

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04Q 3/00 (2006.01)

H04M 3/22 (2006.01)



[12] 发明专利说明书

专利号 ZL 02806932.3

[45] 授权公告日 2007年3月14日

[11] 授权公告号 CN 1305321C

[22] 申请日 2002.3.7 [21] 申请号 02806932.3

[30] 优先权

[32] 2001.3.21 [33] EP [31] 01107062.0

[86] 国际申请 PCT/EP2002/002525 2002.3.7

[87] 国际公布 WO2002/078364 德 2002.10.3

[85] 进入国家阶段日期 2003.9.19

[73] 专利权人 西门子公司

地址 德国慕尼黑

[72] 发明人 赫尔穆特·斯迪弗特

诺贝特·克罗伊施

[56] 参考文献

US5923738A 1999.7.13

CN1220808A 1999.6.23

CN1209699A 1999.3.3

CN1166908A 1997.12.3

EP1018844A1 2000.7.12

审查员 赵晶晶

[74] 专利代理机构 中国国际贸易促进委员会专利
商标事务所

代理人 李 勇

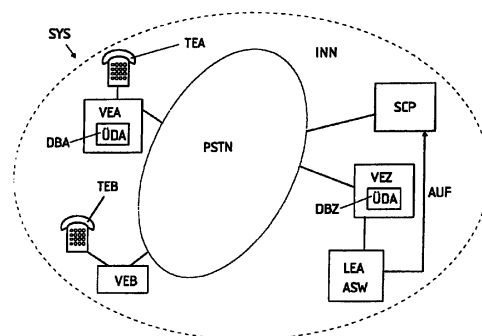
权利要求书 3 页 说明书 7 页 附图 1 页

[54] 发明名称

管理监控数据的方法

[57] 摘要

用于管理监控数据 (ü DA) 的方法和通信系统 (SYS)，所述监控数据用于利用智能网 (INN) 中与通信终端设备相应的本地交换节点 (VEA) 来监控电信终端设备 (TEA)，其中监控数据 (ü DA) 在智能网中所选出的交换节点 (VEZ) 中进行集中管理，并应请求传输到本地交换节点 (VEA)，本地交换节点借助于监控数据 (ü DA) 对电信终端设备 (TEA) 进行监控。



1. 管理监控数据 (ÜDA) 的方法, 所述监控数据用于利用智能网(INN)中与电信终端设备相应的本地交换节点 (VEA) 来对电信终端设备(TEA)进行监控, 其特征在于, 监控数据 (ÜDA) 在智能网中所选出的交换节点 (VEZ) 中进行集中管理, 且这些数据应请求被传输到本地交换节点 (VEA), 本地交换节点借助于监控数据(ÜDA)对电信终端设备(TEA)进行监控。

2. 如权利要求 1 所述的方法, 其特征在于, 在所选出的交换节点 (VEZ) 中对监控数据的集中管理是借助于数据库 (DBZ) 来进行的。

3. 如权利要求 1 或 2 所述的方法, 其特征在于, 在与其它电信终端设备(TEB)建立 IN 连接时, 传输监控数据 (ÜDA) 的请求(ANF)是由本地交换节点 (VEA) 产生并传输给所选出的交换节点 (VEZ)。

4. 如权利要求 1 所述的方法, 其特征在于, 在激活受监控的电信终端设备(TEA)时, 传输监控数据 (ÜDA) 的请求(ANF)是由本地交换节点 (VEA) 产生并传输到所选出的交换节点 (VEZ)。

5. 如权利要求 1 所述的方法, 其特征在于, 监控数据 (ÜDA) 的传输是根据 TCAP 协议实现的。

6. 如权利要求 1 所述的方法, 其特征在于, 在监控过程中, 所传输的监控数据 (ÜDA) 被存储在本地交换节点 (VEA) 中, 并在完成监控过程之后被清除。

