基于BFD协议的承载网业务毫秒级保护方案研究及实践

Research and Practice of Millisecond-Level Protection Scheme for Bearer Network Services Based on BFD Protocol

康　琳[1]，张文治[1]，郝文胜[1]，李　征[2]（1. 中国移动通信集团河南有限公司，河南 郑州 450000；2. 郑州能通网络技术有限公司，河南 郑州 450000）

Kang Lin[1]，Zhang Wenzhi[1]，Hao Wensheng[1]，Li Zheng[2]（1. China Mobile Group Henan Co.，Ltd.，Zhengzhou 450000，China；2. Zhengzhou NengTong Networks Technology Co.，Ltd.，Zhengzhou 450000，China）

摘　要：

运营商承载网采用双星型结构组网，下联边缘路由器双平面接入，可保证主备链路的容灾性。但在链路误码闪断场景下，网络层未达到收敛标准将导致路由无法切换，并造成链路传送数据出现丢包或中断的情况，下联网元与核心网通信受到严重影响。为避免该场景对业务造成影响，提出一种基于BFD协议的承载网业务毫秒级保护方案。该方案通过监测链路质量，自动改变链路开销，从而实现路由协议的毫秒级感知，完成链路的快速切换，避免影响业务。

关键词：

承载网；链路误码；路由协议；快速切换

doi：10.12045/j.issn.1007-3043.2025.06.013

文章编号：1007-3043（2025）06-0065-06

中图分类号：TN919

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

The carrier's transport network of operators adopts a dual-star topology，with edge routers in the lower network layer connected through dual-plane access to ensure disaster recovery of primary/backup links. However，in scenarios of link error-code flapping or transient interruptions，the network layer fails to meet convergence criteria，preventing route switching. This results in packet loss or transmission interruptions in physical links，severely impacting communication between lower-layer network elements and the core network. To mitigate service impact in such scenarios，a millisecond-level protection scheme for transport network services based on the bidirectional forwarding detection（BFD）protocol has been proposed. By continuously monitoring link quality and automatically adjusting link cost metrics，this solution enables millisecond-level route protocol perception，achieving rapid link switching to maintain service continuity and prevent operational disruptions.

Keywords：

Bearer network；Link bit errors；Routing protocols；Quick switching

引用格式：康琳，张文治，郝文胜，等. 基于BFD协议的承载网业务毫秒级保护方案研究及实践[J]. 邮电设计技术，2025（6）：65-70.

1 运营商承载网保护方案简介

目前，国内的区域级通信运营商承载网主要通过BGP MPLS VPN方式承载5G网络云、传统核心网、各类资源池（私有云、移动云）、物联网、大客户业务、各专业网管系统、视频会议等中国移动最核心业务，网络划分不同的VPN来实现各业务系统的隔离[1]。但由于5G时代高带宽、大连接、低延迟的特点，网络承载能力面临新的挑战，对于通信运营商来说，更多的高敏感业务对网络承载设备性能提出了更高的要求[2]。

承载网采用三层结构组网，接入层使用边缘路由器（Customer Edge，CE）完成业务数据的接入；汇聚层接入路由器（Access Router，AR）完成数据的汇聚，以减轻核心层设备的负荷；核心层使用核心路由器（Core Router，CR）实现骨干网络之间的优化传输，实现跨区域网络通信[3]。运营商网络三层总体架构如图1所示。

