

以太网探秘

应用指南

更低噪声、更多通道
更高带宽



MSO6B混合信号示波器

摘要：本文以双绞线以太网为分析对象，以混合信号示波器为分析工具，深入探秘了 2 类常见的双绞线以太网的编码，且实地查看并验证了以太网在物理层的信号传输情况，最后通过一个实战例子来对比了实际网络中软件接收到的数据和示波器捕获信号之间的一致性。本文打通软硬件之间的隔阂，从物理层揭示了以太网数据传输的机制，也充分发挥了现代化混合信号示波器的总线解码能力。

关键词：以太网；示波器；总线解码；逻辑分析

目录

| | |
|-------------------------|---|
| 一、以太网概述 | 3 |
| 二、10 Base-T 以太网 | 3 |
| 三、100 Base-TX 以太网 | 4 |
| 3.1 4B5B | 4 |
| 3.2 MLT-3 | 5 |
| 3.3 NRZ-I | 5 |
| 3.4 示例 | 5 |
| 3.5 实战 | 6 |
| 四、总结 | 7 |
| 参考文献 | 7 |

一、以太网概述

以太网（Ethernet）是一种常见的计算机组网技术，其技术标准在 IEEE 802.3 中规定 [1]。目前广泛使用的以太网通过双绞线（俗称网线）交换信息，其技术标准主要在 TIA/EIA-568 中规定 [2]。

本文以最常见的以太网标准为例，利用混合信号示波器的协议解码功能，揭秘以太网上的信号是如何传输的。通常对于网络数据的分析都在软件上进行，例如著名的 Wireshark 工具可以对指定网卡上传的数据进行捕获并解析 [3]。但这样的操作屏蔽了物理层的差异，本文将更进一步，揭秘物理层上数据具体是如何转变成电信号并传输的。

以太网（10 Base-T）和快速以太网（100 Base-TX）可以使用同一种双绞线进行数据传输，其引脚定义如图 1 所示。


| Pin | T568A pair | T568B pair | 10BASE-T 100BASE-TX | Wire | T568A color | T568B color | Pins on plug face |
|-----|------------|------------|---------------------|------|---------------------|---------------------|---|
| 1 | 3 | 2 | TX+ | tip | white/green stripe | white/orange stripe |  |
| 2 | | | TX- | ring | green solid | orange solid | |
| 3 | 2 | 3 | RX+ | tip | white/orange stripe | white/green stripe | |
| 4 | | | not used | ring | blue solid | | |
| 5 | 1 | | not used | tip | white/blue stripe | | |
| 6 | 2 | 3 | RX- | ring | orange solid | green solid | |
| 7 | | | not used | tip | white/brown stripe | | |
| 8 | 4 | | not used | ring | brown solid | | |

图 1：网线的引脚定义 [1]

以 T568B 为例，其中用到了 4 根线，构成 2 个差分对（TX 和 RX）。不失一般性，我们取其中一对（TX）作为分析对象。因此需要引出 Pin 1 和 Pin 2，用于连接示波器探头来抓取信号。这里剪开一根网线，在 Pin 1 和 2 上分别引出一根导线，做成分析用的专用跳线，如图 2 所示。

