



## paomadi的专栏

微信:MHB360



## tcpdump交叉编译及使用

2013年07月23日 22:34:25

阅读数：5904

## 第一步.下载

官方网站:<http://www.tcpdump.org/>

需要下载libpcap包和tcpdump包

我下载的版本是:libpcap-1.4.0.tar.gz和tcpdump-4.4.0.tar.gz

## 第二步.编译libpcap包

## 2.1 解压

```
[cpp]
1. tar -zxvf libpcap-1.4.0.tar.gz
```

## 2.2 进入解压目录

```
[cpp]
1. cd libpcap-1.4.0/
```

## 2.3 配置生成makefile文件

```
[cpp]
1. CC=arm-none-linux-gnueabi-gcc ac_cv_linux_vers=2 ./configure --host=arm-linux --with-pcap=linux
```

(CC是交叉工具链)

## 2.4 编译

```
[cpp]
1. make
```

## 第三步.编译tcpdump包

## 3.1 解压

```
[cpp]
1. tar -zxvf tcpdump-4.4.0.tar.gz
```

## 3.2 进入解压目录

```
[cpp]
1. cd tcpdump-4.4.0/
```

## 3.3 配置生成makefile文件

```
[cpp]
1. CC=arm-none-linux-gnueabi-gcc ac_cv_linux_vers=2 ./configure --host=arm-linux --with-pcap=linux
```

(CC是交叉工具链)

## 3.4 编译

[cpp]

1. make

#### 第四步:测试体验

##### 4.1 拷贝

将tcpdump-4.4.0目录下的tcpdump文件拷贝到目标板文件系统/bin目录下

##### 4.2 简介

tcpdump 是一个运行在命令行下的嗅探工具。它允许用户拦截和显示发送或收到过网络连接到该计算机的TCP/IP和其他数据包。tcpdump能够分析网络行为, 性能和应用产生或接收网络流量。它支持针对网络层、协议、主机、网络或端口的过滤, 并提供and、or、not等逻辑语句来帮助你去掉无用的信息, 从而使用户能够进一步找出问题的根源。

##### 4.3 快速体验

root权限直接运行tcpdump不带任何参数,将监视第一个网络界面上所有流过的数据包.(ping一下或打开网页试试)

##### 4.4 命令参数简介

tcpdump --help 显示命令格式

[cpp]

```
1. Usage: tcpdump [-aAdDefIKlLnNOpqRStuUvxX] [ -B size ] [ -c count ]
2.           [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
3.           [ -i interface ] [ -M secret ] [ -r file ]
4.           [ -s snaplen ] [ -T type ] [ -w file ] [ -W filecount ]
5.           [ -y datalinktype ] [ -z command ] [ -Z user ]
6.           [ expression ]
```

##### 4.4 命令参数细分

[cpp]

```
1. -a 将网络地址和广播地址转变成名字;
2. -d 将匹配信息包的代码以人们能够理解的汇编格式给出;
3. -dd 将匹配信息包的代码以c语言程序段的格式给出;
4. -ddd 将匹配信息包的代码以十进制的形式给出;
5. -e 在输出行打印出数据链路层的头部信息;
6. -f 将外部的Internet地址以数字的形式打印出来;
7. -l 使标准输出变为缓冲行形式;
8. -n 不把网络地址转换成名字;
9. -t 在输出的每一行不打印时间戳;
10. -v 输出一个稍微详细的信息,例如在ip包中可以包括ttl和服务类型的信息;
11. -vv 输出详细的报文信息;
12. -c 在收到指定的包的数目后, tcpdump就会停止;
13. -F 从指定的文件中读取表达式,忽略其它的表达式;
14. -i 指定监听的网络接口;
15. -r 从指定的文件中读取包(这些包一般通过-w选项产生);
16. -w 直接将包写入文件中,并不分析和打印出来;
17. -T 将监听到的包直接解释为指定的类型的报文,常见的类型有rpc(远程过程调用)和snmp(简单网络管理协议);
```

##### 4.5 具体使用的外部链接

man手册:[http://www.tcpdump.org/tcpdump\\_man.html](http://www.tcpdump.org/tcpdump_man.html)

超级详细Tcpdump 的用法:<http://bbs.chinaunix.net/forum.php?mod=viewthread&tid=2011433>

Linux tcpdump命令详解:<http://www.cnblogs.com/ggjucheng/archive/2012/01/14/2322659.html>

wireshark软件官方下载页:<http://www.wireshark.org/download.html>

文章标签: tcpdump 交叉编译 移植 libpcap tcpdump for arm

个人分类: linux应用层

想对作者说点什么?

