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~~on-demand user plane security protection between the terminal device and an access network device~~, 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 ciphering protection and/or~~ 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 021-1 constructed by the target access network device.~~

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

~~determining, by the target access network device, that a user plane security activation status between the target access network device and the terminal device is that user plane ciphering protection is enabled and user plane integrity protection is not enabled; and~~

~~constructing, by the target access network device, the user plane security policy 021-1 that matches the user plane security activation status.~~

~~5. The method according to claim 3 or 4, wherein the user plane security policy 021-1 comprises a user plane ciphering protection policy and a user plane integrity protection policy, the user plane ciphering protection policy indicates that enabling is required or enabling is preferred, and the user plane integrity protection policy indicates that enabling is not needed or enabling is preferred.~~

~~6~~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.

~~7~~5. The method according to claim ~~6~~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.

~~8~~6. The method according to claim ~~7~~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.

~~9~~7. The method according to any one of claims 1 to ~~8~~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 ciphering protection and/or~~ 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 ciphering protection and/or~~ user plane integrity protection ~~are~~ is currently enabled between the target access network device and the terminal device.

~~11. The method according to claim 1, wherein the method further comprises:~~

~~when the indication information 011 indicates that the terminal device does not support on-demand user plane security protection between the terminal device and an access network device, sending, by the target access network device to the mobility management entity, a path switch request 032 that carries no user plane security policy; and~~

~~receiving, by the target access network device from the mobility management entity, a path switch response 042 that carries no user plane security policy.~~

~~12. The method according to claim 1, wherein the method further comprises:~~

~~when the indication information 011 indicates that the terminal device does not support on-demand user plane security protection between the terminal device and an access network device, sending, by the target access network device to the mobility management entity, a path switch request 033 that carries no user plane security policy, wherein the path switch request 033 carries the indication information 011;~~

~~receiving, by the target access network device from the mobility management entity, a path switch response 043 that carries a user plane security policy 023; and~~

~~storing, by the target access network device, the user plane security policy 023 in a context of the terminal device.~~

~~13. The method according to claim 12, wherein the path switch response 043 carrying the user plane security policy 023 further carries indication information 012, and the indication~~

~~information 012 indicates that the terminal device supports on-demand user plane security protection between the terminal device and an access network device.~~

~~14. The method according to claim 12 or 13, 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 023, enabling or skipping enabling, by the target access network device, user plane ciphering protection and/or user plane integrity protection for the terminal device according to the user plane security policy 023, wherein the current user plane security activation status is a status of whether user plane ciphering protection and/or user plane integrity protection are currently enabled between the target access network device and the terminal device.~~

~~15~~11. The method according to any one of claims 1 to ~~14~~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.

~~16~~13. The method according to any one of claims 1 to ~~15~~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.

~~17.~~ A communication ~~device~~ 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.

a receiving module, configured to receive a message 001 from a source access network device, wherein the message 001 comprises indication information 011; and

a processing module, configured to: when the indication information 011 indicates that a terminal device supports on-demand user plane security protection between the terminal device and an access network device, control a sending module to send, 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 ciphering protection and/or whether to enable user plane integrity protection.

18. The communication device according to claim 17, wherein the access network device is an evolved NodeB eNB.

19. The communication device according to claim 17 or 18, wherein when the communication 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 021-1 constructed by the communication device.

20. The communication device according to claim 19, wherein the processing module is further configured to:

determine that a user plane security activation status between the access network device and the terminal device is that user plane ciphering protection is enabled and user plane integrity protection is not enabled; and

construct the user plane security policy 021-1 that matches the user plane security activation status.

21. The communication device according to claim 19 or 20, wherein the user plane security policy 021-1 comprises a user plane ciphering protection policy and a user plane integrity protection policy, the user plane ciphering protection policy indicates that enabling is required or enabling is preferred, and the user plane integrity protection policy indicates that enabling is not needed or enabling is preferred.

22. The communication device according to claim 17 or 18, wherein when the communication 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 communication device.

23. The communication device according to claim 22, 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.

24. The communication device according to claim 23, 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.

25. The communication device according to any one of claims 17 to 24, wherein

the receiving module is further configured to receive a path switch response 041 from the mobility management entity, wherein the path switch response 041 carries a user plane security policy 022; and

the communication device further comprises a storage module, wherein

the storage module is configured to store the user plane security policy 022 in a context of the terminal device.

26. The communication device according to claim 25, wherein the processing module is further configured to:

when a current user plane security activation status of the terminal device does not match the user plane security policy 022, enable or skip enabling user plane ciphering protection and/or 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 ciphering protection and/or user plane integrity protection are currently enabled between a target access network device and the terminal device.

27. The communication device according to claim 17, wherein

the sending module is further configured to:

when the indication information 011 indicates that the terminal device does not support on-demand user plane security protection between the terminal device and an access network device, send, to the mobility management entity, a path switch request 032 that carries no user plane security policy; and

the receiving module is further configured to receive, from the mobility management entity, a path switch response 042 that carries no user plane security policy.