在图1中，承载网CR、AR构成双星型结构，下联

收稿日期：2025-04-10

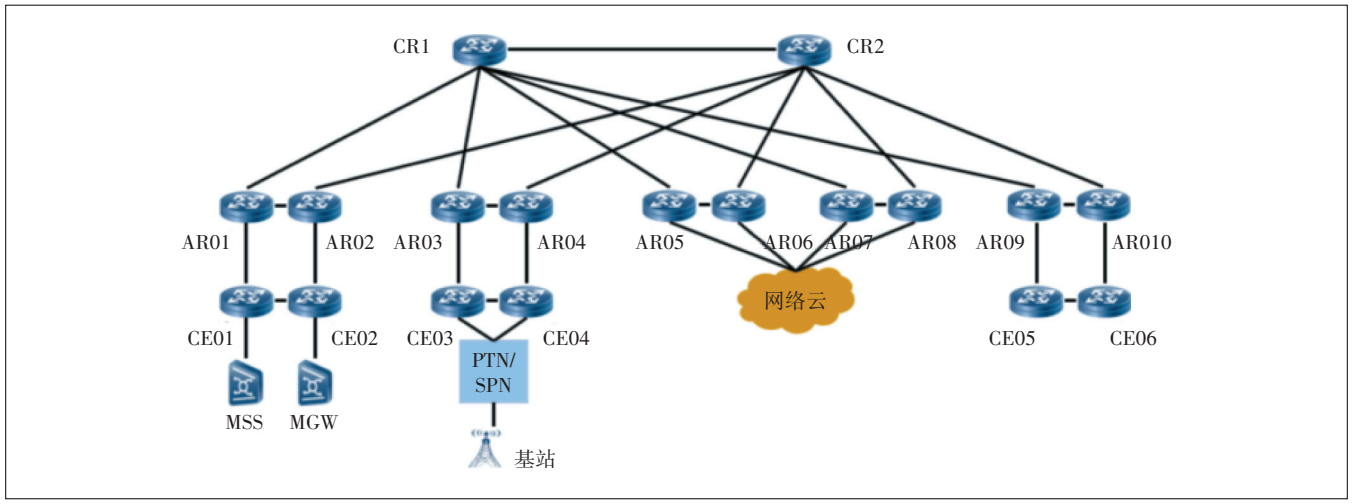

图1　运营商级三层网络架构

网络边缘路由器，采用“口”字形双平面接入AR设备，一对CE之间采用内部网关协议（Internal Gateway Protocol，IGP[4]）互联。CE与下联业务之间一般采用静态路由方式或虚拟路由冗余协议（Virtual Router Redundancy Protocol，VRRP[5]）对接，为实现链路故障的快速感知，可部署双向转发检测机制（Bidirectional Forwarding Detection，BFD[6]），并通过与三层路由协议联动，完成路由的快速收敛，确保业务的永续性。CE与上连接入路由器AR之间通过开放最短路径优先（Open Shortest Path First，OSPF[7]）路由协议互联，一对AR以及AR与上联CR之间部署内部网关协议，如中间系统到中间系统（Intermediate System to Intermediate System，IS-IS）路由协议，外部网关协议采用BGP-4（Border Gateway Protocol-4[8]）路由协议[9]。

现网结构可保证主备链路的容灾性。但在链路误码及传输闪断场景下，汇聚层、核心层路由设备端口无法自动进入down状态，此时如仍根据动态路由协议的自有收敛特性（如OSPF协议依靠Hello包，ISIS协议依靠Hello报文），只能在秒级甚至十秒级内完成路由收敛，无法满足语音等毫秒级业务保护要求[10]。即在该特殊场景下，当物理链路传送数据出现严重丢包或中断时，由于路由协议未达到收敛标准，会造成下联业务中断，下联网元与省中心核心网通信将受到严重影响（见图2）。

在图2中，当AR至CE链路发生传输链路质量劣化（线路老化、光路抖动等），导致CRC/symbol、B1/B2/B3误码增加，或链路故障及传输告警导致IP承载网设备端口频繁down/up[11]时，业务传送路径无法自动发

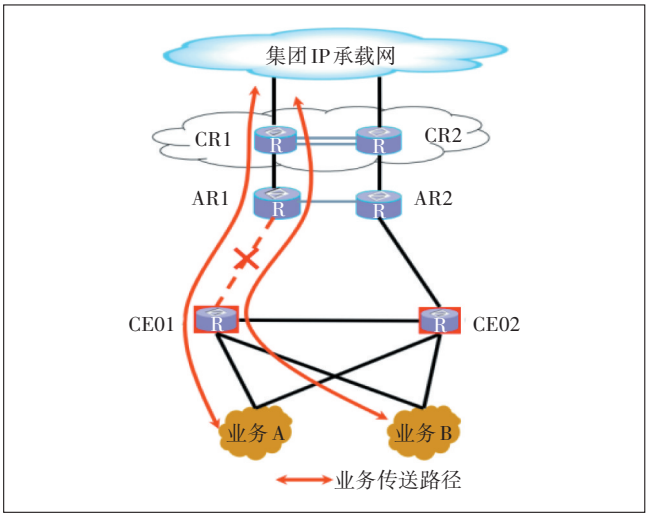

图2　传输误码影响业务示意

生切换，需在排查传输故障后手动进行业务路径切换，或等待本地光缆修复后才能恢复业务，光缆修复时长不低于120 min[5]。

针对这种情况，本文提出了一种基于BFD协议实现承载网业务毫秒级保护的方案。该方案通过监测链路质量，自动改变链路开销，从而实现路由协议的毫秒级感知，完成链路的快速切换，避免影响业务。

