

通信方法及通信装置

5 技术领域

本申请涉及通信领域，并且更具体地，涉及一种通信方法及通信装置。

背景技术

10 用户面安全按需保护机制是第五代（5th Generation，5G）网络中的一种安全机制，该用户面安全按需保护包含用户面加密保护和用户面完整性保护。该用户面安全按需保护机制要求 5G 网络中的接入网设备根据从核心网设备接收到的用户面安全策略判断是否开启与用户设备（user equipment，UE）之间的用户面加密保护和/或用户面完整性保护。用户面安全按需保护机制能够为 UE 提供更加灵活的用户面安全保护。

15 然而，现有的第四代（4th Generation，4G）网络并不支持用户面安全按需保护机制。在 4G 网络中，4G 网络中的接入网设备与 UE 的用户面安全是固定的，即用户面安全固定为用户面加密保护开启，用户面完整性保护不开启。

在 4G 网络短期内不会退网的情况下，如何将前述用户面安全按需保护机制应用于 4G 网络中已经成为业界研究的热点。

20 4G 网络一旦引入用户面安全按需保护机制后，如何在 4G 和 5G 网络之间互通，是当前标准中亟需解决的问题。

发明内容

25 本申请提供一种通信方法，以期解除在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下，终端设备在第一网络中建立的会话不能切换到第二网络中的限制。

30 第一方面，提供了一种通信方法，该方法可以包括：在终端设备在第一网络中建立会话的过程中，会话管理网元获取第一指示信息，该第一指示信息用于指示在第二网络中支持用户面完整性保护；该会话管理网元根据该第一指示信息，向该第一网络的接入和移动性管理功能网元发送第一请求消息，该第一请求消息用于请求为该会话分配承载标识，该承载标识与该终端设备在该第二网络的承载上下文对应；该会话管理网元接收来自该接入和移动性管理功能网元的第一响应消息，该第一响应消息包括该承载标识。

35 基于上述技术方案，会话管理网元根据第一指示信息可以解除在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下，终端设备在第一网络中建立的会话不能切换到第二网络中的限制。因为，按照现有方案，在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下，会话管理网元不会向接入和移动性管理功能网元请求承载标识，从而接入和移动性管理功能网元本地也不会保存有相应的承载标识，这种情况下，后续接入和移动性管理功能网元接收到来自第一网络的接入网设备的切换需求时，是不会执行将终端设备在第一网络中建立的会话切换到第二网络的相关流程的。

在一种可能的实现方式中，该会话管理网元根据该第一指示信息，不考虑该第一网络的用户面安全策略，向该接入和移动性管理功能网元发送第一请求消息。

其中，会话管理网元不考虑第一网络的用户面安全策略可以理解为，会话管理网元不考虑第一网络的用户面安全策略的取值。也就是说，不论第一网络的用户面安全策略的取值是什么，会话管理网元可以根据第一指示信息向接入和移动性管理功能网元发送第一请求消息。例如，会话管理网元可以在第一网络的用户面安全策略包括开启用户面完整性保护（即用户面完整性保护取值为需要（required））的情况下，根据第一指示信息向接入和移动性管理功能网元发送第一请求消息。

应理解，在终端设备是非第三代合作伙伴计划接入，且终端设备请求建立的会话不支持与第二网络基于 N26 接口的互通的情况下，会话管理网元不会向接入和移动性管理功能网元发送第一请求消息。因此，会话管理网元根据第一指示信息，不考虑第一网络的用户面安全策略，向接入和移动性管理功能网元发送第一请求消息，可以理解为，在终端设备是第三代合作伙伴计划接入，以及终端设备请求建立的会话支持与第二网络基于 N26 接口的互通情况下，会话管理网元根据第一指示信息，不考虑第一网络的用户面安全策略，向接入和移动性管理功能网元发送第一请求消息。

示例性地，第一网络是第五代（5th generation, 5G）网络，第二网络是第四代（4th generation, 5G）网络，终端设备在第一网络的会话是协议数据单元（protocol data unit, PDU）会话，承载上下文是演进分组系统承载上下文（evolved packet system bearer context, EPS bearer context）。

示例性地，终端设备在第一网络建立会话的过程包括，终端设备发送 PDU 会话建立请求消息之后至终端设备接收 PDU 会话建立接受消息之前。

结合第一方面，在第一方面的某些实现方式中，该方法还包括：该会话管理网元将该终端设备在该第一网络中的用户面安全策略映射为该终端设备在该第二网络的用户面安全策略；该会话管理网元将该第二网络的用户面安全策略保存在该承载上下文中。

基于上述技术方案，会话管理网元可以将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略，并可以将终端设备在第二网络的用户面安全策略保存在承载上下文。进而，在终端设备从第一网络切换至第二网络的过程中，第一网络中的接入和移动性管理功能网元从会话管理网元获取所述承载上下文，进而将获取到的承载上下文发送给第二网络的移动管理实体，从而有助于实现终端设备从第一网络切换至第二网络。

示例性地，终端设备在第一网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略，终端设备在第二网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略。

示例性地，该第一网络的用户面安全策略是会话管理网元本地存储的，或者，该第一网络的用户面安全策略是会话管理网元从统一数据管理网元获取的。

示例性地，终端设备在第一网络的用户面安全策略为 PDU 会话的粒度，终端设备在第一网络的用户面安全策略为演进分组系统承载（evolved packet system bearer, EPS bearer）的粒度。

终端设备在第一网络的用户面安全策略还可以是数据网络名称（data network name, DNN）+单网络切片选择支撑信息（single network slice selection assistance information,

S-NSSAI) 粒度。

终端设备在第二网络的用户面安全策略还可以是演进型通用陆地无线接入网无线接入承载 (evolved universal terrestrial radio access network radio access bearer, E-RAB) 粒度或接入点名称 (access point name, APN) 粒度。

5 结合第一方面, 在第一方面的某些实现方式中, 该方法还包括: 该会话管理网元获取第三指示信息, 该第三指示信息用于指示执行用户面安全策略映射; 该会话管理网元将所述终端设备在该第一网络中的用户面安全策略映射为该终端设备在该第二网络的用户面安全策略, 包括: 该会话管理网元根据该第三指示信息, 将该终端设备在该第一网络中的用户面安全策略映射为该终端设备在该第二网络的用户面安全策略。

10 基于上述技术方案, 会话管理网元在接收到第三指示信息的情况下, 将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略, 可以避免会话管理网元进行不必要的映射, 优化了会话管理网元的处理逻辑。若会话管理网元在没有接收到第三指示信息的情况下, 会话管理网元直接将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略, 若第二网络不支持开启用户面完整性保护, 15 则终端设备不能从第一网络切换至第二网络, 会话管理网元进行的映射就是不必要的映射。

结合第一方面, 在第一方面的某些实现方式中, 该方法还包括: 该会话管理网元通过该接入和移动性管理功能网元将该承载上下文发送给该第二网络中的目标移动管理实体; 其中, 该目标移动管理实体为将该会话切换到该第二网络时为该终端设备服务的网元。

20 基于上述技术方案, 会话管理网元将终端设备在第二网络的用户面安全策略发送给目标移动管理实体, 使得终端设备从第一网络切换至第二网络的过程中, 目标移动管理实体可以根据终端设备在第二网络的用户面安全策略确定终端设备在第二网络的用户面安全激活状态, 从而有利于实现终端设备成功从第一网络切换至第二网络。

结合第一方面, 在第一方面的某些实现方式中, 该方法还包括: 该会话管理网元根据 25 该第一指示信息, 不考虑该终端设备在该第一网络的用户面安全策略, 向统一数据管理网元发送该会话管理网元在 S5/S8 接口上的全量域名。

基于上述技术方案, 会话管理网元根据第一指示信息向统一数据管理网元发送会话管理网元在 S5/S8 接口上的全量域名, 可以解除在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下, 终端设备在第一网络中建立的会话不能切换到第二网络中的 30 限制。因为, 按照现有方案, 在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下, 会话管理网元不会向统一数据管理网元发送会话管理网元在 S5/S8 接口上的全量域名。从而, 终端设备在第一网络中建立的会话后续也不能切换到第二网络。

其中, 会话管理网元不考虑第一网络的用户面安全策略可以理解为, 会话管理网元不考虑第一网络的用户面安全策略的取值。也就是说, 不论第一网络的用户面安全策略的取值是什么, 会话管理网元可以根据第一指示信息向统一数据管理网元发送 S5/S8 接口的全量域名。例如, 会话管理网元可以在第一网络的用户面安全策略包括开启用户面完整性保护 (即用户面完整性保护取值为需要 (required)) 的情况下, 根据第一指示信息向统一 35 数据管理网元发送 S5/S8 接口的全量域名。

应理解, 在终端设备不支持与第二网络互通和/或终端设备在第一网络的会话不支持 40 与第二网络互通的情况下, 会话管理网元不会向统一数据管理网元发送 S5/S8 接口的全量

域名。因此，会话管理网元根据第一指示信息，不考虑第一网络的用户面安全策略，向统一数据管理网元发送 S5/S8 接口的全量域名，可以理解为，在终端设备支持与第二网络互通，以及终端设备在第一网络的会话支持与第二网络互通的情况下，会话管理网元根据第一指示信息，不考虑第一网络的用户面安全策略，向统一数据管理网元发送 S5/S8 接口的全量域名。

结合第一方面，在第一方面的某些实现方式中，该会话管理网元获取第一指示信息，包括：该会话管理网元接收来自该接入和移动性管理功能网元的该第一指示信息。

示例性地，该第一指示信息包含在协议数据单元会话建立会话管理上下文请求消息中。

结合第一方面，在第一方面的某些实现方式中，该会话管理网元获取第一指示信息，包括：该会话管理网元通过该接入和移动性管理功能网元接收来自该终端设备的该第一指示信息。

示例性地，该第一指示信息包含在协议数据单元会话建立请求消息中。

第二方面，提供了一种通信方法，该方法可以包括：第一网络中的接入和移动性管理功能网元接收来自终端设备的注册请求消息，该注册请求消息包括第二指示信息，其中，该第二指示信息用于指示终端设备在第二网络中支持用户面完整性保护；在该终端设备在该第一网络建立会话的过程中，该接入和移动性管理功能网元根据该第二指示信息，向会话管理网元发送第一指示信息，该第一指示信息用于指示在第二网络中支持用户面完整性保护；该接入和移动性管理功能网元接收第一请求消息，该第一请求消息用于请求为该会话分配承载标识，该承载标识与该终端设备在该第二网络的承载上下文对应；该接入和移动性管理功能网元向该会话管理网元发送第一响应消息，该第一响应消息包括该承载标识。

基于上述技术方案，接入和移动性管理功能网元将第一指示信息发送给会话管理网元，使得会话管理网元可以根据第一指示信息解除在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下，终端设备在第一网络中建立的会话不能切换到第二网络中的限制。因为，按照现有方案，在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下，会话管理网元不会向接入和移动性管理功能网元请求承载标识，从而接入和移动性管理功能网元本地也不会保存有相应的承载标识，这种情况下，后续接入和移动性管理功能网元接收到来自第一网络的接入网设备的切换需求时，是不会执行将终端设备在第一网络中建立的会话切换到第二网络的相关流程的。

示例性地，第一网络是第五代网络，第二网络是第四代网络，终端设备在第一网络的会话是协议数据单元会话，承载上下文是演进分组系统承载上下文。

示例性地，终端设备在第一网络建立会话的过程包括，终端设备发送 PDU 会话建立请求消息之后至终端设备接收 PDU 会话建立接受消息之前。

结合第二方面，在第二方面的某些实现方式中，该方法还包括：该接入和移动性管理功能网元向该会话管理网元发送第二请求消息；该接入和移动性管理功能网元接收来自该会话管理网元的第二响应消息，该第二响应消息包括该承载上下文，该承载上下文包括终端设备在该第二网络的用户面安全策略，该第二网络的用户面安全策略是根据该终端设备在该第一网络的用户面安全策略得到的；该接入和移动性管理功能网元向该第二网络中的目标移动管理实体发送该承载上下文，该目标移动管理实体为将该会话切换到该第二

网络时为该终端设备服务的网元。

基于上述技术方案，接入和移动性管理功能网元可以从会话管理网元获取终端设备在第二网络的用户面安全策略，并可以将终端设备在第二网络的用户面安全策略发送给目标移动管理实体，从而解决了在终端设备从第一网络切换至第二网络的过程中，接入和移动性管理功能网元如何获取终端设备在第二网络的用户面安全策略的问题，有助于终端设备成功从第一网络切换至第二网络。

示例性地，终端设备在第一网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略，终端设备在第二网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略。

示例性地，该第一网络的用户面安全策略的粒度为协议数据单元会话的粒度；该第二网络的用户面安全策略的粒度为演进分组系统承载的粒度。

终端设备在第一网络的用户面安全策略还可以是数据网络名称+单网络切片选择支撑信息粒度。

终端设备在第二网络的用户面安全策略还可以是演进型通用陆地无线接入网无线接入承载粒度或接入点名称粒度。

示例性地，第二请求消息为协议数据单元会话上下文请求消息，第二响应消息为协议数据单元会话上下文响应消息。

结合第二方面，在第二方面的实现方式中，该第二请求消息包括第三指示信息，该第三指示信息用于指示执行用户面安全策略映射，该方法还包括：该接入和移动性管理功能网元根据第二本地策略，确定在该第二请求消息中携带该第三指示信息；该第二本地策略包括以下一项或多项：该会话是否支持与该第二网络互通，该目标移动管理实体是否支持用户面完整性保护，该目标移动管理实体为将所述会话切换到所述第二网络时为所述终端设备服务的网元。

基于上述技术方案，接入和移动性管理功能网元向会话管理网元发送第三指示信息，使得会话管理网元在接收到第三指示信息的情况下，将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略，可以避免会话管理网元进行不必要的映射，优化了会话管理网元的处理逻辑。若会话管理网元在没有接收到第三指示信息的情况下，会话管理网元直接将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略，若第二网络不支持开启用户面完整性保护，则终端设备不能从第一网络切换至第二网络，会话管理网元进行的映射就是不必要的映射。

结合第二方面，在第二方面的实现方式中，该方法还包括：该接入和移动性管理功能网元根据第一本地策略，确定向该会话管理网元发送该第一指示信息，该第一本地策略包括该会话是否支持与该第二网络互通。

第三方面，提供了一种通信方法，该方法可以包括：终端设备向第一网络中的接入和移动性管理功能网元发送第二指示信息，该第二指示信息用于指示该终端设备在第二网络中支持用户面完整性保护；该终端设备接收来自该第二网络的接入网设备发送的无线资源控制重配置，该无线资源控制重配置包括开启用户面完整性保护的指示信息。

基于上述技术方案，终端设备向第一网络中的接入和移动性管理功能网元发送第二指示信息，可以实现终端设备成功从第一网络切换至第二网络。

示例性地，该第二指示信息包含在注册请求消息中。

示例性地, 该第二指示信息包含在协议数据单元会话建立请求消息中。

第四方面, 提供了一种通信方法, 该方法可以包括: 会话管理网元接收来自第一网络的接入和移动性管理功能网元的第二请求消息; 响应于该第二请求消息, 该会话管理网元向接入和移动性管理功能网元发送第二响应消息, 该第二响应消息包括承载上下文, 该承载上下文包括该终端设备在第二网络的用户面安全策略, 该第二网络的用户面安全策略是根据该终端设备在该第一网络的用户面安全策略得到的。

基于上述技术方案, 会话管理网元将终端设备在第二网络的用户面安全策略发送给接入和移动性管理功能网元, 从而解决了在终端设备从第一网络切换至第二网络的过程中, 接入和移动性管理功能网元如何获取终端设备在第二网络的用户面安全策略的问题, 有助于终端设备成功从第一网络切换至第二网络。

