# MSN协议

[MSN协议 1](#_Toc264109787)

[MSN协议分类： 2](#_Toc264109788)

[MSN架构： 2](#_Toc264109789)

[MSN Client 2](#_Toc264109790)

[MSN Dispatch Server 2](#_Toc264109791)

[MSN Notification Server (NS) 2](#_Toc264109792)

[MSN Switchboard Server (SB) 2](#_Toc264109793)

[MSN建立连接并通信的主要步骤： 3](#_Toc264109794)

[协议基础： 6](#_Toc264109795)

[编码： 6](#_Toc264109796)

[URL编码 6](#_Toc264109797)

[XML编码 7](#_Toc264109798)

[命令： 7](#_Toc264109799)

[名 字 10](#_Toc264109800)

[通知服务器相关协议： 13](#_Toc264109801)

[**通知服务器** 19](#_Toc264109802)

[**The Passport Nexus** 20](#_Toc264109803)

[**The Login Server** 21](#_Toc264109804)

[会 话示例 45](#_Toc264109805)

[交换板服务器相关协议： 51](#_Toc264109806)

[会 话示例 58](#_Toc264109807)

[MSN客户端相关的协议 64](#_Toc264109808)

## MSN协议分类：

1：MSN Messenger

客户端，**通知服务器**之间的通信协议

适用类型举例：上线，下线时候的通知，实时信息更新等。

目前MSN Messenger支持客户端使用：MSNP8，MSNP9，MSNP10，MSNP11，MSNP12，MSNP13，MSNP14，MSNP15,MSNP16这些协议版本。

2：MSN Client

客户端，客户端之间的通信协议（**交换板服务器**作为中介）

适用类型举例：客户端之间的聊天，多人聊天等

目前MSN Client协议主要有三个版本“MSNC0”、“MSNC1”、“MSNC2”

注：MSN客户端除了文件传输和语音聊天是直接的"点对点"通信之外,其它所有的情形全部通过服务器中转。

## MSN架构：

### MSN Client

MSN的客户端，用户通过它进行端到端的沟通

### MSN Dispatch Server

派遣服务器，简称DS，客户端最初连接的服务器，负责给客户端分配合适的通知服务器。有固定的域名与端口。完成派遣任务后切断TCP连接。（在高版本中已 不用）

### MSN Notification Server (NS)

通知服务器，简称NS，建立到通知服务器的连接是MSN Messenger会话的基础，因为它保留着你的会话期间在线信息：如果你离线，对于你的伙伴来说你也将离线。通知服务器的目的主要就是保留你的在线信 息，还有其他你所关心的重要人员的信息。通知服务器同样也提供其他通知服务，如hotmail的新邮件提示和让你创建（或者加入）交换会话等。当你直接加 入一个交换会话中时，你应该打开一个到交换板的新的连接，并且保持通知服务器打开。

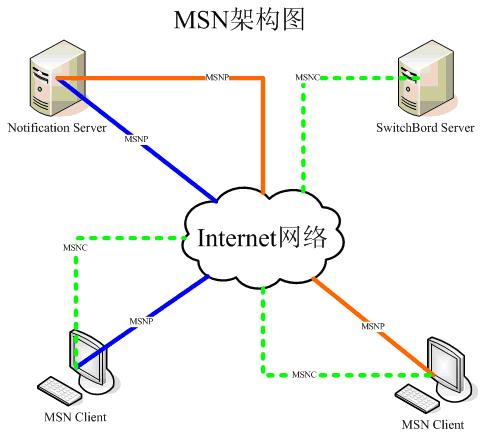
### MSN Switchboard Server (SB)

接线服务器，也叫交换板，客户端之间聊天使用的中转服务器，每开一个聊天窗口，客户端和服务器就建立一个TCP会话。开始聊天前，发起方必须先申请并连接 这个服务器。换句话说，每个MSN中的用户对应连接到一个共享交换板的会话中。在同一时刻有（分别）两个会话意味着要同时连接两个交换服务器。在MSN Messenger中不能直接在各用户间建立连接，并且交换板的作用就像你与对话人之间的代理一样。

如果你愿意的话，一个交换板会话可以有很多人加入，这不像一对一谈话，两个以上的人员将不被接受（client-client）。

SB也可以邀请其他服务，例如文件传输、视频会议。移动寻呼是仅有的通信格式之一，并不会在SB服务器上发生。

注意：SB和NS结合的并不十分紧密。例如，当交换板会话中变更他（她）的显示名时，交换板发送的信息或命令中仍旧使用旧名称。另外某个用户从NS中退 出，所有的交换板会话都将保持打开状态直到客户端明确的关闭他们。



### MSN建立连接并通信的主要步骤：

a：MSN客户端首先连接gateway网关，从网关的反馈取得通知服务器地址

b：MSN客户端连接通知服务器并完成login操作

c：MSN客户端要想去和其它MSN客户端通信，**通过通知服务器取得交换板服务器地址**

d：MSN客户端通过交换板服务器与其它MSN客户端进行通信，完成相关操作



**在详细介绍之前首先简单介绍一下登陆MSN的流程：**

启动msn  
　 　初始化连接  
　　（1） 连接的第一步是连接dispatch服务器。打开一个tcp socket，通过ip地址messenger.hotmail.com和1863端口连接dispatch服务器。  
　　（2） 当连接dispatch服务器成功后，本机客户端向dispatch服务器发送一个ver命令，以msnp7 msnp6 msnp5 msnp4 cvr0（协议版本）作为参数。服务器收到请求后，同样返回ver命令，如果参数为0，表示协商失败。  
　　（3） 本机客户端收到回复后，向服务器发送一个无参数的inf请求，请求一个认证算法。当dispatch服务器收到后返回md5。  
　　（4） 本机客户端根据返回的参数向服务器发送usr命令，其中传入两个参数，第一个为服务器返回的md5，第二个参数为客户申请登陆的电子邮件地址。服务器根据 收到的请求返回一个xfr命令，把notification服务器的ip地址和端口作为参数返回给客户端。  
　　（5） 最后客户端根据ip地址和端口去连接notification服务器。以下是客户端和dispatch服务器的实际通信过程。  
　　 connect: messenger.hotmail.com 1863  
　　>>> ver 0 msnp7 msnp6 msnp5 msnp4 cvr0  
　　<<< ver 0 msnp7 msnp6 msnp5 msnp4 cvr0  
　 　>>> inf 1  
　　<<< inf 1 md5  
　　>>> usr 2 md5 i [email]example@passport.com[/email]  
　　<<< xfr 2 ns 64.4.12.132:1863 0  
　　disconnect  
　　  
　　连接notification服务器  
　　连接 notification服务器成功后，前三步执行的操作与dispatch服务器相同。  
　　（6） 同样本机客户端根据返回的参数向notification服务器发送usr命令，其中传入两个参数，第一个为notification服务器返回的 md5，第二个参数为客户登陆的电子邮件地址。服务器收到请求后返回usr ，包含两个参数 md5 s #.#。 #.# 为 md5 hash。  
　 　（7） 客户端根据收到的答复后再次发送一个usr，参数为md5 s #。其中#为上次服务器返回的md5 hash的小写16进制。服务器收到后返回usr，参数为ok user@host name 1。user@host为用户登陆的电子邮件地址，name为用户的映射名。  
　　（8） 当用户成功登陆msn后，客户端向服务器发送一个chg请求，请求服务器修改新登陆用户的状态，参数为nln。参数nln表示在线，这是每个用户登陆后需 要做的第一步初始化用户状态。以下为notification服务器与客户端之间的通信过程。  
　　connect: 64.4.12.132 1863  
　　>>> ver 3 msnp7 msnp6 msnp5 msnp4 cvr0  
　　 <<< ver 3 msnp7 msnp6 msnp5 msnp4 cvr0  
　　>>> inf 4  
　 　<<< inf 4 md5  
　　>>> usr 5 md5 i [email]example@passport.com[/email]  
　　<<< usr 5 md5 s 1013928519.693957190  
　　>>> usr 6 md5 s 23e54a439a6a17d15025f4c6cbd0f6b5  
　　<<< usr 6 ok [email]example@passport.com[/email] my%20screen%20name 1  
　　 >>> chg 7 nln  
　　<<< chg 7 nln  
　　continue session . . .

## 协议基础：

### 编码：

在MSN服务器中发送和接收的编码为UTF-8编码，一种ASCII兼容的多语言编码，可以描述两个及以上字节的非ASCII字符。当有必要在屏 幕上显示多语言时，你仅需要担心UTF-8和ASCII的区别，届时你可以看看你的编程环 境是否支持Unicode编码（如果你这样的话，也只好如此了）。

如果你发送接受纯文本信息而没有带“charset=UTF-8”参数，则将默认为ISO 8859-1编 码，一个ASCII兼容编码，在西欧使用的非ASCII字符描述为单 字节的编码。如果你指定另外的字符集即（如charset=KOI8-R），官方客户端 将忽略你的信息。官方客户端发送的信息中总是会包含charset=UTF-8，所以你也必须这 样做。

### URL编码

协议中许多场合，文本需要进行URL编码（可以查阅URL相关），昵称，显示名，组名，电话号码都是其中需要编码的示例。URL编码用来确信参数的详细信息中不包含任何空格、换行、或者其他非法字符。

URL编码在RFC 1738的2.2节定义。基本上，它替换特殊字符为一个百分号%接着两个十六进制字符。如，空格变为%20，百分号变为%25，换行变为%0A，回车变为%0D。

至于URL应该应用到哪里，RFC告诉我们所有字符除了数字、字母和“$-\_.+!\*’(),;/?:@=&”都应该使用URL编码。实际上，你 仅需对十六进制值20及以下的字符（也就是空格及以下），%（十六进制值为25）进行编码，但是你 如果愿意你可以编码其他字符。

由于官方客户端解码每个字符，而且并不针对某些（如%25和%20），所以其他客户端也必须对每个字符进 行解码。

如果你确需要对多字节UTF-8字符进行URL编码，你应该一次取一个字节来编码，如UTF-8值为D786的字符，应该编码为“%D7%86”，而不是“%D786”。 因此，当解码一个串的时候，应该首先进行URL解码，然后在转换到UTF-8。

### XML编码

XML是“eXtensible Markup Language”的缩写，有点像HTML的归纳。在MSN Messenger中用到了XML。在XML编码的文本中，&必须替换成&amp;。无论哪里出现了URL编码的特殊字符“%NN”（NN是字符的十六进制值），XML编码将用“&#xNN;”替换。官方的客户端把“~^=[{}\|;:?” 作为特殊字符，但服务器并不要求如此。

### 命令：

客户端与服务器间信息都是以命令格式传递的。命令被描述为三个字符、所有字母大写的命令代号。所有 一般命令都有一个事务ID并且以新行结束。客户端发送的命令一般会使服务器响应一个及以上的命令。

**有四种特殊类型的命令，它们的表现略不同于一般命令。有效载荷命令可以跨越多行。错误命令的命令代 码部分的字母替换为数字。异步命令是不经客户端明确请求由服务器端发送的，而且并不包含事务ID。最后是PNG命令和一些SYN应答，也不包含事务ID。**

**新行**

每个一般命令以新行结束（有效载荷命令中有特殊情况）。官方客户端及服务器总是以\r\n结束命令，所以建议你也应该这样实 现。

然而，服务器能接受\n结束的命令，但不能仅有\r。如果你确有必要节省更多带宽，那就使用\n吧，而且如果MSN不替换服务器代码的话，应该不会有什么问题。

在有效载荷命令的组配中，新行的处理略有不同。详情请见有效载荷命令。

参数

参数可以用来为命令提供附加信息。大多数命令都至少有一个参数，参数间用空格分割。有些命令也会在 参数前包含事务ID。 为了整体描述需要，事务ID在本文中就不记作参数了，如下命令包含一个参数：

<<< FLN example@passport.com\r\n

FLN是命令，example@passport.com是 参数部分，\r\n表 示新行。

发送的命令中，参数的分隔符可能用多个空格分隔，或者TAB，或者TAB与空格混杂等等。这些没有经过彻底测 试。不管怎么说，服务器总是在参数间用一个空格进行分隔，而且尾部没有空白（标准新行除外）。

**事务ID**

事务ID，缩写为TrIDs，用来匹配一个客户端与服务器的应答。客户端发送的命令需要一个事务ID，在服务器直接响应的命令中会包含同样的 事务ID。大多数 情况下，这就是针对客户端命令的一次响应。

事务ID是0到4294967295（2的32次方减1）之间的数值。即使完全合法，但还是建议你不要使用0作为事务ID，因为有些异步命令使用0作为事务ID，可能会造成不必要的混淆。事务ID通常在三个字母之后（或者三个数字，如 错误命令中）的命令代码中，并用空格分隔。如果命令包含参数，参数将置于事务ID之后，同样以空格分隔，否则事务ID后就不要加任何空格了。下例中，将以事务ID15发送VER命令，并得到了服务器的响应：

**>>> VER 15 MSNP8 FOO CVR0 BAR\r\n**

**<<< VER 15 MSNP8 CVR0\r\n**

服务器不会对你的事务ID作任何修改，仅用同样的事务ID做出响应。如果你的事务ID大于4294967295，服务器的响应将不可预知。如果你发送的事务ID不是正整数，服务器将立即断开。如果你在多个命令中重复相同的事务ID，服务器不会做出任何不同事，只是对于一 个客户端要跟踪响应来说就太难了。

官方客户端每发送一条命令后事务ID就会自增。尽量使用正确范围的值，不要重复事务ID，这不会造成什么误会。保持这个数值尽量 小将节约少量带宽 — 可能总共不会超过5%。使用随机数只会增加你的处理，而并不会增加安全性。

**错误命令**

错误命令可以说是服务器响应的一种特殊格式的命令，他表示客户端的命令不正确或者不能被正确解释。 错误命令的格式同一般命令类似，只是命令部分的三个字符需要换成三个数字。

如果有什么不对头，错误将替换命令部分。例如，如果客户端发送ADD命令，通常应该接收另外一个服务器端响 应的ADD命令。 但如果客户端指定了一个并不存在的账号作为参数，服务器将响应201错误，而不是ADD命令。

客户端从不向服务器发送错误命令，服务器也不会不针对客户端命令就发送错误代码。

**错误语法**

错误命令的语法十分简单，命令部分就是三个数字，然后添加所响应客户端命令的事务ID，就再没有其他附加参数了。

然而，按照原始IETF草案来说，错误可以发送附加参数。虽然我从未见过发送附加参数的，但事实上，每个客户端都应该做好 接收参数的准备，以避免Crash。

**有效载荷命令**

大多数信息仅有一行数据，然后以新行结束。有效载荷命令解决了一堆包含新行的数据发送的问题，在命 令的最后一个参数中指出了数据的长度（按字节）。MSNP8的有效载荷命令中有QRY，PAG，NOT，还有（最重要的）MSG。下面是一些范例：

**>>> QRY 1049 msmsgs@msnmsgr.com 32\r\n**   
**8f2f5a91b72102cd28355e9fc9000d6e (no newline)**

**异步命令**

**异步命令是服务器发送的命令**，而且并不是针对任何客户端发送的命令的响应。由他们的性质决定了异步 命令并不需要委派事务ID。有些异步命令不包含事务ID，其后直接加参数部分，如NLN，FLN还有BPR。还有一些异步命令总是包含为0的事务ID。如ADD和REM。这些命令包含事务ID的原因是，他们还需要被客户端使用，并作为对服务器的响应。只有在特殊情况下，如哪里一个联系人被 加为黑名单，服务器就发送一个事务ID为0的异步命令到哪里。

异步命令可以在协议的任意合法位置发送 — 即使在有联系的 应答间，如两个ILN间。

**命令次序**

通常，应答命令会以它们被发送的次序发送。但并不总是这样，有时你可能以1，2，3的次序发送命令，而服务器以2，3，1的次序响应，现在你应该明白事务ID为什么如此重要了。

有些命令会得到服务器的多个应答。这些应答中包含相同的事务ID和原始命令（除了SYN应答），一个命令可以有多个应答的例 子是CHG。

不幸的是，无关命令的次序没有确切的规则。例如，客户端可以在BPR列表中间接受ILN。如果你对一个服务器的行为充分了 解，你可以着手制定规则，但微软经常变更服务器的执行，你不得不重新开始。所以最好的是客户端能够对可能发生的事情作充分考虑。

**有效载荷命令**

什么是有效载荷命令

一个有效载荷命令是一种特殊形式的命令，它包含了若干行。对于它最好的理解是，一个正规单行命令后 加了一堆二进制数据（有效载荷）。最后的参数总是指定了其中所包含的字节数。

不同于其他命令，有效载荷命令没有通用的格式，他们的格式就是每个特殊的有效载荷命令所指定的那 样。不要试图象正规命令流一样找出在那里结束—有效载荷命令不易定以新行结束。你比如通过读取命令中指定的字节数来读取有效载荷中具体的数目的字节。

格式

有些有效载荷命令包含事务ID，有些则不包含。命令中可以包含任意数目的参数，但最后一个参数总是一个正整数。这个正整数用来标 识有效载荷的字节数，命令中必然指定并限制了有效载荷的长度。在有效载荷长度后，象其他命令一样加上一个新行，然后组成了整个有效载荷命令。有效载荷的长 度按字节计算。随后，一般的命令就可以继续了。

**执行**

发送一个有效载荷命令非常简单。大多数编程语言都包含有计算发送字符串字节数的函数（可能叫“len()”或者类似函数），用这个函数计 算出有效载荷的长度。记住计算时，不要包括命令本身和命令末尾新行的长度。

注意：服务器会按提供的长度提取信息，如果你要发送88个字节，但你指出了87，服务器就会一直等待，直到你再发送点 什么，那将提取下一个命令中的首个字节作为有效载荷的末尾字节，你将结束当前发送到服务器的非法命令。如果信息长度太短，一样会出现类似问题。

接收有效载荷命令时会更困难写。你不能依靠一个包中的整条命令，也不能就以新行作为结束。你绝对绝 对应该读取指定的消息长度，然后从socket读取自最初的新行后指定长度的字节数。

### 名 字

**概述**

    MSN Messenger通 过三个名字标识一个联系人：账号（也称“Passport”，“user handle”，或者“logon name”），显示名（也称“friendly name”，“custom name”或者“custom user name”），还有昵称。

**账号**

账号是你登录时的护照，就像principal@hotmail.com，你不能改变它，仅需要当登录时输入一次，虽然很多账号都是以“@hotmail.com”结尾，但通过在passport.com注册可以把任意邮 箱注册为护照。Hotmail和MSN账号会自动注册到护照系统，一个账号最大长度为129字节。

所有命令都需要按账号查阅联系人（不是显示名也不是昵称），因为账号可以保证唯一性。

**显示名**

显示名是您自己标识自己的一个字符串，你可以通过REA命令设置显示名。

显示名最长387字节，但官方客户端只能设置不超过129字符（3个字节的URL编码表示一个字符，译者注：387/3=129），当超过129个字符时，将存储不正确。

**昵称**

**由于昵称通常作为命令中的单个参数使用，所以需要经过URL编码**。例如，如果协议中看到昵称如同Two%20Words，应该翻译并显示为Two Words。（**这就巧妙的防止了如果用户取的名字引起系统误解如：中间带有空格，或&等，所以我们需要用url编码**）

一个联系人的昵称是你给定义的，可以与他们的显示名一致，或者不同。这个名字将在你的联系表中显 示。昵称可以用ADD和REA命 令进行变更。昵称将在SYN应答的LST部分发送。昵称格式上就像显示名一样，也需要进行URL编码，也有相同的长度限制等。

官方客户端总是保持昵称与显示名一致 — 当一个联系人发 送一个新的显示名是，官方客户端用REA命令也发送那个名字。然而，当一个联系人变更了他的显示名时，而当时你没有在线，你就仍能看到过期的 昵称。在MSN Messenger协议中这是一个缺陷。

**Http请求服务器**：

如下是请求通知服务器会话及应答示例：

**POST http://gateway.messenger.hotmail.com/gateway/gateway.dll?Action=open&Server=NS&IP=messenger.hotmail.com HTTP/1.1\r\n**  
**Accept: \*/\*\r\n**  
**Accept-Language: en-us\r\n**  
**Accept-Encoding: gzip, deflate\r\n**  
**User-Agent: MSMSGS\r\n**  
**Host: gateway.messenger.hotmail.com\r\n**  
**Proxy-Connection: Keep-Alive\r\n**  
**Connection: Keep-Alive\r\n**  
**Pragma: no-cache\r\n**  
**Content-Type: application/x-msn-messenger\r\n**  
**Content-Length: 18\r\n**  
**\r\n**  
**VER 5 MSNP8 CVR0\r\n**

**HTTP/1.0 200 OK\r\n**  
**Server: Microsoft-IIS/5.0\r\n**  
**Date: Tue, 18 Mar 2003 07:39:53 GMT\r\n**  
**X-MSN-Messenger: SessionID=954547325.13160; GW-IP=207.46.110.18\r\n**  
**Content-Length: 18\r\n**  
**Content-Type: application/x-msn-messenger\r\n**  
**Age: 0\r\n**  
**Via: HTTP/1.1 ntl\_site (Traffic-Server/5.2.0-R [c sSf ])\r\n**  
**X-Cache: MISS from nautilus.localdomain\r\n**  
**X-Cache-Lookup: MISS from nautilus.localdomain:80\r\n**  
**Proxy-Connection: keep-alive\r\n**  
**\r\n**  
**VER 5 MSNP8 CVR0\r\n**

**其中反馈回来的207.46.110.18就是我们接下来需要连接的通知服务器地址。**

如下是发送消息到服务器**请求信息列表**（前提是已经login通知服务器，这里只是举例，假设已经登录通知服务器成功）：

**POST http://207.46.110.18/gateway/gateway.dll?Action=poll&SessionID=954547325.32498 HTTP/1.1\r\n**  
**Accept: \*/\*\r\n**  
**Accept-Language: en-us\r\n**  
**Accept-Encoding: gzip, deflate\r\n**  
**User-Agent: MSMSGS\r\n**  
**Host: 207.46.110.18\r\n**  
**Proxy-Connection: Keep-Alive\r\n**  
**Connection: Keep-Alive\r\n**  
**Pragma: no-cache\r\n**  
**Content-Type: application/x-msn-messenger\r\n**  
**Content-Length: 0\r\n**  
**\r\n**

