[SAMBA协议分析](http://blog.chinaunix.net/uid-28193347-id-3420341.html)

[1 介绍](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604100)

[2 消息](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604101)

[2.1 传输](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604102)

[2.2 消息语法](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604103)

[2.2.1 通用数据类型](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604104)

[2.2.2 定义常数](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604105)

[2.2.3 SMB消息结构](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604106)

[2.2.4 SMB命令](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604107)

[2.2.4.1 SMB\_COM\_CREATE\_DIRECTORY (0x00)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604108)

[2.2.4.2 SMB\_COM\_DELETE\_DIRECTORY (0x01)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604109)

[2.2.4.3 SMB\_COM\_OPEN (0x02)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604110)

[2.2.4.4 SMB\_COM\_CREATE (0x03)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604111)

[2.2.4.5 SMB\_COM\_CLOSE (0x04)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604112)

[2.2.4.6 SMB\_COM\_FLUSH (0x05)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604113)

[2.2.4.7 SMB\_COM\_DELETE (0x06)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604114)

[2.2.4.8 SMB\_COM\_RENAME (0x07)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604115)

[2.2.4.9 SMB\_COM\_QUERY\_INFORMATION (0x08)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604116)

[2.2.4.10 SMB\_COM\_SET\_INFORMATION (0x09)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604117)

[2.2.4.11 SMB\_COM\_READ (0x0A)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604118)

[2.2.4.12 SMB\_COM\_WRITE (0x0B)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604119)

[2.2.4.13 SMB\_COM\_LOCK\_BYTE\_RANGE (0x0C)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604120)

[2.2.4.14 SMB\_COM\_UNLOCK\_BYTE\_RANGE (0x0D)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604121)

[2.2.4.15 SMB\_COM\_CREATE\_TEMPORARY (0x0E)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604122)

[2.2.4.16 SMB\_COM\_CREATE\_NEW (0x0F)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604123)

[2.2.4.17 SMB\_COM\_CHECK\_DIRECTORY (0x10)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604124)

[2.2.4.18 SMB\_COM\_PROCESS\_EXIT (0x11)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604125)

[2.2.4.19 SMB\_COM\_SEEK (0x12)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604126)

[2.2.4.20 SMB\_COM\_LOCK\_AND\_READ (0x13)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604127)

[2.2.4.21 SMB\_COM\_WRITE\_AND\_UNLOCK (0x14)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604128)

[2.2.4.22 SMB\_COM\_READ\_RAW (0x1A)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604129)

[2.2.4.23 SMB\_COM\_READ\_MPX (0x1B)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604130)

[2.2.4.24 SMB\_COM\_READ\_MPX\_SECONDARY (0x1C)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604131)

[2.2.4.25 SMB\_COM\_WRITE\_RAW (0x1D)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604132)

[2.2.4.26 SMB\_COM\_WRITE\_MPX (0x1E)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604133)

[2.2.4.27 SMB\_COM\_WRITE\_MPX\_SECONDARY (0x1F)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604134)

[2.2.4.28 SMB\_COM\_WRITE\_COMPLETE (0x20)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604135)

[2.2.4.29 SMB\_COM\_QUERY\_SERVER (0x21)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604136)

[2.2.4.30 SMB\_COM\_SET\_INFORMATION2 (0x22)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604137)

[2.2.4.31 SMB\_COM\_QUERY\_INFORMATION2 (0x23)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604138)

[2.2.4.32 SMB\_COM\_LOCKING\_ANDX (0x24)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604139)

[2.2.4.33 SMB\_COM\_TRANSACTION (0x25)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604140)

[2.2.4.34 SMB\_COM\_TRANSACTION\_SECONDARY (0x26)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604141)

[2.2.4.35 SMB\_COM\_IOCTL (0x27)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604142)

[2.2.4.36 SMB\_COM\_IOCTL\_SECONDARY (0x28)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604143)

[2.2.4.37 SMB\_COM\_COPY (0x29)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604144)

[2.2.4.38 SMB\_COM\_MOVE (0x2A)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604145)

[2.2.4.39 SMB\_COM\_ECHO (0x2B)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604146)

[2.2.4.40 SMB\_COM\_WRITE\_AND\_CLOSE (0x2C)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604147)

[2.2.4.41 SMB\_COM\_OPEN\_ANDX (0x2D)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604148)

[2.2.4.42 SMB\_COM\_READ\_ANDX (0x2E)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604149)

[2.2.4.43 SMB\_COM\_WRITE\_ANDX (0x2F)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604150)

[2.2.4.44 SMB\_COM\_NEW\_FILE\_SIZE (0x30)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604151)

[2.2.4.45 SMB\_COM\_CLOSE\_AND\_TREE\_DISC (0x31)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604152)

[2.2.4.46 SMB\_COM\_TRANSACTION2 (0x32)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604153)

[2.2.4.47 SMB\_COM\_TRANSACTION2\_SECONDARY (0x33)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604154)

[2.2.4.48 SMB\_COM\_FIND\_CLOSE2 (0x34)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604155)

[2.2.4.49 SMB\_COM\_FIND\_NOTIFY\_CLOSE (0x35)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604156)

[2.2.4.50 SMB\_COM\_TREE\_CONNECT (0x70)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604157)

[2.2.4.51 SMB\_COM\_TREE\_DISCONNECT (0x71)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604158)

[2.2.4.52 SMB\_COM\_NEGOTIATE (0x72)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604159)

[2.2.4.53 SMB\_COM\_SESSION\_SETUP\_ANDX (0x73)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604160)

[2.2.4.54 SMB\_COM\_LOGOFF\_ANDX (0x74)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604161)

[2.2.4.55 SMB\_COM\_TREE\_CONNECT\_ANDX (0x75)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604162)

[2.2.4.56 SMB\_COM\_SECURITY\_PACKAGE\_ANDX (0x7E)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604163)

[2.2.4.57 SMB\_COM\_QUERY\_INFORMATION\_DISK (0x80)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604164)

[2.2.4.58 SMB\_COM\_SEARCH (0x81)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604165)

[2.2.4.59 SMB\_COM\_FIND (0x82)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604166)

[2.2.4.60 SMB\_COM\_FIND\_UNIQUE (0x83)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604167)

[2.2.4.61 SMB\_COM\_FIND\_CLOSE (0x84)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604168)

[2.2.4.62 SMB\_COM\_NT\_TRANSACT (0xA0)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604169)

[2.2.4.63 SMB\_COM\_NT\_TRANSACT\_SECONDARY (0xA1)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604170)

[2.2.4.64 SMB\_COM\_NT\_CREATE\_ANDX (0xA2)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604171)

[2.2.4.65 SMB\_COM\_NT\_CANCEL (0xA4)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604172)

[2.2.4.66 SMB\_COM\_NT\_RENAME (0xA5)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604173)

[2.2.4.67 SMB\_COM\_OPEN\_PRINT\_FILE (0xC0)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604174)

[2.2.4.68 SMB\_COM\_WRITE\_PRINT\_FILE (0xC1)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604175)

[2.2.4.69 SMB\_COM\_CLOSE\_PRINT\_FILE (0xC2)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604176)

[2.2.4.70 SMB\_COM\_GET\_PRINT\_QUEUE (0xC3)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604177)

[2.2.4.71 SMB\_COM\_READ\_BULK (0xD8)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604178)

[2.2.4.72 SMB\_COM\_WRITE\_BULK (0xD9)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604179)