2　基于BFD协议的承载网保护改进方案

为了尽量减少或避免因链路误码及传输闪断对业务造成的严重影响，在现网常规容灾架构的基础上，部署BFD联动IGP cost值调整，从而实现当网络中存在链路误码或者链路闪断时，路由器会提前检测BFD会话中断，并自动调整接口IGP cost值，切换到备

用链路恢复业务。此外，当主用链路恢复后，该方案可根据策略自动实现业务回切。此方案实施后，可实现路由协议的毫秒级感知，从而实现业务传送链路的快速切换，减少或避免对业务造成影响。基于BFD协议的承载网保护改进方案如下。

a）汇聚层保护方案。CE上联链路AR部署BFD联动OSPF开销调整，实现特殊场景下的业务迂回及回切。

b）核心层保护方案。AR至CR链路部署BFD联动ISIS开销调整，实现特殊场景下的业务迂回及回切。

2.1 汇聚层保护方案

在汇聚层保护方案中，承载网网络边缘路由器CE采用“口”字形双平面接入AR设备，CE与上连接入路由器AR之间通过OSPF路由协议互联。对CE上联链路部署BFD联动OSPF cost值调整，从而实现特殊场景下OSPF开销值的自动调整，使路由切换到备用链路，恢复业务。在主用链路恢复后，通过合理配置延时参数，实现业务自动回切至主链路。业务切换流程如图3所示。

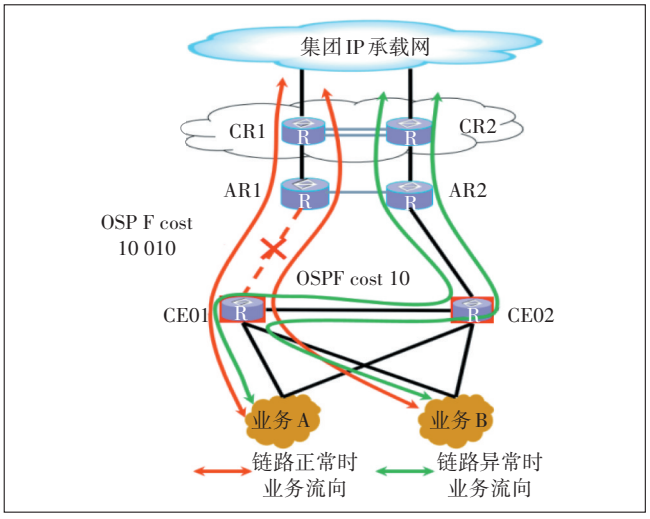

图3　汇聚层业务切换流程

在图3中，当传输原因导致主用链路〔CE01上联地（市）AR1链路〕劣化时，方案将自动增加主用链路开销，使业务快速切换至备用链路〔CE02上联地（市）AR2链路〕。当主用链路恢复正常时，方案通过自动恢复主用链路原有开销值，实现业务自动切换至主用链路。方案部署流程如图4所示。

a）“主备链路分别建立OSPF邻居”阶段。该阶段主要完成CE与AR之间的端口参数配置及OSPF参数配置[12]，最终建立OSPF邻居，其具体参数值配置如表1所示。

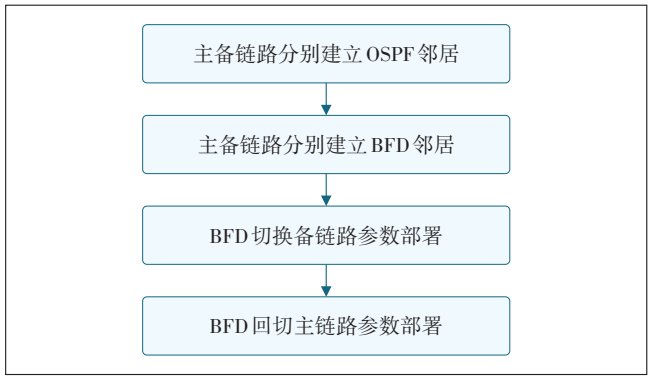

图4　汇聚层方案部署流程

表1　“主备链路分别建立OSPF邻居”阶段参数值配置

参数名称	参数说明	AR参数	CE参数
area	区域	0	0
cost	链路开销	10	10
Router ID	路由号	按规划配置	按规划配置
network-type	网络类型	p2p	p2p
timer hello	发现hello报文间隔	1	1

