

常问问题 • 10/2014

如何用 Wireshark 工具诊断时间同步

PCS 7 时间同步

目录

1. 引言	3
2. 准备工作	3
3. 如何捕捉网络上时钟同步的通讯报文	4
3.1 如何捕捉网络上的报文，并过滤出时间同步相关报文	5
3.1.1 捕捉报文的设置	5
3.1.2 报文显示过滤	6
3.1.3 报文的保存	6
3.2 如何查找网络上的多个时间主站	7
3.2.1 使用捕捉过滤器	7
3.3 如何分析计算机之间的同时同步报文	9

1. 引言

在 PCS7 项目里，一定要配置好系统总线和终端总线的时间同步，保证网络里所有的控制器和操作员站的时间都是一致的，这对于生产管理和事故分析是非常重要的，例如：项目里有多个 CPU，在进行故障分析时，由于 CPU 之间的时间没有同步，有可能发现事件发生的顺序前后矛盾的问题。

关于时间同步的设置，请参考下面的文档：

《S7 V6.1 下实现时间同步功能（更新版）》

<http://www.ad.siemens.com.cn/download/searchResult.aspx?searchText=A0147>

通常只要按照手册设置好相关的参数，就很容易做好时间同步工作，但是特殊情况下也有同步不上的情况，例如：项目里使用了第三方的时钟源，在调试时出现问题，不容易判断到底是哪方面的问题，这时如果能够得到时间同步的报文，对于问题的分析就很有帮助，Wireshark 就是这样一款功能强大的开源网络协议分析器，它可以实时检测网络通讯数据，也可以检测其抓取的网络通讯数据快照文件。可以通过图形界面浏览这些数据，可以查看网络通讯数据包中每一层的详细内容。

2. 准备工作

Wireshark 软件是开源软件，不需要授权，可以方便地从网站下载到，也可以在官方下载，下面是下载的连接：

<http://www.wireshark.org/download.html>

Wireshark 官方下载链接

下面以 Wireshark V1.8.1 为例，介绍如何用它来分析时间同步。

下载好程序后，双击它开始安装，实际上安装只是解压缩的过程，不会对系统产生不良影响。找到 Wireshark 软件，双击它，按提示选择一个路径，用以存放文件。指定的路径可以随意，建议找一独立的文件夹，如下所示：





图 1 安装 Wireshark

安装完成后，在 Windows 的资源管理器里找到前边安装时指定的路径，双击 wireshark 可执行程序即可。

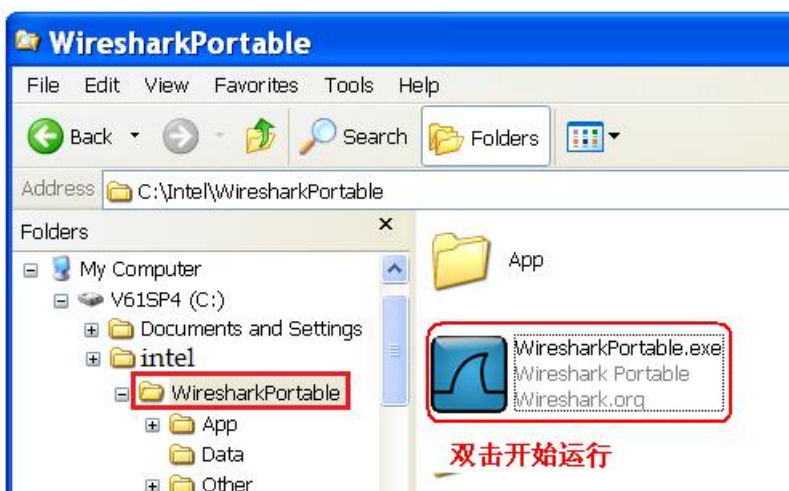


图 2 安装完成之后的 wireshark 可执行文件

3. 如何捕捉网络上时钟同步的通讯报文

在使用 Wireshark 时一般用到如下的功能：

(1) 选择捕获接口。一般都是选择连接到 Internet 网络的接口，这样才可以捕获到与网络相关的数据。否则，捕获到的其它数据对自己也没有任何帮助。

(2) 使用捕获过滤器。通过设置捕获过滤器，可以避免产生过大的捕获文件。这样用户在分析数据时，也不会受其它数据干扰。而且，还可以为用户节约大量的时间。

(3) 使用显示过滤器。通常使用捕获过滤器过滤后的数据，往往还是很复杂。为了使过滤的数据包再更细致，此时使用显示过滤器进行过滤。

下面以常见的问题为例子，介绍如何使用 **Wireshark** 来获取报文、分析。

如果发现 **PLC** 或者操作员站的时间都没有被同步，或者被同步的时间有跳变的现象，应当检查是否存在多个时间同步主站，通过需要捕捉网络上所有的广播报文，通常捕捉 3 分钟左右就够了，步骤如下：

