(54) **METHOD FOR TIME DIVISION MULTIPLEX SERVICE PROTECTION**

(75) Inventors: **Ruichun Dai**, Shenzhen (CN);
Dezhi Zhang, Shenzhen (CN)

(73) Assignee: **ZTE CORPORATION**, Shenzhen,
Guangdong (CN)

Publication Classification

(57) **ABSTRACT**

The present application provides a method for time division multiplex service protection. The method includes: on an OLT in a passive optical network, a working uplink port and a protection uplink port are set for a time division multiplex service and a protection group is created for the working uplink port and the protection uplink port; when a service flow protection for the time division multiplex service is triggered, the time division multiplex service flow is switched from the working uplink port to the protection uplink port, therefore realizing the protection for the time division multiplex service flow. The present application provides an uplink channel protection mechanism for important services in an access system, such as the time division multiplex service, which needs no protection switching protocol, and makes the service recovery time stand within 50 ms, thereby realizing fast and nondestructive recovery of the time division multiplex service.

Downlink port   Working uplink port

CPE   OLT   Protection uplink port

Fig. 1

Downlink port   Working uplink port

OLT

CPE

Protection uplink port

Fig. 2

Start

S201
A protection group is created on the uplink port side of the OLT, and corresponding working and protection uplink ports are determined

S202
For the TDM service required to be protected, corresponding VLAN and Access Control List (ACL) are configured for the above determined working/ protection uplink port

