



## ***AP180 Application Note for JTAG ISP***

***AN-03  
December 2004***

### **Application Notice Title**

**AP180 JTAG ISP Data**

### **Revision History**

<b>Rev.</b>	<b>History</b>	<b>Issue Date</b>	<b>Remark</b>
1.0	Initial issue	April 27, 2004	Preliminary
1.1	Increase Example description	December 21, 2004	Page 13

PRELIMINARY

**AP180 JTAG ISP****AP180 ON-CHIP FLASH MEMORY**

There are two on-chip flash memory blocks for AP180. The full program memory size for main ROM code is 64KB which can be fetched by the processor automatically. There is also a separate 128 bytes flash memory for security use. Only 1 byte addressed 0000h is used to support a standard three-level lock options. Serial programming is supported through the JTAG port. This application note describes how to serial programming the AP180 on-chip flash memory.

**JTAG (JOINT TEST ACTION GROUP) ISP**

The AP180 has an on-chip JTAG interface to support FLASH read/write operations (JTAG ISP). The JTAG interface is implemented via four dedicated pins on the processor, which are TCK, TMS, TDI, and TDO. These pins are all 5 volt input tolerant. The advised rising/falling time for pin TCK is 20ns typically.

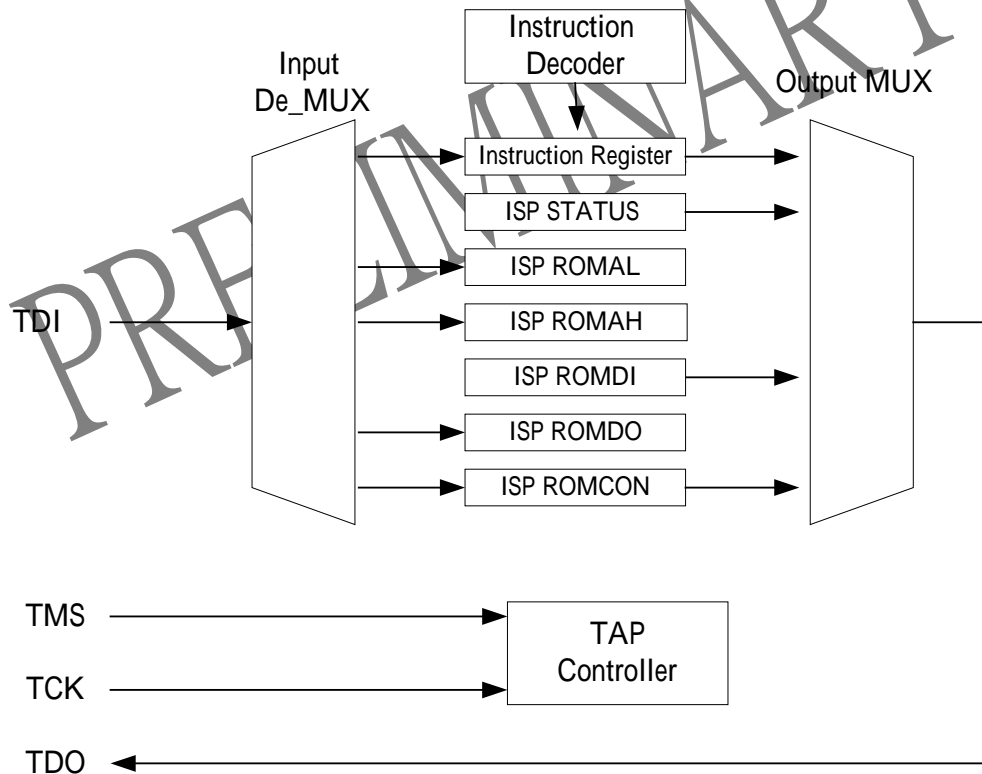
**Table1. JTAG ISP PIN DESCRIPTION**

Pin Name	Pin Description
<b>TDI</b>	<b>Test Data Input</b> -This input provides a serial data stream to the JTAG. It is sampled on the rising edge of TCK and has an on-chip pull-up resistor.(50K ohm) Data is always shifted LSB-first.