3.1 如何捕捉网络上的报文，并过滤出时间同步相关报文

3.1.1 捕捉报文的设置

打开 **wireshark** 后，点击启动按钮，打开启动界面后，在工具栏里点击“捕捉”按钮，开始捕捉的相关设置。

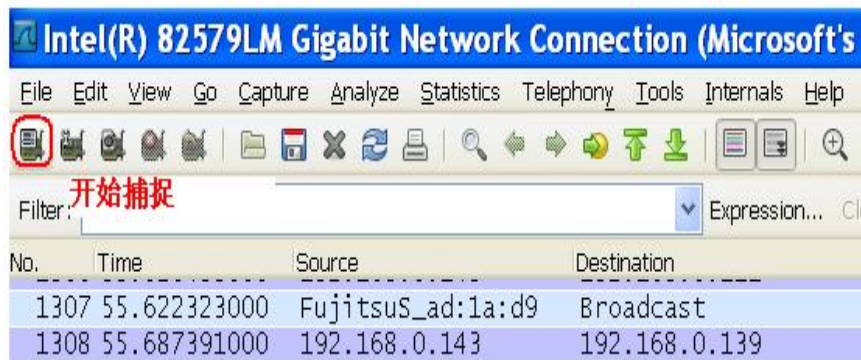


图 3 启动报文捕捉

在选择网卡界面里选择本机的网卡，选中后按下 **Start** 按钮，开始捕捉。

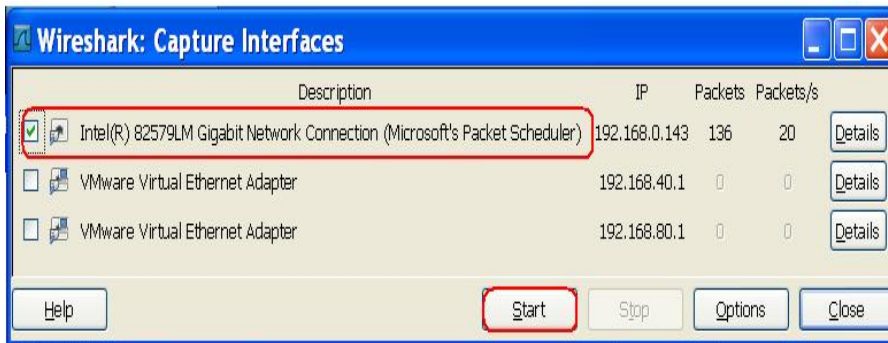


图 4 选择需要监控的网卡

捕捉的时间到后，按下 **STOP** 按钮，即可停止。

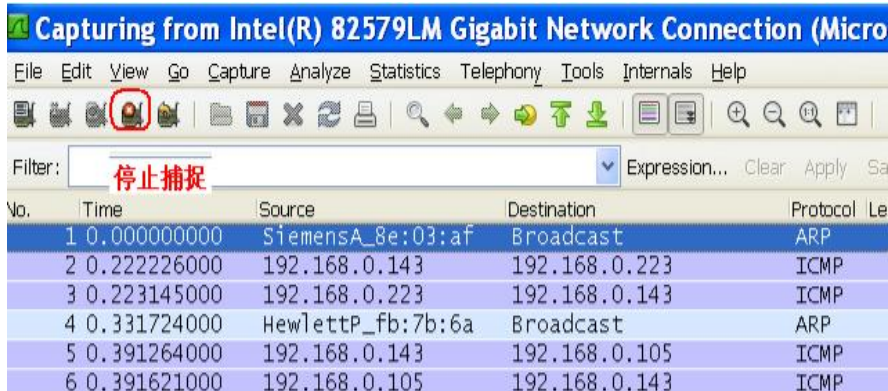


图 5 停止捕捉

3.1.2 报文显示过滤

对报文分析需要对报文进行过滤, 方法是在 **Filter** 选项里输入如下条件
 “ eth.dst==08:00:06:01:ff:ef ”, 再按下 **Apply**, 即可看到报文里 WINCC 或者 PLC 广播的时间同步报文。