(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2007 年7 月26 日 (26.07.2007)

PCT

(10) 国际公布号
WO 2007/082477 A1

(51) 国际专利分类号:
H04L 12/24 (2006.01)

(21) 国际申请号: PCT/CN2007/000192

(22) 国际申请日: 2007 年1 月18 日 (18.01.2007)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
200610001517.8
2006 年1 月18 日 (18.01.2006) CN

(71) 申请人 (对除美国外的所有指定国): 华为技术有限公司(HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人; 及

(75) 发明人/申请人 (仅对美国): 郑波(ZHENG, Bo) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

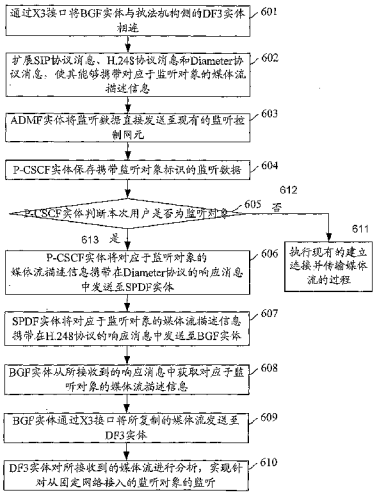
(74) 代理人: 北京德琦知识产权代理有限公司(DEQI INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区知春路1号学院国际大厦7层, Beijing 100083 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[见续页]

(54) Title: A METHOD FOR REALIZING THE LEGAL LISTENING IN THE NEXT GENERATION NETWORK AND A SYSTEM THEREOF

(54) 发明名称: 一种在下一代网络中实现合法监听的方法和系统



601 NNECTING THE BGF FUNCTION ENTITY AND THE DF3 ENTITY ON THE EXECUTING AGENCY SIDE BY X3 INTERFACE
602 EXTENDING THE SIP PROTOCOL MESSAGE, H.248 PROTOCOL MESSAGE AND DIAMETER PROTOCOL MESSAGE, AND ENABLING THEM TO CARRY THE DESCRIPTION INFORMATION OF THE MEDIA STREAM CORRESPONDING TO THE LISTENED OBJECT
603 ADMF ENTITY DIRECTLY SENDS THE LISTENING DATA TO THE CURRENT LISTENING CONTROL NETWORK ELEMENT
604 P-CSCF ENTITY SAVES THE LISTENING DATA CARRYING IDENTIFICATION OF THE LISTENED OBJECT
605 P-CSCF ENTITY DETERMINES WHETHER THE CURRENT USER IS A LISTENED OBJECT?
606 P-CSCF SENDS THE DESCRIPTION INFORMATION CORRESPONDING TO THE LISTENED OBJECT BY CARRYING THE INFORMATION INTO THE RESPONSE MESSAGE OF THE DIAMETER PROTOCOL TO THE SPDF ENTITY
607 SPDF ENTITY SENDS THE DESCRIPTION INFORMATION CORRESPONDING TO THE LISTENED OBJECT BY CARRYING THE INFORMATION INTO THE RESPONSE MESSAGE OF THE H.248 PROTOCOL TO THE BGF ENTITY
608 BGF ENTITY OBTAINS THE DESCRIPTION INFORMATION CORRESPONDING TO THE LISTENED OBJECT FROM THE RECEIVED RESPONSE MESSAGE
609 BGF ENTITY SENDS THE COPIED MEDIA STREAM BY THE X3 INTERFACE TO THE DF3 ENTITY
610 DF3 ENTITY ANALYSES THE RECEIVED MEDIA STREAM TO REALIZE THE LISTENING AIMED AT THE LISTENED OBJECT ACCESSING FROM THE FIXED NETWORK
611 PERFORMING THE EXISTING PROCEDURE FOR ESTABLISHING A CONNECTION AND TRANSMISSION OF MEDIA STREAM
612 NO
613 YES

(57) Abstract: A method for realizing the legal listening in the next generation network and a system thereof. The system comprises: a 3 channel delivering function entity, a listening information providing entity and a border gateway function entity. The method comprises: connecting the border gateway function entity in the next generation network and the 3 channel delivering function entity on the side of the executing agency; the listening information providing entity sends the listening information of the listened object to the border gateway function entity; the border gateway function entity sends the media stream of the listened object to the 3 channel delivering function entity based on the received information of the listened object. The legal listening of user accessing from fixed network is realized in the next generation network. The range of legal listening service is extended and the quality of service in the next generation network is improved.

[见续页]

WO 2007/082477 A1

(84) 指定国（除另有指明，要求每一种可提供的地区保护）：ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 欧洲 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告。

— 在修改权利要求的期限届满之前进行，在收到该修改后 将重新公布。

所引用双字母代码及其它缩写符号，请参考刊登在每期PCT公报期刊起始的“代码及缩写符号简要说明”。

(57) 摘要：本发明公开了一种在下一代网络中实现合法监听的方法和系统，该系统包括：3通道递交功能实体、监听信息提供实体和边界网关功能实体。该方法包括：将下一代网络中的边界网关功能实体与执法机构侧的3通道递交功能实体相连；监听信息提供实体将监听对象信息发送至边界网关功能实体；边界网关功能实体根据接收到的监听对象信息，将监听对象的媒体流发送至3通道递交功能实体。本发明能够实现在下一代网络中对从固定网络接入的用户进行合法监听的目的，极大地扩展了合法监听业务的应用范围，提高了下一代网络的业务服务质量。

一种在下一代网络中实现合法监听的方法和系统

技术领域

本发明涉及监听技术，特别是涉及一种在下一代网络（NGN）中针对从固定网络接入的用户实现合法监听的方法和系统。

发明背景

合法监听是指执法机构（LEA）经相应的授权机关批准，根据国家相关法律和公众通信网行业规范对公众通信网通信业务进行监听的执法行为。合法监听的基本实现过程为：执法机构侧合法监听的管理功能（ADMF）实体通过数据接口 X1_1 将监听数据发送至通信网络中的监听控制网元；监听控制网元接收到监听数据后对被监听对象进行监听，当监听到被监听对象的活动时，通过 X2 接口将被监听对象的监听相关信息发送至 2 通道递交功能（DF2）实体，并通过 X3 接口将被监听对象的媒体流发送至监听中心即 3 通道递交功能（DF3）实体。

NGN 网络是基于分组技术的融合型网络，它继承了原有固定网络的所有业务，同时也继承了移动网络的业务能力。在目前各标准组织研究的 NGN 网络中，重点研究的 NGN 网络的核心网是 IP 多媒体子系统（IMS）网络，IMS 网络可以同时为从固定网络接入的用户以及从移动网络接入的用户提供服务。

目前3GPP给出的标准中，在NGN中实现合法监听业务时，是由IMS网络中的监听控制网元3G GSN，包括GPRS网关支持节点（GGSN）和服务GPRS支持节点（SNSN），对监听对象进行监听，并在接收到监听对象的媒体流时，将该媒体流发送至执法机构侧的DF3实体。但是，IMS网络中的3G GSN包括GGSN和SNSN，是用户通过移动网络接入NGN

时所涉及的网络实体，也就是说，当用户从移动网络接入 NGN 时，该用户媒体流的传输会经过 3G GSN，这样，3G GSN 便可对所接收到的用户媒体流进行复制，并将所复制的媒体流发送至监听中心，从而实现对用户的监听。然而，IMS 网络中的 3G GSN 却不是用户通过固定网络接入 NGN 时所涉及的网络实体，也就是说，当用户从固定网络接入 NGN 时，该用户媒体流的传输不会经过 3G GSN，3G GSN 无法将从固定网络接入 NGN 的用户的媒体流发送至监听中心。而针对用户从固定网络接入的情况，目前也没有其它的合法监听媒体流的采集方案。

由此可见，在目前的 NGN 网络中，无法实现对从固定网络接入 NGN 的用户的监听，极大地限制了合法监听业务的应用范围，降低了 NGN 网络的业务服务质量。

发明内容

本发明的主要目的在于提供一种在下一代网络中实现合法监听的方法，本发明的另一目的在于提供一种在下一代网络中实现合法监听的系统，以便针对从固网接入下一代网络的用户实现合法监听。

为了达到上述目的，本发明的技术方案是这样实现的：

一种在下一代网络中实现合法监听的方法，将下一代网络中的边界网关功能实体与执法机构侧的 3 通道递交功能实体相连，该方法还包括：

A、监听信息提供实体将监听对象信息发送至边界网关功能实体；

B、边界网关功能实体根据接收到的监听对象信息，将对应于监听对象的媒体流发送至 3 通道递交功能实体。

一种在下一代网络中提供合法监听的系统，包括：3 通道递交功能实体，用于接收对应于监听对象的媒体流，并对所接收到的媒体流进行分析，实现监听，该系统还包括：监听信息提供实体和边界网关功能实

体，其中，

监听信息提供实体，用于将监听对象信息发送至边界网关功能实体；

边界网关功能实体，用于根据接收到的监听对象信息，将对应于监听对象的媒体流发送至 3 通道递交功能实体。

由此可见，本发明能够通过监听数据或对应于监听对象的媒体流描述信息来触发 BGF 实体对从固定网络接入的监听对象的媒体流进行复制，并将所复制的媒体流发送至 DF3 实体，从而实现了在 NGN 中对从固定网络接入的用户进行合法监听的目的，极大地扩展了合法监听业务的应用范围，提高了 NGN 网络的业务服务质量。