[2.2.4.73 SMB\_COM\_WRITE\_BULK\_DATA (0xDA)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604180)

[2.2.4.74 SMB\_COM\_INVALID (0xFE)](http://blog.chinaunix.net/uid-28193347-id-3420341.html#_Toc306604181)

2.2.4.75 SMB\_COM\_NO\_ANDX\_COMMAND (0xFF)

1 介绍 2 消息 2.1 传输 2.2 消息语法 2.2.1 通用数据类型 2.2.2 定义常数 2.2.3 SMB消息结构 2.2.4 SMB命令 2.2.4.1 SMB\_COM\_CREATE\_DIRECTORY (0x00)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用TRANS2\_CREATE\_DIRECTORY替代。

创建目录命令用来在连接的共享服务器上建立一个新的目录。客户端必须提供一个有效的UID和TID，以及需要创建的目录的名称(相对于TID)。

为了新建一个目录，服务器要求客户端至少提供子目录的创建权限。创建者对新建目录的存取权限有服务器的本地策略决定。

2.2.4.2 SMB\_COM\_DELETE\_DIRECTORY (0x01)

这是原始核心协议的一个命令，用来删除一个空的目录。

2.2.4.3 SMB\_COM\_OPEN (0x02)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用SMB\_COM\_NT\_CREATE\_ANDX替代。

此命令用来打开一个已存在的常规文件，不能用来打开目录文件或命名管道文件。命令携带了客户端想要打开的文件的路径名称。如果命令执行成功，服务器的响应报文中必须携带此文件的标识符FID，客户端在后续的对此文件的操作命令中也必须携带相同的FID。

2.2.4.4 SMB\_COM\_CREATE (0x03)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用SMB\_COM\_NT\_CREATE\_ANDX替代。

此命令用来创建并打开一个新文件，或打开一个已存在的文件并将其内容清空。返回的FID在后续对此文件的操作命令中使用，比如读、写、锁、解锁和关闭。这个命令不能被用来创建目录或命名管道。命令请求中携带了需要创建的文件名及其路径。如果命令执行成功，服务器的响应命令中必须携带FID，客户端在后续对此文件的操作命令中也必须携带相同的FID。客户端必须拥有对文件父目录的写权限，才能在其中新建文件；或对文件本身具有写权限，才能清空文件内容。客户端对新建的文件的访问权限必须是读和写。如果文件原来已存在，只是打开后清空其内容，原来的访问权限保持不变。文件以读/写/兼容模式打开。

2.2.4.5 SMB\_COM\_CLOSE (0x04)

这是原始核心协议的一个命令，用来关闭和一个有效的FID关联的对象的一个实例。

2.2.4.6 SMB\_COM\_FLUSH (0x05)

这是原始核心协议的一个命令，用来要求服务器将当前文件的所有数据和信息都写回到存储器上。

2.2.4.7 SMB\_COM\_DELETE (0x06)

这是原始核心协议的一个命令，用来删除一个或多个常规文件。支持文件名中有通配符，允许一次删除多个文件。

2.2.4.8 SMB\_COM\_RENAME (0x07)

这是原始核心协议的一个命令，用来重命名一个或多个文件或目录。允许文件名中有通配符，允许一次修改多个文件的文件名。

2.2.4.9 SMB\_COM\_QUERY\_INFORMATION (0x08)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用SMB\_COM\_TRANSACTION2的子命令TRANS2\_QUERY\_PATH\_INFORMATION来替代。

客户端可以用这个命令来获取服务器上某个文件的属性信息，前提是提供文件名和路径，不需要提供FID。

2.2.4.10 SMB\_COM\_SET\_INFORMATION (0x09)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用SMB\_COM\_TRANSACTION2的子命令TRANS2\_SET\_PATH\_INFORMATION来替代。

客户端可以用这个命令来改变一个常规文件或目录的属性。文件名不可以包含通配符，必须使用全名，所有的参数都是可选的。如果服务器不识别某个参数，必须忽略它。如果LastWriteTime字段包含0x00000000，文件的LastWriteTime必须不能改变。

2.2.4.11 SMB\_COM\_READ (0x0A)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用SMB\_COM\_READ\_ANDX命令来替代。

此命令用来从一个普通文件中读取数据。如果客户端和服务器协商可以支持命名管道或直接读取设备，也可以从其中读取数据。如果服务器返回的字节数比客户端要求的少，表示已经读到文件末尾。如果读取请求的起始地址在或超过了文件尾部，返回0字节。如果要求读取的字节数超过了SMB连接规定的最大字节数**MaxBufferSize**，服务器必须终止此连接，因为只能支持最大32-bit位移的客户请求，不适合拥有超过32-bit大小的文件。客户端最少要拥有文件的读权限。

2.2.4.12 SMB\_COM\_WRITE (0x0B)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用SMB\_COM\_WRITE\_ANDX命令来替代。在**LAN Manager 1.0** 中，引入了对命名管道和I/O设备的支持。

此命令用来向普通文件中写入数据。如果客户端和服务器协商支持命名管道、邮箱或直接读取设备，这个命令也可向这些设备中写入数据。命令也可以用来截断或延长文件到某一指定位置。请求命令中必须包含合法的TID和FID。这个命令最大支持32-bit长度的文件，不适合更大的文件，如果要对大文件进行操作，需要使用命令SMB\_COM\_WRITE\_ANDX。

当FID指示操作的文件是一个硬盘文件，而指定的写入起始偏移量(WriteOffsetInBytes)超过了当前文件的结尾时，文件必须被扩充，文件原来尾部到要求的偏移量之间数据都初始化为0x00。如果指定写入的数据长度(CountOfBytesToWrite)为0x0000，文件将被截断(或扩充)到偏移量的位置。

客户端必须最少要拥有文件的写权限。

2.2.4.13 SMB\_COM\_LOCK\_BYTE\_RANGE (0x0C)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用SMB\_COM\_LOCKING\_ANDX命令来替代。

此命令不适用于长度超过32-bit的文件。在**LAN Manager 1.0**引入的命令SMB\_COM\_LOCKING\_ANDX支持长度超过32-bit的文件，最大支持64-bit长度。SMB\_COM\_LOCKING\_ANDX是**LAN Manager 1.0版本以后的客户端进行锁/解锁一段数据的首选。如果客户端需要支持64-bit长度的文件，必须使用NT LAN Manage或以后的版本。**

此命令用来锁定一个打开的普通文件中一段连续的数据。支持锁定任一指定文件中任意多的数据段，前提是这些数据段没有重叠的部分。锁定可以防止其他客户或PID对锁定的数据段进行锁定、读和写操作。如果锁定的数据段之间有重叠的部分，必须返回失败，错误码为STATUS\_LOCK\_NOT\_GRANTED (ERRDOS/ERRlock)。锁定的范围可以超出文件大小，但是不会引起文件大小的扩充。只有加锁的进程才可以对其进行解锁。

因为此请求只支持最大32-bit的offset，所以对于大于32-bit的文件不适用。客户端必须至少有文件的读权限。

2.2.4.14 SMB\_COM\_UNLOCK\_BYTE\_RANGE (0x0D)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用SMB\_COM\_LOCKING\_ANDX命令来替代。

此命令不适用于长度超过32-bit的文件。在**LAN Manager 1.0**引入的命令SMB\_COM\_LOCKING\_ANDX支持长度超过32-bit的文件，最大支持64-bit长度。SMB\_COM\_LOCKING\_ANDX是**LAN Manager 1.0版本以后的客户端进行锁/解锁一段数据的首选。如果客户端需要支持64-bit长度的文件，必须使用NT LAN Manage或以后的版本。**

