CLAIMS

What is claimed is:

1. A security policy processing method, comprising:

receiving, by a communication device, a message from a source access network device, wherein the message comprises indication information, the communication device is a target access network device or a chip in the target access network device; and

when the message carries no user plane security policy indicating whether to enable user plane integrity protection and the communication device determines that a terminal device supports user plane integrity protection based on the indication information, sending, by the communication device to a mobility management entity, a path switch request that carries a first user plane security policy preconfigured on the target access network device, wherein the first user plane security policy indicates whether to enable user plane integrity protection.

2. The method according to claim 1, wherein the target access network device is a target evolved NodeB (eNB), and the source access network device is a source eNB.

3. The method according to claim 2, wherein the target eNB is an eNB supporting user plane security protection, and the source eNB is an eNB not supporting user plane security protection.

4. The method according to any one of claims 1 to 3, wherein the message 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 further comprises the identifiers of the N evolved radio access bearers.

5. The method according to claim 4, wherein the path switch request comprises N user plane security policies, and each of the identifiers of the N evolved radio access bearers corresponds to one of the N user plane security policies.

6. The method according to any one of claims 1 to 5, wherein after the sending, by the communication device to a mobility management entity, a path switch request that carries a first user plane security policy, the method further comprises:

receiving, by the communication device and from the mobility management entity, a path switch response that carries a second user plane security policy; and

storing, by the communication device, the second user plane security policy in a context of the terminal device.

7. The method according to claim 6, wherein the storing, by the target access network device, the second user plane security policy in a context of the terminal device comprises:

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

8. The method according to claim 6 or 7, wherein the method further comprises:

when a current user plane security activation status of the terminal device does not match the second user plane security policy, enabling or skipping enabling, by the communication device, user plane integrity protection for the terminal device according to the second user plane security policy , 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.

9. The method according to claim 8, wherein when a current user plane security activation status of the terminal device does not match the second user plane security policy, enabling or skipping enabling, by the communication device, user plane integrity protection for the terminal device according to the second user plane security policy comprises:

when the user plane security activation status of the terminal device is that the user plane integrity protection for the terminal device is not enabled and the second user plane security policy indicates that enabling is required, indicating the terminal device, by the communication device, to enable user plane integrity protection; or

when the user plane security activation status of the terminal device is that the user plane integrity protection for the terminal device is enabled and the second user plane security policy indicates that enabling is not needed, indicating the terminal device, by the communication device, to disable user plane integrity protection.

10. The method according to any one of claims 1 to 9, wherein the indication information 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.

11. The method according to claim 10, wherein the indication information is represented by EIA7 in the evolved packet system security capability of the terminal device.

12. The method according to any one of claims 1 to 11, wherein the message is a handover

request or a context retrieve response.

13. The method according to any one of claims 1 to 12, further comprising, when the message carries no user plane security policy and the communication device determines that the terminal device supports the user plane integrity protection based on the indication information:

determining, by the communication device based on the first user plane security policy, a user plane security activation status for the terminal device; and

sending, by the communication device, a handover request acknowledge to the source access network device, wherein the handover request acknowledge comprises the user plane security activation status which is to be sent to the terminal device.

14. The method according to claim 13, wherein the handover request acknowledge comprises radio resource control (RRC) connection reconfiguration, and the RRC connection reconfiguration comprises the user plane security activation status.

15. The method according to claim 13 or 14, wherein the determining, by the communication device based on the first user plane security policy, the user plane security activation status comprises:

if the first user plane security policy is "required", determining, by the communication device, user plane security activation statuses corresponding to all data radio bearer, DRBs of the terminal device are enabled; or

if the first user plane security policy is "not needed", determining, by the communication device, the user plane security activation statuses corresponding to all the DRBs of the terminal device are not enabled; or

if the first user plane security policy is "preferred", determining, by the communication device, the user plane security activation statuses corresponding to all the DRBs of the terminal device are enabled or not enabled.

16. The method according to claim any one of claims 13 to 15, wherein the user plane security activation status indicates user plane integrity protection is enabled or not enabled.

17. A communication device, 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 one processor, the communication device is enabled to perform the method according to any one of the claims 1 to 16.

18. 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 16.

19. A communication system, comprising: the communication device according to claim 17, and further comprising a mobility management entity configured to receive a path switch request carrying a first user plane security policy.

20. The communication system according to claim 19, wherein the mobility management entity is further configured to send, to the target access network device, a path switch response that carries a second user plane security policy on the mobility management entity, if the first user plane security policy is inconsistent with the second user plane security policy.

21. The communication system according to claim 19, further comprising a source access network device, configured to send a message comprises indication information to the target access network device.

22. The communication system according to claim 21, wherein the source network device is further configured to:

receive a handover request acknowledge from the target access network device, wherein the handover request acknowledge comprises a user plane security activation status; and

send the user plane security activation status to a terminal device.

23. The communication system according to claim 22, further comprising the terminal device, configured to receive the user plane security activation status from the source access network device.

24. A communication method, comprising the method according to any of claims 1-16, and further comprising:

receiving, by the mobility management entity, the path switch request that carries a first user plane security policy.

25. The method according to claim 24, further comprising:

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

26. The method according to claim 24 or 25, further comprising:

sending, by the source access network device, the message comprising indication information to the target access network device.

27. The method according to claim 26, further comprising:

receiving, by the source access network device, a handover request acknowledge from the target access network device, wherein the handover request acknowledge comprises a user plane security activation status; and

sending, by the source access network device, the user plane security activation status to a terminal device.

28. The method according to claim 27, further comprising:

receiving, by the terminal device, the user plane security activation status from the source access network device.

29. A computer program 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.