

# 一种高可靠可控双冗余以太网的设计与实现

王一茗 张可 陈龙

(电子科技大学电子科学技术研究院 成都 611731)

**摘要** 提出了一种高可靠可控双冗余以太网架构方案,其通过在两个网卡上发送内容相同的数据包,防止出现网络丢包时的信息丢失。在以太网的用户数据头部添加帧冗余标签用于标识冗余和非冗余数据以及区别冗余数据的不同帧,当网络出现故障时,可以达到零故障恢复时间。引入网络诊断功能,通过节点间的软件收发和处理诊断相关的 UDP 报文来判断网络是否出现故障,并及时记录。通过 Winsock SPI 和 API 实现网络的冗余通信和诊断功能,以保持对应用层网络程序透明,同时又保证网络的高可靠性和可用性。实验表明,在局域网内可以容忍多个不同节点到交换机的故障,增加网络发送的数据量,以实现较高的容错率。

**关键词** 双冗余,以太网,高可靠,网络诊断

**中图分类号** TP393.11 **文献标识码** A

## Design and Realization of High-available Controlling Integrated Double-redundant Ethernet Scheme

WANG Yi-ming ZHANG Ke CHEN Long

(Research Institute of Electronic Science and Technology, University of Electronic Science and Technology of China, Chengdu 611731, China)

**Abstract** This paper presented a scheme of highly-available, controllable redundant Ethernet, which sends same data packets through two network cards to avoid losing information when packets lost in the network. A frame redundancy label is added before Ethernet user data, used for marking redundant and irredundant data and distinguishing different frame from redundant data, which can reach zero recovery time when network problems happen. Network diagnosis is introduced in the scheme, which monitors network's state through the software in the nodes sending, receiving and dealing with UDP messages. Winsock SPI and API are used respectively for achieving redundant communication and network diagnosis, in order to keep transparent to the application layer as well as guarantee the network's high availability and usability. Experiment shows that the LAN can tolerate multi-problems from nodes to switches, increase the data sent in the network and consequently achieve higher fault tolerance.

**Keywords** Double redundancy, Ethernet, High availability, Network diagnosis

## 1 引言

以太网具有传输速度快、低耗、易于安装和兼容性好等方面的优势,并支持几乎所有流行的网络协议,所以多年来被广泛采用。传统的以太网采用总线式拓扑结构,在条件较为恶劣的工业环境中,网络的故障可能会引起大范围的网络瘫痪,因此对以太网的研究具有工程实用价值。在很多工业应用中,要求网络具有零故障恢复时间,现在普遍使用网络冗余来增加网络的可靠性<sup>[1]</sup>。然而,以太网协议和 TCP/IP 协议本身未定义冗余通信方式,因此冗余以太网通信得到广泛研究。

IEC 62439-3<sup>[2]</sup>提出了两种可行的增加网络冗余的解决方案:网络内部冗余和冗余至终端节点<sup>[3]</sup>。网络内部冗余方式有冗余的链路和交换机,但是节点只有一个端口连入交换机,网络是部分冗余的,并且通常处于非活动状态,所以引入了故障恢复延迟。冗余至终端节点方式中终端节点有额外的通信链路,并行网络或路径提供了高可靠性和零故障恢复时

间,从而能够满足一些特殊场合的应用。

冗余协议通常分为两类,第一类是动态冗余管理,此时冗余实体只会在网络发生故障时工作,比如生成树协议(STP)、快速生成树协议(RSTP)<sup>[4]</sup>以及 IEC 提出的介质冗余协议(MRP)<sup>[5]</sup>。这些协议正常工作时通过阻塞有环路的节点的一条链路来避免环路,故障发生后启用被阻塞的冗余通路,从而尽量减少故障恢复时间<sup>[6]</sup>。另一类是静态冗余,此时冗余实体与正常网络同时工作,例如并行冗余协议(PRP)<sup>[7]</sup>和高可靠无缝冗余(HSR)<sup>[8]</sup>。PRP 在第二层引入冗余机制,从而对上层的协议保持完全透明<sup>[9]</sup>。其双连接节点同时使用两个相互独立的网络传输数据,从而保证零故障恢复时间<sup>[10]</sup>。HSR 常用于环型拓扑,在两条独立的物理路径上发送重复数据帧,保证零故障恢复时间。其与 PRP 相比成本更低,但是容易造成网络拥塞<sup>[11]</sup>。

