Chapter 05

Advanced Microprocessors

LEARNING OBJECTIVES

This chapter aims at describing the following:

- *Evolution of Intel microprocessor from intel 80286 to Intel Pentium II microprocessor.*
- *Protected modes of advanced microprocessors, virtual memory, and multitasking*
- *Internal structure, signals, registers, and instructions of 80286, 80386, 80486, and Pentium processors*
- *Features of Pentium-MMX, Pentium-Pro, and Pentium-II microprocessors*

5.1 INTRODUCTION

Intel has regularly improved the performance and features of microprocessors for PCs since the introduction of 8088, the first microprocessor for PC. The 8088 has just 20-bit address bus, 8-bit data bus and operates up to 5 MHz. The 8086 microprocessor also has 20-bit address bus but it has 16-bit data bus and operates up to 8 MHz. The next advanced popular microprocessor Intel 80286 has 24-bit address bus, 16-bit data bus and operates at the clock speed of 16 MHz. The 80386 processor has 32-bit address bus, 32-bit data bus, and operates at 33 MHz clock frequency. The 80486 microprocessor also has 32-bit address and data buses, but operates at 66 MHz clock and provides additional features than 80386. The Pentium, Pentium-MMX, Pentium-Pro, Pentium-II, and Pentium-III processors also have improved performances over their predecessors.

We describe in the following sections the techniques employed in microprocessors for improving their performance. We also explain the features of various microprocessors.

5.2 PROTECTED MODE OPERATION

The most important advancement in 80286 and above microprocessors is their protected mode operation. Advanced microprocessors can operate in real, protected, and virtual real modes.

5.2.1 Limitations of Real Mode Operation

The 8088 and 8086 processors operate only in real mode. The limitations of real mode operation are:

(a) The processor can access only 1MB of memory. The 1MB address space is referred to as *real mode memory*.

(b) Real mode operation allows only a single program to run at a time under a unitasking operating system such as DOS.

5.2.2 Features of Protected Mode Operation

The 80286 and above microprocessors can operate in real and protected modes. The features of protected mode operation are:

(a) The processor can access memory above the 1MB address space also. Memory above the 1MB address space is referred to as *extended memory*.

(b) It supports virtual memory. Virtual memory is memory management technique that extends the processor's capability to access much more memory beyond its maximum possible physical memory.

(c) It allows multitasking. Multitasking refers to loading multiple programs into memory and executing them simultaneously under a multitasking operating system such as Windows.

(c) It allows multitasking. Multitasking refers to loading multiple programs into memory and executing them simultaneously under a multitasking operating system such as Windows.

5.2.3 Memory Addressing in Protected Mode

Programs provide logical addresses to microprocessors to access a memory location. In real mode, a logical address contains two parts, the 16-bit segment base and the 16-bit offset. The microprocessor uses the two parts and computes the 20-bit physical address. It is known as segment addressing.

In protected mode also, the logical addresses have two parts, but represent the 16-bit segment selector and the 16-bit offset. The integrated memory management unit in the advanced microprocessors uses a different scheme to compute the physical addresses from the segment selector and the offset, as described in the following:

Segment, descriptors, and descriptor tables

In protected mode, a segment is described by a segment descriptor. The segment descriptor contains the base address, size and access rights of the segment. The size of the segment descriptor is 8 bytes. Two descriptor tables, called *global descriptor table* and *local descriptor table*, are created in memory to describe the segments. Each descriptor table can hold the maximum of 8 K (8,192) descriptors.