此命令用来解锁一个打开的普通文件中一段连续的数据。指定的数据段范围必须和先前加锁的范围完全一致，并且是由同一CIFS客户端和进程所加的锁，FID和PID也必须一致。对未加锁的数据进行解锁将被作为一个错误操作。

如果服务器没有立即（200-300毫秒内）同意对指定数据段范围进行解锁，必须返回一个错误给客户端。此命令只支持最大32-bit的文件，不适用大于32-bit的文件。客户端必须最少拥有文件的读权限。

2.2.4.15 SMB\_COM\_CREATE\_TEMPORARY (0x0E)

这是原始核心协议的一个命令，已被废弃。

客户端使用此命令来创建一个临时文件。消息包含希望创建文件所在的路径。服务器会在指定的目录中为文件生成一个唯一的文件名。指定的目录必须和SMB头部的TID相关联。客户端必须拥有指定路径的写权限。如果执行成功，服务器返回一个FID，在后续路程中如果还要对此文件进行操作，客户端必须提供这个FID。文件以读写兼容模式打开。在客户端关闭文件后服务器不会自动删除它，如果不再使用，客户端必须下命令给服务器删除此文件。

2.2.4.16 SMB\_COM\_CREATE\_NEW (0x0F)

这是原始核心协议的一个命令，不推荐使用。客户程序应该使用SMB\_COM\_NT\_CREATE\_ANDX命令来替代。

此命令用来创建一个新文件。不能截断或覆盖一个已存在的文件，如果请求的文件已经存在，返回失败。此命令不能用来创建目录或命名管道。

请求消息中包含了路径名（原句：The request message includes the pathname of the file relative to the supplied TID that the client requests to create.），如果执行成功，服务器返回一个FID，在后续的read、write、lock、unlock和close操作中，客户端必须提供相同的FID。客户端必须有文件所在目录的写权限，对新建的文件拥有读写权限。文件以读写兼容模式打开。服务器对客户端提供的创建时间**CreationTime**(见2.2.4.16.1)**的支持是可选的。**

2.2.4.17 SMB\_COM\_CHECK\_DIRECTORY (0x10)

这是原始核心协议的一个命令。

此命令用来检查指定的路径是否在服务器上存在。

2.2.4.18 SMB\_COM\_PROCESS\_EXIT (0x11)

这是原始核心协议的一个命令，在**LAN Manager 1.0中声明已被废弃，但是在后续的文档中又被包含。[MS-CIFS]将其列为已废弃。**

**此命令请求由客户端发起，通知客户端程序已崩溃。收到请求后，服务器关闭消息头部PID进程的所有资源。**

2.2.4.19 SMB\_COM\_SEEK (0x12)

这是原始核心协议的一个命令，已被废弃。

此命令用来设置一个常规文件的文件指针，也可以用来查询当前文件指针的位置，文件指针的位置由服务器管理。文件指针在响应报文中以unsigned 32-bit的格式返回，表明从文件头开始的偏移量。可以设置超过文件大小的偏移量，但是如果设置一个负数的偏移量，将会被重置为0，即文件的起始位置。

在读或写文件之前没有必要使用SMB\_COM\_SEEK来设置文件指针，IFS在读或写的请求命令中已包含了偏移量字段，读或写操作时也会改变文件指针，指针会从要求的offset位置向后移动，读或写多少字节，就向后移动多少。

正是因为读或写之前不必使用Since SMB\_COM\_SEEK，这个命令的作用就非常有限了。你可以用它来获取当前文件指针，或者通过获取文件末尾offset的形式来获得文件大小，但是不适用于非常大的文件（比如接近或大于4G的文件）。

2.2.4.20 SMB\_COM\_LOCK\_AND\_READ (0x13)

此命令在CorePlus中引入，但是经常作为LAN Manager 1.0的一部分。此命令已废弃。客户端应该使用SMB\_COM\_LOCKING\_ANDX来替代。

此命令用来锁定并读取一段常规文件中的数据。数据段首先被锁定，然后被读取。锁类型是排他性的读/写锁。如果服务器不能立即锁定数据段，要返回给客户端错误。如果没有获取到锁，服务器不应该再去读数据。

如果服务器返回的数据比请求的少，说明文件已经到末尾了。如果文件从文件末尾或者超过文件末尾的位置读取，将会返回0字节。如果请求的字节数超过SMB连接中标记的**MaxBufferSize大小，服务器会中断此连接。此命令只适用于文件大小小于32-bit的情况。客户端必须最少拥有文件的读权限。**

2.2.4.21 SMB\_COM\_WRITE\_AND\_UNLOCK (0x14)

此命令在CorePlus中引入，但是经常作为LAN Manager 1.0的一部分。此命令已废弃。客户端应该使用SMB\_COM\_LOCKING\_ANDX来替代。

此命令用来向文件中写入一段数据并解锁数据。通常用在SMB\_COM\_LOCK\_AND\_READ之后，作用在同一文件的同一数据段。服务器的响应消息中用**ByteCountWritten来指示实际写入的字节数。**

**除了不能处理0字节长度的写操作外，此命令和**SMB\_COM\_UNLOCK+ SMB\_COM\_WRITE命令组合具有相同的作用。对此命令的支持是可选的，如果支持，服务器应该在SMB\_COM\_NEGOTIATE 命令的响应消息中，将SMB Header的Flag字段的bit 0设为1。如果消息长度超过了TID指定的**MaxBufferSize（原句：If the command sends a message of length greater than the MaxBufferSize for the TID specified），服务器可以中断此连接。如果写数据过程中发生了错误，数据保持锁状态。**

**此命令只支持最大32-bit大小的文件，如果需要支持64-bit大小的文件，客户端应该使用SMB\_COM\_WRITE\_ANDX命令。**

如果FID指示此文件是一个磁盘文件并且写入数据的范围超过了文件大小，文件会被扩充。文件末尾到指定的offset之间填充0x00。如果要求写入的字节数为0，不论指定offset是多少，文件大小都不会改变，既不会截断也不会扩充。

客户端必须最少拥有文件的写权限

2.2.4.22 SMB\_COM\_READ\_RAW (0x1A)

此命令在CorePlus中引入，但是经常作为LAN Manager 1.0的一部分。此命令已废弃。客户端应该使用SMB\_COM\_READ\_ANDX来替代。

如果服务器支持此命令，会在SMB\_COM\_NEGOTIATE命令的响应消息中设置CAP\_RAW\_MODE capabilities bit。

2.2.4.23 SMB\_COM\_READ\_MPX (0x1B)

此命令在LAN Manager 1.0中引入，已被废弃，在NT LAN Manager中被重新设计。在此文档中只介绍其在NT LAN Manager中的行为。详情请见2.1.2.1

这是一个专门用于读取普通文件中大块数据的命令，使性能最大化，允许客户端和服务器之间的其他操作同时进行。只有使用multiplexed session (见2.1.3)时才有效。服务器在响应此命令请求时，会发几个响应消息，直到请求的数据全部传送完毕，或中间发生错误。每个响应消息中必须包含TID、UID、PID、MID、客户端请求的CID、返回数据的offset和长度。

当客户端收到响应中的DataLength之和等于希望获取的字节数时(最小长度的数据段已收到)，说明所有请求的数据都已传送完毕。这种机制下，即使响应报文没有按顺序返回协议也可以正常工作。