国内的研究机构和企业也积极地致力于网络冗余技术的研究。浙江大学、浙大中控集团以及中科院沈阳自动化所等

收稿日期:2013-07-01 返修日期:2013-10-21 本文受航空科学基金项目(20110580002)资助。

王一茗(1989—),男,硕士生,主要研究方向为以太网与信息处理,E-mail:wym320@126.com;张可(1979—),男,副研究员,CCF 高级会员,主要研究方向为传感器网络、计算机网络等;陈龙(1988—),男,硕士生,主要研究方向为高可靠以太网技术。

单位制定了基于工业以太网的实时通信控制系统解决方案——EPA 标准。2007 年 8 月, EPA 标准被正式列入现场总线国际标准 IEC61158(第 4 版)。对于环形网络,它是基于专利的主动并行故障探测技术,分散了故障风险,大大缩短了环形网络自愈时间<sup>[12]</sup>。同时,参与国内 EPA 标准和技术开发的核心单位对以太网的冗余技术进行了深入研究,于 2006 年提出了分布式冗余协议(Distributed Redundancy Protocol, DRP),并于 2010 年将其编入 IEC62439-6 标准<sup>[13]</sup>。

上述方案普遍在较低层加入冗余处理层,不能对节点的收发通路选择进行控制,且实现起来比较复杂,特别是对于中小型的局域网。研究提出一种高可靠可控双冗余以太网设计,在应用层下加入冗余处理层,可以在原先协议的基础上方便地进行改进,同时还能实现节点收发通路的自由控制。通过在冗余模式下收发重要的数据,避免丢包带来的数据丢失。牺牲一些带宽来增加冗余,达到提高网络可靠性的目的,同时对用户透明。此外加入网络诊断功能,能够及时发现和定位网络故障,进一步提高以太网的可靠性。

## 2 冗余以太网架构设计

### 2.1 网络拓扑结构

使用冗余至节点的方式,网络拓扑结构的设计采用星型网络与环型网络相结合的方法。如图 1 所示,以太网交换机之间采用环形总线的方式进行互联,而节点以星型连接的方式连入交换机环的端口,形成星型-环型拓扑结构。该系统的核心包括:几组以太网交换机以及负责数据收发的网络节点等。

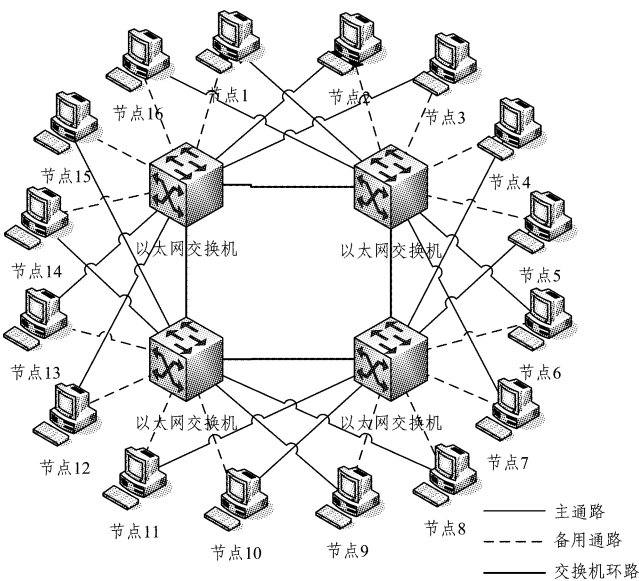


图 1 网络拓扑结构

节点代表工作的主机,内部配置双网卡;以太网交换机是基于以太网传输数据的交换机,其结构是每个端口都直接与主机相连,并且一般都工作在全双工方式。交换机能同时连通许多对端口,使每一对相互通信的主机都能无冲突地进行数据传输。

从网络拓扑图中可以看出,节点通过两条通路分别与两个相邻的交换机相连,从而减少了共享式以太网带来的冲突<sup>[14]</sup>。两个网卡分别连入不同的内网,通过配置,使它们的子网掩码与主机号都相同,这样能够方便地识别来自同一源