S203
When the OLT detects that the TDM service in the working channel is failed, the OLT configures redirection for the TDM service flow by resetting the ACL rule and cooperating with the pre-configured VLAN ID data corresponding to the protection channel, thereby switching the invalid TDM service flow to the protection port for receiving and transmitting
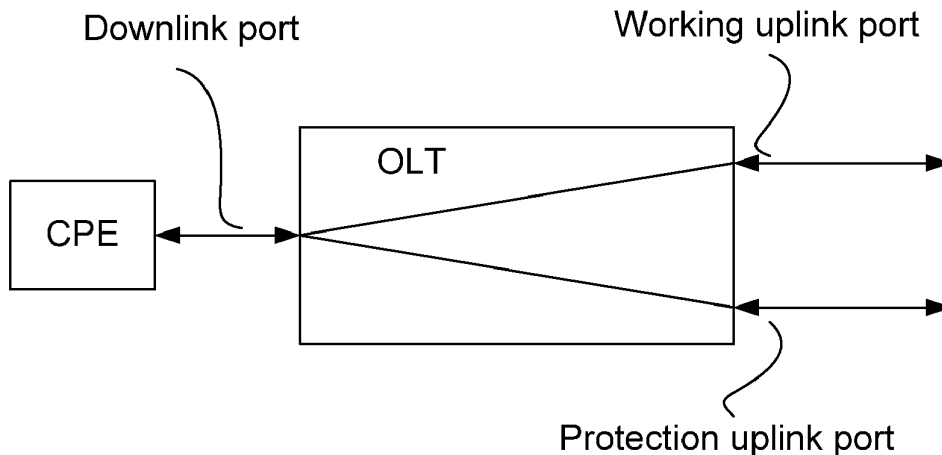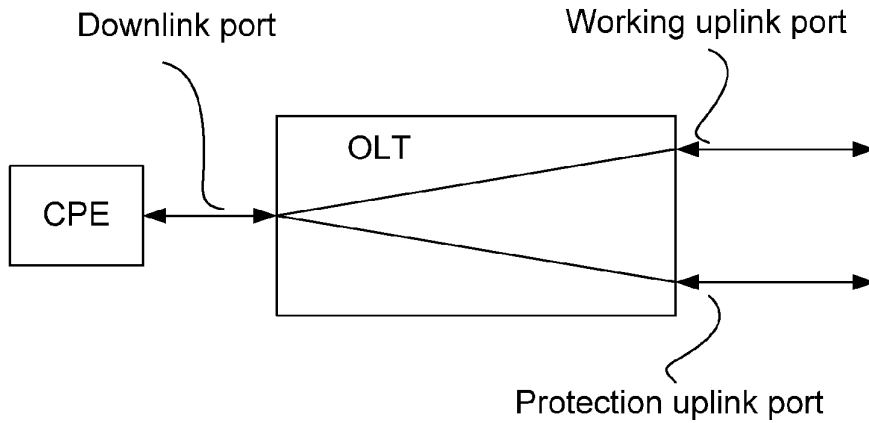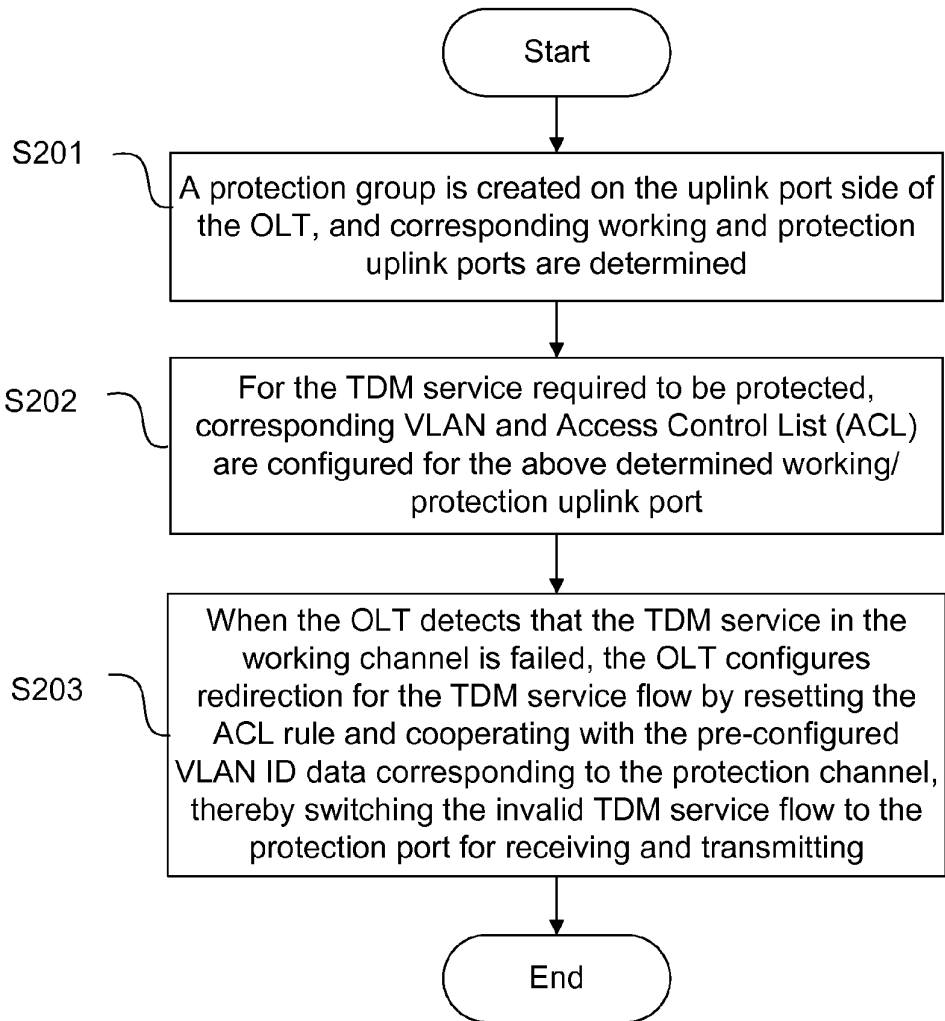
End

METHOD FOR TIME DIVISION MULTIPLEX SERVICE PROTECTION

TECHNICAL FIELD

[0001] The present application relates to the Passive Optical Network (PON) technology, in particular to a method for time division multiplex service protection in a passive optical network access system.

