(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 104092685 B
(45)授权公告日 2017.10.10

(21)申请号 201410325086.5

(22)申请日 2014.07.09

(65)同一申请的已公布的文献号
申请公布号 CN 104092685 A

(43)申请公布日 2014.10.08

(73)专利权人 东方通信股份有限公司
地址 310053 浙江省杭州市滨江区东信大道66号东方通信大厦

(72)发明人 傅永斌 季立明 刘卓 张闯 朱燕娜

(74)专利代理机构 浙江杭州金通专利事务所有限公司 33100
代理人 刘晓春

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/24(2006.01)

(56)对比文件
US 2005/0084092 A1,2005.04.21,
CN 1819666 A,2006.08.16,
CN 1825811 A,2006.08.30,
CN 1802007 A,2006.07.12,
US 2011/0041176 A1,2011.02.17,
CN 101001396 A,2007.07.18,

审查员 赵颖

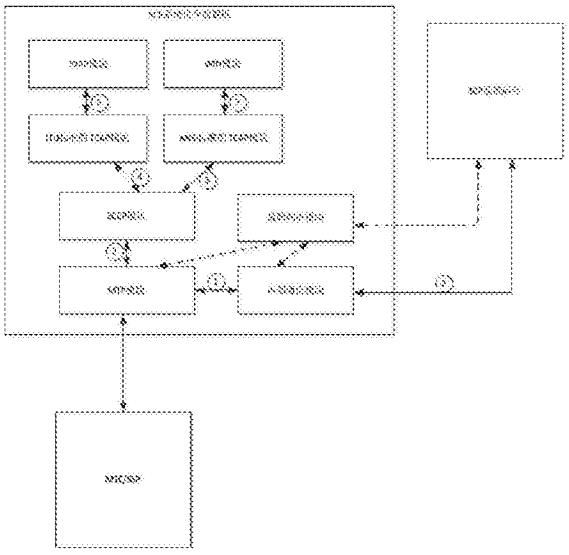
权利要求书2页 说明书8页 附图6页

(54)发明名称

一种利用信令前置机实现智能网SCP容灾保护的方法与装置

(57)摘要

本发明公开了一种利用智能网SCP系统中信令前置机实现在SCP系统后台异常或内部网络故障时的容灾保护装置和方法。该装置和方法的特征在于利用了SCP系统信令前置机的信令处理能力和冗余计算能力，在检出SCP系统后台故障时，全面接管SCP系统信令处理。该装置和方法的特征还在于在信令前置机中不保存智能网用户业务数据，因此信令前置机接管SCP信令处理后，将呼叫按正常的普通呼叫接续，而忽略用户的智能网业务特征。本发明提供了除传统智能网N+1容灾备份方式之外的补充，简单易行、低成本，可以提高SCP系统后台异常情况下的用户电话接通率。本发明可以应用于CDMA网络和固网的智能网SCP系统中。



CN 104092685 B

1.一种利用信令前置机实现智能网SCP容灾保护的方法，其特征在于利用业务控制点SCP系统信令前置机的信令处理能力和冗余计算能力，在所述信令前置机检出业务控制点SCP系统后台故障后，由所述信令前置机全面接管业务控制点SCP系统信令处理，所述信令前置机的信令处理忽略用户的智能网特征，按普通呼叫进行接续；

所述方法包含以下步骤：

(1)、SCP系统初始，在所述信令前置机中增加信息传递部分MTP本地用户配置，以及本地SCCP、ITU标准的TCAP、ANSI标准的TCAP、WIN、INAP协议层中的路由配置和数据配置；

(2)、SCP系统正常运行时，所述信令前置机完成MTP协议处理，并与SCP系统后台通信，通信介质为以太网，且所述信令前置机监控SCP后台的可用性和内部网络的可达性；当SCP后台异常或网络异常，则进入步骤(3)；

(3)、所述信令前置机切换MTP用户数据的目的指向，由原来送往SCP系统后台改为送到本地信令连接控制协议SCCP协议层；

(4)、MTP用户数据流经本地信令连接控制协议SCCP协议层、事务处理能力应用部分TCAP协议层处理后，到达所述信令前置机本地的WIN协议层或者INAP协议层，本地WIN协议层或者INAP协议层按普通呼叫处理，返回智能网响应消息给业务交换点SSP，进行呼叫的接续；

(5)、在SCP后台或网络故障恢复后，将MTP用户数据的目的指向切换回SCP系统后台，由SCP系统后台接管并恢复正常的智能网业务处理过程。

2.如权利要求1所述的一种利用信令前置机实现智能网SCP容灾保护的方法，其特征在于，所述信令前置机根据在CDMA网络或固网中分配的不同点码，在步骤(4)中SCCP协议层根据GT翻译结果区分不同网络采用是ITU标准的TCAP协议还是ASNI标准的TCAP协议，并将SCCP协议层用户数据正确送达不同的TCAP协议层。

3.如权利要求1所述的一种利用信令前置机实现智能网SCP容灾保护的方法，其特征在于，步骤(4)中WIN协议层和INAP协议层包括以下流程：C网主叫信令流程、C网被叫信令流程、C网无条件或遇忙呼叫前转信令流程、C网无应答呼叫前转信令流程以及固网信令流程。

4.实现权利要求1所述方法的一种利用信令前置机实现智能网SCP容灾保护的装置，其特征在于它内嵌于业务控制点SCP系统信令前置机中，包括以下模块：

支持切换用户数据流向的MTP模块，用于权利要求1步骤(1)中MTP本地用户配置，以及在权利要求1步骤(2)中SCP系统正常运行时，所述信令前置机中的MTP协议处理以及权利要求1步骤(3)和步骤(5)中MTP用户数据目的指向的切换；

内部通信模块，用于MTP模块与SCP系统后台之间提供通信；

故障判决模块，用于在权利要求1步骤(2)中监控SCP系统后台的可用性和内部网络的可达性、判定故障状态、决定信令前置机是否进入权利要求1步骤(3)或者步骤(5)；

SCCP模块，用于权利要求1步骤(4)信令前置机中SCCP协议处理，并支持权利要求1步骤(1)中SCCP协议层的路由配置和数据配置；

ITU标准的TCAP模块，用于权利要求1步骤(4)信令前置机中ITU标准的TCAP协议处理，并支持权利要求1步骤(1)中ITU标准的TCAP协议层数据配置；

ANSI标准的TCAP模块，用于权利要求1步骤(4)信令前置机中ANSI标准的TCAP协议处理，并支持权利要求1步骤(1)中ANSI标准的TCAP协议层数据配置；

WIN模块，用于权利要求1步骤(4)信令前置机中的WIN协议处理，将所有C网呼叫按普通呼叫处理流程执行，同时支持权利要求1步骤(1)中WIN协议层数据配置；

INAP模块，用于权利要求1步骤(4)信令前置机中的INAP协议处理，将所有固网网呼叫按普通呼叫处理流程执行，同时支持权利要求1步骤(1)中INAP协议层数据配置。