节点的不同通路的数据。以太网交换机之间则采用环形互联的形式,不仅可以保证当节点通往交换机的一条链路中断时数据能够正常传输,同时也可以保证交换机之间出现链路故障时依旧能够找到通往目的节点的路径。

### 2.2 冗余发送控制

在应用层中加入冗余处理层,在内网中传输的以太网帧内的用户数据的前两个字节定义为帧冗余标签,其格式如图 2 所示。帧冗余标签分为两部分,包括 1 位的冗余符,用于标识数据是否冗余;以及 15 位的循环序列码,用于接收方判断收到的冗余数据是否重复。冗余符为 0 的数据帧标识为非冗余帧,否则为冗余帧。当数据为非冗余时,循环序列码始终为 0;而为冗余的数据帧时,循环序列码在冗余模式下发送后加 1,当增加至 0x7fff 时又重置为 0。

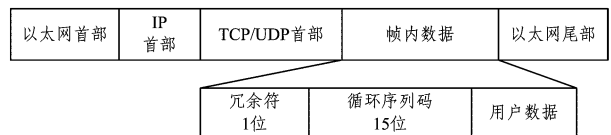


图 2 冗余数据包格式

### 2.3 冗余接收控制

为了能对重复的冗余数据进行检测及处理,在节点中加入循环序列码寄存器,以存储冗余帧的循环序列码,如图 3 所示。序列码数组有 10 个元素,当存满时,传入的循环序列码覆盖最先存入的元素。当收到冗余数据时,取得源节点的主机号并在链表中进行比对,若在链表表中存在则把当前帧的循环序列码与循环序列码数组依次比较,若重复则丢弃,否则写入循环序列码数组;若不存在则在链表尾添加新元素,并写入当前的循环序列码。

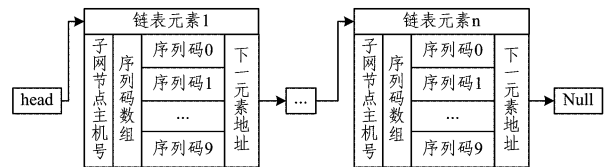


图 3 循环序列码寄存器

### 2.4 网络自诊断

为了保证该系统的正常运行,对运行状态进行周期性监控,同时在出现故障的时候及时做出预警,加入网络自诊断功能。当有新节点加入网络时,广播自己的本地信息,并请求接收来自其他节点的网络信息,同时存储记录,用于网络自诊断。在诊断过程中,节点通过冗余的方式向全网发送诊断报文,诊断报文发送出去之后设置一个时间限制,在限制时间内接收其它节点回复的确认报文,限制时间过后,若没有收到相应节点的确认报文则判断该网络出现故障。此时,节点会出现以下 3 种情况:

- 节点健康:终端节点收到两个确认报文,由该节点的两个网卡分别发送。
- 节点故障:终端节点只收到该节点发送的一个确认报文。
- 节点丢失:终端节点没有收到该节点的确认报文。

当网络中出现节点故障和节点丢失两种情况时,表明网络出现问题,需及时广播诊断结果并通知用户。根据需要,软件在一个固定的自定义端口收发 UDP 数据包,数据的前两个

字节为包头 ID,用于标识不同的内容。诊断过程定义了 5 个不同的数据包:节点信息包、诊断包、确认包、故障信息包和请求信息包。

### 3 实现

设置每个节点的网卡 IP 地址,使得两个 IP 地址子网号不同而主机号相同,这样就可以根据远程节点的一个 IP 地址获得其另一个 IP 地址。

冗余功能通过 Winsock SPI 实现,它打破了服务提供者的透明,让开发者可以编写自己的服务提供者程序。分层服务提供者(Layered Service Provider,LSP)本身是动态链接库(DLL),工作在应用层,可以将它安装到 Winsock 目录,为上层 API 调用提供接口函数,以便创建套接字的应用程序不必知道此 LSP 的任何信息就能调用它<sup>[15]</sup>。在自定义的 LSP 中,包括一个冗余控制类和 LSP 实现函数。