7. 如权利要求 1 所述的方法, 其特征在于, 设置了中央管理单元 (SCP), 它监控是否应该在受监控的电信终端设备 (TEA) 的参与下建立连接, 和/或是否激活了受监控的电信终端设备 (TEA)。

8. 如权利要求 7 所述的方法, 其特征在于, 对监控电信终端设备 (TEA) 的监控请求 (AUF) 被记录在中央管理单元 (SCP) 中。

9. 如权利要求 7 或 8 所述的方法, 其特征在于, 当初始化连接

建立和/或激活电信终端设备 (TEA) 时, 在本地交换节点 (VEA) 与中央管理单元 (SCP) 之间交换通知数据 (BE1, BE2)。

10. 如权利要求 9 所述的方法, 其特征在于, 在中央管理单元 (SCP) 和本地交换节点 (VEA) 之间交换通知数据 (BE1, BE2) 是通过 INAP 接口实现的。

11. 如权利要求 8 所述的方法, 其特征在于, 监控请求 (AUF) 包含与受监控的电信终端设备相应的 IN 地址和/或 E.164 呼叫号。

12. 如权利要求 1 所述的方法, 其特征在于, 监控的结果数据 (EDA) 从本地交换节点 (VEA) 传输到一个分析单元 (ASW)。

13. 用于管理监控数据 (ÜDA) 的电信系统 (SYS), 所述监控数据用于利用智能网 (INN) 中与电信终端设备相应的本地交换节点 (VEA) 来对电信终端设备 (TEA) 进行监控, 其特征在于, 设置了用于集中管理监控数据 (ÜDA) 的智能网 (INN) 中选出的交换节点 (VEZ), 这些数据应请求被传输到本地交换节点 (VEA), 本地交换节点借助于监控数据 (ÜDA) 对电信终端设备 (TEA) 进行监控。

14. 如权利要求 13 所述的电信系统, 其特征在于, 所选出的交换节点 (VEZ) 具有用于管理监控数据的数据库 (DBZ)。

15. 如权利要求 13 或 14 所述的电信系统, 其特征在于, 当与其它电信节点 (TEB) 建立 IN 连接, 和/或激活受监控的电信终端设备 (TEA) 时, 本地交换节点 (VEA) 被设置用于产生传输监控数据 (ÜDA) 的请求 (ANF), 并将其传输到所选出的交换节点 (VEZ)。

16. 如权利要求 13 所述的电信系统, 其特征在于, 该系统这样来设置: 使得监控数据 (ÜDA) 根据 TCAP 协议来传输。

17. 如权利要求 13 所述的电信系统, 其特征在于, 在监控过程 (ÜWV) 中, 本地交换节点 (VEA) 被设置用来存储接收到的监控数据, 并在完成监控过程之后再将该数据清除。

18. 如权利要求 13 所述的电信系统，其特征在于，设置了中央管理单元（SCP），它用于监控是否借助于受监控的电信终端设备（TEA）来建立 IN 连接，和/或是否激活了电信终端设备。

19. 如权利要求 18 所述的电信系统，其特征在于，该系统这样来设置：如果应该建立 IN 电信连接，和/或完成了激活，则在本地交换节点（VEA）与中央管理单元（SCP）之间交换通知数据（BE1，BE2）。

20. 如权利要求 19 所述的电信系统，其特征在于，为了在中央管理单元（SCP）与本地交换节点（VEA）之间交换通知数据（BE1，BE2），该系统具有 INAP 接口。

21. 如权利要求 18 所述的电信系统，其特征在于，中央管理单元（SCP）被设置用于接受监控请求（AUF）。

22. 如权利要求 21 所述的电信系统，其特征在于，监控请求（AUF）包含与受监控的电信终端设备相应的 IN 地址和/或 E.164 呼叫号。

23. 如权利要求 13 所述的电信系统，其特征在于，监控的结果数据（EDA）从本地交换节点（VEA）传输到分析单元（ASW）。

管理监控数据的方法

本发明涉及一种管理监控数据的方法，所述监控数据用于利用智能网中的与电信终端设备相应的本地交换节点对电信终端设备进行监控。

此外本发明还涉及一种用于管理监控数据的电信系统，所述监控数据用于利用智能网中的与电信终端设备相应的本地交换节点对电信终端设备进行监控。

智能网简称 IN，它涉及到一个网络概念，利用它可以提供成本更低的电信业务。智能网并不是特殊的物理网络平台，而是一种面向业务的结构体系，它建立在现有网络结构（如 PSTN 网）的基础上，并且具备附加的性能特征。此外，性能特征的管理是在 IN 集中进行的。

