Android Internals

Nimit Kalaria

M.Tech CSE,
Indian Institute of Technology Bombay

3rd March 2013

AAKASH
tablet for every indian
NME-ICT(MHRD),AAKASH PROJECT, IIT BOMBAY

Indian Institute of
Technology Bombay

सत्यमेव जयते
The National Mission on
Education through ICT
(NME-ICT)

Contents

- Android Kernel
- Runtime Walkthrough
  - Zygote
- Binder (IPC) Driver
- Layer Interaction
  - JNI

Android Kernel

- Why Linux Kernel ?
  - Good memory and process management
  - Permission-based security model
  - Proven driver model
  - Support for shared libraries
  - Provide core system services

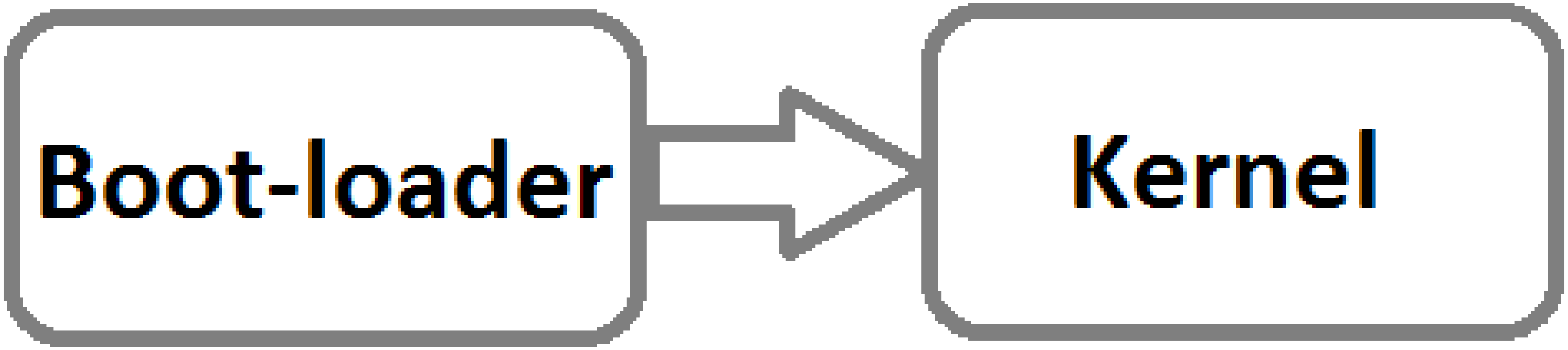
- Enhancements to Linux Kernel
    - Binder (IPC) Driver
    - Ashmem (Android shared memory driver)
    - Alarm Driver and Logger
    - Power Management
    - Low Memory Killer

Contents

- Android Kernel
- Runtime Walkthrough
  - Zygote
- Binder (IPC) Driver
- Layer Interaction
  - JNI

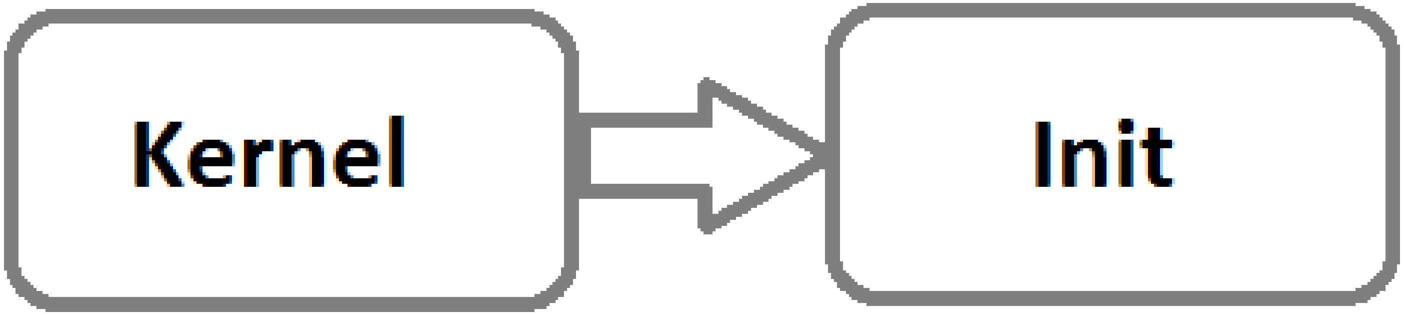
Runtime Walkthrough

- Similar to Linux based system
- Boot-loader loads the Linux kernel



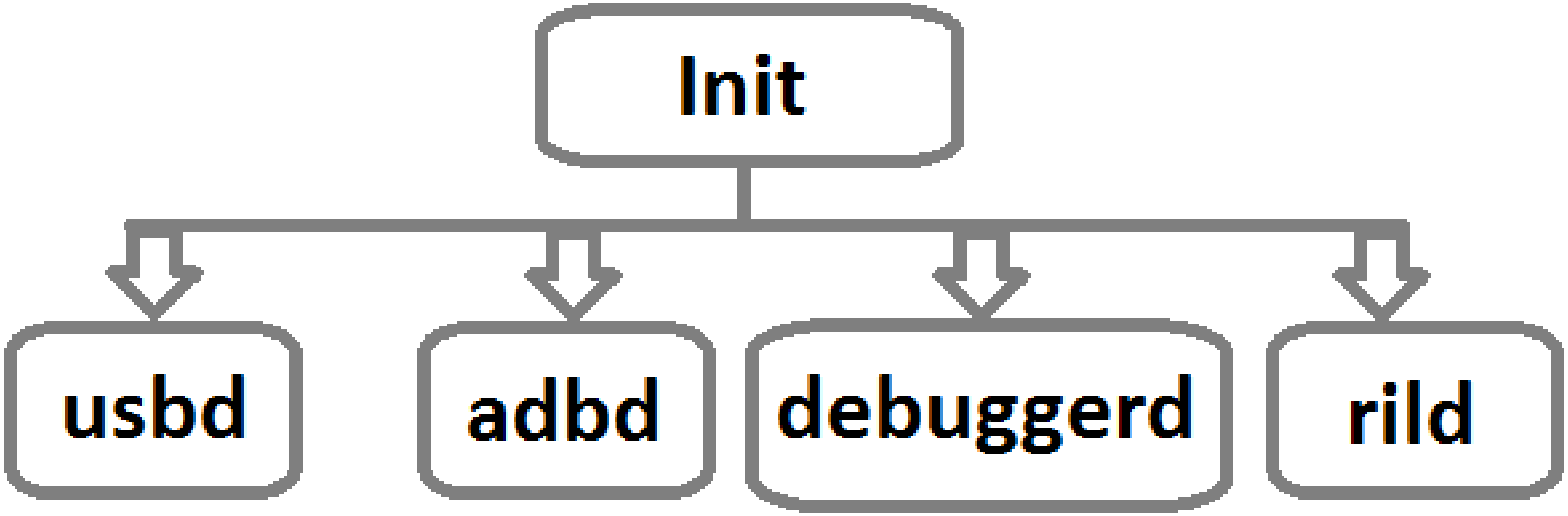
Runtime Walkthrough

- Kernel
  - Initializes environment
  - Mounts root file system
  - Starts the 'Init' process



