证联网异地灾备链路应急切换方案

证联网管理办公室

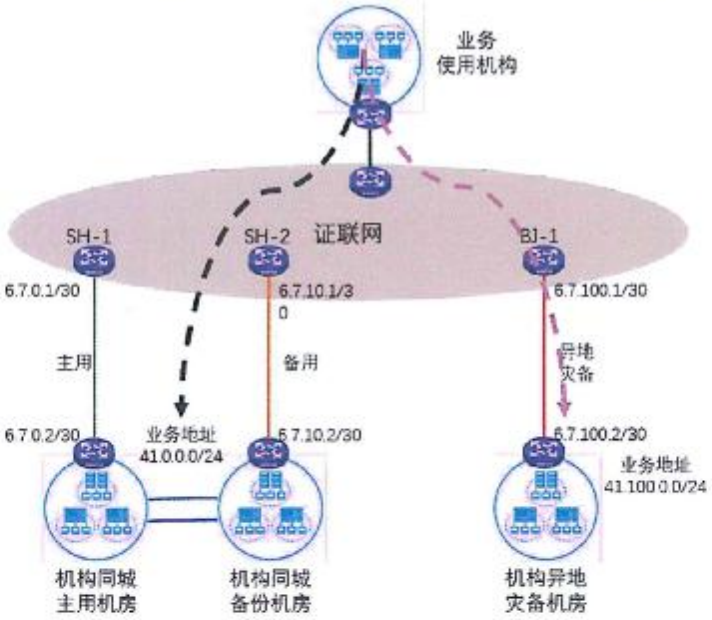
2018.05

一、背景

银证业务在证联网逐步上线，目前工行、农行、建行、交行等18家银行已完成全部上线工作。承载银证业务给证联网安全稳定运行提出了更高的要求。具备两地三中心机房条件的机构已有部分机构申请了异地灾备链路。目前，证联网接入机构共448家，其中有43家证券期货经营机构申请了灾备线路。

二、存在问题

按照证联网设计原则，不同AS域（以接入节点城市区分）具有不同的IP地址池，因此，接入机构同城主备链路业务地址共用一段业务地址，异地灾备链路业务地址分配另外一段业务地址。



如上图所示，正常情况下，业务提供机构使用41.0.0.0/24对外提供服务，当主备链路同时中断或者同城主备系统出现故障时，需要启用异地灾备系统，此时对外提供服务的IP地址将变更为41.100.0.0/24，业务使用机构需要变更应用配置才能访问新的服务

地址。

以银证业务为例，业务地址变更将导致以下问题:

银行端: 银行与多家经营机构有业务交互，比如工商银行与244家经营机构有业务关系，如果工商银行启用异地灾备，需要逐一通知所有244家经营机构进行业务地址切换，异地灾备切换时间长，工作量大，银证业务中断时间长。

证券期货端: 未接入证联网之前，经营机构要启用异地灾备系统时，只需要手动修改NAT配置，不需要通知银行变更IP地址。接入证联网后，如果某证券公司启用异地灾备系统，需要通知银行变更IP地址，银行变更流程长。部分银行银证系统需要重启服务才能变更地址，故交易时间段无法实施变更，会造成该证券公司银证业务长时间中断。

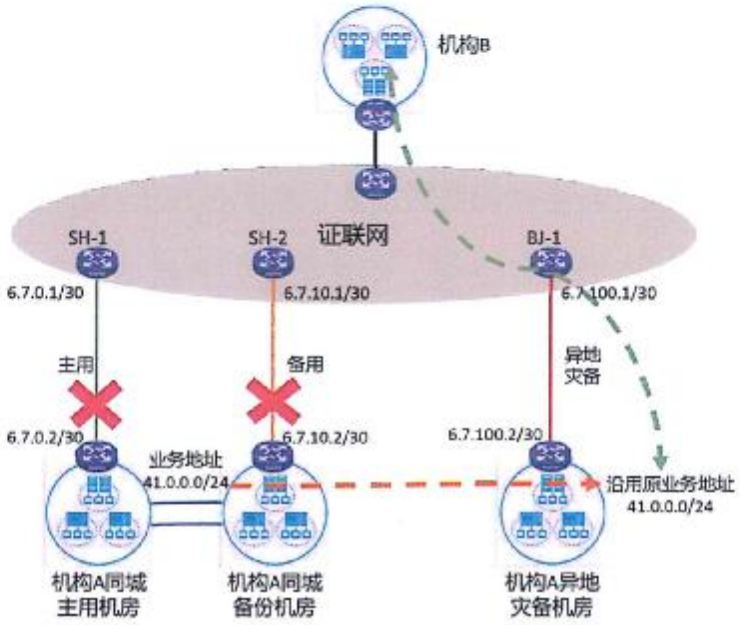
三、解决方案

按照目前的网络结构，机构两条线路一主一备分别接入到证联网同城两个节点，具备灾备环境的，有另一条灾备线路接入到证联网异地节点（如上第二部分附图）。主备线路互为备份，只有当主备线路同时中断时才会触发灾备链路的启用。

