS 消息的处理也在图中通过 RRQ 消息内传输地址的转换和校验和的重新计算显示了出来。

LRQ/LCF 交换也是采用类似的顺序，使用同样的消息单元，且结果可能被用于处理和认证此会议后续的信令消息。



SP2=H.235.5安全概要
Addrx=x域中的地址
SGID（ A*）=SG-id ClearToken标识SG A的出现
（ *表示端点所使用的发现地址的出现。）
SID=对话ID（ 由网守指派）
K_a=SID的消息认证密钥
SGKEY （ A，K_a）=SG-key ClearToken 用A的秘密密钥加密的K_a
SGNAT=SG-NAT ClearToken
Cx=域 x 内的消息校验和

图 3/H.235.9－两级SG的遍历交换

6.3 地址操作

当每个 H.225.0 或 H.245 信令信息通过，SG 务必检查并替换携带在信息里的传输地址，这样它们在消息将经过的下一个域仍然有效。这可能要求 SG 建立新的流量针孔以支持有关的信令与/或媒体在这些打算建立的地址上流过。注意那些代表着监听端口的地址，它们务必“就在那种情况下”开启；当/如果数据包到达监听端口时一个完全指定的针孔将建立起来。

每个 SG 可以检查每个接收到的目的地传输地址，以察看它是否确实代表了那个 SG 的目的地地址。考虑图 4 中的域配置与媒体通路的示例。一个媒体流从域 B 中的端点流向域 C 中的端点时，将流经 SG B 和 SG C，这条路径在图中标注为“1”。在不特别指定流经 SG B 的情况下，域 B 两个端点间的媒体流就通过一个效果相同的路径，上到域 A 再返回到域 B，这条路径在图中标注为“2”。现在，如果 SG B 意识到提供给域 A 的数据流的源头和目的地地址时 SG B 的真实地址时，它可以将数据流通过以下两种方式“短路”：可在内部选路，这条路径在图中标注为“3”（为清晰起见在 SG C 中显示）；或者如果它意识到两个端点都驻守在域 B 中，它可以将域 B 的端点地址替换，以使数据流直接在端点间流动，这条路径在图中标注为“4”。注意 SG B 所看到的“端点”地址可能实际上是连接到了另一个域的 SG（就称之为 D）上的地址。当 SG B 修改地址以执行 SG D 上地址之间的“直接”路径时，SG D 也可能以同样的方式将数据流短路。

