Processes

Dr. Ailbhe Gill

Textbook: Operating Systems: Internals and Design Principles, 9th Edition by William Stallings

Today's Lecture

- What is a process?
- Process states
- Process description
- Process control
- Execution of the operating system
- UNIX SVR4 process management

Learning Objectives

After studying this chapter, you should be able to:

- Define the term process and explain the relationship between processes and process control blocks.
- Explain the concept of a process state and discuss the state transitions the processes undergo.
- List and describe the purpose of the data structures and data structure elements used by an OS to manage processes.
- Assess the requirements for process control by the OS.
- Understand the issues involved in the execution of OS code.
- Describe the process management scheme for UNIX SVR4.

What Is a Process?

OS Management of Application Execution

Why is it important to manage application execution effectively?

- Resources are made available to multiple applications
- The processor is switched among multiple applications so all will appear to be progressing
- The processor and I/O devices must be used efficiently to do this.

Process Elements

Two essential elements of a process are:

Two essential elements of a process are:

1. Program code

   Which may be shared with other processes that are executing the same program

2. A set of data associated with that code

When the processor begins to execute the program code, we refer to this executing entity as a process

Process Control Block

- Contains the process elements which uniquely characterize a process.
- Makes it possible to interrupt a running process and later resume execution as if the interruption had not occurred
- Created and managed by the operating system
- Key tool that allows support for multiple processes

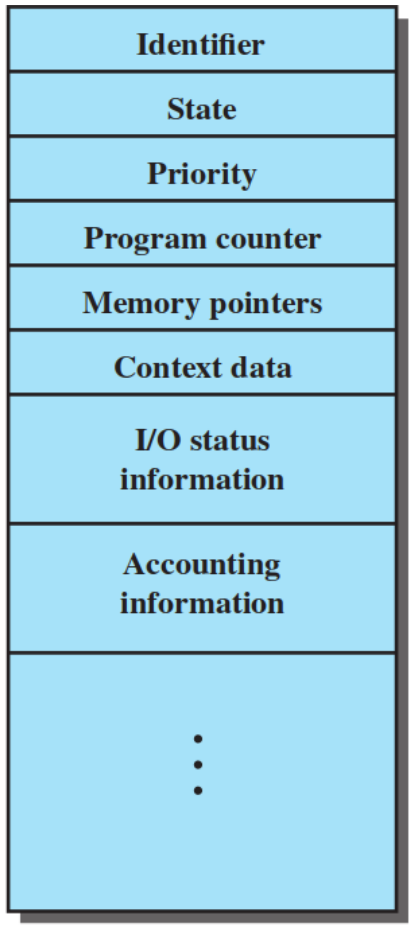


Figure 1: Simplified Process Control Block

Process States

Trace

Lists the sequence of instructions that execute for that process.

The behavior of the processor can be characterized by showing how the traces of the various processes are interleaved.

Dispatcher

Small program that switches the processor from one process to another

Traces of Processes

(a) Trace of Process A	(b) Trace of Process B	(c) Trace of Process C
5000	8000	12000
5001	8001	12001
5002	8002	12002
5003	8003	12003
5004		12004
5005		12005
5006		12006
5007		12007
5008		12008
5009		12009
5010		12010
5011		12011

5000 = Starting address of program of Process A
8000 = Starting address of program of Process B
12000 = Starting address of program of Process C

Figure 2: Traces of Processes

Combined Trace of Processes

Example

Let us view these traces from the processor's point of view.
The figure on the next slide shows the interleaved traces resulting from the first 52 instruction cycles (for convenience, the instruction cycles are numbered).
The shaded areas represent code executed by the dispatcher.
The same sequence of instructions is executed by the dispatcher in each instance because the same functionality of the dispatcher is being executed.
We assume that the OS only allows a process to continue execution for a maximum of six instruction cycles, after which it is interrupted; this prevents any single process from monopolizing processor time.

Combined Trace of Processes

1	5000
2	5001
3	5002
4	5003
5	5004
6	5005
----------	Timeout
7	100
8	101
9	102
10	103
11	104
12	105
13	8000
14	8001
15	8002
16	8003
----------	I/O Request
17	100
18	101
19	102
20	103
21	104
22	105
23	12000
24	12001
25	12002
26	12003
27	12004
28	12005
----------	Timeout
29	100
30	101
31	102
32	103
33	104
34	105
35	5006
36	5007
37	5008
38	5009
39	5010
40	5011
----------	Timeout
41	100
42	101
43	102
44	103
45	104
46	105
47	12006
48	12007
49	12008
50	12009
51	12010
52	12011
----------	Timeout

100 = Starting address of dispatcher program

Shaded areas indicate execution of dispatcher process;
first and third columns count instruction cycles;
second and fourth columns show address of instruction being executed

Figure 3: Combined Trace of Processes

Process Execution

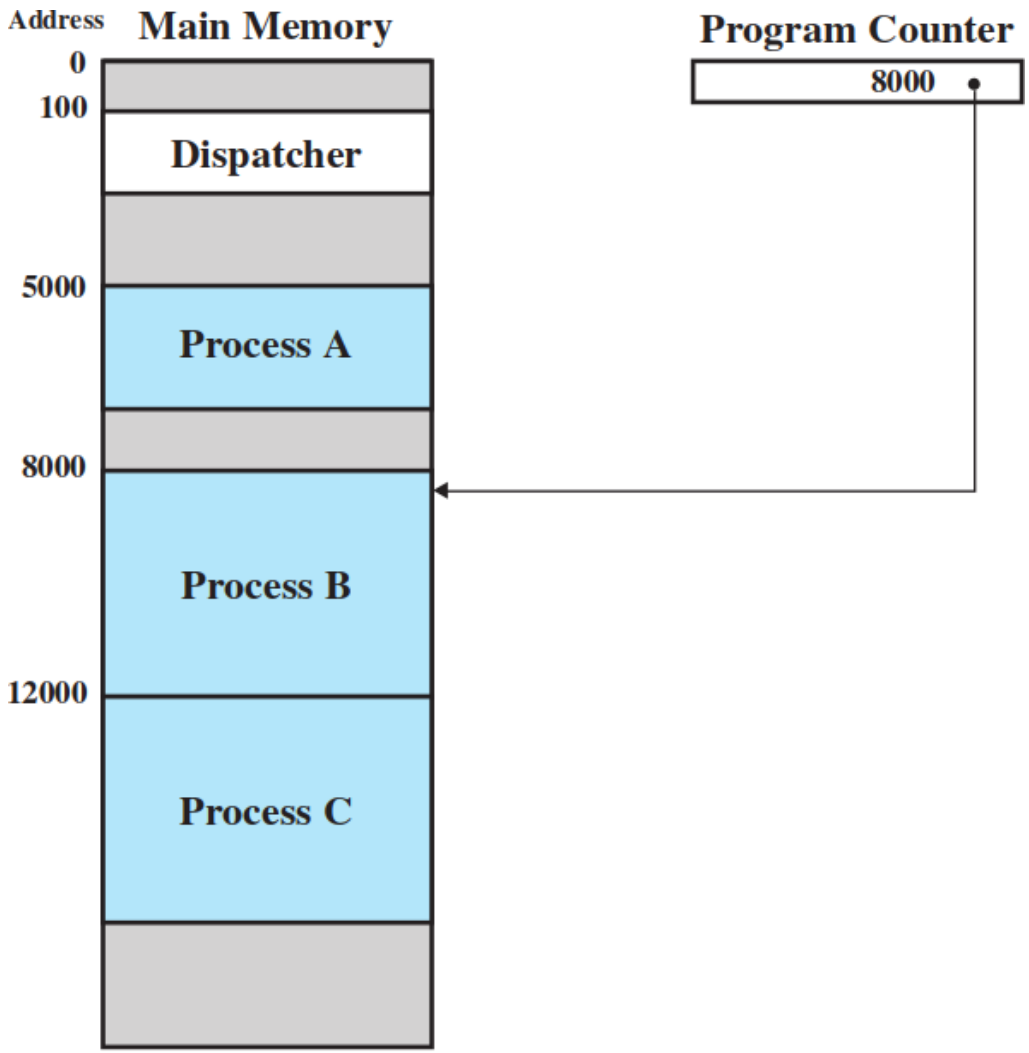


Figure 4: Snapshot of Example Execution at Instruction Cycle 13 (Fig. 3)