一个事实是，如果请求的数据超出了磁盘文件的范围，返回数据的总数可能小于请求的读取的字节数。在这种情况下，只返回存在的字节。如果一个读取请求的数据段范围完全超出了文件，响应消息中Count要置为0x0000.如果返回的字节数小于请求的字节数，表明已经读到了文件的末尾（如果读取的不是标准块磁盘文件，只返回0字节来表明已到文件末尾）。

一旦开始读取，需要一直执行完毕。客户端期望收到所有客户端的响应数据报。在命令执行期间，客户端不能发送会引起冲突的命令（比如关闭文件命令）。

此命令只支持32-bit长度的文件。服务器可以支持此命令。如果服务器支持此命令，需要在SMB协议的传输协商响应中将Capabilities域置为CAP\_MPX\_MODE (0x00000002)。

2.2.4.24 SMB\_COM\_READ\_MPX\_SECONDARY (0x1C)

此命令在LAN Manager 1.0中引入，在NT LAN Manager中被废弃。

此命令不在被用来和SMB\_COM\_READ\_MPX结合使用。客户端不应该再发送此命令。服务器如果收到了这个命令，应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOS/ERRbadfunc)。

2.2.4.25 SMB\_COM\_WRITE\_RAW (0x1D)

此命令在CorePlus中引入，但是经常作为LAN Manager 1.0的一部分。此命令已废弃。客户端应该使用SMB\_COM\_WRITE\_ANDX来替代。

服务器对此命令的支持是可选的。如果支持，需要在协议协商过程中将CAP\_RAW\_MODE相应bit置位。

这是一个专门用于向打开的普通文件、命名管道、设备或后台中写入大量数据的命令。此命令允许客户通过SMB传输大量的未格式化的数据（原始字节），而不用普通的SMB请求格式。也允许客户端发送超过session启动时规定最大buffer大小的消息。

服务器必须可以接收最多65535字节的原始数据。也必须允许客户端的SMB\_COM\_WRITE\_RAW请求中包含一个非格式化的消息。客户端可能会使用此命令发送要写入数据的一部分。

2.2.4.26 SMB\_COM\_WRITE\_MPX (0x1E)

此命令在LAN Manager 1.0中引入，已被废弃，在NT LAN Manager中被重新设计。在此文档中只介绍其在NT LAN Manager中的行为。详情请见2.1.2.1

此命令用于客户端向服务器写入大量数据，使性能最大化。只有使用multiplexed session (见2.1.3)时才有效。在一个命令交互中，所有请求和响应消息中的TID、UID、PID、MID、CID必须相同。

此命令只支持最大32-bit的文件。服务器对此命令的支持是可选的。如果服务器支持，必须在SMB协议协商时设置将Capabilities字段的CAP\_MPX\_MODE bit置位。

2.2.4.27 SMB\_COM\_WRITE\_MPX\_SECONDARY (0x1F)

此命令在LAN Manager 1.0中引入，在NT LAN Manager中被废弃。

此命令不在被用来和SMB\_COM\_WRITE\_MPX结合使用。客户端不应该再发送此命令。服务器如果收到了这个命令，应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOS/ERRbadfunc)。

2.2.4.28 SMB\_COM\_WRITE\_COMPLETE (0x20)

此命令在LAN Manager 1.0中引入，已被废弃。此命令由服务器在SMB\_COM\_WRITE\_RAW的最后一个响应消息中发出。

2.2.4.29 SMB\_COM\_QUERY\_SERVER (0x21)

此命令在NT LAN Manager中引入，但是还没有实现。

客户端不应该发送此命令，服务器收到此命令后应当返回STATUS\_NOT\_IMPLEMENTED (ERRDOS/ERRbadfunc)。

2.2.4.30 SMB\_COM\_SET\_INFORMATION2 (0x22)

此命令在LAN Manager 1.0中引入，已被废弃。新的客户端应当使用SMB\_COM\_TRANSACTION2的子命令TRANS2\_SET\_FILE\_INFORMATION来替代。

此命令可以被客户端用来设置服务器上一个打开文件的属性。客户端要在SMB头部提供一个有效的FID。这个FID由前面成功打开文件的命令获得。客户端必须最少拥有文件的写权限。目标文件的属性将按照请求更新。如果请求中的date或time为0，表明服务器不要修改文件的这两个属性。和SMB\_COM\_SET\_INFORMATION（2.2.4.10）相比，此命令允许客户端设置更多的文件属性。

2.2.4.31 SMB\_COM\_QUERY\_INFORMATION2 (0x23)

此命令在LAN Manager 1.0中引入，已被废弃。新的客户端应当使用SMB\_COM\_TRANSACTION2的子命令TRANS2\_QUERY\_FILE\_INFORMATION来替代。

此命令可以被客户端用来获取服务器上一个打开文件的属性。客户端在请求消息中必须提供合法的FID。这个FID由前面成功打开文件的命令获得。和SMB\_COM\_QUERY\_INFORMATION相比，此命令允许客户端获取更多的文件属性。服务器只能提供最大32-bit的文件的属性。

2.2.4.32 SMB\_COM\_LOCKING\_ANDX (0x24)

此命令在LAN Manager 1.0中引入，不适用大于32-bit的文件。支持最大64-bit的实现在NT LAN Manager中引入。

此命令用来锁定一个普通文件中一段连续的数据。支持锁定任一指定文件中任意多的数据段，前提是这些数据段没有重叠的部分。锁定可以防止其他进程使用一个独立的文件句柄(FID)对文件锁定部分进行锁、读和写操作。任何进程使用获取锁的文件的FID都可以访问被锁定的数据（原句：Locks prevent attempts to lock, read, or write the locked portion of the file by other processes using a separate file handle (FID). Any process using the same [FID](http://msdn.microsoft.com/en-us/library/6498785a-3c55-4e75-adf9-f8925d282820%28PROT.13%29#fid) specified in the request that obtained the lock has access to the locked bytes.）

此命令也可以被服务器用来发送一个OpLock中断通知消息给客户端，客户端收到后发送确认消息。这是CIFS协议中服务器发送请求消息的一个例子。

下面列举的是SMB\_COM\_LOCKING\_ANDX后可能发送的命令

SMB\_COM\_CLOSE (section 2.2.4.5 )

SMB\_COM\_FLUSH (section 2.2.4.6 )

SMB\_COM\_LOCKING\_ANDX

SMB\_COM\_READ (section 2.2.4.11 )

SMB\_COM\_READ\_ANDX (section 2.2.4.42 )

SMB\_COM\_WRITE (section 2.2.4.12 )

SMB\_COM\_WRITE\_ANDX (section 2.2.4.43 )

2.2.4.33 SMB\_COM\_TRANSACTION (0x25)

此命令在LAN Manager 1.0中引入。

此命令为事务处理协议的传输子协议服务。这些命令可以用于CIFS文件系统内部通信的邮箱和命名管道。如果出书的数据超过了会话建立时规定的MaxBufferSize，必须使用SMB\_COM\_TRANSACTION\_SECONDARY命令来传输超出的部分：SMB\_Data.Trans\_Data 和 SMB\_Data.Trans\_Parameter。这两部分在初始化消息中没有固定。

