# 1.ARM体系CPU的7种工作模式

（1）用户模式（usr）：ARM处理器正常的程序执行状态。

（2）快速中断模式（fiq）：用于高速数据传输或通道处理。

（3）中断模式（irq）：用于通用的中断处理。

（4）管理模式（svc）：操作系统使用的保护模式。

（5）数据访问终止模式（abt）：当数据或指令预取终止时进入该模式，可用于虚拟存储及存储保护。

（6）系统模式（sys）：运行具有特权的操作系统任务。

（7）未定义指令中止模式（und）：当未定义的指令执行时进入该模式，可用于支持硬件协处理器的软件仿真。

可以通过软件进行模式的切换，或者发生各类中断、异常时CPU自动进入相应的模式。除用户模式以外的6种工作模式都属于特权模式，大多数程序运行于用户模式，进入特权模式是为了处理中断、异常，或者访问被保护的系统资源。

# 2.ARM920T的寄存器

ARM920T有31个通用的32位寄存器和6个程序状态寄存器，这37个寄存器分为7组，进入某个工作模式时就使用它的那组寄存器。有些寄存器，不同的工作模式下有自己的副本，当切换到另一个工作模式时，那个工作模式的寄存器副本将被使用：这些寄存器被称为备份寄存器。从下图中可以看出fiq模式的备份寄存器最多，这是为了提高fiq的响应速度，减少保存寄存器值所花费的时间。

CPSR在七种模式下都是同一个寄存器，所以可以修改里面的值来转换到不同的工作模式下。R0~R15可以直接访问，除R15外均为通用寄存器，既可以用于保存数据也可以用于保存地址。R13~R15稍有特殊：R13又被称为栈指针寄存器sp，通常用于保存栈指针；R14又被称为程序连接寄存器，当执行BL子程序调用指令时，R14中得到R15（程序计数器PC）的备份，而当发生中断或异常时，对应的R14\_svc、R14\_irq、R14\_fiq、R14\_abt或R14\_und保存R15的返回值；R15又被称为程序计数器PC。

# 3.CPSR寄存器

CPSR中主要包括以下几种状态位：

（1）T位：置位时，CPU处于Thumb状态；否则处于ARM状态。

（2）中断禁止位：I位和F位属于中断禁止位。它们被置位时，IRQ中断、FIQ中断分别被禁止。

（3）工作模式位：表明CPU当前处于什么工作模式，可以更改这些位，使CPU进入指定的工作模式。

# 4.SPSR寄存器

SPSR寄存器，即程序状态保存寄存器，就是在除系统和用户模式外的5种模式下来保存CPSR寄存器的备份寄存器。当一个异常发生时，将切换进入相应的工作模式，这时ARM920T的CPU将自动完成如下事情。

（1）在异常工作模式的连接寄存器R14中保存前一个工作模式的下一条，即将执行的指令的地址。对于ARM状态，这个值是当前的PC值加4或者加8。

（2）将CPSR的值复制到异常模式的SPSR。

（3）将CPSR的工作模式位设为这个异常对应的工作模式。

（4）将PC值等于这个异常模式在异常向量表中的地址，即跳转去执行异常向量表中的相应指令。

相反地，从异常工作模式退出回到之前的工作模式时，需要通过软件完成如下事情。

（1）前面进入异常工作模式时，连接寄存器中保存了前一个工作模式的一个指令地址，将它减去一个适当的值后赋给PC寄存器。

（2）将SPSR的值复制回CPSR。

从表中可以看出，进入和退出异常时PC的计算方法会根据不同的模式进行不同的计算，主要分为3类（在表格中的（1）（2）（3）表示该模式属于的分类）：

（1）PC值是这些指令的地址：SWI、未定义的指令、在预取时就失败的指令。本条指令已经被执行，下一条指令的地址就是PC+4。

（2）PC值是这些指令的地址：进入快速中断、中断模式前，被打断而未执行的指令。本条指令就已经被打断，所以下一条指令就是PC当前指向的指令。

（3）PC值是这些指令的地址：导致数据访问终止的加载/存储指令（LDR、STR、LDM和STM）。这几个特殊指令，流水线技术会导致后面几条的指令都是这个指令的副本，所以该条指令相当于并未执行成功，下一条指令也就是PC当前指向的指令。

注：流水线技术导致PC的值是当前被执行指令的地址+8，然而已经被取指令的指令会继续执行，中断等打断的也只是取指令，前面已经在流水线中的指令会继续执行完毕。