几年前的某天晚上 9 时，两个“大虾”进入一个聊天室，提议里面的 50 多个网民“去响应号召，做爱国的事”，以下是原话摘录：

大虾甲：今晚 10 点，大家一起去 ping 白宫！

大虾乙：嗯嗯！ping 死白宫！

网民：怎么做？

大虾甲：你怎么这么笨？开 MS-DOS 窗口，输入 ping xxx.xxx.xxx.xxx -l 65500 -t 就可以了！

网民：这样有什么用？

大虾甲：只要这样做，白宫网站就进不去了。

网民：哦~~原来如此~~~这样做是什么原理？高手可以解释一下吗？

大虾甲：这个嘛……还是让他来说吧！

大虾乙：这个……这个……咳，总之别问这么多，照着做就是了，上头说过好像是什么 DOS 攻击吧，这样做，白宫网站的服务器就会垮掉。

大虾甲：总之到时候你们一起这样做就可以了！10 点准时开始，我们先去准备了!

网民：不懂……

不懂归不懂，当晚 10 点，爱国的网民们一起用上面“高手”给出的命令开始了雄伟的“爱国反击战”——一场无聊的闹剧！

他们这样做是什么原理？那样的“攻击”有效吗？要解释这些，就要从 ICMP 协议说起。

一、什么是 ICMP 协议？

ICMP 全称 Internet Control Message Protocol（网际控制信息协议）。提起 ICMP，一些人可能会感到陌生，实际上，ICMP 与我们息息相关。在网络体系结构的各层次中，

都需要控制，而不同的层次有不同的分工和控制内容，IP 层的控制功能是最复杂的，主要负责差错控制、拥塞控制等，任何控制都是建立在信息的基础之上的，在基于 IP 数据报的网络体系中，网关必须自己处理数据报的传输工作，而 IP 协议自身没有内在机制来获取差错信息并处理。为了处理这些错误，TCP/IP 设计了 ICMP 协议，当某个网关发现传输错误时，立即向信源主机发送 ICMP 报文，报告出错信息，让信源主机采取相应处理措施，它是一种差错和控制报文协议，不仅用于传输差错报文，还传输控制报文。

二、ICMP 报文格式

ICMP 报文包含在 IP 数据报中，属于 IP 的一个用户，IP 头部就在 ICMP 报文的前面，所以一个 ICMP 报文包括 IP 头部、ICMP 头部和 ICMP 报文（见图表，ICMP 报文的结构和几种常见的 ICMP 报文格式），IP 头部的 Protocol 值为 1 就说明这是一个 ICMP 报文，ICMP 头部中的类型（Type）域用于说明 ICMP 报文的作用及格式，此外还有一个代码（Code）域用于详细说明某种 ICMP 报文的类型，所有数据都在 ICMP 头部后面。RFC 定义了 13 种 ICMP 报文格式，具体如下：

类型代码 类型描述

0 响应应答（ECHO-REPLY）

3 不可到达

4 源抑制

5 重定向

8 响应请求（ECHO-REQUEST）

11 超时

12 参数失灵

13 时间戳请求

14 时间戳应答

15 信息请求（*已作废）

16 信息应答（*已作废）

17 地址掩码请求

18 地址掩码应答

其中代码为 15、16 的信息报文已经作废。

下面是几种常见的 ICMP 报文：

1.响应请求

我们日常使用最多的 ping，就是响应请求（Type=8）和应答（Type=0），一台主机向一个节点发送一个 Type=8 的 ICMP 报文，如果途中没有异常（例如被路由器丢弃、目标不回应 ICMP 或传输失败），则目标返回 Type=0 的 ICMP 报文，说明这台主机存在，更详细的 tracert 通过计算 ICMP 报文通过的节点来确定主机与目标之间的网络距离。

