



Certification of Accuracy of Translation

Sun IP Project # 24-6052

Name: Xin Min Liu

Address: 12856 Whitebridge Dr. Fishers, IN 46037

Telephone: 405.823.6550

I, Xin Min Liu, hereby declare that I am a professional translator, with over 30 years of professional experience, and am knowledgeable and well acquainted with the Chinese language and the English language.

The document CN101645848A in the English language attached hereto is to the best of my ability, knowledge, and expertise, the correct English language translation of the original document written in the Chinese language.

I translated the original document into the English language. I declare that all statements made herein on my own knowledge are true and that all statements made on information and belief are believed to be true, and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 or Title 18 of the United States Code.

A handwritten signature in black ink, appearing to read "Xin Min Liu", is written over a horizontal line.

Xin Min Liu

Signed in Fishers, Indiana on this 17th of October 2024

[19] China National Intellectual Property Administration



[12] Instructions for Publication
of Invention Patent Application

[51] Int. Cl.

H04L 12/56 (2006.01)

H04L 12/26 (2006.01)

H04L 12/24 (2006.01)

[21] Application Number 200910170173.7

[43] Publication Date February 10, 2010

[11] Publication number CN 101645848 A

[22] Application Date September 04, 2009

[21] Application Number 200910170173.7

[71] Applicant HUAWEI TECHNOLOGIES
CO., LTD.

Address 518129, Huawei Base
Headquarters Office Building,
Bantian, Longgang District,
Shenzhen City, Guangdong
Province

[72] Inventors LI Zhenbin, HUANG
Yongnian, JIANG Hu

[74] Patent Agency BEIJING ZBSD PATENT &
TRADEMARK AGENT LTD.
Agent SHEN Jian

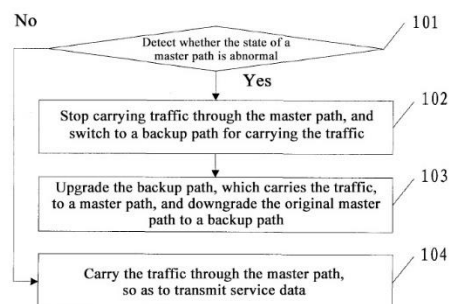
2 pages of Claims, 12 pages of Specification, 4
pages of Drawings

[54] Title

TRAFFIC PROTECTION METHOD AND
APPARATUS, AND SYSTEM

[57] Abstract

The present invention relates to the field of communications, and discloses a traffic protection method and apparatus, and a system which solve the problem in the prior art of poor traffic reliability caused by frequent traffic switching. The present invention comprises: a master path for carrying traffic and at least one backup path playing a protective role existing between terminals; detecting whether the state of the master path is abnormal, wherein if the state of the master path is abnormal, switching to the backup path for carrying traffic; and upgrading the backup path, which carries traffic, to a master path, and downgrading the original master path to a backup path. The embodiments of the present invention are mainly used in a process of data service transmission between terminals in a network having an MPLS function.



1. A traffic protection method, characterized in that a master path for carrying traffic and at least one backup path playing a protective role exist in a multi-protocol label switching (MPLS) network, and the method comprises:

detecting whether the state of the master path is abnormal;

if the state of the master path is abnormal, switching to the backup path for carrying traffic; and

upgrading the backup path, which carries traffic, to a master path, and downgrading the original master path to a backup path, characterized in that if the original master path is restored to normal, traffic is still locked on and carried through the backup path that is upgraded to the master path, without being switched back to the original master path.

2. The traffic protection method according to claim 1, further comprising: setting priorities for the master link and the at least one backup path.

3. The traffic protection method according to claim 2, characterized in that when the state of the master path is abnormal, the switching to the backup path for carrying traffic specifically comprises:

according to the priorities of the backup path, switching traffic to a normally working backup path, which has a high priority, for carrying traffic.

4. The traffic protection method according to claim 3, characterized in that upgrading the backup path, which carries traffic, to the master path, and downgrading the original master path to the backup path specifically comprise: swapping the priority of the original master path with the priority of the backup path carrying traffic, such that the backup path carrying traffic is upgraded to the master path, and the original master path is downgraded to the backup path.

5. A traffic protection apparatus used in a multi-protocol label switching (MPLS) network with a master path for carrying traffic and at least one backup path playing a protective role in the MPLS network therein, comprising:

a detection module, configured to detect whether the state of the master path is abnormal;

a switching module, configured to switch, when the detection module detects that the state of the master path is abnormal, to the backup path for carrying traffic; and

an adjustment module, configured to upgrade the backup path, which carries traffic, to a master path, and downgrade the original master path to a backup path, wherein if the original master path is restored to normal, traffic is still locked on and carried through the backup path that is upgraded to the master path, without being switched back to the original master path.

6. The traffic protection apparatus according to claim 5, characterized in that it further comprises:

a setting module, configured to set priorities for the master path and the at least one backup path.

7. The traffic protection apparatus according to claim 6, characterized in that the switching module is specifically configured to switch, when the detection module detects that the state of the master path is abnormal, according to the priorities of the backup path, traffic to a normal backup path, which has a high priority, to carry traffic.

8. The traffic protection apparatus according to claim 5, characterized in that the adjustment module is specifically configured to swap the priority of the original master path with the priority of the backup path after traffic is switched to and carried through the normal backup path having a high priority according to the priorities of the backup path when a state abnormality occurs in the master link.

9. A communication system comprising a terminal, characterized in that the system is used in a multi-protocol label switching (MPLS) network with a master path for carrying traffic and at least one backup path playing a protective role therein, and the terminal comprises:

a detection module, configured to detect whether the state of the master path is abnormal;

a switching module, configured to switch, when the detection module detects that the state of the master path is abnormal, to the backup path for carrying traffic; and

an adjustment module, configured to upgrade the backup path, which carries traffic, to a master path, and downgrade the original master path to a backup path, wherein if the original master path is restored to normal, traffic is still locked on and carried through the backup path that is upgraded to the master path, without being switched back to the original master path.

10. The communication system according to claim 9, characterized in that the terminal is

a client or a server.

TRAFFIC PROTECTION METHOD AND APPARATUS, AND SYSTEM

Technical Field

The present invention relates to the field of communications, and in particular, to a method and apparatus for protecting service traffic, and a system.

Background

In telecommunications networks, high reliability is always the most basic and critical performance requirement, especially for voice services, of which the time for end-to-end protection switching must be less than 200 ms to meet the requirement. To meet this standard, it is necessary to provide rich and reliable traffic engineering (TE) protection solutions. Multi-protocol label switching (MPLS) TE provides rich traffic protection solutions, including end-to-end backup path protection technology, backup tunnel protection technology, etc. In these protection mechanisms, users must specify a master path and multiple backup paths. When the master path fails, service traffic is switched to a backup path; and when the master path is restored, the service traffic is switched back to the master path.

In the process of implementing the foregoing traffic switching, the inventor found that there is at least the following problem in the prior art: when the master path fails, a backup path immediately replaces the master path to protect traffic. Once the master path is restored to a normal state, traffic is switched back to the master path. traffic needs to be switched twice for one link flapping. If a network is complex and not stable enough, frequent switching of traffic in the network will occur, which will cause an unnecessary burden on a system and affect the reliability of traffic.

Summary of the Invention

Embodiments of the present invention provide a traffic protection method and apparatus, and a communication system, which solve the problem of severe impact on traffic reliability caused by frequent traffic switching when a network is unstable.

To achieve the foregoing objective, the following technical solutions are used in the embodiments of the present invention:

A traffic protection method, wherein a master path for carrying traffic and at least one backup path playing a protective role exist in a multi-protocol label switching (MPLS) network, and the method comprises:

detecting whether the state of the master path is abnormal;

if the state of the master path is abnormal, switching to the backup path for carrying traffic; and

upgrading the backup path, which carries traffic, to a master path, and downgrading the original master path to a backup path, wherein if the original master path is restored to normal, traffic is still locked on and carried through the backup path that is upgraded to the master path, without being switched back to the original master path.

A traffic protection apparatus used in a multi-protocol label switching (MPLS) network with a master path for carrying traffic and at least one backup path playing a protective role in the MPLS network therein, comprising:

a detection module, configured to detect whether the state of the master path is abnormal;

a switching module, configured to switch, when the detection module detects that the state of the master path is abnormal, to the backup path for carrying traffic; and

an adjustment module, configured to upgrade the backup path, which carries traffic, to a master path, and downgrading the original master path to a backup path, wherein if the original master path is restored to normal, traffic is still locked on and carried through the backup path that is upgraded to the master path, without being switched back to the original master path.