附图简要说明

图 1 是本发明系统的基本结构示意图。

图 2A1 是仅当 ADMF 实体作为监听信息提供实体时本发明系统的基本结构示意图。

图 2A2 是仅当 ADMF 实体作为监听信息提供实体时本发明系统的优化结构示意图。

图 2B 是当 ADMF 实体和 P-CSCF 实体共同作为监听信息提供实体时本发明系统的基本结构示意图。

图 2C 是当 NGN 网络中的监听控制网元实体作为监听信息提供实体时本发明系统的基本结构示意图。

图 3 是本发明实施例 1 的流程图。

图 4 是本发明实施例 2 的流程图。

图 5 是本发明实施例 3 的流程图。

图 6 是本发明实施例 4 的流程图。

实施本发明的方式

目前，欧洲电信标准协会（ETSI）下属 TISPAN（Telecommunications and Internet Converged Services and Protocols for Advanced Networking）组织在 NGN 网络中定义了资源和准入控制子系统（RACS），RACS 子系统定义了基于服务的策略决策功能（SPDF）实体、BGF 实体和其他的网元。其中，SPDF 实体与 IMS 网络中的管理功能（AF）实体即代理呼叫会话控制功能（P-CSCF）实体相连，BGF 实体与 SPDF 实体相连，并且，BGF 实体是一个 packet-to-packet 网关，位于从固定网络接入的用户的媒体流传输路径中。可见，当用户从固定网络接入 NGN 时，BGF 实体是可以获得用户的媒体流的，因此，可以利用 BGF 实体来实现对从固定网络接入 NGN 的用户的合法监听。针对这一特点，本发明提出了一种在 NGN 中实现合法监听的方法，其核心思想是：将 BGF 实体与 DF3 实体相连；监听信息提供实体将监听对象信息发送至 BGF 实体；BGF 实体根据接收到的监听对象信息，将对应于监听对象的媒体流发送至 DF3 实体。

在本发明中，所述的监听信息提供实体可以为执法机构侧的 ADMF 实体，此时，ADMF 实体将监听对象信息发送至 BGF 实体的过程可以是：将 BGF 实体作为监听控制网元，也就是说通过已有的 X1_1 接口将 ADMF 实体与 BGF 实体相连，这样，当需要对一个监听对象执行监听时，执法机构侧的 ADMF 实体直接将携带监听对象标识的监听数据作为所述的监听对象信息发送至 BGF 实体；或者，当需要对一个监听对象执行监听时，执法机构侧的 ADMF 实体首先将监听数据发送至现有的监听控制网元，该监听控制网元将 BGF 实体的标识发送至 ADMF 实体，ADMF 实体再根据接收到的 BGF 实体的标识将携带监听对象标识的监听数据或者是对应于监听对象的媒体流描述信息作为所述的监听对象

信息发送至 BGF 实体。

另外，当所述的监听信息提供实体为 ADMF 实体且 BGF 实体作为监听控制网元时，本发明还可以预先在 NGN 网络中设置一个监听数据处理功能实体；这样，ADMF 实体通过该监听数据处理功能实体的转发，实现上述的将监听数据发送至 BGF 实体的过程。

在本发明中，所述的监听信息提供实体还可以为 NGN 网络中现有的监听控制网元，此时，该现有的监听控制网元将监听对象信息发送至 BGF 实体的过程可以是：NGN 网络中现有的监听控制网元接收到 ADMF 实体发来的携带监听对象标识的监听数据后，将携带监听对象标识的监听数据或对应于监听对象的媒体流描述信息作为监听对象信息发送至 BGF 实体。

图 1 是本发明系统的基本结构示意图。参见图 1，本发明还提出了一种在 NGN 网络中实现合法监听的系统，该系统包括：监听信息提供实体、BGF 实体和 DF3 实体，其中，

监听信息提供实体，用于将监听对象信息发送至 BGF 实体；

BGF 实体，用于根据接收到的监听对象信息，将对应于监听对象的媒体流发送至 DF3 实体；

DF3 实体，用于接收对应于监听对象的媒体流，并对所接收到的媒体流进行分析，实现监听。

图 2A1 是当 ADMF 实体作为监听信息提供实体且 BGF 实体作为监听控制网元时本发明系统的基本结构示意图。参见图 2A1，在本发明系统中，所述的监听信息提供实体可以是 ADMF 实体，该 ADMF 实体可以与作为监听控制网元的 BGF 实体通过 X1_1 接口直接相连。

图 2A2 是当 ADMF 实体作为监听信息提供实体且 BGF 实体作为监听控制网元时本发明系统的优化结构示意图。参见图 2A2，当监听信息

提供实体为 ADMF 实体且 BGF 实体作为监听控制网元时，为了避免执法机构侧的 ADMF 实体与大量的 BGF 实体进行消息交互，从而减少 ADMF 实体的业务负荷量，较佳地，在本发明系统中，还可以进一步包括监听数据处理功能实体，ADMF 实体用于将监听数据发送至监听数据处理功能实体，该监听数据处理功能实体用于将接收到的监听数据发送至 BGF。

图 2B 是当 ADMF 实体作为监听信息提供实体且 BGF 实体不作为监听控制网元时本发明系统的基本结构示意图。参见图 2B，在本发明系统中，当所述的监听信息提供实体是 ADMF 实体，但 BGF 实体不作为监听控制网元，可以由现有的监听控制网元执行本发明系统中监听控制网元的功能，该现有的监听控制网元可以是合法监听应用服务器（LI-AS），或 P-CSCF 实体，或 S-CSCF 实体，该监听控制网元用于根据 ADMF 实体发来的携带监听对象标识的监听数据获取对应的 BGF 实体的标识，并将所获取的 BGF 实体的标识的对应于监听对象的媒体流描述信息发送至 ADMF 实体；ADMF 实体根据接收到的 BGF 实体的标识，将对应于监听对象的媒体流描述信息作为监听对象信息发送至 BGF 实体。

图 2C 是当 NGN 网络中的监听控制网元实体作为监听信息提供实体时本发明系统的基本结构示意图。参见图 2C，在本发明系统中，当所述的监听信息提供实体是监听控制网元时，该监听控制网元可以将 ADMF 实体发来的监听数据携带在消息中发送至 BGF 实体，也可以根据 ADMF 实体发来的携带监听对象标识的监听数据，将会话中对应于监听对象的媒体流描述信息携带在消息中发送至 BGF 实体。

为使本发明的目的、技术方案和优点更加清楚，下面结合附图及具体实施例对本发明作进一步地详细描述。

实施例 1：

图 3 是本发明实施例 1 的流程图。参见图 2A1 和图 3，在实施例 1 中，以执法机构侧的 ADMF 实体作为本发明中所述的监听信息提供实体，且 BGF 实体作为监听控制网元为例，在 NGN 网络中，本实施例针对从固定网络接入的用户实现合法监听的过程包括以下步骤：

步骤 301：预先通过 X3 接口将 NGN 网络中的 BGF 实体与执法机构侧的 DF3 实体相连。

步骤 302：预先通过现有的 X1_1 接口将执法机构侧的 ADMF 实体与 BGF 实体相连。

步骤 303：当需要对一个监听对象执行监听时，执法机构侧的 ADMF 实体通过 X1_1 接口将携带监听对象标识的监听数据直接发送至 BGF 实体。

这里以及以下所述的监听数据中还可以包括监听所需的其他相关信息，比如，ADMF 实体的标识、接收所监听媒体流的 DF3 实体的标识以及监听内容信息等。其中，所述的监听对象标识可以是监听对象的会话初始协议统一资源标识符（SIP URI）和电话统一资源定位符（TEL URL）。

通过上述步骤 302 至步骤 303 的过程，ADMF 实体将携带监听对象标识的监听数据发送至了 BGF 实体，从而使得 BGF 实体作为监听控制网元获取了监听数据。在本实施例中，还可以通过一个实体的转发使 BGF 实体作为监听控制网元获取监听数据，参见图 2A2，此时，本实施例预先在 NGN 网络中设置一个监听数据处理功能实体，并将所设置的监听数据处理功能实体分别与执法机构侧的 ADMF 实体和 BGF 实体相连，其中，所设置的监听数据处理功能实体通过 X1_1 接口与 ADMF 实体相连；这样，步骤 302 至步骤 303 的过程变为：当需要对一个监听对象执行监听时，执法机构侧的 ADMF 实体通过 X1_1 接口将携带监听对象标识的监听数据直接发送至监听数据处理功能实体；该监听数据处理

功能实体将接收到的携带监听对象标识的监听数据发送至 BGF 实体。其中，所设置的监听数据处理功能实体可以通过 Diameter 协议与 BGF 实体进行所述的交互过程。