“业务控制点”作为 IN 中的业务控制中心而起作用，在此 IN 中所有网络成员都对应于某个地址，以此地址才能对网络成员进行访问。业务控制点可以是一台计算机或数据库系统，它运行业务程序并通过交换系统提供客户业务。

业务控制点的功能实质上在于，借助于中央数据库对 IN 中的连接进行路由，并承担费用及统计数据的管理。

在此业务管理点接受用于配置及业务管理的数据。在使用某项 IN 业务时，来自所谓的“业务交换点”（简称 SSP）的请求被识别，并由业务控制点来处理。SSP 节点是数字交换节点，它具有特殊的控制功能。它可以识别智能电信业务，并承担智能网中的以业务为中心的连接控制。ITU 的推荐标准中通过 Q.1200 描述了此类智能网。

由于智能网中的交换、业务功能单元彼此分开，所以智能网从

一开始就比其他面向交换的网络更为灵活。智能网概念里的交换功能不再仅集中在交换节点，而是可以由特殊的计算机（上面已提及的业务交换点）来实现。IN 中的交换技术任务通常通过 SS#7 网络来实施。交换和业务功能的分开被称为分布式业务特征控制。

智能网由于其以业务为中心的软件可以快速产生新的业务。它与其它网络概念的实质区别在于，它可以快速实现和网络无关的新的业务。因此业务可以通过简单的描述（所谓的业务计划）来定义。

此外智能网与所提供的业务和现有网络无关。

从应用的角度来看，智能网涉及许多性能特征，这些特征使优化电信流程成为可能。

需要从立法者那里尽可能多地获悉，什么功能供智能网的运营商使用，这些功能使必要时对单个用户的数据交换进行监控成为可能。

合法监听数据流，即所谓的“Lawful Interception”，目前在智能网中被区别对待。

通常对智能网中的数据业务量的监控是非集中式进行的。即所有带 SSP 功能的交换节点（在此只能进行 IN 连接处理）应具有管理和实施监控所必需的数据。这些管理和实施监控所必需的数据在本文中被称为监控数据，它以已知的方式包含如下监听信息，如是否应该开票，此票包含系统功能信息，如唤醒请求，通过此请求激活电信终端设备；是否应该进行语言数据的记录，相关资料见标准 ETSI ES 201 158, EZSI ES 201 671 以及 ETSI ER 331。此外监控数据应该可以传输路由信息，即在监控范围内记录下来的结果数据的流向，如用于分析。监控数据也可以包含以下信息，某个受监控的电信终端设备的地址编码是否以及应该如何进行，如传输事先指定的 ID 号，而不是传输地址。

监控数据在监控情况中被使用，用于建立监控连接。

若必须建立一个新的监控情况，它是在所有带 SSP 功能的交换节点实施的。智能网中“合法监听”的概念也见标准 ETSI EG 201

781 V1.1.1.

上述方法需要监控局进行很麻烦的管理工作，以保持数据的一致性。例如，若交换节点具有 SSP 功能，但并不马上通知监控局，这样就会出现任何情况下都应避免的监控间隙。

因此本发明的一个任务在于，克服上述缺点以及保证对监控数据的简单和一致的管理。

本任务将通过开始提及的方法解决，即监控数据在智能网中所选出的交换节点中进行集中管理，并应请求被传输到本地交换节点，这些本地交换节点借助于监控数据对电信终端设备进行监控。