诊断功能通过软件实现,使用 UDP 交换相关信息,并根据内容做出相应的处理和判断。

#### 3.1 冗余控制类

该类在自定义的 LSP 中使用,进行冗余通信和控制相关的操作。

- 本地信息相关的函数和变量:用于获取和存储两个网卡的 IP 和子网号。

- 套接字操作相关函数和变量:为了能够进行冗余发送和接收,每次需要两个相关联的套接字,通过链表存储和使用套接字信息。函数包括链表元素添加、删除和查询操作,变量包括链表头和链表尾。

- 帧冗余标签相关函数:若输入为非冗余模式则返回 0,否则根据 DLL 内共享的循环序列码生成冗余模式下的帧冗余标签。接收时,根据收到的帧冗余标签判断数据是否重复,并做相应处理。

- 数据缓冲区生成相关函数:根据输入生成新的数据缓冲区,用于在用户数据头部添加或删除帧冗余标签。

#### 3.2 SPI 实现函数

作为一个标准的 Windows DLL,必须实现和导出 WSP-Startup 函数。其输入参数 lpProcTable 是一个指向 SPI 函数表结构的指针,用来返回 30 个 SPI 服务函数的地址。在 WSPStartup 函数中,需要根据协议链找到下层提供者,调用它的 WSPStartup 函数初始化下层服务提供者,并取得 SPI 服务函数的指针,在向上返回这些指针前,可用自定义的函数指针覆盖它,以截获 Winsock 的调用。

我们主要修改其中一些主要的函数:WSPSocket、WSPCloseSocket、WSPBind、WSPConnect、WSPAccept、WSPListen、WSPSend、WSPSendTo、WSPRecv、WSPRecvFrom 等。

节点的两个网卡处于子网号不同而主机号相同的子网,为了能够在两个网卡上进行数据的收发控制,需对 SPI 的函数进行修改,以便进行冗余操作,同时对上层的应用程序透明。在 HOOK 函数中,每次都对相关连的两个套接字调用原始的 WSP 函数进行两个操作,返回其中一个调用函数的返回值。以 WSPSocket 代码和 WSPSendTo 流程示意图为例。

SOCKET WSPAPI WSPSocket(int af,int type,int protocol,LPWSA-PROTOCOL\_INFOW lpProtocolInfo, GROUP g, DWORD dwFlags,

LPINT lpErrno )

```
{ //在函数内定义一个套接字数组,这一对套接字都使用传入的参数,分别用于不同内网的数据收发。
    SOCKET s[2];
    s[0]=g_NextProcTable.lpWSPSocket(af, type, protocol, lpPro-
        tocolInfo,g,dwFlags,lpErrno);
    s[1]=g_NextProcTable.lpWSPSocket(af, type, protocol, lpPro-
        tocolInfo,g,dwFlags,lpErrno);
    //将这一对冗余套接字写入套接字链表中,以后可根据套接字值在链
    表中找到这一对套接字并用于冗余的数据过程。
    gRedun.AddSocketElem( s[0],s[1] );
    return s[0];
    //s[0]用于主通路,s[1]用于备用通路,由于只能返回一个值,所以只
    返回主通路的套接字值。
}
```

由于使用了成对的冗余套接字,在其他的一些 HOOK 函数中需要对成对的冗余套接字进行操作,如在其他一些函数中,首先根据传入的套接字值 s 查找其在冗余套接字链表中的位置,从而得到套接字对。再在这两个套接字上分别执行相似的操作。

WSPSendTo 流程如图 4 所示,通过传入的套接字 s 找到对应的冗余套接字,并根据设置的通路值进行发送。由于 WSPSendTo 是面向非连接的,在冗余模式下可以依次进行发送而不会被阻塞,但是 WSPRecv 和 WSPRecvFrom 函数中可能因为网络故障而处于阻塞状态,所以采用多线程实现。