示例性地, 在终端设备从第一网络切换至第二网络的过程中, 会话管理网元接收来自第一网络的接入和移动性管理功能网元的第二请求消息, 并响应于第二请求消息, 向接入和移动性管理功能网元发送第二响应消息。

示例性地, 第一网络是第五代网络, 第二网络是第四代网络, 承载上下文是演进分组系统承载上下文。

示例性地, 终端设备在第一网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略, 终端设备在第二网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略。

示例性地, 终端设备在第一网络的用户面安全策略为协议数据单元会话的粒度, 终端设备在第一网络的用户面安全策略为演进分组系统承载的粒度。

终端设备在第一网络的用户面安全策略还可以是数据网络名称+单网络切片选择支撑信息粒度。

终端设备在第二网络的用户面安全策略还可以是演进型通用陆地无线接入网无线接入承载粒度或接入点名称粒度。

示例性地, 第二请求消息为协议数据单元会话上下文请求消息, 第二响应消息为协议数据单元会话上下文响应消息。

结合第四方面, 在第四方面的某些实现方式中, 该方法还包括: 该会话管理网元将该第一网络的用户面安全策略映射为该第二网络的用户面安全策略; 该会话管理网元将该第二网络的用户面安全策略保存在该承载上下文中。

基于上述技术方案, 会话管理网元可以将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略, 并可以将终端设备在第二网络的用户面安全策略保存在承载上下文。进而, 在终端设备从第一网络切换至第二网络的过程中, 第一网络中的接入和移动性管理功能网元从会话管理网元获取所述承载上下文, 进而将获取到的承载上下文发送给第二网络的移动管理实体, 从而有助于实现终端设备从第一网络切换至第二网络。

结合第四方面, 在第四方面的某些实现方式中, 该方法还包括: 该会话管理网元获取第一指示信息, 该第一指示信息用于指示在该第二网络中支持用户面完整性保护; 该会话管理网元将该第一网络的用户面安全策略映射为该第二网络的用户面安全策略, 包括: 该会话管理网元在接收到该第一指示信息的情况下, 将该第一网络的用户面安全策略映射为该第二网络的用户面安全策略。

基于上述技术方案，会话管理网元在接收到第一指示信息的情况下，可以不用考虑第一网络的用户面安全策略，直接将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略，优化了会话管理网元的处理逻辑。若会话管理网元在没有接收到第一指示信息的情况下，则会话管理网元在做映射之前，可选的需要先判断第一网络的用户面安全策略是否要求开启用户面完整性保护，如果不要求开启用户面完整性保护，将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略。

示例性地，该第一网络的用户面安全策略是会话管理网元本地存储的，或者，该第一网络的用户面安全策略是会话管理网元从统一数据管理网元获取的。

结合第四方面，在第四方面的某些实现方式中，该方法还包括：该会话管理网元获取第一指示信息，该第一指示信息用于指示在该第二网络中支持用户面完整性保护；该会话管理网元根据该第一指示信息，向该接入和移动性管理功能网元请求该承载标识，该承载标识与该承载上下文对应。

示例性地，在终端设备在第一网络中建立会话的过程中，会话管理网元获取第一指示信息。示例性地，终端设备在第一网络建立会话的过程包括，终端设备发送 PDU 会话建立请求消息之后至终端设备接收 PDU 会话建立接受消息之前。

在一种可能的实现方式中，该会话管理网元根据该第一指示信息，不考虑该第一网络的用户面安全策略，向该接入和移动性管理功能网元发送第一请求消息。

其中，会话管理网元不考虑第一网络的用户面安全策略可以理解为，会话管理网元不考虑第一网络的用户面安全策略的取值。也就是说，不论第一网络的用户面安全策略的取值是什么，会话管理网元可以根据第一指示信息向接入和移动性管理功能网元发送第一请求消息。例如，会话管理网元可以在第一网络的用户面安全策略包括开启用户面完整性保护（即用户面完整性保护取值为需要（required））的情况下，根据第一指示信息向接入和移动性管理功能网元发送第一请求消息。

应理解，在终端设备是非第三代合作伙伴计划接入，且终端设备请求建立的会话不支持与第二网络基于 N26 接口的互通的情况下，会话管理网元不会向接入和移动性管理功能网元发送第一请求消息。因此，会话管理网元根据第一指示信息，不考虑第一网络的用户面安全策略，向接入和移动性管理功能网元发送第一请求消息，可以理解为，在终端设备是第三代合作伙伴计划接入，以及终端设备请求建立的会话支持与第二网络基于 N26 接口的互通情况下，会话管理网元根据第一指示信息，不考虑第一网络的用户面安全策略，向接入和移动性管理功能网元发送第一请求消息。

基于上述技术方案，会话管理网元根据第一指示信息可以解除在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下，终端设备在第一网络中建立的会话不能切换到第二网络中的限制。因为，按照现有方案，在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下，会话管理网元不会向接入和移动性管理功能网元请求承载标识，从而接入和移动性管理功能网元本地也不会保存有相应的承载标识，这种情况下，后续接入和移动性管理功能网元接收到来自第一网络的接入网设备的切换需求时，是不会执行将终端设备在第一网络中建立的会话切换到第二网络的相关流程的。

结合第四方面，在第四方面的某些实现方式中，该方法还包括：该会话管理网元根据该第一指示信息，不考虑该终端设备在该第一网络的用户面安全策略，向统一数据管理网

元发送该会话管理网络网元在 S5/S8 接口上的全量域名。

基于上述技术方案，会话管理网元根据第一指示信息向统一数据管理网元发送会话管理网元在 S5/S8 接口上的全量域名，可以解除在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下，终端设备在第一网络中建立的会话不能切换到第二网络中的限制。因为，按照现有方案，在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下，会话管理网元不会向统一数据管理网元发送会话管理网元在 S5/S8 接口上的全量域名。从而，终端设备在第一网络中建立的会话后续也不能切换到第二网络。

其中，会话管理网元不考虑第一网络的用户面安全策略可以理解为，会话管理网元不考虑第一网络的用户面安全策略的取值。也就是说，不论第一网络的用户面安全策略的取值是什么，会话管理网元可以根据第一指示信息向统一数据管理网元发送 S5/S8 接口的全量域名。例如，会话管理网元可以在第一网络的用户面安全策略包括开启用户面完整性保护（即用户面完整性保护取值为需要（required））的情况下，根据第一指示信息向统一数据管理网元发送 S5/S8 接口的全量域名。

应理解，在终端设备不支持与第二网络互通和/或终端设备在第一网络的会话不支持与第二网络互通的情况下，会话管理网元不会向统一数据管理网元发送 S5/S8 接口的全量域名。因此，会话管理网元根据第一指示信息，不考虑第一网络的用户面安全策略，向统一数据管理网元发送 S5/S8 接口的全量域名，可以理解为，在终端设备支持与第二网络互通，以及终端设备在第一网络的会话支持与第二网络互通的情况下，会话管理网元根据第一指示信息，不考虑第一网络的用户面安全策略，向统一数据管理网元发送 S5/S8 接口的全量域名。

结合第四方面，在第四方面的某些实现方式中，该会话管理网元获取第一指示信息，包括：该会话管理网元接收来自该接入和移动性管理功能网元的该第一指示信息。

示例性地，该第一指示信息包含在协议数据单元会话建立会话管理上下文请求消息中。

结合第四方面，在第四方面的某些实现方式中，该会话管理网元获取第一指示信息，包括：该会话管理网元通过该接入和移动性管理功能网元接收来自该终端设备的该第一指示信息。

示例性地，该第一指示信息包含在协议数据单元会话建立请求消息中。

第五方面，提供了一种通信方法，该方法可以包括：第一网络的接入和移动性管理功能网元向会话管理网元发送第二请求消息；该接入和移动性管理功能网元接收来自该会话管理网元的第二响应消息，该第二响应消息包括承载上下文，该承载上下文包括该终端设备在第二网络的用户面安全策略，该第二网络的用户面安全策略是根据该终端设备在第二网络的用户面安全策略得到的；该接入和移动性管理功能网元向该第二网络中为该终端设备服务的目标移动管理实体发送该承载上下文。

基于上述技术方案，接入和移动性管理功能网元可以从会话管理网元获取终端设备在第二网络的用户面安全策略，并可以将终端设备在第二网络的用户面安全策略发送给目标移动管理实体，从而解决了在终端设备从第一网络切换至第二网络的过程中，接入和移动性管理功能网元如何获取终端设备在第二网络的用户面安全策略的问题，有助于终端设备成功从第一网络切换至第二网络。

示例性地，终端设备在第一网络的用户面安全策略包括用户面加密保护策略和/或用

户面完整性保护策略,终端设备在第二网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略。

示例性地,该第一网络的用户面安全策略的粒度为协议数据单元会话的粒度;该第二网络的用户面安全策略的粒度为演进分组系统承载的粒度。

5 终端设备在第一网络的用户面安全策略还可以是数据网络名称+单网络切片选择支撑信息粒度。

终端设备在第二网络的用户面安全策略还可以是演进型通用陆地无线接入网无线接入承载粒度或接入点名称粒度。

10 示例性地,第二请求消息为协议数据单元会话上下文请求消息,第二响应消息为协议数据单元会话上下文响应消息。

结合第五方面,在第五方面的某些实现方式中,该方法还包括:该接入和移动性管理功能网元接收来自该终端设备的第二指示信息,该第二指示信息用于指示该终端设备在该第二网络中支持用户面完整性保护;该接入和移动性管理功能网元根据该第二指示信息向该会话管理网元发送第一指示信息,该第一指示信息用于指示在该第二网络中支持用户面完整性保护。

15 示例性地,该第二指示信息包含在注册请求消息中,该第一指示信息包含在协议数据单元会话建立会话管理上下文请求消息中。

结合第五方面,在第五方面的某些实现方式中,该方法还包括:该接入和移动性管理功能网元根据第一本地策略确定是否向该会话管理网元发送该第一指示信息,该第一本地策略包括该终端设备在该第一网络的会话是否支持与该第二网络互通。

20 第六方面,提供了一种通信装置,包括用于执行上述第一方面或第一方面中任一种实现方式中的方法的各步骤的单元。

第七方面,提供了一种通信装置,包括用于执行上述第二方面或第二方面中任一种实现方式中的方法的各步骤的单元。

25 第八方面,提供了一种通信装置,包括用于执行上述第三方面或第三方面中任一种实现方式中的方法的各步骤的单元。

第九方面,提供了一种通信装置,该通信装置可以包括收发单元,该收发单元用于接收来自第一网络的接入和移动性管理功能网元的第二请求消息;响应于该第二请求消息,该收发单元还用于向接入和移动性管理功能网元发送第二响应消息,该第二响应消息包括承载上下文,该承载上下文包括该终端设备在第二网络的用户面安全策略,该第二网络的用户面安全策略是根据该终端设备在该第一网络的用户面安全策略得到的。

30 示例性地,在终端设备从第一网络切换至第二网络的过程中,该收发单元用于接收来自第一网络的接入和移动性管理功能网元的第二请求消息,并响应于第二请求消息,向接入和移动性管理功能网元发送第二响应消息。

35 示例性地,第一网络是第五代网络,第二网络是第四代网络,承载上下文是演进分组系统承载上下文。

示例性地,终端设备在第一网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略,终端设备在第二网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略。

40 示例性地,终端设备在第一网络的用户面安全策略为协议数据单元会话的粒度,终端

设备在第一网络的用户面安全策略为演进分组系统承载的粒度。

终端设备在第一网络的用户面安全策略还可以是数据网络名称+单网络切片选择支撑信息粒度。

5 终端设备在第二网络的用户面安全策略还可以是演进型通用陆地无线接入网无线接入承载粒度或接入点名称粒度。

示例性地，第二请求消息为协议数据单元会话上下文请求消息，第二响应消息为协议数据单元会话上下文响应消息。

10 结合第九方面，在第九方面的某些实现方式中，该通信装置还包括处理单元，该处理单元用于将该第一网络的用户面安全策略映射为该第二网络的用户面安全策略；该处理单元还用于将该第二网络的用户面安全策略保存在该承载上下文中。

结合第九方面，在第九方面的某些实现方式中，该收发单元还用于获取第一指示信息，该第一指示信息用于指示在该第二网络中支持用户面完整性保护；该处理单元具体用于在接收到该第一指示信息的情况下，将该第一网络的用户面安全策略映射为该第二网络的用户面安全策略。

15 示例性地，该第一网络的用户面安全策略是会话管理网元本地存储的，或者，该第一网络的用户面安全策略是会话管理网元从统一数据管理网元获取的。

20 结合第九方面，在第九方面的某些实现方式中，该收发单元还用于获取第一指示信息，该第一指示信息用于指示在该第二网络中支持用户面完整性保护；该收发单元还用于根据该第一指示信息，向该接入和移动性管理功能网元请求该承载标识，该承载标识与该承载上下文对应。

示例性地，在终端设备在第一网络中建立会话的过程中，收发单元用于获取第一指示信息。示例性地，终端设备在第一网络建立会话的过程包括，终端设备发送 PDU 会话建立请求消息之后至终端设备接收 PDU 会话建立接受消息之前。

25 在一种可能的实现方式中，该收发单元用于根据该第一指示信息，不考虑该第一网络的用户面安全策略，向该接入和移动性管理功能网元发送第一请求消息。

结合第九方面，在第九方面的某些实现方式中，该收发单元还用于根据该第一指示信息，不考虑该终端设备在该第一网络的用户面安全策略，向统一数据管理网元发送该会话管理网络网元在 S5/S8 接口上的全量域名。

30 结合第九方面，在第九方面的某些实现方式中，该会话管理网元获取第一指示信息，包括：该会话管理网元接收来自该接入和移动性管理功能网元的该第一指示信息。

示例性地，该第一指示信息包含在协议数据单元会话建立会话管理上下文请求消息中。

35 结合第九方面，在第九方面的某些实现方式中，该会话管理网元获取第一指示信息，包括：该会话管理网元通过该接入和移动性管理功能网元接收来自该终端设备的该第一指示信息。

示例性地，该第一指示信息包含在协议数据单元会话建立请求消息中。

40 第十方面，提供了一种通信装置，该通信装置可以包括收发单元，该收发单元用于向会话管理网元发送第二请求消息；该收发单元还用于接收来自该会话管理网元的第二响应消息，该第二响应消息包括承载上下文，该承载上下文包括该终端设备在第二网络的用户面安全策略，该第二网络的用户面安全策略是根据该终端设备在第二第一网络的用户面安

全策略得到的；该收发单元还用于向该第二网络中为该终端设备服务的目标移动管理实体发送该承载上下文。

5 示例性地，终端设备在第一网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略，终端设备在第二网络的用户面安全策略包括用户面加密保护策略和/或用户面完整性保护策略。

示例性地，该第一网络的用户面安全策略的粒度为协议数据单元会话的粒度；该第二网络的用户面安全策略的粒度为演进分组系统承载的粒度。

终端设备在第一网络的用户面安全策略还可以是数据网络名称+单网络切片选择支撑信息粒度。

10 终端设备在第二网络的用户面安全策略还可以是演进型通用陆地无线接入网无线接入承载粒度或接入点名称粒度。

示例性地，第二请求消息为协议数据单元会话上下文请求消息，第二响应消息为协议数据单元会话上下文响应消息。

15 结合第十方面，在第十方面的某些实现方式中，该收发单元还用于接收来自该终端设备的第二指示信息，该第二指示信息用于指示该终端设备在该第二网络中支持用户面完整性保护；该收发单元还用于根据该第二指示信息向该会话管理网元发送第一指示信息，该第一指示信息用于指示在该第二网络中支持用户面完整性保护。