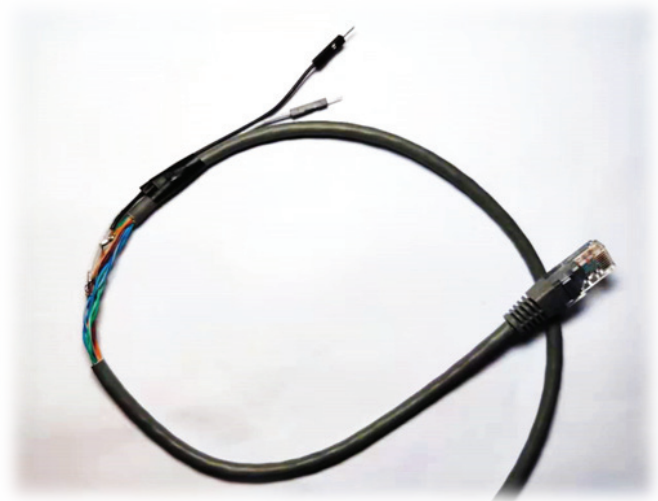


图 2：在双绞线的 Pin 1 和 2 上分别引出一根导线

这一对线上传输的是差分信号，因此最好用差分探头（例如 TDP1500）。当然这里用到的跳线比较短，用普通的无源探头也可以，只是信号质量会受到一定的影响。

二、10 Base-T 以太网

10 Base-T 的传输速率是 10Mbps，使用曼彻斯特编码（相位编码）数据。“0”用下降沿表示，“1”用上升沿表示。如图 3 所示的是一段由示波器抓取到的差分波形。在确认最小脉宽后，可以通过判断周期性的边沿方向来辨识“0”或“1”。

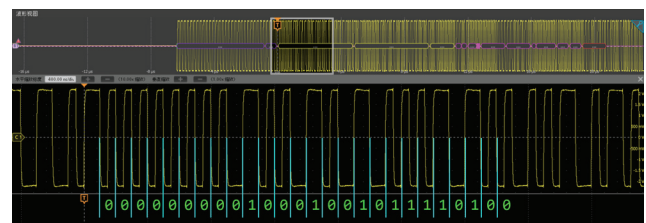


图 3：10 Base-T 的曼彻斯特编码解析

接下来需要将二进制序列组装成数据帧，由于包含多个协议的堆叠（MAC、IP、TCP 等），手动解码会比较复杂，可以直接使用示波器的总线解码工具进行解码并显示。如图 4 所示，将总线设为“Ethernet”，速度设为“10 Base-T”，信号类型设为“差分”，其它选项根据实际情况选择或保持默认就可以了。

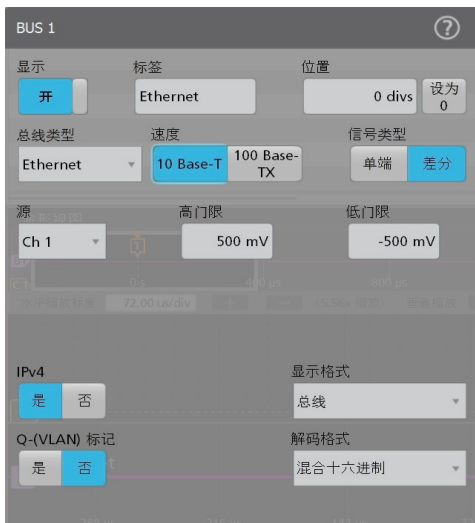


图 4：10 Base-T 解码设置

解码结果如图 5 所示，可以看到这是一个 IPv4 的数据帧，放大后可以看到 MAC 地址等数据包内的具体内容。

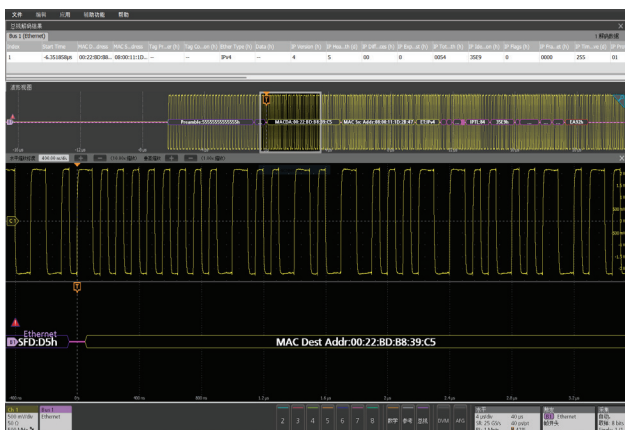


图 5：10 Base-T 解码结果

三、100 Base-TX 以太网

相比 10 Base-T，100 Base-TX 带来了 10 倍的速度提升，达到 100Mbps。它的编码协议也变得复杂得多，主要涉及 3 个关键词：4B5B、MLT-3 和 NRZ-I。