<b>TDO</b>	<b>Test Data Output</b> -This tri-state output provides a serial data stream from the JTAG. It is driven in the Shift-IR and Shift-DR controller states of the JTAG state machine and changes on the falling edge of TCK.
<b>TCK</b>	<b>Test Clock Input</b> -This input proves a gate clock to synchronize the test logic and shift serial data through the JTAG port. The TCK pin has an on-chip pull-down resistor. (50K ohm)
<b>TMS</b>	<b>Test Mode Select Input</b> -This input sequences the TAP controller's state machine. It is sampled on the rising edge of TCK and has an on-chip pull-up resistor. (50K ohm)

## JTAG ISP OVERVIEW

Figure1 shows a block diagram of the JTAG ISP. The TAP controller (Test Access Port) is a state machine controlled by the TCK and TMS signals. The TAP controller selects either the JTAG Instruction Register or ROM Flash Data Registers between the TDI-input and TDO-output. The Instruction Register holds JTAG instructions controlling the behavior of a ROM Flash Data Register.

**Figure1. JTAG ISP BLOCK DIAGRAM**

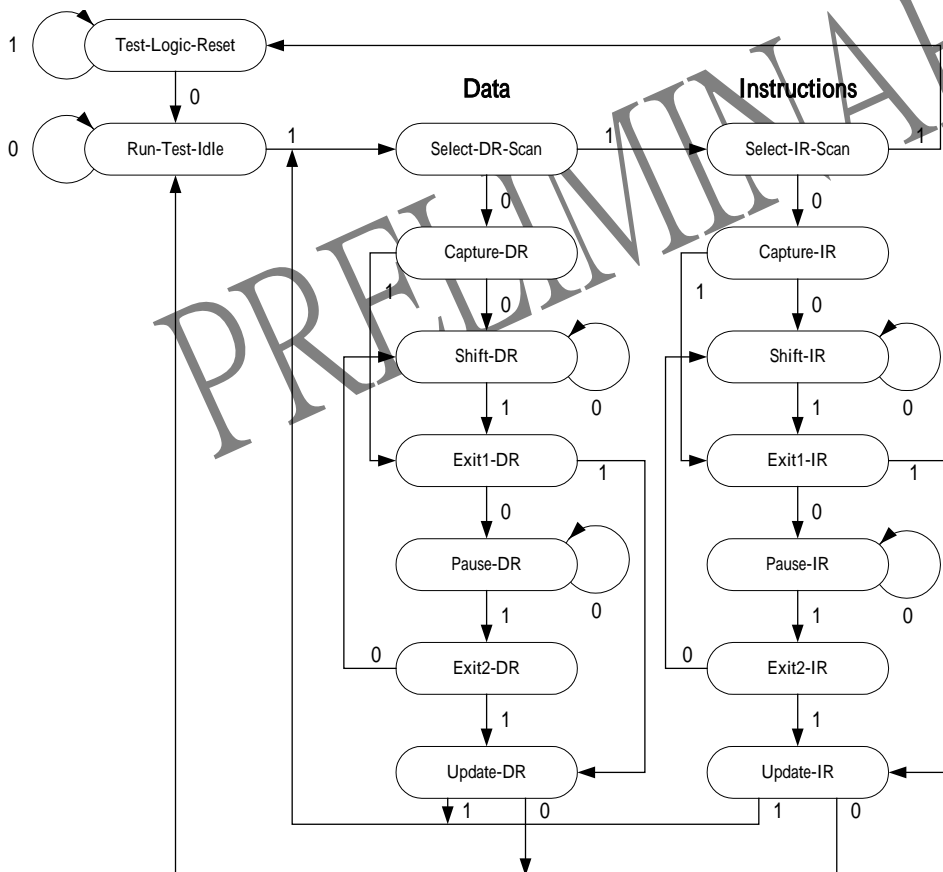


## JTAG ISP TAP CONTROLLER

The TAP controller is a 16-state finite state machine that controls the JTAG ISP. The state transitions depicted in Figure 2 depends on the signal present on TMS at the time of the rising edge at TCK. The TAP state is Test-Logic-Reset after a power-on reset or by holding TMS logic high and toggling TCK at least five times.