2.目标不可到达、源抑制和超时报文

这三种报文的格式是一样的，目标不可到达报文（Type=3）在路由器或主机不能传递数据报时使用，例如我们要连接对方一个不存在的系统端口（端口号小于 1024）时，将返回 Type=3、Code=3 的 ICMP 报文，它要告诉我们：“嘿，别连接了，我不在家的！”，常见的不可到达类型还有网络不可到达（Code=0）、主机不可到达（Code=1）、协议不可到达（Code=2）等。源抑制则充当一个控制流量的角色，它通知主机减少数据报流量，由于 ICMP 没有恢复传输的报文，所以只要停止该报文，主机就会逐渐恢

复传输速率。最后，无连接方式网络的问题就是数据报会丢失，或者长时间在网络游荡而找不到目标，或者拥塞导致主机在规定时间内无法重组数据报分段，这时就要触发 ICMP 超时报文的产生。超时报文的代码域有两种取值：Code=0 表示传输超时，Code=1 表示重组分段超时。

3.时间戳

时间戳请求报文（Type=13）和时间戳应答报文（Type=14）用于测试两台主机之间数据报来回一次的传输时间。传输时，主机填充原始时间戳，接收方收到请求后填充接收时间戳后以 Type=14 的报文格式返回，发送方计算这个时间差。一些系统不响应这种报文。

三、回到正题：这样的攻击有效吗？

在前面讲过了，ping 使用的是 ECHO 应答，不知道大家注意过没有，ping 的返回很慢，用 NetXRAY 抓包仅为 1--5 包/秒，这是为什么呢？事实上，ICMP 本身并不慢（由于 ICMP 是 SOCK_RAW 产生的原始报文，速度比 SOCK_STREAM 的 SYN 和 SOCK_DGRAM 的 UDP 要快几乎 10 倍！），这样的速度是 ping 程序故意延迟的（为什么？M$可不想每个人都能用 ping 来干坏事），同样，我测试过一些号称“ping 洪水”的程序，发现它们的效率和 ping.exe 没什么两样，经过 Dependency Walker 查看程序调用的函数发现，他们用的是 icmp.dll 提供的 IcmpSendEcho 这个 API，这个函数是计算 ECHO 时间的，速度当然慢！而那两个“高手”号召的 ping 攻击实际上就是为了实现 ICMP 洪水攻击，但是他们用的方法……想想洪水的速度和山涧小溪的速度相差多少吧！就用 ping.exe 和 IcmpSendEcho 这种小溪慢慢流淌的速度能做什么？还不是让人家看笑话！这种攻击根本就是浪费自己的时间！（如今还经常有人问 ping -l 65500 -t 的攻击威力如何……哎，悲哀啊悲哀……）

四、什么是 ICMP 洪水？

1.ICMP 洪水的成因

ping.exe 和 IcmpSendEcho 速度慢的另一个原因是它们必须等待目标主机返回 REPLY 信息，这个过程需要花费大量时间，而 Flood——洪水，顾名思义，是速度极快的，当一个程序发送数据包的速度达到了每秒 1000 个以上，它的性质就成了洪水产生器，洪水数据是从洪水产生器里出来的，但这样还不够，没有足够的带宽，再猛的洪水也只能像公路塞车那样慢慢移动，成了鸡肋。要做真正的洪水，就需要有一条足够宽的高速公路才可以。极慢的发送速度+56Kbps 小猫等于什么？等于一个未关紧的水龙头，根本没用。

由于 ping.exe 无法提速，这就需要专门的工具来做洪水了。足够快的数据包速度+足够的带宽，这才是洪水。

2.实现 ICMP 洪水的前提

最大的前提是攻击者的速度！如果你要用 56K 拨号去攻击一个 512Kbps ADSL 用户，后果和一只蚂蚁伸腿想绊倒大象的天方夜谭是一样的！其次是你的机器运行速度和数据吞吐量，由于涉及 IP 校验和的计算（先设置头校验和域的数值为 0，然后对整个数据报头按每 16 位求异或，再把结果取反，就得到了校验和），如果数据处理能力不够，在这步就慢了一个级别，效果当然大打折扣。最后就是目标机器的带宽！如果对方比你大很多（例如你 2M ADSL，别人用 DDN 或 T1），那么任何 Flood 都是无病呻吟，挠痒都不够！（希望不要再问“小金，你的 R-Series 怎么不好用啊”、“我用小金的 AnGryPing 攻击别人半天都没事！”、“独裁者的攻击怎么无效啊？”这样的问题了，天啊，我头都大了！）