Figure 5.1 explains protected mode segment addressing. In protected mode, the segment register no longer holds the segment base as in real mode but holds a segment selector. The selector points to a segment descriptor in one of two descriptor tables. The 13 MSB bits, D15-D3, of the selector identifies the descriptor, the bit D2 identifies the global or local descriptor table, and the 2 LSB bits, D1-D0, indicate the privilege level. Microprocessor holds the base and

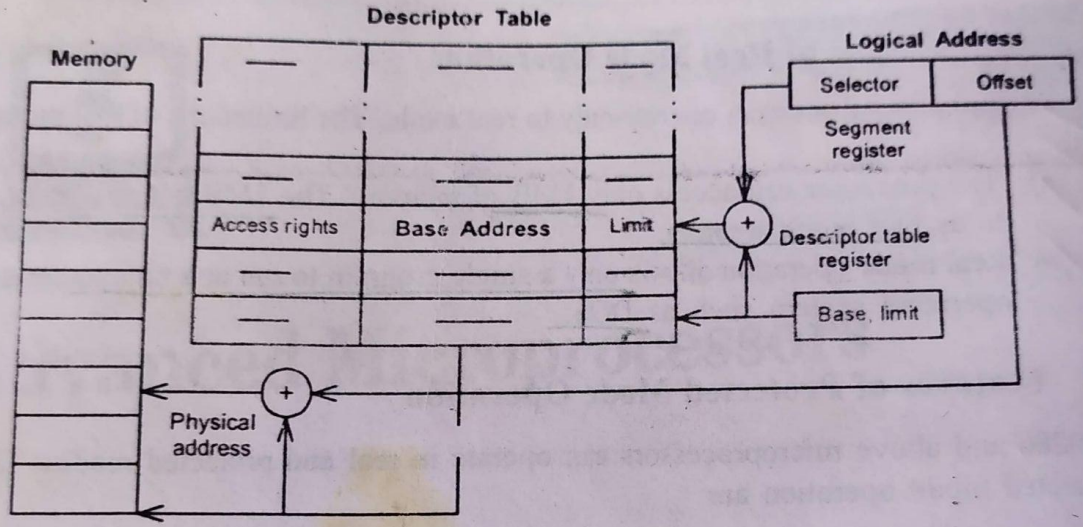


Figure 5.1 The protected mode segment addressing.

the limit of descriptor tables in its internal global and local descriptor table registers, which are not accessible to programmers. An integrated memory management unit (MMU) in the microprocessor computes the physical address of a memory location by adding the offset part of the logical address to the segment base in a segment descriptor.

5.2.4 Virtual Memory

The protected mode not only supports much higher amount of physical memory than supported by the real mode, but also supports virtual memory. In protected mode, when memory more than actually present in the system is required for an application, the processor can use hard disk as memory. This is referred to as virtual memory. The process of managing the virtual memory is accomplished by the MMU within the processor.

When the microprocessor accesses a memory location, the MMU first checks if the segment addressed by the processor is currently present in physical memory or not. The descriptor provides a 'P' bit to indicate this. If the segment is in the physical memory, it simply adds the offset to the segment base and enables the memory for data transfer. If the segment is not in the physical memory, it interrupts the processor to load the segment from the hard disk into the physical memory. After the segment is loaded into the memory, it enables the memory for data transfer.

The 80286 processor can address the maximum of 16 MB of physical memory and 1 GB of virtual memory and the 80386/80486 processors can address the maximum of 4 GB of physical memory and 64 TB of virtual memory.

5.2.5 Multitasking

The protected mode supports multitasking, also in which multiple programs can co-exist in memory and run simultaneously. A task refers to a simple subroutine program or an application program.

The protected mode also supports real mode sessions within the protected mode. It is known as *virtual real mode*, *virtual 8086 mode* or *V86 mode*. Running a real mode program (DOS program) under protected mode operating systems (Windows 95/98) create a real mode session in protected mode. However, the real mode program can access only the 1 MB of the total available memory. Since the protected mode supports multitasking, it allows several real mode sessions to co-exist in memory.

5.3 THE 80286 MICROPROCESSOR

The 8088 and 8086 microprocessors were used in IBM compatible PC and PC-XT (Personal Computer eXtended Technology) systems. The next advanced microprocessor that became popular after the 8088/8086 microprocessors in PC systems is Intel 80286. The 80286 microprocessor is used in PC-AT (Personal Computer-Advanced Technology) systems. The 80286 has 16-bit data bus, 24-bit address bus and operate at 16 MHz clock frequency. It can access 16 MB memory locations. The features of 80286 over 8088/8086 are:

(a) The 80286 processor includes memory management hardware
(b) It supports protected mode.