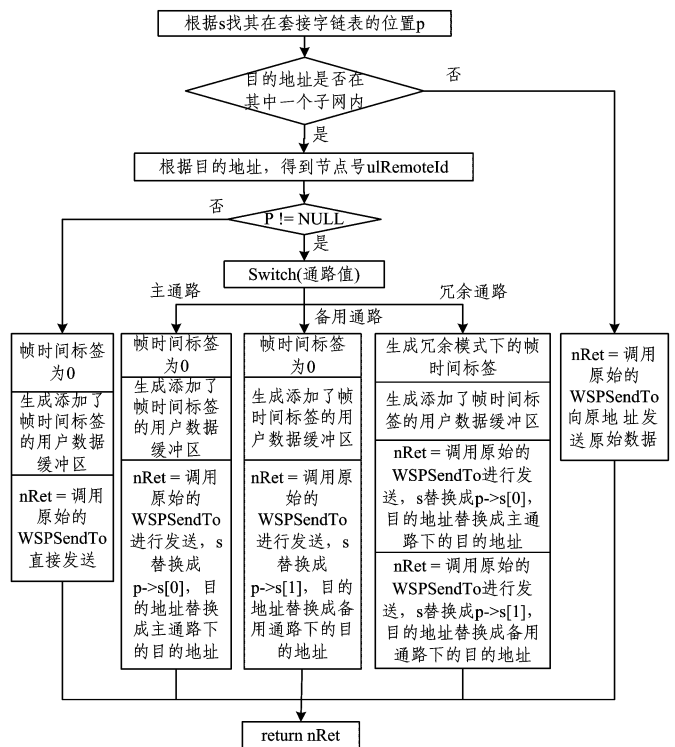


图 4 WSPSendTo 流程示意图

#### 3.3 诊断功能的实现

首先,检测本地的两个网卡的 IP 地址。若有 IP 地址为 0,则表明本地网卡有故障,应立即返回。提醒用户并在未发生故障的网卡上广播本地的故障信息。

其次,从两个网卡分别发送诊断包。此时,根据存储的网络其他节点的信息生成一个包含网络所有节点信息的链表,

并在当前端口接收数据包。软件使用多线程 UDP 传输信息，主线程接收用户消息，当有需要时发送相应的 UDP 数据包，而线程 1 和线程 2 调用 `recvfrom` 函数分别在两个网卡阻塞接收 UDP 数据包，并根据包头 ID 做出相应的处理：收到节点信息包，判断是否为新加入节点，记录信息或丢弃；收到诊断包，回复确认包；收到故障信息包，提醒本地用户；收到请求信息包，回复本地的节点信息包。在发出诊断包后，接收确认包，取得确认包内的信息后找到节点信息链表内的对应元素并删除。3 秒后若节点信息链表的链表头不为 NULL，则说明有网络故障发送，链表元素则为失去连接的网卡地址信息。此时应写入诊断日志中，并及时提醒用户，广播故障信息。

#### 4 测试与验证

实验中，使用 4 个 8 口 10/100M 自适应以太网交换机 TP-Link TL-SF1008+ 连接成环型拓扑结构，构成基础的骨干网络。每个节点主机配置两个 Realtek 网卡，每个网卡连入两个相邻的交换机中，形成星型-环型拓扑结构，如图 5 所示。设置主通路子网地址为 192.168.1.0/24，备用通路子网地址为 10.1.1.0/24。