The primary purpose of the TAP state machine is to select which of two shift registers, the Instruction Register or the Data Register. In general, the Instruction Register is used to select which Data Register to scan. There are two primitive operations that the state machine controls: IR scan, and DR scan. In a scan operation, data is sampled at TDI on the rising edge of TCK, and is output on TDO on the falling edge of TCK. Data is always shifted LSB-first and 8 bits in length.

**Figure 2. TAP CONTROLLER STATE MACHINE**





## JTAG ISP REGISTER SUMMARY

There are two shift registers for JTAG use: Instruction Register (IR) and Data Register (DR).

### IR DECODING

7	6	5	4	0	Reset Value
State Cntl		R/W	DRAddress (5 bits)		00H

**Table2. "StateCntl" DECODING**

StateCntl Code	JTAG State
00	<b>Normal Mode</b> - AP180 is in normal mode with running Flash ROM code.
01	<b>JTAG ISP Request Mode</b> - This instruction asserts a request to halt the core for entry to JTAG Mode. JTAG ISP functions is provided through the JTAG port.
10	<b>MCU-Reset Mode</b> -JTAG will reset the MCU and MCU starts with the vector 0000H.
11	RESERVED

### R/W (Bit5)

0: Write to the ISP DR register specified by the DRAddress bits.

1: Read from the ISP DR register specified by the DRAddress bits.

**Table3. DRAAddress DECORding**

DRAAddress Code	JTAG Register Selected	Mode	R/W	Reset Value
00000	RESET REGISTER	-	-	-
00001	ISP STATUS	R (all mode)	Read Only	00H
10111	ISP ROMAL ISP ROM Address	JTAG	Write Only	00H
11000	ISP ROMAH ISP ROM Address	JTAG	Write Only	00H
11001	ISP ROMDI ISP ROM Data-In Register from MCU	JTAG	Read Only	00H
11010	ISP ROMDO ISP ROM Data-Out Register to MCU	JTAG	Write Only	00H
11011	ISP ROMCON ISP ROM Access Control Register	JTAG	R/W	00H
The others	RESERVED	-	-	-

## REGISTER DESCRIPTION

### ISP STATUS REGISTER

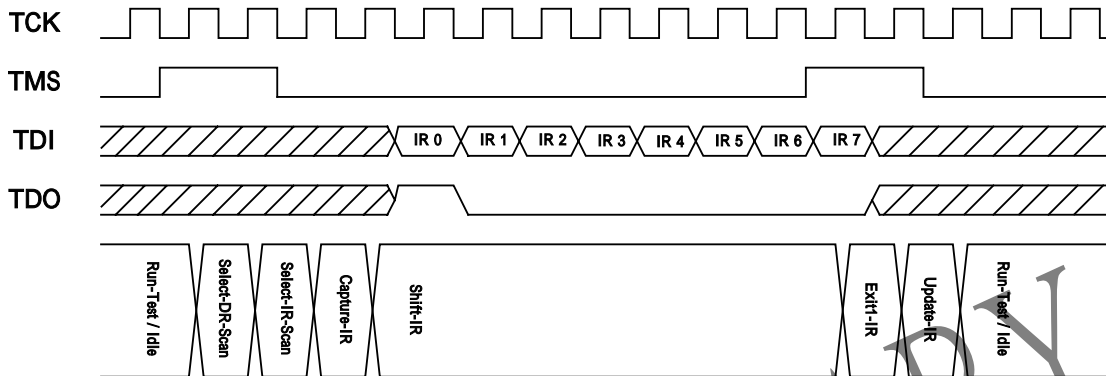
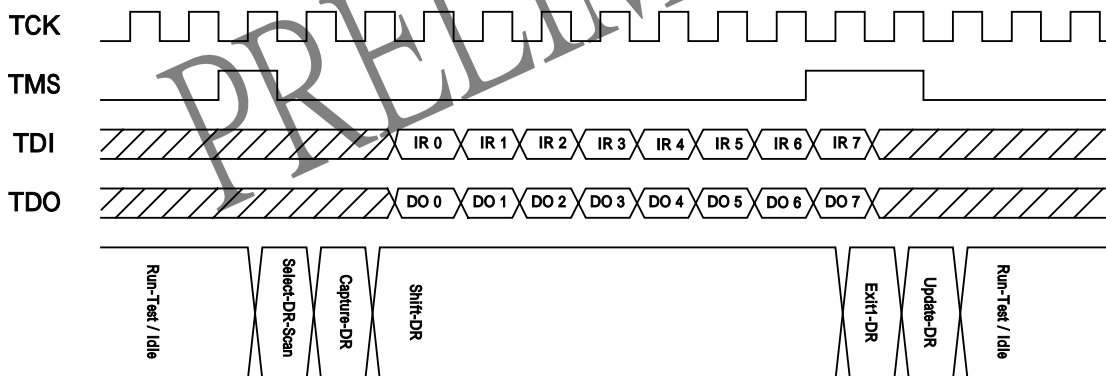
-	-	-	-	ISP_IN	-	-	-
---	---	---	---	--------	---	---	---