由于灾备链路的启用属于小概率事件，结合技术复杂度和变更风险控制考虑，证联网不设计通过修改现网配置、调整路由选路，实现自动切换的方案，而采用当灾难发生后以临时修改配置的应急方式手动切换。

具体方案如下:

1. 故障发生后，证联网取消接入机构业务地址在主备线路的路由发布（线路中断后业务地址路由虽会自动消失，但为防止频繁闪断导致路由翻动的情况，采取将接入端口直接关闭的方式），然后在该机构异地灾备链路的接入路由器发布原业务地址路由。



如上图，当机构 A 主备链路同时中断后，证联网将其业务地址路由 41.0.0.0/24 转移至机构异地灾备机房接入路由器发布。机构 A 灾备机房服务器沿用原业务地址即可与外部通信。机构 B 无需更改自身任何设备配置，待机构 A 的灾备系统启动后即可正常通信。

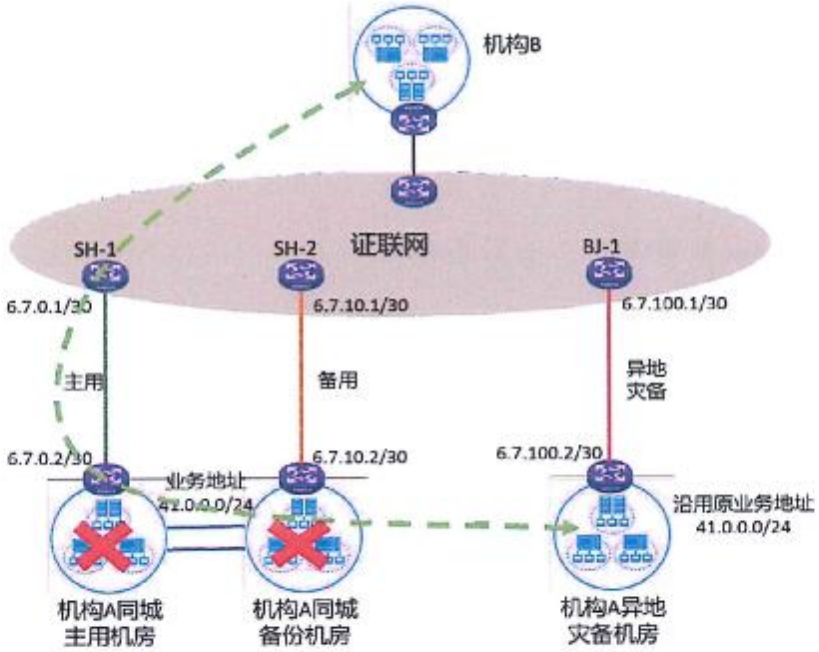
2. 接入机构负责自身灾备系统的部署调试和内部网络变更。

3. 分配给接入机构灾备链路使用的业务地址继续保留，但不建议机构使用此段地址在证联网开展业务。证联网与接入机构在链路两端配置静态路由并与 BFD 关联，用作链路监控。

4. 为减少证联网日常运维的复杂度，当灾备链路启用时，临时配置业务地址段到证联网全网（41.0.0.0/8）的访问策略，故障恢复后

再将其删除。因为各接入机构都有防火墙进行网络隔离，对自身业务进行防护，所以临时开放发生灾难机构访问全网的策略并不会对网络安全造成太大影响。

5. 如果主备线路正常，是由于机构主备机房系统故障需切换至灾备机房的情况，原则上不启用证联网异地灾备链路，机构需要通过调整内部网络配置，将灾备机房的系统流量引向主用线路，证联网将不做网络调整。如机构确实不方便调整路由，证联网也可以配合机构进行灾备链路切换。



四、应急准备

按照上述方案，证联网相关机构平时需做好以下应急准备工作，以减少切换时间，降低故障影响。

证联网运管中心和各承建单位需持续监控灾备链路的连通性，保证故障发生时链路可用；检查灾备链路接入路由器的访问控制策略配置是否规范，并确认是否已在相应接口调用；提供用以受理切换申请