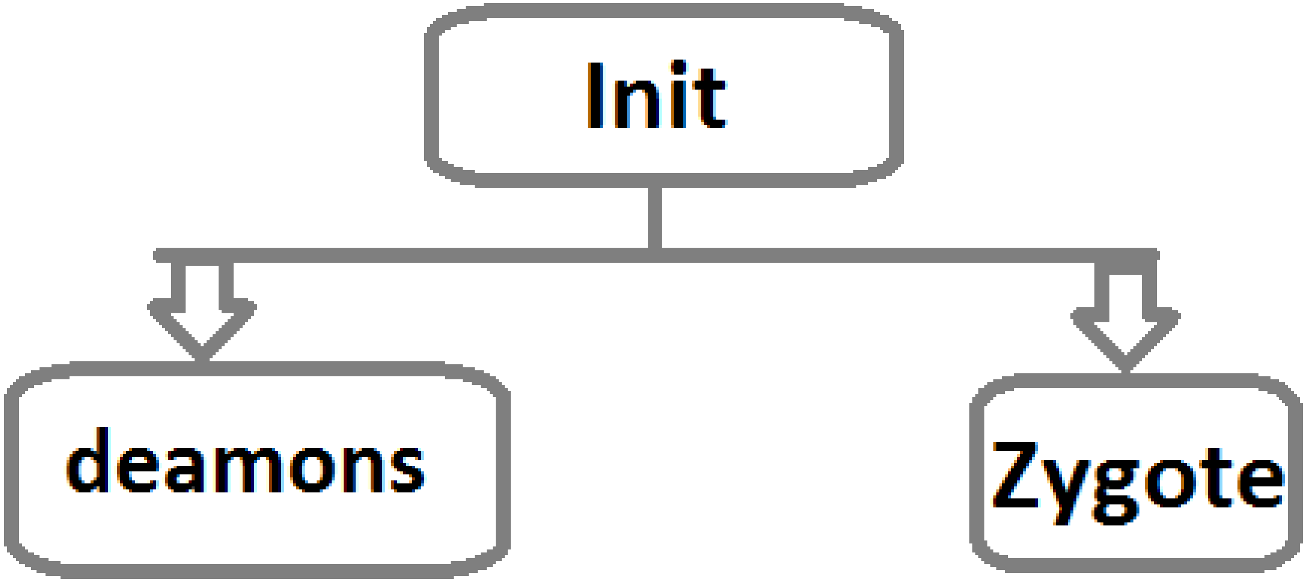
Runtime Walkthrough

- Init starts daemons



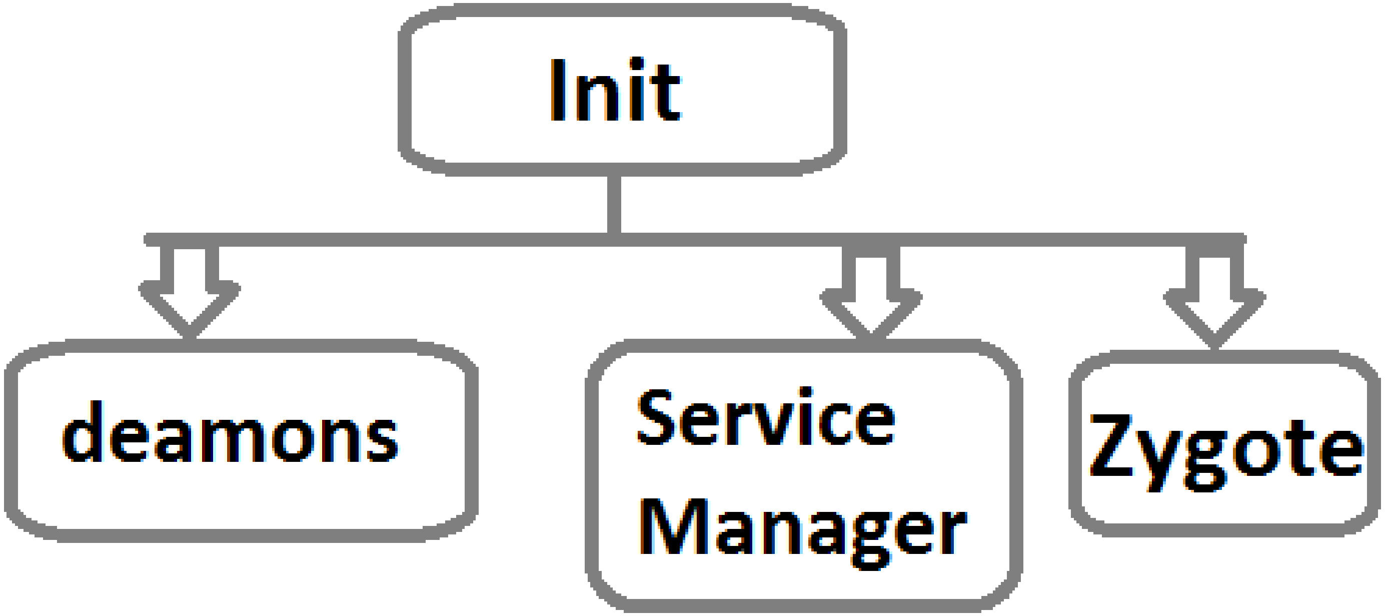
Runtime Walkthrough

- Init starts the zygote process
  - Initializes a Dalvik VM instance
  - Links all core libraries and share it
  - Use copy-on-write



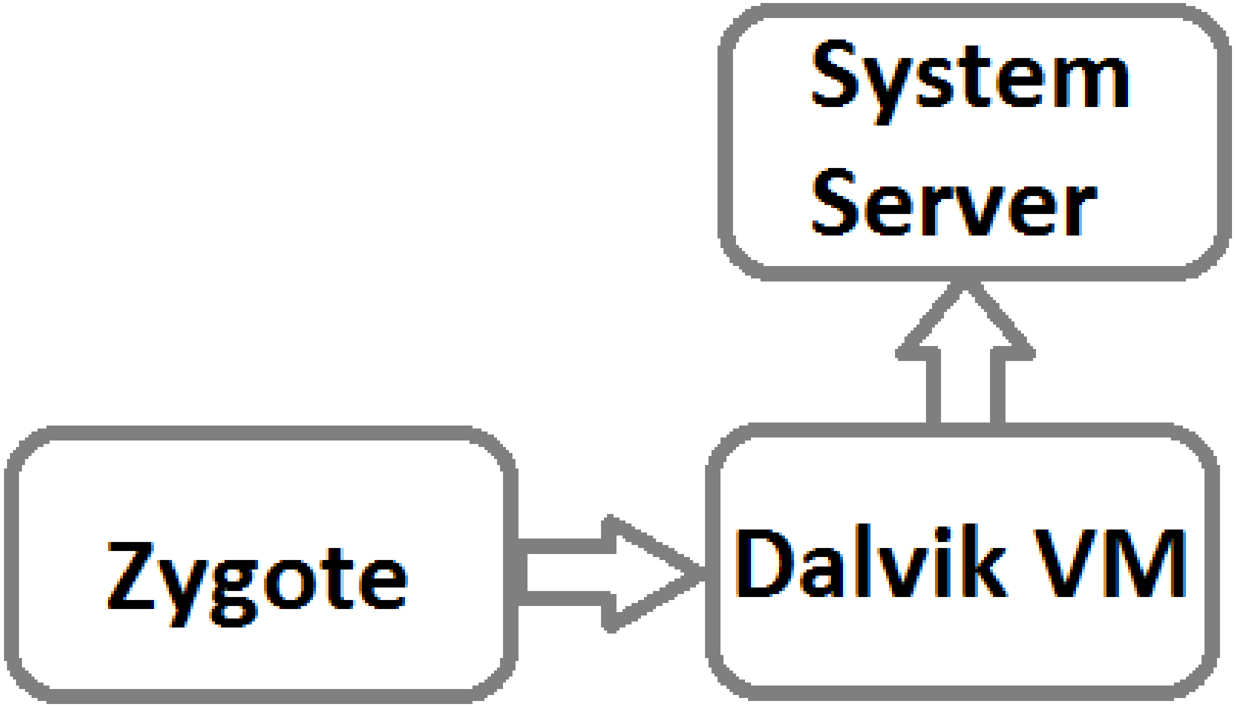
Runtime Walkthrough

- Init starts runtime process
  - Initializes Service Manager
  - Context manager for Binder



