CLAIMS

What is claimed is:

1. A method for security table entry maintenance, which is applied to a first network device, the first network device comprising a remote MAC-IP table, the remote MAC-IP table comprising at least one remote MAC-IP table entry notified by a second network device, wherein the method comprises:

acquiring, in response to determining that a protocol connection between the first network device and the second network device is disconnected, a valid lifetime value included in each remote MAC-IP table entry, the valid lifetime value is used to indicate a valid lifetime of an IP address included in the remote MAC-IP table entry;

deleting, in response to determining that a duration during which the protocol connection is disconnected reaches the valid lifetime value, the at least one remote MAC-IP table entry.

2. The method of claim 1, further comprising:

establishing, in response to determining that the first network device generates a DHCP relay table entry, a local MAC-IP table entry based on the DHCP relay table entry, and issuing a forwarding MAC-IP table entry corresponding to the local MAC-IP table entry to hardware resources, the local MAC-IP table entry includes a first valid lifetime value of a first IP address;

sending a first MAC-IP notification message to a third network device to enable the third network device to establish a first remote MAC-IP table entry;

wherein, the first MAC-IP notification message includes a first sequence number and the first valid lifetime value, and the first remote MAC-IP table entry includes the first sequence number and the first valid lifetime value;

the first sequence number is a sum of 1 and a maximum sequence number in a remote MAC-IP table entry or remote MAC-IP table entries that matches/match the local MAC-IP table entry.

3. The method of claim 2, wherein after issuing a forwarding MAC-IP table entry corresponding to the local MAC-IP table entry to hardware resources, the method further comprises:

deleting, in response to determining that an access table entry that matches the local

MAC-IP table entry is deleted, the forwarding MAC-IP table entry.

4. The method of claim 1, wherein before acquiring, in response to determining that a protocol connection between the first network device and the second network device is disconnected, a valid lifetime value included in each remote MAC-IP table entry, the method further comprises:

receiving a second MAC-IP notification message sent by the second network device, wherein the second MAC-IP notification message includes a second valid lifetime value of a second IP address and a second sequence number;

establishing a second remote MAC-IP table entry, which includes the second valid lifetime value and the second sequence number.

5. The method of claim 4, wherein the first network device includes a local MAC-IP table, the local MAC-IP table includes at least one local MAC-IP table entry;

after establishing the second remote MAC-IP table entry, the method further comprises:

receiving a first packet sent by a terminal, the first packet includes a MAC address and an IP address of the terminal;

in response to determining that there is no local MAC-IP table entry in the local MAC-IP table which matches the MAC address and the IP address of the terminal, and the MAC address and the IP address of the terminal match the second remote MAC-IP table entry, performing access detection on the terminal;

generating, in response to determining that an access response sent by the terminal is received, a synthetic MAC-IP table entry, which includes a port identifier, a VLAN identifier, the MAC address and the IP address of the terminal;

generating a forwarding MAC-IP table entry based on the synthetic MAC-IP table entry, the forwarding MAC-IP table entry comprises the MAC address and the IP address of the terminal;

issuing the forwarding MAC-IP table entry to hardware resources.

6. The method of claim 5, wherein after issuing the forwarding MAC-IP table entry to the hardware resources, the method further comprises:

deleting, in response to determining that an access table entry of the terminal is deleted, the synthetic MAC-IP table entry and the forwarding MAC-IP table entry.

7. The method of claim 4, wherein the first network device includes a local MAC-IP table, the local MAC-IP table includes a first local MAC-IP table entry, and the first local MAC-IP table entry includes a third sequence number; after establishing the second remote MAC-IP table entry, the method further comprises:

in response to determining that the second remote MAC-IP table entry matches the first local MAC-IP table entry, and the second sequence number is greater than the third sequence number, deleting the first local MAC-IP table entry, and deleting a DHCP relay table entry corresponding to the first local MAC-IP table entry.

8. The method of any one of claims 1-7, wherein the MAC-IP notification message sent by the first network device includes a first extended community attribute, and the first extended community attribute includes a valid lifetime value of an IP address.

9. The method of claim 8, wherein the MAC-IP notification message sent by the first network device further comprises a second extended community attribute, which comprises a sequence number of a MAC-IP table entry.

10. A method for security table entry maintenance, which is applied to a second network device, the second network device comprising a first remote MAC-IP table, the first remote MAC-IP table comprising at least one remote MAC-IP table entry notified by a fourth network device, wherein the method comprises:

acquiring, in response to determining that a protocol connection between the second network device and the fourth network device is disconnected, a valid lifetime value included in each remote MAC-IP table entry, wherein the valid lifetime value is used to indicate a valid lifetime of an IP address included in the remote MAC-IP table entry;

deleting, in response to determining that a duration during which the protocol connection is disconnected reaches the valid lifetime value, the at least one remote MAC-IP table entry.

