

金融pos与前置机无法正常通讯案例

R2621配置6fcm模块通过pstn网络连接pos机，通过以太网口与前置机以tcp方式连接，配置如下：

Now create configuration...

Current configuration

```
!  
version 1.74  
pos-server enable  
pos-server app tcp 0 192.168.20.3 50000  
pos-server map default 0  
firewall enable  
aaa-enable  
aaa accounting-scheme optional
```

!

```
interface Aux0  
  async mode flow  
  link-protocol ppp
```

!

```
interface Ethernet0  
  ip address 192.168.20.1 255.255.255.0
```

!

```
interface Serial0  
  link-protocol ppp
```

!

```
interface Serial1  
link-protocol ppp
```

!

```
interface FCM0  
  async mode pos 1  
  link-protocol ppp
```

!

```
interface FCM1  
  async mode pos 2  
  link-protocol ppp
```

!

```
interface FCM2  
  async mode pos 3  
  link-protocol ppp
```

!

```
interface FCM3  
  async mode pos 4  
  link-protocol ppp
```

!

```
interface FCM4  
  async mode pos 5  
  link-protocol ppp
```

!

```
interface FCM5  
  async mode pos 6  
  link-protocol ppp
```

!

return

**故障现象：**pos机与前置机之间无法通讯

**处理过程：**

1. 打开debug开关，debugging pos - interface和debugging pos - app，

输出调试信息如下:

Interface FCM2 is DOWN  
Interface FCM0 is UP

---

POSINTorAPP: POS1  
PACTYPE: pos\_packet  
FAILEDTYPE:  
STX:  
BCD(HEX):  
TPDU: 60 00 00 00 00  
ETX:  
LRC:  
PACKET: [Length:45 ]  
60 00 00 00 00 60 21 00 00 00 00 08 00 36 0E 36 36 36 F6 3E 36  
00 00  
38 16 05 17 05 19 30 33 30 30 31 30 38 37 30 35 31 32 32 34 30  
30

---

POSINTorAPP: APP0  
PACTYPE: pos\_packet  
FAILEDTYPE:  
STX:  
BCD(HEX): 00 2D  
TPDU: 60 00 00 00 01  
ETX:  
LRC:  
PACKET: [Length:47 ]  
00 2D 60 00 00 00 01 60 21 00 00 00 00 08 00 36 0E 36 36 36  
F6 3E 36  
00 00 38 16 05 17 05 19 30 33 30 30 31 30 38 37 30 35 31 32 32  
34 30  
30

---

[Router]d\_\_[\_1Ddebugging pos-app\_[17D  
\_17Ddebugging pos-interface  
[Router]  
Interface FCM0 is DOWN  
Interface FCM1 is UP

---

POSINTorAPP: POS2  
PACTYPE: pos\_packet  
FAILEDTYPE:  
STX:  
BCD(HEX):  
TPDU: 60 00 00 00 00  
ETX:  
LRC:  
PACKET: [Length:45 ]  
60 00 00 00 00 60 21 00 00 00 00 08 00 36 0E 36 36 36 F6 3E 36  
00 00  
39 16 06 22 05 19 30 33 30 30 31 30 38 37 30 35 31 32 32 34 30  
30

---

```

POSINTorAPP: APP0
PACTYPE: pos_packet
FAILEDTYPE:
STX:
BCD(HEX): 00 2D
TPDU: 60 00 00 00 02
ETX:
LRC:
PACKET: [Length:47]
00 2D 60 00 00 00 02 60 21 00 00 00 00 08 00 36 0E 36 36 36
F6 3E 36
00 00 39 16 06 22 05 19 30 33 30 30 31 30 38 37 30 35 31 32 32
34 30
30

```

正常情况下一笔交易的debug信息是四段报文，在做第一笔交易时出现五段报文，是因为路由器收到报文并向前置机发送报文时，TCP/IP连接还没有建立起来，这时报文会缓存起来，等连接建立之后，报文继续发送，因此多显示一次报文，以后的交易中就只有四段报文了。四段的顺序为：

pos接口（下行）收到的pos机的POS报文（pos—packet）  
 》pos应用（上行）向前置机发送的POS报文（pos—packet）  
 ——》pos应用（上行）收到的前置机发送的应用报文（app—packet）  
 ——》pos接口（下行）向POS机发送的应用报文（app—packet）