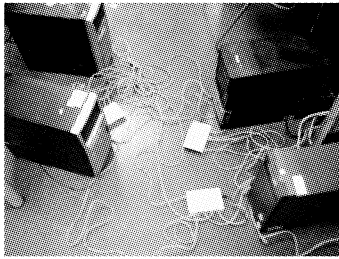


图 5 高可靠综合控制冗余以太网网络系统实验图

##### 4.1 冗余控制测试

在测试程序中，源节点只定义一个套接字，并绑定至备用通路下的地址 10.1.1.75，在自定义端口号 0xff22 上以 1s 为周期向目的节点其中一个地址 10.1.1.159 发送 UDP 报文，并在发送过程中从冗余模式切换至主通路模式。通过 Wireshark 在目的节点主通路网卡上抓取到达的 UDP 数据包。如图 6 和图 7 所示，数据的源 IP 地址为 192.168.1.75，目的 IP 地址为 192.168.1.159，用户数据包的前两个字节从 0x80d6 变为 0x0000。实验结果表明，应用层程序本来只在备用通路上发送数据，但是根据设置先在两条通路上发送冗余的数据，再在主通路上发送非冗余的数据。源节点可以向指定的内网发送数据，并更改相应的标签，成功实现了可控的冗余通信过程。

```
No. Time Source Destination Protocol Length Info
263 366.911192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
264 367.911192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
265 368.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
266 369.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
267 370.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
268 371.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
269 372.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
270 373.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
271 374.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
272 375.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
273 376.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
274 377.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
275 378.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
276 379.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
277 380.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314

Frame 271: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Tp-LinkT_6e15:db (d8:5d:4c:6e:15:db), Dst: Tp-LinkT_70:62:25 (d8:5d:4c:70:62:25)
Address: Tp-LinkT_70:62:25 (d8:5d:4c:70:62:25)
...
0000 d8 5d 4c 70 62 25 d8 5d 4c 6e 15 db 08 00 45 00 ..lpbk..Ln....E.
0010 00 2a 64 00 00 00 40 11 72 7b c0 a8 01 3d c0 a8 ...w...f...hell
0020 01 ff ff 77 ff 77 02 06 64 19 82 c0 08 65 6c 6c ...w...f...hell
0030 6f 20 77 6f 72 6e 64 2e 00 00 00 00 00 00 00 00 o world....
```

图 6 网络切换时目的节点主通路 UDP 数据包捕获一

```
No. Time Source Destination Protocol Length Info
263 366.911192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
264 367.911192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
265 368.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
266 369.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
267 370.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
268 371.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
269 372.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
270 373.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
271 374.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
272 375.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
273 376.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
274 377.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
275 378.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
276 379.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314
277 380.910192.168.1.75 192.168.1.159 UDP 60 Source port: 65399 Destination port: 65314

Frame 272: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Tp-LinkT_6e15:db (d8:5d:4c:6e:15:db), Dst: Tp-LinkT_70:62:25 (d8:5d:4c:70:62:25)
Address: Tp-LinkT_70:62:25 (d8:5d:4c:70:62:25)
...
0000 d8 5d 4c 70 62 25 d8 5d 4c 6e 15 db 08 00 45 00 ..lpbk..Ln....E.
0010 00 2a 64 00 00 00 40 11 72 7b c0 a8 01 3d c0 a8 ...w...f...hell
0020 01 ff ff 77 ff 77 02 06 64 19 82 c0 08 65 6c 6c ...w...f...hell
0030 6f 20 77 6f 72 6e 64 2e 00 00 00 00 00 00 00 00 o world....
```

图 7 网络切换时目的节点主通路 UDP 数据包捕获二

主机通过双网卡进行数据收发，不会增加每条通路上的带宽消耗。另外，通过对重要数据的发送进行通路选择，保证了重要数据的传输，同时只让普通数据在网络上传输一份，避免了过度消耗网络带宽。这样既增加了网络的冗余，提高了可靠性，也不会过度消耗网络带宽。与普通以太网相比，多消耗的带宽与重要数据所占比例成正比。

##### 4.2 故障收包测试

丢包率是指在一定时间间隔内，由源节点发往目的节点过程中丢失的数据包占所发送数据包总量的百分比。实验中，源节点向目的节点分别以 1ms、5ms 和 10ms 为周期发送 10000 个数据包，在网络正常的情况下，普通网络和双冗余网络都能全部正常接收，即丢包率为 0。但网络出现故障时，普通网络出现明显丢包，而双冗余网络的丢包率不到 0.1%。实验表明，普通网络中，节点只有一条通路连入网络，当通信链路故障时，会严重影响数据收发，故容错性不高；而在冗余网络中，当其中一条通路发生故障后，另一条通路还能实现零故障恢复时间的通信，从而大幅降低丢包率，提高容错性。处于冗余模式时，能够正常进行数据收发，当其中一条通路发生故障时，仍然能够进行数据的收发，而在非冗余网络中已不能进行通信。

```
Time Destination Source Protocol Length Info
07:22:39.146192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:40.147192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:41.147192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:42.147192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:43.147192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:44.147192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:45.147192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:46.147192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:47.147192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:48.147192.168.1.75 192.168.1.159 UDP 101 Source port: 65399 Destination port: 65399

Internet Protocol Version 4, Src: 192.168.1.159 (192.168.1.159), Dst: 192.168.1.75 (192.168.1.75)
User Datagram Protocol, Src Port: 65399 (65399), Dst Port: 65399 (65399)
Data: 80e556e6976657273697479206f66620456c05637420f6e...
[Length: 59]
0000 08 5d 4c 70 62 25 d8 5d 4c 70 62 25 08 00 45 00 ..[n...]lpbk..E.
0010 00 2a 64 00 00 00 40 11 72 7b c0 a8 01 3d c0 a8 ...w...f...hell
0020 01 ff ff 77 ff 77 02 06 64 19 82 c0 08 65 6c 6c ...w...f...hell
0030 6f 20 77 6f 72 6e 64 2e 00 00 00 00 00 00 00 00 o world....
0040 6f 20 77 6f 72 6e 64 2e 00 00 00 00 00 00 00 00 o world....
```