一种利用信令前置机实现智能网SCP容灾保护的方法与装置

技术领域

[0001] 本发明涉及CDMA网络和固定通信网络，具体涉及应用于两种网络中的智能网SCP系统，尤其涉及利用信令前置机实现智能网SCP容灾保护的方法与装置。

背景技术

[0002] 智能网(Intelligent Network)是在传统的通信网络上，为迅速快捷地提供新业务而设置的一种附加网络结构。智能网将网络的交换功能和业务的控制功能相分离，通过集中的业务控制、业务数据、业务管理和业务生成体系，快速、方便、灵活、经济、有效地生成和实现各种新业务。随着电信业务的迅猛发展，用户规模不断扩大、业务需求不断增长，智能网已成为运营商发展业务的一个重要手段。在各运营商所拥有的用户群体中，智能网用户已达到50%或更高的比例。

[0003] 对于电信运营商而言，智能网系统各设备节点的可靠性至关重要。在智能网系统中设备节点的故障往往将会造成一段时间内大量的用户呼损，进而引起用户的投诉甚至转网，给运营商带来巨大的经济损失，如何提高智能网系统中各设备节点的可靠性、如何提供在设备节点故障后的容灾保护是各大电信运营商的一个重要课题。

发明内容

[0004] 本发明首先所要解决的问题是提供一种利用信令前置机实现智能网SCP容灾保护的方法，该方法能利用SCP系统信令前置机的信令处理能力和冗余计算能力，相对于传统的N+1备份系统，具有投入小，简单易行的特点。为此，本发明采用以下技术方案：

[0005] 一种利用信令前置机实现智能网SCP容灾保护的方法，其特征在于利用业务控制点SCP系统信令前置机的信令处理能力和冗余计算能力，在所述信令前置机检出业务控制点SCP系统后台故障后，由所述信令前置机全面接管业务控制点SCP系统信令处理，所述信令前置机的信令处理忽略用户的智能网特征，按普通呼叫进行接续。

[0006] 在采用上述技术方案的基础上，本发明还可采用以下进一步的技术方案：

[0007] 所述方案包含以下步骤：

[0008] (1)、SCP系统初始，在所述信令前置机中增加信息传递部分MTP本地用户配置，以及本地SCCP、ITU标准的TCAP、ANSI标准的TCAP、WIN、INAP协议层中的路由配置和数据配置；

[0009] (2)、SCP系统正常运行时，所述信令前置机完成MTP协议处理，并与SCP系统后台通信，通信介质为以太网，且所述信令前置机监控SCP后台的可用性和内部网络的可达性；当SCP后台异常或网络异常，则进入步骤(3)；

[0010] (3)、所述信令前置机切换MTP用户数据的目的指向，由原来送往SCP系统后台改为送到本地信令连接控制协议SCCP协议层；

[0011] (4)、MTP用户数据流经本地信令连接控制协议SCCP协议层、事务处理能力应用部分TCAP协议层处理后，到达所述信令前置机本地的WIN协议层或者INAP协议层，本地WIN协议层或者INAP协议层按普通呼叫处理，返回智能网响应消息给业务交换点SSP，进行呼叫的

接续；

[0012] (5)、在SCP后台或网络故障恢复后，将MTP用户数据的目的切换回SCP系统后台，由SCP系统后台接管并恢复正常的智能网业务处理过程。

[0013] 所述信令前置机根据在CDMA网络或固网中分配的不同点码，在步骤(4)中SCCP协议层根据GT翻译结果区分不同网络采用是ITU标准的TCAP协议还是ASNI标准的TCAP协议，并将SCCP协议层用户数据正确送达不同的TCAP协议层。

[0014] 所述信令前置机在步骤(4)中WIN协议层和INAP协议层包括以下流程：C网主叫信令流程、C网被叫信令流程、C网无条件或遇忙呼叫前转信令流程、C网无应答呼叫前转信令流程以及固网信令流程。

[0015] 本发明另一个所要解决的技术问题是提供一种实现上述方法的装置。为此，本发明采用以下技术方案：

[0016] 本发明装置其特征在于它内嵌于业务控制点SCP系统信令前置机中，包括以下模块：

[0017] 支持切换用户数据流向的MTP模块，用于所述步骤(1)中MTP本地用户配置，以及在所述步骤(2)中SCP系统正常运行时，所述信令前置机中的MTP协议处理以及所述步骤(3)和步骤(5)中MTP用户数据目的指向的切换；

[0018] 内部通信模块，用于MTP模块与SCP系统后台间之间提供通信；

[0019] 故障判决模块，用于在所述步骤(2)中监控SCP系统后台的可用性和内部网络的可达性、判定故障状态、决定信令前置机是否进入所述步骤(3)或者步骤(5)；

[0020] SCCP模块，用于所述步骤(4)信令前置机中SCCP协议处理，并支持所述步骤(1)中SCCP协议层的路由配置和数据配置。

[0021] ITU标准的TCAP模块，用于所述步骤(4)信令前置机中ITU标准的TCAP协议处理，并支持所述步骤(1)中ITU标准的TCAP协议层数据配置；

[0022] ANSI标准的TCAP模块，用于所述步骤(4)信令前置机中ANSI标准的TCAP协议处理，并支持所述步骤(1)中ANSI标准的TCAP协议层数据配置。

[0023] WIN模块，用于所述步骤(4)信令前置机中的WIN协议处理，将所有C网呼叫按普通呼叫处理流程执行，同时支持所述步骤(1)中WIN协议层数据配置；

[0024] INAP模块，用于所述步骤(4)信令前置机中的INAP协议处理，将所有固网网呼叫按普通呼叫处理流程执行，同时支持所述步骤(1)中INAP协议层数据配置。

[0025] 名称解释：

[0026] SCP：业务控制点(Service Control Point)

[0027] MTP：信息传递部分(Message Transfer Part)

[0028] SCCP：信令连接控制协议(Signaling Connection (and) Control Part)

[0029] TCAP：事务处理能力应用部分(Transaction Capabilities Application Part)

[0030] WIN：无线智能网(Wireless Intelligent Network)

[0031] INAP：智能网应用协议(Intelligent Network Application Protocol)

[0032] GT：全局码(Global Title)

[0033] MSC：移动交换中心(Mobile Switching Center)

[0034] GMSC：移动交换中心网关(Gateway Mobile Switching Center)

[0035] SSP：业务交换点(Service Switching Point)

[0036] ASNI：美国国家标准协会(American National Standards Institute)是北美的标准制定机构

[0037] ITU：国际电信联盟(International Telecommunication Union)是一个国际组织，主要负责确立国际无线电和电信的管理制度和标准

[0038] C网：CDMA网络

[0039] 固网：传统的PSTN网络

[0040] 普通呼叫：指主被叫双方均无签约智能网业务的呼叫

[0041] 由于采用本发明的技术方案，能利用业务控制点SCP系统信令前置机的信令处理能力和冗余计算能力，在所述信令前置机检出业务控制点SCP系统后台故障后，由所述信令前置机全面接管业务控制点SCP系统信令处理，相对于传统的N+1备份系统，具有投入小，简单易行的特点。