Process States

Two-State Process Model

- The first step in designing an OS to control processes is to describe the behavior that we would like the processes to exhibit.
- We can construct the simplest possible model by observing that, at any time, a process is either being executed by a processor or not.
- In this model, a process may be in one of two states: **Running or Not Running**

Two-State Process Model

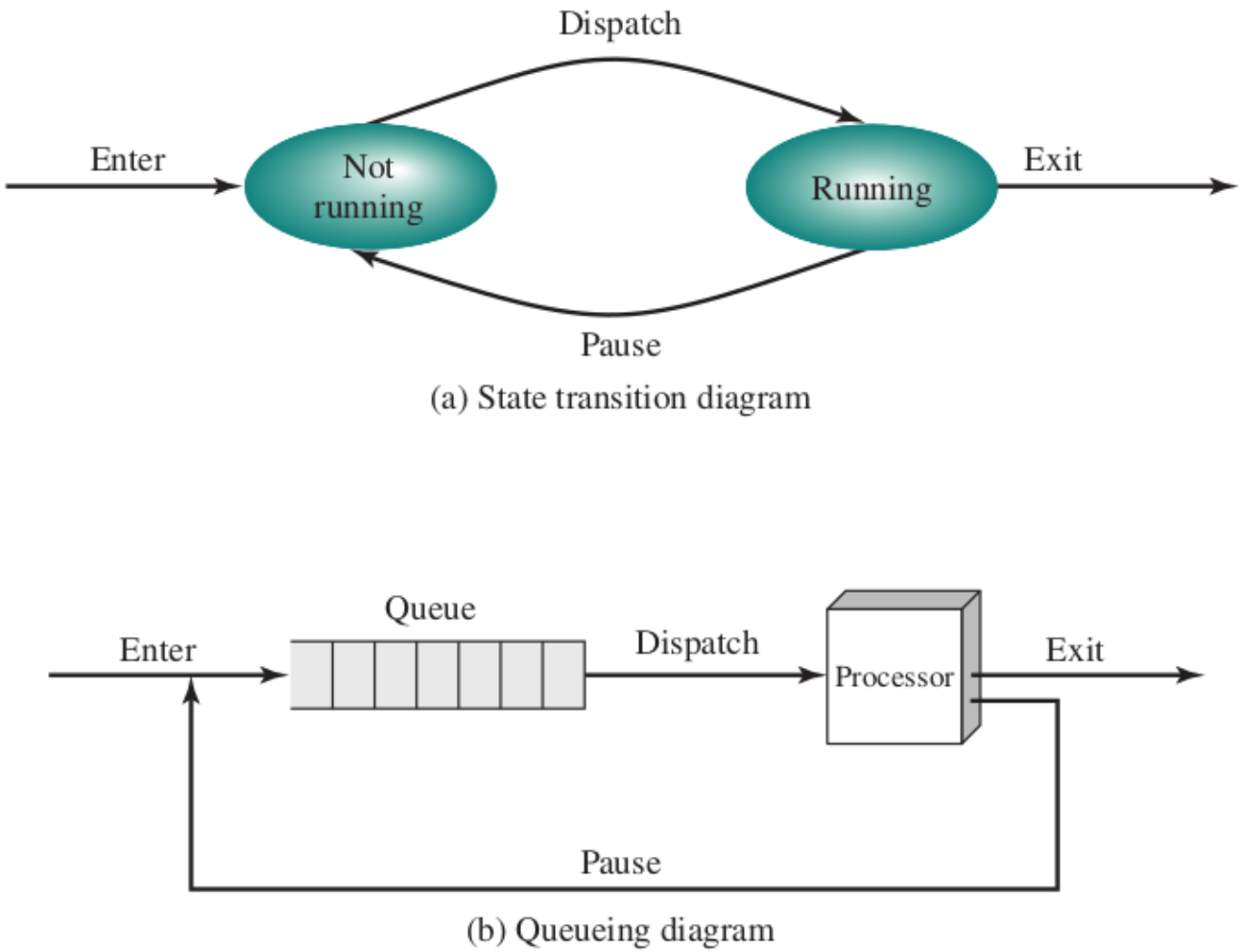


Figure 5: Two-State Process Model

Reasons for Process Creation

Table 3.1 Reasons for Process Creation

New batch job	The OS is provided with a batch job control stream, usually on tape or disk. When the OS is prepared to take on new work, it will read the next sequence of job control commands.
Interactive log-on	A user at a terminal logs on to the system.
Created by OS to provide a service	The OS can create a process to perform a function on behalf of a user program, without the user having to wait (e.g., a process to control printing).
Spawned by existing process	For purposes of modularity or to exploit parallelism, a user program can dictate the creation of a number of processes.

Process Creation

Process spawning

When the OS creates a process at the explicit request of another process

Parent process

Is the original, creating, process

Child process

Is the new process

Reasons for Process Termination

Table 3.2 Reasons for Process Termination

Normal completion	The process executes an OS service call to indicate that it has completed running.
Time limit exceeded	The process has run longer than the specified total time limit. There are a number of possibilities for the type of time that is measured. These include total elapsed time ("wall clock time"), amount of time spent executing, and, in the case of an interactive process, the amount of time since the user last provided any input.
Memory unavailable	The process requires more memory than the system can provide.
Bounds violation	The process tries to access a memory location that it is not allowed to access.
Protection error	The process attempts to use a resource such as a file that it is not allowed to use, or it tries to use it in an improper fashion, such as writing to a read-only file.
Arithmetic error	The process tries a prohibited computation (such as division by zero) or tries to store numbers larger than the hardware can accommodate.
Time overrun	The process has waited longer than a specified maximum for a certain event to occur.
I/O failure	An error occurs during input or output, such as inability to find a file, failure to read or write after a specified maximum number of tries (when, for example, a defective area is encountered on a tape), or invalid operation (such as reading from the line printer).
Invalid instruction	The process attempts to execute a nonexistent instruction (often a result of branching into a data area and attempting to execute the data).
Privileged instruction	The process attempts to use an instruction reserved for the operating system.
Data misuse	A piece of data is of the wrong type or is not initialized.
Operator or OS intervention	For some reason, the operator or the operating system has terminated the process (e.g., if a deadlock exists).
Parent termination	When a parent terminates, the operating system may automatically terminate all of the offspring of that parent.
Parent request	A parent process typically has the authority to terminate any of its offspring.

