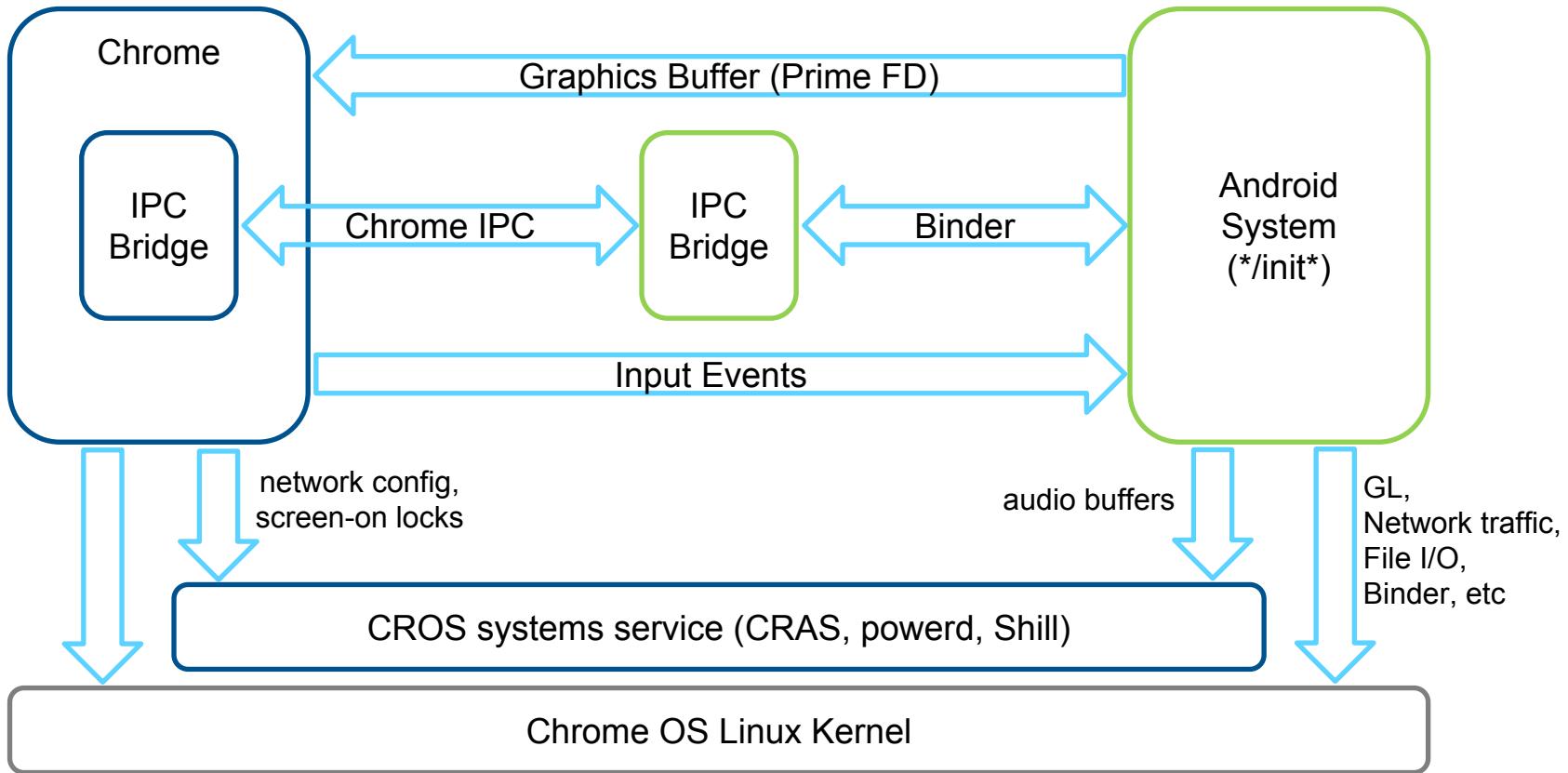


Running Android in a Container

How the play store runs on Chrome OS

How Android Runs On Chrome OS



Android Containerization



- Namespaces
- Device Access
- File System
- Input
- Audio/Video/Graphics
- Network

