金融pos与前置机无法正常通讯案例

贾文宇 2006-05-24 发表

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，
前置机收到路由发来的报文

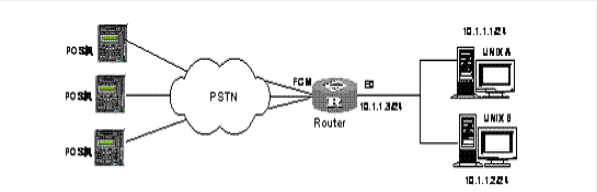
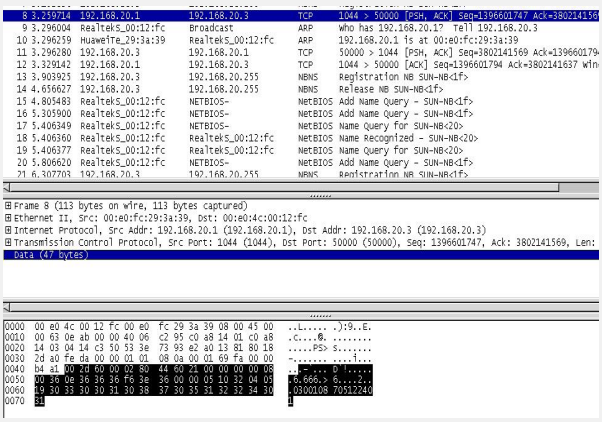


图7-5 路由器位于前置机端并采用TCP/IP连接方式的组网图

前置机发给路由的报文



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 37 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）**