附图说明

[0042] 图1本发明所提供的利用信令前置机实现智能网SCP容灾保护装置的示意图。

[0043] 图2本发明所提供的智能网SCP容灾保护方法的C网主叫信令流程图。

[0044] 图3本发明所提供的智能网SCP容灾保护方法的C网被叫信令流程图。

[0045] 图4本发明所提供的智能网SCP容灾保护方法的C网无条件或遇忙呼叫前转信令流程图。

[0046] 图5本发明所提供的智能网SCP容灾保护方法的C网无应答呼叫前转信令流程图。

[0047] 图6本发明所提供的智能网SCP容灾保护方法的固网信令流程。

具体实施方式

[0048] 本实施例以电信固网和C网提供智能网业务的SCP系统改造为例，对SCP系统的信令前置机进行本发明所述的装置改造，达到如下要求：自动检出SCP系统后台故障或网络故障，切换到信令前置机接管模式，信令前置机实现按普通呼叫接续呼叫的目的。

[0049] 本实施例的利用信令前置机实现智能网SCP容灾保护的方法包含以下步骤：

[0050] (1)、SCP系统初始，在所述信令前置机中增加信息传递部分MTP本地用户配置，以及本地SCCP、ITU标准的TCAP、ANSI标准的TCAP、WIN、INAP协议层中的路由配置和数据配置；

[0051] (2)、SCP系统正常运行时，所述信令前置机完成MTP协议处理，并与SCP系统后台通信，通信介质为以太网，且所述信令前置机监控SCP后台的可用性和内部网络的可达性；当SCP后台异常或网络异常，则进入步骤(3)；

[0052] (3)、所述信令前置机切换MTP用户数据的目的指向，由原来送往SCP系统后台改为送到本地信令连接控制协议SCCP协议层；

[0053] (4)、MTP用户数据流经本地信令连接控制协议SCCP协议层、事务处理能力应用部分TCAP协议层处理后，到达所述信令前置机本地的WIN协议层或者INAP协议层，本地WIN协议层或者INAP协议层按普通呼叫处理，返回智能网响应消息给业务交换点SSP，进行呼叫的接续；

[0054] (5)、在SCP后台或网络故障恢复后，将MTP用户数据的目的切换回SCP系统后台，由

SCP系统后台接管并恢复正常的智能网业务处理过程。

[0055] 所述信令前置机根据在CDMA网络或固网中分配的不同点码，在步骤(4)中SCCP协议层根据GT翻译结果区分不同网络采用是ITU标准的TCAP协议还是ASNI标准的TCAP协议，并将SCCP协议层用户数据正确送达不同的TCAP协议层。

[0056] 所述信令前置机在步骤(4)中WIN协议层和INAP协议层包括以下流程：C网主叫信令流程、C网被叫信令流程、C网无条件或遇忙呼叫前转信令流程、C网无应答呼叫前转信令流程以及固网信令流程。

[0057] 参考附图1，信令前置机中的容灾保护装置包括以下模块：

[0058] 支持切换用户数据流向的MTP模块，用于所述步骤(1)中MTP本地用户配置，以及在所述步骤(2)中SCP系统正常运行时，所述信令前置机中的MTP协议处理以及所述步骤(3)和步骤(5)中MTP用户数据目的指向的切换；

[0059] 内部通信模块，用于MTP模块与SCP系统后台间之间提供通信；

[0060] 故障判决模块，用于在所述步骤(2)中监控SCP系统后台的可用性和内部网络的可达性、判定故障状态、决定信令前置机是否进入所述步骤(3)或者步骤(5)；

[0061] SCCP模块，用于所述步骤(4)信令前置机中SCCP协议处理，并支持所述步骤(1)中SCCP协议层的路由配置和数据配置。

[0062] ITU标准的TCAP模块，用于所述步骤(4)信令前置机中ITU标准的TCAP协议处理，并支持所述步骤(1)中ITU标准的TCAP协议层数据配置；

[0063] ANSI标准的TCAP模块，用于所述步骤(4)信令前置机中ANSI标准的TCAP协议处理，并支持所述步骤(1)中ANSI标准的TCAP协议层数据配置。

[0064] WIN模块，用于所述步骤(4)信令前置机中的WIN协议处理，将所有C网呼叫按普通呼叫处理流程执行，同时支持所述步骤(1)中WIN协议层数据配置；

[0065] INAP模块，用于所述步骤(4)信令前置机中的INAP协议处理，将所有固网网呼叫按普通呼叫处理流程执行，同时支持所述步骤(1)中INAP协议层数据配置。

[0066] SCP系统初始时，故障判决模块配置故障检测开关，用于控制是否开启本保护装置功能；MTP模块除配置MTP协议层基本的信令链路、信令路由等数据外，还需要配置切换的本地目的地，用于控制检出故障后MTP用户数据的流向；SCCP模块配置SCCP协议层的GT翻译数据以及对应用户层是ITU标准的TCAP模块还是ANSI标准的TCAP模块；ITU标准的TCAP模块和ANSI标准的TCAP模块分别配置TCAP协议层的本地事务处理数量；WIN模块配置智能业务类型，如VPN配置为96，PPC配置为128，INAP模块配置前插码，为普通呼叫流程的处理提供依据。

[0067] MTP模块除了具备7号信令规范要求功能外，本实施中需增加与故障判决模块间的控制功能，根据故障判断模块的判决结果，决定是否将MTP用户数据流切换到前置机本地处理，如图1中由①->②路径切换为③->④->⑥路径或③->⑤->⑦路径；内部通信模块除负责与SCP系统后台建立可靠通信连接外，增加通信通路状态检测并上报故障判决模块功能；故障判断模块通过建立与SCP系统后台间的心跳检测、监控网口状态、收集内部通信模块状态信息等手段监控SCP系统后台的可用性与网络可达性等关键信息，如果根据监控结果判定需启动信令前置机容灾保护功能，则通知MTP模块故障发生，切换用户数据流；SCCP模块具备7号信令规范要求功能，智能网TCAP消息均采用了SCCP无连接类型传递报文，此外本实施中

还具有根据GT翻译结果，正确选择上层采用ITU 标准的TCAP协议还是ANSI标准的TCAP协议处理功能；ITU标准的 TCAP模块和ANSI 标准的TCAP模块均符合7号信令规范要求，它们的上层用户分别为INAP模块和WIN模块； INAP模块和WIN模块并不提供完整INAP或WIN协议层功能，而是采用了特殊处理流程，详见附图2~6。由于在信令前置机本地并不保存智能网用户业务数据，该系列流程目的是保证接续呼叫，而不保留呼叫的智能网属性。

[0068] 附图2，C网主叫信令流程。

[0069] 步骤2.1~2.4，MSC/SSP检测到触发器向SCP系统发起ORREQ，WIN模块收到对应请求事务查询指示原语，响应orreq（其中，WIN模块不做号码翻译不提供terminatiolist参数，业务键（DMH_ServiceID）参数为预配置数据），指示MSC/SSP继续进行呼叫处理；

[0070] 步骤2.5~2.8， SCP系统收到ANLYZD，WIN模块直接响应anlyzd，业务键（DMH_ServiceID）为预配置数据；

[0071] 步骤2.9~2.10，用户接听后，SCP 系统收到MSC/SSP 送来的OANSWER 消息。WIN模块记录呼叫开始时间，不做其他处理；

[0072] 步骤2.11~2.14，用户通话结束后，SCP 系统收到MSC/SSP 送上来的ODISCONNECT，WIN模块记录通话结束时间、通话时长，向MSC/SSP 下发odisconnect，切断呼叫。