如果客户端没有发送完所有的**SMB\_Data.Trans\_Data，会将DataCount设置为小于TotalDataCount的一个值。同样的，如果SMB\_Data.Trans\_Parameters没有发送完，会设置ParameterCount为一个小于TotalParameterCount的值。参数部分优先级高于数据部分，客户端在每个消息中应该尽量多的发送数据。服务器应该可以接收无序到达的SMB\_Data.Trans\_Parameters** 和 **SMB\_Data.Trans\_Data，不论是大量还是少量的数据。**

**在请求和响应消息中，SMB\_Data.Trans\_Parameters和SMB\_Data.Trans\_Data的位置和长度都是由SMB\_Parameters.ParameterOffset、SMB\_Parameters.ParameterCount, SMB\_Parameters.DataOffset和SMB\_Parameters.DataCount决定。另外需要说明的是，SMB\_Parameters.ParameterDisplacement和SMB\_Parameters.DataDisplacement可以用来改变发送数据段的序号。服务器应该优先发送SMB\_Data.Trans\_Parameters。客户端应该准备好组装收到的SMB\_Data.Trans\_Parameters和SMB\_Data.Trans\_Data，即使它们是乱序到达的。**

2.2.4.34 SMB\_COM\_TRANSACTION\_SECONDARY (0x26)

此命令在LAN Manager 1.0中引入。

此命令用来完成SMB\_COM\_TRANSACTION中未传输完毕数据的传输。

**在请求和响应消息中，SMB\_Data.Trans\_Parameters和SMB\_Data.Trans\_Data的位置和长度都是由SMB\_Parameters.ParameterOffset、SMB\_Parameters.ParameterCount, SMB\_Parameters.DataOffset和SMB\_Parameters.DataCount决定。另外需要说明的是，SMB\_Parameters.ParameterDisplacement和SMB\_Parameters.DataDisplacement可以用来改变发送数据段的序号。服务器应该优先发送SMB\_Data.Trans\_Parameters。客户端应该准备好组装收到的SMB\_Data.Trans\_Parameters和SMB\_Data.Trans\_Data，即使它们是乱序到达的。**

2.2.4.35 SMB\_COM\_IOCTL (0x27)

此命令在LAN Manager 1.0中引入，在NT LAN Manager中被废弃。NT LAN Manager

同时去掉了多路请求和响应消息的传输行为的支持（原句：NT LAN Manager also removed the transaction-like behavior that supported multiple request and response messages to complete an IOCTL）。此命令现在支持一个信号请求及其后的信号响应。

此命令发送一个设备或文件的IOCTL请求到服务器，然后返回IOCTL的响应给客户端。目标设备或文件由FID区分。请求消息要求指定的设备执行指定的功能。此功能并不是由SMB协议提供，而是由CIFS运行所在的系统提供。协议只是简单的传送请求和响应。

2.2.4.36 SMB\_COM\_IOCTL\_SECONDARY (0x28)

此命令在LAN Manager 1.0中引入，在NT LAN Manager中被废弃，经过考虑后保留但不实现。客户端不应该使用这个命令，服务器收到此命令后要返回STATUS\_NOT\_IMPLEMENTED (ERRDOS/ERRbadfunc)。

这个命令是与SMB\_COM\_IOCTL配合的，但是SMB\_COM\_IOCTL也已被废弃。

2.2.4.37 SMB\_COM\_COPY (0x29)

此命令在LAN Manager 1.0中引入，在NT LAN Manager中被废弃。

此命令用来执行服务器侧的文件拷贝，现在已不使用。客户端不应该使用这个命令，服务器收到此命令后要返回STATUS\_NOT\_IMPLEMENTED (ERRDOS/ERRbadfunc)。

2.2.4.38 SMB\_COM\_MOVE (0x2A)

此命令在LAN Manager 1.0中引入，在NT LAN Manager中被废弃。

此命令用来移动服务器上的文件，现在已不使用。客户端不应该使用这个命令，服务器收到此命令后要返回STATUS\_NOT\_IMPLEMENTED (ERRDOS/ERRbadfunc)。

2.2.4.39 SMB\_COM\_ECHO (0x2B)

此命令在LAN Manager 1.0中引入。

客户端发送此命令测试和服务器的传输层连接。

2.2.4.40 SMB\_COM\_WRITE\_AND\_CLOSE (0x2C)

此命令在LAN Manager 1.0中引入，已被废弃。客户端应该使用SMB\_COM\_WRITE\_ANDX命令替代。

此命令用来向指定的FID的文件写入一段数据并关闭文件。和SMB\_COM\_WRITE+ SMB\_COM\_CLOSE组合具有相同的功能。详细情况请查看SMB\_COM\_WRITE和SMB\_COM\_CLOSE命令。命令支持两种请求格式：一种6个参数，另一种12个参数。

此命令只支持最大32-bit大小的文件，客户端应该使用SMB\_COM\_WRITE\_ANDX以支持最大64-bit大小的文件。

客户端至少要拥有文件的写权限。如果在写文件到磁盘过程中出错，服务器应该关闭文件。

2.2.4.41 SMB\_COM\_OPEN\_ANDX (0x2D)

此命令在LAN Manager 1.0中引入。

此命令用来创建并打开一个文件，或者打开一个已存在的普通文件，并执行命令链中的命令。命令链详情见3.2.4.1.1，命令中包含客户端要打开的文件名，命名管道或设备。如果执行成功，服务器响应消息中要携带一个合法的FID。客户端在后续对此文件的操作请求中要提供相同的FID。

下面这些命令是可以放在SMB\_COM\_OPEN\_ANDX命令的AndX链中：

SMB\_COM\_READ (section 2.2.4.11)

SMB\_COM\_READ\_ANDX (section 2.2.4.42 )

SMB\_COM\_IOCTL (section 2.2.4.35 )

SMB\_COM\_NO\_ANDX\_COMMAND (section 2.2.4.75 )

2.2.4.42 SMB\_COM\_READ\_ANDX (0x2E)

此命令在LAN Manager 1.0中引入，在NT LAN Manager中对其进行了扩展。

此命令用来读取数据，可以读取普通文件，命名管道，或直接访问设别，比如串口(COM)或打印机接口(LPT)。如果客户端用NT LAN Manager或以后的版本协商，应该发送带有12个参数的请求，这个版本支持最大64-bit的文件。此命令是唯一一个支持读取64-bit大小文件的读取命令。

下面这些命令是可以放在SMB\_COM\_READ\_ANDX命令的AndX链中：

SMB\_COM\_CLOSE (section 2.2.4.5 )

2.2.4.43 SMB\_COM\_WRITE\_ANDX (0x2F)

此命令在LAN Manager 1.0中引入。

此命令用来向普通文件，命名管道，或直接访问设别，比如串口(COM)或打印机接口(LPT)中写入数据。如果客户端用NT LAN Manager或以后的版本协商，应该发送带有14个参数的请求，这个版本支持最大64-bit的文件。此命令是唯一一个支持写64-bit大小文件的读取命令。

下面这些命令是可以放在SMB\_COM\_WRITE\_ANDX命令的AndX链中：

SMB\_COM\_READ (section 2.2.4.11 )

SMB\_COM\_READ\_ANDX (section 2.2.4.42 )

SMB\_COM\_LOCK\_AND\_READ (section 2.2.4.20 )

SMB\_COM\_CLOSE (section 2.2.4.5 )

2.2.4.44 SMB\_COM\_NEW\_FILE\_SIZE (0x30)

此命令保留但是没有实现，也没有定义。它在[SNIA]中被列出，但是并没有被定义，在其他参考资料中也没有出现过。

客户端不应该发送此命令，服务器收到此命令后应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOC/ERRbadfunc)。