我来说两句

## tcpdump交叉编译

移植需要libpcap和tcpdumplibpcap编译: config ./configure --host=arm-linux CC=arm-none-linux-gnueabi-gcc --wi...

 lanyou1900 2016-03-28 13:38:21 阅读数：805


## TCPDUMP交叉编译

下面介绍一下具体过程。1.在<http://www.tcpdump.org>下载libpcap-1.0.0.tar.gz和tcpdump-4.0.0.tar.gz两个文件。2.将这两个文件放在/home下...

 qiaoliang328 2009-09-25 14:07:00 阅读数：8335

## 编译libpcap和tcpdump

编译libpcap mkdir installed 注释掉下面的几行，否则会编译不过。5436 #zw-del if test -z "\$with\_pcap" && test "\$cros...

 k7arm 2017-04-20 15:39:09 阅读数：763

## NDK交叉编译tcpdump实现安卓抓包

下面介绍一下具体过程。1.Git clone libpcap和tcpdump两个项目。git clone <https://github.com/the-tcpdump-group/tc...>

 xuqiang1993 2017-03-27 16:09:11 阅读数：988

## 交叉编译tcpdump

交叉编译TCPDUMP 编译平台 PC:ubuntu-14.04 Cross-tool:arm-none-linux-gnueabi-gcc 4.8.3 Target:Atmel9260 ...

 linux\_embedded 2016-03-05 11:33:51 阅读数：1407

## tcpdump交叉编译方法

本文档描述源代码版本为最新的：libpcap-1.8.1以及tcpdump-4.9.0

 litao31415 2017-03-19 23:33:17 阅读数：451


## tcpdump交叉编译和一些简单命令

下面介绍一下具体过程。1.在<http://www.tcpdump.org>下载libpcap-1.0.0.tar.gz和tcpdump-4.0.0.tar.gz两个文件。2.将这两个文件放在/h...

 petershina 2013-05-25 14:20:52 阅读数：3384

## tcpdump工具编译记录

本文主要记录tcpdump，一个linux平台的抓包工具在arm平台上的编译方法，不涉及其使用。下载tcpdump工具，地址：<http://www.tcpdump.org/> 需要下载2个压缩包：...

 subfate 2013-10-20 10:46:15 阅读数：1829

## tcpdump的源码包安装方法&抓取HTTP包的方法

背景：外包把代码放到我们的测试机上，有可能出现这样那样的调用问题，尽管前面说过要注意host配置的问题并记录，但是往往出现在上到测试机时，忘记了，于是用下tcpdump来抓包，可以实现有效的对其跨...

 kalman2008 2015-05-22 11:30:29 阅读数：2474

## ini文件解析c库(iniparser)

一.交叉编译ini解析库 1.官方网站<http://ndevilla.free.fr/iniparser> 下载iniparser-3.1.tar.gz 2.解压 tar -zxvf iniparser...

 paomadi 2013-07-27 22:01:26 阅读数：9361

## C语言ini形式配置文件解析库——iniparser

C语言ini形式配置文件解析库——iniparser最近在做一个嵌入式设备开发项目，主要使用C语言，当碰到配置文件解析时遇到了问题，由于水平太差，自己拿链表改改写了一个，发现并不能很好地满足项目需求，...