**HTTP/1.0 200 OK\r\n**  
**Server: Microsoft-IIS/5.0\r\n**  
**Date: Tue, 18 Mar 2003 07:39:56 GMT\r\n**  
**X-MSN-Messenger: SessionID=954547325.6942; GW-IP=207.46.110.18\r\n**  
**Content-Length: 0\r\n**  
**Content-Type: application/x-msn-messenger\r\n**  
**Age: 1\r\n**  
**Via: HTTP/1.1 ntl\_site (Traffic-Server/5.2.0-R [c sSf ])\r\n**  
**X-Cache: MISS from nautilus.localdomain\r\n**  
**X-Cache-Lookup: MISS from nautilus.localdomain:80\r\n**  
**Proxy-Connection: keep-alive\r\n**  
**\r\n**

上面的反馈信息并没有好友(content为空的，不然会有好友信息)

从客户端发送消息来关闭会话：

**POST http://207.46.110.18/gateway/gateway.dll?SessionID=954547325.3500 HTTP/1.1\r\n**  
**Accept: \*/\*\r\n**  
**Accept-Language: en-us\r\n**  
**Accept-Encoding: gzip, deflate\r\n**  
**User-Agent: MSMSGS\r\n**  
**Host: 207.46.110.18\r\n**  
**Proxy-Connection: Keep-Alive\r\n**  
**Connection: Keep-Alive\r\n**  
**Pragma: no-cache\r\n**  
**Content-Type: application/x-msn-messenger\r\n**  
**Content-Length: 5\r\n**  
**\r\n**  
**OUT\r\n**

**HTTP/1.0 200 OK\r\n**  
**Server: Microsoft-IIS/5.0\r\n**  
**Date: Tue, 18 Mar 2003 07:41:39 GMT\r\n**  
**X-MSN-Messenger: SessionID=954547325.1484; GW-IP=207.46.110.18; Session=close\r\n**  
**Content-Length: 0\r\n**  
**Content-Type: application/x-msn-messenger\r\n**  
**Age: 0\r\n**  
**Via: HTTP/1.1 ntl\_site (Traffic-Server/5.2.0-R [c sSf ])\r\n**  
**X-Cache: MISS from nautilus.localdomain\r\n**  
**X-Cache-Lookup: MISS from nautilus.localdomain:80\r\n**  
**Proxy-Connection: keep-alive\r\n**  
**\r\n**

如下是第一次请求交换服务器会话的示例：

（**交换服务器的地址是由先前向通知服务器索取的，此例获取的交换板服务器地址为207.46.108.13，那么我们拿到这个ip地址就可以连接交换板服务器咯**）

**POST http://gateway.messenger.hotmail.com/gateway/gateway.dll?Action=open&Server=SB&IP=207.46.108.13 HTTP/1.1\r\n**  
**Accept: \*/\*\r\n**  
**Accept-Language: en-us\r\n**  
**Accept-Encoding: gzip, deflate\r\n**  
**User-Agent: MSMSGS\r\n**  
**Host: gateway.messenger.hotmail.com\r\n**  
**Proxy-Connection: Keep-Alive\r\n**  
**Connection: Keep-Alive\r\n**  
**Pragma: no-cache\r\n**  
**Content-Type: application/x-msn-messenger\r\n**  
**Content-Length: 55\r\n**  
**\r\n**  
**USR 3 phil\_sayers@hotmail.com 214963.1047973248.28908\r\n**

## 通知服务器相关协议：

通知

认 证

概述

MSN Messenger会话首先应该登 录到通知服务器，如果有通知服务器IP地址，就直接连接，走则，就必须连接到“分派服务器”，官方客户端使用messenger.hotmail.com， 端口1863的分 派服务器作为直接的SOCK连接，并使用gateway.messenger.hotmail.com，80端口作为分布服务器的HTTP连接。如果想连接到第三方的MSN Messenger网络，应该使用不同的分布服务器。

如果不能连接到历史通知服务器，那就尝试分派服务器。如果仍不能连接到分派服务器，那么不是你的连 接有问题，就是MSN Messenger网络Down掉了（有时还是会发生的）。

如果你首先连接到一个通知服务器，那么你就处于“登录”处，包含了协议版本验证，身份验证，如果当 前服务器超负荷，还有可能转移到其他通知服务器。

登录期间，服务器行为与通常情况不同，通信是本质上同步的 — 客户端发送一个 命令，服务器响应，客户端发送另一个命令，……。如果在错误的时候发送了一个命令（如正当协议版本在洽谈时，你发送了一个VER命令），服务器会返回715错误，并断开。如果发送了登录期间无 意义的命令（如SYN），你将立即被断开，并得到一个错误。登录期外不需要遵守此规则。

VER

VER命令指出了MSN Messenger协议所支持的版 本信息。VER命 令包含一个事务ID、 一串协议版本信息和参数（注意协议版本大小写敏感）。服务器会返回相同事务ID的VER响应。如果服务器至少支持一种协议，参数中就会给出所支持的列表，否则应答中就会仅仅包含参数0，并断开连接（一般不应该发生）。

第一个参数（不包括CVR0）是会话中应该使用的协议版本，原则上，CVR0可能出现在参数列表的任意位置，实际上，通常它被放在列表的最后。在MSN Messenger协议版本8种，你必须至少支持“MSNP8”和“CVR0”。

下面是一些例子：

**<o> Connect: messenger.hotmail.com 1863**

**>>> VER 0 MSNP8 CVR0\r\n**

**<<< VER 0 MSNP8 CVR0\r\n**

**<o> Continue Session . . .**

**<o> Connect: messenger.hotmail.com 1863**

**>>> VER 0 MSNP8 MYPROTOCOL CVR0 \r\n**

**<<< VER 0 CVR0 MSNP8\r\n**

**<o> Continue Session . . .**

**<o> Connect: messenger.hotmail.com 1863**

**>>> VER 0 MYPROTOCOL\r\n**

**<<< VER 0 0\r\n**

**<o> Server Closes Connection**

**<o> Connect: messenger.hotmail.com 1863**

**>>> VER MSNP8 CVR0\r\n** (No TrID)

**<o> Server Closes Connection**

**CVR**

CVR发送客户端及操作系统的版本信息到服 务器，对于官方客户端来说，服务器会响应建议用户使用的客户端版本信息（可能与您正使用的版本相同）。

CVR包含你使用的语言信息，客户端的名称 及版本，还有操作系统的名称及版本。登录后你随时可以发送CVR命令到NS，但官方客户端总是在发送最初的CHG后就立即发送CVR。你可以多次发送CVR命令，CVR需要事务ID和8个参数：

.第一个参数是十六进制数字，用来指定你的locale ID（如0x0409表示美国英语）。

.第二个参数是你的操作系统类型（win表示Windows）

.第三个参数表示你的操作系统版本信息（如4.10表示Windows 98）

.第四个参数是你的计算机体系（如i386表示Intel兼容PC，386及以上型号）

.第五个参数是客户端名称（如MSMSGR表示官方客户端MSN Messenger客户端）。

.第六个参数是客户端版本（如6.0.0602）

.第七个参数在官方客户端中总会是“MSMSGS”，看来你得像我一样猜猜它是 什么意思了。

.第八个参数是护照信息。

如同其他命令一样，服务器将应答CVR命令。处于某些因素，官方客户端更希望你用CVQ应答，而不是CVR。包含五个参数：

.第一个参数是建议客户端版本，或者“1.0.000”（如果你的客户端信息不被认可）。

.第二个参数同第一个一样

.第三个参数客户端可安全运行的最小版本 号，或者当前版本信息（如果你的客户端信息不被认可）。

.第四个参数是你可以下载建议版本客户端的URL。

.第五个参数是可以获得更多客户端信息的URL。

如果你的当前客户端版本小于最小安全版本，那将意味着你的版本有某些严重缺陷。官方客户端会立即断 开，可能尽管服务器不会介意。下面是6.0.0602的官方客户端发送的CVR信息：

**>>> CVR 2 0x0409 win 4.10 i386 MSNMSGR 5.0.0544 MSMSGS example@passport.com\r\n**

**<<< CVR 2 6.0.0602 6.0.0602 1.0.0000 http://download.microsoft.com/download/8/a/4/8a42bcae-f533-4468-b871-d2bc8dd32e9e/SETUP9x.EXE http://messenger.msn.com\r\n**

**初始的USR**

接收到CVR的响应后，你必须发送USR命令，它拥有一个事务ID。

.第一个参数是认证系统（总是TWN）。

.第二个参数总会是字母I（代表开始Initiating认证）

.第三个参数是用来登录的账号

如果你的USR不规范，服务器将断开连接，可能会不给出任何应答，也可能首先发送一个错误，911错误会在你把I替换为S时发生，或者非法的账号名如hotmail.com时发生。928错误将在你发送了一个有害的ticket时发生。

有些时候，当服务器出现问题或者为了维护而down掉时，也会发送一个错误避免登录。可能的错误有500、601、910、921。

否则，服务器或者响应XFR（转到另一个通知服务器）或者并发的USR应答。

**XFR**

messenger.hotmail.com总 是发送XFR，但gateway.messenger.hotmail.com从来不这样做。微软的其他通知服务器极少发送XFR，大概在超负荷或者加入维护时会发送吧。

XFR命令与之前的USR具有相同的事务ID，并有四个参数。

.第一个参数是NS，告诉你正在转换到一个通知服务器。

.第二个参数是通知服务器的IP和端口号，以冒号分隔。端口号看起来总 是1863，但最 好按照给出的端口号进行处理。

.第三个参数是总会是0。

.第四个参数是你当前连接的服务器的IP和端口号（以冒号分隔）。

如下是USR与XFR的示例：

**>>> USR 2 TWN I example@passport.com\r\n**

**<<< XFR 2 NS 207.46.106.145:1863 0 207.46.104.20:1863\r\n**

接收XFR后服务器就会关闭连接，你必须按照指定通知服务器，重新开始登录过程。通知服务器间没有通讯，所以你 在登录新服务器时可以指定一个不同的协议版本，名字等。

 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

并发的USR应答

并发的USR应答包含三个参数：TWN，S（subsequent）替换了I，还有一个TWN认证使用的串。

TWN认证

TWN（“Tweener”）认证是MSN Messenger接入微软护照认 证体系的方式。护照认证是微软为Internet服务提供“标识一次”系统所做的尝试。一些具体信息可以在MSDN上找到。理解TWN不需要什么护照的背景知识，但应该有HTTP协议1.0或1.1的基本知识。

TWN认证包含以下步骤：

1.       客户端保存USR应答串；

2.       客户端（可选）连接到护照“Nexus”，得到登录服务器URL。这个结果不会经常变更，可以被缓存。

3.       客户端使用存储串、护照、口令，通过登录服务器验证，服务器将作下列操作之一：

         重新定位客户端到另外一个登录服务器，并进行认证（注意：这个服务器不必缓存）；

         返回一个登录错误，并携带适当错误信息。

         返回一个“ticket”，ticket将在USR应答中发送给通知服务器。

**通过MS护照认证包含发送HTTPS请求道微软护照服务器，来得到一个护照“ticket”，并用它提交给你真正连接的服务器**。HTTPS是HTTP应用“Secure Socket Layer”加密协议。建议为你所用的编程语言找到一个支持HTTPS的库 — 即便你自己实 现HTTP解析， 也不要实现SSL（对 于一个较大工程来说，它太复杂了，而且安全性极其敏感）。护照服务器允许你在请求主体中作为HTML文件发送你的登录信息，或者作为HTTPS的头部信息。HTML仅为浏览器提供，但对于MSN Messenger客户端来说同样工作良好。“头部”对于MSN Messenger来说是建议方 案，并且本文也仅对“头部”加以说明。

连接到Nexus包含发送一个HTTPS GET请求，URL为https://nexus.passport.com/rdr/pprdr.asp，服务器总是会返回200 OK的空信息。重要的信息被包含在“PassportURLs”头部中，其中包含用逗号分隔的信息列表。“DALogin”包含登录服务器的地址，这个值够不上合法的URL，所以你的HTTPS库可能需要你在首部添加“https://”。

然后，客户端发送一个HTTPS GET请求到Nexus给定的URL，请求信息中应该包含“Authorization”头部信息，其值是一大长串并且没有空格，由三部分组成：“Passport1.4 OrgVerb=GET,OrgURL=http%3A%2F%2Fmessenger%2Emsn%2Ecom,sign-in=”，URL编码的护照，“,pwd=”，URL编码的口令，“,”，通知服务器给出的口令串。

服务器的响应应该是200 OK（成功的话），302 Found（重定位）或者401 Unauthorized（失败的话），信息中将包含“Authentication-Info” 或者“WWW-Authenticate”头部信息，真不知道为什么会出现两个不同的头部名，但目前“WWW-Authenticate”仅在登录 失败时使用。最保险的方案是假定两个头部信息可以互换。头部值以“Passport1.4”开始，然后是形同“key=value”的字段列表。头一个字段是“da-status”关键字，值可以是“success”、“failed”或者“redir”（redirect）。

如果失败的话，响应的头部信息中将包含“cbtxt”字段（URL编码的错误信息），“cburl”字段（一个图形的URL地址，可能需要用来显示）。

如果需要重定位，会包含一个“Location”头部信息，其中有重定位的登录服务器URL。本稿写作时，客户端仅当护照以“@hotmail.com”或“@msn.com”结尾时才会重定位，然后客户端重新开始登录过程。

如果响应成功，头部信息中将包含“from-PP”字段，其中包含恢复到通知服务器的ticket。这个字段格式有些特殊，其中包含一些省略号，还有等号（但不包含逗号）。

最后的USR命令

得到ticket后，你必须发送最终的USR命令，他包含一个事务ID，第一个参数为TWN，第二个参数为S，第三个参数是你的ticket。

如果ticket正确，服务器将用USR应答，其中第一参数是OK，第二个参数是你的账号，第三个参数十你的显示名，0或者1 是第四个参数，第五个参数为0。第四个参数表示你的护照是否已经通过检 验（1真，0假）。我们还不知道第五个参数有什么作 用。

如果ticket不正确，服务器将响应911错误，并关闭连接。如果其他信息不正确（包含非法分类大小），服务器将关闭连接，并且不发送任何错 误。

有时，服务器出现问题，或者进行维护时，也会响应一个错误。可能的错误有500、601、910，还有921。

下一步做什么

现在你应该已经成功登陆，可以入列席中所讲进行进行列席操作了。一旦登录后，就应该同步你的列表。 接收最终的USR信 息后，你可能从NS上 接收一个或多个消息（MSG）。

最大效率

登录时想尽可能快的话，你应该不等待应答一次发送多行命令（基于某些原因，合装到同一个包中有一些 问题）。一块发送VER和USR到DS。仅指定你打算使用的一个协议版本，并 以a@b.c作为 邮件地址发送到messenger.hotmail.com。不用理会INF。你也可以以\n替换\r\n来节省带宽。

4.1.2.       登出

要登出NS的话（MSN会发送你的断线信息给每个人），最简单的方法就是关闭Socket。如果你非正常断开（如你使用了Modem，并被断开），你仍将在线几分 钟，但不能响应。

正确的方法是发送OUT命令到NS服务器，不用携带任何参数及事务ID。服务器将立即断开连接。参照协议草案中的说明，服务器应该发回OUT，但实际中，从来就没有这样做过。

服务器主动关闭连接

有时服务器会主动关闭连接，可能有两个原因：服务器要down掉，或者有人在别处用你的账号登录到 了MSN。

当有人在别处用你的账号登录时，原来的连接将被关闭，新连接将被建立。关闭连接前，NS将给客户端发送OUT命令并携带参数OTH — 联系人从另外一个地点登录。

当服务器要进行维护时，将会发送OUT SSD — server shutting down，发送后就立即关闭连接。

通常情况下，发送OUT SSD前服务器将发送一个警告信息。如，你可能在MSN Messenger中看到“The server will be shutting down for maintenance in 5 minutes”等。

4.1.3.       示例

下例中使用协议版本8登录到MSN Messenger服务器。这里使用“example@passport.com”用户以官方客户端版本5登录，口令为“password”。

**通知服务器**

客户端首先登录到分派服务器(messenger.hotmail.com),然后 转到207.46.106.35，然后登录并成功。出稿时，messenger.hotmail.com 的IP为207.46.104.20。

**<o> Client connects to messenger.hotmail.com, port 1863 (Dispatch Server)**

**>>> VER 1 MSNP8 CVR0\r\n**

**<<< VER 1 MSNP8 CVR0\r\n**

**>>> CVR 2 0x0409 win 4.10 i386 MSNMSGR 5.0.0544 MSMSGS example@passport.com\r\n**

**<<< CVR 2 6.0.0602 6.0.0602 1.0.0000 http://download.microsoft.com/download/8/a/4/8a42bcae-f533-4468-b871-d2bc8dd32e9e/SETUP9x.EXE http://messenger.msn.com\r\n**

**>>> USR 3 TWN I example@passport.com\r\n**

**<<< XFR 3 NS 207.46.106.35:1863 0 207.46.104.20:1863\r\n**

**<o> messenger.hotmail.com closes connection**

**<o> client connects to 207.46.106.35, port 1863**

**>>> VER 1 MSNP8 CVR0\r\n**

**<<< VER 1 MSNP8 CVR0\r\n**

**>>> CVR 2 0x0409 win 4.10 i386 MSNMSGR 5.0.0544 MSMSGS example@passport.com\r\n**

**<<< CVR 2 6.0.0602 6.0.0602 1.0.0000 http://download.microsoft.com/download/8/a/4/8a42bcae-f533-4468-b871-d2bc8dd32e9e/SETUP9x.EXE http://messenger.msn.com.\r\n**

**>>> USR 3 TWN I example@passport.com\r\n**

**<<< USR 3 TWN S lc=1033,id=507,tw=40,fs=1,ru=http%3A%2F%2Fmessenger%2Emsn%2Ecom,ct=1062764229,kpp=1,kv=5,ver=2.1.0173.1,tpf=43f8a4c8ed940c04e3740be46c4d1619\r\n**

**<o> Client authenticates itself with MS Passport**

**>>> USR 4 TWN S t=53\*1hAu8ADuD3TEwdXoOMi08sD\*2!cMrntTwVMTjoB3p6stWTqzbkKZPVQzA5NOt19SLI60PY!b8K4YhC!Ooo5ug$$&p=5eKBBC!yBH6ex5mftp!a9DrSb0B3hU8aqAWpaPn07iCGBw5akemiWSd7t2ot!okPvIR!Wqk!MKvi1IMpxfhkao9wpxlMWYAZ!DqRfACmyQGG112Bp9xrk04!BVBUa9\*H9mJLoWw39m63YQRE1yHnYNv08nyz43D3OnMcaCoeSaEHVM7LpR\*LWDme29qq2X3j8N\r\n**

**<<< USR 4 OK example@passport.com example%20display%20name 1 0\r\n**

the client had to authenticate itself with MS Passport to get the ticket used in the final **USR** message.

**The Passport Nexus**

Passport authentication begins with the Passport Nexus, just as logging into Messenger begins with the Dispatch Server. The client sends the following HTTPS GET request for the URL "https://nexus.passport.com/rdr/pprdr.asp", using HTTPS version 1.0:

**<o> Client connects to nexus.passport.com, port 443 (Passport Nexus)**

**>>> GET /rdr/pprdr.asp HTTP/1.0\r\n**  
**\r\n**

**<<< HTTP/1.1 200 OK\r\n**  
**<<< Server: Microsoft-IIS/5.0\r\n**  
**<<< Date: Mon, 02 Jun 2003 11:57:47 GMT\r\n**  
**<<< Connection: close\r\n**  
**<<< PassportURLs: DARealm=Passport.Net,DALogin=login.passport.com/login2.srf,DAReg=http://register.passport.net/uixpwiz.srf,Properties=https://register.passport.net/editprof.srf,Privacy=http://www.passport.com/consumer/privacypolicy.asp,GeneralRedir=http://nexusrdr.passport.com/redir.asp,Help=http://memberservices.passport.net/memberservice.srf,ConfigVersion=11\r\n**  
**<<< Content-Length: 0\r\n**  
**<<< Content-Type: text/html\r\n**  
**<<< Cache-control: private\r\n**  
**<<< \r\n**

**<o> nexus.passport.com closes connection**

As you can see, the Nexus returned "login.passport.com/login2.srf" as the login server to connect to.

**The Login Server**

The client sends an HTTPS GET request for the URL given to it by the Nexus. Login servers require you to use HTTPS version 1.1, and therefore to send a "Host" header in every request. Note that the challenge string used here is taken from the **USR** message sent by the Notification Server.