A communication system comprising a terminal, wherein the system is used in a multi-protocol label switching (MPLS) network with a master path for carrying traffic and at least one backup path playing a protective role therein, and the comprises:

a detection module, configured to detect whether the state of the master path is abnormal;

a switching module, configured to switch, when the detection module detects that the state of the master path is abnormal, to the backup path for carrying traffic; and

an adjustment module, configured to upgrade the backup path, which carries traffic, to a master path, and downgrading the original master path to a backup path, wherein if the original master path is restored to normal, traffic is still locked on and carried through the backup path that is upgraded to the master path, without being switched back to the original

master path

In the technical solution of the present invention, there is a master path carrying traffic and a backup path playing a protective role between two terminals, wherein when an abnormality occurs in the master path, traffic is switched to and carried through the backup path, and the backup path carrying traffic is upgraded to a master path, and the original master path is downgraded to a backup path; and when the state of the original master path is restored to a normal state, a link carrying traffic no longer switches back to the master path, and instead, the backup path carrying traffic continues to carry traffic until an abnormality occurs in the state of the backup path, at which point switching of the link carrying traffic is performed, such that only one link switching is required for one link flapping to lock traffic; compared with the prior art in which two times of link switching are required for one link flapping, the frequency of traffic switching in a network is greatly reduced, and the reliability of traffic carrying is improved.

Brief Description of the Drawings

In order to describe technical solutions in the embodiments of the present invention or in the prior art more clearly, drawings required to be used in the description of the embodiments or the prior art are briefly introduced below. Obviously, the drawings in the following description show merely some embodiments of the present invention. For a person of ordinary skills in the art, other drawings can also be obtained based on these drawings without exerting creative efforts.

FIG. 1 is a flow chart of a traffic protection method in Embodiment 1 of the present invention;

FIG. 2 is a composition block diagram of a traffic protection apparatus in Embodiment 1 of the present invention;

FIG. 3 is a schematic diagram of switching of a link carrying traffic in a traffic protection method in Embodiment 2 of the present invention;

FIG. 4 is a flow chart of a traffic protection method in Embodiment 2 of the present invention;

FIG. 5 is a composition block diagram of a traffic protection apparatus in Embodiment 2 of the present invention;

FIG. 6 is a schematic diagram of switching of a tunnel carrying traffic in a traffic protection method in Embodiment 3 of the present invention; and

FIG. 7 is a flow chart of a traffic protection method in Embodiment 3 of the present invention.

Detailed Description of Embodiments

The technical solutions of the embodiments of the present invention are clearly and fully described as below in combination with the accompanying drawings in the embodiments of the present invention. Apparently, the embodiments to be described are merely a part rather than all of the embodiments of the present invention. All other embodiments obtained by a person of ordinary skills in the art based on the embodiments of the present invention without creative efforts shall fall within the protection scope of the present invention.

Embodiment 1

The embodiment of the present invention provides a traffic protection method used in a network having multi-protocol label switching (MPLS) with a master path for carrying traffic and at least one backup path playing a protective role therein. In an end-to-end backup path protection mechanism, the master path and the backup path are label switch paths (LSPs), and in a backup tunnel protection (tunnel protection group) mechanism, the master path and the backup path are tunnels; and certainly, the master path and the backup path may also be in other manners, and are not limited to LSPs and tunnels.

As shown in FIG. 1, the method comprises the following steps:

101. Detecting whether the state of the master path is abnormal, wherein if it is detected that the state of the master path is abnormal, step 102 is performed; and if it is detected that the state of the master path is not abnormal, step 104 is performed.

An abnormality in the state of the master path may be in, but not limited to, the following forms, including: link failure, data packet loss, transmission interruption, etc.; and there is no limitation for this in the embodiment of the present invention.

102. Stopping carrying traffic through the master path, switching to a backup path for carrying traffic, and the backup channel carrying traffic transmits service data.

103. After a link carrying traffic being switched from the master path to the backup path, upgrading the backup path carrying traffic to a master path, and downgrading the original

master path to a backup path, wherein if the original master path is restored to normal, traffic is still locked on and carried through the backup path that is upgraded to the master path, without being switched back to the original master path.

104. Carrying traffic through the master path, so as to transmit the service data.

The embodiment of the present invention provides a traffic protection apparatus is used in an MPLS network with a master path for carrying traffic and at least one backup path playing a protective role therein. As shown in FIG. 2, the apparatus comprises: a detection module 21, a switching module 22, and an adjustment module 23.

The detection module 21 is configured to detect whether the state of the master path is abnormal;

The switching module 22 is configured to switch, when the detection module 21 detects that the state of the master path is abnormal, to a backup path for carrying traffic; and

The adjustment module 23 is configured to upgrade the backup path, which carries traffic, to a master path, and downgrade the original master path to a backup path after the switching module 22 switches the link, which carries traffic, from the master path to the backup path.

If the detection module 21 does not detect any abnormality in the state of the master path, traffic is still carried through the master path to transmit the service data between terminals.

When the foregoing traffic protection method and apparatus are used in a network, it is necessary to install the corresponding apparatus in terminals using the foregoing method, and if the foregoing apparatus is installed in two terminals, which need to communicate with each other, in a certain network, a traffic protection system is formed.

In the embodiment of the present invention, when an abnormality occurs in the master path, traffic is switched to and carried through the backup path, the backup path carrying traffic is upgraded to the master path, and the original master path is downgraded to the backup path; and when the state of the original master path is restored to a normal state, a link carrying traffic no longer switches back to the master path, and instead, the backup path carrying traffic continues to carry traffic until an abnormality occurs in the state of the backup path, at which point switching of the link carrying traffic is performed, such that only one link switching is required for one link flapping to lock traffic; compared with the prior art in which

two times of link switching are required for one link flapping, the frequency of traffic switching in a network is greatly reduced, and the reliability of traffic carrying is improved.

Embodiment 2

The embodiment of the present invention provides a traffic protection method, which is specifically illustrated in the embodiment of the present invention by an instance that the link is an LSP, in combination with FIGs. 3 and 4, so as to explain end-to-end backup path protection, wherein, as shown in FIG. 4, the method comprises the following steps:

A master LSP for carrying traffic and at least one backup LSP playing a protective role existing between label switched routers (LSRs) of an ingress interface and an egress interface; and Setting priorities for the master LSP and the backup LSP, wherein when the state of the master LSP carrying traffic is abnormal, the backup LSP having a relatively high priority is preferably selected as an LSP carrying traffic. In the embodiment of the present invention, traffic protection method is specifically illustrated by an instance that the at least one backup LSP playing a protective role includes two backup LSPs.

301. A master LSP for carrying traffic and two backups LSP1, LSP2 playing a protective role exist between the LSRs of the ingress interface and the egress interface, wherein priorities are set for the master LSP, the backup LSP1, and the backup LSP2, respectively; and specifically, the master LSP is set to have the highest priority, which is set as master, and the priorities of the backup LSP1 and the backup LSP2 are set from high to low as backup 1 and backup 2.

302. Carry traffic through the master LSP between the LSRs of the ingress interface and the egress interface, so as to transmit service data.

303. The state of the master LSP is detected, wherein if it is detected that the state of the master LSP is abnormal, step 304 is performed, and if it is detected that the state of the master LSP is not abnormal, step 306 is performed. An abnormality in the state of the master LSP may be in, but not limited to, the following forms, including: link failure, data packet loss, transmission interruption, etc.; and there is no limitation for this in the embodiment of the present invention.

304. Stopping carrying traffic through the master LSP, and according to the priorities of the backup LSP1 and the backup LSP2, traffic being switched to and carried through a normal

backup path having a high priority.

In the embodiment of the present invention, the priority level of the backup LSP1 is higher than the priority level of the backup LSP2, such that the link carrying traffic is switched from the master LSP to the backup LSP1, and the backup LSP1 carrying traffic transmits the service data.

If an abnormality also occurs in the high-priority backup LSP1, the link carrying traffic is switched from the master LSP to the backup LSP2, that is, according to the priorities of the backup LSP1 and the backup LSP2, traffic is switched to and carried through the normal backup path having a high priority.

305. After traffic is switched to and carried through the normal backup path having the high priority, the priority of the backup LSP1 carrying traffic is swapped with the priority of the original master LSP, that is, the priority of the master LSP is downgraded to backup 1, and the priority of the backup LSP1 is upgraded to master; and if a tunnel carrying traffic is the backup tunnel LSP2, the priority of the original master LSP is downgraded to backup 2, and the priority of the backup LSP2 is upgraded to master.

In the present step, by changing the priorities, when the original master LSP is restored to normal, traffic is still locked on and carried through the backup LSP2 that is upgraded to the master path, without being switched back to the original master LSP.

306. Carry traffic through the master LSP carrying traffic, so as to transmit the service data.

The embodiment of the present invention further provides a traffic protection apparatus, wherein, as shown in FIG. 5, the apparatus comprises: a setting module 41, a detection module 42, a switching module 43, and an adjustment module 44.

