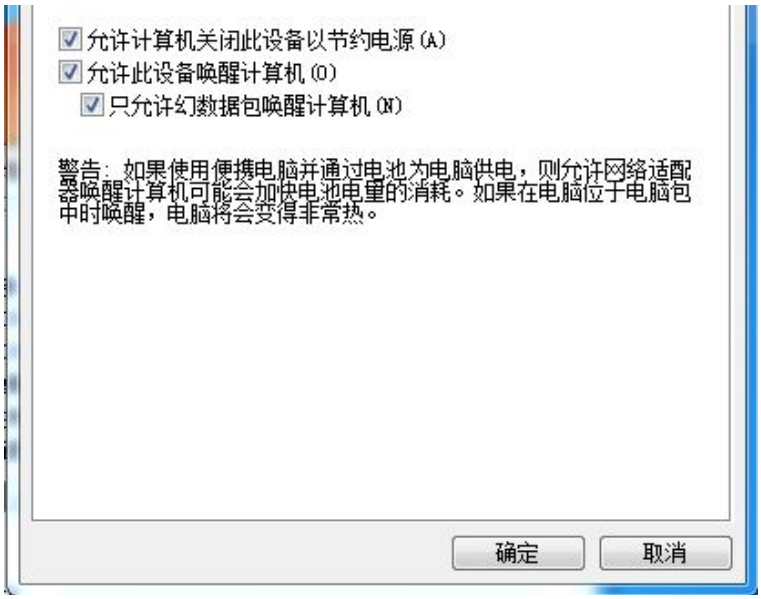
大年三十儿来研究一下计算机的远程唤醒（WOL）的 幻数据包（Magic Packet）

sina.com.cn

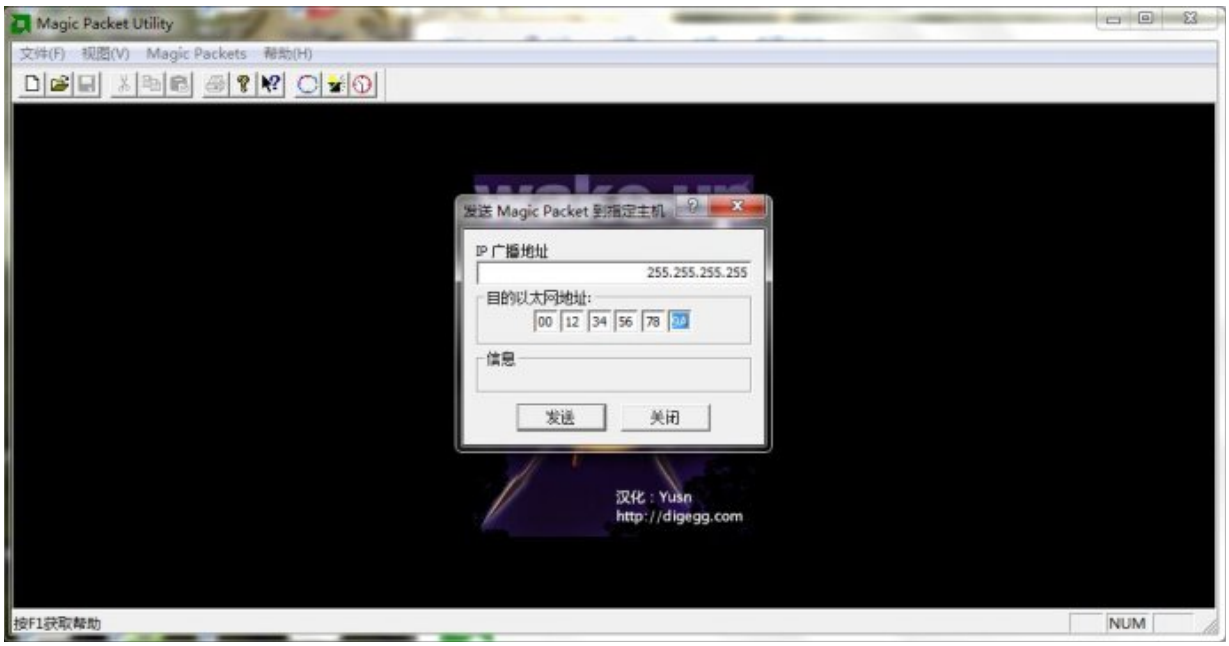
放假了，赶在年前给家里升级了千兆网络环境（内网）。各种布线、换件，实在是件体力活。