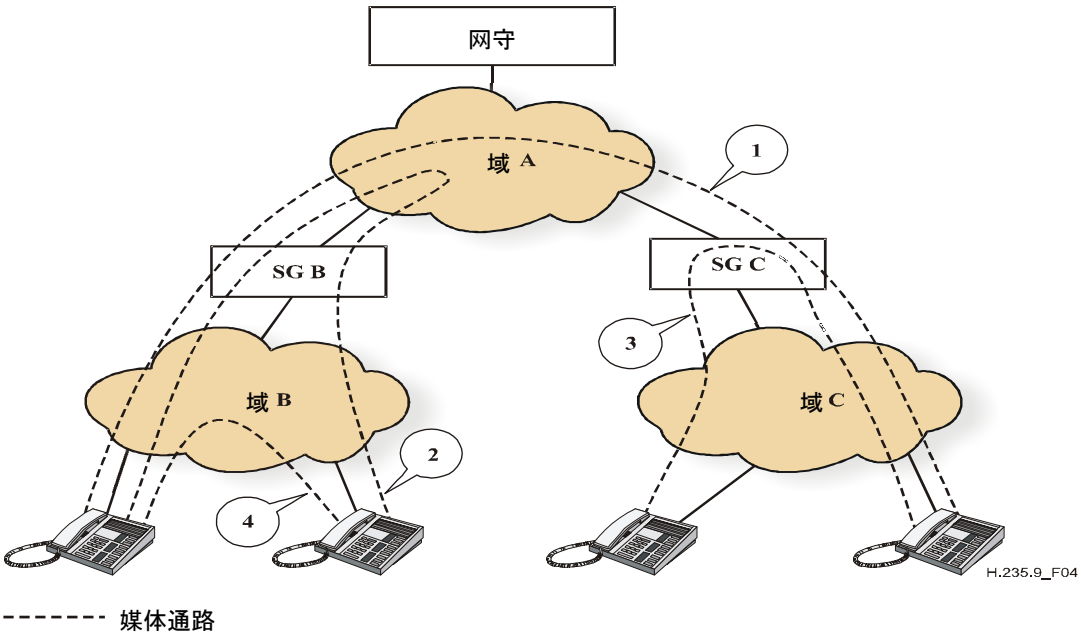


图 4/H.235.9－媒体通路

此方案未能处理的一种配置是当一个区域通过多于一个的 SG 获得路径时的情况。如果端点通过一个 SG 注册并发信号，而另一个处于同一区域的端点向第二个 SG 发信号，或端点将使用的地址从另一个 SG 发出信号，那么对于两边的 SG 而言要想发现两个端点处于同一域是很难的。为避免这一问题，采用一个能够处理预期信令等级的 SG 是适宜的；媒体流处理负载可能被降级，以分离在 SG 控制之下的媒体网关。

7 信令详情

对于此能力的支持可通过一个处于生效的纯文本标记中的标准的对象标识符（OID）来最有效地加以识别。此后，这些标记将被认为是 SG 标记。这使得所有接收的网守（或中间网关或其他未参与的设备）可略去此特征。指派的 OID 可用于标识携带以下单元的 **ClearToken**s。

- **tokenOID** — 设置指派给此特性的 OID，称之为“SG1”，具体见第 11 节。
- **generalID** — 如果出现，将它设置为此 **ClearToken** 指向的 SG 的名称（在 SG-key 标记中使用过）
- **sendersID** — 设置为建立此 **ClearToken** 的 SG 的名称（在 SG-id 标记中使用过）
- **profileInfo** — 包含此 **ClearToken** 携带的指定消息，具体在表 1 中指定。

表 1/H.235.9－SG发现的轮廓单元

单元名称	单元ID值	单元类型（长度）	单 元 描 述
标记类型	1	完整	0 = SG-id 令牌 1 = SG-key 令牌 2 = SG-NAT 令牌 3 = SG-register 令牌
加密密钥	2	八比特组（SP2 为 16）	从指示的安全概要、在指定的 SG 和 GK 间通过两者间的秘密加密的对话认证密钥。用 SG-key 标记发送。必要的解密 IV 在 ProfileElement.paramS 中指定。
服务域	3	名称	能够/必须提供的网守发现地址的域的名称

8 SG的配置考虑

本建议书描述的进程取决于网络中的 SG 发现到网守的通路的手段，这些网守的服务可以被在网络中不同域中的用户获得。每个 SG 务必能够与该域中它的网守（或其他网守）取得联系，并为网守与处于其他域中的端点（或其他网守）提供通路。例如，如图 3 所示，SG B 在域 Z 中与网守接通。它同样也可以为域 Y 中的单元提供通路至网守。这样 SG A 可以通过 SG B 与网守接通。只要 SG B 网守与网守接通，它就能够为域 X 中的各方提供通路。这也表明 SG 自己要使用发现协议如 RAS。这些进程还可以用于识别每个 SG 到它可接通的网守，并协商（一套）密钥以保护用户信令交换。

8.1 SG注册

一个 SG 可作为一个域中的代表为其他域中的可接通的网守服务。例如，如图 1 所示，一旦 SG A 知道域 A 中的网守的发现地址 SG A，即可在域 B 中提供一个代表（一个发现地址）给域 A 中的网守。此技术可扩展到多层 SG；每个 SG 发现一个网守（或一个代表），它就可提供一个或多个新域中的发现地址，此时 SG 与发现那些地址的域建立连接。

SG 必须使用 H.225.0 RAS 进程来发现和与任意它们希望作为安全网关服务的域的网守进行注册。SG 必须将它自己识别为**网关**端点类型的设备。如果 SG 希望指定支持前缀与/或带宽限制，它可以指定 H.323 的协议支持，但并没有这样的要求。如 ITU-T H.235.1、H.235.2、H.235.3 和 H.235.5 建议书所述的标准安全进程，必须用于认证至网守的 SG，并用于协商下述进程中使用的安全共享秘密。H.235.1、H.235.2、H.235.3 和 H.235.5 中的进程能够穿越本建议书支持的其他安全网关。SG 还务必在它发给网守的 RRQ 中包含 SG-register ClearToken。此标记用于将网关标记为 SG，且它必须为每个 SG 将服务的新域包含一个 **ServedRealm** 单元。每个单元在它各自的域内代表一个潜在的新网守发现地址。可对每个 SG 进行配置以限制为域提供的网守发现地址。例如，如图 1 所示，SG B 可配置成不为域 D 中的网守 C 提供发现地址，这样就迫使域 D 中的端点注册到网守 A。目前由于 SG 自身并不发出或接收电话，在注册时它不需要提供呼叫信令地址，它可以在 RRQ 中的 **callSignalAddress** 提供一个空的 SEQUENCE。网守必须像对 RCF 中 **callSignalAddress** 那样响应。