Process Termination

- There must be a means for a process to indicate its completion
- A batch job should include a HALT instruction or an explicit OS service call for termination
- For an interactive application, the action of the user will indicate when the process is completed (e.g., log off, quitting an application)

Five-State Process Model

- If all processes were always ready to execute, then the queuing discipline suggested by Fig. 5(b) would be effective.
- The queue is a first-in-first-out list and the processor operates in round-robin fashion on the available processes (each process in the queue is given a certain amount of time, in turn, to execute and then returned to the queue, unless blocked).
- However, even with the simple example that we have described, this implementation is inadequate: Some processes in the Not Running state are ready to execute, while others are blocked, waiting for an I/O operation to complete.
- Thus, using a single queue, the dispatcher could not just select the process at the oldest end of the queue.
- Rather, the dispatcher would have to scan the list looking for the process that is not blocked and that has been in the queue the longest.
- A more natural way to handle this situation is to split the Not Running state into two states: **Ready and Blocked**

Five-State Process Model

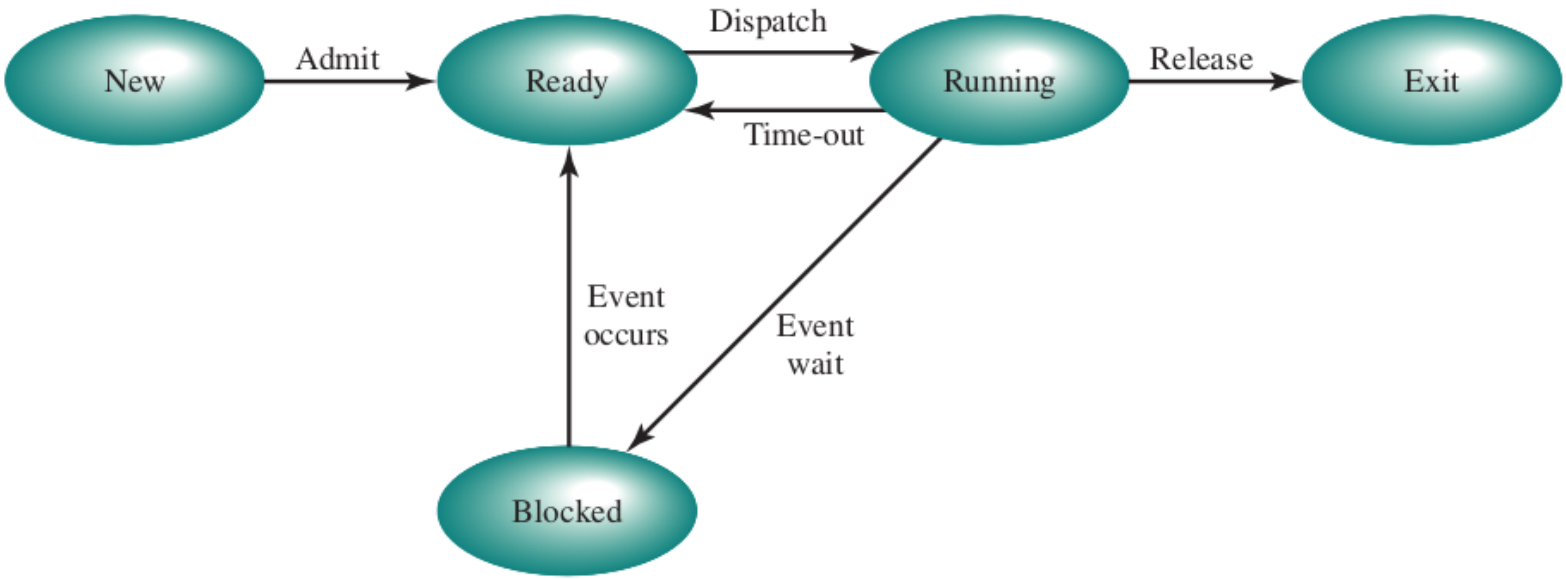


Figure 6: Five-State Process Model

Process States for Trace

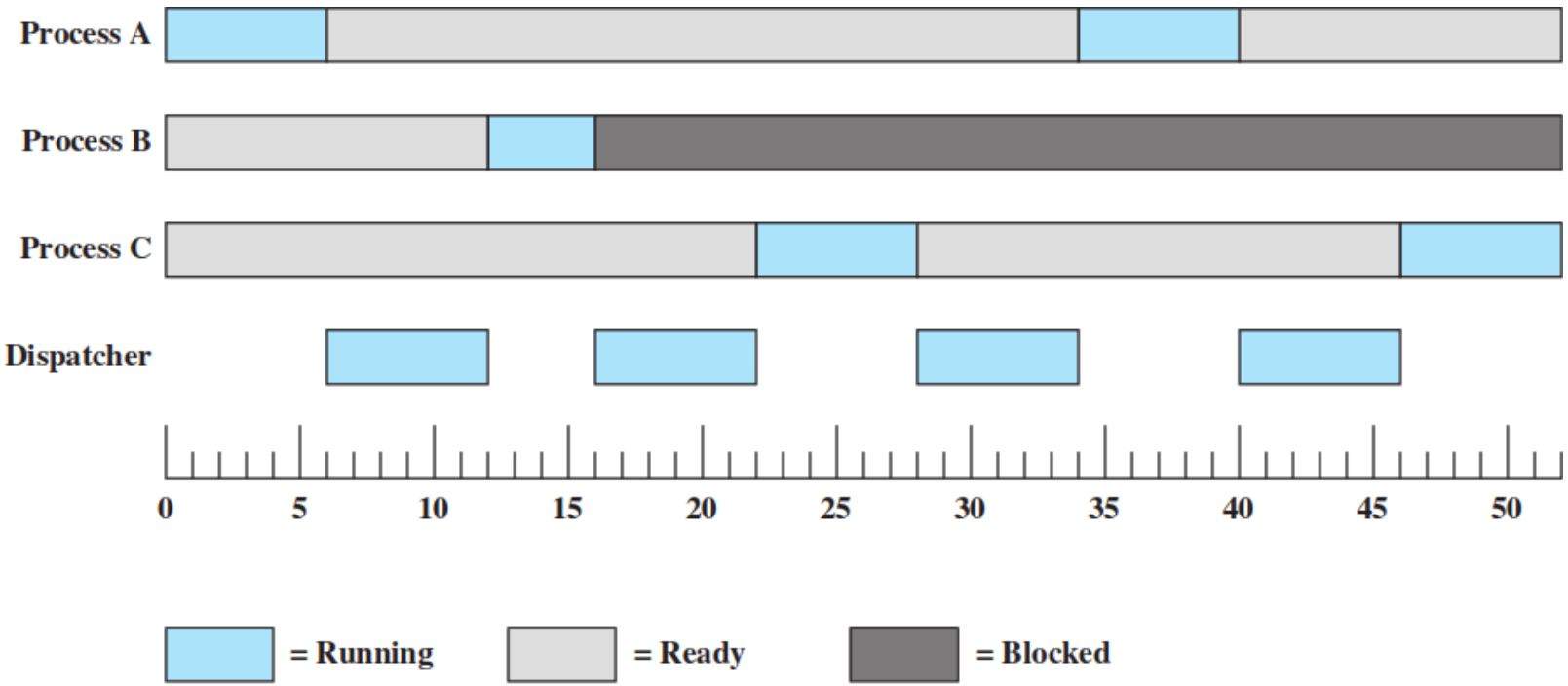


Figure 7: Process States for Trace

Queuing Model for Process State Transition Diagram with Suspend States

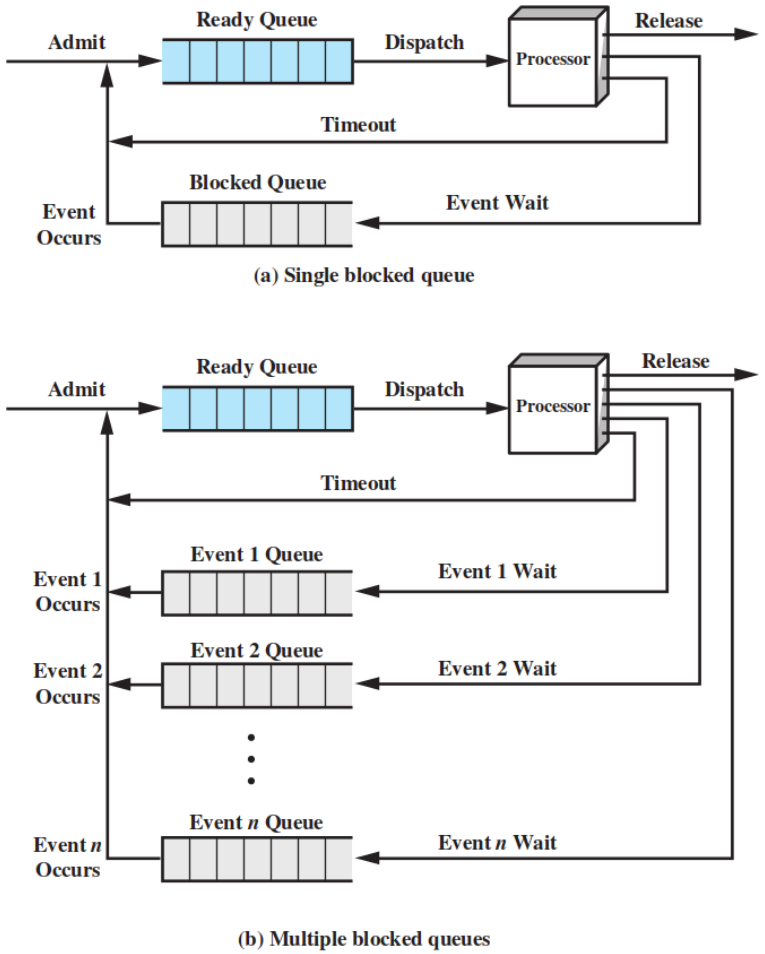


Figure 8: Queuing Model for Process State Transition Diagram with Suspend States

Reasons for Process Suspension

Table 3.3 Reasons for Process Suspension

Swapping	The OS needs to release sufficient main memory to bring in a process that is ready to execute.
Other OS reason	The OS may suspend a background or utility process or a process that is suspected of causing a problem.