2.2.4.45 SMB\_COM\_CLOSE\_AND\_TREE\_DISC (0x31)

此命令在NT LAN Manager中引入，但是被保留没有实现。

客户端不应该发送此命令，服务器收到此命令后应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOC/ERRbadfunc)。

2.2.4.46 SMB\_COM\_TRANSACTION2 (0x32)

此命令在LAN Manager 1.2中引入。

此子命令支持服务器文件系统更丰富的语义集。允许客户端设置和获取扩展的key/value属性对，支持长文件名(比原始的8.3名字格式要长)，可以执行目录搜索及其他任务。

如果客户端没有发送完所有的**SMB\_Data.Trans\_Data，会将DataCount设置为小于TotalDataCount的一个值。同样的，如果SMB\_Data.Trans\_Parameters没有发送完，会设置ParameterCount为一个小于TotalParameterCount的值。参数部分优先级高于数据部分，客户端在每个消息中应该尽量多的发送数据。服务器应该可以接收无序到达的SMB\_Data.Trans\_Parameters** 和 **SMB\_Data.Trans\_Data，不论是大量还是少量的数据。**

**在请求和响应消息中，SMB\_Data.Trans2\_Parameters和SMB\_Data.Trans2\_Data的位置和长度都是由SMB\_Parameters.ParameterOffset、SMB\_Parameters.ParameterCount, SMB\_Parameters.DataOffset和SMB\_Parameters.DataCount决定。另外需要说明的是，SMB\_Parameters.ParameterDisplacement和SMB\_Parameters.DataDisplacement可以用来改变发送数据段的序号。服务器应该优先发送SMB\_Data.Trans2\_Parameters。客户端应该准备好组装收到的SMB\_Data.Trans2\_Parameters和SMB\_Data.Trans2\_Data，即使它们是乱序到达的。**

2.2.4.47 SMB\_COM\_TRANSACTION2\_SECONDARY (0x33)

此命令在LAN Manager 1.2中引入。

此命令用来完成SMB\_COM\_TRANSACTION2中未传完的数据。

2.2.4.48 SMB\_COM\_FIND\_CLOSE2 (0x34)

此命令在LAN Manager 1.2中引入。

此命令用来关闭由命令TRANS2\_FIND\_FIRST2而打开的搜索句柄，服务器释放所有和此句柄相关的资源。

2.2.4.49 SMB\_COM\_FIND\_NOTIFY\_CLOSE (0x35)

此命令在LAN Manager 1.2中引入，被保留而没有使用。

此命令用来关闭由命令TRANS2\_FIND\_NOTIFY\_FIRST打开的目录搜索句柄。命令TRANS2\_FIND\_NOTIFY\_FIRST和TRANS2\_FIND\_NOTIFY\_NEXT同样没有使用。

客户端不应该发送此命令，服务器收到此命令后应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOC/ERRbadfunc)。

2.2.4.50 SMB\_COM\_TREE\_CONNECT (0x70)

这是一个原始核心协议命令，已被废弃，客户端应该使用SMB\_COM\_TREE\_CONNECT\_ANDX来替代。

此命令用来建立一条客户端和服务器之间的连接，共享资源依靠共享名确定。连接建立后，此连接将用服务器返回的TID作为识别标记。

2.2.4.51 SMB\_COM\_TREE\_DISCONNECT (0x71)

这是一个原始核心协议命令。

此命令用来关闭客户端访问服务器资源时使用的一条逻辑连接，连接依靠SMB头部的TID识别，断开后服务器将此TID视为无效的TID。所有和此TID相关的文件、目录及其他资源都被释放，文件和目录的锁也会被释放。

2.2.4.52 SMB\_COM\_NEGOTIATE (0x72)

这是一个原始核心协议命令。

此命令用来初始化服务器和客户端之间的SMB会话，必须在其他任何SMB命令发送之前完成。

每个SMB会话只能有一次协商过程，后续的SMB\_COM\_NEGOTIATE会被服务器拒绝并返回一个错误响应。

2.2.4.53 SMB\_COM\_SESSION\_SETUP\_ANDX (0x73)

此命令在LAN Manager 1.0中引入。相比最初的定义，请求和响应消息的格式都有所改变。本文介绍CIFS格式，在NT LAN Manager中定义。当协商使用NT LAN Manager时必须使用此格式。

此命令用来配置一个SMB会话。如果服务器运行在user级访问控制模式，至少发送一个SMB\_COM\_SESSION\_SETUP\_ANDX命令，执行用户登录服务器并建立一个有效的UID。

在CIFS协议中，在SMB\_COM\_SESSION\_SETUP\_ANDX命令执行成功之前发送SMB\_COM\_TREE\_CONNECT或SMB\_COM\_TREE\_CONNECT\_ANDX是违反协议的，即使服务器运行在share级的访问控制模式。在SMB\_COM\_SESSION\_SETUP\_ANDX请求之后，包含SMB\_COM\_TREE\_CONNECT\_ANDX批处理请求的AndX链可以满足这一需求，匿名认证也可以满足这一需求（原句：Including an SMB\_COM\_TREE\_CONNECT\_ANDX batched request in an AndX chain (section 2.2.3.4) following an SMB\_COM\_SESSION\_SETUP\_ANDX request is sufficient to fulfill this requirement. Anonymous authentication is also sufficient to fulfill this requirement）。

一个SMB会话用允许有多个SMB\_COM\_SESSION\_SETUP\_ANDX，用来建立额外的UID或建立额外的虚拟链路。

下面的命令可以放在SMB\_COM\_SESSION\_SETUP\_ANDX后面的AndX链中：

SMB\_COM\_TREE\_CONNECT\_ANDX (section 2.2.4.55 )

SMB\_COM\_OPEN (section 2.2.4.3 )

SMB\_COM\_OPEN\_ANDX (section 2.2.4.41 )

SMB\_COM\_CREATE (section 2.2.4.4 )

SMB\_COM\_CREATE\_NEW (section 2.2.4.16 )

SMB\_COM\_CREATE\_DIRECTORY (section 2.2.4.17 )

SMB\_COM\_DELETE (section 2.2.4.7 )

SMB\_COM\_DELETE\_DIRECTORY (section 2.2.4.2 )

SMB\_COM\_FIND (section 2.2.4.59 )

SMB\_COM\_FIND\_UNIQUE (section 2.2.4.60 )

SMB\_COM\_RENAME (section 2.2.4.8 )

SMB\_COM\_NT\_RENAME (section 2.2.4.66 )

SMB\_COM\_CHECK\_DIRECTORY (section 2.2.4.17)

SMB\_COM\_QUERY\_INFORMATION (section 2.2.4.57 )

SMB\_COM\_SET\_INFORMATION (section 2.2.4.10 )

SMB\_COM\_OPEN\_PRINT\_FILE (section 2.2.4.67 )

SMB\_COM\_TRANSACTION (section 2.2.4.33 )

2.2.4.54 SMB\_COM\_LOGOFF\_ANDX (0x74)

SMB头部UID标记的用户被注销，服务器将释放所有此UID相关的资源，包括释放锁，关闭所有的文件，断开连接，取消所有没有处理完的命令，标记此UID无效。

下面的命令可以放在SMB\_COM\_LOGOFF\_ANDX后面的AndX链中：

SMB\_COM\_SESSION\_SETUP\_ANDX.

