# PSI-QOT实施方案

# 1 物理拓扑

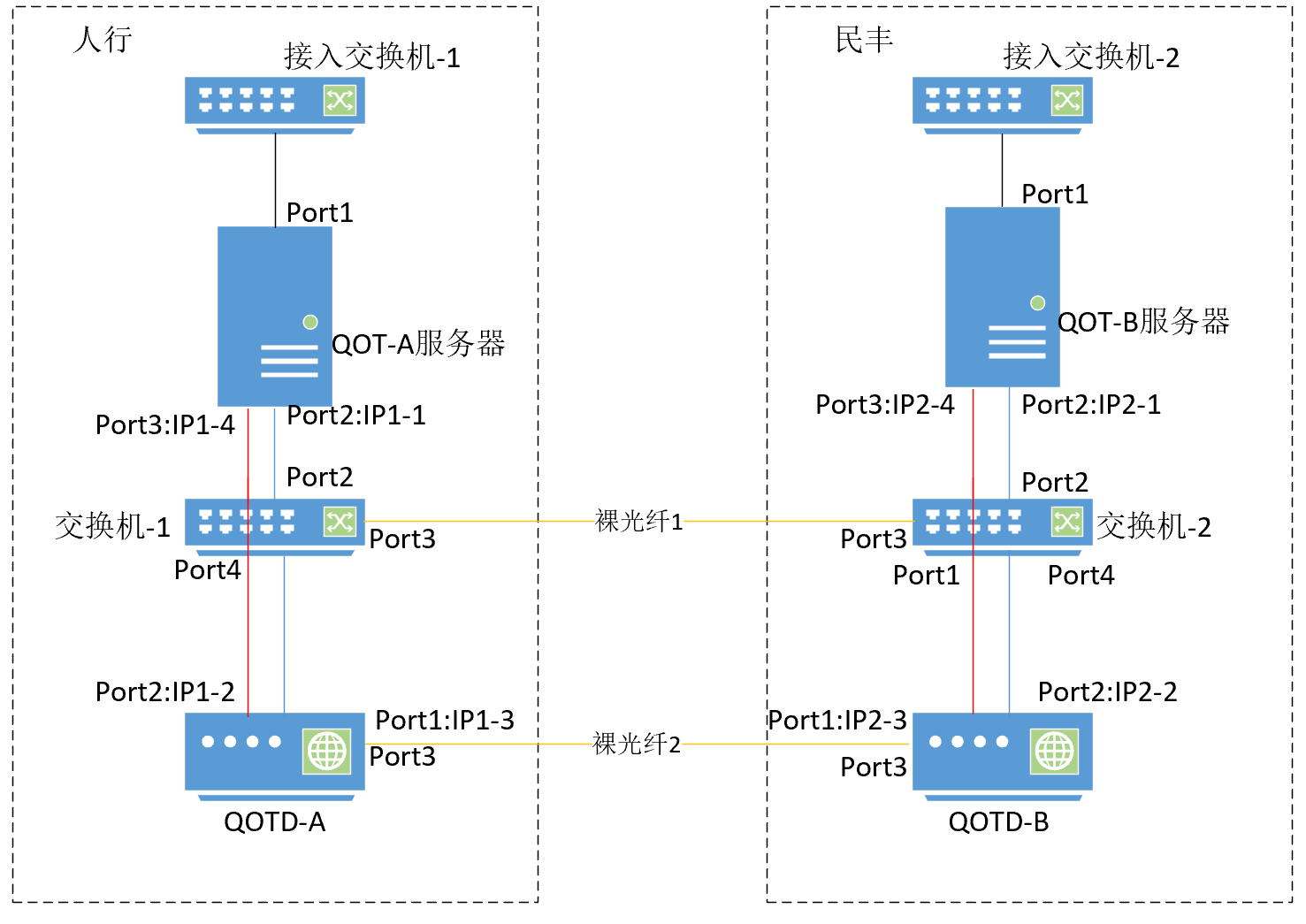


图1 物理拓扑

# 2 计划安排

## 2.1 准备阶段

备注：红色字体为技术人员入场前各方需要做的准备工作；蓝色字体为入场后要做的相关工作。

|  |  |  |
| --- | --- | --- |
| 物理设备 | 宿迁分行、民丰银行 | 成方金科、国科量子 |
| QOT-A/B服务器 | 1、硬件：在各自机房上架通电、确认硬件配置（前期已沟通为曙光H620-G30，配置为E5-2650V4x2/256G内存/600G SATA）；  2、基础环境：安装基础的操作系统（麒麟V10），提前安装基础软件（需准备openssl，1.1版本及以上）；  3、网络：Port1接入内部业务网，能够与原来的反诈系统网络联通，从系统安全的角度考虑，该部分最好能够有访问控制（防火墙）；补充说明：由于安全的考量，两台服务器先不接入业务网； | 1、基础环境：梳理服务器需要安装的基础软件，需准备openssl，1.1版本及以上；  2、网络：Port2分别接入交换机1和交换机2，配置内网地址； |
| 交换机-1、交换机-2 | 1. 准备好裸光纤1； 2. 提前确认是否有进场手续要求，配合做好设备的进场（每个节点会上架1台1U的交换机）。 | 1. 入场时由技术人员带入并做好相关配置。 2. 由国科准备一对单芯双向光模块。 |
| QOTD-A/B | 1. 准备好裸光纤2，要求40km以内，光衰10db以内，LC接口，单模； 2. 提前确认是否有进场手续要求，配合做好设备的进场（每个节点会上架1台1U的QKD设备）。 | 1. 入场时由技术人员带入并做好相关配置； 2. 网络配置由入场技术人员来做，全部配置为内部IP地址。 |