Interactive user request	A user may wish to suspend execution of a program for purposes of debugging or in connection with the use of a resource.
Timing	A process may be executed periodically (e.g., an accounting or system monitoring process) and may be suspended while waiting for the next time interval.
Parent process request	A parent process may wish to suspend execution of a descendent to examine or modify the suspended process, or to coordinate the activity of various descendants.

Suspended Processes

Swapping

Involves moving part of all of a process from main memory to disk

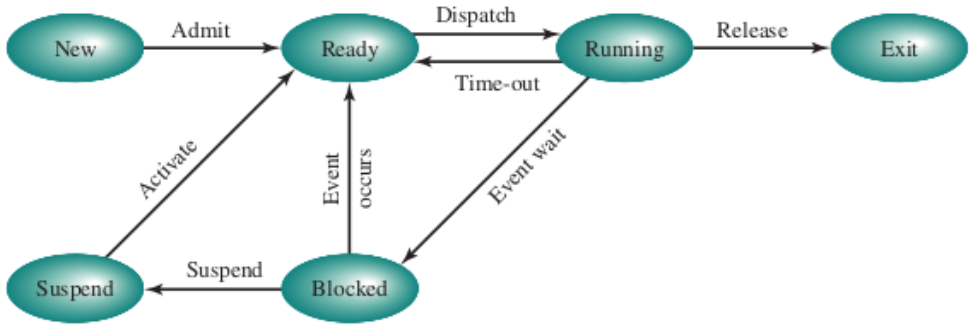
Because disk I/O is generally the fastest I/O on a system, swapping will usually enhance performance
However, swapping is also an I/O operation and therefore there is the potential for making the problem worse, not better.

Suspended Processes

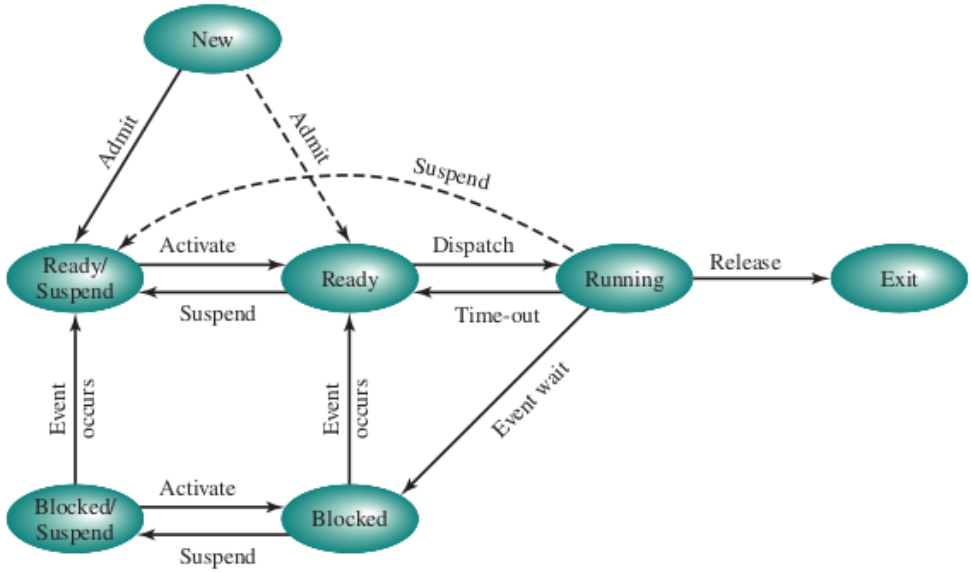
When none of the processes in main memory is in the Ready state, the OS **swaps** one of the blocked processes out on to disk into a **suspend queue**.

- The suspend queue is a queue of existing processes that have been temporarily kicked out of main memory, or suspended
- The OS then brings in another process from the suspend queue or it honors a new-process request
- Execution then continues with the newly arrived process

Process State Transition Diagram with Suspend States



(a) With one Suspend state



(b) With two Suspend states

Figure 9: Process State Transition Diagram with Suspend States

Characteristics of a Suspended Process

Characteristics of a Suspended Process

- The process is not immediately available for execution
- The process was placed in a suspended state by an agent: either itself, a parent process, or the OS, for the purpose of preventing its execution
- The process may or may not be waiting on an event
- The process may not be removed from this state until the agent explicitly orders the removal