[0073] 附图3，C网被叫信令流程。

[0074] 步骤3.1~3.4，SCP系统收到ANLYZD（Initial 触发器）消息，向MSC/SSP 返回响应anlyzd，业务键（DMH_ServiceID）为预配置数据；

[0075] 步骤3.5~3.8，SCP系统 收到ANLYZD（Called_Routing_Address_Available 触发器）消息，WIN模块向MSC/SSP 返回响应anlyzd，业务键（DMH_ServiceID）为预配置数据；

[0076] 步骤3.9~3.10，用户接听后，SCP系统 收到MSC/SSP 送来的TANSWER 消息。WIN模块记录呼叫开始时间，不做其他处理；

[0077] 步骤3.11~3.14，用户通话结束后，SCP系统 收到MSC/SSP 送上来的TDISCONNECT。WIN模块 记录通话结束时间、通话时长，向MSC/SSP 下发tdisconnect，切断呼叫。

[0078] 附图4，C网无条件/遇忙前转信令流程。

[0079] 步骤4.1~4.4，SCP系统收到ANLYZD（Initial 触发器）消息，WIN模块向MSC/SSP 返回响应anlyzd，业务键（DMH_ServiceID）为预配置数据；

[0080] 步骤4.5~4.8，核心网做前转，SCP 系统收到ANLYZD（Calling_Routing_Address_Available 触发器）消息（其中，参数DMH_RedirectionIndicator 指示为前转呼叫）。WIN模块返回响应analyzd 消息，业务键（DMH_ServiceID）为预配置数据；

[0081] 步骤4.9~4.10，用户接听后，SCP 系统收到MSC/SSP 送来的OANSWER 消息。WIN模块记录呼叫开始时间，不做其他处理；

[0082] 步骤4.11~4.14，用户通话结束后，SCP 系统收到MSC/SSP 送上来的ODISCONNECT，WIN模块 记录通话结束时间、通话时长，向GMSC/SSP 下发odisconnect，切断呼叫。

[0083] 附图5，C网无应答前转信令流程。

[0084] 步骤5.1~5.4，SCP系统收到ANLYZD（Initial 触发器）消息，WIN模块向MSC/SSP 返回响应anlyzd，业务键（DMH_ServiceID）为预配置数据；

[0085] 步骤5.5~5.8，SCP 系统收到ANLYZD（Called_Routing_Address_Available 触发器）消息，WIN模块按正常的被叫业务进行处理，向MSC/SSP 返回响应anlyzd，业务键（DMH_

ServiceID)为预配置数据；

[0086] 步骤5.9~5.12,用户无应答后，核心网做前转，SCP 系统收到ANLYZD(Calling_Routing_Address_Available 触发器) 消息(其中，参数DMH_RedirectionIndicator 指示为前转呼叫)。WIN模块向MSC/SSP返回响应analyzd消息；

[0087] 步骤5.13~5.14,用户接听后,SCP系统收到MSC/SSP送来的OANSWER消息。WIN模块记录呼叫开始时间,不做其他处理；

[0088] 步骤5.15~5.18,用户通话结束后,SCP系统收到MSC/SSP送上来的ODISCONNECT,WIN模块记录通话结束时间、通话时长,向SCP下发odisconnect,切断呼叫。

[0089] 附图6,固网信令流程。

[0090] 步骤6.1~6.4,SCP系统收到MSC/SSP送来的IDP消息,WIN模块检查IDP消息中被叫号码参数,并匹配预配置的前插码,去掉被叫号码中匹配到的前插码,获得真实被叫号码。WIN模块以TC-END携带connect 操作,填写真实被叫号码参数,通知SSP自主接续呼叫,并结束与当前TC对话；

[0091] 步骤6.5~6.8,SCP系统收到MSC/SSP送来的非IDP消息,WIN模块以TC-END携带reject操作,通知SSP并结束当前TC对话。

[0092] 以下对附图中的各消息进行说明

[0093] 图2

[0094]

编号	消息	说明
2.1	ORREQ	始发试呼鉴权触发点操作请求
2.2	TC_QUERY_WITH_PERM_IND	事务查询指示原语
2.3	TC_CONVERSATION_WITH_PERM_REQ	事务会话请求原语
2.4	Orreq	始发试呼鉴权触发点操作响应
2.5	ANLYZD	分析信息触发点操作请求
2.6	TC_CONVERSATION_WITH_PERM_IND	事务会话指示原语
2.7	TC_CONVERSATION_WITH_PERM_REQ	事务会话请求原语
2.8	Analyzd	分析信息触发点操作响应
2.9	OANSWER	主叫应答触发点操作请求
2.10	TC_UNI_INDICATION	事务单向指示原语
2.11	ODISCONNECT	主叫拆线触发点操作请求
2.12	TC_RESPONSE_IND	事务响应指示原语
2.13	TC_RESPONSE_REQ	事务响应请求原语
2.14	Odisconnect	主叫拆线触发点操作响应

[0095] 图3

[0096]

编号	消息	说明
3.1	ANLYZD(Initial)	分析信息触发点操作请求(Initial触发器)
3.2	TC_QUERY_WITH_PERM_IND	事务查询指示原语
3.3	TC_CONVERSATION_WITH_PERM_REQ	事务会话请求原语
3.4	Anlyzd	分析信息触发点操作响应
3.5	ANLYZD(Called_Routing_Address_Available)	分析信息触发点操作请求(Called_Routing_Address_Available触发器)
3.6	TC_CONVERSATION_WITH_PERM_IND	事务会话指示原语
3.7	TC_CONVERSATION_WITH_PERM_REQ	事务会话请求原语
3.8	Analyzd	分析信息触发点操作响应
3.9	TANSWER	被叫应答触发点操作请求

3.10	TC_UNI_INDICATION	事务单向指示原语
3.11	TDISCONNECT	被叫拆线触发点操作请求
3.12	TC_RESPONSE_IND	事务响应指示原语
3.13	TC_RESPONSE_REQ	事务响应请求原语
3.14	Tdisconnect	被叫拆线触发点操作响应

[0097] 图4

[0098]

编号	消息	说明
4.1	ANLYZD(initial)	分析信息触发点操作请求(initial触发器)
4.2	TC_QUERY_WITH_PERM_IND	事务查询指示原语
4.3	TC_CONVERSATION_WITH_PERM_REQ	事务会话请求原语
4.4	Analyzd	分析信息触发点操作响应
4.5	ANLYZD(Calling_Routing_Address_Available)	分析信息触发点操作请求(Calling_Routing_Address_Available触发器)
4.6	TC_CONVERSATION_WITH_PERM_IND	事务会话指示原语
4.7	TC_CONVERSATION_WITH_PERM_REQ	事务会话请求原语
4.8	Analyzd	分析信息触发点操作响应
4.9	OANSWER	主叫应答触发点操作请求
4.10	TC_UNI_INDICATION	事务单向指示原语
4.11	ODISCONNECT	主叫拆线触发点操作请求
4.12	TC_RESPONSE_IND	事务响应指示原语
4.13	TC_RESPONSE_REQ	事务响应请求原语
4.14	Odisconnect	主叫拆线触发点操作响应