## 2.2 现场实施

|  |  |  |
| --- | --- | --- |
| 任务标号 | 任务描述 | 备注 |
| 1 | 设备上架加电（QOTD+交换机） | 设备分配规则为，以民丰银行作为PSI的发起端和结果的获取方。 |
| 2 | QOTD、交换机设备连接光纤，配置网络基础环境 |  |
| 3 | QOT设备连接交换机配置网络，QOTD和QOT的联通测试 |  |
| 4 | QOT软件部署 | 参见第5节“软件部署和测试”的具体步骤 |
| 5 | 任务1-4先在人行端执行，完成后在民丰银行重复任务1-4 |  |
| 6 | 两端的联通测试 |  |
| 7 | PSI、QOT的功能和性能测试 |  |
| 8 | 业务测试 | 场景：人民银行端取涉案名单（大约为1w条），民丰银行取7天内的开卡数据（大约为3k），民丰发起查询的任务，查看开发人员是否在涉案名单中。  （业务人员按照csv格式准备真实数据） |

# 3 基础物理环境说明

本次实施范围包括以下硬件设备：

1、QOT-A及QOT-B服务器，执行QOT经典协商功能，所运行的服务器由本地人行准备；

2、交换机1及交换机2，连接QOTD与QOT，以及两机房间的一芯光纤，交换机设备及光模块国科准备；

3、QOTD，QOT传输设备，国科提供。（QOTD人行为Alice，民丰为Bob）

4、接入交换机1及接入交换机2：若本次测试需要与其他系统对接通信，建议在服务器选取另外一个接口（Port1）接入所在测试网络区域的接入交换机，接入交换机默认为本地机房已有设施。