BACKGROUND

[0002] In the face of access demand of future composite combined services, the passive optical network technology becomes a predominant technology for developing Fiber To The Home (FTTx) due to its natural advantages of high bandwidth and full service access capacity. Wherein, a PON system needs to provide electric interfaces such as E1/T1, even SDH/SONET optical interfaces to develop relative services, in order to meet the demands from business customers on Time division Multiplex (TDM) services (such as an E1/T1 private line), particularly, when it needs to join with a traditional Synchronous Digital Hierarchy (SDH)/Synchronous Optical Network (SONET) based is multi-service transmission platform network.

[0003] Generally, a PON system employs Circuit Emulation Service over Packet (CESoP) to provide access of TDM services. In addition to high-level service quality requirements of TDM services, such as low delay and no error code, nondestructive protection for services is also an important requirement. The above CESoP includes E1/T1, SDH/SONET optical interfaces, and etc. At present, a common method of realizing TDM service protection in a PON system is that the protection for CESoP service flows is realized through an existing PON physic port, or realized through port mirroring by utilizing the exchange function of internal layer 2 (L2). However, protection switching time cannot be guaranteed within 50 ms, TDM channel-level protection cannot be realized, and the practicality is poor, due to the existing of the problems, such as, an Optical Network Unit (ONU) may become online again and MAC address learning are involved.

SUMMARY

[0004] The present application provides a method for time division multiplex service protection, to solve the technical problem that there is no channel-level protection switching to recover all services in the channel fast in the prior art, in the event that the quality degradation of services or an interruption occurs on a TDM service working channel.

[0005] The method includes: setting a working uplink port and a protection uplink port for a time division multiplex service on an Optical Line Terminal (OLT) in a passive optical network, and creating a protection group for the working uplink port and the protection uplink port; when triggering service flow protection for the Time division Multiplex (TDM) service, switching the TDM service flow from the working uplink port to the protection uplink port, therefore realizing the protection for the TDM service flow.

[0006] Wherein, the protection group may be a 1:1 protection group, or a 1+1 protection group, or a N:1 protection group.

[0007] Wherein, the creating a protection group for the working uplink port and the protection uplink port further may include: configuring corresponding VLAN IDs for the working uplink port and the protection uplink port of the

protection group, and setting a corresponding relationship between the TDM service flow and the working uplink port as well as a corresponding relationship between the TDM service flow and the protection uplink port.

[0008] Wherein, after creating a protection group for the working uplink port and the protection uplink port, the method may further include: configuring Access Control Lists (ACLS) for the working uplink port and the protection uplink port.

[0009] Wherein, when the protection for the TDM service flow is triggered, the switching the TDM service flow from the working uplink port to the protection uplink port may specifically include:

[0010] after the OLT detects that a working channel is interrupted or the TDM service in the working channel is failed, the OLT sets redirection of the TDM service flow by resetting an ACL rule and cooperating with the pre-configured VLAN ID corresponding to the protection uplink port, thereby the failed TDM service flow is switched to the protection port for receiving and transmitting.

[0011] Preferably, before the protection for the TDM service flow is triggered, the method may further include:

[0012] duplicating an identical duplicated TDM service flow for original TDM service flow required to be protected; configuring a same VLAN ID for both the original TDM service flow and the duplicated TDM service flow; setting an uplink port of the original TDM service flow as a working uplink port, and setting an uplink port of the duplicated TDM service flow as a protection uplink port; setting an ACL rule of the working uplink port as allowing the TDM service flow with the specific VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the TDM service flow with the specific VLAN ID;

[0013] and after the protection of the TDM service flow is triggered, the method may further is include:

[0014] exchanging ACL rules of the working uplink port and the protection uplink port, and switching the TDM service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

[0015] Wherein, before the protection of the TDM service flow is triggered, the method may further include:

[0016] configuring a specific VLAN ID for a TDM service flow required to be protected; setting an uplink port of the TDM service flow as a working uplink port; setting an ACL rule of the working uplink port as allowing the TDM with the specific VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the TDM service flow with the specific VLAN ID;

[0017] and after the protection of the TDM service flow is triggered, the method may further include:

[0018] resetting the uplink port of the TDM service flow as the protection uplink port, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the TDM service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

[0019] The present application provides an uplink channel protection mechanism for important service flows in an access system, such as TDM services, which does not need protection switching protocols, and makes the service recovery time stand within 50 ms, thereby helping the operators to realize fast and nondestructive recovery of TDM services,

making the operators have capabilities of providing higher quality of service for important services, and increasing the customer satisfaction.

BRIEF DESCRIPTION OF THE DRAWINGS

[0020] FIG. **1** illustrates a diagram of the working principle of the processing of recovery of the TDM service; and

[0021] FIG. **2** illustrates a flow chart of a method for TDM service protection according to an embodiment of the present application.

DETAILED DESCRIPTION

[0022] The specific embodiment of the present application will be described in details below in conjunction with drawings.

[0023] As shown in FIG. **1**, a Client Premise Equipment (CPE) is connected with an OLT through a downlink port, and the OLT is provided with a working uplink port and a protection uplink port. The core idea of the present application is that, on an uplink port side of an OLT in an access network system, creating 1+1 or 1:1 backup of a TDM service channel by setting redirection for service flow and cooperating with Access Control List (ACL) function or 1:1 Virtual Local Area Network (VLAN), that is, protecting a working uplink port in real time by a protection uplink port, carrying out real-time switching according to the situation of the channel, and thus realizing fast service recovery.

[0024] With reference to FIG. **2** and in conjunction with FIG. **1**, a method for TDM service protection according to an embodiment of the present application comprises:

[0025] S201: A protection group is created on an uplink port side of an OLT, and corresponding working uplink port and protection uplink port are determined;

[0026] S202: For the TDM service required to be protected, a corresponding VLAN ID is configured for the above determined working/protection uplink port, a corresponding relationship between the service flow and the working uplink port/protection uplink port is set, and an ACL is configured;

[0027] herein, 1:1 VLAN may be created for a protection uplink port channel to avoid time taken to carry out MAC address learning again after the switching to a protection channel. Conversely, the time will extend to tens of milliseconds if it is needed to carry out MAC address learning again.

[0028] S203: when the OLT detects that the TDM service in a working channel is failed due to interruption of the working channel, a protection control module of the OLT sets redirection for the TDM service flow by resetting an ACL rule and cooperating with is pre-configured VLAN ID data corresponding to the protection channel, to switch the failed TDM service flow to the protection port for receiving and transmitting, thereby realizing fast and nondestructive recovery of service.

[0029] Wherein, an existing technical means can be used for the OLT to check whether the TDM service in the working channel is failed.

[0030] Embodiments of realization of different backup protection of a TDM service channel will be described in details below.

Embodiment 1

Realization of 1+1 Backup Protection of the TDM Service Channel

[0031] During service configuration, Circuit Emulation Service (CES) pseudo wire service configuration is carried out on a CPE (may be an ONU) side, and each TDM service is distinguished with different C-VLAN IDs by means of labeling, for example, C-VLAN ID=1, in this way, the VLAN ID of this service flow is C-VLAN ID=1.

[0032] The CES pseudo wire service flow is provided with an outer label on an Optical Line Terminal (OLT) side, and the numeric value of an S-VLAN ID is used for identifying a TDM service, for example, if the S-VLAN ID is set as 128, it means this service is a TDM service flow. In this way, the VLAN ID of this service flow is S-VLAN ID=128, and C-VLAN ID=1.

[0033] The CES pseudo wire service flow is duplicated on a layer 2 exchange unit of the OLT, a same S-VLAN ID as the original service flow numeric value is also configured for the duplicated service flow. In this way, the duplicated service flow also has the same VLAN service label: S-VLAN ID=128, and C-VLAN ID=1.

