

## 项目概况

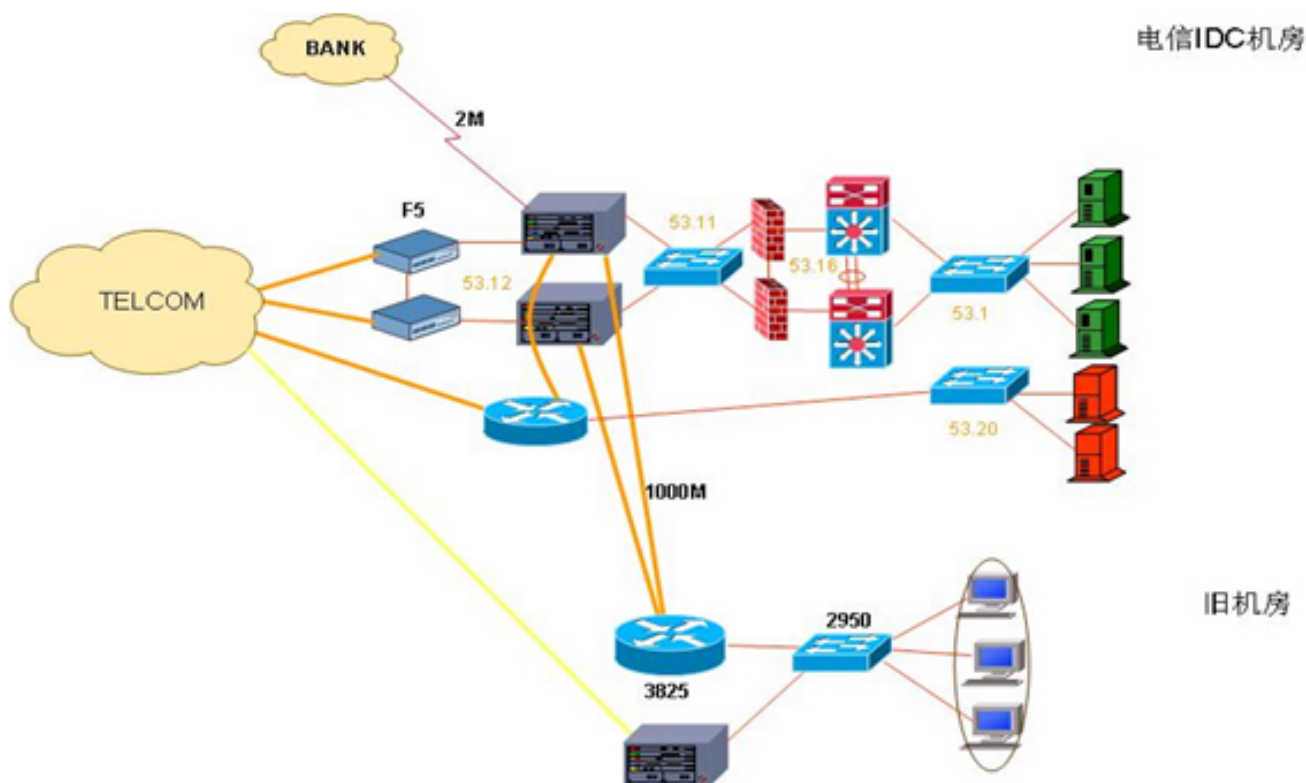
各彩票点是通过VPDN拨号的方式连接到后台的彩票系统，进行彩票的选号，购买，打印等操作。

单台VPDN路由器存在单点故障及负载瓶颈，一旦出现故障或者超过VPDN路由器的处理能力，将引起彩票系统瘫痪。

对外单条运营商链路也存在单点故障问题

## 网络结构

## Network Diagram



## 客户需求

- ☆ 采用负载均衡设备对两台VPDN路由器流量分配，尽量使负载均衡。
- ☆ VPDN路由器需要向外部的Radius服务器验证拨号用户。
- ☆ VPDN路由器设置的地址为私网地址。
- ☆ 两条电信的链路做到负载均衡，流量尽量平均。

## 解决方案

- ☆ 采用BIG-IP LTM对多台VPDN路由器进行负载均衡
- ☆ 同运营商的链路速度上不存在很大的差异，因此不需要用到LC或3DNS来做链路负载均衡
- ☆ 对Inbound访问，由电信端的路由器进行路由分发做到均衡，对Inbound访问,F5 BIG-IP LTM用轮询的方法即可以实现较好的均衡。
- ☆ BIG-IP LTM对每台VPDN设备的服务端口进行健康检查，当某台设备VPDN服务发生故障，则停止该台设备的工作。
- ☆ 电信端路由器和F5 BIG-IP LTM同时对两条链路进行健康检查。当某条链路出现故障时，电信端路由器和F5 BIG-IP LTM将会识别到，不会再向该条链路发送数据
- ☆ 将VPDN路由器的VIP地址在Radius上注册为NAS地址。