Runtime Walkthrough

- Forks a new Dalvik VM
- Start system server



Runtime Walkthrough

- Start native services
  - Surface and Audio Flinger

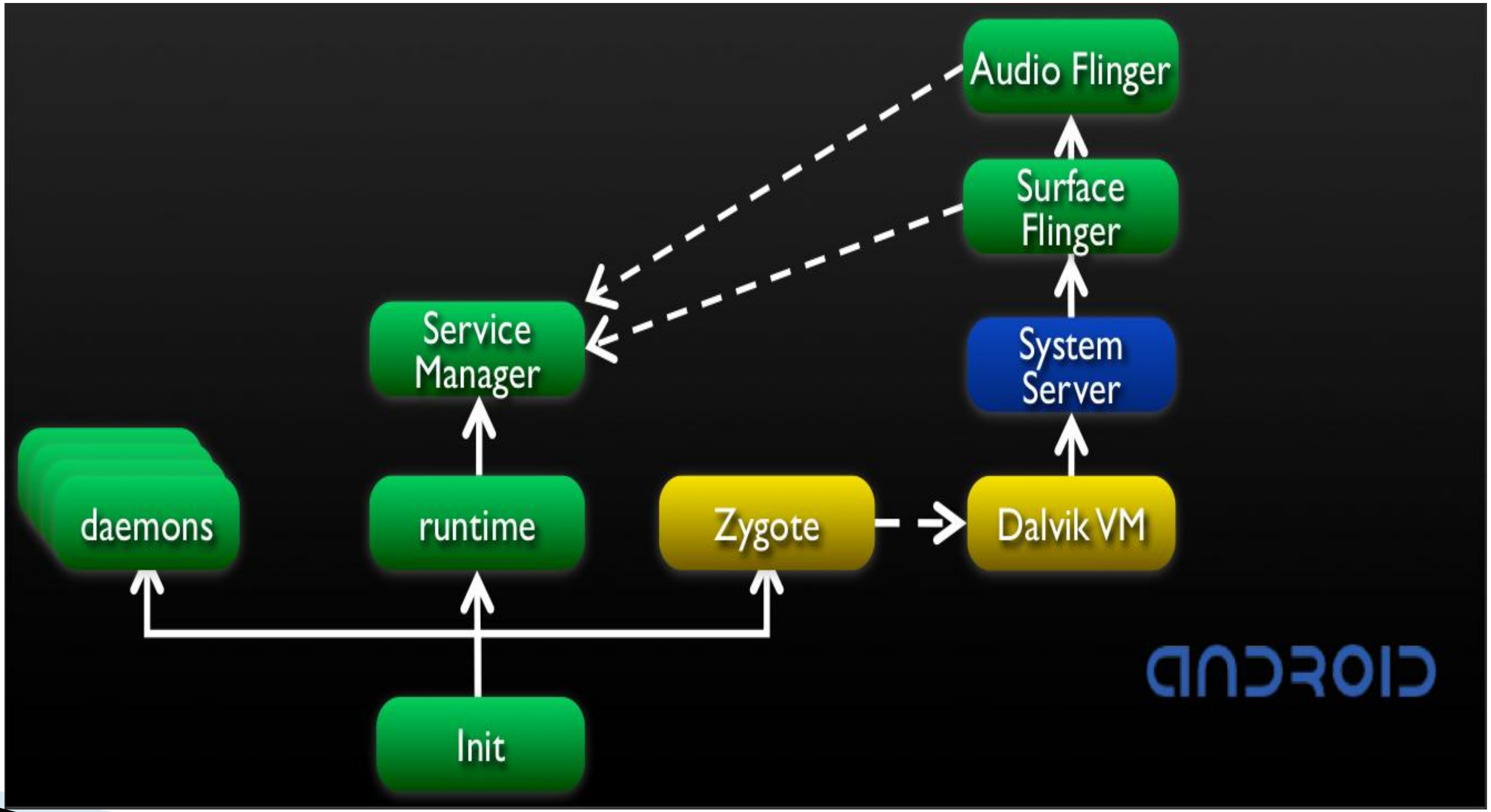


Image is taken from : https://sites.google.com/site/io/anatomy--physiology-of-an-android

Runtime Walkthrough

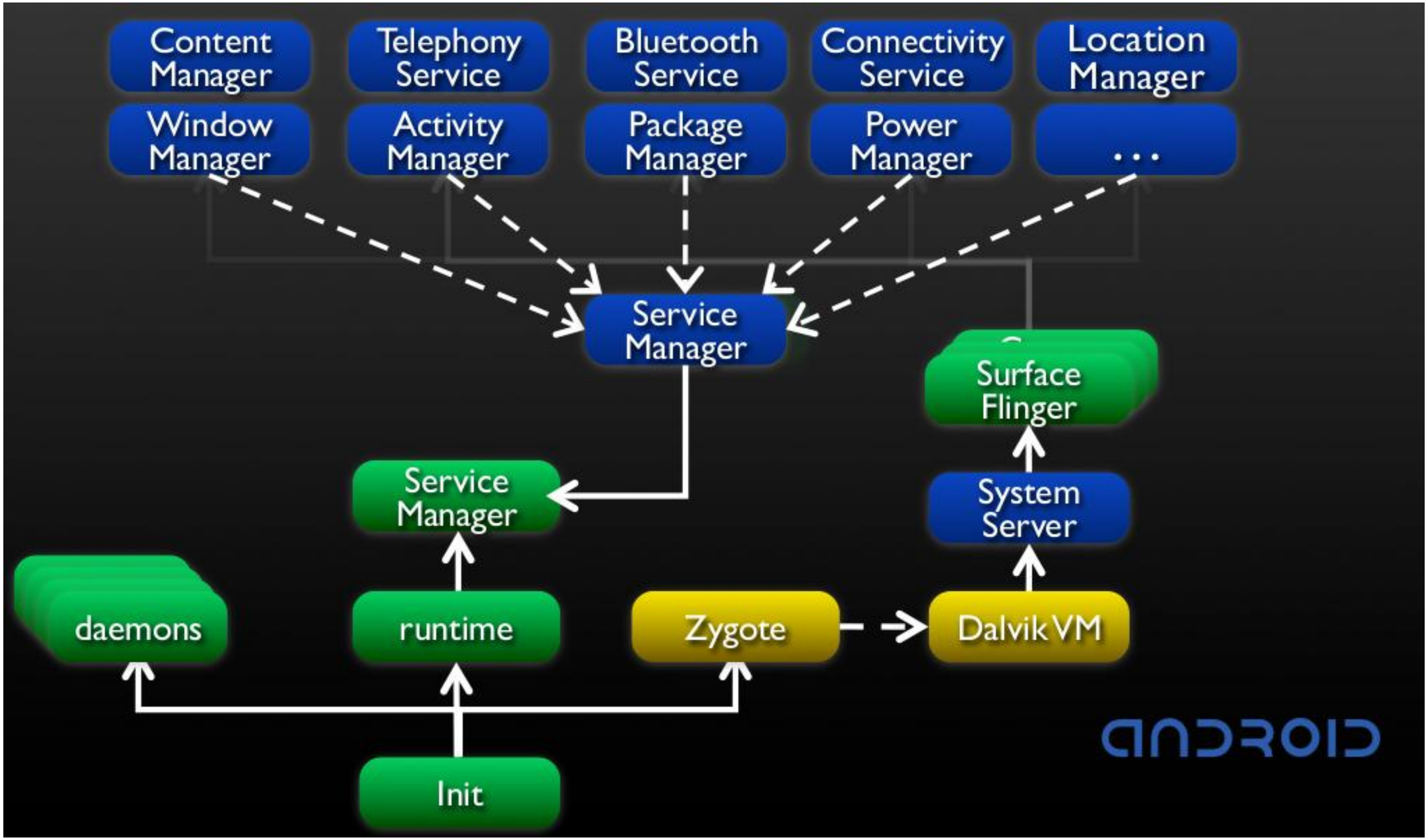


Image is taken from : https://sites.google.com/site/io/anatomy--physiology-of-an-android

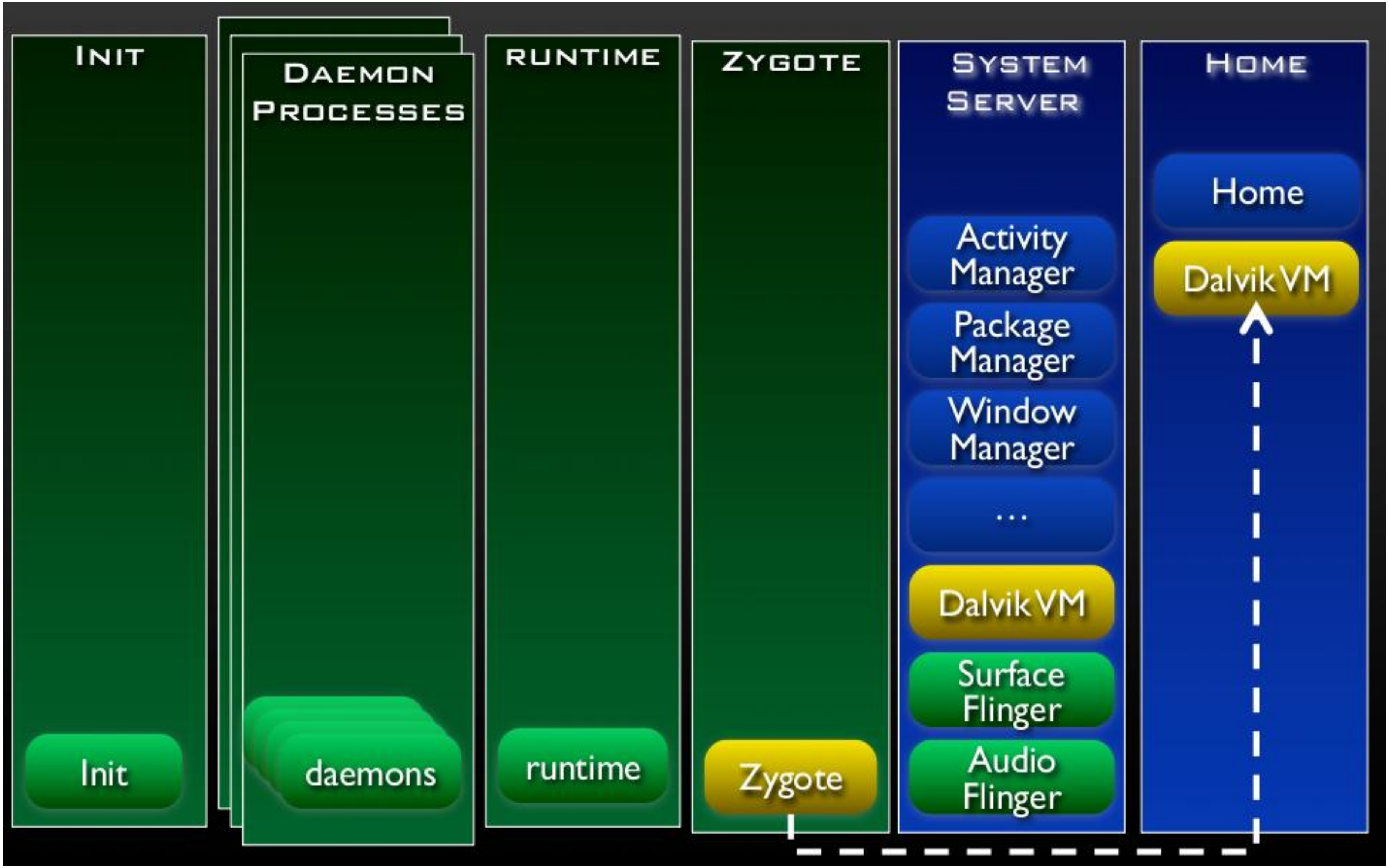


Image is taken from : https://sites.google.com/site/io/anatomy--physiology-of-an-android