本发明的一个优点在于，通过对监控数据的集中管理来保证数据的一致性，并且借助于其它 SSP 交换节点使得简单扩展网络成为可能，而不会影响监控功能。以新的、集中式的管理方法可以在网络中任意选择一个交换节点，来获取监控数据。监控局只需管理该交换节点中的监控数据。此外减少了潜在的出现故障的可能性，这些故障可能性来自迄今常见的 n 倍数据保存，其中 n 与交换节点的数目一致，在这些交换节点中监控数据是用已知的非集中式管理方法来存储的。

还有一个优点就是，所选出的交换节点中监控数据的集中管理是借助于数据库来进行的。

本发明的一个有利变化在于，在与其它电信终端设备建立 IN 连接时，由本地交换节点产生传输监控数据的请求，并传输给所选出的交换节点。

另外还可以看出，在与其它电信终端设备建立 IN 连接时，和/或激活受监控的电信终端设备时，由本地交换节点产生传输监控数据的请求，并传输给所选出的交换节点。

有利的一点是，监控数据的传输是根据 TCAP 协议来进行的。

本发明的一个有利的变化在于，所传输的监控数据在监控过程中存储在本交换节点，并在监控完成之后被清除。

进一步的优点可以通过如下方式获得，设置一个中央管理单元，此单元监控连接建立是否应该在受监控的电信终端设备的参与下完成，以及/或者是否需要激活受监控的电信终端设备，其中，当初始化连接建立和/或激活受监控的电信终端设备时，在本地交换节点和管理单元之间将交换通知数据。

另一个优点就是，本地交换节点和中央管理单元之间通知数据的交换是通过 INAP 接口来进行的。

另外，监控请求可以记录在中央管理单元中。

特别的优点可以通过如下方式获得，即监控请求包括与受监控的电信终端设备相应的 IN 地址和/或 E.164 呼叫号。

为了进行进一步分析，监控的结果数据可以从本地交换节点传输到分析单元。

为了实施本发明所述的方法，开始提到的电信系统特别适合，在此系统中设置有选出的智能网交换节点，此交换节点集中管理监控数据，且这些数据应请求被传输到本地交换节点，这些本地交换节点借助于此监控数据对电信终端设备进行监控。

还有一个优点就是，所选出的交换节点具有用于管理监控数据的数据库。

此外可以建立本地交换节点，它在监控过程中存储接收到的监控数据，此后又将其清除。

进一步的优点可以通过如下方式获得，设置一个电信系统，当 IN 电信连接应该在激活的电信终端设备的参与下建立、和/或激活电信终端设备之一时，在本地交换节点和中央管理单元之间进行通知数据交换。

为了在本地交换节点和中央管理单元之间交换通知数据，可以设定 INAP 接口。

本发明的一个有利的变化在于，设置接受监控请求的中央管理单元。

监控请求可以包含对应于受监控电信终端设备的 IN 地址和/或

E.164 呼叫号。

为了进行进一步分析，监控的结果数据可以从本地交换节点传输到分析单元。

本发明连同其它优点借助于附图中所示的几个并不限于此的实施例进行说明，如图所示：

图 1 根据本发明的电信系统，及

图 2 根据本发明的方法的示例流程图。

按照图 1，根据本发明的电信系统 SYS(用于在一个智能网 INN 中管理监控数据 ÜDA)具有与受监控的电信终端设备 TEA 相应的本地交换节点 VEA，以及用于集中管理监控数据的所选出的交换节点 VEZ。为了监控电信终端设备 TEA，被授权的机关登记中央管理单元 SCP(最好是业务控制点)的监控请求 AUF。所示实施例中的智能网在 PSTN 网的基础上建立。

电信终端设备 TEA 在智能网 INN 中可以对应于一个 IN 地址和/或 E.164 呼叫号。中央管理单元 SCP 是按照所获得的监控请求 AUF 来设置的，例如此请求包含电信终端设备 TEA 的 IN 地址和/或 E.164 呼叫号，用以验证是否应该通过电信终端设备 TEA 建立 IN 连接，以及是否进行电信终端设备的激活。电信终端设备的激活在本文中可理解为，如智能网 INN 系统功能所要求的唤醒业务的使用。