在调试网卡1Gbps速率协商的时候，发现网卡驱动设置里有个名为“Wake on Magic Packet”的选项（图），应该是做局域网远程唤醒计算机用的。之前没怎么关注过，不过前些天升级千兆网的时候顺便向楼上的奶奶家布置了一根网线，远程开机就成为潜在的需求了。



与“幻数据包”相同功能的还有一个“模式匹配（Pattern Match）”，暂时还不清楚，求高人解达。这里先说说我对前者学习到的一些皮毛。

用“Magic Packet”当关键字问度娘，找到了一些相关的资料。发现这个东西是AMD研发的协议，不过已经被所有的网卡支持了。AMD自己出了个"Magic Packet Utility"，图形化应用，可以方便的使用（图）。 当然，既然是学计算机的就不能满足于“能用”，研究原理当然更重要 [^o^].

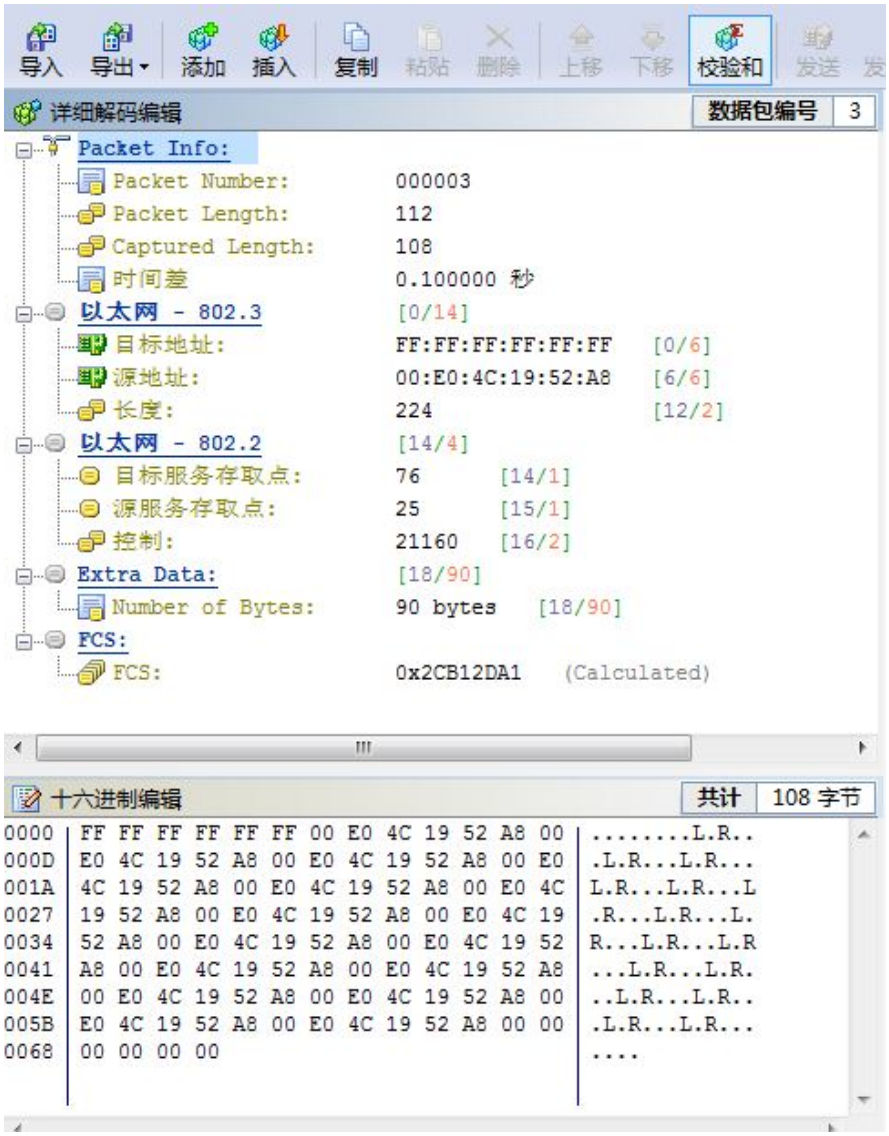


大致原理如下：在bios开启远程唤醒，且电源支持网卡供电的情况下，网卡会一直检测收到的数据。当收到一个特殊的幻数据包（Magic Packet）时，便会向BIOS发送开机信号。