The setting unit 41 is configured to set priorities for the master path and the backup paths;

The detection module 42 is configured to detect whether the state of the master path is abnormal;

The switching module 43 is configured to switch, when the detection module 42 detects that the state of the master path is abnormal, according to the priorities of the backup paths, traffic to a normal backup path, which has a high priority, to carry traffic;

The adjustment module 44 is configured to swap the priority of the backup path, which carries traffic, with the priority of the original master path after the switching module 43 switches the link, which carries traffic, from the master path to the normal backup path having a high priority.

If in the detection module of the embodiment of the present invention, there is a master path carrying traffic and at least one backup path playing a protective role between terminals, and priorities are set for the master path and the backup path, when an abnormality occurs in the master path, according to the priorities of the backup path, traffic is switched to and carried through the backup path having a relatively high priority, and the priority of the backup path carrying traffic is swapped with the priority of the original master path; and when the state of the original master path is restored to a normal state, the link carrying traffic no longer switches back to the original master path, and instead, the backup path having a relatively high priority continues to carry traffic, such that only one link switching is required for one link flapping to lock traffic; compared with the prior art in which two times of link switching are required for one link flapping, the frequency of traffic switching in a network is greatly reduced, system overhead is reduced, and the reliability of traffic carrying is improved.

Moreover, after traffic is switched from the master path to the backup path having a relatively high priority, the priority of the original master path is swapped with the priority of the foregoing backup path, and the backup path carries traffic until an abnormality occurs in the state of the backup path, at which point the selection of a backup path for carrying traffic is performed according to the priorities of the backup paths, such that when service traffic is transmitted between terminals, there is no strong priority distinction between paths through which the master path and the backup path pass, and traffic may be carried through links of various priorities for a long term.

Embodiment 3

The embodiment of the present invention provides a traffic protection method, which is specifically illustrated in the embodiment of the present invention by an instance that the link is a tunnel, in combination with FIGs. 6 and 7, so as to explain backup path protection in a tunnel protection group, as shown in FIG. 7, the method comprises the following steps:

A master tunnel for carrying traffic and at least one backup tunnel playing a protective role existing in the tunnel protection group; Setting priorities for the master tunnel and the backup tunnel, wherein when the state of the master tunnel carrying traffic is abnormal, the backup tunnel having a relatively high priority is preferably selected as a tunnel carrying traffic. In the embodiment of the present invention, traffic protection method is specifically illustrated by an instance that the at least one backup tunnel playing a protective role includes two backup paths, and traffic protection method is specifically illustrated by an instance that the backup tunnels include two tunnels.

501. A master tunnel P for carrying traffic and two backup tunnels P1, P2 playing a protective role exist in the tunnel protection group, wherein priorities are set for the master tunnel P, the backup tunnel P1, and the backup tunnel P2, respectively; and specifically, the master path LSP is set to have the highest priority, which is set as master, and the priorities of the two backup tunnels P1, P2 are set from high to low as backup 1 and backup 2.

502. Carry traffic through the master tunnel P in the tunnel protection group, so as to transmit service data.

503. The state of the master tunnel P is detected, wherein if it is detected that the state of the master tunnel P is abnormal, step 504 is performed; and if it is detected that the state of the master tunnel P is not abnormal, step 506 is performed. An abnormality in the state may be in, but not limited to, the following forms, including: link failure, data packet loss, transmission interruption, etc.; and there is no limitation for this in the embodiment of the present invention.

504. Carrying traffic through the master tunnel P is stopped, and according to the priorities of the backup tunnels, traffic is switched to the backup tunnel that has no abnormal state and has a high priority.

In the embodiment of the present invention, the priority level of the backup tunnel P1 is higher than the priority of the backup tunnel P2, wherein if the state of the backup tunnel P1 is not abnormal, traffic is switched from the master tunnel to the backup tunnel P1, and if the state of the backup tunnel P1 is abnormal, traffic is switched from the master tunnel to the backup tunnel P2, and the backup tunnel transmits the service data.

If an abnormality also occurs in the high-priority backup tunnel P1, the link carrying

traffic is switched from the master LSP to the backup tunnel P2, that is, according to the priorities of the backup P1 and the backup P2, traffic is switched to and carried through the normal backup path having a relatively high priority.

505. After traffic is switched to the backup tunnel that has no abnormal state and has a high priority, the priority of the backup tunnel carrying traffic is swapped with the priority of the original master tunnel, that is, if the tunnel carrying traffic is the backup tunnel P1, the priority of the original master tunnel is downgraded to backup 1, and the priority of the backup tunnel P1 is upgraded to master; and if the tunnel carrying traffic is the backup tunnel P2, the priority of the original master tunnel P is downgraded to backup 2, and the priority of the backup tunnel P2 is upgraded to master.

In the present step, by changing the priorities, when the original master tunnel P is restored to normal, traffic is still locked on and carried through the backup tunnel P1 or the backup tunnel P2 that is upgraded to the master path, without being switched back to the original master LSP.

506. The master tunnel carrying traffic continues to carry traffic, so as to transmit the service data between terminals.

The embodiment of the present invention further provides a traffic protection apparatus as shown in FIG. 5, which is specifically described in Embodiment 2, and thus is not further described herein.

When the foregoing traffic protection method and apparatus are used in a network, it is necessary to install the corresponding apparatus in terminals using the foregoing method, and if the foregoing apparatus is installed in two terminals, which need to communicate with each other, in a certain network, a traffic locking system is formed.

In the embodiment of the present invention, a master tunnel carrying traffic and at least one backup tunnel playing a protective role are established between two terminals, and priorities are set for the master path and the backup tunnel. wherein when an abnormality occurs in the master tunnel, according to the priorities of the backup tunnel, traffic is switched to and carried through the backup tunnel that has a normal state and a relatively high priority, and the priority of the backup tunnel carrying traffic is swapped with the priority of the original master tunnel; and when the state of the original master tunnel is restored to a normal

state, the tunnel carrying traffic no longer switches back to the original master tunnel, and instead, the backup tunnel having a relatively high priority continues to carry traffic, such that only one tunnel switching is required for one tunnel flapping to lock traffic; compared with the prior art in which two times of tunnel switching are required for one tunnel flapping, the frequency of traffic switching in a network is greatly reduced, system overhead is reduced, and the reliability of traffic carrying is improved.

Moreover, after traffic is switched from the master tunnel to the backup tunnel having a relatively high priority, the priority of the original master tunnel is swapped with the priority of the foregoing backup tunnel, and the backup tunnel carries traffic until an abnormality occurs in the state of the backup tunnel, at which point the selection of a backup tunnel for carrying traffic is performed according to the priorities of the backup tunnels, such that when service traffic is transmitted between terminals, there is no strong priority distinction between paths through which the master tunnel and the backup tunnel pass, and traffic may be carried through tunnels of various priorities for a long term.

In the present implementation of the invention, when link conditions are unstable, an abnormality occurs in the master path, an abnormality occurs in the state of the backup path having a relatively high priority to which a normal state has not been restored, traffic is switched to the backup path having a relatively low priority, such that the stability of data transmission is further ensured.

In the embodiment of the present invention, applications of the present invention are mainly illustrated by instances of a tunnel protection group and end-to-end backup path protection in MPLS TE, wherein during specific implementation, traffic locking in other traffic engineering may be established according to different circumstances and requirements, and there may be multiple backup paths.

Through the description of the foregoing implementation, a person skilled in the art may clearly understand that the present invention may be implemented by software in addition to necessary general hardware, and of course, by hardware only, however, in many circumstances, the former is a preferred implementation. Based on such an understanding, the technical solutions of the present invention essentially or, in other words, the part contributing to the prior art may be embodied in a form of software product, wherein the computer

software product is stored in a readable storage medium, such as a floppy disk, a hard disk, or an optical disc of a computer, and contains several instructions for enabling a computer device (which may be a personal computer, a server or a network device, etc.) to perform the methods described in the embodiments of the present invention.

The foregoing descriptions are merely specific implementations of the present invention, but are not intended to limit the protection scope of the present invention, and any variation or substitution readily conceivable to a person skilled in the art within the technical scope disclosed in the present invention shall fall within the protection scope of the present invention. Therefore, the protection scope of the present invention shall be subject to the protection scope of the claims.