此外需要在所选出的交换节点 VEZ 中设置监控数据 ÜDA。如前面所提及，此监控数据用于实施具体的监控请求，并在所选出的交换节点 VEZ 中被管理。为了管理监控数据 ÜDA，可以提供一数据库 DBZ。

监控数据 ÜDA 的管理可以由监控局 LEA 或自动通过所选出的交换节点 VEZ 来进行。

监控的结果数据可以被提交给监控局 LEA 的分析单元 ASW。

现以两个电信终端设备 TEA 和 TEB 之间的 IN 连接为例说明根

据本发明的方法。在受监控的电信终端设备 TEA 和另一个电信终端设备 TEB 的参与下建立 IN 连接时（图 2），监控情况由中央管理单元 SCP 识别，并且通过一个在此没有表示出来的“智能网应用协议”的接口（简称 INAP 接口）来通知受监控的电信终端设备 TEA 的用户交换节点 VEA。INAP 接口可理解为智能网 INN 的标准接口。

用户交换节点 VEA 现在开始和所选出的交换节点 VEZ 进行通信，如根据“传输容量应用部分”（简称 TCAP）协议，此 VEZ 集中管理监控数据，产生用于传输监控数据的请求并将其传输到所选出的交换节点 VEZ。

TCAP 协议可理解为无连接的用于信息交换的 SS#7 协议，此信息交换与呼叫和连接无关。

SS#7 是一种已知的协议，它是为数字远程通话网络的信令而开发的，并由 ITU-T 标准化。在这种应用于 ISDN 和移动无线网（如 GSM 或 DCS 网）的方法中，涉及所谓的带外或中央信道的信令。这种信令系统是和有效数据的传输分开的，因此具有自己的网络结构，此结构可以和有效数据网络平行建立。

SS#7 协议是按四层构造的。下面三层协议具有一个适用于所有应用的共同的信息传输部分。此传输部分构成了有效数据的传输系统，其中用户部分控制有效信道和业务特征。这里有用于电路交换的数据网和用于 ISDN、以及用于移动无线网络、用于运营及维护、和用于所谓的智能网的不同用户部分。通过信令连接的数据传输以数据包的形式、以 64kbit/s 的速率进行。SS#7 协议通常用于 ISDN、GSM 和 ATM。SS#7 协议的介绍可见 ITU-T-Q.700 至 Q.795。

典型的一点是，TCAP 过程是通过至少一个系统业务控制中心（在本例中对应于中央管理单元 SCP）和一个信息传输部分来进行的。系统业务控制中心管理网络配置，在网络用户之间进行协调，并管理网络地址和映射表；信息传输部分允许网络中符号信息的可靠与快速传输。

对于现有监控情况，接收到监控数据 ÜDA 后，此数据将临时存储在本地交换节点 VEA 中，供以后使用。为此目的，例如可以在交换节点设置数据库 DBA。

为了找到所选出的交换节点 VEZ，受监控的电信终端设备 TEA 的本地交换节点 VEA 的 IN 网络地址例如可以通过中央管理单元 SCP 传输。另一种可能在于，所选出的交换节点 VEZ 的 IN 网络地址固定存储在本地交换节点 VEA。

最后通过对应于第二个电信终端设备 TEB 的交换节点 VEB 建立 IN 连接，对两个终端设备之间数据交换的监控是按照已知的方式进行的，例如根据开始被引用的标准 ETSI EG 201 781 V1.1.1。监控的结果数据 EDA 可以记录并中间存储在本地交换节点 VEA，并在以后某个时刻提交给监控局 LEA 的分析单元 ASW。另一种可能在于，结果数据 EDA 永久地提交给监控局 LEA 的分析单元 ASW。

完成监控之后，临时存储在本地交换节点 VEA 中的监控数据 ÜDA 可以被清除。