**<o> Client connects to login.passport.com, port 443**

**>>> GET /login2.srf HTTP/1.1\r\n**  
**>>> Authorization: Passport1.4 OrgVerb=GET,OrgURL=http%3A%2F%2Fmessenger%2Emsn%2Ecom,sign-in=example%40passport.com,pwd=password,lc=1033,id=507,tw=40,fs=1,ru=http%3A%2F%2Fmessenger%2Emsn%2Ecom,ct=1062764229,kpp=1,kv=5,ver=2.1.0173.1,tpf=43f8a4c8ed940c04e3740be46c4d1619\r\n**  
**>>> Host: login.passport.com\r\n**

If the server redirected the client to "https://loginnet.passport.com/login2.srf?lc=1033", the response might look like this:

**<<< HTTP/1.1 302 Found\r\n**  
**<<< Server: Microsoft-IIS/5.0\r\n**  
**<<< Date: Mon, 02 Jun 2003 11:58:32 GMT\r\n**  
**<<< PPServer: H: LAWPPLOG5C006\r\n**  
**<<< Connection: close\r\n**  
**<<< Content-Type: text/html\r\n**  
**<<< Expires: Mon, 02 Jun 2003 11:57:32 GMT\r\n**  
**<<< Cache-Control: no-cache\r\n**  
**<<< cachecontrol: no-store\r\n**  
**<<< Pragma: no-cache\r\n**  
**<<< P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"\r\n**  
**<<< Authentication-Info: Passport1.4 da-status=redir\r\n**  
**<<< Location: https://loginnet.passport.com/login2.srf?lc=1033\r\n**  
**<<< \r\n**

If the request was successful, the response might look like this:

**<<< HTTP/1.1 200 OK\r\n**  
**<<< Server: Microsoft-IIS/5.0\r\n**  
**<<< Date: Mon, 02 Jun 2003 11:59:00 GMT\r\n**  
**<<< PPServer: H: LAWPPIIS6B061\r\n**  
**<<< Connection: close\r\n**  
**<<< Content-Type: text/html\r\n**  
**<<< Expires: Mon, 02 Jun 2003 11:58:00 GMT\r\n**  
**<<< Cache-Control: no-cache\r\n**  
**<<< cachecontrol: no-store\r\n**  
**<<< Pragma: no-cache\r\n**  
**<<< P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"\r\n**  
**<<< Set-Cookie: MSPSec1= ; expires=Thu, 30-Oct-1980 16:00:00 GMT;domain=.passport.com;path=/;HTTPOnly= ;version=1\r\n**  
**<<< Set-Cookie: MSPSec=5Cdd1SshOELpwqafsSuYSiDEuEtP1PUaX99YOZcaoJP3vkIn7DXozt868I7eJNjcWG; HTTPOnly= ; domain=.passport.com;path=/;secure=\r\n**  
**<<< Set-Cookie: MSPAuth=5yDBU0BqvDa7UiY9W9nVEncRXCLD4gjLmtEr2XkunnafkOgdgG5x\*CEpqe7MyZEOir\*EiA1PbwLKzqCGO671TeTQ$$; HTTPOnly= ; domain=.passport.com;path=/\r\n**  
**<<< Set-Cookie: MSPProf=5a0mKE6PKDsxz!\*4apQt0amnQOGLYqcCm78ie!MmHq0KnAiIJM0z0Zajs8NL7ux7Ae0hnH5AAoB!zXIZ9jTA2rcQttC\*RKKRsc9k7JflwThB!H0Qa\*6ipGcdj5co6taPir; HTTPOnly= ; domain=.passport.com;path=/\r\n**  
**<<< Set-Cookie: MSPVis=507;domain=.passport.com;path=/\r\n**  
**<<< Set-Cookie: MSPPre=esqkk@hotmail.com; HTTPOnly= ; domain=.passport.com;path=/;Expires=Wed, 30-Dec-2037 16:00:00 GMT\r\n**  
**<<< Set-Cookie: MSPShared= ; HTTPOnly= ; domain=.passport.com;path=/;Expires=Thu, 30-Oct-1980 16:00:00 GMT\r\n**  
**<<< Authentication-Info: Passport1.4 da-status=success,tname=MSPAuth,tname=MSPProf,tname=MSPSec,from-PP='t=53\*1hAu8ADuD3TEwdXoOMi08sD\*2!cMrntTwVMTjoB3p6stWTqzbkKZPVQzA5NOt19SLI60PY!b8K4YhC!Ooo5ug$$&p=5eKBBC!yBH6ex5mftp!a9DrSb0B3hU8aqAWpaPn07iCGBw5akemiWSd7t2ot!okPvIR!Wqk!MKvi1IMpxfhkao9wpxlMWYAZ!DqRfACmyQGG112Bp9xrk04!BVBUa9\*H9mJLoWw39m63YQRE1yHnYNv08nyz43D3OnMcaCoeSaEHVM7LpR\*LWDme29qq2X3j8N',ru=http://messenger.msn.com\r\n**  
**<<< Content-Length: 0\r\n**  
**<<< \r\n**

The client's ticket is **t=53\*1hAu8ADuD3TEwdXoOMi08sD\*2!cMrntTwVMTjoB3p6stWTqzbkKZPVQzA5NOt19SLI60PY!b8K4YhC!Ooo5ug$$&p=5eKBBC!yBH6ex5mftp!a9DrSb0B3hU8aqAWpaPn07iCGBw5akemiWSd7t2ot!okPvIR!Wqk!MKvi1IMpxfhkao9wpxlMWYAZ!DqRfACmyQGG112Bp9xrk04!BVBUa9\*H9mJLoWw39m63YQRE1yHnYNv08nyz43D3OnMcaCoeSaEHVM7LpR\*LWDme29qq2X3j8N**, which is returned to the Notification Server.

If the request failed, the response might look like this:

**<<< HTTP/1.1 401 Unauthorized\r\n**  
**<<< Server: Microsoft-IIS/5.0\r\n**  
**<<< Date: Mon, 02 Jun 2003 11:58:15 GMT\r\n**  
**<<< PPServer: H: LAWPPIIS6B077\r\n**  
**<<< Connection: close\r\n**  
**<<< Content-Type: text/html\r\n**  
**<<< Expires: Mon, 15 Sep 2003 07:57:14 GMT\r\n**  
**<<< Cache-Control: no-cache\r\n**  
**<<< cachecontrol: no-store\r\n**  
**<<< Pragma: no-cache\r\n**  
**<<< P3P: CP="DSP CUR OTPi IND OTRi ONL FIN"\r\n**  
**<<< PassportConfig: ConfigVersion=11\r\n**  
**<<< WWW-Authenticate: Passport1.4 da-status=failed,srealm=Passport.NET,ts=-3,prompt,cburl=http://www.passportimages.com/XPPassportLogo.gif,cbtxt=Type%20your%20e-mail%20address%20and%20password%20correctly.%20If%20you%20haven%E2%80%99t%20registered%20with%20.NET%20Passport%2C%20click%20the%20Get%20a%20.NET%20Passport%20link.\r\n**  
**<<< Content-Length: 390\r\n\r\n**

**列 席**

“列席”信息，广义上讲，是联系人与（或）客户端的存在状态，MSNP8中，包含你的状态（忙碌、发呆、隐 身等），你的显示名，还有关于客户端不同状态码（如webcam支持）。

下例是服务器发送的列席通知命令：

**NLN AWY example@passport.com example%20display%20name 268435492**

以上说明“example@passport.com”联系人虽然仍可以接收即时信息，但已经离开，并希望你以“example display name” 显示他的名字。从上也可以看出，他的客户端能够解释MSNC1协议，而且能够读懂“ink”消息。

4.2.2.       状态

状态用来显示联系人的在线状态信息，主要有两种基本信息：open（在线）和closed（离线）。在线状态下，你可以 与其他用户聊天，离线时则不能。当你断开与通知服务器的连接时，你的状态自动变为离线状态，但一旦连接到服务器，你不得不手工变更你的在线状态。关闭在线 状态，又需要在线的话，可以设置为“hiding”或者“appearing offline”。

你的联系表中每个人，或者更明确的讲，你的允许列表中的联系人，可以看到你的状态。你可以看到那些 你在他们的允许列表中的每个人的状态，你可以自动接收forward列表中的每个人的状态。

在线的联系人，必须设置一个子状态，这不会对服务器造成什么影响，但是对于其他联系人来说就很有趣 了。

.NLN — 可用

.BSY — 忙碌

.IDL — 发呆

.BRB — 马上回来

.AWY — 离开

.PHN — 打电话

.LUN — 外出就餐

也可以设置HDN以达到隐身的目的。

**客户端标识码**

为了能够正确理解一个客户端在MSN Messenger中是如何工作的，你需要对二进制算法有个基本认识，本 文没有这方面的知识，所以这里对客户端ID码的讨论还是很浅显得，客户端标识与列表码非常类似，只是更为复杂一些。

客户端ID是它所能支持协议版本的指定的几个数值得总和，下面是我们知道的几个客户端标识使用的值：

1

客户端运行在Windows移动设备上，如智能电话或者Pocket PC。官方客户端将把联系人的图标由一个小人变为一个持电话的小人，并在 他们的名字后面加“(phone)”。

2

目前我们还不知道它有什么涵义，但是官方客户端有时在重新设置性能时会用到它。

4

客户端能够查阅“ink”信息。

8

客户端能够查阅并创建“ink”信息。

16

客户端可以分享视频会话，官方客户端仅当你包含一个视频头，并选择共享你的视频头时才会设置此值。

32

我们也不晓得有什么意思。但官方客户端的6.0及以上版本总是会设置（对于客户端来说是硬性编码的），所以应该是不可以被关闭的。

64

客户端有MSN移动设备可以被翻阅，相当于BPR列表中包含了MOB值，且Windows Mobile不做任何事情。

128

客户端拥有MSN直控设备，你可以直接翻页。等同于BPR列表中包含WWE值。

268435456

客户端支持包含协议MSNC1

536870912

客户端支持包含协议MSNC2。

创建客户端ID时，需要把以上值列表相加，然后应用。例如，如果你的客户端是移动电话并支持MSNC0，那你的客户端ID为1。如果你的客户端支持MSNC2，并可以接收ink消息，还有语音支持，客户端ID将为536870932（536870912+16+4）。注意：仅 可以指定一个支持的客户端协议 — 如果既应用268435456又应用536870912，客户端行为将不可预知。

如同列表码一样，你可以通过位与把另一个客户端的ID中的各项值提取出来，虽然可以如此，但得 到客户端版本的更好办法是客户端ID除以268435456，并取得最近的整型值，这又叫做整除，大多数编程语言提供此功能函数或操作符。对于MSNC0d的客户端，整除总会是0，MSNC1客户端总会是1，MSNC2客户端总会是2。

得到客户端版本信息时，整除比位与更安全，比如又出现了MSNC3协议版本，值将为805306368，位与就会出现问题，但 整除会工作良好，并返回3。

Ink是什么

Ink是微软提出的可以在屏幕上手写的技 术。在微软的Platform SDK最近版本中tablet PC上可用，还有微软的下一个Windows操作系统“Longhorn”。

4.2.4.       设置你的列席状态

发送CHG命令（带事务ID）来设置或改变你的列席状态，状态码为三个字母，命令中还应该包含客户端ID。如果操作成功，服务器将回显命令，否 则，极有可能立即断开。记住状态码是大小写敏感的，所以发送nln的话，服务器将立即关闭连接，如下是一些相关示例：

**>>> CHG 12 NLN 0\r\n**  
**<<< CHG 12 NLN 0\r\n**

**>>> CHG 13 HDN 24\r\n**  
**<<< CHG 13 HDN 24\r\n**

**>>> CHG 14 AWY 268435492\r\n**  
**<<< CHG 14 AWY 268435492\r\n**

如果频繁尝试修改状态，可能会收到800错误。

初始列席状态

当与服务器同步交互之后（译者注：登录之后），就应该设置你的初始列席状态，不过官方客户端总会立 即设置为NLN， 其实任何状态都是被服务器接受的。

如果你不设置自己的初始列席状态，状态总会是离线的，而且也不会收到什么列席状态通知。如果你想在 登录后保持列席状态为脱机，应该设置初始状态为HDN。

过去可以设置状态为FLN，但现在不再允许了，如果坚持尝试的话，会收到201错误指出非法参数。如果隐身时用XFR命令请求交换板会话，将收到913错误。

并更显示名

用REA命令来变更显示名，设置细节中有详细介绍。

**接收列席信息**

初始化列席通知

初始化列席通知，用来告诉在你登录前其他联系人已经在线了（或者你添加一个联系人后）。发送你的初 始列席状态后，将收到一个ILN命令，指出了你在对方的允许列表中的在线的联系人，当然也需要在你的forward列表中了。如果你添加一个联系 人到forward列 表中，他们在线并允许你看到他们的在线状态的话，也会收到一个ILN命令。

客户端不应该非要设法通知联系人有一个初始列席状态通知。比如官方客户端就不会非要弹出一个信息框 告诉你有人上线啦。

ILN命令包含事务ID（与你的CHG或ADD命令中的事务ID相同），并包含四个参数：

.第一个参数是联系人的3个字母的状态码

.第二个参数是联系人的账号

.第三个参数是联系人的显示名（URL编码的）

.第四个参数是联系人的客户端ID

ILN命令是MSN Messenger协议中最少的好的 可执行的部分之一了（译者注：搞不懂，讽刺微软？？），没有办法晓得对于CHG命令的ILN响应什么时候结束，也不知道ADD命令后是否会收到ILN。如果这对你的客户端来说是个问题，那么收到CHG响应后就ping服务器，可以假定如果收到ping应答则列表响应结束。可作选择的是，你可以在接收ILN命令数秒后就假定响应结束了。即使如 此，你也应该做好准备接收ILN，毕竟它们是异步命令。

下例用来接收在线联系人列表：

**>>> CHG 12 NLN 6\r\n**

**<<< CHG 12 NLN 6\r\n**

**>>> PNG\r\n**

**<<< ILN 12 AWY example@passport.com Mike 0\r\n**

**<<< ILN 12 NLN name\_123@hotmail.com Name\_123 536870948\r\n**

**<<< ILN 12 BSY myname@msn.com My%20Name 268435492\r\n**

**<<< QNG\r\n**

变更列席通知

一旦设置了初始列席状态，你的forward列表中的联系人状态变更时都会使服务器发送一个通知给你。

当一个联系人关闭了他们的列席状态（可能是离线或者隐身），服务器将发送一个FLN命令（不带事务ID）与他们的护照过来：

**<<< FLN example@passport.com\r\n**

联系人的列席状态有任何变更都将使服务器发送一个NLN命令（注意：字符串NLN可以用来做命令也可以表示在线状 态）。可以触发NLN命令的事件有：联系人打开了列席状态（如连接到NS后），变更为在线状态，客户端ID中有所变更，显示名变更等。收到NLN命令意味着以上几个或者仅一个或者一个都没有变更，所以你应该自行检查，并决定通知用户与否。

NLN同ILN的语法相同，除了不包含事务ID外：

**<<< NLN NLN example@passport.com Mike 12\r\n**

**<<< NLN AWY example@passport.com Mike 0\r\n**

**<<< NLN AWY example@passport.com Mike%20Changed%20His%20Name 36\r\n**

**Pings/Challenges**

    Ping命令是服务器或客户 端发送用来确认连接的，有点类似于IRC中的PING与PONG。客户端发送的Ping命令是PNG，服务器用QNG来响应。服务器发送的Ping命令是CHL命令，客户端用QRY命令响应。

4.3.2.       客户端pings

客户端的Ping通常用来确信连接仍然可用或者避免被NAT关闭发呆的Socket。另外也可以被用来测量客户端与服务器之间的响应时间。

PNG可以在USR及口令发送后的任意时间使用。

客户端Ping可以说是所有命令中最简单的命令了，客户端发送PNG而且不用携带事务ID或者任何参数，服务器也仅需要响应QNG。如下：

**>>> PNG\r\n**

**<<< QNG\r\n**

**服务器端Pings(Challenges)**

服务器段发送的Ping命令是CHL，而更通常的说法是Challenge，这是因为对于那三个字母（CHL）所表示的意义最好的解释了。

有时NS会发送Challenge命令，首先是初始状态用CHG设置不久，CHL之间没有固定周期，它包含两个参数 — 头一个总会是0，第二个被称作“Challenge串”，Challenge串通常包含20位数字，但客户端不会依靠这个串，它看 起来如下：

**<<< CHL 0 15570131571988941333\r\n**

接收Challenge命令后，你必须在50秒内发送一个QRY命令到服务器，否则将被断开。QRY是一个有效载荷命令，包含事务ID和两个参数：客户端标识串与有效载荷长度。同所有有效载荷命令一样，长度后跟新行，有效载荷指的是 不加新行前的部分。QRY中有效载荷部分是MD5的challenge串与客户端标识码。MD5摘要通常为32字节长。

如果你发送一个非法email地址或者不正确的MD5校验串，服务器将发送540错误，并关闭连接。如果你得到有效载荷错误，结果将很难预知。另外，服务器将以相同事务ID的命令QRY响应，并且不带任何参数。

**客户端标识信息**

不同微软客户端使用了不同的ID码与ID串，下面给出了标识串及其对应得标识码：

  客户端标识串                 客户端标识码

|  |  |
| --- | --- |
| msmsgs@msnmsgr.com | Q1P7W2E4J9R8U3S5 |
| PROD0038W!61ZTF9 | VT6PX?UQTM4WM%YR |
| PROD0058#7IL2{QD | QHDCY@7R1TB6W?5B |
| PROD0061VRRZH@4F | JXQ6J@TUOGYV@N0M |

使用哪个标识串不关键，关键的是要使用相应得标识码，如：你不能使用**msmsgs@msnmsgr.com**，而应该**VT6PX?UQTM4WM%YR**。

MD5概要

MD5是一个信息概 要运算，对于一个串应用MD5摘要，将得到一 个32字节的指纹串。 如有可能，尽量找到创建MD5指纹的库或者扩 展程序，当然如果你觉得你有足够的能力，你也可以参照官方描述（RFC 1321）来实现。确 认你的库可以产生小写的十六进制数字（应该作为其中的一个选项）。

当服务器给你 一个Challenge串时，添加你的 客户端码到尾部。如，服务器给出的是**abcdefg**,而你的客户端码为**1234567**，提供给MD5函数的串就应该为**abcdefg1234567**，指纹为**d1713d0f1d2e8fae230328d8fd59de01**，建议你用这 个例子验证你的实现。

服务器Ping示例

下例是服务器Ping及响应的示 范，你应该通过它来验证你的MD5实现的是否正 确。最可能的错误是在challenge串编码前或后添 加了一个新行到尾部：

**<<< CHL 0 15570131571988941333\r\n**

**>>> QRY 1049 msmsgs@msnmsgr.com 32\r\n**   
**8f2f5a91b72102cd28355e9fc9000d6e (no newline)**

**<<< QRY 1049\r\n**

**获 取个人详细资料**

本节阐述了如何从MSN Messenger得到自己的个人资料，其中包括了联系人员名单及他们所 属的组，个人电话及其他私人设置。

官方客户端登录后，所作的第一件事情就是发送SYN命令找回联系表中所有信息，本节对于联系表给出了一些背景信息，并给出了SYN的详细描述。

以下将介绍一些MSN中关于私人信息方面的基本概念。

版本号

完整的个人资料中包含一个版本信息，每次联系表有改变（不管是你还是别人改变的），版本信息将增 加，如果资料改变后又改回去（即使你离线了），版本号还是会增加两次。

版本号的目的是保持服务器与客户端联系资料一致。客户端应该对于所有的联系资料缓存。客户端登录 时，如果发现与上次登出时没有变化，就会避免下载所有的个人详细资料。版本号总是在0与4294967295(2^32-1)之间。

Forward列表(FL)

Forward列表，简写为FL，是一群联系人的列表，你订阅了他们的 状态。你期望服务器能够通知他们的在线状态，电话号码，等等。外行可能把他们叫做“联系表”。

这个列表目前（2003年3月23日）最多可以有150人，旧版本为75人。如果尝试添加第151个人，将收到210错误，且不能添加。

Forward列表中的每一个人属于一个或 多个组，这些组通过组码来区分，例如默认情况下，他们都属于0这一组。

反向列表

反向列表简写为RL，是那些在他们的Forward列表中有你的联系人们。你不能修改该列表，如果尝试增加或者删除，NS将立即断开，还不告诉你为什么。

许可列表

许可列表缩写AL，是你允许他们看到你的在线状态的联系人们 — 与反向列表相 对，是请求能够看到你在线状态的人员们。如果有人从他（她）的联系表中把你去除，你的RL中也会自动去除他（她），但AL中确不会。他（她）不会在接收到你的在线状态信息，但他（她）如果重新加你的话，你的客户端会按照 你原来的设置允许他（她）可以看到你的在线状态。

黑名单

简称BL，其中的人员被阻止看到你的在线状态。他们不会收到你的状态，并且当他们尝试要求你加入一个交换板会 话中时，他们会被通知你不在线。AL与BL中不应该有同样一个人，如果你尝试添加一个人到两个列表，你会收到219错误。

组列表

你的Forward列表中所属的组。每个组包含一个名字和ID。你被保证至少有一个组（联系表中所有人属于默认组），默认的名字是“~”。

客户端与服务器通常使用组ID而不是名字。

电话号码

MSN Messenger允许你登记你的 个人、家庭和单位的电话号码，同样也可以登记你的MSN Mobile和MSN Direct设备，如果你有的话。你的FL中的人员电话号码应该会自动发送给你，但2003年11月时，微软的服务器中的一个bug显示这个并没有实现。你可以选择电话号码是否可用，并且黑名单中的人们应该得到空号码信息，毕竟这 还涉及到很多个人隐私性的问题。

4.4.3.       同步

SYN就是用来同步以上四个列表，组列表， 电话号码，还有一些与服务器的隐私设置。官方客户端会在登录后，初始化状态前同步。在同一个会话中发送SYN多次是没有任何意义的，而且还很有可能 被断开。应该是登录后就立即发送SYN，因为服务器不会主动发送给你某些命令，除非你先（比如反向列表的附加信息）。客户端应该缓存数据的 版本信息，这将有助于减少登录时间。

发送SYN

SYN包含一个事务ID和一个参数—缓存的版本信息（0，如果客户端没有任何个人资料）。如果缓 存版本与服务器版本相同（也就是说没有什么变更），服务器便不会发送列表到客户端。否则，服务器将把所有信息发送过来。

下载这些资料需要花费一定时间 — 在一个慢连接上 下载一个大列表需要10秒以上。最好在变更初始状态前发送SYN，毕竟你不会希望在收到信息前，其他人不得不等待你下载资料。

下面是两个示例：

**>>> SYN 12 2194\r\n**

**>>> SYN 13 0\r\n**

SYN响应

SYN应答是MSN Messenger应答中极少因情形 不同发挥参数不同的应答之一。如果客户端缓存过期，应答会包含一个事务ID和一个参数（版本）。否则应答将包含事务ID和3个参数：更新后的版本，联系表中人员数，你定义的组个数。

如果缓存是最新的，同步将结束，并且不再有任何应答。否则，服务器将发送如下额外应答（以如下次 序）：

.GTC — 某人添加你到他的联系表中时，做什么

.BLP — 默认列表，指出那些明确允许及阻止的人们。

.PRP — 电话号码（可使用的/非空号码，仅发送一次）。

.LSG — 组列表（你以前定义的组们，仅发送一次）。

.LST — 人员列表（你的联系表中的人员们，仅发送一次）

这些应答都不包含事务ID。

SYN应答实例

如下实例中缓存的版本信息为“125”，对于服务器来说是最新的版本信息。

**>>> SYN 1 125\r\n**

**<<< SYN 1 125\r\n**

下例中，客户端没有缓存，服务器发送全部列表。为了方便阅读，响应中添加了空行，协议中是没有的。

**>>> SYN 1 0\r\n**

**<<< SYN 1 139 5 4\r\n**  
  
**<<< GTC A\r\n**  
**<<< BLP AL\r\n**  
  
**<<< PRP PHH 01%20234\r\n**  
**<<< PRP PHM 56%20789\r\n**  
  
**<<< LSG 0 Other%20Contacts 0\r\n**  
**<<< LSG 1 Coworkers 0\r\n**  
**<<< LSG 2 Friends 0\r\n**  
**<<< LSG 3 Family 0\r\n**  
  
**<<< LST principal1@passport.com principal1 4\r\n**  
**<<< LST principal2@passport.com principal2 10\r\n**  
**<<< LST principal3@passport.com principal3 11 1,3\r\n**  
**<<< LST principal4@passport.com principal4 11 0\r\n**  
**<<< BPR PHH 01%20234\r\n**  
**<<< BPR MOB Y\r\n**  
**<<< LST principal5@passport.com principal5 12\r\n**  
**<<< LST principal6@passport.com principal6 11 2\r\n**  
**<<< BPR PHW 45%206789\r\n**