这条过滤条件的作用就是将所有发往 MAC 地址为“ 08:00:06:01: ff: ef”的报文都显示出来, 而在 **SIMATIC Mode** 下进行的时钟同步, PLC 或者 WinCC 作为时钟服务器时均会按照固定间隔往这个 MAC 地址发送报文。

在下图可以看出, 时间主站的 MAC 地址是 08-00-06-99-56-f0, 它每隔 10 秒向全网络广播一次时间同步的报文。

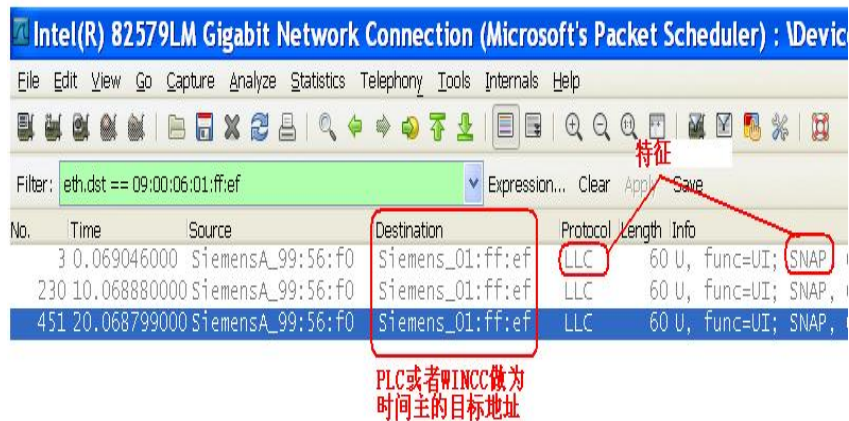


图 6 过滤时钟同步报文

3.1.3 报文的保存

如果需要把报文保存下来供以后分析, 从 **File** 菜单选择“**Save**”, 即可存到本地硬盘里, 建议起名字包括了日期和网段的描述, 如下所示:

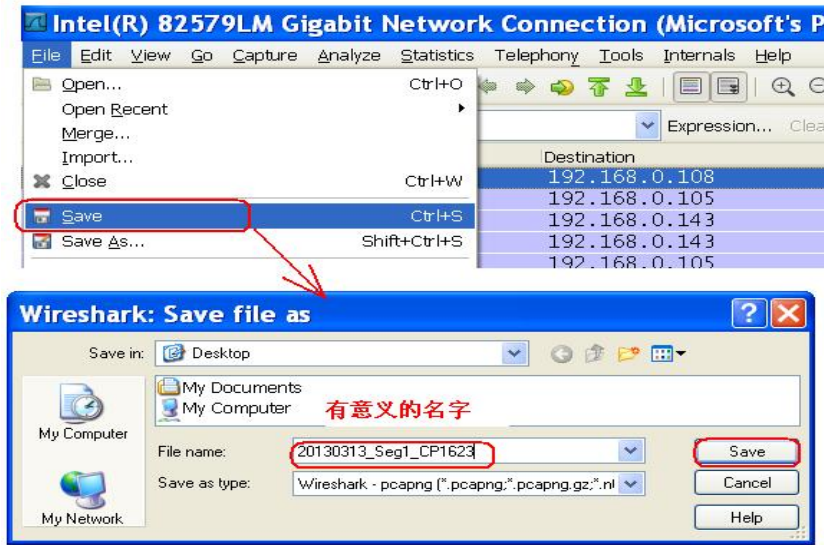


图 7 保存捕获的报文

3.2 如何查找网络上的多个时间主站

如果发现网络上时间同步不正常，偶尔有时钟跳变的情况，这时极有可能是网络上多个时间主站，通过前边的方法可以检查出问题，但是如果这个问题偶尔出一次，就需要长时间捕捉 CPU 或者 WINCC 的时间同步报文，以观察是否有其它的第三个时钟报文广播到网络里。