Process Description

General Structure of Operating System Control Tables

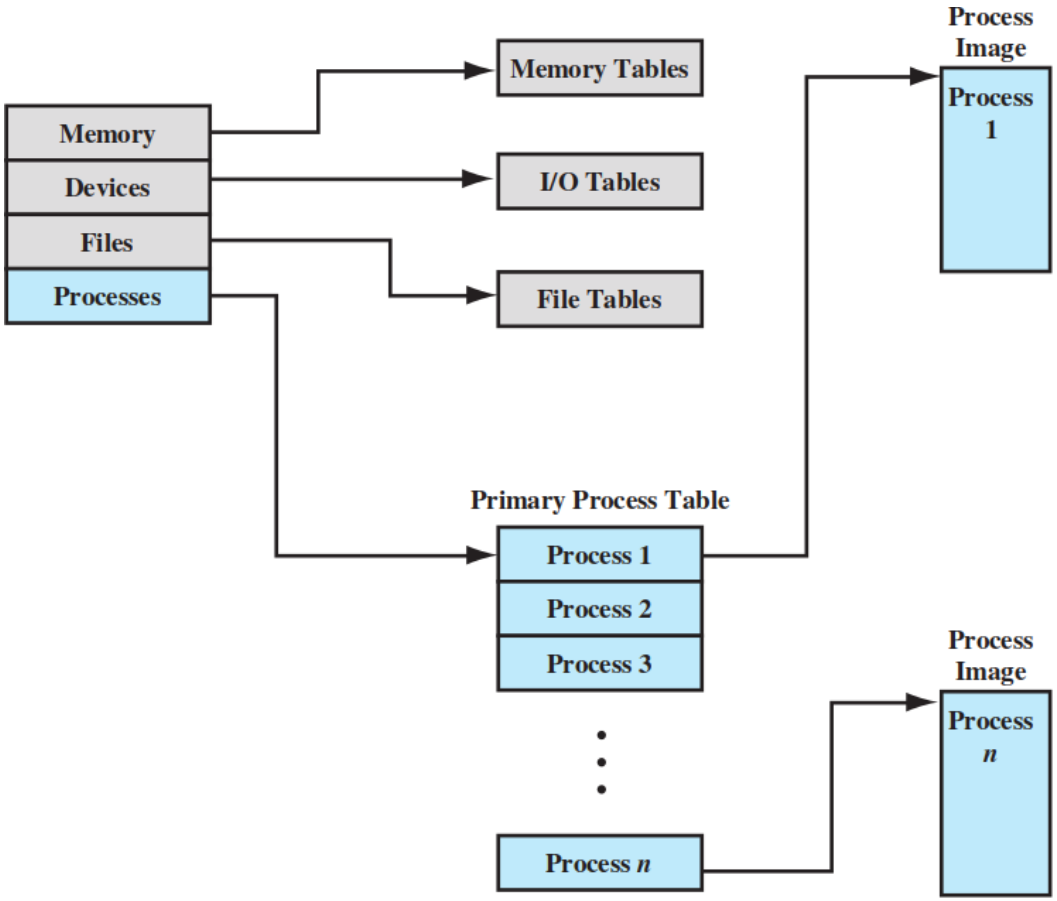


Figure 10: General Structure of Operating System Control Tables

Process Tables

- Must be maintained to manage processes
- There must be some reference to memory, I/O, and files, directly or indirectly
- The tables themselves must be accessible by the OS and therefore are subject to memory management

Process Control Structures

To manage and control a process the OS must know:

- The attributes of the process that are necessary for its management
- Where the process is located

Process Control Structures

Regarding **process attributes**

- Each process has associated with it a number of attributes that are used by the OS for process control

Process Image

The collection of program, data, stack, and attributes is referred to as the process image

Regarding **process location**

- A process must include a program or set of programs to be executed; A process will consist of at least sufficient memory to hold the programs and data of that process
- Process image location will depend on the memory management scheme being used

Typical Elements of a **Process Image**

1. **User Data**

   The modifiable part of the user space. May include program data, a user stack area, and programs that may be modified.

2. **User Program**

   The program to be executed.

3. **Stack**

   The execution of a program typically involves a **stack** that is used to keep track of procedure calls and parameter passing between procedures. So, each process has one or more stacks associated with it.

4. **Process Control Block**

   Data needed by the OS to control the process (see Table 3.5).

*stacks are last-in-first-out (LIFO) data structures

User Processes in Virtual Memory

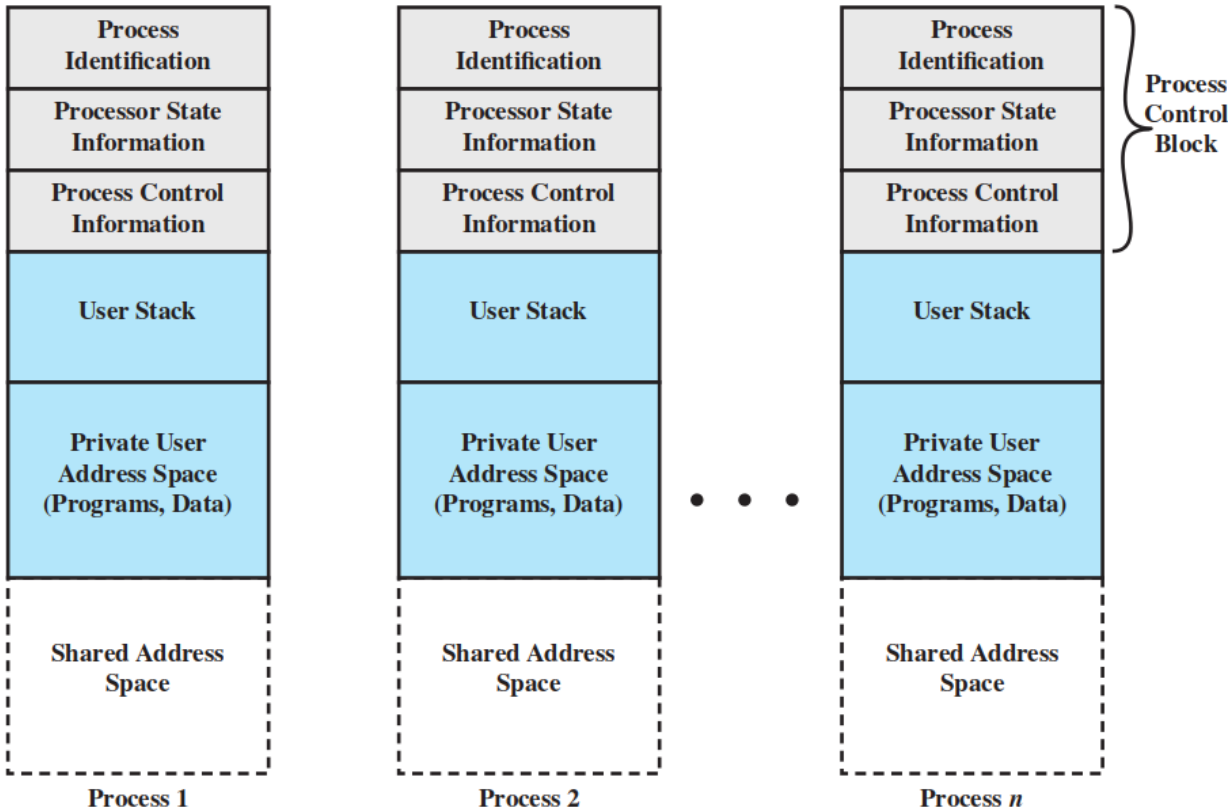


Figure 11: User Processes in Virtual Memory

Role of the Process Control Block

The most important data structure in an OS!

Process Control Block

- Contains all of the information about a process that is needed by the OS
- Blocks are read and/or modified by virtually every module in the OS
- Defines the state of the OS

Difficulty is not access, but protection:

- A bug in a single routine could damage process control blocks, which could destroy the system's ability to manage the affected processes
- A design change in the structure or semantics of the process control block could affect a number of modules in the OS

Typical Elements of a **Process Control Block**

1. **Processor State Information**
   Consists of the contents of processor registers. Typically, the register set will include:
   - User-visible registers: A user-visible register is one that may be referenced by means of the machine language that the processor executes while in user mode.
   - Control and status registers: These are a variety of processor registers that are employed to control the operation of the processor.
     E.g.
     - Program counter: Contains the address of the next instruction to be fetched
     - Condition codes: Result of the most recent arithmetic or logical operation (e.g., sign, zero, carry, equal, overflow)
     - Status information: Includes interrupt enabled/disabled flags, execution mode
   - Stack pointers: The stack pointer points to the top of the stack.