5.3.1 Internal Blocks and Signals

Internal blocks

The internal structure of 80286 has four functional units that are called as, (i) bus interface unit, (BIU) (ii) instruction unit, (IU) (iii) execution unit, (EU), and (iv) address unit, (AU). Figure 5.2 shows the internal blocks and the signals of the 80286 microprocessor. The bus

5.3.2 Modes of Operation

The 80286 can operate in real and protected modes.

Real mode

In real mode, the operation is exactly the same as that of 8088 and 8086 microprocessors. The microprocessor accesses only 1 MB of physical memory and locates the interrupt vector table in first 1 K memory space as in 8088/8086 systems. A few more interrupts are predefined for 80286 to handle some error conditions during the execution of an instruction that are called as *exceptions*.

Protected mode

The 80286 microprocessor has 24-bit address bus and hence, it can address 16 MB (2^{24}) physical memory space. In 286 protected mode, a descriptor stores the 24-bit base address (the starting location), the 16-bit limit (the length), and the access-rights of a segment. The memory management unit computes the physical address of a memory location by adding the 24-bit segment base from the descriptor pointed to by a selector in a segment register, and the 16-bit offset provided by the instruction.

Since a segment base is specified by a 24-bit address, a segment may begin at any location in the 16 MB memory space and since the length of the segment is indicated by a 16-bit limit, the size of the segment may vary between 1 byte and 64 KB. The 16 K descriptors in descriptor tables hold the base addresses of 16 K segments. It means that a program can access the maximum of 16 K segments of each 64 KB in length or, 1 GB of memory (16 K × 64 KB). Though, the 80286 processor can have the maximum of 16 MB physical memory space, it can access 1 GB memory space. The 1 GB memory space is called as *virtual memory*. Hence, it can address 16 MB of physical memory and 1 GB of virtual memory. The integrated MMU manages virtual memory. The 80286 MMU also provides protection for multitasking.

Example 5.1

Hence, it can address 16 MB of physical memory and 1 GB of virtual memory. The integrated MMU manages virtual memory. The 80286 MMU also provides protection for multitasking.

Example 5.1

(a) Determine the physical address of the memory location accessed in 80286 real mode, if (i) DS = 2000H, SI = 1234H, and (ii) ES = 3000H, DI = AAAAH.

(b) Determine the physical addresses of the starting and ending memory locations of the segment in 80286 protected mode, if the descriptor (pointed to by the selector in a segment register) holds A00000H for the base address and 0FFFH for the limit of the segment.

Solution

(a) The physical addresses of the memory locations in real mode are:

(i) (2000H × 16) + 1234H = 21234H

(ii) (3000H × 16) + AAAAH = 3AAAAH

(b) The physical address of

(i) the starting memory location of the segment is A00000H + 0000H = A00000H

(ii) the ending memory location of the segment is A00000H + 0FFFH = A00FFFH

Example 5.2

If DS contains 0020H in protected mode, determine the descriptor table and the descriptor it refers.

Solution

Since, the D15-D3 bits are '0000000000100' and the D2 bit is '0' the content of DS refers to the 4th descriptor in global descriptor table.