还有许多人都忽略的问题：发送的速度与数据包大小成反比，而且太大的数据包会被路由器等设备过滤掉！找到一个合适的数据包大小，对提高 Flood 的效率有很大帮助！

3.洪水——两败俱伤的攻击方式

别以为洪水无所不能，实际上，你展开洪水攻击时，攻击程序在消耗对方带宽和资源时，也在消耗你的带宽和资源。这只是个看谁撑得住的攻击而已。实际上，有经验的攻击者都是用被控制的服务器（肉鸡）来代替自己的机器发动攻击的，不到万不得已或者你对自己的机器网速有自信，否则尽量少用自己的机器来拼搏！

五、不同方式的 ICMP 洪水

1.直接 Flood

要做这个的首要条件是你的带宽够，然后就是要一个好用的 ICMP Flooder，别用 ping.exe 那种探路用的垃圾，例如我以前发布的 AnGryPing，发包速度达到 6000---9000 包/秒（512 Kbps ADSL），默认是 32bytes 的 ECHO 报文洪水，用它即使不能 flood 别人下去，防火墙也叫得够惨的了。直接攻击会暴露自己 IP（如果对方没有还击能力那还无所谓，固定 IP 用户不推荐使用这种 Flood），直接 Flood 主要是为了顾及 Win9x/Me 不能伪造 IP 的缺陷，否则一般还是别用为妙。

简单示意：

ICMP

攻击者[IP=211.97.54.3]---------->受害者[截获攻击者 IP=211.97.54.3]==>换 IP 回来反击，嘿嘿

2.伪造 IP 的 Flood

如果你是 Win2000/XP 并且是 Administrator 权限，可以试试看 FakePing，它能随意伪造一个 IP 来 Flood，让对方摸不到头脑，属于比较隐蔽阴险的 Flood。

简单示意：

伪造 IP=1.1.1.1 的 ICMP

攻击者[IP=211.97.54.3]---------->受害者[截获攻击者 IP=1.1.1.1]==>倒死

3.反射

用采取这种方式的第一个工具的名称来命名的“Smurf”洪水攻击，把隐蔽性又提高了一个档次，这种攻击模式里，最终淹没目标的洪水不是由攻击者发出的，也不是伪造 IP 发出的，而是正常通讯的服务器发出的！

实现的原理也不算复杂，Smurf 方式把源 IP 设置为受害者 IP，然后向多台服务器发送 ICMP 报文（通常是 ECHO 请求），这些接收报文的服务器被报文欺骗，向受害者返回 ECHO 应答（Type=0），导致垃圾阻塞受害者的门口……

从示意图可以看出，它比上面两种方法多了一级路径——受骗的主机（称为“反射源”），所以，一个反射源是否有效或者效率低下，都会对 Flood 效果造成影响！

简单示意：

伪造受害者的 ICMP 应答

攻击者[IP=211.97.54.3]---------->正常的主机---------->受害者[截获攻击者 IP=……网易？！]==>哭啊……

以上是几种常见的 Flood 方式，在测试中，我发现一个有趣的现象：一些防火墙只能拦截 ECHO 请求（Ping）的 ICMP 报文，对于其他 ICMP 报文一概睁只眼闭只眼，不知道其他防火墙有没有这个情况。所以想神不知鬼不觉对付你的敌人时，请尽量避开直接 ECHO Flood，换用 Type=0 的 ECHO 应答或 Type=14 的时间戳应答最好，其他类型的 ICMP 报文没有详细测试过，大家可以试试看 Type=3、4、11 的特殊报文会不会有更大效果。