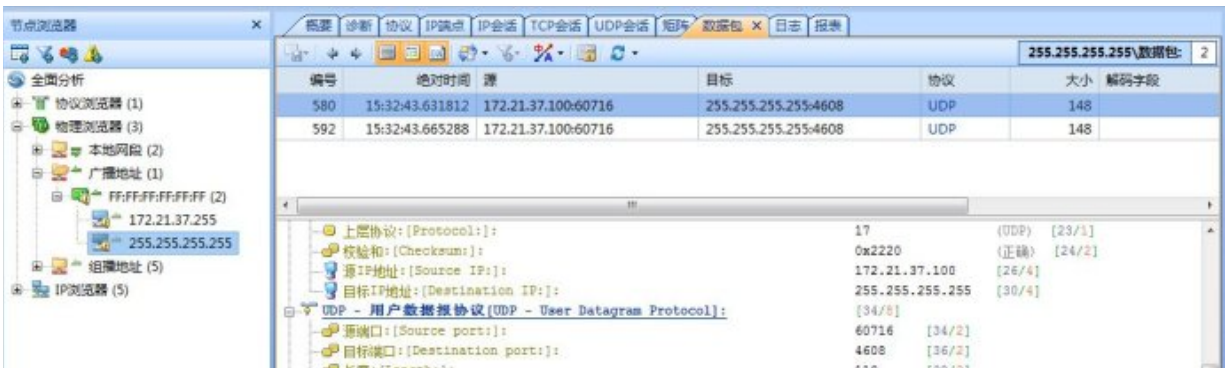
原理很简单，我也想自己尝试构建一个数据包进行测试。

搜到一篇帖子，大致说明了Magic Packet的内容格式：

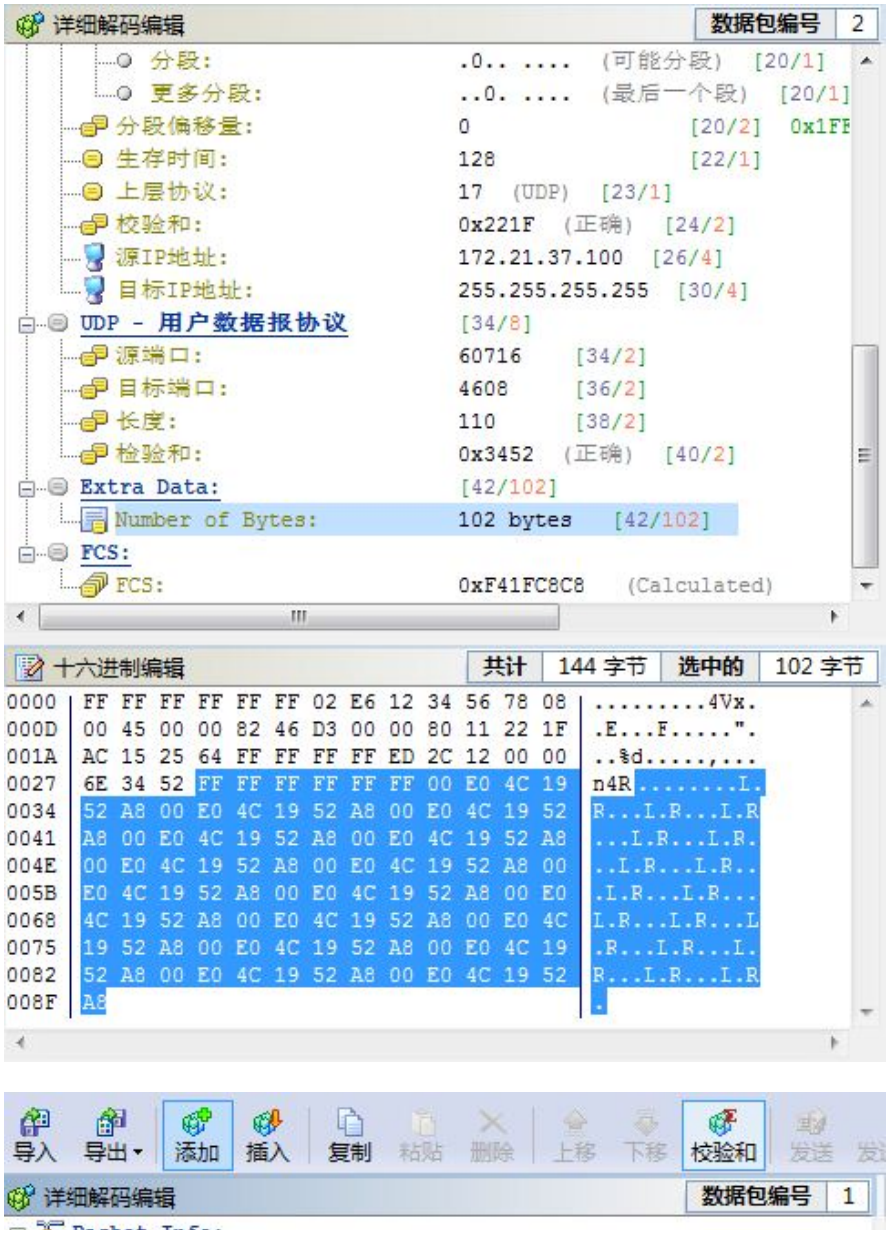
内容共108字节，前6字节是全FF填充，接下来的96字节填充被唤醒的网卡MAC地址（6字节MAC重复6次），最后6字节填写密码，无密码用00补位。
按照这个格式，我构建了如下的一个数据包（图）。

