CLAIMS

1. A secure small form-factor pluggable transceiver (SFP) comprising a separation module operatively connectible to a network device, the separation module being configured to control data communication in the communication network, the separation module being assigned with a network-id associating the separation module with a given network environment;

the separation module being further configured to: tag, based on the network-id, a payload of a data packet received by the network device to be forwarded in a first direction, in order to associate the data packet with the given network environment; and

determine whether a payload of a data packet received by the network device to be forwarded in a second direction, is tagged with a tag compatible with the assigned network-id, and if it is, remove the tag from the payload of the data packet and allow transmission of the data packet.

2. The SFP according to claim 1, wherein the separation module is an internal separation module, wherein the first direction is an uplink direction towards the switching fabric of the network device and the second direction is a downlink direction away from the network device.

3. The SFP according to claim 1, wherein the separation module is an external separation module, wherein the first direction is a downlink direction away from the switching fabric of the network device and the second direction is an uplink direction towards the network device.

4. The SFP of claim 1, wherein the separation module comprises a direction determination module configured to adapt the separation module to match one of a first directionality or a second directionality, wherein in the first directionality the first direction is an uplink direction towards the network device and the second direction is a downlink direction away from the network device, and in the second directionality the first direction is a downlink direction away from the network device and the second direction is an uplink direction towards the network device.

5. The SFP according to claim 1, wherein the separation module is configured as a one time programming device.

6. The SFP according to claim 1, wherein the separation module is associated with a plurality of network-ids, each network-id assigned to a respective network environment; the separation module is further configured to determine whether a tag, associated with a payload of a data packet received by the network device from the second direction, is compatible with any one of the plurality of the network network-ids, and if it is, remove the tag from the payload of the data packet and allow transmission of the data packet.

7. The SFP according to claim 6, wherein the separation module comprises a data repository for storing the plurality of network-ids.

8. The SFP according to claim 1, wherein the separation module further comprises:

a data-repository for storing the network-id and a processor associated with a tagging module configured to perform the tagging; and

a validation module configured to determine whether the tag is compatible with the separation module.

9. A network device configured to control communication of data between nodes associated with one or more network environments; the network device comprising:

at least a first separation module and a second separation module, the first separation module being operatively connected to a first node connected to the network device;

the first separation module and the second separation module being each configured to operate as part of a a physical layer of the network device and being operatively connected to a respective switching fabric;

the first separation module is configured to tag a payload of a data packet received from the first node, based on a network-id assigned to the first separation module, the tag being indicative of a respective network environment of the first node; and transmit the data packet towards the second separation module.

10. The network device according to claim 9, wherein the second separation module is operatively connected to a second node connected to the network device;

the second separation module is configured to:

receive the data packet;

determine whether the payload of the data packet is tagged with a tag which is compatible with the second separation module; and

if it is, remove the tag from the payload of the data packet and allow transmission of the data packet to the second node.

11. The network device according to claim 9, wherein the second separation module is an external separation module associated with an external communication network connecting the network device to a second network device;

the external separation module is configured to:

tag the payload of the data packet received from the first separation module, with a second tag, the second tag being indicative of a respective network environment of the network device; and transmit the data packet towards the second network device.

12. The network device according to claim 11, wherein the second external separation module is configured to:

receive a data packet sent from a second node connected to the second network device; the data packet comprising a first tag and a second tag;

determine whether the second tag, associated with the data packet, is compatible with the external separation module;

if it is, remove the tag from the payload of the data packet;

transmit the data packet to the separation module; the separation module is configured to:

determine whether the first tag, associated with the data packet, is compatible with the separation module;

if it is, remove the tag from the data packet; and

transmit the data packet to a node connected to the network device.

13. The SFP according to claim 1, wherein the separation module is incorporated in a security manager;

the security manager operatively connected to a network device and to an external network, and being operable to control transmission of data between the network device and the external network; the security manager comprises or otherwise associated with a data repository configured for storing network-ids;

the separation module is configured to:

receive a data packet, sent via an external separation module in the network device; the data packet comprising a first tag and a second tag;

determine whether the second tag, associated with the data packet, is compatible with any one of network-ids stored in the data repository;

if it is, remove the tag from the data packet; and

determine whether the first tag, associated with the data packet, is compatible with any one of network-ids stored in the data repository;

if it is, remove the tag from the data packet; and

allow the transmission of the data packet to the external network.

14. A method of controlling transmission of data in a communication network, the method comprising:

tagging, at a secure small form-factor pluggable transceiver payload of a data packet received by a network device to be forwarded in a first direction in the communication network; the tagging is performed by a separation module which is connected between a

physical layer and a switching fabric of the network device and assigned based on a network-id to the network device; the network-id is indicative that the data packet is associated with a given network environment; and

determining, at a secure small form-factor pluggable transceiver, whether a payload of a data packet, received by the network device to be forwarded in a second direction, is tagged with a tag compatible with a network-id assigned to a target device, and if it is, removing the tag from the payload of the data packet and allowing transmission of the data packet to the target device.

15. The method according to claim 14, wherein the first direction is an uplink direction towards the switching fabric of the network device and the second direction is a downlink direction away from the switching fabric of the network device.

16. The method according to claim 14, wherein the first direction is a downlink direction away from the switching fabric of the network device and the second direction is an uplink direction towards the switching fabric of the network device.

17. The method according to claim 14, wherein the network device is connected to a first node and a second node, the method comprising:

performing the tagging on a payload of a data packet received from a first node connected to the network device; and

performing the determining on the data packet being transmitted to a second node connected to the network device, thereby controlling transmission of data between the first node and the second node.

18. The SFP according to claim 1, wherein the separation module is configured between a physical layer and a respective switching fabric in the network device such uplinked data and down-linked data passes through the separation module.

19. The SPF according to claim 1, wherein the tagging of the payload by the separation module, comprises encrypting the payload; and

wherein determining whether the payload is tagged with a tag compatible with the assigned network-id, comprises decrypting the payload.