b）“主备链路分别建立BFD邻居”阶段。该阶段主要完成CE与AR之间的BFD参数配置，最终成功建立BFD邻居[13]，具体参数配置如表2所示。

表2　“主备链路分别建立BFD邻居”阶段参数值配置

参数名称	参数说明	AR参数	CE参数
discriminator local	本地标识	10170	10171
discriminator remote	远端标识	10171	10170
min-tx-interval	BFD报文发送间隔/ms	100	100
min-rx-interyal	BFD报文接收间隔/ms	100	100
detect-multiplier	指定BFD会话的检测时间倍数	3	3

c）“BFD切换备链路参数部署”阶段。该阶段主要完成BFD联动CE与AR OSPF邻居，并设置OSPF开销变化参数，实现链路劣化时主用链路开销增加，最终将业务自动切换至备用链路。其实现原理为：当感知到主用链路BFD down时，OSPF接口的开销值会自动增加，其他路由器监测到主用链路开销增大，将自动进行主备链路开销比较，此时由于备用链路开销小于主用链路，将选择备用链路作为业务路径，完成故障链路切换。具体参数配置如表3所示。

d）“BFD回切主链路参数部署”阶段。该阶段主要完成链路延时回切参数设置，实现主用链路恢复后

表3　“BFD切换备链路参数部署”阶段参数值配置

参数名称	参数说明	AR参数	CE参数
Ospf bfd incr-cost	配置接口下BFD联动Cost增加值	10 000	10 000

的业务自动回切。其实现原理为:当感知到主用链路BFD up时,接口的开销值会自动恢复为之前的开销值,但为了避免因链路质量引起BFD状态频繁变化,导致链路不稳定而出现流量丢失的情况,方案配置了开销调整的延迟恢复时间来推迟接口的开销值恢复,在延迟时间内BFD状态的变化不会引起算路变化,以此保证网络的可靠性。具体参数配置如表4所示。

表4　“BFD回切主链路参数部署”阶段参数值配置

参数名称	参数说明	AR参数	CE参数
wtr	指定接口开销调整延迟恢复时间/s	600	600

2.2 核心层保护方案

在核心层保护方案中,一对AR之间以及AR与上联CR之间部署ISIS路由协议。对AR上联链路部署BFD联动ISIS cost值调整,从而实现特殊场景下ISIS开销值的自动调整,使路由切换到备用链路,恢复业务。在主用链路恢复后,通过合理配置延时参数,实现业务自动回切至主链路。业务切换流程如图5所示。

在图5中,红线代表链路正常时的业务流向,绿色线代表链路异常时的业务流向。当传输原因导致主用链路〔地(市)AR1上联CR1链路〕劣化时,方案将自动增加主用链路开销,使业务快速切换至备用链路