步骤 304: BGF 实体保存所接收到的携带监听对象标识的监听数据。

步骤 305: P-CSCF 实体接收到会话建立请求（INVITE）后，将本次用户的标识发送至 SPDF 实体。

这里，P-CSCF 实体可以通过认证授权请求（AA-Request）消息将本次用户的标识发送至 SPDF 实体。并且，此处以及以下所述的本次用户标识可以是本次用户的 SIP URI 和 TEL URL。

步骤 306: SPDF 实体将本次用户的标识发送至 BGF 实体。

这里，由于 SPDF 实体与 BGF 实体之间通过 H.248 协议进行交互，因此，本发明可以预先扩展 H.248 协议消息，即在 H.248 协议消息中增加一个用户标识包，比如，所增加的用户标识包可以定义为如下的形式:

PackageID: normal int (如 0xCD)

Properties:

Subscriber Identifier:

PropertyID: SubscriberId (0x0001)

Description:定义用户标识"Subscriber Identifier", 用来描述相关的用户身份标识。

Type: string

Defined in: Local Control descriptor

Characteristics: Read/Write

Events: none

Statistics: none

Signals: none

Procedures: 媒体网关控制（MGC）可以在任何命令中指定相关用户

身份标识。

如：SubscriberId = abcdefg@ims.example.com，指示相关用户身份标识为 abcdefg@ims.example.com。

这样，在本步骤中，SPDF 实体可以将本次用户的标识携带在 H.248 协议消息中，比如 Add 消息中，所增加的用户标识包内，然后发送至 BGF 实体。

需要说明的是，在上述步骤 305 至步骤 306 中，P-CSCF 实体没有直接将本次用户标识发送至 BGF 实体，而是由 SPDF 实体通过扩展的携带用户标识包的 H.248 协议消息将本次用户标识发送至 BGF 实体。在实际的业务实现中，在上述步骤 305 至步骤 306 的过程中，也可以由 P-CSCF 实体通过扩展的携带用户标识包的 H.248 协议消息将本次用户标识发送至 BGF 实体，具体实现包括：P-CSCF 实体将本次用户标识携带在 H.248 协议消息中扩展的用户标识包内，直接发送至 BGF 实体；或者，P-CSCF 实体将本次用户标识携带在 H.248 协议消息中扩展的用户标识包内，首先发送至 SPDF 实体，该 SPDF 实体将所接收到的在扩展的用户标识包中携带本次用户标识的 H.248 协议消息透传至 BGF 实体。

步骤 307：BGF 实体根据本次用户的标识以及自身保存的携带用户标识的监听数据，判断本次用户是否为监听对象，如果是，则执行步骤 308，否则，执行现有的建立连接并传输媒体流的过程，结束当前流程。

这里，如果 BGF 实体接收到的是携带用户标识包的 H.248 协议消息比如 Add 消息，则 BGF 实体对该 Add 消息进行分析，从该 Add 消息的用户标识包中获取本次用户的标识。

步骤 308：BGF 实体分配合法监听的复制资源。

步骤 309：在本次会话的主被叫连接建立完成，主被叫用户实现通信后， BGF 实体利用所分配的合法监听复制资源对所接收到的对应于

本次用户的媒体流进行复制。

步骤 310：BGF 实体通过 X3 接口将所复制的媒体流发送至 DF3 实体。

步骤 311：DF3 实体对所接收到的媒体流进行分析，实现针对从固定网络接入 NGN 的监听对象的监听。

实施例 2:

图 4 是本发明实施例 2 的流程图。参见图 2B 和图 4，在实施例 2 中，以 ADMF 实体作为本发明中所述的监听信息提供实体，但 BGF 实体不作为监听控制网元为例，在 NGN 网络中，本发明针对从固定网络接入的用户实现合法监听的过程包括以下步骤：

步骤 401：预先通过 X3 接口将 NGN 网络中的 BGF 实体与执法机构侧的 DF3 实体相连。

步骤 402：当需要对一个监听对象执行监听时，执法机构侧的 ADMF 实体通过 X1_1 接口将携带监听对象标识的监听数据发送至现有的监听控制网元。

这里，P-CSCF 实体、S-CSCF 实体和 LI-AS 作为监听控制网元均可接收到携带监听对象标识的监听数据。为便于描述，以下以 P-CSCF 实体作为本实施例中也即图 2B 中的监听控制网元为例来说明本实施例的后续实现过程。

步骤 403：P-CSCF 实体保存携带监听对象标识的监听数据。

步骤 404：在本次会话建立过程中，P-CSCF 实体根据所保存的携带监听对象标识的监听数据和本次用户的标识，判断本次用户是否为监听对象，如果是，则执行步骤 405，否则，执行现有的建立连接并传输媒体流的过程，结束当前流程。

步骤 405：P-CSCF 实体将本次会话中，对应于监听对象的媒体流所

经过的 BGF 实体的标识发送至 ADMF 实体。

这里监听对象即为所述的本次用户。并且，在本步骤中，P-CSCF 实体可以通过执法机构侧的 DF2 实体将对应于监听对象的媒体流所经过的 BGF 实体的标识发送至 ADMF 实体。

步骤 406: ADMF 实体根据接收到的 BGF 实体的标识，将携带监听对象标识的监听数据发送至对应的 BGF 实体。

步骤 407: 该 BGF 实体根据接收到的携带监听对象标识的监听数据，对自身接收到的对应于监听对象的媒体流进行复制。

步骤 408: 该 BGF 实体根据接收到的携带监听对象标识的监听数据，将所复制的媒体流发送至 DF3 实体。

在上述步骤 405 中，P-CSCF 实体还可以进一步将本次会话中，对应于监听对象的媒体流描述信息发送至 ADMF 实体，这样，步骤 406 至步骤 408 的过程则为：ADMF 实体根据接收到的 BGF 实体的标识，将对应于监听对象的媒体流描述信息发送至对应的 BGF 实体；该 BGF 实体根据接收到的对应于监听对象的媒体流描述信息，对接收到的对应于监听对象的媒体流进行复制，并根据接收到的对应于监听对象的媒体流描述信息，将所复制的媒体流发送至 DF3 实体。其中，所述的对应于监听对象的媒体流描述信息包括: 对应于监听对象媒体流的源 IP 地址、目的 IP 地址、源端口号、目的端口号等。

步骤 409: DF3 实体对所接收到的媒体流进行分析，实现针对从固定网络接入 NGN 的监听对象的监听。

实施例 3:

在本实施例 3 中，由 NGN 网络中的监听控制网元作为本发明中所述的监听信息提供实体，且该监听控制网元通过在消息中携带监听数据触发 BGF 实体复制监听对象的媒体流。

图 5 是本发明实施例 3 的流程图。参见图 2C 和图 5，为便于描述，以 NGN 网络中的合法监听应用服务器（LI-AS）作为监听控制网元，并通过在消息中携带监听数据触发 BGF 实体复制监听对象的媒体流为例，本实施例针对从固定网络接入的用户实现合法监听的过程包括以下步骤：

步骤 501: 预先通过 X3 接口将 NGN 网络中的 BGF 实体与执法机构侧的 DF3 实体相连。

步骤 502: 预先扩展 SIP 协议消息、H.248 协议消息和 Diameter 协议消息，使其能够携带监听数据。

在本步骤中，在扩展所述的 SIP 协议消息时，可以在 SIP 协议消息中增加一个基于 XML 格式的应用类型，比如，所增加的基于 XML 格式的应用类型可以定义为如下的形式：

```
Content-type: application/interception-data+xml
<?xml version="1.0"?>
    <interception-data xmlns="urn:ietf:params:xml:ns:interception-data"
                       version="0" state="full"
                       entity="sip:alice@example.com">
      <monitor identity="abcd@example.com">
        <type>both</type>
        <df2addr>sip:df2@lea.com</df2addr>
        <df3addr>sip:df3@lea.com</df3addr>
      </monitor>
    </interception-data>
```

在上述基于 XML 格式的消息体中，给出当前监听对象身份标识为 abcd@example.com，并给出当前对用户监听需要输出监听相关信息和监听内容。同时给出了输出监听相关信息的地址为 df2@lea.com，输出监

听内容的地址为 df3@lea.com。

在本步骤中，在扩展 H.248 协议消息时，可以在 H.248 协议消息中增加一个监听数据包，比如，所增加的监听数据包可以定义为如下的形式：

监听数据包定义： (Lawful Interception Data Package)

PackageID: normal int (如 0xCE)

Properties:

Monitored Subscriber Identifier:

PropertyID: SubscriberId (0x0001)

Description:定义被监听对象用户身份标识" Monitored Subscriber Identifier", 用来描述被监听对象相关的用户身份标识。

Type: string

Defined in: Local Control descriptor

Characteristics: Read/Write

Monitor Type:

PropertyID: MonitorType (0x0002)

Description:定义被监听对象当前监听类型"Monitor Type", 用来描述被监听对象当前的监听类型。对没有显式该属性的认为是当前监听既不需要输出监听相关信息，也不需要输出通信内容。

Type: Enumeration

Possible Values:

"None" (0x0000) 无任何输出。

"IRI" (0x0001) 仅输出 IRI。

"CC" (0x0002) 仅输出 CC。

"Both" (0x0003) 输出 IRI 和 CC。

Default: " None " (0x0000) 无任何输出。

Defined in: Local Control descriptor

Characteristics: Read/Write

DF2 Address:

PropertyID: DF2Address (0x0003)

Description:定义被监听对象 IRI 输出的 DF2 地址"DF2 Address", 用来描述被监听对象监听相关信息输出的 DF2 地址。

Type: string

Defined in: Local Control descriptor

Characteristics: Read/Write

DF3 Address:

PropertyID: DF3Address (0x0004)

Description:定义被监听对象 CC 输出的 DF3 地址"DF3 Address", 用来描述被监听对象通信内容输出的 DF3 地址。

Type: string

Defined in: Local Control descriptor

Characteristics: Read/Write

Events: none

Statistics: none

Signals: none

Procedures: MGC 可以在任何命令中携带监听数据包指示该用户被监听和当前该用户的监听数据。

在本步骤中，在扩展所述的 Diameter 协议消息时，可以在 Diameter 协议消息中增加一个属性值对（AVP），比如，所增加的属性值对可以定义为如下的形式:

Attribute Name: Monitor-Data

AVP Code: 整型值，如 530，AVP 中建议携带"V"比特，建议携带"M"比特，表示该 AVP 是厂商专用的，是接收者必须识别的。可以进行端到

端安全加密。

Value Type: Grouped

该 AVP 格式定义如下:

AVP Format:

Globally-Unique-IP-Address ::= < AVP Header: xxx 13019 >

[Monitored-Subscriber-Identifier]

[Monitor-Type]

[Delivery-Function2-Address]

[Delivery-Function3-Address]

其中，Monitored-Subscriber-Identifier 描述当前被监听对象身份标识，Monitor-Type 描述当前对被监听对象的监听是否需要输出通信内容和监听相关信息。Delivery-Function2-Address 给出监听相关信息输出地址，Delivery-Function3-Address 给出监听内容输出地址。

步骤 503: 当需要对一个监听对象执行监听时，执法机构侧的 ADMF 实体通过 X1_1 接口将携带监听对象标识的监听数据发送至监听控制网元。

这里，P-CSCF 实体、S-CSCF 实体和 LI-AS 作为监听控制网元均可接收到携带监听对象标识的监听数据。

步骤 504: LI-AS 保存所接收到的携带监听对象标识的监听数据。

步骤 505: 在会话建立过程中，当 LI-AS 接收到会话建立请求时，LI-AS 根据自身保存的携带监听对象标识的监听数据和本次用户的标识，判断本次用户是否为监听对象，如果是，则执行步骤 506，否则，执行现有的建立会话连接实现通信的过程，结束当前流程。

步骤 506: LI-AS 将自身加入到本次会话的信令路由中，并将该会话建立请求发送至被叫用户。

步骤 507: 当 LI-AS 接收到被叫用户返回的响应消息时，LI-AS 在

SIP 协议的消息中携带自身所保存的携带监听对象标识的监听数据。

这里，LI-AS 可以利用在 SIP 协议的响应消息中所增加的基于 XML 格式的应用类型的消息体来携带自身所保存的监听数据。

步骤 508：LI-AS 将携带监听数据的 SIP 协议的响应消息发送至 P-CSCF 实体。

需要说明的是，上述步骤 504 至步骤 508 的过程中所涉及的 LI-AS 可以替换为 S-CSCF 实体。

步骤 509: P-CSCF 实体将携带监听数据的 Diameter 协议的消息发送至 SPDF 实体。

这里，P-CSCF 实体首先从接收到的 SIP 协议响应消息中所增加的基于 XML 格式的应用类型的消息体中获取监听数据，然后可以利用在 Diameter 协议响应消息中增加的属性值对来携带所获取的监听数据，并发送至 SPDF 实体。

步骤 510：SPDF 实体从所接收到的 Diameter 协议响应消息中获取监听数据，并将所获取的监听数据携带在 H.248 协议包中扩展的监听数据包中，然后发送至 BGF 实体。

步骤 511：BGF 实体解析 H.248 协议包中扩展的监听数据包，获取监听数据。

步骤 512：BGF 实体根据所获取的监听数据，复制对应于监听对象的媒体流，并通过 X3 接口将所复制的媒体流发送至 DF3 实体。

步骤 513：DF3 实体对所接收到的媒体流进行分析，实现针对从固定网络接入 NGN 的监听对象的监听。

在本实施例 3 中，也可以由 P-CSCF 实体首先执行构造携带监听数据的 Diameter 协议的消息，并将该消息通过 SPDF 实体发送至 BGF 实体，其具体实现与上述图 5 所示过程的原理相同，只是此时可以无需扩

展 SIP 消息。

实施例 4:

在本实施例 4 中，由 NGN 网络中的监听控制网元作为本发明中所述的监听信息提供实体，且该监听控制网元通过在消息中携带媒体流间拓扑描述来触发 BGF 实体复制监听对象的媒体流。

图 6 是本发明实施例 4 的流程图。参见图 2C 和图 6，为便于描述，以 NGN 网络中的 P-CSCF 实体作为监听控制网元，并通过在消息中携带媒体流间拓扑描述来触发 BGF 实体复制监听对象的媒体流为例，本实施例针对从固定网络接入的用户实现合法监听的过程包括以下步骤:

步骤 601: 预先通过 X3 接口将 NGN 网络中的 BGF 实体与执法机构侧的 DF3 实体相连。

步骤 602: 预先扩展 SIP 协议消息、H.248 协议消息和 Diameter 协议消息，使其能够携带对应于监听对象的媒体流描述信息。

在本步骤中，在扩展所述的 SIP 协议消息时，可以在 SIP 协议消息中增加一个基于 XML 格式的应用类型，通过该应用类型的消息体来携带对应于监听对象的媒体流描述信息。比如，所增加的基于 XML 格式的应用类型可以定义为如下的形式:

Content-type: application/session-topology+xml

```
<?xml version="1.0"?>
    <session-topology xmlns="urn:ietf:params:xml:ns:session-topology"
                      version="0" state="full"
                      entity="sip:alice@example.com">
      <session name="abcd@example.com">
        <copiedstream>
          <sourceaddr>[5555::1:2:3:4]:1357</sourceaddr>
          <destinationaddr>[5555::a:b:c:d]:7531</destinationaddr>
```

```
                <protocol>RTP</protocol>
        </copiedstream>
        <direction>upstream</direction>
            </session>
         </interception-data>
```

在上述 XML 消息体中，给出当前呼叫需要拷贝从[5555::1:2:3:4]:1357 到[5555::a:b:c:d]:7531 的上行（upstream）媒体流。

在本步骤中，使用标准的 H.248 拓扑描述方式就可以描述在一个上下文(Context)中各个端点间的拓扑关系，具体实施方式可以参考 3GPP 33107 附录 D，这里不再赘述。同样，也可以扩展所述的 H.248 协议消息，使其能够携带对应于监听对象的媒体流描述信息时，可以利用目前已有的扩展 H.248 监听包的方式，其核心思想是:

1、定义监听包标识;

2、定义监听包媒体复制指示属性"Interception indication"，用来指定端点的复制从属属性。指示该终端是 slave 还是 common，对没有显式该属性的认为是与复制无关的终端，一律为 common。

3、定义监听端点从属关系"Master termination"， 用来对 slave 终端保存其需要复制端点的终端标识（简称 Master 端点，其媒体复制指示属性为 common），Master termination 对 slave 端点有效，类型为长度为 8 个字节的字符串。

4、定义监听端点复制模式"Interception mode"，取值 "上行流"， "下行流" 和"合并流"。用来表达 slave 终端与被复制端点的连接方式，是复制原端点的上行媒体还是下行媒体或者是上下行混合媒体。该属性对 slave 端点有效。

并且，当处于同一个 context 中的某一（多）个端点被指示属性为

slave，并指定其 master 端点和复制模式，slave 端点就从指定 master 端点复制相应流向的数据包。

在本步骤中，在扩展所述的 Diameter 协议消息，使其能够携带对应于监听对象的媒体流描述信息时，可以在 Diameter 协议消息中增加一个属性值对（AVP），比如，所增加的属性值对可以定义为如下的形式：

Attribute Name: Stream-Copied

AVP Code: 整型值，如 531，AVP 中建议携带"V"比特，建议携带"M"比特，表示该 AVP 是厂商专用的，是接收者必须识别的。可以进行端到端安全加密。

Value Type: Grouped

该 AVP 格式定义如下：

AVP Format:

Globally-Unique-IP-Address ::= < AVP Header: xxx 13019 >

[Media-Stream-Description]

[Copy-Direction]

其中，Media-Stream-Description 描述需要拷贝的媒体流信息，如，可以在 Media-Stream-Description 中给出需要拷贝的媒体流源 IP 地址、目的 IP 地址、源端口号、目的端口号和协议类型等。Copy-Direction 描述需要拷贝的媒体流方向。如可以使用 Copy-Direction 描述当前仅拷贝从源 IP 地址到目的 IP 地址方向的媒体流。

步骤 603：当需要对一个监听对象执行监听时，执法机构侧的 ADMF 实体通过 X1_1 接口将携带监听对象标识的监听数据发送至监听控制网元 P-CSCF 实体。