3.1 4B5B

4B5B 表示使用 5 位二进制编码来表示 1 组 4 bits 数据 [4]。这样做的原因是使得传输线上有足够多的跳变用来恢复时钟。4B5B 的编码规则是预先定义的，如果仅仅用来解码，只需要查表即可，如图 6 所示。举例：“0000”或“1111”如果直接传输，会带来 4 个一样的编码，很有可能引入较强的直流分量，但经过 4B5B 编码后，分别变成了“11110”和“11101”，就缓解这个问题了。4B5B 的缺点是，需要增加额外的 25% 传输带宽，因此 100 Base-TX 虽然数据传输率是 100Mbps，却需要 125Mhz 的时钟频率。

| Data | | 4B5B code |
|-------|----------|-----------|
| (Hex) | (Binary) | |
| 0 | 0000 | 11110 |
| 1 | 0001 | 01001 |
| 2 | 0010 | 10100 |
| 3 | 0011 | 10101 |
| 4 | 0100 | 01010 |
| 5 | 0101 | 01011 |
| 6 | 0110 | 01110 |
| 7 | 0111 | 01111 |
| 8 | 1000 | 10010 |
| 9 | 1001 | 10011 |
| A | 1010 | 10110 |
| B | 1011 | 10111 |
| C | 1100 | 11010 |
| D | 1101 | 11011 |
| E | 1110 | 11100 |
| F | 1111 | 11101 |

图 6：4B5B 对应关系表

3.2 MLT-3

MLT-3 表示 “Multi-Level Transmit”，即使用多个电压级别来传输数据 [5]。MLT-3 使用 3 个电压，在差分传输线上，3 个电压可以归一化记为 “-1”、“0” 和 “+1”。MLT-3 通过切换电压来实现跳变，顺序遵循 2 个规则：

- (1) 如果跳变前电压是 -1 或 +1，则跳变后电压是 0；
- (2) 如果跳变前电压是 0，则跳变后电压与上一个非 0 值的电压相反。

因此可简单总结跳变顺序为：-1 → 0 → +1，或 +1 → 0 → -1。

3.3 NRZ-I

MLT-3 描述了电压跳变的规则，但没有说明电压跳变与数据 “0”、“1” 的关系。NRZ-I 为 “Non-Return-to-Zero Inverted” 的缩写，即不归零反转码。这种编码规定数据 “0” 不跳变，数据 “1” 跳变。

3.4 示例

综合前面 3 个关键词，可以简单概括 100 Base-TX 的电信号变化规律如下：

100 Base-TX 首先通过 4B5B 编码将每 4 位数据编码成 5 位二进制编码；接着使用 3 种电压传输数据，如果数据为 “0”，电压不跳变，如果数据为 “1”，电压跳变 1 次，且总是往历史电平相反的方向跳变，例如 -1 → 0 → +1，或 +1 → 0 → -1。

最后，100 Base-TX 并不直接传输信号本身，而是传输信号与扰码的异或结果，如图 7 所示。截取的信号首先通过 MLT-3 的规则解码，每 5 位一组，用绿色字体标识。接下来找到解扰码 (scrambler key) 序列。

扰码不是加密，只是用来改善电磁特性，因此加扰和解扰都只需做异或 (XOR) 操作，使用同一个序列。100 Base-TX 使用一个 11 位的线性反馈移位寄存器 (LFSR) 来生成 2047 位长的伪随机数序列。这对于手动找到同步的位置带来了非常大的困难，但是如果是程序自动同步，就非常容易了。解扰后的数据是 5 bits 一组，反查 4B5B 的编码表，就可以得到 4 bits 一组的数据。图 7 中展示了 3 个字节的编码分析结果。