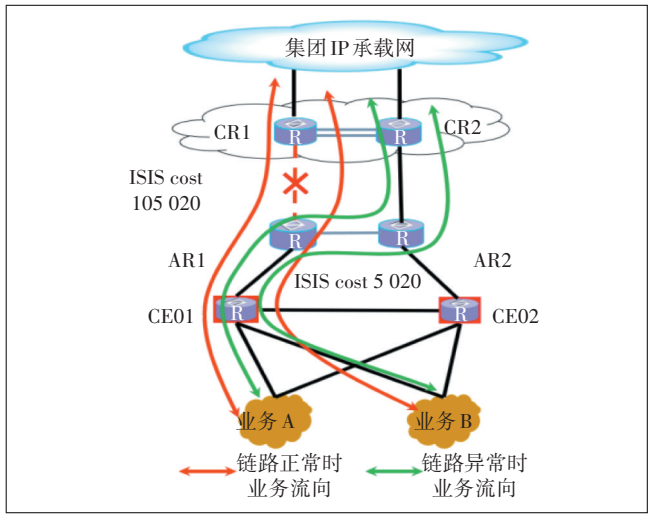

图5　核心层业务切换流程

〔地(市)AR2上联CR2链路〕。当主用链路恢复正常时,方案通过自动恢复主用链路原有开销值,实现业务自动切换至主用链路。方案部署流程如图6所示。

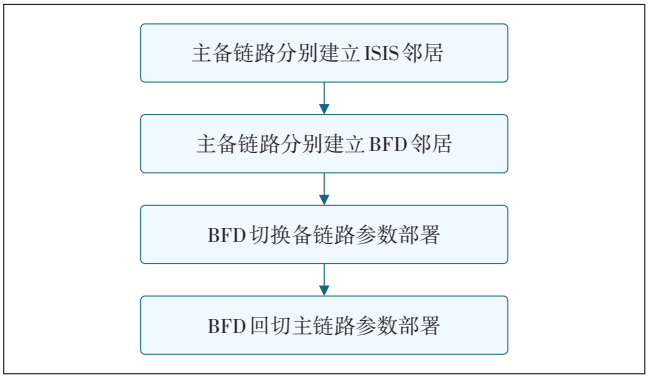

图6　核心层方案部署流程

a)“主备链路分别建立ISIS邻居”阶段。该阶段主要完成CE与AR之间的端口参数配置及ISIS参数配置,最终成功建立ISIS邻居[14]。具体参数配置如表5所示。

表5　“主备链路分别建立ISIS邻居”阶段参数值配置

参数名称	参数说明	AR参数	CR参数
mtu	配置以太网接口的最大传输单元	4 470	4 470
isis circuit-type	ISIS广播网接口的网络类型	p2p	p2p
isis circuit-level	Level-1-2 ISIS设备的接口链路类型	level-2	level-2
cost	链路开销值	5 020	5 020
network-entity	ISIS进程的网络实体名称	按需配置	按需配置

b)“主备链路分别建立BFD邻居”阶段。该阶段主要完成CE与AR之间的BFD参数配置,最终建立BFD邻居,具体参数配置如表6所示。

c)“BFD切换备链路参数部署”阶段。该阶段主要完成BFD联动AR与CR ISIS邻居,并设置ISIS开销变化参数,实现在链路劣化时主用链路开销增加,最

表6　“主备链路分别建立BFD邻居”阶段参数值配置

参数名称	参数说明	AR参数	CE参数
discriminator local	本地标识	10170	10171
discriminator remote	远端标识	10171	10170
min-tx-interval	BFD报文发送间隔/ms	100	100
min-rx-interyal	BFD报文接收间隔/ms	100	100
detect-multiplier	指定BFD会话的检测时间倍数	3	3

终将业务自动切换至备用链路。该阶段实现原理为：当感知到主用链路BFD down时，ISIS接口的开销值会自动增加，其他路由器监测到主用链路开销增大，将自动进行主备链路开销比较，此时由于备用链路开销小于主用链路，将选择备用链路作为业务路径，完成故障链路切换。具体参数配置如表7所示。

表7　“BFD切换备链路参数部署”阶段参数值配置

参数名称	参数说明	AR参数	CR参数
isis bfd incr-cost	配置接口下BFD联动Cost增加值	100 000	100 000

d）“BFD回切主链路参数部署”阶段。该阶段主要完成链路延时回切参数设置，实现主用链路恢复后的业务自动回切。该阶段实现原理为：当感知到主用链路BFD up时，接口的开销值会自动恢复为之前的开销值，但为了避免因链路质量引起BFD状态频繁变化，导致链路不稳定而出现流量丢失的情况，配置了开销调整的延迟恢复时间，以推迟接口的开销值恢复，在延迟时间内BFD的状态变化不会引起算路变化，从而保证了网络的可靠性。具体参数配置如表8所示。

表8　“BFD回切主链路参数部署”阶段参数值配置

参数名称	参数说明	AR参数	CE参数
wtr	指定接口开销调整延迟恢复时间/s	600	600

3 方案实施后的效果验证

方案已在运营商IP承载网进行了全网部署，并在部署后针对链路切换进行了验证，通过MPLS OAM[15]呈现出明显的路径变化，且切换过程中业务未受影响。以下通过承载网A地（市）CE1至B地（市）CE1路径测试情况介绍验证效果。