步骤 604：P-CSCF 实体保存所接收到的携带监听对象标识的监听数据。

步骤 605：在会话建立过程中，P-CSCF 实体根据所保存的携带监听对象标识的监听数据和本次用户的标识，判断本次用户是否为监听对象，如果是，则执行步骤 606，否则，执行现有的建立连接并传输媒体流的过程，结束当前流程。

步骤 606：P-CSCF 实体将本次会话中对应于监听对象的媒体流描述信息携带在 Diameter 协议的响应消息中发送至 SPDF 实体。

这里，根据步骤 602 中扩展 Diameter 协议消息的过程，P-CSCF 实体可以利用在 Diameter 协议响应消息中增加的属性值对来携带对应于监听对象的媒体流描述信息。

步骤 607：SPDF 实体将本次会话中对应于监听对象的媒体流描述信息携带在 H.248 协议的响应消息中发送至 BGF 实体。

这里，根据步骤 602 中扩展 H.248 协议消息的过程，SPDF 实体可以利用在 H.248 协议响应消息中增加的监听包来携带对应于监听对象的媒体流描述信息。

步骤 608：BGF 实体从所接收到的响应消息中获取本次会话中对应于监听对象的媒体流描述信息。

步骤 609：BGF 实体根据所获取的对应于监听对象的媒体流描述信息，复制对应于监听对象的媒体流，并通过 X3 接口将所复制的媒体流发送至 DF3 实体。

步骤 610：DF3 实体对所接收到的媒体流进行分析，实现针对从固定网络接入 NGN 的监听对象的监听。

在本实施例 4 中，是由 P-CSCF 实体首先构造携带对应于监听对象的媒体流描述信息的消息，并将该消息通过 SPDF 实体发送至 BGF 实体。在实际的业务实现中，也可以由 LI-AS 或 S-CSCF 实体利用所扩展的 SIP 协议的消息来首先构造携带对应于监听对象的媒体流描述信息的消息，

并将该消息通过P-CSCF实体和SPDF实体发送至BGF实体，其具体实现过程与上述图6所示过程的原理相同。

在本发明中，还可以通过上述各实施例的方法将ADMF实体发出的查询命令和合法监听去激活命令等发送至BGF实体，从而触发BGF实体执行对应的查询监听对象相关属性和取消监听等操作。

在本发明中，所述的本次用户可以是本次会话中的主叫用户和/或被叫用户。

在本发明中，所述的BGF实体可以是提供用户终端与接入网连接的接入边界网关功能（A-BGF）实体，也可以是提供接入网与核心网间连接的核心边界网关功能（C-BGF）实体。

总之，以上所述仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权利要求书

1、一种在下一代网络中实现合法监听的方法，其特征在于，将下一代网络中的边界网关功能实体与执法机构侧的 3 通道递交功能实体相连，该方法还包括:

A、监听信息提供实体将监听对象信息发送至边界网关功能实体;

B、边界网关功能实体根据接收到的监听对象信息，将对应于监听对象的媒体流发送至 3 通道递交功能实体。

2、根据权利要求 1 所述的方法，其特征在于，所述监听信息提供实体为执法机构侧的管理功能实体。

3、根据权利要求 2 所述的方法，其特征在于，该方法进一步包括:在下一代网络中设置监听数据处理功能实体，并将所设置的监听数据处理功能实体分别与管理功能实体和边界网关功能实体相连;

所述监听对象信息为携带监听对象标识的监听数据;

所述步骤 A 包括: 管理功能实体将携带监听对象标识的监听数据发送至监听数据处理功能实体，该监听数据处理功能实体将接收到的携带监听对象标识的监听数据发送至边界网关功能实体。

4、根据权利要求 3 所述的方法，其特征在于，在步骤 A 与步骤 B 之间进一步包括:

A11、在本次会话建立过程中，将本次用户的标识发送至边界网关功能实体;

A12、边界网关功能实体根据本次用户的标识和携带监听对象标识的监听数据判断本次用户是否为监听对象，如果是，则执行步骤 B。

5、根据权利要求 4 所述的方法，其特征在于，该方法进一步包括:在 H.248 协议消息中增加用户标识包;

在步骤 A11 中，所述将本次用户的标识发送至边界网关功能实体的步骤包括：将本次用户的标识携带在 H.248 协议消息中所增加的用户标识包内发送至边界网关功能实体；

在步骤 A12 中，在执行所述的判断之前，进一步包括：边界网关功能实体从所接收到的 H.248 协议消息中所增加的用户标识包内获取所述的本次用户的标识。

6、根据权利要求 5 所述的方法，其特征在于，在步骤 A11 中，

由代理呼叫会话控制功能实体在接收到本次用户发来的会话建立请求时，执行所述的携带和发送的步骤；

或者，由代理呼叫会话控制功能实体将接收到的会话建立请求中的本次用户的标识发送至基于服务的策略决策功能实体，并由基于服务的策略决策功能实体执行所述的携带和发送的步骤。

7、根据权利要求 2 所述的方法，其特征在于，所述步骤 A 包括：

A21、执法机构侧的管理功能实体将携带监听对象标识的监听数据发送至现有的监听控制网元，该监听控制网元保存所接收到的携带监听对象标识的监听数据；

A22、在本次会话建立过程中，所述监听控制网元根据所保存的携带监听对象标识的监听数据和本次用户的标识，判断本次用户是否为监听对象，如果是，则执行步骤 A23；

A23、所述监听控制网元将本次会话中对应于监听对象的媒体流所经过的边界网关功能实体的标识发送至执法机构侧的管理功能实体；

A24、执法机构侧的管理功能实体根据接收到的边界网关功能实体的标识，将监听对象信息发送至边界网关功能实体。

8、根据权利要求 7 所述的方法，其特征在于，所述监听对象信息为携带监听对象标识的监听数据。

9、根据权利要求 7 所述的方法，其特征在于，所述步骤 A23 进一步包括：监听控制网元将本次会话中对应于监听对象的媒体流描述信息发送至执法机构侧的管理功能实体；

所述监听对象信息为对应于监听对象的媒体流描述信息。

10、根据权利要求 1 所述的方法，其特征在于，所述监听信息提供实体为现有的监听控制网元。

11、根据权利要求 10 所述的方法，其特征在于，该方法进一步包括：扩展 H.248 协议消息和 Diameter 协议消息；

所述监听控制网元为代理呼叫会话控制功能实体；

在步骤 A 之前进一步包括：执法机构侧的管理功能实体将携带监听对象标识的监听数据发送至所述代理呼叫会话控制功能实体；

所述步骤 A 包括：

A31、在本次会话建立过程中，所述代理呼叫会话控制功能实体根据所接收到的携带监听对象标识的监听数据和本次用户的标识，判断本次用户是否为监听对象，如果是，则执行步骤 A32；

A32、所述代理呼叫会话控制功能实体通过所扩展的 Diameter 协议消息将监听对象信息发送至基于服务的策略决策功能实体；

A33、基于服务的策略决策功能实体通过所扩展的 H.248 协议消息将监听对象信息发送至边界网关功能实体。

12、根据权利要求 10 所述的方法，其特征在于，该方法进一步包括：扩展 H.248 协议消息、Diameter 协议消息和会话初始协议 SIP 消息；

在步骤 A 之前进一步包括：接收执法机构侧的管理功能实体发来的携带监听对象标识的监听数据；

所述步骤 A 包括：

A41、在本次会话建立过程中，根据所接收到的携带监听对象标识

的监听数据和本次用户的标识，判断本次用户是否为监听对象，如果是，则执行步骤 A42;

A42、通过所扩展的 SIP 消息将监听对象信息发送至代理呼叫会话控制功能实体;

A43、代理呼叫会话控制功能实体通过所扩展的 Diameter 协议消息将监听对象信息发送至基于服务的策略决策功能实体;

A44、基于服务的策略决策功能实体通过所扩展的 H.248 协议消息将监听对象信息发送至边界网关功能实体。

13、根据权利要求 12 所述的方法，其特征在于，由合法监听应用服务器或服务呼叫会话控制功能实体执行所述的接收监听数据、判断以及通过所扩展的 SIP 消息将监听对象信息发送至代理呼叫会话控制功能实体的步骤。

14、根据权利要求 11、12 或 13 所述的方法，其特征在于，所述监听对象信息为携带监听对象标识的监听数据，或对应于监听对象的媒体流描述信息。

15、根据权利要求 11、12 或 13 所述的方法，其特征在于，所述扩展 H.248 协议消息的步骤包括：在 H.248 协议消息中增加一个监听数据包;

所述通过所扩展的 H.248 协议消息将监听对象信息发送至边界网关功能实体的步骤包括：基于服务的策略决策功能实体将监听对象信息携带在 H.248 协议消息中所增加的监听数据包内，然后将该 H.248 协议消息发送至边界网关功能实体。

16、根据权利要求 11、12 或 13 所述的方法，其特征在于，所述扩展 Diameter 协议消息的步骤包括:在 Diameter 协议消息中增加一个属性值对 AVP;

所述通过所扩展的Diameter协议消息将监听对象信息发送至基于服务的策略决策功能实体的步骤包括：将监听对象信息携带在Diameter协议消息中所增加的属性值对 AVP 内，然后将该 Diameter 协议消息发送至基于服务的策略决策功能实体。