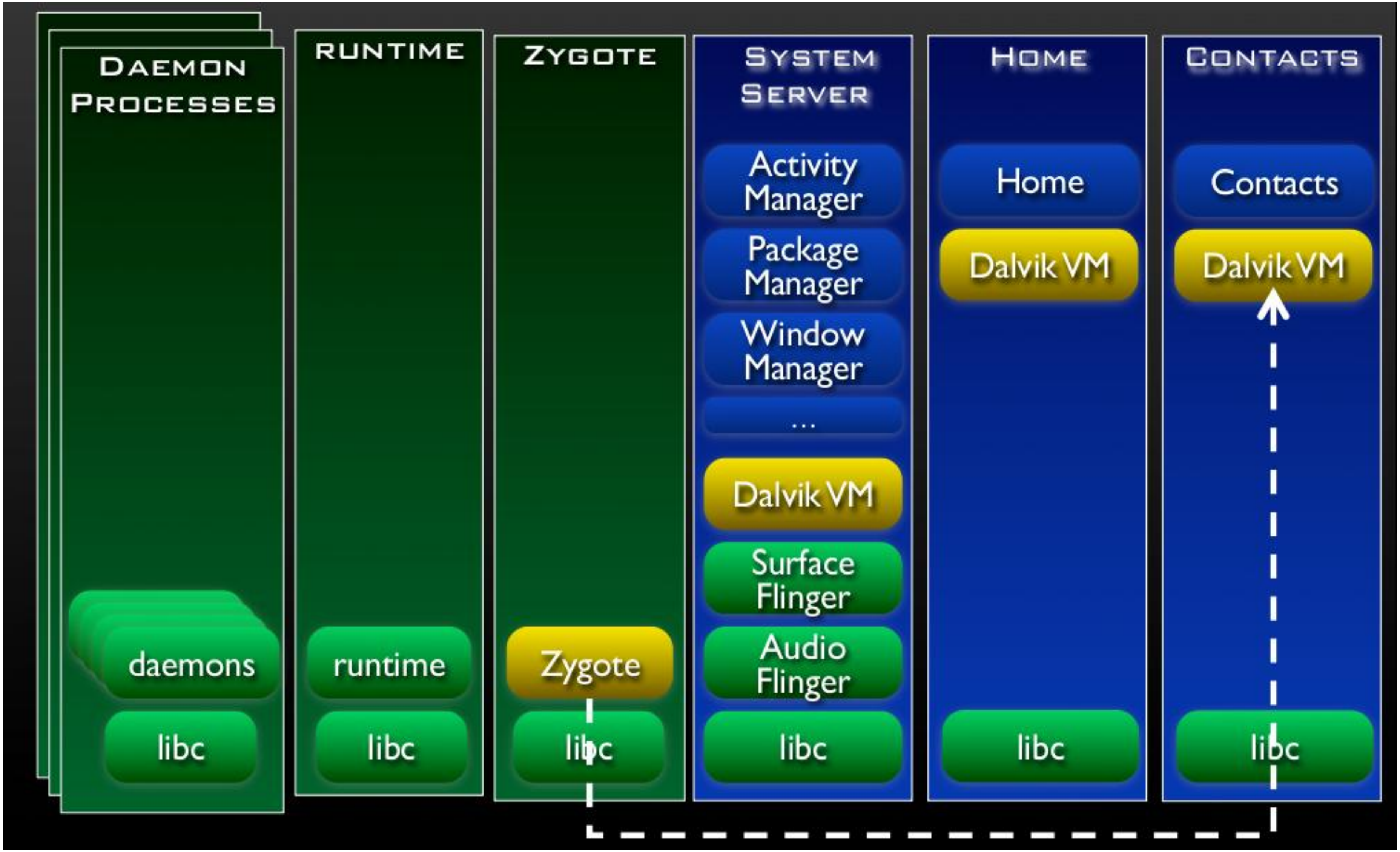


Image is taken from : https://sites.google.com/site/io/anatomy--physiology-of-an-android

Contents

- Android Kernel
- Runtime Walkthrough
  - Zygote
- Binder (IPC) Driver
- Layer Interaction
  - JNI

Inter-Process Communication(IPC)

- What is IPC?
  - Exchanges data with another process
- Why IPC?
  - Owns address space
  - Provides data isolation
  - Avoids direct interaction

IPC Mechanisms

- Linux
  - Signal
  - Pipe
  - Socket
  - Semaphore
  - Message Queue
  - Shared Memory

IPC Mechanisms

- Android
  - Binder : Lightweight RPC (Remote Procedure Call) mechanism

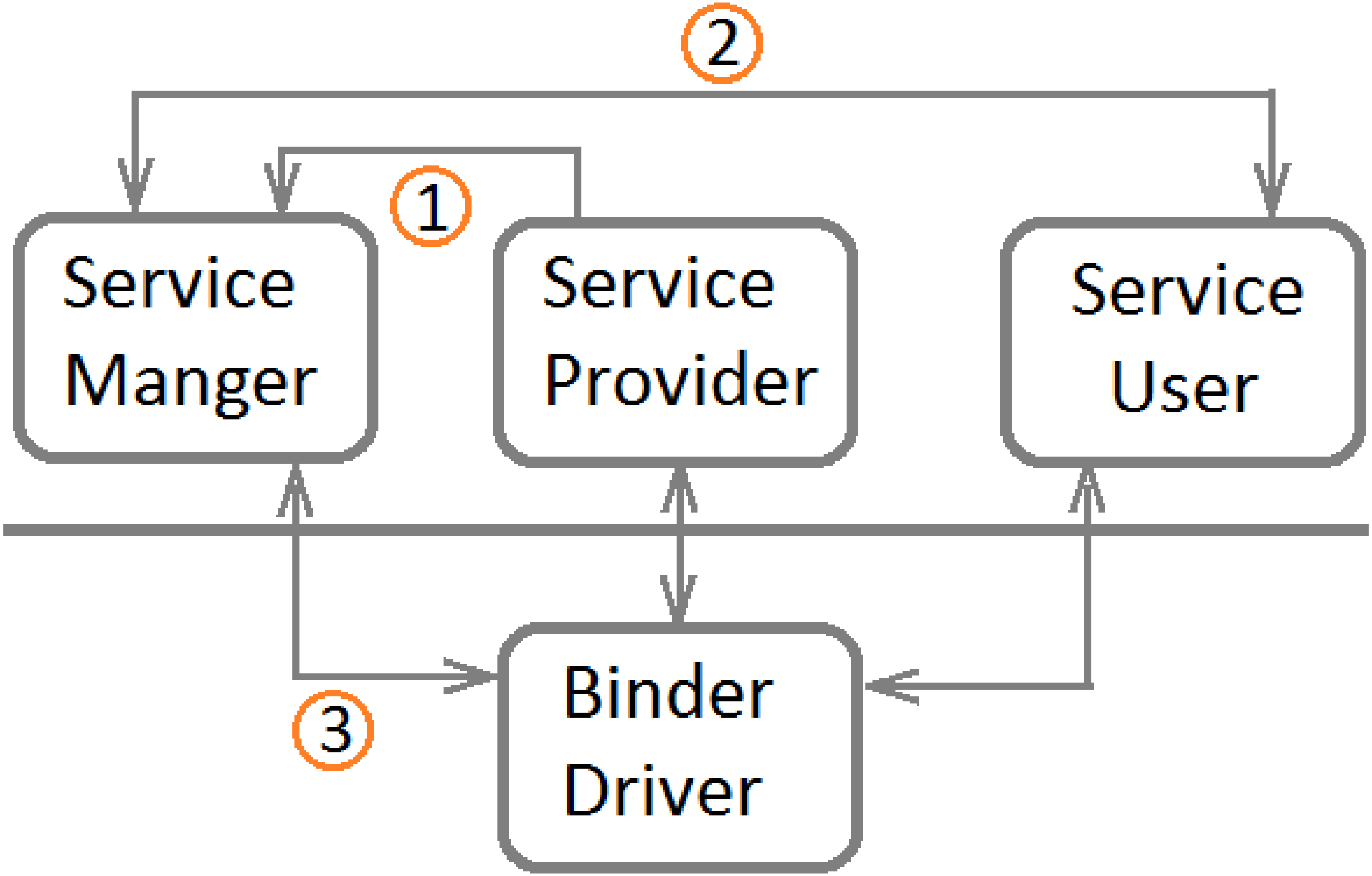
IPC Mechanisms

- Problems with old IPC Mechanisms
    - Separate processes
    - Security holes

IPC Mechanisms

- Solution
  - Driver
  - Shared memory
  - Per-process thread pool
  - Synchronous