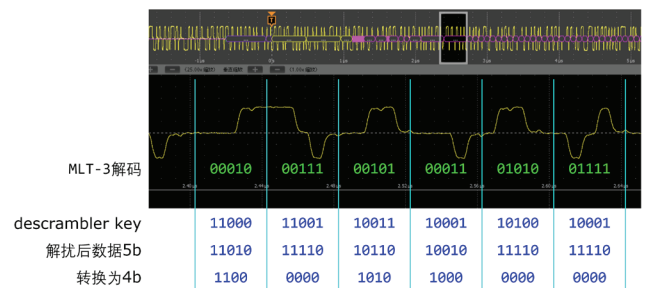


图 7: 100 Base-TX 的编码解析

虽然 100 Base-TX 手动解码非常困难，但是借助示波器的总线解码工具，可以非常快速方便地完成解码。示波器的设置如图 8 所示。由于是标准协议，并没有太多选项，将总线设为 “Ethernet”，速度设为 “100 Base-TX”，信号类型设为 “差分”，其它选项根据实际情况选择或保持默认就可以了。



图 8: 100 Base-TX 解码设置

解码结果如图 9 所示。

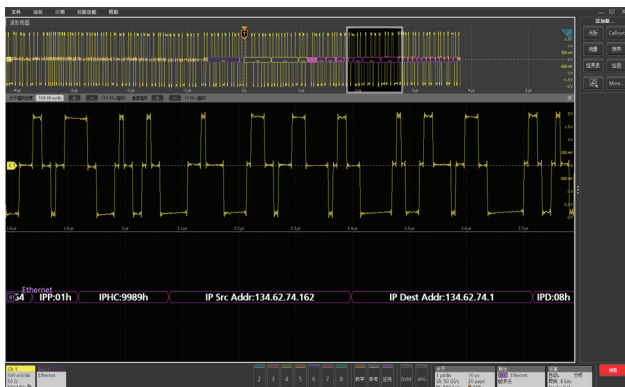


图 9：100 Base-TX 解码结果

100 Base -TX 的解码流程复杂，数据量大，检索不方便，通常需要协议分析软件辅助才可以进一步分析。现在混合信号示波器中已经集了解码和分析功能，只需要一根特制的网线，就可以完成全部分析工作，彻底将以太网的传输机制展示在屏幕上。

3.5 实战

我们通过 2 台计算机组成一个小局域网，在局域网之间进行 ping 操作的实战验证。通过 Wireshark 捕获，我们可以看到在网口上已经有了若干 ping request 和 reply 数据包，如图 10 所示。在 TX 差分对上，我们理应找到发出去的 ping request 数据包，源地址是 192.168.0.2，目标地址是 192.168.0.1。

在示波器上，我们设置好 Ethernet 总线解码，并将触发设置为指定的 IP。如图 11 所示，触发位置选为“IP 标头”，源地址设为“192.168.0.2”，这样当出现指定源地址的数据包后，示波器就会被触发。