[0099] 图5

[0100]

编号	消息	说明
5.1	ANLYZD(initial)	分析信息触发点操作请求(initial触发器)
5.2	TC_QUERY_WITH_PERM_IND	事务查询指示原语
5.3	TC_CONVERSATION_WITH_PERM_REQ	事务会话请求原语
5.4	Analyzd	分析信息触发点操作响应
5.5	ANLYZD(called_Routing_Address_Available)	分析信息触发点操作请求(called_Routing_Address_Available触发器)
5.6	TC_CONVERSATION_WITH_PERM_IND	事务会话指示原语
5.7	TC_CONVERSATION_WITH_PERM_REQ	事务会话请求原语
5.8	Analyzd	分析信息触发点操作响应
5.9	ANLYZD(Calling_Routing_Address_Available)	分析信息触发点操作请求(Calling_Routing_Address_Available触发器)
5.10	TC_CONVERSATION_WITH_PERM_IND	事务会话指示原语
5.11	TC_CONVERSATION_WITH_PERM_REQ	事务会话请求原语
5.12	Analyzd	分析信息触发点操作响应
5.13	OANSWER	主叫应答触发点操作请求
5.14	TC_UNI_INDICATION	事务单向指示原语
5.15	ODISCONNECT	主叫拆线触发点操作请求
5.16	TC_RESPONSE_IND	事务响应指示原语
5.17	TC_RESPONSE_REQ	事务响应请求原语
5.18	Odisconnect	主叫拆线触发点操作响应

[0101] 图6

[0102]

编号	消息	说明
6.1	IDP	启动DP操作
6.2	ITU_TC_BEGIN_IND(IDP)	BEGIN指示原语(带IDP操作)
6.3	ITU_TC_END_REQ(CONNECT)	END请求原语(带CONNECT操作)

6.4	CONNECT	连接操作
6.5	not IDP	非IDP操作
6.6	ITU_TC_BEGIN_IND	BEGIN指示原语
6.7	ITU_TC_END_REQ(REJECT)	END请求原语(带REJECT操作)
6.8	REJECT	拒绝操作

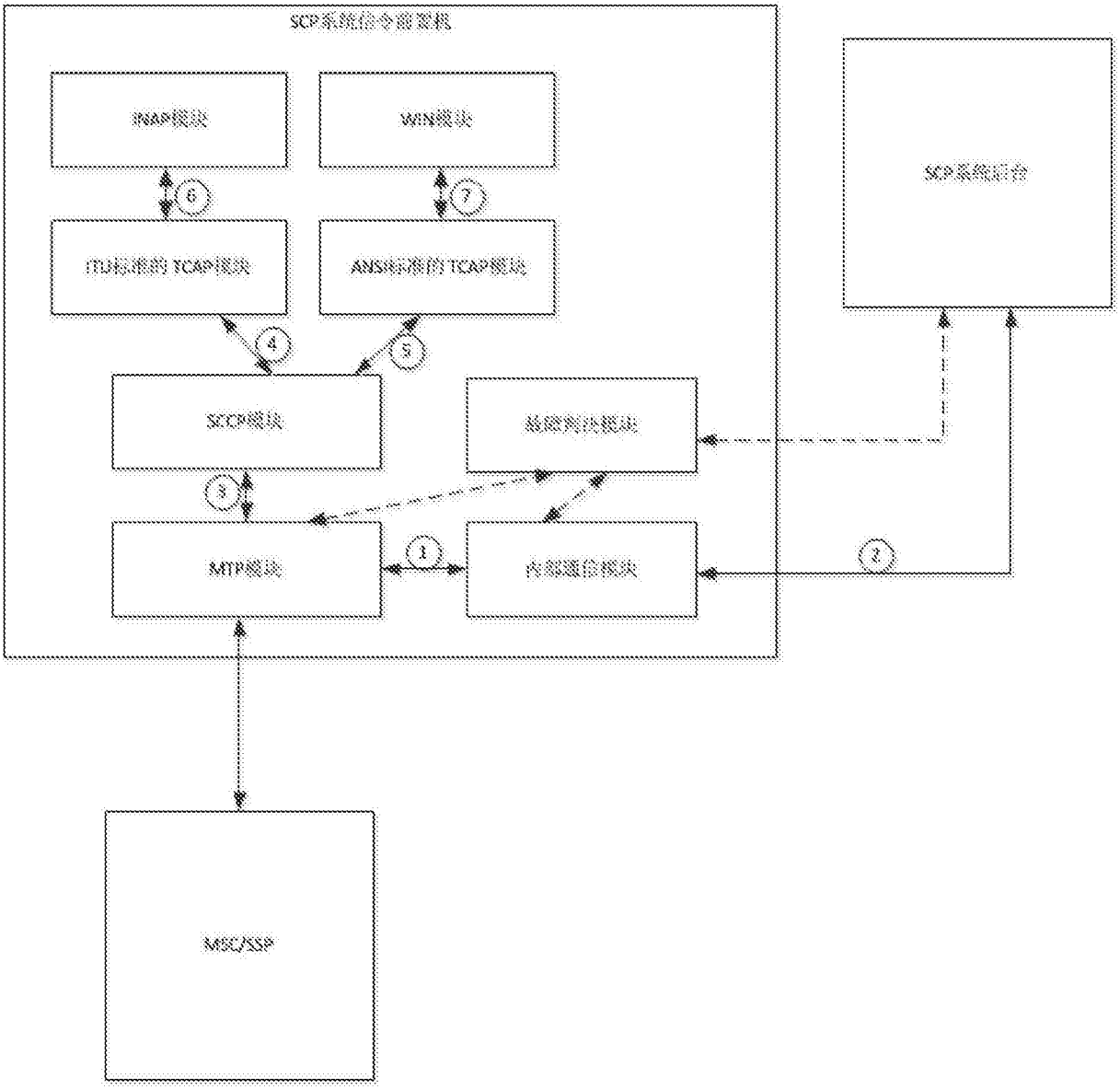

SCP系统综合维管模块
INAP模块
WIN模块
6
7
ITU标准的 TCAP模块
ANSI标准的 TCAP模块
4
5
SCCP模块
3
MTP模块
1
2
MSC/SSP