11. The method of claim 10, wherein before acquiring, in response to determining that a protocol connection between the second network device and the fourth network device is disconnected, a valid lifetime value included in each remote MAC-IP table entry, the method further comprises:

receiving a first MAC-IP notification message sent by the fourth network device, wherein the first MAC-IP notification message comprises a first valid lifetime value of a first IP address

and a first sequence number;

establishing a first remote MAC-IP table entry, which includes the first valid lifetime value and the first sequence number.

12. The method of claim 11, wherein the second network device further comprises at least one second remote MAC-IP table, the at least one second remote MAC-IP table comprises a second remote MAC-IP table entry, the second remote MAC-IP table entry matches the first remote MAC-IP table entry, and the second remote MAC-IP table entry comprises a second sequence number; after establishing the first remote MAC-IP table entry, the method further comprises:

sending, in response to determining that the first sequence number is greater than the second sequence number, a second MAC-IP notification message to other network devices other than the fourth network device, wherein the second MAC-IP notification message comprises the first valid lifetime value and the first sequence number.

13. The method of claim 10, wherein the second remote device further comprises at least one third remote MAC-IP table, each third remote MAC-IP table comprises at least one remote MAC-IP table entry; after deleting the at least one remote MAC-IP table entry, the method further comprises:

for each deleted remote MAC-IP table entry, in response to determining that there is no remote MAC-IP table entry in the at least one third remote MAC-IP table which matches this deleted remote MAC-IP table entry, sending a first MAC-IP revocation message to other network devices other than the fourth network device, wherein the first MAC-IP revocation message comprises a MAC address and an IP address in the remote MAC-IP table entry; or,

for each deleted remote MAC-IP table entry, in response to determining that there are remote MAC-IP table entries in the at least one third remote MAC-IP table that match this deleted remote MAC-IP table entry, selecting a third remote MAC-IP table entry with a highest sequence number from the matched remote MAC-IP table entries, wherein the third remote MAC-IP table entry comprises a second valid lifetime value and a third sequence number; and sending a third MAC-IP notification message to other network devices other than a fifth network device, wherein the third MAC-IP notification message comprises the second valid lifetime value and the third sequence number, and the fifth network device is a source device of the third

remote MAC-IP table entry.

14. The method of any one of claims 10-13, wherein the MAC-IP notification message sent by the second network device comprises a first extended community attribute, and the first extended community attribute comprises a valid lifetime value of an IP address.

15. The method of claim 14, wherein the MAC-IP notification message sent by the second network device further comprises a second extended community attribute, which comprises a sequence number of a MAC-IP table entry.

16. An apparatus for security table entry maintenance, which is applied to a first network device, the first network device comprising a remote MAC-IP table, the remote MAC-IP table comprising at least one remote MAC-IP table entry notified by a second network device, wherein the apparatus comprises:

an acquisition module, to acquire, in response to determining that a protocol connection between the first network device and the second network device is disconnected, a valid lifetime value included in each remote MAC-IP table entry, the valid lifetime value is used to indicate a valid lifetime of an IP address included in the remote MAC-IP table entry;

a deletion module, to delete, in response to determining that a duration during which the protocol connection is disconnected reaches the valid lifetime value, the at least one remote MAC-IP table entry.

17. An apparatus for security table entry maintenance, which is applied to a second network device, the second network device including a first remote MAC-IP table, the first remote MAC-IP table including at least one remote MAC-IP table entry notified by a fourth network device, wherein the apparatus comprises:

an acquisition module, to acquire, in response to determining that a protocol connection between the second network device and the fourth network device is disconnected, a valid lifetime value included in each remote MAC-IP table entry, the valid lifetime value is used to indicate a valid lifetime of an IP address included in the remote MAC-IP table entry;

a deletion module, to delete, in response to determining that a duration during which the protocol connection is disconnected reaches the valid lifetime value, the at least one remote MAC-IP table entry.

18. A first network device, wherein the first network device includes a remote MAC-IP

table, the remote MAC-IP table includes at least one remote MAC-IP table entry notified by a second network device, and the first network device comprises:

a processor;

a transceiver;

a machine storage medium having stored therein machine executable instructions which, when being executed by the processor, cause the processor to perform the method of any one of claims 1-9.

19. A second network device, wherein the second network device includes a first remote MAC-IP table, the first remote MAC-IP table includes at least one remote MAC-IP table entry notified by a fourth network device, and the second network device comprises:

a processor;

a transceiver;

a machine storage medium having stored therein machine executable instructions which, when being executed by the processor, cause the processor to perform the method of any one of claims 10-15.

20. A machine readable storage medium having stored therein machine executable instructions that, when invoked and executed by a processor, cause the processor to perform the method of any one of claims 1-9 or 10-15.