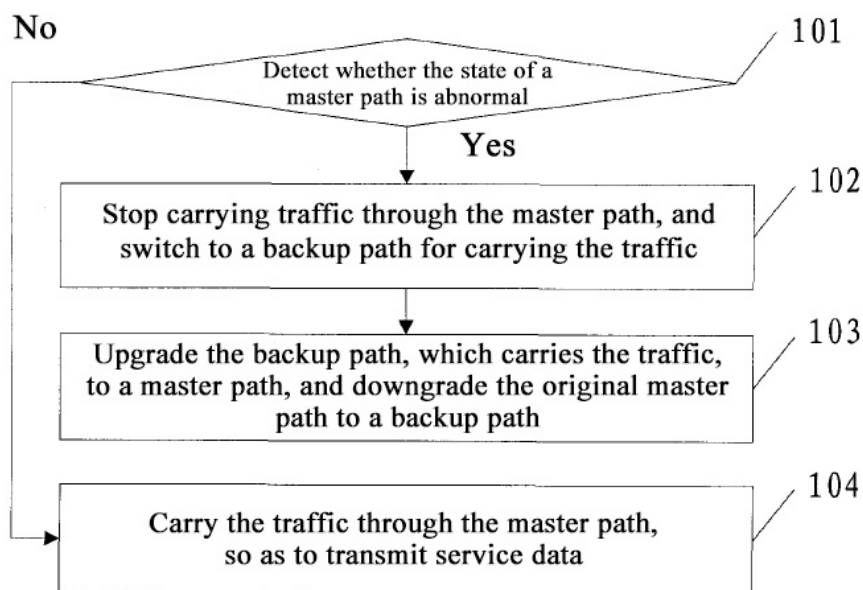


FIG. 1

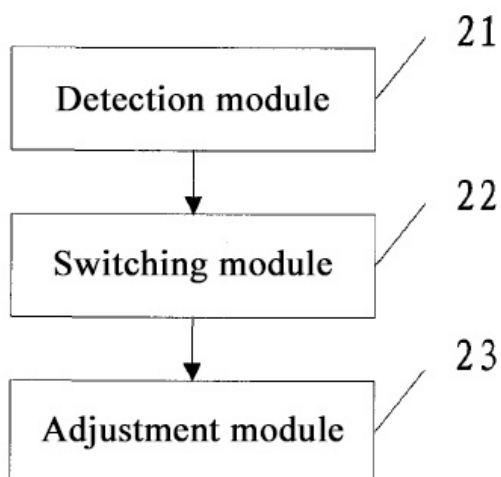


FIG. 2

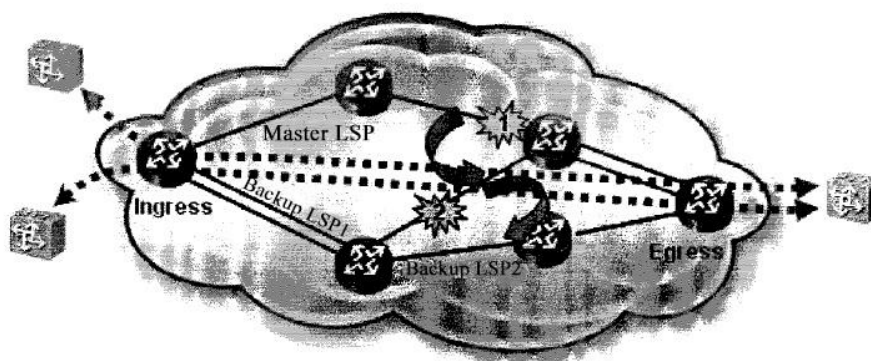


FIG. 3

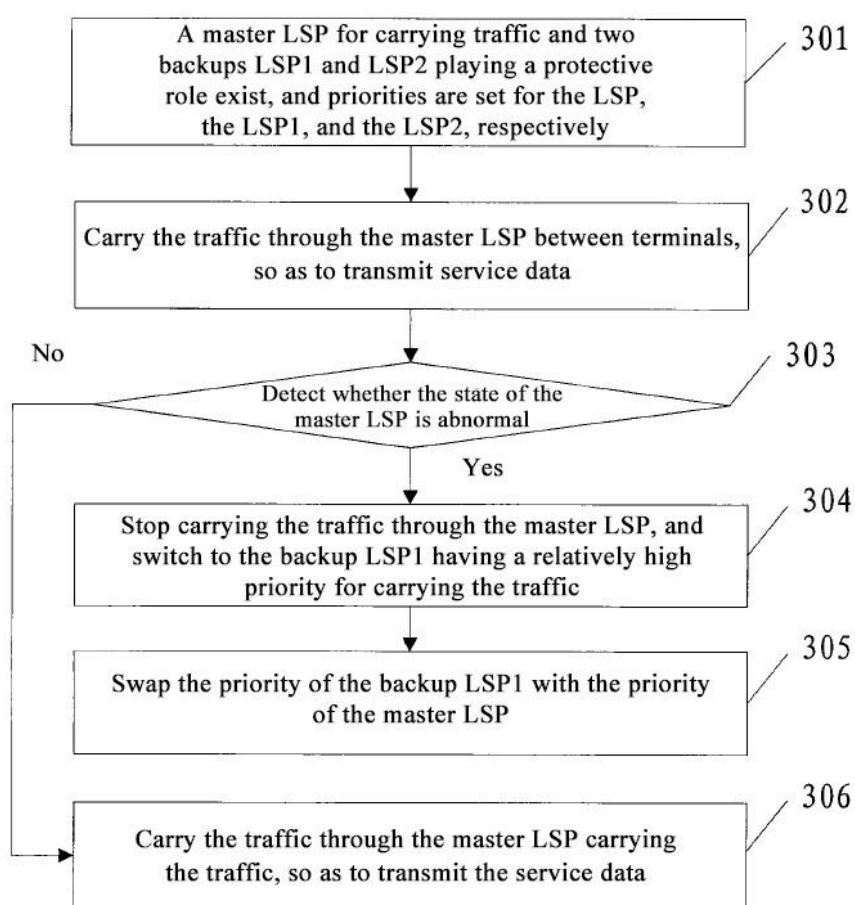


FIG. 4

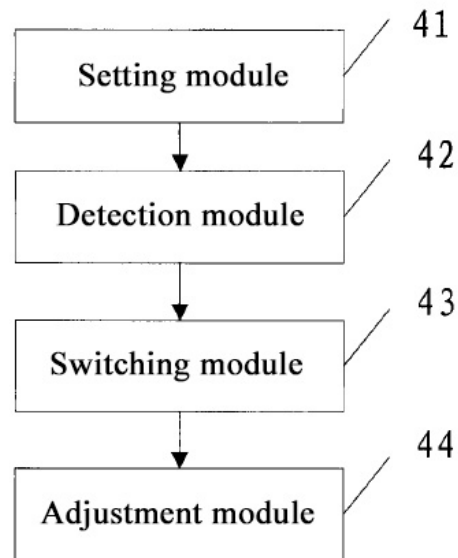


FIG. 5

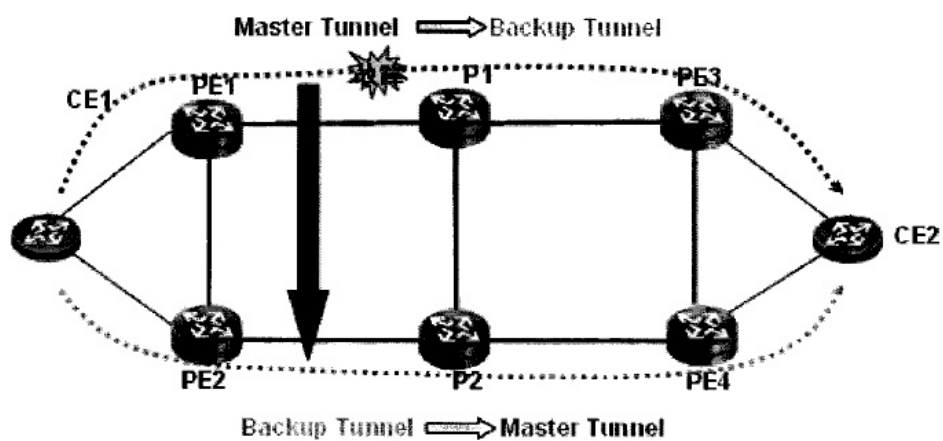


FIG. 6

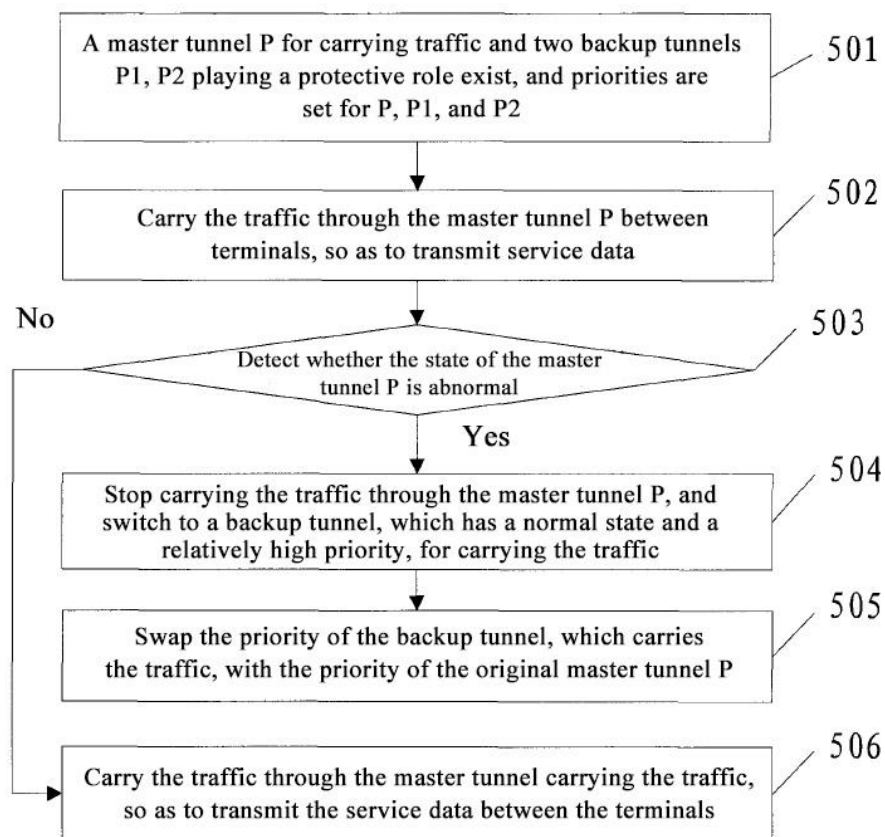


FIG. 7

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

H04L 12/56 (2006.01)

H04L 12/26 (2006.01)

H04L 12/24 (2006.01)



[12] 发明专利申请公布说明书

[21] 申请号 200910170173.7

[43] 公开日 2010 年 2 月 10 日

[11] 公开号 CN 101645848A

[22] 申请日 2009.9.4

[21] 申请号 200910170173.7

[71] 申请人 华为技术有限公司

地址 518129 广东省深圳市龙岗区坂田华为
基地总部办公楼

[72] 发明人 李振斌 黄永年 蒋 虎

[74] 专利代理机构 北京中博世达专利商标代理有
限公司

代理人 申 健

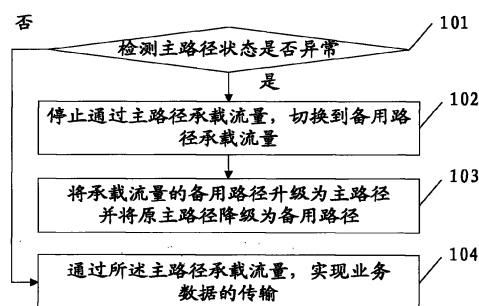
权利要求书 2 页 说明书 10 页 附图 4 页

[54] 发明名称

流量保护方法、装置及系统

[57] 摘要

本发明公开了一种流量保护方法、装置及系统，涉及通信领域，解决了现有技术中由于流量的频繁切换而带来的流量可靠性差的问题。本发明包括：终端之间存在一条用以承载流量的主路径，和至少一条起保护作用的备用路径；检测主路径的状态是否异常，若所述主路径的状态异常，则切换到备用路径承载流量；并将承载流量的备用路径升级为主路径，并将原主路径降级为备用路径。本发明实施例主要用于具有 MPLS 功能的网络中终端之间数据业务传输的过程中。



1、一种流量保护方法，其特征在于，在多协议标签交换 MPLS 的网络中，存在一条用以承载流量的主路径，和至少一条起保护作用的备用路径，该方法包括：

检测主路径状态是否异常；

若所述主路径的状态异常，切换到备用路径承载流量；

将承载流量的备用路径升级为主路径，将原主路径降级为备用路径，其中，若所述原主路径恢复正常，仍将流量锁定在升级为主路径的所述备用路径来承载，不回切到所述原主路径上。

2、根据权利要求 1 所述的流量保护方法，其特征在于，还包括：为所述主链路和所述至少一条备用路径设置优先级。

3、根据权利要求 2 所述的流量保护方法，其特征在于，当所述主路径的状态异常时，所述切换到备用路径承载流量，具体包括：

根据所述备用路径优先级的高低，将流量切换到优先级高的正常工作的备用路径承载。

4、根据权利要求 3 所述的流量保护方法，其特征在于，将承载流量的备用路径升级为主路径，将原主路径降级为备用路径，具体包括：将原主路径的优先级与所述承载流量的备用路径的优先级进行互换，使得承载流量的备用路径升级为主路径，原主路径降级为备用路。

5、一种流量保护装置，其特征在于，所述装置用于多协议标签交换 MPLS 的网络中，所述 MPLS 网络中存在一条用以承载流量的主路径，和至少一条起保护作用的备用路径，所述装置包括：

检测模块，用于检测主路径的状态是否异常；

切换模块，用于在所述检测模块检测到主路径的状态异常时，切换到备用路径承载流量；