图1

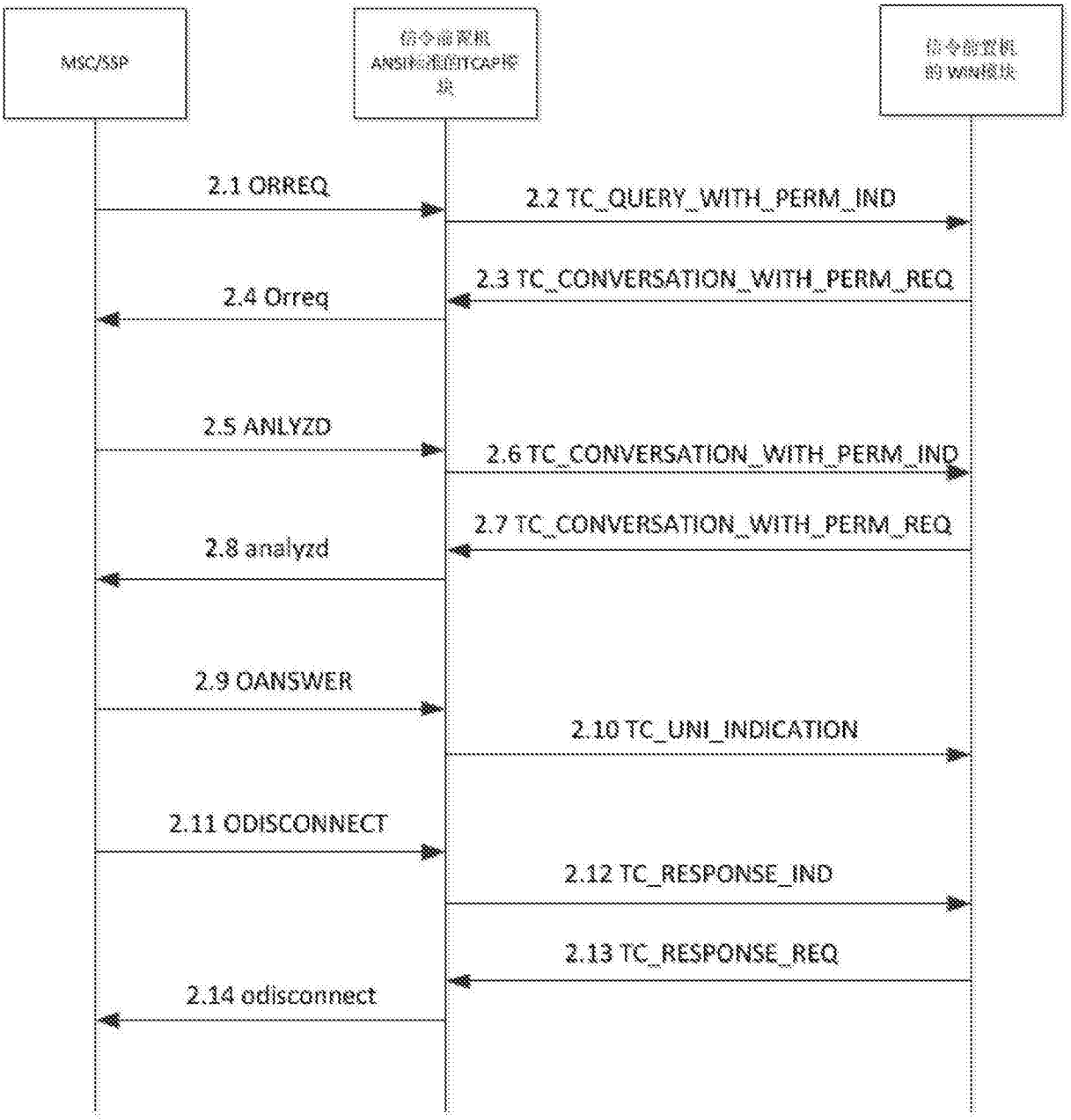

MSC/SSP
2.1 ORREQ
2.2 TC_QUERY_WITH_PERM_IND
2.3 TC_CONVERSATION_WITH_PERM_REQ
2.4 Orreq
2.5 ANLYZD
2.6 TC_CONVERSATION_WITH_PERM_IND
2.7 TC_CONVERSATION_WITH_PERM_REQ
2.8 analyzd
2.9 OANSWER
2.10 TC_UNI_INDICATION
2.11 ODISCONNECT
2.12 TC_RESPONSE_IND
2.13 TC_RESPONSE_REQ
2.14 odisconnect