2.2.4.55 SMB\_COM\_TREE\_CONNECT\_ANDX (0x75)

此命令在LAN Manager 1.0中引入。

此命令用来建立一条客户端和服务器之间的连接，共享资源依靠共享名确定。连接建立后，此连接将用服务器返回的TID作为识别标记。

下面的命令可以放在SMB\_COM\_TREE\_CONNECT\_ANDX后面的AndX链中：

SMB\_COM\_OPEN (section 2.2.4.3 )

SMB\_COM\_OPEN\_ANDX (section 2.2.4.41 )

SMB\_COM\_CREATE (section 2.2.4.4 )

SMB\_COM\_CREATE\_NEW (section 2.2.4.16 )

SMB\_COM\_CREATE\_DIRECTORY (section 2.2.4.17 )

SMB\_COM\_DELETE (section 2.2.4.7 )

SMB\_COM\_DELETE\_DIRECTORY (section 2.2.4.2 )

SMB\_COM\_SEARCH (section 2.2.4.58 )

SMB\_COM\_FIND (section 2.2.4.59 )

SMB\_COM\_FIND\_UNIQUE (section 2.2.4.60 )

SMB\_COM\_RENAME (section 2.2.4.8 )

SMB\_COM\_NT\_RENAME (section 2.2.4.66 )

SMB\_COM\_CHECK\_DIRECTORY (section 2.2.4.17)

SMB\_COM\_QUERY\_INFORMATION (section 2.2.4.9 )

SMB\_COM\_SET\_INFORMATION (section 2.2.4.10 )

SMB\_COM\_OPEN\_PRINT\_FILE (section 2.2.4.67 )

SMB\_COM\_TRANSACTION (section 2.2.4.33 )

2.2.4.56 SMB\_COM\_SECURITY\_PACKAGE\_ANDX (0x7E)

此命令在LAN Manager 1.0中引入，现在已被废弃。

此命令用来协商包加密以及相关信息，但是现在已不再使用。关于此命令的实现描述可以在[XOPEN-SMB]的11.2节找到。

客户端不应该发送此命令，服务器收到此命令后应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOC/ERRbadfunc)。

2.2.4.57 SMB\_COM\_QUERY\_INFORMATION\_DISK (0x80)

这是一个核心协议命令，已被废弃。新的实现使用SMB\_COM\_TRANSACTION2和其子命令TRANS2\_QUERY\_FS\_INFORMATION。

此命令可以由客户端发送，在SMB头部指明TID，获取相关目录的空间及剩余空间大小。客户端必须提供一个有效的TID，此TID应该由前面相关的SMB命令获取到的。

响应消息中返回的块或已申请单元大小，可能会与服务器实际物理或逻辑分配算法不一样，但是必须真实反映服务器上空间大小。

响应消息为每个域只返回16bit大小的信息，可能有些系统会请求大于此大小的信息。TotalUnits通常要远大于65535. 然而，典型的客户端一般只是请求磁盘大小和可用空间大小，因此服务器应该调整BlocksPerUnit和BlockSize的单位来适应16-bit的限制。如果经过调整还是超过了16-bit的限制，应该返回TotalUnits和FreeUnits所能表达的最大值。

2.2.4.58 SMB\_COM\_SEARCH (0x81)

这是一个原始核心协议命令，已被废弃。新的实现使用TRANS2\_FIND\_FIRST2代替。

此命令用来在目录中搜索名字与指定通配符模板匹配的文件或其它对象。响应消息中在允许的最大传输字节内返回尽可能多的匹配的名字。响应消息中也包含一个key，用在后面的SMB\_COM\_SEARCH命令中返回下一组匹配的名字。

此命令只返回8.3格式的文件名称，和文件的基本属性，不支持Unicode，文件名只以扩展ASCII(OEM)字符返回。此命令后续没有关闭的操作。服务器要管理搜索的状态，直到搜索完成，或者PID或TID关闭，UID被置为无效(注销)，或会话关闭。

2.2.4.59 SMB\_COM\_FIND (0x82)

此命令在LAN Manager 1.0中引入，已被废弃。新的实现使用SMB\_COM\_TRANSACTION2的子命令TRANS2\_FIND\_FIRST2来替代。

此命令的结构和目的都和SMB\_COM\_SEARCH相同，唯一不同的是有一个匹配的SMB\_COM\_FIND\_CLOSE命令，允许用户主动关闭一个搜索操作。

2.2.4.60 SMB\_COM\_FIND\_UNIQUE (0x83)

此命令在LAN Manager 1.0中引入，已被废弃。新的实现使用SMB\_COM\_TRANSACTION2的子命令TRANS2\_FIND\_FIRST2来替代。

SMB\_COM\_FIND\_UNIQUE有着和SMB\_COM\_SEARCH及SMB\_COM\_FIND几乎一样的格式，不同的是请求消息中没有SMB\_Date.ResumeKey。和SMB\_COM\_SEARCH及SMB\_COM\_FIND用法不同的是，它不要求服务器管理搜索上下文或其它状态。命令是单独使用的，没有后续命令。

和其它的搜索命令一样，请求可以包含至少一个的匹配名字。当响应返回后，搜索关闭。

2.2.4.61 SMB\_COM\_FIND\_CLOSE (0x84)

此命令在LAN Manager 1.0中引入，已被废弃。新的实现使用SMB\_COM\_TRANSACTION2的子命令TRANS2\_FIND\_FIRST2替代。

此命令关闭由SMB\_COM\_FIND打开的目录搜索。初始化SMB\_COM\_FIND请求逻辑上打开并启动了搜索。后续的SMB\_COM\_FIND使用合法的ResumeKey可以继续搜索。SMB\_COM\_FIND\_CLOSE关闭了搜索，服务器释放管理搜索上下文用到的所有资源。

如果SMB\_COM\_FIND失败（返回错误），搜索不会打开，这个命令也不用调用来关闭搜索。此命令不应该用来关闭SMB\_COM\_SEARCH开启的搜索。

此命令的格式和SMB\_COM\_SEARCH及SMB\_COM\_FIND几乎相同，只是响应消息中没有字段SMB\_Data.DirectoryInformationData。

2.2.4.62 SMB\_COM\_NT\_TRANSACT (0xA0)

此命令在NT LAN Manager中引入。

此命令扩展了由SMB\_COM\_TRANSACTION2提供的文件系统访问服务，允许处理非常大的参数和数据块。

SMB\_COM\_NT\_TRANSACT消息可以超过单个SMB消息允许的最大值（由参数MaxBufferSize决定）。在这种情况下，客户端使用一个或多个SMB\_COM\_NT\_TRANSACT\_SECONDARY消息来传输和消息初始化不匹配的data和Parameter。

如果客户端没有发送完所有的**SMB\_Data.Trans\_Data，会将DataCount设置为小于TotalDataCount的一个值。同样的，如果SMB\_Data.Trans\_Parameters没有发送完，会设置ParameterCount为一个小于TotalParameterCount的值。参数部分优先级高于数据部分，客户端在每个消息中应该尽量多的发送数据。服务器应该可以接收无序到达的SMB\_Data.Trans\_Parameters** 和 **SMB\_Data.Trans\_Data，不论是大量还是少量的数据。**

