OPENSSH

zlib:

CC=arm-linux-gnueabihf-gcc ./configure --prefix=$PWD/_INSTALL
make
make install

```
cp zlib.3 /home/akenoxd/eltex/cross-comp/zlib-1.3.1/_INSTALL/share/man/man3
chmod 644 /home/akenoxd/eltex/cross-comp/zlib-1.3.1/_INSTALL/share/man/man3/zlib.3
rm -f /home/akenoxd/eltex/cross-comp/zlib-1.3.1/_INSTALL/lib/pkgconfig/zlib.pc
cp zlib.pc /home/akenoxd/eltex/cross-comp/zlib-1.3.1/_INSTALL/lib/pkgconfig
chmod 644 /home/akenoxd/eltex/cross-comp/zlib-1.3.1/_INSTALL/lib/pkgconfig/zlib.pc
rm -f /home/akenoxd/eltex/cross-comp/zlib-1.3.1/_INSTALL/include/zlib.h /home/akenoxd/eltex/cross
cp zlib.h zconf.h /home/akenoxd/eltex/cross-comp/zlib-1.3.1/_INSTALL/include
chmod 644 /home/akenoxd/eltex/cross-comp/zlib-1.3.1/_INSTALL/include/zlib.h /home/akenoxd/eltex/c
.h
akenoxd@DESKTOP:~/eltex/cross-comp/zlib-1.3.1$ cd _INSTALL/
akenoxd@DESKTOP:~/eltex/cross-comp/zlib-1.3.1/_INSTALL$ ls
include  lib  share
akenoxd@DESKTOP:~/eltex/cross-comp/zlib-1.3.1/_INSTALL$ cd lib/
akenoxd@DESKTOP:~/eltex/cross-comp/zlib-1.3.1/_INSTALL/lib$ file libz.
libz.a         libz.so        libz.so.1      libz.so.1.3.1
akenoxd@DESKTOP:~/eltex/cross-comp/zlib-1.3.1/_INSTALL/lib$ file libz.so.1.3.1
libz.so.1.3.1: ELF 32-bit LSB shared object, ARM, EABI5 version 1 (SYSV), dynamically linked, Bui
7946fbae, not stripped
akenoxd@DESKTOP:~/eltex/cross-comp/zlib-1.3.1/_INSTALL/lib$
```

Скопировали библиотеку в openssh, проверим:
./configure --prefix=$PWD/_install --host=arm-linux-gnueabihf --with-zlib=$PWD/zlib

```
checking for getpgrp... yes
checking if getpgrp accepts zero args... yes
checking for openssl... /usr/bin/openssl
configure: error: *** working libcrypto not found, check config.log
akenoxd@DESKTOP:~/eltex/cross-comp/openssh-portable$ ./configure --p
```

ошибки нет, пока все хорошо

openssl:

./Configure linux-generic32 --prefix=$PWD/_INSTALL
--cross-compile-prefix=arm-linux-gnueabihf- no-asm
make
make install

скопировали его в папку с openssh

ssh:

после множества проб и ошибок, получилось это:

./configure --prefix=$PWD/_install --host=arm-linux-gnueabihf --with-zlib=$PWD/zlib --with-ssl-dir=$PWD/ssl -disable-strip

```
OpenSSH has been configured with the following options:
                    User binaries: /home/akenoxd/eltex/cross-comp/openssh-portable/_install/bin
                  System binaries: /home/akenoxd/eltex/cross-comp/openssh-portable/_install/sbin
              Configuration files: /home/akenoxd/eltex/cross-comp/openssh-portable/_install/etc
                  Askpass program: /home/akenoxd/eltex/cross-comp/openssh-portable/_install/libexec/ssh-askpass
                     Manual pages: /home/akenoxd/eltex/cross-comp/openssh-portable/_install/share/man/manX
                         PID file: /var/run
  Privilege separation chroot path: /var/empty
            sshd default user PATH: /usr/bin:/bin:/usr/sbin:/sbin:/home/akenoxd/eltex/cross-comp/openssh-portable/_install/bin
                    Manpage format: doc
                       PAM support: no
                   OSF SIA support: no
                 KerberosV support: no
                   SELinux support: no
                   libedit support: no
                   libldns support: no
  Solaris process contract support: no
           Solaris project support: no
         Solaris privilege support: no
      IP address in $DISPLAY hack: no
          Translate v4 in v6 hack: yes
                 BSD Auth support: no
              Random number source: OpenSSL internal ONLY
             Privsep sandbox style: seccomp_filter
                   PKCS#11 support: yes
                  U2F/FIDO support: yes

             Host: arm-unknown-linux-gnueabihf
         Compiler: arm-linux-gnueabihf-gcc
    Compiler flags: -g -O2 -pipe -Wno-error=format-truncation -Wall -Wextra -Wpointer-arith -Wuninitialized -Wsign-compare -Wformat
-security -Wsizeof-pointer-memaccess -Wno-pointer-sign -Wno-unused-parameter -Wno-unused-result -Wimplicit-fallthrough -Wmisleading
-indentation -fno-strict-aliasing -D_FORTIFY_SOURCE=2 -ftrapv -fzero-call-used-regs=used -ftrivial-auto-var-init=zero -fno-builtin-
memset -fstack-protector-strong -fPIE
Preprocessor flags: -I/home/akenoxd/eltex/cross-comp/openssh-portable/ssl/include -I/home/akenoxd/eltex/cross-comp/openssh-portable
/zlib/include  -I/home/akenoxd/eltex/cross-comp/openssh-portable/openbsd-compat/include -D_XOPEN_SOURCE=600 -D_BSD_SOURCE -D_DEFAUL
T_SOURCE -D_GNU_SOURCE
      Linker flags: -L/home/akenoxd/eltex/cross-comp/openssh-portable/ssl/lib -L/home/akenoxd/eltex/cross-comp/openssh-portable/zli
b/lib  -Wl,-z,relro -Wl,-z,now -Wl,-z,noexecstack -fstack-protector-strong -pie
         Libraries:
     +for channels: -lcrypto  -lz
```

