Claims

1. An IFIT information configuration method, wherein the method is applied to a tail node and comprises:

receiving a first BGP update packet from a head node, wherein the first BGP update packet comprises IFIT configuration information;

receiving a first service packet from the head node through a first path, wherein the first service packet comprises a first IFIT option, and the first IFIT option comprises first indication information;

if a value of the first indication information is a first value, generating a service flow identification rule based on the configuration information, wherein the service flow identification rule is to identify a service flow requiring IFIT, and the service flow is transmitted through a second path, the second path is a forwarding path from the tail node to the head node, and the first path and the second path pass through a same intermediate node.

2. The method according to claim 1, wherein the configuration information comprises a tunnel-level enabling flag;

wherein generating a service flow identification rule based on the configuration information comprises:

if a value of the tunnel-level enabling flag is a first value, generating a first-type service flow identification rule that comprises a segment list identifier, wherein a path indicated by the segment list identifier is the second path, and the second path constitutes a transmission tunnel.

3. The method according to claim 2, wherein the first service packet comprises an original packet, the original packet comprises multiple first flow characteristics; the configuration information further comprises enabling information for multiple second flow characteristics;

wherein generating a service flow identification rule based on the configuration information comprises:

if a value of the tunnel-level enabling flag is a second value, obtaining a value of each second flow characteristic from the multiple first flow characteristics based on each enabled second flow characteristic indicated by the enabling information;

generating a second-type service flow identification rule based on values of the second flow characteristics.

4. The method according to any one of claims 1 to 3, wherein the first BGP update packet comprises an SR Policy SAFI NLRI field, the SR Policy SAFI NLRI field comprises Tunnel Encaps Attribute comprising IFIT Attributes TLV;

the IFIT Attributes TLV comprise at least one sub-TLV that is to carry the configuration information.

5. The method according to claim 4, wherein the at least one sub-TLV comprises a first sub-TLV, a value field of the first sub-TLV comprises a service flow identifier, a device node identifier, an extension flow monitor type identifier, enabling information of the multiple second flow characteristics, and a tunnel-level enabling flag; the multiple second flow characteristics comprise a destination IP address, a source IP address, a DSCP, a protocol name, a destination port, and a source port; the enabling information of the multiple second flow characteristics comprises a destination IP address mask, a source IP address mask, a D-Flag, and an L4-Flag;

the extension flow monitor type identifier comprises an F-Flag, and the F-Flag is to indicate whether to identify the enabling information of the multiple second flow characteristics;

the destination IP address mask is to indicate whether each bit comprised in the destination IP address is enabled;

the source IP address mask is to indicate whether each bit comprised in the source IP address is enabled;

the D-Flag is to indicate whether the DSCP is enabled;

the L4-Flag comprises 3 bits, a first bit is to indicate whether the protocol name is enabled, a second bit is to indicate whether the destination port is enabled, and a third bit is to indicate whether the source port is enabled.

6. The method according to claim 5, wherein the at least one sub-TLV further comprises a second sub-TLV, and a value field of the second sub-TLV comprises a first flag, a second flag, a third flag and encapsulation information;

the first flag is to indicate whether the head node supports alternating coloring IFIT, the second flag is to indicate whether the head node supports enhanced alternating coloring IFIT, and the third flag is to indicate whether the head node supports dynamically establishing the service flow identification rule;

the encapsulation information comprises an H-Flag, a D-Flag, and an S-Flag, wherein the H-Flag is to indicate whether the head node supports encapsulating an IFIT option in a hop-by-hop header, the D-Flag is to indicate whether the head node supports encapsulating an IFIT option in a destination header, and the S-Flag is to indicate whether the head node supports encapsulating an IFIT option in an SRH.

7. The method according to claim 1, wherein after generating a service flow identification rule based on the configuration information, the method further comprises:

storing the service flow identification rule in a forwarding plane;

when receiving a second service packet that complies with the service flow identification rule, encapsulating the second service packet with a second IFIT option to obtain a third service packet;

transmitting the third service packet to the head node through the second path.