**在请求和响应消息中，SMB\_Data.NT\_Trans\_Parameters和SMB\_Data.nt\_Trans\_Data的位置和长度都是由SMB\_Parameters.ParameterOffset、SMB\_Parameters.ParameterCount, SMB\_Parameters.DataOffset和SMB\_Parameters.DataCount决定。另外需要说明的是，SMB\_Parameters.ParameterDisplacement和SMB\_Parameters.DataDisplacement可以用来改变发送数据段的序号。服务器应该按照自己顺序发送，优先发送SMB\_Data.NT\_Trans\_Parameters。客户端应该准备好组装收到的SMB\_Data.NT\_Trans\_Parameters和SMB\_Data.NT\_Trans\_Data，即使它们是乱序到达的。**

2.2.4.63 SMB\_COM\_NT\_TRANSACT\_SECONDARY (0xA1)

此命令用来完成SMB\_COM\_NT\_TRANSACT中未传完的数据。

2.2.4.64 SMB\_COM\_NT\_CREATE\_ANDX (0xA2)

此命令在NT LAN Manager中引入。

此命令用来创建并打开一个新文件，或者打开一个已存在的文件，或打开并清空一个已存在的文件，或创建一个目录，或创建一个命名管道。返回的FID可以用在后续的请求消息中。

消息中包含客户端想要创建或打开的文件名，目录，或命名管道和RootDirectoryFID。如果执行成功，服务器返回一个FID标记打开的资源。客户端在后续的请求消息中必须携带此FID。客户端必须拥有对资源所在目录的写权限，才能创建一个新的文件或目录；或者拥有文件的写权限来执行截断文件的操作。

下面的命令可以放在SMB\_COM\_NT\_CREATE\_ANDX后面的AndX链中：

SMB\_COM\_READ (section 2.2.4.11 )

SMB\_COM\_READ\_ANDX (section 2.2.4.42 )

SMB\_COM\_IOCTL (section 2.2.4.35 )

2.2.4.65 SMB\_COM\_NT\_CANCEL (0xA4)

此命令在NT LAN Manager中引入。

此命令使客户端可以取消掉pending态的请求。服务器用SMB\_Header中的信息识别客户端想要取消哪些请求，服务器可以取消或立即处理这些请求。服务器对此消息不能回复响应消息。客户端应该依靠服务器对指定取消的消息的响应来判断取消消息的结果。如果服务器不能识别客户端请求中的指定消息，也不应该发送响应。

此命令主要用来取消由SMB\_COM\_NT\_TRANSACT和NT\_TRANSACT\_NOTIFY\_CHANGE子命令引起的多余的通知消息。客户端一般用NT\_TRANSACT\_NOTIFY\_CHANGE命令避免轮询目录的改变。此命令另外的用途包括取消一个无限期等待繁忙资源的请求，或尝试很多次来等待一个资源的请求。

2.2.4.66 SMB\_COM\_NT\_RENAME (0xA5)

此命令在NT LAN Manager中引入，已不使用。

客户端可以使用此命令在源端服务器上建立一个硬链接，来执行一个本地的文件重命名，并在存在的路径结构上移动文件（原句：to perform an in-place file rename, and to move a file within its existing path hierarchy）。详情请看请求消息中的InformationLevel字段。此命令不支持目录或文件名中含有通配符，每次只操作一个文件。已存在的文件不能被覆盖。如果请求消息中NewFileName为空，新文件的目标路径必须是文件头部TID所表示的目录的根目录。在本地重命名是，文件路径必须相同，否则会返回一个错误码。

2.2.4.67 SMB\_COM\_OPEN\_PRINT\_FILE (0xC0)

这是一个原始核心协议命令。

此命令用来创建一个打印队列缓冲文件。此文件将会在打印机中排队。当文件打印完毕后，服务器应该删除这个文件。

2.2.4.68 SMB\_COM\_WRITE\_PRINT\_FILE (0xC1)

这是一个原始核心协议，已不使用。应该使用SMB\_COM\_WRITE\_ANDX来向打开的spool文件写入数据。

此命令用来向打开的打印队列spool文件中写入数据。

最先写入打印文件的数据是打印机的控制信息，控制信息的长度由SMB\_COM\_OPEN\_PRINT\_FILE请求命令中的参数SMB\_Parameters.Words.SetupLength指定。在一个SMB\_COM\_WRITE\_PRINT\_FILE中可以同时包含打印机控制数据和打印文件数据，只要保证控制数据已完全写入即可。

2.2.4.69 SMB\_COM\_CLOSE\_PRINT\_FILE (0xC2)

这是一个原始核心协议命令，已不使用。客户端应该使用SMB\_COM\_CLOSE来关闭由SMB\_COM\_OPEN\_PRINT\_FILE打开的spool文件。

此命令关闭指定的打印队列spool文件，会触发服务器将此文件排队并打印。

2.2.4.70 SMB\_COM\_GET\_PRINT\_QUEUE (0xC3)

这是一个原始核心协议(见[SMB-CORE]5.26章节)。在NT LAN Manager中注明已不使用，在[CIFS]中指定为可选。

此命令用来产生一个和指定TID相关的打印队列的对象列表，客户端不应该发送此命令，服务器收到此命令后应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOC/ERRbadfunc)

2.2.4.71 SMB\_COM\_READ\_BULK (0xD8)

此命令被保留没有使用。它被列在早期的微软和第三方的文档中。尽管如此，此命令还没有一个正式的定义，并且也从没有被使用过。两个相关的命令SMB\_COM\_WRITE\_BULK和SMB\_COM\_WRITE\_BULK\_DATA也从来没有被使用过。

客户端不应该发送此命令，服务器收到此命令后应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOC/ERRbadfunc)。

2.2.4.72 SMB\_COM\_WRITE\_BULK (0xD9)

此命令被保留没有使用。它被列在早期的微软和第三方的文档中。尽管如此，此命令还没有一个正式的定义，并且也从没有被使用过。两个相关的命令SMB\_COM\_READ\_BULK和SMB\_COM\_WRITE\_BULK\_DATA也从来没有被使用过。

客户端不应该发送此命令，服务器收到此命令后应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOC/ERRbadfunc)。

2.2.4.73 SMB\_COM\_WRITE\_BULK\_DATA (0xDA)

此命令被保留没有使用。它被列在早期的微软和第三方的文档中。尽管如此，此命令还没有一个正式的定义，并且也从没有被使用过。两个相关的命令SMB\_COM\_READ\_BULK和SMB\_COM\_WRITE\_BULK也从来没有被使用过。

客户端不应该发送此命令，服务器收到此命令后应该返回STATUS\_NOT\_IMPLEMENTED (ERRDOC/ERRbadfunc)。

2.2.4.74 SMB\_COM\_INVALID (0xFE)

此命令在LAN Manager 1.0中引入。这是一个保留的值，指明一个非法的命令。

客户端不应该发送此命令，服务器收到此命令后应该返回STATUS\_SMB\_BAD\_COMMAND (ERRDOC/ERRbadfunc)。

2.2.4.75 SMB\_COM\_NO\_ANDX\_COMMAND (0xFF)

此命令在LAN Manager 1.0中引入。设计此命令的目的是用来指明一个AndX链的结束。

客户端不应该在主命令中使用此命令，服务器在主命令中收到此命令后应该返回STATUS\_SMB\_BAD\_COMMAND (ERRSRV/ERRbadcmd)。

在早期的SMB协议规格(见[IBM-SMB])中，此命令保留来做特定协议的扩展。这个用法已过时。在最新的微软协议文档中，包括[SMB-CORE]和[MSFT-XEXTNP]，都没有描述此命令作为协议扩展或其它目的的作用。