图 8 发生网络故障时目的节点主通路的 UDP 数据包捕获

```
Time Destination Source Protocol Length Info
07:22:44.147 10.1.1.75 10.1.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:45.147 10.1.1.75 10.1.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:46.147 10.1.1.75 10.1.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:47.147 10.1.1.75 10.1.1.159 UDP 101 Source port: 65399 Destination port: 65399
07:22:48.147 10.1.1.75 10.1.1.159 UDP 101 Source port: 65399 Destination port: 65399

Frame 1055: 101 bytes on wire (808 bits), 101 bytes captured (808 bits) on interface 0
Ethernet II, Src: HONHAIPr_45:ba:21 (44:37:0e:45:ba:21), Dst: AsustekC_8d:06:8e (20:cf:30:8d:06:8e)
Internet Protocol Version 4, Src: 10.1.1.159 (10.1.1.159), Dst: 10.1.1.75 (10.1.1.75)
User Datagram Protocol, Src Port: 65399 (65399), Dst Port: 65399 (65399)
Data (59 bytes)
0000 20 cf 30 8d 06 b8 44 37 0e 45 ba 21 08 00 45 00 ..0.f.67..E.L...E.
0010 00 2a 64 00 00 00 40 11 72 7b c0 a8 01 3d c0 a8 ...w...f...hell
0020 01 ff ff 77 ff 77 02 06 64 19 82 c0 08 65 6c 6c ...w...f...hell
0030 6f 20 77 6f 72 6e 64 2e 00 00 00 00 00 00 00 00 o world....
0040 6f 20 77 6f 72 6e 64 2e 00 00 00 00 00 00 00 00 o world....
```

图 9 发生网络故障时目的节点备用通路的 UDP 数据包捕获

在正常运行的网络中进行通信,主机号为 159 的源节点向主机号为 75 的目的节点以 1s 为间隔发送 UDP 数据包。如图 8 和图 9 所示,网络正常时目的节点能够在两个网卡上收到数据包,通过处理,丢弃冗余重复的数据包,在应用层不会收到多余的数据。在时间 07:22:49.147 之后,目的节点的主通路发生故障,已经接收不到源节点发送的数据包,但是不影响在备用通路上接收数据包,实现了网络故障下的正常通信。

### 4.3 网络自诊断测试

实验中,网络故障后,软件诊断网络故障并做记录。如图 10 所示,列表中详细列出了发生网络故障的时间、用户名、IP 地址、通路及 MAC 地址,表明软件能够准确地发现和定位网络故障,提醒用户并做详细记录以备查询,成功实现了网络诊断功能。

时间	用户名	IP地址	通路	MAC地址
2013年4月7日 16:13:26	Y610912	本地地址	主通路	d9-5d-4c-6e-15-d8
2013年4月7日 16:14:9	Y311009	192.168.1.159	主通路	d9-5d-4c-70-62-25
2013年4月7日 16:14:32	Y311009	10.1.1.159	备用通路	44-37-e6-45-ba-21
2013年4月7日 16:15:21	Y311009	10.1.1.159	备用通路	44-37-e6-45-ba-21
2013年4月7日 16:15:27	Y610912	本地地址	备用通路	20-df-30-8d-66-b8
2013年4月7日 16:15:32	Y610912	本地地址	备用通路	20-df-30-8d-66-b8