Mode switching

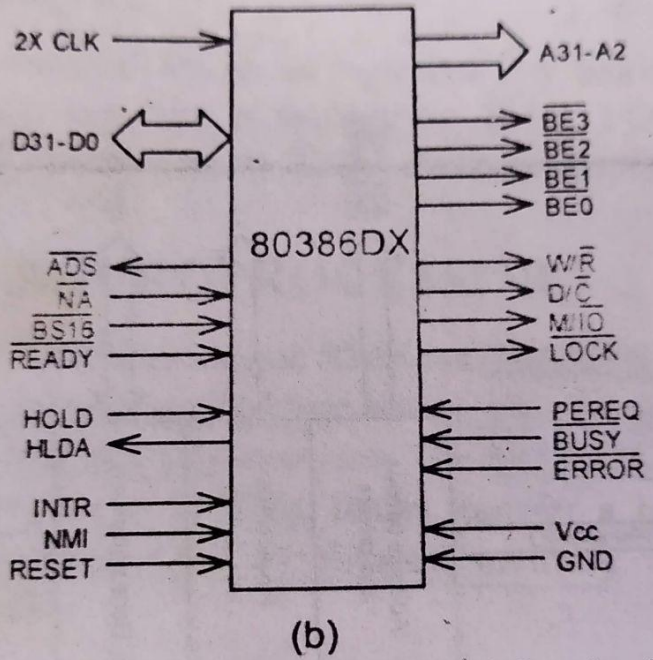
The 286 has a 16-bit Machine Status Word (MSW) register. The processor is switched to protected mode by setting the protection enable PE bit of the MSW. The 286 provides an instruction Load Machine Status Word (LMSW) to load the MSW register from a register or a memory location and allows setting or resetting of the PE bit. However, the 286 can be switched back to the real mode only by resetting the system.

bank is enabled by A0 and low bank is enabled by BHE. I/O for the 80286 system is also similar to 8086. An 80286 system uses an 82284 clock-generator, and an 82288 bus-controller.

5.4 THE 80386 MICROPROCESSOR

There are two versions of 80386 processor. They are 80386SX and 80386DX. The 80386SX microprocessor has 32-bit internal architecture but 16-bit external data bus and 24-bit address bus. It can access only 16 MB memory locations. The 80386DX processor has 32-bit data bus, 32-bit address bus and operates at 33 MHz. It can transfer a byte, a word or a double word in one bus cycle. It can access 4 GB of physical memory. The 80386 processor has the following features over 80286:

(a) It has 32-bit internal registers and 32-bit arithmetic and logic unit.
(b) It has 16-byte instruction queue.
(c) It supports multitasking.
(d) It supports virtual real mode in which multiple real mode applications run simultaneously under a multitasking operating system.
(e) The 80386 supports external cache called Level-2 cache (L2), for improving memory access. Cache is a high-speed memory (usually SRAM) used in between the processor and the DRAM in the system. The size of a L2 cache memory in 386 systems may be 32 K or 64 K.



(b)

Figure 5.3 The 80386DX microprocessor—(a) functional blocks, (b) signals.

- **A31-A2, and $\overline{\text{BE3}}$-$\overline{\text{BE0}}$.** The 30 Address lines and the four Byte Enable lines form the address bus for the 386 based system.
- **D31-D0.** The 32-bit Data bus.

- **A31-A2, and $\overline{BE3}$-$\overline{BE0}$**. The 30 Address lines and the four Byte Enable lines form the address bus for the 386 based system.
- **D31-D0**. The 32-bit Data bus.
- **W/$\overline{R}$**. The signal differentiates the Write and Read operations.
- **D/$\overline{C}$**. The Data or Control signal differentiates the data read/write and op-code fetch operations.
- **M/$\overline{IO}$**. The Memory or I/O signal differentiates the memory and I/O accesses.
- **$\overline{LOCK}$**. The Lock output signal is used during DMA operation.
- **$\overline{ADS}$**. The Address Data Strobe signal indicates that valid address and control signals are present on the bus.
- **$\overline{NA}$**. The Next Address input is used to instruct the processor to output the address of the next instruction in the current cycle.
- **$\overline{BS16}$**. The Bus Size input allows the processor to use the data bus for 16-bit or 32-bit data transfer.
- **$\overline{READY}$**. The Ready signal is used to insert wait states while accessing slow memory or I/O devices.
- **HOLD, HLDA, INTR, NMI, and RESET**. The signals perform the same functions as they do in 808286 and 8086 processors.
- **PEREQ, $\overline{BUSY}$, and $\overline{ERROR}$**. Co-processor in a system uses these signals.
- **CLK**. A Clock of frequency twice than that of the operating frequency of the processor is applied.