28. The communication device according to claim 17, wherein

the sending module is further configured to:

when the indication information 011 indicates that the terminal device does not support on-demand user plane security protection between the terminal device and an access network device, send, to the mobility management entity, a path switch request 033 that carries no user plane security policy, wherein the path switch request 033 carries the indication information 011;

the receiving module is further configured to receive, from the mobility management entity, a path switch response 043 that carries a user plane security policy 023; and

the communication device further comprises a storage module, wherein

the storage module is configured to store the user plane security policy 023 in a context of the terminal device.

29. The communication device according to claim 28, wherein the path switch response 043 carrying the user plane security policy 023 further carries indication information 012, and the indication information 012 indicates that the terminal device supports on-demand user plane security protection between the terminal device and an access network device.

30. The communication device according to claim 28 or 29, wherein the processing module is further configured to:

when a current user plane security activation status of the terminal device does not match the user plane security policy 023, enable or skip enabling user plane ciphering protection and/or user plane integrity protection for the terminal device according to the user plane security policy 023, wherein the current user plane security activation status is a status of whether user plane ciphering protection and/or user plane integrity protection are currently enabled between a target access network device and the terminal device.

31. The communication device according to any one of claims 17 to 30, 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.

32. The communication device according to any one of claims 17 to 31, wherein the message 001 is a handover request or a context retrieve response.

33. A communication device, wherein the communication device comprises a processor, a memory, and a transceiver, the memory stores program code, and the processor is configured to

invoke the program code stored in the memory, to perform the following operations:

controlling the transceiver to receive 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 on-demand user plane security protection between the terminal device and an access network device, controlling the transceiver to send, 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 ciphering protection and/or whether to enable user plane integrity protection.

34. The communication device according to claim 33, wherein the access network device is an evolved NodeB eNB.

35. The communication device according to claim 33 or 34, wherein when the communication 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 021-1 constructed by the communication device.

36. The communication device according to claim 35, wherein the processor is further configured to:

determine that a user plane security activation status between the access network device and the terminal device is that user plane ciphering protection is enabled and user plane integrity protection is not enabled; and

construct the user plane security policy 021-1 that matches the user plane security activation status.

37. The communication device according to claim 35 or 36, wherein the user plane security policy 021-1 comprises a user plane ciphering protection policy and a user plane integrity protection policy, the user plane ciphering protection policy indicates that enabling is required or enabling is preferred, and the user plane integrity protection policy indicates that enabling is not needed or enabling is preferred.

38. The communication device according to claim 33 or 34, wherein when the communication 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 communication device.

39. The communication device according to claim 38, 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.~~

~~40. The communication device according to claim 39, 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.~~

~~41. The communication device according to any one of claims 33 to 40, wherein the processor is further configured to:~~

~~control the transceiver to receive a path switch response 041 from the mobility management entity, wherein the path switch response 041 carries a user plane security policy 022; and~~

~~store the user plane security policy 022 in a context of the terminal device.~~

~~42. The communication device according to claim 41, wherein the processor is further configured to:~~

~~when a current user plane security activation status of the terminal device does not match the user plane security policy 022, enable or skip enabling user plane ciphering protection and/or 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 ciphering protection and/or user plane integrity protection are currently enabled between a target access network device and the terminal device.~~

~~43. The communication device according to claim 33, wherein the processor is further configured to:~~

~~when the indication information 011 indicates that the terminal device does not support on-demand user plane security protection between the terminal device and an access network device, control the transceiver to send, to the mobility management entity, a path switch request 032 that carries no user plane security policy; and~~

~~control the transceiver to receive, from the mobility management entity, a path switch response 042 that carries no user plane security policy.~~

~~44. The communication device according to claim 33, wherein the processor is further configured to:~~

~~when the indication information 011 indicates that the terminal device does not support on-~~

~~demand user plane security protection between the terminal device and an access network device, control the transceiver to send, to the mobility management entity, a path switch request 033 that carries no user plane security policy, wherein the path switch request 033 carries the indication information 011;~~

~~control the transceiver to receive, from the mobility management entity, a path switch response 043 that carries a user plane security policy 023; and~~

~~store the user plane security policy 023 in a context of the terminal device.~~

~~45. The communication device according to claim 44, wherein the path switch response 043 carrying the user plane security policy 023 further carries indication information 012, and the indication information 012 indicates that the terminal device supports on-demand user plane security protection between the terminal device and an access network device.~~

~~46. The communication device according to claim 44 or 45, wherein the processor is further configured to:~~

~~when a current user plane security activation status of the terminal device does not match the user plane security policy 023, enable or skip enabling user plane ciphering protection and/or user plane integrity protection for the terminal device according to the user plane security policy 023, wherein the current user plane security activation status is a status of whether user plane ciphering protection and/or user plane integrity protection are currently enabled between a target access network device and the terminal device.~~

~~47. The communication device according to any one of claims 33 to 46, 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.~~

~~48. The communication device according to any one of claims 33 to 47, wherein the message 001 is a handover request or a context retrieve response.~~

~~49~~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 1~~3~~6.

~~50. A computer program product comprising instructions, wherein when the instructions run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 16.~~

~~51~~20. A communication system, comprising:

~~a mobility management entity and~~ the communication apparatus ~~device~~ according to any one of claims ~~17~~ 16 to ~~32~~18, and further comprising a mobility management entity, a source access network device and/or a terminal device.

~~52. The communication system according to claim 51, wherein the communication system further comprises a source access network device and/or a terminal device.~~