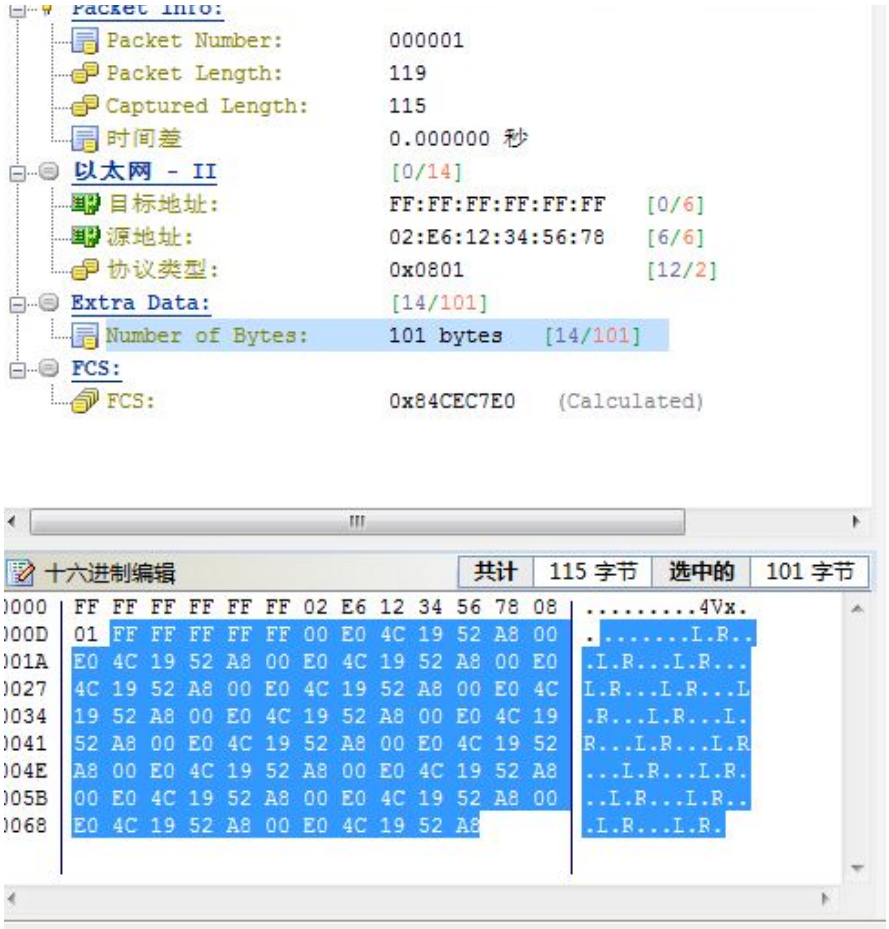


发送数据包测试，没唤醒。想不出为什么（当时脑残了），于是抓包看了看（图）。



开头赫然的帧封装，当时自己就囧了。啥封装都没有直接把内容扔上去当然不行了。抓到的数据包是UDP封装的，自己构建了一遍，果然OK。测试了一下TCP，IP封装，都可以，甚至直接封装在二层数据帧里都能唤醒计算机（图）！可见只要有这段内容，而且网卡能解开封装，唤醒就能实现。





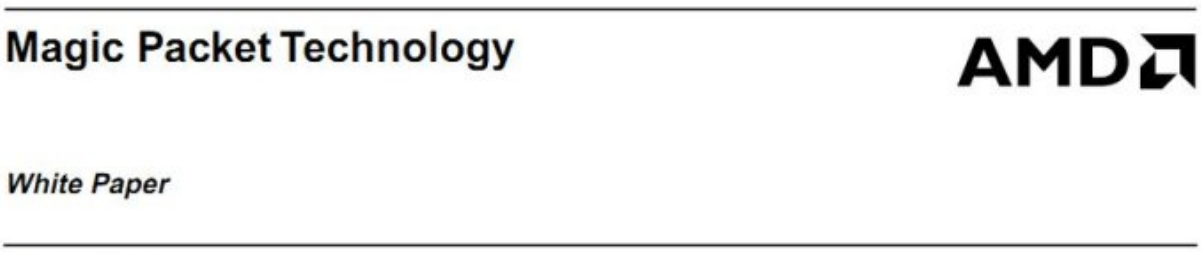
在构建数据包进行尝试的过程中，发现几点有意思的事情。

1. 抓到Magic Packet Utility包的96字节MAC后是空的，也就是说密码位可以省略，实际构建数据包证实。

2. 只要保证以太网封装是正确的，IP和TPC/UDP内容胡乱写也是可以的，伪造IP和端口反正没问题。但不知校验位不重新进行计算是否能过关，我这边包生成器自动计算更新FCS了，没法测试。

3. 以太网封装有三个部分，6字节目的MAC，6字节源MAC，2字节上层协议类型。其中，目的MAC只能用广播帧FF:FF:FF:FF:FF:FF，源MAC只能用发出端的MAC不可乱写。想了一下二层帧发送的原理，只要有交换机捣乱填写单播目的MAC就是徒劳，直连两台PC则可以单播，但是没有实际意义。**不明白为什么伪造的源MAC不可以，求解答。** 另外，上层协议可以瞎写写。（0800是IP协议，0806是ARP协议等等）写个0801没有对应协议，也就不需要上层封装，可以直接填充幻数据包内容。

做完测试又去AMD的官网搜了一下Magic Packet关键字，找到了《Magic Packet Technology White Paper》，白皮书里面写的很详细，对于构建幻数据包做了非常明确的交代，值得读一读。已发微盘共享。http://vdisk.weibo.com/s/25Hul



ABSTRACT

This white paper presents a description of the Magic Packet Technology and how it works. It also covers some issues involving the sleeping Green PC and how the Magic Packet Technology can be used to put a PC in a low-power state and still be manageable by a network system administrator.

SCOPE

The PC market has many forces influencing the design and implementation of PCs, operating systems, and peripheral devices. Most of the time, these forces are complementary, such as CPU performance and multimedia uses, or the desire for end users to have their machines backed up each night, and the Information Systems (IS) department's desire to maintain data integrity throughout the network.