5.4.2 The Internal Registers

The internal registers of 80386 are shown in Figure 5.4(a). Follwing is their description.

General purpose registers

The general purpose registers and the instruction pointer are 32-bit wide and they are designated as **EAX, EBX, ECX, EDX, ESP, EBP, ESI, EDI, and EIP**. The registers can be accessed for

8-bit, 16-bit or 32-bit operations using their respective labels (for example, AH/AL for 8-bit, AX for 16-bit and EAX for 32-bit operations).

Flag register

The flag register of 386 is shown in Figure 5.4(b). It is also 32-bit wide and is designated as EFLAGS. It has all the flags of 286. In addition it has 4 more flags labelled as I/O privilege level (IOPL), nested task (NT), resume flag (RF), and virtual mode (VM). The IOPL flag uses two bits to provide the protection features. The 80386 executes I/O instructions only if the privilege level of the task is less than or equal to the IOPL. The NT flag controls IRET operations to return from normal interrupt or to return from interrupt via task switching. If RF is set, the 80386 ignores debug faults, if reset the 80386 generates debug exception. The VM flag is set to execute real mode programs. If the bit is reset, the processor operates in protected mode.

Segment registers

The 386 has six 16-bit segment registers, designated as CS, DS, ES, SS, FS, and GS. The FS and GS are the two additional data segment registers. The four data segment registers permit the programs to access different types of data in four different areas of memory.

... table registers

... registers labelled as, GDTR,

the programs to access different types of data in four different areas of memory.

Descriptor table registers

The 386 also contains global, local, and interrupt descriptor table registers labelled as, GDTR, LDTR, and IDTR respectively. The GDTR holds the base address of the global descriptor table and the limit. The LDTR holds the base address and the limit of the local descriptor table for the task currently being executed. The IDTR holds the base address and limit of interrupt descriptor table. The interrupt descriptor table holds the 256 interrupt-levels. The special feature of the interrupt descriptor table is that it can be located any where in memory. In real mode, the interrupt vector table is located in the first 1 K space of memory. The descriptor table registers are program invisible.

The 80386 has a Task Register (TR). The TR holds the selector for Task State Segment descriptor for the currently executing task.

Control, debug and test registers

The special feature of 386 compared with the earlier microprocessors is that it has three control (CR3, CR2, and CR0) registers, eight debug (DR7-DR0) registers, and two test (TR7-TR6) registers. All of these registers are 32-bit wide. The LSB 16-bits of CR0 is the same as the MSW register of 286.

processor starts execution from the location FFFFFFF0H.

5.5 THE 80486 MICROPROCESSOR

There are four versions of 80486 microprocessor. They are 486SX, 486DX, 486DX2, and 486DX4. The 486DX has 32-bit address bus, 32-bit internal architecture, and 32-bit data bus. The 486DX2 operates at 66 MHz and the 486DX4 operates at 100 MHz. The 486 also transfers a byte, word or double word in one bus cycle. In protected mode, the 486 can address 4 GB of physical memory in the address range from 00000000H to FFFFFFFFH and 64 TB of virtual memory. It offers paging and task switching. It also supports virtual real mode. Features of 486 over 386 are:

(a) The 486 has a parity checker/generator. Parity is generated and stored in a memory during each memory write operation and tested during memory read operation.

(b) The 486 has an 8 KB Level-I (L1) cache. The cache memory stores code and data used by program. The internal cache works with an 8 KB built-in SRAM.

(c) It has built-in math coprocessor.

(d) It has reduced instruction execution time. The 486 takes an average of only two clock cycles for executing an instruction whereas the 386 takes an average of 4 clock cycles.