示例性地，该第二指示信息包含在注册请求消息中，该第一指示信息包含在协议数据单元会话建立会话管理上下文请求消息中。

20 结合第十方面，在第十方面的某些实现方式中，该通信装置还包括处理单元，该处理单元用于根据第一本地策略确定是否向该会话管理网元发送该第一指示信息，该第一本地策略包括该终端设备在该第一网络的会话是否支持与该第二网络互通。

25 第十一方面，本申请提供了一种通信设备，包括处理器。该处理器与存储器耦合，可用于执行存储器中的指令，以实现上述第一方面或第一方面中任一种可能实现方式中的方法，或者实现上述第四方面或第四方面中任一种可能实现方式中的方法。其中，该通信设备还包括存储器。其中，该通信设备还包括通信接口，处理器与通信接口耦合。

在一种实现方式中，该通信设备为会话管理网元。当该通信设备为会话管理网元时，所述通信接口可以是收发器，或，输入/输出接口。

30 在另一种实现方式中，该通信设备为配置于会话管理网元中的芯片或芯片系统。当该通信设备为配置于会话管理网元中的芯片或芯片系统时，该通信接口可以是输入/输出接口。

其中，该收发器可以为收发电路。其中，该输入/输出接口可以为输入/输出电路。

35 第十二方面，本申请提供了一种通信设备，包括处理器。该处理器与存储器耦合，可用于执行存储器中的指令，以实现上述第二方面或第二方面中任一种可能实现方式中的方法，或者实现上述第五方面或第五方面中任一种可能实现方式中的方法。其中，该通信设备还包括存储器。其中，该通信设备还包括通信接口，处理器与通信接口耦合。

在一种实现方式中，该通信设备为接入和移动性管理功能网元。当该通信设备为接入和移动性管理功能网元时，所述通信接口可以是收发器，或，输入/输出接口。

40 在另一种实现方式中，该通信设备为配置于接入和移动性管理功能网元中的芯片或芯片系统。当该通信设备为配置于接入和移动性管理功能网元中的芯片或芯片系统时，该通

信接口可以是输入/输出接口。

其中，该收发器可以为收发电路。其中，该输入/输出接口可以为输入/输出电路。

第十三方面，本申请提供了一种通信设备，包括处理器。该处理器与存储器耦合，可用于执行存储器中的指令，以实现上述第三方面或第三方面中任一种可能实现方式中的方法。其中，该通信设备还包括存储器。其中，该通信设备还包括通信接口，处理器与通信接口耦合。

在一种实现方式中，该通信设备为终端设备。当该通信设备为终端设备时，所述通信接口可以是收发器，或，输入/输出接口。

在另一种实现方式中，该通信设备为配置于终端设备中的芯片或芯片系统。当该通信设备为配置于终端设备中的芯片或芯片系统时，该通信接口可以是输入/输出接口。

其中，该收发器可以为收发电路。其中，该输入/输出接口可以为输入/输出电路。

第十四方面，本申请提供了一种处理器，包括：输入电路、输出电路和处理电路。所述处理电路用于通过所述输入电路接收信号，并通过所述输出电路发射信号，使得所述处理器执行上述各个方面中的方法。

在具体实现过程中，上述处理器可以为芯片，输入电路可以为输入管脚，输出电路可以为输出管脚，处理电路可以为晶体管、门电路、触发器和各种逻辑电路等。输入电路所接收的输入的信号可以是由例如但不限于接收器接收并输入的，输出电路所输出的信号可以是例如但不限于输出给发射器并由发射器发射的，且输入电路和输出电路可以是同一电路，该电路在不同的时刻分别用作输入电路和输出电路。本申请实施例对处理器及各种电路的具体实现方式不做限定。

第十五方面，本申请提供了一种处理装置，包括通信接口和处理器。所述通信接口与所述处理器耦合。所述通信接口用于输入和/或输出信息。所述信息包括指令或数据中的至少一项。所述处理器用于执行计算机程序，以使得所述处理装置执行上述各个方面中的方法。

第十六方面，本申请提供了一种处理装置，包括处理器和存储器。该处理器用于读取存储器中存储的指令，并可通过接收器接收信号，通过发射器发射信号，以使得所述处理装置执行上述各个方面中的方法。

可选地，上述处理器为一个或多个。如果有存储器，存储器也可以为一个或多个。

可选地，所述存储器可以与所述处理器集成在一起，或者所述存储器与处理器分离设置。

在具体实现过程中，存储器可以为非瞬时性（non-transitory）存储器，例如只读存储器（read only memory, ROM），其可以与处理器集成在同一块芯片上，也可以分别设置在不同的芯片上，本申请实施例对存储器的类型以及存储器与处理器的设置方式不做限定。

应理解，相关的信息交互过程，例如发送指示信息可以为从处理器输出指示信息的过程，接收指示信息可以为向处理器输入接收到的指示信息的过程。具体地，处理输出的信息可以输出给发射器，处理器接收的输入信息可以来自接收器。其中，发射器和接收器可以统称为收发器。

上述第十五方面和第十六方面中的装置可以是芯片，该处理器可以通过硬件来实现也可以通过软件来实现，当通过硬件实现时，该处理器可以是逻辑电路、集成电路等；当通

过软件来实现时，该处理器可以是一个通用处理器，通过读取存储器中存储的软件代码来实现，该存储器可以集成在处理器中，可以位于该处理器之外，独立存在。

第十七方面，本申请提供了一种计算机程序产品，所述计算机程序产品包括：计算机程序（也可以称为代码，或指令），当所述计算机程序被运行时，使得计算机执行上述各个方面中的方法。

第十八方面，本申请提供了一种计算机可读介质，所述计算机可读介质存储有计算机程序（也可以称为代码，或指令）当其在计算机上运行时，使得计算机执行上述各个方面中的方法。

第十九方面，本申请提供了一种通信系统，包括前述的会话管理网元、终端设备和接入和移动性管理功能网元。

附图说明

图 1 是适用于本申请实施例的一种网络架构的示意图。

图 2 是本申请实施例提供的通信方法的示意性流程图。

图 3 是本申请另一实施例提供的通信方法的示意性流程图。

图 4 是本申请另一实施例提供的通信方法的示意性流程图。

图 5 是本申请另一实施例提供的通信方法的示意性流程图。

图 6 是本申请另一实施例提供的通信方法的示意性流程图。

图 7 是本申请另一实施例提供的通信方法的示意性流程图。

图 8 是本申请实施例提供的通信装置的示意性框图。

图 9 是本申请实施例提供的通信设备的示意性框图。

具体实施方式

下面将结合附图，对本申请中的技术方案进行描述。

本申请实施例的技术方案可以应用于各种通信系统，例如：长期演进（long term evolution, LTE）系统、LTE 频分双工（frequency division duplex, FDD）系统、LTE 时分双工（time division duplex, TDD）系统、通用移动通信系统（universal mobile telecommunication system, UMTS）、全球互联微波接入（worldwide interoperability for microwave access, WiMAX）通信系统、第五代（5th generation, 5G）系统、新无线（new radio, NR）或未来网络等，本申请中所述的 5G 移动通信系统包括非独立组网（non-standalone, NSA）的 5G 移动通信系统或独立组网（standalone, SA）的 5G 移动通信系统。本申请提供的技术方案还可以应用于未来的通信系统，如第六代移动通信系统。通信系统还可以是陆上公用移动通信网（public land mobile network, PLMN）网络、设备到设备（device-to-device, D2D）通信系统、机器到机器（machine to machine, M2M）通信系统、物联网（internet of Things, IoT）通信系统或者其他通信系统。

图 1 是适用于本申请实施例的网络架构。具体地，在系统架构 100 中，可以包括 4G 网络中的网元和 5G 网络中的网元。系统架构 100 中的某些模块包含有 4G 网络中的网元和 5G 网络中的网元的功能，例如用户面功能（user plane function, UPF）+分组数据网网关用户面功能（packet data network gateway user plane function, PGW-U）实体、会话管理功能（session management function, SMF）+分组数据网网关控制面功能（packet data network

gateway control plane function, PGW-C) 实体、策略控制功能 (policy control function, PCF) +策略和计费规则功能 (policy and charging rules function, PCRF) 实体、归属签约用户服务器 (home subscriber server, HSS) +统一数据管理 (unified data management, UDM) 实体。

5 UPF+PGW-U 实体: 用于用户数据的传输管理, 互通系统架构中, 该模块既能用于 4G 的数据传输, 又能提供 5G 的数据传输功能。

SMF+PGW-C 实体: 用于会话的建立、删除和修改管理, 互通系统架构中, 该模块既能提供 4G 的会话管理功能, 又能提供 5G 的会话管理功能。

10 PCF+PCRF 实体: 用于策略和计费控制, 互通系统架构中, 该模块既能为终端提供 4G 的策略和计费控制, 又能提供 5G 的策略和计费控制。

HSS+UDM 实体: 用于存储用户的签约数据, 互通系统架构中, 该模块既存储有终端的 4G 的签约信息, 又存储有终端的 5G 的签约信息。

15 应理解, 上述“+”表示合设, UPF 为 5G 网络的用户面功能, PGW-U 是与 UPF 对应的 4G 网络的网关用户面功能; SMF 是 5G 网络的会话管理功能, PGW-C 是与 SMF 对应的 4G 网络中的网关控制面功能; PCF 是 5G 网络的策略控制功能、PCRF 是与 PCF 对应的 4G 网络的策略计费规则功能。这里的“合设”是指同一个网元可以同时具备两个网络功能实体的功能。

20 本申请实施例中, 为方便表述, 将 HSS+UDM 实体称之为用户数据管理网元, 将 SMF+PGW-C 称之为会话管理网元, 将 UPF+PGW-U 称之为用户面功能网元, 在此进行统一说明, 以下不再赘述。当然, 上述合设后的网络设备也可以用其他名称, 本申请实施例对此不作具体限定。

此外, 在系统架构 100, 还可以包括: 4G 网络中的移动管理实体 (mobile management entity, MME) 和服务网关 (serving gateway, SGW) 以及 5G 网络中的接入和移动性管理功能 (access and mobility management function, AMF) 实体。

25 MME: 用于用户的移动性管理。例如, 主要包含用户的附着管理、可达性管理、移动性管理、寻呼管理、接入认证和授权非接入层信令的加密和完整性保护等。

SGW: 用户面的网关, 与演进型通用陆地无线接入网 (evolved universal terrestrial radio access network, E-UTRAN) 的用户面终结点。管理数据包的路由和传输, 添加传输层的包标签等。

30 AMF 实体: 用于用户的接入和移动性管理, 主要包含用户的注册管理、可达性管理、移动性管理、寻呼管理、接入认证和授权非接入层信令的加密和完整性保护等。

其中, 终端通过 E-UTRAN 接入 4G 网络, 终端通过下一代无线接入网 (next generation radio access network, NG-RAN) 设备接入 5G 网络。

NG-RAN 设备: 用于为终端提供无线空口接入核心网络, 从而获取对应的业务。

35 E-UTRAN: 用于无线资源管理, 为终端建立、修改或删除空口资源, 为终端提供数据和信令的传输等。

下面将介绍在系统架构 100 中, 上述模块之间的通信接口。

S1-MME 接口: MME 和 E-UTRAN 之间的控制面接口。

S1-U 接口: S-GW 和 E-UTRAN 之间的用户面接口。

40 S5-U 接口: SGW 和 PGW-U 之间的用户面接口, 用于传输终端的用户面数据。

S5-C 接口: SGW 和 PGW-U 之间的控制面管理接口, 用于为终端建立 SGW 和 PGW-U 用户面连接。

S6a 接口: MME 与 HSS 之间的接口, 用于获取用户的签约数据和为终端执行认证和授权功能。

- 5 S11 接口: SGW 和 MME 之间的接口, 用于建立用户面的承载。
N1 接口: 终端和 AMF 之间的接口, 用户非接入层的信令管理和传输。
N2 接口: NG-RAN 和 AMF 之间的接口, 用于信令的传输。
N3 接口: UPF 和 NG-RAN 之间的接口, 用于传输用户的数据。
N4 接口: SMF 和 UPF 之间的接口, 用于建立用户面的传输通道。
10 N7 接口: SMF 和 PCF 之间的接口, 用于策略控制和计费信息的制定和下发。
N8 接口: AMF 与 UDM 之间的接口, 用于获取用户的移动性相关签约信息等。
N10 接口: SMF 和 UDM 之间的接口, 用于获取用户的会话管理相关签约信息等。
N11 接口: SMF 和 AMF 之间的接口, 用于会话管理信息的传输等。
N15 接口: AMF 和 PCF 之间的接口, 用于获取接入和移动性相关的策略信息。

- 15 应理解, 在系统架构 100 中, 为了支持 4G 网络和 5G 网络的互通, 引入了第一接口。该第一接口是指 5G 网络中的 AMF 与 4G 网络中的 MME 之间的通信接口, 该第一接口可以用 N26 接口表示。系统架构对 N26 接口的支持是可选的, 只有在支持 N26 接口的互通系统架构中才能使用切换的流程来保证业务的连续性。

- 需要说明的是, 在系统架构 100 中, 各个模块之间的接口名字只是一个示例, 具体实
20 现中接口名字可能为其他名字, 本申请实施例对此不作具体限定。

- 还需要说明的是, 在系统架构 100 中, 5G 网络中的 NG-RAN 设备也可以称为接入设备, 该接入设备指的是接入核心网的设备, 例如可以是基站, 宽带网络业务网关 (broadband network gateway, BNG), 汇聚交换机, 非第三代合作伙伴计划 (3rd generation partnership project, 3GPP) 接入设备等。其中, 基站可以是包括宏基站, 微基站 (也称为小站), 中
25 继站, 接入点等在内的各种形式的基站, 本申请实施例对此不作限定。

- 当然, 在系统架构 100 中, 4G 网络和 5G 网络中还可以有其它的模块, 比如, 4G 网络中还可以包括通用分组无线系统 (general packet radio system, GPRS) 业务支撑节点 (serving GPRS support node, SGSN) 模块等, 5G 网络中还可以包括鉴权服务功能 (authentication server function, AUSF) 模块和网络切片选择功能 (network slice selection
30 function, NSSF) 模块等, 本申请实施例对此不作限定。

- 本申请实施例中所涉及到的终端 (terminal) 可以包括各种具有无线通信功能的手持设备、车载设备、可穿戴设备、计算设备或连接到无线调制解调器的其它处理设备; 还可以包括用户单元 (subscriber unit)、蜂窝电话 (cellular phone)、智能电话 (smart phone)、无线数据卡、个人数字助理 (personal digital assistant, PDA) 电脑、平板型电脑、无线调制解调器 (modem)、手持设备 (handheld)、膝上型电脑 (laptop computer)、无绳电话
35 (cordless phone) 或者无线本地环路 (wireless local loop, WLL) 台、机器类型通信 (machine type communication, MTC) 终端、用户设备 (user equipment, UE), 移动台 (mobile station, MS), 终端设备 (terminal device) 等, 为方便描述, 本申请实施例中统称为终端设备。

- 应理解, 随着终端设备的不断移动, 终端设备的位置变化可能导致终端设备在不同网络之间进行切换。例如当终端设备从 4G 网络移动到 5G 网络时, 需要由 4G 网络中的演进
40

分组系统 (evolved packet system, EPS) 承载 (bearer) 切换到 5G 网络中的协议数据单元 (protocol data network, PDU) 会话, 或者当终端设备从 5G 网络移动到 4G 网络时, 需要由 5G 网络中的 PDU 会话切换到 4G 网络中的 EPS 承载。

