CLAIMS

What is claimed is:

1. A security policy processing method, comprising:

receiving, by a target access network device, a message 001 from a source access network device, wherein the message 001 comprises indication information 011; and

when the indication information 011 indicates that a terminal device supports user plane integrity protection, sending, by the target access network device to a mobility management entity, a path switch request 031 that carries a user plane security policy 021, wherein the user plane security policy 021 indicates whether to enable user plane integrity protection.

2. The method according to claim 1, wherein the access network device is an evolved NodeB eNB.

3. The method according to claim 1 or 2, wherein when the target access network device does not receive a user plane security policy from the source access network device, the user plane security policy 021 is a user plane security policy 021-2 preconfigured on the target access network device.

4. The method according to claim 3, wherein the method further comprises:

when the target access network device determines that the terminal device supports user plane security protection based on the indication information 011, determining, by the target access network device based on the user plane security policy 021-2 preconfigured on the target access network device, a user plane security activation status; and

indicating, by the target access network device, the user plane security activation status to the terminal device.

5. The method according to claim 3 or 4, wherein the message 001 further comprises identifiers of N evolved radio access bearers of the terminal device, and N is an integer greater than or equal to 1; and

the path switch request 031 further comprises the identifiers of the N evolved radio access bearers.

6. The method according to claim 5, wherein the path switch request 031 comprises N user plane security policies 021-2, and each of the identifiers of the N evolved radio access bearers corresponds to one of the N user plane security policies 021-2.

7. The method according to any one of claims 1 to 6, wherein after the sending, by the target access network device to a mobility management entity, a path switch request 031 that carries a user plane security policy 021, the method further comprises:

receiving, by the target access network device, a path switch response 041 from the mobility management entity, wherein the path switch response 041 carries a user plane security policy 022; and

storing, by the target access network device, the user plane security policy 022 in a context of the terminal device.

8. The method according to claim 7, wherein the storing, by the target access network device, the user plane security policy 022 in a context of the terminal device comprises:

when the user plane security policy 021 is stored in the context of the terminal device, updating, by the target access network device using the user plane security policy 022, the user plane security policy 021 stored in the context of the terminal device.

9. The method according to claim 7 or 8, wherein the method further comprises:

determining, by the mobility management entity, whether the user plane security policy 021 is consistent with a user security policy on the mobility management entity;

if the user plane security policy 021 is inconsistent with the user security policy on the mobility management entity, sending, by the mobility management entity, the path switch response 041 to the target access network device.

10. The method according to any one of claims 7 to 9, wherein the method further comprises:

if a current user plane security activation status of the terminal device does not match the user plane security policy 022, enabling or skipping enabling, by the target access network device, user plane integrity protection for the terminal device according to the user plane security policy 022, wherein the current user plane security activation status is a status of whether user plane integrity protection is currently enabled between the target access network device and the terminal device.

11. The method according to any one of claims 1 to 10, wherein the indication information 011 is represented by a part of bits of an evolved packet system security capability of the terminal device, and the evolved packet system security capability of the terminal device indicates at least one security algorithm supported by the terminal device.

12.The method according to claim 11, wherein the indication information 011 is represented by EIA7 in the evolved packet system security capability of the terminal device.

13. The method according to any one of claims 1 to 12, wherein the message 001 is a handover request or a context retrieve response.

14. The method according to any one of claims 1 to 13, further comprising:

receiving, by the mobility management entity, the path switch request 031.

15. The method according to any one of claims 1 to 14, further comprising:

sending, by the source access network device, the message 001 to the target access network device.

16. A communication apparatus, comprising function modules configured to perform the method according to any one of the claims 1 to 13.

17. A communication apparatus, comprising: at least one processor coupled to at least one memory, wherein when instructions stored in the at least one memory are executed by the at least processor, the communication device is enabled to perform the method according to any one of the claims 1 to 13.

18. The communication apparatus according to claim 17, wherein the communication apparatus is a target access network device, or a chip in the target access network device.

19. A computer-readable storage medium, wherein the computer-readable storage medium stores instructions, and when the instructions run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 13.

20. A communication system, comprising: the communication apparatus according to any one of claims 16 to 18, and further comprising a mobility management entity, a source access network device and/or a terminal device.