However, sometimes the forces working on the PC market seem to be in direct conflict. One such example is the desire of the IS department to be able to do end node management (software updates, backups, etc.) and the US Government's desire, through the Energy

Below are details on the silicon implementation of Magic Packet Technology, as well as some of the system and software implications.

Magic Packet Technology Overview

The basic technical details of Magic Packet Technology are simple and easy to understand. There is also a second set of details, which will be implementation specific. In other words, silicon- or gate-level implementations of Magic Packet Technology may differ from AMD's approach and be completely interoperable, as long as the basic feature set is maintained.

Magic Packet Technology is a feature designed to be incorporated into an Ethernet controller. The basic fea-

AMD

SOURCE ADDRESS, DESTINATION ADDRESS (which may be the receiving station's IEEE address or a MULTICAST address which includes the BROADCAST address), and CRC. The specific sequence consists of 16 duplications of the IEEE address of this node, with no breaks or interruptions.

This sequence can be located anywhere within the packet, but must be preceded by a synchronization stream. The synchronization stream allows the scanning state machine to be much simpler. The synchronization stream is defined as 6 bytes of FFh. The device will also accept a MULTICAST frame, as long as the 16 duplications of the IEEE address match the address of the machine to be awakened.

If the IEEE address for a particular node on the network was 11h 22h 33h 44h 55h 66h, then the LAN controller would be scanning for the data sequence (assuming an Ethernet Frame):

DESTINATION SOURCE MISC FF FF FF FF FF FF 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 11 22 33 44 55 66 MISC CRC

Magic Packet Mode Disable

It should not take much design effort, time, or silicon area to add the Magic Packet Technology to an existing Ethernet controller. This was one of the primary reasons for going with a solution that uses the IEEE address as the identifier for the Magic Packet frame, since the circuitry already exists to match this data stream.

SYSTEM IMPLEMENTATION

To utilize the Magic Packet Technology in a PC, there are several modifications which must be done to ensure proper operation of the feature. Let's take the case of a motherboard implementation, where the Ethernet controller will be located on the motherboard, with an RJ-45 connector coming out the back of the computer. This implementation is becoming more and more common as Ethernet establishes itself as a de facto standard for the desktop LAN.

First, let's address the hardware steps necessary to allow the Ethernet controller to wake up the system when it receives a Magic Packet frame. Most desktop PC's these days already have pretty advanced power management circuitry either built into the chipset or as a separate functional block on the motherboard. In this example, it is a simple matter to connect one of the LED pins, such as LED 3, into the power management circuitry. The Magic Packet frame indication becomes just another possible alert to the power management cir-

白皮书里还介绍了如何跨子网实现远程唤醒，暂时没精力看完，以后有空继续学习。
在搜索的过程中看到了微软MSDN的一个连接（点这里），对Magic Packet有一个狭义的说明。

The magic packet is a UDP packet that is encapsulated in an IPv4 or IPv6 datagram. The IP datagram is sent as a link layer broadcast packet.

If IPv4 is used, the destination IP address MUST be the IP subnet broadcast address.

If IPv6 is used, the destination IP address MUST be FF:2::1.

The payload of the UDP packet MUST adhere to the AMD magic packet specification.

文中特意强调幻数据包是个UDP包，而我在测试中得到结论，内容在任何网卡可解开的封装中都可以。

查了一些论坛的资料，原因有三：

封装到帧的障碍：Windows 本身并没有提供发送以太网帧的接口，需要第三方软件，如 winpcap

封装到IP的障碍：唤醒网络封包直接作为数据封装在IP协议里，需要原始套接字编程，要构造IP头，Windows 对原始套接字编程做了限制

封装到TCP的障碍：不支持255.255.255.255的广播

综上，UDP既能广播又容易编程，被广泛采用。毕竟不是谁都闲的用包生成器做测试的 --|

最后，附上网络中广为流传的一份SendMagic.cpp的源码，用C++实现的，简洁易懂，很不错。
希望能够多和大家交流！欢迎拍砖~