SYSC3601
Microprocessor Systems

Unit 2a:
The Intel x86 Protected Mode
1. Protected Mode (Ch 2.3)
Protected Mode

• The Windows operating system domain.
• 4G of memory with 2G for the system and 2G for the application.
• Protected mode still uses segment and offset addresses, but the offset address is 32-bits.
• Protection is provided by restricting access through priority levels and access rights.
Descriptors Describe Memory

• A descriptor is selected by the number placed in the segment register.
• The descriptor describes the base address (starting address) and limit (offset to the ending address) of a segment.
• The descriptor also defines the privilege level and access rights to a memory segment.
### Descriptor Table Entry Format

#### 80286 descriptor

<table>
<thead>
<tr>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

- **Access rights**
- **Base** (B23–B16)
- **Base** (B15–B0)
- **Limit** (L15–L0)

#### 80386 through Pentium 4 descriptor

<table>
<thead>
<tr>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base (B31–B24)</td>
<td>G</td>
<td>D</td>
<td>O</td>
<td>A</td>
<td>V</td>
<td>Limit (L19–L16)</td>
</tr>
<tr>
<td>Access rights</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base (B23–B16)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Base (B15–B0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limit (L15–L0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Descriptor Table Entry Format

• The base address is a 32-bit address (Pentium class) that addresses the start of a memory segment.
• The limit is a 20-bit number added to the base address to address the last address of a segment.
• The limit has a modifier bit called Granularity (G) that select a multiplier of 4K for the limit (4K is 12-bits) (20-bits +12-bits is 32-bits)
Descriptor Table Entry Example

- base = 23000000H and a limit of 012FFH

G = 0 (limit = 000012FFH)
Segment start = 23000000H
Segment end = 230012FFH

G = 1  (limit = 012FFFFFFH)
Segment start = 23000000H
Segment end = 242FFFFFFFH
Access Rights

A = 0  Segment not accessed
A = 1  Segment has been accessed

E = 0  Descriptor describes a data segment
ED = 0  Segment expands upward (data segment)
ED = 1  Segment expands downward (stack segment)
W = 0  Data may not be written
W = 1  Data may be written

E = 1  Descriptor describes code segment
C = 0  Ignore descriptor privilege level
C = 1  Abide by privilege level
R = 0  Code segment may not be read
R = 1  Code segment may be read

S = 0  System descriptor
S = 1  Code or data segment descriptor
DLP = Sets the descriptor privilege level

P = 0  Descriptor is undefined
P = 1  Segment contains a valid base and limit

Note: Some of the letters used to describe the bits in the access rights bytes vary in Intel documentation.
Segment Register

RPL = Requested privilege level where 00 is the highest and 11 is the lowest

TI = 0  Global descriptor table
TI = 1  Local descriptor table

Selects one descriptor from 8192 descriptors in either the global or the local descriptor table
Segment Register Example

Global descriptor table

Descriptor 1

Memory system

Data segment
Program Invisible Registers

<table>
<thead>
<tr>
<th>Segment registers</th>
<th>Descriptor cache</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS</td>
<td>Base address</td>
</tr>
<tr>
<td>DS</td>
<td>Limit</td>
</tr>
<tr>
<td>ES</td>
<td>Access</td>
</tr>
<tr>
<td>SS</td>
<td></td>
</tr>
<tr>
<td>FS</td>
<td></td>
</tr>
<tr>
<td>GS</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TR</th>
<th>Base address</th>
<th>Limit</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDTR</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Descriptor table addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDTR</td>
</tr>
<tr>
<td>IDTR</td>
</tr>
</tbody>
</table>

Notes:
1. The 80286 does not contain FS and GS nor the program-invisible portions of these registers.
2. The 80286 contains a base address that is 24-bits and a limit that is 16-bits.
3. The 80386/80486/Pentium/Pentium Pro contain a base address that is 32-bits and a limit that is 20-bits.
4. The access rights are 8-bits in the 80286 and 12-bits in the 80386/80486/Pentium.
Control Registers

CR4: Pentium, Pentium Pro, Pentium II, Pentium III, and Pentium 4 only

CR3

CR2

CR1

CR0

Page directory base address

Page fault linear address

Reserved

MCE

PSE

PE

PF

PWT

PCDT

TS

SVME

RSVT

I
Paging

• The paging mechanism translates a logic address (address generated by the program) into a physical address (address that accesses a memory location).

• It does this by sectioning the address into three parts: (1) directory, (2) page table, and (3) memory offset.

• The directory and page table fields are each 10-bits wide and the memory offset is 12-bits.