Typical Elements of a Process Control Block

2. **Process Identification** (using identifiers)
   Numeric identifiers that may be stored with the process control block include:
   - Identifier of this process
   - Identifier of the process that created this process (parent process)
   - User identifier
3. **Process Control Information**
   Scheduling and state information that is needed by the OS to control and coordinate the various active processes.
   E.g.
   - Process state: Defines the readiness of the process to be scheduled for execution (e.g., running, ready, waiting, halted).
   - Priority: One or more fields may be used to describe the scheduling priority of the process. In some systems, several values are required (e.g., default, current, highest-allowable).
   - Scheduling-related information: This will depend on the scheduling algorithm used. E.g. the amount of time that the process has been waiting.
   - Event: Identity of event the process is awaiting before it can be resumed.

Typical Elements of a Process Control Block

6. **Data Structuring**
   A process may be linked to other process in a queue, ring, or some other structure.
   E.g.
   - All processes in a waiting state for a particular priority level may be linked in a queue.
   - A process may exhibit a parent-child (creator-created) relationship with another process.
   - The process control block may contain pointers to other processes to support these structures.
7. **Interprocess Communication**
   Various flags, signals, and messages may be associated with communication between two independent processes.
   - Some or all of this information may be maintained in the process control block.

Typical Elements of a Process Control Block

8. **Process Privileges**
   Processes are granted privileges in terms of the memory that may be accessed and the types of instructions that may be executed.
   - In addition, privileges may apply to the use of system utilities and services.
9. **Memory Management**
   - This section may include pointers to segment and/or page tables that describe the virtual memory assigned to this process.
10. **Resource Ownership and Utilization**
    - Resources controlled by the process may be indicated, such as opened files.
    - A history of utilization of the processor or other resources may also be included; this information may be needed by the scheduler.

Processes and Resources

A snapshot of resource allocation to three processes P1, P2 and P3. Undashed lines indicate allocated resources, dashed lines indicate resources still needed.

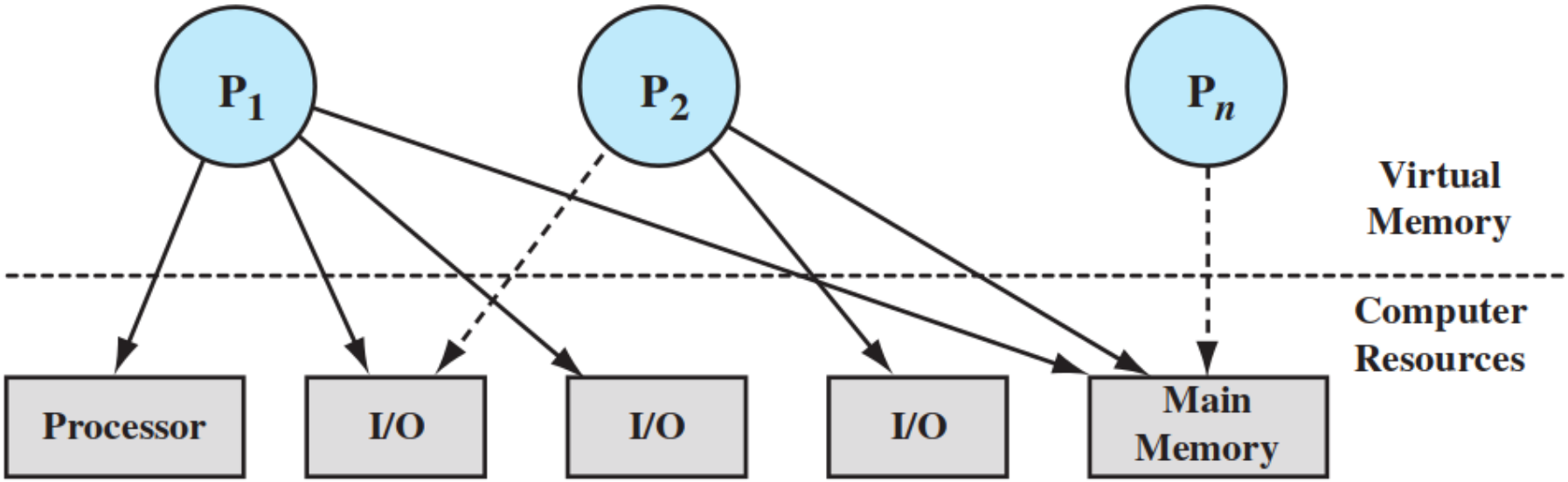


Figure 12: Processes and Resources (Resource Allocation at One Snapshot in Time)

Process Identification

- Each process is assigned a **unique numeric identifier**
  - Otherwise there must be a mapping that allows the OS to locate the appropriate tables based on the process identifier
- Many of the tables controlled by the OS may use process identifiers to cross-reference process tables
- Memory tables may be organized to provide a map of main memory with an indication of which process is assigned to each region
  - Similar references will appear in I/O and file tables
- When processes communicate with one another, the process identifier informs the OS of the destination of a particular communication
- When processes are allowed to create other processes, identifiers indicate the parent and descendants of each process

Program Status Word

All processor designs include a register or set of registers, often known as the **program status word (PSW)**:

- Contains condition codes plus other status information
- EFLAGS register is an example of a PSW used by any OS running on an x86 processor