5 目前, 5G 网络中使用的一种安全机制为用户面安全按需保护, 用户面安全按需保护包括用户面加密保护和用户面完整性保护。用户面安全按需保护机制要求接入网设备根据从核心网设备接收到用户面安全策略判断是否开启与终端设备之间的用户面加密保护和/或用户面完整性保护。然而, 现有的 4G 网络并不支持用户面安全按需保护机制。在 4G 网络中, 接入网设备与终端设备之间的用户面安全的保护方法是固定的, 即固定为用户面加密保护开启, 用户面完整性保护不开启。

10 因此, 若 5G 网络中的 PDU 会话对应的用户面安全策略要求必须开启用户面完整性保护, 则该 PDU 会话将无法切换至 4G 网络中的 EPS 承载。因为 4G 网络的接入网设备无法为终端设备开启用户面完整性保护。

目前, 会话管理网元根据以下因素判断是否向 AMF 为请求建立的 PDU 会话请求 EPS 承载标识: 1) 接入类型是 3GPP 接入或者非 3GPP 接入, 2) 在第一网络中请求建立的会话的用户面完整性保护策略是否设置为必须开启, 3) 在第一网络中请求建立的会话支持与第二网络基于 N26 接口的互通或者支持与第二网络不基于 N26 接口的互通。当接入类型是 3GPP 接入, 且在第一网络中请求建立的会话的用户面完整性保护策略不是设置为必须开启, 且在第一网络中请求建立的会话支持与第二网络基于 N26 接口的互通时, 会话管理网元会向 AMF 为请求建立的 PDU 会话请求 EPS 承载标识。

20 目前, 会话管理网元根据以下因素判断是否向统一数据管理网元发送会话管理网元在 S5/S8 接口上的全量域名 (fully qualified domain name, FQDN): 1) 终端设备是否支持与第二网络的互通, 2) 在第一网络中请求建立的会话的用户面完整性保护策略是否设置为必须开启, 3) 在第一网络中请求建立的会话是否支持与第二网络的互通。当终端设备支持与第二网络的互通, 且在第一网络中请求建立的会话的用户面完整性保护策略不是设置为必须开启, 且在第一网络中请求建立的会话支持与第二网络的互通时, 会话管理网元向统一数据管理网元发送会话管理网元在 S5/S8 接口上的 FQDN, 否则, 不发送会话管理网元在 S5/S8 接口上的 FQDN。

30 基于此, 5G 网络在准备 EPS 承载上下文 (EPS bearer context) 的过程中, 若 PDU 会话对应的用户面安全策略包括用户面完整性开启, 则会话管理网元不会向 AMF 为该 EPS 承载上下文请求 EPS 承载标识 (EPS bearer identifier, EBI), 并且, 会话管理网元也不会向 UDM 发送会话管理网元在 S5/S8 接口上的全量域名, 进一步地, 导致该 PDU 会话不能切换至 EPS 承载。

35 在 4G 网短期内不会退网的情况下, 一旦 4G 网络也支持用户面完整性保护之后, 如何解除 5G 网络对用户面完整性保护有强制开启要求的情况下不能与 EPS 互通 (interworking) 的限制, 将成为一个亟需解决的问题。

40 此外, 虽然已经提出了, 在 5G 网络中的 PDU 会话切换至 4G 网络中的 EPS 承载的过程中, AMF 向目标 MME 发送的转发重定位请求 (forward relocation request) 消息可以携带终端设备在 4G 网络中的用户面安全策略, 但是 AMF 如何获取终端设备在 4G 网络中的用户面安全策略这一问题并未得到解决。因为, 终端设备在 5G 网络中的用户面安全策略是 PDU 会话粒度的, 而终端设备在 4G 网络中的用户面安全策略是 E-UTRAN 无线接入承

载 (E-UTRAN radio access bearer, E-RAB) 粒度。

有鉴于此, 本申请提供了一种通信方法, 以期解除 5G 网络对用户面完整性保护有强制开启要求的情况下不能与 EPS 互通的限制。

5 应理解, 下文示出的实施例并未对本申请实施例提供的方法的执行主体的具体结构特别限定, 只要能够通过运行记录有本申请实施例的方法的代码的程序, 以根据本申请实施例提供的方法进行通信即可, 例如, 本申请实施例提供的方法的执行主体可以是终端设备或核心网设备, 或者, 是终端设备或核心网设备中能够调用程序并执行程序的功能模块。

10 还需要说明的是, 下文实施例中, 会话管理网元是第一网络和第二网络中的网元, 即会话管理网元可以在第一网络中与其他第一网络中的网元通信, 也可以在第二网络中与其他第二网络中的网元通信。接入和移动性管理功能网元是第一网络中的网元, 移动管理功能实体是第二网络中的网元, 在终端设备从第一网络切换至第二网络的过程中, 第一网络中的接入和移动性管理功能网元可以与第二网络中的目标移动管理功能实体通信。

其中, 第一网络可以是 5G 网络, 第二网络可以是 4G 网络, 或者, 第一网络可以是 4G 网络, 第二网络可以是 5G 网络。

15 图 2 示出了本申请实施例提供的通信方法的示意性流程图。如图 2 所示, 方法 200 可以包括 S210 至 S240, 下面详细描述各个步骤。

S210, 会话管理网元获取第一指示信息。

具体地, 在终端设备在第一网络建立会话的过程中, 会话管理网元获取第一指示信息。终端设备在第一网络建立会话的过程包括终端设备发送会话建立请求消息之后, 终端设备与网络完成会话建立的过程。示例性地, 所述会话是协议数据单元(protocol data unit, PDU) 会话, PDU 会话建立的过程包括终端设备发送 PDU 会话建立请求消息之后完成 PDU 会话建立的过程。例如, PDU 会话建立的过程可以参考 3GPP 技术标准(technical specification, TS)23.502 中 4.3.2 节的相关内容。

25 第一指示信息用于指示在第二网络中支持用户面完整性保护。或者, 第一指示信息用于指示支持与第二网络的接入网设备的用户面完整性保护。或者, 第一指示信息用于指示支持与第二网络的接入网设备的用户面按需保护, 用户面按需保护指的是: 第二网络的接入网设备可以根据从核心网设备接收的用户面安全策略判断是否开启与终端设备之间的用户面加密保护和/或用户面完整性保护。或者, 第一指示信息用于指示支持第一网络与第二网络的接入网设备的用户面安全策略的互通, 即用于指示终端设备支持第一网络与第二网络的接入网设备的用户面完整性保护, 或者, 可以替换为支持与第二网络的接入网设备的用户面按需保护, 或者, 可以替换为支持第一网络与第二网络的接入网设备的用户面安全策略的互通, 或者, 可以替换为支持第一网络与第二网络的接入网设备的用户面安全策略的映射。

本申请实施例对会话管理网元获取第一指示信息的方式不做限定。

35 作为一个示例, 会话管理网元从接入和移动性管理功能网元接收第一指示信息。在该示例中, S210 可以包括:

S211a, 终端设备向接入和移动性管理功能网元发送第二指示信息。相应地, 在 S211a 中, 接入和移动性管理功能网元接收第二指示信息。

第二指示信息用于指示终端设备在第二网络中支持用户面完整性保护。

40 或者, 第二指示信息用于指示终端设备支持与第二网络的接入网设备的用户面完整性

5

10

15

20

25

30

35

40

Session Establishment Request) 消息包括所述第一指示信息。

一种可能的实现方式中, 终端设备向接入和移动性管理功能网元发送非接入层 (non access stratum, NAS) 消息, 所述 NAS 消息包括 N1 会话管理 (session management, SM) 容器, 所述 N1 SM 容器包括所述第一指示信息。所述接入和移动性管理功能网元向所述
5 会话管理网元发送所述 N1 SM 容器。可选的, 所述 N1 SM 容器包括所述 PDU 会话建立请求, 且 PDU 会话建立请求包括所述第一指示信息。

S220, 会话管理网元根据第一指示信息, 向所述接入和移动性管理功能网元发送请求消息#1 (第一请求消息的一例)。相应地, 在 S220 中, 所述接入和移动性管理功能网元接收所述请求消息#1。

10 请求消息#1 用于请求承载标识, 承载标识与承载上下文对应, 承载上下文与第二网络对应。

可选的, 请求消息#1 包含会话标识, 请求消息#1 用于请求为该会话分配承载标识。

示例性地, 第一网络是 5G 网络, 第二网络是 4G 网络, 会话为 PDU 会话, 会话标识为 PDU 会话 ID, 承载为 EPS 承载, 承载标识为 EBI, 请求消息#1 为 EBI 分配请求
15 (Namf_Communication_EBIAssignment Request) 消息。

可选的, 当第一指示信息指示支持与第二网络的接入网设备的用户面完整性保护时, 会话管理网元根据第一指示信息向接入和移动性管理功能网元发送请求消息#1。

具体地, 会话管理网元根据第一指示信息, 向接入和移动性管理功能网元发送请求消息#1, 包括: 会话管理网元根据第一指示信息, 不考虑终端设备在第一网络的用户面安全策略, 向接入和移动性管理功能网元发送请求消息#1。示例性地, 会话管理网元不考虑终端设备在第一网络的用户面安全策略指的是, 会话管理网元不考虑终端设备在第一网络的用户面完整性保护策略的取值。也就是说, 不论终端设备在第一网络的用户面完整性保护策略的取值是以下三个取值中的哪一个: 需要 (required)、不需要 (not needed)、推荐 (preferred), 在第一网络的会话支持与第二网络互通的情况下, 会话管理网元都会根据
20 第一指示信息向接入和移动性管理功能网元发送请求消息#1。

一种可能的实现方式中, 所述会话管理网元根据第一指示信息, 确定所述终端设备在第一网络的用户面安全策略对所述终端设备在第一网络中建立的会话是否能够切换到第二网络不再有限制作用。

一种可能的是实现方式中, 所述会话管理网元还接收来自所述接入和移动性管理功能网元的第二网络基于 N26 接口的互通指示, 所述第二网络基于 N26 接口的互通指示用于指示请求建立的会话支持与第二网络基于 N26 接口的互通; 所述会话管理网元还接收来自所述接入和移动性管理功能网元的接入类型, 所述接入类型用于指示当前是 3GPP 接入还是非 3GPP 接入。在接入类型是 3GPP 接入, 所述第二网络基于 N26 接口的互通指示用于指示请求建立的会话支持与第二网络基于 N26 接口的互通的情况下, 如果会话管理网元接
30 收到所述第一指示信息, 则所述会话管理网元不需要考虑所述终端设备在第一网络的用户面安全策略, 直接确定所述终端设备在第一网络中的会话支持 EPS 互通。

所述会话管理网元确定所述终端设备在第一网络中的会话支持 EPS 互通之后, 为了便于后续将所述会话切换到第二网络, 所述会话管理网元可以执行 S220 和 S230 以请求所述接入和移动性管理功能网元为所述会话分配承载标识。

40 S230, 响应于请求消息#1, 接入和移动性管理功能网元发送响应消息#1 (第一响应消

息的一例)。相应地,在 S230 中,会话管理网元接收响应消息#1。

响应消息#1 包括接入和移动性管理功能网元为所述会话分配的承载标识,承载标识可以被第二网络识别,第一网络是 5G 网络,第二网络是 4G 网络,承载标识为 EBI,。示例性地,响应消息#1 为 EBI 分配回复(Namf_Communication_EBIAssignment Response)

5 消息。

在本申请实施例中,会话管理网元根据第一指示信息可以解除在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下,终端设备在第一网络中建立的会话不能切换到第二网络中的限制。因为,按照现有方案,在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下,会话管理网元不会向接入和移动性管理功能网元请求承载标识,从而接入和移动性管理功能网元本地也不会保存有相应的承载标识,这种情况下,后续接入和移动性管理功能网元接收到来自第一网络的接入网设备的切换需求时,是不会执行将终端设备在第一网络中建立的会话切换到第二网络的相关流程的。

10 可选地,方法 200 还可以包括 S240: 会话管理网元根据第一指示信息向统一数据管理网元发送会话管理网元在 S5/S8 接口上的 FQDN。

15 可选的,当第一指示信息指示支持与第二网络的接入网设备的用户面完整性保护时,会话管理网元向统一数据管理网元发送会话管理网元在 S5/S8 接口上的全量域名。

具体地,会话管理网元根据第一指示信息向统一数据管理功能网元发送会话管理网元在 S5/S8 接口上的 FQDN,包括: 会话管理网元根据第一指示信息,不考虑第一网络的用户面安全策略,向统一数据管理功能网元发送会话管理网元在 S5/S8 接口上的 FQDN。其中示例性地,会话管理网元不考虑终端设备在第一网络的用户面安全策略指的是,会话管理网元不考虑终端设备在第一网络的用户面完整性保护策略的取值。也就是说,不论终端设备在第一网络的用户面完整性保护策略的取值是以下三个取值中的哪一个: required、not needed、preferred,在第一网络的会话支持与第二网络互通的情况下,会话管理网元都会根据第一指示信息向统一数据管理用户面功能网元发送会话管理网元在 S5/S8 接口上的 FQDN。

25 一种可能的是实现方式中,所述会话管理网元还接收来自所述接入和移动性管理功能网元的 EPS 互通指示(EPS interworking indication),所述 EPS 互通指示用于指示终端设备支持与 EPS 的互通;所述会话管理网元还根据所述终端设备的签约数据确定所述终端设备在第一网络中的会话允许 EPS 互通。在所述终端设备支持 EPS 互通,且所述终端设备在第一网络中的会话允许 EPS 互通的情况下,如果会话管理网元接收到所述第一指示信息,则所述会话管理网元不需要考虑所述终端设备在第一网络的用户面安全策略,直接确定所述终端设备在第一网络中的会话支持 EPS 互通。

30 所述会话管理网元确定所述终端设备在第一网络中的会话支持 EPS 互通之后,为了便于后续将所述会话切换到第二网络,所述会话管理网元可以进一步执行 S240 将自身的 FQDN 存储到统一数据管理网元。

35 在本申请实施例中,会话管理网元根据第一指示信息向统一数据管理网元发送会话管理网元在 S5/S8 接口上的 FQDN,可以解除在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下,终端设备在第一网络中建立的会话不能切换到第二网络中的限制。因为,按照现有方案,在第一网络的用户面安全策略要求用户面完整性保护必须开启的情况下,会话管理网元不会向统一数据管理网元发送会话管理网元在 S5/S8 接口上的

FQDN。从而，终端设备在第一网络中建立的会话后续也不能切换到第二网络。

上述实施例解除了第一网络的用户面安全策略要求用户面完整性保护必须开启对终端设备在第一网络中建立的会话不能与 EPS 互通的限制，然后第二网络中的设备（如第二网络中的移动管理实体或者第二网络中的接入设备）如何获得所述终端设备在第二网络中的用户面安全策略这一问题仍未得到解决。

有鉴于此，本申请实施例还提供一种通信方法，以期实现在将终端设备在第一网络中建立的会话切换至第二网络的过程中，便于第二网络中设备能够获取到终端设备在第二网络的用户面安全策略，从而有助于终端设备在第一网络中的会话可以成功的切换到第二网络中。