隐私设置

MSN Messenger中包含两种隐私 设置：GTC和BLP。

GTC

可以设置GTC的值为A或者N。客户端应该按照这个值约束它的行为。该值不会经服务器处理，而且对其他客户端也非建议。

该值用来指示某人被添加到RL，并且他还没有被放入AL或BL中时，期望客户端应该如何处理。有可能，例如，某人曾经在你的RL中，后来被删除了，然后又添加，这个时候 他就获取在你的BL或 者AL中。默认的 设置是A。因为服 务器对该值仅存储，所以添加联系人到某个列表还应该是客户端的工作。服务器不会自动做这些操作。

如果GTC值为A或者BLP为BL，官方客户端将提醒用户某人新加入到反向列表，并询问允许还是阻止他们。否则，将自动加入允许列表。

BLP

类似GTC，BLP的值存储在服务器上，但每次客户端登录时都会重新得到。BLP也有两个值：AL和BL。不像GTC，服务器读取该值，并依靠该值作某些不 同的事情。

既不在AL也不在BL中的人员将按照BLP中指定的那样对待。如果BLP设置为AL，他们将被允许邀请你到一个交换板会话中，并进行聊天。如果为BL，他们将被告知你不再现，同时也不能要请 你聊天。默认值为AL。

4.4.5.       电话号码

仅有的获取设置的电话号码的机会就是在一个SYN中。个人电话号码将会在BLP后立即发送，并包含在PRP应答中。每个PRP应答包含两个参数：三字母的电话类型和电话号码。

以下是5种不同电话类型，按发送次序排列：

.PHH — 家庭电话

.PHW — 工作单位电话

.PHM — 移动电话

.MOB — 大概是其他人可以通过MSN Mobile联系我的方式？

.MBE — 是不是我在MSN Mobile上有一个移动设备并可使用？

电话号码如果为空将不会发送，MOB和MBE除非可以使用否则不会发送。如上因素，当接收到第一个LSG应答时就应该断定电话号码已经完成接收 （总是会至少有一个LSG应答）。

以上头三个的值部分可以为昵称中允许的任意字符（URL编码），最长为95个字符。

MOB与MBE的值可以仅仅是Y（Yes）。如果MOB被设置，客户端将允许用移动设备通过PAG命令联系他。如果MBE被设置，看起来客户端在MSN Mobile上激活了一个移动设 备。注意：这些值与PHM移动电话号码是绝对互不相干的。

有报告称有第六个值（WWE）被用来指出MSN Direct设备。WWE应用同MOB，但如果可以使用的会被设置为“2”。MSNP8种没有发现该值，并且到2003年11月为止，在正当测试中，MSN Messenger服务器处理电话号码时依然存在Bugs。

下例是某人的电话号码资料，她的家庭电话，拥有一个移动设备但不允许在MSN上查阅。注意，家庭电话是URL编码的，解码后结果应该是“555 555-0690”。

**<<< PRP PHH 555%20555-0690\r\n**  
**<<< PRP MBE Y\r\n**

组列表

    PRP发送完毕后，NS将用LSG发送你定义的组信息，每个组信息都会用 到一个LSG，每 个LSG都包含组ID，URL编码的组名，和一个数字（官方客户端总 会设置为０，但其他值也可以。译者注：不理解，服务器发送的数跟客户端设置不设置有什么关系？？？），如果没有添加到任何组，默认组名为“~”，ID为0。

联系表

发送LSG应答后，NS将发送联系表中的人员信息。最后一个LST响应结束后，整个同步过程就完成了。

LST是另外一个可变参数的应答：

.第一个参数是帐号

.第二个参数是昵称

.第三个参数是所在列表ID

.如果人员在你的FL中，第四个参数是用逗号分隔的所属组ID。

如果人员在你的FL中，在LST后还会紧随一些BPR应答（如果他们设置了他们的电话号码）。BPR的格式同PRP类似，除了没有MBE应答对应。如果一个联系人的MOB设置为Y，意味着你可以通过PAG命令翻阅，如果WWE设置为2，你可以用PGD命令直接翻阅（译者注：Page单词太简单，却不太好翻译，这里译为翻阅）。

还有可能在SYN后收到BPR，在设置细节中有详细讨论。

列表码

第三个参数是联系人的列表码，表示他们处于那个列表中（允许列表、黑名单、Forward，反向列表）。每个列表有一 个数值—FL为1，AL为2，BL为4，还有RL为8。列表码可以相加以表示联系人在哪些列表 中。如，一个联系人在FL与AL中 但既不在BL也不 在RL中，那么列 表码为3。

因为列表码都是2的某次方，你可以通过位与知道一个联系人位于哪个列表。让联系人的列表码与各列表码相位与，就知道 是否在那个列表中。举例，如果联系人列表码为3，“3 AND 1”返回1（意味着在forward列表中），“3 AND 2”返回2（意味着在允许列表中），“3 AND 4”，“3 AND 8”都为0（意味着不在BL中，也不在RL中）。

反向列表中的每个人也应该在AL或BL中，但也并不总是这样（比如，如果总从你上一次登出后被加入），用14进行位与来验证（8+4+2），如果结果为8，就表示在RL中但没有在其他列表中。例如，如果一个联 系人的列表码为“１１”，“11 AND 14” 结果为10（意味着他们已经添加到AL中），然而如果是9的话，“9 AND 14”结果为8（意味着还没有加入到你的AL和BL中）。

设 置细节

    本节主要解释如何变更个人资 料，访问规则，隐私设置。

隐私设置

GTC

要改变GTC的值，就需要发送GTC命令然后携带事务ID及新值作为参数。如果成功，服务器就返回GTC，其后携带你的TrID，及新版本作为第一个参数，新GTC值作为第二个参数。如果尝试设置已经设置的值，将收到218错误，如果发送了一个错误参数，将会立 即被断开。

如下为一些设置GTC的例子：

**>>> GTC 20 A\r\n**

**<<< GTC 20 200 A\r\n**

**>>> GTC 21 N\r\n**

**<<< GTC 21 201 N\r\n**

**>>> GTC 22 N\r\n**

**<<< 218 22\r\n**

**<<< GTC 23 F\r\n**

**<o> Server Closes Connection**

BLP

如同改变GTC一样就可以改变BLP。如下：

**>>> BLP 24 AL\r\n**

**<<< BLP 24 202 AL\r\n**

**>>> BLP 25 BL\r\n**

**<<< BLP 25 203 BL\r\n**

**>>> BLP 26 BL\r\n**

**<<< 218 26\r\n**

**<<< BLP 27 FL\r\n**

**<o> Server Closes Connection**

有趣的是，当你的BLP设置为BL时，不在AL或BL中的人尝试邀请你到一个交换板会话中，他们就会收到216错误，而不是217。因为那样的话，就会知道你在线，但 他们或者在你的BL中， 或者因为BLP的 设置而自动被阻止。

4.5.3.       设置你的电话号码

要设置个人电话号码，就需要发送PRP命令，携带事务ID，还有三个字母的电话类型代码及其值。如果要设置空值的话，省去第二个参数。如果需要禁用或者取消MSN移动设备注册，把第二个参数设置为“N”。

如果成功的话，服务器将响应一个PRP命令加事务ID，版本信息，三字符代码，与电话号码。

如果发送的电话号码超过95字节长（一个URL编码字符按3字节计），服务器立即断开连接，且不响应任何错误。

如果尝试设置一种不存在的类型或者类型字符过短，如phh或PH，服务器将响应715错误。

如果电话类型超过3字符长，服务器将立即断开连接。

如果在MBE为N时设置MOB，服务器将响应MOB仍设置为N，并且不做任何变化。如果没有移动设备也可以把MBE设置为Y，但这样做没有任何意义。你也可以设置MBE为N，即便MOB仍旧为Y。

如果MOB或者MBE设置值不为Y也不为N，服务器将设置为N，而不管响应中如何回答。还有许多不可思议的异常，所以尽量不要让这些怪异的事情发生。

示例如下：

**>>> PRP 55 PHH 555-1234\r\n**

**<<< PRP 55 12183 PHH 555-1234\r\n**

**>>> PRP 56 PHW\r\n**

**<<< PRP 56 12184 PHW\r\n**

**>>> PRP 57 PHV 1234\r\n**

**<<< 715 57\r\n**

**>>> PRP 58 MOB Y\r\n**

**<<< PRP 58 12185 MOB Y\r\n**

**增删联系人**

增加联系人（ADD）

使用ADD命令来增加一个联系人。

.第一个参数是你想把此人加入到的列表

.第二个参数是联系人的帐号

.第三个参数是你指派的联系人的昵称。官方 客户端总会使用账号名作昵称，这就是为什么添加一个联系人后，总会显示他（她）的账号，除非他（她）登录你才会更新显示名。

.如果添加一个联系人到FL，就需要有第四个参数指出加入到的组ID。如果不指定，默认为0。你也可以回头再把联系人加入到另外一个 组，使得多个组中都包含此人。

当你头一次把某人加入到FL中时，你会收到所有的BPR列表。如果他们已经把你加入到他们的AL中，就会包含他们的实际电话。否则，电话号码将会是空值，当然只要他们加入到他们的AL后，正确的值也会发送给你。添加一个人 到一个新组，不会导致发送BPR，下面有关于SYN外接收BPR的讨论。

下面是你做不了的一些事情：

.不要添加一个联系人到RL，如果尝试，就会被立即断开。

.如果想把联系人同时加入AL与BL中，将收到219错误。

.如果FL中加入超过150个人（2003年3月23日最大值），产生210错误。

.如果尝试加入一个非法邮件地址返回201错误

.如果加入的合法地址不存在，你将收到205错误。

.如果把一个联系人加入到一个不存在的组，224错误。

.如果添加一个人到列表（或者FL中的组），但该人已经存在，215错误。

.201、205错误优先于224。

另外，2003年3月29日，如果昵称长于387字节（一个URL编码的字符计作3个字节，而不是1个），将立即被断开。这个长度同REA命令中相同。官方客户端不会显示大于129字符的显示名（3字节的URL编码字符计作揖个字符），注意129\*3=397。

如果ADD执行成功，服务器将以相同的ADD及参数返回，只不过列表类型及账号之间又多了一个新的版本信息。

如果添加联系人到FL中，ADD响应后将收到BPR，这些BPR将全部为空（除了MOB为N），即使联系人已经设置了电话号码。注意如果你没有发送过SYN命令的话（当前会话中），你不会收到BPR。

还有，如果你把某人加入到FL中时，联系人正好在线，并且你也在他们的AL的话，你将接收到一个ILN，携带与ADD相同的事务ID，及对方的初始状态。否则，对方加入你到他们的AL中时，你将收到NLN。注意：如果他们离线，这可能会等待一段时间。

示例：

**>>> ADD 18 AL a@b a@b\r\n**

**<<< 201 18\r\n**

**>>> ADD 19 FL non\_existent\_account@passport.com non\_existent\_account@passport.com\r\n**

**<<< 205 19\r\n**

**>>> ADD 20 AL example@passport.com example@passport.com\r\n**

**<<< ADD 20 AL 1200 example@passport.com example@passport.com\r\n**

**>>> ADD 21 BL example@passport.com example@passport.com\r\n**

**<<< 219 21\r\n**

**>>> ADD 22 AL example@passport.com example@passport.com\r\n**

**<<< 215 22\r\n**

**>>> ADD 23 FL myname\_123@hotmail.com myname\_123@hotmail.com 1\r\n**

**<<< ADD 23 FL 1201 myname\_123@hotmail.com myname\_123@hotmail.com 1\r\n**  
**<<< BPR 1201 myname\_123@hotmail.com PHH\r\n**  
**<<< BPR 1201 myname\_123@hotmail.com PHW\r\n**  
**<<< BPR 1201 myname\_123@hotmail.com PHM\r\n**  
**<<< BPR 1201 myname\_123@hotmail.com MOB N\r\n**

**>>> ADD 24 FL principal@msn.com principal@msn.com 15\r\n** (nonexistent Group)

**<<< 224 24\r\n**

**>>> ADD 25 RL principal@msn.com principal@msn.com\r\n**

**<o> Server Closes Connection**

删除联系人(REM)

要删除一个联系人，就需要用到REM命令。同ADD命令十分相同，除了REM不需要昵称参数外。

如果你要从FL中删除一个联系人并且你也想从一个指定组中删除他，你需要指出组ID，就像ADD中那样。

如果REM执行成功，服务器也会返回REM命令及原来的参数，除了列表类型及账号间的版本信息。如下是导致错误的某些因素：

.删除一个并不在你的列表中的联系人，不管 他是否是一个合法的账号，都会产生错误216。

.尝试从RL中删除联系人，将会立即被断开。

.尝试从一个并不存在的组中删除一个联系 人，224。

.尝试从一个存在但并不属于的组中删除联系 人，225。

.216优先于225，224优先于216。

示例：

**>>> REM 26 AL a@b\r\n**

**<<< 216 26\r\n**

**>>> REM 27 FL non\_existent\_account@passport.com\r\n**

**<<< 216 27\r\n**

**>>> REM 28 FL valid\_account@hotmail.com\r\n** (Principal Not In List)

**<<< 216 28\r\n**

**>>> REM 29 FL principal123@msn.com 15\r\n** (nonexistent Group)

**<<< 224 29\r\n**

**>>> REM 30 FL principal321@msn.com 3\r\n** (Principal Not In Group)

**<<< 225 30\r\n**

**>>> REM 31 FL myname\_123@hotmail.com\r\n**

**<<< REM 31 FL 1202 myname\_123@hotmail.com\r\n**

**>>> REM 32 FL principal@msn.com 1\r\n**

**<<< REM 32 FL 1203 principal@msn.com 1\r\n**

**>>> REM 33 AL principal@msn.com\r\n**

**<<< REM 33 AL 1204 principal@msn.com\r\n**

**>>> REM 34 RL principal@msn.com\r\n**

**<o> Server Closes Connection**

组间移动联系人

移动联系人到另外一个组，只需要用REM命令从原组中删除，然后ADD到目的组。由于联系人可以在不同的组，所以不会介意你这样做有什么目的，示例如下：

**>>> REM 35 FL principal@msn.com 1\r\n**

**>>> ADD 36 FL principal@msn.com principal@msn.com 2\r\n**

**<<< REM 35 FL 1205 principal@msn.com 1\r\n**

**<<< ADD 36 FL 1206 principal@msn.com principal@msn.com 2\r\n**

MSN也支持一个联系人在多个组中，要实现 如此，只需要多次执行ADD命令，每次包含不同组ID即可。

阻止联系人

要阻止一个联系人，需要首先从AL移除该人（如果他（她）在AL中的话），然后把他（她）加入BL即可。

**>>> REM 27 AL principal@msn.com\r\n**

**<<< REM 27 AL 3053 principal@msn.com\r\n**

**>>> ADD 28 BL principal@msn.com principal@msn.com\r\n**

**<<< ADD 28 BL 3054 principal@msn.com principal@msn.com\r\n**

联系人更名（REA）

如下同样适用于个人显示名。

变更任意列表中某人的昵称，必须使用REA。REA有两个参数：欲修改的账号，URL编码的新昵称。如果成功，服务器将返回REA，其中包含新版本号，联系人账号和新昵称。

如果是你的账号，REA将正式修改你的显示名，并NLN通知其他在线人员（除非你看起来离线，或者阻止了那个联系人）。如果尝试修改你的显示名过于频繁， 将收到800错 误。注意，这样在变更其他人员时不适用。

如同ADD命令，昵称长于387字节（2003年3月29日止），将被立即断开。官方客户端也不允许联系人设置名称超过129字符（3个URL编码对应一个字符），并且不能正确显示129字节以上的显示名。如果想修改不再你 的任意列表中的人员名称，将收到216错误。这同样适用于账号是非法邮件地址。

基于某些原因，MSN可能不会让你使用某些词作为昵称，服务器将发送209错误。如果你尝试修改你的显示名，但是 护照并未验证也会收到此错误。（当你提交护照后，你将收到一个email来核实你的护照的真实性）注意当给出非法人员的非法昵称时，209错误优先于216错误。

昵称中一些众所周知的限制单词有“msn”，“Microsoft”。不过突破这个限制太简单了，当你设置一个昵称时，把它进行URL编码，或者其中的某些字符，然后MSN就不会告诉你不合法了。如“MSN%20SUCKS”替换为“%4DSN%20SUCKS”，或者你的客 户端对每个字符进行编码。注意%4D就是M，%20就是空格。

示例：

**>>> REA 101 random\_principal@randomdomain.com nickname\r\n** (Principal Not In List)

**<<< 216 101\r\n**

**>>> REA 102 mypassport@passport.com msn%20help\r\n**

**<<< 209 102\r\n**

**>>> REA 103 mypassport@passport.com new%20name\r\n**

**<<< REA 103 3055 mypassport@passport.com new%20name\r\n**

组

组是从MSNP7开始添加到MSN协议中的，每个FL中的联系人可以属于1个或多个组。如果没有指定，联系人默认属于0组。每个组都有一个名字及ID，但通常我们都用ID来引用一个组，组名只是为了终端用户显示使用的。

添加组（ADG）

增加一个新组，就要用到ADG命令，它包含2个参数，第一个参数是URL编码的组名，第二个参数是0。

.如果组名长度大于128字节（2003年3月29日），服务器将立即断开。

.如果组名大于61字节（2003年3月29日），将收到229错误，注意%20是3个 字节，而不是一个字节。

.如果尝试增加第31个组（2003年3月29日时30是 最大值），将收到223错误。注意组0也是30个 组中之一。

如果ADG执行成功，服务器响应ADG，第一个参数是你的新版本信息，第二个是组名（应该与你指定的一致），第三个是组ID。第四个是0。

示例：

**>>> ADG 37 this%20group's%20name%20is%20sixty%20two%20bytes%20in%20length 0\r\n**

**<<< 229 37\r\n**

**>>> ADG 38 My%20New%20Group 0\r\n**

**<<< ADG 38 4029 My%20New%20Group 4 0\r\n**

**>>> ADG 39 thirtyfirst%20group 0\r\n** (31st Group)

**<<< 223 39\r\n**

因为组是用ID来描述的，所以你可以指定不同的组相同的名称，确认你的客户端可以这样实现。当然，因为你不能添加大 于30个组，所以 所有的组ID应该 在0到29之间。组ID是可以重新使用的（如果使用了第三个组， 然后删除组3，再 添加另外一个组，这个组将变成组3），但也不要依赖这个特点，应该是合乎情理的就接受。

ADG的最后一个参数很怪，在早些时间（MSNP7中还是这样），服务器将依赖一个 怪异的串，而不是0。 如果你指定了其他数字，结果也没什么不同，但服务器同样响应那个值。真不知道，这个参数是做何用途，看来还是需要你来探索了。

删除组 （RMG）

RMG命令可以用来删除一个组，并且需要挟 带仅有的一个参数 — 组ID，服务器将用另外一个RMG来响应，第一个参数是版本，第二个参数是组ID。如果组不存在，服务器将响应224错误，如果尝试删除默认组，会得到230错误。

如果你删除了一个组，请记住其中的联系人也将不再那个组中了，如果其中的联系人在多个不同的组中， 则对方将仍属于其他组，但是如果那个联系人仅属于已删除的组，对方也将从你的FL中被删除。

**>>> RMG 40 4\r\n**

**<<< RMG 40 4030 4\r\n**

**>>> RMG 41 4\r\n**

**<<< 224 41\r\n**

**>>> RMG 42 0\r\n**

**<<< 230 42\r\n**

组更名

REG用来给一个组更名，其中第一个参数为 组ID，第二个参 数为URL编码的 名称，第三个参数同ADG一样，客户端总会发送0，但你发送其他数值也没什么不同。

就像ADG命令，如果新的名称大于128字符（2003年3月29日），将被立即断开。但少于128个字符的话不会出现什么错误，所以如果你想把一个组的名称定义为127个字符，你必须首先添加一个61或更小长度的字符串，然后再更名到127个长度。如果尝试对一个不存在的组更 名，会得到224错 误。由于组的总数有限制（３０个），如果尝试对一个大于29的组ID更名，将会立即被断开。但删除组时不是这样。另外，变更默认组的名称也不会有什么错误。

如果REG成功，服务器将对应REG，第一个参数为新版本，第二个参数为组ID，第三个参数为新的组名（应该同你指定的相同），第四个参数同ADG的一样（一般为0）。

示例：

**>>> REG 43 3 My%20New%20Name 0\r\n**

**<<< REG 43 4031 3 My%20New%20Name 0\r\n**

**>>> REG 44 20 NewName 0\r\n** (Group Does Not Exist)

**<<< 224 44\r\n**

**>>> REG 45 30 NewName 0\r\n**

**<o> Server Closes Connection**

**他人变更资料时**

RL变更

他人从FL中添加/删除你，他们也会从你的RL中被添加/删除，因此你会从服务器收到ADD或REM命令，他包含为0的事务ID，并且有3个或四个参数：

.第一个参数总会是RL

.第二个参数是新版本

.第三个参数是联系人的帐号

.如果为ADD，第四个参数为联系人的显示名

**<<< ADD 0 RL 3049 example@passport.com My%20Name\r\n**

**<<< REM 0 RL 3050 example@passport.com\r\n**

电话号码变更

注意：截至2003年11时，微软的服务器的一个BUG告诉我们BPR不会在SYN外发送，但如果他们被发送，版本号依然会更新，对于客户端就有很多问题了（包括官方客户端）。

如果ＦＬ中的某人变更了电话号码，就同接收ADD一样应该会收到 BPR，即使一次收到多个BPR，每一个都会包含一个不同的版本。

与SYN中的BPR不同，这里的BPR包含四个参数：

.第一个参数是新版本号

.第二个参数是联系人账号

.第三个参数是电话类型（PHH，MOB等等）

.第四个是电话号码

**<<< BPR 12183 example@passport.com PHH 555%20555-4321\r\n**

如果你阻塞了某人，他们只能收到空白信息（你的电话非空的话）。

**消 息(通知服务器发送给MSN客户端的消息)**

       概述

消息(MSG)在有效载荷命令中有所介绍，可以被用来从NS发送信息到客户端。DS服务器从来就不发送消息。客户端也从来不应该发送消息到NS或DS，如果尝试的话，服务器将立即关闭连接。