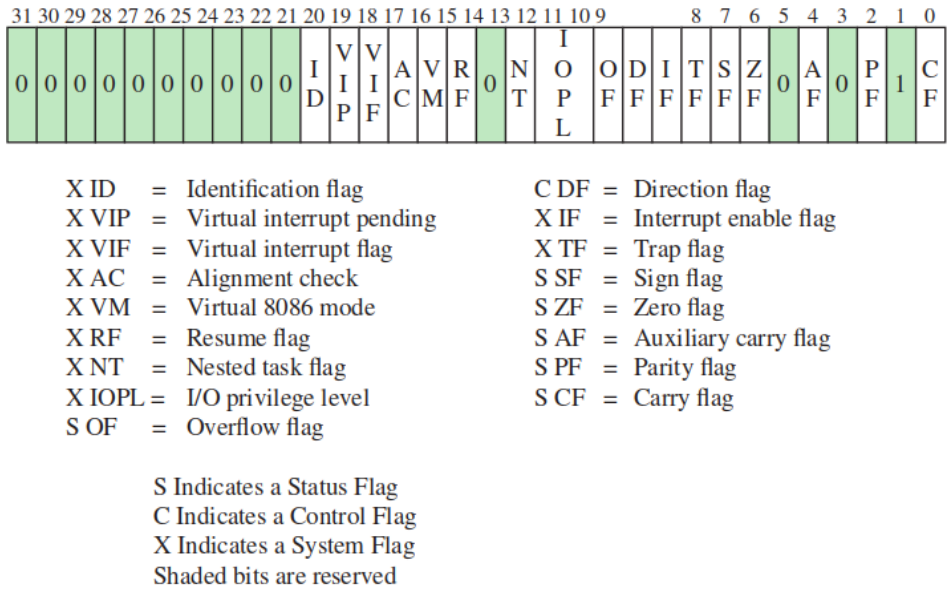


Figure 13: x86 EFLAGS Register

Process List Structures

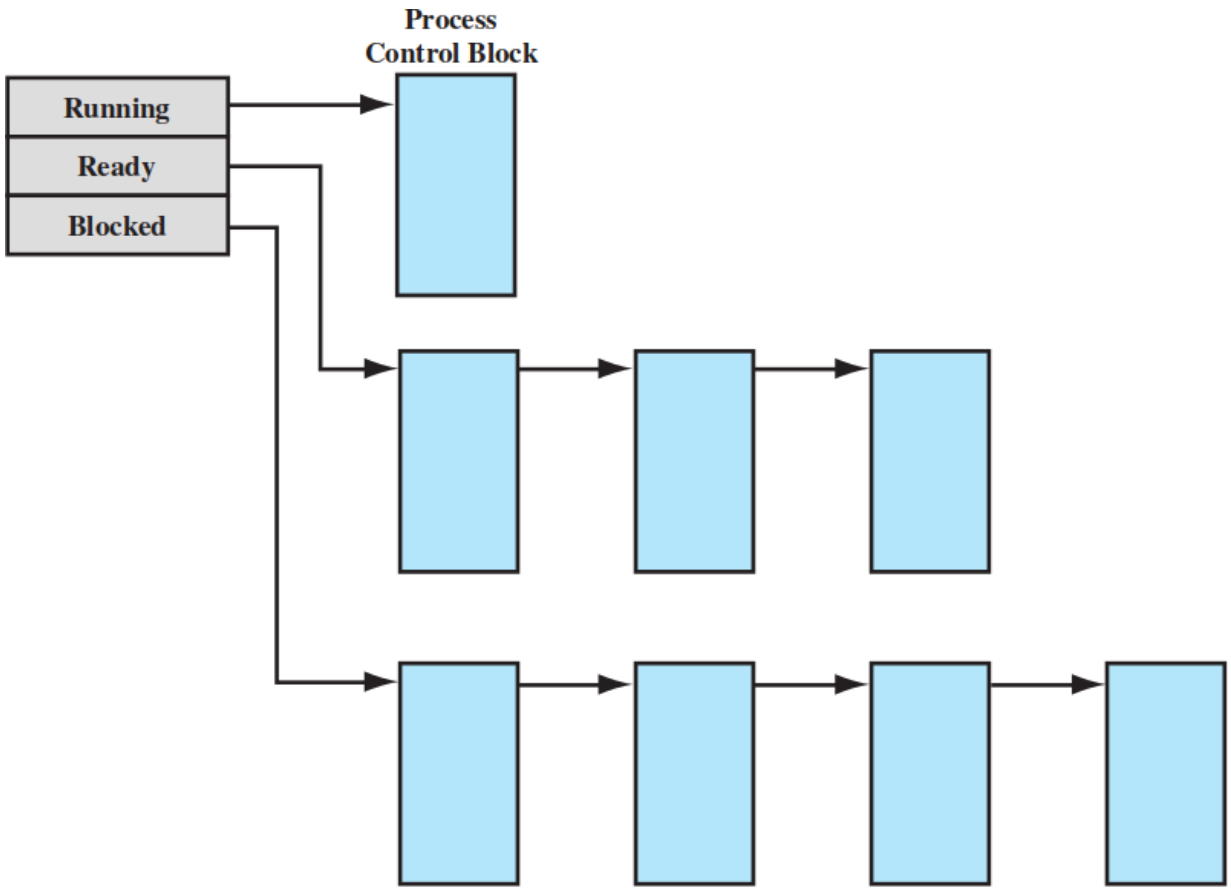


Figure 14: Process List Structures

Process Control

Modes of Execution

1. **User Mode**
   - Less-privileged mode
   - User programs typically execute in this mode
2. **System Mode**
   - More-privileged mode
   - Also referred to as control mode or kernel mode
   - Kernel of the operating system

Typical Functions of an Operating System Kernel

1. Process Management
   e.g. creation, termination, scheduling, control block management, switching
2. Memory Management
   e.g. address space allocation to processes, swapping
3. I/O Management
4. Support Functions
   e.g. interrupt handling

Process Creation

Once the OS decides to create a new process it:

- Assigns a unique process identifier to the new process
- Allocates space for the process
- Initializes the process control block
- Sets the appropriate linkages
- Creates or expands other data structures

Mechanisms for Interrupting the Execution of a Process

Table 3.8 Mechanisms for Interrupting the Execution of a Process

Mechanism	Cause	Use
Interrupt	External to the execution of the current instruction	Reaction to an asynchronous external event
Trap	Associated with the execution of the current instruction	Handling of an error or an exception condition
Supervisor call	Explicit request	Call to an operating system function

System Interrupts

1. **Interrupt**

   Due to some sort of event that is external to and independent of the currently running process

   - **Clock interrupt:**
     The OS determines whether the currently running process has been executing for the maximum allowable unit of time (time slice).
     If it has, this process must be switched to a Ready state and another process dispatched.
     - **Time Slice:** The maximum amount of time that a process can execute before being interrupted

System Interrupts

- **I/O interrupt:** The OS determines what I/O action has occurred. If the I/O action constitutes an event for which one or more processes are waiting, then the OS moves all of the corresponding blocked processes to the Ready state (and Blocked/Suspend processes to the Ready/Suspend state).
  The OS must then decide whether to resume execution of the process currently in the Running state or to preempt that process for a higher-priority Ready process.
- **Memory fault:**
  The processor encounters a virtual memory address reference for a word that is not in main memory. The OS must bring in the block (page or segment) of memory containing the reference from secondary memory to main memory.
  After the I/O request is issued to bring in the block of memory, the process with the memory fault is placed in a blocked state; the OS then performs a process switch to resume execution of another process.
  After the desired block is brought into memory, that process is placed in the Ready state.

System Interrupts

2. **Trap**
   An error or exception condition generated within the currently running process
   OS determines if the condition is fatal
   - Moved to the Exit state and a process switch occurs
   - Action will depend on the nature of the error and the design of the OS

Mode Switching

- If no interrupts are pending the processor:
  - Proceeds to the fetch stage and fetches the next instruction of the current program in the current process
- If an interrupt is pending the processor:
  - Sets the program counter to the starting address of an interrupt handler program
  - Switches from user mode to kernel mode so that the interrupt processing code may include privileged instructions

Change of Process State

The steps in a full process switch are:

1. Save the context of the processor
2. Update the process control block of the process currently in the Running state
3. Move the process control block of this process to the appropriate queue
4. Select another process for execution
5. Update the process control block of the process selected
6. Update memory management data structures
7. Restore the context of the processor to that which existed at the time the selected process was last switched out

If the currently running process is to be moved to another state (Ready, Blocked, etc.), then the OS must make substantial changes in its environment

Supplemental Material: UNIX SVR4 Process Management

UNIX SVR4

- Uses the model where most of the OS executes within the environment of a user process
- System processes run in kernel mode
  - Executes operating system code to perform administrative and housekeeping functions
- User Processes
  - Operate in user mode to execute user programs and utilities
  - Operate in kernel mode to execute instructions that belong to the kernel
  - Enter kernel mode by issuing a system call, when an exception is generated, or when an interrupt occurs

UNIX Process States

Table 3.9 UNIX Process States

User Running	Executing in user mode.
Kernel Running	Executing in kernel mode.
Ready to Run, in Memory	Ready to run as soon as the kernel schedules it.
Asleep in Memory	Unable to execute until an event occurs; process is in main memory (a blocked state).
Ready to Run, Swapped	Process is ready to run, but the swapper must swap the process into main memory before the kernel can schedule it to execute.
Sleeping, Swapped	The process is awaiting an event and has been swapped to secondary storage (a blocked state).
Preempted	Process is returning from kernel to user mode, but the kernel preempts it and does a process switch to schedule another process.
Created	Process is newly created and not yet ready to run.
Zombie	Process no longer exists, but it leaves a record for its parent process to collect.