图 3 示出了本申请实施例提供的通信方法的示意性流程图。如图 3 所示，方法 300 可以包括 S310 和 S320，下面详细描述各个步骤。

S310，会话管理网元将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略。

示例性地，第一网络可以是 5G 网络，第二网络可以是 4G 网络。

终端设备在第一网络/第二网络的用户面安全策略可以包括用户面安全加密保护策略和用户面完整性保护策略。其中，用户面加密保护策略用于指示是否开启用户面加密保护。用户面加密保护策略存在三种可能的取值，分别为 required、preferred 和 not needed。其中，required 表示必须开启，preferred 表示可以开启也可以不开启，not needed 表示不需要开启。用户面完整性保护策略用于指示是否开启用户面完整性保护。用户面完整性保护策略也存在三种可能的取值，分别为 required、preferred 和 not needed。其中，required 表示必须开启，preferred 表示可以开启也可以不开启，not needed 表示不需要开启。上述三种可能的取值可以采用 2 比特（bit）来指示，例如，00 指示不需要开启，01 指示可以开启也可以不开启，10 指示必须开启。

示例性地，终端设备在第一网络的用户面安全策略的粒度可以是以下任一粒度：协议数据单元（protocol data unit，PDU）会话粒度、数据网络名称（data network name，DNN）粒度。

示例性地，终端设备在第二网络的用户面安全策略的粒度可以是以下任一粒度：EPS 承载粒度、E-RAB 粒度、接入点名称（access point name，APN）粒度。

本申请实施例对会话管理网元获取终端设备在第一网络的用户面安全策略的方式不做限定。例如，终端设备第一网络的用户面安全策略可以是会话管理网元本地保存的。又例如，终端设备在第一网络的用户面安全策略可以是统一数据管理网元获取的。下文将结合其他实施例对会话管理网元从统一数据管理网元获取终端设备在第一网络的用户面安全策略的方法进行详细描述，为了简洁，此处暂不详述。

将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络用户面安全策略可以理解为：将第一网络可识别的用户面安全策略转化为第二网络可识别的用户面安全策略，或者将第一网络的用户面安全策略保存到第二网络可识别的上下文中。示例性地，第一网络可识别的用户面安全策略是 DNN 粒度或 PDU 会话粒度的。第二网络可识别的用户面安全策略是 EPS 承载粒度，或者是 E-RAB 粒度，或者是 APN 粒度。其中，DNN 与 PDU 会话可以是一对多的关系，PDU 会话与 EPS 承载可以是一对多的关系，DNN 与 APN 可以是一对一的关系，APN 与 EPS 承载可以是一对多的关系，EPS 承载与 E-RAB 可以是

一对多的关系。

会话管理网元本地存储的/从统一数据管理网元获得的终端设备在第一网络的用户面安全策略可以是 DNN+单网络切片选择支撑信息 (single network slice selection assistance information, S-NSSAI) 粒度, 若在 S310 中, 会话管理网元映射得到的终端设备在第二网络的用户面安全策略为 EPS 承载的粒度, 则会话管理网元首先将终端设备在第一网络的 DNN+S-NSSAI 粒度的用户面安全策略映射为 PDU 会话粒度的用户面安全策略, 再将终端设备在第一网络的 PDU 会话粒度的用户面安全策略映射为终端设备在第二网络的 EPS 承载粒度的用户面安全策略。若在 S310 中, 会话管理网元映射得到的终端设备在第二网络的用户面安全策略为 APN 的粒度, 则会话管理网元将终端设备第一网络的 DNN 粒度的用户面安全策略映射为终端设备第二网络的 APN 粒度的用户面安全策略。

会话管理网元本地存储的/从统一数据管理网元获得的终端设备在第一网络的用户面安全策略可以是 PDU 会话粒度, 若在 S310 中, 会话管理网元映射得到的终端设备在第二网络的用户面安全策略为 EPS 承载的粒度, 则会话管理网元将 PDU 会话粒度的用户面安全策略映射为终端设备在第二网络的 EPS 承载粒度的用户面安全策略。若在 S310 中, 会话管理网元映射得到终端设备在第二网络的用户面安全策略为 E-RAB 的粒度。则会话管理网元采用上述方式获得终端设备在第二网络的 EPS 承载粒度的用户面安全策略, 然后将终端设备在第二网络的 EPS 承载粒度的用户面安全策略映射为 E-RAB 粒度的用户面安全策略。

例如, 会话管理网元将第一网络的用户面安全策略保存到第二网络可识别的上下文中的实现方式可以是: 会话管理网元获取到的终端设备在第一网络的用户面安全策略 1, 该用户面安全策略 1 与 PDU 会话 1 对应, 会话管理网元将用户面安全策略 1 保存到与 PDU 会话 1 对应的 EPS 承载上下文中。

又例如, 会话管理网元将第一网络的用户面安全策略保存到第二网络可识别的上下文中的实现方式可以是: 会话管理网元获取到的终端设备在第一网络的用户面安全策略 1, 该用户面安全策略 1 与 DNN1+S-NSSAI1 对应, 会话管理网元确定与 DNN1+S-NSSAI1 对应的 PDU 会话 1 和 PDU 会话 1, 会话管理网元将用户面安全策略 1 保存到与 PDU 会话 1 对应的 EPS 承载上下文 1 中, 以及将用户面安全策略 1 保存到 PDU 会话 2 对应的 EPS 承载上下文 2 中。

可选地, 会话管理网元可以在终端设备从第一网络切换至第二网络的过程中, 执行 S310, 具体地, 可以参考下文方法 700 的描述。可选地, 会话管理网元可以在终端设备从第一网络切换至第二网络之前, 执行 S310, 具体地, 可以参考下文方法 500 和方法 600 中的描述。

会话管理网元可以在获取到终端设备在第一网络的用户面安全策略的情况下, 将第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略, 也可以在获取到第三指示信息/第一指示信息的情况下, 将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略。

在会话管理网元根据第三指示信息/第一指示信息将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略的情况下, 方法 300 还包括 S320: 会话管理网元获取第三指示信息/第一指示信息。

关于第一指示信息的描述和关于会话管理网元获取第一指示信息的描述可以参考上

文 S210 中的描述，为了简洁，此处不再详述。

第三指示信息用于指示会话管理网元映射第二网络的用户面安全策略，更对关于第三指示信息的描述和关于会话管理网元获取第三指示信息的描述可以参考下文图 7 中的 S718 中的描述，为了简洁，此处不再详述。

5 可选地，方法 300 还可以包括：会话管理网元将终端设备在第二网络的用户面安全策略保存在终端设备在第二网络的承载上下文文。

可选地，方法 300 还可以包括：会话管理网元将终端设备在第二网络的用户面安全策略保存在本地，并保存终端设备在第二网络的用户面安全策略与承载上下文的绑定关系。

10 在本申请实施例中，会话管理网元可以将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略，并可以将终端设备在第二网络的用户面安全策略保存在承载上下文文。进而，在终端设备从第一网络切换至第二网络的过程中，第一网络中的接入和移动性管理功能网元从会话管理网元获取所述承载上下文文，进而将获取到的承载上下文文发送给第二网络的移动管理实体，从而有助于实现终端设备从第一网络切换至第二网络。

15 此外，会话管理网元在接收到第三指示信息的情况下，将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略，可以避免会话管理网元进行不必要的映射，优化了会话管理网元的处理逻辑。若会话管理网元在没有接收到第三指示信息的情况下，会话管理网元直接将终端设备在第一网络的用户面安全策略映射为终端设备在第二网络的用户面安全策略，若第二网络不支持开启用户面完整性保护，则终端设备不能从第一网络切换至第二网络，会话管理网元进行的映射就是不必要的映射。

20 下面结合图 4 至图 7，以终端设备从 5G 切换至 4G 为例，对本申请实施例提供的通信方法进行详细说明。应理解，下文中的源 AMF 对应上文中的接入和移动性管理功能网元，SMF+PGW-C 对应上文中的会话管理网元，UE 对应上文中的终端设备，UDM 对应上文中的统一数据管理网元。还应理解，下文中的 UE 能力指示可以对应于上文中的第二指示信息或第一指示信息，指示信息#1 可以对应上文的第一指示信息，指示信息#2 可以对应上文中的第三指示信息。

图 4 示出了本申请实施例提供的方法的示意性流程图。具体地，图 4 示出了 UE 从 5G 网络切换至 4G 网络的过程中，源 AMF 如何从 SMF+PGW-C 获取 4G 网络的用户面安全策略的流程图。如图 4 所示，方法 400 包括 S401 至 S413，下面详细说明各个步骤。

30 S401，源下一代基站节点（next generation Node Base station，gNB）决定触发 N2 切换。

UE 通过源 gNB 接入 5G 网络，并且在 5G 网络中建立了 PDU 会话；以及源 gNB 确定发起 5G 系统（5G system，5GS）到 EPS 切换，以便于将 UE 切换到 4G 网络中的 eNB，下文中将 4G 网络的 eNB 记为目标 eNB。

35 源 gNB 在 UE 接入 5G 网络的过程中，会从核心网侧获取 UE 在 5G 网络中的用户面安全策略，并使用 UE 在 5G 网络中的用户面安全策略激活自身与 UE 之间的用户面安全。源 gNB 还将获取的 UE 在 5G 网络的用户面安全策略存储在 UE 的接入层（access stratum，AS）上下文文。

40 其中，源 gNB 确定需要将 UE 切换至目标 eNB 时，5GS 到 EPS 切换可以是基于如下条件触发：（1）当前无线网络状态较差；（2）负载均衡；（3）语音服务要求。

S402, 源 gNB 向源 AMF 发送切换需求 (handover required) 消息。

切换需求消息携带 UE 的标识。UE 的标识用于获取 UE 的上下文, UE 的标识可以包括: 终端设备在源 gNB 侧 NG 接口上的唯一标识 (gNB UE NG application protocol identifier, gNB UE NGAP ID) 或者终端设备在源 AMF 侧 NG 接口上的唯一标识 (AMF UE NG application protocol identifier, AMF UE NGAP ID)。

S403, 源 AMF 向 SMF+PGW-C 发送 PDU 会话上下文请求 (Nsmf_PDU Session Context Request) 消息 (第二请求消息的一例)。

源 AMF 向 SMF+PGW-C 发送 PDU 会话上下文请求消息之前, 源 AMF 根据本地策略 #2 判断是否从 SMF+PGW-C 获得 EPS 承载上下文。如果源 AMF 根据本地策略 #2 确定从 SMF+PGW-C 获得 EPS 承载上下文, 则源 AMF 向 SMF+PGW-C 发送 PDU 会话上下文请求消息。PDU 会话上下文请求消息包含 PDU 会话 ID。

源 AMF 的本地策略 #2 可以包括: 源 AMF 已经为需要切换的 PDU 会话分配了 EBI。具体地, 源 AMF 根据 UE 的标识获取 UE 的上下文, 进一步地, 源 AMF 根据 UE 的上下文获得需要切换的 PDU 会话, 并判断是否为该 PDU 会话分配了 EBI。

需要说明的是, 根据图 2 所述的实施例, 在 UE 在 5G 网络中建立 PDU 会话的时候, SMF+PGW-C 在确定 PDU 会话支持切换到 EPS 的情况下, 会执行 S220 和 S230 以请求 AMF 为所述 PDU 会话分配 EBI。AMF 为所述 PDU 会话分配 EBI 之后, 可以将分配的 EBI 保存在 UE 的上下文中。

S404, SMF+PGW-C 根据 PDU 会话 ID 获得 UE 的 EPS 承载上下文。

在一种可能的实现方式中, 根据图 3 所述的实施例, UE 的 EPS 承载上下文中已经保存了 UE 在 4G 网络的用户面安全策略。

在另一种可能的实现方式中, 根据图 3 所述的实施例, SMF+PGW-C 可以将 UE 在 4G 网络的用户面安全策略保存在本地, 并保存 UE 在 4G 网络的用户面安全策略和 EPS 承载上下文的对应关系, 则 SMF+PGW-C 可以根据 PDU 会话 ID 确定对应的 EPS 承载上下文, 再根据 EPS 承载上下文获取 UE 在 4G 网络的用户面安全策略。

UE 在 4G 网络的用户面安全策略包括用户面加密保护策略和用户面完整性保护策略。其中, 用户面加密保护策略用于指示是否开启用户面加密保护, 用户面完整性保护策略用于指示是否开启用户面完整性保护。用户面加密保护策略存在三种可能的值, 分别为 not needed、preferred 和 required, 用户面完整性保护策略也存在三种可能的值, 分别为 not needed、preferred 和 required。其中, not needed 表示不需要开启, preferred 表示可以开启也可以不开启, required 表示必须开启。上述三种可能的值可以采用 2 比特 (bit) 来指示, 例如 00 指示不需要开启, 01 指示可以开启可以不开启, 11 指示必须开启。

UE 在 4G 网络的用户面安全策略可以是 EPS 承载/E-RAB/APN 粒度。示例性地, EPS 承载上下文的形式是 {EPS 承载 1: 用户面安全策略 1}; {E-RAB1: 用户面安全策略 1}; {APN1: 用户面安全策略 1}。其中, {EPS 承载 1: 用户面安全策略 1} 表示 EPS 承载 1 与用户面安全策略 1 对应, 即用户面安全策略 1 是 EPS 承载粒度; {E-RAB1: 用户面安全策略 1} 表示 E-RAB1 与用户面安全策略 1 对应, 即用户面安全策略 1 是 E-RAB 粒度; {APN1: 用户面安全策略 1} 表示 APN1 与用户面安全策略 1 对应, 即用户面安全策略 1 是 APN 粒度。

S405, SMF+PGW-C 向源 AMF 发送 PDU 会话上下文响应 (Nsmf_PDU Session Context

Response) 消息 (第二响应消息的一例)。

在一种可能的实现方式中, PDU 会话上下文响应消息包括 EPS 承载上下文, EPS 承载上下文包含 UE 在 4G 网络的用户面安全策略。

5 在另一种可能的实现方式中, PDU 会话上下文响应消息包括 EPS 承载上下文和 UE 在 4G 网络的用户面安全策略。

S406, 源 AMF 向目标 MME 发送转发重定位请求 (forward relocation request) 消息。

在一种可能的实现方式中, 转发重定位请求消息包括 EPS 承载上下文, EPS 承载上下文包括 UE 在 4G 网络的用户面安全策略。

10 在另一种可能的实现方式中, 转发重定位请求消息包括 EPS 承载上下文和 UE 在 4G 网络的用户面安全策略。

S407, 目标 MME 向目标 eNB (4G 网络中的接入网设备) 发送切换请求 (handover request) 消息。

切换请求消息包括 UE 在 4G 网络的用户面安全策略。

15 在一种可能的实现方式中, 目标 MME 根据 EPS 承载上下文获取 UE 在 4G 网络的用户面安全策略。可选地, 若目标 MME 获得的 UE 在 4G 网络的用户面安全策略是 EPS 承载粒度/APN 粒度的, 则目标 MME 将 EPS 承载粒度/APN 粒度的用户面安全策略映射为 E-RAB 粒度的用户面安全策略。

S408, 目标 eNB 根据 UE 在 4G 网络的用户面安全策略确定 UE 在 4G 网络的用户面安全激活状态。

20 用户面安全激活状态用于指示是否开启用户面加密保护和/或用户面完整性保护。其中, 目标 eNB 根据 E-RAB 粒度的用户面安全策略, 确定数据无线承载 (data radio bearer, DRB) 粒度的用户面安全激活状态。E-RAB 与 DRB 的关系是一对多的映射关系, 例如, 目标 eNB 从 E-RAB1 映射出 DRB1, DRB2, 然后根据 E-RAB1 对应的用户面安全策略 1, 确定 DRB1 的用户面安全激活状态, 再根据用户面安全策略 1 确定 DRB2 的用户面安全激活状态。