17、根据权利要求 12 所述的方法，其特征在于，所述扩展 SIP 协议消息的步骤包括：在 SIP 协议消息中增加一个基于可扩展标记语言 XML 格式的应用类型；

所述步骤 A42 包括：将监听对象信息携带在 SIP 消息中所增加的基于 XML 格式应用类型的消息体内，然后将该 SIP 消息发送至代理呼叫会话控制功能实体。

18、根据权利要求 1 所述的方法，其特征在于，所述边界网关功能实体为提供用户终端与接入网连接的接入边界网关功能 A-BGF 实体，或提供接入网与核心网间连接的核心边界网关功能 C-BGF 实体。

19、一种在下一代网络中提供合法监听的系统，包括：3 通道递交功能实体，用于接收对应于监听对象的媒体流，并对所接收到的媒体流进行分析，实现监听，其特征在于，该系统还包括：监听信息提供实体和边界网关功能实体，其中，

监听信息提供实体，用于将监听对象信息发送至边界网关功能实体；

边界网关功能实体，用于根据接收到的监听对象信息，将对应于监听对象的媒体流发送至 3 通道递交功能实体。

20、根据权利要求 19 所述的系统，其特征在于，所述监听信息提供实体为执法机构侧的管理功能实体。

21、根据权利要求 20 所述的系统，其特征在于，所述执法机构侧的管理功能实体通过 X1_1 接口与所述边界网关功能实体直接相连。

22、根据权利要求 20 所述的系统，其特征在于，该系统进一步包括

监听数据处理功能实体，用于通过 X1_1 接口接收执法机构侧的管理功能实体发来的携带监听对象标识的监听数据，并将该携带监听对象标识的监听数据发送至边界网关功能实体；

执法机构侧的管理功能实体，用于通过 X1_1 接口将携带监听对象标识的监听数据发送至监听数据处理功能实体。

23、根据权利要求 20 所述的系统，其特征在于，该系统进一步包括：现有的监听控制网元，用于接收执法机构侧的管理功能实体发来的携带监听对象标识的监听数据，根据该监听数据获取监听对象的媒体流所经过的边界网关功能实体的标识，并将所获取的边界网关功能实体的标识发送至执法机构侧的管理功能实体；

所述执法机构侧的管理功能实体，用于根据接收到的边界网关功能实体的标识，将监听对象信息发送至边界网关功能实体。

24、根据权利要求 19 所述的系统，其特征在于，所述监听信息提供实体为现有的监听控制网元，用于根据执法机构侧的管理功能实体发来的携带监听对象标识的监听数据，获取对应于监听对象的媒体流描述信息，并发送至边界网关功能实体，或直接将该携带监听对象标识的监听数据发送至边界网关功能实体；