Binder with Service Manager



Binder in Transaction

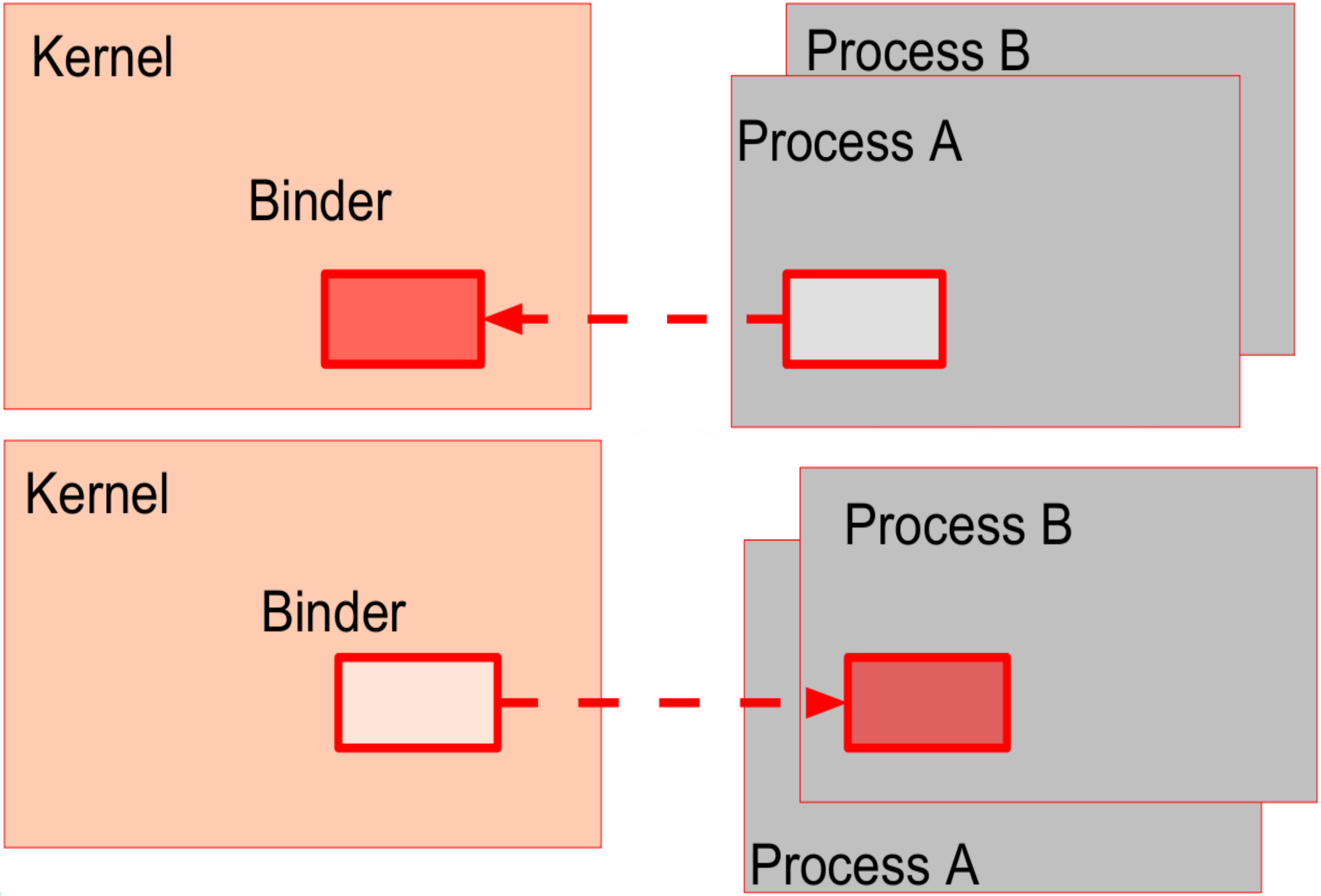


Image is taken from : http://www.slideshare.net/jserv/android-ipc-mechanism

Limitation of Binder

- Not ideal for transferring large data

- Data has to be converted into Parcel

Contents

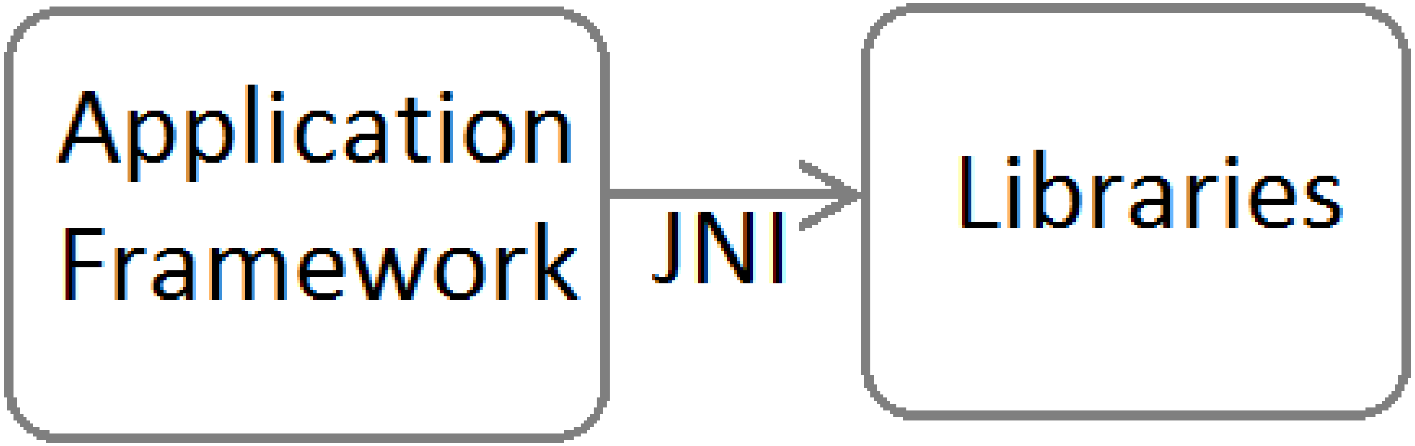
- Android Kernel
- Runtime Walkthrough
    - Zygote
- Binder (IPC) Driver
- Layer Interaction
    - JNI

Layer Interaction

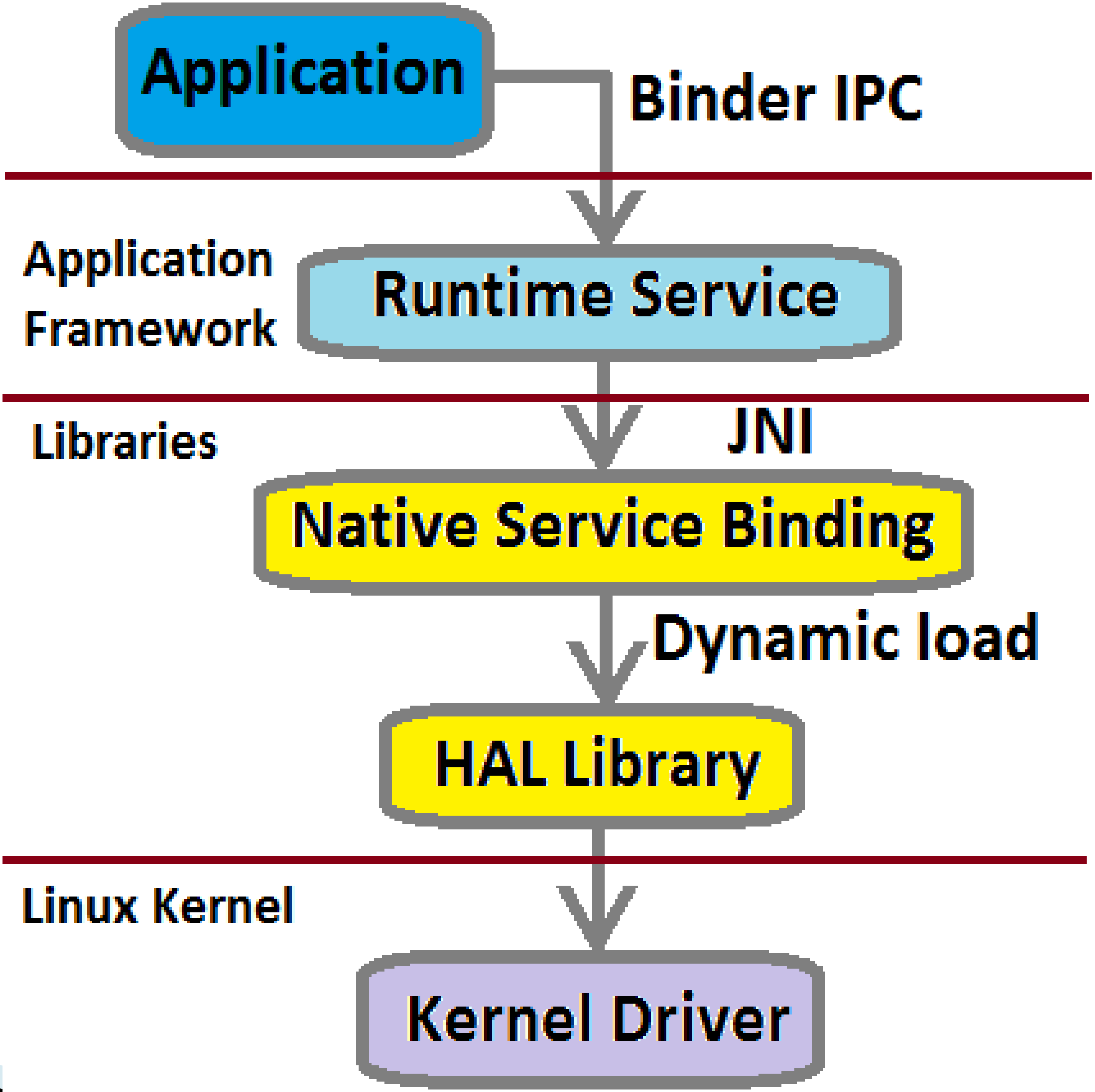
- Application – Runtime Service – lib
- Application – Runtime Service – Native Service – lib
- Application – Runtime Service – Native Daemon – lib
- Depends on type of application, and type of native library.