25 具体的, 若用户面加密保护策略是 required, 则对于该 E-RAB 对应的所有 DRB, 目标 eNB 确定其对应的加密激活状态都为开启。若 E-RAB 对应的用户面加密保护策略是 preferred, 则对于该 E-RAB 对应的所有 DRB, 目标 eNB 确定其对应的加密激活状态可以为开启或不开启。目标 eNB 可以根据本地策略 (例如, 自身运行状态、控制策略、法规要求等) 进行判断是否开启加密激活状态。若 E-RAB 对应的用户面加密保护策略是 not needed, 则对于该 E-RAB 对应的所有 DRB, 目标 eNB 确定其对应的加密激活状态都为不

30 开启。

若用户面完整性保护策略是 required, 则对于该 E-RAB 对应的所有 DRB, 目标 eNB 确定其对应的完整性保护激活状态都为开启。若 E-RAB 对应的用户面完整性保护策略是 preferred, 则对于该 E-RAB 对应的所有 DRB, 目标 eNB 确定其对应的完整性保护激活状态可以为开启或不开启。目标 eNB 可以根据本地策略 (例如, 自身运行状态、控制策略、法规要求等) 进行判断是否开启完整性保护激活状态。若 E-RAB 对应的用户面完整性保护策略是 not needed, 则对于该 E-RAB 对应的所有 DRB, 目标 eNB 确定其对应的完整性保护激活状态都为不

40 S409, 目标 eNB 向目标 MME 发送切换请求响应 (handover request acknowledge) 消

息。

切换请求响应消息中包含无线资源控制（radio resource control，RRC）重配置（connection reconfiguration），该 RRC 重配置由目标 eNB 构造。

5 RRC 重配置中携带配置信息，配置信息用于指示 UE 是否在 4G 网络中开启用户面加密保护和/或用户面完整性保护。配置信息由 S408 中的用户面安全激活状态确定。

具体的，若目标 eNB 确定加密激活状态为开启，则在配置信息中封装禁用加密（ciphering disabled）字段；若目标 eNB 确定加密激活状态为不开启，则不在配置信息中封装禁用加密（ciphering disabled）字段。若目标 eNB 确定完整性保护激活状态为开启，则在配置信息中封装完整性保护（integrity protection）字段；若目标 eNB 确定完整性保护
10 激活状态为不开启，则不在配置信息中封装完整性保护（integrity protection）字段。

完整性保护字段用于指示开启用户面完整性保护，完整性保护字段可以等同于开启用户面完整性保护的指示信息，或者，完整性保护字段的内容可以是开启用户面完整性保护的指示信息。因此在配置信息封装完整性保护字段的情况下，可以认为 RRC 重配置包括开启用户面完整性保护的指示信息。

15 S410，目标 MME 向源 AMF 发送转发重定位回复（forward relocation response）消息。该转发重定位回复消息包含 RRC 重配置，该 RRC 重配置包括上述配置信息。

S411，源 AMF 向源 gNB 发送切换命令（handover command）消息。该切换命令消息包含上述 RRC 重配置，该 RRC 重配置包括上述配置信息。

20 S412，源 gNB 向 UE 发送 RRC 重配置。UE 根据 RRC 重配置中的包括的上述配置信息确定是否开启自身与目标 eNB 之间的用户面安全加密保护和/或用户面完整性保护。

具体的，若配置信息中封装了禁用加密（ciphering disabled）字段，则 UE 在 4G 网络中不开启加密保护；若配置信息中未封装禁用加密（ciphering disabled）字段，则 UE 在 4G 网络中开启加密保护。若配置信息中封装了完整性保护（integrity protection）字段，则 UE 在 4G 网络中开启完整性保护；若配置信息中未封装完整性保护（integrity protection）
25 字段，则 UE 在 4G 网络中不开启完整性保护。

S413，UE 向目标 eNB 发送 RRC 重配置完成消息，完成切换。

图 5 示出了本申请实施例提供的方法的示意性流程图。具体地，图 5 示出了 SMF+PGW-C 在 UE 从 5G 网络切换至 4G 网络之前，将 UE 在 5G 网络的用户面安全策略映射为 UE 在 4G 网络的用户面安全策略的流程，以及图 5 还示出了 SMF+PGW-C 根据指
30 示信息#1 请求分配 EBI 和发送 S5/S8 接口的 FQDN 的流程。如图 5 所示，方法 500 包括 S501 至 S516，下面详细说明各个步骤。

S501，UE 向 AMF 发送注册请求（registration request）消息。

注册请求消息包含 UE 能力指示，UE 能力指示等同于图 2 实施例中第二指示信息，相关描述可以参考图 2 实施例相关内容，这里不再赘述。UE 能力指示可以携带在 5G MM
35 能力、UE 安全能力或 S1 UE 网络能力中。

S502，AMF 向 UE 发送注册接受（registration accept）消息。

可选的，AMF 将 UE 能力指示保存到 UE 的上下文中。

S503，UE 向 AMF 发送上行 NAS 传输（uplink NAS transport）消息。

上行 NAS 传输消息中包括 SM 容器信息，SM 容器信息包括 PDU 会话建立请求消息。
40 上行 NAS 传输消息还包括 DNN 和 S-NSSAI。

可选地，方法 500 还可以包括 S504，AMF 判断是否发送指示信息#1。

指示信息#1 等同于图 2 实施例中第一指示信息，相关描述可以参考图 2 实施例相关内容，这里不再赘述。

AMF 根据上行 NAS 传输消息，获得 UE 的上下文；进一步地，AMF 根据上行 NAS 传输消息以及 UE 的上下文判断是否发送指示信息#1。一种可能的实现方式中，AMF 根据 UE 上下文中保存的对于该 DNN 和 S-NSSAI 支持与 EPS 互通的指示以及 UE 能力指示判断是否发送指示信息#1。若对于该 DNN 和 S-NSSAI 支持与 EPS 互通的指示用于指示 UE 支持与 EPS 互通，且 UE 能力指示用于指示 UE 支持与 eNB 的用户面完整性保护，则 AMF 确定发送指示信息#1。

其中，AMF 根据上行 NAS 传输消息以及 UE 的上下文判断是否发送指示信息#1 的过程，等同于上文图 2 实施例所述的接入和移动性管理功能网元根据本地策略#1 确定是否发送第一指示信息。即接入和移动性管理功能网元的本地策略#1 可以包括：DNN 和 S-NSSAI 是否支持与 EPS 互通、是否获得 UE 能力指示。DNN+S-NSSAI 是否支持与 EPS 互通也可以理解为 DNN+S-NSSAI 对应的 PDU 会话是否支持与 EPS 互通。

其中，支持与 EPS 互通的指示用于指示 UE 是否支持与 EPS 互通，支持与 EPS 互通的指示保存在 UE 的签约信息中。在 UE 注册到网络时，AMF 从 UDM 获取 UE 的签约信息中保存的支持与 EPS 互通的指示，并将支持与 EPS 互通的指示保存在 UE 的上下文中的。

S505，AMF 向 SMF+PGW-C 发送 PDU 会话建立 SM 上下文请求 (Nsmf_PDUSession_CreateSMContext Request) 消息。PDU 会话建立 SM 上下文请求消息包括 UE 的永久身份标识 (subscription permanent identifier, SUPI)、DNN、S-NSSAI 以及指示信息#1。

AMF 根据上行 NAS 传输消息，获得 UE 的上下文；进一步地 AMF 根据上行 NAS 传输消息以及 UE 的上下文选择 SMF+PGW-C。可选地，AMF 根据上行 NAS 传输消息中的 DNN、S-NSSAI 以及 UE 上下文中保存的 UE 支持演进分组核心网 (evolved packet core, EPC) NAS 指示选择 SMF+PGW-C。可选地，AMF 还根据 UE 上下文中保存的对于该 DNN 和 S-NSSAI 支持与 EPS 互通的指示选择 SMF+PGW-C。其中，UE 支持 EPC NAS 指示用于指示 UE 是否支持 S1 模式(接入网设备使用 S1 接口与核心网设备进行交互的模式)。UE 在注册到网络时，UE 通过 5G 移动管理能力 (5G MM capability) 上报 UE 支持 EPC NAS 指示。

S506，SMF+PGW-C 向 UDM 发送获得签约数据管理请求 (Nudm_SubscriberDataManagement_Get) 消息，用于请求 UE 的签约信息。获得签约数据管理请求消息包括 SUPI、DNN、S-NSSAI。

S507，UDM 向 SMF+PGW-C 发送签约数据管理回复 (Nudm_SubscriberDataManagement_Response) 消息。

签约数据管理回复消息包括 UE 的会话管理签约数据。UE 的会话管理签约数据包含 DNN、S-NSSAI、UE 在 5G 网络的用户面安全策略以及支持与 EPS 互通的指示。其中，UE 在 5G 网络的用户面安全策略以及支持与 EPS 互通的指示是 DNN 粒度或 S-NSSAI 粒度或 DNN+S-NSSAI 粒度。以 UE 在 5G 网络的用户面安全策略以及支持与 EPS 互通的指示是 DNN+S-NSSAI 粒度为例，UE 的会话管理签约数据可以表示为：{S-NSSAI1, DNN1,

用户面安全策略 1, 支持与 EPS 互通的指示 1}, {S-NSSAI1, DNN1, 用户面安全策略 1, 支持与 EPS 互通的指示 1}表示用户面安全策略 1 和支持与 EPS 互通的指示 1 与 S-NSSAI1+DNN1 对应, 即用户面安全策略 1 和支持与 EPS 互通的指示 1 是 S-NSSAI1+DNN1 粒度的。

5 若 UE 的会话管理签约数据包括的 UE 在 5G 网络的用户面安全策略是 DNN+S-NSSAI 粒度的, 则 SMF+PGW-C 可以将 UE 在 5G 网络的 DNN+S-NSSAI 粒度的用户面安全策略映射为 PDU 会话粒度的用户面安全策略。一个 DNN+S-NSSAI 可以对应一个或多个 PDU 会话。例如, SMF+PGW-C 从 DNN1+S-NSSAI1 映射出 PDU 会话 1, 然后根据 DNN1+S-NSSAI1 对应的用户面安全策略 1, 确定 PDU 会话 1 对应的用户面安全策略 1。

10 S508, SMF+PGW-C 向 UDM 发送 SMF+PGW-C 的 S5/S8 接口的 FQDN。

具体地, SMF+PGW-C 根据指示信息#1 向 UDM 发送 SMF+PGW-C 的 S5/S8 接口的 FQDN。更多的关于 SMF+PGW-C 如何根据指示信息#1 发送 SMF+PGW-C 的 S5/S8 接口的 FQDN 的描述, 可以参考上文 S240 中的描述, 为了简洁, 此处不再详述。

可选地, SMF+PGW-C 可以将 SMF+PGW-C 的 S5/S8 接口的 FQDN 包含在签约数据管理请求消息中发送给 UDM。在此情况下, S508 和 S506 可以合并为一个步骤。

S509, SMF+PGW-C 将 5G 上下文映射为 EPS 承载上下文。

SMF+PGW-C 将 5G 上下文映射为 EPS 承载上下文包括将 5G QoS 参数映射为 EPS QoS 参数, 还包括将 5G 用户面安全策略映射为 EPS 用户面安全策略。

20 可选地, SMF+PGW-C 根据指示信息#1 将 5G 用户面安全策略映射为 EPS 用户面安全策略。SMF+PGW-C 将映射后的 EPS 用户面安全策略保存到 UE 的 EPS 上下文中。也就是说, SMF+PGW-C 在收到指示信息#1 的情况下将 5G 上下文映射为 EPS 承载上下文。

具体地, 关于 SMF+PGW-C 如何将用户面安全策略映射为 EPS 用户面安全策略的描述, 可以参考上文 S310 中的描述, 为了简洁, 此处不再详述。

25 S510, SMF+PGW-C 向 AMF 发送 N1N2 消息传输 (Nam_Communication_N1N2MessageTransfer) 消息。

N1N2 消息传输消息中包含 N1 SM 信息以及 N2 SM 信息。其中, AMF 不解析 N1 SM 信息, 并将 N1 SM 信息透传给 UE, N1 SM 信息中包含 PDU 会话建立接受 (PDU Session Establishment Accept) 消息。AMF 不解析 N2 SM 信息, 并将 N2 SM 信息透传给 gNB, N2 SM 信息中包含 PDU 会话粒度的用户面安全策略。

30 S511, AMF 向 gNB 发送 N2 SM 信息, gNB 根据 PDU 会话粒度的用户面安全策略确定 DRB 粒度的用户面安全激活状态。

S512a, gNB 向 UE 发送 RRC 重配置, 该 RRC 重配置包括配置信息。UE 根据 RRC 重配置中的包括的配置信息确定是否开启自身与 gNB 之间的用户面安全加密保护/用户面完整性保护。

35 S512b, AMF 向 UE 发送 N1 SM 信息的内容, 即 PDU 会话建立接受消息, 完成 PDU 会话建立。

S513, SMF+PGW-C 根据本地策略#3 决定是否需要请求 AMF 分配 EBI。

本地策略#3 例如包括当前 PDU 会话是第三代合作伙伴计划 (3rd generation partnership project, 3GPP) 接入且支持使用 N26 接口与 EPS 互通。

40 进一步地, SMF+PGW-C 还根据指示信息#1 以及 UE 在 5G 网络的用户面安全策略中

的完整性保护策略进行进一步判断。例如，若 SMF+PGW-C 获得指示信息#1，则无需再判断 UE 在 5G 网络的用户面安全策略；若 SMF+PGW-C 没有获得 UE 指示信息#1，则若 UE 在 5G 网络的用户面安全策略中的完整性保护策略不是 required，则需要请求 AMF 分配 EBI，如果 UE 在 5G 网络的用户面安全策略中的完整性保护策略是 required，

5 SMF+PGW-C 将不能请求 AMF 分配 EBI。

SMF+PGW-C 如何确定是否请求 AMF 为 PDU 会话分配 EBI 可以参考上述图 2 实施例中 S220 中相关的描述，这里不再赘述。

S514，如果 SMF+PGW-C 判断需要请求 AMF 分配 EBI，则 SMF+PGW-C 向 AMF 发送 EBI 分配请求消息。EBI 分配请求消息包括 PDU 会话 ID。

10 S515，AMF 为 PDU 会话分配一个 EBI。

S516，AMF 向 SMF+PGW-C 发送 EBI 分配回复消息。EBI 分配回复消息中包括分配的 EBI。SMF+PGW-C 将该 EBI 关联到映射的 EPS 上下文。

应理解，在方法 500 中，各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对方法 500 的实施过程构成任何限定。例如。

15 S508 可以在 S505 到 S512 (S512a/ S512b) 之间执行，或者，S508 可以在 S516 之后执行，即 SMF+PGW-C 在成功接收到 EBI 分配回复消息后，代表 SMF+PGW-C 确认 AMF 成功分配 EBI 后，执行 S508。又例如，S511b 中的 N1 SM 信息内容可以承载在 S511a 中的 RRC 重配置消息中，因此，S511a 和 S511b 可以同时执行。又例如，S509 可以在 S505 到 S516 之间执行，或者，S509 可以在 S516 之后执行。

20 在本申请实施例中，在 UE 从 5G 网络切换至 4G 网络之前，SMF+PGW-C 将 UE 在 5G 网络的用户面安全策略映射为 UE 在 4G 网络的用户面安全策略，便于后续 UE 从 5G 网络切换至 4G 网络过程中，5G 网络中的 AMF 可以直接从 SMF+PGW-C 获取 UE 在 4G 网络的用户面安全策略，而不用等待 SMF+PGW-C 将 UE 在 5G 网络的用户面安全策略映射为 UE 在 4G 网络的用户面安全策略，从而减小切换时延。