[0034] Flow direction of service flows in the OLT is configured as follows: the original service flow is configured to flow to an uplink network through the working uplink port of the OLT; and the duplicated service flow is configured to flow to the uplink network through the protection uplink port of the OLT.

[0035] The ACL rule of the uplink ports of the OLT is configured as follows: the working uplink port is set to allow the service flow {S-VLAN ID=128, and C-VLAN ID=1} to pass, while the protection uplink port is set to abandon the above service flow {S-VLAN ID=128, and C-VLAN ID=1}.

[0036] When protection switching is triggered because it is detected by existing technologies that some problems occur in the working channel, the protection control module on the OLT side resets the ACL rule: the working port abandons the service flow {S-VLAN ID=128, and C-VLAN ID=1}, while the protection port allows the service flow {S-VLAN ID=128, and C-VLAN ID=1} to pass, and in this way, the original service flow can be cut off, so as to make the duplicated service flow to the uplink network through the protection uplink port, thereby realizing the purpose of fast and nondestructive protection for service.

Embodiment 2

Realization of 1:1 Backup Protection of the TDM Service Channel

[0037] During service configuration, CES pseudo wire service configuration is carried out on a CPE (may be an ONU) side, each TDM service is distinguished with different C-VLAN IDs by means of labeling, for example, C-VLAN ID=1, and in this way, the VLAN ID of this service flow is C-VLAN ID=1.

[0038] The CES pseudo wire service flow is provided with an outer label on an Optical Line Terminal (OLT) side, and the numeric value of an S-VLAN ID is used for identifying a TDM service, for example, if the S-VLAN ID is set as 128, it means this service is a TDM service flow, in this way, the VLAN ID of this service flow is S-VLAN ID=128, and C-VLAN ID=1.

[0039] This embodiment differs from embodiment 1 in that the duplication of a service flow is not carried out during protection.

[0040] Flow direction of service flows in the OLT is configured as follows: original service flow is configured to flow to an uplink network through the working uplink port of the OLT.

[0041] The ACL rule of the uplink ports of the OLT is configured as follows: the working uplink port is set to allow the service flow {S-VLAN ID=128, and C-VLAN ID=1} to pass, while the protection uplink port is set to abandon the service flow {S-VLAN ID=128, and C-VLAN ID=1}.

[0042] When protection switching is triggered because it is detected by existing technologies that some problems occur in the working channel, the OLT side carries out two steps of automatic setting: 1) the OLT deletes configuration data of the Step 505, and generates data to configure original service flow to flow to an uplink network through the protection uplink port of the OLT; 2) the protection control module of the OLT reconfigures the ACL rule: the working port abandons the service flow {S-VLAN ID=128, and C-VLAN ID=1}, while the protection port allows the service flow {S-VLAN ID=128, and C-VLAN ID=1} to pass, and in this way, the service flow, which originally flows to the uplink network through the working port, is redirected to the protection uplink port, thus realizing the purpose of fast and nondestructive protection of service.

Embodiment 3

Realization of N:1 Backup Protection of the TDM Service Channel

[0043] During service configuration, CES pseudo wire service configuration is carried out on CPE 1 to CPE N (may be ONUs) side, each CPE identifies its own TDM service through C-VLAN ID=x (it is a customer virtual local area network identity, representing a numeric value of a C-VLAN ID, with each CPE using a different numeric value), for example, CPE 1 identifies the C-VLAN ID of its own TDM service flow as 1, CPE 2 identifies the C-VLAN ID of its own TDM service flow as =2, and so on, N CPEs have N TDM service flows with their own C-VLAN IDs.

[0044] Each CES pseudo wire service flow is provided with same outer label on the OLT side, and a numeric value of an S-VLAN ID is used for identifying a TDM service, for example, if the S-VLAN ID is set as 128, it means this service is a TDM service flow. In this way, the VLAN IDs of multiple TDM service flows are: S-VLAN ID=128, and C-VLAN ID=x, wherein x is a C-VLAN ID provided by a CPE for its own service flow in the last step.