本次实施在传输链路方面需要准备如下：

1、光纤1，由单芯双向光模块，在交换机-1-Port3和交换机-2-Port-3之间使用光口做物理直连，用于经典通信，由本地人行准备。

2、光纤2，QOTD-A及QOTD-B之间做物理直连，为量子信道传输量子信号使用，由本地人行准备。

3、网线若干，其余经典交换机与服务器、QOTD设备间的链路使用以太口做物理连接即可，由国科准备。

# 4 接口、IP及路由

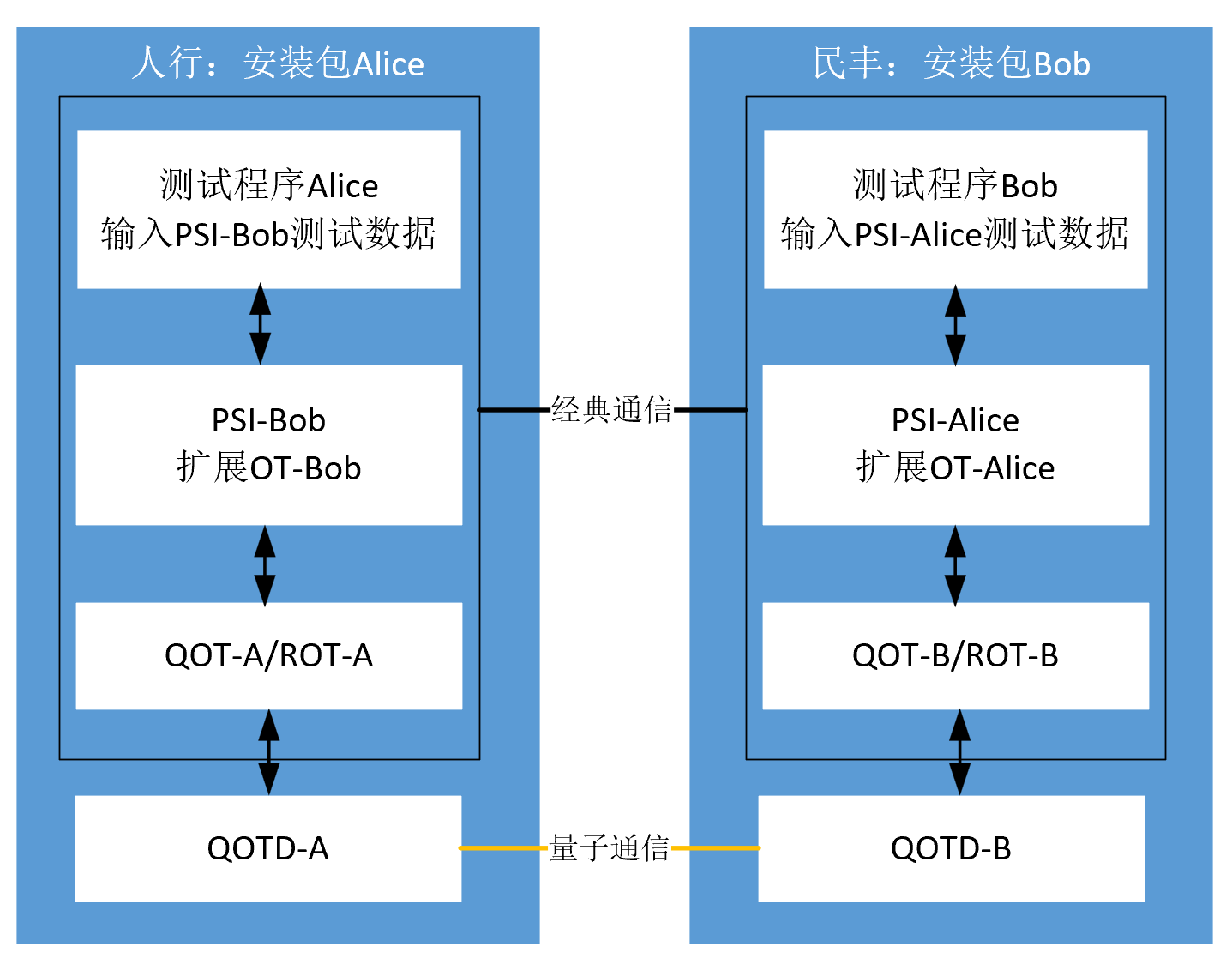
|  |  |  |  |
| --- | --- | --- | --- |
| 人行 | | | 说明 |
| 设备名称 | 接口 | IP |  |
| QOT-A服务器 | Port2 | 172.31.234.11/24 | QOT-A与QOTD-A连接及与对端QOT-B通信的IP |
| Port3 | 172.31.235.11/24 | QOT-A与QOT-B通信的IP |
| QOTD-A | Port2 | 172.31.234.113/24 | QOTD-A与QOT-A通信的IP |
| 民丰银行 | | |  |
| 设备名称 | 接口 | IP |  |
| QOT-B服务器 | Port2 | 172.31.234.12/24 | QOT-B与QOTD-B连接及与对端QOT-A通信的IP |
| Port3 | 172.31.235.12/24 | QOT-B与QOT-A通信的IP |
| QOTD-B | Port2 | 172.31.234.114 | QOTD-B与QOT-B通信的IP |

人行和民丰银行对测试环境的IP地址使用没限制，QOT服务器Port2接口及QOTD的Port2接口四个IP地址在同一网段。QOTD的经典通信IP地址设置任意直连地址即可。

为实现对PSI通信量的统计，第二轮测试服务器新增Port3接口用于服务器间通信，与服务器和QOTD设备间通信接口隔离，使用vnstat工具统计Port3网卡通信量。对应交换机需将不同网段接口做vlan隔离。

# 5 软件部署和测试

按照2.2章节表格第8项描述业务测试需求，民丰银行作为PSI的发起端和结果获取方，对应PSI的Alice角色，按照系统PSI和OT角色对应关系，民丰银行部署QOTD-B，人行方作为PSI的Bob，部署QOTD-A ，整体软件和硬件部署角色对应关系如下：