25 图 6 示出了本申请实施例提供的方法的示意性流程图。具体地，图 6 示出了 SMF+PGW-C 在 UE 从 5G 网络切换至 4G 网络之前，将 UE 在 5G 网络的用户面安全策略映射为 UE 在 4G 网络的用户面安全策略的流程，以及图 6 还示出了 SMF+PGW-C 根据 UE 能力指示请求分配 EBI 和发送 S5/S8 接口的 FQDN 的流程。如图 6 所示，方法 600 包括 S601 至 S613，下面详细说明各个步骤。

30 S601，UE 向 AMF 发送上行 NAS 传输消息。

上行 NAS 传输消息中包括 SM 容器信息，SM 容器信息包括 PDU 会话建立请求消息。上行 NAS 传输消息还包括 DNN 和 S-NSSAI。

PDU 会话建立请求消息包含 UE 能力指示，UE 能力指示等同于图 2 实施例中 S211b 和 S212b 中的第一指示信息，相关描述可以参考图 2 实施例相关内容，这里不再赘述。

35 S602，AMF 向 SMF+PGW-C 发送 PDU 会话建立 SM 上下文请求消息。PDU 会话建立 SM 上下文请求消息包括 UE 的 SUPI、DNN、S-NSSAI 以及 PDU 会话建立请求消息。

S603 至 S613 与方法 500 中的 S506 至 S516 相同，为了简洁，此处不再详述。

应理解，在方法 600 中，各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对方法 600 的实施过程构成任何限定。例如。

40 S606 可以在 S604 到 S609 (S609a/S609b) 之间执行，或者，S606 可以在 S613 之后执行，

即 SMF+PGW-C 在成功接收到 EBI 分配回复消息后, 代表 SMF+PGW-C 确认 AMF 成功分配 EBI 后, 执行 S606。又例如, S609b 中的 N1 SM 信息内容可以承载在 S609a 中的 RRC 重配置消息中, 因此, S609a 和 S609b 可以同时执行。又例如, S605 可以在 S602 到 S613 之间执行, 或者, S605 可以在 S613 之后执行。

5 在本申请实施例中, 在 UE 从 5G 网络切换至 4G 网络之前, SMF+PGW-C 将 UE 在 5G 网络的用户面安全策略映射为 UE 在 4G 网络的用户面安全策略, 便于后续 UE 从 5G 网络切换至 4G 网络过程中, 5G 网络中的 AMF 可以直接从 SMF+PGW-C 获取 UE 在 4G 网络的用户面安全策略, 而不用等待 SMF+PGW-C 将 UE 在 5G 网络的用户面安全策略映射为 UE 在 4G 网络的用户面安全策略, 从而减小切换时延。

10 图 7 示出了本申请实施例提供的方法的示意性流程图。具体地, 图 7 中的 (a) 示出了 SMF+PGW-C 在 UE 从 5G 网络切换至 4G 网络之前, SMF+PGW-C 根据指示信息#2 请求分配 EBI 和发送 S5/S8 接口的 FQDN 的流程。图 7 中的 (b) 示出了 SMF+PGW-C 在 UE 从 5G 网络切换至 4G 网络过程中, 将 UE 在 5G 网络的用户面安全策略映射为 UE 在 4G 网络的用户面安全策略的流程。如图 7 所示, 方法 700 包括 S701 至 S728, 下面详细说明各个步骤。

15 S701 至 S708 与方法 500 中的 S501 至 S508 相同, S709 至 S715 与方法 500 中的 S510 至 S516 相同, 为了简洁此处不再详述。

 可选的, 在 S705 中, SMF+PGW-C 保存指示信息#1 在终端设备的上下文中。

 S716 至 S717 与方法 400 中的 S401 至 S402 相同, 为了简洁, 此处不再详述。

20 S718, 源 AMF 判断是否发送指示信息#1/指示信息#2。

 指示信息#1 等同于图 2 实施例中第一指示信息, 相关描述可以参考图 2 实施例相关内容, 这里不再赘述。

 指示信息#2 用于指示执行用户面安全策略映射。或者, 指示信息#2 用于指示支持与 4G 网络的接入网设备的用户面完整性保护。或者, 指示信息#2 用于指示支持与 4G 网络的接入网设备的用户面按需保护。或者, 指示信息#2 用于指示支持 5G 网络和 4G 网络之间的用户面安全策略的互通, 即用于指示支持 5G 网络和 4G 网络之间的用户面安全策略的映射。

25 源 AMF 根据上行 NAS 传输消息, 获得 UE 的上下文; 进一步地, 源 AMF 根据上行 NAS 传输消息以及 UE 的上下文以及目标 MME 是否支持用户面完整性保护判断是否发送指示信息#1/指示信息#2。源 AMF 中还保存有目标 MME 的能力信息, 目标 MME 的能力信息指示目标 MME 是否支持用户面完整性保护, 若目标 MME 支持用户面完整性保护, 则源 AMF 确定发送 UE 指示能力#1/指示信息#2。目标 MME 的能力信息是 AMF 本地配置的。

30 AMF 根据上行 NAS 传输消息以及 UE 的上下文判断是否发送指示信息#1 的过程, 等同于上文图 2 实施例所述的接入和移动性管理功能网元根据本地策略#1 确定是否发送第一指示信息。即接入和移动性管理功能网元的本地策略#1 还可以包括: 目标 MME 是否支持用户面完整性保护。源 AMF 根据本地策略#4 (第二本地策略的一例) 判断是否发送指示信息#2。本地策略#4 包括: 可以包括: DNN 和 S-NSSAI 是否支持与 EPS 互通、是否获得 UE 能力指示、目标 MME 是否支持用户面完整性保护。源 AMF 确定 DNN 和 S-NSSAI 是否支持与 EPS 互通以及确定目标 MME 是否支持用户面完整性保护的方式, 可以参考图

5 实施例和图 7 实施例中关于本地策略#1 的描述。

S719, 源 AMF 向 SMF+PGW-C 发送 PDU 会话上下文请求(Nsmf_PDU Session_Context Request) 消息

源 AMF 向 SMF+PGW-C 发送 PDU 会话上下文请求消息之前, 源 AMF 根据本地策略
5 #2 判断是否从 SMF+PGW-C 获得 EPS 承载上下文。如果源 AMF 根据本地策略#2 确定从 SMF+PGW-C 获得 EPS 承载上下文, 则源 AMF 向 SMF+PGW-C 发送 PDU 会话上下文请求消息。PDU 会话上下文请求消息包含 PDU 会话 ID。

可选的, PDU 会话上下文请求消息还包含指示信息#2。

源 AMF 的本地策略#2 可以包括: 源 AMF 已经为需要切换的 PDU 会话分配了 EBI。
10 具体地, 源 AMF 根据 UE 的标识获取 UE 的上下文, 进一步地, 源 AMF 根据 UE 的上下文获得需要切换的 PDU 会话, 并判断是否为该 PDU 会话分配了 EBI。

需要说明的是, 结合图 2 和图 7 的实施例, 在 S703 至 S711b 之间(即 UE 在 5G 网络建立 PDU 会话的过程), SMF+PGW-C 在确定 PDU 会话支持切换到 EPS 的情况下, 方法 700 会执行 S713 至 S715 以请求 AMF 为所述 PDU 会话分配 EBI。AMF 为所述 PDU 会话分配 EBI 之后, 可以将分配的 EBI 保存在 UE 的上下文中。
15

S720, SMF+PGW-C 将 5G 用户面安全策略映射为 EPS 用户面安全策略。

可选的, SMF+PGW-C 根据 PDU 会话上下文请求消息获得 UE 的上下文信息, 从 UE 的上下文信息中获得指示信息#1, SMF+PGW-C 根据指示信息#1, 将 5G 用户面安全策略映射为 EPS 用户面安全策略

20 可选的, SMF+PGW-C 根据 PDU 会话上下文请求消息获得的指示信息#2, 将 5G 用户面安全策略映射为 EPS 用户面安全策略

具体地, 更多关于 SMF+PGW-C 将 5G 用户面安全策略映射为 EPS 用户面安全策略的描述可以参考上文 S310 中的描述。

S721 至 S729 与方法 400 中的 S405 至 S413 相同, 为了简洁, 此处不再详述。

25 在本申请实施例中, 在 UE 从 5G 网络切换至 4G 网络的过程中, SMF+PGW-C 将 UE 在 5G 网络的用户面安全策略映射为 UE 在 4G 网络的用户面安全策略, 可以避免不必要的映射。例如, 在 UE 从 5G 网络切换至 4G 网络之前, SMF+PGW-C 将 UE 在 5G 网络的用户面安全策略映射为 UE 在 4G 网络的用户面安全策略之后, UE 一直没有移动到 4G 网络, 从而 UE 也不会执行切换流程, 在此情况下, SMF+PGW-C 进行的的就是不必要的映射, 浪费了 SMF+PGW-C 的计算资源和存储资源。
30

以上, 结合图 2 至图 7 详细说明了本申请实施例提供的方法。以下, 结合图 8 至图 9 详细说明本申请实施例提供的通信装置。应理解, 装置实施例的描述与方法实施例的描述相互对应, 因此, 未详细描述的内容可以参见上文方法实施例, 为了简洁, 这里不再赘述。

本申请实施例可以根据上述方法示例对发射端设备或者接收端设备进行功能模块的划分, 例如, 可以对应各个功能划分各个功能模块, 也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现, 也可以采用软件功能模块的形式实现。需要说明的是, 本申请实施例中对模块的划分是示意性的, 仅仅为一种逻辑功能划分, 实际实现时可以有另外的划分方式。下面以采用对应各个功能划分各个功能模块为例进行说明
35

40 图 8 是本申请实施例提供的通信装置 800 的示意性框图。如图所示, 该通信装置 800

可以包括：收发单元 810 和处理单元 820。

在一种可能的设计中，该通信装置 800 可以是上文方法实施例中的会话管理网元，也可以是用于实现上文方法实施例中会话管理网元的功能的芯片。

应理解，该通信装置 800 可对应于根据本申请实施例的方法 200 至方法 700 中的会话管理网元，该通信装置 800 可以包括用于执行图 2 中的方法 200、图 3 中的方法 300、图 4 中的方法 200、图 5 中的方法 500、图 6 中的方法 600 和图 7 中的方法 700 中的会话管理网元执行的方法的单元。并且，该通信装置 800 中的各单元和上述其他操作和/或功能分别为了实现图 2 中的方法 200、图 3 中的方法 300、图 4 中的方法 200、图 5 中的方法 500、图 6 中的方法 600 和图 7 中的方法 700 的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

在另一种可能的设计中，该通信装置 800 可以是上文方法实施例中的接入和移动性管理功能网元，也可以是用于实现上文方法实施例中接入和移动性管理功能网元的功能的芯片。

应理解，该通信装置 800 可对应于根据本申请实施例的方法 200 至方法 700 中的接入和移动性管理功能网元，该通信装置 800 可以包括用于执行图 2 中的方法 200、图 3 中的方法 300、图 4 中的方法 200、图 5 中的方法 500、图 6 中的方法 600 和图 7 中的方法 700 中的接入和移动性管理功能网元执行的方法的单元。并且，该通信装置 800 中的各单元和上述其他操作和/或功能分别为了实现图 2 中的方法 200、图 3 中的方法 300、图 4 中的方法 200、图 5 中的方法 500、图 6 中的方法 600 和图 7 中的方法 700 的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

在另一种可能的设计中，该通信装置 800 可以是上文方法实施例中的终端设备，也可以是用于实现上文方法实施例中终端设备的功能的芯片。

应理解，该通信装置 800 可对应于根据本申请实施例的方法 200 至方法 700 中的终端设备，该通信装置 800 可以包括用于执行图 2 中的方法 200、图 3 中的方法 300、图 4 中的方法 200、图 5 中的方法 500、图 6 中的方法 600 和图 7 中的方法 700 中的终端设备执行的方法的单元。并且，该通信装置 800 中的各单元和上述其他操作和/或功能分别为了实现图 2 中的方法 200、图 3 中的方法 300、图 4 中的方法 200、图 5 中的方法 500、图 6 中的方法 600 和图 7 中的方法 700 的相应流程。应理解，各单元执行上述相应步骤的具体过程在上述方法实施例中已经详细说明，为了简洁，在此不再赘述。

还应理解，该通信装置 800 中的收发单元 810 可对应于图 9 中示出的通信设备 900 中的收发器 920，该通信装置 800 中的处理单元 820 可对应于图 9 中示出的通信设备 900 中的处理器 910。

还应理解，当该通信装置 800 为芯片时，该芯片包括收发单元和处理单元。其中，收发单元可以是输入输出电路或通信接口；处理单元可以为该芯片上集成的处理器或者微处理器或者集成电路。

收发单元 810 用于实现通信装置 800 的信号的收发操作，处理单元 820 用于实现通信装置 800 的信号的处理操作。

可选地，该通信装置 800 还包括存储单元 830，该存储单元 830 用于存储指令。

图 9 是本申请实施例提供的通信设备 900 的示意性框图。如图所示，该通信设备 900

包括：至少一个处理器 910 和收发器 920。该处理器 910 与存储器耦合，用于执行存储器中存储的指令，以控制收发器 920 发送信号和/或接收信号。可选地，该通信设备 900 还包括存储器 930，用于存储指令。

5 应理解，上述处理器 910 和存储器 930 可以合成一个处理装置，处理器 910 用于执行存储器 930 中存储的程序代码来实现上述功能。具体实现时，该存储器 930 也可以集成在处理器 910 中，或者独立于处理器 910。

还应理解，收发器 920 可以包括接收器（或者称，接收机）和发射器（或者称，发射机）。收发器 920 还可以进一步包括天线，天线的数量可以为一个或多个。收发器 920 有可以是通信接口或者接口电路。

10 当该通信设备 900 为芯片时，该芯片包括收发单元和处理单元。其中，收发单元可以是输入输出电路或通信接口；处理单元可以为该芯片上集成的处理器或者微处理器或者集成电路。本申请实施例还提供了一种处理装置，包括处理器和接口。所述处理器可用于执行上述方法实施例中的方法。

应理解，上述处理装置可以是一个芯片。例如，该处理装置可以是现场可编程门阵列（field programmable gate array, FPGA），可以是专用集成芯片（application specific integrated circuit, ASIC），还可以是系统芯片（system on chip, SoC），还可以是中央处理器（central processor unit, CPU），还可以是网络处理器（network processor, NP），还可以是数字信号处理电路（digital signal processor, DSP），还可以是微控制器（micro controller unit, MCU），还可以是可编程控制器（programmable logic device, PLD）或其他集成芯片。

20 在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

应注意，本申请实施例中的处理器可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现场可编程门阵列（FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

可以理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（read-only memory, ROM）、可编程只读存储器（programmable ROM, PROM）、可擦除可编程只读存储器（erasable PROM, EPROM）、电可擦除可编程只读存储器（electrically EPROM,

EEPROM)或闪存。易失性存储器可以是随机存取存储器(random access memory, RAM),其用作外部高速缓存。通过示例性但不是限制性说明,许多形式的RAM可用,例如静态随机存取存储器(static RAM, SRAM)、动态随机存取存储器(dynamic RAM, DRAM)、同步动态随机存取存储器(synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(double data rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器(enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(synchlink DRAM, SLD RAM)和直接内存总线随机存取存储器(direct rambus RAM, DR RAM)。应注意,本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

5 根据本申请实施例提供的方法,本申请还提供一种计算机程序产品,该计算机程序产品包括:计算机程序代码,当该计算机程序代码在计算机上运行时,使得该计算机执行图2至图7所示实施例中任意一个实施例的方法。