ISP\_IN(Read Only): Hardware set for entry to JTAG ISP Mode.  
Keep the other bits at logic low.

### ISP ROMCON REGISTER

-	-	ROM_OE	ROM_PROG	ROM_MASE	ROM_NVSTR	ROM_IFREN	ROM_AE
---	---	--------	----------	----------	-----------	-----------	--------

The control signals are high level active for 64KB ROM memory and Lock-bit read/write.  
Keep Bit [7] & Bit [6] at logic High.

**Timing Waveforms [4]**

**Figure 4. Instruction Register Scan Timing**

**Figure 5. Data Register Scan Timing**

**64KB/128B ON-CHIP ROM FLASH DESCRIPTION****READ OPERATION**

To read data at the output, three control functions must be satisfied:

**AE** is the address enable and should pull high (VIH). Address will be valid after AE is high.

**OE** is the output enable and high active.

**IFREN** signal determines whether to read from 64KB main ROM memory or 128B memory.

**BYTE PROGRAMMING**

The programming operation is a byte basis. **AE**, **PROG**, **NVSTR** and **IFREN** signals activate a program operation. The address and the data are latched on the rising edge of PROG. The internal programming voltages and timing is controlled by NVSTR signal.

A data "0" can not be programmed back to a "1". Only erase operation can convert "0"s to "1"s. A mass erase should be executed before the target array location being programmed.

**MASE ERASE OPERATION**

The entire memory array including both 64KB and 128B memory blocks can be erased through a mass erase operation. **AE**, **MASE**, **IFREN** and **NVSTR** signals active mass erase. The internal erasure voltage and timing is controlled by NVSTR signal.

