附件1

10M MSTP线路并网测试流程

一、测试要求

使用10M MSTP线路接入交易的会员席位均应参加测试，并应做好以下工作：

（一）参试单位应仔细阅读本流程，测试前做好系统和数据备份，测试后恢复备份，防止影响下一交易日的正常业务。

（二）测试中，应认真观察各个场景中交易情况，并注意是否有异常情况。

（三）测试结束后，10M MSTP线路将恢复测试前访问状态，会员仅能访问交易所测试前置，请会员注意切勿将正式系统直接部署到10M线路。

（四）行情商应注意不可将测试行情作为生产数据保存。

（五）参与测试的每个会员，在测试完成后，应各自填写《10M MSTP线路并网测试报告》（附件2），请在2016年4月23日下午17点前将WORD文件email至shfenet@shfe.com.cn，同时将文件盖章后转换成PDF文件在2016年4月26日之前email至shfenet@shfe.com.cn。

二、时间安排

测试日期为2016年4月23日，测试时间安排如下：

（一）08:55至09:00，集合竞价测试；

（二）09:00至11:30，交易测试；

（三）11:30测试结束。

测试用交易数据使用4月22日结算后的合约价格、持仓、保值额度和客户数据，模拟4月25日的交易。

三、场景说明

|  |  |  |
| --- | --- | --- |
| **时间** | **场景说明** | **会员席位注意事项** |
| **测试场景一：模拟测试会员通过10M MSTP线路正常登录交易系统** |
| 8：30前 | 准备测试环境，会员将系统切换至10M MSTP线路。 | 确保10M 线路与交易所通讯正常 |
| 08:55至09:20 集合竞价及连续交易阶段 | 4月23日测试开始 | 会员席位完成系统接入、登录，并进行交易 |
| **测试场景二：模拟测试大厦10M MSTP线路故障，会员切换至张江10M MSTP线路** |
|  9:20线路切换  | 本场景将完成模拟期货大厦10M线路故障情况下，会员席位能否通过张江10M MSTP线路交易。 | 主线路为大厦线路的会员席位连接断开后重连 |
| 9:20至9:40正常交易 | 连续交易，会员检查线路切换情况和席位登录情况是否正常。 | 会员席位再次登录，并进行交易测试。 |
| **测试场景三：模拟测试大厦10M MSTP线路恢复，会员切换至大厦10M MSTP线路** |
| 9:40线路恢复 | 本场景将完成模拟期货大厦10M线路恢复，会员席位切换、主备线路冗余恢复情况。 | 席位断开重连 |
| 9:40至10:00 | 连续交易，会员检查线路切换情况和席位登录情况是否正常。 | 会员席位再次登录，并进行交易测试。 |
| **测试场景四：模拟测试张江10M MSTP线路故障，会员切换至大厦10M MSTP线路** |
|  10:00线路切换  | 本场景将完成模拟张江10M线路故障情况下，会员席位能否通过大厦10M MSTP线路交易。 | 主线路为张江线路的会员席位连接断开后重连 |
| 10:00至10:20 | 连续交易，会员检查线路切换情况和席位登录情况是否正常。 | 会员席位再次登录，并进行交易测试。 |
| **测试场景五：模拟测试张江10M MSTP线路恢复，会员切换至张江10M MSTP线路** |
| 10:20线路恢复 | 本场景将完成模拟张江10M线路恢复，会员席位切换、主备线路冗余恢复情况。 | 席位断开重连 |
| 10:20至10:40 | 连续交易，会员检查线路切换情况和席位登录情况是否正常。 | 会员席位再次登录，并进行交易测试。 |
| **测试场景六：10M MSTP线路停止访问交易前置，会员恢复从原有2M线路登录正常访问交易系统** |
| 10:40线路恢复 | 本场景将停止10M MSTP线路访问交易前置，会员恢复测试前2M 线路，测试线路恢复情况和席位登录情况。 | 会员恢复测试前2M线路，席位断开重连。 |
| 10:40至11:30 | 连续交易，会员检查线路恢复情况和席位登录情况是否正常。 | 会员席位再次登录，并进行交易测试。 |
| **11:30****测试结束** | **会员席位清除测试数据，恢复备份，做好下一交易日工作准备。** |  |

四、通讯参数

我所将使用正式交易系统进行测试，通讯参数如下：

（一） FENS服务器的IP地址为：192.168.11.31、192.168.11.32、192.168.12.41、192.168.12.42、192.168.16.31、192.168.16.32。

（二）使用FENS服务器获取交易前置机地址参数的TCP普通链路端口号为4901，SSL加密链路端口号为4911；使用FENS服务器获取行情前置机地址参数的TCP普通链路端口号为4903，SSL加密链路端口号为4913。

（三）各单位的安全控制策略应打开对192.168.11.X、192.168.12.X、192.168.16.X网段上TCP端口为4901、4911、4903、4913、33005、44305、33011、44311的访问；及对192.168.9.X、192.168.13.X、192.168.17.X网段上TCP端口为80、443、7002的访问。