(e) Burst-mode memory cycle. A normal 32-bit memory transfer takes place in 2 clock cycles. The burst-mode memory cycle transfers the first 32-bit data in two clock cycles and the subsequent three 32-bit data in just three clock cycles.

(f) Built-In-Self-Test, (BIST). It tests the microprocessor, coprocessor, and cache at reset time.

5.5 THE 80486 MICROPROCESSOR

There are four versions of 80486 microprocessor. They are 486SX, 486DX, 486DX2, and 486DX4. The 486DX has 32-bit address bus, 32-bit internal architecture, and 32-bit data bus. The 486DX2 operates at 66 MHz and the 486DX4 operates at 100 MHz. The 486 also transfers a byte, word or double word in one bus cycle. In protected mode, the 486 can address 4 GB of physical memory in the address range from 00000000H to FFFFFFFFH and 64 TB of virtual memory. It offers paging and task switching. It also supports virtual real mode. Features of 486 over 386 are:

(a) The 486 has a parity checker/generator. Parity is generated and stored in a memory during each memory write operation and tested during memory read operation.
(b) The 486 has an 8 KB Level-I (L1) cache. The cache memory stores code and data used by program. The internal cache works with an 8 KB built-in SRAM.
(c) It has built-in math coprocessor.
(d) It has reduced instruction execution time. The 486 takes an average of only two clock cycles for executing an instruction whereas the 386 takes an average of 4 clock cycles.
(e) Burst-mode memory cycle. A normal 32-bit memory transfer takes place in 2 clock cycles. The burst-mode memory cycle transfers the first 32-bit data in two clock cycles and the subsequent three 32-bit data in just three clock cycles.
(f) Built-In-Self-Test, (BIST). It tests the microprocessor, coprocessor, and cache at reset time.