## 为什么选择F5

- ☆ 稳定性：BIG-IP LTM完善的冗余和实际应用中的稳定性是保证项目成功的决定性因素。福利彩票VPDN路由器的能否正常工作决定了彩票点能否正常开展投注业务，因此负载均衡设备相应成为业务支撑的关键，需要很高的稳定性。
- ☆ 灵活性：F5设备在配置上的灵活性，保证设备能够适应于一些非标准的网络结构，并能够正确的工作。
- ☆ 成功案例：对福彩VPN系统的负载均衡在其它省市采用F5设备成功地实施过，因此对F5产品有着比较高的信任度。

## 关键技术阐述

- ☆ 如何配合电信路由器做Inbound访问链路负载均衡？

电信有两条链路，假设VIP是属于某条链路的地址，那么流量将都经过这条链路，无法均衡。因此VIP地址必须设为一个不同于两条链路的第三网段的地址。这样电信路由器将可以设置路由的分发策略。

- ☆ 关于F5上多条链路的配置建议

在福利彩票的应用中，同运营商的多条链路一定要划分为一个VLAN。在多条VLAN上配置多个网段的地址即可。原因是BIG-IP LTM的SNAT表是基于VLAN来建的。如果两条链路划分为两个VLAN，系统的处理将出现问题，以下为一个过程描述（假设两条链路分别为link1, link2,两台VPDN路由器分别为route1,route2）：

- 1) 彩票投注站VPDN拨号,F5 BIG-IP LTM从link1收到请求
- 2) BIG-IP LTM根据负载均衡算法将请求分配给其中一台VPDN路由器（假设为route1）
- 3) Route1 向外部Radius路由器请求验证用户，请求包通过BIG-IP LTM的link1发到Radius,此时在link1上建立了一个SNAT表
- 4) Radius 返回应答，BIG-IP LTM从link2收到Radius应答，link2上并没有当次请求的SNAT表，因此如果vip配置的是某个服务端口，BIG-IP LTM将把该应答包丢弃。如果vip配置的服务器是0也就是任意服务，BIG-IP LTM将把该应答根据负载均衡算法

分配，这个时候可能另一台VPDN路由器（route2）将收到应答包。

5) 最终的结果将是route1没有收到验证应答包，验证失败，从而拨号失败，系统无法工作。

#### ☆ VPDN路由器Radius请求包的内容及BIG-IP LTM SNAT地址的设置

由于VPDN路由器通过F5 BIG-IP LTM做了负载均衡，因此VPDN路由器在构建Radius请求包的时候，有个Nas-IP的选项要设置成VIP的地址，同样BIG-IP LTM在转发请求包的时候要转换成VIP的地址转发出去。否则Radius在验证时将报告错误，具体的细节可以通过tcpdump抓包验证。

#### ☆ 关于某条链路断掉后，无法拨号成功的处理

F5设备对连接有一定的保持时间，BIG-IP LTM会对client访问VIP然后选择某台服务器建立一个连接表。当某条链路断掉后，如果原有连接没有超时，由于同一连接的持续性问题，F5将不能对客户新的拨号请求进行应答，所以当客户的链路断掉要想再次拨入，只能等待连接超时。然而客户端在连接超时前会不停的重拨，这样就使得连接时间不停的更新。因此必须清除连接才能解决这个问题。清除连接有两种方法：一种是在active设备上删除连接，另一种是切换到另一台设备。然而本项目网络的连接方式无法根据VLAN来进行切换，所以只有用脚本检查，在某条链路down的时候清除连接，脚本如下：

```
#!/bin/sh
statfile=/usr/local/node_stat/$1"_statfile"
b node $1 | sed -e 's/ / /g' | awk '{print $3}' | while read nodestat
do
if [ $nodestat = "UP" ]
then
echo "UP">$statfile
exit
else
if [ $nodestat = "DOWN" ]
then
if [ -f $statfile ]
$stat=`cat $statfile`
if [ $stat = "UP" ]
then
b conn all delete
echo "DOWN">$statfile
exit
else
```

```
exit  
fi  
else  
echo "DOWN">$statfile  
b conn all delete  
exit  
fi  
fi  
fi  
done
```

最后在crontab里设置每分钟调用一次该脚本，对两条链路进行检查