3.2.1 使用捕捉过滤器

在启动捕捉后，不要直接选择启动，点击“Options”按钮。

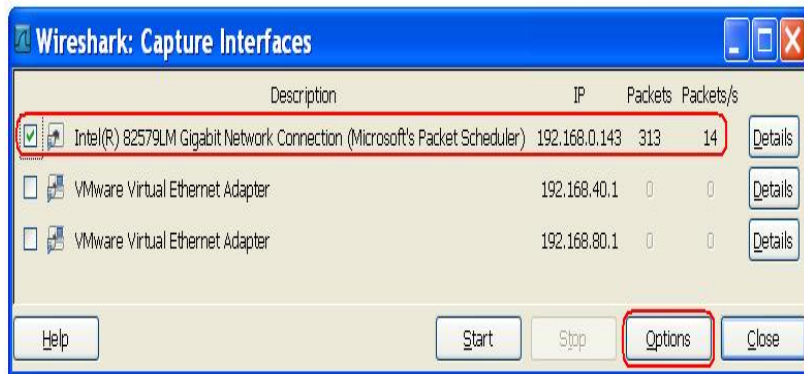


图 8 从网卡选择窗口进入 Option 设置

在弹出的窗口里双击系统总线上的网卡，如下图：



图 9 再次选择需要监视的网卡

在下面的过滤条件里手动输入过滤条件“ ether host 09:00:06:01:ff:ef ”，然后接下 OK。

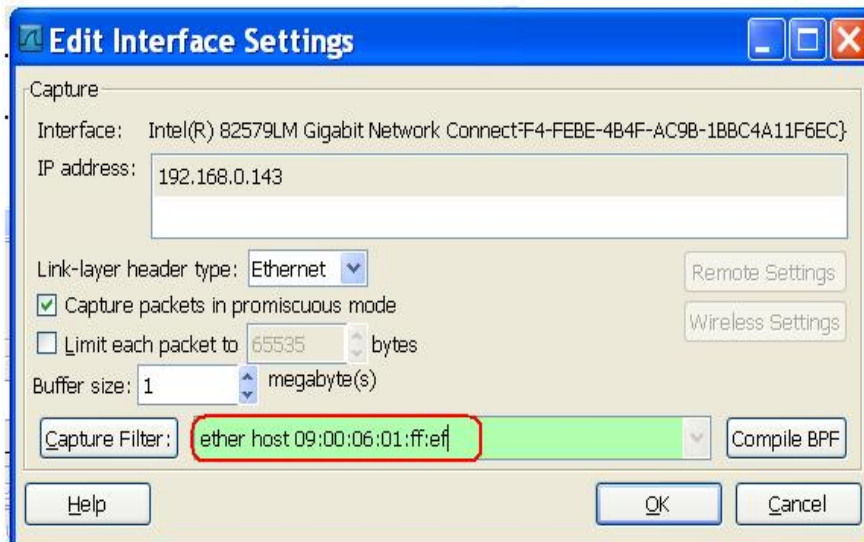


图 10 设定过滤条件

按下 OK 后， 返回到主界面， 这时点击“ Start ” 开始捕捉：

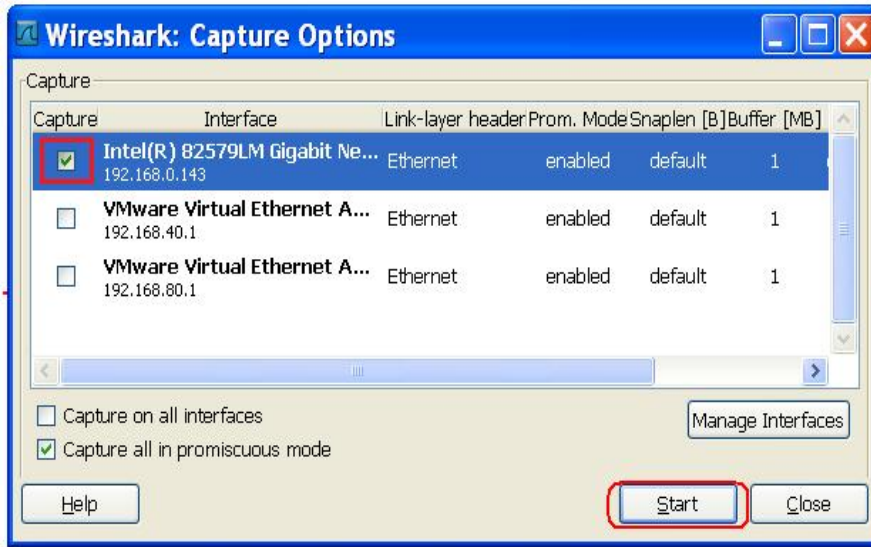


图 11 启动捕获

由于预先设置好了 Capture filter 条件，系统只会捕捉符合条件的报文，如果网络上有 WINCC 或者 PLC 来广播，Wireshark 就会捕捉到时间同步的报文，如下图所示：