PID Namespace

- Allows Android's init to be PID 1

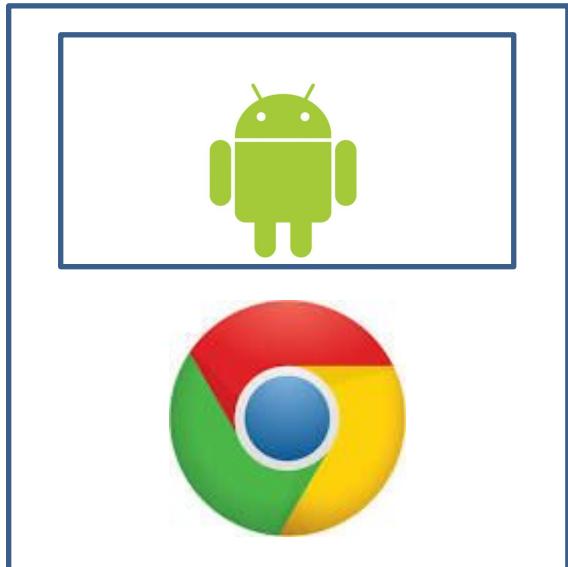
Chrome OS

```
cros# pstree -ap
init,1
| ... <snip> ...
|-minijail0,4514 -u cras -g cras -G -- /usr/bin/cras
|   `-cras,4865,cras
|   ... <snip> ...
|-session_manager,1744
|   |-chrome,1811,chronos
|   |   |-chrome,2372
|   |   ... <snip> ...
`-init,6057,android-root --second-stage
    |-adb,6143,657360 --root_seclabel=u:r:su:s0
    |   `-{adb},6144
    |-keystore,6140,656377 /data/misc/keystore
    |-mediaserver,6138,656373
    |   `-{mediaserver},6167
    |   ... <snip> ...
    |-servicemanager,6117,656360
    |-surfaceflinger,6118,656360
    |   `-{surfaceflinger},6125
... <snip> ...
```

Android Container

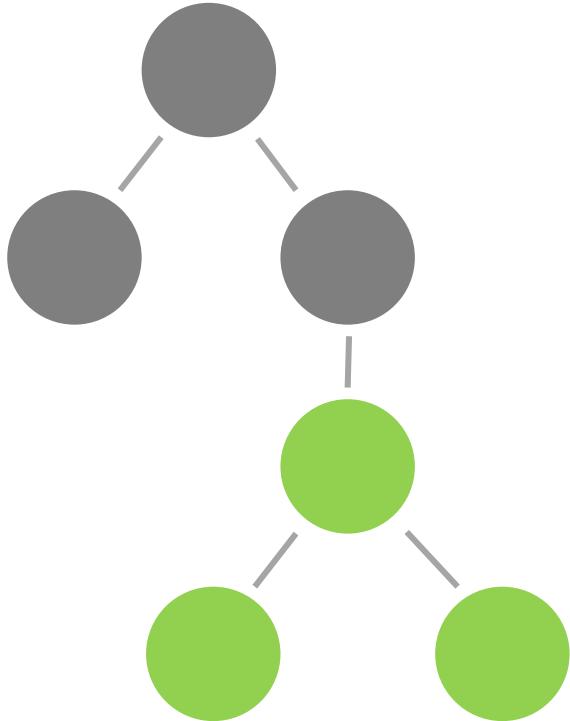
```
andoid# ps
USER      PID  PPID NAME
root      1     0   /init
shell     40    1   /sbin/adbd
keystore  37    1   /system/bin/keystore
media     35    1   /system/bin/mediaserver
system    17    1   /system/bin/servicemanager
system    18    1   /system/bin/surfaceflinger
... <snip> ...
```

User Namespace



- Allows Android to believe it is running as root
- Android actually runs as UID=655360
- Clone flag CLONE_NEWUSER
- Allows mounting of certain file systems