调整模块，用于将承载流量的备用路径升级为主路径，并将原主路径降级为备用路径，其中，若所述原主路径恢复正常，仍将流量锁定在升级为主路径的所述备用路径来承载，不回切到所述原主路径上。

6、根据权利要求5所述的流量保护装置，其特征在于，还包括：

设置模块，用于为所述主路径和所述至少一条备用路径设置优先级。

7、根据权利要求6所述的流量保护装置，其特征在于，所述切换模块具体用于，当所述检测模块检测到所述主路径的状态异常时，根据所述备用路径优先级的高低，将流量切换到优先级高的正常的备用路径承载。

8、根据权利要求5所述的流量保护装置，其特征在于，所述调整模块具体用于当主所述链路发生状态异常时，根据所述备用路径优先级的高低，将流量切换到优先级高的正常的备用路径承载后，将原主路径的优先级与所述备用路径的优先级进行互换。

9、一种通信系统，包括终端，其特征在于，所述系统用于多协议标签交换MPLS的网络中，所述MPLS网络中存在一条用以承载流量的主路径，和至少一条起保护作用的备用路径，所述终端包括：

检测模块，用于检测主路径的状态是否异常；

切换模块，用于在所述检测模块检测到主路径的状态异常时，切换到备用路径承载流量；

调整模块，用于将承载流量的备用路径升级为主路径，并将原主路径降级为备用路径，其中，若所述原主路径恢复正常，仍将流量锁定在升级为主路径的所述备用路径来承载，不回切到所述原主路径上。

10、根据权利要求9所述的通信系统，其特征在于，所述终端为客户端或者服务器。

流量保护方法、装置及系统

技术领域

本发明涉及通信领域，特别涉及对业务流量进行保护方法、装置及系统。

背景技术

在电信网络中，高可靠性始终是最基础、最关键的性能要求，特别是话音业务，端到端保护倒换的时间必须小于 200ms 才能满足要求。为了达到这个标准，需要提供丰富、可靠的 TE (Traffic Engineering, 流量工程) 保护解决方案。MPLS (Multi - Protocol Label Switching, 多协议标签交换协议) TE 提供了丰富的流量保护解决方案，包括端到端备份路径保护、备份 Tunnel (隧道) 保护技术等。在这些保护机制中，用户须指定一条主路径和多条备份路径。当主路径发生故障，业务流量切换至备份路径；当主路径恢复，业务流量回切至主路径。

在实现上述流量切换的过程中，发明人发现现有技术中至少存在如下问题：当主路径发生故障时，备份路径马上替代主路径，实现流量的保护。当主路径恢复正常状态后，流量再回切到主路径。对于一次链路震荡，流量要进行两次切换。如果网络比较复杂，同时网络不够稳定，那么网络中的流量会出现频繁的切换，这样会给系统造成不必要的负担，影响流量的可靠性。

发明内容

本发明的实施例提供一种流量保护方法、装置及通信系统，其解决了在网络不稳定的情况下，频繁的流量切换而带来的严重影响流量可靠性的问题。

为达到上述目的，本发明的实施例采用如下技术方案：

一种流量保护方法，在多协议标签交换 MPLS 的网络中，存在一条用以承载

流量的主路径, 和至少一条起保护作用的备用路径, 该方法包括:

检测主路径状态是否异常;

若所述主路径的状态异常, 切换到备用路径承载流量;

将承载流量的备用路径升级为主路径, 并将原主路径降级为备用路径, 其中, 若所述原主路径恢复正常, 仍将流量锁定在升级为主路径的所述备用路径来承载, 不回切到所述原主路径上。

一种流量保护装置, 所述装置用于多协议标签交换 MPLS 的网络中, 所述 MPLS 网络中存在一条用以承载流量的主路径, 和至少一条起保护作用的备用路径, 所述装置包括:

检测模块, 用于检测主路径的状态是否异常;

切换模块, 用于在所述检测模块检测到主路径的状态异常时, 切换到备用路径承载流量;

调整模块, 用于将承载流量的备用路径升级为主路径, 并将原来的主路径降级为备用路径, 其中, 若所述原主路径恢复正常, 仍将流量锁定在升级为主路径的所述备用路径来承载, 不回切到所述原主路径上。