六、ICMP Flood 能防吗？

先反问你一个问题：洪水迅猛的冲来时，你能否拿着一个脸盆来抵挡？（坐上脸盆做现代鲁宾逊倒是个不错的主意，没准能漂到 MM 身边呢）

软件的网络防火墙能对付一些漏洞、溢出、OOB、IGMP 攻击，但是对于洪水类型的攻击，它们根本无能为力，我通常对此的解释是“倾倒垃圾”：“有蟑螂或老鼠在你家门前逗留，你可以把它们赶走，但如果有人把一车垃圾倾倒在你家门口呢？”前几天看到 mikespook 大哥对此有更体面的解释，转载过来——“香蕉皮原理：如果有人给你一个香蕉和一个香蕉皮你能区分，并把没有用的香蕉皮扔掉。（一般软件防火墙就是这么判断并丢弃数据包的。）但是如果有人在同一时间内在你身上倒一车香蕉皮，你再能区分有用没用也没啥作用了~~因为你被香蕉皮淹没了~~~~（所以就算防火墙能区分是 DoS 的攻击数据包，也只能识别，根本来不及丢弃~~死了，死了，死了~~）”

所以，洪水没法防！能做的只有提高自己的带宽和预防洪水的发生（虽然硬件防火墙和分流技术能做到，但那价格是太昂贵的，而且一般人也没必要这样做）。

如果你正在被攻击，最好的方法是抓取攻击者 IP（除非对方用第一种，否则抓了没用——假的 IP）后，立即下线换 IP！（什么？你是固定 IP？没辙了，打电话找警察叔叔吧）

七、被 ICMP Flood 攻击的特征

如何发现 ICMP Flood？

当你出现以下症状时，就要注意是否正被洪水攻击：

1.传输状态里，代表远程数据接收的计算机图标一直亮着，而你没有浏览网页或下载

2.防火墙一直提示有人试图 ping 你

3.网络速度奇慢无比

4.严重时系统几乎失去响应，鼠标呈跳跃状行走

如果出现这些情况，先不要慌张，冷静观察防火墙报警的频率及 IP 来确认是否普通的 Ping 或是洪水，做出相应措施（其实大多数情况也只能换 IP 了）。

1.普通 ping

这种“攻击”一般是对方扫描网络或用 ping -t 发起的，没多大杀伤力（这个时候，防火墙起的作用就是延迟攻击者的数据报发送间隔时间，请别关闭防火墙！否则后果是严重的！），通常表现如下：

==========

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:24] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:26] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:30] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

==========

这么慢的速度，很明显是由 ping.exe 或 IcmpSendEcho 发出的，如果对方一直不停的让你的防火墙吵闹，你可以给他个真正的 ICMP Flood 问候。

2.直接 Flood

这是比较够劲的真正意义洪水了，防火墙的报警密度会提高一个数量级：

==========

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

```
[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。
```

```
[13:09:20] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:21] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:21] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:21] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:21] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:21] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:21] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:21] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。

[13:09:21] 61.151.252.106 尝试用 Ping 来探测本机，
该操作被拒绝。
===========================================================
```

这时候你的防火墙实际上已经废了，换个 IP 吧。

3.伪造 IP 的 Flood

比较厉害的 ICMP Flood，使用的是伪造的 IP 而且一样大密度，下面是 the0crat 用 56K 拨号对我的一次攻击测试的部分数据（看看时间，真晕了，这可是 56K 小猫而已啊）

==========

[18:52:12] 1.1.1.1 尝试用 Ping 来探测本机，
该操作被拒绝。

[18:52:12] 1.1.1.1 尝试用 Ping 来探测本机，
该操作被拒绝。

[18:52:12] 1.1.1.1 尝试用 Ping 来探测本机，
该操作被拒绝。

[18:52:12] 1.1.1.1 尝试用 Ping 来探测本机，
该操作被拒绝。

[18:52:12] 1.1.1.1 尝试用 Ping 来探测本机，
该操作被拒绝。

[18:52:12] 1.1.1.1 尝试用 Ping 来探测本机，
该操作被拒绝。

[18:52:12] 1.1.1.1 尝试用 Ping 来探测本机，
该操作被拒绝。

[18:52:12] 1.1.1.1 尝试用 Ping 来探测本机，
该操作被拒绝。

==========

无言……

4、反射 ICMP Flood

估计现在 Smurf 攻击还没有多少人会用（R-Series 的 RSS.EXE 就是做这事的，RSA.EXE 和 RSC.EXE 分别用作 SYN 反射和 UDP 反射），所以这种方法还没有大规模出现，但 Smurf 是存在的！而且这个攻击方法比前面几种更恐怖，因为攻击你的是大网站（或一些受苦受难的服务器）！