从上面的调试信息可以看出，只有pos机发给路由器fcm卡的报文，和路由发给前置机的报文，但是没有前置机发回路由器的报文。

## 2. 在前置机进行抓包查看，前置机收到路由来的报文

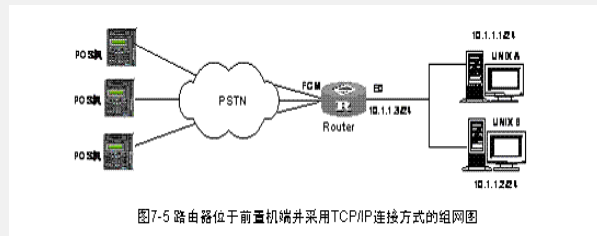


图7-5 路由位于前置机端并采用TCP/IP连接方式的组网图

### 前置机发给路由的报文

8	3.239714	192.168.20.1	192.168.20.3	TCP	1044 > 50000 [PSH, ACK] Seq=1396601747 Ack=3802141569
9	3.296004	Realtek_S_00:12:fc	Broadcast	ARP	who has 192.168.20.1? [R] 192.168.20.3
10	3.296159	Huawei_Fc_29:3a:39	Realtek_S_00:12:fc	ARP	192.168.20.1 % at 00:00:00:00:00:00
11	3.296280	192.168.20.3	192.168.20.1	TCP	50000 > 1044 [PSH, ACK] Seq=3802141569 Ack=1396601794
12	3.329142	192.168.20.1	192.168.20.3	TCP	1044 > 50000 [ACK] Seq=1396601794 Ack=3802141637 Win=0
13	3.903925	192.168.20.3	192.168.20.255	NBNS	Registration NB SUN-NB<f>
14	4.656627	192.168.20.3	192.168.20.255	NBNS	Release NB SUN-NB<f>
15	4.805483	Realtek_S_00:12:fc	NETBIOS-	NETBIOS Add Name Query - SUN-NB<f>	
16	5.305900	Realtek_S_00:12:fc	NETBIOS-	NETBIOS Add Name Query - SUN-NB<f>	
17	5.406349	Realtek_S_00:12:fc	NETBIOS-	NETBIOS Name Query For SUN-NB<2>	
18	5.406360	Realtek_S_00:12:fc	Realtek_S_00:12:fc	NETBIOS Name Recognized - SUN-NB<2>	
19	5.406377	Realtek_S_00:12:fc	Realtek_S_00:12:fc	NETBIOS Name Query For SUN-NB<2>	
20	5.806620	Realtek_S_00:12:fc	NETBIOS-	NETBIOS Add Name Query - SUN-NB<f>	
21	6.107703	192.168.20.3	192.168.20.255	NBNS	Registration NB SUN-NB<f>

# Frame 8 (113 bytes on wire, 113 bytes captured) on interface 0  
 # Ethernet II, Src: 00:00:0c:12:fc:39, Dst: 00:00:00:00:00:00  
 # Internet Protocol, Src Addr: 192.168.20.1 (192.168.20.1), Dst Addr: 192.168.20.3 (192.168.20.3)  
 # Transmission Control Protocol, Src Port: 1044 (1044), Dst Port: 50000 (50000), Seq: 1396601747, Ack: 3802141569, Len: 47 (47 bytes)

```

0000  00 e0 4c 00 12 fc 00 e0 fc 29 3a 39 08 00 45 00  .L...:..E.
0010  00 63 0e ab 00 00 00 06 c2 95 c0 a8 14 01 c0 a8  .C...#.....
0020  14 03 04 14 14 15 19 73 99 a0 80 18 01 80 18    ....PSH S.....
0030  28 a0 fa 01 00 00 01 01 08 03 00 01 69 fa 00 00  ....
0040  b4 a1 20 2d 60 00 02 80 44 60 21 00 00 00 00 08  .....D.....
0050  00 00 00 36 36 36 36 36 00 00 00 00 12 04 68  966666 36...
0060  19 30 35 30 30 31 30 36 37 30 35 31 32 32 34 30  9802108 7051240
0070  88

```

由此可以看出前置机收到了路由发过来的报文，并且已向路由回复报文，但是路由器于某种原因没有处理并转发

### 3. 把pos机发来的报文与前置机抓包得到的报文部分进行对比

报文发送：02 00 2D 60 00 04 80 44 60 21 00 00 00 00 08 00 36 0E 36 36 36 F6 3E 36 00 15 41 10 08 01 05 19 30 33 30 30 31 30 38 3 7 30 30 31 30 30 51 30 31 03 0A

报文接收：00 2D 60 00 04 80 44 60 21 00 00 00 00 08 00 36 0E 36

36 36 F6 3E 36 00 15 41 10 08 01 05 19 30 33 30 30 31 30 38 37 3  
0 30 31 30 30 51 30 31

**发现pos机发出的报文经过路由处理转发后少了第一个字节和后两个字节**

**因为路由器与前置机之间有两种连接方式tcp\异步模式，它们的报文格式分别为：**

tcp格式：

两个字节的长度 + tpdu + iso8583

异步格式：

0x02开头 + 两个字节的长度 + tpdu + iso8583 + 0x03+crc

**可以得出结论：**

**前置机的报文格式错误，它封装的异步模式，而路由器为tcp连接方式，**

**将报文格式修改为tcp格式后正常（将第字节和尾部两字节去掉）**