图 10 诊断结果测试图

**结束语** 根据一些场合对以太网通信的高可靠性要求,在应用层加入了冗余处理层。发送方在冗余模式下可以发送两份相同的数据,根据帧冗余标签来进行标记。接收方根据帧冗余标签进行相应的处理,保证了网络数据传输的可靠性以及对用户的透明。同时还引入网络诊断功能,通过对网络的周期性监控,得到网络的故障信息,以及时排除问题。实验结果表明:在冗余模式下,改进的 LSP 使得应用程序能够发送两份相同的数据,而且网络能够容忍多处故障而进行数据传输;同时,网络自诊断功能能够定位和记录故障信息。与动态冗余管理的协议相比,其增加了主机至网络的一条通路,通过在两条通路上同时发送冗余的数据实现零故障恢复时间,同时可以容忍多处主机至网络的故障。与 PRP<sup>[7]</sup> 的两个独立网络使得成本价加倍不同,本方案在一个网络中使用,减小了成本;通过通路选择保证了重要数据的可靠传送,尽量避免了网络拥塞,而且引入网络自诊断功能,可以及时发现和处理网络故障。网络具有高可靠性和可操作性,同时易于实现,可用于对一些重要数据的可靠性和实时性有特别要求的中小型的局域网中。

### 参考文献

[1] Araujo J A, Lázaro J, Astarloa A. High Availability Automation Networks: PRP and HSR Ring Implementations[C] // IEEE International Symposium on Industrial Electronics (ISIE). Hang-

zhou, China, 2012; 1197-1202

[2] Hoga C. Seamless Communication Redundancy of IEC 62439 [C] // The International Conference on Advanced Power System Automation and Protection. Beijing, China, 2011; 489-494

[3] Kirrmann H, Hansson M, Müri P. IEC 62439 PRP: Bumpless Recovery for Highly Available, Hard Real-Time Industrial Networks[C] // IEEE Conference on Emerging Technologies and Factory Automation (ETFA). Patras, Greece, 2007; 1396-1399

[4] Goraj M, Harada R. Migration Paths for IEC 61850 Substation Communication Networks Towards Superb Redundancy Based on Hybrid PRP and HSR Topologies[C] // International Conference on Developments in Power Systems Protection (DPSP). Birmingham, UK, 2012; 1-6

[5] Giorgetti A, Cugini F, Paolucci F, et al. Performance Analysis of Media Redundancy Protocol (MRP)[J]. IEEE Transactions on Industrial Informatics, 2011, 9(1): 218-227

[6] Kleineberg O, Ries M, Rentschler M, et al. Automatic device configuration for Ethernet ring redundancy protocols [C] // IEEE Conference on Emerging Technologies & Factory Automation (ETFA). Mallorca, 2009; 1-8

[7] Rentschler M, Heine H. The Parallel Redundancy Protocol for Industrial IP Networks[C] // IEEE International Conference on Industrial Technology (ICIT). Cape Town, 2013; 1404-1409

[8] Nsaif S A, Rhee J M. Improvement of High-Availability Seamless Redundancy (HSR) Traffic Performance for Smart Grid [J]. Journal of Communications and Networks, 2012, 14 (6): 653-661

[9] Heine H, Kleineberg O. The High-Availability Seamless redundancy protocol (HSR): Robust fault-tolerant networking and loop prevention through duplicate discard [C] // IEEE International Workshop on Factory Communication Systems (WFCS). Lemgo, 2012; 213-222

[10] Imtiaz J, Jasperneite J, Weber K. Redundant Structures for a Generic Real-time Ethernet System [C] // IEEE Conference on Emerging Technologies and Factory Automation (ETFA). Bilbao, 2010; 1-4

[11] Allawi S, Myung J. Improvement of High-availability Seamless Redundancy (HSR) Traffic Performance [C] // International Conference on Advanced Communication Technology (ICACT). PyeongChang, 2012; 814-819

[12] 肖贺, 管海兵, 宦飞. 工业以太网冗余技术分析[J]. 信息安全与通信保密, 2012(3): 59-67

[13] International Electrotechnical Commission, Geneva. IEC62439-6 Distributed Redundancy Protocol (DRP)[S]. 2009

[14] 杨佳丽, 窦军. 高速以太网时延仿真分析[J]. 计算机科学, 2011, 38(10A): 341-344

[15] 熊安萍. 基于 Winsock 技术的数据包解析研究[J]. 计算机科学, 2006, 33(12): 81-82