图2

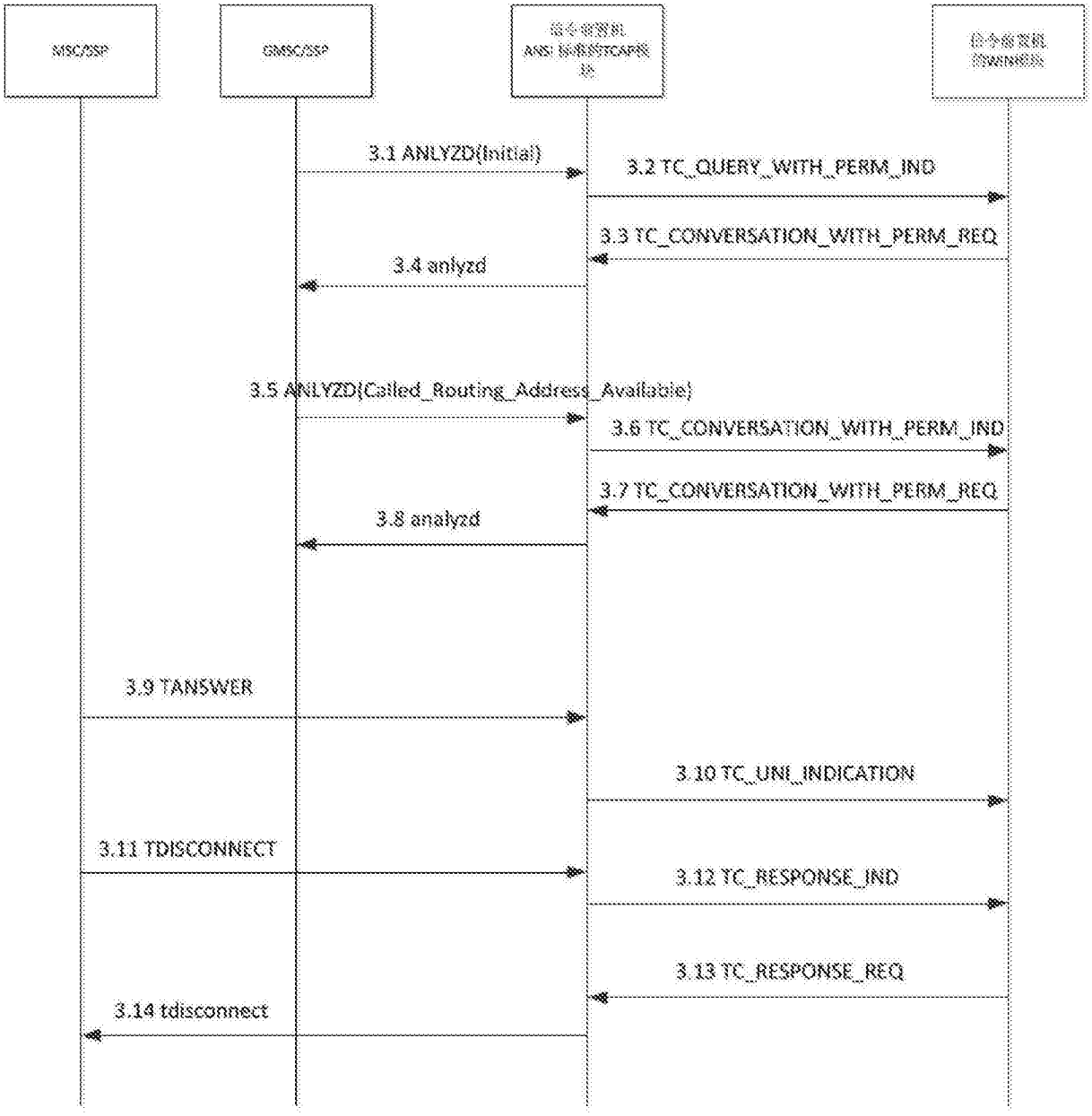

MSC/SSP
GMSC/SSP
3.1 ANLYZD(Initial)
3.2 TC_QUERY_WITH_PERM_IND
3.3 TC_CONVERSATION_WITH_PERM_REQ
3.4 anlyzd
3.5 ANLYZD(Called_Routing_Address_Available)
3.6 TC_CONVERSATION_WITH_PERM_IND
3.7 TC_CONVERSATION_WITH_PERM_REQ
3.8 analyzd
3.9 TANSWER
3.10 TC_UNI_INDICATION
3.11 TDISCONNECT
3.12 TC_RESPONSE_IND
3.13 TC_RESPONSE_REQ
3.14 tdisconnect

图3

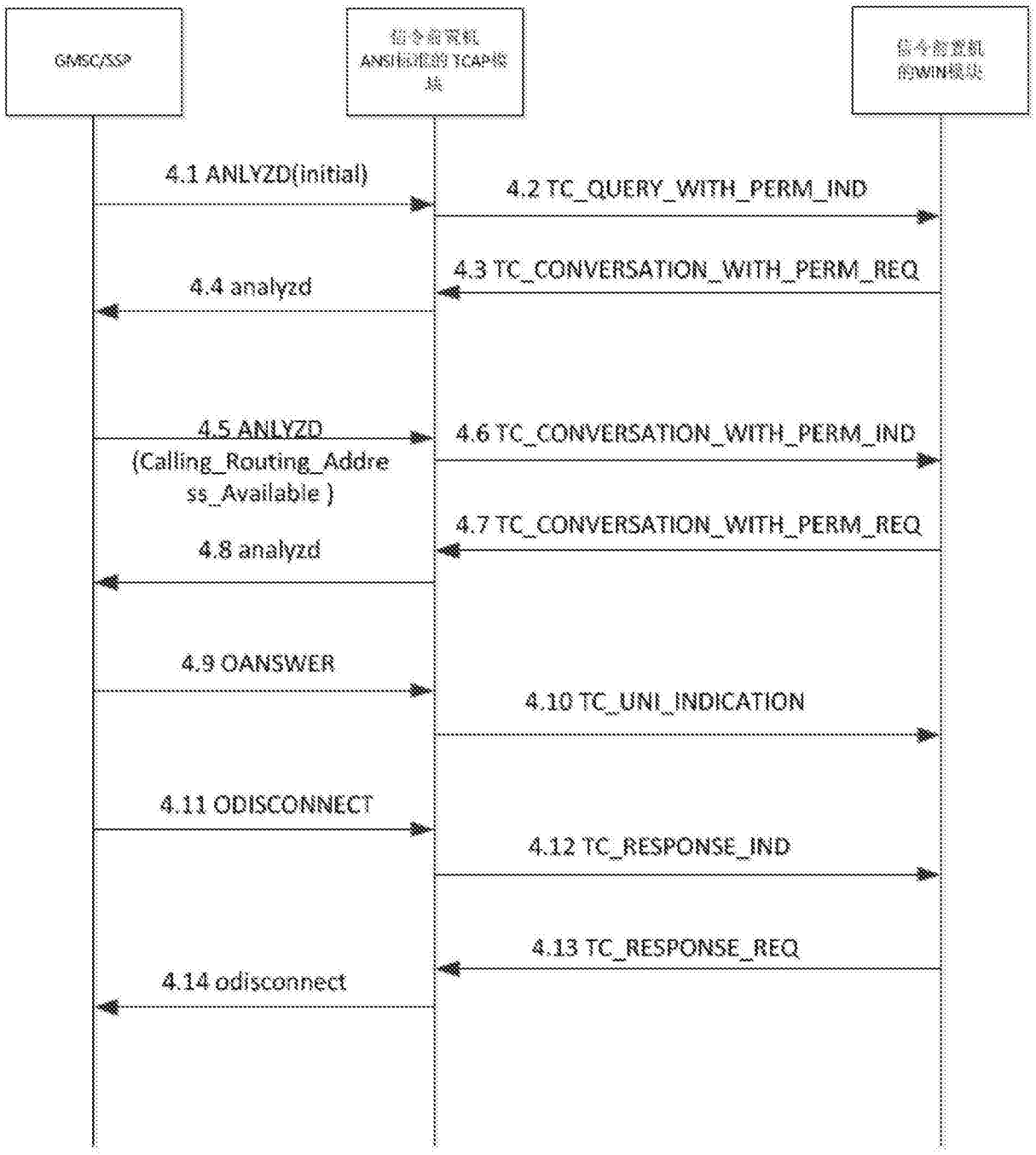

GMSC/SSP
4.1 ANLYZD(initial)
4.2 TC_QUERY_WITH_PERM_IND
4.3 TC_CONVERSATION_WITH_PERM_REQ
4.4 analyzd
4.5 ANLYZD
(Calling_Routing_Addre
ss_Available)
4.6 TC_CONVERSATION_WITH_PERM_IND
4.7 TC_CONVERSATION_WITH_PERM_REQ
4.8 analyzd
4.9 OANSWER
4.10 TC_UNI_INDICATION
4.11 ODISCONNECT
4.12 TC_RESPONSE_IND
4.13 TC_RESPONSE_REQ
4.14 odisconnect