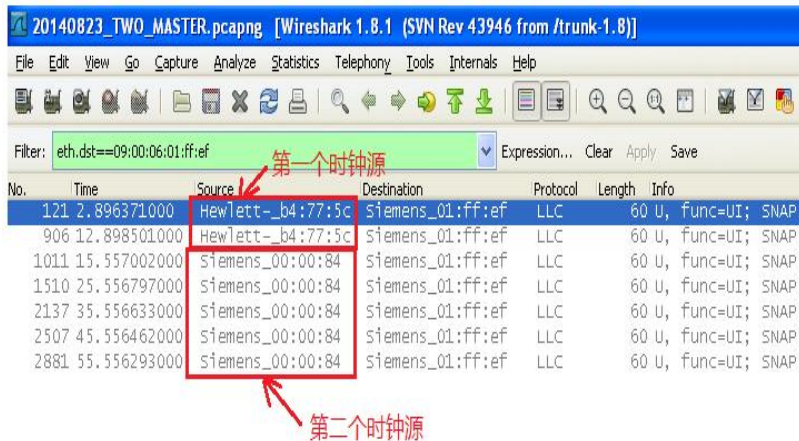


图 12 软件自动记录符合条件的报文

根据需要，将此段报文保存到指定的目录，以便于之后分析。

3.3 如何分析计算机之间的同时同步报文

WINCC 支持将网络上其它的计算机（第三方时钟源）做为时间主，设置如下。在下面例子里，设置网络上 IP 地址为“192.168.0.107”的计算机为主，如下所示。（注：本机的地址是 192.168.0.178）

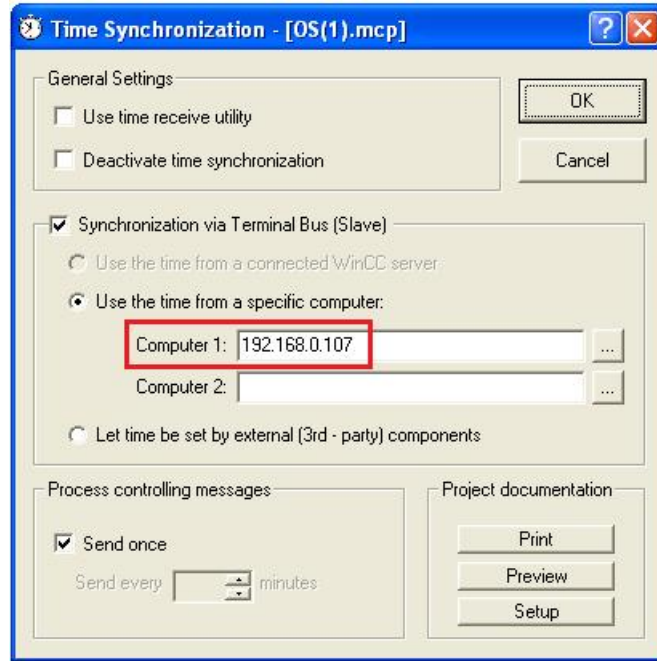


图 13 WinCC 中的时钟同步设置

在使用中发现时间同步没有成功，用 Wireshark 抓取报文发现如下的报文，发现如下的错误：“Error:STATUS_LOGON_FAILURE”，这说明本机连接到 192.168.0.107 这台计算机时登录失败，将两台计算机的用户名和密码统一后问题解决。