[0045] Flow direction of service flows in the OLT is configured as follows: all N original TDM service flows are configured to flow to an uplink network through the working uplink port of the OLT.

[0046] The ACL rule of the uplink ports of the OLT is configured as follows: the working uplink port is set to allow the service flow {S-VLAN ID=128, and C-VLAN ID=x} to pass, while the protection uplink port is set to abandon the service flow {S-VLAN ID=128, and C-VLAN ID=x}.

[0047] When protection switching is triggered because it is detected by existing technologies that some problems occur in the working channel, the OLT side carries out two steps of automatic setting: 1) the OLT deletes the configuration data generated in the last step, and regenerates data to configure original service flow to flow to the uplink network through the protection uplink port of the OLT; 2) the protection control module of the OLT reconfigures the ACL rule: the working port abandons the service flow {S-VLAN ID=128, and C-VLAN ID=x}, while the protection port allows the service flow {S-VLAN ID=128, and C-VLAN ID=x} to pass, and in this way, the service flow, which originally flows to the uplink

network through the working port, is redirected to the protection uplink port, thus realizing the purpose of fast and nondestructive protection of service.

[0048] The above are only preferred embodiments of the present application and are not used for limiting the present application. For those skilled in the art, the present application may have various alternations and changes. Any modifications, equivalent substitutes and improvements which are made within the spirit and principle of the present application should be contained within the protection scope of the present application.

1. A method for time division multiplex service protection, comprising: setting a working uplink port and a protection uplink port for a time division multiplex service on a terminal equipment in a passive optical network, and creating a protection group for the working uplink port and the protection uplink port; when triggering service flow protection for the time division multiplex service, switching the time division multiplex service flow from the working uplink port to the protection uplink port.

2. The method according to claim 1, wherein the protection group is a 1:1 protection group, or a 1+1 protection group, or a N:1 protection group.

3. The method according to claim 2, wherein the creating a protection group for the working uplink port and the protection uplink port further comprises:
configuring corresponding Virtual Local Area Network (VLAN) IDs for the working uplink port and the protection uplink port of the protection group, and setting a corresponding relationship between the time division multiplex service flow and the working uplink port, as well as a corresponding relationship between the time division multiplex service flow and the protection uplink port.

4. The method according to claim 3, further comprising: after creating a protection group for the working uplink port and the protection uplink port, configuring Access Control Lists (ACLS) for the working uplink port and the protection uplink port.

5. The method according to claim 4, wherein the switching the time division multiplex service flow from the working uplink port to the protection uplink port comprises:
after the terminal equipment detects that a working channel is interrupted or the time division multiplex service in the working channel is invalid, setting redirection of the time division multiplex service flow by the terminal equipment by resetting an ACL rule and according to the pre-configured VLAN ID corresponding to the protection uplink port, to switch the invalid time division multiplex service flow to the protection uplink port.

6. The method according to claim 1, further comprising: before triggering protection of the time division multiplex service flow, duplicating original time division multiplex service flow which is required to be protected; configuring a same VLAN ID for both the original time division multiplex service flow and the duplicated time division multiplex service flow; setting an uplink port of the original time division multiplex service flow as a working uplink port, and setting an uplink port of the duplicated time division multiplex service flow as a protection uplink port; setting an ACL rule of the working uplink port as allowing the time division multiplex service flow with the specific VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

7. The method according to claim 1, further comprising: before triggering protection of the time division multiplex service flow, configuring a VLAN ID for a time division multiplex service flow which is required to is be protected; setting an uplink port of the time division multiplex service flow as a working uplink port; setting an ACL rule of the working uplink port as allowing the time division multiplex service flow with the VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, resetting the uplink port of the time division multiplex service flow as the protection uplink port, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