Java Native Interface(JNI)

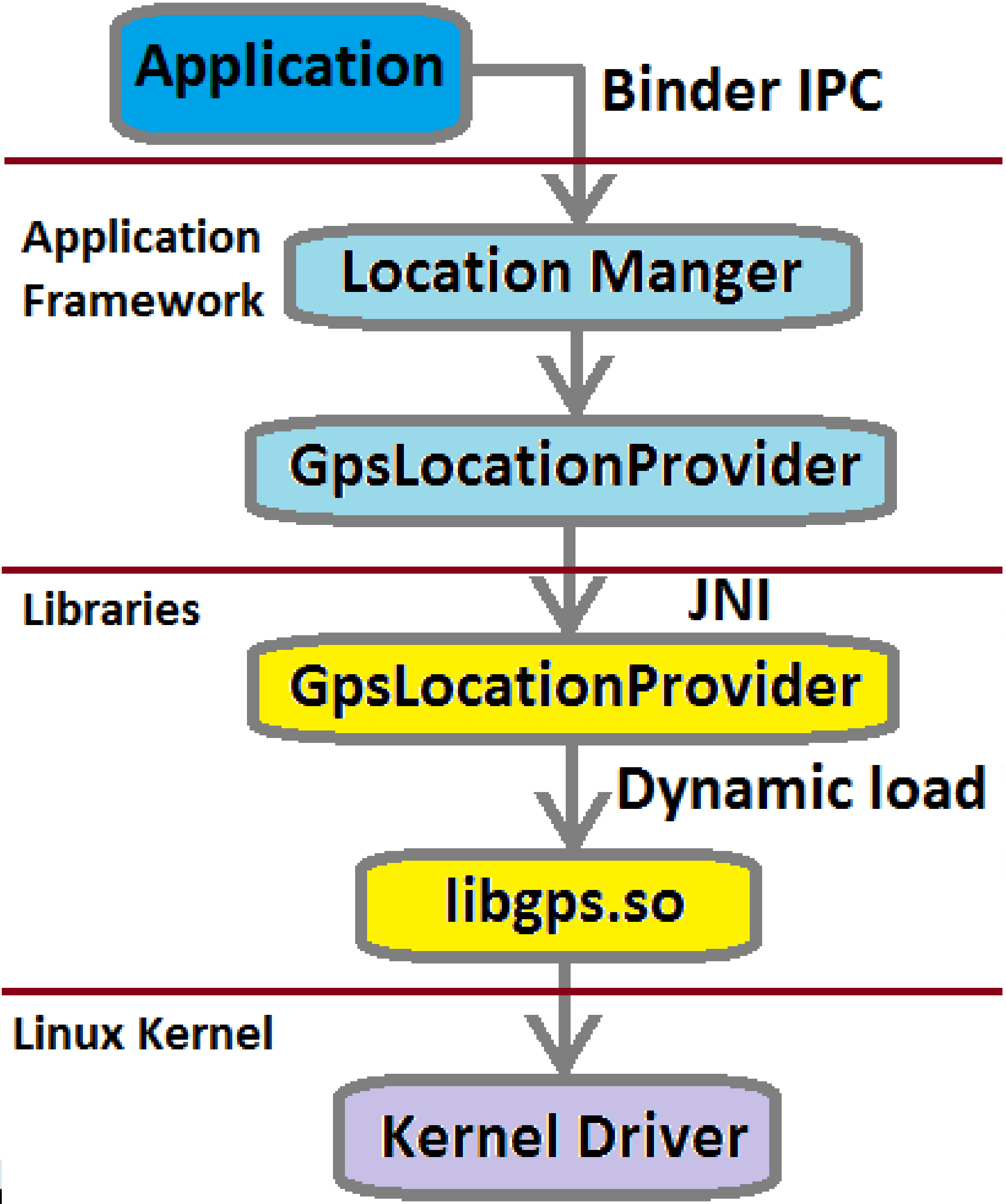
- Bridge between Application framework layer and Libraries.
- Call gate for languages, like ‘C’ or ‘C++’