3.1 汇聚层保护方案效果验证

方案部署前，路径如图7所示。在图7中，第1跳为IP承载网AR1与接入CE1链路的互联地址，业务传送路径为A地（市）CE1—A地（市）AR1—B地（市）AR1—B地（市）CE1（由于CR部署为路由反射器，trace路由结果不显示CR信息，以下trace结果同理）。

```
<HAZZ-NGN-C  -HWNE40E>tracert -vpn-instance
Chin  Media 10.4  02.166
traceroute to China  Media
10.4  2.166(10.  2.166),max hops:30,
packet length:40,press CTRL_C to break
1 10.4  52.161  6 ms  17 ms  7 ms
2 10.4  02.165  9 ms  17 ms  7 ms
3 10.4  02.166  9 ms  24 ms  8 ms
```

图7　汇聚层保护方案部署前业务路径

方案部署后，当A地（市）CE1—A地（市）AR1的链路发生劣化时，流量自动切换至备用链路，路径如图8所示。在图8中，第1跳为IP承载网CE1与CE2链路的互联地址，业务传送路径为A地（市）CE1—A地（市）CE2—A地（市）AR2—B地（市）AR2—B地（市）CE2—B地（市）CE1。

```
<HAZZ-NGN-C  -HWNE40E>tracert -vpn-instance
China  _Media 10.4  02.166
traceroute to ChinaM  N_Media
10.4  02.166(10.4  02.166),max hops:30,
packet length:40,press CTRL_C to break
1 10.9.  0.245  3 ms  12 ms  7 ms
2 10.4.  53.161  6 ms  17 ms  7 ms
3 10.4.  03.165  9 ms  17 ms  7 ms
4 10.4.  03.166  9 ms  24 ms  8 ms
5 10.4.  02.166  9 ms  24 ms  8 ms
```

图8　汇聚层保护方案部署后业务切换路径

如图9所示，当故障链路恢复后，BFD到达等待时间，业务传送路径自动回切至原链路进行承载。

```
<HAZZ-NGN-C  -HWNE40E>tracert -vpn-instance
ChinaM  _Media 10.4  2.166
traceroute to China  _  Media
10.4  2.166(10.4  02.166),max hops:30,
packet length:40,press CTRL_C to break
1 10.4  52.161  7 ms  18 ms  8 ms
2 10.4  02.165  8 ms  19 ms  7 ms
3 10.4  02.166  7 ms  24 ms  8 ms
```

图9　汇聚层保护方案部署后业务回切路径

通过验证数据可知，业务可由原来的A地（市）CE1至B地（市）CE1主链路切换至备用链路进行传送，当原链路恢复并达到稳定后，业务自动回切至主链路承载，切换效果得到了进一步的验证。

3.2 核心层保护方案效果验证

方案部署前，路径如图10所示。从业务传送路径

```
<HAZZ-NGN-C  -HWNE40E>tracert -vpn-instance
ChinaM  _Media 10.4  02.166
traceroute to China  Media
10.4  2.166(10.4  02.166),max hops:30,
packet length:40,press CTRL_C to break
1 10.4  52.161  6 ms  17 ms  7 ms
2 10.4  02.165  7 ms  18 ms  8 ms
3 10.4  02.166  9 ms  24 ms  8 ms
```

图10　核心层保护方案部署前业务路径

可以分析出第1跳为IP承载网AR与接入CE链路的互联地址，业务传送路径为A地（市）CE—A地（市）AR—B地（市）AR—B地（市）CE。

方案部署后，当A地（市）AR1—CR1链路发生劣化时，流量自动切换至备用链路，路径如图11所示。从业务传送路径可以分析出第2跳为IP承载网A地（市）AR1与A地（市）AR2链路的互联地址，业务传送路径为A地（市）CE1—A地（市）AR1—A地（市）AR2—B地（市）AR2—B地（市）CE2—B地（市）CE1。

```
<HAZZ-NGN-C  -HWNE40E>tracert -vpn-instance
ChinaM        Media 10.4   02.166
traceroute to  ChinaM        Media
10.4   02.166(10.4   02.166), max hops:30,
packet length:40, press CTRL_C to break
1 10.4.   52.161   6 ms   17 ms  7 ms
2 10.1.   2.2      7 ms   12 ms  5 ms
3 10.4.   03.165   9 ms   17 ms  7 ms
4 10.4.   03.166   9 ms   24 ms  8 ms
5 10.4.   02.166   9 ms   24 ms  8 ms
```