消息可以用来发送指出系统消息，邮件通知，profile信息等，这些消息与通过交换板发送的直接会话消息相互独立，虽然他们用了同样的命令。

从NS发送的消息其账号为Hotmail，显示名为Hotmail。但没有规则约束非要如此，所以客户端应该可以接收任意地址的消息。

4.6.2.       初始化消息

登录成功后，NS总是会发送一个profile消息给客户端，另外，如果客户端用Hotmail的账号登录并且收件箱中有未读邮件，NS将发送一个邮件通知。

Profile消息

在所有已知的情况中，发送最后一个USR后，NS将立即发送一个profile消息，它的Content-Type为**text/x-msmsgsprofile**，这个消息有一个大的头部信息，并包含许多字段，而且没有主体。

微软有过偶尔变更字段的历史，下面的例子中是2003年11月17日，你不应该认为这些字段将全部发送，也不应该认为都是按此顺序发送。

**MSG Hotmail Hotmail 425\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsprofile; charset=UTF-8\r\n**  
**LoginTime: 1050223062\r\n**  
**EmailEnabled: 0\r\n**  
**MemberIdHigh: 85040\r\n**  
**MemberIdLow: -517030579\r\n**  
**lang\_preference: 1033\r\n**  
**preferredEmail: example@hotmail.com\r\n**  
**country: US\r\n**  
**PostalCode: 90201\r\n**  
**Gender: m\r\n**  
**Kid: 0\r\n**  
**Age: \r\n**  
**BDayPre: 5\r\n**  
**Birthday: 0\r\n**  
**Wallet: 0\r\n**  
**Flags: 1027\r\n**  
**sid: 507\r\n**  
**kv: 4\r\n**  
**MSPAuth: 4sCuECZ4UsAaBIy0AIsk!c9bWcuATTmuQ$$\r\n**  
**ClientIP: 1.2.3.4\r\n**  
**ClientPort: 516.\r\n**

其中很多字段对于自动登录到Hotmail是很有用的，有些就是信息性的，还有一些我们也不知道该做何解释。

.LoginTime — 你登录的Unix时间，也就是说1970年1月1日午夜至今的秒数（UTC时间）。

.EmailEnabled — 用户的账号是否包含邮件通知（目前仅Hotmail，MSN.com帐号），1或0

.MemberIDHigh — 不知道

.MemberIDLow — 不知道

.lang\_preference — 首选语言码

.preferredEmail — 用户的主要邮件地址

.country — 两位数字的国家码

.PostalCode — 用户的邮政编码（US: zip code）

.Gender — 用户性别（m,f或者U未指定）

.Kid — 账号是否是儿童护照（0或1）

.Age — 年龄

.BDayPre — 不知道

.Birthday — 数字型生日

.Wallet — 是否拥有MS Wallet（0或1）

.Flags — 不知道

.sid — Hotmail登录需要的数值

.kv — Hotmail登录需要的数值

.MSPAuth — 不确信的长串，Hotmail登录用（90字节，可能会变更）

.ClientIP — 服务器认为的你的IP地址

.ClientPort — 你连接用的端口号。

MSPAuth的值已被截短。大多数信息看 起来没有用，除了Hotmail自动的登录用的那些外。

注意：MSN.com账号基本相同，但因为某些原因，使用MSN.com的账号，客户端将收到2个profile消息：一个EmailEnabled设置为0，另外一个设置为1但不包含LoginTime字段，除了这些，消息是完全相同的。

客户端IP及端口号

ClientIP及ClientPort指出了服务器所认为的 客户端连接用的IP及 端口号。连接的原端口在客户端机器上，目的端口（MSN Messenger会话中通常为1863）是服务器的监听端口。不幸的是，MSN Messenger服务器端有一个Bug可以导致“ClientPort”毁坏，你需要做些工作 得到真正的端口号。

技术的讨论中，说这个值已经被“字节交换”了，关于到底做了些什么已经超出我们的范围了。有很多方 法可以得到正确的值，但建议按（（ClientPort AND 255）\*256）+((ClientPort AND 65280)/256)计算，按照公式写一个函数很简单，但要解释这些二 进制运算很难。……

客户端端口及地址可以被用来猜测，是否到服务器的连接经过了某种网络地址转换（NAT）或者代理服务器。MSNP8中，这些信息仅用来在文件传输中 决定“Connectivity”字段的值，其他高级应用在MSNP9中有介绍。

### 会 话示例

概述

本节对通知会话的整个过程作了一个示范，但本节并没有（也不会）显示每一个与NS交互的命令。

约定

本节中客户端以alice@passport.com为例。

示例

登录 — messenger.hotmail.com

客户端（alice@passport.com）连接到messenger.hotmail.com:1863，客户端使用协议8，支持CVR0。

**>>> VER 1 MSNP8 CVR0\r\n**

**<<< VER 1 MSNP8 CVR0\r\n**

成功商议协议版本后，客户端给出了它的协议版本信息。

**>>> CVR 2 0x0409 win 4.10 i386 MSNMSGR 5.0.0544 MSMSGS example@passport.com\r\n**

**<<< CVR 2 6.0.0602 6.0.0602 1.0.0000 http://download.microsoft.com/download/8/a/4/8a42bcae-f533-4468-b871-d2bc8dd32e9e/SETUP9x.EXE http://messenger.msn.com\r\n**

Alice的客户端尝试自行认证，而服务器 重定位到baym-cs118.msgr.hotmail.com(IP:207.46.106.118)，端口号1863。

**>>> USR 3 TWN I alice@passport.com\r\n**

**<<< XFR 3 NS 207.46.106.118:1863 0 207.46.104.20:1863\r\n**

登录 — baym-cs118.msgr.hotmail.com

客户端连接到baym-cs118.msgr.hotmail.com:1863，客户端可以解释协议版本8，CVR0。

**>>> VER 4 MSNP8 CVR0\r\n**

**<<< VER 4 MSNP8 CVR0\r\n**

客户端再次给出协议版本信息

**>>> CVR 5 0x0409 win 4.10 i386 MSNMSGR 5.0.0544 MSMSGS example@passport.com\r\n**

**<<< CVR 5 6.0.0602 6.0.0602 1.0.0000 http://download.microsoft.com/download/8/a/4/8a42bcae-f533-4468-b871-d2bc8dd32e9e/SETUP9x.EXE http://messenger.msn.com\r\n**

Alice的客户端尝试自行认证，服务器返 回了Passport认证所需的一长字符串。

**>>> USR 6 TWN I alice@passport.com\r\n**

**<<< USR 6 TWN S lc=1033,id=507,tw=40,fs=1,ru=http%3A%2F%2Fmessenger%2Emsn%2Ecom,ct=1062764229,kpp=1,kv=5,ver=2.1.0173.1,tpf=43f8a4c8ed940c04e3740be46c4d1619**

Alice通过MS Passport认证，响应她的ticket：

**>>> USR 7 TWN S t=53\*1hAu8ADuD3TEwdXoOMi08sD\*2!cMrntTwVMTjoB3p6stWTqzbkKZPVQzA5NOt19SLI60PY!b8K4YhC!Ooo5ug$$&p=5eKBBC!yBH6ex5mftp!a9DrSb0B3hU8aqAWpaPn07iCGBw5akemiWSd7t2ot!okPvIR!Wqk!MKvi1IMpxfhkao9wpxlMWYAZ!DqRfACmyQGG112Bp9xrk04!BVBUa9\*H9mJLoWw39m63YQRE1yHnYNv08nyz43D3OnMcaCoeSaEHVM7LpR\*LWDme29qq2X3j8N\r\n**

**<<< USR 7 OK alice@passport.com Alice 1 0\r\n**

现在Alice成功登录到NS。她的客户端可能会记住下次直接访问baym-cs118.msgr.hotmail.com，而不是messenger.hotmail.com。服务器这时会发送Alice的profile：

**<<< MSG Hotmail Hotmail 491\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsprofile; charset=UTF-8\r\n**  
**LoginTime: 1050223062\r\n**  
**EmailEnabled: 0\r\n**  
**MemberIdHigh: 85040\r\n**  
**MemberIdLow: -517030579\r\n**  
**lang\_preference: 1033\r\n**  
**preferredEmail: alice@passport.com\r\n**  
**country: US\r\n**  
**PostalCode: 90201\r\n**  
**Gender: m\r\n**  
**Kid: 0\r\n**  
**Age: \r\n**  
**BDayPre: 5\r\n**  
**Birthday: 0\r\n**  
**Wallet: 0\r\n**  
**Flags: 1027\r\n**  
**sid: 507\r\n**  
**kv: 4\r\n**  
**MSPAuth: MSPAuth: 41bbzZ\*NzDmDQ8ic4HWo89b9zhCBk!?ONDJKB3Los8UMgBnCOLSwQKo!8IeIH?QF0vVItSlOzIL36e5MAdMaB3mpZw$$\r\n**  
**ClientIP: 1.2.3.4\r\n**  
**ClientPort: 516.\r\n**  
**\r\n**

同步

Alice的客户端现在需要同步她的联系 表，上次登录时Alice的客户端版本号为6，但现在版本号已经是27了。

**>>> SYN 8 6\r\n**

**<<< SYN 8 27 5 4\r\n**

由于版本信息不匹配，服务器将发送所有Alice的联系信息（而不是版本6与27之间更改的部分）。首先，服务器在每个数据包中发送一个信息。

**<<< GTC A\r\n**  
**<<< BLP AL\r\n**  
  
**<<< PRP PHH 01%20234\r\n**  
**<<< PRP PHM 56%20789\r\n**

然后服务器在一个包中发送全部组列表。由于Alice的客户端使用的编程语言一次获取一个数据包，不得不把每行都分开，然后每次处理一行。

**<<< LSG 0 Other%20Contacts 0\r\n**  
**LSG 1 Coworkers 0\r\n**  
**LSG 2 Friends 0\r\n**  
**LSG 3 Family 0\r\n**

然后服务器发送Alice的联系表，联系表中第一个人是Bob，昵称为“Bob”，他在FL，BL与RL中。他没有共享电话号码，但我们却可以使用一个MSN mobile设备。他的详细信息在一个包中被发送，我们也不得不分开， 然后一行一行处理。

**<<< LST bob@passport.com Bob 13 0\r\n**  
**BPR MOB Y\r\n**

Alice列表中的第二个人是Carol，昵称Carol，她共享了她的工作电话（9876-54321），但没有其他信息 了。不幸的是，服务器用两个包来发送Carol的资料，中间有间隔。Alice的客户端必须重建这些行数据，然后才可以进行处理。

**<<< LST carol@passport.com Carol 3 0\r\n**  
**BPR PHM 9876**

**<<< -54321\r\n**

然后服务器发送来Dave的资料，Dave在Alice的FL中，并处在Coworkers、Friends、Family组中。他的家庭电话为“3.1415926535”，工作电话为“2.71841844”，移动号码为sqrt(-1)，服务器用了几个包来发送资料。

**<<< LST dave@passport.com 1 1,2**

**<<< ,3\r\n**  
**BPR PHH 3.1415926535\r\n**  
**BPR PH**

**<<< W**

**<<<**

**<<< 2.71841844\r\n**  
**BPR PHM sqrt(-1)\r\n**

下一个是Eve（邪恶的偷听者），已经被阻止，而看不到Alice的在线状态。

**<<< LST eve@passport.com Eavesdropper 12\r\n**

最后是Fred，应该是最近添加的，因为他在Alice的RL中，但既不在AL也不在BL中。

**<<< LST fred@passport.com Fred 8\r\n**

下面是相互之间能接收状态信息的描述：

.Alice想得到Bob, Carol与Dave的在线信息，但她不知道对方是否允 许她知道。

.Bob想得到Alice的在线状态，Alice也允许。

.Carol可以得到Alice的在线状态，但他并不想。

.Dave想得到Alice的在线信息，但不被允许

.Eve想得到Alice的在线信息，但不被允许

.Fred想得到Alice的在线信息，且允许得到。他既不 在Alice的AL中也不在BL中，但由于Alice的BLP设置为AL，所以他将按AL处理。Alice的客户端应该马上提示Alice应该加入哪个列表中。

初始状态

好的，Alice已经同步完毕她的联系表，现在她需要发送她的初始状态，并且允许Fred看到她的在线状态。在线状态命令将导 致服务器发送状态信息给联系人。注意ADD响应处在了ILN中，这样更难处理了一些。

**>>> CHG 9 NLN 0\r\n**  
**>>> ADD 10 AL fred@passport.com Fred\r\n**

**<<< CHG 9 NLN 0\r\n**  
**ILN 9 NLN bob@passport.com Bob 24\r\n**  
**ILN 9 IDL carol@passport.com Carol 268435492\r\n**

**<<< ADD 10 AL 28 fred@passport.com Fred 1\r\n**  
**ILN 9 BSY emily@passport.com Emily 268435492\r\n**

Challenge

服务器用“29409134351025259292”询问Alice的客户端

**<<< CHL 0 29409134351025259292\r\n**

客户端添加“Q1P7W2E4J9R8U3S5”到尾部，得到串“29409134351025259292Q1P7W2E4J9R8U3S5”，然后获得MD5摘要“d0c1178c689350104350d99f8c36ed9c”。

**>>> QRY 11 msmsgs@msnmsgr.com 32\r\n**  
**d0c1178c689350104350d99f8c36ed9c (no newline)**

服务器接收了Alice的响应

**<<< QRY 11**

在线状态变更

Alice离开了她的计算机，数分钟后，Alice的客户端设置她的在线状态为“idle”。

**>>> CHG 12 IDL 0\r\n**

**<<< CHG 12 IDL 0\r\n**

这个时候，Bob离线了

**<<< FLN bob@passport.com\r\n**

Alice回来后，客户端设置在线状态为“online”

**>>> CHG 13 NLN 0\r\n**

**<<< CHG 13 NLN 0\r\n**

不久，Carol设置为“Busy”，并改变了她的显示名

**<<< NLN BSY carol@passport.com Caroline 268435492\r\n**

昵称变更

由于Carol最后改变在线状态时变更了显示名，Alice的客户端就需要更新资料。

**>>> REA 14 carol@passport.com Caroline\r\n**

**<<< REA 14 28 carol@passport.com Caroline\r\n**

Alice决定不再让Bob看到她的在线信息了，于是她的客户端 把Bob从AL中删除，然后添加到BL中。

**>>> REM 15 AL bob@passport.com\r\n**  
**ADD 16 BL bob@passport.com Bob\r\n**

登出

最后，Alice退出MSN Messenger。

**OUT\r\n**

**<o> Server closes connection**

## 交换板服务器相关协议：

交换板

认 证

连接到一个交换板有两种方法：或者请求一个交换板会话或者被邀请加入一个已存在的交换板中。这两个 事件都是发生在NS上。 当连接到一个交换板时，客户端需要处理会话创建(XFR)与被邀请(RNG)之间的不同。

**请求一个交换板会话**

通知服务器

要请求一个交换板会话，客户端必须发送XFR命令到NS，其中包含事务ID及一个参数SB(交换板)，服务器将用另外的XFR响应，其响应需要依照交换板认证指示，下面是一个示例：

**>>> XFR 15 SB\r\n**

**<<< XFR 15 SB 207.46.108.37:1863 CKI 17262740.1050826919.32308\r\n**

.第一个参数告诉你正在转入交换板中（这应 该总是相同的）。注意DS中，这个参数将变为NS。

.第二个是交换板服务器的地址与端口（总会 是1863），其 间用冒号分隔

.第三个指出了认证类型，总应该是CKI

.第四个是认证串，当连接到交换板时，客户 端用它来证明身份。

然而如果你没有设置你的初始状态，或者你处于HDN中，你就不能连接到交换板中，并收到913错误，而不是XFR应答。

交换板服务器

现在，客户端必须创建一个TCP连接到指定IP及端口（不要关闭NS连接）。客户端可以等待至少2分钟，而连接到交换板还很安全。

一旦连接到交换板，客户端必须发送USR命令，它包含事务ID，帐号及认证串。这个命令必须在约一分钟内发送，否则交换板将断开连接。

如果成功的话，服务器将用USR响应，并包含事务ID、OK、你的帐号及显示名。

.如果账号与认证串之一（或全部）不正确， 服务器将响应911错 误，并关闭连接。

.如果格式不正确，服务器将立即关闭连接， 不响应错误。

.如果用正确的认证串尝试错误的交换板服务 器（不同ＩＰ），将被立即断开，不响应错误。

.如果已经用此认证串登录到交换板服务器， 还尝试登录，将收到911错误，并断开。注意你可以同时连接多个交换板，但你需要发送多个XFR，然后根据一个连接一个。

示例：（正确登录）

**<o> Client Connects to 207.46.108.37 1863 (Switchboard)**

**>>> USR 1 example@passport.com 17262740.1050826919.32308\r\n**

**<<< USR 1 OK example@passport.com Example%20Name\r\n**

**<o> Continue SB Session . . .**

示例（不正确）：

**<o> Client Connects to 207.46.108.37 1863 (Switchboard)**

**>>> USR 1 example@passport.com 17262740.1050826919.32307\r\n**

**<<< 911 1\r\n**

**<o> Switchboard Closes Connection**

你已经连接到交换板，现在邀请他人加入吧。

**被邀请到交换板会话中**

通知服务器

当一个联系人邀请你加入一个交换板会话，你会收到通过NS发送的RNG命令，官方客户端将自动连接到一个交换 板会话中，并且如果直到文本消息被发送对话框才会打开，但第三方的客户端能选择不同行为。

RNG不带事务ID，带6个参数：

.第一个参数是新的交换板会话的session ID。每个交换板会话都有 一个唯一ID，每 个被邀请的联系人使用同一个session ID。你需要拿ID与交换板进行认证。

.第二个参数是交换板服务器的IP及地址（冒号分隔）

.第三个参数是认证类型，总会是CKI。

.第四个参数是认证串，与交换板认证是需要 用到。

.第五个、第六个参数是邀请你的联系人的账 号及URL编码的 显示名。

示例：

**<<< RNG 11752013 207.46.108.38:1863 CKI 849102291.520491113 example@passport.com Example%20Name\r\n**

客户端不响应此命令，而是根据第二个参数打开一个到指定IP及端口的连接。

交换板服务器

由于XFR的原因，你应该在两分钟内打开一个TCP连接到服务器以接收RNG命令。首先你应该发送ANS命令，它包含事务ID及3个参数：账号名、认证串及交换板会话ID。

如果成功的话，服务器将响应一个或多个IRO，最后跟随一个ANS，但毕竟还有很多事情会导致错误发生：

.如果你连接，但没有发送ANS，交换板将在约1分钟后关闭连接，且不含任何错误。

.如果接收RNG一分钟内你没有连接，交换板将关闭连 接，在ANS前不 包含任何错误。

.无论怎样，只要会话ID错误，将立即断开，不含错误。

.如果你发送一个不存在的或者非法的账号， 并且（或者）不正确的认证串，911错误，服务器将关闭连接。

.如果ANS语法错误，立即断开，没有错误

.连接到错误的交换板，并尝试认证，断开并 不含错误。

.你（或攻击者）已经连接并认证，再次认 证，将得到911错 误，交换板将关闭连接。

.如果交换板会话中的联系人在你连接并发送ANS前离开，交换板会话将在你进入前撤 销，因此你ANS发 送后也将被断开且不含任何错误。

已在交换板中的参与者被发送IRO命令，可能作为初始名册。每个参与者将收到一个IRO。注意你，已经进入，但并不包含在这个 名单内。IRO包 含ANS中同样的 事务，并且有4个 参数：

.第一个参数表示当前IRO为列表中的第几个。第一个IRO命令中为1，第二个中为2，依次类推。

.第二个参数是IRO命令总数。

.第三个参数是参与者的账号

.第四个参数是参与者的显示名，如果自从加 入会话板后，参与者修改了他们的显示名，这个参数将过期。

由于交换板给你的显示名可以是过期的，你应该使用尽可能使用NS给你的显示名。

收到最后一个IRO后（增加数同总数同），你将收到ANS，事务ID与你发送的相同，并携带参数OK。收到此命令后，你将正式进入交换板会话，可以收发消息了。

如下，是交换板的认证，并且找到了两个参与者（总共3人）：

**<o> Client Connects to 207.46.108.38 1863 (Switchboard)**

**>>> ANS 1 name\_123@hotmail.com 849102291.520491113 11752013\r\n**

**<<< IRO 1 1 2 example@passport.com Mike\r\n**

**<<< IRO 1 2 2 myname@msn.com My%20Name\r\n**

**<<< ANS 1 OK\r\n**

**<o> Continue SB Session . . .**

**杂 项**

邀请参与者

如果没有被当前的一个参与者邀请的话，一个联系人不能进入一个交换板会话中。任何参与者，不一定是 会话的创建者，都可以邀请其他联系人。不知道一个交换板中最多可以有多少人，但很可能大于30。过去的限制为5人。

你可以邀请同一个联系人到不同的交换板中 — 如，在一个中交 谈，另外一个中传输文件。然而，官方客户端将尝试在单个窗口中处理所有的会话，可能导致结果有些混乱。如果你有一个以上的会话需要选择，你应该总是发送消 息到最后收到消息的会话中。

CAL

邀请一个联系人到交换板会话中，就需要发送CAL命令，它包含事务ID还有要邀请的账号。

如果成功的话，服务器将用CAL加刚才的事务ID响应，同时RINGING作为第一个参数，交换板的会话ID作为第二个参数。注意这只不过是邀请某人的一个确认 — 这个联系人还没 有加入会话中。稍后，我们就知道还需要JOI命令。当然，会话ID对于客户端来说并不重要，对于每个被邀请的联系人来说他们是相同的。

下列情况将会导致CAL命令错误：

.如果你尝试邀请已在会话中的联系人（包括 你自己），215错 误。这个错误同样会在对方已经被邀请或者被另外的参与者邀请但还没有加入时产生。

.如果格式不正确（如太少或者太多参数）， 将被交换板立即断开。然而对于交换板其他的事实是，NS不被通知，而且NS的连接仍旧会保持打开着。

.如果账号非法，如@@a，208错误，但仍保持连接。

.如果联系人离线或者账号名不存在（比如说myname@hotmail），217错误，但不会断开连接。

.如果你尝试邀请的联系人虽然在线但阻止了 你，或者BLP设 置为AL但你不在 对方的AL中，216错误。不会被断开。

.如果重复邀请已经阻止你的联系人，你将收 到713错误。

示例：

**>>> CAL 2 name\_123@hotmail.com\r\n**

**<<< CAL 2 RINGING 11752013\r\n**

**>>> CAL 3 nonexistent@passport.com\r\n**

**<<< 217 3\r\n**

**>>> CAL 4 offline@passport.com\r\n**

**<<< 217 4\r\n**

**>>> CAL 5 @@a\r\n**

**<<< 208 5\r\n**

**>>> CAL 5 blocking\_you@passport.com\r\n**

**<<< 216 5\r\n**

**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 713 5\r\n**

发送CAL的人才会看到这些来往的CAL命令还有错误。当制定的联系人加入会话时，每个联系人将受到一个JOI命令。

JOI

如果CAL成功，指定的联系人将收到NS发送的RNG命令，如果他们连接到交换板并认证的话，他们将加入到会话中，一旦发生，每个会话中的联系人（除了刚 被加入的）将被发送JOI命令。