一种通信系统, 包括终端, 所述系统用于多协议标签交换 MPLS 的网络中, 所述 MPLS 网络中存在一条用以承载流量的主路径, 和至少一条起保护作用的备用路径, 所述包括:

检测模块, 用于检测主路径的状态是否异常;

切换模块, 用于在所述检测模块检测到主路径的状态异常时, 切换到备用路径承载流量;

调整模块, 用于将承载流量的备用路径升级为主路径, 并将原主路径降级为备用路径, 其中, 若所述原主路径恢复正常, 仍将流量锁定在升级为主路径的所述备用路径来承载, 不回切到所述原主路径上

本发明技术方案中, 两个终端之间存在承载流量的主路径和起保护作用的备用路径, 当主路径发生异常时, 切换到备用路径承载流量, 并将承载流量的

备用路径升级为主路径，将原来的主路径降级为备用路径；当原来主路径的状态恢复正常状态时，承载流量的链路不再回切至主路径，而是由承载流量的备用路径继续承载流量，直到该备用路径的状态出现异常时才进行承载流量的链路的切换，这样一次链路震荡仅需要一次链路的切换，便可以锁定流量，与现有技术中一次链路的震荡需要两次链路的切换相比，极大地减少网络中流量切换的频率，提高流量承载的可靠性。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本发明实施例 1 中流量保护方法的流程图；

图 2 为本发明实施 1 中流量保护装置的组成框图；

图 3 为本发明实施例 2 中流量保护方法中的承载流量的链路切换示意图；

图 4 为本发明实施例 2 中流量保护方法的流程图；

图 5 为本发明实施例 2 中流量保护装置的组成框图；

图 6 为本发明实施例 3 中流量保护方法中的承载流量的隧道切换示意图；

图 7 为发明实施例 3 中流量保护的方法流程图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

实施例 1

本发明实施例提供一种流量保护方法，用于在具有多协议标签交换（MPLS）的网络中，存在一条用以承载流量的主路径，和至少一条起保护作用的备用路径。在端到端备份路径保护机制中，该主路径和备份路径为 LSP (Label Switch Path, 标签交换路径)，在备份 Tunnel 保护（隧道保护组）机制中，该主路径和备份路径为隧道，当然该主路径和备份路径还可以有其它的方式，并不局限于 LSP 和隧道。

如图 1 所示，该方法包括如下步骤：

101、检测主路径状态是否异常，若检测到所述主路径的状态异常，则执行步骤 102；若检测到所述主路径的状态无异常，则执行步骤 104。

其中所述主路径状态的异常可以为但不限于以下形式，包括：链路故障、数据丢包、传输中断等；本发明实施例对此不进行限制。

102、停止通过主路径承载流量，换到备用路径承载流量，由承载流量的备用通道实现业务数据的传输。

103、在将承载流量的链路由主路径切换到备用路径后，将承载流量的备用路径升级为主路径，并将原来的主路径降级为备用路径，其中，若原主路径恢复正常，仍将流量锁定在升级为主路径的备用路径来承载，不回切到原主路径上。

104、通过所述主路径承载流量，实现业务数据的传输。

本发明实施例提供一种流量保护装置，该装置用于 MPLS 的网络中，所述 MPLS 网络中存在一条用以承载流量的主路径，和至少一条起保护作用的备用路径。

如图 2 所示，该装置包括：检测模块 21、切换模块 22 和调整模块 23。

检测模块 21，用于检测主路径的状态是否异常；

切换模块 22，用于在所述检测模块 21 检测到主路径的状态异常时，切换到备用路径承载流量；

调整模块 23，用于在切换模块 22 将承载流量的链路由主路径切换到到备用路径后，将承载流量的备用路径升级为主路径，并将原主路径降级为备用路径。

若所述检测模块 21 没有检测到主路径状态的异常，还是通过所述主路径承载流量实现终端之间业务数据的传输。

上述流量保护的方法及装置用在网络中时，需要在采用上述方法的终端中安装相应的装置，如果某个网络中需要相互通信的两个终端安装了上述装置，则构成了流量保护系统。

本发明实施例中，当主路径发生异常时，切换到备用路径承载流量，并将承载流量的备用路径升级为主路径，将原主路径降级为备用路径；并且当原主路径的状态恢复正常状态时，承载流量的链路不再回切至主路径，而是由承载流量的备用路径继续承载流量，直到该备用路径的状态出现异常时才进行承载流量的链路的切换，这样一次链路震荡仅需要一次链路的切换，便可以锁定流量，与现有技术中一次链路的震荡需要两次链路的切换相比，极大地减少网络中流量切换的频率，提高流量承载的可靠性。

实施例 2

本发明实施例提供一种流量保护方法，本发明实施例以所述链路为 LSP (Label Switch Path, 标签交换路径) 为例，结合图 3 和图 4 具体阐述所述流量保护的方法，说明端到端备份路径的保护，如图 4 所示，该方法包括如下步骤：

入接口和出接口的 LSR (Label Switched Router, 标签交换路由器) 之间存在一条用以承载流量的主 LSP，和至少一条起保护作用的备用 LSP；为主 LSP 和备用 LSP 设置优先级，优先级较高的备用 LSP 在承载流量的主 LSP 的状态异常时，优先被选作承载流量的 LSP。本发明实施例中以所述至少一条起保护作用的备用 LSP 为两条备用 LSP 为例具体阐述流量保护的方法。

301、入接口和出接口的 LSR 之间存在一条用以承载流量的主 LSP，和两条起保护作用的备用 LSP1、LSP2；为主 LSP、备用 LSP1 和备用 LSP2 分别设置优先级；具体设置为，主 LSP 的优先级最高，设置优先级为主，且将备用 LSP1 和备用 LSP2 优先级由高到低设定为备 1、备 2。

302、入接口和出接口的 LSR 之间通过主 LSP 承载流量，实现业务数据的传

输。

303、检测主 LSP 的状态，若检测到主 LSP 的状态异常时，执行步骤 304；若检测到主 LSP 的状态无异常时，执行步骤 306。其中所述主 LSP 状态的异常可以为但不限于以下形式，包括：链路故障、数据丢包、传输中断等；本发明实施例对此不进行限制。

304、停止通过主 LSP 承载流量，根据备用 LSP1 和备用 LSP2 优先级的高低，将流量切换到优先级高的正常的备用路径承载。

本发明实施例中备用 LSP1 的优先级别高于备用 LSP2 的优先级别，所以将承载流量的链路由主 LSP 切换到备用 LSP1，由承载流量的备用 LSP1 实现业务数据的传输。

如果高优先级的备用 LSP1 也出现异常，则将承载流量的链路由主 LSP 切换到备用 LSP2 上，即根据备用 LSP1 和备用 LSP2 优先级的高低，将流量切换到优先级高的正常的备用路径承载。

305、在将流量切换到优先级高的正常的备用路径承载后，将承载流量的备用 LSP1 的优先级与原主 LSP 的优先级进行互换，即将主 LSP 的优先级降为备 1，将备用 LSP1 的优先级升为主；若承载流量的隧道为备用隧道 LSP2，则将原主 LSP 的优先级降级为备 2，将备用 LSP2 的优先级升级为主。

在本步骤中，通过变换优先级，当原主 LSP 恢复正常后，仍将流量锁定在升级为主路径的备用 LSP2 来承载，不回切到原主 LSP 上。

306、由承载流量的主 LSP 承载流量，实现业务数据的传输。

本发明实施例还提供一种流量保护装置，如图 5 所示，该装置包括：设置模块 41、检测模块 42、切换模块 43 和调整模块 44。

设置单元 41，用于为主路径和备用路径设置优先级；

检测模块 42，用于检测主路径的状态是否异常；

切换模块 43，用于在检测模块 42 检测到主路径的状态异常时，根据备用路径优先级的高低，将流量切换到优先级高的正常的备用路径承载；

调整模块 44, 用于在切换模块 43 将承载流量的链路由主路径切换到优先级高的正常的备用路径后, 将承载流量的备用路径的优先级与原主路径的优先级进行互换。

若所述检测模块本发明实施例中, 终端之间存在承载流量的主路径和至少一条起保护作用的备用路径, 并且为所述主路径和备用路径设置优先级, 当主路径发生异常时, 根据所述备用路径优先级的高低, 将流量切换到优先级较高的备用路径承载, 并将承载流量的备用路径的优先级与原主路径进行互换; 当原来主路径的状态恢复正常状态时, 承载流量的链路不再回切至原主路径, 而是由优先级较高的备用路径继续承载流量, 因此一次链路震荡仅需要一次链路的切换, 便可以锁定流量, 与现有技术中一次链路的震荡需要两次链路的切换相比, 极大地减少网络中流量切换的频率, 降低系统开销, 提高流量承载的可靠性。