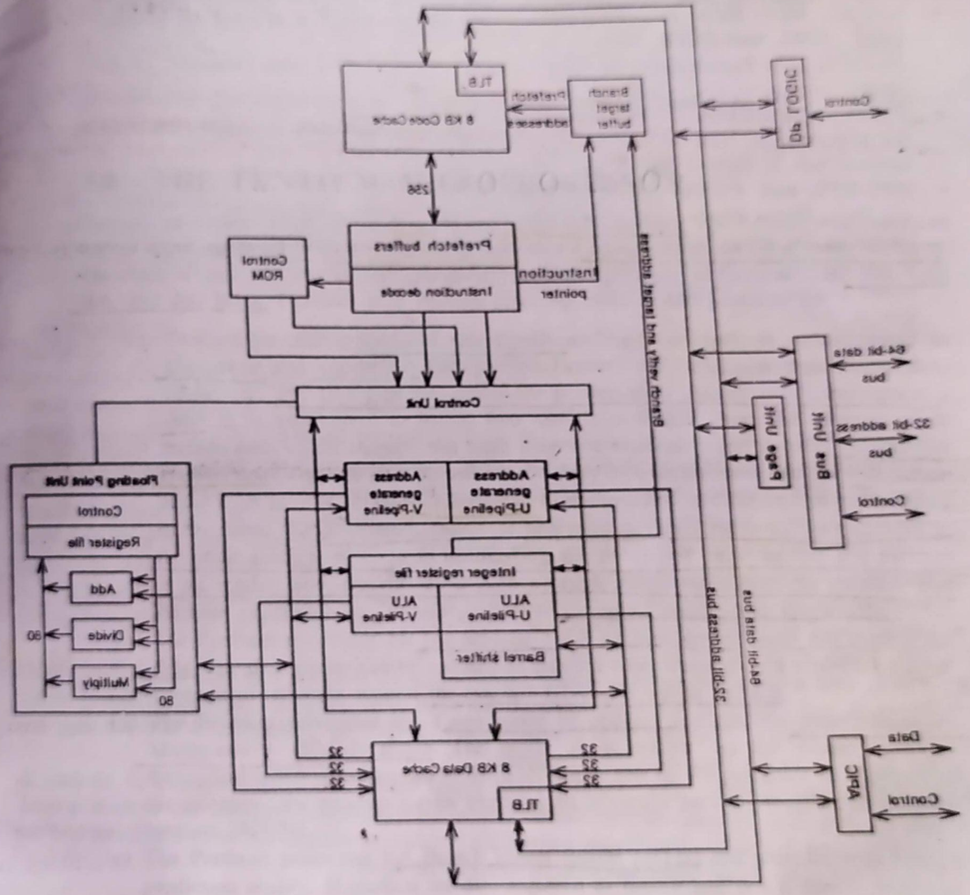


Figure 5.8 Internal blocks of Pentium processor.

5.6 THE PENTIUM MICROPROCESSOR

Pentium processors have 64-bit data bus and 32-bit address bus. The Pentium processors can access a maximum of 4 GB of physical memory and a maximum of 64 TB of virtual memory. There are several versions of Pentium microprocessors operating at frequencies 66, 100, 133, 166, and 200 MHz. Features of a Pentium processor over a 486 processor are:

(a) Pentium processor has dual data pipelines. The two pipelines are designated as U-pipeline and V-pipeline. Each pipeline has its own ALU, address generators, data cache, etc. The two pipelines enable the processor to execute two instructions at a time. It is equivalent to having two 486 on a single chip. The microprocessor architecture which incorporates more than one execution unit is called *superscalar architecture*. The use of superscalar technology to execute more than one instruction at the same time is called *multithreading*. Multithreading is different from multitasking in the sense that in multithreading the processor actually performs two processes at the same instant, whereas in multitasking the processor performs only one process at an instant and presents an illusion of performing more than one process. The Pentium processor has another pipeline to execute floating-point instructions.

(b) The Pentium processor has two separate 8 KB caches, one for code and another for data. The data cache can be operated as either a write-through or a write-back cache.

(c) Pentium processors support the external L2 cache up to 512 KB.

(d) The Pentium processor has a new mode of operation called the System Memory Management (SMM) mode. The mode is accessed via the system memory management interrupt applied to the SMI input pin to the processor. In response to the interrupt, the microprocessor executes an interrupt service procedure at memory location 38000H.

(e) The Pentium processor has Branch Target Buffer (BTB) and provided with branch prediction ability. It predicts the data required in future and gets it from memory or hard disk and keeps ready in a prefetch buffer. It enables the processor to keep both pipelines operating at full speed.

(f) The paging unit of Pentium allows 4 MB pages instead of 4 KB pages.

(g) It includes on-board power management features.

(h) The Pentium processor also has built-in math co-processor.

also similar to the I/O for the systems based on earlier processors.

5.9 THE PENTIUM-II MICROPROCESSOR

Pentium-Pro processor with MMX features is designated as Pentium-II processor. It has two integer pipelines, one floating-point pipeline and one MMX pipeline. Different versions of Pentium-II processors, operating at 233, 266, 300, 333, 350, 400 and 450 MHz clock speeds are available. The processors are widely used in desktops, workstations, and servers. It has 36-bit address bus and can address 64 GB of physical memory and 64 TB of virtual memory. It has two 16 KB non-blocking L1 caches and one 512 KB non-blocking L2 cache. The non-blocking basically refers to allowing subsequent operations even if the previous operation is not fully completed. The L1 cache provides fast access to data. The L2 cache supports memory cacheability for up to 4 GB of addressable memory space. The processor includes Error Correction Code (ECC), Fault Analysis, Recovery, and Functional Redundancy Checking for both system and L2 Cache buses.

Dual Independent Bus (DIB) architecture of the Pentium-II processor increases the bandwidth and the performance over the single-bus processors. The 350, 400 and 450 MHz versions increase the system bus speed from 66 MHz to 100 MHz.

The features of Pentium-II processors are:

The microarchitecture dynamic execution technology

Multiple branch prediction. Predicts program execution through several branches, accelerating the flow of work to the processor.