JOI命令不包含事务ID。第一个参数是刚进入会话的联系人的账 号，第二个参数是他的显示名（URL编码），示例：

**<<< JOI name\_123@hotmail.com Name\_123\r\n**

**退出交换板会话**

要离开交换板，客户端应该发送OUT命令，并且不需要挟带事务ID及任何参数。交换板将关闭连接并从会话中把你去除。断开连接但没有发送OUT命令，效果是相同的。示例：

**>>> OUT\r\n**

**<o> Switchboard Closes Connection**

当一个参与者离开会话，其他参与者（如果还有的话）将收到BYE命令，不带事务ID，包含刚离开的联系人的账号。示例：

**<<< BYE example@passport.com\r\n**

空闲会话

如果你是会话中唯一的一个参与者（或者你没有邀请别人或者其他人都已经离开），交换板将在5分钟后关闭连接。关闭连接前，服务器不会 发送任何命令。

如果会话中有两个人，但互相间有5分钟没有发送任何命令，交换板将给两人都发送BYE命令，显示对方离开并立即关闭连接。然而BYE命令在账号后包含一个附加参数，值为1，表示交换板是由于发呆而被关闭的。示例：

**<<< BYE example@passport.com 1\r\n**

**<o> Switchboard Closes Connection**

会话中3个及以上人员的情况同2个的类似，除了发呆期间延长为15分钟，并且你只将收到一个参与者的BYE（随机选择）。

官方客户端

无论使用官方客户端的用户何时关闭了打开交换板的消息窗口，它将断开与交换板的连接。3个及以上的参与者的会话，如果有一个人离 开官方客户端都会通知你，但如果为2个的话，不会通知。

与NS的关系

由于交换板服务器与NS结合并不十分紧密，一个联系人可以退出了NS，但仍然在一个或多个交换板会话中。官方客户端退出MSN Messenger时，首先对每个会 话板发送OUT命 令，然后才OUT NS。

5.3.        消 息

5.3.1.       概述

    在交换板会话中MSG是发送消息给其他联系人仅有的方法。 每个发送给会话的消息都会转而发送给会话中其他的人。MSG可以是即时会话，类型通知，应用邀请，或者任意类型（只要你想发送的话）— 但并不是所有客户端都会识别所有类型。

5.3.2.       输出消息

发送消息到交换板，需要发送MSG命令

.必须有一个事务ID

.第一个参数是你希望收到的确认类型，可以 为U，N或者A。如果为U，你将收不到任何确认。如果为N，你仅在消息没有正确被接收时得到确认。 如果为A，不管被 接收成功与否，都会得到确认。该参数是大小写敏感的（必须为大写，否则交换板将关闭连接，并不发送消息）。确认将叙述如后。

.第二个参数是有效载荷的长度。

.MSG的有效载荷在新行后，有效载荷可以 为0字节长。

.一个消息最多可达1664字节长（2003年4月30日），再长的话，交换板将关闭连接，且不会发送消息。有趣的是：1664=13\*2^7。许多迷信的人认为13是一个不吉利的数字，7是一个吉利数字。……

示例：

**>>> MSG 4 N 133\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/plain; charset=UTF-8\r\n**  
**X-MMS-IM-Format: FN=Arial; EF=I; CO=0; CS=0; PF=22\r\n**  
**\r\n**  
**Hello! How are you?**

你不必以新行结束一个有效载荷。有效载荷的结尾决定了有效载荷的长度，一个附加的新行将在有效载荷 结尾添加了一个空行。

确认

确认是被交换板发回以确定接收者是否成功接收。服务器可以用ACK或NAK响应，他们包含事务ID及外出消息MSG。ACK意味着所有接收者接收成功。NAK意味着一个或多个参与者不能正确接收 消息。如果交换板会话中只有你的话，NAK将被发送。

如果确认参数设置为A，则成功的话返回ACK，否则NAK。与协议草案中暗示的相反，类型A工作着，并且正确与否都会回应。如果为N仅当不成功时才会收到消息，且为NAK。如果为U，不会有任何确认。

示例：

**>>> MSG 4 N 133\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/plain; charset=UTF-8\r\n**  
**X-MMS-IM-Format: FN=Arial; EF=I; CO=0; CS=0; PF=22\r\n**  
**\r\n**  
**Hello! How are you?**

**<<< ACK 4**

官方客户端用N发送即时消息(text/plain)，U发送键入通知（text/x-msmsgscontrol），N发送应用邀请。

**来报**

来报的格式已经在有效载荷命令中叙述了，第一个参数是发送人的帐号，第二个参数是发送人的显示名 （注意加入会话后变更显示名，仍将为原名），第三个参数是有效载荷的长度。

示例

**<<< MSG example@passport.com Mike 133\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/plain; charset=UTF-8\r\n**  
**X-MMS-IM-Format: FN=Arial; EF=I; CO=0; CS=0; PF=22\r\n**  
**\r\n**  
**Hello! How are you?**

按照长度解析来报长度非常重要！消息就像其他命令一样，可能被分割到若干包中，然后与其他命令合成 一个包。现在知道长度有多重要了吧。

### 会 话示例

本节演示了交换板会话的整个过程，至少看上去是这样的。有两个例子：第一个是来报RNG，第二个是外出的XFR。

约定

本节示例都是从Alice的客户端（alice@passport.com）角度看的。

示例1

通知服务器

另外一个联系人（bob@passport.com）邀请Alice加入一个会话，当前会话中已经有两个人：Bob与Carol。

**<<< RNG 17342299 207.46.108.78:1863 CKI 1056411141.26158 bob@passport.com Bob\r\n**

保持打开NS连接，Alice的客户端按指定服务器又打开一个新连接。现在开始NS不会影响SB，反之亦然。

交换板

Alice的客户端连接服务器207.46.108.78:1863，然 后发送认证信息

**>>> ANS 1 alice@passport.com 1056411141.26158 17342299\r\n**

认证成功，服务器发送参与者名单，并以ANS应答来确认。

Bob输入了一条信息并发送，这个信息是以Lucida Sans Unicode字 体写的，并加粗，颜色为绿色。

**<<< MSG bob@passport.com Bob 89\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgscontrol\r\n**  
**TypingUser: bob@passport.com\r\n**  
**\r\n**  
**\r\n**

**<<< MSG bob@passport.com Bob 143\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/plain; charset=UTF-8\r\n**  
**X-MMS-IM-Format: FN=Lucida%20Sans%20Unicode; EF=B; CO=ff0000; CS=0; PF=22\r\n**  
**\r\n**  
**Hello.**

Alice输入消息，然后发送，消息以MS Sans Serif字体，黑色书 写，并没有其他效果。

**<<< MSG 2 U 91\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgscontrol\r\n**  
**TypingUser: alice@passport.com\r\n**  
**\r\n**  
**\r\n**

**>>> MSG 3 N 127\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/plain; charset=UTF-8\r\n**  
**X-MMS-IM-Format: FN=MS%20Sans%20Serif; EF=; CO=0; CS=0; PF=0\r\n**  
**\r\n**  
**Hi.**

Alice输入了另外一个消息并发送。然而Carol网络出了问题，没有收到此消息， 所以Alice的 客户端收到了NAK， 即使Bob收到了 消息。Alice被 通知有一个或多个参与者没有收到消息。

**>>> MSG 4 U 91\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgscontrol\r\n**  
**TypingUser: alice@passport.com\r\n**

**>>> MSG 5 N 138\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/plain; charset=UTF-8\r\n**  
**X-MMS-IM-Format: FN=MS%20Sans%20Serif; EF=; CO=0; CS=0; PF=0\r\n**  
**\r\n**  
**Are you there?**

**<<< NAK 5\r\n**

接着Alice再次输入消息并发送，但她花费了很长时间输入，所以我们的客户端发送了两次键入通知。这次消息以类型A（没有特殊原因），每个人都收到，Alice的客户端收到ACK。

**>>> MSG 6 U 91\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgscontrol\r\n**  
**TypingUser: alice@passport.com\r\n**

**>>> MSG 7 U 91\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgscontrol\r\n**  
**TypingUser: alice@passport.com\r\n**

**>>> MSG 8 A 139\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/plain; charset=UTF-8\r\n**  
**X-MMS-IM-Format: FN=MS%20Sans%20Serif; EF=; CO=0; CS=0; PF=0\r\n**  
**\r\n**  
**I like turtles.**

**<<< ACK 7\r\n**

Alice邀请Dave（dave@passport.com），Dave加入会话。

**>>> CAL 8 dave@passport.com\r\n**

**<<< CAL 8 RINGING 17342299\r\n**

**<<< JOI dave@passport.com Dave\r\n**

Alice尝试邀请Ed(ed@passport.com)， 但他离线了。

**>>> CAL 10 ed@passport.com\r\n**

**<<< 217 10\r\n**

Alice尝试邀请Frank（Frank@passport.com），但 他的个人设置及列表设置表明Alice不被允许邀请他，尽管他在线。

**>>> CAL 10 frank@passport.com\r\n**

**<<< 216 10\r\n**

Bob邀请了George(goerge@passport.com)，并加入

**<<< JOI george@passport.com George\r\n**

Carol离开

**<<< BYE carol@passport.com\r\n**

15分钟没有动作，会议超时。

**<<< BYE bob@passport.com 1\r\n**

交换板服务器关闭连接，Alice的客户端通知Alice会议超时终止。

5.4.3.       示例2

通知服务器

客户端(alice@passport.com)登录到NS并成功认证，但由于“显示为脱机”，收到913错误。

**>>> XFR 7 SB\r\n**

**<<< 913 7\r\n**

Alice更改了状态为NLN，并重新请求。

**>>> CHG 8 NLN 0\r\n**

**<<< CHG 8 NLN 0\r\n**

**>>> XFR 9 SB\r\n**

**<<< XFR 9 SB 207.46.108.46:1863 CKI 189597.1056411784.29994\r\n**

到NS仍旧打开，但Alice的客户端建立到指定服务器的连接。现在NS与SB之间不会有什么事情发生了。

交换板

Alice的客户端连接到207.46.108.46:1863并发 送认证信息，认证正确，服务器给出了确认信息。

**>>> USR 7 alice@passport.com 189597.1056411784.29994\r\n**

**<<< USR 7 OK alice@passport.com Alice\r\n**

Alice邀请Bob(bob@passport.com)加 入会话并加入

**>>> CAL 8 bob@passport.com\r\n**

**<<< CAL 8 RINGING 189597\r\n**

**<<< JOI bob@passport.com Bob\r\n**

Bob想发送一个文件给Alice

**<<< MSG bob@passport.com Bob 277\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Application-Name: File Transfer\r\n**  
**Application-GUID: {5D3E02AB-6190-11d3-BBBB-00C04F795683}\r\n**  
**Invitation-Command: INVITE\r\n**  
**Invitation-Cookie: 135395\r\n**  
**Application-File: turtle.txt\r\n**  
**Application-FileSize: 2341\r\n**  
**\r\n**

Alice接收这个文件。

**>>> MSG 9 N 182\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Invitation-Command: ACCEPT\r\n**  
**Invitation-Cookie: 135395\r\n**  
**Launch-Application: FALSE\r\n**  
**Request-Data: IP-Address:\r\n**  
**\r\n**

**<<< MSG bob@passport.com Bob 244\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Invitation-Command: ACCEPT\r\n**  
**Invitation-Cookie: 135395\r\n**  
**IP-Address: 203.121.147.134\r\n**  
**Port: 6891\r\n**  
**AuthCookie: 1639797\r\n**  
**Launch-Application: FALSE\r\n**  
**Request-Data: IP-Address:\r\n**  
**\r\n**

Alice的客户端建立到Bob的IP及端口6891的连接，并在当前交换板外进行文件传 输。

然而，如果Alice的客户端在一段时间内（官方客户端为30秒）没有连接的话，Bob的客户端将停止等待连接，并发送如下消息，提示超时了。

**<<< MSG bob@passport.com Bob 152\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Invitation-Command: CANCEL\r\n**  
**Invitation-Cookie: 135395\r\n**  
**Cancel-Code: FTTIMEOUT\r\n**  
**\r\n**

Alice邀请Bob实用NetMeeting会话，然而他拒绝了，并 没有更多事情发生。

**>>> MSG 10 A 292\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Application-Name: NetMeeting\r\n**  
**Application-GUID: {44BBA842-CC51-11CF-AAFA-00AA00B6015C}\r\n**  
**Session-Protocol: SM1\r\n**  
**Invitation-Command: INVITE\r\n**  
**Invitation-Cookie: 6185072\r\n**  
**Session-ID: {60F887C8-A5D0-11D7-A88E-0040F43DB1D9}\r\n**  
**\r\n**

**<<< ACK 10\r\n**

**<<< MSG bob@passport.com Bob 225\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Invitation-Command: CANCEL\r\n**  
**Cancel-Code: REJECT\r\n**  
**Invitation-Cookie: 6185072\r\n**  
**Session-ID: {CE1ABB0F-D40D-432F-A359-5AEC532CDBC3}\r\n**  
**Session-Protocol: SM1\r\n**  
**\r\n**

Bob邀请Alice使用白板，但Alice没有安装，所以她的客户端以REJECT\_NOT\_INSTALLED自 动拒绝了邀请。

**<<< MSG bob@passport.com Bob 335\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Application-Name: Whiteboard\r\n**  
**Application-GUID: {1DF57D09-637A-4ca5-91B9-2C3EDAAF62FE}\r\n**  
**Session-Protocol: SM1\r\n**  
**Application-URL: http://www.microsoft.com\r\n**  
**Invitation-Command: INVITE\r\n**  
**Invitation-Cookie: 3861056\r\n**  
**Session-ID: {463CB365-0213-4933-AA8A-D01FAA996858}\r\n**  
**\r\n**

**>>> MSG 11 A 216\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Invitation-Command: CANCEL\r\n**  
**Cancel-Code: REJECT\_NOT\_INSTALLED\r\n**  
**Invitation-Cookie: 3861056\r\n**  
**Session-ID: {60F887CB-A5D0-11D7-A88E-0040F43DB1D9}\r\n**  
**\r\n**

**<<< ACK 11\r\n**

Alice关闭了会话窗，因此客户端发送了OUT。

**>>> OUT\r\n**

服务器关闭了连接。

## MSN客户端相关的协议

.         客户端

消 息

消息类型

官方客户端使用了三种标准类型：即时会话(text)，键入类型通知与应用程序邀请。每种不同类型的消息都被头部信息中Content-Type唯一标识着。客户端 可以发送非官方的类型如加密和特色商议等。官方客户端忽略所有非标准类型的消息，因此所有客户端也应该如此。另外，官方客户端忽略畸形消息：如不带MIME头的消息。

**即时消息(text/plain)**

    即时消息，又被称为文本消 息，是MSN来往 间正规的消息类型。他们以Content-Type: text/plain或者Content-Type: text/plain; charset=UTF-8（指定了不同的编码 方式）被发送。

**键入通知（text/x-msmsgscontrol）**

键入通知将会发送给其他参与者，告诉他们你正在键入消息。

.它使用Content-Type: text/x-msmsgscontrol，不必携带charset=UTF-8

.它的头部包含一个TypingUser字段，内容应该为你的 账号。

.主体仅为一个新行(\r\n)

示例（仅为有效载荷部分，不是MSG行）

**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgscontrol\r\n**  
**TypingUser: example@passport.com\r\n**  
**\r\n**  
**\r\n**

.如果用户正在键入信息，官方客户端将每隔5秒钟发送一个键入通知。

.如果官方客户端收到一个键入通知，它将指 示那个联系人正在键入信息。收到消息后或者10秒没有收到新的键入通知的话，这个提示将被取消。

.如果某人变更了TypeingUser字段，官方客户端将 出现一个Bug， 它将显示那个值，而不是你的显示名。

**应用邀请（text/x-msmsgsinvite）**

    应用邀请用来邀请联系人加入应用，如文件传输、音频会话、视频会议、NetMeeting、远程辅助、白板、游戏 等等。邀请使用Content-Type: text/x-msmsgsinvite; charset=UTF-8，字符集不是可选的。

非官方的消息类型

    如果你要编写一个自己的MSN Messenger客户端，你可以 发送任意的消息类型，当然那这些会被官方客户端所忽略。如果要这样做，建议对你的消息类型写一个详细描述，以便其他人也可以使用它。

**纯 文本消息**

    文本消息，又称为即时消息， 是联系人之间发送的常规信息。发送一个文本消息，指示客户端接收，并显示，可选择携带一些简单格式。

消息格式

Content-Type字段

文本消息以**Content-Type: text/plain**发 送，默认为ISO 8859-1编码。**Content-Type: text/plain; charset=UTF-8**，UTF-8编码。如果创建了其他类型的字符集（比如charset=iso-8859-15），官方客户端将不会显示，ISO-8859-1与UTF-8在基础知识的连接节中有描述。

X-MMS-IM-Format字段

指出了消息格式，如字体、颜色等。这个字段是可选的。如果忽略，客户端按默认格式显示。

Body

文本消息的主体就是纯文本 — 没有特殊字符，转移字符等。如果你的客户端收到ISO 8859-1格式的信息，可能需要 转换为UTF-8。

手工添加新行或者空行，需要添加\r\n，单个的\r或者\s将造成不可预知结果。

图释可能会包含在纯文本信息中，他们将以文本形式表现。如笑脸应该为“:)”，不需要任何特殊代码。

信息示例

两行信息及UTF-8编码

**MIME-Version: 1.0\r\n**  
**Content-Type: text/plain; charset=UTF-8\r\n**  
**X-MMS-IM-Format: FN=Arial; EF=I; CO=ff0000; CS=0; PF=22\r\n**  
**\r\n**  
**Hello!\r**  
**How are you?**

ISO 8859-1编码，两行，没有格式 选项，带一个图释

**MIME-Version: 1.0\r\n**  
**Content-Type: text/plain\r\n**  
**\r\n**  
**I'm fine. :)\r\n**  
**And you?**

X-MMS-IM-Format字段

X-MMS-IM-Format字段值是一 列参数。你不要期望这些参数按照固定次序排列，或者包含全部参数。2003年夏天的时候，如果FN被包含的话，交换板服务器将把它作为第一个，如果不是这样的话，服务器将不发送任何信息并关闭连 接。这大概是老版本的官方客户端中字体名有bug的原因。

官方客户端总是发送大写的参数名，如果发送小写，或者大小写混杂的参数给官方的话，结果不可预知。 但第三方客户端应该大小写都可。

注意：有可能指定字体大小。客户端应该按照用户设置决定字体大小。

**字体名(FN)**

FN指出了字体的名称，必须为URL编码的。如“MS Sans Serif”，应该为“**FN=MS%20Sans%20Serif**”，字体名大小写不敏感，但空格必须被URL编码。对于其他字符如数字与字母进行编码，结果不可预知。如果客户端不包含指定字体，应该判断PF与CS参数。基本上，客户端应按照CS指定选择可以支持的字体，并且最接近PF的指定。如果那些参数都不存在，使用默 认字体。

过去使用官方客户端收到消息的字体包含许多%20时会有冲突发生。微软已经对SB服务器打了补丁，因此如果一个联系人尝试这样做的话，将会被断开连接。

**效果(EF)**

EF参数指出了可选的风格效果。可能的效果 有加粗、斜体、下划线与删除线。每种效果按它的名称的首字符引用。如一段文本需要加粗、斜体。包含参数EF=IB或者EF=BI。次序不惯间。不知道的效果将被忽 略。官方客户端以大写字母发送效果，如果收到小写效果结果不可预知。如果不需要效果，参数为空即可。

**颜色(CO)**

CO参数指出了字体颜色。许多版本的官方客 户端限制你仅能发送一些可选的颜色，实际上指定1千7百万中颜色是可能的（24-bit颜色）。CO字段的值是六个十六进制BGR串(blue-green-red，与HTML标准的RGB正好相反)。头两个十六进制的值在00到ff间，为蓝色的强度，接着是绿色，然后是红色。如要全红的话，就是CO=0000ff。

官方客户端总是发送小写十六进制字母，大写也无所谓。官方客户端将外出的信息中删除前置0，如0000ff就会变为ff，但都是合法的。黑色将被表示为单个0。其他情况，如7个字符的串，或者异常字符将导致不可预知 错误。

**字符集(CS)**

“character set”非常不明确。Content-Type字段中的charset=UTF-8与X-MMS-IM-Format字段中的CS意义完全不同。

字符集，最为X-MMS-IM-Format中的一部分时，指示的是一个字体应该知道如何转换到屏幕显示的字符集。主要应用于Windows中，在Unicode被广泛应用前的中间产物。一 个字体必须支持一种字符集，但可以支持多于一种，如Wingdings指示Symbol字符集，Verdana支持Western，Greek，Turkish，Central European与Cyrillic字符集。关于字符集的说明见MSDN页：http://msdn.microsoft.com/library/en-us/gdi/fontext\_89gz.asp。

CS参数中的字符集用一或两个十六进制数标 识（前置0被官方 客户端去掉并忽略），下面是Windows中预置的全部字符集列表：

**0** - **ANSI\_CHARSET**

ANSI characters

**1** - **DEFAULT\_CHARSET**

Font is chosen based solely on name and size. If the described font is not available on the system, Windows will substitute another font.