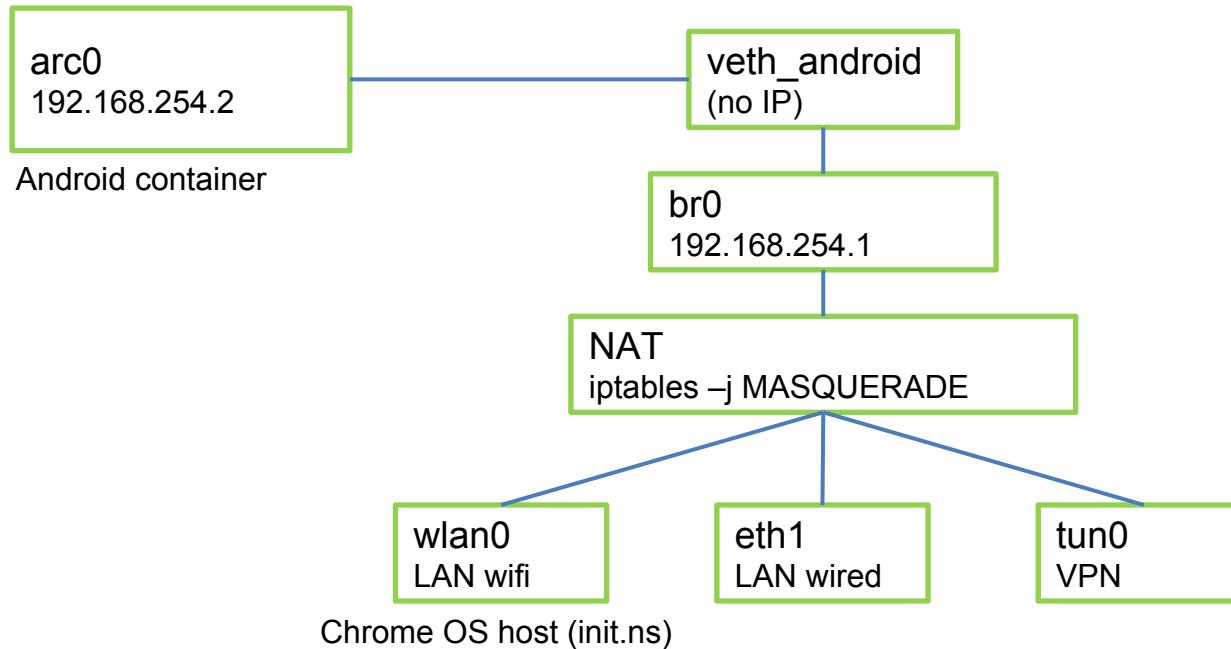
Mount Namespace



- Gives Android its own view of system mounts
- Pivot root to new location that Android sees as root
- Really a squash FS filesystem image
- Android can modify this mount namespace

Net Namespace

- Isolates Android network interfaces
- Give Android one bridged interface “arc0”
- Network configuration is handled outside the container by shill



cgroup Namespace

```
cros# tree /sys/fs/cgroup/cpu/
|-- <control files, e.g. cpu.shares>
|-- session_manager_containers
|   |-- android
|   |   |-- bg_non_interactive
|   |   |   |-- <control files, e.g. cpu.shares>
|   |   |   `-- tasks
|   |   |-- <control files, e.g. cpu.shares>
|   |   `-- tasks
|   |-- <control files, e.g. cpu.shares>
|       `-- tasks
`-- tasks
```



Android owned

```
android# tree /dev/cpuctl
|-- bg_non_interactive
|   |-- <control files, e.g. cpu.shares>
|   `-- tasks
|-- <control files, e.g. cpu.shares>
`-- tasks
```

Speed

Boot Time

Android Startup

Chrome
Performance

App Performance

Security



- Maintain Chrome OS security story
- Verity, root of trust
- Updates
- Cgroups
- Android Device Node Access
- Alt-syscall
- SELinux