LANBO 2016-02-22 18:35:41 阅读数：770

IniParser+win7解析配置文件INI

最近做实验用到了ini配置文件，读取过程高端到我不太敢相信做实验的人自己会写一个用键值对来存取文件的库，后来一查原来Iniparser是一个比较通用的读取ini配置文件的库，看起来我还是知道的太少了....

iloveayu 2017-08-05 17:45:55 阅读数：169

INI file and Iniparser

1、概述：INI file是配置文件，保存的是数据，主要是系统或者软件的配置信息。Iniparser则是对INI file的解析或者操作(get,set,delete 等等)。下面分别就I...

fivedoumi 2014-03-27 21:20:46 阅读数：893

C语言配置文件解析库——iniparser

C语言配置文件解析库——iniparser 前言：在对项目的优化时，发现Linux下没有专门的供给C语言使用的配置文件函数，于是搜索到了iniparser库，可以像那些面向对象语言一样，使用in...

linyangspring 2017-03-03 16:30:54 阅读数：196

使用iniparser 处理INI文件

使用iniparser 处理INI文件，详细代码如下。#include #include #include #include #include "iniparser.h" ...

tody\_guo 2013-12-07 22:25:44 阅读数：4529

tcpdump交叉编译和使用

#!/bin/sh #export LDFLAGS="-L\${PREFIX\_PATH}/lib -L\${PREFIX\_PATH}/usr/lib -ldl -lm" #export CC=\$GCC ...

hpp205 2015-10-15 17:31:55 阅读数：284

编译Arm板上的tcpdump

编译在开发板上运行的tcpdump 在板上调试网络通信不方便，所以下载tcpdump编译在板上运行，这样方便多了。linux: ubuntu 10.0.4 板是海思芯片的板 ...

jhting 2014-08-29 16:53:47 阅读数：2588

移植tcpdump到arm linux

以前已经移植过libpcac库，现在可以tcpdump 1、http://www.tcpdump.org/#latest-release下载tcpdump源码 2、解压：tar -xf tcp...

wanghelou123 2014-12-16 18:35:45 阅读数：1518

arm路由系统下可用的tcpdump抓包工具

2013年12月25日 下载

tcpdump for Arm

2017年09月19日 下载

个人资料



paomadi

关注

原创

86

粉丝

322

喜欢

3

评论

65

等级： 博客 5

访问： 30万+

积分： 4125

排名： 9594

最新文章

三轴陀螺仪MPU3050驱动解析

三轴加速度传感器bma150驱动解析

exec函数族

动态域名ddns开源客户端inadyn的移植

深入解析linux下rtc架构

博主专栏



linux设备驱动

阅读量： 157077

41 篇

个人分类

linux设备驱动

51篇

linux应用层

28篇

linux内核相关

16篇

linux其他

5篇

android应用层

4篇

展开

归档

2014年3月

2篇

2014年1月

1篇

2013年11月

3篇

2013年10月

2篇

2013年9月

4篇

展开

热门文章

ini文件解析c库(iniparser)

阅读量： 9356

【android】根据init.rc启动action和service

阅读量：9089

让qt应用程序支持触摸

阅读量：8814

uvc摄像头代码解析2

阅读量：7991

linux网络设备—PHY

阅读量：7504

最新评论

让qt应用程序支持触摸

weixin\_41540461：630117403@qq.com 最近写了一个白板，但是最终要在触摸屏上实现，所以想看看博主的...

让qt应用程序支持触摸

weixin\_35741448：请问能发份源码参考下吗？13727539957@163.com 万分感谢~

让qt应用程序支持触摸

xbdh：前辈能发给源码给我吗？17858936224@163.com

alsa音频架构3-pcm

kangear：[code=cpp] //capture专用命令 SNDRV\_PCM\_IOCTL\_WRITEI...

uvc摄像头代码解析4

ykeastronaut：大侠，请教一下，我正在开发一种基于H264编码的UVC 摄像头，参考的规范是uvc1.1，在uvc...

联系我们



请扫描二维码联系客服  
✉ webmaster@csdn.net  
☎ 400-660-0108  
👤 QQ客服 🗨 客服论坛

关于 招聘 广告服务 百度  
©1999-2018 CSDN版权所有  
京ICP证09002463号

经营性网站备案信息  
网络110报警服务  
中国互联网举报中心  
北京互联网违法和不良信息举报中心