8. The method according to claim 2, further comprising: before triggering protection of the time division multiplex service flow, duplicating original time division multiplex service flow which is required to be protected; configuring a same VLAN ID for both the original time division multiplex service flow and the duplicated time division multiplex service flow; setting an uplink port of the original time division multiplex service flow as a working uplink port, and setting an uplink port of the duplicated time division multiplex service flow as a protection uplink port; setting an ACL rule of the working uplink port as allowing the time division multiplex service flow with the specific VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

9. The method according to claim 3, further comprising: before triggering protection of the time division multiplex service flow, duplicating original time division multiplex service flow which is required to be protected; configuring a same VLAN ID for both the original time division multiplex service flow and the duplicated time division multiplex service flow; setting an uplink port of the original time division multiplex service flow as a working uplink port, and setting an uplink port of the duplicated time division multiplex service flow as a protection uplink port; setting an ACL rule of the is working uplink port as allowing the time division multiplex service flow with the specific VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, exchanging the ACL rules of the working uplink port

and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

10. The method according to claim 4, further comprising: before triggering protection of the time division multiplex service flow, duplicating original time division multiplex service flow which is required to be protected; configuring a same VLAN ID for both the original time division multiplex service flow and the duplicated time division multiplex service flow; setting an uplink port of the original time division multiplex service flow as a working uplink port, and setting an uplink port of the duplicated time division multiplex service flow as a protection uplink port; setting an ACL rule of the working uplink port as allowing the time division multiplex service flow with the specific VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

11. The method according to claim 5, further comprising: before triggering protection of the time division multiplex service flow, duplicating original time division multiplex service flow which is required to be protected; configuring a same VLAN ID for both the original time division multiplex service flow and the duplicated time division multiplex service flow; setting an uplink port of the original time division multiplex service flow as a working uplink port, and setting an uplink port of the duplicated time division multiplex service flow as a protection uplink port; setting an ACL rule of the working uplink port as allowing the time division multiplex service flow with the specific VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

12. The method according to claim 2, further comprising: before triggering protection of the time division multiplex service flow, configuring a VLAN ID for a time division multiplex service flow which is required to be protected; setting an uplink port of the time division multiplex service flow as a working uplink port; setting an ACL rule of the working uplink port as allowing the time division multiplex service flow with the VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, resetting the uplink port of the time division multiplex service flow as the protection uplink port, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the

5

protection uplink port and making it enter into an uplink network though the protection uplink port.

13. The method according to claim 3, further comprising: before triggering protection of the time division multiplex service flow, configuring a VLAN ID for a time division multiplex service flow which is required to be protected; setting an uplink port of the time division multiplex service flow as a working uplink port; setting an ACL rule of the working uplink port as allowing the time division multiplex service flow with the VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, resetting the uplink port of the time division multiplex service flow as the protection uplink port, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

14. The method according to claim 4, further comprising: before triggering protection of the time division multiplex service flow, configuring a VLAN ID for a time division multiplex service flow which is required to be protected; setting an uplink port of the time division multiplex service flow as a working uplink port; setting an ACL rule of the working uplink port as allowing the time division multiplex service flow with the VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, resetting the uplink port of the time division multiplex service flow as the protection uplink port, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

15. The method according to claim 5, further comprising: before triggering protection of the time division multiplex service flow, configuring a VLAN ID for a time division multiplex service flow which is required to be protected; setting an uplink port of the time division multiplex service flow as a working uplink port; setting an ACL rule of the working uplink port as allowing the time division multiplex service flow with the VLAN ID to pass, and setting an ACL rule of the protection uplink port as abandoning the time division multiplex service flow with the specific VLAN ID;

and the method further comprising: after triggering the protection of the time division multiplex service flow, resetting the uplink port of the time division multiplex service flow as the protection uplink port, exchanging the ACL rules of the working uplink port and the protection uplink port, and switching the time division multiplex service flow from the working uplink port to the protection uplink port and making it enter into an uplink network though the protection uplink port.

* * * * *