并且在将流量从主路径切换到优先级较高的一条备用路径后, 将所述原来的主路径与上述备用路径的优先级进行互换, 由该备用路径承载流量, 直到该备用路径的状态出现异常时才再根据备用路径的优先级选择承载流量的备用路径, 因此终端之间进行业务流量的传输时, 主路径和备用路径所经过的路径不存在强烈的主次之分, 流量可以由各个优先级的链路长期承载。

实施例 3

本发明实施例提供一种流量保护方法, 本发明实施例以所述链路为隧道为例, 结合图 6 和图 7 具体阐述所述流量保护的方法, 说明隧道保护组备份路径的保护, 如图 7 所示, 该方法包括如下步骤:

隧道保护组中存在一条用以承载流量的主隧道, 和至少一条起保护作用的备用隧道; 为主隧道和备用隧道设置优先级, 优先级较高的备用隧道在承载流量的主隧道的状态异常时, 优先被选作承载流量的隧道。本发明实施例中以所

述至少一条起保护作用的备用隧道为两条备用两路为例具体阐述流量保护的方法并以所述备用隧道为两条隧道为例具体阐述所述流量保护的方法。

501、隧道保护组中之间存在一条用以承载流量的主隧道 P，和两条起保护作用的备用隧道 P1、P2，为主隧道 P、备用隧道 P1 和备用隧道 P2 分别设置优先级；具体设置为，主路径 LSP 的优先级最高，设置优先级为主，且将所述两条备用隧道 P1、P2 优先级由高到低设定为备 1、备 2。

502、隧道保护组中之间通过主隧道 P 承载流量，实现业务数据的传输。

503、检测主隧道 P 的状态，若检测到主隧道 P 的状态异常时，执行步骤 504；若检测到主隧道 P 的状态无异常时，执行步骤 506。其中所述状态异常可以为但不限于以下形式，包括：链路故障、数据丢包、传输中断等；本发明实施例对此不进行限制。

504、停止通过主隧道 P 承载流量，根据备用隧道优先级的高低，将流量切换到状态无异常且优先级高备用隧道。

本发明实施例中备用隧道 P1 的优先级别高于备用隧道 P2 的优先级，若备用隧道 P1 的状态无异常，则将流量由主隧道切换到备用隧道 P1，若备用隧道 P1 的状态存在异常，由将流量由主隧道切换到备用隧道 P2，由备用隧道实现业务数据的传输。

如果高优先级的备用隧道 P1 也出现异常，则将承载流量的链路由主 LSP 切换到备用隧道 P2 上，即根据备用 P1 和备用 P2 优先级的高低，将流量切换到优先级高的正常的备用路径承载。

505、在将流量切换到状态无异常且优先级高备用隧道后，将承载流量的备用隧道的优先级与原主隧道的优先级进行互换，即若承载流量的隧道为备用隧道 P1，则将原主隧道的优先级降为备 1，将备用隧道 P1 的优先级升级为主；若承载流量的隧道为备用隧道 P2，则将原主隧道 P 的优先级降级为备 2，将备用隧道 P2 的优先级升级为主。

在本步骤中，通过变换优先级，当原主隧道 P 恢复正常后，仍将流量锁定在升级为主路径的备用隧道 P1 或者备用隧道 P2 来承载，不回切到原主 LSP 上。

506、由承载流量的主隧道继续承载流量，实现终端之间业务数据的传输。

本发明实施例还提供一种如图 5 所示流量保护装置，具体描述在实施例 2 中，故在此不赘述。

上述流量保护的方法及装置用在网络中时，需要在采用上述方法的终端中安装相应的装置，如果某个网络中需要相互通信的两个终端安装了上述装置，则构成了流量锁定系统。

本发明实施例中，两个终端之间建立了承载流量的主隧道和至少一条起保护作用的备用隧道，并且为所述主路径和备用隧道设置优先级，当主隧道发生异常时，根据所述备用隧道优先级的高低，将流量切换到状态正常并且优先级较高的备用隧道承载，并将承载流量的备用隧道的优先级与原主隧道进行互换；当原来主隧道的状态恢复正常状态时，承载流量的隧道不再回切至原主隧道，而是由优先级较高的备用隧道继续承载流量，因此一次隧道震荡仅需要一次隧道的切换，便可以锁定流量，与现有技术中一次隧道的震荡需要两次隧道的切换相比，极大地减少网络中流量切换的频率，降低系统开销，提高流量承载的可靠性。

并且在将流量从主隧道切换到优先级较高的一条备用隧道后，将所述原来的主隧道与上述备用隧道的优先级进行互换，由该备用隧道承载流量，直到该备用隧道的状态出现异常时才再根据备用隧道的优先级选择承载流量备用隧道，因此终端之间进行业务流量的传输时，主隧道和备用隧道所经过的路径不存在强烈的主次之分，流量可以由各个优先级的隧道长期承载。

在发明本实施中，当链路情况不稳定，当主路径发生异常，且优先级较高的备用路径状态发生异常还没有恢复至正常状态，这时将流量切换至优先级较低的备用路径上来，进一步保证了数据传输的稳定性。

本发明实施例中主要是以 MPLS TE 中的隧道保护组和端到端备份路径保护来为例说明本发明的应用，在具体实施时，可以根据情况和需求的不同，建立其他流量工程中的流量锁定，并且可以存在多个备用路径。

通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在可读取的存储介质中，如计算机的软盘，硬盘或光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等等）执行本发明各个实施例所述的方法。

