# 1 组网环境

宿主机：SLES7.4 使用代理上网

Hypervisor：qemu-system-i386

启动环境：Android Studio

目标：Android 虚拟机桥接到宿主机物理网卡上，配置和宿主机同一个网段的地址，也通过代理上网

# 2 共享宿主机网卡

## 2.1 avd命令化（可忽略）

# 从android studio的avd manager中启动avd

# 从进程/proc/$PID/environ中还原环境变量设置

cat /proc/`ps -ef | grep "3.2\_HVGA\_slider\_ADP1\_API\_19" | grep -v grep | awk '{print $2}'`/environ | tr '\0' '\n' | sed 's/^/export /' | sed 's/=/="/' | sed 's/$/"/' > startEmulator.sh

# 还原启动脚本

cat /proc/`ps -ef | grep "3.2\_HVGA\_slider\_ADP1\_API\_19" | grep -v grep | awk '{print $2}'`/cmdline | tr '\0' ' ' >> startEmulator.sh

# 添加可写参数，root准备

echo "-writable-system" >> startEmulator.sh

# 关闭avd虚拟机窗口，清理残留avd进程

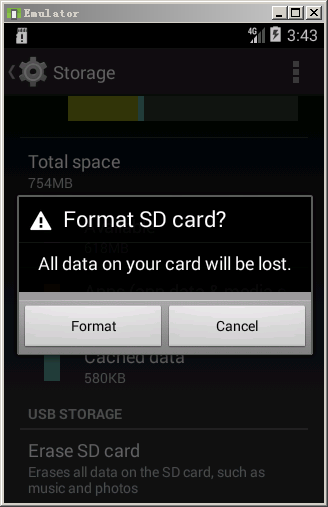
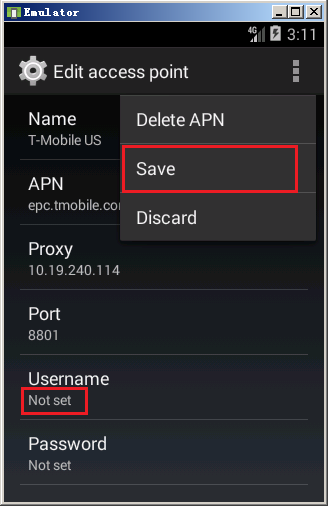
ps -ef | grep "3.2\_HVGA\_slider\_ADP1\_API\_19" | awk '{print $2}' | xargs kill -9

# 启动虚机

nohup ./startEmulator.sh &

## 2.2 设置代理

Settings 🡺 Wireless & Networks 🡺 More… 🡺 Mobile Networks 🡺 启用Data Enabled选项 🡺 Access Point Names 🡺 T-Mobile US 🡺 Edit access point 🡺 Proxy, Port Settings 🡺 Save



# 3 root虚拟机

# 启动虚拟机后查看系统adt server的进程，在找到adb的路径

**ps -ef | grep adb**

root 4125 1 0 08:59 ? 00:00:01 adb -L tcp:5037 fork-server server --reply-fd 4

**lsof -p 4125 | grep /adb**

adb 4125 root txt REG 253,0 2660025 5257536 /home/Android/Sdk/platform-tools/adb

# 将adb路径添加到path，添加内容过程略

vi ~/.bash\_profile

source ~/.bash\_profile

# 查看devices

**adb devices**

List of devices attached

emulator-5554 device

# 尝试修改系统文件，发现为readonly system

adb root

adb remount

adb shell

**cp /system/xbin/su /system/xbin/su.original**

# 下载supersu



# 解压到宿主机

unzip SuperSU-v2.11.zip

# 检查虚拟机的设备类型

**adb device -l**

List of devices attached

emulator-5554 device product:google\_sdk\_x86 model:Android\_SDK\_built\_for\_x86 device:**generic\_x86** transport\_id:5

# 选择x86目录下的su进行推送

# 进入SuperSU解压完成的目录里，推送

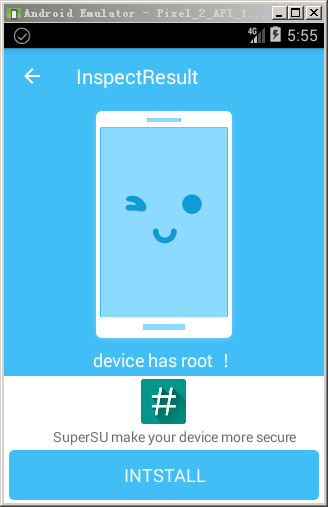
adb -e push ./x86/su /system/xbin/su

# 修改su的权限

adb -e shell

chmod 06755 /system/xbin/su

# 安装supersu.apk检查root结果



# 4 安装xposed

# 安装xposed

adb install de.robv.android.xposed.installer\_v33\_36570c.apk

# 在宿主机上解压缩

unzip de.robv.android.xposed.installer\_v33\_36570c.apk

# 推送XposedBridge.jar到虚拟机

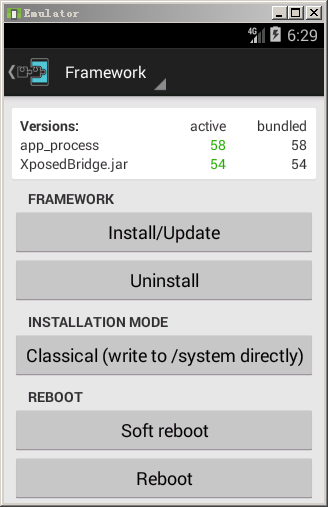
adb push assets/XposedBridge.jar /data/data/de.robv.android.xposed.installer/bin

# 推送app\_process到虚拟机

adb push assets/x86/app\_process\_xposed\_sdk16 /system/bin/app\_process

# 修改app\_process属性

adb shell "chmod 06755 /system/bin/app\_process"



# 5 Inspeckage