图11　核心层保护方案部署后业务切换路径

当劣化链路恢复后，BFD到达等待时间自动变为up状态，业务传送路径自动回切至原链路进行承载，路径如图12所示。

```
<HAZZ-NGN-C  -HWNE40E>tracert -vpn-instance
ChinaM        Media 10.4   02.166
traceroute to ChinaM        Media
10.4   2.166(10.4   02.166), max hops:30,
packet length:40, press CTRL_C to break
1 10.4   52.161   9 ms   18 ms  9 ms
2 10.4   02.165   7 ms   16 ms  7 ms
3 10.4   02.166   9 ms   24 ms  8 ms
```

图12　核心层保护方案部署后业务回切路径

通过验证数据可知，业务可由原来的A地（市）CE1至B地（市）CE1主链路切换至备用链路传送，当原链路恢复并达到稳定后，业务自动回切至主链路进行承载，切换效果得到了进一步的验证。

4 结语

运营商承载网络双平面组网架构及动态路由协议部署能在一定程度上提高业务容灾性。但在链路误码及传输闪断场景下，仅依靠路由协议收敛特性，将无法快速完成路由切换，从而导致链路丢包或中断，进而影响业务。基于此，本文提出了一种基于BFD协议实现承载网业务毫秒级保护方案。通过部署双向监测机制并合理设置切换规则，可实现路由毫秒级切换，避免链路劣化对业务造成影响。

参考文献：

[1] 张志华，于群. IP承载网的高可靠性技术与实现[J]. 邮电设计技术，2011(7)：60-64.
[2] LAN J L，HU Y X，ZHANG Z，et al. Future network architectures and core technologies[M]. Hackensack：World Scientific，2022.
[3] 贾佳. 面向VoLTE的IP承载网设计思路探讨[J]. 邮电设计技术，2017(7)：74-79.
[4] MAYR C，RISSO C，GRAMPÍN E. Crafting optimal and resilient iBGP-IP/MPLS overlays for transit backbone networks[J]. Optical Switching and Networking，2021，42：100635.
[5] 王丽琼，徐东，张红，等. 本地网县乡WDM问题探讨[J]. 邮电设计技术，2017(11)：51-55.
[6] KATZ D，WARD D. Bidirectional forwarding detection (BFD)[EB/OL].[2024-02-15]. https://www.rfc-editor.org/rfc/rfc5880.html.
[7] AZIZ Z，LIU J，MARTEY A，et al. Troubleshooting IP routing protocols[M]. Hoboken，USA：Cisco Press，2002.
[8] SHUKLA S，KUMAR M. Optimized MRAI timers for border gateway protocol in large networks[J]. International Journal of Distributed Systems and Technologies，2019，10(4)：31-44.
[9] 中国移动通信. 中国移动通信网路由组织规范：IP承载网CE路由组织原则分册：WL-CZ-1-005-LYYZ-2013[R]. 北京：中国移动集团公司，2013.
[10] SATHYASRI B，JANANI P，MAHALAKSHMI V. Redistribution of dynamic routing protocols (Isis，OSPF，EIGRP)，IPvfi networks，and their performance analysis[C]//Recent Trends in Communication and Intelligent Systems. Singapore：Springer Singapore，2021：179-191.
[11] 姜元山，王运付，李佳. 5G CPE传输性能提升研究与实现[J]. 邮电设计技术，2021(7)：27-30.
[12] 杜宇扬. OSPF协议动态配置技术研究[J]. 西安邮电学院学报，2010，15(1)：134-138，147.
[13] 刘春余. 双向转发检测(BFD)关键参数研究[J]. 数字技术与应用，2014(11)：56-57，59.
[14] 泰克教育集团，刘大伟，陈亮，等. HCIE路由交换学习指南[M]. 北京：人民邮电出版社，2017：202-248.
[15] DINI P，HASAN M Z，MORROW M，et al. IP/MPLS OAM：challenges and directions[C]//2004 IEEE International Workshop on IP Operations and Management. Beijing，China：IEEE，2004：1-8.

作者简介：
康琳，毕业于山东大学，高级工程师，硕士，主要从事移动互联网维护工作；张文治，毕业于北京邮电大学，高级工程师，学士，主要从事移动互联网维护工作；郝文胜，毕业于解放军信息工程大学，高级工程师，学士，主要从事移动互联网维护工作；李征，毕业于河南经贸职业学院，高级工程师，主要从事移动互联网维护工作。