успешно сконфигурировался, собираем
-disable-strip – отключил, потому что при сборке использовался стрип под мою архитектуру x86, а не целевую ARM.

make
make install-nokeys # не генерируем ключи
с генерацией ключей выдавал ошибку, не проблема сгенерировать ключи уже на машине

после успешной установки проверяем:

```
akenoxd@DESKTOP:~/eltex/cross-comp/openssh-portable$ ls _install/*
_install/bin:
scp  sftp  ssh  ssh-add  ssh-agent  ssh-keygen  ssh-keyscan

_install/etc:
moduli  ssh_config  sshd_config

_install/libexec:
sftp-server  ssh-keysign  ssh-pkcs11-helper  ssh-sk-helper  sshd-auth  sshd-session

_install/sbin:
sshd

_install/share:
man
```

все собралось, архитектура правильная

```
akenoxd@DESKTOP:~/eltex/cross-comp/openssh-portable$ readelf -d _install/bin/ssh

Dynamic section at offset 0xa78b4 contains 30 entries:
  Tag        Type                         Name/Value
 0x00000001 (NEEDED)                     Shared library: [libcrypto.so.1.1]
 0x00000001 (NEEDED)                     Shared library: [libz.so.1]
 0x00000001 (NEEDED)                     Shared library: [libc.so.6]
 0x00000001 (NEEDED)                     Shared library: [ld-linux-armhf.so.3]
 0x0000000c (INIT)                       0x4d7c
```

ВАЖНО не забыть добавить в прошивку нужные библиотеки!
копируем все файлы в busybox, собираем initramfs

```
akenoxd@DESKTOP:~/eltex/busybox-1.37.0/_install$ ls -lha initramfs.cpio.gz
-rw-r--r-- 1 akenoxd akenoxd 26M Sep 14 16:57 initramfs.cpio.gz
akenoxd@DESKTOP:~/eltex/busybox-1.37.0/_install$
```

Получилось 26МБ, наверное это много. Скорее всего можно было некоторые библиотеки не копировать, но пока будет так. Запустим

QEMU_AUDIO_DRV=none qemu-system-arm -M vexpress-a9 -kernel zImage -dtb vexpress-v2p-ca9.dtb -initrd initramfs.cpio.gz -append "console=ttyAMA0 rdinit=/bin/ash" -nographic

Проблемы:

- нужно создать пользователя root
- нужна сеть
- нет конфига для ssh сервера
- нужно создать некоторые директории (dev, proc, var, root)
- нужно сгенерировать ключи (т.к. собирал без них)

Создадим пользователя и группу:

```
akenoxd@DESKTOP:~/eltex/busybox-1.37.0/_install/etc$ cat passwd
root:x:0:0:root:/root:/bin/ash
akenoxd@DESKTOP:~/eltex/busybox-1.37.0/_install/etc$ cat group
root:x:0:
nogroup:x:65534:
akenoxd@DESKTOP:~/eltex/busybox-1.37.0/_install/etc$
```

Чтобы появилась сеть, добавим при запуске новые флаги:

QEMU_AUDIO_DRV=none qemu-system-arm -M vexpress-a9 -kernel zImage -dtb vexpress-v2p-ca9.dtb -initrd initramfs.cpio.gz -append "console=ttyAMA0 rdinit=/bin/ash" -netdev user,id=net0,hostfwd=tcp::2222-:22,dns=8.8.8.8 -device virtio-net-device,netdev=net0 -nographic

```
# Basic configuration
Port 22
Protocol 2
ListenAddress 0.0.0.0

# Host keys
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Authentication
PermitRootLogin yes
PasswordAuthentication yes
PermitEmptyPasswords no
PubkeyAuthentication yes

# Security
StrictModes yes
MaxAuthTries 3
MaxSessions 5
LoginGraceTime 1m

# File paths
AuthorizedKeysFile .ssh/authorized_keys

Subsystem sftp /libexec/sftp-server
SshdSessionPath /libexec/sshd-session
SshdAuthPath /libexec/sshd-auth

# Performance and compatibility
UseDNS no
Compression no

# Logging
SyslogFacility AUTH
LogLevel INFO

# Network
ClientAliveInterval 60
ClientAliveCountMax 2
```

Возьмем базовый конфиг для сервера.
Выделенные пути прописал в конфиге, потому что по умолчанию он ожидал их по пути, куда они установились после make install (пути с хост машины).

Чтобы удобно поднять сеть и сгенерировать ключи, напишем небольшой скрипт:

```
mount -t proc proc proc

ip link set eth0 up
ip addr show eth0

ip addr add 10.0.2.15/24 dev eth0
ip route add default via 10.0.2.2

ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key -N ""
ssh-keygen -t ecdsa -f /etc/ssh/ssh_host_ecdsa_key -N ""
ssh-keygen -t ed25519 -f /etc/ssh/ssh_host_ed25519_key -N ""
```

ip-адреса перед этим узнал с помощью udhcpc

после всего этого соберем еще раз файловую систему
find . | cpio -o -H newc | gzip > initramfs.cpio.gz

и запустим

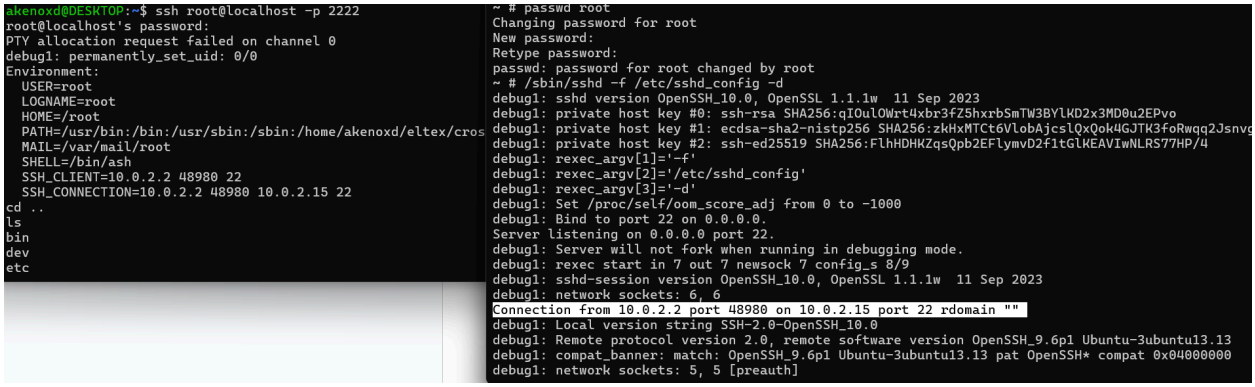
QEMU_AUDIO_DRV=none qemu-system-arm -M vexpress-a9 -kernel zImage -dtb vexpress-v2p-ca9.dtb -initrd initramfs.cpio.gz -append "console=ttyAMA0 rdinit=/bin/ash" -m 512 -netdev user,id=net0,hostfwd=tcp::2222-:22,dns=8.8.8.8 -device virtio-net-device,netdev=net0 -nographic

выполним скрипт, поднимем сеть, сгенерируем ключи

```
~ # sh init_net.sh
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 52:54:00:12:34:56 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::5054:ff:fe12:3456/64 scope link tentative
       valid_lft forever preferred_lft forever
Generating public/private rsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_rsa_key
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub
The key fingerprint is:
SHA256:qIOulOWrt4xbr3fZ5hxrbSmTW3BYlKD2x3MD0u2EPvo root@(none)
The key's randomart image is:
+---[RSA 3072]----+
|         ....    |
```

```
~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:00:12:34:56
          inet addr:10.0.2.15  Bcast:0.0.0.0  Mask:255.255.255.0
          inet6 addr: fe80::5054:ff:fe12:3456/64 Scope:Link
          inet6 addr: fec0::5054:ff:fe12:3456/64 Scope:Site
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:221 errors:0 dropped:0 overruns:0 frame:0
          TX packets:143 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:25473 (24.8 KiB)  TX bytes:21400 (20.8 KiB)
```

зададим пароль для root
запускаем сервер
и пробуем подключиться



Работает!