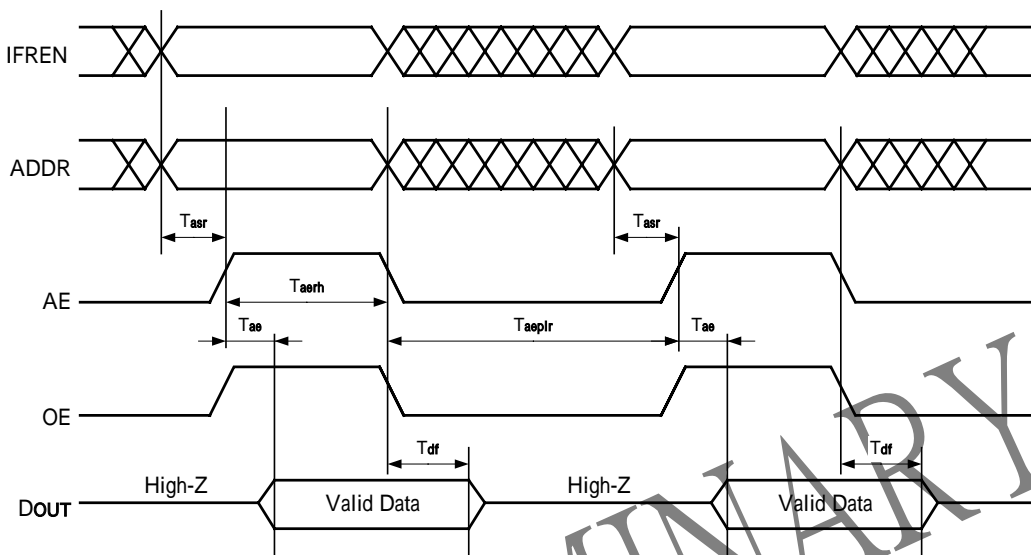
**Table4. USER MODE TRUTH TABLE FOR 64KB/128B FLASH MEMORY**

Mode	AE	OE	PROG	MASE	NVSTR	IFREN	DATA	ADDRESS
Standby	L	X	X	X	X	X	Z	X
Read	H	H	L	L	L	active	Dout	active
Program	H	L	H	L	H	active	Din	active
Mase Erase	H	L	L	H	H	active	X	X

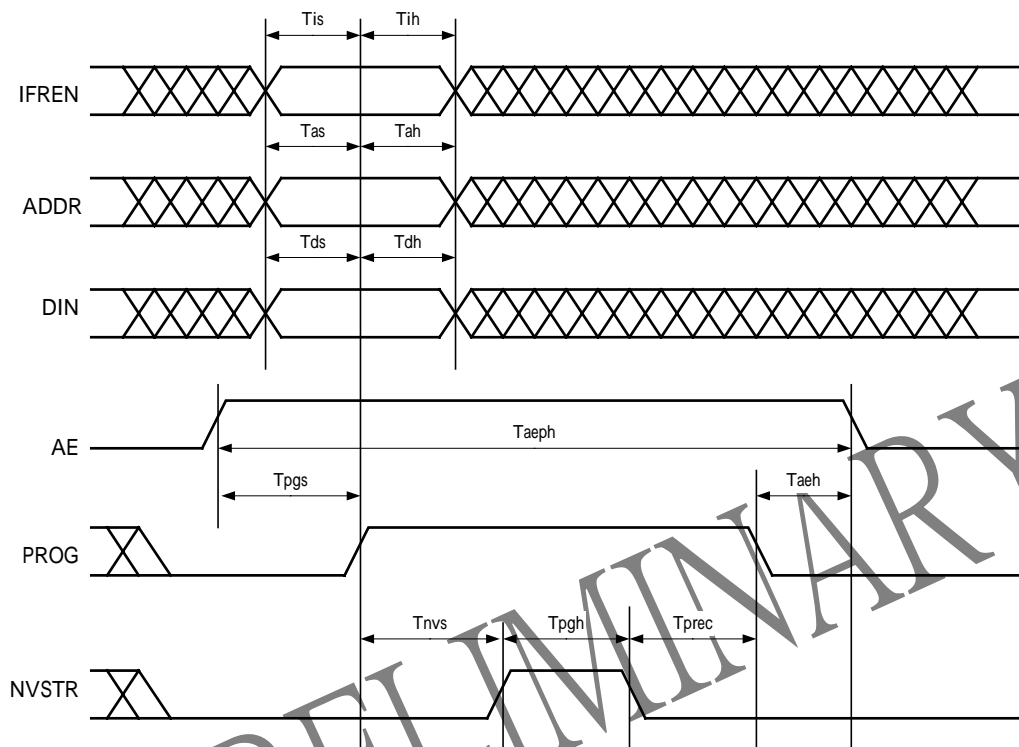
**Table5. IFREN TRUTH TABLE**

Mode	IFREN = 1	IFREN = 0
Read	Read 128B memory block	Read 64KB memory block
Program	Program 128B memory block	Program 64KB memory block
Mase Erase	Erase both blocks	Erase 64KB memory block