**2** - **SYMBOL\_CHARSET**

Standard symbol set

**4d** - **MAC\_CHARSETLT**

Macintosh characters

**80** - **SHIFTJIS\_CHARSET**

Japanese shift-JIS characters

**81** - **HANGEUL\_CHARSET**

Korean characters (Wansung)

**82** - **JOHAB\_CHARSET**

Korean characters (Johab)

**86** - **GB2312\_CHARSET**

Simplified Chinese characters (Mainland China)

**88** - **CHINESEBIG5\_CHARSET**

Traditional Chinese characters (Taiwanese)

**a1** - **GREEK\_CHARSET**

Greek characters

**a2** - **TURKISH\_CHARSET**

Turkish characters

**a3** - **VIETNAMESE\_CHARSET**

Vietnamese characters

**b1** - **HEBREW\_CHARSET**

Hebrew characters

**b2** - **ARABIC\_CHARSET**

Arabic characters

**ba** - **BALTIC\_CHARSET**

Baltic characters

**cc** - **RUSSIAN\_CHARSET\_DEFAULT**

Cyrillic characters

**de** - **THAI\_CHARSET**

Thai characters

**ee** - **EASTEUROPE\_CHARSET**

Sometimes called the "Central European" character set, this includes diacritical marks for Eastern European countries

**ff** - **OEM\_DEFAULT**

Depends on the codepage of the operating system

不要假定收到消息的客户端会明白所有字符集（Windows NT 3.51就包含了极少的字符集）。MSN Messenger仅允许你在一个CS中指定单个字符集。虽然可以任意指定， 但还是建议你选择一种最常用的、可以显示正确的字符集。

**字库与字间距（PF）**

PF定义了FN参数失败的话使用的字体。经常在客户端没 有找到指定字体时使用。值为两位十六进制数，用Windows API编程时，在RichEdit与LOGFONT中是PitchAndFamily的值。

头一个数描述了字体库，如下给出了对应列表。MSDN中：http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gdi/fontext\_9583.asp。

**0\_** - **FF\_DONTCARE**

指出一个 一般库名，This name is used when information about a font does not exist or does not matter. The default font is used.

**1\_** - **FF\_ROMAN**

Specifies a proportional (variable-width) font with serifs. An example is Times New Roman.

**2\_** - **FF\_SWISS**

Specifies a proportional (variable-width) font without serifs. An example is Arial.

**3\_** - **FF\_MODERN**

Specifies a monospace font with or without serifs. Monospace fonts are usually modern; examples include Pica, Elite, and Courier New.

**4\_** - **FF\_SCRIPT**

Specifies a font that is designed to look like handwriting; examples include Script and Cursive.

**5\_** - **FF\_DECORATIVE**

Specifies a novelty font. An example is Old English.

第二个数字指出了字间距 — 或者说字间的间隔，或者说可变宽度。

**\_0** - **DEFAULT\_PITCH**

Specifies a generic font pitch. This name is used when information about a font does not exist or does not matter. The default font pitch is used.

**\_1** - **FIXED\_PITCH**

Specifies a fixed-width (monospace) font. Examples are Courier New and Bitstream Vera Sans Mono.

**\_2** - **VARIABLE\_PITCH**

Specifies a variable-width (proportional) font. Examples are Times New Roman and Arial.

PF示例：

**12**

Times New Roman, MS Serif, Bitstream Vera Serif

**22**

Arial, Verdana, MS Sans Serif, Bitstream Vera Sans

**31**

Courier New, Courier

**42**

Comic Sans MS

**右对齐（RL）**

RL指出了信息是否应该右对齐。为1，则右对齐。如果这个参数值不为1，官方客户端总是忽略该参数。但其他任何 值都不会有什么效果，仍保持左对齐。

示例

       **X-MMS-IM-Format: FN=MS%20Sans%20Serif; EF=; CO=0; CS=0; PF=22**   
This **X-MMS-IM-Format** field expresses the MS Sans Serif font with no effects and a black colour.

       **X-MMS-IM-Format: FN=Comic%20Sans%20MS; EF=S; CO=800000; CS=0; PF=42**   
This field expresses the Comic Sans MS font in a dark blue colour, underlined, and bold.

       **X-MMS-IM-Format: FN=Verdana; CO=ff; EF=UB; PF=22; CS=cc**   
This field expresses the Verdana font in full red colour, with the strikeout effect, and with a Cyrillic charset. The parameters are in an unusual order, but as long as **FN** is in the front, it's all right.

       **X-MMS-IM-Format: FN=Courier%20New; EF=; CO=ff00ff; CS=0; PF=31**   
This field expresses the Courier New font in a bright magenta colour with no effects.

       **X-MMS-IM-Format: FN=My%20Hebrew%20Font; EF=; CS=b1; PF=00; RL=1**   
This field expresses a made up font called My Hebrew Font with no specified colour, no effects, a Hebrew charset, and right-alignment.

**邀 请消息**

MSN Messenger包含一个客户端 邀请他们进行频带外的会话机制。如远程协助、NetMeeting、文件传输及其他。出于某些原因文件传输的机制与其他邀请类型不同，建议你分开实现。

唯一标识

唯一标识是一个串唯一标识了某些资源。必须假定同一个标识不会产生两次。Windows下，有标准函数产生Globally Unique Identifiers(GUID)，格式被严格定义的。然而，这里的标识不必像GUID一样—任意串都是可以被接受的，大小写不敏感。如果你没有使用Windows，可以把当前时间、网卡的MAC地址与随机数，还有你的程序进程ID组合为一个标识。

**文件传输**

文件传输出现在官方客户端的版本3种，在版本5中已经升级，解决了接收进入TCP连接有困难的问题（不如在NAT防火墙后的那些计算机们）。后续章节中对该协议有详细描述。

概述

Alice要发送一个文件给Bob，所以她发送一个邀请，这个邀请必须 给出文件名及大小。如果Alice不能接收进入连接，邀请中应该提及。

Bob或者接收或者取消文件传输，如果拒绝 了，必须给出一个原因（如文件拒绝），如果接受了，由于Alice的邀请状态说明她不能接收进入连接，所以他应该在文件传输中作服务器，简单接受就可以了。

如果Bob作服务器，商议完毕。否则，Alice必须发送一个应答接受Bob的信息，然后作服务器。

商议最后结束，如果文件传输失败，可能提示超时错误。

指定作服务器的一端必须给出IP及端口，且给出本地IP及端口。如果Bob作服务器，他必须指出Alice（发送者）将连接到Bob（接收方）。

发送邀请

邀请信息以MSG命令发送，通过交换板会话，MIME-Version: 1.0，Content-Type: text/x-msmsgsinvite; charset=UTF-8。 主体部分为字段集合。通常，字段是任意次序的，不能被识别的字段必须被忽略掉。文件传输中，客户端可能会忽略所有可选字段 — 5.0以下的官方客户端总是忽略可选字段，5.0及以上版本不会这样。除了一个特殊情况：如果你发送了Connectivity字段，如果Sender-Connect字段存在于应 答中的话，就必须进行处理。

官方客户端仅在恰好两人的交换板会话中商议，所以如果邀请者与被邀请者没有共享这样一个会话的话， 发送邀请的客户端必须首先创建一个。不必在邀请发送的会话中响应。如，如果Alice与Bob在一个交换板中，Alice发送邀请给Bob，接着Carol进入了这个交换板，Bob就必须在不同的交换板会话中发送他的应答。

协议

每个信息包含一个邀请命令，每个命令的次序必须为：

* 1. 邀请者发送INVITE命令
  2. 被邀请者ACCEPT邀请
  3. 如果被邀请者不能提供服务，邀请者ACCEPT
  4. 任一客户端可能发送CANCEL命令，并携带撤销码FTTIMEOUT，如果传输中出现错误的话。如，官方客户端将在30秒内监听接入连接，然后就取消了服务。

头一个信息发送后，任一方都可以在任意时间发送CANCEL。其后不应该发送任何信息。

命令字段

协商中所有信息包含以下字段：

Invitation-Command

消息类型

Invitation-Cookie

1到2^32-1间的随机整数，唯一标识一个协商 （0是不合法 的）。该值决定了发送INVITE的发送方，必须在整个协商中保持一致。

INVITE字段

包含以下字段：

Application-Name

类的自然语言描述，可以不同，比如，官方客户端用英语称文件传输为File Transfer，Norwegian中为**Filoverføring**，日语中为**ファイル送信**。这仅应该是为用户描述用 — 如果说应用程序的GUID的话，谁会识别呢？

Application-GUID

类的唯一标识。一个类总会有相同的GUID，并且不会有第二个类与之相同。严格的说，应该是CLSID（通常用来标识一个类的GUID）。文件传输的GUID为{5D3E02AB-6190-11d3-BBBB-00C04F795683}，出于某种原因，官方客户端大小写敏感。

Application-File

发送的文件名

Application-FileSize

要发送的文件的字节长。如果发送中这个值与文件传输中指定值不同，将参照那个值。

Connectivity（可选）

如果客户端知道它不能接收接入连接，它应该发送该字段，并指示值为“N”。官方客户端依照初始profile决定该值，如果你愿意，也可 以让用户自己指定。

Cancel字段

CANCEl命令中只需要一个字段就是Cancel-Code，这是撤消的简要原 因。你应该看作是任意形式的字符串，官方客户端所使用的有：

FAIL

接收客户端不能识别任意指定的会话协议。

FTTIMEOUT

传输文件时出现错误

OUTBANDCANCEL

发送邀请的交换板窗口被关闭

REJECT

邀请被拒绝

REJECT\_NOT\_INSTALLED

客户端不支持应用GUID

TIMEOUT

等待ACCEPT超时（或者联系人撤销请求）

ACCEPT字段

下面的字段出现在所有的ACCEPT命令中

Launch-Application

指示另外的客户端需要（不要）载入一个扩展应用。由于文件传输在官方客户端内部处理，所以这里正常 情况下为“FALSE”，我们不知道有什么情况需要设置为“TRUE”。

提供服务的ACCEPT命令应该包含如下字段：

IP-Address

客户端需要连接到的IP地址，官方客户端从初始profile中得到你的Internet网关地址。

IP-Address-Internal（可 选）

如果头一个IP地址连接失败的话，需要尝试的第二个IP地址。最近的版本中官方客户端把你的网卡地址放在此处。

Port

主要的TCP监听端口。应该为6891。某些版本的官方客户端当你使用了不同地址时行为不一致。与IP-Address对应。

PortX（可选）

可选的第二个TCP端口。应该为11178。这个与IP-Address-Internal对应，所以如果你包含IP-Address-Internal的话，就需要包含该字段

PortX-Internal（可选）

如果包含该字段，其值必定与PortX相同，大概是兼容旧版本的官方客户端吧。

AuthCookie

1至2^32-1间的随机数，标识文件传输会话中 发送的文件（一旦有两个文件同时发送的话）

Sender-Connect（可选）

通常，接收文件的计算机连接到发送者方，如果发送者需要连接到接收者（如：发送者处在防火墙后）。

邀请示例

下面是两个客户端间成功文件传输邀请的示例，并支持改良的邀请方法。

**>>> MSG 12 N 294**  
**MIME-Version: 1.0  
    Content-Type: text/x-msmsgsinvite; charset=UTF-8  
      
    Application-Name: File Transfer  
    Application-GUID: {5D3E02AB-6190-11d3-BBBB-00C04F795683}  
    Invitation-Command: INVITE  
    Invitation-Cookie: 85366  
    Application-File: Autoexec.bat  
    Application-FileSize: 187  
    Connectivity: N**

**<<< MSG bob@hotmail.com Bob 306**  
**MIME-Version: 1.0  
    Content-Type: text/x-msmsgsinvite; charset=UTF-8  
      
    IP-Address: 81.99.77.64  
    IP-Address-Internal: 10.5.1.3  
    Port: 6891  
    PortX: 11178  
    AuthCookie: 544120  
    Sender-Connect: TRUE  
    Invitation-Command: ACCEPT  
    Invitation-Cookie: 227948  
    Launch-Application: FALSE  
    Request-Data: IP-Address:**

两个客户端间文件传输成功的邀请，但不支持更新的邀请方法，而且传输出现问题：

**>>> MSG 4 N 277**  
**MIME-Version: 1.0  
    Content-Type: text/x-msmsgsinvite; charset=UTF-8  
      
    Application-Name: File Transfer  
    Application-GUID: {5D3E02AB-6190-11d3-BBBB-00C04F795683}  
    Invitation-Command: INVITE  
    Invitation-Cookie: 33267  
    Application-File: readme.txt  
    Application-FileSize: 60904**

**<<< MSG example@passport.com Tim 179**  
**MIME-Version: 1.0  
    Content-Type: text/x-msmsgsinvite; charset=UTF-8  
      
    Invitation-Command: ACCEPT  
    Invitation-Cookie: 33267  
    Launch-Application: FALSE  
    Request-Data: IP-Address:**

**>>> MSG 4 N 238**  
**MIME-Version: 1.0  
    Content-Type: text/x-msmsgsinvite; charset=UTF-8  
      
    Invitation-Command: ACCEPT  
    Invitation-Cookie: 33267  
    IP-Address: 10.44.102.65  
    Port: 6891  
    AuthCookie: 93301  
    Launch-Application: FALSE  
    Request-Data: IP-Address:**

**>>> MSG 4 N 151**  
**MIME-Version: 1.0  
    Content-Type: text/x-msmsgsinvite; charset=UTF-8  
      
    Invitation-Command: CANCEL  
    Invitation-Cookie: 85366  
    Cancel-Code: FTTIMEOUT**

6.4.3.       其他邀请类型

    本节将讨论除文件传输外，其 他邀请的运行机制。官方客户端允许第三方的应用程序注册为邀请类型（如游戏“MechWarrior Mecenaries”）。如果你写了一个应用，并希望官方客户端支持 你的邀请类型，查阅MSDN’s Messenger API documentation：http://msdn.microsoft.com/library/default.asp?url=/library/en-us/messenger/messenger\_entry.asp。

概述

Alice想与Bob协商一个会话，就需要发送一个邀请，这 个邀请必须指出邀请类型（如voice conversation），并且能包含Bob需要知道的特定信息（如Alice的计算机支持的音频会话协议）。

Bob或者接受或者拒绝邀请。如果接受，应 答中必须包含他的IP地址，必须包含Alice的IP地址，并可以包含Alice需要的一些信息（如他选择的音频协议）。如果拒绝，应答中必须给出原因（比如语音传输不被支持）。

Alice接收了Bob的应答，并发送信息。她的应答必须包 含她的IP。

依据邀请类型，Bob可能会根据上下文发送最终信息。

协商结束。

发送邀请

每个邀请都作为交换会话中的MSG命令发送，MIME-Version: 1.0，Content-Type: text/x-msmsgsinvite; charste=UTF-8。 内容主体部分是若干字段，同样没有次序限制，不能识别的字段应该被忽略。客户端必须做好可选字段不存在的准备，与文件传输不同，客户端必须处理可选字段， 如果他们被发送的。

官方客户端只在有两个人的交换板会话中进行协商，所以如果邀请者与被邀请者没有共享一个私有会话， 发送邀请的客户端就必须首先创建一个。没有必要在发送邀请的会话中应答。如，如果Alice与Bob在一个交换板中，Alice发送了一个邀请，这时Carol进入了这个交换板，Bob就必须在另外的交换板会话中进行应答。

如果你希望在同一个会话中邀请两个人，你应该发送两个单独的邀请。

协议

每条信息包含一个“邀请命令”，必须按以下序列发送：

1、邀请者发送INVITE

2、被邀请者发送ACCEPT

3、邀请者打开监听，然后ACCEPT

4、邀请者发送一些Context（仅某些邀请类型时）

第一个消息发送后，CANCEL可以在任意部分任意时间发送。

一般字段

所有邀请包含以下字段

Invitation-Command

消息类型

Invitation-Cookie

1至2^32-1之间的整数，唯一表示一个商议（0为非法Cookie），该值被发送者的INVITE所确定，在整个协商期间内保持 一致。官方客户端随意选择Cookie。

Session-ID

当前MSN Messenger客户端的唯一标识，该值指出了一个特定客户端的特定实例 — 每个客户端每次 运行时都会产生一个新会话ID，并在整个生存期内使用同一个会话ID，直到程序结束。如果客户端退出，然后又重新进入，应该继续使用同一个会话ID。

INVITE字段

包含以下字段：

Application-Name

类的自然语言描述，可以是不同的，如官方客户端在English中称文件传输为File Transfer，Norwegian中称**Filoverføring**，日语中为**ファイル送信**。这仅应该是为用户描述用 — 如果说应用程序的GUID的话，谁会知道是什么呢

Application-GUID

类的唯一标识，抛开名称不管，这可以作为以上讨论的任何标识。一个类总会只有一个应用程序GUID，不会存在第二个类也使用该GUID。严格的说，更应该是CLSID。与文件传输不同，GUID大小写敏感。

Application-URL（可选）

下载指定应用的URL，一个应用总会有相同的Application-URL。如果Application-GUID不能被识别，客户端就需要建议用户防卫该URL。注意：绝对不要自动调入该URL，因为一个攻击者可能会利用该功能载入一个页，然后利用浏览器的Bug。

Session-Protocol

会话协议，应该被客户端所支持，官方客户端仅支持SM1。

Context-Data（可选）

特定目的的串（如协商协议的详细资料）

CANCEL字段

CANCEL命令仅需要一个额外字段Cancel-Code，其中简要描述了撤 销原因，你应该按任意格式的字符串对待，但官方客户端中会使用以下值：

FAIL

接收方不能解析你的邀请信息（如某些特定会话协议）

OUTBANDCANCEL

发送邀请信息的窗口被关闭。

REJECT

拒绝

REJECT\_NOT\_INSTALLED

应用未安装

TIMEOUT

超时（或者撤销了邀请）

第一个ACCEPT字段

第一个ACCEPT命令包含以下字段：

Session-Protocol

选用的会话协议（从INVITE消息中的列表中获得）。如果没有可以接受的协议，邀请将以cancel-code为FAIL被撤消。

Context-Data（可选）

特定目的串（如协商协议的详细资料）

Launch-Application

指示对方需要（不要）调入一个扩展程序。通常为“TRUE”，不知道什么时候可以为“FALSE”。

Request-Data

这个字段的值必须为“IP-Address:”，请求对方发送它的IP地址。

IP-Address

将作为客户端的IP地址（端口号可选）

第二个ACCEPT字段

包含以下字段

Launch-Application

指示对方（不）调入一个扩展，通常为“TRUE”，不知道什么情况可以设置为“FALSE”。

IP-Address

将作为服务器的IP地址（端口号可选）

Context字段

Context命令中包含：

Context-Data

特定目的串（如协商协议的详细资料）

邀请示例

下面从被邀请者角度，示范一个成功音频会话邀请过程：

**>>> MSG bob@hotmail.com Bob 353\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Application-Name: voice conversation\r\n**  
**Application-GUID: {02D3C01F-BF30-4825-A83A-DE7AF41648AA}\r\n**  
**Session-Protocol: SM1\r\n**  
**Context-Data: Requested:SIP\_A,;Capabilities:SIP\_A,;\r\n**  
**Invitation-Command: INVITE\r\n**  
**Invitation-Cookie: 1578608\r\n**  
**Session-ID: {CD482FDC-AE24-3574-C2A5-493813AD94D1}\r\n**  
**\r\n**

**<<< MSG 16 N 319\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Invitation-Command: ACCEPT\r\n**  
**Context-Data: Requested:SIP\_A,;\r\n**  
**Invitation-Cookie: 1578608\r\n**  
**Session-ID: {A8B34C0E-2EEF-932F-F120-F7492E39CDA9}\r\n**  
**Session-Protocol: SM1\r\n**  
**Launch-Application: TRUE\r\n**  
**Request-Data: IP-Address:\r\n**  
**IP-Address: 203.122.147.102\r\n**  
**\r\n**

**>>> MSG bob@hotmail.com Bob 242\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Invitation-Command: ACCEPT\r\n**  
**Invitation-Cookie: 1578608\r\n**  
**Session-ID: {CD482FDC-AE24-3574-C2A5-493813AD94D1}\r\n**  
**Launch-Application: TRUE\r\n**  
**IP-Address: 203.122.147.102:13455\r\n**  
**\r\n**

**<o> Connect to 203.122.147.102:13455 . . .\r\n**

下例中，由于被邀请者没有安装音频，音频会话邀请失败：

**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Application-Name: Remote Assistance\r\n**  
**Application-GUID: {56b994a7-380f-410b-9985-c809d78c1bdc}\r\n**  
**Session-Protocol: SM1\r\n**  
**Application-URL: http://www.microsoft.com\r\n**  
**Invitation-Command: INVITE\r\n**  
**Invitation-Cookie: 3863032\r\n**  
**Session-ID: {DF93A302-30D2-DF92-C392-F391049DB9EA}\r\n**  
**\r\n**

**<<< MSG 7 N 162\r\n**  
**MIME-Version: 1.0\r\n**  
**Content-Type: text/x-msmsgsinvite; charset=UTF-8\r\n**  
**\r\n**  
**Invitation-Command: CANCEL\r\n**  
**Invitation-Cookie: 3863032\r\n**  
**Cancel-Code: REJECT\_NOT\_INSTALLED\r\n**  
**\r\n**

邀 请类型

    许多Messenger相关协议被称为邀请，本节描述了协商特定协议时一些邀请类型。协议中需要你发送“IP-Address: IP:port” 而不是仅仅“IP-Address: IP”，其描述为“IP-Address port”。

共享应用

共享应用是我们不能理解的某种基于HTTP的SOAP应用。仅针对微软来说，基于某些原因，不带端口号的IP地址在第一个ACCEPT信息中发送，Context中也发送同样的IP，但带上了端口号。

Application-GUID

{F1B1920C-6A3C-4ce7-B18C-AFAB305FD03D}

Application-URL

http://www.microsoft.com

Context Context-Data

让对方连接用的IP及端口号。仅观察到过10337端口。

NetMeeting

MS NetMeeting是微软提供的音 频聊天及共享白板程序。NetMeeting使用了H.323及T.120标准，所以（不要管名称）你可以遵照标准使用任意程序，比如GnomeMeeting与ohphone支持H.323。

协议说明中暗示“NetMeeting 3.01”，有不同GUID，但看来没什么不同。

Application-GUID

{44BBA842-CC51-11CF-AAFA-00AA00B6015C}

远程协助

Windows XP允许通过官方客户端请 求远程协助，这个协议被XP的远程协助包所使用，为RDP5.1。

Application-GUID

{56b994a7-380f-410b-9985-c809d78c1bdc}

Application-URL

[http://www.microsoft.com](http://www.microsoft.com/)

Context Context-Data

一个我们 不能解释的长串

音频及视频会话

音频会话及视频会议协商了一个SIP（Session Initiation Protocol）会话。官方客户端使用了内置的SIP程序，任何SIP程序皆可。SIP在RFC 3261中定义。音频被引用为“SIP\_A”，视频被引用为“SIP\_V”。

Application-GUID

{02D3C01F-BF30-4825-A83A-DE7AF41648AA}

INVITE Context-Data

客户端发送INVITE的能力，及对方申请的能力。如音频及视频会话中，应该为“Requested:SIP\_A,SIP\_V,;Capabilities:SIP\_A,SIP\_V,;”。仅音频的话为“Requested:SIP\_A,;Capabilities:SIP\_A,SIP\_V,;”（如果发送端支持视频的话）或者“Requested:SIP\_A,;Capabilities:SIP\_A,;”（如果客户端仅支持音频）。

ACCEPT Context-Data

发送INVITE的客户端被请求的能力，如仅音频会话的话，“Requested:SIP\_A,;”，对于一个音频及视频会话，“Requested:SIP\_A,SIP\_V,;”。

IP-Address port

13455，16253与55039被发现使用过。

摄像头

摄像头支持（清晰视频聊天）使用了RFC1889中定义的“实时协议”。官方的摄像头GUID指定中不支持{括号。

Application-GUID

2A23868E-B45F-401d-B8B0-1E16B774A5B7

白板

    白板是我们不能理解的某种基 于HTTP的SOAP应用。仅针对微软来说，基于某些原 因，不带端口号的IP地址在第一个ACCEPT信息中发送，Context中也发送同样的IP，但带上了端口号。

Application-GUID

{1DF57D09-637A-4ca5-91B9-2C3EDAAF62FE}

Application-URL

[http://www.microsoft.com](http://www.microsoft.com/)

Context Context-Data

IP address and port (10869) for the other computer to connect to.