所述边界网关功能实体，用于将接收到的对应于监听对象的媒体流描述信息或携带监听对象标识的监听数据发送至 3 通道递交功能实体。


监听信息提供实体
BGF实体
X3接口
DF3实体

图 1


ADMF实体
X1_1接口
BGF实体
X3接口
DF3实体

图 2A1

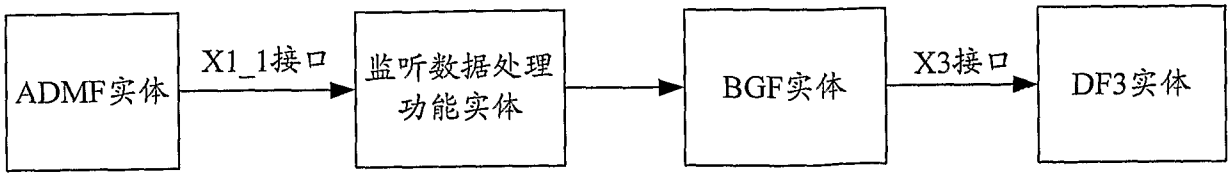

ADMF实体
X1_1接口
监听数据处理功能实体
BGF实体
X3接口
DF3实体

图 2A2

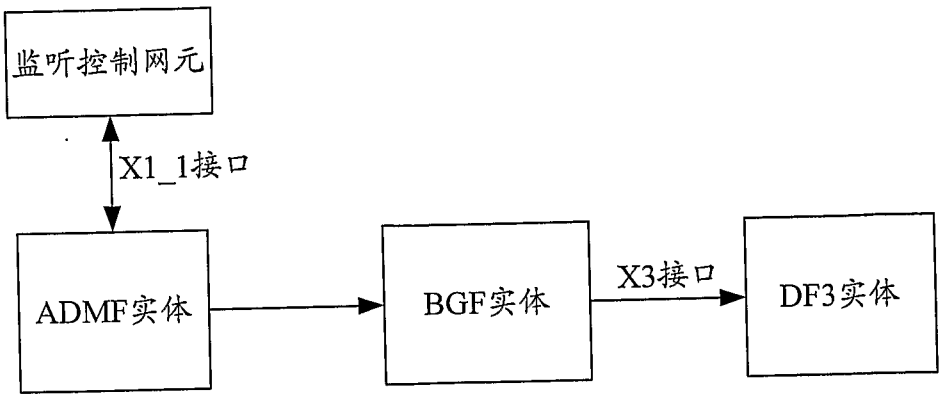

监听控制网元
X1_1接口
ADMF实体
BGF实体
X3接口
DF3实体

图 2B

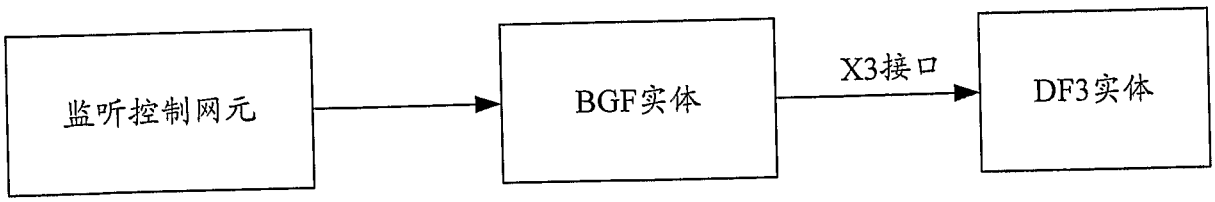

监听控制网元
BGF实体
X3接口
DF3实体

图 2C

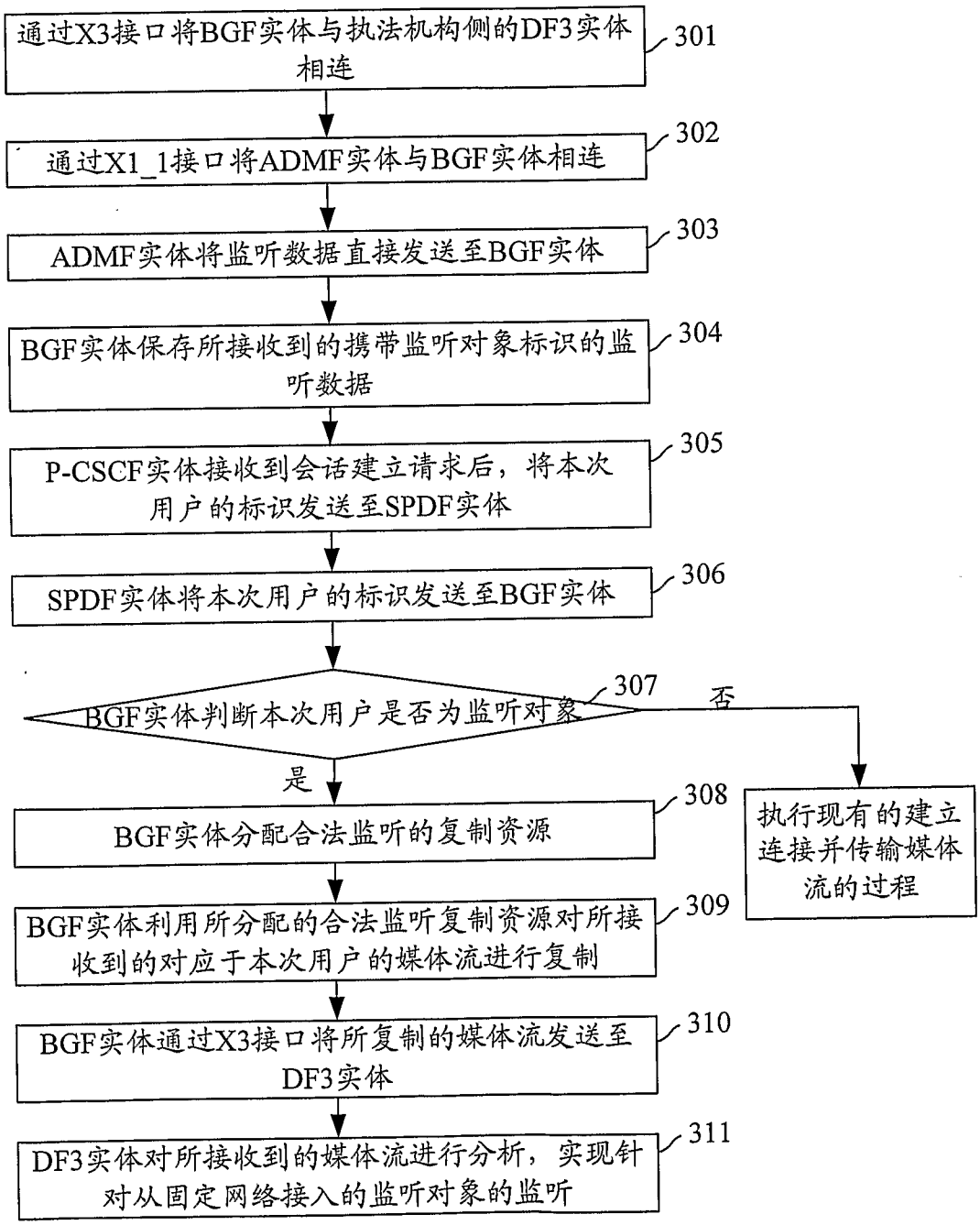

通过X3接口将BGF实体与执法机构侧的DF3实体相连
301
通过X1_1接口将ADMF实体与BGF实体相连
302
ADMF实体将监听数据直接发送至BGF实体
303
BGF实体保存所接收到的携带监听对象标识的监听数据
304
P-CSCF实体接收到会话建立请求后，将本次用户的标识发送至SPDF实体
305
SPDF实体将本次用户的标识发送至BGF实体
306
BGF实体判断本次用户是否为监听对象
307
否
是
BGF实体分配合法监听的复制资源
308
执行现有的建立连接并传输媒体流的过程
BGF实体利用所分配的合法监听复制资源对所接收到的对应于本次用户的媒体流进行复制
309
BGF实体通过X3接口将所复制的媒体流发送至DF3实体
310
DF3实体对所接收到的媒体流进行分析，实现针对从固定网络接入的监听对象的监听
311

图 3

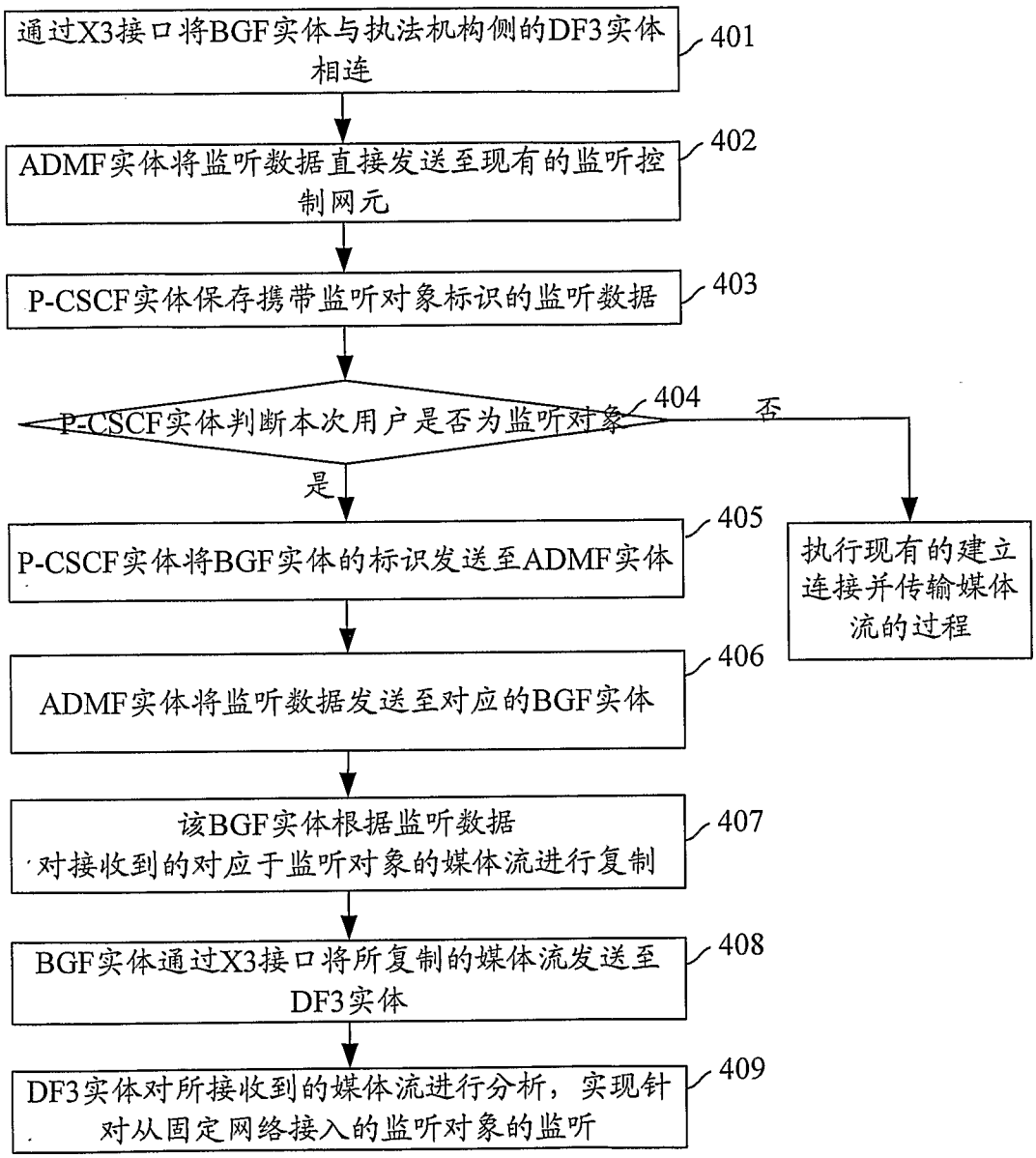

通过X3接口将BGF实体与执法机构侧的DF3实体相连
401
ADMF实体将监听数据直接发送至现有的监听控制网元
402
P-CSCF实体保存携带监听对象标识的监听数据
403
P-CSCF实体判断本次用户是否为监听对象
404
否
是
P-CSCF实体将BGF实体的标识发送至ADMF实体
405
执行现有的建立连接并传输媒体流的过程
ADMF实体将监听数据发送至对应的BGF实体
406
该BGF实体根据监听数据对接收到的对应于监听对象的媒体流进行复制
407
BGF实体通过X3接口将所复制的媒体流发送至DF3实体
408
DF3实体对所接收到的媒体流进行分析，实现针对从固定网络接入的监听对象的监听
409