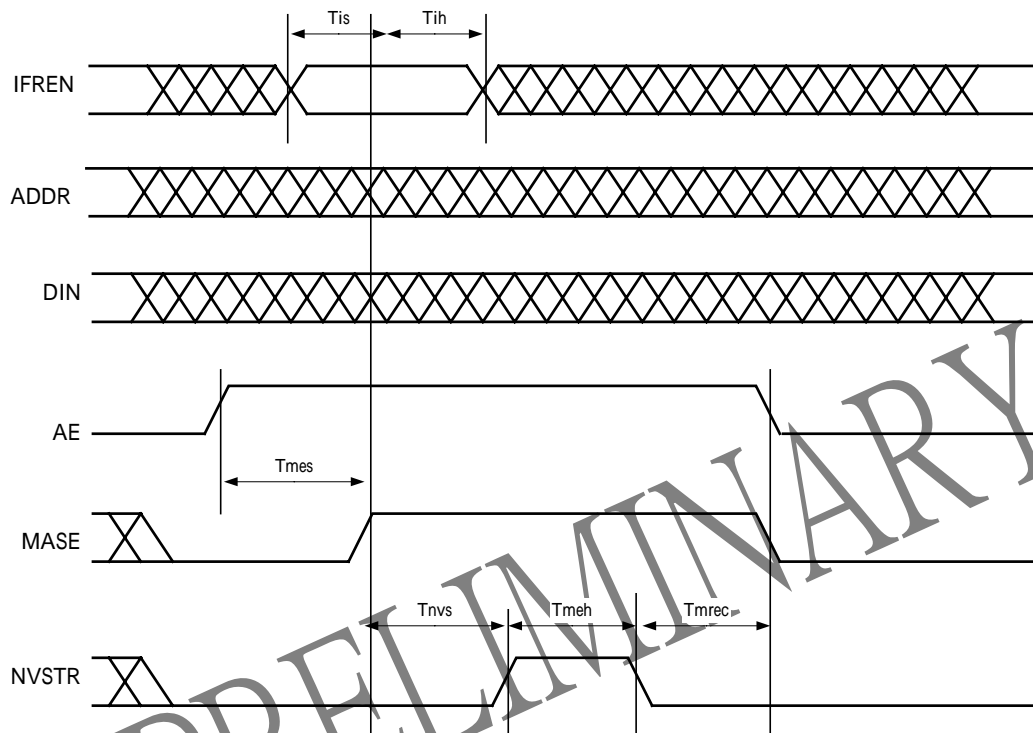


**Timing Waveforms [1]**

**Figure 6. Read Operation Timings (AE Controlled)**

Parameter	Symbol	Min.	Max.	Unit
Address setup time at read	Tasr	0	-	ns
AE high and address hold time at read	Taerh	55	-	ns
AE access time at read	Tae	-	50	ns
AE pulse low hold time at read	Taeplr	10	-	ns
AE to output high Z	Tdf	-	10	ns

**Timing Waveforms [2]**

**Figure 7. Program Operation Timings**

Parameter	Symbol	Min.	Max.	Unit
Program setup time	Tpgs	20	-	ns
AE enable program hold time	Taeph	20	-	us
NVSTR setup time	Tnvs	120	-	ns
Program hold time	Tpgh	20	40	us
Program recovery time	Tprec	3	-	us
AE hold time	Taeh	0	-	ns
IFREN setup time in program	Tis	0	-	ns
IFREN hold time in program	Tih	20	-	ns
Address setup time	Tas	0	-	ns
Address hold time	Tah	20	-	ns
Data setup time	Tds	0	-	ns
Data hold time	Tdh	20	-	ns