我正在被网易、万网和新浪网站攻击中（懒得修改策略，直接用其他工具抓的。实际攻击中，反射的 IP 会多几倍！）

==========

[15:26:32] RECV:ICMP Packet from 202.108.37.36 (Type=0,Code=0,Len=52)
[15:26:32] RECV:ICMP Packet from 202.108.36.206 (Type=0,Code=0,Len=52)
[15:26:32] RECV:ICMP Packet from 210.192.103.30 (Type=0,Code=0,Len=52)
[15:26:32] RECV:ICMP Packet from 202.108.37.36 (Type=0,Code=0,Len=52)
[15:26:32] RECV:ICMP Packet from 210.192.103.30 (Type=0,Code=0,Len=52)
[15:26:32] RECV:ICMP Packet from 202.108.36.206 (Type=0,Code=0,Len=52)

[15:26:32] RECV:ICMP Packet from 202.108.37.36 (Type=0,Code=0,Len=52)

[15:26:32] RECV:ICMP Packet from 210.192.103.30 (Type=0,Code=0,Len=52)

[15:26:32] RECV:ICMP Packet from 210.192.103.30 (Type=0,Code=0,Len=52)

[15:26:32] RECV:ICMP Packet from 202.108.36.206 (Type=0,Code=0,Len=52)

[15:26:33] RECV:ICMP Packet from 210.192.103.30 (Type=0,Code=0,Len=52)

[15:26:33] RECV:ICMP Packet from 202.108.36.206 (Type=0,Code=0,Len=52)

[15:26:33] RECV:ICMP Packet from 202.108.37.36 (Type=0,Code=0,Len=52)

[15:26:33] RECV:ICMP Packet from 202.108.37.36 (Type=0,Code=0,Len=52)

[15:26:33] RECV:ICMP Packet from 202.108.36.206 (Type=0,Code=0,Len=52)

[15:26:33] RECV:ICMP Packet from 210.192.103.30 (Type=0,Code=0,Len=52)

[15:26:33] RECV:ICMP Packet from 202.108.37.36 (Type=0,Code=0,Len=52)

[15:26:33] RECV:ICMP Packet from 202.108.36.206 (Type=0,Code=0,Len=52)

[15:26:33] RECV:ICMP Packet from 210.192.103.30 (Type=0,Code=0,Len=52)

==========

可以看出，攻击者使用的是 32bytes 的 ECHO 请求，所以服务器返回 52-20=32bytes 的 REPLY 报文，在这个情况下，是不会报警的。

还是那句话，报警也没用了。

八、自己编写 ICMP Flooder

以上说的都是理论，如何才能自己写一个呢？相信很多人已经跃跃欲试了，下面就用 VC6.0 来写一个直接的 ICMP Flooder（能在 Win98/Me 环境使用）……先等等——最重要的是原理。

1.程序原理

当然不能用 IcmpSendEcho 来做，我们必须自己从最原始的 IP 报文里做一个。构造一个 SOCK_RAW 报文后，填充 ICMP 数据和计算校验和（CheckSum），循环 sendto 发出去就完成了，so easy！

2.ICMP 报文的声明

一个 ICMP 报文包括 IP 头部、ICMP 头部和 ICMP 报文，用 IPPROTO_ICMP 创建这个类型的 IP 包，用以下结构填充：

```
typedef struct _ihdr
{
BYTE i_type; //8 位类型
BYTE i_code; //8 位代码
USHORT i_cksum; //16 位校验和
USHORT i_id; //识别号
USHORT i_seq; //报文序列号
ULONG timestamp; //时间戳
}ICMP_HEADER;
```

这样我们就声明了一个 ICMP 报文结构，就等后面的填充了