8. The method according to claim 3, wherein after generating a service flow identification rule based on the configuration information, the method further comprises:

if a second BGP update packet is received from the head node, and the second BGP update packet does not comprise the configuration information, deleting the service flow identification rule; or,

if no packet comprising the multiple first flow characteristics is received for a preset duration, deleting the service flow identification rule.

9. An IFIT information configuration method, wherein the method is applied

to a head node and comprises:

sending a first BGP update packet to a tail node, wherein the first BGP update packet comprises IFIT configuration information;

receiving a first service packet;

sending a second service packet to the tail node through a first path, wherein the second service packet comprises a first IFIT option, the first IFIT option comprises first indication information, the first indication information is to indicate whether the tail node generates a service flow identification rule based on the configuration information, the service flow identification rule is to identify a service flow requiring IFIT, the service flow is transmitted through a second path, the second path is a forwarding path from the tail node to the head node, and the first path and the second path pass through a same intermediate node.

10. The method according to claim 9, wherein the first BGP update packet comprises an SR Policy SAFI NLRI field, the SR Policy SAFI NLRI field comprises Tunnel Encaps Attribute comprising IFIT Attributes TLV;

the IFIT Attributes TLV comprise at least one sub-TLV that is to carry the configuration information,

preferably, wherein the at least one sub-TLV comprises a first sub-TLV, a value field of the first sub-TLV comprises a service flow identifier, a device node identifier, an extension flow monitor type identifier, enabling information of the multiple second flow characteristics, and a tunnel-level enabling flag; the multiple second flow characteristics comprise a destination IP address, a source IP address, a DSCP, a protocol name, a destination port, and a source port; the enabling information of the multiple second flow characteristics comprises a destination IP address mask, a source IP address mask, a D-Flag, and an L4-Flag;

the extension flow monitor type flag comprises an F-Flag, and the F-Flag is to indicate whether to identify the enabling information of the multiple second flow characteristics;

the destination IP address Mask is to indicate whether each bit comprised in the destination IP address is enabled;

the source IP address Mask is to indicate whether each bit comprised in the source IP address is enabled;

the D-Flag is to indicate whether the DSCP is enabled;

the L4-Flag comprises 3 bits, a first bit is to indicate whether the protocol name is enabled, a second bit is to indicate whether the destination port is enabled, and a third bit is to indicate whether the source port is enabled,

more preferably, wherein the at least one sub-TLV further comprises a second sub-TLV, and a value field of the second sub-TLV comprises a first flag, a second flag, a third flag and encapsulation information;

the first flag is to indicate whether the head node supports alternating coloring IFIT, the second flag is to indicate whether the head node supports enhanced alternating coloring IFIT, and the third flag is to indicate whether the head node supports dynamically establishing the service flow identification rule;

the encapsulation information comprises an H-Flag, a D-Flag, and an S-Flag, wherein the H-Flag is to indicate whether the head node supports encapsulating an IFIT option in a hop-by-hop header, the D-Flag is to indicate whether the head node supports encapsulating an IFIT option in a destination header, and the S-Flag is to indicate whether the head node supports encapsulating an IFIT option in an SRH.

11. The method according to any one of claims 9 to 10, wherein after sending a second service packet to the tail node through a first path, the method further comprises:

sending a second BGP update packet to the tail node, wherein the second BGP update packet does not comprise the configuration information and is to instruct the tail node to delete the service flow identification rule.

12. A network device, wherein the network device is applied to a tail node and comprises:

a processor;

a transceiver;

a machine-readable storage medium storing machine-executable instructions

that can be executed by the processor; when executed, the machine-executable instructions cause the processor to: implement the method according to any one of claims 1 to 8.

13. A network device, wherein the network device is applied to a head node and comprises:

a processor;

a transceiver;

a machine-readable storage medium storing machine-executable instructions that can be executed by the processor; when executed, the machine-executable instructions cause the processor to: implement the method according to any one of claims 9 to 11.

14. A machine-readable storage medium, which stores machine-executable instructions thereon that, when called and executed by a processor, cause the processor to: implement the method according to any one of claims 1 to 11.

15. A computer program product, which causes a processor to implement the method according to any one of claims 1 to 11.