**Timing Waveforms [3]**

**Figure 8. Mass Erase Operation Timings**

Parameter	Symbol	Min.	Max.	Unit
Mase Erase setup time	Tmes	20	-	ns
NVSTR setup time	Tnvs	120	-	ns
Mase Erase hold time	Tmeh	40	80	ms
Mase Erase recovery time	Tmrec	100	-	us
IFREN setup time in Mase Erase	Tis	0	-	ns
IFREN hold time in Mase Erase	Tih	20	-	ns



## SECURITY FEATURES

The AP180 supports three-level lock restricts viewing of the internal 64KB ROM code memory contents. By programming the two Lock-bit, the user can select a level of security as specified in Table6. Once a security level is selected and programmed, the setting of the Lock-bit remains. But after AP180 device is powered-on, it is default restricted at level 3 and the user can not read or write 64KB memory through JTAG mode or on programmer. It needs Lock-bit read operation to reload the content of the Lock-bit. Only a mass erase can erase these bits to allow reprogramming the security level to a less restricted protection.

### FLASH MEMORY LOCK-BIT

-	-	-	-	-	-	<b>LB2</b>	<b>LB1</b>	0000H
---	---	---	---	---	---	------------	------------	-------

**Table6. LOCK BITS FEATURES**

Level	LB2	LB1	Protection Type
1	U	U	No program lock feature enabled.
2	U	P	Data verification is disabled. (“Verify Signature Byte” and “Verify Lock Bits” are still enabled.)
3	P	P	Same as 2, also further written operation of the Flash is disabled.

Notes :

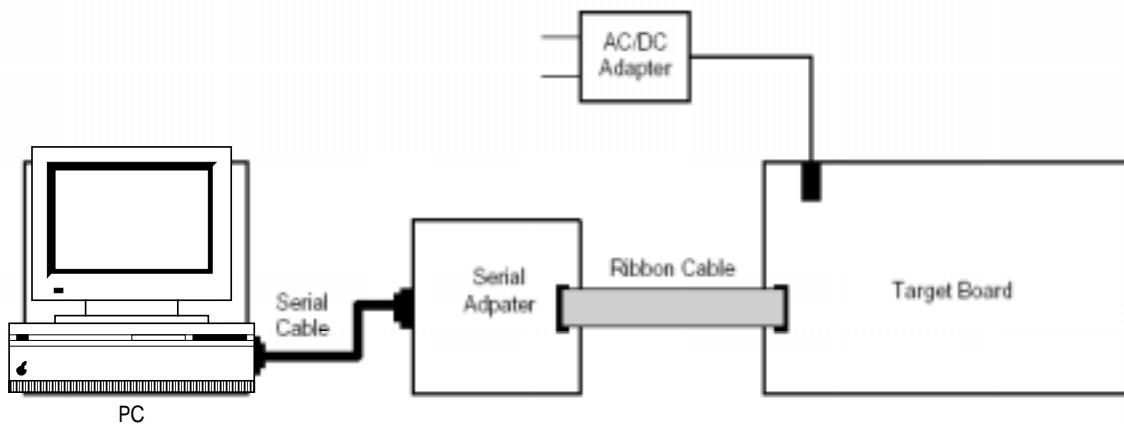
1. ‘U’= Non programmed or “1” level.
2. ‘P’= Programmed or “0” level

---

**EXAMPLE DESCRIPTION****Hardware Configuration**

The target board is connected to a PC running the AP180 ISP tool via the Serial Adapter as shown in Figure9.

1. Connect one end of the RS232 serial cable to a serial (COM) port on the PC.
2. Connect the other end of the RS232 serial cable to the port on the Serial Adapter.
3. Connect the Serial Adapter to the JTAG port on the target board using the 10-pin ribbon cable.



**Figure9. Hardware Setup**

**Software Configuration**

1. PC\_Source\_Code: It is the example source code for AP180\_ISP tool in PC.
2. JTAG\_Board\_12T\_Source\_Code: It is the serial adapter example code for standard 12T 8052 series, The serial adaptor function is processing the protocol for RS232 (PC) to JTAG interface (AP180).

## Serial Adaptor Example Circuit