图4

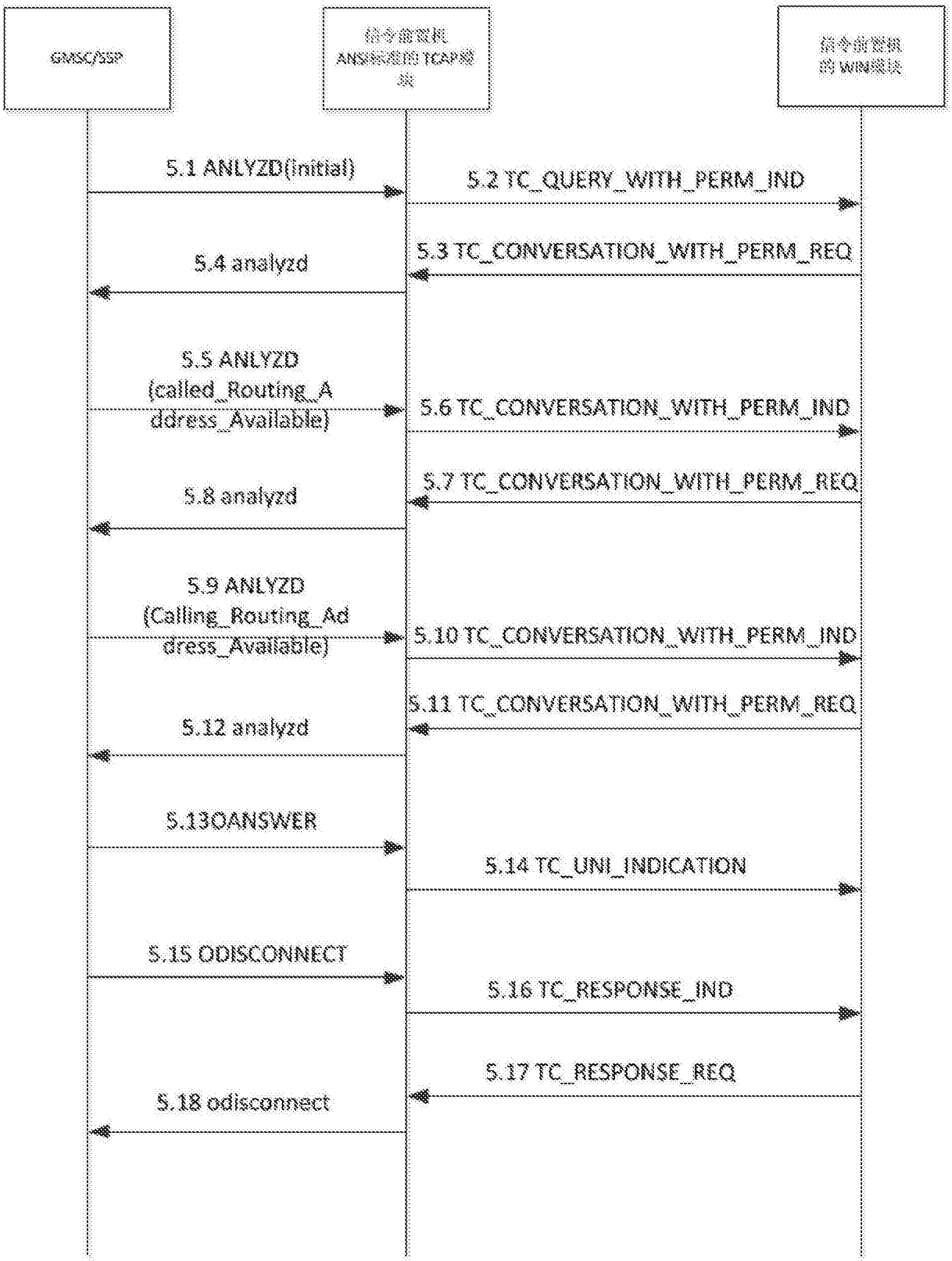

GMSC/SSP
信令监测机
ANSI标准的 TCAP模块
信令监测机
的 WIN模块
5.1 ANLYZD(initial)
5.2 TC_QUERY_WITH_PERM_IND
5.3 TC_CONVERSATION_WITH_PERM_REQ
5.4 analyzd
5.5 ANLYZD (called_Routing_Address_Available)
5.6 TC_CONVERSATION_WITH_PERM_IND
5.7 TC_CONVERSATION_WITH_PERM_REQ
5.8 analyzd
5.9 ANLYZD (Calling_Routing_Address_Available)
5.10 TC_CONVERSATION_WITH_PERM_IND
5.11 TC_CONVERSATION_WITH_PERM_REQ
5.12 analyzd
5.13OANSWER
5.14 TC_UNI_INDICATION
5.15 ODISCONNECT
5.16 TC_RESPONSE_IND
5.17 TC_RESPONSE_REQ
5.18 odisconnect

图5

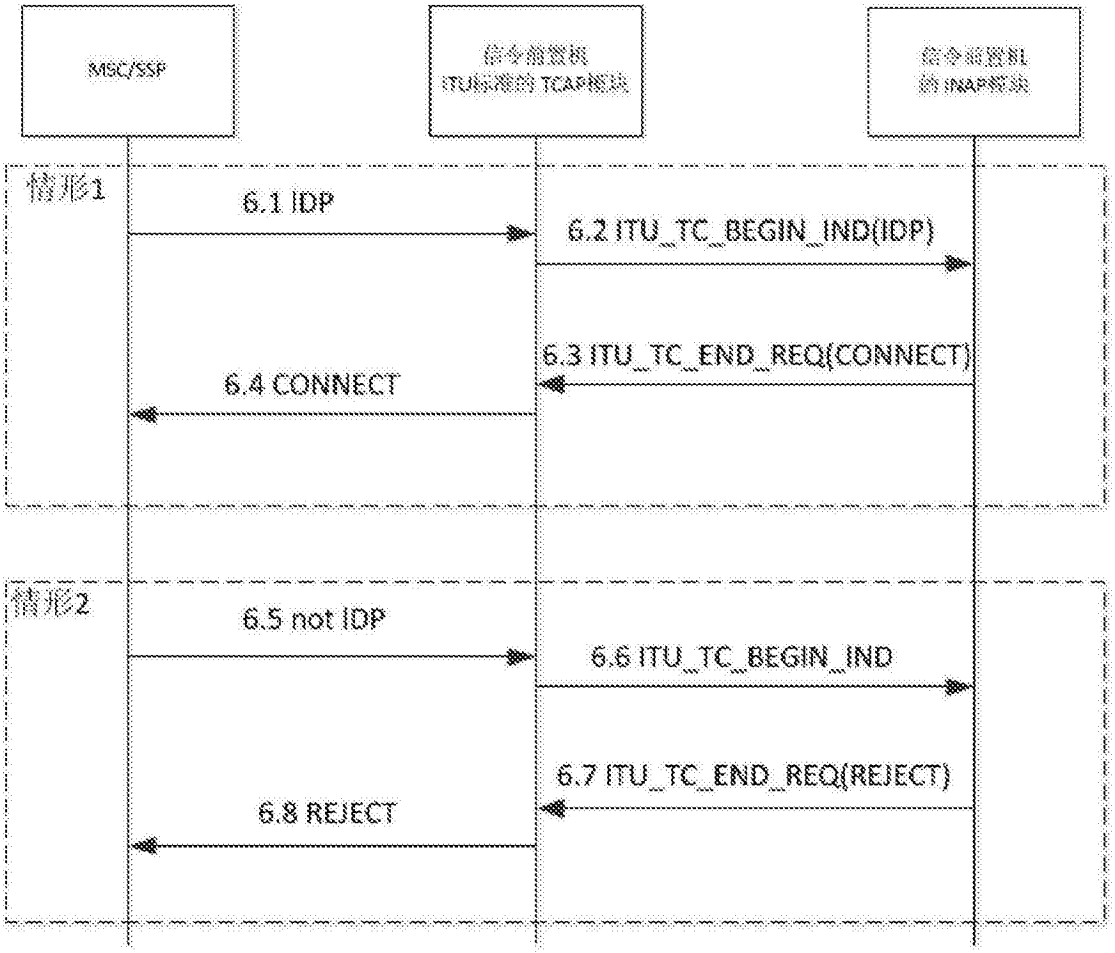

MSC/SSP
情形1
6.1 IDP
6.2 ITU_TC_BEGIN_IND(IDP)
6.3 ITU_TC_END_REQ(CONNECT)
6.4 CONNECT
情形2
6.5 not IDP
6.6 ITU_TC_BEGIN_IND
6.7 ITU_TC_END_REQ(REJECT)
6.8 REJECT

图6