的 7*24 热线和公共邮箱。

接入机构需根据自身情况将异地灾备机房就近接入证联网，并持续监控灾备链路的连通性；提前做好内部路由、防火墙策略及灾备系统规划部署，当故障发生时，可迅速将灾备系统投入使用；准备灾备链路切换的应急预案，确定用以发送切换申请的值班电话和邮箱。

运管中心协调各承建单位与接入机构一起进行切换演练，熟悉操作流程。

五、应急操作步骤

1. 故障定位

（1）通过 ping 检查路由器直连链路是否畅通。

（2）检查主备链路两端的接口配置，BFD 相关配置，通过 display bfd session 查看 BFD 会话是否正常。

（3）通过 display ip routing-table protocol static 检查机构静态路由是否存在。

（4）联系接入机构，询问其同城主备系统是否出现故障，是否无法提供服务。

2. 处理流程

（1）如果是银行链路故障，由银行向运营商报障，并督促运营商尽快解决。相关承建单位检查本节点设备状态，配合银行进行故障处理。若短时间故障无法恢复，银行使用值班电话拨打证联网运管中心热线将情况告知运管中心申请灾备链路切换，并使用专用邮箱将申请发送至运管中心。运管中心收到申请后与相关承建单位沟通，将情

况向证信办汇报，并发起紧急变更申请，协调相关承建单位实施。

（2）如果是行业机构链路故障，由机构向运营商报障，并督促运营商尽快解决。相关承建单位检查本节点设备状态，配合机构进行故障处理。若短时间故障无法恢复，行业机构先将情况告知上级主管部门，然后使用值班电话拨打证联网运管中心热线将情况告知运管中心申请灾备链路切换，并使用专用邮箱将申请发送至运管中心。运管中心收到申请后，与相关承建单位沟通，将情况向证信办汇报，并发起紧急变更申请，协调相关承建单位实施。

（3）如果是接入机构自身主备系统出现故障，原则上不启用证联网异地灾备链路，机构需要通过调整内部网络配置，将灾备机房的系统流量引向主用线路，证联网将不做网络调整。切换完成后，接入机构需将情况告知运管中心。如机构不方便调整路由，也可以向运管中心申请灾备链路切换，具体流程请参照上述说明。

（4）当接入机构故障恢复，需要将线路切回时，由机构使用值班电话拨打运管中心热线申请线路回退切换，并使用专用邮箱将申请发送至运管中心。运管中心收到申请后，与相关承建单位沟通，将情况向证信办汇报，并发起变更申请，协调相关承建单位实施。

3. 变更操作步骤

首先，机构主备线路接入节点手动关闭端口，然后，机构灾备线路接入节点在接入路由器上手动发布机构的业务地址路由，并临时开放访问控制策略。

以接入机构（业务地址段 41.0.0.0/24，主备接入 SH-1 和 SH-2、

灾备接入 BJ-1）为例，具体配置如下：

关闭主备线路端口：

SH-1:

interface GigabitEthernet0/0/1.X　//主线接入端口

shutdown

SH-2:

interface GigabitEthernet0/0/2.X　//备线接入端口

shutdown

在灾备线路上发布业务地址路由，增加访问控制策略条目：

BJ-1:

ip route-static 41.0.0.0 255.255.255.0 GigabitEthernet0/0/1.X 6.7.100.2 bfd control-packet preference 1 description To_xxx_ZaiBei

bgp 65001

network 41.0.0.0 255.255.255.0 route-policy 2000

acl number 3XXX

rule 3XXX permit ip source 41.0.0.0 0.0.0.255 destination 41.0.0.0 0.255.255.255

4. 故障恢复后配置还原

恢复操作需在非业务保障期进行。

接入机构主备链路恢复后，需将业务地址路由切回原主备线路时，机构将切换申请以书面或邮件的形式提交至运管中心。运管中心与相关承建单位沟通后发起一般变更申请，相关承建单位实施，删除

灾备线路接入节点路由器新增的路由配置，再将主备线路接入节点的接入路由器端口恢复启用。

以上述情况为例，具体配置如下：

在灾备线路上取消业务路由发布，删除访问控制策略条目：

BJ-1:

undo ip route-static 41.0.0.0 255.255.255.0

bgp 65001

undo network 41.0.0.0 255.255.255.0

acl number 3XXX

undo rule 3XXX

打开主备线路端口：

SH-1:

interface GigabitEthernet0/0/1.X　//主线接入端口

undo shutdown

SH-2:

interface GigabitEthernet0/0/2.X　//备线接入端口

undo shutdown