以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

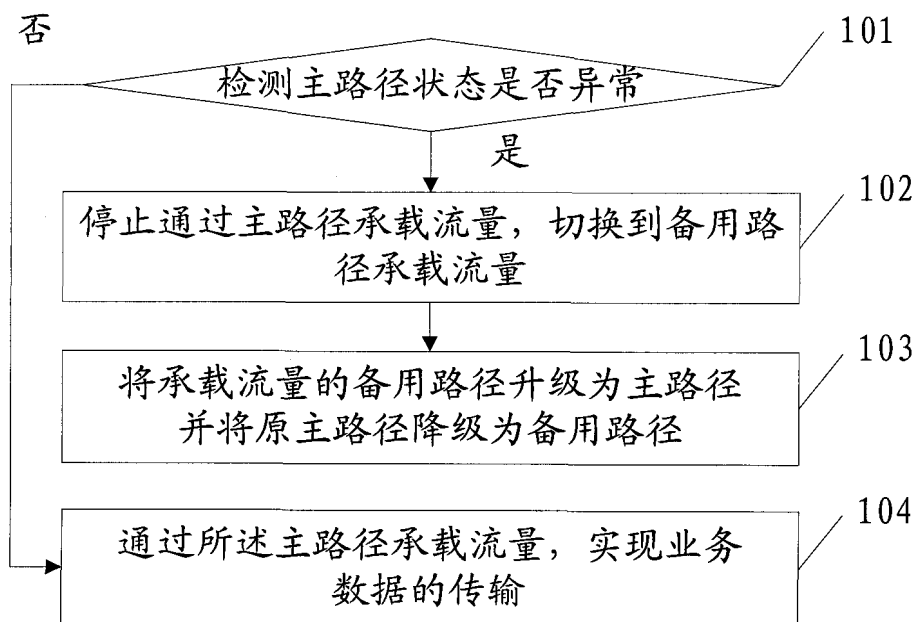


图 1

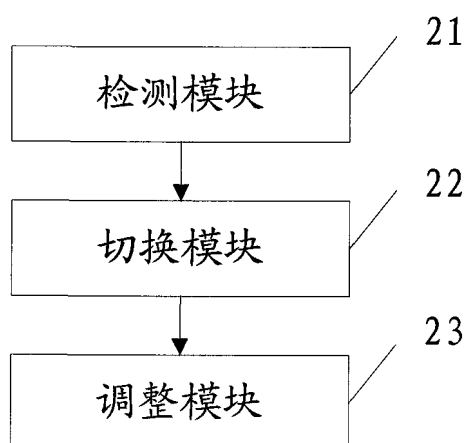


图 2

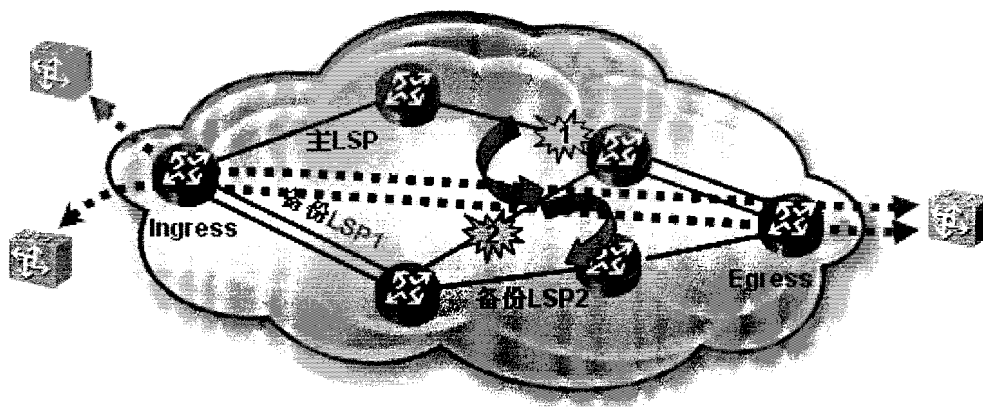


图 3

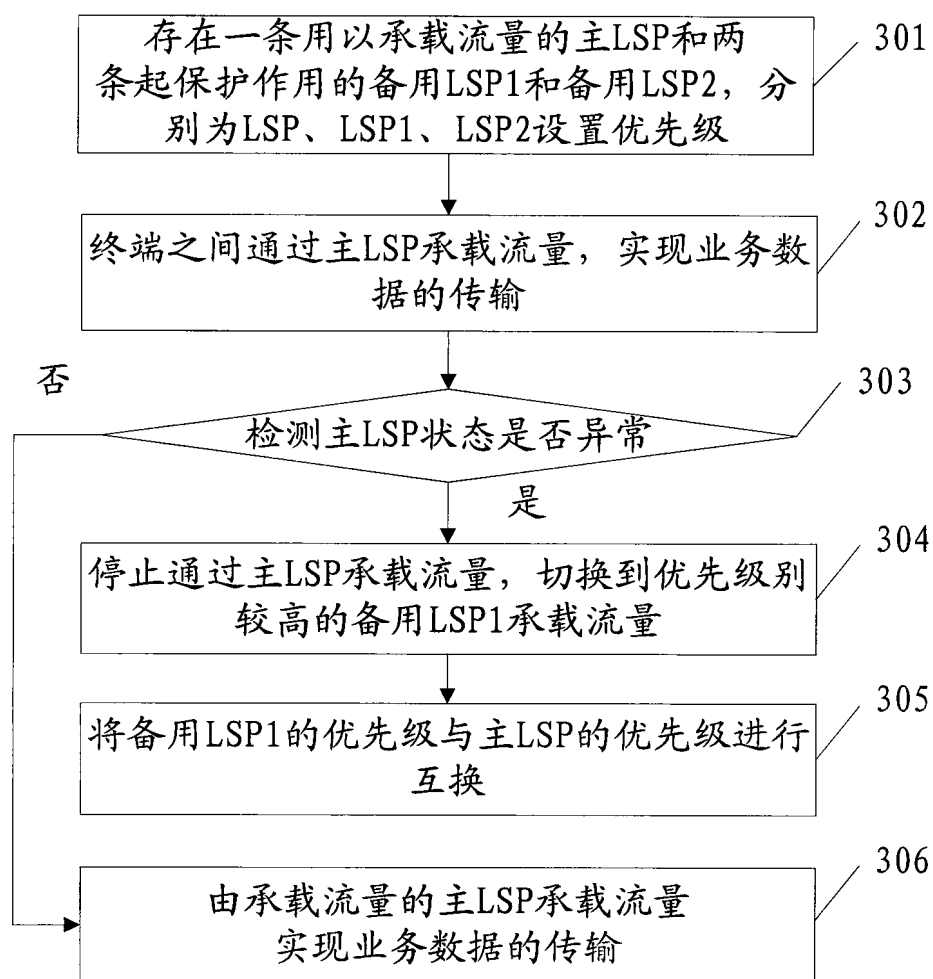


图 4

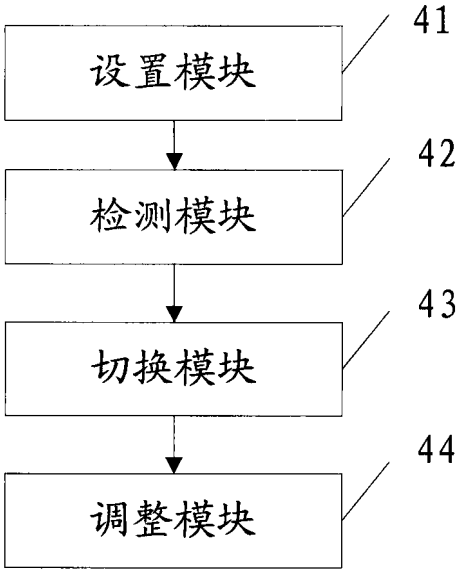


图 5

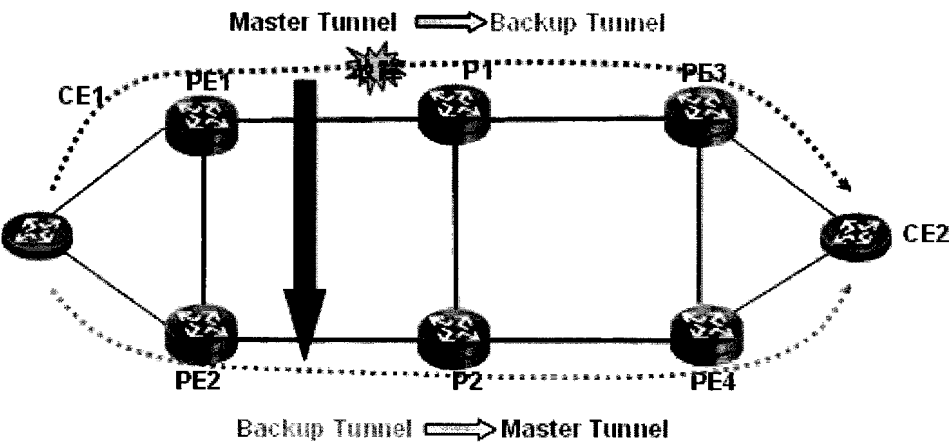


图 6

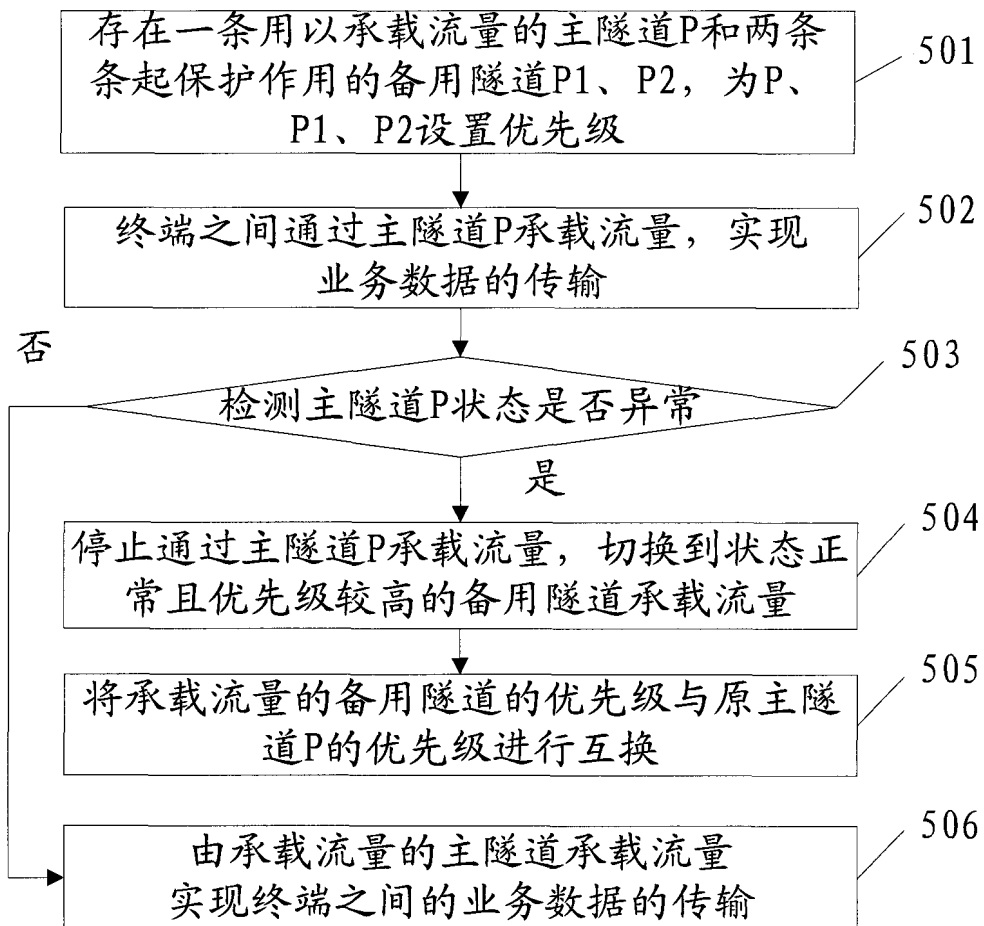


图 7