图 4

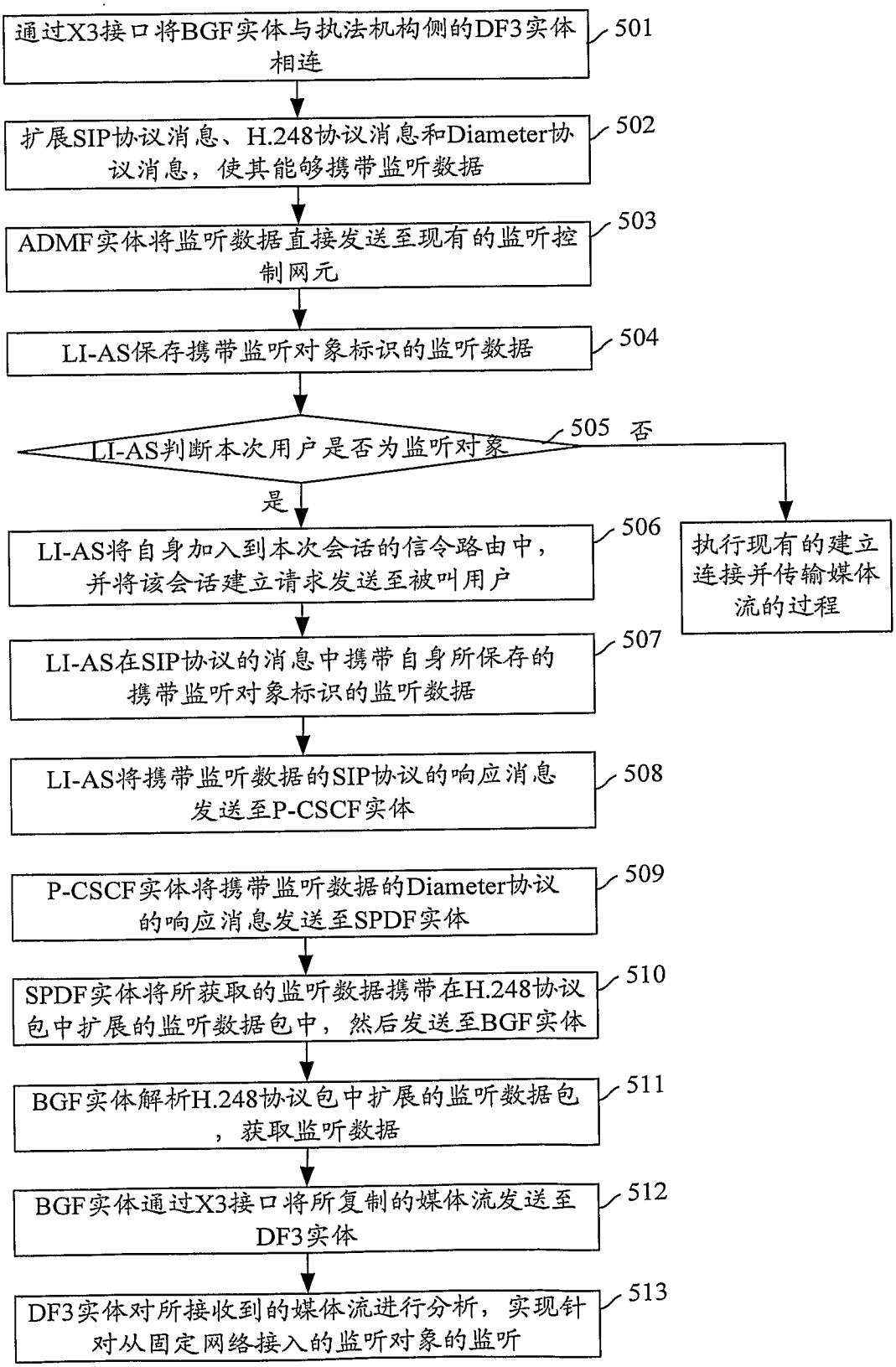

通过X3接口将BGF实体与执法机构侧的DF3实体相连
501
扩展SIP协议消息、H.248协议消息和Diameter协议消息，使其能够携带监听数据
502
ADMF实体将监听数据直接发送至现有的监听控制网元
503
LI-AS保存携带监听对象标识的监听数据
504
LI-AS判断本次用户是否为监听对象
505
否
是
执行现有的建立连接并传输媒体流的过程
LI-AS将自身加入到本次会话的信令路由中，并将该会话建立请求发送至被叫用户
506
LI-AS在SIP协议的消息中携带自身所保存的携带监听对象标识的监听数据
507
LI-AS将携带监听数据的SIP协议的响应消息发送至P-CSCF实体
508
P-CSCF实体将携带监听数据的Diameter协议的响应消息发送至SPDF实体
509
SPDF实体将所获取的监听数据携带在H.248协议包中扩展的监听数据包中，然后发送至BGF实体
510
BGF实体解析H.248协议包中扩展的监听数据包，获取监听数据
511
BGF实体通过X3接口将所复制的媒体流发送至DF3实体
512
DF3实体对所接收到的媒体流进行分析，实现针对从固定网络接入的监听对象的监听
513

图 5

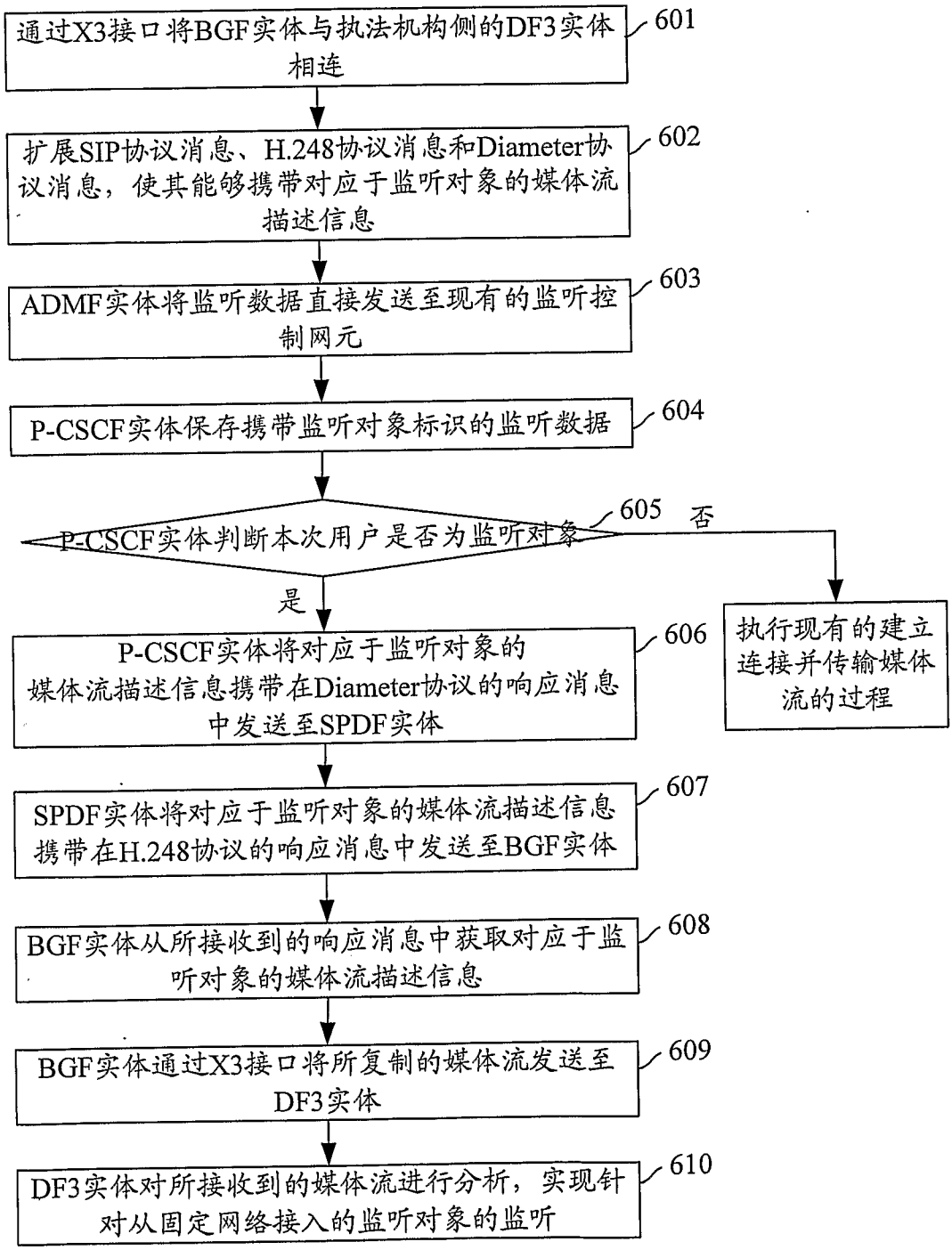

通过X3接口将BGF实体与执法机构侧的DF3实体相连
601
扩展SIP协议消息、H.248协议消息和Diameter协议消息，使其能够携带对应于监听对象的媒体流描述信息
602
ADMF实体将监听数据直接发送至现有的监听控制网元
603
P-CSCF实体保存携带监听对象标识的监听数据
604
P-CSCF实体判断本次用户是否为监听对象
605
否
是
执行现有的建立连接并传输媒体流的过程
P-CSCF实体将对应于监听对象的媒体流描述信息携带在Diameter协议的响应消息中发送至SPDF实体
606
SPDF实体将对应于监听对象的媒体流描述信息携带在H.248协议的响应消息中发送至BGF实体
607
BGF实体从所接收到的响应消息中获取对应于监听对象的媒体流描述信息
608
BGF实体通过X3接口将所复制的媒体流发送至DF3实体
609
DF3实体对所接收到的媒体流进行分析，实现针对从固定网络接入的监听对象的监听
610

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/000192

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/24(2007.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, PAJ: LISTEN GATEWAY LEGAL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN1691601A (HUAWEI TECH CO LTD), 02 November 2005 (02.11.2005), description, page 5, line 5-line 15	1-24
A	CN1509015A (HUAWEI TECH CO LTD),30 June 2004 (30.06.2004), the whole document.	1-24
A	CN1684425A (HUAWEI TECH CO LTD), 19 October 2005(19.10.2005), the whole document.	1-24

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 April 2007 (17.04.2007)	**24 May 2007 (24.05.2007)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer Leilianhong Telephone No. (86-10)62086065

Form PCT/ISA /210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2007/000192

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN1691601A	02. 11. 2005	None	
CN1509015A	30. 06. 2004	None	
CN1684425A	19. 10. 2005	None	

国际检索报告

国际申请号
PCT/CN2007/000192

A. 主题的分类

H04L12/24(2007.01) i

按照国际专利分类表(IPC)或者同时按照国家分类和 IPC 两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,CNKI, WPI, EPODOC, PAJ: 监听 网关 合法 LISTEN GATEWAY LEGAL

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN1691601A(华为技术有限公司)，02.11 月 2005（02.11.2005），说明书第 5 页第 5 行－第 15 行	1-24
A	CN1509015A（华为技术有限公司）30.6 月 2004（30.06.2004），全文	1-24
A	CN1684425A（华为技术有限公司），19.10 月 2005（19.10.2005），全文	1-24

☐ 其余文件在 C 栏的续页中列出。　　☒ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
17.4 月 2007（17.04.2007）	**24.5 月 2007 (24.05.2007)**
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路 6 号 100088 传真号： (86-10)62019451	受权官员 雷连虹 电话号码：(86-10) **62086065**

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2007/000192

检索报告中引用的专利文件	公布日期	同族专利	公布日期
CN1691601A	02.11.2005	无	
CN1509015A	30.06.2004	无	
CN1684425A	19.10.2005	无	