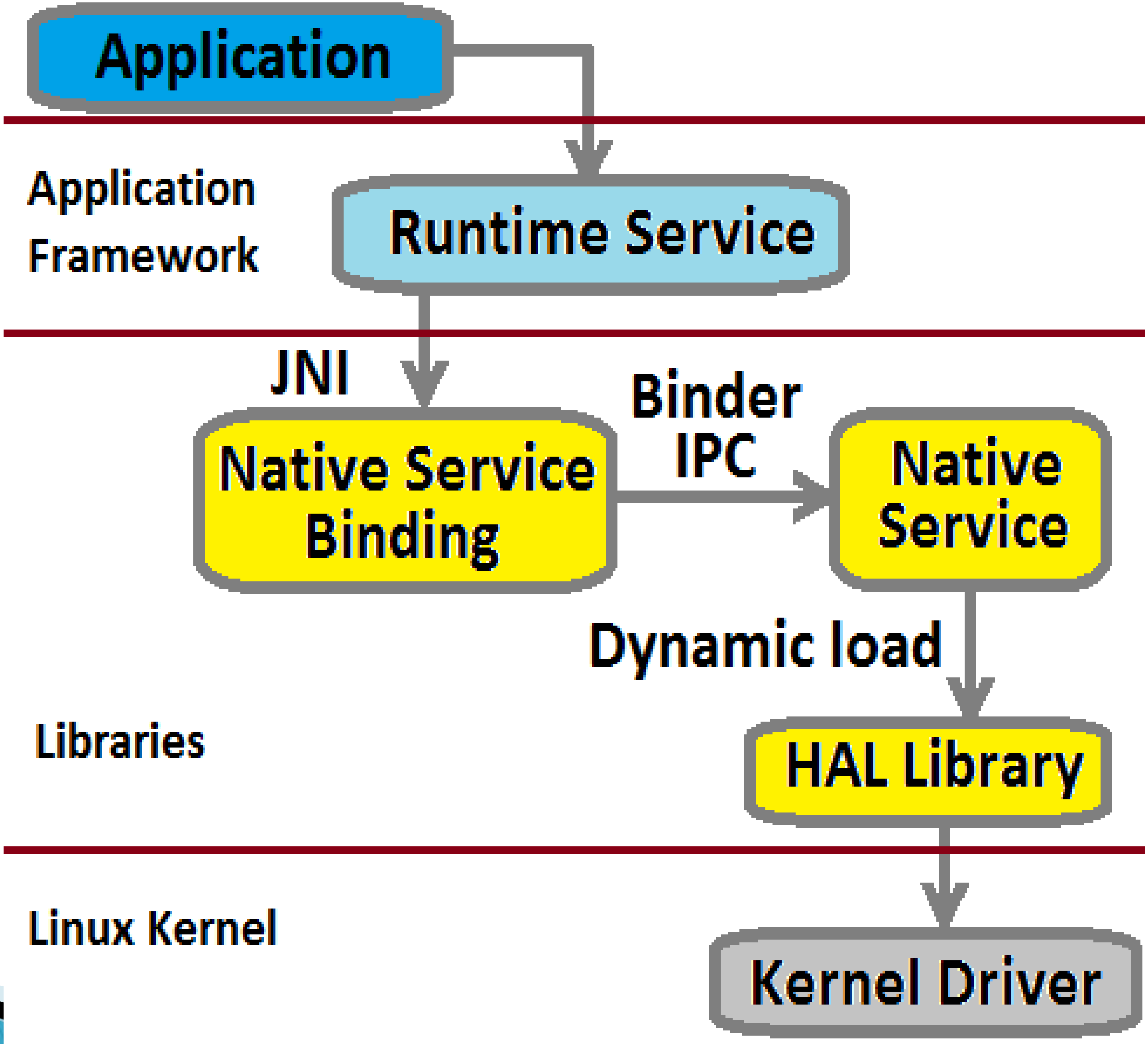
Runtime Service



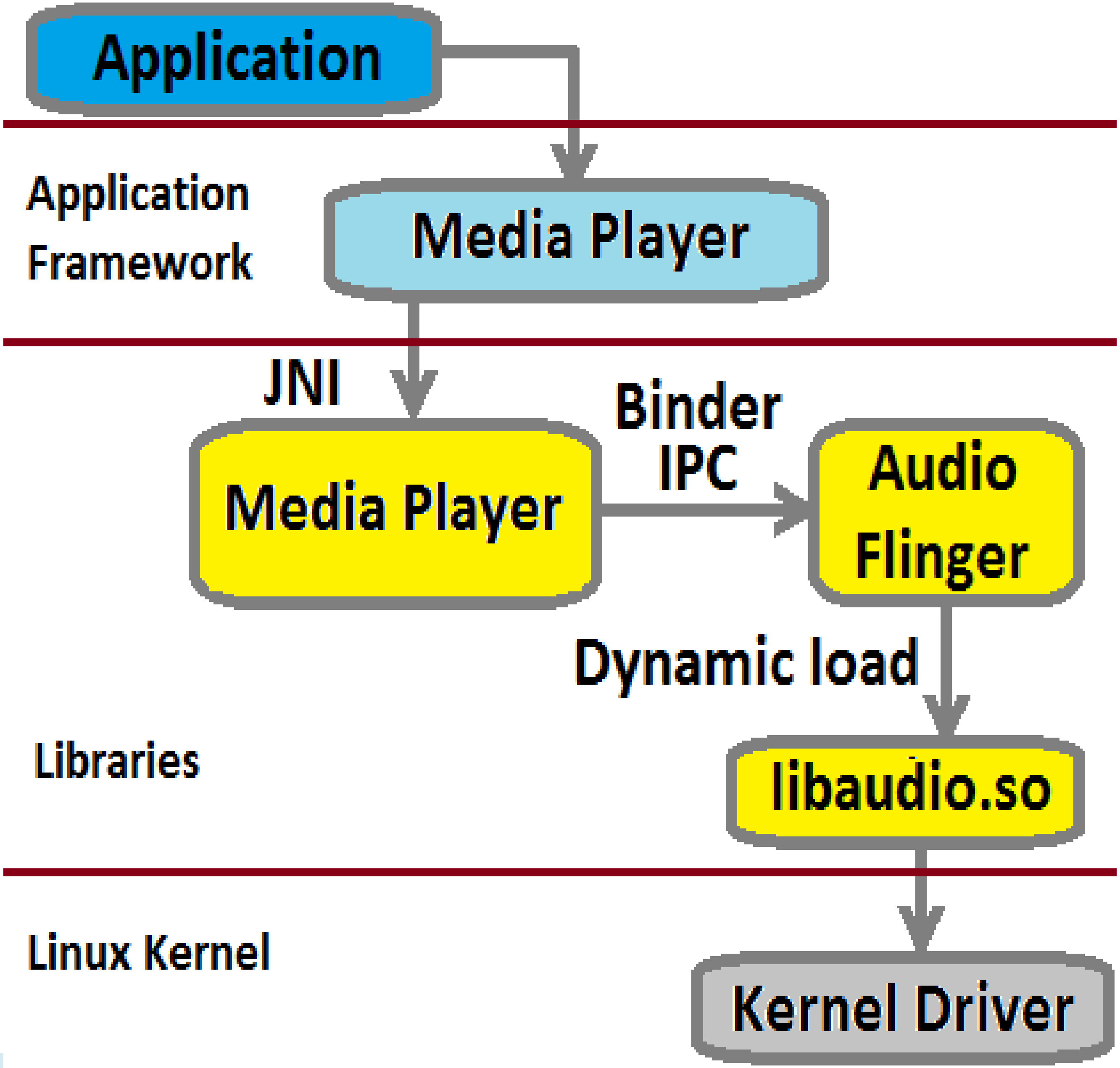
Example: Runtime Service



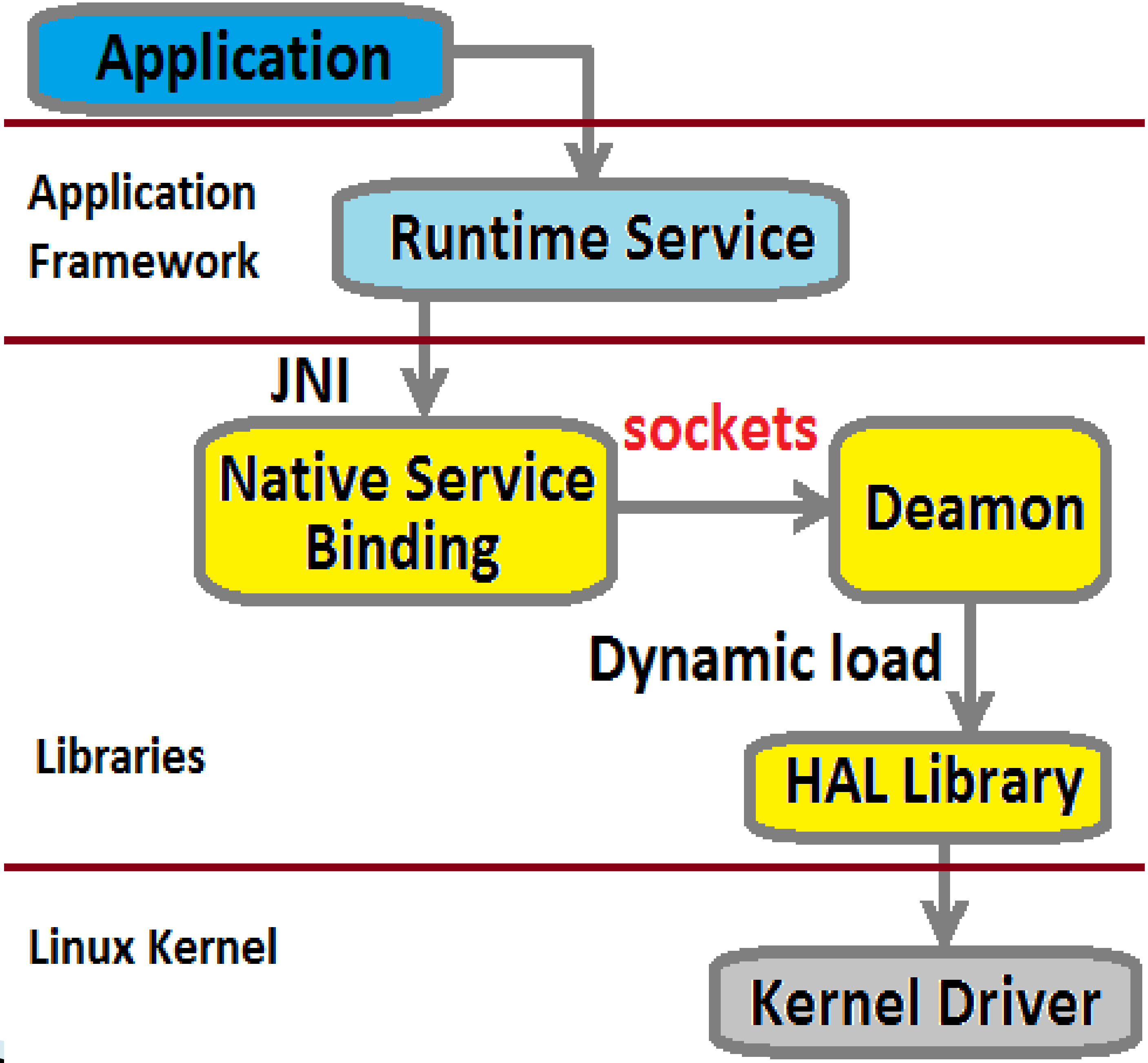
Native Service



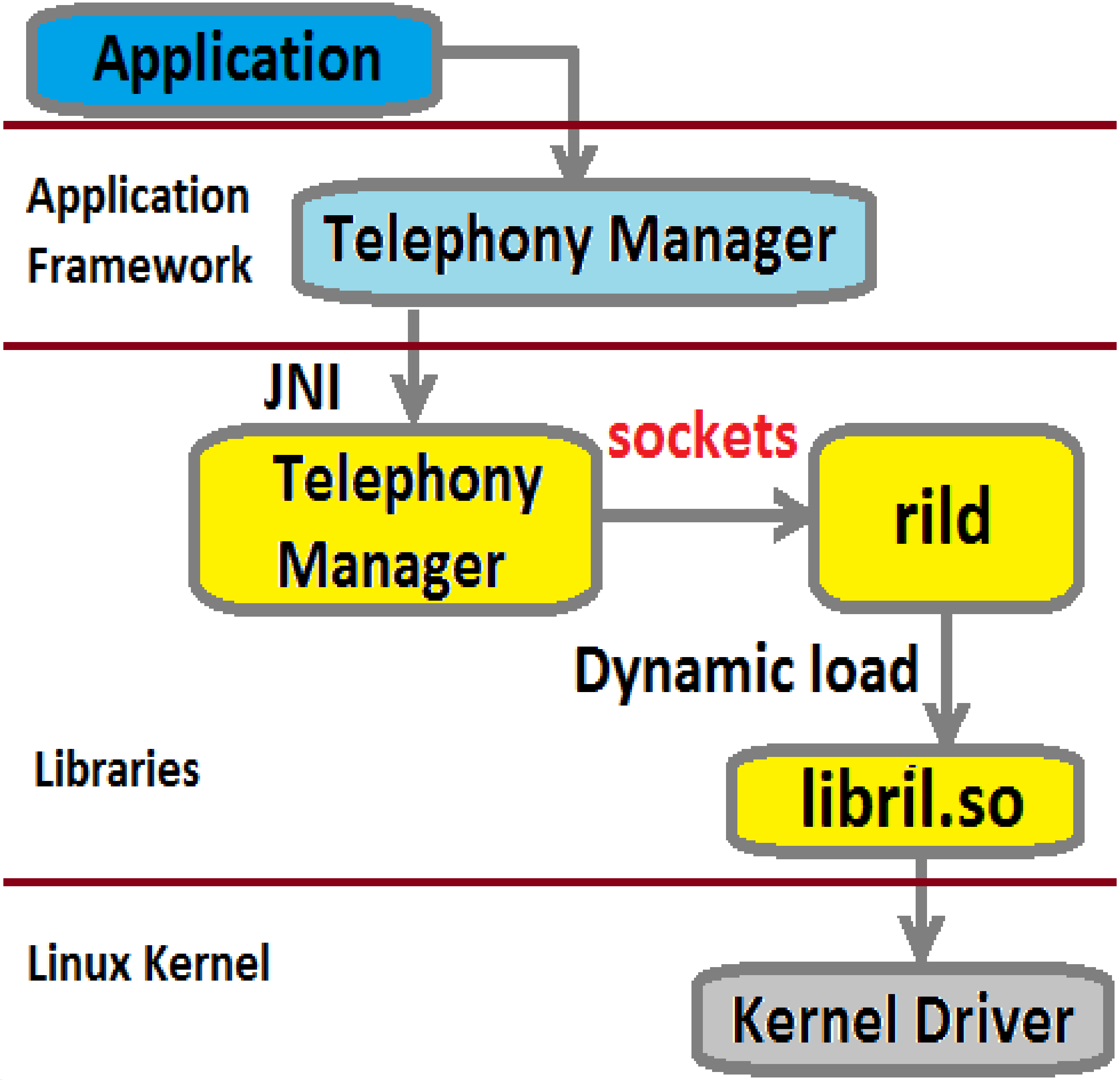
Example: Native Service



Native Daemon



Example: Native Daemon



Application

Application Framework

Telephony Manager

JNI

Telephony Manager

sockets

rild

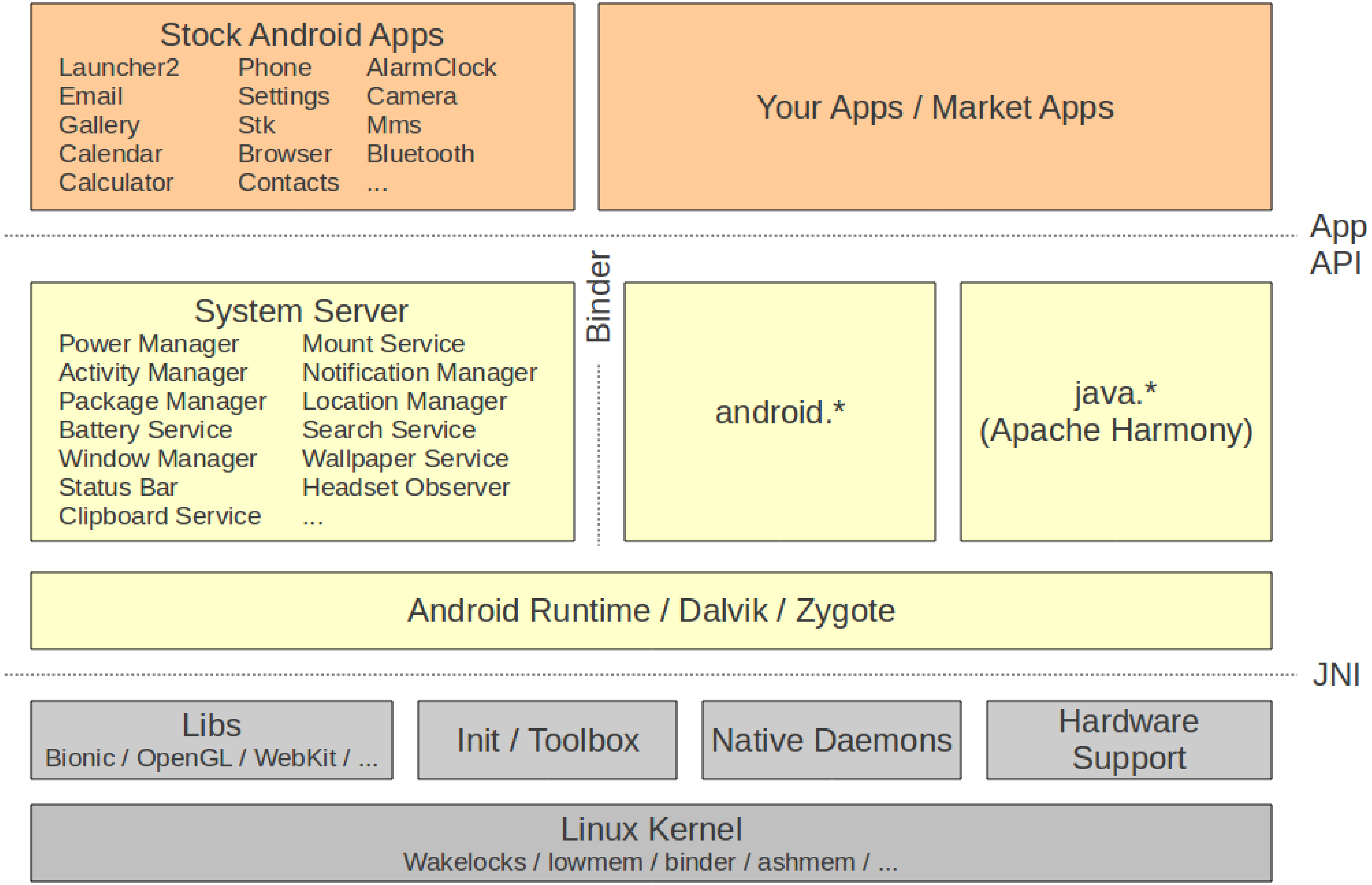
Dynamic load

Libraries

libril.so

Linux Kernel

Kernel Driver



Stock Android Apps

Launcher2, Phone, AlarmClock, Email, Settings, Camera, Gallery, Stk, Mms, Calendar, Browser, Bluetooth, Calculator, Contacts, ...

Your Apps / Market Apps

App API

System Server

Power Manager, Mount Service, Activity Manager, Notification Manager, Package Manager, Location Manager, Battery Service, Search Service, Window Manager, Wallpaper Service, Status Bar, Headset Observer, Clipboard Service, ...

Binder

android.*

java.* (Apache Harmony)

Android Runtime / Dalvik / Zygote

JNI

Libs: Bionic / OpenGL / WebKit / ...

Init / Toolbox

Native Daemons

Hardware Support

Linux Kernel: Wakelocks / lowmem / binder / ashmem / ...

Image is taken from : https://events.linuxfoundation.org/.../abs2011_yaghmour_internals.ppt

References

- A Survey on Android vs. Linux, Frank Maker1 and Yu-Hsuan Chan

- Android Interprocess Communication By, Thorsten Schreiber

- Android Devlopers Team, http://developer.android.com/guide/basics/what-is-android.html [Online; accessed on 25-02-2013]

- Patrick Brady, https://sites.google.com/site/io/anatomy--physiology-of-an-android [Online; accessed on 25-02-2013]

References

- Jim Huang, http://www.slideshare.net /jserv/android-ipc-mechanism [Online; accessed on 25-02-2013]