## 5.1 docker环境

1、准备x86架构的docker离线部署文件。

2、执行部署脚本

## 5.2 QOT测试程序部署

1、准备QOT测试程序部署文件qot\_random.zip。

2、将部署文件上传至服务器内并解压。

3、修改配置文件。

qot\_config\_a.ini 和qot\_config\_b.ini 为qot的配置文件。config\_a.ini和config\_b.ini为QOTD设备的配置文件。

测试程序使用：

程序启动：./qot\_qkd\_test <party> <port> <ServerIp/peerid> <RequestLen> <SleepSecond>

Part：1或者2。1时为主动端，2时为从端。

Port：主端的监听端口号或者为从端的连接端口号。

ServerIp/peerid：主端时，填写对端的设备号；从端时填写主端的服务器的连接IP。

RequestLen：申请长度，512字节的整数倍。

SleepSecond：连续申请时的时间间隔，单位为（s）。

注： 从端会将获取到的测量基底和量子比特发送给主端，用于计算测量基底的正确率及量子比特的正确率。

QOT测试程序也可以放到PSI容器里执行测试，但由于容器里的OpenSSL版本和服务器不一致，需要替换其中一个动态链接库libqot.so。

## 5.3 PSI容器化部署

**方式一：整体部署**

整体部署是通过包含了psi运行环境、psi依赖包、psi源码、psi集成qot测试程序等所有内容的psi镜像文件进行容器化部署，启动容器后可直接在容器里执行测试程序。部署步骤如下：

1. 准备整体部署的docker镜像文件 psi-1.1.tar。
2. 导入docker镜像文件。

docker load -i psi-1.1.tar

1. 通过镜像创建并启动容器。

docker run -itd --name psi --security-opt seccomp=unconfined --network=host psi

**方式二：拆分部署**

由于psi-1.1.tar文件有75G左右大小，性能较差的服务器环境下直接导入该镜像文件可能会导致docker服务崩溃。针对这种清空，可选择拆分部署。将镜像中内容较大的psi依赖包和集成QOT部分的自定义文件拆分出来，减少镜像文件的大小，待导入镜像并启动容器后再通过文件传输导入容器内，再进行测试。部署步骤如下：

1. 准备镜像文件psi-1.0.tar、psi依赖包cache\_bazel.tar.gz和集成QOT程序文件core\_src\_20240314.tar。
2. 导入docker镜像文件。

docker load -i psi-1.0.tar

1. 通过镜像创建并启动容器。

docker run -itd --name psi --security-opt seccomp=unconfined --network=host psi

1. 将psi依赖包和集成QOT程序文件导入容器。

docker cp {主机文件目录}/cache\_bazel.tar.gz psi:/root/.cache/

docker cp {主机文件目录}/core\_src\_20240314.tar psi: /home/psi/psi/psi/core/

1. 进入容器。

docker exec -it psi bash

1. 解压psi依赖包。

cd /root/.cache/

tar -zxvf cache\_bazel.tar.gz

1. 解压集成QOT程序文件。

cd /home/psi/psi/psi/core/

tar -zxvf core\_src\_20240314.tar

1. 修改配置文件。

PSI的测试程序位于 /home/psi/bazel-bin/psi/psi/core 目录下。qot\_config\_a.ini 和qot\_config\_b.ini 为qot的配置文件。config\_a.ini和config\_b.ini为QOTD设备的配置文件。kkrt\_psi\_config.ini 为kkrt\_psi的配置文件。

## 5.4 执行测试脚本

**QOTD 设备功能测试。（服务器上即可）**

测试程序：qot\_qkd\_test

测试目的：

1、配置文件是否正常。

2、QOTD设备功能正常。

3、测试误码率是否达标。

4、测试获取量子比特和基底的性能情况。

测试方法：两端改好配置，启动程序，注意日志。

**（二）QOT功能测试。（服务器上即可）**

测试程序：qot\_test

测试目的：

1、在QOTD设备功能正常的基础上，测试QOT协议执行以及ROT协议执行的正确性。

2、测试QOT以及ROT的性能。

测试方法：两端改好配置，启动程序，注意日志。

**（三）PSI功能测试。（docker容器内）**

测试程序：kkrt\_psi\_test\_a 和kkrt\_psi\_test\_b

测试目的：

1、在QOT功能以及ROT功能正常的基础上，测试KKRT\_PSI协议执行的正确性。

2、测试KKRT\_PSI的性能。

测试方法：两端改好配置，启动程序，注意日志。