No.	Source	Destination	Length	Info
243	FujitsuT_21:3d	Broadcast	60	who has 192.168.0.225? Tell 192.168.0.3
253	192.168.0.107	192.168.0.178	62	netbios-ssn > aplx [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1
254	192.168.0.107	192.168.0.178	60	microsoft-ds > dfn [ACK] Seq=541 Ack=727 win=63652 Len=0
255	192.168.0.107	192.168.0.178	62	microsoft-ds > omnivision [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1
256	192.168.0.178	192.168.0.107	54	omnivision > microsoft-ds [ACK] Seq=1 Ack=1 win=65535 Len=0
257	192.168.0.107	192.168.0.178	62	netbios-ssn > hhb-gateway [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1
258	192.168.0.178	192.168.0.107	191	Negotiate Protocol Request
259	192.168.0.107	192.168.0.178	60	microsoft-ds > dfn [RST, ACK] Seq=541 Ack=727 win=0 Len=0
260	192.168.0.107	192.168.0.178	185	Negotiate Protocol Response
261	192.168.0.178	192.168.0.107	294	Session Setup Andx Request, NTLMSSP_NEGOTIATE
262	192.168.0.107	192.168.0.178	424	Session Setup Andx Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED
263	192.168.0.178	192.168.0.107	402	Session Setup Andx Request, NTLMSSP_AUTH, User: GONGDY\Administrator
264	192.168.0.107	192.168.0.178	93	Session Setup Andx Response, Error: STATUS_LOGON_FAILURE
265	192.168.0.106	192.168.0.178	60	Echo (ping) request id=0x0008, seq=7312/36892, ttl=255
266	192.168.0.178	192.168.0.106	42	Echo (ping) reply id=0x0008, seq=7312/36892, ttl=128
267	Hewlett-_aa:2f	Broadcast	60	who has 192.168.0.184? Tell 192.168.0.106
268	192.168.0.178	192.168.0.13	42	Echo (ping) request id=0x0200, seq=35078/1673, ttl=128
269	192.168.0.13	192.168.0.178	60	Echo (ping) reply id=0x0200, seq=35078/1673, ttl=128
270	192.168.0.178	192.168.0.107	54	omnivision > microsoft-ds [ACK] Seq=726 Ack=541 win=64995 Len=0
271	siemens_00:00:7	Hewlett-_b4:77	118	detachUserRequest
272	Hewlett-_b4:77	siemens_00:00:7	60	AK TPOU (40) dst-ref: 0x0402 Credit: 1
273	192.168.0.178	192.168.0.107	42	Echo (ping) request id=0x0200, seq=35334/1674, ttl=128
274	192.168.0.107	192.168.0.178	60	Echo (ping) reply id=0x0200, seq=35334/1674, ttl=128
275	FujitsuT_21:3d	Broadcast	60	who has 192.168.0.114? Tell 192.168.0.57

图 14 通过报文监控读取到问题根源

附录一 推荐网址

自动化系统

西门子（中国）有限公司 工业业务领域 支持中心

网站首页: www.4008104288.com.cn

自动化系统 下载中心: <http://www.ad.siemens.com.cn/download/SearchResult.aspx?pid=1>

自动化系统 全球技术资源:

<http://support.automation.siemens.com/CN/view/zh/10805045/130000>

基于产品的支持与服务主页: <http://www.ad.siemens.com.cn/productportal/Default.aspx>

注意事项

应用示例与所示电路、设备及任何可能结果没有必然联系，并不完全相关。应用示例不表示客户的具体解决方案。它们仅对典型应用提供支持。用户负责确保所述产品的正确使用。这些应用示例不能免除用户在确保安全、专业使用、安装、操作和维护设备方面的责任。当使用这些应用示例时，应意识到西门子不对在所述责任条款范围之外的任何损坏/索赔承担责任。我们保留随时修改这些应用示例的权利，恕不另行通知。如果这些应用示例与其它西门子出版物(例如，目录)给出的建议不同，则以其它文档的内容为准。

声明

我们已核对过本手册的内容与所描述的硬件和软件相符。由于差错难以完全避免，我们不能保证完全一致。我们会经常对手册中的数据进行检查，并在后续的版本中进行必要的更正。欢迎您提出宝贵意见。

版权© 西门子（中国）有限公司 2001-2013 版权保留

复制、传播或者使用该文件或文件内容必须经过权利人书面明确同意。侵权者将承担权利人的全部损失。权利人保留一切权利，包括复制、发行，以及改编、汇编的权利。

西门子（中国）有限公司