**文 件传输**

    虽然文件传输不是MSN Messenger协议中的一部 分，但在官方客户端中仍被包含并称为“MSNFTP”协议。它与FTP没有关系，与其他文件传输协议也没有关系。

    若干相似条款被MSNFTP使用着，这些可能会使你更难理解本节。这里的发送者和接收者分别指的是文件的发送方及接收方。服务 器及客户端分别指的是TCP连接的建立方及接收方。一个消息被传递，不要同发送一个消息及发送文件混淆。

在请求过程中，消息客户端将决定谁将成为文件传输的服务器及客户端、谁将成为发送者及接收者，被传 输的文件叫什么及会话的认证Cookie。发送者通常作为服务器，但也可能请求接收者提供服务。

一旦客户端连接服务器，MSNFTP就像NS或SB会话中在两个机器间交换命令行。开始，服务器协商协议，接收者给出它的护照及认证Cookie，发送方将响应文件大小。然 后，发送方将按不定长的二进制块发送文件。接收者可以在任意时间取消传输。

建立连接

    在邀请阶段，计算机提供一到 两个可连接的IP地 址及端口。如果仅有一个的话，服务器就会舰艇那个端口，客户端也应该连接到那个端口。如果有两个的话，服务器将监听两个端口，客户端就应该尝试两个地址及 端口。一旦连接被建立，两个计算机应该停止尝试建立另外一个端口的连接。

二进制数据

本节讨论了二进制数据如何被发送和接收。如果你对二进制已经非常熟了，可以忽略本节。

归根结底，所有计算机的信息都是0、1序列。一个字节是8个0、1的组合，所以一个字节可以有256种（2^8）不同状态。在基于文本的协议中，如MSN Messenger，字节们参照某些标准被解释为字符信息 — 通 常为ASCII。 在一个二进制协议中，字节被解释为其他东西 —　0至255之间的数字，黑白色间的灰度级别，或者 是程序冲突的原因，等等。

最主要的应用是解释为数字，通常为16进制而不是10进制数。为了方便阅读，这里我们使用的是10进制数进行运算。有些程序员习惯用十六进制，因为二进制与十六进制之间转换非常简便。

你应该查看一下编程语言的说明文档，看看是如何处理二进制数据的。许多语言中需要查明描述一个字节 与描述一个字符的方式，不要按一种方式处理字节及字符 — 字符“0”与数值0就不相同。VB中Asc(0)等同于数值0，val(‘0’)等同于ASCII字符0。

      协议 — 正文

协议类似于登录通知服务器的步骤，除了没有事务ID，如果任意一方传输了一个非法命令，对方 就会关闭连接，也不会传输错误信息。

首先，接收者发送VER命令，携带本机所支持的MSNFTP协议的版本号，官方客户端仅支持MSNFTP。发送者应答VER含选定的协议。

然后，接收者传送USR加用户名加认证Cookie，发送者用FIL命令响应并发送文件大小。官方客户端使用邀请阶段使用的大小。

接收者发送TFR命令，表示准备好接收了。发送者就发送剩余会话的二进制数据们。

其后，接收者必须发送BYE与单个数值参数，参数表示文件传输的结果：

2147942405

失败，接收者硬盘空间不足

2164261682

失败，接收者取消传输

2164261683

失败，发送者取消传输

2164261694

失败，连接被阻止

1677987

成功

1677989

成功

作为特例，CCL应该被发送并且不带任何参数，而不是BYE 2164261682。实践中，仅BYE 16777989与CCL被观察到过。

一旦发送者发送完毕，它应该等待接收者传输一个BYE命令，如果发送者一段时间后仍未收到BYE（官方客户端大约为1分钟），它会在会话中传输一个邀请命令“Invitation-Command: CANCEL”，并且“Cancel-Code: FTTIMEOUT”。然后发送者就可以在任意时间关闭连接了。

6.6.5.       协议 — 二进制部分

MSNFTP块由一个头部及一个主体组成。 头部指出了文件是否被完全发送，（如果没有的话）块的主体部分的大小，内容包含了指定大小的字节数。

头部为三个字节长，如果文件没有被完全发送，第一个字节将为0，第二个字节为主体长度 — 长度为第二个 字节值加上第三个字节\*256，所以，如主体中有2045个字节（官方客户端的默认长度），第二个字节为253，第三个字节为7（253+7\*256=2045）。主体部分包含了指定长度的字节数。一旦文件传输完毕，最后一个块中，第一个字节为1，第二个字节与第三个字节为0，并且主体部分为空。

如泥要传输一个13字节长的文件，其中包含“Hello, world!”串，整个过程应该是这样的：

1、产生第一个块

由于有13个字节等待传输，因此，头部第一个字节为0。

由于文件长度小于2045字节，所以仅需要发送一个块，然后计算长度，13除以256为0，余13。所以第二个字节为13，第三个字节为0。

文件中的13个字节将作为块的主体部分。

第一个块应该是这样的：0, 13, 0, 72, 101, 108, 108, 111, 44, 32, 119, 111, 114, 108, 100, 33

2、传输第一个块。

3、检查接收者是否发送了BYE或CCL信息，如果发送了的话，关闭Socket。

4、产生第二个块

由于有0字节剩余，所以为最后一个块

第二个块为：1, 0, 0

5、传输第二个块

6、文件传输完毕。

7、等待约1分钟，看是否接收者是否发送BYE或CCL命令，然后关闭连接。

6.6.6.       会话示例

示例中斜体部分表示二进制数据

**<o> Incoming Connection on Port: 6891**

**<<< VER MYPROTO MSNFTP**

**>>> VER MSNFTP**

**<<< USR myname@msn.com 93301**

**>>> FIL 13**

**<<< TFR**

**>>> *0, 13, 0, 72, 101, 108, 108, 111, 44, 32, 119, 111, 114, 108, 100, 33***

**>>> *1, 0, 0***

**<<< BYE 16777989**

And here is a failed negotiation:

**<o> Incoming Connection on Port: 6891**

**<<< VER MYPROTO**

**<o> Disconnect**

**错 误列表**

Below is a detailed list of every error code ever discovered. Some of the commands have never before been encountered, but exist nonetheless. Each error code has details on every way I have seen them used, but it is quite possible that there are missing situations.

**200's**

**200**

**Invalid syntax**  
*Never before encountered.*

**201**

**Invalid parameter**  
*Sent if the command has a parameter that is considered invalid by the server. Setting your status to* ***FLN*** *would be an example.*  
**>>> CHG 19 FLN 0\r\n**  
**<<< 201 19\r\n**  
*Also sent if you try to* ***ADD*** *an invalid email address.*  
**>>> ADD 20 FL a@b a@b\r\n**  
**<<< 201 20\r\n**

**205**

**Invalid principal**  
*Sent if you try to* ***ADD*** *a nonexistent, but valid, account name.*  
**>>> ADD 21 AL non\_existent\_account@passport.com non\_existent\_account@passport.com\r\n**  
**<<< 205 21\r\n**

**206**

**Domain name missing**  
*Never before encountered.*

**207**

**Already logged in**  
*If the client sends a* ***USR*** *after already logging in, this error will be sent in response.*  
**>>> USR 20 TWN I example@passport.com\r\n**  
**<<< 207 20\r\n**  
**>>> USR 21 TWN S 6b05a0f5b1aa0959e128cfdd513ccf5c\r\n**  
**<<< 207 21\r\n**

**208**

**Invalid principal-name**  
*Sent from the switchboard in reply to a* ***CAL*** *which specifies an invalid account name.*  
**>>> CAL 2 @@a\r\n**  
**<<< 208 2\r\n**

**209**

**Nickname change illegal**  
*Sent in reply to a* ***REA*** *when there is a blocked word/phrase in the new nickname or when the Passport has not yet been confirmed.*  
**>>> REA 18 principal@passport.com look%20msn\r\n**  
**<<< 209 18\r\n**

**210**

**Principal list full**  
*Sent in response to an* ***ADD*** *command if the* ***FL*** *is already full. The principal will not be added. Currently (as of March 23, 2003), the limit is 150 principals, as doubled from a previous 75.*  
**>>> ADD 23 FL principal@passport.com principal@passport.com 0\r\n**  
**<<< 210 23\r\n**

**215**

**Principal already on list**  
*Sent if you try to* ***ADD*** *a principal to a list, but the principal is already in that list.*  
**>>> ADD 26 AL principal@passport.com principal@passport.com\r\n**  
**<<< ADD 26 AL 824 principal@passport.com principal@passport.com\r\n**  
**>>> ADD 27 AL principal@passport.com principal@passport.com\r\n**  
**<<< 215 27\r\n**  
*Also sent if you try to* ***ADD*** *a principal to your FL in a group that the principal is already in.*  
**>>> ADD 28 FL principal@passport.com principal@passport.com 2\r\n**  
**<<< ADD 28 825 FL principal@passport.com principal@passport.com 2\r\n**  
**>>> ADD 29 FL principal@passport.com principal@passport.com 2\r\n**  
**<<< 215 29\r\n**  
*Also sent if you try to invite (****CAL****) a principal into a switchboard session that has already been invited and/or is already present.*  
**>>> CAL 5 example@passport.com\r\n**  
**<<< CAL 5 RINGING 286195\r\n**  
**>>> CAL 6 example@passport.com\r\n**  
**<<< 215 6\r\n**

**216**

**Principal not on list**  
*Sent in reply to* ***REM****s that try to remove principals that are not in the list. Also sent if you try to remove nonexistent or invalid account names because, naturally, they couldn't be in your list.*  
**>>> REM 14 FL principal\_not\_in\_list@msn.com\r\n**  
**<<< 216 14\r\n**  
*This error is also sent in reply to invitations to the switchboard (****CAL****s) to principals that either have you in their* ***BL*** *or have their* ***BLP*** *settings so that you are automatically in their* ***BL****. This is only sent when the principal is on-line, but you're not allowed to know their on-line status.*  
**>>> CAL 2 example@passport.com\r\n**  
**<<< 216 2\r\n**  
*Also sent in reply to* ***REA****s that try to rename principals that are not in any of your lists.*  
**>>> REA 48 random\_principal@randomdomain.com nickname\r\n**  
**<<< 216 48\r\n**

**217**

**Principal not on-line**  
*This error is sent in reply to invitations to the switchboard (****CAL****s) to principals that are currently either offline or appearing offline. This error will also be sent in reply to invitations to nonexistent account names.*  
**>>> CAL 2 myname@msn.com\r\n**  
**<<< 217 2\r\n**  
**>>> CAL 3 nonexistent@passport.com\r\n**  
**<<< 217 3\r\n**

**218**

**Already in mode**  
*Sent in reply to a* ***GTC*** *or a* ***BLP*** *if it tries to change the mode to the mode it is already in. In other words, if the* ***GTC*** *value is already set to A, and the client sends the* ***GTC*** *command setting it to A again, it will receive this error.*  
**>>> GTC 15 A\r\n**  
**<<< GTC 15 150 A\r\n**  
**>>> GTC 16 A\r\n**  
**<<< 218 16\r\n**  
  
**>>> BLP 17 BL\r\n**  
**<<< BLP 17 151 BL\r\n**  
**>>> BLP 18 BL\r\n**  
**<<< 218 18\r\n**

**219**

**Principal is in the opposite list**  
*Send in reply to an* ***ADD*** *that causes the same principal to be in the BL and the AL at the same time. Obviously, that cannot be possible, and the principal will not be added.*  
**>>> ADD 15 AL example@passport.com example@passport.com\r\n**  
**<<< ADD 15 AL 108 example@passport.com Mike\r\n**  
**>>> ADD 16 BL example@passport.com example@passport.com\r\n**  
**<<< 219 16\r\n**

**223**

**Too many groups**  
*Sent if you try to add a group (****ADG****) so that you have more than 30 groups (the maximum). The group with the ID of zero counts toward the limit.*  
**>>> ADG 38 thirtyfirst%20group 0\r\n**  
**<<< 223 38\r\n**

**224**

**Invalid group**  
*Sent if you try to* ***ADD*** *a principal to your FL with a nonexistent group ID. Also sent in reply to* ***REM****s to nonexistent groups. Also sent in reply if you try to remove (****RMG****) or rename (****REG****) a nonexistent group.*  
**>>> RMG 24 15\r\n**  
**<<< RMG 24 12065 15\r\n**  
**>>> ADD 25 FL example@passport.com example@passport.com 15\r\n**  
**<<< 224 25\r\n**  
**>>> REM 26 FL example@passport.com 15\r\n**  
**<<< 224 26\r\n**  
**>>> RMG 27 15\r\n**  
**<<< 224 27\r\n**  
**>>> REG 28 15 New%20Name 0\r\n**  
**<<< 224 28\r\n**

**225**

**Principal not in group**  
*Sent if you try to remove (****REM****) a principal from an existent group that they are not currently in.*  
**>>> REM 27 FL example@passport.com 3\r\n**  
**<<< 224 27\r\n**

**229**

**Group name too long**  
*Sent if you try to add a group (****ADG****) with more than 61 bytes in the name.*  
**>>> ADG 50 this%20group's%20name%20is%20sixty%20two%20bytes%20in%20length 0\r\n**  
**<<< 229 50\r\n**

**230**

**Cannot remove group zero**  
*Sent if you try to remove (****RMG****) the group with the ID of zero.*  
**>>> RMG 28 0\r\n**  
**<<< 230 28\r\n**

**231**

**Invalid group**  
*Never before encountered.*

**280**

**Switchboard failed**  
*Never before encountered.*

**281**

**Transfer to switchboard failed**  
*Never before encountered.*

**300's**

**300**

**Required field missing**  
*Never before encountered.*

**302**

**Not logged in**  
*Never before encountered.*

**500's**

**500**

**Internal server error**  
*When the MSN servers are down, this might be sent in reply to your command to the NS containing your digested password. The official client interprets this as "Service Temporarily Unavailable". This error might also be sent if your account has banned from MSN.*  
**>>> USR 28 TWN S 1938acd78b5524ce56a0ab6a01f3239\r\n**  
**<<< 500 28\r\n**

**501**

**Database server error**  
*Never before encountered.*

**502**

**Command disabled**  
*Sent if you try to use a command associated with an MSN Messenger feature that no longer exists.*  
**>>> FND 3 fname=Bill lname=Gates city=\* state=\* country=US\r\n**  
**<<< 502 3\r\n**

**510**

**File operation failed**  
*Never before encountered.*

**520**

**Memory allocation failed**  
*Never before encountered.*

**540**

**Challenge response failed**  
*Sent in response to a* ***QRY*** *that is invalid. The server will close the connection after sending the error.*  
**<<< CHL 0 15570131571988941333\r\n**  
**>>> QRY 10 msmsgs@msnmsgr.com 32\r\n**  
**4f2f5a91b72102cd28355e9fc9000d6e**  
**<<< 540 10\r\n**

**600's**

**600**

**Server is busy**  
*Never before encountered.*

**601**

**Server is unavailable**  
*Can be sent in reply to the initial* ***USR*** *to the NS if the server is somehow "unavailable".*  
**>>> USR 10 TWN I example@passport.com\r\n**  
**<<< 601 10\r\n**

**602**

**Peer nameserver is down**  
*Never before encountered.*

**603**

**Database connection failed**  
*Never before encountered.*

**604**

**Server is going down**  
*Never before encountered.*

**605**

**Server unavailable**  
*Never before encountered.*

**700's**

**707**

**Could not create connection**  
*Never before encountered.*

**710**

**Bad CVR parameters sent**  
*Sent in reply to a* ***CVR*** *if you send an invalid LCID.*  
**>>> CVR 1 0x0809 winnt 5.1 i386 MSNMSGR 6.0.0602 MSMSGS example@passport.com\r\n**  
**<<< 710 1\r\n**

**711**

**Write is blocking**  
*Never before encountered.*

**712**

**Session is overloaded**  
*Never before encountered.*

**713**

**Calling too rapidly**  
*When the client repeatedly calls someone who is offline or blocking them, this error message will be sent in response to the commands that the server rejects.*  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 216 5\r\n**  
**>>> CAL 5 blocking\_you@passport.com\r\n**  
**<<< 713 5\r\n**

**714**

**Too many sessions**  
*Never before encountered.*

**715**

**Not expected**  
*Sent in response to a* ***PRP*** *setting an invalid phone type of three or less characters.*  
**>>> PRP 30 PHV 555-0690\r\n**  
**<<< 715 30\r\n**  
*Also sent in response to a change of display name (****REA****) on an unverified Passport account.*  
**>>> REA 31 me@passport.com newname\r\n**  
**<<< 715 31\r\n**

**717**

**Bad friend file**  
*Never before encountered.*

**731**

**Not expected**  
*Sent in response to a badly formatted CVR*  
**>>> CVR 2 foo\r\n**  
**<<< 731 2\r\n**  
**<o> Server Closes Connection\r\n**

**800's**

**800**

**Changing too rapidly**  
*When the client tries to change the display name (****REA****) too rapidly, this error message will be sent in response to the commands that the server rejects. This does not affect renaming other principals.*  
**>>> REA 100 me@passport.com NAME\r\n**  
**<<< REA 100 2000 me@passport.com NAME\r\n**  
**>>> REA 101 me@passport.com NAME\r\n**  
**<<< REA 101 2001 me@passport.com NAME\r\n**  
**>>> REA 102 me@passport.com NAME\r\n**  
**<<< REA 102 2002 me@passport.com NAME\r\n**  
**>>> REA 103 me@passport.com NAME\r\n**  
**<<< REA 103 2003 me@passport.com NAME\r\n**  
**>>> REA 104 me@passport.com NAME\r\n**  
**<<< 800 104\r\n**  
*Also when the client tries to change the status (****CHG****) too rapidly.*  
**>>> CHG 105 NLN 0\r\n**  
**<<< CHG 105 NLN 0\r\n**  
**>>> CHG 106 HDN 0\r\n**  
**<<< CHG 106 HDN 0\r\n**  
**>>> CHG 107 NLN 0\r\n**  
**<<< CHG 107 NLN 0\r\n**  
**>>> CHG 108 HDN 0\r\n**  
**<<< CHG 108 HDN 0\r\n**  
**>>> CHG 109 NLN 0\r\n**  
**<<< 800 109\r\n**

**900's**

**910**

**Server too busy**  
*When the MSN servers are busy, this might be sent in reply to your command to the NS containing your digested password..*  
**>>> USR 28 TWN S t=53\*1hAu8ADuD3TEwdXoOMi08sD . . . \r\n**  
**<<< 910 28\r\n**

**911**

**Authentication failed**  
*Sent in response to some invalid formats of the* ***USR*** *command to the DS. Also sent if the account name is invalid.*  
**>>> USR 3 TWN S example@passport.com\r\n**  
**<<< 911 3\r\n**  
  
**>>> USR 4 TWN I passport.com\r\n**  
**<<< 911 4\r\n**  
*Sent in response to an invalid* ***TWN*** *value sent in the second* ***USR*** *command to the NS. Also sent if the account name is invalid or nonexistent.*  
**>>> USR 6 TWN S t=some\_invalid\_value\r\n**  
**<<< 911 6\r\n**  
*Also sent in response to problems authenticating with the switchboard with* ***USR*** *or* ***ANS****.*  
**>>> USR 1 myname\_123@hotmail.com 486979.1047702516.105\r\n**  
**<<< 911 1\r\n**  
**>>> ANS 1 myname\_123@hotmail.com 849102291.520491932 11752098\r\n**  
**<<< 911 1\r\n**

**912**

**Server too busy**  
*Never before encountered.*

**913**

**Not allowed when hiding**  
*Sent in reply to commands that are not allowed in the* ***HDN*** *status which the principal is currently in. The only known command that is prohibited when offline is* ***XFR***  
**>>> XFR 13 SB\r\n**  
**<<< 913 13\r\n**

**914**

**Server unavailable**  
*Never before encountered.*

**915**

**Server unavailable**  
*Never before encountered.*

**916**

**Server unavailable**  
*Never before encountered.*

**917**

**Authentication failed**  
*Never before encountered.*

**918**

**Server too busy**  
*Never before encountered.*

**919**

**Server too busy**  
*Never before encountered.*

**920**

**Not accepting new principals**  
*Never before encountered.*

**921**

**Server too busy**  
*When the MSN servers are busy, this might be sent in reply to your command to the NS containing your digested password..*  
**>>> USR 28 TWN S t=53\*1hAu8ADuD3TEwdXoOMi08sD . . . \r\n**  
**<<< 921 28\r\n**

**922**

**Server too busy**  
*Never before encountered.*

**923**

**Kids Passport without parental consent**  
*Sent in reply to the second* ***USR*** *to the NS if client is logging in with a* [*Kids Passport*](http://kids.passport.com/) *without parental consent to chat online.*  
**>>> USR 29 TWN S t=53\*1hAu8ADuD3TEwdXoOMi08sD . . . \r\n**  
**<<< 923 29\r\n**

**924**

**Passport account not yet verified**  
*Never before encountered.*

**928**

**Bad ticket**  
*Sent in reply to the second* ***USR*** *to the NS if your ticket is invalid. Mostly seen if you don't handle redirections properly with the login server connection and use an @msn or @hotmail account*   
**>>> USR 29 TWN S my\_invalid\_passport\r\n**  
**<<< 928 29\r\n**