反过来，网守必须在 RCF 中指示 SG 可以为哪个域提供服务，从 SG 的 RRQ 中，一个 SG-register 令牌包含了一个或多个 **ServedRealm** 单元。一旦注册完成，SG 将为每个指示的域中的网守发现地址开放一个监听套接字。本建议书以外的机制可用于在域内宣布此发现地址。网守可以从一个可选地址的列表中选取 SG 提供的发现地址。

任何 RAS 安全概要都可以使用，只要 SG 被允许读和操作已交换的信令和媒体传输地址，并可重新认证此消息。

网守可利用 SG 域信息来映射网络区域和连通性，并认证 SG。网守必须将信息提供回 SG：

- 网守的证书。
- SG 可以使用的注册地址，以接替从它所服务的域中的端点的 RAS 请求（例如，GK 可以拒绝支持 SG 服务的一个或多个区域的端点。

一个成功的 SG 注册的重要结果应该是 SG 与网守间共享的强秘密密钥，从它可以衍生出加密与/或认证密钥。认证密钥可用于认证 SG 注册方案，而加密密钥应在端点注册时用于加密端点对话认证密钥，以如上文所述，将它分发给 SG。

8.2 认证证书

与端点的数量不同的是，在多区域网络中的 SG 的数量预计相对较少。在大多数情况下，此服务可望通过订购或其他契约式的协议来提供，因此网守将准备一些可能在它这里注册的 SG 的标识信息。最简单的方式是，可以指派口令给 SG，并可使用 H.235.1、H.235.2、H.235.3、H.235.5 或查询—应答响应进程。使用预共享的秘密当然需要一个安全的带外机制以便于分发。

另一个可供选择的机制是基于公钥证书的。网守的证书复本（或属于签发网守证书的管理机构的证书）可以通过某些可信的步骤进行安装。证书的使用方法还有待于进一步研究。

9 安全考虑

此类在传送过程中消息可修改的协议，可能遭受降级攻击。例如，若一个端点同时提供加密和不加密的媒体传输能力，一个恶意的 SG 可能撤去加密提议，而仅提供非加密的能力，这样就确保媒体流不被加密。仅提供根据它们自己的安全策略可接收的能力的端点（和网守）可能会遇到此类攻击。最终，这是端点和它们的用户的责任，以确保建立并维持合适的安全注册。类似的考虑也适用于注册时安全概要的选择：如果端点要求强认证，应在 GRQ 中指明，而且它不应接收从网守处发来的提供较弱认证的提议。

10 适用性

本方案将适用于 ITU-T H.235.5 建议书及它以外的其他 H.235.1、H.235.2、H.235.3 安全概要。也支持所有用于提供协商/恰当的认证密钥的衍生的安全概要也都支持。SG 必须检查 GRQ/GCF 中的单元（例如 **authenticationCapability** 与/或 **authenticationMode**），以查看它们是否能够支持协商的消息认证或安全方案。

11 对象标识符

OID	对象标识符值	描　　述
"SG1"	{ itu-t (0) recommendation (0) h (8) 235 version (0) 4 65 }	为 SG 发现而携带概要单元的 ClearToken。

ITU-T系列建议书

A系列	ITU-T工作的组织
D系列	一般资费原则
E系列	综合网络运行、电话业务、业务运行和人为因素
F系列	非话电信业务
G系列	传输系统和媒质、数字系统和网络
H系列	**视听和多媒体系统**
I系列	综合业务数字网
J系列	有线网和电视、声音节目和其他多媒体信号的传输
K系列	干扰的防护
L系列	线缆的构成、安装和保护及外部设备的其他组件
M系列	电信管理，包括TMN和网络维护
N系列	维护：国际声音节目和电视传输电路
O系列	测量设备技术规程
P系列	电话传输质量、电话装置和本地线路网络
Q系列	交换和信令
R系列	电报传输
S系列	电报业务终端设备
T系列	远程信息处理业务的终端设备
U系列	电报交换
V系列	电话网上的数据通信
X系列	数据网和开放系统通信及安全
Y系列	全球信息基础设施、互联网的协议问题和下一代网络
Z系列	用于电信系统的语言和一般软件问题

瑞士印刷
2006年，日内瓦