UNIX Process State Transition Diagram

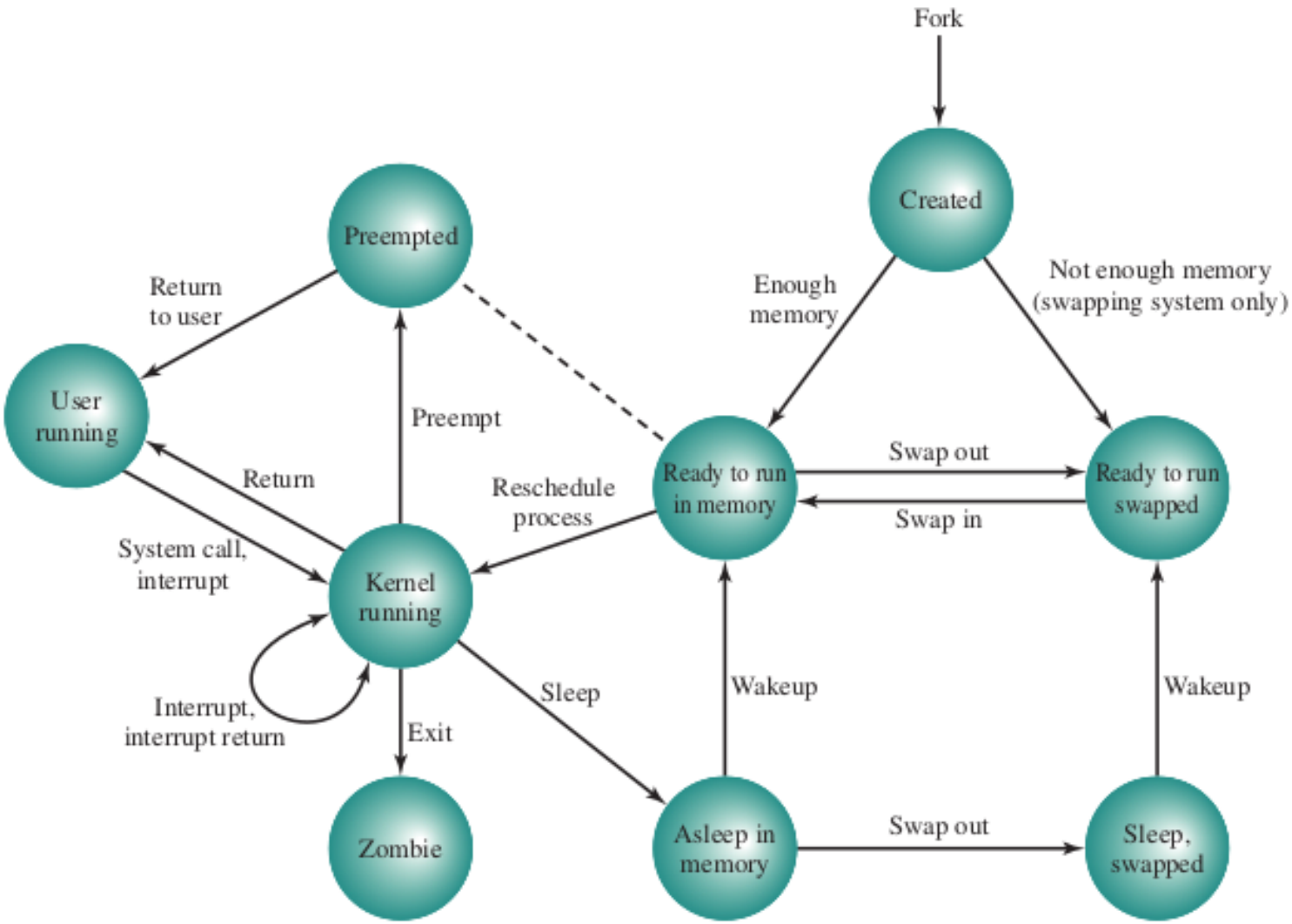


Figure 15: UNIX Process State Transition Diagram

Process Control

Process creation is by means of the kernel system call, `fork()`

When a process issues a `fork()` request, the OS performs the following functions:

1. Allocates a slot in the process table for the new process
2. Assigns a unique process ID to the child process
3. Makes a copy of the process image of the parent, with the exception of any shared memory
4. Increments counters for any files owned by the parent, to reflect that an additional process now also owns those files
5. Assigns the child process to the Ready to Run state
6. Returns the ID number of the child to the parent process, and a 0 value to the child process

After Creation

After creating the process the Kernel can do one of the following, as part of the dispatcher routine:

- Stay in the parent process. Control returns to user mode at the point of the `fork()` call of the parent.
- Transfer control to the child process. The child process begins executing at the same point in the code as the parent, namely at the return from the `fork()` call.
- Transfer control to another process. Both parent and child are left in the Ready to Run state.

UNIX Process Image

Table 3.10 UNIX Process Image

User-Level Context	
Process text	Executable machine instructions of the program
Process data	Data accessible by the program of this process
User stack	Contains the arguments, local variables, and pointers for functions executing in user mode
Shared memory	Memory shared with other processes, used for interprocess communication
Register Context	
Program counter	Address of next instruction to be executed; may be in kernel or user memory space of this process
Processor status register	Contains the hardware status at the time of preemption; contents and format are hardware dependent
Stack pointer	Points to the top of the kernel or user stack, depending on the mode of operation at the time or preemption
General-purpose registers	Hardware dependent
System-Level Context	
Process table entry	Defines state of a process; this information is always accessible to the operating system
U (user) area	Process control information that needs to be accessed only in the context of the process
Per process region table	Defines the mapping from virtual to physical addresses; also contains a permission field that indicates the type of access allowed the process: read-only, read-write, or read-execute
Kernel stack	Contains the stack frame of kernel procedures as the process executes in kernel mode

UNIX Process Table Entry

Table 3.11 UNIX Process Table Entry

Process status	Current state of process.
Pointers	To U area and process memory area (text, data, stack).
Process size	Enables the operating system to know how much space to allocate the process.
User identifiers	The **real user ID** identifies the user who is responsible for the running process. The **effective user ID** may be used by a process to gain temporary privileges associated with a particular program; while that program is being executed as part of the process, the process operates with the effective user ID.
Process identifiers	ID of this process; ID of parent process. These are set up when the process enters the Created state during the fork system call.
Event descriptor	Valid when a process is in a sleeping state; when the event occurs, the process is transferred to a ready-to-run state.
Priority	Used for process scheduling.
Signal	Enumerates signals sent to a process but not yet handled.
Timers	Include process execution time, kernel resource utilization, and user-set timer used to send alarm signal to a process.
P_link	Pointer to the next link in the ready queue (valid if process is ready to execute).
Memory status	Indicates whether process image is in main memory or swapped out. If it is in memory, this field also indicates whether it may be swapped out or is temporarily locked into main memory.

UNIX U Area

Table 3.12 UNIX U Area

Process table pointer	Indicates entry that corresponds to the U area.
User identifiers	Real and effective user IDs used to determine user privileges.
Timers	Record time that the process (and its descendants) spent executing in user mode and in kernel mode.
Signal-handler array	For each type of signal defined in the system, indicates how the process will react to receipt of that signal (exit, ignore, execute specified user function).
Control terminal	Indicates login terminal for this process, if one exists.
Error field	Records errors encountered during a system call.
Return value	Contains the result of system calls.
I/O parameters	Describe the amount of data to transfer, the address of the source (or target) data array in user space, and file offsets for I/O.
File parameters	Current directory and current root describe the file system environment of the process.
User file descriptor table	Records the files the process has opened.
Limit fields	Restrict the size of the process and the size of a file it can write.
Permission modes fields	Mask mode settings on files the process creates.