如图 12 所示，是通过上述设置后示波器捕获并解码的数据包，经过对比，和 Wireshark 上软件捕获的数据相一致。

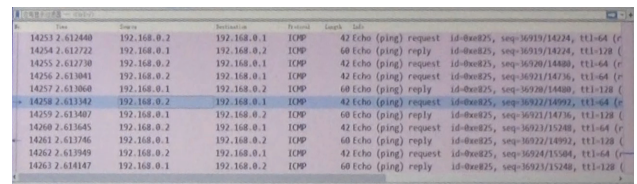


图 10：Wireshark 捕获的 ping request 和 reply 数据包

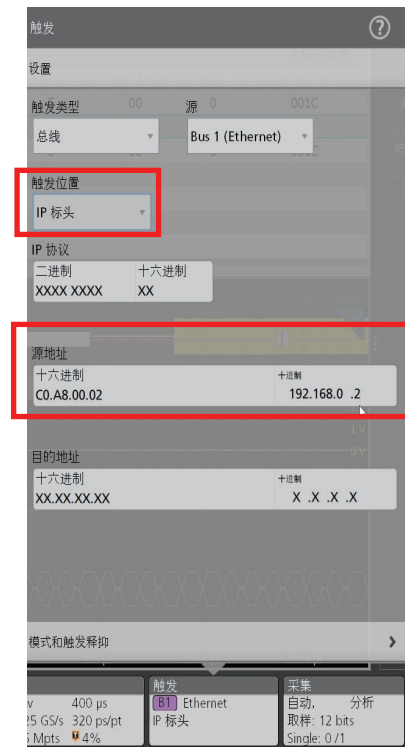


图 11：触发设置为指定 IP



图 12：示波器捕获并解码的 ping request 数据包

四、总结

软件和硬件总是存在一些隔阂。例如在以太网分析上，传统的计算机网络领域主要从软件层面介绍逻辑链路层及更高层的设计和实现，对于物理层的介绍比较简单。而传统的硬件领域对于数字信号往往只介绍简单的串行总线，并不会拿比较复杂的以太网作为例子。本文深入分析了 2 类常见的双绞线以太网的编码，并利用混合信号示波器的总线解码功能，查看并验证了以太网在物理层的信号传输情况。最后通过一个实战例子来对比了实际网络中软件接收到的数据和示波器捕获信号之间的一致性，从物理层揭示了以太网数据传输的机制。

参考文献

- [1] <https://en.wikipedia.org/wiki/Ethernet>
- [2] <https://en.wikipedia.org/wiki/ANSI/TIA-568>
- [3] <https://www.wireshark.org>
- [4] <https://en.wikipedia.org/wiki/4B5B>
- [5] https://en.wikipedia.org/wiki/MLT-3_encoding



泰克官方微信

如需所有最新配套资料，请立即与泰克本地代表联系！

或登录泰克公司中文网站：www.tek.com.cn

泰克中国客户服务中心全国热线：400-820-5835

泰克科技(中国)有限公司

上海市浦东新区川桥路1227号
邮编：201206
电话：(86 21) 5031 2000
传真：(86 21) 5899 3156

泰克北京办事处

北京市朝阳区酒仙桥路6号院
电子城·国际电子总部二期
七号楼2层203单元
邮编：100015
电话：(86 10) 5795 0700
传真：(86 10) 6235 1236

泰克上海办事处

上海市长宁区福泉北路518号
9座5楼
邮编：200335
电话：(86 21) 3397 0800
传真：(86 21) 6289 7267

泰克深圳办事处

深圳市深南东路5002号
信兴广场地王商业大厦3001-3002室
邮编：518008
电话：(86 755) 8246 0909
传真：(86 755) 8246 1539

泰克成都办事处

成都市锦江区三色路38号
博瑞创意成都B座1604
邮编：610063
电话：(86 28) 6530 4900
传真：(86 28) 8527 0053

泰克西安办事处

西安市二环南路西段88号
老三届世纪星大厦26层L座
邮编：710065
电话：(86 29) 8723 1794
传真：(86 29) 8721 8549

泰克武汉办事处

武汉市洪山区珞喻路726号
华美达大酒店702室
邮编：430074
电话：(86 27) 8781 2760

泰克香港办事处

香港九龙尖沙咀弥敦道132号
美丽华大厦808-809室
电话：(852) 2585 6688
传真：(852) 2598 6260

更多宝贵资源，敬请登录：WWW.TEK.COM.CN

© 泰克公司版权所有，侵权必究。泰克产品受到已经签发及正在申请的美国专利和外国专利保护。本文中的信息代替所有以前出版的材料中的信息。本文中的技术数据和价格如有变更，恕不另行通告。TEKTRONIX 和 TEK 是泰克公司的注册商标。本文中提到的所有其它商号均为各自公司的服务标志、商标或注册商标。

11/2021