根据本申请实施例提供的方法,本申请还提供一种计算机可读介质,该计算机可读介质存储有程序代码,当该程序代码在计算机上运行时,使得该计算机执行图2至图7所示实施例中任意一个实施例的方法。

15 根据本申请实施例提供的方法,本申请还提供一种系统,其包括前述的会话管理网元、终端设备和接入和移动性管理功能网元。

在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机指令时,全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、20 计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(digital subscriber line, DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质(例如,软盘、硬盘、磁带)、光介质(例如,高密度数字视频光盘(digital video disc, DVD))、或者半导体介质(例如,固态硬盘(solid state disc, SSD))等。

25 上述各个装置实施例中网络侧设备与终端设备和方法实施例中的网络侧设备或终端设备对应,由相应的模块或单元执行相应的步骤,例如通信单元(收发器)执行方法实施例中接收或发送的步骤,除发送、接收外的其它步骤可以由处理单元(处理器)执行。具体单元的功能可以参考相应的方法实施例。其中,处理器可以为一个或多个。

在本说明书中使用的术语“部件”、“模块”、“系统”等用于表示计算机相关的实体、硬件、固件、硬件和软件的组合、软件、或执行中的软件。例如,部件可以是但不限于,在35 处理器上运行的进程、处理器、对象、可执行文件、执行线程、程序和/或计算机。通过图示,在计算设备上运行的应用和计算设备都可以是部件。一个或多个部件可驻留在进程和/或执行线程中,部件可位于一个计算机上和/或分布在两个或更多个计算机之间。此外,这些部件可在上面存储有各种数据结构的各种计算机可读介质执行。部件可例如根据具有一个或多个数据分组(例如来自与本地系统、分布式系统和/或网络间的另一部件交互40

的二个部件的数据，例如通过信号与其它系统交互的互联网）的信号通过本地和/或远程进程来通信。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory, ROM）、随机存取存储器（Random Access Memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以所述权利要求的保护范围为准。

权 利 要 求 书

1. 一种通信方法，其特征在于，包括：

5 在终端设备在第一网络中建立会话的过程中，会话管理网元获取第一指示信息，所述第一指示信息用于指示在第二网络中支持用户面完整性保护；

所述会话管理网元根据所述第一指示信息，向所述第一网络的接入和移动性管理功能网元发送第一请求消息，所述第一请求消息用于请求为所述会话分配承载标识，所述承载标识与所述终端设备在所述第二网络的承载上下文对应；

10 所述会话管理网元接收来自所述接入和移动性管理功能网元的第一响应消息，所述第一响应消息包括所述承载标识。

2. 根据权利要求1所述的方法，其特征在于，所述方法还包括：

所述会话管理网元将所述终端设备在所述第一网络中的用户面安全策略映射为所述终端设备在所述第二网络的用户面安全策略；

所述会话管理网元将所述第二网络的用户面安全策略保存在所述承载上下文中。

15 3. 根据权利要求2所述的方法，其特征在于，所述方法还包括：

所述会话管理网元获取第三指示信息，所述第三指示信息用于指示执行用户面安全策略映射；

所述会话管理网元将所述终端设备在所述第一网络中的用户面安全策略映射为所述终端设备在所述第二网络的用户面安全策略，包括：

20 所述会话管理网元根据所述第三指示信息，将所述终端设备在所述第一网络中的用户面安全策略映射为所述终端设备在所述第二网络的用户面安全策略。

4. 根据权利要求2或3所述的方法，其特征在于，所述方法还包括：

25 所述会话管理网元通过所述接入和移动性管理功能网元将所述承载上下文发送给所述第二网络中的目标移动管理实体；其中，所述目标移动管理实体为将所述会话切换到所述第二网络时为所述终端设备服务的网元。

5. 根据权利要求1至4中任一项所述的方法，其特征在于，所述会话管理网元根据所述第一指示信息，向所述第一网络的接入和移动性管理功能网元发送第一请求消息，包括：

30 所述会话管理网元根据所述第一指示信息，不考虑所述终端设备在所述第一网络的用户面安全策略，向所述接入和移动性管理功能网元发送所述第一请求消息。

6. 根据权利要求1至5中任一项所述的方法，其特征在于，所述方法还包括：

所述会话管理网元根据所述第一指示信息，不考虑所述终端设备在所述第一网络的用户面安全策略，向统一数据管理网元发送所述会话管理网元在S5/S8接口上的全量域名。

35 7. 根据权利要求5或6所述的方法，其特征在于，所述终端设备在第一网络的用户面安全策略包括开启用户面完整性保护。

8. 根据权利要求1至7中任一项所述的方法，其特征在于，所述会话管理网元获取第一指示信息，包括：

所述会话管理网元接收来自所述接入和移动性管理功能网元的所述第一指示信息。

9. 根据权利要求8所述的方法，其特征在于，所述第一指示信息包含在协议数据单

元会话建立会话管理上下文请求消息中。

10. 根据权利要求 1 至 9 中任一项所述的方法，其特征在于，所述会话管理网元获取第一指示信息，包括：

5 所述会话管理网元通过所述接入和移动性管理功能网元接收来自所述终端设备的所述第一指示信息。

11. 根据权利要求 1 至 10 中任一项所述的方法，其特征在于，所述第一网络为第五代通信系统网络，所述第二网络为演进分组系统网络，所述承载上下文为演进分组系统承载上下文。

12. 一种通信方法，其特征在于，包括：

10 第一网络中的接入和移动性管理功能网元接收来自终端设备的注册请求消息，所述注册请求消息包括第二指示信息，其中，所述第二指示信息用于指示终端设备在第二网络中支持用户面完整性保护；

15 在所述终端设备在所述第一网络建立会话的过程中，所述接入和移动性管理功能网元根据所述第二指示信息，向会话管理网元发送第一指示信息，所述第一指示信息用于指示在第二网络中支持用户面完整性保护；

所述接入和移动性管理功能网元接收第一请求消息，所述第一请求消息用于请求为所述会话分配承载标识，所述承载标识与所述终端设备在所述第二网络的承载上下文对应；

所述接入和移动性管理功能网元向所述会话管理网元发送第一响应消息，所述第一响应消息包括所述承载标识。

20 13. 根据权利要求 12 所述的方法，其特征在于，所述方法还包括：

所述接入和移动性管理功能网元向所述会话管理功能网元发送第二请求消息；

25 所述接入和移动性管理功能网元接收来自所述会话管理网元的第二响应消息，所述第二响应消息包括所述承载上下文，所述承载上下文包括终端设备在所述第二网络的用户面安全策略，所述第二网络的用户面安全策略是根据所述终端设备在所述第一网络的用户面安全策略得到的；

所述接入和移动性管理功能网元向所述第二网络中的目标移动管理实体发送所述承载上下文，所述目标移动管理实体为将所述会话切换到所述第二网络时为所述终端设备服务的网元。

30 14. 根据权利要求 13 所述的方法，其特征在于，所述第二请求消息包括第三指示信息，所述第三指示信息用于指示执行用户面安全策略映射；

所述方法还包括：

所述接入和移动性管理功能网元根据第二本地策略，确定在所述第二请求消息中携带所述第三指示信息；

35 所述第二本地策略包括以下一项或多项：所述会话是否支持与所述第二网络互通，所述目标移动管理实体是否支持用户面完整性保护，所述目标移动管理实体为将所述会话切换到所述第二网络时为所述终端设备服务的网元。

15. 根据权利要求 13 或 14 所述的方法，其特征在于，

所述第一网络的用户面安全策略的粒度为协议数据单元会话的粒度；

所述第二网络的用户面安全策略的粒度为演进分组系统承载的粒度。

40 16. 根据权利要求 12 至 15 中任一项所述的方法，其特征在于，所述方法还包括：

所述接入和移动性管理功能网元根据第一本地策略，确定向所述会话管理网元发送所述第一指示信息，所述第一本地策略包括：所述会话是否支持与所述第二网络互通。

17. 根据权利要求 12 至 16 中任一项所述的方法，其特征在于，所述第一网络为第五代通信系统网络，所述第二网络为演进分组系统网络，所述承载上下文为演进分组系统承载上下文。

18. 一种通信方法，其特征在于，包括：

终端设备向第一网络中的接入和移动性管理功能网元发送第二指示信息，所述第二指示信息用于指示所述终端设备在第二网络中支持用户面完整性保护；

所述终端设备接收来自所述第二网络的接入网设备发送的无线资源控制重配置，所述无线资源控制重配置包括开启用户面完整性保护的指示信息。

19. 根据权利要求 18 所述的方法，其特征在于，所述第二指示信息包含在注册请求消息中。

20. 根据权利要求 18 所述的方法，其特征在于，所述第二指示信息包含在协议数据单元会话建立请求消息中。

21. 一种通信装置，其特征在于，包括收发单元，

在终端设备在第一网络中建立会话的过程中，所述收发单元用于获取第一指示信息，所述第一指示信息用于指示在第二网络中支持用户面完整性保护；

所述收发单元还用于根据所述第一指示信息，向所述第一网络的接入和移动性管理功能网元发送第一请求消息，所述第一请求消息用于请求为所述会话分配承载标识，所述承载标识与所述终端设备在所述第二网络的承载上下文对应；

所述收发单元还用于接收来自所述接入和移动性管理功能网元的第一响应消息，所述第一响应消息包括所述承载标识。

22. 根据权利要求 21 所述的通信装置，其特征在于，所述通信装置还包括处理单元，所述处理单元用于将所述终端设备在所述第一网络中的用户面安全策略映射为所述终端设备在所述第二网络的用户面安全策略；

所述处理单元还用于将所述第二网络的用户面安全策略保存在所述承载上下文中。

23. 根据权利要求 22 所述的通信装置，其特征在于，所述收发单元还用于获取第三指示信息，所述第三指示信息用于指示执行用户面安全策略映射；

所述处理单元具体用于根据所述第三指示信息，将所述终端设备在所述第一网络中的用户面安全策略映射为所述终端设备在所述第二网络的用户面安全策略。

24. 根据权利要求 22 或 23 所述的通信装置，其特征在于，所述收发单元还用于通过所述接入和移动性管理功能网元将所述承载上下文发送给所述第二网络中的目标移动管理实体；其中，所述目标移动管理实体为将所述会话切换到所述第二网络时为所述终端设备服务的网元。

25. 根据权利要求 21 至 24 中任一项所述的通信装置，其特征在于，所述收发单元具体用于根据所述第一指示信息，不考虑所述终端设备在所述第一网络的用户面安全策略，向所述接入和移动性管理功能网元发送所述第二请求消息。

26. 根据权利要求 21 至 25 中任一项所述的通信装置，其特征在于，所述收发单元还用于根据所述第一指示信息，不考虑所述终端设备在所述第一网络的用户面安全策略，向统一数据管理网元发送所述通信装置在 S5/S8 接口上的全量域名。

27. 根据权利要求 25 或 26 所述的通信装置, 其特征在于, 所述终端设备在第一网络的用户面安全策略包括开启用户面完整性保护。

28. 根据权利要求 21 至 27 中任一项所述的通信装置, 其特征在于, 所述收发单元具体用于接收来自所述接入和移动性管理功能网元的所述第一指示信息。

5 29. 根据权利要求 21 至 28 中任一项所述的通信装置, 其特征在于, 所述收发单元具体用于通过所述接入和移动性管理功能网元接收来自所述终端设备的所述第一指示信息。

30. 根据权利要求 29 所述的通信装置, 其特征在于, 所述第一指示信息包含在协议数据单元会话建立请求消息中。

10 31. 根据权利要求 21 至 30 中任一项所述的通信装置, 其特征在于, 所述第一网络为第五代通信系统网络, 所述第二网络为演进分组系统网络, 所述承载上下文为演进分组系统承载上下文。

32. 一种通信装置, 其特征在于, 包括收发单元,

15 所述收发单元用于在第一网络接收来自终端设备的注册请求消息, 所述注册请求消息包括第二指示信息, 其中, 所述第二指示信息用于指示终端设备在第二网络中支持用户面完整性保护;

在所述终端设备在所述第一网络建立会话的过程中, 所述收发单元还用于根据所述第二指示信息, 向会话管理网元发送第一指示信息, 所述第一指示信息用于指示在第二网络中支持用户面完整性保护;

20 所述收发单元还用于接收第一请求消息, 所述第一请求消息用于请求为所述会话分配承载标识, 所述承载标识与所述终端设备在所述第二网络的承载上下文对应;

所述收发单元还用于向所述会话管理网元发送第一响应消息, 所述第一响应消息包括所述承载标识。

33. 根据权利要求 32 所述的通信装置, 其特征在于, 所述收发单元还用于向所述会话管理功能网元发送第二请求消息;

25 所述收发单元还用于接收来自所述会话管理网元的第二响应消息, 所述第二响应消息包括所述承载上下文, 所述承载上下文包括终端设备在所述第二网络的用户面安全策略, 所述第二网络的用户面安全策略是根据所述终端设备在所述第一网络的用户面安全策略得到的;

30 所述收发单元还用于向所述第二网络中的目标移动管理实体发送所述承载上下文, 所述目标移动管理实体为将所述会话切换到所述第二网络时为所述终端设备服务的网元。

34. 根据权利要求 33 所述的通信装置, 其特征在于, 所述第二请求消息包括第三指示信息, 所述第三指示信息用于指示执行用户面安全策略映射;

所述通信装置还包括处理单元,

35 所述处理单元用于根据第二本地策略, 确定在所述第二请求消息中携带所述第三指示信息;

所述第二本地策略包括以下一项或多项: 所述会话是否支持与所述第二网络互通, 所述目标移动管理实体是否支持用户面完整性保护, 所述目标移动管理实体为将所述会话切换到所述第二网络时为所述终端设备服务的网元。

40 35. 根据权利要求 33 或 34 所述的通信装置, 其特征在于, 所述第一网络的用户面安全策略的粒度为协议数据单元会话的粒度;

所述第二网络的用户面安全策略的粒度为演进分组系统承载的粒度。

36. 根据权利要求 32 至 35 中任一项所述的通信装置，其特征在于，所述通信装置还包括处理单元，

5 所述处理单元用于根据本地策略，确定向所述会话管理网元发送所述第一指示信息，
所述本地策略包括所述会话是否支持与所述第二网络互通。

37. 根据权利要求 32 至 36 中任一项所述的通信装置，其特征在于，所述第一网络为第五代通信系统网络，所述第二网络为演进分组系统网络，所述承载上下文为演进分组系统承载上下文。

38. 一种通信装置，其特征在于，包括收发单元，
10 所述收发单元用于向第一网络中的接入和移动性管理功能网元发送第二指示信息，所述第二指示信息用于指示所述通信装置在第二网络中支持用户面完整性保护；

所述收发单元还用于接收来自所述第二网络的接入网设备发送的无线资源控制重配置，所述无线资源控制重配置包括开启用户面完整性保护的指示信息。

39. 根据权利要求 38 所述的通信装置，其特征在于，所述第二指示信息包含在注册
15 请求消息中。

40. 根据权利要求 38 所述的通信装置，其特征在于，所述第二指示信息包含在协议数据单元会话建立请求消息中。

41. 一种通信设备，其特征在于，包括：
存储器，所述存储器用于存储计算机程序；
20 收发器，所述收发器用于执行收发步骤；
处理器，所述处理器用于从所述存储器中调用并运行所述计算机程序，使得所述通信设备执行权利要求 1 至 20 中任一项所述的方法。

42. 一种计算机可读存储介质，其特征在于，包括：所述计算机可读介质存储有计算机程序；所述计算机程序在计算机上运行时，使得所述计算机执行权利要求 1 至 20 中任
25 一项所述的方法。